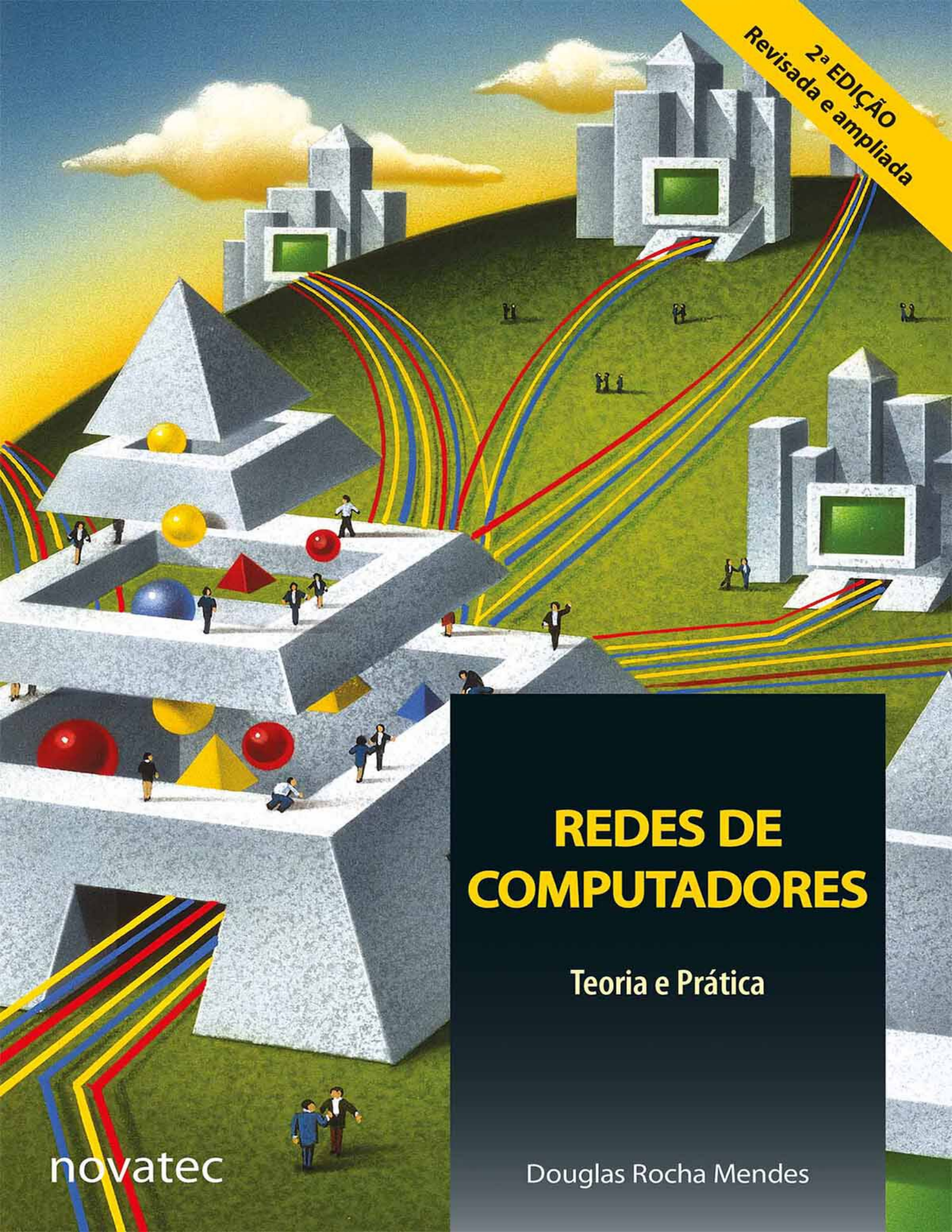

2ª EDIÇÃO
Revisada e ampliada
REDES DE COMPUTADORES
Teoria e Prática
Douglas Rocha Mendes
novatec

# Redes de Computadores
# Teoria e Prática
# 2ª EDIÇÃO

**Douglas Rocha Mendes**

Novatec

Editor: Rubens Prates
Assistente editorial: Priscila A. Yoshimatsu
Revisão: Patrizia Zagni
Editoração Eletrônica: Camila Kuwabata
Capa: Camila Araújo e Marcelo Nardeli

ISBN do ebook: 978-65-86057-16-4

ISBN do impresso: 978-85-7522-368-0

Novatec Editora Ltda.
Rua Luís Antônio dos Santos 110
02460-000 – São Paulo, SP – Brasil
Tel.: +55 11 2959-6529
E-mail: novatec@novatec.com.br
Site: www.novatec.com.br
Twitter: twitter.com/novateceditora
Facebook: facebook.com/novatec
LinkedIn: linkedin.com/in/novatec

*Dedico a toda a minha família e amigos, que ajudaram e incentivaram o desenvolvimento deste projeto.*

# Sumário

# Agradecimentos

Primeiramente, gostaria de agradecer a Deus por ter me permitido escrever a segunda edição deste livro. Foi o grande sucesso da primeira edição que motivou a preparação desta segunda edição bem mais completa, com novos capítulos e atualizações envolvendo novas tecnologias e protocolos. Por fim, gostaria de agradecer a toda a minha família, Letícia Zanetti, Davi Zanetti Rocha Mendes e Pedro Zanetti Rocha Mendes, por terem acompanhado e incentivado esta nova edição. Agradeço, ainda, à minha avó Ermantina de Almeida Cabrera por ter me acompanhado, mesmo a distância, sempre orando e pedindo a bênção da minha família.

# Sobre o autor

Douglas Rocha Mendes é coordenador e professor do curso de Sistemas de Informação do Instituto Superior do Litoral do Paraná (Isulpar), onde ministra as disciplinas de Java, Gerenciamento de Projetos e Redes de Computadores. Atua também como coordenador de Pós-graduação da Faculdade de Ciências Sociais e Aplicadas do Paraná (Facet), atualmente dos cursos de Desenvolvimento de Sistemas Web e Mobile, Gestão da Tecnologia da Informação e Engenharia de Software. É palestrante sobre os temas Internet sobre GPON e Infraestrutura para o Transporte do IPTV.

Atualmente, é analista de Suporte na Copel Telecom, atuando com gerência e suporte a redes locais e remotas, envolvendo os principais protocolos e tecnologias de rede, como BGP, OSPF, MPLS, Internet e GPON.

Foi analista de sistemas da Copel atuando com programação Java nas plataformas JSE/JEE, gestão de projetos e com a ferramenta DataStage. Foi instrutor do HSBC de 2004 a 2009, sendo responsável por treinamentos nas áreas de Gestão de Projetos, Análise e Design Orientado a Objetos, Use Case, Linguagens de Programação (C, C++ e Java) e Programação Shell Script.

De 1998 a 2004, atuou como analista de sistemas no HSBC, desenvolvendo aplicações bancárias e de seguros em Java e C++. Em 2007, publicou o livro *Redes de Computadores – Teoria e Prática*; em 2009, *Programação Java com Ênfase em Orientação a Objetos* e o artigo "Analisando Estratégias de Herança para Mapeamento Objeto-Relacional com JPA", na edição 37 da revista MundoJ. Em 2011, publicou o livro *Programação Java em Ambiente Distribuído*.

Foi professor da Pós-graduação da Universidade Positivo, da Pontíficia Universidade Católica do Paraná e da Universidade Federal do Paraná. Atuou nos cursos de Engenharia de Software e Desenvolvimento Java. Foi professor nas Faculdades Sociedade

Paranaense de Ensino e Informática (Spei), Opet e Educacional Araucária (Facear). Atuou como analista de suporte em uma rede de lojas situada na região Sul e no estado de São Paulo de 1994 a 1998.

É bacharel em Informática pela Universidade Positivo e concluiu o mestrado em Telemática na UTFPR em 2002. Nesse mesmo ano, publicou o artigo *Bandwidth Fairness of a Single Rate Three Color Marker Algorithm Implementation* no 8o Congresso Internacional da *International Conference on Communication Systems* (IEEE). Pode ser contatado pelo email *dmendes@novatec.com.br*.

# Prefácio

A motivação para escrever este livro surgiu ao lecionar a disciplina de Redes de Computadores no curso de Sistemas de Informação, durante o curso de mestrado e as atividades desenvolvidas como analista de suporte na Copel Telecom.

Ao elaborar este livro, tive em mente as faculdades de bacharelado em Sistemas de Informação, Ciência da Computação e cursos de tecnologia em redes de computadores e afins. Em razão de a teoria de redes de computadores apresentar inúmeros conceitos novos aos estudantes, minha preocupação foi elaborar uma linguagem simples e prática que permita a fácil leitura e o aprendizado do estudante.

Nesse contexto, procurei abordar todos os assuntos importantes para a formação de um profissional de Sistemas de Informação que, mesmo que não atue diretamente na área de redes, possa basear-se neste livro para tomar decisões sobre softwares e protocolos que utilizará.

Espero que este livro seja uma ferramenta útil para os que procuram se aperfeiçoar na área de redes de computadores e telecomunicações.

CAPÍTULO 1

# Introdução às redes de computadores

O capítulo 1 apresenta uma introdução às redes de computadores explanando sua evolução, os termos utilizados e as principais entidades de padronização. Também aborda as vantagens e desvantagens das redes de computadores, seus componentes, o histórico da formação da internet, a definição de termos populares, além de uma apresentação dos modelos de referências OSI e TCP/IP.

## 1.1 Introdução

As redes de computadores estabelecem a forma-padrão de interligar computadores para o compartilhamento de recursos físicos ou lógicos. Esses recursos podem ser definidos como unidades de CD-ROM, diretórios do disco rígido, modems, ONUs GPON, impressoras, scanners, pendrive etc. Saber definir que tipo de rede e que sistema operacional deve ser utilizado, bem como efetuar a montagem desse tipo de ambiente, é um pré-requisito para qualquer profissional de informática que pretenda uma boa colocação no mercado de trabalho.

A tecnologia de rede chegou ao estágio da massificação no momento em que os computadores começaram a se espalhar pelo mundo comercial, quando programas complexos multiusuários começaram a ser desenvolvidos (navegação na web, email, banco de dados, redes sociais, blogs, Twitter, YouTube). Os componentes para sua montagem (hardware, software, infraestrutura e acessórios) podem ser encontrados em qualquer loja especializada em informática, sendo esses elementos procedentes de dezenas de fabricantes. Esse processo gerou um fato interessante: o baixo custo dos componentes proporcionado pela concorrência entre os fabricantes em um primeiro estágio e o baixo valor final proporcionado pela concorrência entre as diversas lojas de

informática. Aliada a tudo isso, a evolução tecnológica simplificou o processo, o que torna o trabalho técnico mais fácil e com mais possibilidades. No entanto, nem sempre o custo e a interoperabilidade dos equipamentos de redes estiveram à disposição dos administradores de redes de forma barata e flexível.

No início da concepção das redes, cada fabricante possuía sua forma de trabalho e sua própria linha de desenvolvimento de tecnologia. Como exemplo, podemos citar a placa de rede do fabricante X que só poderia ser conectada a uma placa do mesmo fabricante, por um meio físico (fio) também desenvolvido por ele. Caso houvesse problemas relacionados a preços ou relacionamento entre as partes, a empresa detentora dos equipamentos não teria como procurar outra opção. A única alternativa existente naquela época era substituir todo o parque de hardware e software instalado por equipamentos de outro fabricante. Dessa forma, o problema não era resolvido, mas contornado, e os prejuízos eram grandes.

A fim de resolver essa situação de incompatibilidade entre fabricantes, na década de 1970 a ISO (International Organization for Standardization) criou um padrão universal para a troca de informações entre e dentro das redes e também por meio de fronteiras geográficas. Esse padrão para arquitetura de redes era o modelo de referência OSI, estabelecido em sete camadas, o qual incentivou a padronização de redes de comunicação e controle de processos distribuídos. O fato de ser desenhado em sete camadas se dá em virtude de o modelo da IBM, o modelo de referência SNA, ter essas características. No início das redes, a IBM era uma das maiores empresas ligadas a essa área e uma das integrantes do processo de padronização das redes e de criação do modelo de referência OSI.

No que diz respeito ao padrão OSI, é importante ressaltar o longo tempo para a sua definição. Durante esse período, o Departamento de Defesa do Governo dos Estados Unidos (DoD – *Department of Defense*) desenvolveu o modelo de referência TCP/IP, com o objetivo principal de manter, ao menos em parte, seus equipamentos conectados. Esse padrão ficou conhecido como o modelo de

referência TCP/IP, estabelecido em quatro camadas. Em razão de alguns fabricantes iniciarem o desenvolvimento de equipamentos seguindo esse padrão, quando o padrão OSI foi finalizado, muitos equipamentos já estavam funcionando no modelo de referência denominado TCP/IP. Logo, o modelo de referência OSI nasceu e não se tornou um padrão da indústria de rede. As instituições acadêmicas não aceitaram substituir seus equipamentos com o argumento de que isso demandaria alto custo e muito tempo para treinamento e novas configurações.

O nome TCP/IP refere-se a uma pilha de protocolos que tem como principais protocolos o TCP (*Transmission Control Protocol*) e o IP (*Internet Protocol*), além de outros protocolos conhecidos, como ARP, RARP, UDP e ICMP. Assim, não se pode confundir a pilha de protocolos TCP/IP com os protocolos TCP e o protocolo IP, que possuem características de funcionamento bem distintas um do outro. A internet que surgiu baseada nas redes de instituições acadêmicas dos Estados Unidos é um bom exemplo de rede que utiliza a pilha de protocolos TCP/IP.

Apesar do esforço da ISO em padronizar os equipamentos de rede, atualmente voltamos a enfrentar certa dificuldade na interoperabilidade de equipamentos, como na plataforma GPON (Gigabit Passive Optic Network). Essa tecnologia de transporte de dados (mesmo nível do padrão Ethernet) oferece um canal de controle (OMCI – ONT *Management and Control Interface*) para a configuração remota das ONUs (*Optical Network Unit*). Esse canal normalmente não funciona adequadamente quando utilizamos OLTs (*Optical Line Terminal*) e ONUs de fabricantes diferentes. Esse padrão foi padronizado pelo ITU-T e o abordaremos com mais detalhes no capítulo 17. O GPON representa uma solução para o acesso à internet em alta velocidade a um baixo custo.

Na plataforma GPON, podemos nos referir ao CPE (*Customer Premises Equipment*) instalado no cliente de duas formas, ONU (*Optical Network Unit*) ou ONT (*Optical Network Terminal*). A ONU, como o próprio nome indica, é uma unidade óptica de rede que, ao ser instalada no endereço do cliente, atua como um equipamento

intermediário, e após a ONU, o cliente conecta um switch ou roteador para, então, estender para a rede interna. Esse conceito aplica-se a redes instaladas em ambientes empresariais. A ONT, como o próprio nome indica, é um terminal óptico de rede, ou seja, ao ser instalada no endereço do cliente, atua como um equipamento terminal, e nele o cliente conecta seus computadores e celulares.

## 1.2 Histórico da internet

No final da década de 1960, a Agência de Projetos de Pesquisas Avançadas do Departamento de Defesa dos Estados Unidos (ARPA – *Department of Defense's Advanced Reserch Projects Agency*), mais tarde chamada de DARPA, começou a consolidar uma rede experimental de computadores de longa distância, denominada ARPANET, que se espalhou pelos Estados Unidos. O objetivo original da ARPANET era permitir aos fornecedores do governo compartilhar caros e também escassos recursos computacionais. Inicialmente, a ARPANET permitia que os laboratórios de pesquisa americanos [Universidade da Califórnia (UCLA), em Los Angeles; Universidade de Utah, em Salt Lake City; Universidade da Califórnia, em Santa Barbara (UCSB); Stanford Research Institute (SRI), em Stanford] trocassem informações. Desde o início, entretanto, usuários da ARPANET também usaram a rede para colaboração. Essa colaboração abrangia desde compartilhamento de arquivos e programas e troca de mensagens via correio eletrônico (email) até desenvolvimento conjunto e pesquisas usando computadores remotos compartilhados.

O conjunto de protocolos do modelo de referência TCP/IP foi desenvolvido no início da década de 1980 e rapidamente se tornou protocolos de rede na ARPANET. A inclusão do conjunto de protocolos sobre o popular sistema operacional *BSD Unix* (gratuito para universidades) de Berkeley, na Universidade da Califórnia, foi instrumento de democratização entre as redes. Esse sistema operacional ofereceu às empresas a possibilidade de conectar-se à rede com baixo custo. Muitos dos computadores conectados à ARPANET estavam também conectados a redes locais, de modo

que, em pouco tempo, os outros computadores das redes locais também passaram a se comunicar via ARPANET. A rede cresceu, passando de um punhado de computadores a dezenas de milhares de computadores. A ARPANET original tornou-se o backbone (espinha dorsal) de uma confederação de redes locais e regionais baseadas no modelo de referência TCP/IP. Atualmente, essa rede é conhecida como internet.

Em 1988, entretanto, o DARPA decidiu que o experimento estava terminado. Assim, o Departamento de Defesa começou a desmantelar a ARPANET. Uma outra rede, criada pela Fundação Nacional de Ciência (National Science Foundation) e chamada de NSFNET, substituiu a ARPANET como backbone. Mesmo mais recentemente, no primeiro semestre de 1995, a internet sofreu uma transição do uso da NSFNET como backbone para usar múltiplos backbones comerciais, passando a trafegar seus dados sobre linhas de longa distância da MCI, Sprint e antigas redes comerciais, como PSINet e Alternet. A figura 1.1 apresenta a topologia física da internet, a qual é constituída por uma série de redes menores, interligadas por roteadores, funcionando logicamente como uma única rede.

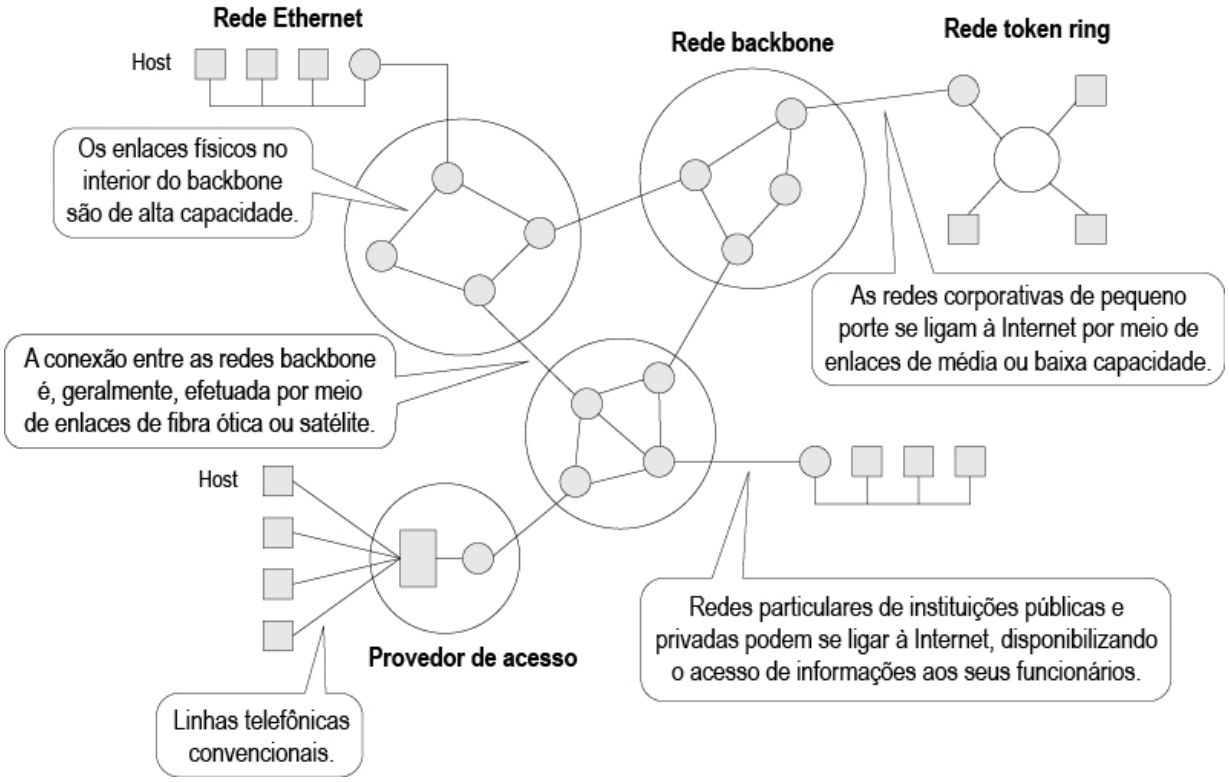



*Figura 1.1 – Topologia física da internet e sua estrutura genérica.*

## 1.3 Internet

O termo “internet”é muito utilizado para descrever uma rede em que tudo se pode e tudo se consegue. Essa popularização está relacionada à sua ampla utilização por usuários com ou sem experiência na área de Informática, ou seja, qualquer pessoa com um computador conectado a um modem xDSL ou uma ONU GPON (*Gigabit Passive Optic Network*), com uma identificação e uma senha válida, poderá navegar pela rede fechando uma sessão PPPoE (*Point-to-Point over Ethernet*) entre o seu CPE (*Customer Premises Equipment*) e o equipamento da operadora. A internet trouxe a todas as áreas a possibilidade de compartilhar conhecimento e muito entretenimento.

Na internet, mesmo os que não estão adaptados ao mundo da informática devem ser capazes de diferenciar e entender alguns dos termos utilizados pelos programas especializados, isso porque, no momento em que se conectam a uma rede, podem se ver diante das seguintes dúvidas: o que significa URL, WWW, HTTP, FTP,

Internet 2, entre outros termos usuais. A seguir, discorreremos sobre alguns desses termos, ao passo que outros serão comentados no decorrer deste livro.

### 1.3.1 Internet, Intranet e Extranet

A Internet refere-se à rede que começou sua vida, como a ARPANET, e continua como, grosseiramente falando, a confederação de todas as redes TCP/IP interligadas direta ou indiretamente. Nessa interligação, temos os backbones TCP/IP comerciais norte-americanos, brasileiros, europeus, asiáticos, redes TCP/IP regionais, redes TCP/IP governamentais, sendo todas interconectadas por circuitos digitais de alta velocidade. Existem ainda redes locais de corporações conhecidas como Intranets ou Extranets.

Intranet é uma rede de propriedade privada, construída sobre o modelo de referência TCP/IP, que disponibiliza os mesmos serviços de comunicação da rede mundial Internet. Utiliza os protocolos da família TCP/IP e oferece serviços similares aos da Internet, como servidor de páginas, servidor DNS, HTTP ou, ainda, servidor de email. Uma rede Intranet não tem necessariamente relação com a Internet, pois seus serviços são acessíveis apenas a funcionários com acesso à rede local interna (LAN).

Uma Extranet é uma rede geograficamente distribuída (WAN). Sua construção utiliza enlaces de comunicação privados e protocolos de comunicação do modelo de referência TCP/IP. Além disso, oferece serviços similares aos da rede Internet e é geralmente usada por corporações para interligar várias sedes que utilizam Intranets.

A figura 1.2 apresenta, de forma clara, a relação entre Internet, Intranet e Extranet:

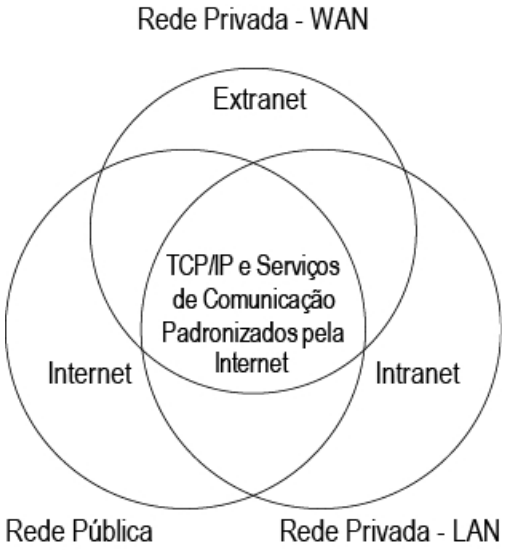



*Figura 1.2 – Relação entre Internet, Intranet e Extranet.*

## 1.3.2 Função do WWW

O principal serviço da Internet é a World Wide Web, a parte multimídia da rede. É na web que você pode ler jornais eletrônicos, fazer compras em shoppings virtuais, acessar redes sociais e consultar bancos de dados. Além dessas facilidades, a web ainda permite que um usuário acesse diversos documentos por meio dos hiperlinks disponíveis nas páginas escritas em HTML (linguagem de desenvolvimentos de páginas).

Em razão de haver uma grande variedade de itens disponíveis na web, é preciso utilizar serviços de catalogação para encontrar as informações que você esteja procurando. A web funciona basicamente com dois tipos de programas: os clientes e os servidores. O cliente é o programa utilizado pelos usuários para manipular as páginas apresentadas pelo *browser* (por ex., Internet Explorer, Google Chrome ou Mozilla Firefox), enquanto os servidores são responsáveis por armazenar e permitir o acesso ao conteúdo da rede. Neste livro, chamaremos o programa cliente de navegador (em inglês, *browser*). O que o navegador faz é requisitar um arquivo para um servidor e, se a informação pedida realmente estiver armazenada nesse servidor, o pedido será enviado de volta e mostrado na tela do navegador, após ter sido interpretado.

A informação na web é organizada na forma de páginas, que podem conter textos, imagens, sons e, ainda, vídeos animados. Além disso, as páginas da web podem ser interligadas, formando o que se chama de um conjunto de hipertextos. Assim, é possível, por exemplo, que um trabalho de faculdade faça referência direta a um texto que serviu de base para a sua composição. O leitor interessado na fonte de pesquisa pode saltar imediatamente para o texto original. Dessa forma, qualquer documento pode levar a um outro texto que também esteja disponível na rede. O fato de ser possível acessar documentos em diversos sites espalhados pelo mundo deu origem ao termo *World Wide Web*, que significa teia de alcance mundial.

## 1.3.3 O que significa URL

Já que definimos o significado da palavra Internet, vamos então aprender como encontrar os recursos disponíveis nessa rede. Cada endereço aponta para um determinado lugar e só para esse lugar, de modo que, para ver alguma informação, basta saber o endereço, ou seja, a sua URL (*Uniform Resource Locator*). Digamos que seja necessário acessar a página *http://www.minhaempresa.com.br:80/cursos/redes.html* para obter informações sobre os cursos de redes. Para isso, inserimos a URL apresentada em um navegador. A seguir, descreveremos, como exemplo, cada um dos itens que compõem a URL.

### 1.3.3.1 Protocolo

A primeira parte da URL refere-se ao protocolo em que se pretende realizar a conexão. O protocolo HTTP (*HyperText Transfer Protocol*) é quem informa ao navegador como conversar com o servidor que possui a página com a relação dos cursos de redes. Sempre que você vir o protocolo HTTP, significará que está navegando pelas páginas na Internet. Além do protocolo HTTP, existem muitos outros, como DNS, SMTP e FTP.

### 1.3.3.2 Nome do servidor

A segunda parte da URL trata do servidor em que se pretende

recuperar o recurso desejado, o qual, no nosso exemplo, é a página que contém a relação dos cursos de redes. Essa parte do endereço indica onde, na Internet, procurar o arquivo html desejado. Você já sabe que a Internet é constituída de muitas máquinas, e é justamente essa parte da URL que informa em qual máquina se deve procurar os dados. Assim, os nomes dos servidores terão sempre mais de uma palavra utilizada para sua correta identificação, as quais deverão estar separadas por ponto umas das outras, uma vez que esse é o padrão de nomes utilizado na Internet.

Os servidores da web geralmente começam por www, os servidores de FTP, por ftp, e assim por diante. Contudo, lembre-se de que esses nomes podem mudar de acordo com a filosofia de quem está nomeando os servidores. A segunda palavra indica o nome da empresa ou instituição à qual o recurso pertence, sendo, no nosso exemplo, minhaempresa. As empresas comerciais, da área de educação ou de áreas do governo podem utilizar o nome que melhor lhes convier, desde que ainda não esteja sendo utilizado por outra empresa ao redor do mundo.

A terceira parte do nome do servidor indica a finalidade do servidor, segundo os padrões na Internet, regulamentados pela IANA. Você já deve ter percebido que a maioria dos servidores possui como terceira parte a palavra “com”. Essa parte identifica o servidor como comercial. Há outros tipos que podem servir de exemplos: “edu” para instituições educacionais, “gov” para governamentais, “org” para instituições não comerciais ou “net” para redes. A quarta parte do nome do servidor indica o país onde o servidor se localiza. No caso de não existir a sigla do país, pode-se considerar que o servidor está localizado nos EUA. É importante observar que no Brasil o nome de um domínio termina com “br”.

#### 1.3.3.3 Diretório

Daqui em diante, será possível fazer uma analogia com os computadores pessoais, aqueles que usamos no dia a dia. É no diretório que está localizado o arquivo (ou página) no servidor. Os servidores também são computadores e estão organizados em diretórios (ou pastas), logo é necessário dizer em que diretório está

o arquivo procurado. No nosso exemplo, teríamos /redes/.

#### 1.3.3.4 Nome do arquivo

Para terminar a localização dos dados, é necessário dizer qual é o nome do arquivo (ou página) que você está querendo recuperar. Funciona da mesma forma que em seu computador: letras, números separados por ponto. Semelhantemente ao que acontece em seu computador, os arquivos têm extensões, e na Internet é a extensão que identifica o tipo de arquivo que está sendo transferido. Os arquivos-texto que contêm formatação possuem extensão .htm ou .html, enquanto imagens têm extensão .gif, .jpg ou .jpeg. A página do nosso exemplo chama-se *redes.html* e é do tipo que usa formatação html, portanto tem a extensão .html.

### 1.3.4 Nomes de email

Com as URLs, os emails são utilizados em larga escala pelos usuários da Internet. Esses endereços possuem o sinal de arroba (@), que divide o nome em duas partes, sendo a primeira parte referente ao nome do usuário e a segunda, ao nome do servidor de email. Veremos cada uma delas em detalhes.

Como não estamos acessando um arquivo, não utilizamos barras (/), mas devemos dizer ao servidor o nome do destinatário, ou seja, a quem estamos enviando a mensagem. Por exemplo, o nosso email de solicitações de informações é o suporteredes. Se juntarmos as duas partes, nome de usuário e nome do servidor de email, teremos as seguintes informações: *suporteredes@minhaempresa.com.br*. Na realidade, o @ significa *at*, em inglês. O que vem depois do sinal de arroba é o nome do servidor em que está localizada essa caixa postal. Tal procedimento segue as mesmas regras dos servidores que descrevemos anteriormente, mas com uma diferença: não há a primeira palavra, pois não é necessário identificar o tipo de servidor.

## 1.4 Por que estudar redes?

A cada dia, o uso das redes vem se tornando um recurso

indispensável em todos os locais onde existe um conjunto de computadores. Com o crescimento da Internet abrangendo todos os ramos de atividade, aumentou ainda mais a necessidade de ligação dos computadores em redes. Entretanto, é importante conhecer as vantagens e desvantagens do uso das redes, além dos cuidados que devemos tomar para evitar problemas. A seguir, apresentaremos a situação de uma escola que não possui uma rede instalada, motivo pelo qual o trabalho e a produtividade foram totalmente comprometidos.

Imagine uma escola que possui uma sala para tarefas administrativas, uma biblioteca, uma sala para os professores e uma sala de estudos, todas com computadores que não estejam interligados entre si, ou seja, *stand-alone*. Na sala da administração, a secretária possui dois computadores disponíveis conhecidos por *Sec1* e *Sec2*. O computador Sec1 é utilizado para registro de notas e emissão de boletins na impressora jato de tinta, conhecida por *Sprn1*. O computador Sec2 é utilizado para registro dos pagamentos efetuados e emissão dos carnês na impressora laser, conhecida por *Sprn2*.

Nessa escola, por questões de ordem interna, o boletim dos alunos só pode ser emitido se os pagamentos estiverem em dia, então é necessário transferir por pen drive esses arquivos do computador Sec2 para Sec1, praticamente todos os dias. Como os computadores não estão interligados em rede e as conexões com a Internet estão disponíveis por meio de link ADSL na sala dos professores ou na sala de estudos, os funcionários precisam deslocar-se até essas salas para enviar ou receber emails ou para efetuar pesquisas na Internet.

Na biblioteca, existe um computador *Bib1* que fica à disposição dos alunos para consulta de livros e registro de empréstimos e devoluções. O sistema só libera empréstimos para alunos com os pagamentos em dia, por isso a secretária não pode esquecer-se de copiar periodicamente os arquivos do computador Sec2 para Bib1. A biblioteca não tem impressora e quando a bibliotecária quer emitir os cartões de empréstimo ou atualizar a listagem de livros que são

comprados ou recebidos por doação, o arquivo precisa ser levado em um pen drive para ser impresso na Sprn1, na sala da administração.

Na sala de estudos, existe um computador conhecido por *Est1*, que permite aos alunos efetuarem pesquisas na Internet e imprimirem os resultados na impressora a jato de tinta colorida Eprn1. A bibliotecária constantemente precisa deixar a biblioteca para ir até a sala de estudos efetuar pesquisas na Internet.

Na sala dos professores, existem dois computadores multimídia conhecidos por *Prof1* e *Prof2*, que são usados, respectivamente, para preparação de aulas e lançamento de notas e acesso à Internet e ao correio eletrônico. As notas lançadas pelos professores precisam ser copiadas para Sec1, a fim de possibilitar a geração de boletins, pois só poderão ser emitidos caso o pagamento esteja em dia. Na sala dos professores, estão disponíveis os computadores Prof1, Prof2, um chaveador ligado a duas impressoras a jato de tinta colorida Pprn1 e Pprn2 para impressão de correio eletrônico e programas de aula.

Esse exemplo não é muito diferente do que acontece em pequenos escritórios de trabalho, pois muitos ainda não se conscientizaram da importância do estudo e da utilização das redes de computadores. Mesmo os usuários de informática que não possuem formação na área devem conhecer os princípios, as vantagens e as desvantagens das redes de computadores. A seguir, apresentaremos as vantagens e as desvantagens da utilização dessas redes.

### 1.4.1 Vantagens do uso das redes

O exemplo anterior apresentou um cenário extremamente confuso, no qual não existia a filosofia de trabalho em rede, o que, consequentemente, gerou um caos nessa instituição. A seguir, apresentaremos de forma resumida algumas das vantagens do uso de redes que deveriam ser implementadas na instituição comentada anteriormente.

#### 1.4.1.1 Compartilhamento de arquivos de trabalho

Esse é um dos recursos mais utilizados, pois permite que os usuários acessem arquivos armazenados em outros computadores interligados entre si, evitando o deslocamento de pessoas portando pen drives, conforme foi apresentado no exemplo anterior. Além disso, com os arquivos centralizados em servidores, poderemos realizar um backup, oferecendo segurança caso um arquivo seja perdido ou corrompido.

#### 1.4.1.2 Compartilhamento de programas

Os computadores podem acessar programas que ficam instalados fisicamente no disco rígido de outros computadores, o que evita o desperdício de espaço local e padroniza a versão do programa em uso. Além disso, pode-se economizar no custo dos programas, pois o custo de um software para operar em rede é menor se comparado à compra de uma licença para cada computador da rede.

Atualmente, com o crescimento da cloud computing, muitas empresas vêm utilizando o conceito de nuvem para armazenar seus arquivos (exs.: DropBox, OneDrive) e aplicativos de escritórios instalados nesse ambiente. O armazenamento de dados é feito em ambientes (ex.: datacenters) que poderão ser acessados de qualquer lugar do mundo, a qualquer hora, não havendo necessidade de instalação de programas específicos. O acesso aos programas, serviços e arquivos é remoto, por meio da Internet. Pela alta disponbilidade e desconhecimento da origem desse acesso, criou-se a alusão a nuvem.

#### 1.4.1.3 Compartilhamento de periféricos

Com a grande diversidade de mídias existentes, torna-se inviável ter em cada computador um leitor de CD-RW, um leitor de DVD-RW ou um scanner. Quando os computadores estão ligados em rede, o próprio sistema operacional permite, de forma simples, o compartilhamento de periféricos, garantindo mais produtividade dentro da empresa. Embora o custo desses equipamentos seja baixo, muitas empresas, por questões de segurança, preferem não os liberar a todos os usuários.

#### 1.4.1.4 Compartilhamento de impressoras

O compartilhamento de impressoras é um dos mais utilizados pelos usuários da rede, pois permite que todos os integrantes dessa rede imprimam em qualquer impressora, desde que estejam compartilhadas, possibilitando, assim, otimizar os investimentos futuros. O sistema operacional oferece um caminho muito simples para o compartilhamento de impressoras. Também podemos compartilhar impressoras por meio dos servidores de impressão, sem a necessidade de uma máquina dedicada a receber os pedidos de impressão. Essas impressoras são conectadas diretamente à rede por meio de um cabo par trançado. É importante observar que atualmente as impressoras, além da tradicional impressão, realizam cópias, atuam como scanners e ainda enviam emails com o conteúdo dos trabalhos copiados.

#### 1.4.1.5 Compartilhamento de acesso à Internet

Mesmo quando se tem apenas um modem ADSL ou uma ONU GPON para acessar a Internet, é possível compartilhar essa conexão na rede, o que possibilita que vários usuários estejam habilitados a realizar o acesso por meio de uma única conexão. Quando a conexão com a Internet é do tipo dedicada e utiliza um serviço ADSL, VDSL, GPON ou cable TV, o compartilhamento dessa conexão é praticamente obrigatório, pois o custo desse link só se justifica quando mais de um equipamento o utiliza. O uso da Internet, principalmente dos serviços de HTTP e email, tornou-se indispensável pela rapidez. É possível comunicar-se com pessoas do outro lado do mundo em poucos segundos, a um custo muito baixo. Depois do surgimento da Internet, a comunicação entre duas pessoas, que era baseada em ligações telefônicas ou troca de cartas, pode ser realizada gastando-se pouco dinheiro.

### 1.4.2 Desvantagens do uso das redes

Como nem tudo é facilidade e felicidade, além de inúmeras vantagens no uso de rede, também existem algumas desvantagens. A seguir, vamos descrevê-las.

#### 1.4.2.1 Ataque de vírus

Talvez este seja um dos piores problemas encontrados nas redes locais, já que a invasão da rede por um vírus pode prejudicar a conexão com a Internet (gerando tráfego desordenado), danificar os softwares instalados e até o hardware em alguns casos. Um arquivo infectado por vírus pode se espalhar pela rede em poucos minutos, obrigando todos na rede a interromperem suas atividades para que um especialista realize a manutenção necessária. Além da interrupção dos sistemas de redes, esses vírus podem roubar informações sigilosas de uma empresa, ocasionando perdas financeiras e sociais.

#### 1.4.2.2 Problemas nos equipamentos ativos e passivos

Além dos danos que os vírus causam ao computador, também podemos ter problemas com os equipamentos que centralizam as informações, como switches ou servidores de rede. Problemas ocorridos nos equipamentos que centralizam os cabos das redes (*patch pannel*) podem gerar lentidão da rede, de uma parte da rede ou até sua interrupção definitiva, independentemente da topologia utilizada. Quando param, os servidores de rede comprometem os usuários de seus programas, os usuários das impressoras ou os periféricos compartilhados.

#### 1.4.2.3 Invasão de hackers internos e externos

Esses ataques estão mais presentes em redes conectadas à Internet 24 horas por dia por meio de ADSL, VDSL, GPON, cable TV ou conexões dedicadas. É importante observar que a conexão contínua facilita ao hacker a procura por portas (portas são coordenadas pelos protocolos TCP ou UDP) que fornecem acesso à rede local. Com o acesso a uma dessas portas, o hacker pode monitorar o tráfego da rede, instalar programas do tipo *cavalo de troia* ou, ainda, acessar a caixa postal e enviar emails indesejáveis. Nesse tipo de conexão, o endereço IP do computador ligado à Internet é fixo por um grande período de tempo, logo o intruso pode ficar tentando a invasão durante horas. É muito importante observar que a maior parte dos ataques ocorridos em uma rede é feita pelos

próprios funcionários ou prestadores de serviço, então tenha sempre o controle de senhas como prioridade dentro da sua empresa.

A seguir, apresentaremos os componentes mínimos utilizados para que uma rede de computadores possa funcionar adequadamente.

## 1.5 Componentes de uma rede

Uma rede de computadores torna-se operacional quando há interligação dos computadores de forma local ou remota. Para fazê-la, são necessários cabos, conectores, comutadores (ex.: switch), placas de rede, sistema operacional e cliente de acesso. A seguir, descreveremos cada um dos componentes citados nesta seção.

### 1.5.1 Software de comunicação

O Sistema Operacional de Rede (SOR) é o componente responsável por garantir que o servidor de rede se mantenha estável, respondendo a todos os pedidos dos usuários de forma rápida e segura. Esse software deve garantir, por exemplo, que um usuário somente acesse arquivos que tenham sido liberados para uso e que apenas tenham acesso à rede usuários previamente cadastrados. A escolha do sistema operacional é um dos pontos mais importantes na implantação de uma rede e deve considerar vários fatores, como os serviços que deverão ser oferecidos à rede, os aplicativos que deverão ser compartilhados, a necessidade de integração com outros sistemas operacionais, a segurança, o desempenho, o suporte nacional e o internacional, a estabilidade e a facilidade de administração.

Quando pensam em um sistema operacional, muitos levam em consideração somente o fator segurança, porém essa característica não garante um sistema operacional adequado, ou seja, todos os fatores comentados anteriormente influenciam na obtenção de um ambiente seguro. Os sistemas operacionais mais utilizados são Unix (de vários fabricantes), as diferentes versões do Windows e Linux. A maioria das estações clientes utiliza os sistemas operacionais Windows ou Linux.

### 1.5.2 Cliente de acesso

Esse é o software que permite a comunicação da estação de trabalho com o servidor e a Internet.

### 1.5.3 Servidor

O servidor está presente somente nas redes que seguem a filosofia das redes cliente/servidor, nas quais os servidores ficam o tempo todo à disposição da rede, apenas para fornecer recursos compartilhados aos usuários. Por exemplo: impressoras, discos rígidos para armazenamento, aplicativos e acessos a outras redes. Naturalmente, tais servidores são dimensionados para essa tarefa, com bastante espaço em disco, grande capacidade de memória RAM, boa capacidade de processamento, bons componentes, boa ventilação, sistema inteligente de backup e tolerância a falhas. O desempenho dos recursos compartilhados é otimizado pelo fato de que, além de o servidor ser dimensionado para a tarefa em questão, tem todo o poder de processamento destinado a tarefas da rede. Atualmente, tem-se procurado manter tais servidores em datacenters, em que a disponibilidade de energia e climatização pode ser garantida.

O uso de servidores dedicados permite também um melhor gerenciamento dos usuários e do uso dos recursos, podendo controlar quem entra no sistema e quais recursos podem acessar.

### 1.5.4 Estação de trabalho

Estações de trabalho são computadores que fazem parte da rede e são dedicados aos usuários da rede local. Geralmente, fazem o papel de cliente, sendo os computadores que solicitarão recursos ao servidor. Uma coleção de estações de trabalho pode também formar uma rede de computadores independentemente da presença de um servidor, a qual chamamos de rede ponto a ponto. Nesse tipo de rede, todos os computadores fornecem recursos para a rede, mas também são clientes ou usuários dos recursos fornecidos pelos outros computadores. Normalmente, o desempenho e a confiabilidade do sistema são menores do que quando se tem um

servidor dedicado, porém é uma solução que garante bom aproveitamento dos recursos disponíveis e possui um custo mais baixo. Este modelo de rede é muito utilizado em pequenas empresas, escolas ou até mesmo residências.

### 1.5.5 Meio de comunicação

O nome meio de comunicação é dado aos cabos que conduzirão as tensões elétricas entre o computador origem e o destino, no caso de cabos de cobre ou luminosidade, quando falamos de fibras ópticas.

### 1.5.6 Placa de rede

A placa de rede é um equipamento interno instalado nos computadores que torna possível a comunicação entre as estações de trabalho e entre as estações e o servidor, sendo também conhecidas por NIC (*Network Interface Card*). A figura 1.3 representa uma placa de rede:

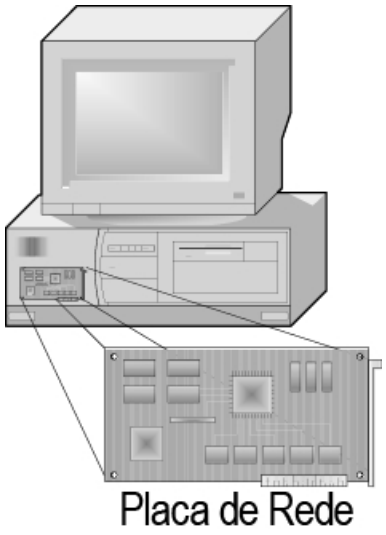



*Figura 1.3 – Placa de rede.*

### 1.5.7 Cabeamento

Trata do conjunto dos cabos que podem ser coaxial, fibra óptica ou cabo par trançado dos tipos UTP ou STP. Quando citamos cabeamento, devemos nos lembrar do cabeamento estruturado que será discutido no capítulo 5.

### 1.5.8 Equipamentos ativos

Os principais equipamentos ativos utilizados para a interligação das estações de trabalho a outros computadores da rede são os concentradores (também conhecidos por hub) e os comutadores (chamados de switch). O hub tem a característica de formar dentro de seus circuitos um barramento Ethernet, que permite que todos os computadores conectados a ele possam se comunicar e ainda faz a regeneração do sinal digital transmitido. Essa característica é importante em razão de o sinal ser degradado ao percorrer o caminho entre o computador origem e o destino. O switch também permite que os computadores ligados a ele se comuniquem e ainda regenera o sinal recebido. Cada conexão oferecida pelo switch é um novo barramento Ethernet e, dessa forma, oferece para cada equipamento conectado a ele uma banda passante exclusiva, excluindo o problema de colisão, o que não acontece com os hubs. Por meio dos switches, cada porta poderá trafegar em *full-duplex*, o que garante maior desempenho aos dados trafegados. Posteriormente, abordaremos com mais detalhes a comunicação *full-duplex* neste livro.

Atualmente, quando um cliente contrata um serviço de uma operadora, esta entrega no endereço do cliente um equipamento CPE com capacidade de converter o sinal óptico em elétrico e permite um tráfego em modo *full-duplex*. Caso o tráfego seja um *half-duplex*, o cliente perceberá perdas que, apesar de pequenas, podem comprometer o tráfego de aplicações de missão crítica, como VoIP, rádio ou TV.

## 1.6 Utilização das redes de computadores

Os computadores têm capacidade de se comunicar e, por meio dessa comunicação, podem emprestar ou tomar emprestado dados e recursos. Tal comunicação pode ser feita de duas formas: com a utilização de modems xDSL, ONUs GPON ou por meio das placas de redes locais.

Os modems, discutidos em um capítulo independente neste livro, utilizam linhas telefônicas ou ondas de rádio para realizar a

comunicação, enquanto as placas de rede podem se comunicar por meio de cabos de cobre, fibra óptica ou, ainda, utilizam o ar como meio de transmissão (placas *wireless*). As ONUs GPON apresentadas no capítulo 17 utilizam apenas os cabos de fibra óptica para transportar seus dados. Se os computadores podem trocar dados e recursos, então não importa em que local os dados estão armazenados. Podem estar fisicamente no mesmo local ou estar em lugares geograficamente diferentes. Quando os recursos estão fisicamente no mesmo local, considera-se que estão em uma rede LAN (*Local Area Network*); quando os recursos estão geograficamente em lugares diferentes, afirma-se que estão em uma rede WAN (*Wide Area Network*).

Uma rede existe quando é feita a interligação de computadores de forma local ou remota. Para fazer essa interligação, são necessários os componentes que formam a rede, como placas, cabos, conectores e outros aparelhos, os quais serão discutidos ao longo deste livro. Quando a interconexão é local, dizemos que nossa rede é uma LAN. Quando é remota, nossa rede é conhecida como WAN.

A rede LAN é formada por computadores interligados por meio de cabos, ondas de rádio, o ar (placas *wireless*) ou infravermelho, e todos pertencem a um mesmo local físico, dispensando a necessidade de modems ou ONUs. O conjunto de elementos que permitem a comunicação entre os computadores define o meio, o qual pode utilizar diversas tecnologias, como Ethernet, Token Ring, Token Bus ou GPON (*Gigabit Passive Optic Network*). A tecnologia mais utilizada é conhecida por Ethernet. Isso acontece em razão de sua simplicidade de instalação, seu baixo custo e, principalmente, em razão dos investimentos realizados pela indústria nessa tecnologia, que a levaram ao topo entre as concorrentes. O Ethernet é um canal físico pelo qual os dados podem fluir de um computador para outro.

A velocidade com a qual os dados conseguem fluir pelo barramento determina a sua largura de banda. Assim, quanto maior o valor da largura de banda, mais dados podem ser transferidos em um mesmo intervalo de tempo. As larguras de banda mais comuns para o padrão Ethernet estão representadas na tabela 1.1:

*Tabela 1.1 – Largura de banda em redes Ethernet*

| Largura de banda | Descrição |
|---|---|
| 10 Mbps | Transmite 10 milhões de bits por segundo. |
| 100 Mbps | Transmite 100 milhões de bits por segundo. |
| 1 Gbps | Transmite 1 bilhão de bits por segundo. |
| 10 Gbps | Transmite 10 bilhões de bits por segundo. |
| 40 Gbps | Transmite 40 bilhões de bits por segundo. |
| 100 Gbps | Transmite 100 bilhões de bits por segundo. Devido ao alto custo de uma interface 100 Gbps, muitas empresas ainda investem nas interfaces de 10 Gbps. |

O padrão Ethernet oferece às redes um bom desempenho a um baixo custo. Por isso, essa arquitetura está presente na maioria das redes do mundo inteiro. A figura 1.4 apresenta uma rede local padrão Ethernet:

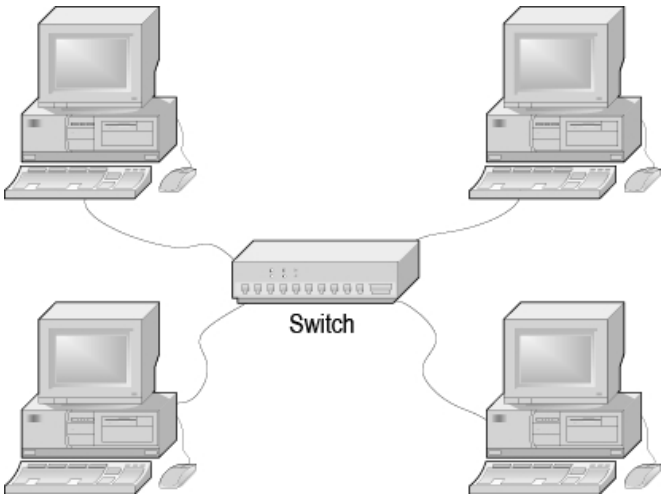



*Figura 1.4 – Rede local padrão Ethernet.*

As redes WAN são formadas pela interligação de pequenas ou grandes redes LANs. Cada ponta da rede WAN possui a mesma estrutura de uma rede LAN, e a conexão entre elas é feita por meio

de fibras ópticas ou ondas de rádio. A Internet pode ser considerada uma grande rede WAN, pois interliga milhões de pequenas redes LANs ao redor do mundo.

Como regra básica, uma WAN sempre é formada pela interligação de, no mínimo, dois roteadores. Um roteador representa um equipamento ativo responsável pela interligação de duas redes em que os endereços de rede de cada uma são diferentes (Exs.: rede 1: 10.0.0.0/8 e rede 2: 192.168.0.0/24, em que /8 significa que os 8 primeiros bits são dedicados à parte rede e /24, os primeiros 24 bits. Veremos no decorrer deste livro com mais detalhes a máscara de rede). A figura 1.5 apresenta uma rede WAN, que é formada entre a porta WAN do roteador *A* e a porta WAN do roteador *B*:

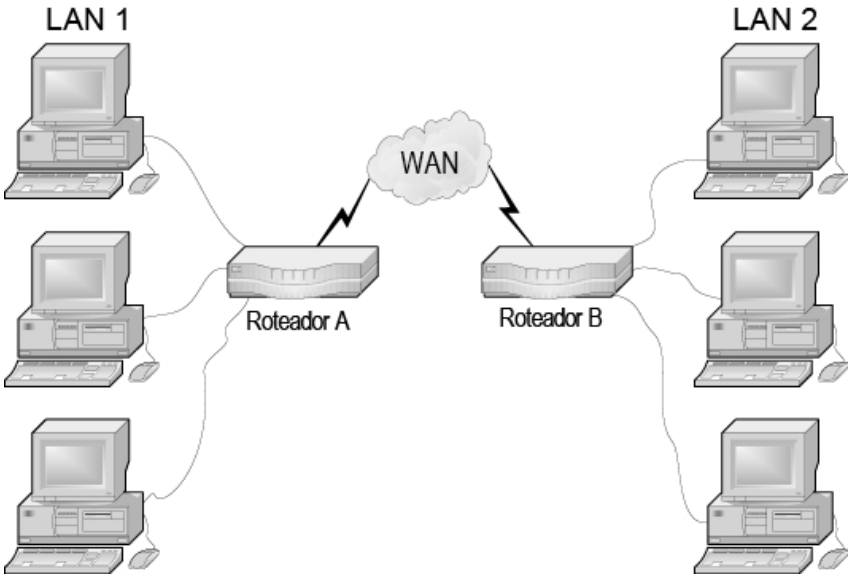



*Figura 1.5 – Rede WAN.*

# 1.7 Entidades de padronização

As entidades de padronização tiveram um papel fundamental para o sucesso das redes de computadores. A seguir, comentaremos a importância da padronização e a relevância de algumas das entidades mais importantes para o mundo das redes.

## 1.7.1 Importância da padronização

Produtos que apresentam restrições de compatibilidade e aplicação

praticamente perderam espaço no mercado. Será que alguém ainda se lembra dos primeiros videocassetes que eram fabricados em dois sistemas distintos: Betamax ou VHS? Venceu o VHS, logo padronizado. No mundo das redes, nada é diferente. Para que uma tecnologia alcance o sucesso, a padronização deve ser realizada em consenso e com cautela. O mundo globalizado exige produtos que funcionem tanto no Japão quanto no Brasil. Isso só é possível graças à padronização. No Brasil, grande parte dos produtos e processos tem suas normas e padrões técnicos regidos pela ABNT (Associação Brasileira de Normas Técnicas), seguindo modelos internacionais. As tecnologias de redes são padronizadas por entidades estabelecidas pelo mundo, as quais comentaremos a seguir.

#### 1.7.1.1 ISO (International Standards Organization)

É uma organização voluntária e independente, fundada em 1946, responsável por todos os tipos de padrões. A ISO publica padrões sobre uma vasta gama de assuntos, que vão de parafusos e porcas (literalmente) ao revestimento usado nos postes de telecomunicações. Pode-se citar como exemplos de padrões definidos pela ISO o modelo de referência OSI e o protocolo IS-IS (*Intermediate System-to-Intermediate System* ou Sistema Intermediário para Sistema Intermediário). Abordaremos os detalhes deste protocolo no capítulo 9.

#### 1.7.1.2 IEEE (Institute of Electrical and Eletronics Engineers)

Maior organização profissional do mundo na área de publicação de jornais especializados, o IEEE promove diversas conferências anuais, sempre tratando de assuntos ligados à área de Telemática. Possui um grupo de padronização que desenvolve padrões nas áreas de Engenharia Elétrica e de Informática. Por exemplo, o famoso padrão 802, do IEEE, para as redes Ethernet, o mais importante para as redes locais. A seguir, analisaremos cada uma das ramificações do padrão 802, as quais são conhecidas por 802.3, 802.4 e 802.5. A tabela 1.2 resume os detalhes de cada padrão:

*Tabela 1.2 – Exemplos dos primeiros padrões definidos pelo IEEE*

| Padrão | Descrição |
|---|---|
| 802.3 | Ethernet (criado pela Xerox). Utiliza cabo par trançado ou fibra óptica. Pode operar de 10 Mbps até 100 Gbps. |
| 802.4 | Token Bus (criado pela General Motors). Utiliza cabo coaxial de banda larga de 10 Mbps, possui prioridade nas mensagens, utiliza passagem de ficha (token) e é pouco utilizado no Brasil. |
| 802.5 | Token Ring (criado pela IBM). Utiliza par trançado STP de 4 a 16 Mbps. Essa é uma rede com alta confiabilidade. Também possui passagem de ficha (token) em um anel. |

O termo *token,* comentado nos padrões 802.4 e 802.5, refere-se a um bit que circula pela rede com o objetivo de garantir que somente uma máquina transmitirá seus dados a cada período de tempo. Somente a máquina que obtiver esse bit poderá transmitir dados; as outras deverão esperar o bit ficar livre para iniciar a transmissão dos seus dados.

#### 1.7.1.3 ITU-T (International Telecommunications Union)

Antigo CCITT (*Comité Consultatif International Téléphonique et Télégraphique* – Comitê Consultivo International de Telegrafia e Telefonia), foi criado em 1992 e tem o objetivo de formular e propor recomendações para telecomunicações. Serve como exemplo a definição do padrão GPON (*Gigabit Passive Optic Network ITU-T.984.1-4*). As redes GPON serão apresentadas em detalhes no capítulo 17.

### 1.7.2 Entidades de padronização direcionadas à Internet

A Internet tem seus próprios mecanismos de padronização, que são diferentes dos adotados pela ISO. Por ser uma rede pública mundial e autônoma baseada em padrões abertos, não existe nenhuma autoridade central que controle seu funcionamento. Entretanto, para permitir a interoperabilidade das diversas redes que compõem a Internet, várias organizações colaboram no estabelecimento de padrões e políticas gerais de operação da rede. Vejamos as principais organizações.

#### 1.7.2.1 IETF (Internet Engineering Task Force)

Grupo de trabalho que identifica, prioriza e endereça assuntos considerados de curto prazo, incluindo protocolos, arquitetura e operações de serviços. Os padrões propostos são publicados na Internet por meio de RFC (*Request for Comments*). O termo RFC refere-se aos documentos que especificam padrões e serviços para a Internet e para o modelo de referência TCP/IP. É importante observar que, antes de ser concluída e aprovada, a RFC é chamada de *Internet Draft*. As RFCs são numeradas sequencialmente na ordem cronológica em que são escritas. Quando um padrão é revisado, as alterações são escritas em uma RFC com um novo número.

#### 1.7.2.2 IRTF (Internet Research Task Force)

Grupo de trabalho que desenvolve assuntos estratégicos de longo prazo, incluindo esquemas de endereçamento e novas tecnologias.

#### 1.7.2.3 Internic (Internet Network Information Center)

Até a década de 1990, a InterNIC foi a responsável pela alocação de nomes de domínio e endereços IP, ou seja, até a década de 1990, os registros de domínios com extensão *.com*, *.net* e *.org* foram controlados pela InterNIC. No Brasil, o controle de nome de domínio depois da descentralização ficou a cargo da Fapesp (Fundação de Amparo a Pesquisa do Estado de São Paulo).

#### 1.7.2.4 IANA (The Internet Assigned Numbers Authority)

Organização internacional responsável por coordenar a distribuição de endereços IP entre as diversas redes de computadores que se conectam à Internet. No Brasil, a distribuição de endereços IP e a atribuição de nomes de domínio br foram inicialmente realizadas pela Fapesp, a qual pode ser consultada pelo site *www.fapesp.org*.

#### 1.7.2.5 RIR (Regional Internet Registry)

Atualmente, existem cinco entidades regionais distribuídas pelo mundo responsáveis pelos últimos endereços IPs versão 4 ainda disponíveis. Essas entidades regionais são subordinadas à IANA.

Vejamos onde cada uma das entidades atua:

- LACNIC (*Latin America and Caribbean Network Information Centre*) – Atua na América Latina e Caribe.
- ARIN (*American Registry for Internet Numbers*) – Atua na América do Norte.
- AFRINIC (*African Network Information Center*) – Atua na África.
- RIPE NCC (*Réseaux IP Européens Network Coordination Centre*) – Atua na Europa.
- APNIC (*Asia-Pacific Network Information Centre*) – Atua na Ásia e Pacífico.

#### 1.7.2.6 CGI.br (Comitê Gestor de Internet no Brasil)

O CGI.br foi fundado em maio de 1995 com a intenção de fazer efetivamente a sociedade participar das decisões envolvendo a implantação, administração e uso da Internet no Brasil. Para isso, o Ministério das Comunicações e o Ministério da Ciência, Tecnologia e Inovação constituíram, de forma conjunta, o Comitê Gestor da Internet. Desde sua fundação o CGI.br compartilhou com a Fapesp muitas das atividades administrativas. O CGI.br é a principal entidade relacionada à governança da Internet no Brasil e tem como principais objetivos:

- Fomentar o desenvolvimento da Internet no Brasil.
- Recomendar padrões, treinamentos e procedimentos relacionados à Internet.
- Coletar, organizar e disseminar indicadores e dados estatísticos sobre a Internet.
- Gerenciar os domínios .br e a atribuição de endereços IPs no Brasil.

O CGI.br criou o NIC.br, uma organização sem fins lucrativos para ajudá-lo a cumprir suas funções. Por sua vez, o NIC.br passou a gerir outros departamentos, como Registro.br, CERT.br, CETIC.br, CEPTRO.br e W3C. A seguir, abordaremos os departamentos comentados.

### 1.7.2.7 Registro.br

Desde 1995, o Registro.br foi o executor de parte das atribuições do NIC.br, entre as quais as atividades de registro de nomes de domínio, a administração e a publicação do DNS para o domínio <.br>. Essas atividades foram conduzidas em conjunto com membros da Fapesp. Atualmente, quando uma operadora fornece um bloco de endereços IPs a um de seus clientes, acessa o site do registro.br e realiza o relacionamento entre o bloco de endereço IP e o CPF ou CNPJ do cliente. Desta forma, por meio de qualquer acesso indevido desse endereço IP será possível identificar o seu responsável.

### 1.7.2.8 NIC.br (Núcleo de Informação e Coordenação do Ponto BR)

Desde a sua fundação, as responsabilidades do Registro.br foram controladas pela Fapesp, porém, a partir de dezembro de 2005, após uma reunião realizada pelo Comitê Gestor da Internet no Brasil (CGI.br), ficou decidido que as funções administrativas relativas ao domínio .br seriam repassadas ao Núcleo de Informação e Coordenação do Ponto BR (NIC.br). Como atividades administrativas, citamos registro de nomes de domínio, alocação de endereços IP, operação de computadores, servidores e rede e toda a infraestrutura necessária, manutenção dos domínios sob .br, atender aos requisitos de segurança e emergências na Internet brasileira em articulação e cooperar com as entidades e os órgãos responsáveis, desenvolver projetos que visem melhorar a qualidade da Internet no Brasil e disseminar seu uso, com especial atenção para seus aspectos técnicos e de infraestrutura, fomentar e acompanhar a disponibilização e a universalização de serviços de Internet no país, entre várias outras.

Para registrar um domínio, precisa-se de um usuário (geralmente formado por três letras) e senha. A solicitação deve ocorrer pelo site *http://registro.br/*. Esse usuário pode ser uma pessoa física ou jurídica. O registro de um determinado domínio é realizado uma vez, porém a alocação de endereços IPs pode ocorrer múltiplas vezes. Desta forma, quando uma empresa precisa acessar a Internet, contrata-se

um link com alguma operadora que fará sua conexão com a Internet. Neste caso, a empresa pode receber dessa operadora uma range de endereços IPs válidos na Internet. A operadora acessa o site do Registro.BR e vincula a range de endereços IPs ao CPF ou CNPJ do cliente. Isto ocorrerá todas as vezes que a empresa solicitar novos ranges de endereços. Assim, qualquer acesso legal/ilegal do respectivo endereço IP poderá ser rastreado. Caso o cliente seja um provedor de Internet, por exemplo, e tenha sua própria conta no registro.br, poderá realizar a administração de seus endereços IPs com seus clientes.

#### 1.7.2.9 CERT.br

O Centro de Estudos, Resposta e Tratamento de Incidentes de Seguranca no Brasil (CERT.br) é o Grupo de Resposta a Incidentes de Seguranca para a Internet brasileira, mantido pelo NIC.br do Comitê Gestor da Internet no Brasil. Este grupo é responsável por tratar incidentes de seguranca em computadores, envolvendo redes conectadas à Internet brasileira. Como exemplo de incidentes tratados pelo CET.br, temos a notificação de um DNS recursivo aberto. Neste caso, DNS recursivo aberto fará que o servidor seja vítima de ataques de envenenamento de cache e ainda poderá ser utilizado para ataques de negação de serviço (DOS), consumindo recursos da sua rede. A prática de DOS prejudica a qualidade dos serviços prestados pela empresa que poderá ser atacada. Essa entidade também notifica o responsável por um endereço IP quando ele realiza download de arquivos de sites que infringem leis de propriedade intelectual.

#### 1.7.2.10 CETIC.br

O Centro de Estudos sobre as Tecnologias da Informação e da Comunicação (CETIC.br) foi criado em 2005 e tornou-se responsável pela coordenação e publicação de pesquisas sobre a disponibilidade e uso da Internet no Brasil. Esses estudos são referência para a elaboração de políticas públicas que garantam o acesso da população às Tecnologias da Informação e da Comunicação (TICs), assim como para monitoramento e avaliação

do impacto socioeconômico das TICs.

#### 1.7.2.11 CEPTRO.br

O Centro de Estudos e Pesquisas em Tecnologias de Redes e Operações é a área do NIC.br responsável por serviços e projetos relacionados principalmente à infraestrutura da Internet no Brasil e ao seu desenvolvimento. Essa área desenvolve soluções em infraestrutura de redes, software e hardware, além de gerenciar projetos executados por parceiros externos.

Os Pontos de Troca de Tráfego (PTTs), hoje em várias localidades diferentes (São Paulo, Curitiba, Rio de Janeiro), são a atividade mais importante do CEPTRO, ajudando a organizar a infraestrutura da Internet no país, tornando-a mais resiliente (capacidade de retomar seu estado atual após sofrer interferências exernas) e diminuindo seus custos. Esta área também mede a qualidade da Internet, divulga a Hora Legal Brasileira via NTP e dissemina o protocolo IPv6 no país através de cursos gratuitos.

## 1.8 Exercícios do capítulo 1

**1**. Cite sete recursos que podem ser compartilhados em uma rede.

**2**. O que levou as redes de computadores a se tornarem tão acessíveis?

**3**. Qual o objetivo do padrão OSI? Por que foi concebido?

**4**. Qual a influência da IBM no processo de definição do modelo de referência OSI?

**5**. Comente o modelo de referência TCP/IP.

**6**. Qual a diferença entre LAN, MAN e WAN?

**7**. Onde surgiu a Internet? Descreva sua origem.

**8**. Qual a diferença entre intranet e extranet?

**9**. Cite vantagens e desvantagens das redes de computadores.

**10**. Quais os componentes de uma rede?

**11**. Qual a arquitetura de rede local utilizada pela maioria das redes no mundo? A rede em que você trabalha possui qual arquitetura?

**12**. Qual a largura de banda da rede onde você estuda ou trabalha? Qual a largura de banda que você considera ideal para seu ambiente de estudo ou trabalho?

**13**. Cite e comente cinco entidades de padronização.

**14**. Que entidade no Brasil é responsável pela distribuição de endereços IP e nomes de domínio?

**15**. Descreva a URL (*Uniform Resource Locator*) da empresa onde você trabalha.

**16**. Descreva como foi composto seu endereço de email.

**17**. Quais são os equipamentos ativos que sua empresa possui instalados?

**18**. Qual é o sistema operacional de rede instalado nos servidores de sua empresa?

**19**. Qual é o sistema operacional e qual o modelo da placa de rede do seu computador?

**20**. Qual é o modelo do cabo de rede que seu computador utiliza?

**21**. Qual a largura de banda da rede onde você trabalha ou estuda?

**22**. Uma Intranet tradicional é:

a) uma rede-padrão LAN que utiliza o protocolo TCP/IP para comunicação.

b) uma rede corporativa que utiliza o protocolo IPX da Internet para seu transporte fundamental.

c) composta de inúmeras redes de empresas distintas.

d) uma rede privativa que permite fácil acesso à Internet, utilizando o protocolo TCP/IP, diferentemente de uma Extranet.

e) uma rede na qual não podemos ter servidores, existindo apenas máquinas de usuários.

CAPÍTULO 2

# Arquitetura e topologias de redes

O capítulo 2 apresentará o padrão Ethernet, detalhando o protocolo CSMA-CD e o processo de detecção de colisões. Também serão comentados o problema da atenuação quando se utilizam hubs, a definição do termo impedância e uma descrição detalhada das principais topologias de rede disponíveis.

## 2.1 Arquitetura Ethernet

O padrão Ethernet é um dos mais populares e difundidos meios de transmissão de dados utilizados nas redes instaladas e, certamente, é o mais empregado em novos projetos residenciais, comerciais e industriais. Sua grande popularidade deve-se exclusivamente à aceitação do padrão por diversos fabricantes de dispositivos de rede e a seu baixo custo.

Uma rede Ethernet pode utilizar como meio de comunicação cabos de par trançado ou, ainda, fibras ópticas. Os cabos de par trançado utilizam tensões elétricas para representar os bits 0s e 1s, enquanto a fibra óptica utiliza luz para representá-los. Em redes Ethernet, é possível transmitir dados sob as topologias em barramento e em estrela, e a estrela necessariamente utiliza um switch como concentrador, ao passo que, sob a topologia em barramento, os computadores são interligados uns aos outros diretamente por meio do cabo coaxial.

É característica das redes Ethernet a disputa pela utilização do meio de comunicação entre os diversos computadores. Essa disputa representa um problema quando a rede está conectada por hubs, os quais não possuem inteligência no momento da transmissão. Todo o controle de concorrência é feito pelo protocolo CSMA/CD (*Carrier Sense Multiple Access with Collision Detection*). Assim, o padrão Ethernet permite que somente um equipamento transmita seus bits por vez. Para entendermos melhor, vejamos um exemplo.

Qualquer máquina que queira transmitir um bit deverá antes analisar o meio de comunicação (cabo) e, caso não exista nenhuma variação de tensão (bits transmitidos) no meio, essa máquina iniciará sua transmissão. O protocolo responsável por ouvir o que está sendo transmitido na rede e dar sinal verde para uma placa de rede iniciar a transmissão é o CSMA/CD. Esse protocolo faz com que qualquer estação que queira transmitir escute o meio de acesso, seja ele cabo metálico ou fibra óptica.

Essa operação tem o objetivo de detectar se existe alguma transmissão em curso. Caso a resposta seja positiva, a estação deve esperar até que os meios fiquem livres. Mesmo com esse controle, ainda há probabilidade de que duas estações iniciem uma transmissão simultaneamente, causando o que chamamos de colisão. Essa colisão obrigará ambas as estações a retransmitir os seus bits, visto que estão dividindo o mesmo meio de comunicação, e a técnica de transmissão utiliza a mesma frequência. Na verdade, a colisão é a grande responsável por uma rede Ethernet não ser determinística. Assim, devemos lembrar que o protocolo CSMA/CD ajuda a evitar colisões, mas não garante que elas não acontecerão.

O fluxograma apresentado na figura 2.1 apresenta o caminho básico seguido pelo protocolo CSMA/CD tanto para identificar se o meio de comunicação está ou não livre como para minimizar as colisões.

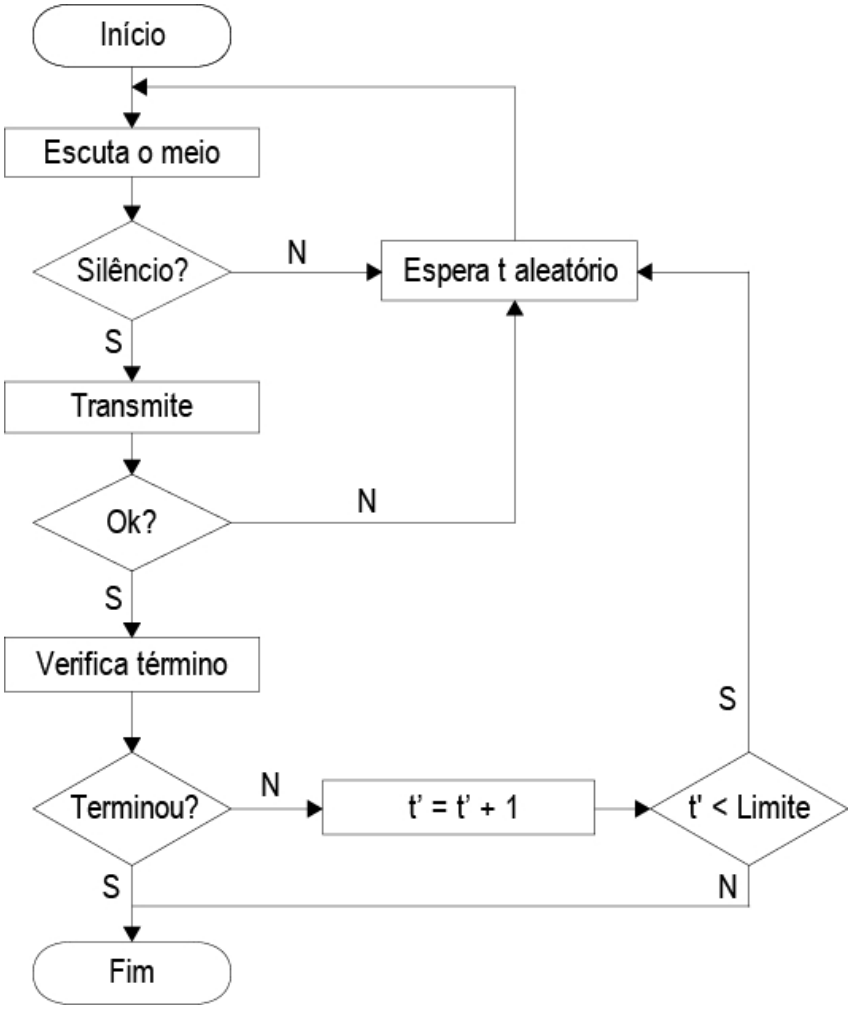



*Figura 2.1– Fluxograma do CSMA/CD.*

Esse fluxograma envolve tentativas e colisões, pois duas estações podem escutar o meio ao mesmo tempo e iniciar uma transmissão (isso acontece frequentemente), ocorrendo, então, uma colisão e a perda dos bits. Nesse caso, cada computador espera um tempo aleatório (na casa dos milissegundos), que é diferente para cada estação, e retransmite seus bits.

A colisão é detectada pelas placas de rede das máquinas por meio do protocolo CSMA/CD. A colisão caracteriza-se por uma variação de tensão maior do que a normalmente utilizada na rede para representar os bits 1 e 0, ou seja, quando detecta uma tensão que corresponde, por exemplo, ao dobro da variação conhecida, essa placa identifica uma colisão. O computador que identificou a colisão envia uma mensagem a todos os outros computadores da rede,

solicitando que parem de transmitir, pois uma colisão foi identificada.

As chances de uma colisão ocorrer dependem do tráfego da rede, geralmente proporcional à quantidade de computadores ativos no domínio de colisão. A figura 2.2 apresenta a relação entre a quantidade de computadores no domínio de colisão e a quantidade de colisões que serão geradas caso a quantidade de máquinas cresça.

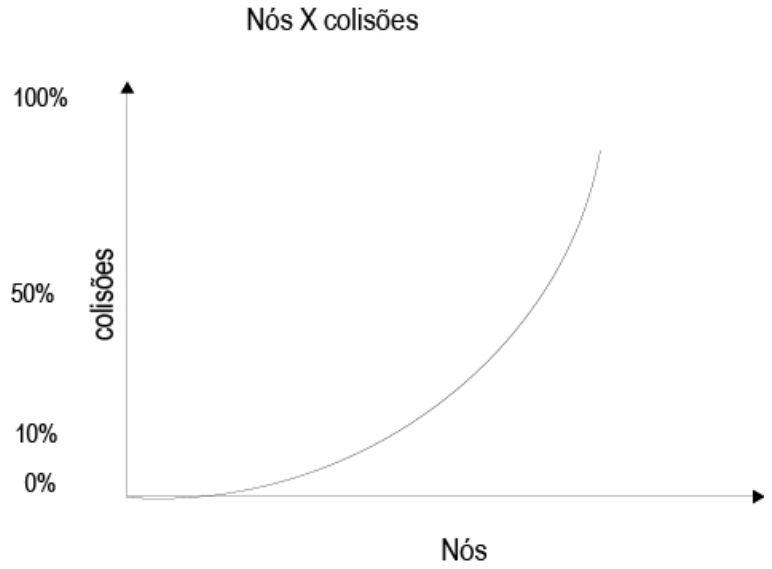



*Figura 2.2 – Relação entre quantidade de computadores e quantidade de colisões.*

## 2.1.1 Detectando colisões

As colisões podem ser detectadas de várias maneiras, porém alguns métodos são mais precisos do que outros. Deve-se deixar claro que é responsabilidade da placa de rede detectar colisões. As placas de rede identificam uma colisão por meio da percepção, ou seja, o sinal recebido foi superposto no meio físico, ficando sua frequência alterada. É importante estar atento e observar as situações em que uma colisão pode ser confundida. Essas situações referem-se à ocorrência de atenuação ou quando um repetidor ou hub não trata a colisão.

## 2.1.2 Atenuação

Atenuação representa uma perda de sinal ao longo do caminho. Se a atenuação for muito elevada, será difícil distinguir uma colisão de atividades ruidosas. Por que isso é difícil?

A colisão significa uma tensão desconhecida pelas placas de rede, a qual fica maior do que o normal recebido. Caso exista atenuação, a tensão pode baixar e a placa de rede pode receber um sinal que não significa nada, ou seja, a intensidade da tensão elétrica está dentro dos padrões esperados pela placa de rede. Assim, a colisão não será identificada e os bits recebidos não serão os mesmos que foram enviados. Esse é um dos motivos pelos quais se deve limitar os efeitos de atenuação. Algumas sugestões podem ser seguidas para não haver confusão entre uma colisão e um sinal normal, como manter a distância do cabo segundo os padrões e instalá-lo nas condições especificadas pelos manuais especializados.

### 2.1.3 Hub

Se houver hubs nas sub-redes, a detecção das colisões será mais simples. Como todo o tráfego da sub-rede passa pelo hub, qualquer detecção indicando atividade simultânea em duas ou mais de suas portas é evidência de colisão. O próprio hub encarrega-se de enviar um sinal a todas as placas de rede informando o que aconteceu. Isso ocorre até que os sinais emitidos pelas estações da rede cessem completamente, ou seja, até que todos os dispositivos conectados percebam o que ocorreu. Devido ao baixo custo dos switches e às desvantagens dos hubs (inundação dos quadros recebidos, colisões, operação em *half-duplex*), atualmente se prefere utilizar switches.

## 2.2 Topologias de rede

A topologia de rede descreve o modo como todos os dispositivos estão ligados entre si e a forma como se processa a troca de informação entre eles. Essa topologia garante a redução de custos e o aumento da eficiência do sistema por meio da combinação de recursos. A seguir, detalharemos as principais topologias de rede disponíveis.

### 2.2.1 Topologia estrela

A topologia estrela é caracterizada por um elemento central que gerencia o fluxo de dados da rede, estando diretamente conectado (ponto a ponto) a cada dispositivo de rede, por isso a sua designação: “estrela”. Toda informação enviada de um dispositivo de rede para outro deverá obrigatoriamente passar pelo ponto central (ou concentrador), tornando o processo muito mais eficaz, já que os dados nessa topologia não deverão, necessariamente, passar por todas as estações. A figura 2.3 apresenta uma rede concebida na topologia estrela.

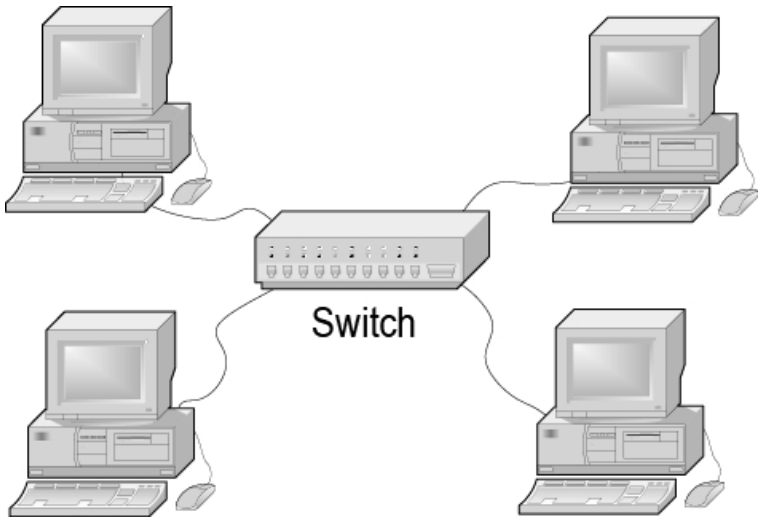



*Figura 2.3 – Topologia estrela.*

### 2.2.2 Topologia linear

A topologia linear é simples e fácil de ser implementada. Redes dispostas nessa topologia possuem todos os computadores interligados por meio de um cabo contínuo, de modo que todos os dados enviados para o cabo serão entregues a todos os computadores interligados. Esse tipo de topologia é indicado para redes simples, já que um barramento único é limitado em termos de distância, gerenciamento e quantidade de tráfego. A figura 2.4 apresenta uma rede LAN com seus equipamentos ligados na topologia linear:

*Figura 2.4 – Topologia linear.*

### 2.2.3 Topologia anel

Como o nome indica, uma rede anel é constituída de um circuito lógico fechado e tem como vantagem a ausência de atenuação, já que o sinal transmitido é regenerado cada vez que passa por uma estação. A figura 2.5 apresenta uma rede com topologia em anel:

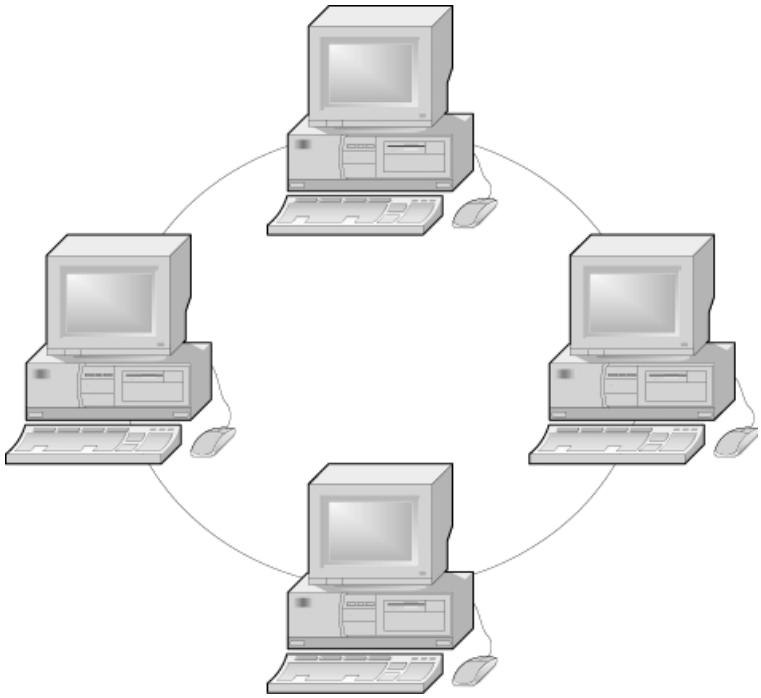


*Figura 2.5 – Rede na topologia em anel.*

## 2.3 Exercícios do capítulo 2

**1**. Qual a arquitetura de redes mais usada em projetos de redes?

**2**. Como são conhecidas as redes que transmitem dados a 100 Mbps?

**3**. Como são conhecidas as redes que transmitem dados a 1 Gbps?

**4**. Qual é a função do protocolo CSMA/CD nas redes Ethernet? Qual

é sua importância?

**5**. Quais os meios de comunicação utilizados pelo padrão Ethernet para transmissão de dados?

**6**. O que acontece quando duas estações transmitem dados ao mesmo tempo em uma rede Ethernet?

**7**. Quando mais equipamentos são inseridos no domínio de colisão, qual o comportamento da rede?

**8**. Que protocolo Ethernet faz a detecção de colisão?

**9**. Que topologia de rede você utiliza na escola/trabalho?

**10**. Defina o processo de reflexão apresentado nos cabos coaxiais.

**11**. (Sanepar, 2004) Assinale a alternativa que descreve corretamente o comportamento do protocolo Ethernet na ocorrência de uma colisão:

a) O protocolo retransmite imediatamente.

b) O protocolo aguarda um tempo aleatório e retransmite.

c) O protocolo aguarda um tempo aleatório, verifica se há portadora no meio e, caso não haja, retransmite.

d) O protocolo aguarda o meio ficar livre e retransmite.

e) O protocolo aguarda o meio ficar livre e retransmite com uma probabilidade p, definida pelo padrão IEEE802.3.

**12**. (Sanepar, 2004) Uma colisão pode ocorrer em alguns protocolos quando duas máquinas compartilham o mesmo meio de transmissão e tentam utilizá-lo ao mesmo tempo. Considere as afirmativas a seguir relativas às colisões em redes locais.

I. Colisões podem ocorrer em redes Fast Ethernet não comutadas, ou seja, utilizando um hub.

II. Uma colisão pode ocorrer em redes com topologia em anel, como a rede Token Ring.

III. Colisões nunca ocorrem em redes Ethernet comutadas, ou seja, utilizando um switch.

IV. O número de colisões está diretamente relacionado ao desempenho da rede.

a) Somente as afirmativas I, III e IV são verdadeiras.

b) Somente as afirmativas I e IV são verdadeiras.

c) Somente as afirmativas II e III são verdadeiras.

d) Somente as afirmativas II, III e IV são verdadeiras.

e) Somente as afirmativas III e IV são verdadeiras.

**13**. (Enade, 2008 – Computação) Em redes locais de computadores, o protocolo de controle de acesso ao meio define um conjunto de regras que devem ser adotadas pelos múltiplos dispositivos para compartilhar o meio físico de transmissão. No caso de uma rede Ethernet IEEE 802.3 conectada fisicamente a um concentrador (hub), em que abordagem se baseia o protocolo de controle de acesso ao meio?

a) Na passagem de permissão em anel.

b) Na ordenação com contenção.

c) Na ordenação sem contenção.

d) Na contenção com detecção de colisão.

e) Na arbitragem centralizada.

CAPÍTULO 3

# Arquiteturas de redes

O capítulo 3 apresenta em detalhes os modelos de referência utilizados pela indústria para produzir componentes na área das redes de computadores. Neste capítulo, detalharemos as sete camadas do modelo de referência OSI e as quatro camadas do modelo de referência TCP/IP, além de fazer uma análise comparativa entre os dois modelos de referência.

## 3.1 Introdução

Quando surgiram, as redes de computadores eram, na sua totalidade, proprietárias, isto é, uma determinada tecnologia só era suportada por seu fabricante. Não havia a possibilidade de misturar soluções de fabricantes diferentes, pois não existia compatibilidade. Dessa forma, um fabricante era responsável pelo fornecimento de praticamente todos os componentes da rede. Para facilitar a interconexão de sistemas de computadores, a ISO (*International Standards Organization*) desenvolveu um modelo de referência chamado OSI (*Open Systems Interconection*) para que os fabricantes pudessem criar protocolos e componentes a partir desse modelo. O modelo de referência OSI compõe-se de sete camadas, as quais serão discutidas neste capítulo.

Em paralelo com a especificação do modelo de referência OSI, foi também especificado o modelo de referência TCP/IP, definido com quatro camadas. A seguir, descreveremos cada um dos modelos de referência apresentados e faremos uma comparação entre eles.

## 3.2 Modelo de referência OSI

O modelo de referência OSI é composto de sete camadas, que são apresentadas no texto a seguir em conjunto com uma comparação entre elas e o modelo telefônico que utilizamos no nosso dia a dia.

- **Camada 1 (Física)** – Trata das características físicas, elétricas, ópticas e mecânicas necessárias à operação das redes. Essa camada está totalmente ligada ao hardware, enquanto as outras cuidam do software. Como exemplos de equipamentos atuantes nessa camada, temos as placas de rede, o conector do telefone (RJ-11) e o conector de redes Ethernet (RJ-45), ambos transparentes à visão do usuário e utilizados para conectorizar o hardware ao software.
- **Camada 2 (Enlace de dados)** – Faz a interface confiável entre o meio físico e os dados do computador, detectando erros e controlando o fluxo. Como exemplo, temos a ação de tirar o fone do gancho e ouvir o dial-tone. Assim, podemos tomar a decisão de ligar ou não. Se o tom é ouvido, podemos ligar; do contrário, temos problemas.
- **Camada 3 (Rede)** – É responsável pelo redirecionamento dos pacotes entre redes diferentes. Por exemplo, a ação de digitar os números do telefone com o qual queremos conversar. Primeiro vem o DDD (rota) e, na sequência, qual o destino que se deve seguir. A partir desse momento, será definido o direcionamento da conversa entre os diversos caminhos possíveis pelos troncos da telefonia.
- **Camada 4 (Transporte)** – Controla o fluxo de dados entre o emissor e o receptor. Uma pessoa precisa falar na velocidade adequada para que a outra possa ouvir, não pode falar muito rápido, pois corre o risco de a outra não a ouvir ou não a entender. Como segundo exemplo, temos a indagação da outra ponta: “O quê? Como? Dá para falar mais alto”. Essa camada também realiza o controle e o estabelecimento de um nível de conversa e recebe os dados da camada superior e divide-os em pacotes.
- **Camada 5 (Sessão)** – Inicia a comunicação fim a fim e complementa as funções da camada 4. A conversa pode ser interrompida e reiniciada no ponto em que parou, em razão de essa conversa estar sempre sendo gerenciada. A camada de sessão estabelece um canal de comunicação entre os usuários

emissor e receptor. Como exemplo do mundo telefônico, temos o estabelecimento e o gerenciamento do diálogo entre duas pessoas conectadas por uma linha telefônica.

- **Camada 6 (Apresentação)** – Tem como objetivo converter dados para um formato-padrão. Por exemplo, a conversão da onda analógica da voz para sinal digital entendido pela secretária eletrônica.
- **Camada 7 (Aplicação)** – Determina como ocorrerá o diálogo, identificando nomes ou endereços. Em uma ligação, isso pode ser feito por um BINA (B identifica o número de A), que representa a interface entre o protocolo de comunicação (voz) e o aplicativo que pediu ou receberá a informação por meio da rede (usuário).

A seguir, detalharemos as sete camadas do modelo de referência OSI.

### 3.2.1 Camada de aplicação

A camada de aplicação faz a interface entre o protocolo de comunicação (a voz no nosso exemplo ou o *browser* Internet) e o aplicativo que pediu ou receberá a informação por meio da rede (secretária eletrônica do receptor). Trazendo para o mundo da computação, a camada de aplicação converte os dados de uma mensagem de email (lida pelo usuário) em bits, anexando um cabeçalho para identificar o computador-emissor e o computador-receptor. As principais funções da camada de aplicação são determinar como ocorrerá o diálogo, identificar endereços ou nomes, controlar o acesso e a integridade dos dados.

A camada de aplicação é a do modelo de referência OSI mais próxima do sistema final e determina se existem recursos suficientes para a comunicação entre os sistemas. Os aplicativos mais comuns que atuam nessa camada são programas de email, processadores de textos, planilhas eletrônicas e *browsers*.

### 3.2.2 Camada de apresentação

A camada de apresentação é também chamada de camada de

tradução (tradução da voz analógica para sinais digitais), pois converte o formato do dado recebido pela camada de aplicação em um formato comum a ser usado na transmissão desse dado, ou seja, um formato entendido pelo protocolo usado. Como exemplo, podemos citar a conversão do padrão de caracteres (código de página). Quando um dispositivo transmissor usa um padrão diferente do *American National Standard Code for Information Interchange* (ASCII), como o *Extended Binary Coded Decimal Interchange Code* (EBCDIC), a camada de apresentação deverá compatibilizar o emissor e o receptor. Também como outras tarefas dessa camada, temos a compreensão dos dados e a criptografia.

A compressão dos dados pega os dados recebidos da camada 7 e os compacta (como se fosse um compactador comumente encontrado, como Winrar ou Zip). A camada 6 do dispositivo receptor é responsável por descompactar esses dados. Dessa forma, a transmissão fica mais rápida, já que haverá menos dados a serem transmitidos.

### 3.2.3 Camada de sessão

A camada de sessão permite que usuários de diferentes máquinas estabeleçam sessões entre si. Nessa sessão estabelecida, as aplicações definem como será feita a transmissão de dados e colocam marcações nos dados que estão sendo transmitidos. Essas marcações são também chamadas de pontos de sincronização e têm como objetivo restabelecer uma comunicação interrompida por algum motivo a partir do ponto de interrupção.

Uma sessão permite o transporte de dados normal, mas também oferece serviços aperfeiçoados que podem ser de grande utilidade em algumas aplicações. Se, porventura, a rede falhar, os computadores reiniciarão a transmissão dos dados a partir da última marcação recebida pelo computador-receptor. Como exemplo dessa camada, temos o processo utilizado por aplicativos de download de emails. Quando se está baixando emails de um servidor SMTP (*Simple Mail Transfer Protocol*), podem ocorrer interrupções na comunicação. Nesse caso, quando voltar a ser executado, o

download terá sua continuidade a partir do ponto em que parou, não sendo necessário reiniciá-lo.

### 3.2.4 Camada de transporte

A camada de transporte é responsável por pegar os dados enviados da camada de sessão e dividi-los em mensagens que serão transmitidas pela rede, ou seja, as mensagens serão repassadas à camada de rede que vai roteá-las até o seu destino.

A camada de transporte tem como responsabilidades a realização do controle de fluxo, a correção de erros e o controle de sequência. A camada de transporte aparentemente possui muitas funções semelhantes às funções da camada de enlace, entretanto os equipamentos operam de forma diferente quando se referem a essas camadas. A relação entre as camadas de transporte e enlace será apresentada na seção 3.2.6.1.

### 3.2.5 Camada de rede

A camada de rede é responsável pelo endereçamento dos pacotes, convertendo endereços lógicos em endereços físicos. Além disso, determina a rota que os pacotes seguirão para atingir o destino, baseada em fatores como condições de tráfego da rede e prioridades.

Depois de receber as mensagens da camada de transporte, essa camada adiciona informações para o seu controle, como o endereço IP origem, o endereço IP destino etc. Essas informações de controle permitem que uma requisição seja entregue diretamente para quem a requisitou, pois não pode existir mais de uma máquina com o mesmo endereço IP em uma rede. Portanto, essa camada é usada quando a rede possui mais de um segmento (caminho a seguir) e, com isso, há mais de um caminho para um pacote de dados trafegar da origem até o destino. A Internet é uma rede que utiliza fielmente o protocolo IP. É importante lembrar que o protocolo IP foi definido no modelo de referência TCP/IP. Aqui ele foi utilizado apenas para exemplificar a camada de rede.

### 3.2.6 Camada de enlace

A camada de enlace (também conhecida por camada de link de dados) recebe os pacotes de dados da camada de rede, transforma-os em quadros na camada de enlace e, finalmente, em tensões elétricas na camada física para serem transmitidas no meio físico. Todas as vezes que um elemento cruzar uma camada, ele receberá informações adicionais.

No caso da transição entre as camadas de rede e enlace, o quadro na camada de enlace será acrescido de endereço MAC da placa de rede de origem, endereço MAC da placa de rede de destino, dados de controle e CRC (*Cyclic Redundancy Check*). Todas as informações contidas nas camadas superiores serão interpretadas como dados normais nas camadas inferiores. Quando recebe um quadro, o equipamento destino remonta-o, analisando se todos os bits recebidos estão íntegros.

Com o advento do padrão IEEE 802.3 (padrão Ethernet), a camada de enlace teve de passar por algumas mudanças em relação à sua definição inicial: foi dividida em duas outras camadas conhecidas como LLC (*Logical Link Controle*) e MAC (*Media Access Control*). A camada MAC tem como principal objetivo delimitar os quadros recebidos, enquanto a camada LLC deve ajustar a comunicação aos protocolos da camada superior.

#### 3.2.6.1 Diferenças entre as camadas de transporte e de enlace

As camadas de transporte e enlace são parecidas no sentido de fazerem que os dados transitem da origem até o seu destino, realizando o tratamento de erros, controle de fluxo e sequenciamento. Apesar de parecer que ambas fazem o mesmo trabalho, existem diferenças entre ambas.

Na camada de enlace, dois roteadores comunicam-se diretamente por um meio físico, ao passo que, na camada de transporte, entre o emissor e o receptor, pode haver uma rede ou mesmo várias redes. Assim, a camada de enlace torna possível a comunicação entre dois computadores ligados ponto a ponto, enquanto a camada de transporte permite a comunicação entre dois computadores

interligados por diferentes redes.

### 3.2.7 Camada física

A camada física é responsável por pegar os quadros enviados pela camada de enlace e os transformar em sinais compatíveis com o meio pelo qual os dados deverão ser transmitidos. Se o meio for elétrico, essa camada converterá os 0s e 1s em sinais elétricos a serem transmitidos pelo cabo; caso o meio seja óptico (uma fibra óptica), essa camada converterá os 0s e 1s dos quadros em sinais luminosos.

A camada física especifica o conector utilizado para transmitir as informações e a maneira com que os 0s e 1s dos quadros serão enviados pela rede. Essa camada não sabe o significado dos 0s nem dos 1s que está recebendo ou transmitindo. No caso da recepção de um quadro, a camada física converte os sinais do cabo em 0s e 1s e envia essas informações para a camada de enlace, que montará o quadro e verificará se ele foi recebido corretamente, recalculando o CRC. Toda a inteligência dessa camada está embutida na placa de rede. A camada física executa um papel-chave na comunicação entre computadores, mas os seus esforços sozinhos não são suficientes, de modo que cada uma de suas funções tem suas limitações. A camada de enlace fornece soluções para as limitações da camada física. A seguir, comentaremos as soluções propostas:

- A camada física não pode se comunicar com as camadas de nível superior, assim a camada de enlace faz isso por meio do *Logical Link Control* (LLC).
- A camada física não pode nomear ou identificar computadores; a camada de enlace usa um processo de endereçamento utilizando o endereço físico da placa de rede (MAC) para identificação.
- A camada física pode descrever apenas os fluxos de bits; a camada de enlace usa o enquadramento para organizar, delimitar ou agrupar os bits.
- A camada física não pode decidir qual computador transmitirá os

seus dados binários de um grupo em que todos tentam transmitir ao mesmo tempo. A camada de enlace usa um sistema chamado *Media Access Control* (MAC) para garantir que cada computador transmita seus *bits* de forma única. Para isso, é utilizado o protocolo CSMA/CD. Essa camada, por meio do protocolo CSMA/CD, também identifica e contorna os problemas gerados pelas colisões. Mais adiante, apresentaremos a tabela 3.2, que resume os detalhes das camadas do modelo de referência OSI.

A seguir, apresentaremos, de forma resumida, os detalhes das camadas do modelo de referência OSI:

- **Aplicação (***Application***)** – Converte os dados de uma mensagem de email (lida pelo usuário) em bits. Anexa um cabeçalho para identificar o computador emissor e o receptor. Nessa camada, ocorre a adaptação dos processos de aplicação ao ambiente de comunicação. Suas principais funções são determinar como ocorrerá o diálogo, identificar endereços ou nomes, controlar o acesso e a integridade dos dados.
- **Apresentação (***Presentation***)** – Assegura que a mensagem seja transmitida em uma linguagem que o computador receptor possa entender, geralmente o ASCII. Caso um computador transmita dados usando o formato EBCDIC, essa camada converterá os dados para o formato ASCII. Nela, também ocorrem a criptografia e a compressão de dados. Para isso, a camada de apresentação acrescenta outro cabeçalho especificando a linguagem, bem como os esquemas de criptografia e compressão. Um dos recursos implementados nesse nível é a criação de PIPES, os quais atuam como canos e são instalados pelo software de rede.
- **Sessão (***Session***)** – Abre a comunicação e tem a tarefa de manter a comunicação fluindo entre todos os nós da rede, determina fronteiras para o início e o fim da mensagem e estabelece se a mensagem será enviada em *half-duplex*, com cada computador enviando e recebendo alternadamente, ou em *full-duplex*, com ambos enviando e recebendo simultaneamente. Os detalhes dessas opções são colocados no cabeçalho da sessão. Essa

camada ainda fornece a estrutura de controle para a comunicação entre as aplicações, bem como estabelece, gerencia e termina conexões (sessões) entre aplicações. Nessa camada, são executadas funções de reconhecimento de nomes para efeito de segurança relacionada a aplicações que requeiram comunicação por meio da rede. É responsável também pela autenticação e permissão do uso da rede.

- **Transporte (***Transport***)** – É responsável pela transferência de dados entre dois pontos de forma transparente e confiável com funções como controle de fluxo e correção de erro fim a fim.
- **Rede (***Network***)** – fornece para as camadas superiores independência das tecnologias de transmissão e comutação usadas para conectar os sistemas. É responsável por estabelecer, manter e terminar conexões.
- **Enlace de dados (***Data Link***)** – Supervisiona a transmissão, confirma o checksum, endereça e duplica os quadros, além de manter uma cópia de cada quadro até receber a confirmação do receptor que o quadro chegou ou expirou em um tempo predefinido. É responsável pela transmissão confiável de informação por meio do enlace físico e por enviar blocos de dados (quadros/frames) com sincronização, controle de erro e de fluxo necessários.
- **Física (***Physical***)** – É responsável pela transmissão de uma sequência de bits de forma não estruturada em um meio físico. Trata das características mecânicas, elétricas, ópticas, funcionais e procedurais para acessar o meio físico.

A seguir, apresentaremos o modelo de referência TCP/IP, o qual é implementado pela Internet e na maioria das redes de empresas do mundo todo.

## 3.3 Modelo de referência TCP/IP

A ideia do modelo de referência TCP/IP surgiu durante a guerra entre os Estados Unidos e a extinta União Soviética. O Departamento de Defesa Americano tinha como objetivo manter a

comunicação entre as bases militares, mesmo que fosse apenas parte dela, em uma ocorrência de ataques ou catástrofes que afetassem os meios de comunicação. Dessa necessidade, surgiu a ARPANET, uma rede em que, mesmo tendo uma base destruída, a comunicação entre as outras continuaria intacta.

Para ilustrar melhor essa situação, imagine um mundo em guerra, entrecruzado por diferentes tipos de conexões: cabos, ondas de rádio, fibras ópticas e links de satélites. Pense, então, que talvez você precise que informações na forma de pacotes trafeguem independentemente da condição de qualquer dispositivo ou rede particular que, nesse caso, pode ter sido destruída pela guerra. Imagine ainda que o Departamento de Defesa dos Estados Unidos quisesse que seus pacotes fossem sempre, em qualquer condição, de um ponto a outro. Foi esse complexo problema de projeto que levou à criação do modelo TCP/IP e que se tornou, desde então, o padrão no qual a Internet se desenvolveu.

A ARPANET cresceu e se tornou a rede mundial de computadores conhecida como Internet. Quando se menciona TCP/IP, vem imediatamente a associação com a Internet, ocorrendo de modo idêntico o inverso: a Internet está diretamente relacionada à arquitetura TCP/IP. Esse modelo tem quatro camadas: a camada de aplicação, a camada de transporte, a camada de Internet e a camada de rede. É importante notar que algumas das camadas do modelo TCP/IP têm o mesmo nome das camadas no modelo OSI, embora não se possa confundi-las. A seguir, comentaremos cada uma das quatro camadas do modelo de referência TCP/IP.

### 3.3.1 Camada de aplicação

Os criadores do modelo de referência TCP/IP decidiram que os protocolos de mais alto nível, como HTTP, SSH, Telnet, SMTP, DNS, POP3, FTP etc., deveriam incluir os detalhes da camada de aplicação, apresentação e de sessão. Assim as três primeiras camadas do modelo de referência OSI são representadas por apenas uma camada no modelo de referência TCP/IP.

### 3.3.2 Camada de transporte

A camada de transporte possui extrema importância na comunicação entre dois equipamentos em uma rede TCP/IP. É importante observar que um fluxo dessa camada só se comunica com o seu fluxo par do dispositivo destino. A camada de transporte lida com questões de QoS (Qualidade de Serviço), controle de fluxo, controle de sequência e correção de erros. Os principais protocolos dessa camada são os protocolos TCP e UDP.

O TCP é um protocolo orientado à conexão, ou seja, ele mantém um diálogo entre a origem e o destino enquanto empacota as informações da camada de aplicação em unidades conhecidas por segmentos. A mensagem recebida da camada de aplicação será dividida em pedaços pequenos que serão repassados à camada de Internet. O TCP garante a entrega dos pacotes, assegura seu sequenciamento e providencia um checksum que valida tanto o cabeçalho quanto os dados do pacote. No caso de a rede perder ou corromper um pacote TCP durante a transmissão, é tarefa do TCP retransmitir o pacote faltoso ou incorreto. A retransmissão é feita baseando-se em um tempo acordado entre o receptor e o emissor. Essa confiabilidade torna o TCP o protocolo escolhido para transmissões baseadas em sessão, aplicativos cliente-servidor e serviços críticos, nos quais a qualidade é mais importante do que a velocidade.

Os cabeçalhos dos pacotes TCP requerem o uso de bits adicionais para assegurar o correto sequenciamento da informação, bem como um checksum obrigatório para garantir a integridade do cabeçalho e dos dados. Para garantia da entrega dos pacotes, o protocolo TCP requisita que o destinatário informe, por meio do envio de um *acknowledgement* (ACK), qual foi o último pacote recebido com sucesso. Orientado à conexão não significa que exista um circuito entre os computadores que se comunicam (o que poderia ser comutação de circuitos); significa que segmentos da camada de transporte trafegam entre dois computadores para confirmar que a conexão existe (informações de controle) logicamente durante um certo período. Isso é conhecido como comutação de pacotes.

O segundo protocolo da camada de transporte utilizado na Internet é o UDP (*User Datagram Protocol*). Esse protocolo não está presente no modelo de referência OSI, porque este especifica que o nível de transporte é composto de protocolos orientados à conexão, logo, como o UDP é um protocolo não orientado à conexão, não está presente no modelo de referência OSI. O protocolo UDP não é confiável, pois não implementa acknowledgements, janelas ou sequenciamento. O único controle feito é um checksum opcional, que está dentro do seu próprio header. O UDP é utilizado por aplicações que não geram altos volumes de tráfego na Internet. Como exemplos de protocolos que utilizam o UDP, podemos citar DNS, TFTP e DHCP.

### 3.3.2.1 Detalhes da camada de transporte

A camada de transporte é responsável por pegar os dados enviados da camada de aplicação e dividi-los em mensagens que serão transmitidas pela rede. Depois de receber os dados da camada de aplicação, essa camada adiciona informações para o seu controle, como a porta de origem, a porta de destino, entre outras informações. Essas portas serão utilizadas para diferenciar qual aplicação dentro do computador fez o requerimento das informações. Por exemplo, caso o usuário execute três interfaces do *browser* e requeira, para cada uma, uma página diferente, o servidor de páginas devolverá para cada aplicação iniciada o conteúdo requerido sempre para a mesma máquina (mesmo endereço); entretanto, dentre os itens de controle, está o número da porta que corresponderá a uma única aplicação. Quando as mensagens chegarem, serão apresentadas, na aplicação, à porta que lhes for correspondente.

A camada de transporte deve realizar o controle de fluxo, a correção de erros e o controle de sequência. A seguir, apresentaremos o que cada uma dessas responsabilidades significa.

#### Controle de fluxo

O controle de fluxo é útil para identificar situações de sobrecarga no

buffer de dados do receptor. Quando isso acontecer, o protocolo TCP pedirá ao remetente dos dados que reduza a velocidade de emissão, para que ocorram menos erros e descarte de pacotes, garantindo que os dados realmente cheguem ao destinatário e este possa processá-los. A seguir, analisaremos como o TCP trabalha para controlar o fluxo entre dois computadores.

Os mecanismos de transporte utilizam um sistema de controle de fluxo denominado janela deslizante. Esse mecanismo consiste na realização de um número de transmissões preestabelecidas sem necessitar de uma confirmação de chegada, o que minimiza o tempo de espera de confirmações. Quando há o envio dessa confirmação de chegada, a janela desliza para o próximo grupo de pacotes a ser enviado e envia esse novo grupo. O protocolo TCP utiliza a janela deslizante (*sliding window*) para permitir que uma quantidade configurada de bytes seja transmitida sem a necessidade de confirmação.

Cada computador mantém duas janelas deslizantes: uma para receber a informação e outra para enviar. O tamanho da janela indica a quantidade de informação que pode ser guardada no buffer do computador para transmissão ou recepção. O protocolo TCP, ao receber dados que serão transmitidos, coloca-os na janela de envio e adiciona um número de sequência a cada pacote colocado na janela. Quando um pacote é transmitido, o emissor ativa um temporizador, especificando quanto tempo esperará pelo ACK, antes de o pacote ser retransmitido. Para permitir a retransmissão em caso de falha, o emissor mantém uma cópia do pacote no seu buffer até receber o ACK do receptor.

Caso o temporizador do emissor chegue ao final e ainda não tenha recebido uma confirmação do receptor (ACK), inicia-se a retransmissão. Se o pacote for recebido fora de sequência, um temporizador de confirmação poderá ser ativado no receptor. Se durante esse tempo, os pacotes que faltam forem recebidos, o ACK será enviado; caso contrário, o pacote será descartado. Ao receber o ACK do receptor, o emissor desliza a janela de envio passando para a frente do último segmento confirmado e inicia a transmissão

da segunda parte dos dados. O reenvio de pacotes adiciona carga à rede e ao emissor, logo uma rede pode vir a ficar inutilizável se a quantidade de retransmissões for muito grande.

**Controle de sequência**

Quando uma informação é transmitida por meio de uma rede, os dados são divididos em mensagens de dados embalados em um pacote e enviados do emissor para o receptor. No envio, pode ocorrer de os pacotes chegarem ao receptor fora de ordem. Assim, quando recebe os pacotes, o receptor vai remontando os segmentos na ordem correta, baseando-se na numeração de cada pacote adicionada pela camada de transporte.

Podemos comparar esse controle de sequência com o envio de um livro muito grande pelo correio. Para baratear o custo, em vez de enviá-lo por inteiro, desmonta-se o livro em pequenas partes e envia-se cada parte em um envelope diferente. Essas cartas que contêm partes do livro podem alcançar o destino por meio de diferentes centros de distribuição dos correios, uns mais lentos e outros mais ágeis, de modo que, quando o receptor receber os envelopes, baseando-se na numeração das páginas de cada um, remontará o livro independentemente da ordem em que esses envelopes chegarem. Para cada grupo de pacotes (envelopes) que chega, o protocolo TCP situado na camada de transporte envia um pacote chamado de ACK (*acknowledgement*), informando que o pacote foi recebido com sucesso e que o emissor pode enviar o próximo grupo de pacotes.

**Controle de erros**

O controle de erros na camada de transporte tem o objetivo de detectar e corrigir erros gerados pelas camadas inferiores. A camada de transporte deve se preocupar com erros relacionados a integridade do conteúdo do pacote recebido, entrega duplicada ou pacotes recebidos fora de sequência.

Para identificar erros de conteúdo, a camada de transporte analisa o CRC (*Cyclic Redundancy Check*) do pacote recebido. Esse CRC é recalculado pelo receptor e, caso não esteja igual ao CRC enviado

pelo emissor, apontará erro no recebimento do pacote. Problemas dessa ordem podem ser gerados por ruídos na rede. No caso da entrega duplicada de um pacote, o protocolo TCP se baseará em um número que acompanha o pacote para saber se já foi ou não recebido. No caso do recebimento de um pacote em sequência diferente, o protocolo da camada de transporte, também por meio do número que acompanha o pacote, poderá recolocá-lo em ordem.

Para resolver problemas de conteúdo, os protocolos da camada de transporte no receptor enviam regularmente mensagens de retorno ao emissor, notificando-o da situação em que se encontra. Existem duas situações possíveis: a primeira trata dos pacotes enviados pelo emissor, mas não recebidos pelo receptor por questões de *time-out*; a segunda trata dos pacotes que, em decorrência de erros de CRC, foram descartados. Em ambos os casos, será necessária a retransmissão dos pacotes.

É importante observar que camadas inferiores à camada de transporte também fazem controle de erros de conteúdo, por isso tal atividade na camada de transporte acaba sendo redundante.

### 3.3.3 Camada de Internet

A finalidade da camada de Internet é endereçar, rotear e controlar o envio e a recepção dos pacotes recebidos da camada de transporte. Essa camada tem o objetivo de enviar pacotes da origem de qualquer rede para qualquer outra rede interconectada, fazendo que os pacotes cheguem ao destino, independentemente do caminho e das redes a serem percorridas para atingir o destino. O caminho escolhido para conduzir os pacotes leva em consideração o menor caminho a ser percorrido ou o menos congestionado. Pense nisso em termos do sistema postal.

Quando você envia uma carta, não sabe como ela vai chegar ao seu destino (existem várias rotas possíveis), mas o que realmente importa é que ela chegue. Caso essas correspondências possuam alguma sequência, a camada de transporte vai organizá-las no destino, mas quem vai conduzi-las é o protocolo da camada Internet.

O protocolo principal dessa camada é conhecido como protocolo de Internet (IP), porém existem outros que também atuam nessa camada, como o ARP (*Address Resolution Protocol*), o RARP (*Reverse Address Resolution Protocol*) e o ICMP (*Internet Control Message Protocol*).

A camada de Internet não é orientada à conexão e se comunica por meio de pacotes, ou seja, os pacotes IP ou ARP não possuem garantia de que chegarão ao seu destino, nem que serão recebidos na ordem em que foram enviados, assim quem deve organizá-los ou pedir retransmissão é o protocolo TCP, presente na camada de transporte.

O protocolo ARP é utilizado quando o emissor precisa saber qual é o endereço físico do receptor. Para isso, o emissor envia um pacote ARP na rede em *broadcast* contendo todos os campos conhecidos preenchidos, e o receptor retorna uma réplica ARP depois de preencher os campos desconhecidos. Ainda neste livro, detalharemos o protocolo ARP.

Por sua vez, o protocolo ICMP é responsável por garantir que roteadores e equipamentos interligados a roteadores sejam informados de que um destino não está mais disponível na rede. Como exemplo do uso desse protocolo, temos o comando *ping*, presente na maioria dos sistemas operacionais de rede. Depois de ser executado, esse comando informa ao usuário ou ao roteador se um equipamento destino está ou não respondendo na rede. Atualmente, o comando *ping* é um dos principais meios utilizados pelos usuários para garantir a comunicação entre dois pontos. Assim, o tempo de resposta apresentado pelo comando *ping* precisa ser interpretado corretamente.

#### 3.3.3.1 Tempo de resposta do comando ping

Um dos principais testes realizados pelos usuários para avaliar a conectividade com a rede e o tempo de resposta é feito pelo comando *ping*, que utiliza os protocolos IP e ICMP, presentes na camada Internet. Muitos usuários se baseiam no tempo de resposta do comando *ping* para avaliar se a comunicação está ou não adequada. O tempo de resposta deve ser interpretado corretamente,

pois o valor apresentado pelo comando dependerá da distância física entre o emissor e o receptor. Vejamos um exemplo sobre como avaliar o resultado do comando:

Considerando que a velocidade da luz no vácuo é de 300 km/ms, caso o pacote do comando *ping* viaje nessa velocidade, partindo do Paraná até Miami, nos EUA, teremos aproximadamente 7.000 km de distância entre o emissor e o receptor. O tempo de ida é a divisão de 7.000 km por 300.000 km/ms, resultando em um tempo de ida em torno de 23 ms (milissegundos). Precisamos contabilizar também o tempo de volta e, assim, o tempo total ficará em 46 ms. Entretanto, existem equipamentos eletrônicos no meio do caminho, como roteadores, switches, entre outros, que não conseguem transmitir dados na velocidade da luz. Dessa forma, o tempo real seria bem maior. Para se ter uma ideia, em uma rede bem ajustada, podemos conseguir um tempo de 20 ms quando o emissor e o receptor estiverem a 1.200 km, ou seja, o valor real é bem diferente do exemplificado com a velocidade da luz. Assim, ao avaliar o tempo do *ping*, leve em consideração a situação apresentada.

Outra questão importante é observar que um tempo de resposta de 150 ms é suportável em redes com transmissão de voz sobre IP, porém, acima disso, o usuário deverá com certeza buscar ajuda com a operadora que lhe forneceu seu link, pois comprometerá seus negócios. Um elemento que contribui com o aumento do tempo nas redes ópticas é o nível medido nos receptores ópticos. Assim, recomenda-se avaliar a potência do sinal medido em dBm (decibéis) da fibra óptica nos equipamentos instalados no endereço do cliente antes de iniciar uma avaliação nos ativos internos da rede. Os valores válidos deverão ser consultados nos manuais do fabricante dos equipamentos.

A seguir, apresentamos o resultado do comando *ping* que realmente poderá ser interpretado como lentidão, porém este teste foi realizado com um computador que acessou a Internet por meio de uma conexão 3G.

```
ping www.uol.com.br
Disparando homeuol.ipv6uol.com.br [200.147.67.142] com 32 bytes de dados:
```

```
Resposta de 200.147.67.142: bytes=32 tempo=437ms TTL=245
Resposta de 200.147.67.142: bytes=32 tempo=456ms TTL=245
Resposta de 200.147.67.142: bytes=32 tempo=268ms TTL=245
Resposta de 200.147.67.142: bytes=32 tempo=320ms TTL=245
Estatísticas do Ping para 200.147.67.142:
  Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (0% de perda),
Aproximar um número redondo de vezes em milissegundos:
  Mínimo = 268ms, Máximo = 456ms, Média = 370ms
```

Apesar da lentidão desta conexão, conseguimos navegar na Internet, acessar redes sociais, porém aplicações mais complexas, como VoIP e YouTube, poderão não funcionar adequadamente. Sempre deveremos realizar testes com o computador conectado diretamente em um cabo, pois, nesse ambiente, não sofreremos com as interferências que podem existir internamente a uma residência ou escritório.

### 3.3.4 Camada de rede

A seguir, descreveremos as características e as funções da camada de rede representadas no modelo de referência TCP/IP pelas camadas físicas e de enlace do modelo de referência OSI.

A camada de rede é responsável por converter as tensões elétricas recebidas pela placa de rede em bits 0s ou 1s. Em seguida, esses bits são agrupados em pacotes e entregues à camada superior, que, por sua vez, continuará repassando-os até chegar à camada de aplicação, na qual o conteúdo recebido será processado e apresentado ao usuário.

A camada de rede fornece uma interface elétrica, para transmissão dos sinais elétricos, uma interface óptica, para transmissão de sinais ópticos, e uma interface mecânica, para conexão dos diferentes conectores aos cabos presentes nas redes de computadores. A tabela 3.1 descreve as principais características inerentes à camada de rede:

*Tabela 3.1 – Características inerentes à camada física*

| Interface | Descrição |
|---|---|

| Interface | Descrição |
|---|---|
| Mecânica | Representa o ambiente físico para a junção entre o conector da placa de rede e o cabo utilizado. Como exemplo de cabos, temos: cabos par trançado, cabo de fibra óptica ou cabo coaxial. Os exemplos de conectores são RJ-45, BNC e os conectores de fibra óptica que podem variar entre:<br>- SFPs (Small Form-factor Pluggable), GBIC (Gigabit Interface Converter)<br>- XFP (10 Gigabit Small Form Factor Pluggable)<br>- QSFP (40 Gigabit Quad Small Form-factor Pluggable)<br>- CFP (100 Gigabit C Form-factor Pluggable)<br>Todas as questões e considerações sobre os conectores são gerenciadas pela camada de física. |
| Elétrica | A interface elétrica tem a função de controlar questões elétricas da transmissão, como impedância do sinal recebido, além de converter as tensões elétricas em bits 0 ou 1. A forma de conversão dos bits dependerá dos padrões de codificação configurados nas placas de rede, sendo Manchester para redes 10 Mbps ou NRZI para redes 100 Mbps. O algoritmo para a codificação dos sinais elétricos em bits fica instalado na placa de rede. |
| Óptica | A interface óptica tem a função de controlar questões ópticas como a potência em que o sinal é recebido e enviado. Esses valores devem sempre ficar dentro dos limites especificados pelos fabricantes. Tem ainda a função de converter a luminosidade em bits 0 ou 1 |

A camada de rede no modelo de referência TCP/IP também é responsável pelas funções descritas na tabela 3.2, as quais são indispensáveis para o funcionamento das redes de computadores.

*Tabela 3.2 – Funções da camada de rede*

| Função | Descrição |
|---|---|
| Estabelecimento/encerramento de conexões | Estabelece e encerra uma conexão mediante solicitação da camada de rede. |

| Função | Descrição |
|---|---|
| Sincronismo do quadro | Garante que os bits transmitidos na origem sejam entregues na mesma ordem enviada ao destino. |
| Controle de fluxo | Garante que o emissor não envie bits mais rápido do que o receptor possa receber. |
| Controle de erro | Garante que o conjunto de bits transmitidos seja o mesmo conjunto de bits recebidos. |

A seguir, apresentaremos uma comparação entre o modelo de referência TCP/IP e o modelo de referência OSI.

## 3.4 Comparação entre os modelos de referência OSI e TCP/IP

O modelo de referência TCP/IP, quando comparado ao modelo OSI, possui duas camadas formadas a partir da fusão de outras camadas: as camadas de aplicação (aplicação, apresentação e sessão) e rede (enlace e física). Na figura 3.1, podemos visualizar a comparação entre os dois modelos de referência com os protocolos divididos nas suas respectivas arquiteturas:

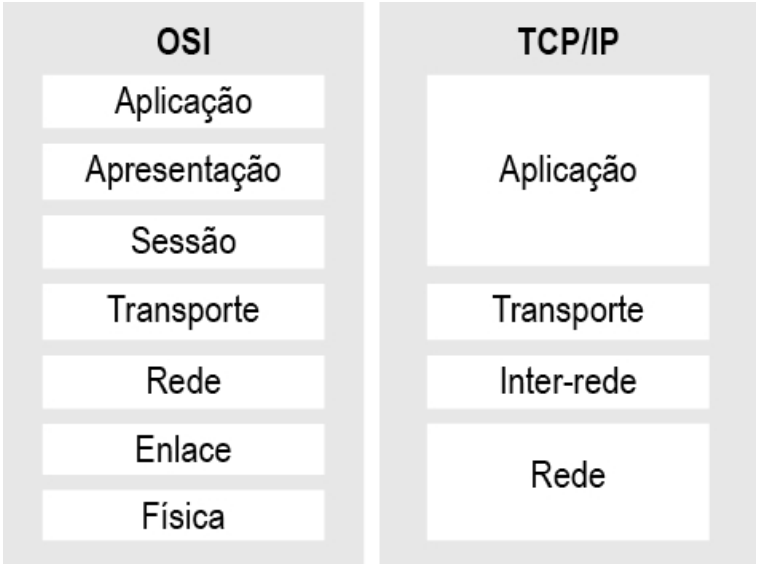



*Figura 3.1 – Comparação entre o modelo de referência OSI e o modelo de referência TCP/IP.*

Apesar de apresentarem alguns nomes de camadas semelhantes,

os modelos de referência OSI e TCP/IP possuem a forma de operação totalmente diferente. O modelo de referência OSI foi construído por um comitê que tinha como objetivo desenvolver um modelo de referência-padrão em camadas, no qual os protocolos poderiam ser desenvolvidos em cima; o modelo de referência TCP/IP foi desenvolvido pelo governo americano e pela comunidade acadêmica, de modo que os protocolos utilizados não poderiam ser substituídos, pois o modelo de referência foi criado baseando-se nos protocolos.

Em termos de flexibilidade de substituição de protocolos, caso necessário, o modelo de referência OSI, por ter sido desenvolvido antes da definição dos protocolos, possui vantagens quando comparado ao modelo de referência TCP/IP, visto que esse modelo foi desenvolvido em cima dos protocolos já existentes. É importante lembrar que o modelo de referência OSI especifica que os protocolos da camada de transporte devem ser orientados à conexão. Logo, nesse modelo de referência, o protocolo UDP não está presente.

## 3.5 Exercícios do capítulo 3

**1**. Qual o principal objetivo da arquitetura OSI/ISO?

**2**. Quantas e quais são as camadas dos modelos de referência OSI e TCP/IP?

**3**. Que camada do modelo OSI é responsável pelas funções de criptografia, conversão de códigos e formatação?

a) Apresentação.

b) Sessão.

c) Transporte.

d) Física.

**4**. O modelo de referência OSI é:

a) Padrão direcionado à interconexão homogênea.

b) Padrão de arquitetura proprietária.

c) Exemplo de sistema fechado.

d) Exemplo de sistema aberto.

**5**. Que camada do modelo OSI suporta diretamente as aplicações do usuário final?

a) Aplicação.

b) Sessão.

c) Apresentação.

d) Rede.

**6**. Qual é a camada do modelo OSI que atua como um dispositivo de chaveamento (switch) para a rede local?

a) Física.

b) Enlace.

c) Rede.

d) Transporte.

**7**. A camada OSI de comunicação de dados, que atende às funções de criptografia, compreensão de texto e conversão de padrões de terminais, é a camada de:

a) Sessão.

b) Aplicação.

c) Apresentação.

d) Transporte.

**8**. Em qual camada do modelo OSI atua o dispositivo bridge:

a) **Físico** – A camada física é a única que possui acesso físico ao meio de transmissão da rede. Cuida de diversos fatores, como especificações elétricas, mecânicas, funcionais e de procedimento de interface física entre o equipamento e o meio de transmissão. Como exemplo, temos o controle da distância máxima dos cabos. Resumindo, a principal tarefa da camada física é adaptar o sinal ao meio de transmissão sem levar em conta o significado dos dados. Aqui não importa a sequência dos bits tratados individualmente.

b) **Camada de enlace** – A camada de enlace tem o objetivo de fornecer uma conexão confiável com o meio físico. Deve detectar

e, em alguns casos, corrigir erros que possam ter ocorrido no nível físico, como colisões de dados, por exemplo. Essa camada, diferentemente da camada física, gerencia o acesso ao meio de transmissão, o fluxo de dados em frames e sua sequência. Outro controle efetuado é a sincronização de dados transmitidos entre o receptor e o emissor. Em geral, isso ocorre quando os dados são transmitidos a taxas mais elevadas do que as suportadas pelo receptor, o que provocaria o esgotamento do buffer de recepção existente na placa de rede do receptor.

c) **Rede** – A tarefa da camada de rede é preparar o modo pelo qual os recursos existentes nas camadas inferiores serão utilizados para implementar conexões de rede, ou seja, aqui é reconhecida a existência de vários computadores conectados em rede, o que não ocorre nas camadas física e de enlace. É nessa camada que eventuais sub-redes com diferentes sistemas operacionais terão suas diferenças compatibilizadas, já que, para o usuário, o que interessa é o serviço a ser realizado, independentemente do sistema utilizado. Nesse nível, ocorrerão o roteamento e a escolha dos melhores caminhos.

d) **Transporte** – Nessa camada, encontramos os mecanismos para transferência de dados fim a fim. Sua principal função é negociar o *throughtput* (taxa de transferência de dados na rede). O tamanho dos pacotes trocados pelas camadas também deve ser compatibilizado, já que diferentes camadas trabalham com pacotes de tamanhos diferentes. Ainda nessa camada, os pacotes são colocados em ordem e checados para confirmar se formam a sequência completa dos dados enviados. Na camada de transporte, leva-se em conta a existência de diversas tarefas resultantes de diversos aplicativos em uso na rede. A camada de transporte cuida para que os dados sejam destinados à tarefa correta, ou seja, à aplicação correta.

**9**. A camada de enlace de dados é responsável por promover uma transmissão livre de erros à camada de rede. Dentre as funções apresentadas a seguir, identifique qual não é executada pela camada de enlace:

a) Enquadramento.

b) Controle de erros.

c) Controle de congestionamento.

d) Controle de fluxo.

**10**. O modelo de referência OSI é dividido em sete camadas. Qual das camadas a seguir é a que se preocupa com a comunicação fim a fim:

a) Camada física.

b) Camada enlace.

c) Camada rede.

d) Camada transporte.

**11**. Assinale a camada do modelo de referência OSI responsável por funções como controle de congestionamento e encaminhamento de pacotes:

a) Transporte.

b) Rede.

c) Sessão.

d) Apresentação.

**12**. Na arquitetura IEEE 802, o controle de enlace lógico (LLC) com o controle de acesso ao meio (MAC) é uma adaptação de qual camada do modelo de referência OSI?

a) Sessão.

b) Transporte.

c) Rede.

d) Física.

e) Enlace de dados.

**13**. (Sanepar, 2004) No que concerne ao modelo ISO/OSI, é incorreto afirmar:

a) A camada de transporte implementa um mecanismo de controle de fluxo, de forma a evitar que um host rápido possa sobrecarregar um host mais lento.

b) A arquitetura descrita pelo modelo OSI é largamente utilizada pela maioria dos protocolos de redes atuais.

c) Cada camada intermediária do modelo OSI, ao receber dados da camada superior, anexa um cabeçalho à informação recebida e transmite o item resultante à camada inferior.

d) Os padrões definidos para as camadas do modelo OSI são de difícil implementação e de operação ineficiente.

e) No modelo OSI, funções como controle de fluxo e detecção de erros são especificadas em mais de uma camada, o que é desnecessário.

**14**. Acerca do modelo OSI, definido pela ISO, avalie as seguintes afirmativas:

I. Os protocolos da Internet foram originalmente concebidos de acordo com o modelo OSI, mas em razão de esse modelo ter se tornado obsoleto, esses protocolos passaram a seguir o modelo TCP/IP.

II. O modelo OSI propõe uma pilha de protocolos, organizados em camadas hierarquicamente distribuídas, e foi criado com o propósito de padronizar protocolos de redes de computadores.

III. Os protocolos do modelo OSI somente se aplicam a redes de tecnologia local, também chamadas de LANs (*Local Area Networks*).

IV. O modelo de referência OSI é seguido por todos os protocolos de domínio público. Apenas protocolos proprietários não utilizam esse modelo.

Assinale a alternativa correta:

a) Somente as afirmativas I, II e III são verdadeiras.

b) Somente as afirmativas I e IV são verdadeiras.

c) Somente as afirmativas II e IV são verdadeiras.

d) Apenas a afirmativa II é verdadeira.

e) Apenas a afirmativa I é verdadeira.

**15**. (Sanepar, 2004) Relacione as camadas citadas do modelo ISO/OSI às funcionalidades correspondentes, enumerando a coluna da direita com base nas informações da esquerda:

| | |
|---|---|
| 1. Física | ( ) Responsável pelo roteamento. |
| 2. Enlace | ( ) Responsável pela representação sintática, compressão e criptografia dos dados. |
| 3. Rede | ( ) Controla a comunicação entre duas máquinas; sincronização. |
| 4. Sessão | ( ) Especifica interfaces mecânicas e elétricas. |
| 5. Apresentação | ( ) Protocolos de controle de acesso ao meio. |

Assinale a sequência correta de cima para baixo:

a) 5, 3, 2, 1, 4

b) 2, 1, 4, 3, 5

c) 3, 4, 5, 1, 2

d) 3, 5, 2, 1, 4

e) 3, 5, 4, 1, 2

**16**. (Copel, 2010) Marque a opção que indica funções executadas pelo protocolo de camada de rede do modelo OSI:

a) Multiplexação lógica e controle de fluxo.

b) Endereçamento lógico e roteamento.

c) Enquadramento e controle de erros.

d) Gerência de sessões de rede e autenticação.

e) Conversões de padrões e criptografia.

**17**. (Enade, 2008 – Computação) Uma arquitetura de rede é usualmente organizada em um conjunto de camadas e protocolos com o propósito de estruturar o hardware e o software de comunicação. Como exemplos, têm-se as arquiteturas OSI e TCP/IP. A arquitetura TCP/IP, adotada na Internet, é um exemplo concreto de tecnologia de interconexão de redes e sistemas heterogêneos usada em escala global. Com relação à arquitetura TCP/IP, assinale a opção correta:

a) A camada de interface de rede, também denominada intrarede, adota o conceito de portas para identificar os dispositivos da rede física. Cada porta é associada à interface de rede do dispositivo e

os quadros enviados transportam o número das portas para identificar os dispositivos de origem e de destino.

b) A camada de rede, também denominada inter-rede, adota endereços IP para identificar as redes e seus dispositivos. Para interconectar redes físicas que adotam diferentes tamanhos máximos de quadros, a camada de rede adota os conceitos de fragmentação e remontagem de datagramas.

c) A camada de transporte é responsável pelo processo de roteamento de datagramas. Nesse processo, a camada de transporte deve selecionar os caminhos ou rotas que os datagramas devem seguir entre os dispositivos de origem e de destino, passando, assim, através das várias redes interconectadas.

d) A camada de aplicação é composta de um conjunto de protocolos que são implementados pelos processos executados nos dispositivos. Cada protocolo de aplicação deve especificar a interface gráfica ou textual oferecida pelo respectivo processo para permitir a interação com os usuários da aplicação.

e) A arquitetura TCP/IP é uma implementação concreta da arquitetura conceitual OSI. Portanto, a arquitetura TCP/IP é também estruturada em 7 camadas, que são as camadas: física, de enlace, de rede, de transporte, de sessão, de apresentação e de aplicação.

**18**. (Enade, 2008 – Tecnologia em Redes de Computadores) A técnica de encapsulamento utilizada em arquiteturas de redes tem como objetivo prover a abstração de protocolos e serviços e promover a independência entre camadas. Por quê?

O encapsulamento esconde as informações de uma camada nos dados da camada superior.

Analisando as afirmações anteriores, conclui-se que:

a) As duas afirmações são verdadeiras e a segunda justifica a primeira.

b) As duas afirmações são verdadeiras e a segunda não justifica a primeira.

c) A primeira afirmação é verdadeira e a segunda é falsa.

d) A primeira afirmação é falsa e a segunda é verdadeira.

e) As duas afirmações são falsas.

**19**. (Enade, 2008 – Tecnologia em Redes de Computadores) As atuais arquiteturas de redes de computadores são baseadas em dois conceitos fundamentais: modelo em camadas e protocolos de comunicação. Com relação a esses conceitos, qual descrição a seguir aborda de modo consistente um aspecto da relação entre camadas e protocolos?

a) O uso de camadas em redes de computadores permite o desenvolvimento de protocolos cada vez mais abrangentes e complexos, em que cada camada adiciona, de maneira transparente, uma nova característica a um protocolo. A estruturação de várias funções no mesmo protocolo dá origem à expressão “pilha de protocolos”.

b) Os protocolos IP e TCP foram padronizados pela ISO para as camadas de rede e transporte, respectivamente. A estruturação do protocolo IP sobre o TCP dá origem à expressão “pilha de protocolos”.

c) Os protocolos atuam como um padrão de comunicação entre as interfaces das camadas de uma arquitetura de redes e se comunicam por meio da troca de unidades de dados chamadas de PDU. O uso de protocolos para a comunicação entre camadas sobrepostas dá origem à expressão “pilha de protocolos”.

d) As camadas das arquiteturas de redes de computadores foram concebidas para separar e modularizar a relação entre protocolos nas topologias lógica em barramento e física em estrela. A estruturação dos protocolos lógicos sobre os físicos dá origem à expressão “pilha de protocolos”.

e) As arquiteturas de redes de computadores são organizadas em camadas para obter modularidade e as funções abstratas dentro de cada camada são implementadas por protocolos. A estruturação com vários protocolos usados em camadas distintas dá origem à expressão “pilha de protocolos”.

CAPÍTULO 4

# Arquitetura Ethernet

O capítulo 4 apresenta em detalhes a arquitetura Ethernet, abordando sua história, os modos de transmissão *simplex*, *half-duplex* e *full-duplex*, a diferença entre sinalização analógica e digital e a arquitetura Ethernet no modelo de referência OSI. Também serão apresentados os detalhes do quadro Ethernet, abordando como são representados o início e o fim de um quadro e quais são os campos de controle utilizados pelo receptor para decidir se irá ou não processar o quadro recebido. Comentaremos também as formas de codificação Manchester, NRZI, 4D-PAM5, 8B/10B, DSQ128D/PAM-16 e 64B/66B. É importante lembrar que é por meio das formas de codificação que os equipamentos ativos (switches e roteadores) identificam com qual velocidade (10 Mbps, 100 Mbps, 1Gbps ou 10 Gbps) deverão operar.

## 4.1 História da arquitetura Ethernet

A arquitetura Ethernet é um padrão que deu certo e serve de exemplo a uma indústria que usa produtos-chave para dominar o mercado de transmissão de dados em redes locais. O padrão Ethernet deve seu sucesso ao seu criador, que liberou a ideia em vez de torná-la proprietária. O padrão Ethernet é uma tecnologia tão importante quanto o sistema operacional Microsoft Windows, e eles se diferenciam justamente na forma como foram entregues à indústria. A Microsoft segurou o código-fonte em suas mãos, enquanto o padrão Ethernet seguiu um caminho público, o que deu à indústria a possibilidade de investir nessa tecnologia, e por isso evoluiu nos últimos anos, atingindo velocidades de até 100 Gbps.

O Ethernet é uma combinação de software e hardware utilizados para conectar computadores em redes e foi desenvolvido pela Xerox que a cedeu à indústria. O Ethernet originou-se em meados de 1970 da mesma confluência de esforços de pesquisa que levou ao

desenvolvimento do modelo de referência TCP/IP, sobre o qual está baseada a Internet. Quando chegou à Xerox, em princípios da década de 1970, Robert Metcalfe voltou sua atenção para o desenvolvimento de uma rede para escritórios que, pela primeira vez, permitiria compartilhar equipamentos comuns, como impressoras, computadores pessoais e servidores de arquivos.

O resultado surgiu em 1973, quando ele e outros colaboradores da Xerox inventaram uma rede capaz de transmitir e receber dados a 3 milhões de bits por segundo (3 Mbps). A Xerox, reconhecendo que não precisava ficar no negócio de redes de escritórios, pois queria incentivar o uso de suas copiadoras, suas impressoras e seus computadores, decidiu ceder a tecnologia Ethernet a outras indústrias interessadas.

Chegar a ponto de ser um padrão totalmente padronizado custou muito empenho dos seus criadores e também apoio da indústria. Seis anos depois de ter sido patenteado, em 1979, o Ethernet ainda não tinha se transformado em produtos reais. Então, a Xerox deu um passo inusitado: patenteou o Ethernet de modo que garantisse o uso da tecnologia como um padrão aberto. A ideia era ceder a licença de uso das patentes do Ethernet a qualquer pessoa ou empresa, mediante uma taxa de US$ 1 mil, e entregar a administração do padrão e de seus aperfeiçoamentos a um grupo da indústria.

## 4.2 A origem das redes Ethernet

Nas primeiras redes Ethernet, todas as estações compartilhavam o mesmo meio de transmissão, por meio de um cabo coaxial, ou seja, a configuração utilizada para essa conexão foi a de barramento com taxa de transmissão em torno de 3 Mbps. No início, esse padrão foi chamado de *Alto Aloha Network*, mas depois foi modificado para Ethernet pelo próprio criador.

Metcalfe optou pela palavra *ether* de maneira a descrever uma característica imprescindível do sistema; o meio físico, que transporta os bits para todas as estações, como se acreditava que acontecia com o éter, o meio que preenchia o universo e o espaço

entre os corpos celestes e que propagava as ondas eletromagnéticas pelo espaço. O padrão Ethernet teve sua aceitação pelo mercado depois de ser padronizado pelo IEEE.

## 4.3 Padrão IEEE 802.3

A especificação do sistema Ethernet foi supervisionada por um grupo da indústria conhecido como Comitê de Padrões 802.3, do Instituto de Engenheiros Elétricos e Eletrônicos (IEEE 802.3). A falta de padronização dificultava o progresso das pesquisas e a venda de equipamentos. Com o intuito de resolver esse problema, foi homologada ao IEEE, em 1980, a responsabilidade de criar e administrar a padronização do Ethernet. Desde a regulamentação pelo IEEE, suas especificações foram totalmente disponibilizadas, permitindo, assim, que qualquer empresa pudesse desenvolver uma placa de rede seguindo o padrão Ethernet. Essa abertura, combinada com a facilidade na utilização, bem como sua robustez, resultou em uma ampla utilização dessa tecnologia nas redes de computadores de todo o mundo.

## 4.4 O que é Ethernet?

O padrão Ethernet é representado em nossas redes locais pela placa de rede, também conhecida como NIC (*Network Interface Card*). Esse equipamento pode ser adquirido de diversos fornecedores, em razão da forma que foi conduzida a padronização do padrão Ethernet. Assim, quando queremos conectar computadores em rede, devemos necessariamente adquirir placas de rede que seguem esse padrão. No mesmo nível do Ethernet (IEEE 802.3), encontramos a arquitetura Token Ring (IEEE 802.5), o FDDI (*Fiber Distributed Data Interface*), o ATM e também os padrões 802.11b, 802.11g, 802.11n e 802.11ac que permitem a transmissão de dados em redes sem fio (*wireless*). Recentemente, chegaram ao Brasil os padrões GPON e EPON que também permitem o tráfego de dados em alta velocidade a longas distâncias (20 km). Dessa forma, se for preciso, o meio utilizado para transportar os dados pode ser alterado sem a necessidade de modificar protocolos e programas que

executam sobre esse padrão. A seguir, comentaremos os elementos e as características que compõem o padrão IEEE 802.3.

## 4.5 Modos de transmissão de dados em redes Ethernet

Eletronicamente falando, existem três formas possíveis de transmissão de dados, ou seja, três formas de utilização do meio físico, as quais serão descritas a seguir.

### 4.5.1 Simplex

O modo de transmissão *simplex* transmite a informação sempre no mesmo sentido. Nesse modo, um dispositivo sempre é o transmissor e o outro sempre é o receptor, de modo que esse papel não se inverte. Como exemplos do modo simplex, temos o rádio AM e FM, a TV e, em comunicações de dados, podemos citar um terminal de coleta de dados que apenas envia informações ao centro de impressão que dispõe de impressoras de grande porte. A figura 4.1 apresenta o modo simplex:


*Figura 4.1 – Transmissão simplex.*

### 4.5.2 Half-duplex

O modo de transmissão *half-duplex* (HDX) transmite a informação em ambos os sentidos, porém não simultaneamente. Em transmissões de dados *half-duplex*, a comunicação se faz uma vez em cada direção e tende, nas redes Ethernet, a operar somente em 40% ou 60% de seus 10 Mbps potenciais em razão das colisões. As placas de rede podem acomodar as colisões, porém ao custo da lentidão de toda a rede. Nesse modo de transmissão de dados, torna-se necessário o uso do protocolo CSMA/CD para a detecção de colisões e o controle de acesso ao meio. Como exemplo do modo *half-duplex*, temos o rádio amador ou walk-talk. Grande parte das redes locais (LANs) suporta esse modo de transmissão. A figura 4.2

apresenta o modo *half-duplex*.


*Figura 4.2 – Transmissão half-duplex.*

É importante observar que atualmente as operadoras que possuem redes metro Ethernet (redes metropolitanas formadas por switches e roteadores Ethernet) não oferecem esse tipo de comumicação devido à baixa qualidade na tansmissão. Por isso, em circuitos corporativos, devemos sempre optar pelo modo de transmissão *full-duplex*.

Outro ponto a que devemos nos ater é que quando interligamos dois switches de fabricantes diferentes (exs.: Cisco e Datacom), ambos, automaticamente, utilizam a autonegociação entre suas portas para fechar na velocidade máxima, que pode ser 100 Mbps, 1 Gbps ou 10 Gbps. Porém, podem ocorrer problemas na autonegociação e tais portas, em vez de fechar em *full-duplex,* acabam fechando em *half-duplex*, tornando a comumicação lenta e com perda de pacotes. Assim, como sugestão, para eliminar tal situação, sempre que a conexão ocorrer entre equipamentos diferentes, devemos nos ater a isso e, sempre que possível, forçar a velocidade das portas e desligar a autonegociação.

### 4.5.3 Full-duplex

Ethernet *full-duplex* dobra o *throughput* (velocidade em Mbps) da rede Ethernet *half-duplex* tradicional, combinando comutação de rede em alta velocidade com transmissão e recepção simultânea. O modo *full-duplex* (FDX) permite a comunicação simultânea entre duas estações, entretanto o enlace deve ser ponto a ponto, utilizando determinados meios, como o par trançado ou a fibra óptica. A seguir, analisaremos os requisitos definidos para a operação *full-duplex*.

- O meio deve ter caminhos independentes para transmissão e recepção, tipicamente par trançado e fibra óptica. Existem

exatamente duas estações conectadas ao enlace ponto a ponto, assim o algoritmo de controle de acesso ao meio (CSMA/CD) não é utilizado.

- Ambas as estações devem estar configuradas para funcionarem no modo *full-duplex*.

Conforme comentado nos equipamentos ativos atuais, utiliza-se autonegociação e, assim, o modo *full-duplex* será escolhido automaticamente. Caso se verifiquem problemas, deveremos desligar a autonegociação. Como exemplo de equipamentos que normalmente exigem que o administrador de rede interfira e force o modo full-duplex temos os encoders/decoders, utilizados para a transmissão de dados de TV. Seus encoders/decoders normalmente exigem que a autonegociação seja desligada e o modo full-duplex, forçado.

Felizmente, os hubs não operam nesse modo e os benefícios são sentidos em enlaces entre switches. Pelo fato de poder operar em ambas as direções, o modo *full-duplex* exige que a rede utilize um switch como concentrador central. Essa necessidade se dá em razão de o *full-duplex* usar conexões ponto a ponto, estando essa conexão livre de colisões. A conexão entre o computador e o switch não é compartilhada com os outros computadores, de forma que cada computador fica fisicamente em segmentos diferentes. Assim, para essa situação, o protocolo CSMA/CD não precisa ser utilizado. O *full-duplex*, aprovado em 1997, está especificado no suplemento IEEE 802.3x do padrão Ethernet. Como exemplo do modo *full-duplex*, temos o telefone e as redes de computadores que possuem placas de rede com essa característica. A figura 4.3 apresenta o modo *full-duplex*:


*Figura 4.3 – Transmissão full-duplex.*

É importante observar que as operadoras que possuem redes metro (redes metropolitanas formadas por switches) preferencialmente oferecem esse tipo de comumicação devido à alta qualidade exigida pelos clientes.

## 4.6 Sinalização nas redes Ethernet

Nas redes Ethernet *full-duplex*, a sinalização utilizada é a digital, que permite somente dois estados representados pelo bit 0 e pelo bit 1. A seguir, comentaremos as sinalizações digital e analógica, muito utilizadas nas transmissões de dados via linha telefônica.

### 4.6.1 Sinalização analógica

No mundo real, as informações são analógicas, isto é, as tensões transmitidas podem assumir qualquer valor em volts ao longo do tempo, dentro do intervalo -8 a +8 volts, por exemplo. O som e a luz são exemplos de sinais analógicos. A figura 4.4 apresenta um sinal analógico.

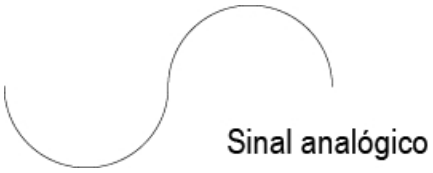



*Figura 4.4 – Sinal analógico.*

A grande vantagem da informação analógica é a possibilidade de representar qualquer valor, ao mesmo tempo que essa é sua grande desvantagem. Como o receptor é também analógico e o sinal analógico pode assumir qualquer valor ao longo do tempo (qualquer voltagem), o receptor não tem como verificar se o sinal recebido está ou não correto. Com isso, se houver qualquer ruído no caminho, como uma interferência eletromagnética no cabo, alterando a informação original, o receptor, mesmo que verificasse se existem erros, aceitaria a informação como correta ou solicitaria a retransmissão. Como existem inúmeras fontes de interferência eletromagnética, o uso de informações analógicas é inviável em sistemas de computadores. Nos sistemas de computadores, a informação enviada (bits enviados) deve ser exatamente a mesma que a recebida na outra extremidade.

### 4.6.2 Sinalização digital

Os computadores usam um sistema de informação digital em que,

dependendo da técnica de codificação, são possíveis dois valores, o bit 0 (representado pela variação de tensão de 5 volts a 0 volt) e o bit 1 (representado por uma variação de tensão de 0 volt a 5 volts). O exemplo aqui apresentado segue a codificação Manchester utilizada em redes Ethernet operando a 10 Mbps. Em redes que operam a 100 Mbps, utiliza-se a codificação NRZI, enquanto em redes 1 Gbps, utiliza-se a codificação 4D-PAM5 quando a transmissão ocorre por cabos do tipo par trançado e 8B/10B quando a transmissão ocorre sobre fibra óptica. Com essas técnicas de codificação, tereremos outros valores de voltagens. Atualmente, o padrão Ethernet permitiu a utilização em grande escala da transmissão em 10 Gbps. Para essa velocidade, utiliza-se a codificação DSQ128D/PAM-16 quando a transmissão ocorre por cabo par trançado e 64B/66B quando a transmissão ocorre sobre fibra óptica. Nesse modelo de codifição no cabo par trançado, o termo PAM16 representa 16 diferentes valores de voltagens.

Na sinalização digital, que só pode representar dois valores, ao contrário do sistema analógico, que pode representar infinitos valores, o receptor pode simplesmente descartar qualquer valor diferente de 0 e 1 que receba. Assim, caso o dado seja corrompido no meio do caminho por causa de um ruído qualquer, o receptor tem como recusar o seu recebimento, caso o sinal recebido seja diferente de 0 ou de 1. Fisicamente falando, o 0 e o 1 são tensões elétricas que tradicionalmente variam de 0 volt a 5 volts ou de 5 volts a 0 volt, conforme o protocolo de codificação. Como os dados transmitidos são, na realidade, números, o dispositivo receptor pode usar mecanismos de correção de erro para verificar se o quadro enviado está ou não correto. O receptor, antes de enviar o quadro Ethernet para o destino, efetua um cálculo matemático, baseando-se nos bits que serão enviados, chamado de CRC (*Ciclic Redundance Check*). No destino, depois do recebimento do quadro, este refaz o CRC e compara com o valor enviado; se forem iguais, o quadro foi recebido com sucesso.

Os computadores só entendem números, portanto toda e qualquer informação é transmitida pela rede em forma de números. Por

exemplo, quando mandamos um email, apesar de a mensagem conter caracteres e até mesmo fotos, essas informações são transmitidas pelos cabos da rede em forma de números, uma sequência de 0 e 1. Essa transformação é feita pelas camadas do modelo de referência TCP/IP apresentadas no capítulo 3. O computador-receptor trata de pegar esses números e transformá-los novamente em dados compreensíveis por nós, sendo essa conversão realizada pelos protocolos de rede situados nas camadas 1 e 2 do modelo de referência OSI e na camada 1 do modelo de referência TCP/IP. A figura 4.5 apresenta um sinal analógico e o mesmo sinal no formato digital.


*Figura 4.5 – Sinal digital.*

### 4.6.3 Camadas LLC e MAC

O modelo de referência OSI foi adaptado para referenciar também as redes locais. A camada de enlace foi subdividida em duas camadas conhecidas por LLC (*Logical Link Control*) e MAC (*Media Access Control*). A seguir, comentaremos sobre as camadas formadas pela subdivisão da camada de enlace.

- A camada LLC é responsável por adicionar informações de qual protocolo na camada de rede (exs.: IP, IPX) foi o responsável por gerar os dados, adicionar os endereços MAC origem e MAC destino, fornecer serviços como multiplexação na comunicação fim a fim, controle de fluxo, controle de erros e definição de diferentes classes de serviço. O endereço MAC conhecido também por endereço físico ou endereço Ethernet é uma maneira única para identificação de uma interface (placa) de rede na rede.
- A camada MAC é responsável por manipular as características específicas das várias tecnologias de redes locais (exs., Ethernet, Token Ring), isto é, fica responsável pelo acesso ao meio. Nessa camada, a informação é formatada (delimitada) em quadros (*frames*). Um quadro representa a exata estrutura dos dados

fisicamente transmitidos entre dois equipamentos.

#### 4.6.3.1 Características gerais da subcamada MAC

O Ethernet é um padrão de camada física e camada de enlace; opera a 10 Mbps, 100 Mbps, 1 Gbps, 10 Gbps, 40 Gbps ou 100 Gbps, com quadros que possuem tamanho entre 64 e 1.534 bytes (quando se utiliza QinQ). O endereçamento é feito por meio de uma numeração, que é única para cada host, com 6 bytes, sendo os primeiros 3 bytes utilizados para a identificação do fabricante (definidos pela IEEE e específicos de cada fabricante) e os 3 bytes seguintes, para o número sequencial do dispositivo de rede, seja placa de rede, seja porta de roteador. Na tabela 4.2, apresentaremos exemplos de endereços MAC:

*Tabela 4.2 – Endereço MAC e seu fabricante*

| Endereço MAC | Fabricante |
|---|---|
| 00 00 0C XX XX XX | Cisco |
| 00 E0 98 XX XX XX | LinkSys |
| 00 10 5A XX XX XX | 3Com |
| 08 00 20 XX XX XX | Sun |
| 08 00 5A XX XX XX | IBM |
| 00-09-6B-XX-XX-XX | Intel |

A subcamada MAC pertence à camada 2 do modelo de referência OSI. Ela controla a transmissão, a recepção e atua diretamente no meio físico, de modo que cada tipo de meio físico requer características diferentes da camada MAC. A seguir, descreveremos as características da camada MAC:

- Modo de transmissão *half-duplex* ou *full-duplex*.
- Encapsulamento dos dados das camadas superiores.
- Desencapsulamento dos dados para as camadas superiores.
- Transmissão dos quadros.
- Recepção dos quadros.

### 4.6.3.2 Quadro Ethernet

O quadro Ethernet é dividido em campos, os quais carregam informações de vital importância para a comunicação entre computadores. A seguir, serão apresentados os campos que compõem o quadro Ethernet:

- **Preâmbulo** – Cada quadro começa com um preâmbulo de 7 bytes, cada um contendo o padrão de bits 10101010, assim os equipamentos de rede sempre receberão esse conjunto de 7 bytes no início de um quadro. A sequência de bits segue sempre esse padrão, mas a forma de enviá-los pela rede muda de acordo com os protocolos de codificação, como Manchester, NRZI ou 4D-PAM5. Dessa forma, já no início da comunicação, o concentrador (switch), de acordo com a forma que receber os bits, definirá sua taxa de transmissão. É importante observar que o campo preâmbulo com o campo SFD formam um padrão de sincronismo, isto é, ao encontrar 7 bytes 10101010 e um byte 10101011, o dispositivo receptor saberá que está diante do início de um quadro.
- **SFD (***Start Frame Delimiter***)** – Delimitador inicial do quadro de rede. Esse é sempre um byte 10101011.
- **Endereço MAC destino** – Nesse campo, é inserido o endereço MAC da placa de rede de destino, que possui 6 bytes.
- **Endereço MAC origem** – Nesse campo, é inserido o endereço MAC da placa de rede de origem, que possui 6 bytes.
- **Comprimento** – Indica quantos bytes estão sendo transferidos no campo de dados do quadro, já que o campo de dados de um quadro Ethernet tem tamanho variável e não fixo.
- **Dados** – São os dados enviados pela camada acima da camada de Controle de Acesso ao Meio (enlace dividido em duas – MAC e LLC). Esse campo possui comprimentos mínimo de 46 bytes e máximo de 1.500 bytes. O conteúdo desse campo corresponde aos dados gerados na camada de aplicação.
- **PAD** – Se a camada de Controle do Link lógico (LLC) enviar menos do que 46 bytes no campo dados para a camada de

Controle de Acesso ao Meio (MAC), então serão inseridos dados chamados de PAD, para que o campo de dados atinja o seu tamanho mínimo de 46 bytes. Como o campo de dados do quadro usado em redes Ethernet é variável (pode ter entre 46 e 1.500 bytes), o tamanho total do quadro Ethernet (campo dados + campos de controle) torna-se variável, de modo que o tamanho mínimo de um quadro Ethernet é de 72 bytes e o tamanho máximo é de 1.526 bytes sem o uso de VLAN, 1.530 bytes quando utilizamos VLAN e 1.534 quando utilizamos QinQ (802.1Q in 802.1Q ou VLAN in VLAN). O valor 72 se refere aos 46 bytes referentes ao tamanho mínimo do campo dados mais 26 bytes dos demais campos de controle. É importante observar que quando o tamanho do quadro Ethernet supera o MTU (*Maximum Transfer Unit*) padrão das interfaces e equipamentos de rede (ex.: switch), torna-se necessário ajustar esse parâmetro em todos os equipamentos envolvidos no caminho em que os dados seguirão.

- **FCS (***Frame Check Sequence***)** – Contém informações para o controle de correção de erros (CRC – *Cyclic Redundancy Check*). Possui 4 bytes ou 32 bits. O FCS não leva em consideração três dos blocos – ele próprio, os bits de sincronia (preâmbulo) e o SFD (ou seja, os conteúdos desses campos) não farão parte do cálculo do CRC.

O CRC é o resultado de uma operação matemática efetuada com os dados presentes no campo de dados do quadro, sendo responsabilidade da placa de rede, ao colocar um quadro de dados no cabo de rede, fazer esse cálculo e inseri-lo no quadro. Esse cálculo consiste em somar todos os bytes presentes no quadro de dados e enviar o resultado dentro do próprio quadro. A placa de rede do dispositivo receptor refará essa conta e verificará se o resultado calculado corresponde ao valor enviado pelo dispositivo transmissor. Caso os valores sejam iguais, significa que o quadro chegou intacto ao seu destino; do contrário, significa que houve algum erro na transmissão.

Podemos citar como exemplo de erro uma interferência no cabo que poderá causar diferença entre os bits transmitidos e os bits

enviados. Nesse caso, o dispositivo receptor pede ao transmissor uma retransmissão do quadro defeituoso. É importante observar que o protocolo responsável por solicitar a retransmissão é o TCP.

### 4.6.3.3 Características gerais da subcamada de Controle de Link Lógico (LLC)

A camada de controle do link lógico, que é regida pelo padrão IEEE 802.2, permite que mais de um protocolo seja usado acima dela (protocolos de camada de rede do modelo de referência OSI). Para isso, essa camada define pontos de comunicação entre o transmissor e o receptor chamados SAP (*Service Access Point* – Ponto de Acesso a Serviços). Na figura 4.6, exemplificamos três conexões entre os computadores A e B. Essas três conexões poderiam ser efetuadas por três diferentes protocolos presentes na camada superior da pilha de protocolos.

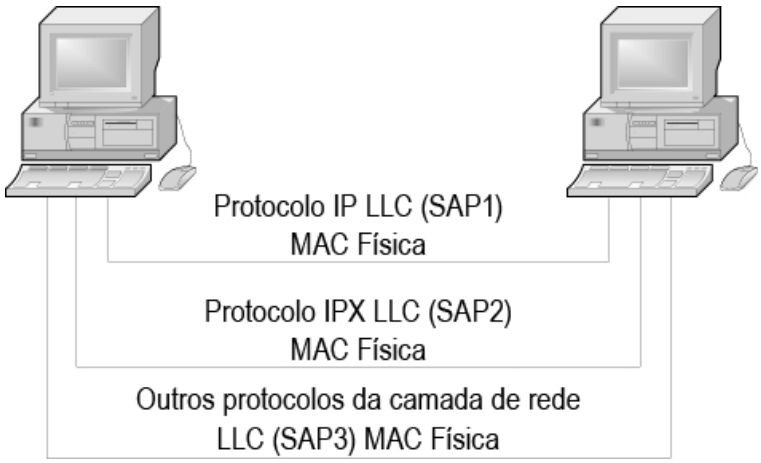



*Figura 4.6 – Conexões na camada LLC.*

### 4.6.3.4 Funcionamento da camada Controle do Link Lógico (LLC)

O papel da camada de controle do link lógico é adicionar, ao lado recebido, informações de quem enviou a informação (o protocolo responsável por ter passado essa informação. Ex.: IP ou IPX) para que, no receptor, a camada de controle do link lógico consiga entregar a informação ao protocolo de destino, que conseguirá ler a informação corretamente. A seguir, comentaremos a principal função da camada LLC.

### 4.6.3.5 Multiplexação

No nível de enlace, a multiplexação com a camada superior acontece por meio dos Pontos de Acesso a Serviços (*Service Access Points* – SAPs), ou seja, como a camada de enlace é dividida em MAC e LLC, temos que a camada LLC é quem se relaciona diretamente com a camada superior. Vejamos como ocorrem as identificações em ambas as camadas. Na camada MAC, endereços MAC carregados no cabeçalho identificam a estação de origem e uma ou mais estações de destino do quadro. De forma análoga, campos de endereçamento LLC identificam o SAP de origem (*Source Service Access Point* – SSAP) e os de destino (*Destination Service Access Point* – DSAP). Visto isso, chegamos à conclusão de que temos dois níveis de endereçamento na camada de enlace: o endereço MAC, que identifica um ponto de conexão física, e o SAP LLC, que identifica um usuário do nível de enlace, permitindo, assim, a multiplexação entre diferentes protocolos da camada de rede.

Os campos DSAP e SSAP de um quadro ou PDU (*Protocol Data Unit*) LLC contêm endereços de 7 bits. O bit menos significativo do campo DSAP indica se o endereço é individual ou de grupo e, no campo SSAP, indica se o quadro carrega um comando ou uma resposta. Uma PDU LLC é transportada no campo de informação de um quadro MAC, e o campo de controle da PDU LLC depende do serviço realizado. A seguir, comentaremos a estrutura do quadro LLC.

### 4.6.3.6 Estrutura de um quadro LLC

A camada LLC tem como objetivos:

- receber os dados do protocolo da camada superior (IPX, IP ou NetBEUI);
- montar o quadro com a informação de qual protocolo foi responsável por gerar os dados e enviar o quadro para a camada MAC.

A camada LLC passa para a camada MAC um conjunto de bytes contendo as informações citadas anteriormente, que pode variar entre 46 e 1.500 bytes. Desses bytes de dados, 8 bytes são usados

para armazenar informações de controle (soma dos campos DSAP, SSAP, Controle, Código, Tipo) inseridas por essa camada, e os dados (informações) são passados pela camada de rede. Esses dados adicionados referem-se aos campos apresentados na figura 4.7, que apresenta o formato do quadro LLC, e à tabela 4.3, que apresenta os campos do quadro.

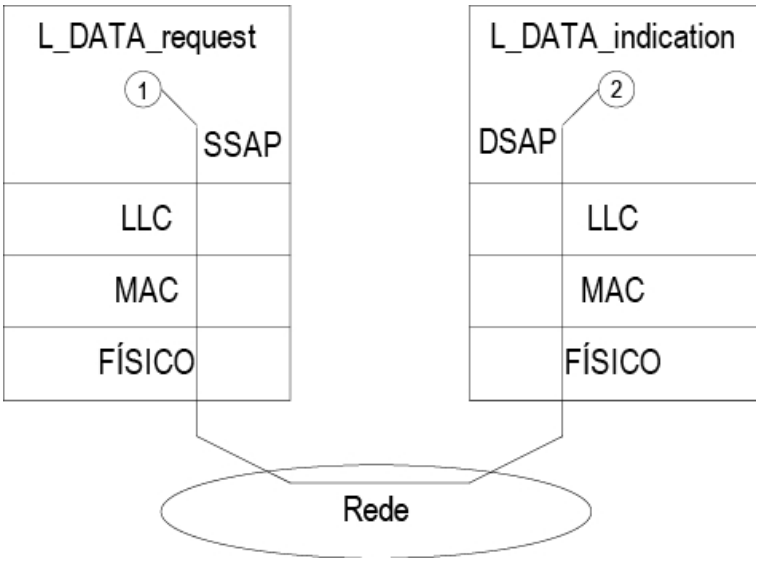



*Figura 4.7 – Quadro LLC.*

*Tabela 4.3 – Descrição do quadro LLC*

| Campo | Descrição |
|---|---|
| DSAP | (Destination Service Access Point): indica o endereço SAP de destino. Se o campo SNAP for usado, o DSAP será fixado em 10101010. O bit 0 do DSAP indica se é um endereço Unicast ou multicast. |
| SSAP | (Source Service Access Point): indica o endereço SAP de origem. Se o campo SNAP for usado, o SSAP será fixado em 10101010. O bit 0 do SSAP indica se o quadro LLC é um comando ou uma resposta. |

| Campo | Descrição |
|---|---|
| Controle | O campo controle pode assumir três valores: UI (Unnumbered Information), usado quando se está transmitido dados; XID (exchange identification), utilizado para troca de identificação entre receptor e transmissor. Exemplo: um comando que informa a identidade do emissor e pede a identidade do receptor, ou uma resposta, que retorna a identidade do receptor quando um comando é solicitado; e teste, no qual o transmissor envia um dado e o receptor o recebe e o envia de volta, a fim de testar a comunicação. |
| Código | É o código do fabricante/desenvolvedor do protocolo no IEEE. |
| Tipo | É o código dado pelo fabricante/desenvolvedor ao protocolo por ele desenvolvido. |

O SNAP (*Sub Network Access Protocol*) compreende os campos código e tipo. Foi incluído pelo IEEE na finalização da especificação da camada LLC e tem como principal objetivo identificar o fabricante ou o desenvolvedor do protocolo e o próprio protocolo.

## 4.7 Fast Ethernet

O Fast Ethernet é uma evolução do padrão Ethernet no sentido de permitir a transmissão de dados a 100 Mbps. O Fast Ethernet surgiu na década de 1990 como uma excelente alternativa ao antigo Ethernet, que transmitia dados a, no máximo, 10 Mbps.

O padrão Fast Ethernet trouxe no seu padrão o mesmo formato de endereçamento MAC, o formato e o tamanho do quadro e o mecanismo de detecção de erro. Como melhorias, o Fast Ethernet apresentou aumento de velocidade e modos de transmissão *half-duplex* ou *full-duplex*. É importante observar que para transmitir dados a 100 Mbps, devemos utilizar cabos com categoria 5 (CAT5) ou maior.

## 4.8 Gigabit Ethernet

Padronizado em junho de 1998 como IEEE 802.3z, teve como principal missão possuir as seguintes características:

- Utilização do frame Ethernet (IEEE 802.3).

- Manter compatibilidade com o padrão Ethernet e Fast Ethernet.
- Utilização do CSMA/CD como protocolo de controle de acesso ao meio físico.
- Compatibilidade com os padrões 10BASET e 100BASET.
- Operação em *half-duplex* e *full-duplex* a velocidade de 1 Gbps.

Esse novo padrão agregou valor não só ao tráfego de dados, como também ao de voz, vídeo e, ainda, sinal de TV em alta definição (*HD – High Definition*). O Gigabit Ethernet foi desenvolvido para suportar o quadro-padrão Ethernet. Isso significa manter compatibilidade com a base instalada de dispositivos Ethernet e Fast Ethernet e não requerer tradução do quadro. O Gigabit Ethernet possui taxa de transmissão de 1 Gbps e, em sua essência, segue o padrão Ethernet com detecção de colisão e, ainda, aceita os modos de transmissão *half-duplex* e *full-duplex*. Para operar em *half-duplex*, algumas mudanças foram necessárias, as quais serão comentadas a seguir. Atualmente, o modo *half-duplex* está praticamente extinto nos circuitos comercializados pelas operadoras de telecomunicações. Quando um circuito passa a operar em *half-duplex*, o cliente rapidamente percebe a diferença e busca na operadora a correção para voltar a operar no modo *full-duplex*. Com o modo *half-duplex*, percebem-se lentidão e perda de pacotes.

Para transmitir dados a 1 Gbps, devemos utilizar cabos com categoria 5 ou maior. É importante observar que o padrão 1 Gbps criou algumas nomenclaturas relacionadas ao padrão, como:

- **1000BASE-T** – Este padrão define que a distância de conexão entre dois equipamentos é de 100 metros. Utiliza cabo par trançado classificado na categoria 5 ou maior. Neste padrão, utilizamos os 4 pares do cabo par trançado para tansmissão e recepção seguindo o modo de transmissão full duplex.
- **1000BASE-SX** – Este padrão define que a distância de conexão entre dois equipamentos pode chegar a 1 km sobre fibra óptica multimodo.
- **1000BASE-LX/LH** – Este padrão define que a distância de conexão entre dois equipamentos pode chegar a 10 km sobre

fibra óptica monomodo ou 550 metros sobre fibra óptica multimodo.

- **1000BASE-EX** – Este padrão utiliza SFPs de longo alcance e define que a distância de conexão entre dois equipamentos pode chegar a 40 km sobre fibra óptica monomodo.
- **1000BASE-ZX** – Este padrão define que a distância de conexão entre dois equipamentos pode chegar a 70 km sobre fibra óptica monomodo.

É importante observar que cada um dos padrões comentados utiliza SFPs (*Small Form Factor Pluggable*) específicos que permitem alcançar as distâncias citadas. Um SFP pode ser adquirido de diversos fornecedores, como Datacom, Cisco, entre outros.

### 4.8.1 Padrão 10 Gigabit Ethernet

A entidade que comanda as pesquisas e a padronização desse padrão é o 10 Gigabit Ethernet Alliance. Este, na sua essência, segue o padrão Gigabit Ethernet, porém seu modo de transmissão é único e exclusivamente *full-duplex*, utilizando cabos par trançado ou cabos de fibra óptica do tipo multimodo ou monomodo. Em razão do aumento da distância abrangida pela fibra óptica, o 10 Gigabit Ethernet já está sendo utilizado em redes metropolitanas, pois os backbones das operadoras exigem velocidades de 100 Gbps ou mais. Atualmente é possível adquirir roteadores e switches no mercado com interfaces de rede que operam a 40 e 100 Gbps. A tabela 4.5 apresenta as diferenças entre os padrões Gigabit Ethernet:

*Tabela 4.5 – Comparação entre 1 Gigabit Ethernet, 10 Gigabit Ethernet e 40/100 Gigabit Ethernet*

| 1 Gigabit Ethernet | 10 Gigabit Ethernet | 40/100 Gigabit Ethernet |
|---|---|---|
| CSMA/CD e full-duplex | Somente full-duplex | Somente full-duplex |
| Fibra óptica e cabo par trançado categoria 5 e/ou | Somente fibra óptica (monomodo ou multímodo) | Somente fibra óptica |

| | | |
|---|---|---|
| maior | | (monomodo ou multímodo) |
| A distância suportada dependerá do GBIC ou SFP utilizados. Existem GBICs e SFPs bifibra (uma para transmissão e outra para recepção) que atingem até 100 km | A distância suportada dependerá do XFP utilizado. Se utilizarmos XFP 10G Short-Reach, alcançará 300 metros, enquanto se utilizarmos XFP 10G Long-Reach, poderemos chegar a 40 km | A distância suportada dependerá do QSFP (Quad Small Form-factor Pluggable) ou CFP utilizados |

É importante observar que o padrão 10 Gbps criou algumas nomenclaturas relacionadas ao padrão que serão descritas a seguir.

- **10GBASE-T** – Este padrão define que a distância de conexão entre dois equipamentos é de 100 metros. Utiliza cabo par trançado classificado na categoria 6 ou maior. Neste padrão, utilizamos os 4 pares do cabo par trançado para transmissão e recepção seguindo o modo de transmissão *full-duplex*. O termo T utilizado no nome do padrão vem do inglês e significa um cabo elétrico sobre 4 pares de fios trançados categoria 6 ou maior com sinalização bidirecional (*full-duplex*).
- **10GBASE-SR** – Este padrão define que a distância de conexão entre dois equipamentos é de 300 metros sobre fibra multimodo classificada como OM3. Neste padrão, utilizamos fibra óptica com comprimento de onda de 850 nm. O termo SR utilizado no nome vem do inglês e significa circuito óptico que utiliza um comprimento de onda curta (*Short* – 850 nm) sobre um par de fibra óptica multimodo com embaralhamento (*scRambled*).
- **10GBASE-LR** – Este padrão define que a distância de conexão entre dois equipamentos é de 10 km sobre 2 fibras monomodo. Neste padrão, utilizamos fibra óptica com comprimento de onda de 1.310 nm. O termo LR utilizado no nome do padrão vem do inglês e significa circuito óptico que utiliza um comprimento de onda longa (*Long* – 1310 nm) sobre um par de fibra óptica monomodo com embaralhamento (*scRambled*).
- **10GBASE-ER** – Este padrão define que a distância de conexão

entre dois equipamentos é de 40 km sobre 2 fibras monomodo. Neste padrão, utilizamos fibra óptica com comprimento de onda de 1.550 nm. O termo ER utilizado no nome do padrão vem do inglês e significa circuito óptico que utiliza um comprimento de onda extralonga (*Extra long* – 1550 nm) sobre um par de fibra óptica monomodo com embaralhamento (*scRambled*).

#### 4.8.1.1 Características do 10 Gigabit Ethernet

O padrão de redes 10 Gigabit Ethernet, dez vezes mais rápido do que o anterior, iniciou o seu desenvolvimento em 1999. Esse padrão é bastante interessante do ponto de vista técnico, pois, além da velocidade, o seu alcance máximo pode chegar a 100 km, utilizando cabos de fibra óptica monomodo.

O uso do padrão 10 Gigabit Ethernet representa o fim da utilização dos hubs. O padrão permite apenas o modo de operação *full-duplex*, em que ambas as estações podem enviar e receber dados simultaneamente, o que só é possível por meio do uso de switches. Isso encarece ainda mais o novo padrão, porém traz ganhos de desempenho consideráveis. Conforme comentado, somente permite o uso do modo *full-duplex* que está disponível nos switches. Com isso, acabam-se as colisões de quadros.

Outra mudança importante é que esse padrão no início da sua homologação só transmitia dados sobre cabos de fibra óptica. Entretanto, em 2006, o IEEE homologou o padrão 802.3an-2006 (10GBASE-T), que passou a transmitir dados sobre cabos par trançado. Porém, é importante observar que quando transmite dados sobre cabos de par trançado, a distância máxima é de 100 metros com cabo categoria 6A ou maior.

O 10 Gigabit Ethernet não se destina a substituir os padrões anteriores, pelo menos no médio prazo. Na verdade, a ideia é complementar os padrões de 10, 100 e 1.000 Mbps, oferecendo uma solução capaz de interligar redes distantes com uma velocidade comparável à dos backbones DWDM (*Dense Wavelength Division Multiplexing* – multiplexação densa por comprimento de onda), uma tecnologia muito mais cara, utilizada nos backbones das

operadoras de telecomunicações.

Suponha, por exemplo, que você precise interligar 5.000 PCs, divididos entre as universidades e órgãos públicos do estado do Paraná. Para essa rede, poderíamos utilizar um backbone 10 Gigabit Ethernet para interligar os roteadores de grande porte instalados entre as cidades estratégicas. Conectado a esse backbone, teríamos uma rede metro Ethernet que, de forma econômica, concentra e distribui a conectividade até a rede de acesso, que, por sua vez, é quem atende o cliente final. A rede metro é formada por switches gerenciávies (bem mais baratos que os roteadores) de grande porte, que concentram a conectivadade da rede de acesso. A rede de acesso é quem atende o cliente final que, neste caso, são as universidades e órgãos públicos. Dentro dessas localidades, teríamos as redes locais. A figura 4.8 apresenta a relação entre a rede que atende ao backbone que poderia ser 10 Gbps, a rede metro Ethernet que poderia ser de 1 Gbps e a rede de acesso que pode variar com pontos desde 1 Mbps até 1 Gbps. Na rede local normalmente operam os computadores com placas de rede 10/100/1000 Mbps.

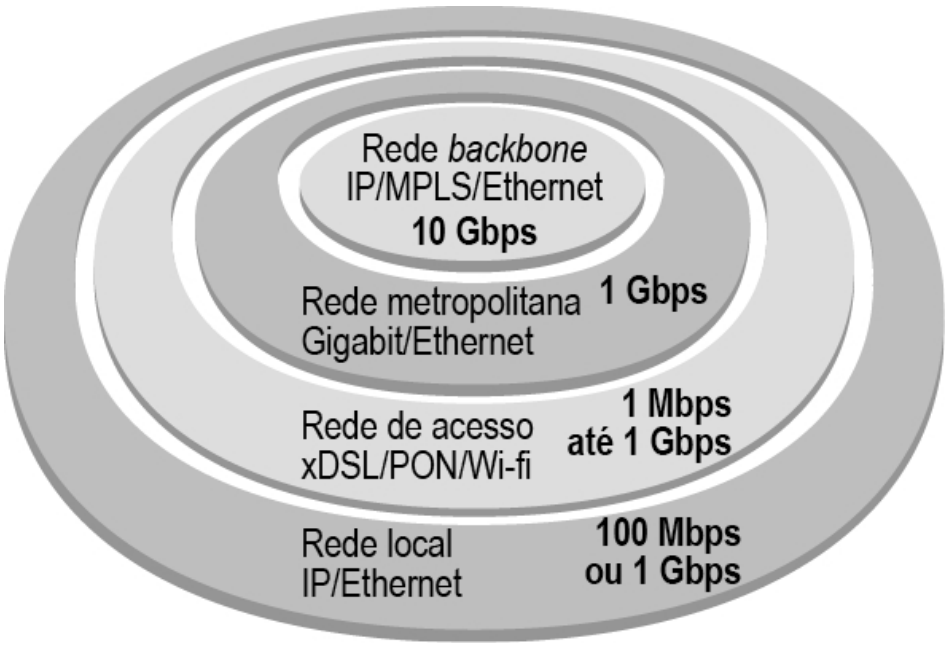



*Figura 4.8 – Relação entre backbone, rede metro e rede de acesso.*

O aumento da utilização da banda, a necessidade de qualidade de

serviço, a mudança no perfil do tráfego, entre outros fatores, impulsionaram a evolução do padrão Ethernet. No entanto, as mudanças não aconteceram somente no aumento da taxa, mas também no meio físico. Toda a evolução do padrão Ethernet foi acompanhada pela padronização feita pelo IEEE, fazendo parte do projeto 802.3.

### 4.8.2 Padrões 40 e 100 Gigabit Ethernet

Existem muitas razões que pressionam uma operadora a oferecer uma maior banda de transmissão em seu backbone, seja para aumentar o número de clientes que precisam de acesso à Internet em alta velocidade (links de 1 Gbps), a utilização de cloud computing (computação em nuvem) até o compartilhamento da rede IP para transmitir VoIP (voz sobre IP) ou sinais de TV em HD (*High Definition*) ou no formato 4k.

Ao perceber que a escalabilidade do padrão Ethernet precisava acompanhar as novas aplicações e demandas, o IEEE, em junho de 2010, disponibilizou o padrão 802.3ba com a intenção de aumentar a taxa de transmissão do padrão Ethernet. Esse padrão envolveu duas velocidades diferentes, sendo 40 Gbps e 100 Gbps. Os principais objetivos adotados pelo IEEE em relação ao padrão 802.3ba foram:

- Suporte a comunicação em *full-duplex*.
- Preservar o formato do quadro Ethernet especificado pelo padrão 802.3.
- Preservar o tamanho mínimo e o máximo do quadro Ethernet especificado pelo padrão 802.3.
- Operar com fibra óptica monomodo ou multimodo.

O advento de tecnologias inovadoras para datacenters, como virtualização de servidores e roteadores e cloud computing, além das atividades tradicionais, fez que os tradicionais datacenters precisassem se adaptar a essas novidades, oferecendo maior banda para inteligação de seus equipamentos.

Inicialmente, a velocidade de 40 Gbps foi focada para a

interligação de equipamentos dentro de datacenters, pois internamente a distância entre os equipamentos é de curto alcance. Para essa interligação a 40 Gbps, podemos utilizar cabos de cobre (*twinax cable* – similar ao cabo coaxial, porém com dois condutores) ou fibra óptica multimodo. Com cabos de cobre, consegue-se estender o cabo por 7 metros, enquanto com fibras ópticas multimodo (classificadas pelo EIA/TIA -492AAAD como OM4 – *Optical multi-Mode*), consegue-se estender um cabo por até 150 metros, ou seja, isso é suficiente para atender às necessidades de um datacenter.

O padrão 802.3ba (padrão que envolve 40 Gbps e 100 Gbps) evoluiu rapidamente e hoje permite interligar dois equipamentos a uma distância ainda maior. Assim, quando se precisa interligar dois datacenters, a fim de buscar redundância, ou, ainda, fechar um backbone entre duas cidades próximas, podemos utilizar fibras ópticas monomodo (*SMF – Single-Mode Fiber* classificadas como OM4) que permitem alcançar até 40 km. Uma fibra classificada como OM4 (*Optical multi-Mode*) possui um laser otimizado, desenhado para permitir a transmissão de dados em longa distância.

Por outro lado, a velocidade de 100 Gbps foi focada para atender a operadoras de telecomunicações com a finalidade de interligar suas redes ou, ainda, expandir a capacidade de transmissão de todo um backcone regional ou nacional. Com esse padrão, consegue-se, por meio de cabos de cobre chamados de *twinax cable*, interligar dois equipamentos também por 7 metros, enquanto com fibra óptica multimodo pode-se alcançar até 150 metros. No caso da velocidade de 40 Gbps para interligar dois equipamentos a uma distância maior, utilizamos fibra óptica monomodo, com a qual se permite atualmente alcançar 40 km de distância.

É importante observar que para trafegar dados a uma taxa de 40 Gbps, utiliza-se um cabo com quatro vias, e cada uma possui transmissão e recepção de dados (RX e TX) a 10 Gbps. Cada via é comumente conhecida como *lane*, ou seja, canal óptico que transmite e recebe dados. Cada uma delas representa um link de 10 Gbps, ou seja, para conseguir 40 Gbps, utilizam-se quatro vias, em

que cada uma transmite a 10 Gbps.

No caso da velocidade de 100 Gbps, utilizam-se dez vias de 10 Gbps. Nos padrões mais modernos, para alcançar distâncias de 40 km, precisamos de um conector e cabo que suportem quatro vias de 25 Gbps cada uma. Outro ponto importante a ser observado se refere à técnica de codificação que permaneceu a mesma utilizada pelo padrão 10 Gbps conhecida por 64B/66B.

#### 4.8.2.1 Interfaces utilizadas por 40 Gbps e 100 Gbps

Com o objetivo de minimizar o número de novos conectores, buscando simplificar a produção e promover um menor custo, o padrão 802.3ba apresentou três conectores a serem utilizados para as velocidades de 40 e 100 Gbps, conhecidos por QSFP (*Quad Small Form Factor Pluggable*), CFP (*Centum Form Factor Pluggable*) e CXP (modelo mais antigo).

O conector QSFP foi criado para transportar uma taxa de 40 Gbps sobre quatro canais de 10 Gbps cada um. Quando utilizado para conectar equipamentos por meio de cabo de cobre, permite uma distância máxima de 7 metros, porém, quando utilizado com fibra óptica multimodo, pode chegar a 150 metros. Em 2011, foi lançado o conector QSFP+ (*Quad Small Form Factor Pluggable Plus*) que permitiu aumentar a distância de conexão entre os equipamentos para 10 km, porém deve-se utilizar fibra óptica monomodo.

O conector CXP foi criado para substituir o conector SNAP-12 utilizado para redes Infiniband. Este conector nas redes operando a 100 Gbps possui curto alcance, sendo 7 metros quando utilizado cabos de cobre e 150 m com fibra óptica multimodo e conector MPO (*Multi-fiber Push On*).

O conector CFP permite a transmissão de dados de 40 Gbps quando se utiliza fibra óptica monomodo dupla, com quatro canais de 10 Gbps alcançando 10 km. Esse conector pode também transportar 100 Gbps a 150 metros com dez canais de 10 Gbps utilizando fibra multimodo com conector MPO. Para permitir transmitir a 40 km, é necessário ter em cada canal uma taxa de 25 Gbps, ou seja, em vez de utilizar dez canais de 10 Gbps, utilizam-se

quatro de 25 Gbps. Neste caso, consegue-se alcançar 40 km.

#### 4.8.2.2 Padrões criados para as velocidades de 40 e 100 Gbps

Durante a concepção dessas novas velocidades, alguns padrões de cabos foram criados a fim de formalizar a velocidade e a distância alcançada por cada um. Assim, para a velocidade de 40 Gbps, citamos os seguintes padrões:

- **40GBASE-KR4** – Padrão presente no backplane de placas de servidores e equipamentos ativos (switches, roteadores). O termo KR4 que faz parte do nome do padrão vem do inglês e significa padrão aplicado ao bacKplane de equipamentos ativos com embaralhamento (*scRambled*). Utiliza cabos metálicos e suporta uma distância de 1 metro suficiente para interligar equipamentos internos ao equipamento ativo.
- **40GBASE-CR4** – Padrão presente para interligação de equipamentos ativos (switches, roteadores) por cabo de cobre. Suporta uma distância de 7 metros suficiente para interligar equipamentos internos em um datacenter. O termo CR4 que faz parte do nome do padrão vem do inglês e significa cabos de cobre (*Copper*) com embaralhamento (*scRambled*). Indicado para interligar servidores a switches.
- **40GBASE-SR4** – Padrão presente para interligação de equipamentos ativos (switches, roteadores) por cabo de fibra óptica multimodo. Suporta uma distância de até 150 metros suficiente para interligar equipamentos internos em um datacenter. O termo SR4 que faz parte do nome do padrão vem do inglês e significa circuito óptico que utiliza um comprimento de onda curta (*Short* – 850 nm) sobre 4 fibras óticas multimodo com embaralhamento (*scRambled*) operando em *full-duplex*. Indicado para interligação interna entre equipamentos dentro de um datacenter.
- **40GBASE-LR4** – Padrão presente para interligação de equipamentos ativos (switches, roteadores) por cabo de fibra óptica monomodo. Suporta uma distância de até 10 km suficiente para interligar equipamentos localizados entre bairros de uma

cidade. O termo LR4 que faz parte do nome do padrão vem do inglês e significa circuito óptico que utiliza 4 comprimentos de onda longa (*Long* – 1310 nm) sobre 2 pares de fibra óptica monomodo (*single-mode*) com embaralhamento (*scRambled*). Indicado para interligar redes WAN e MAN.

- **40GBASE-FR** – Padrão presente para interligação de equipamentos ativos (switches, roteadores) por cabo de fibra óptica monomodo. Suporta uma distância de até 2 km suficiente para interligar dois equipamentos localizados em um campus universitário, por exemplo. O termo FR que faz parte do nome do padrão vem do inglês e significa circuito óptico que utiliza comprimentos de onda extralonga (1.550 nm) sobre 2 pares de fibra (*Fibers*) óptica monomodo (*single-mode*) com embaralhamento (*scRambled*). Indicado para interligar redes MAN.

É importante observar que o padrão 100 Gbps também criou algumas nomenclaturas que serão citadas a seguir:

- **100GBASE-CR10** – Padrão presente para interligação de equipamentos ativos (switches, roteadores) por cabo de cobre. Suporta uma distância de 7 metros suficiente para interligar equipamentos internos em um datacenter. O termo CR-10 que faz parte do nome do padrão vem do inglês e significa circuito elétrico que utiliza 10 pares de cabo metálico (*Copper*) operando em *full-duplex* com embaralhamento (*scRambled*). Indicado para interligar redes WAN e MAN e servidores a switches.
- **100GBASE-SR10** – Padrão presente para interligação de equipamentos ativos (switches, roteadores) por cabo de fibra óptica multimodo. Suporta uma distância de 100 metros com fibras multimodo OM3 e até 150 metros com fibra óptica multimodo OM4 (fibra com maior qualidade no momento – oferece largura de banda de 4.700 MHz-km com comprimento de onda de 850 nm). O termo SR10 que faz parte do nome do padrão vem do inglês e significa circuito óptico que utiliza um comprimento de onda curta (*Short* – 850 nm) sobre dez fibras óticas multimodo com embaralhamento (*scRambled*) operando em *full-duplex*. Indicado

para interligação interna entre equipamentos dentro de um datacenter ou de uma empresa.

- **100GBASE-LR10** – Padrão presente para interligação de equipamentos ativos (switches, roteadores) por cabo de fibra óptica monomodo. Suporta uma distância de até 2 km suficiente para interligar equipamentos localizados entre bairros de uma cidade. O termo LR10 que faz parte do nome do padrão vem do inglês e significa circuito óptico que utiliza comprimentos de onda longa (*Long*) com embaralhamento (*scRambled*).
- **100GBASE-LR4** – Padrão presente para interligação de equipamentos ativos (switches, roteadores) por cabo de fibra óptica monomodo. Suporta uma distância de até 10 km suficiente para interligar equipamentos localizados entre dois bairros de uma cidade. O termo LR4 que faz parte do nome do padrão vem do inglês e significa circuito óptico que utiliza comprimentos de onda longa (*Long*) com embaralhamento (*scRambled*). Este padrão utiliza quatro canais de 25 Gbps cada um e, por isso, alcança até 10 km. Indicado para interligar sedes de uma empresa localizadas em bairros diferentes.
- **100GBASE-ER4** – Padrão presente para interligação de equipamentos ativos (switches, roteadores) por cabo de fibra óptica monomodo. Suporta uma distância de até 40 km suficiente para interligar equipamentos localizados entre duas cidades próximas. O termo ER4 (*Extended Reach*) que faz parte do nome do padrão vem do inglês e significa circuito óptico que utiliza comprimentos de onda longa com embaralhamento (*scRambled*). Este padrão é o mais atual e ainda utiliza quatro canais de 25 Gbps cada um e, por isso, alcança até 40 km. Indicado para interligação de sedes de uma empresa localizadas entre cidades diferentes.

Ao adquirir equipamentos para operar nas velocidades atuais, toda empresa precisará avaliar as necessidades, criar um projeto e submeter aos fornecedores para que a compra seja adequada.

## 4.9 Formas de codificação de dados

A camada física do padrão IEEE 802.3 define tanto o tipo de topologia usada pela rede quanto o tipo de conector usado pela placa de rede e, consequentemente, o tipo de cabo usado. O mais importante a saber sobre a camada física do padrão 802.3 é que ela pega os bits 0 e 1 enviados pela camada de acesso ao meio (camada MAC) e não os envia diretamente para o cabo. É importante observar que os bits são primeiramente codificados, ou seja, cada bit será convertido em uma tensão elétrica, no caso dos cabos de par trançado, ou em luz, no caso dos cabos de fibra óptica.

Para entendermos melhor como essa codificação funciona, comentaremos o funcionamento dos protocolos Manchester, NRZI, 4B/5B, 4D-PAM5, 8B/10B, DSQ128D/PAM-16 e 64B/66B, que são utilizados por redes Ethernet operando a 10 Mbps, 100 Mbps, 1 Gbps, 10 Gbps, 40 Gbps e 100 Gbps respectivamente.

### 4.9.1 Codificação Manchester

A codificação Manchester transforma um bit 1 em uma descida de 5 volts para 0 volt e um bit 0 em uma subida de 0 volt para 5 volts, conforme mostra a figura 4.9.

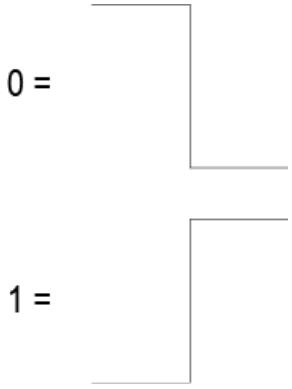



*Figura 4.9 – Codificação dos bits 0 e 1 no formato Manchester.*

O uso desse sistema de codificação é muito interessante, pois exige que o dado transmitido tenha sempre uma inversão de fase. Por exemplo, se o dado a ser transmitido for 00000000, o dado passará a ter 9 inversões de fase, ao passo que originalmente (sem

a codificação Manchester) não haveria inversões. Independentemente do dado que está sendo transmitido, sempre haverá uma inversão de fase por bit transmitido. Desse modo, cria-se um sistema de sincronismo entre o transmissor e o receptor, isto é, um sistema de clock. O sincronismo das estações emissora e receptora ocorre quando o emissor envia um bit ao receptor, e o recebimento desse bit acontece em um tempo acordado por ambos, ou seja, a cada 1 milésimo de segundo, um bit estará chegando.

Como a codificação Manchester requer uma variação de fase por bit enviado, o receptor em conjunto com esse circuito gerador de clock pode facilmente receber os bits que estão sendo enviados, isto é, saber o momento de início e o momento de término de cada bit enviado, já que haverá um sinal de sincronismo. Na codificação Manchester, torna-se desnecessário utilizar bits adicionais, como start bit e stop bit, pois a comunicação é síncrona entre o emissor e o receptor. Dessa forma, a transmissão torna-se mais eficiente. Na figura 4.10, será apresentado um exemplo de transmissão que utiliza a codificação Manchester:

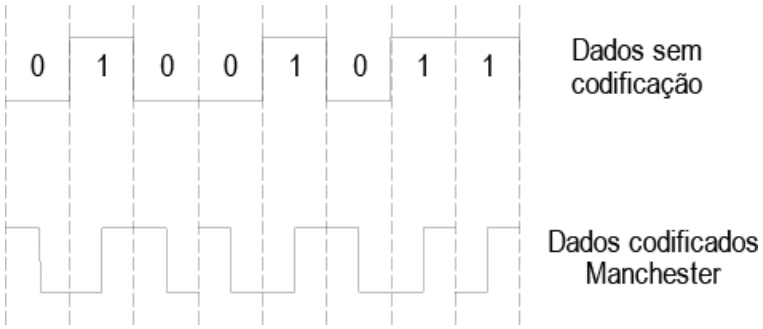



*Figura 4.10 – Exemplo de uma comunicação com codificação Manchester.*

## 4.9.2 NRZI

O sistema NRZI com o 4B/5B são responsáveis pela codificação dos bits em redes Fast Ethernet, as quais operam a 100 Mbps. Depois de a codificação 4B/5B realizar a sincronização, as transmissões ocorrem normalmente bit a bit entre o emissor e o receptor por meio de outro protocolo, conhecido como NRZI. O protocolo que efetivamente transporta e atua no meio físico em transmissões a

100 Mbps é o NRZI (*Non Return to Zero Inverted*), enquanto o protocolo 4B/5B realiza o sincronismo entre o emissor e o receptor.

Para que serve a codificação 4B/5B, se, na verdade, o protocolo que transmite os bits é o NRZI? Um pequeno atraso ao longo do tempo pode resultar em longo atraso, por isso o protocolo 4B/5B é utilizado com a finalidade de garantir a sincronização entre o emissor e o receptor.

É importante observar que o protocolo NRZI não possui sincronização e, portanto, deixa essa tarefa para protocolos auxiliares. Contudo, mesmo sem sincronização, a eficiência do protocolo NRZI, quando comparada com a codificação Manchester, chega a 80%.

### 4.9.3 Codificação 4B/5B

A principal função da codificação 4B/5B é mitigar os problemas relacionados a longas sequências de bits 0 ou bits 1, em transmissões que utilizam o par trançado ou a fibra óptica. Para isso, a codificação 4B/5B insere bits extras no fluxo original de bits, a fim de interromper as longas sequências de bits 1 ou bits 0.

Na metodologia da codificação 4B/5B, cada grupo de 4 bits, em um total de 16 grupos, é codificado em um código de 5 bits. O receptor deverá realizar o processamento inverso, convertendo o código de 5 para 4 bits, e processar os dados. A seleção dos códigos de 5 bits é feita de modo que cada um desses bits não contenha mais de um zero na frente nem termine com mais de dois zeros no final. Assim, quando esses códigos de 5 bits são enviados em sequência, não mais de 3 zeros consecutivos são encontrados, resolvendo a questão de longas sequências de 0s ou 1s. Os códigos de 5 bits são transmitidos pela codificação NRZI, e o resultado do esquema 4B/5B com o NRZI é de uma eficiência de 80% no transporte de dados, quando comparado com a codificação Manchester. A tabela 4.6 apresenta a relação entre os bits expressos em 4 bits que serão codificados em 5 bits.

É importante observar que quando temos mais de 3 zeros, estes serão codificados em 1; entretanto, as sequências de 1 são

mantidas. Isso acontece em razão de o protocolo NRZI sempre aplicar uma inversão de tensão para os bits 1. A figura 4.11 apresenta um exemplo de uma transmissão sendo codificada pelo NRZI (*Non Return to Zero, Invert on One*). A codificação 4B/5B é utilizada em redes Fast Ethernet.

*Tabela 4.6 – Bits expressos em 4 bits codificados em 5 bits*

| **Código dos dados em 4 bits** | **Código dos dados em 5 bits** | **Descrição** |
|---|---|---|
| 0 | 11110 | Decimal 0 |
| 1 | 1001 | Decimal 1 |
| 10 | 10100 | Decimal 2 |
| 11 | 10101 | Decimal 3 |
| 100 | 1010 | Decimal 4 |
| 101 | 1011 | Decimal 5 |
| 110 | 1110 | Decimal 6 |
| 111 | 1111 | Decimal 7 |
| 1000 | 10010 | Decimal 8 |
| 1001 | 10011 | Decimal 9 |
| 1010 | 10110 | Letra A |
| 1011 | 10111 | Letra B |
| 1100 | 11010 | Letra C |
| 1101 | 11011 | Letra D |
| 1110 | 11100 | Letra E |
| 1111 | 11101 | Letra F |
| Vazio | 11111 | IDLE |

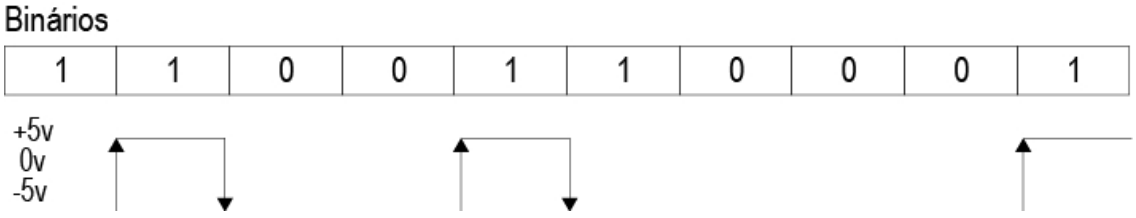



*Figura 4.11 – Transmissão codificada pelo NRZI.*

### 4.9.4 Codificação 4D-PAM5

O sistema Gigabit Ethernet, para a transmissão de dados sobre cabos de par trançado (*IEEE 802.3ab*) categoria 5 ou maior, utiliza um sistema de codificação chamado 4D-PAM5 (*4 Dimensional*, 5 *levels Pulse Amplitude Modulation/Amplitude de pulso de cinco níveis em quatro dimensões*), por meio do qual os dados são transmitidos por quatro pares de fios simultaneamente, ao contrário das redes que operam a 10 Mbps e 100 Mbps, nas quais são usados apenas dois pares.

Nesse padrão, são transmitidos dois bits de dados por vez nos quatro pares. Essa transmissão ocorre por meio de uma modulação por amplitude de pulso (PAM – *Pulse Amplitude Modulation*), isto é, em vez de os dados serem transmitidos em forma de duas tensões elétricas (uma para 0 e outra para 1), eles são transmitidos em forma de várias tensões elétricas, nesse caso, cinco tensões diferentes, por isso o nome PAM5. Quatro das cinco tensões são utilizadas para representar o conjunto de dois bits conforme mostra a tabela 4.7:

*Tabela 4.7 – Tensões utilizadas na codificação 4D-PAM5*

| **Conjunto de bits** | **Nível de tensão nominal do cabo par trançado** |
|---|---|
| 00 | -1 V |
| 01 | -0.5 V |
| 10 | 0 V |
| 11 | + 1 V<br>O nível de tensão + 1 é usado para transferir informações de controle, dentre elas informações para correção de erros. |

É importante observar que em uma rede que opera a 1 Gbps todos os pares são utilizados em um esquema bidirecional, ou seja, os mesmos pares são utilizados para transmissão e recepção, sempre full duplex. O Gigabit Ethernet utiliza um clock de 125 MHz, o mesmo utilizado pelo padrão 100 Mbps, porém como transmite 2 bits por vez, nos quatro pares, a taxa de transferência é oito vezes maior, ou seja, 125 MHz * 2 bits por sinal * 4, alcançamos 1 Gbps.

### 4.9.5 Codificação 8B/10B

O esquema de codificação adotado pelo padrão Gigabit Ethernet para a transmissão sobre cabos de fibra óptica (IEEE 802.3z) é o 8B/10B. A codificação 8B/10B é feita por meio do mapeamento de 8 bits de dados em 10 bits para a transmissão. A intenção desse mapeamento é garantir que a quantidade de bits 1s e 0s transmitidos tenha equilíbrio, ou seja, que não tenhamos muito mais 1s do que 0s. A conversão de 8 bits em 10 bits gera um acréscimo (*overhead*) de 25% nos bits transmitidos. A redundância em torno de 25% fornece os seguintes benefícios:

- Fácil recuperação do clock.
- Não há componente DC. Este padrão de codificação garante um equilíbrio DC, ou seja, significa que a média do sinal é nulo. Ser nulo significa que há equilíbrio entre a quantidade de bits 0s e 1s transmitidos. O aquecimento do laser de transmissão depende dos dados transmitidos, isto é, caso sejam enviados mais 1s do que 0s, haverá aquecimento. Tal situação acarretará maiores taxas de erros.
- Correção de erro.

Atualmente, a comunicação sobre 1 Gbps tornou-se obsoleta para atender ao backbone de uma operadora que exige links de, no mínimo, 10 Gbps. Entretanto, nas redes metro (rede composta de switches) ou rede de acesso (rede que chega ao endereço do cliente), essa velocidade ainda é muito utilizada.

### 4.9.6 Codificação DSQ128/PAM-16

O padrão 10GBASE-T é o padrão especificado pelo IEEE para a transmissão de dados a 10 Gbps sobre cabos de par trançado categoria 6A ou maior. O padrão 10GBASE-T aceita somente o modo de transmissão *full-duplex* e utiliza sinalização com 16 níveis PAM (*Pulse Amplitude Modulation*), isto é, em vez de os dados serem transmitidos em forma de duas tensões elétricas (uma para 0 e outra para 1), eles são transmitidos em forma de várias tensões elétricas, nesse caso, 16 tensões diferentes, por isso o nome

PAM16.

Para alcançar os 10 Gbps, transmite-se em *full-duplex* a uma taxa de 2.5 Mbps por cada par do cabo, assim, com os quatro pares, têm-se 10 Gbps. Comparando com os padrões anteriores para uma rede gigabit, por exemplo, cada um dos quatro pares transmite 250 Mbps, enquanto no padrão Fast Ethernet se transmitem 100 Mbps em dois pares, pois os outros dois não são utilizados.

### 4.9.7 Codificação 64B/66B

A codificação 64B/66B é o padrão de codificação especificado pelo IEEE para a transmissão de dados a 10 Gbps sobre cabos de fibra óptica.

No padrão 64B/66B, cada transferência consecutiva de 32 bits + 32 bits de dados é agregada em um vetor de 64 bits de dados que adicionará um header no ínicio do vetor. No início (*header*) desse vetor são inseridos outros 2 bits de sincronização, gerando, assim, um overhead de 3,125%, pois, para cada 64 bits de dados, transmitiremos, na realidade, 66 bits (ex.: 64 * 1,03125), ou seja, 3,125% bits a mais por transmissão. O header será utilizado primeiramente pelo receptor para alinhar o recebimento dos bits.

O conteúdo dos bits que formam o header dependerá do conteúdo transmitido nos 64 bits de dados. Existem duas possibilidades válidas para a composição dos bits do header. Vejamos:

- **Header composto dos bits 0b01** – Quando o vetor agora formado por 66 bits iniciar por 0b01, informará que este transporta apenas dados.
- **Header composto de 0b10** – Quando o vetor agora formado por 66 bits iniciar por 0b10, informará que este transportará um misto de cacacteres relacionados a dados e caracteres relacionados a controle, ou, ainda, transportará somente caracteres de controle.
- **Header composto de 0b00 ou 0b11** – Quando o vetor agora formado por 66 bits iniciar por 0b00 ou 0b11, será considerado inválido e tratado como erro no lado do receptor.

A figura 4.12 apresenta o formato do vetor gerado pela codificação

64B/66B.

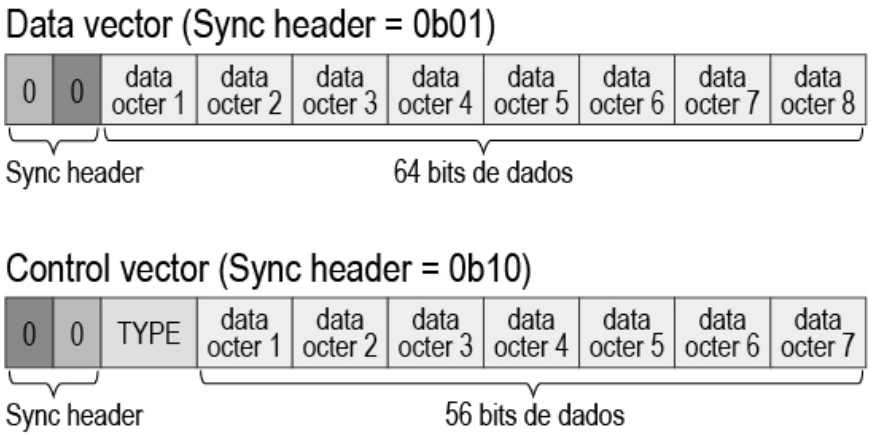



*Figura 4.12 – Codificação 64B/66B.*

Conforme obervado na figura 4.12, quando se transmitem dados de controle no vetor, o primeiro byte será utilizado pelo campo type, que informará o tipo do vetor de controle e sua estrutura interna. Vejamos:

- Caso inicie com start /S/, indicará o início do quadro. Esse indicador aparecerá na posição bit 0 ou bit 4 do primeiro byte do vetor de 64 bits. Caso seja recebido em qualquer outra posição, indicará erro.
- Caso inicie com terminate /T/, indicará o fim do quadro. Esse indicador aparecerá em qualquer posição dos bits que compõem o campo type. Deverá ser seguido de um sinal de controle I (*idle*) ou S (*start*).
- Caso inicie com error /E/, indicará um erro no quadro de dados. Esse indicador aparecerá em qualquer posição dos bits que compõem o byte type.

Para os novos padrões Ethernet 40 Gbps e 100 Gbps, utiliza-se também este modo de codificação.

## 4.9.8 Identificação automática da taxa de transmissão nas placas de rede

Para que um equipamento ativo (switch ou roteador) identifique de forma automática a taxa de transmissão de bits, deve ser capaz de

identificar qual codificação está chegando do emissor pelo quadro Ethernet: se é Manchester (10 Mbps), NRZI (100 Mbps), 4D-PAM5 (1Gbps, par trançado), 8B/10B (1 Gbps, fibra óptica), 64B/66B (10 Gbps, fibra óptica) ou DSQ128D/PAM-16 (10 Gbps, par trançado).

## 4.10 Tipos de transmissão

As redes de computadores transmitem dados digitais entre suas estações e, por isso, são conhecidas por redes *baseband* (uma única frequência ou único canal). Como exemplo de redes baseband, temos o padrão Ethernet. Os dados são representados pelos números 0 e 1. Um sinal digital possui menor variação no percurso percorrido, no entanto não admite transmissões em longas distâncias. Quando se pretende transmitir dados a longas distâncias, o equipamento deve transmitir seus dados em sinais analógicos, pois estes sofrem menos atenuação, garantindo a qualidade do sinal quando chegar ao receptor.

Redes que transmitem dados analógicos são utilizadas por rádios FM e sinal de TV que atualmente vem migrando também para sinais digitais.

Outro tipo de transmissão com que convivemos é o modo *broadband* (múltiplas frequências no mesmo cabo). Como exemplo de redes que possuem múltiplas frequências, temos as redes GPON e as que fornecem TV a cabo.

### 4.10.1 Baseband

No tipo de transmissão baseband, o sinal transmitido tem apenas uma frequência possível; já no broadband, inúmeras frequências transmitem vários canais. Como exemplo de redes baseband, temos as redes que permitem aos computadores se comunicarem entre si a 10 Mbps, 100 Mbps, 1 Gbps, 10 Gbps, 40 Gbps ou 100 Gbps. O sinal transmitido em uma rede baseband utiliza toda a largura de banda do canal para uma única transmissão, de modo que esse tipo de rede dispensa o uso de uma portadora, a qual corresponde ao sinal de frequência contínua capaz de ser modulado.

Uma grande vantagem das redes baseband é a possibilidade de

transmitir dados em *full-duplex*, ou seja, o receptor e o emissor transmitem e recebem dados ao mesmo tempo. A seguir, um resumo das principais características desse tipo de transmissão:

- Sinalização digital.
- Pequenas distâncias por permitir somente sinalização digital.
- Permite transmissões em alta velocidade.
- Permite uma única frequência na transmissão.
- Utiliza cabo coaxial, par trançado e fibra óptica. Exemplo: padrão Ethernet operando a 10/100/1.000 Mbps, 10 Gbps, 40 Gbps e 100 Gbps.

### 4.10.2 Broadband

Conforme comentado, o tipo de transmissão baseband oferece uma transmissão em que o sinal utiliza toda a largura de banda do canal para uma única transmissão. No tipo de transmissão broadband, utiliza-se uma transmissão em que a largura de banda pode ser utilizada para várias transmissões simultâneas, ou seja, em redes broadband, várias frequências podem ser transmitidas pelo mesmo cabo, como a TV a cabo que transmite, além do sinal de TV em vários canais, dados de Internet e VoIP (voz sobre IP). Esse tipo de sinalização pode ocorrer sobre cabos coaxiais (ex.: TV a cabo) ou fibra óptica (ex.: redes no padrão GPON, em que se transmitem TV, VoIP e Internet). Um terceiro meio físico que também pode ser utilizado é o meio aéreo através das redes sem fio e ondas de rádio.

## 4.11 Exercícios do capítulo 4

**1**. O padrão Ethernet deu certo. Explique o porquê de todo esse sucesso.

**2**. Descreva os modos de transmissão simplex, *half-duplex* e *full-duplex*.

**3**. Apesar de a sinalização analógica não ser utilizada para a transmissão de dados entre computadores interligados em rede local, essa técnica é utilizada para a transmissão de dados entre

redes fisicamente separadas. Comente o porquê da utilização da sinalização analógica nesses ambientes.

**4**. O modelo de referência TCP/IP não define regras para a camada física e de enlace. Qual padrão atua nessas camadas no modelo de referência TCP/IP?

5. (Sanepar, 2004) Em relação à tecnologia Ethernet, são feitas as seguintes proposições:

I. No que diz respeito à topologia lógica das redes Ethernet, é possível afirmar que são redes em estrela, pois necessitam de concentradores conhecidos como hubs.

II. As taxas de transmissão para redes Ethernet eram inicialmente de 10 Mbps; com o advento do Fast Ethernet, passaram a atingir velocidades de até 100 Mbps e, com o Gigabit Ethernet, uma taxa de até 1 Gbps é possível.

III. O Ethernet faz uso do protocolo de acesso ao meio conhecido por CSMA/CD, que consiste em verificar se há portadora no meio e, caso não haja, transmitir.

IV. As redes Ethernet permitem *broadcasting*.

Com base nas afirmativas anteriores, é correto afirmar:

a) Somente as afirmativas I, II e III são verdadeiras.

b) Somente as afirmativas II e III são verdadeiras.

c) Somente as afirmativas II, III e IV são verdadeiras.

d) Somente a alternativa II é verdadeira.

e) Todas as alternativas são verdadeiras.

**6**. Descreva a camada MAC, que possui uma forma de endereçamento própria.

**7**. As redes locais (ou LANs – *Local Area Networks*) são redes privadas que podem ter, no máximo, alguns quilômetros de extensão. São amplamente usadas para conectar computadores pessoais e estações de trabalho em escritórios e instalações industriais. Entre os padrões populares para redes locais, estão o padrão IEEE 802.3 (conhecido como Ethernet), o padrão IEEE 802.5 (conhecido como Token Ring) e o padrão IEEE 802.3u

(conhecido como Fast Ethernet). Considere as afirmativas a seguir relativas às LANs:

I. A rede Ethernet utiliza uma topologia em anel.

II. A rede Fast Ethernet utiliza uma topologia em barramento.

III. A rede Token Ring utiliza uma topologia em anel.

IV. A rede Fast Ethernet nada mais é do que uma melhoria do padrão Ethernet, permitindo uma velocidade de até 100 Mbps.

a) Somente as afirmativas I, II e III são verdadeiras.

b) Somente as afirmativas I e IV são verdadeiras.

c) Somente as afirmativas II e III são verdadeiras.

d) Somente as afirmativas II, III e IV são verdadeiras.

e) Somente as afirmativas III e IV são verdadeiras.

CAPÍTULO 5

# Sistema de cabos Ethernet

O capítulo 5 apresentará em detalhes os padrões de cabeamento disponíveis. Serão abordados o cabo coaxial, o cabo par trançado e o cabo de fibra óptica. Ainda serão objetos de comentários o cabeamento estruturado e o não estruturado, pois ambos são conceitos de suma importância na aplicação em projetos de redes locais.

## 5.1 Cabo par trançado

Há alguns anos, os novos projetos de rede levam em consideração a utilização do cabo par trançado como meio físico para a transmissão dos dados. Essa preferência está ligada ao baixo custo e à grande facilidade de instalação e manutenção oferecida por esse meio físico de transmissão de dados. Outra vantagem obtida com a utilização do cabo par trançado se relaciona à possibilidade de atingir taxas de transferência que variam entre 10 Mbps e 10 Gbps.

É importante esclarecer que o cabo par trançado utiliza cobre como condutor interno das tensões elétricas. Muitos se questionam: por que os cabos de rede utilizam cobre como meio de transporte e o que torna esse meio físico tão interessante para o transporte de dados entre redes? A resposta é bastante simples: porque é barato, fácil de instalar, possui baixa resistência à corrente elétrica, o que significa que os sinais podem viajar dentro do meio a longas distâncias mantendo a qualidade do sinal. A seguir, descreveremos os padrões de rede Ethernet que utilizam o cabo par trançado.

## 5.2 Padrão 10BASET

O padrão 10BASET (IEEE 802.3) foi o padrão de cabeamento de rede mais utilizado nas redes domésticas e empresariais. As redes 10BASET empregam a topologia estrela com hub ou switch,

servindo como concentrador central. Apesar de antigo, esse padrão ainda pode ser encontrado em redes antigas de pequenas empresas ou escritórios.

O cabo par trançado é dividido em cabos UTP (*Unshielded Twisted Pair* – Par Trançado sem Blindagem), FTP (*Foil Twisted Pair* – Par Trançado Foliado) e STP (*Shielded Twisted Pair* – Par Trançado com Blindagem). A distância máxima permitida para a conexão entre o comutador central e o computador é de 100 metros. A seguir, comentaremos sobre os cabos UTP e STP com detalhes.

Os cabos UTP, desde a sua origem, foram divididos em categorias, as quais estão descritas na tabela 5.1:

*Tabela 5.1 – Categorias do cabo UTP*

| **Categoria** | **Descrição** |
|---|---|
| 1 e 2 | Utilizados no sistema de telefonia. |
| 3 | Comunicação até 16 Mbps. |
| 4 | Permite comunicações até 20 Mbps. |
| 5 | Permite comunicações até 100 Mbps. O cabo da categoria 5 possui impedância de 100 Ohms e também pode ser utilizado por redes 100BaseT e 1000BaseT. |
| 5e | A letra e contida no nome da categoria significa enhanced (melhorada). Representa uma melhoria das características dos materiais utilizados na categoria 5, o que permite um melhor desempenho. O cabo da categoria 5e pode ser utilizado em redes operando a 1 Gbps. |
| 6 | Os cabos categoria 6 utilizam especificações ainda mais estritas do que os categoria 5e e suportam frequências de até 250 MHz. Além de serem usados em substituição aos cabos das categorias 5 e 5e, podem ser utilizados em redes 10 Gbps, mas respeitando um comprimento máximo de 55 metros. |
| 6a | Essa categoria representa uma evolução dos cabos categoria 6. A letra a contida no nome da categoria significa augmented (ampliado). Cabos nessa categoria podem ser utilizados em redes 10 Gpbs com extensão de até 100 metros. |

| Categoria | Descrição |
|---|---|
| 7 | Essa categoria foi criada para ser usada em redes Ethernet operando a 10 Gpbs com distância máxima do cabo de 100 metros. Uma grande novidade é que essa categoria poderá vir a ser usada no padrão de 100 Gbps. O grande foco dos cabos da categoria 7 está na blindagem contra interferências e ruídos externos. |

A maioria das redes em operação com cabo par trançado utiliza cabos UTP como meio de transporte de dados entre computadores, entretanto sua imunidade a ruídos não é tão perfeita quando comparados aos cabos STP.

Os cabos FTP (*Foiled Twisted Pair*) utilizam uma blindagem mais simples, ou seja, todos os pares do cabo são envolvidos por uma fina folha de aço ou de liga de alumínio, protegendo-os contra interferências externas. A figura 5.1 apresenta um exemplo de um cabo par trançado UTP e FTP.

Os cabos STP são blindados e possuem impedância de 100 Ohms ou 150 Omhs. Os cabos com impedância de 100 Ohms atingem 100 Mbps de velocidade e os cabos de 150 Ohms, 300 Mbps de velocidade, porém não são utilizados em rede Ethernet, somente em redes token ring. Esses cabos possuem conector-padrão da IBM e já vêm prontos de fábrica. A figura 5.2 apresenta um cabo par trançado STP.

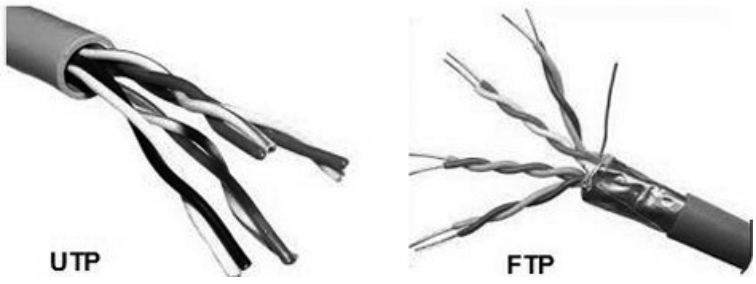



*Figura 5.1 – Par trançado sem blindagem (UTP) e com fina blindagem (FTP).*

O cabo par trançado STP possui quatro pares de fios coloridos: verde e branco com verde; marrom e branco com marrom; azul e

branco com azul; e laranja e branco com laranja.

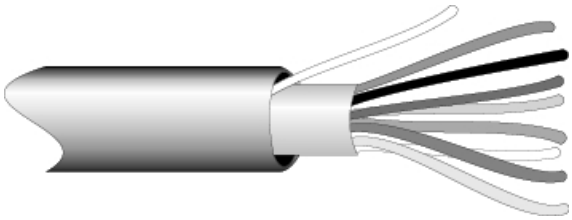


*Figura 5.2 – Par trançado com blindagem (STP).*

## 5.3 Padrão 100BASETX

O padrão 100BaseTX (IEEE 802.3u) é muito similar ao 10BASET e ainda possui topologia estrela. A sinalização é do tipo digital (*baseband*), transmite dados a 100 Mbps e utiliza o modo de codificação NRZI para conversão dos bits 0 e 1 em tensões elétricas.

## 5.4 Padrão1000BASET

No padrão Gigabit Ethernet (IEEE 802.3ab), os quatro pares de fios são usados simultaneamente, isto é, são utilizados para transmitir pedaços da mesma informação. Cada par é bidirecional e trabalha em modo *full-duplex*. No sistema Ethernet tradicional, apenas um bit é transmitido, ao passo que no Gigabit, dois bits são transmitidos por vez. O modo de codificação de bits utilizado pelo padrão 1000BASET é apresentado no capítulo 4.

## 5.5 Padrão10GBASET

O padrão 10GBASET foi homologado em 2002, sendo a fibra óptica inicialmente o único meio de transmissão utilizado. Esse padrão foi nomeado de IEEE 802.3ae-2002 e tornou-se o padrão Ethernet mais rápido. Porém, em 2006, foi também homologado para transmitir dados sobre cabos de par trançado, sendo denominado IEEE 802.3an-2006. O padrão 10GBASET transmite dados em *full-duplex* e utiliza switches como concentrador.

## 5.6 Padrão 10BASE2

O padrão 10BASE2 é também conhecido pelos nomes de *thinnet* e *cheapernet*. Foi o primeiro padrão de cabo utilizado nas primeiras redes locais definitivamente populares. É importante observar que esse padrão utiliza o cabo coaxial como condutor das tensões elétricas. Agora, vamos abordar a impedância, que afeta diretamente os cabos coaxiais.

### 5.6.1 Impedância

A impedância (resistência) é conhecida na matemática pela relação entre fatores de tensão (indutância) e da corrente (capacitância), ou seja, resistência = tensão/corrente. Logo, quanto maior a resistência, menor a corrente. A tensão (indutância) é a capacidade que um condutor tem de induzir tensão em si mesmo e a corrente (capacitância) é a capacidade de armazenamento de carga elétrica que o condutor possui. O resultado dessa relação é a impedância que, por sua vez, é medida em Ohms, nome dado em homenagem ao cientista e físico alemão George Simon Ohm (1787-1854). A lei do Ohm é uma lei básica da eletricidade que relaciona a tensão elétrica, a intensidade da corrente elétrica e a resistência elétrica.

A resistência é necessária nos meios de comunicação de dados, pois fecha o circuito elétrico em que serão colocadas as tensões para enviar os 0 e 1 do emissor ao receptor. O cabo sozinho não possui resistência adequada e necessária para a transmissão de tensões variáveis. Visto que o cabo normalmente possui uma resistência quase nula, insuficiente para a transmissão de tensões variáveis, são necessários dois resistores nas pontas do cabo coaxial. Os resistores colocados nas extremidades fecham o circuito elétrico para que seja possível aplicar as tensões no cabo. Para que a comunicação entre os computadores seja de qualidade, a resistência deve ser sempre constante, e, no caso do cabo coaxial do padrão 10BASE2, deve ficar em torno de 25 Ohms.

Uma resistência poderá ser alterada e, nesses casos, o motivo será o terminador aberto ou danificado. Caso isso ocorra, a qualidade da comunicação será comprometida.

A seguir, algumas respostas a dúvidas frequentes sobre

impedância:

- A impedância em uma rede influencia a qualidade e o desempenho dos bits transmitidos? Caso ela esteja abaixo ou acima de 25 Ohms, a tensão empregada será distorcida e, por consequência, haverá perda do sinal e dos dados (0 e 1). O fato de muitos 0 serem compreendidos como 1 causa retransmissão e, consequentemente, problemas de desempenho.
- Cada resistor conectado no final do cabo possui impedância de 50 Ohms. Contudo, se utilizarmos um multímetro para verificar a impedância da rede, esse multímetro deverá marcar em torno de 25 Ohms. Por que isso acontece? A resposta para a rede manter essa impedância é dada por uma regra da eletricidade que diz que quando dois resistores forem colocados em paralelo, a resistência aplicada ao meio de transmissão (impedância) será dada pela fórmula (Resistor1 * Resistor2)/(Resistor1 + Resistor2). A seguir, apresentamos um exemplo da operação:

  (R1 * R2)/(R1 + R2)

  (50 * 50)/(50 + 50)

  (2.500)/(100)

  25 Ohms

É importante lembrar que cada placa de rede acrescentada ao barramento aumenta a carga das outras, ou seja, reduz a impedância do barramento. Isso pode explicar por que uma rede que utiliza cabo coaxial possui um limite de 30 máquinas ligadas em um segmento. A seguir, comentaremos as vantagens e desvantagens dos cabos coaxiais em relação ao cabo par trançado.

## 5.7 Fibra óptica

A fibra óptica revolucionou o mercado, implantando no país o estado da arte em rede de comunicações para voz e dados. Na década de 1970, foram efetuadas as primeiras pesquisas na área de redes ópticas.

Nessa década, chegou-se à conclusão de que uma fibra de vidro de coração microscópico refletindo a energia luminosa e rodeada de

uma camada opaca constituía um meio de transmissão de dados com a maior velocidade conhecida: a velocidade da luz. O princípio de fabricação de uma fibra óptica repousa no estiramento de uma pré-forma de vidro. Graças a técnicas complexas, é possível esticar um tubo de vidro de 1 metro de comprimento e 10 cm de diâmetro até criar com ele uma fibra óptica de 150 km de comprimento.

O coração da fibra é composto de sílica, ou mais exatamente de óxido de silício, estando esse material presente em muitos minerais, como quartzo, calcedônia ou opala, e apresentando a particularidade de refletir adequadamente os comprimentos de ondas de 850 nm, 1.310 nm, 1.490 nm ou 1.550 nm (nanômetros). Esse coração perfeito está rodeado por uma camada de sílica de menor qualidade que forma o revestimento óptico.

Enquanto os fios de cobre transportam elétrons, os cabos de fibra óptica (cabos de fibra de vidro) transportam luz. Dentre as vantagens dos cabos de fibra óptica, há a imunidade total contra a diafonia e contra as interferências eletromagnéticas e de radiofrequência. A falta de ruídos internos e externos significa que os sinais têm um alcance maior e se movem mais rápido, proporcionando uma velocidade e uma distância maiores do que as obtidas com cabos de cobre. Como não transporta eletricidade, a fibra é o meio mais adequado para conectar prédios com diferentes aterramentos elétricos. Além disso, os cabos de fibra não atraem raios como os de cobre.

Um cabo de fibra óptica é composto de uma cobertura plástica externa, a qual deve obedecer às normas de construção civil e aos códigos de proteção contra incêndio. Sob a cobertura, existe uma camada de fibra Kevlar (o mesmo usado em coletes à prova de bala) cujos objetivos são amortecer impactos no cabo e proporcionar maior resistência a ele quando for, por exemplo, esticado. Todos esses materiais protegem o centro da fibra, no qual se localiza um fio de vidro extremamente fino que pode ser comparado a um fio de cabelo.

As extremidades da fibra possuem transmissores conhecidos como LED (*Light Emitting Diode* – Diodo Emissor de Luz). A figura 5.3

apresenta um cabo composto de várias fibras ópticas, enquanto a figura 5.4 mostra conectores para fibra óptica. A seguir, apresentaremos os padrões de redes locais que utilizam a fibra como meio de transmissão de dados.

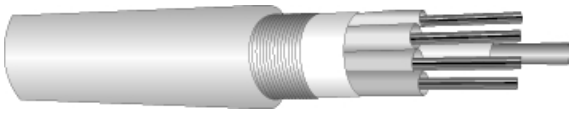


*Figura 5.3 – Fibra óptica.*

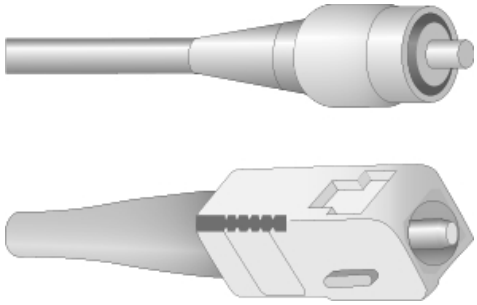


*Figura 5.4 – Cabo de fibra óptica com conector.*

## 5.8 Padrão 100BASEFX

O padrão Ethernet 100BASEFX (velocidade de 100 Mbps, unicanal – *baseband, Fiber*) utiliza cabo de fibra óptica e permite conectar estações até a 2 km do concentrador (switch), utilizando fibras multímodo. Esse padrão pode atingir em torno de 20 km quando utiliza fibras monomodo.

## 5.9 Padrão 1000BaseLX

O 1000BaseLX (LX – longo) é o padrão de redes Gigabit Ethernet que usa fibras ópticas de modo multimodo (múltiplo) ou monomodo (único). O limite de comprimento de cada segmento de fibra óptica é de 550 metros, isso quando utiliza fibras multimodo. Usando fibras ópticas de modo único ou monomodo, o limite de comprimento de cada segmento de fibra óptica é de 5 km. Além das características de transmissão superiores aos cabos metálicos, a fibra, por utilizar luz, tem imunidade eletromagnética.

Em redes locais de grande porte, normalmente se emprega a fibra óptica interligando switches separados por uma longa distância,

formando assim o backbone (espinha dorsal) da rede. A tabela 5.2 apresenta vantagens e desvantagens das fibras ópticas:

*Tabela 5.2 – Vantagens e desvantagens da fibra óptica*

| Vantagens da fibra óptica | Desvantagens |
|---|---|
| Velocidade. | Alto custo de instalação e manutenção. |
| Isolamento elétrico. A luz não causa interferência elétrica. Não é suscetível a interferências elétricas. | Difícil de instalar e difícil de reparar, pois necessita de equipamentos específicos que identifiquem o local do problema. |
| O cabo pode ser longo, ou seja, pode conduzir os pulsos de luz a uma maior distância do que os cabos de cobre. | Quebra com facilidade. |
| Alta taxa de transferência. | Difícil de ser remendada, pois necessita de equipamento especializado para reparos. |

Os detalhes sobre os novos padrões que transmitem dados a 40 e 100 Gbps sobre fibra óptica são apresentados no capítulo 4. Existem ainda estudos para definir um novo padrão Ethernet para operar a 400 Gbps, porém, durante o período em que escrevemos a segunda edição deste livro, esse padrão encontrava-se em fase de estudos.

## 5.10 Como surgiu a fibra óptica?

A comunicação com fibra óptica tem suas raízes nas invenções do século XIX. Um dispositivo denominado Fotofen convertia sinais de voz em sinais ópticos utilizando a luz do sol e lentes montadas em um transdutor que vibrava ao entrar em contato com o som. A fibra óptica tornou-se mais prática durante a década de 1960 com o surgimento das fontes de luz de estado sólido (raio lazer e os LEDs) e das fibras de vidro de alta qualidade livres de impurezas. As companhias telefônicas foram as primeiras a se beneficiarem do uso de técnicas de fibra óptica em conexões de longa distância.

### 5.10.1 Tipos de fibra óptica

As fibras ópticas estão classificadas em dois tipos: fibra multimodo e fibra monomodo. Em linhas gerais, sem a utilização de amplificadores, a primeira tem capacidade de transmissão da ordem de 100 Mbps, até uma distância próxima de 10 km (mais empregada em redes locais), enquanto a segunda (monomodo) alcança algo em torno de 1 Gbps, a uma distância por volta de 100 km (empregada em redes de longa distância) ou 10 Gbps a uma distância de 40 km. A seguir, apresentaremos detalhes das fibras monomodo e multimodo.

### 5.10.1.1 Fibra multimodo ou modo múltiplo

A fibra multimodo, ou MMF (*MultiMode Fiber*), é composta de um coração de diâmetro que varia entre 50 e 85 mícrons, sendo principalmente utilizada nas redes locais de menos de 2 km de comprimento. Os dados a serem transportados são emitidos por meio de um diodo eletroluminescente (LED – *Light Emitting Diode*) de um comprimento de onda de 850 nm ou 1.310 nm.

Fibras do tipo multimodo são mais grossas quando comparadas às fibras monomodo. Essa diferença de espessura implica que a luz seja refletida na parede da fibra e, assim, chegue ao destino de forma duplicada. O receptor terá o trabalho de detectar a informação correta e eliminar os sinais duplicados. Em razão dessa característica, as redes que utilizam fibra multimodo não podem ser longas, pois o problema se agrava quanto maior for a extensão do cabo. A figura 5.5 apresenta uma fibra óptica multimodo que transporta luz no seu interior.

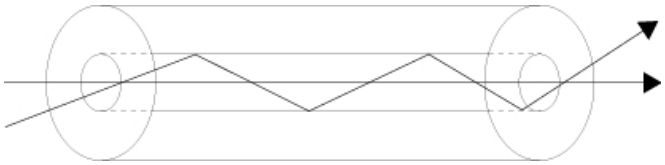


*Figura 5.5 – Fibra óptica multimodo.*

### 5.10.1.2 Fibra monomodo ou modo único

O segundo tipo de fibra óptica é a fibra monomodo, ou SMF (*Single Modo Fiber*), cujo coração é extremamente fino, com diâmetro de 9 mícrons. Esse tipo de fibra é utilizado em conexões de longo

alcance (600 km a 2.000 km). Por ser mais fina, a fibra monomodo evita que a luz ricocheteie em suas paredes, assim consegue ter comprimento e desempenho superiores aos da fibra de modo múltiplo. Apesar disso, é mais cara e possui maior dificuldade no momento da instalação, pois é trabalhoso alinhar o feixe de luz da placa de rede ao feixe de luz da fibra. A figura 5.6 apresenta uma fibra monomodo:

*Figura 5.6 – Fibra óptica monomodo.*

## 5.11 Detalhes do cabo par trançado

Em razão de o cabo par trançado ser o mais utilizado para a implantação de novos projetos de rede, abordaremos, a seguir, detalhes desse meio físico, como categorias, padrões para a confecção de cabos e técnicas para a criação de um cabeamento par trançado considerado estruturado.

### 5.11.1 Pinagem do cabo par trançado em redes Ethernet e Fast Ethernet

Ao adquirir um cabo par trançado, deve-se perceber qual categoria está registrada no cabo. Os cabos comercializados são todos da categoria 5 ou superior, embora nem sempre tenha sido dessa forma. Os cabos disponíveis para as categorias 3 e 4 foram muito úteis na década de 1990 e estão em extinção. Utilizar cabos classificados como categoria 5 ou superior oferece a vantagem de a rede poder operar na velocidade de 1 a 10 Gbps, enquanto os anteriores à categoria 5 transmitiam dados a, no máximo, 20 Mbps.

O cabo par trançado é composto de oito fios relacionados em quatro pares, cada um com uma cor diferente. As cores dos fios são verde, branco verde, azul, branco azul, laranja, branco laranja, marrom e branco marrom. Em cada extremidade do cabo par trançado, deve-se conectar um conector padrão RJ-45, mostrado na

figura 5.7, que possui oito pinos, um para cada fio do cabo.

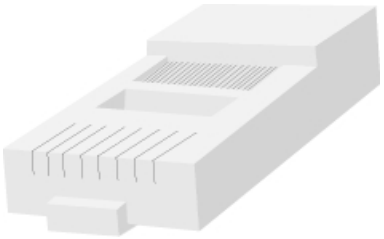


*Figura 5.7 – Conector RJ-45.*

Teoricamente, um cabo par trançado pode conectar dois equipamentos utilizando uma sequência de cores escolhida pelo técnico que montou o cabo. Essa atitude, apesar de errada, permite que o cabo funcione. O técnico somente deve garantir que o pino 1 de uma extremidade seja conectado ao pino 1 da outra extremidade e, assim, sucessivamente para todos os oito pinos dos conectores. Isto é, se você conectar o fio verde ao pino 1 de uma extremidade, deverá conectar o pino 1 ao fio verde da outra extremidade do cabo também.

O uso desse tipo de formação de cabos causa um grande problema dentro da empresa, pois não segue nenhum padrão definido, mas um padrão criado por alguém que julgou que tal sequência seria a melhor sem nenhuma base científica relacionada. No futuro, se um segundo técnico precisar substituir um conector em uma extremidade do cabo, ficará simplesmente perdido e deverá, após muito tempo de testes, chegar à conclusão de que o problema está na sequência dos fios e não na sua forma de conexão, o que é péssimo, visto que um técnico determina o seu custo pelo período dedicado a resolver um problema. Outro problema que pode ocorrer com o uso de uma sequência arbitrária é a paradiafonia (vazamento de energia elétrica entre pares de fios do mesmo cabo), que pode causar problemas na rede.

Podemos observar que, como o próprio nome indica, os fios formam pares trançados, de modo que essas tranças protegem os sinais da interferência externa. Essa proteção só existe quando os pares fazem parte do mesmo circuito elétrico, ou seja, o fio que transmite deve estar entrelaçado com o outro fio que transmite com

polaridade invertida. Então, para evitar esses desencontros entre o seu padrão e o padrão internacional, recomenda-se utilizar os padrões T568A e T568B. Basta optar por um dos dois padrões e fazer os cabos de acordo com a ordem dos fios imposta por eles, assim não haverá dúvidas na hora de montar os cabos nem na sua manutenção. Nas figuras 5.8 e 5.9, você pode observar a ordem dos fios dos padrões T568A e T568B, respectivamente:

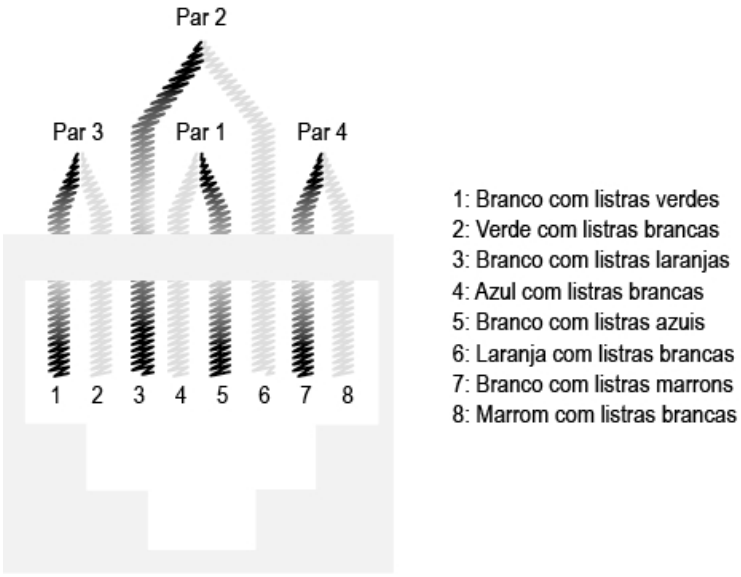



*Figura 5.8 – Padrão T568A.*

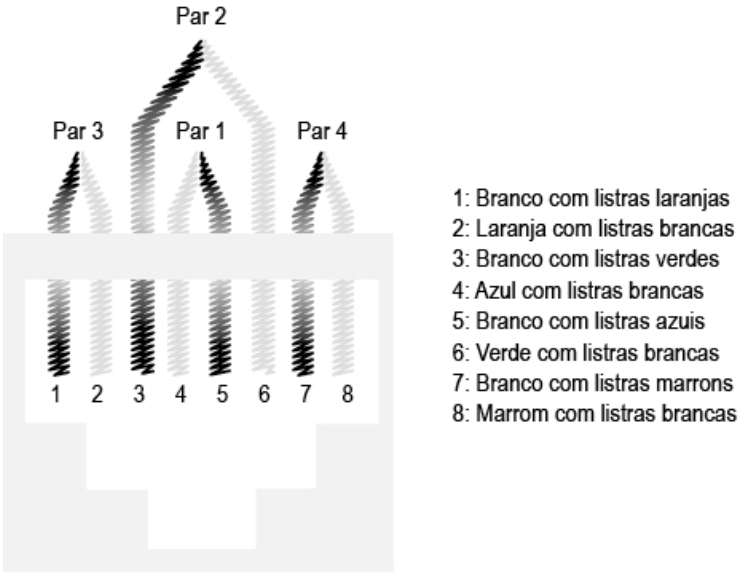



*Figura 5.9 – Padrão T568B.*

A seguir, apresentaremos mais detalhes acerca desses padrões.

## 5.11.2 Padrões de cabeamento

Em sua maioria, as redes de computadores utilizam o cabeamento par trançado, mas o cabeamento coaxial ainda existe somente em pequenas redes que ainda não optaram por realizar uma renovação. Em razão de possuir quatro pares, há a possibilidade de diferentes pinagens e, para possibilitar a utilização de equipamentos de diversos fabricantes, alguns padrões foram criados, como o T568A e o T568B. No Brasil, os padrões mais utilizados são o T568A e o T568B, que utilizam os pinos 1, 2, 3 e 6 para transmitir e receber dados, diferindo-se entre si pela escolha do par.

A seguir, comentaremos em detalhes os padrões de cabeamento que podem ser empregados nos projetos de redes.

## 5.11.3 TIA/EIA T568A

Os sistemas de cabeamento 10BASET, 100BASET, 1000BASET e 10GBASET podem utilizar o padrão T568A, o qual determina que os fios devem ser ligados na ordem apresentada na figura 5.13 e na tabela 5.3.

*Tabela 5.3 – Descrição dos fios do cabo par trançado no padrão T568A*

| Pino | Cor | Função |
|---|---|---|
| 1 | Branco com verde | +TD |
| 2 | Verde | -TD |
| 3 | Branco com laranja | +RD |
| 4 | Azul | Não usado |
| 5 | Branco com azul | Não usado |
| 6 | Laranja | -RD |
| 7 | Branco com marrom | Não usado |
| 8 | Marrom | Não usado |

As indicações T e R significam:

- **Tip** – ponta.
- **Ring** – anel.

As indicações T e R apresentados na tabela 5.3 referem-se ao antigo padrão de cabeamento telefônico. Cada conjunto T e R forma um par, sendo:

- **Par 1** – pinos 4 e 5.
- **Par 2** – pinos 3 e 6.
- **Par 3** – pinos 1 e 2.
- **Par 4** – pinos 7 e 8.

O par 3 funciona como transmissor e o par 2, como receptor.

### 5.11.4 TIA/EIA T568B

Esse esquema pode ser alternativamente utilizado, mas é preferível o padrão T568A, que é o mais usado em todo o mundo. A diferença entre o padrão T568A e o T568B é a posição dos pares. O par 2 (formado pelos pinos 3 e 6 – fios branco laranja e laranja) e o par 3 (formado pelos pinos 1 e 2 – fios branco verde e verde) são trocados conforme se pode verificar na tabela 5.4.

*Tabela 5.4 – Descrição dos fios do cabo par trançado no padrão T568B*

| Pino | Cor – T568B | Cor – T568A |
|---|---|---|
| 1 | Branco com laranja | Branco com verde |
| 2 | Laranja | Verde |
| 3 | Branco com verde | Branco com laranja |
| 4 | Azul | Azul |
| 5 | Branco com azul | Branco com azul |
| 6 | Verde | Laranja |
| 7 | Branco com marrom | Branco com marrom |
| 8 | Marrom | Marrom |

## 5.11.5 Pinagem do cabo par trançado em redes Gigabit Ethernet

Nas redes que operam à taxa de 1 Gbps, utilizam-se todos os fios do cabo para transmissão e recepção dos dados, ao contrário dos padrões com menor velocidade. A tabela 5.5 apresenta com detalhes a descrição dos fios seguindo o padrão T568A.

*Tabela 5.5 – Disposição dos fios no padrão Gigabit Ethernet*

| Pino | Cor | Função (bidirecional) |
|---|---|---|
| 1 | Branco com verde | + BI_DA |
| 2 | Verde | - BI_DA |
| 3 | Branco com laranja | + BI_DB |
| 4 | Azul | + BI_DC |
| 5 | Branco com azul | - BI_DC |
| 6 | Laranja | - BI_DB |
| 7 | Branco com marrom | + BI_DD |
| 8 | Marrom | - BI_DD |

## 5.11.6 Imunidade a ruídos no cabo par trançado

O par trançado sem blindagem, apesar de não ter uma camada metálica de proteção, possui uma ótima proteção contra ruídos, usando uma técnica chamada cancelamento. A figura 5.10 apresentará como funciona esse processo:

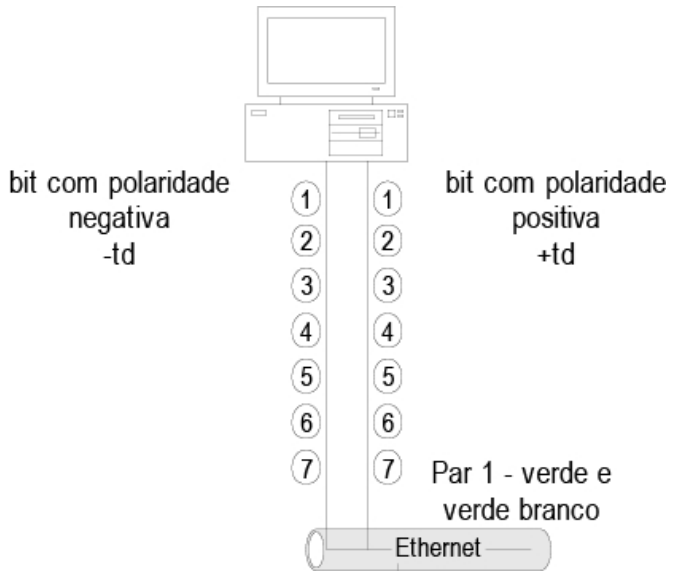



*Figura 5.10 – Cancelamento de eco. Utilizado para dar imunidade a ruídos no cabo par trançado.*

A técnica de cancelamento consiste em transmitir o mesmo sinal pelos dois fios dos pares de transmissão e recepção, entretanto com a polaridade invertida. Dessa forma, o campo magnético gerado por um fio é anulado pelo outro que compõe o par.

## 5.11.7 Cabo par trançado cross-over

Geralmente, o cabo par trançado faz uma ligação pino a pino entre os dispositivos que estão sendo interligados. Como exemplo, temos a ligação de uma impressora a um switch. O cabo *cross-over*, ao contrário do cabo pino a pino, interliga a saída de dados do primeiro micro à entrada de dados do segundo e vice-versa. Todo cabo de rede par trançado possui quatro pares, de modo que um par é utilizado para a transmissão das tensões elétricas e um segundo par é utilizado para a recepção das tensões elétricas. A função do switch é conectar as tensões elétricas que estão sendo emitidas por um equipamento às entradas de dados das demais máquinas. Assim, o switch está realizando o cruzamento dos sinais e, para essa forma de operação, damos o nome de *cross-over*.

Em redes 1000BASET, a pinagem do cabo *cross-over* é a que segue na tabela 5.6, já que, nesse tipo de rede, todos os pares de cabo par trançado são utilizados:

*Tabela 5.6 – Disposição dos fios no padrão Gigabit Ethernet para cabos cross-over*

| Pino conector A | Cor | Pino conector B |
|---|---|---|
| 1 | Branco com verde | 3 |
| 2 | Verde | 6 |
| 3 | Branco com laranja | 1 |
| 4 | Azul | 7 |
| 5 | Branco com azul | 8 |
| 6 | Laranja | 2 |
| 7 | Branco com marrom | 4 |
| 8 | Marrom | 5 |

## 5.11.8 Preparação do cabo par trançado

Para preparar o cabo, você precisará, além de conectores RJ-45, de um alicate para crimp (Figura 5.11). Os fios do cabo par trançado são presos ao conector RJ-45 por pressão, da mesma forma como acontece com os conectores BNC usados no cabo coaxial. Basta alinhar os fios do pino 1 ao pino 8 do conector de acordo com o padrão a ser utilizado (T568A ou T568B) e pressionar o conector com alicate. Não é necessário desencapar os fios coloridos, pois o próprio conector RJ-45 possui pinos em forma de lâmina, desencapando automaticamente os fios durante a montagem do cabo.

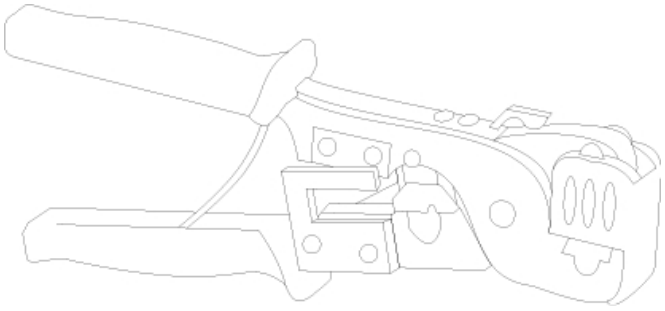


*Figura 5.11 – Alicate para crimp de conectores RJ-45.*

### 5.11.9 Instalação do cabo

Um projeto de instalação de cabos de rede é muito importante e deve ser desenvolvido por pessoas especializadas. De antemão, é preciso averiguar em que lugar estarão presentes os equipamentos de rede e telefonia e instalar as caixas conectoras em todos esses lugares, mesmo que em um primeiro momento ainda não estejam sendo utilizadas. Os micros e os telefones serão conectados a essas caixas conectoras por meio de um cabo de menor comprimento. Da parte traseira da caixa conectora, sairá um cabo que liga a caixa ao patch panel, localizado em uma sala reservada. Do patch panel, sairá um novo cabo utilizado para interligar o equipamento de rede ao switch ou ao PABX telefônico. Esse procedimento, além de facilitar a instalação das estações da rede e dos telefones, facilita a manutenção, pois os problemas de mau contato que geralmente ocorrem entre os equipamentos e o concentrador serão minimizados.

A figura 5.12 apresenta exemplos de caixas conectoras de cabos par trançado, as quais podem ser internas (embutidas na parede) ou externas.

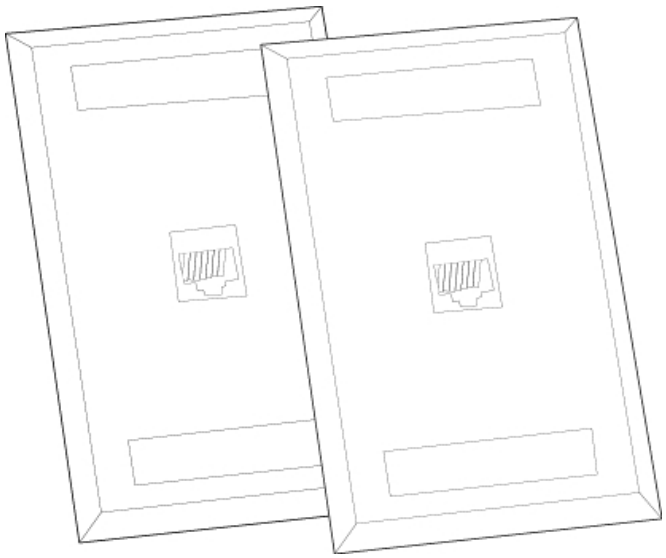


*Figura 5.12 – Caixas conectoras para cabo par trançado.*

Para que você tenha qualidade na conectividade dos fios do cabo nas caixas adaptadoras, sugere-se utilizar ferramentas específicas para esse fim. A figura 5.13 apresenta uma ferramenta de inserção

indispensável em projetos de redes:

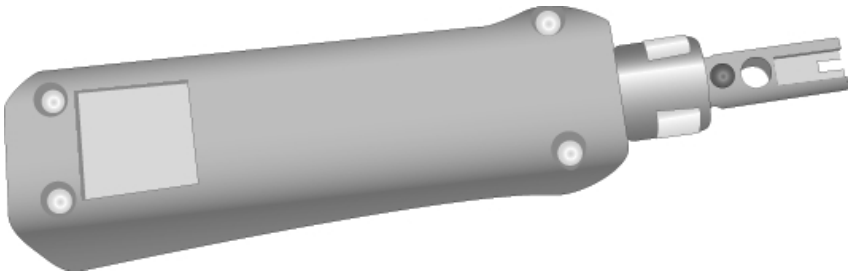


*Figura 5.13 – Ferramenta de inserção.*

## 5.12 Patch panel

O *patch panel* (painel de conexão) funciona como um pool de tomadas que permite manobras e atualizações rápidas e econômicas do cabeamento. Os modelos mais encontrados e usados são os de 24 e 48 portas, mas também existem outros modelos, como o de 12, 16, 64 ou até 96 portas. Cada porta utiliza um conector RJ-45 fêmea e possui a mesma forma de conexão usada nas tomadas conectoras de parede. Para fazer a conexão do cabo par trançado ao patch panel, usamos a mesma ferramenta de impacto utilizada na preparação das caixas conectoras (ferramenta de inserção).

Em todos os projetos de rede que utilizam o cabo par trançado, utiliza-se o patch panel para a ligação de computadores, impressoras e aparelhos telefônicos aos seus respectivos equipamentos, que podem ser para o caso dos computadores, o switch; para o caso dos aparelhos telefônicos, o PABX. Isso acontece em decorrência de sua grande flexibilidade e rapidez para ativar um ponto como ponto de dados ou ativá-lo como ponto de telefonia.

É comum uma rede ter mais pontos de telecomunicação do que realmente necessita, até mesmo porque a norma recomenda 2 pontos a cada 10 metros quadrados. Esse acréscimo é necessário, pois um bom projeto de cabeamento tem que durar pelo menos 10 anos, período em que os computadores serão adicionados ou mudados de posição. Todo esse cabeamento colocado a mais para suportar os pontos que ainda não estão ativos é terminado no patch

panel.

Esses pontos adicionais necessariamente não estarão conectados a um equipamento ativo (switch) ou PABX, visto que seria muito caro adquirir equipamentos com portas suficientes para todos os pontos ainda não usados. Na verdade, eles ficarão ociosos até que seja necessária a sua utilização. Contudo, quando for necessária a ativação de pontos deixados disponíveis (sem utilização em um primeiro momento), mas já terminados, somente serão necessárias a instalação do equipamento ativo e a ligação, via cordão de painel (*patch cord*), à porta do patch panel associada ao ponto.

Uma outra questão importante que justifica a utilização do patch panel é o fato de as manobras serem feitas neles e não nas portas dos switches, que são mais sensíveis a retiradas e inserções de conectores, tendo durabilidade inferior à dos painéis. A seguir, comentaremos como é feito o compartilhamento do mesmo meio físico para a transmissão de dados e voz (telefonia).

O encaixe entre os conectores RJ-11 (conector do cabo telefônico) e RJ-45 (conector do cabo de rede) é totalmente compatível entre eles. Os fios 2 e 3 do cabo de telefonia são conectados ao par azul e branco azul do cabo par trançado. Dessa forma, é possível utilizar uma caixa conectora para ligar ambos os equipamentos (telefones e computador). Para obter essa vantagem, o administrador da rede pode manobrar o cabeamento situado na sala onde está o patch panel. Caso o ponto seja para a transmissão de dados, o cabo deverá ser conectado a um switch, entretanto, quando for um ponto para telefonia, esse deverá ser conectado ao PABX (central telefônica). A figura 5.14 apresenta um exemplo de uma rede que utiliza o patch panel:

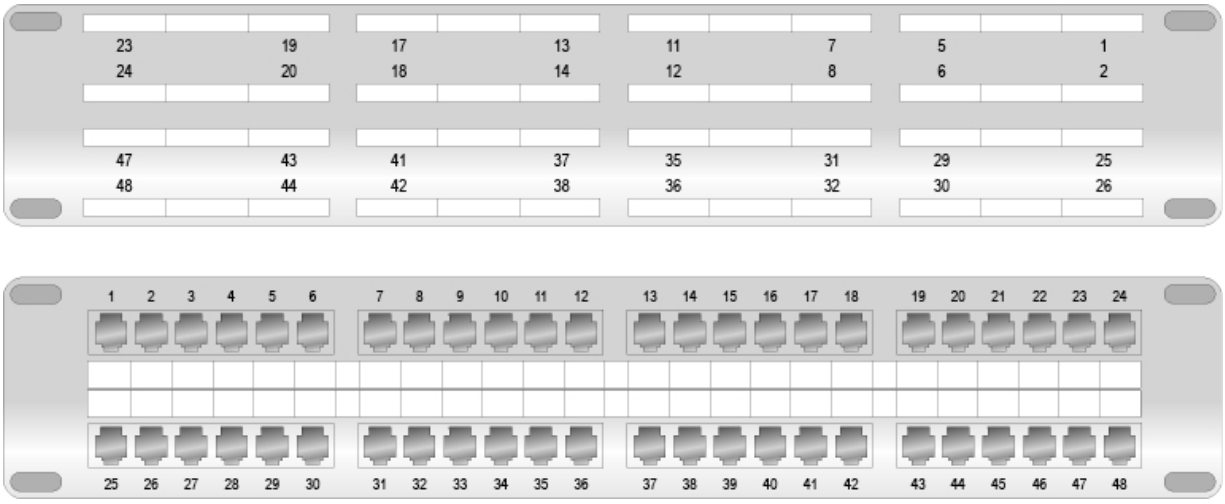



*Figura 5.14 – Acomodação de cabos num patch panel.*

## 5.12.1 Cabeamento estruturado

O cabeamento estruturado tem como objetivo permitir a utilização do mesmo meio físico para a transmissão de dados, voz e imagem. Por meio dessa filosofia, um só cabeamento atende a diferentes tipos de redes, como a rede de telefonia e a rede local (LAN).

O cabeamento estruturado teve origem nos sistemas telefônicos comerciais e, nesse ambiente, havia constante mudança física de posição dos usuários. Para resolver essa questão, foi projetada uma forma inteligente para a disposição dos cabos, em que foi desenvolvida uma rede de cabos fixa, ligada a uma central de distribuição. Na central de distribuição, tornou-se possível decidir qual cabo seria ativado ou desativado. Como nas redes de computadores também havia essa necessidade, a ideia foi trazida a esse ambiente com a finalidade de garantir a mesma versatilidade na decisão de ativar ou desativar um cabo de rede ou, ainda, de ativar como um ramal telefônico ou ponto de rede.

Muitas pessoas acreditam que o cabeamento estruturado é caro. Afinal, o que é caro? Para chegarmos a uma conclusão, temos que avaliar não só o investimento inicial, mas também outros fatores importantes durante a vida útil da infraestrutura de cabeamento. Segue um exemplo prático.

Consideremos, por exemplo, um ambiente de uma faculdade, onde

os alunos e professores necessitarão de infraestrutura de telefone, computador e impressoras, e os funcionários precisarão dos serviços de fax e telefonia. Em uma estrutura convencional, seriam instaladas canaletas, cabos exclusivos para cada uma das necessidades, de acordo com a distribuição dos equipamentos. Depois dos primeiros meses na nova sede, tudo está perfeito, pois todos estão sendo atendidos pelos pontos de acordo com a localização de cada equipamento. No entanto, o ambiente de uma faculdade é muito dinâmico, já que uma instituição de ensino está em constante evolução. Assim, na primeira alteração de layout, há uma imensa correria, pois o local para onde aquela mesa foi movida tem ponto de telefone, mas não de computador, ou tem de computador, mas seriam necessários mais três pontos de telefone. Portanto, há gastos para fazer as mudanças, além dos recursos técnicos (alternativas) para resolver ou solucionar de forma temporária o problema.

Nessa situação, vale tudo, desde passar telefone, computador e rede elétrica pela mesma canaleta ou até mesmo utilizar o rodapé com uma fita plástica sobre o piso. É nessa situação que a rede de dados começa a apresentar problemas, a central telefônica tem prejuízo na qualidade de voz e, assim, tudo o que tinha sido planejado vira um caos. Para esses problemas é que o cabeamento estruturado é projetado, ou seja, uma vez que o cabeamento seja implementado, nenhuma mudança de layout terá impacto na qualidade da rede. Veja a figura 5.15, a qual demonstrará uma relação entre o custo e o tempo de retorno do investimento:

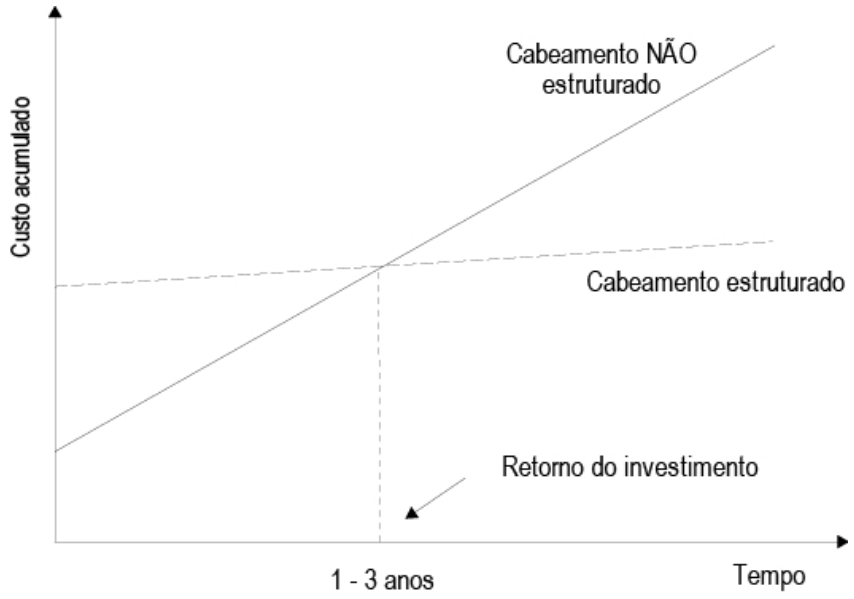



*Figura 5.15 – Relação de tempo e custo do cabeamento estruturado.*

Conforme a figura 5.15, podemos notar que inicialmente o cabeamento estruturado requer um investimento maior em comparação a um cabeamento convencional; no entanto, ao longo dos anos, com a simplicidade de administração, o seu custo de manutenção é bem menor, chegando a um equilíbrio em torno dos dois anos (dependendo do tamanho e características da rede). Assim, se você vai usar seu cabeamento por mais de três anos, o barato pode mesmo sair muito caro.

## 5.13 Exercícios do capítulo 5

**1**. (Sanepar, 2004) Considere o padrão IEEE 802.3 para redes locais, mais conhecido como Ethernet. O tipo de cabeamento mais comum para esse padrão é o 10BASET, usando cabo par trançado. Dessa maneira, várias máquinas são conectadas a um hub ou switch. Qual é o alcance máximo de um cabo desse tipo?

a) Aproximadamente 1 metro.

b) Aproximadamente 10 metros.

c) Aproximadamente 100 metros.

d) Aproximadamente 1.000 metros.

e) Não existe limite para o alcance desse tipo de cabo.

**2**. (Sanepar, 2004) Sobre a especificação 10BASET, é correto afirmar:

a) O meio de transmissão é um cabo coaxial fino de 300 Ohms.

b) A maior taxa de transmissão suportada é de 100 Mbps a distâncias de até 200 metros.

c) No caso de a rede possuir mais de dois dispositivos conectados, o uso de repetidores multiporta (hubs) se faz obrigatório.

d) O conector especificado é o BNC.

e) Para conexão ao cabo, são necessários conectores vampiros, ligados a transceivers AUI/TP.

**3**. Sobre o cabo coaxial, é correto afirmar:

a) O cabo coaxial é composto de dois condutores montados um dentro do outro, um central e um externo. Ambos são separados por um isolante e revestidos por uma capa plástica para isolação e proteção. Atinge 100 metros de distância e permite a ligação de redes broadband. Possui alta flexibilidade.

b) O cabo coaxial é composto de dois condutores montados um dentro do outro, um central e um externo. Ambos são separados por um isolante e revestidos por uma capa plástica para isolação e proteção. Atinge 100 metros de distância e permite a ligação de redes broadband e baseband. Possui alta flexibilidade.

c) O cabo coaxial é composto de dois condutores montados um dentro do outro, um central e um externo. Ambos são separados por um isolante e revestidos por uma capa plástica para isolação e proteção. Atinge 185 metros de distância e permite a ligação de redes broadband e baseband. Possui baixa flexibilidade.

d) Atinge velocidades de até 100 Mbps em topologia linear.

**4**. Sobre o cabo par trançado, é correto afirmar:

a) Basicamente existem três tipos de cabo par trançado conhecidos por UTP, FTP e STP.

b) Basicamente existem dois tipos de cabo par trançado conhecidos por UTP e STP: ambos não possuem blindagem.

c) Basicamente existem dois tipos de cabo par trançado conhecidos por UTP e STP. Ambos possuem formas para garantir a imunidade a ruídos.

d) Os cabos STP são divididos em categorias, sendo a 1 e a 2 utilizadas na telefonia.

**5**. A respeito da técnica utilizada pelo cabo par trançado para oferecer imunidade a ruídos, é correto afirmar:

a) Utiliza a técnica de emplacamento para garantir a imunidade a ruídos.

b) Utiliza a técnica de encapsulamento para garantir a imunidade a ruídos.

c) Utiliza a técnica de cancelamento para garantir a imunidade a ruídos.

d) Esse tipo de cabo não possui técnica para garantir a imunidade a ruídos.

**6**. Acerca da nomenclatura do padrão 10BASET, 10BASE2 e 100BASET, é correto afirmar:

a) O padrão 10BASET refere-se à velocidade de 10 Mbps, transmissão baseband, atinge, no máximo, 10 metros de distância e utiliza o cabo coaxial. O padrão 10BASE2 refere-se à velocidade de 10 Mbps, transmissão baseband, e atinge até 185 metros de distância. O padrão 100BASET refere-se à velocidade de 100Mbps, transmissão baseband, atinge, no máximo, 100 metros de distância e utiliza cabo coaxial.

b) O padrão 10BASET refere-se à velocidade de 1000 Mbps, transmissão baseband, atinge, no máximo, 10 metros de distância e utiliza o cabo par trançado. O padrão 10BASE2 refere-se à velocidade de 10 Mbps, transmissão baseband e atinge até 185 metros de distância. O padrão 100BASET refere-se à velocidade de 10Mbps, transmissão broadband, atinge, no máximo, 100 metros de distância e utiliza cabo par trançado.

c) O padrão 10BASET refere-se à velocidade de 10 Mbps, transmissão broadband, atinge, no máximo, 100 metros de distância e utiliza o cabo par trançado. O padrão 10BASE2 refere-

se à velocidade de 100 Mbps, transmissão broadband, e atinge até 185 metros de distância. O padrão 100BASET refere-se à velocidade de 100Mbps, transmissão baseband, atinge, no máximo, 100 metros de distância e utiliza cabo par trançado.

d) O padrão 10BASET refere-se à velocidade de 10 Mbps, transmissão baseband, atinge no máximo 100 metros de distância e utiliza o cabo par trançado. O padrão 10BASE2 refere-se à velocidade de 10 Mbps, transmissão baseband e atinge até 185 metros de distância. O padrão 100BASET refere-se à velocidade de 100 Mbps, transmissão baseband, atinge, no máximo, 100 metros de distância e utiliza cabo par trançado.

**7**. A respeito do processo de flooding, é correto afirmar:

a) Os hubs fazem flooding em todas as suas transmissões.

b) O switch faz flooding independentemente da quantidade de tempo em que esteja ligado.

c) Os roteadores fazem flooding somente nos primeiros minutos depois de serem ligados.

d) O processo de flooding não é mais implementado por nenhum equipamento ativo.

**8**. (Sanepar, 2004) Assinale a única alternativa correta sobre cabeamento:

a) A especificação 10BASE5 permite comunicação em banda básica, a uma velocidade de 10Mbps, com comprimento máximo do segmento de 500 metros.

b) A especificação 10BASE2 faz uso de cabo par trançado, categoria 5, com conectores RJ-45 e terminadores nas extremidades do cabo.

c) A comunicação por fibra óptica faz uso de um cabo híbrido coaxial duplamente blindado com fibras de vidro, capaz de conduzir luz, definindo um canal upstream, que usa tecnologia eletrônica, e outro canal downstream, que usa tecnologia óptica.

d) A tecnologia mais popular para cabeamento presente na maioria das redes locais é o bluetooth, nome recebido em razão do

famoso cabo de par trançado azul usado para conectar computadores aos hubs.

e) Os cabos de par trançado categoria 5 são blindados e, por essa razão, imunes à interferência eletromagnética, podendo ser colocados em eletrodutos compartilhados com cabos da rede elétrica.

**9**. O que deve ser feito para que um cabo par trançado padrão T-568A torne-se um cabo *cross-over*?

**10**. Qual é a sequência correta de cores dos fios quando for "*crimpar*" um cabo par trançado no padrão T-568A?

**11**. (COPEL, 2010) O sistema de cabeamento estruturado prevê que a topologia física da rede em um ambiente de cabeamento secundário (ou horizontal) será:

a) Barramento.

b) Anel simples.

c) Anel duplo.

d) Ponto a ponto (ou *peer-to-peer*).

e) Estrela.

CAPÍTULO 6

# Equipamentos ativos

Neste capítulo, apresentaremos os detalhes dos equipamentos ativos, que são peças fundamentais no projeto de uma rede de computadores. Os equipamentos ativos apresentados neste capítulo serão bridges, switches e roteadores. Abordaremos o conceito e a utilização de VLANs, como também o conceito e a utilização do QinQ. Mencionaremos, ainda, a importância dos protocolos STP (*Spanning Tree Protocol*), RSTP (*Rapid Spanning Tree Protocol*) e EAPS (*Ethernet Automatic Protection Switching*), indispensáveis para a transmissão de dados em redes que utilizam switches interligados em anel. A fim de melhorar o entendimento sobre roteadores, apresentaremos alguns detalhes sobre o protocolo IP.

## 6.1 Introdução

Equipamentos de redes locais (LAN) estão divididos em dois grupos: os equipamentos passivos e os ativos. No grupo de equipamentos passivos, temos os cabos, os conectores e o patch panel, ou seja, equipamentos necessários para garantir que os equipamentos ativos consigam transportar os bits. Estes equipamentos não são energizados, por isso são classificados como passivos.

Os equipamentos ativos, em uma rede local, são os responsáveis pela geração e pelo transporte dos bits (tensões elétricas) entre os equipamentos de uma rede. Exemplos de equipamentos ativos: switches e roteadores, os quais garantem uma comunicação confiável com o desempenho requerido pela aplicação; portanto, é imprescindível que esses equipamentos estejam dimensionados adequadamente às necessidades da organização. A preocupação com a qualidade e a confiabilidade dos equipamentos ativos de rede é uma questão que deve ser levada em conta não apenas nas grandes empresas, mas em qualquer projeto de rede. A seguir,

comentaremos em detalhes os equipamentos ativos utilizados em projetos de rede.

## 6.2 Bridge

A bridge é um equipamento antigo, sendo que atualmente em novos projetos de rede opta-se pela aquisição e instalação de switches.

## 6.3 Switch

O switch opera na camada de enlace do modelo de referência OSI. O switch, ao receber um quadro, analisa os endereços MAC de origem e desino e, baseando-se em uma tabela construída de forma dinâmica (tabela de *bridging*), decide para qual porta enviar o quadro Ethernet. Com isso, em vez de replicar os quadros recebidos para todas as suas portas, ele envia o quadro somente para a porta na qual o micro ligado possua o endereço MAC igual ao endereço MAC solicitado. O switch, por não enviar seus dados a todos os computadores ligados a ele, permite um melhor desempenho da rede, evitando colisões e inundações. A tabela de *bridging* é conhecida por *MAC address table* em switches das fabricantes Datacom e Cisco ou FDB (*Forwarding DataBase*) em switches da fabricante Extreme.

A tabela de *bridging* é construída dinamicamente pelo switch, precisando apenas que seja recebido um quadro por uma de suas portas. Ao receber um quadro, o switch extrai o endereço MAC de origem e a VLAN, que serão armazenados na tabela de *bridging*. Quando o receptor devolver a requisição ao equipamento origem, o switch analisará o novo quadro e extrairá o endereço MAC de origem e sua VLAN, que também serão armazenados na tabela de *bridging*.

Após registrar os dados na tabela de *bridging*, o switch analisará o endereço MAC de destino recebido. Caso o endereço MAC de destino já exista na tabela, este verificará em qual porta o endereço MAC foi relacionado. É importante observar que antes de repassar o quadro, o switch verificará ainda se a VLAN recebida do equipamento origem e a VLAN da porta de saída coincidem. Caso

positivo, o quadro será repassado à porta e entregue ao equipamento destino. Caso as VLANs não coincidam, o quadro será descartado. Nos casos em que o endereço MAC não estiver cadastrado na table de *bridging*, o switch enviará o quadro a todas as suas portas (exceto à porta que criou o quadro), da mesma forma que os hubs o fazem. Esse processo é conhecido por inundação (*flooding*).

É importante observar que o tempo de permanência do endereço MAC na tabela de *bridging* é finito, ou seja, caso o fluxo de quadros seja interrompido por mais de 300 segundos, a entrada qua havia sido registrada anteriormente será removida. Caso o equipamento mantenha ativo seu fluxo de dados, o switch constantemente atualizará o tempo da respectiva entrada (*age*), a fim de evitar que o endereço MAC seja removido da tabela após o tempo comentado.

Outro ponto importante a ressaltar é que quando o switch recebe um quadro do tipo *broadcast* (pacotes com endereço MAC igual a FF:FF:FF:FF:FF:FF) em uma porta, o switch repassará o quadro a todas as outras portas, sem consultar sua tabela de *bridging*, ou seja, realiza novamente o processo de inundação.

O switch possui três métodos de operação conhecidos por *store and forward*, *fragment free* e *cut-through*. A forma *fragment free* é a menos utilizada, mas existem switches que a implementam. A seguir, descreveremos esses métodos de transmissão de quadros.

- *Store and forward* – Essa forma de operação armazena o quadro inteiro para, então, enviá-lo pela porta destino. Nesse método, o switch lerá todo o quadro para o buffer e verificará se existem erros de CRC. Se houver algum problema, o quadro será descartado. Se estiver OK, verificará qual é a porta associada ao endereço MAC de destino e encaminhará o quadro.
- *Cut-through* – O método *cut-through* é também conhecido como *fast forwarding*. Nesse método, assim que o campo do destinatário (endereço MAC destino) é recebido, inicia-se o envio do pacote pela porta destino. É mais eficiente se comparado ao método *store and forward*. O cut-through lê o endereço MAC (destino) assim que o quadro chega e, depois de descobrir a porta destino, envia o

quadro para a porta, antes mesmo de recebê-lo completamente na porta origem. Poucos switches são totalmente cut-through, pois esse sistema não permite nenhum tipo de correção de erros.

Muitos switches usam cut-through até que um certo nível de erros seja alcançado. Após esse nível predeterminado de erros ser alcançado, o switch passa a operar em store and forward.

- *Fragment free* – Esse método funciona como o cut through, embora o switch armazene os primeiros 64 bytes do quadro antes de enviá-lo. A razão para isso é que a maior parte dos erros ocorre nos primeiros 64 bytes de um quadro.

  Atualmente, quando se ligam switches em cascata, utilizam-se as portas gigabit Ethernet (1 Gbps) ou portas 10 Gbps por garantirem que os clientes conectados nos switches da ponta não sofram com gargalos para alcançarem os roteadores.

### 6.3.1 Protocolos que removem loops em redes com switches ligados em anel

Ao mesmo tempo que os switches melhoram o tráfego da rede, se interligadas em anel, podem gerar loops. Caso isso ocorra, fará que um quadro de *broadcast* fique viajando entre os equipamentos de forma infinita. Como os *broadcasts* são inundados em todas as portas pelo switch, estes aumentarão indefinidamente, fazendo que o processador do switch atinja um consumo que chegará perto de 100%. Quando isso ocorrer, o switch travará e os equipamentos conectados não conseguirão transportar seus dados através dele. Para solucionar esse problema, Radia Perlman desenvolveu o algoritmo de spanning tree, que será descrito neste capítulo.

A seguir, relataremos uma situação em que o problema de loop infinito pode ocorrer, exemplificado na figura 6.1. Digamos que o computador 1 emitiu uma requisição do tipo *broadcast* ao computador 2 por meio do segmento A. Como um broadcast é gerado? O simples fato de um computador dar um *ping* em outro endereço IP de outro computador gerará uma requisição do protocolo ARP. O protocolo ARP utiliza broadcasts para sua operação.

O switch 1 enviará os *broadcasts* aos segmentos D e B. Os switches 2 e 3 também receberão os *broadcasts,* que, por sua vez, vão enviá-los aos segmentos C e E. Nesse momento, o computador 2 receberá o pedido. Entretanto, os quadros de *broadcasts* serão enviados ao segmento C e, na sequência, aos segmentos D, B e assim por diante. Desse modo, esses quadros ficarão viajando pela rede de forma infinita, comprometendo o desempenho da rede.

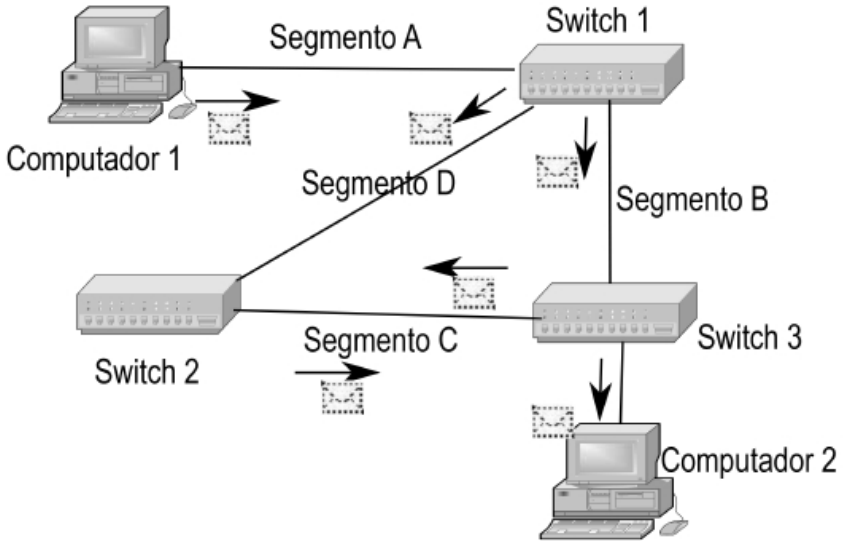



*Figura 6.1 – Rede com múltiplos switches.*

Para solucionar o problema do loop infinito, podemos escolher entre os protocolos STP (*Spanning Tree Protocol*), RSTP (*Rapid Spanning Tree Protocol*) ou EAPS (*Ethernet Automatic Protection Switching*).

Por que interligar switches em anel?

Atualmente, muitas operadoras comercializam serviços de rede em alta velocidade por meio da interconexão de switches por propiciar simples administração, baixo custo, fácil interconexão e banda adequada a qualquer necessidade. Essas redes formadas por switches buscam basicamente interconectar LANs corporativas geograficamente separadas, interconectando-se, ainda, a uma rede WAN ou backbone operado por uma operadora (exs.: COPEL Telecom, GVT, Algar). Essa rede formada por vários switches garante, por meio de caminhos redundantes, que os clientes não deixem de ser atendidos mesmo se houver problemas em parte da

rede, ou seja, se uma fibra óptica for rompida em um determinado ponto, o cliente acessará seu roteador por um dos caminhos redundantes. Esse cenário pode também ser estendido a empresas privadas que tenham inúmeros equipamentos interconectados sobre switches.

Dessa forma, o cliente contrata um link de alta velocidade e a operadora o conecta a um switch de um de seus POPs (pontos de presença). Por sua vez, esse switch será interconectado com outros até que alcancem uma das portas de um roteador de grande porte (exs.: Huawei, Cisco, Juniper). Ao chegar ao roteador, o cliente terá acesso a outras redes da própria empresa (via VPN MPLS) ou à Internet. Para que o cliente possa usufruir da redundância disponibilizada nessa arquitetura de rede, torna-se necessária a ligação em formato anel. Com isso, para que os switches não entrem em loop devido às tormentas de *broadcast*, precisamos utilizar protocolos que tenham a função de logicamente remover os loops. Assim, abordaremos neste capítulo os protocolos STP, RSTP e EAPS, todos voltados à eliminação do loop de uma rede formada por switches.

### 6.3.2 Spanning Tree Protocol (STP)

Conforme comentado anteriormente, quando temos switches interligados em anel, podemos ter problemas de loops infinitos. Esse loop implicará a interrupção total da comunicação entre os equipamentos interligados. O loop ocorre devido a quadros de *broadcast* serem repassados a todas as portas e, por isso, ficarem vagando entre os equipamentos de forma desordenada. Para evitar tempestades de *broadcast* e outros problemas associados ao loop de topologia, foi desenvolvido o algoritmo *Spanning Tree Protocol* (STP), padronizado pelo IEEE como 802.1d em 1990. Esse algoritmo considera que cada switch tem associado um grupo de identificadores (IDs), sendo um para o switch e outro para cada porta.

O ID do switch é conhecido como bridge ID (BID), sendo composto de 8 bytes. Os dois primeiro bytes são definidos pela prioridade

atribuída ao switch que, por padrão, vale 32768. Esse valor poderá ser ajustado no switch para mudar o comportamento do protocolo, dependendo das necessidades de configuração. Neste capítulo, veremos quando fará sentido ajustar esse valor. Os demais 6 bytes são preenchidos pelo endereço MAC do switch. Cada switch possui também um ID composto de 16 bits, sendo 6 bits para definir a prioridade e 10 bits para identificar o número da porta. A figura 6.2 apresenta uma rede com o protocolo STP habilitado.

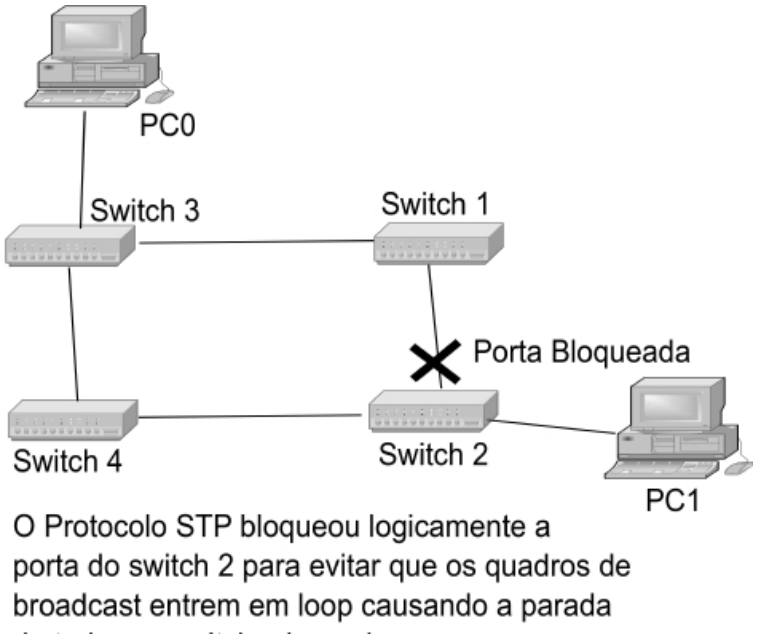



*Figura 6.2 – Rede com STP habilitado.*

Basicamente, o STP detecta e elimina loops em redes segmentadas, ao mesmo tempo que mantém a possibilidade de conexões redundantes entre switches (o que implica mais tolerância a falhas). Na ocorrência de laços, algumas portas são desativadas para eliminar os loops. Para isso, é criada uma árvore que não contém laços. Portas que não fazem parte dessa árvore serão bloqueadas logicamente. Em caso de falha em um caminho ativo, o STP automaticamente ativa caminhos redundantes, desbloqueando automaticamente as portas que haviam sido bloqueadas. A figura 6.3 apresenta a topologia física e lógica de uma rede antes e depois de o protocolo STP atuar.

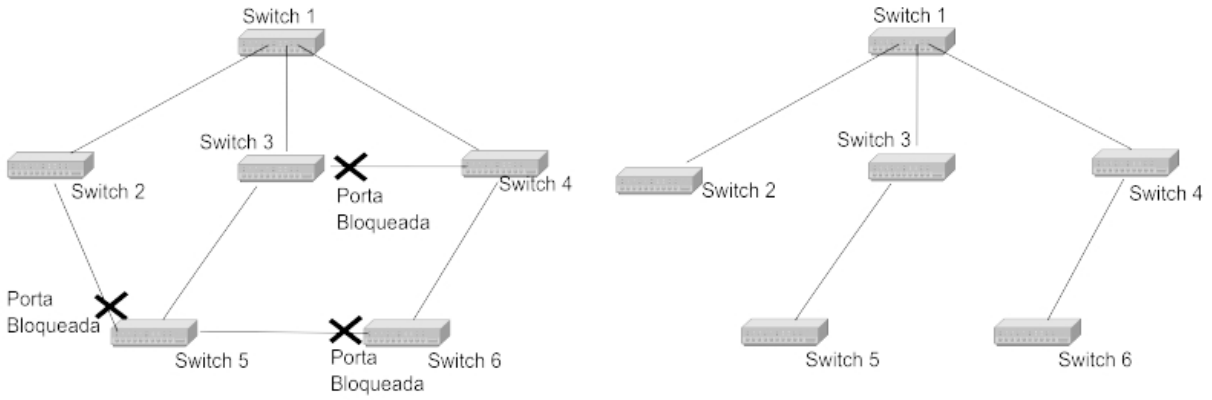



*Figura 6.3 – Topologia física e lógica com STP.*

É importante observar que para o processo de bloqueio e desbloqueio de portas ocorrer de forma automática, segue-se um processo de eleição que envolve os switches e suas portas. Dividiremos o processo de eleição em quatro etapas:

- **Passo 1** – Eleição do switch-raiz (*bridge root*).
- **Passo 2** – Eleição das portas-raiz (*root ports*).
- **Passo 3** – Eleição das portas designadas (*designated ports*).
- **Passo 4** – Bloqueio lógico de uma das portas para evitar o loop, conhecida por porta não designada.

### 6.3.2.1 Eleição do switch-raiz (bridge root)

Ao ser ligado, cada switch presente na rede inicia um procedimento de descobrimento para determinar qual será eleito o switch-raiz, ou seja, em um segmento em que existam vários switches, apenas um será o de referência (raiz). Para essa decisão, o switch envia, por meio de *broadcasts*, quadros especiais chamados de unidades de dados de protocolo de bridge (*Bridge Protocol Data Units* – BPDU), entre todos os switches interconectadas no mesmo segmento. É importante observar que os BPDUs trafegam sobre a VLAN 1. Abordaremos os detalhes das VLANs neste capítulo.

Os campos do quadro BPDU estão descritos na tabela 6.1.

*Tabela 6.1 – Campos do quadro BPDU*

| Campo | Descrição |
|---|---|

| Campo | Descrição |
|---|---|
| BID-raiz | Este é o BID do switch-raiz da árvore. É fornecido pelo fabricante ou configurado pelo administrador da rede. |
| Custo do caminho da switch-raiz | Determina a distância entre o switch-raiz e o switch que está enviando os BPDUs. |
| BID do emissor | BID do switch que envia o BPDU. |
| ID da porta | A porta da qual este BPDU partiu. |

Inicialmente, ao ser ligado, todo switch assume que é o switch-raiz (*bridge root*). Contudo, depois da avaliação dos quadros BPDU, o switch-raiz será escolhido. Essa escolha está baseada em uma eleição entre os switches, e o switch que possuir o menor BID (prioridade igual a 32768 + endereço MAC do switch) ganhará a eleição. Uma vez que o switch-raiz é determinado, iniciará o segundo passo, que trata da eleição das portas-raiz (*root port*). A figura 6.4 apresenta uma rede com STP habilitado, como também o resultado após a eleição do switch-raiz ter sido concluída.

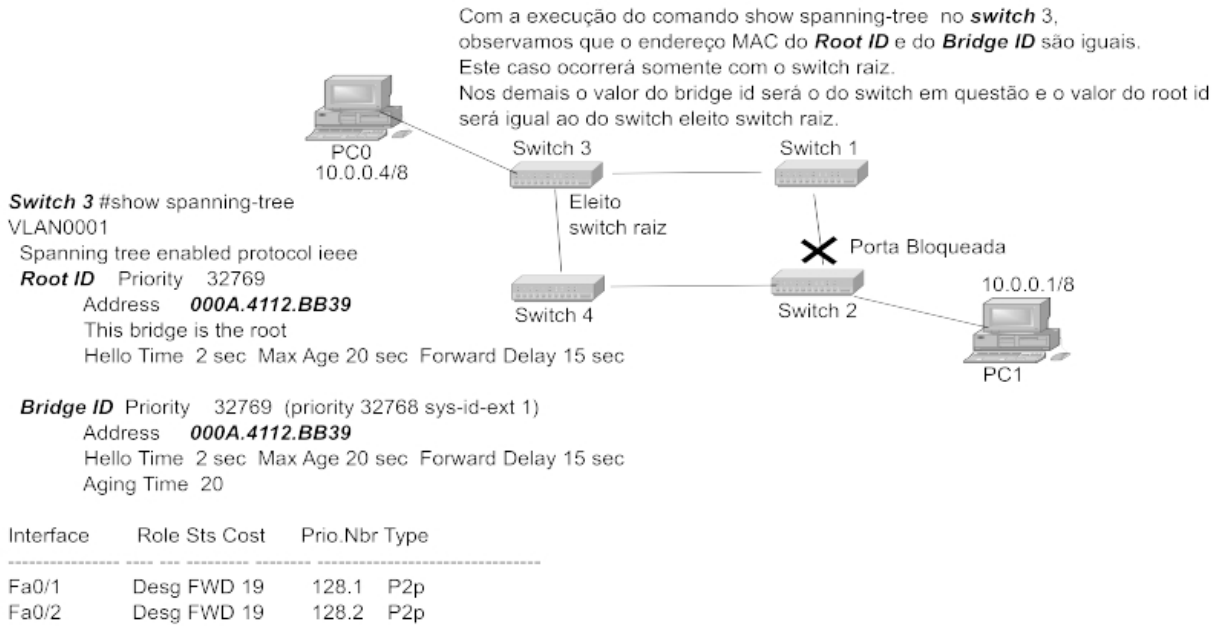


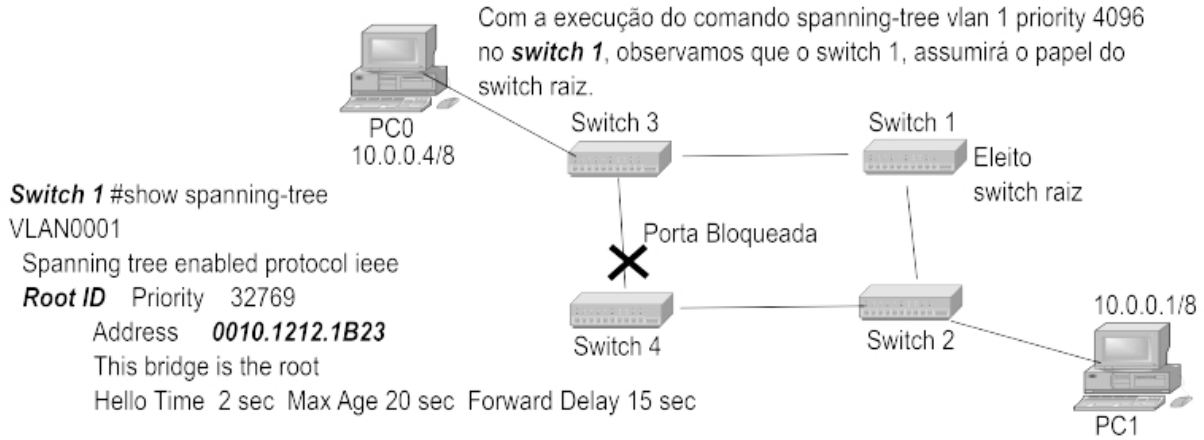

*Figura 6.4 – Switch 3 eleito Switch-raiz.*

Conforme podemos observar na figura 6.4, o switch 3 foi eleito o switch-raiz e uma das portas do switch 2 foi bloqueada logicamente.

Há situações em que o administrador da rede precisa que um

determinado switch assuma o papel de switch-raiz mesmo que, por padrão, não tenha o menor BID. Para que isso ocorra, será necessário modificar o valor do campo prioridade, pois o endereço MAC do switch não pode ser alterado. Conforme comentado, o switch que possuir o menor BID (composto de campo prioridade e endereço MAC) será eleito o switch-raiz. A figura 6.5 apresenta os comandos (padrão Cisco) necessários para que o campo prioridade seja ajustado. Com isso, o switch (neste exemplo, o switch 1) que teve esse parâmetro ajustado tornou-se o switch-raiz. Apesar de o valor informado ser 4096, o equipamento soma uma unidade ao valor, passando-o para 4097.

Conforme podemos observar na figura 6.5, após a execução do comando que altera o valor do campo prioridade para 4096, o switch 1 passou a ser o switch-raiz e uma das portas do switch 4 foi bloqueada.




***Switch 1*** #show spanning-tree
VLAN0001
Spanning tree enabled protocol ieee
***Root ID*** Priority 32769
Address ***0010.1212.1B23***
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

***Bridge ID*** Priority 32769 (priority 32768 sys-id-ext 1)
Address ***0010.1212.1B23***
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 20

| Interface | Role | Sts | Cost | Prio.Nbr | Type |
|---|---|---|---|---|---|
| Fa0/1 | Desg | FWD | 19 | 128.1 | P2p |
| Fa0/2 | Desg | FWD | 19 | 128.2 | P2p |

*Figura 6.5 – Alterando o switch-raiz.*

### 6.3.2.2 Eleição das portas-raiz (root port)

A partir do momento que o switch-raiz é eleito, inicia-se a eleição

nos demais switches sobre qual das portas conectadas ao anel será definida como porta-raiz. Uma porta-raiz é responsável por receber os BPDUs, enquanto as portas eleitas como designadas (próxima etapa que comentaremos) são responsáveis por gerar os BPDUs. É importante observar que no switch-raiz não teremos portas-raiz, somente portas designadas. Essa definição formaliza que o switch-raiz é quem gera os BPDUs e os demais switches conectados ao anel os receberão pelas portas-raiz. Dessa forma, as portas que estiverem mais próximas do switch-raiz serão definidas como portas-raiz.

Para o protocolo STP, uma porta-raiz é a mais próxima do switch-raiz. Essa proximidade é medida levando-se em consideração o custo do link. Esse custo é calculado baseando-se na velocidade do link. A figura 6.6 apresenta os custos de cada link, quando se utiliza a medida por 16 bits e 32 bits. Com o advento do protocolo RSTP, essa tabela foi modificada, alterando o valor dos custos. A tabela de custo de 16 bits se aplica a switches mais antigos, enquanto a tabela de custo de 32 bits se aplica a equipamentos mais modernos. Atualmente, em algumas operadoras, ainda se utilizam switches que possuem o custo baseado nos valores definidos por 16 bits. Alguns simuladores de rede (ex.: *Packet Tracer,* da Cisco, comando show spanning-tree) também utilizam o custo baseado nos valores de 16 bits definidos na época da definição do protocolo STP.

| | Protocolo STP | Protocolo RSTP |
|---|---|---|
| | IEEE 802.1D-1998 | IEEE 802.1W-2001 |
| Velocidade da porta Ethernet | Custo | Custo |
| 10 Mbps | 99 | 2000000 |
| 100 Mbps | 19 | 200000 |
| 1 Gbps | 4 | 20000 |
| 10 Gbps | 2 | 2000 |
| 100 Gbps | 1 | 200 |

*Figura 6.6 – Relação entre os custos dos protocolos STP e RSTP.*

Conforme comentado, o que define se uma porta será ou não a porta-raiz dependerá da soma do custo dessa porta até o switch-raiz. Porém, podem ocorrer casos em que um switch tenha duas

portas cuja soma dos custos de cada link seja a mesma. Na figura 6.7, temos uma rede em que o switch-raiz eleito foi o 7 (isso ocorreu devido a ter o menor BID).

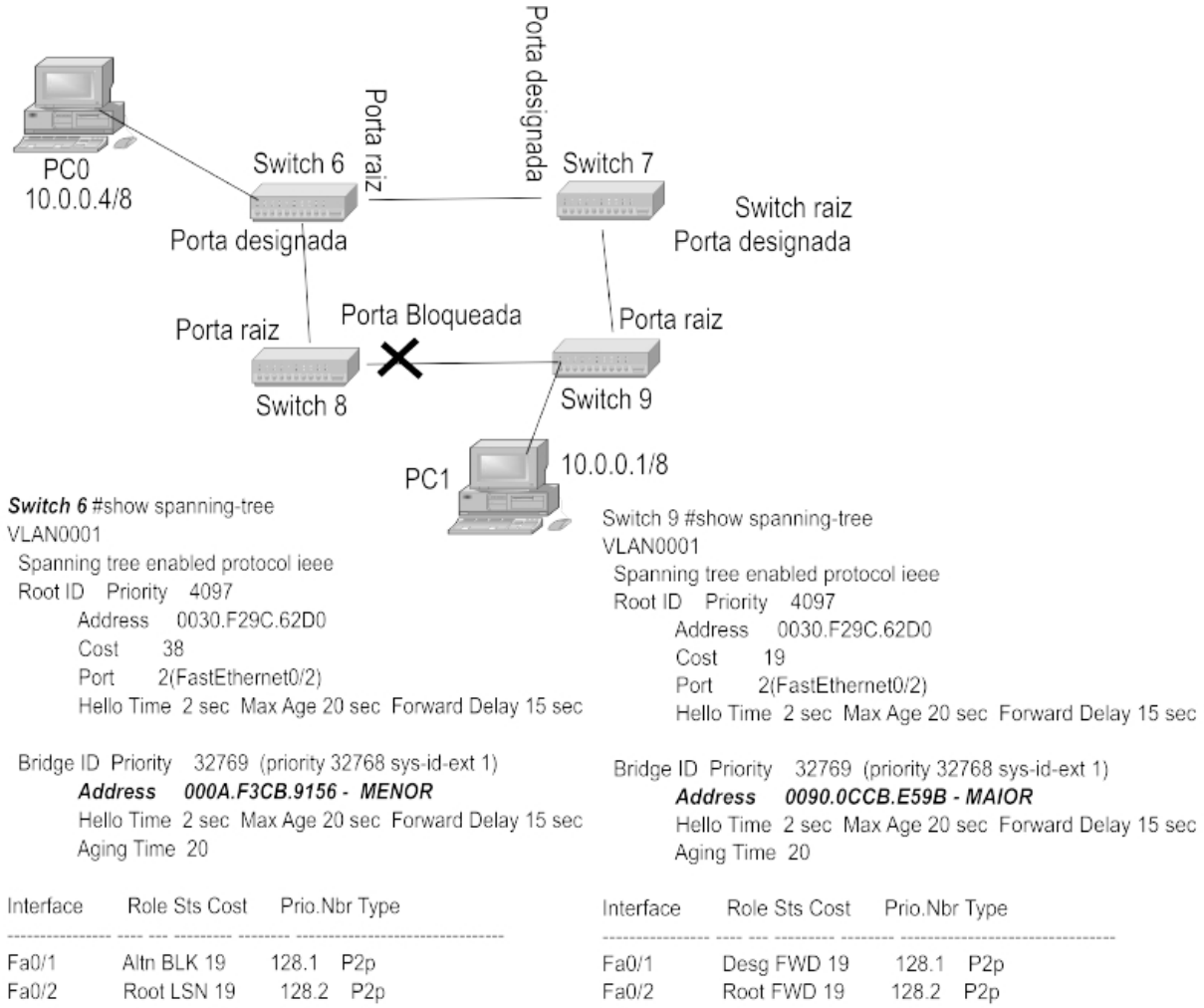



*Figura 6.7 – Ajustes na porta que fica no estado de bloqueada.*

Fica claro nesta figura quais são as portas dos switches 6 e 9 mais próximas do switch-raiz, porém, no caso do switch 8, o custo de ambas as portas é o mesmo, ou seja, temos dois links de 100 Mbps para cada lado do switch. Nesse caso, a soma dos custos de ambas as portas será 38 (dados que todos os links sejam 100 Mbps e a tabela utilizada seja de 16 bits).

Neste caso, quando os custos de ambas as portas são o mesmo, seguimos para o próximo elemento de desempate. Para o protocolo STP, a porta considerada a porta-raiz será aquela que receber o

menor BID do seu respectivo switch vizinho. Na figura 6.7, o switch 6 possui um BID menor que o do switch 9 e, por isso, a porta-raiz do switch 8 foi a porta conectada ao switch 6.

Caso quiséssemos que a porta conectada ao switch 9 fosse a porta-raiz, poderíamos elevar o campo prioridade do switch 6 para um valor igual a 40960, por exemplo. Com isso, automaticamente o protocolo STP mudaria a porta-raiz para a porta conectada ao switch 9. É importante observar que não estamos nos referindo à porta bloqueada que, neste caso, está alternando com a porta-raiz. O foco neste exemplo foi mudar a porta-raiz. Comentaremos como mudar a porta bloqueada ainda neste capítulo.

Há a possibilidade de ambos os elementos de desempate serem iguais, ou seja, terem o mesmo custo e o mesmo BID recebido do switch vizinho. Essa situação ocorrerá quando tivermos dois switches interligados por dois cabos. Neste caso, a porta-raiz será a porta com a menor prioridade recebida do switch vizinho. A prioridade normalmente é a mesma para todas as portas e, por isso, esse elemento não determinará qual deverá assumir como porta-raiz. Neste caso, seguiremos para o último elemento de desempate, que é identificado pela porta do switch. Por exemplo, se conectarmos dois switches utilizando as portas 1 e 10 do switch-raiz com as portas 1 e 10 do segundo switch, a porta-raiz será a porta 1, pois o número 1 é menor que o número 10.

Ao concluir a eleição da porta-raiz, o protocolo STP seguirá para a terceira eleição, definir entre duas ou mais portas designadas qual ficará bloqueada. Para cada loop que houver na rede, uma porta precisará ficar bloqueada logicamente.

#### 6.3.2.3 Eleição das portas designadas e definição da porta bloqueada

Após concluir a eleição das portas-raiz de todos os switches do anel, inicia-se a eleição das portas designadas. Todas as demais portas de um switch que fazem parte do anel, mas não foram eleitas porta-raiz (portas que recebem BPDUs), poderão ser eleitas portas designadas (portas que geram BPDUs). Quando houver duas no

mesmo segmento, uma delas deverá ficar bloqueada logicamente.

Para determinar quais serão as portas designadas e qual será a bloqueada, considera-se o caminho com menor custo até o switch-raiz. A porta com menor custo se manterá como designada, e o valor do custo de cada porta está relacionado à velocidade do link (Figura 6.6). Caso o custo de ambas as portas seja igual, o protocolo STP manterá como designada a porta que pertencer ao switch com o menor BID (campo composto de prioridade e endereço). Assim, a porta que pertencer ao switch com maior BID ficará como bloqueada. A figura 6.8 demonstra que a porta bloqueada foi a do switch 0 em razão de o BID desse switch ser maior que o BID do switch 2.

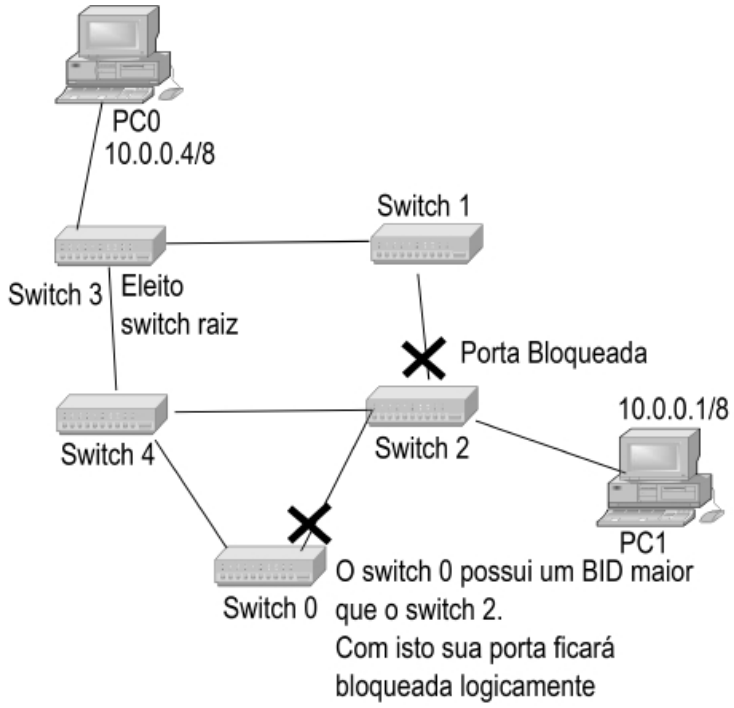



*Figura 6.8 – Ajuste na porta bloqueada em relação a figura 6.7.*

A figura 6.9 apresenta como podemos identificar que o BID do switch 0 é maior que o BID do switch 2.

Caso fosse necessário mudar a posição da porta bloqueada, precisaríamos apenas aumentar o BID do switch 2 para que ficasse maior que o do switch 0.

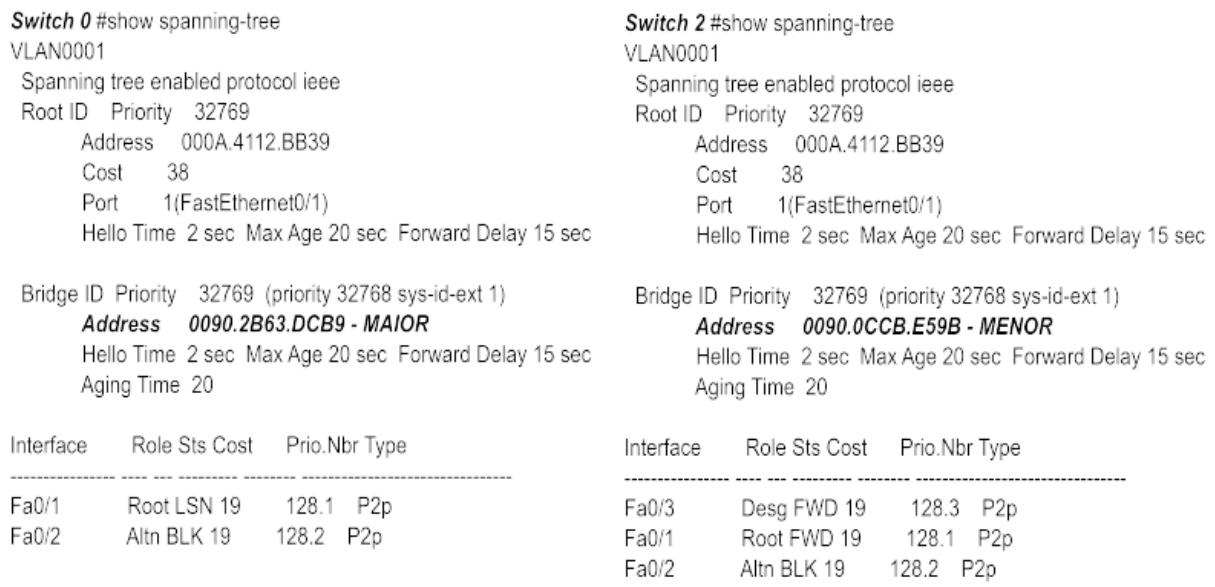



*Figura 6.9 – Observando o BID dos switchs.*

### 6.3.2.4 Processo de convergência do STP

A convergência do protocolo STP é o seu maior problema. Durante o processo de convergência, os switches impedem que as portas interligadas ao anel transmitam dados, ficando dedicados ao restabelecimento dos caminhos, ou seja, somente após o processo de eleição ser concluído é que as portas serão liberadas para transmisão de dados dos clientes. Enquanto esse processo não for encerrado, somente serão transmitidos BPDUs.

O tempo que leva para o processo de convergência ser concluído dependerá de três parâmetros, transportados entre os switches através dos quadros de BPDUs e configuráveis nos switches que dispõem do protocolo STP. O switch-raiz é quem determinará com quais valores os demais switches deverão se basear para o processo de convergência.

O primeiro parâmetro é chamado de *hellotime*, o segundo, *maxage*, e o terceiro, *forwarddelay*. O valor desses parâmetros é transportado entre todos os switches que compõem o anel através dos quadros de BPDUs gerados pelo switch-raiz. Essa garantia é dada no momento da eleição dos switches, pois os BPDUs transmitidas pelo switch-raiz contendo tais parâmetros serão acatadas pelos demais switches. Dessa forma, não adiantará mudar o valor desses

parâmetros em um switch que não seja o switch-raiz, pois se o fizer, não terá validade.

É importante observar que durante o processo de convergência as portas conectadas ao anel poderão assumir os seguintes estados:

- *Blocking* (bloqueada) – Permanecerão neste estado as portas não designadas pela eleição ou quando os switches forem ligados. Neste estado, a porta não encaminha quadros dos clientes, mas apenas recebe e analisa BPDUs.
- *Listening* (escutando) – Permanecerão neste estado as portas que se encontram em transição do estado blocking para o estado de *forwarding*. Neste estado, a porta não encaminhará quadros de clientes, porém receberá e analisará BPDUs. Durante esse estado, as portas do switch receberão e processarão os BPDUs, avaliando o seu custo até o switch-raiz.
- *Learning* (aprendendo) – Neste estado, uma porta não encaminhará os quadros recebidos de clientes, mas apenas os BPDUs. Os dados dos clientes recebidos serão processados pelos switches, ou seja, o switch registrará o endereço MAC de origem na tabela de *bridging*, porém não os encaminhará.
- *Forwarding* (enviando) – Neste estado, uma porta enviará e receberá quaisquer quadros.

O que mais prejudica a utilização do protocolo STP é o tempo de convergência conforme comentado. Por padrão, os parâmetros citados são previamente configurados e determinarão o tempo de convergência da rede. Vejamos os detalhes de cada parâmetro.

- *hellotime* – Por padrão vem configurado com 2 segundos. Esse parâmetro especifica o intervalo de tempo entre a transmissão de um e outro BPDU pelo switch-raiz. Esse valor normalmente pode variar entre 1 e 10 segundos. Ajustar o valor, por exemplo, para 1 segundo significará duplicar a quantidade de BPDUs circulando entre os switches.
- *maxage* – Por padrão vem configurado com 20 segundos. Esse parâmetro representa o tempo que um switch espera pelo recebimento de um BPDU. Após esse tempo transcorrido, o

switch dará como perdida a sua comunicação com o switch-raiz. Nesse caso, o switch afetado reiniciará uma nova convergência seguindo os três passos da eleição comentada. Quando o switch perceber que esse tempo transcorreu, colocará suas portas no estado de *listening* e aguardará um determinado tempo até que possa novamente voltar ao estado de *forwarding*.

- *forwarddelay* – Por padrão, vem configurado com 15 segundos, porém permanece 15 segundos no estado *listening* e outros 15 segundos no estado *learning*.

  O parâmetro f*orwarddelay*, por padrão, bloqueia as portas do switch por 15 segundos para permanência no estado de *listening* e outros 15 segundos para permanência no estado de *learning*, ou seja, eleva o tempo de convergência do protocolo STP em torno de 30 segundos.

É importante observar que na composição desse tempo, leva-se novamente em consideração o tempo do parâmetro *maxage* apresentado anteriormente. Esse é o principal motivo pelo qual o protocolo STP possui convergência lenta. Mesmo que os switches concluam a convergência em menos tempo, será aguardado o valor de 30 segundos. A movimentação da porta para o estado de *listening* indica que há uma mudança na topologia da rede e 15 segundos transcorrerão para que os switches decidam quem é o switch-raiz e quais portas serão raiz, designadas e qual ficará bloqueada. Esse anúncio de mudança é feito pelo envio de quadros BPDUs e fará que a porta fique bloqueada para a transmissão de quadros dos clientes. Em seguida, permanecem-se outros 15 segundos no estado de *learning*, em que o switch ajustará sua tabela de *bridging*. Esse processo ocorrerá quando os switches forem ligados ou quando houver uma mudança na topologia.

Esse alto tempo de convergência fez a indústria buscar outras opções que oferecem um tempo menor de convergência. Entre as opções atualmente utilizadas pelas operadoras e provedores de rede, apresentaremos os protocolos RSTP e EAPS.

### 6.3.3 Rapid Spanning Tree Protocol (RSTP)

O RSTP, em inglês Rapid Spanning Tree Protocol (norma IEEE 802.1w), é uma evolução do protocolo STP (IEEE 802.1d). O RSTP manteve a terminologia do padrão 802.1d, e a maioria dos parâmetros permaneceu inalterada. O RSTP oferece um tempo menor de convergência na rede. O fato de convergir mais rápido faz que esse protocolo seja preferido em relação a seu antecessor..O tempo de convergência fica em torno de 10 segundos contra os até 50 segundos do STP tradicional. É importante observar que o RSTP é totalmente compatível com STP, porém, se ambos forem utilizados no anel, o desempenho da convergência seguirá o padrão STP. Apesar da compatibilidade de operação, o RSTP define três estados para as portas conhecidos por *discarding*, *learning* e *forwarding* contra quatro estados do protocolo STP conhecidos por blocking, *listening*, *learning* e *forwarding*

O RSTP estabelece cinco papéis (*roles*) para definir as portas envolvidas no anel, conhecidas por porta-raiz (root port), porta designada (*designated port*), porta alternada (*alternate port*), porta backup (*backup port*) e porta desabilidata (estado de disable – desabilitado) pelo administrador da rede). É importante observar que as etapas da eleição do switch-raiz, porta-raiz e porta alternada do protocolo RSTP seguem as mesmas regras e políticas já apresentadas no protocolo STP.

#### 6.3.3.1 Processo de convergência do RSTP

Com o protocolo STP (802.1d), mesmo que a convergência ocorra em poucos segundos, cada switch esperará em torno de 30 segundos para alterar o estado de uma porta para *forwarding*. Com o protocolo STP, o switch-raiz é quem comanda os anúncios por meio dos quadros BPDU. As portas-raiz, por serem as mais próximas do switch-raiz, são responsáveis por ouvirem os BPDUs, enquanto as portas designadas enviam os BPDUs. Quando uma porta-raiz não recebe um BPDU por 20 segundos, esta reinicia o processo de convergência. Todo anúncio de BPDU parte do switch-raiz e circula pela hierarquia/árvore.

Com o RSTP (802.1w), o tempo de convergência será em torno de 10 segundos. A maior parte desse tempo será para concluir o

processo de eleição do switch-raiz, das portas-raiz, das portas designadas e, por fim, a definição sobre qual porta designada deverá ficar bloqueada. No protocolo RSTP, o tempo do parâmetro *maxage* é de 6 segundos [3 BPDUs não recebidos * *hellotime* (2 segundos)]. Caso um switch perceba que esse tempo foi alcançado, iniciará o processo de convergência com seu vizinho.

Para acelerar o processo de convergência, o RSTP oferece mecanismos para rapidamente colocar uma porta no estado de *forwarding* com segurança. Esses mecanismos impactam diretamente no tempo de convergência, o que dependerá do tipo da conexão definida em cada porta. O RSTP define três tipos de conexões entre as portas de um switch, conhecidos por porta *edge*, *non-edge* e *link type* igual a ponto a ponto.

Todas as portas diretamente conectadas a estações finais, como computadores, impressoras, roteadores ou switches sem o *spanning tree* habilitado, não podem criar laços lógicos entre switches na rede e, assim, podem ser configuradas como *edge* (conhecidas também por *portfast*). Portanto, uma porta *edge* transita diretamente para o estado *forwarding*, ignorando o estado *learning* (tempo de 15 segundos que o switch utiliza para aprender os endereços MACs). Portas *edge* não geram mudanças na topologia quando o enlace é ativado ou desativado, ou seja, não influenciam o tempo de convergência do protocolo RSTP. Porém, quando uma porta *edge* recebe um BPDU, imediatamente perde o estado de porta *edge*, tornando-se uma porta com configurações spanning tree com tempo de convergência alto.

Uma conexão do tipo *non-edge* denominada em alguns equipamentos por porta *broadcast* ou compartilhada possui tempo de convergência lento igual ao do protocolo STP. Uma porta ficará nesse estado caso seja conectada a um hub ou esteja como *edge* e a porta receba um BPDU. Esse tipo de conexão é o padrão seguido pelos switches ao serem instalados.

Uma porta com link type igual a ponto a ponto (denominada por alguns fabricantes de *P2p*) também alternará seu estado de *discarding* para *forwarding* imediatamente após ser ligada, ignorando o

estado *learning* (definida por 15 segundos para que o switch aprenda os endereços MAC). Essa rápida mudança de estado é obtida devido a o switch considerar que uma porta *P2p* está conectada a um único switch. Para que uma porta possa ser classificada como ponto a ponto, esta deverá ser conectada em *full-duplex* a outra porta de um switch pertencente ao anel. A configuração de uma porta para permanecer em ponto a ponto deverá ocorrer de forma explicíta pelo administrador da rede.

Apesar do tempo menor de convergência oferecido pelo RSTP, sua utilização em redes metro prejudica clientes que utilizam aplicações de missão crítica, como aqueles que transmitem sinais de TV e sinais de rádio FM. Dessa forma, para esses clientes, todas as vezes que ocorrer mudança na topologia da rede haverá interrupção da transmissão de dados, o que prejudicará a qualidade do serviço prestado. Para garantir que o tempo de convergência seja imperceptível para esses clientes, sugere-se a utilização do protocolo EAPS que oferece um tempo de convergência muito menor (na casa dos milissegundos contra a casa dos segundos) que o do RSTP.

### 6.3.4 Protocolo Ethernet Automatic Protection Switching (EAPS)

O protocolo EAPS é uma alternativa aos protocolos STP e RSTP no que tange à eliminação do loop infinito quando interligamos switches em anel dentro de uma rede metro. A redundância em uma rede metro aumenta a sua qualidade, garantindo que a comunicação não será interrompida no caso de rompimento de um dos caminhos da fibra óptica.

Com o protocolo EAPS, ganhamos também na resiliência. O termo resiliência, em uma rede composta de switches ligados em anel, remete ao tempo que os switches levarão para voltar a transportar quadros após sofrerem alguma intervenção externa (ex.: instalação de um novo switch no anel ou rompimento de uma das fibras de um dos caminhos seguidos até atingir o roteador). Nos casos dos clientes que transportam dados em tempo real, como emissoras de

televisão ou emissoras de rádio, estes precisam que a resiliência seja a menor possível, pois a perda de um quadro poderá comprometer seus negócios.

O protocolo EAPS foi desenvolvido pela fabricante Extreme Networks para garantir que uma rede com switches ligados em anel não gere loop infinito e ainda o tempo de resiliência seja muito pequeno. Apesar de ter sido criado pela Extreme Networks, muitos outros fabricantes já o disponibilizam em seus equipamentos (ex.: a brasileira Datacom). A figura 6.10 apresenta uma rede interligada em anel e configurada com o protocolo EAPS.

Quando optamos por utilizar o protocolo EAPS, um dos switches do anel será designado como *master*. Na figura 6.10, este foi o switch S1. As duas portas do switch *master* conectadas ao anel serão configuradas como portas primária (P) e secundária (S) respectivamente. Os demais switches serão classificados como switches de trânsito e também terão suas portas configuradas como primárias e secundárias. Na figura 6.10, os switches S2, S3, S4, S5 e S6 seriam chamados de trânsito. O fluxo de controle do protocolo EAPS é enviar seus dados pela porta primária, e a porta secundária do switch *master* ficará bloqueada logicamente. As demais portas secundárias dos switches de trânsito não ficarão bloqueadas e repassarão os quadros de dados normalmente.

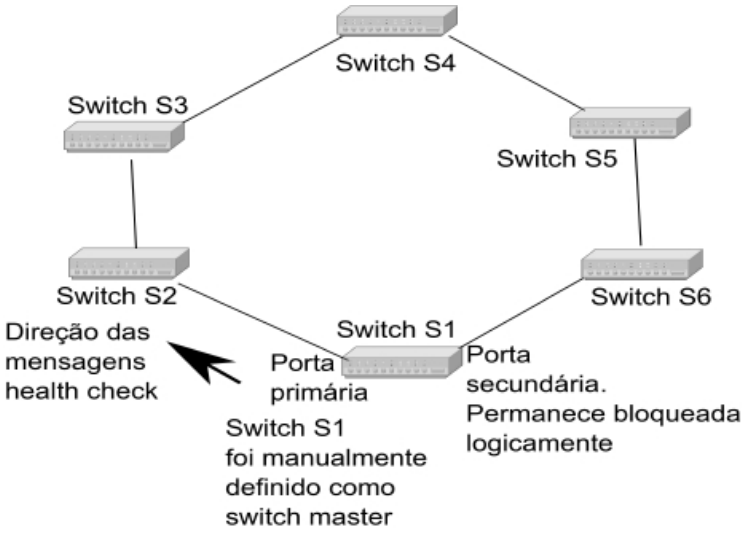



*Figura 6.10 – Rede na topologia em anel.*

A detecção de falhas com o protocolo EAPS tende a ser muito mais rápida se comparada ao protocolo RSTP. Abordaremos os tempos neste capítulo. A figura 6.11 apresenta um exemplo sobre a ocorrência de queda de um dos links de uma rede interligada em anel.

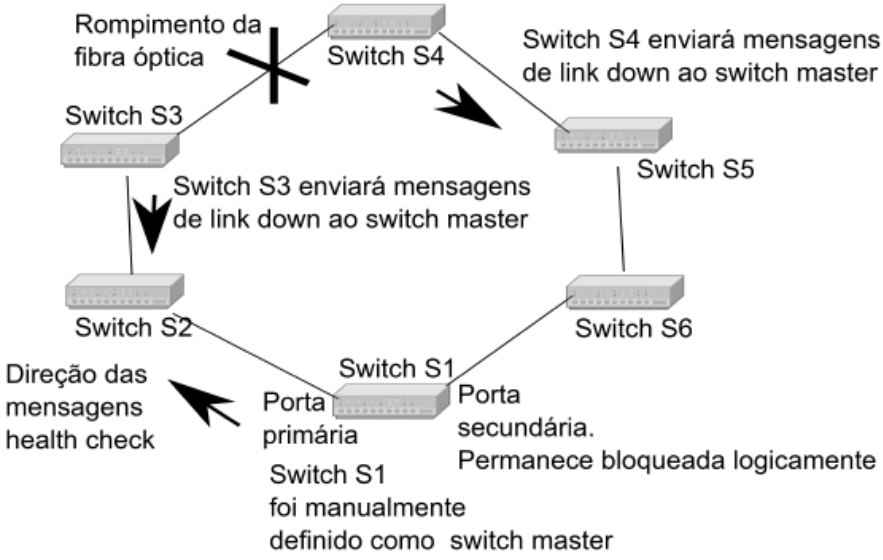



*Figura 6.11 – Demonstra uma falha em uma rede com EAPS.*

Conforme observado na figura 6.11, quando uma falha ocorrer no anel, o switch *master* poderá detectar a falha de duas maneiras.

### 6.3.4.1 Quadro link down

Primeiramente, o switch *master* poderá identificar a falha recebendo quadros de controle dos switches de trânsito que informarão a ele que houve um problema. Esses quadros de controle são chamados de *link down*. Ao receber um quadro do tipo *link down*, o switch *master* desbloqueará a sua porta secundária. Na figura 6.11, houve uma falha entre os switches S3 e S4. Nesse exemplo, ambos os switches de trânsito terão uma de suas portas colocadas em down. Com isso, perceberão que a porta primária do switch *master* deixará de visualizar sua respectiva porta secundária. A partir desse momento, os switches de trânsito enviaram quadros chamados *link down* para avisar ao switch *master* que este precisa liberar sua porta secundária. É importante observar que os quadros de controle são transmitidos através de uma VLAN, configurada para ser a VLAN de

controle. Neste capítulo, comentaremos como definir uma VLAN de controle.

Após o switch *master* tomar conhecimento de que houve um rompimento de fibra óptica na rede, este efetuará um reset em sua tabela de *bridging* [também conhecida por FDB (*Forward Data Base*) ou *Mac Address Table*)]. Em seguida, informará a todos os switches de trânsito para que também resetem suas tabelas de *bridging*. Toda essa comunicação ocorrerá por meio da VLAN de controle. É importante observar que os demais switches da rede não precisam tomar conhecimento da falha da rede, mas sim apenas zerar suas tabelas de *bridging* a fim de evitar que um determinado quadro seja enviado por uma porta que neste momento segue por um caminho com problemas. O fato de zerar a tabela de *bridging* não interromperá a comunicação entre os switches, apenas fará com que eles aprendam que os destinos agora seguem por uma outra porta.

#### 6.3.4.2 Quadro health-check

A segunda forma utilizada pelo switch *master* para identificar falhas é por meio do envio de quadros chamados *health-check* (processo de *polling*), que também são transmitidos através da VLAN de controle. O *polling* é o método utilizado pelo protocolo EAPS para garantir que caso exista uma falha na rede e os alarmes gerados pelos switches de trânsito (quadros *link down*) não consigam alcançar o switch *master*, este mesmo assim tomará conhecimento da falha e liberará sua porta bloqueada. Cada quadro *health-check* será enviado pela porta primária e caso o anel não apresente interrupções, esse quadro será recebido na porta secundária, fazendo que o switch *master* confirme que o anel não apresenta problemas. O intervalo de tempo entre o envio de cada um dos quadros *health-check* dependerá do valor atribuído ao parâmetro *hellotime*, que poderá ser configurado em segundos ou milissegundos. Normalmente, configuramos esse parâmetro com 50 milissegundos. Apenas como comparação, um piscar de olhos involuntário dura em torno de 200 milissegundos.

Podemos ainda configurar o parâmetro *failtime* que representa o tempo que o switch *master* aguardará pelo recebimento do quadro

*health-check*. Se não receber nesse tempo, o switch *master* liberará sua porta secundária, imaginando que houve alguma interrupção na rede metro. Ao receber o quadro *health-check* no tempo configurado, o switch *master* reinicializará seu contador e enviará um novo quadro *health-check*. O tempo configurado no parâmetro *failtime* poderá ser em torno de 150 milissegundos, ou seja, um tempo factível para que o pacote saia do switch *master*, viaje pelo anel e retorne ao switch *master*. Mesmo que exista o descarte de dois quadros, ainda assim o tempo não será alcançado. Utilizar um valor muito pequeno poderá confundir o switch *master* em relação a considerar que houve algum problema nos casos em que o quadro *health-check* não tenha sido recebido no tempo esperado.

É importante observar que o switch *master* continuará a enviar o quadro *health-check* pela porta primária mesmo quando houver um problema no anel e ainda durante todo o tempo que estiver interrompido. Entretanto, quando o anel for restabelecido, o quadro será recebido na porta secundária e o protocolo EAPS precisará retomar a operação normal. Neste momento, devemos nos ater às seguintes situações: o switch *master* manterá a porta secundária desbloqueada até receber o quadro health-check. Dado que o problema tenha sido corrigido, por algum tempo teremos um possível loop na rede, pois o switch *master* poderá não ter recebido o quadro *health-check* e os demais switches poderão trafegar dados dos clientes. Para aplicações de missão crítica (exs.: HD TV, rádio e VoIP), esse loop poderá prejudicar a qualidade dos dados transmitidos. A legislação aplicada às emissoras de televisão, por exemplo, é muito rígida e uma falha da rede poderá gerar multas pelo não atendimento do SLA (*Service Level Agreement*). Como evitar esse rápido e problemático loop na rede?

Como ocorre durante a convergência dos protocolos STP e RSTP, por algum período as portas dos switches que compõem o anel permanecem bloqueadas para o tráfego de dados dos clientes (as BPDUs sempre possuem trânsito livre). Com o protocoo EAPS ocorre algo parecido, porém o tempo em que as portas ficam bloqueadas é muito pequeno, ou seja, fica na casa dos

milisegundos, enquanto nos demais protocolos estas permanecem bloqueadas por vários segundos.

No protocolo EAPS, quando os switches de trânsito que geraram os quadros de *link down* percebem que a rede voltou ao normal (suas portas voltam para o estado de UP), estes colocam suas portas no estado de bloqueio temporário chamado de pre-*forwarding*. Durante esse estado, as portas dos switches de trânsito não trafegam quadros dos clientes, somente os quadros transmitidos na VLAN de controle, que, neste caso, seguem os quadros de *health-check*. Com essa atitude dos switches de trânsito, será evitada qualquer possibilidade de loop na rede. Quando o switch *master* receber o quadro *health-check* na porta secundária, este a bloqueará automaticamente. O próximo passo será reinicializar sua tabela de *bridging*. Em seguida, será enviada uma mensagem aos switches de trânsito que também deverão zerar suas tabelas de *bridging*. Assim, após os switches de trânsito reinicializarem suas tabelas de *bridging*, estes mudarão o estado de suas portas de *pre-forwarding* para o estado normal de transmissão.

### 6.3.4.3 Como configurar o protocolo EAPS

Durante a configuração do protocolo EAPS, a primeira opção a ser informada é o número do domínio (ex.: entre 0 e 63) a ser utilizado. Em cada domínio criado, poderão existir somente 1 switch *master* e uma VLAN de controle. Além disso, deveremos também definir um valor para os campos *hellotime* e *failtime*. Ao final, deveremos selecionar quais VLANs utilizadas pelos clientes serão protegidas pelo domínio criado.

Conforme comentado, os quadros de *link down* e *health-check* circulam através da VLAN de controle. Essa VLAN poderá ser qualquer uma entre as 4096 disponíveis na rede, porém deverá respeitar as seguintes regras:

- Não deverá ser associada a nenhum endereço IP, a fim de evitar loop na rede.
- Somente as portas dos switches que compõem o anel deverão ter esta VLAN associada.

- As portas dos switches que compõem o anel deverão ter esta VLAN como *tagged*. Veremos neste capítulo com mais detalhes as VLANs *tagged*.
- A VLAN de controle não poderá ser associada a mais de um domínio.

Para criar um domínio EAPS e torná-lo operacional em um switch, devemos adotar os seguintes passos (comandos disponíveis nos switches da fabricante Datacom):

**1.** Entrar no modo de configuração do switch. Normalmente, utiliza-se o comando:

configure <enter>

**2.** Criar um grupo de vlans ou vlan-group.

Ex.: vlan-group 0 <enter>

**3.** Relacionar as VLANs que serão protegidas pelo grupo criado.

Ex.: vlan-group 0 range 2 3500 <enter>

**4.** Criar o domínio EAPS.

Ex.: eaps 0

**5.** Escolher um dos switches do anel para ser o *master.*

Ex.: eaps 0 mode master

Nesse comando, poderíamos substituir a opção *master* por *transit.*

**6.** Nomear o domínio EAPS.

Ex.: eaps 0 name ExemploEAPS

**7.** Definir as portas primárias e secundárias. Normalmente, opta-se pelas portas com capacidade de transmissão a 1 Gbps ou 10 Gbps.

Ex.: eaps 0 port primary ethernet 25

Ex.: eaps 0 port secondary ethernet 26

**8.** Definir a VLAN de controle.

Ex.: eaps 0 control-vlan id 4094

**9.** Relacionar o grupo de VLANs com o domínio EAPS.

Ex.: eaps 0 protected-vlans vlan-group 0

**10.** Por padrão, o valor do *hellotime* é 1 segundo e do *failtimer* é 3 segundos. Para ajustar, devemos:

Ex.: eaps 0 hellotime 0 milliseconds 50

Ex.: eaps 0 failtime 0 milliseconds 150

### 6.3.4.4 VLANs em múltiplos domínios EAPS

O protocolo EAPS evita que switches ligados em anel gerem loop. Podem ocorrer situações em que a disposição física dos switches impeça de termos apenas um anel e, neste caso, para garantir que não existirá loop, deveremos configurar dois anéis. O protocolo EAPS permite que uma mesma VLAN presente nos dois anéis fique protegida de possíveis loops. A figura 6.12 apresenta um exemplo de uma rede interligada por dois anéis.

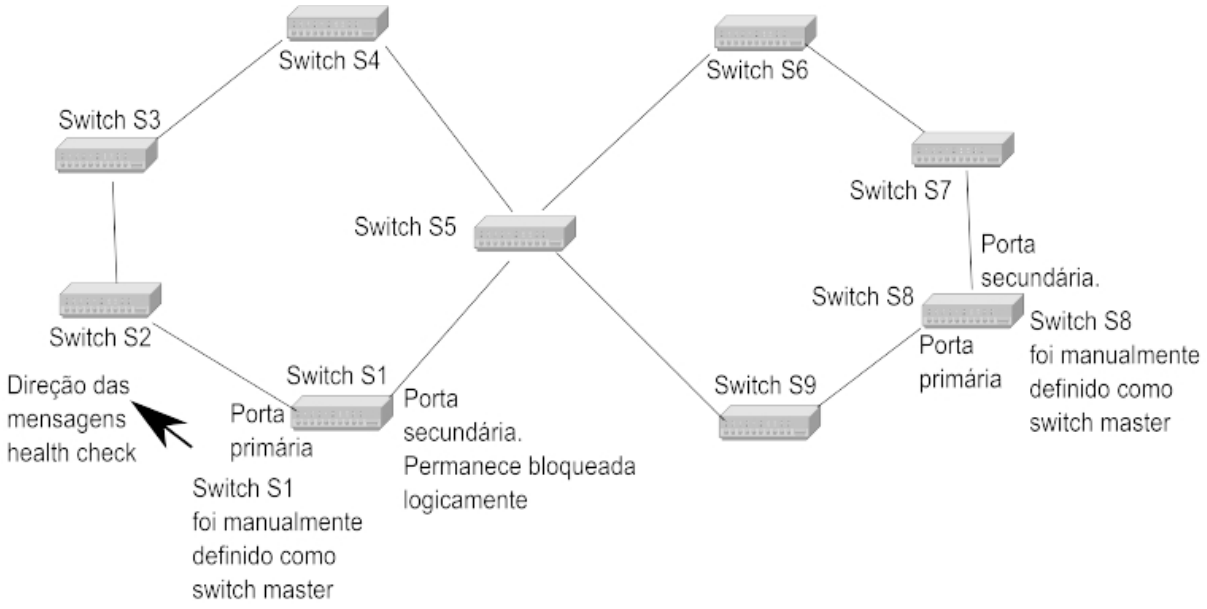



*Figura 6.12 – Duas redes configuradas com EAPS na topologia em anel.*

Conforme podemos observar na figura 6.12, cada anel possui:

- Um switch master.
- Um valor diferente para o domínio.
- Uma VLAN de controle.
- No momento de escolher as VLANs protegidas de cada domínio, será possível incluir as mesmas VLANs em ambos os domínios.

### 6.3.4.5 VLANs compartilhadas em múltiplo domínios

Conforme comentado, se o switch *master* deixa de receber o quadro *health-check* antes de vencer o tempo de *failtimer*, este passa para o estado de falha, pois identifica um problema de comunicação. Em seguida, desbloqueia (abre) a porta secundária, liberando o tráfego de todas as VLANs protegidas por essa porta. O próximo passo é enviar uma mensagem aos demais switches de trânsito para que limpem (*flush*) suas tabelas de *bridging*. Apesar das ações comentadas, é importante observar que a porta primária continuará a transportar dados das VLANs dos clientes. Por esse motivo, devemos ter atenção quando configuramos uma rede seguindo a arquitetura demonstrada na figura 6.13.

A figura demonstra uma situação em que teremos a necessidade de manter configurados os protocolos EAPS e RSTP a fim de evitar loop. Caso estejamos utilizando apenas o EAPS e o link comum entre os switches S5 e S10 romper, os switches *master* de ambos os domínios abrirão suas portas secundárias, porém manterão suas portas primárias tentando recuperar o link. Como a porta primária continuará a transportar os dados de todas as VLANs, as VLANs de clientes que estiverem presentes em ambos os domínios terão o seu conteúdo transportado normalmente. Mesmo com o rompimento do link citado, o anel continuará a existir e, com isso, os *broadcasts* gerados por cada uma das VLANs prejudicarão a qualidade da comunicação, pois ainda existe um anel e para o EAPS o anel foi interrompido.

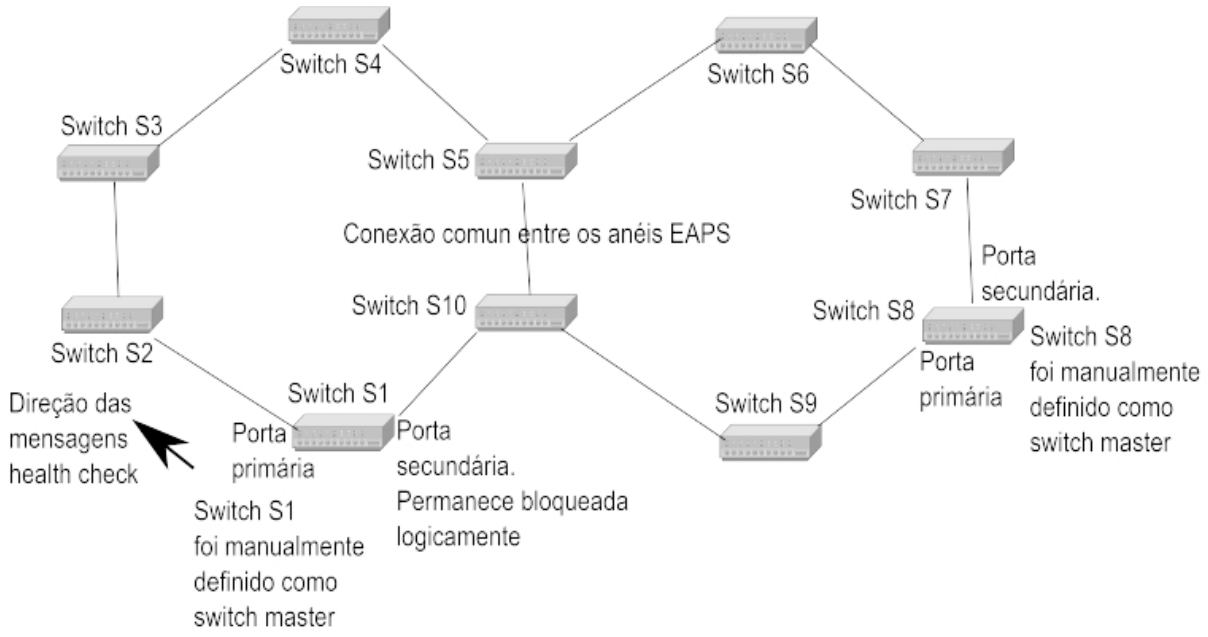



*Figura 6.13 – Link comum entre duas redes configuradas com EAPS na topologia em anel.*

### 6.3.4.6 Características do protocolo EAPS

A seguir, apresentamos as principais características do protocolo EAPS:

- O EAPS é um protocolo com alta resiliência para problemas de queda de fibra óptica em conexões entre switches.
- Foi criado para atuar em redes formadas por switches inteligados em anel.
- Pode coexistir com os protocolos STP e RSTP.
- Um anel poderá ser formado por apenas dois switches e, ainda assim, utilizar EAPS.
- Diferentemente do protocolo STP, o EAPS não apresenta nenhuma recomendação quanto ao limite de switches que compõem o anel.
- Múltiplos domínios EAPS podem coexistir em um mesmo anel.
- Um switch pode participar de múltiplos domínios.
- Em cada domínio, podemos ter apenas um switch atuando como *master*.

- Um domínio EAPS pode ser definido em apenas um anel, mas jamais poderá haver interconexão entre os anéis, ou seja, estes não podem se cruzar.
- Poderemos definir até 64 domínios em um switch.
- Devemos dar prioridade em definir como switch *master* o que estiver menos sobrecarregado.
- Poderemos utilizar como VLAN de controle quaisquer uma das 4096 VLANs disponíveis.
- A VLAN de controle não deverá ser utilizada para o transporte de dados nem poderá receber endereço IP.

### 6.3.5 VLAN (Virtual LAN)

A quantidade de switches presentes em uma rede pode torná-la bastante extensa, o que, para muitos, significa um benefício, na prática pode não ser. A quantidade de *broadcasts* gerados em redes é grande, e quanto maior for a rede, mais longe os *broadcasts* viajarão: temos, então, um grande problema. Conforme já comentado, os switches encaminham todos os quadros de *broadcasts* que recebem para todas as suas outras portas, menos à porta da qual recebeu o *broadcast*. Em uma grande rede, pode não ser necessário que todos os computadores divulguem todos os quadros para todos os segmentos da rede. Para evitar essa divulgação generalizada, podemos criar agrupamentos de máquinas que precisem ver a divulgação uma das outras, pois assim cada grupo receberá somente *broadcasts* do seu grupo.

Para resolver o problema comentado anteriormente, foi desenvolvida uma solução conhecida como virtual LANs (VLANs). As VLANs dividem uma rede LAN em grupos lógicos, permitindo que mesmo computadores ligados fisicamente a switches separados possam formar uma rede virtual. O resultado desse processo será LANs individuais separadas dentro de uma grande LAN. Para diferenciar uma VLAN da outra, é atribuído um ID diferente a cada uma delas. Qualquer computador dentro de uma VLAN pode se comunicar com qualquer outro computador em uma mesma VLAN,

porém não fora da sua. Dessa forma, mesmo que um computador esteja fisicamente ligado a um segmento afastado, somente se comunicará com os computadores que possuam o mesmo identificador, ainda que várias switches estejam entre eles. A figura 6.14 mostra um exemplo de uma LAN com switches configuradas com VLANs.

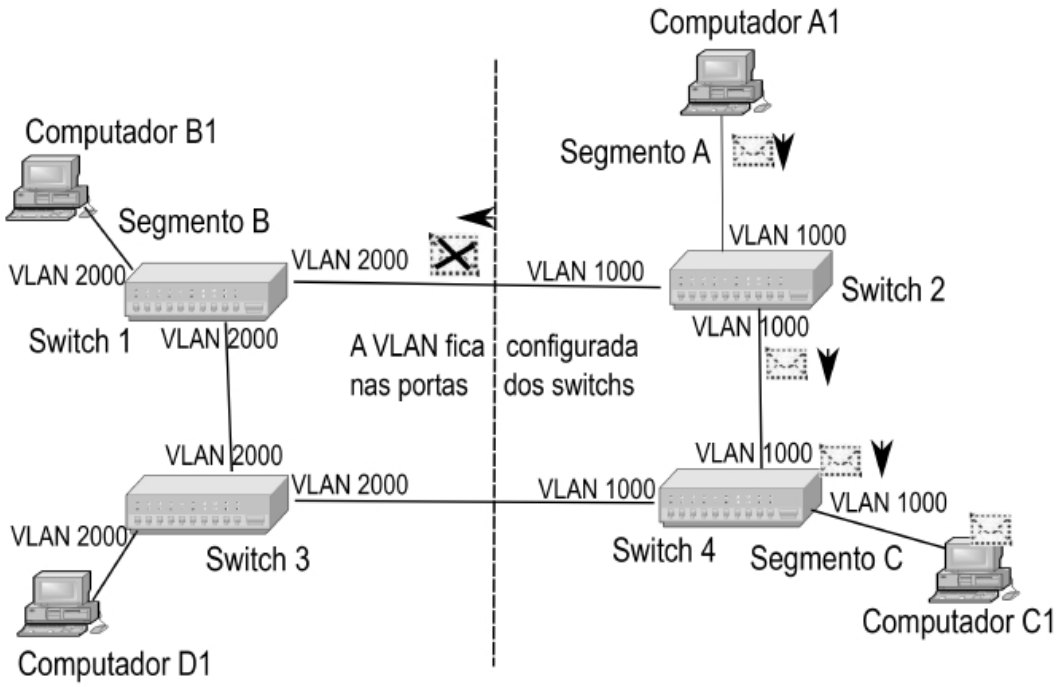



*Figura 6.14 – Rede separada por VLANs.*

Partindo do princípio de que os switches estão no processo de aprendizagem, ou seja, acabaram de ser ligados, quando o computador A1 (localizado no segmento A) enviar um quadro para o computador C1 (localizado no segmento C), o switch 2 examinará o endereço MAC de destino em sua tabela hash (tabela de *bridging*) e, ainda, analisará o número da VLAN da qual veio o quadro. Nesse caso, como o ID da VLAN recebido é igual ao número da VLAN do switch 2, o quadro será encaminhado ao segmento C para ser processado pelo computador C1. Ao mesmo tempo, o switch 1 também receberá o quadro e comparará o ID da VLAN recebido com o ID dos switches. Nesse caso, como o ID é diferente, o quadro não será encaminhado ao computador B1. Todos os quadros originados no segmento B não serão processados por

computadores dos segmentos A e C em razão de esse segmento pertencer à VLAN 2000, enquanto os segmentos A e C pertencem à VLAN 1000.

Uma grande vantagem do processo de configuração das VLANs é o modo como é realizado. As LANs virtuais são subLANs lógicas dentro da LAN, assim cabos ou conexões não precisam ser fisicamente modificados. Se existir alguma mudança na organização física da rede, o administrador poderá refazer a configuração por meio do software fornecido com o switch.

#### 6.3.5.1 Padrão IEEE 802.1Q

O IEEE por meio do padrão IEEE 802.1Q criou o conceito de VLANs. Esse padrão doi desenvolvido para resolver problemas como isolar os dados de clientes ou departamentos, oferecer segurança (permite que os dados de uma VLAN não sejam acessados por outra), isolar domínios de *broadcast* e, ainda, permitir a reutilização de portas dos equipamentos ativos (switch e roteadores).

A reutilização de portas permite, por exemplo, que uma mesma porta de um switch ou roteador atenda um cliente com dois ou mais serviços simultâneos, como acesso à Internet por uma VLAN e a outras filiais da empresa por meio de uma VPN MPLS. Ambos os quadros seguirão por VLANs diferentes e o tráfego de ambas não serão misturados.

O padrão Ethernet (IEEE 802.3) foi ajustado em 1998 para permitir a inclusão de uma *tag* de VLAN no quadro. A figura 6.15 apresenta o formato do quadro Ethernet ajustado para utilizar VLANs.

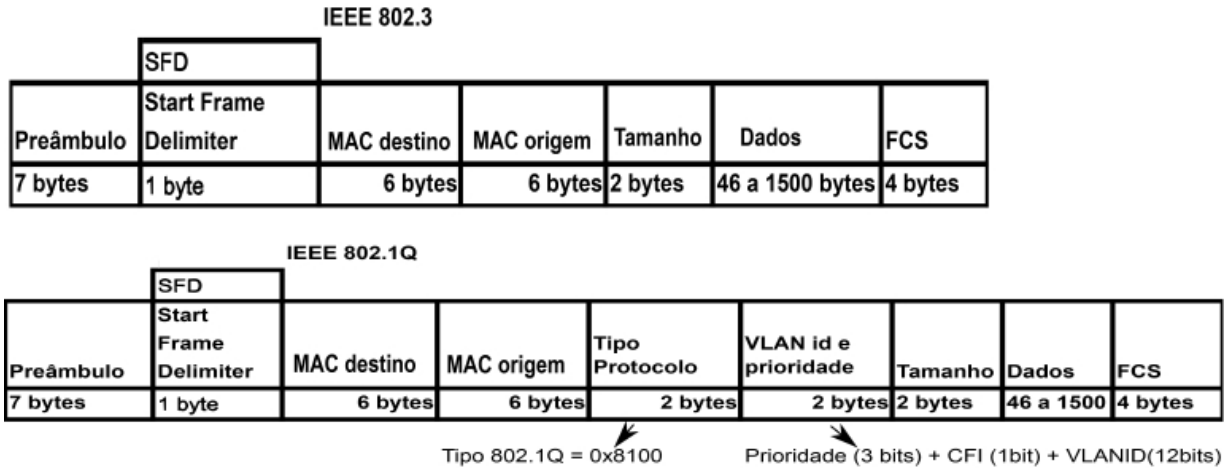



*Figura 6.15 – Formato do quadro Ethernet com a presença de tag de VLAN.*

Conforme observado na figura 6.15, foram adicionados os campos tipo do protocolo (conhecido também por *ethertype*) com 2 bytes e, ainda, os campos prioridade, CF e VLAN ID, ocupando, juntos, outros 2 bytes. O campo prioridade ocupa 3 bits, 1 bit para o campo CF e 12 bits para a *tag* da VLAN.

Caso um switch ofereça suporte a VLANs, o campo tipo do protocolo será preenchido pelo valor hexadecimal 0 x 8100, que formaliza que o quadro deverá ser repassado a outras portas somente se a *tag* carregada pelo quadro coincidir com a *tag* configurada na porta do switch. O campo comentado também pode ser chamado de *Tag Protocol Identifier* (TPID).

Quando o quadro contiver o valor 0 x 8100, os switches passarão a tratá-lo de forma diferenciada, ou seja, passarão a validar se o quadro poderá ou não seguir seu caminho até o próximo switch ou roteador. Se as *tags* coincidirem, o quadro seguirá, caso contrário o switch descartará o quadro. Vejamos um exemplo do uso de VLAN em uma rede local.

O quadro gerado por um computador em uma rede local poderá ou não conter tag, ou seja, ser um quadro com ou sem VLAN. Dado que um determinado computador gere quadros sem VLAN, como alcançará seu destino se a porta do switch foi configurado com *tag* de VLAN? Por padrão, quando o quadro é recebido pelo switch, este colocará uma *tag* automaticamente e repassará o quadro ao próximo

switch ou roteador. Esse procedimento ocorrerá todas as vezes que a porta do switch estiver configurada como acesso (access) ou untagged. Abordaremos esses conceitos nesta seção deste livro.

Para que a *tag* seja adicionada automaticamente, o switch precisará ter definido na respectiva porta um valor entre 1 e 4095 que deverá ser utilizado nesse processo automático. Para a fabricante Datacom, utilizam-se os seguintes comandos:

- configure – Permite acessar o modo de configuração do switch.
- interface ethernet 5 – Este comando dá acesso à porta 5.
- switchport native vlan 2182 – Adiciona a *tag* 2182 à porta 5.

2182 é o identificador da VLAN reservado a um dos serviços contratados pelo cliente e configurado em todo o caminho entre o primeiro switch e os demais que compõem o caminho até alcançar o roteador. Essa tag, neste exemplo representada por 2182, será diferente para cada serviço (exs.: acesso à Internet, acesso a filiais via VPN sobre rede MPLS) contratado pelo cliente. Ser diferente para cada serviço garante que os dados de cada serviço e de cada cliente sigam por vias lógicas independentes. Além de oferecer segurança aos clientes, isso ainda permite que a operadora reuse portas para milhares de clientes.

O quadro ainda contém outros 2 bytes chamado de TCI (*Tag Control Information*). Esse campo foi dividido em três partes, conforme apresentado na figura 6.15, sendo a primeira responsável pela prioridade com 3 bits, a segunda chamada de CFI (*Canonical Format Indicator*) com um bit e, por último, o VLAN ID, com 12 bits.

A primeira parte composta de 3 bits define a prioridade do quadro Ethernet seguindo o padrão IEEE 802.1p. A combinação dos 3 bits gera oito possíveis valores:

- **000 = 0** – Best effort (melhor esforço).
- **001 = 1** – Background.
- **010 = 2** – Não utilizado.
- **011 = 3** – Excellent effort.
- **100= 4** – Carga controlada.

- **101 = 5** – Vídeo.
- **110 = 6** – Voz.
- **111= 7** – Controle de rede.

A ideia da concepção deste campo foi oferecer a capacidade de QoS (*Quality of Service*) no nível Ethernet.

A segunda parte chamada CFI terá o valor zero quando o padrão de rede pelo qual o quadro seguirá for Ethernet. Serve basicamente para diferenciar se um quadro pertence a uma rede Ethernet ou a outra arquitetura de rede, como Token Ring, por exemplo.

A terceira parte é responsável por armazenar o identificador da VLAN, o qual chamamos de tag. Como esse campo contém 12 bits, uma *tag* de VLAN deve variar entre 0 e 4095, somando 4096 (2 elevado a 12) diferentes identificadores. Dentre as possíveis, algumas são reservadas a operações internas do switch. A VLAN 0 é usada internamente pelo switches, assim não pode ser utilizada pelo administrador da rede. A VLAN 1 é a VLAN default, previamente configurada em todas as portas de um switch e utilizada normalmente para o tráfego das BPDUs dos protocolos STP e RSTP. Esta também deve ser evitada pelo administrador da rede Uma porta não pode ficar sem VLAN, e quando isso ocorre, ela é relacionada a VLAN 1. A VLAN 4095 (FFF) também é reservada.

Por padrão, todas as portas são membros untagged da VLAN 1. Todas as portas que não forem configuradas como membros de uma VLAN com *tag* diferente serão membros da VLAN 1, que, por sua vez, não pode ser removida do switch.

### 6.3.5.2 Utilizando VLANs

A comunicação entre duas filiais de uma empresa pode ocorrer das seguintes formas: pela Internet ou por meio de links dedicados estatísticos (sobre VPN MPLS), determinísticos (sobre o padrão SDH) ou sobre links de rádio. No caso de a comunicação ocorrer pela Internet ou por links dedicados estatísticos, a operadora de telecomunicações disponibilizará no endereço do cliente um switch com as seguintes capacidades:

- Converter o sinal de fibra óptica em sinais elétricos (utilizado pelo cabo par trançado e conector RJ-45).
- Gerenciar remotamente e analisar os últimos eventos na rede do cliente. Com isso, a operadora poderá avaliar problemas quando for solicitado.
- Operar sobre diferentes VLANs. Cada VLAN transportará dados de diferentes serviços, como acesso à Internet, TV, VoIP (voz sobre IP) ou link dedicado sobre VPN MPLS.

Desta forma, para cada serviço comercializado pela operadora, utiliza-se uma diferente VLAN, em que se garante que os dados dos diferentes serviços não sejam mesclados. Ao alcançar o switch localizado no POP (ponto de presença), este processará os quadros e os transportará até o próximo switch ou roteador configurado para o cliente, ou seja, cada cliente, para ter acesso a Internet ou outra filial, precisará passar pelo roteador. Essa topologia é um exemplo de como uma operadora atende seus clientes.

Roteadores como os switches localizam-se em pontos estratégicos dentro de uma cidade e possuem capacidade para atender a milhares de clientes, seja por uma única porta, seja por várias.

É importante observar que mesmo que milhares de clientes sejam processados por uma única porta, cada um dos clientes terá a garantia de que seus dados não serão acessados por outros clientes, pois cada porta física do roteador é configurada com subinterfaces lógicas, em que cada subinterface será identificada pelo mesmo número da VLAN configurada no switch. Desta forma, desde o switch demarcador (EDD), instalado no cliente, até sua porta do roteador, o mesmo identificador de *tag* será utilizado. A figura 6.16 apresenta um exemplo de uma rede com a presença do switch demarcador, três switches instalados em POPs (ponto de presença situado em uma região estratégica em uma cidade) diferentes e um roteador.

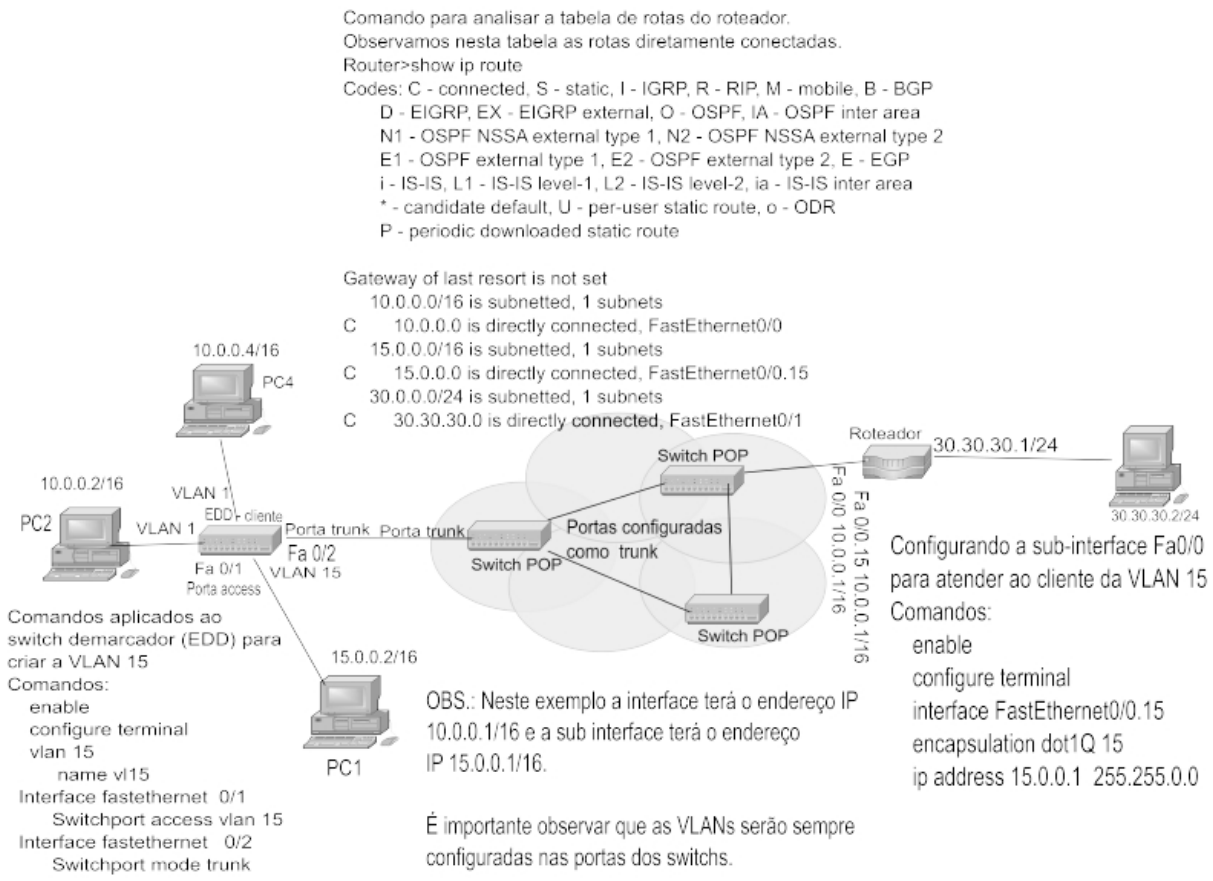



*Figura 6.16 – Rede configurada com VLANs.*

Conforme podemos observar na figura 6.16, além de apresentar uma rede com diversos equipamentos, os switches foram configurados para operar na VLAN 15 e as interfaces dos roteadores foram configuradas para receber os dados em uma subinterface, também nomeada pelo *tag* 15. Outro importante conceito apresentado nesta figura foi que entre as portas do switch, definimos que a VLAN 15 foi configurada como trunk (termo utilizado pela fabricante Cisco. Equivale ao termo tagged para outros fabricantes, como Datacom. Abordaremos esses conceitos neste capítulo).

É importante observar que dois equipamentos em VLANs diferentes podem se comunicar desde que o switch no qual estão conectados permita a configuração de um endereço IP nas VLANs. A tabela 6.2 apresenta uma sequência de comandos a fim de demonstrar na prática como configurar VLANs em switches e

também como as utilizar em roteadores.

*Tabela 6.2 – Utilizando uma VLAN na prática*

| **Comandos aplicados no switch demarcador, do fabricante Datacom, instalado no endereço do cliente** | |
|---|---|
| **Sequência de comandos** | **Descrição** |
| Configure | Acessa o modo de configuração do equipamento. |
| interface vlan 2182 | Entra no modo de configuração da VLAN 2182. Poderia ser qualquer outro número, por exemplo VLAN 15. Atenção, pois ID ou tag utilizado aqui deverá ser o mesmo configurado nos demais equipamentos. |
| name vl2182 | Toda VLAN precisa ser nomeada. Sugere utilizar o prefixo vl seguido do número da VLAN. |
| set-member untagged ethernet 5 | Relaciona a porta Ethernet 5 com a VLAN no modo untagged, sendo também conhecida por alguns fabricantes como porta access. Porta do switch demarcador configurada como sendo untagged normalmente será a utilizada para conectar os equipamentos do cliente. Essa porta fará a adição da tag automaticamente, em qualquer quadro que seja recebido de um dos equpamentos do cliente. Fará a remoção da tag quando o quadro for retornado ao equipamento do cliente. |
| set-member tagged ethernet 1/3 | Relaciona a porta Ethernet 3 com a VLAN no modo tagged, sendo também conhecida por alguns fabricantes como porta trunk. Neste exemplo, a porta configurada como tagged será a porta de up-link utilizada para a conexão do switch demarcador com o switch do POP (normalmente a porta que recebe a fibra óptica). O switch do POP fica instalado em uma localidade estratégica e recebe as conexões de todos os clientes da região na qual foram instalados. |
| interface ethernet 5 | Entra no modo de configuração da porta 5. |
| switchport native vlan 2182 | Define a tag de VLAN que a porta 5 adicionará automaticamente ao campo VLAN ID dos quadros após recebidos. Normalmente, um quadro gerado pelo clietne não possui uma tag, desta forma, para que este consiga alcançar o seu roteador, precisará de uma tag para |

| | |
|---|---|
| | percorrer sua viagem na rede da operadora. Esse comando formaliza que o quadro sem tag será ajustado para conter o ID informado neste comando, que, neste exemplo, foi 2182. |
| **Comandos aplicados ao switch do POP** | |
| **Sequência de comandos** | **Descrição** |
| Configure | Acessa o modo de configuração do equipamento. |
| interface vlan 2182 | Entra no modo de configuração da VLAN 2182. Atenção, pois o tag utilizado aqui deverá ser o mesmo configurado na porta de up-link do switch demarcador e na porta em que o cliente conectou seu equipamento. |
| set-member tag ethernet 1/9 | Relaciona a porta Ethernet 9 do switch com a VLAN no modo tagged. |
| interface ethernet 1/9 | Entra no modo de configuração da porta 9. |
| switchport native vlan 2182 | Define a VLAN que a porta 9 utilizará. Atenção, pois o ID utilizado aqui deverá ser o mesmo configurado nos demais equipamentos. |
| **Comandos aplicados ao roteador padrão Huawei** | |
| **Sequência de comandos** | **Descrição** |
| Interface GigabitEthernet 1/0/0.2182 | Acesso à interface física 1/0/0, subinterface 2182. |
| vlan-type dot1q 2182 | Formaliza que a subinterface 1/0/0.2182 responderá pela VLAN 2182. Este comando faz referência ao padrão IEEE 802.1Q. Atenção, pois a tag utilizada aqui deverá ser a mesma configurada nos demais equipamentos. |
| ip address 200.100.100.7 255.255.255.248 | Endereço IP e máscara da subinterface do roteador utilizados pelo cliente como default gateway. |

### 6.3.5.3 Relação entre VLAN untagged/access e tagged/trunk

Para diferenciar uma VLAN da outra, é atribuída uma etiqueta (*tag*) a

cada uma delas. Qualquer computador dentro de uma VLAN pode comunicar-se com qualquer outro computador em uma mesma VLAN, mas não fora da sua. É importante observar que na contratação de um link de uma operadora, a VLAN somente aparecerá como *tagged* na porta de *uplink* do switch demarcador (Figura 6.16), porém na porta em que o cliente conectará seus equipamentos esta ficará normalmente no modo untagged.

As portas de um switch podem trabalhar em dois modos conhecidos por:

- Modo access ou untagged, usados para conectar a rede do cliente ao switch demarcador. Uma porta configurada como untagged ou access (dependerá do fabricante; Cisco utiliza o termo access, enquanto Datacom utiliza o termo untagged) fará que todos os quadros recebidos do cliente sejam alterados, ou seja, o switch demarcador incluirá uma tag. No sentido inverso, ou seja, os quadros devolvidos pelo roteador, ao serem recebidos pela porta, terão a *tag* removida e repassada ao equipamento do cliente.
- Modo trunk ou tagged, usados para interconectar as portas dos switches que compõem o backbone da rede metropolitana. Conforme apresentado, para que o quadro de um cliente alcance o roteador designado, este passará por um ou mais switches. Uma porta configurada como *tagged* ou *trunk* (dependerá do fabricante; Cisco utiliza o termo *trunk*, enquanto Datacom utiliza o termo *tagged*) fará que todos os quadros recebidos de outro switch sejam avaliados, e caso tenha uma *tag* igual à configurada, permitirá sua passagem. Neste modo de configuração, o quadro não será alterado, mas apenas avaliado. Uma porta configurada como *trunk* ou *tagged* permitirá conter ou processar múltiplas VLANs, enquanto no modo access apenas uma VLAN será suportada.

A seguir, abordaremos a possibilidade de incluir mais uma VLAN no quadro Ethernet, ou seja, o quadro passará a ser transmitidos com duas *tags*. Essa novidade foi chamada de QinQ, alusão ao padrão 802.1q sobre 802.1q. Esse padrão foi registrado pelo IEEE

como 802.1ad e normalmente é utilizado em conexões comercializadas entre duas operadoras, como entre COPEL Telecom e TIM.

### 6.3.6 QinQ

O padrão IEEE 802.1ad nomeado QinQ (802.1q sobre 802.1q), conhecido também como VLAN empilhada (stacked VLAN) ou VLAN sobre VLAN, suporta a utilização de duas *tags* 802.1q no mesmo quadro Ethernet, ou seja, podemos dizer que é uma expansão do padrão 802.1q. Com o QinQ, será adicionada mais uma *tag* ao quadro Ethernet. A figura 6.17 apresenta o quadro Ethernet com o padrão QinQ.

A utilização do QinQ permite que provedores e operadoras trafeguem dados de clientes de forma transparente, sem interferir na marcação de VLAN de seus quadros.

Para o cliente é como se a operadora estendesse um cabo entre os seus switches, não importando se o caminho seguido por ela contém ou não VLANs. Já para a operadora não importa se o cliente está mandando um quadro com *tag* ou sem *tag*, pois adicionará mais uma *tag* ao cabeçalho Ethernet e a removerá na outra ponta. É importante observar que na extremedidade do destino somente a VLAN externa (VLAN da operadora) será removida. A figura 6.18 apresenta uma rede em que o cliente comunica-se entre dois pontos controlados por um backbone fornecido por uma operadora.

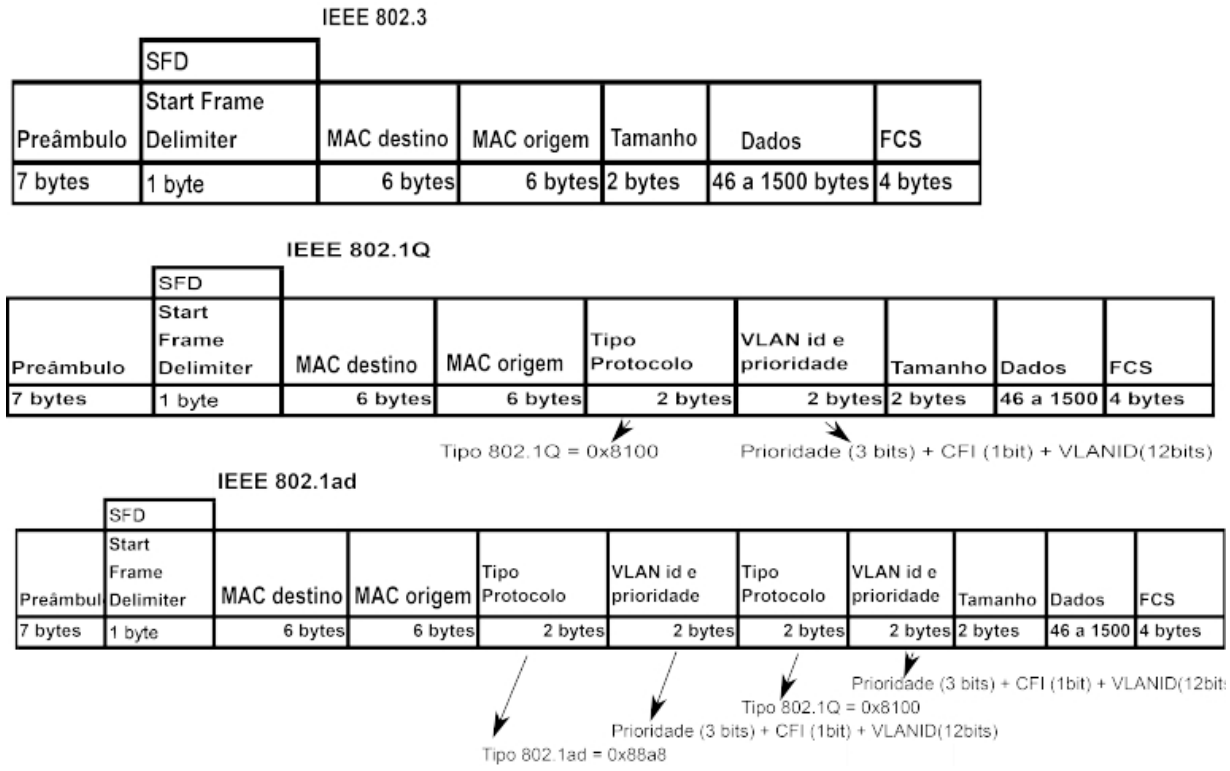



*Figura 6.17 – Formato do quadro Ethernet contendo os campos para QinQ.*

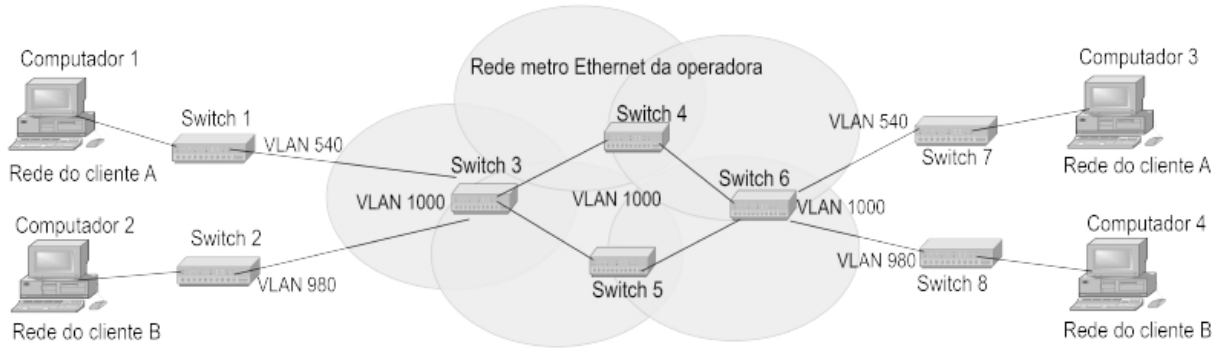



*Figura 6.18 – Exemplo de uma rede que opera com o uso de QinQ.*

A grande vantagem do QinQ é permitir que o cliente e a operadora não precisem conhecer a VLAN uma da outra. Vejamos alguns cenários em que a comunicação ocorre com e sem QinQ.

- Digamos que um cliente precise transportar seus dados entre duas extremidades sem utilizar VLAN, ou seja, do ponto de vista dele, as VLANs não são importantes ou as desconhece. Este seria o caso de o cliente contratar um link de alta velocidade de

uma operadora para interligar sua matriz com uma ou mais filiais. Neste cenário, a operadora entregará um equipamento na residência do cliente (ex.: switch demarcador), que receberá o cabo de fibra óptica e oferecerá algumas portas no padrão RJ-45. O cliente configurará seus equipamentos sem se preocupar com VLANs, entretanto a operadora, por questões de qualidade e segurança, formalizará que cada serviço será transportado por uma VLAN. Assim, apesar de o cliente não conhecer ou utilizar VLANs, a operadora o fará. Neste cenário, a operadora configurará a porta de *uplink*, a qual se conecta a fibra óptica como trunk ou tagged e a porta RJ-45 ficará como access ou untagged.

Quando os quadros enviados pelos equipamentos do cliente chegarem à porta RJ-45, o switch demarcador alterará o quadro Ethernet, inserindo uma *tag* previamente definida pela operadora e o enviará até seu destino. Ao receber a resposta, o mesmo switch removerá a *tag* e a entregará ao equipamento do cliente que a processará normalmente.

- Digamos que um cliente precise transportar seus dados entre duas extremidades com VLANs, ou seja, do ponto de vista do cliente, as VLANs são importantes. Este seria o caso de o cliente contratar um link de alta velocidade de uma operadora para interligar sua matriz com uma ou mais filiais. Neste cenário, a operadora entregará um equipamento na residência do cliente (ex.: switch demarcador), que receberá o cabo de fibra óptica e oferecerá algumas portas no padrão RJ-45. O cliente configurará seus equipamentos, porém combinará com a operadora as VLANs que serão utilizadas. Por sua vez, a operadora reservará as VLANs para atender esse específico cliente.

  Com isso, cada serviço será transportado por uma VLAN e o cliente estará ciente desse modelo de transporte. Neste cenário, a operadora configurará a porta de *uplink*, a qual se conecta a fibra óptica como trunk ou tragged, com a *tag* combinada, e a porta RJ-45 também receberá uma tag, ou seja, neste cenário, esta porta também será trunk ou tagged. Quando os quadros do cliente chegarem à porta RJ-45, o switch demarcador simplesmente os

repassará à frente sem efetuar nenhuma alteração no quadro. Ao receber a resposta, o mesmo switch repassará o quadro sem se preocupar com a tag. A responsabilidade por remover a *tag* será dos equipamentos do cliente.

Neste cenário, o único incômodo será que a operadora precisará gerir um conjunto de VLANs que serão utilizadas por clientes que venham precisar delas. Caso ocorra desencontro desses valores, a comunicação não ocorrerá, ou seja, apesar de possível, este cenário aumenta a responsabilidade de ambos os lados em relação às VLANs reservadas.

- Digamos que um cliente precise transportar seus dados entre duas extremidades, porém não possui condições de combinar as *tags* de VLAN em razão de a operadora já ter utilizado as *tags* que planejava utilizar ou, ainda, simplesmente se negar a reservar VLANs para esse fim. Devido ao grande volume de ativações de circuitos pela operadora, isso poderá comprometer esse acordo, pois, caso este não seja cumprido, o projeto do uso de VLANs ficará comprometido. Assim, para que não exista dependência entre as empresas, podemos utilizar QinQ, ou seja, o cliente poderá transportar seus dados com *tags* de VLAN e a operadora poderá transportá-los sobre as VLANs que considerar mais apropriadas.

  É importante observar que a segunda *tag,* quando adicionada ao quadro, será colocada logo após o campo MAC origem (*Source Address*), ou seja, antes da primeira *tag* adicionada. Podemos, ainda, considerar que a *tag* adicionada inicialmente é chamada de C-TAG (*tag* do cliente – *Customer TAG*) com campo ethertype (também conhecido por TPID (*Tag Protocol Identifier*) com valor igual a 0 x 88a8 (obs.: definido em 2007 pelo padrão 802.1QinQ2007 com valor igual a 0 x 9100, porém atualmente se utiliza 0 x 88a8). A segunda *tag* adicionada poderá também ser chamada de S-TAG (*tag* da operadora – *Service TAG*) com campo *ethertype* igual a 0 x 8100.

### 6.3.6.1 Modos Internal e External

A implementação do QinQ por alguns fabricantes (ex.: Datacom) disponibiliza dois diferentes modos para configuração de uma porta no switch. Assim, quando configuramos um switch para prover ou não o recurso de QinQ, precisamos formalizar quais das portas ficarão no modo interno (*internal*) e quais deverão permanecer no modo externo (*external*).

Alguns equipamentos assumem por padrão um ou outro modo em cada uma das suas portas, assim é importante verificar e garantir que o modo de cada porta seja adequado à realidade da instalação. É fundamental obsevar que mesmo que não seja utilizado QinQ, a porta precisará estar no modo externo. Dada a importância de conhecer esses modos, descreveremos em detalhes cada um deles.

O modo externo é o padrão normalmente aplicado às interfaces FastEthernet (interfaces que operam em 100 Mbps) dos switches, ou seja, normalmente as portas as quais os clientes conectam seus equipamentos (exs.: switch, roteador, computador). No modo externo, todos os quadros Ethernet recebidos pela interface receberão mais uma *tag* de VLAN. A VLAN que o quadro receberá será a VLAN configurada como native VLAN na interface. Outro ponto importante a ser observado com este modo é o tipo de VLAN configurada nesta porta, que deverá ser *untagged* ou *access* (dependerá do fabricante). No modo externo, todos os quadros recebidos pela porta receberão mais uma tag. Assim, caso o quadro chegue sem *tag,* receberá a primeira, e caso chegue com uma, receberá a segunda.

Como macete para utilizar e configurar o QinQ, podemos seguir a seguinte regra: habilitar o QinQ na caixa do switch [para o fabricante Datacom, entrar no modo de configuração (comando configure) e habilitar o QinQ na caixa (digitar vlan qinq)]. Precisamos ainda garantir que as portas dos switches fiquem como untagged e em modo external. Na tabela 6.3, veja os comandos envolvidos na explicação apresentada:

*Tabela 6.3 – Comando para habilitar o QinQ em um switch Datacom – Modo external*

| Comando aplicado ao switch | Descrição |
|---|---|
| vlan qinq | Habilita o QinQ na caixa do switch. |
| interface ethernet 1/3 | Entra no modo de configuração da porta Ethernet 3, porta de uplink. Essa porta recebe a fibra óptica da operadora. |
| description PortaUplink | Registra um nome para a interface. |
| interface ethernet 1/8 | Entra no modo de configuração da porta Ethernet 8, porta utilizada pelo cliente. Porta com interface RJ-45. |
| description PortaCliente | Registra um nome para a interface. |
| switchport native vlan 965 | Define a tag que será adicionada aos quadros recebidos na porta Ethernet 8. |
| switchport qinq external | Formaliza o modo externo (external) para a porta 8. |
| interface vlan 965 | Entra no modo de configuração da VLAN 965. |
| Name vl965 | Nomeia a VLAN. |
| set-member tagged ethernet 1/3, | Formaliza que a porta Ethernet 3 é tagged para a VLAN 965. |
| set-member untagged ethernet 1/8 | Formaliza que a porta Ethernet 8 é untagged para a VLAN 965. |

Observação: ambas as portas que interconectam esse cliente precisarão ficar untagged e em modo external.

O modo interno (*internal*) é o padrão para as portas de up-link que normalmente operam em 1 Gbps ou mais. No modo interno, os quadros com VLAN são repassados à frente desde que a *tag* de VLAN recebida seja a mesma da porta. Existe ainda uma segunda avaliação nesse modo de operação do QinQ. Avalia-se se no quadro existe um campo TPID com valor igual a 0 x 8100. Caso exista, avalia-se a *tag* de VLAN na porta de saída (deve exisitr uma configurada) e repassa-se o quadro à frente (caso exista uma VLAN

configurada na porta de saída). Caso não exista, será adicionado um novo campo contendo o TPID-padrão com valor 0 x 8100 e VLAN ID igual à definida como nativa na porta.

O TPID são os primeiros 2 bytes no *tag* de VLAN, que também correspondem ao campo ethertype. O valor para esse campo é 0 x 8100 no padrão 802.1q. A configuração do valor do TPID ocorre por porta, ou seja, não está relacionada à *tag* de VLAN. É possível, porém não usual, alterar o valor do TPID para uma específica porta. É importante observar que a VLAN definida em uma porta com o modo internal habilitado deverá ser configurada também como tagged ou trunk.

É importante observar que existem situações em que precisamos manter o modo interno também nas portas do cliente. Isso ocorre quando uma operadora comercializa um link para outra operadora. Nesse caso, a segunda operadora transportará seus quadros com *tag* de VLAN e, por isso, a primeira operadora não poderá escolher qualquer VLAN de sua range. Ambas as operadoras precisarão combinar a VLAN, pois a segunda enviará sua *tag* de VLAN e a primeira operadora deverá simplesmente repassar o quadro sem efetuar nenhum ajuste. Por isso, nesse caso a porta ficará com modo internal, que é responsável por avaliar a *tag* recebida com a *tag* configurada e, quando iguais, simplesmente repassa o quadro. Veja na tabela 6.4 os comandos envolvidos na explicação apresentada:

*Tabela 6.4 – Comando para habilitar o QinQ em um switch Datacom – Modo internal*

| **Comando aplicado ao switch** | **Descrição** |
|---|---|
| vlan qinq | Habilita o QinQ na caixa do switch. |
| interface ethernet 1/3 | Entra no modo de configuração da porta Ethernet 3, porta de uplink. |
| description PortaUplink | Registra um nome para a interface. |

| Comando aplicado ao switch | Descrição |
|---|---|
| interface vlan 965 | Acessa o modo de configuração da VLAN 965. |
| name vl965 | Registra um nome para a VLAN. |
| set-member tagged ethernet 1/3 | Formaliza que a porta Ethernet 3 é tagged para a VLAN 965. |
| set-member tagged ethernet 1/8 | Formaliza que a porta Ethernet 8 é tagged para a VLAN 965. |
| interface ethernet 1/8 | Entra no modo de configuração da porta Ethernet 8, que é utilizada pelo cliente. Porta com interface RJ-45. |
| description PortaCliente | Registra um nome para a interface. |
| switchport native vlan 965 | Define a tag que será adicionada aos quadros recebidos na porta 8. |
| switchport qinq internal | Formaliza o modo interno (internal) para a porta 8. |

Observação: para utilizar o modo internal, temos como pré-requisito que o micro ou outro equipamento utilizado para os testes de conectividade precisará ser equipado com suporte à VLAN.

## 6.4 Roteador

O roteador (*router*) é o equipamento responsável pela interligação entre redes LANs atuando nas camadas 1, 2 e 3 do modelo de referência TCP/IP. Os roteadores possuem como função a decisão sobre qual caminho o tráfego de informações deve seguir, ou seja, por qual caminho deve seguir um pacote de dados recebido da camada superior (transporte). Os roteadores inicialmente interpretam o endereço IP contido no pacote de dados e, em seguida, consultam sua tabela de roteamento. Se o endereço estiver cadastrado, o roteador fará o envio na porta específica; caso contrário, o roteador enviará o pacote de dados para a sua rota-

padrão (*default*). É importante lembrar que os pacotes de dados, depois de serem recebidos pelos roteadores, são desmontados e remontados novamente. Essa característica dos roteadores permite que consigam interligar duas redes com arquiteturas diferentes, como Ethernet e Token Ring.

A fim de posicionar o leitor sobre esse assunto e com o objetivo de abordar com mais detalhes os roteadores, faremos uma introdução ao protocolo IP – objeto principal dos roteadores.

O Protocolo IP (*Internet Protocol*) é responsável pela comunicação entre máquinas em uma estrutura de rede TCP/IP. Ele provê a capacidade de comunicação entre todos os equipamentos presentes na rede, ou seja, permite o transporte de um pacote de um equipamento origem até o seu destino. O protocolo IP fornece um serviço sem conexão e não confiável entre máquinas em uma estrutura de rede, por isso todos os controles (controle de fluxo, sequência e conexão) devem ser fornecidos pelos protocolos de níveis superiores, como o TCP. As funções mais importantes realizadas pelo protocolo IP são:

- A atribuição de uma forma de endereçamento independentemente do hardware de rede e da própria topologia da rede utilizada (estrela ou linear).
- A capacidade de rotear e tomar decisões de roteamento para o transporte dos pacotes entre os elementos que interligam as redes.

No modelo de referência TCP/IP, os equipamentos ativos responsáveis por interligar duas ou mais redes distintas (redes com máscaras diferentes) são chamados de roteadores. Uma máscara de rede é um tipo de endereço IP utilizado para definir a classe do endereço IP usado no equipamento de rede. O endereço da máscara de rede é composto de 4 bytes e inicia com 255, podendo ser seguido de outro valor, 255 ou 0 (ex.: 255.255.0.0).

As redes interligadas pelos roteadores podem ser locais (LANs), metropolitanas (MAN) ou globais (WANs). Um roteador sempre oferecerá mais de uma interface de rede (uma ou mais portas RJ-45

ou uma ou mais portas ópticas). É importante observar que, dependendo do modelo do roteador, cada uma de suas portas poderá ser configurada com um endereço IP, o qual deve ser fornecido de forma manual pelo administrador da rede. Atualmente, os roteadores permitem configurar endereços IPs para suas subinterfaces, possibilitando que uma mesma interface física atenda a milhares de clientes. As subinterfaces são configuradas utilizando-se o mesmo identificador físico (ex.: interface 1/1/0), porém com identificadores diferentes. Esse identificador será igual à VLAN (ex.: 1/1/0.2709) utilizada nos switches. A tabela 6.2 (na seção Comandos aplicados no roteador, padrão Huawei) apresenta um exemplo de como configurar uma subinterface de um roteador Huawei. A figura 6.16 apresenta os comandos para configurar a subinterface de um roteador Cisco.

Um roteador pode ser um equipamento específico ou um computador de uso geral com mais de uma placa de rede. Quando o objetivo é reduzir custo, a utilização de um computador como roteador torna-se mais interessante. É importante observar que atualmente diversos sistemas operacionais oferecem a possibilidade de atuarem como roteador. A figura 6.19 apresenta duas redes locais interligadas por um computador que funciona como roteador.

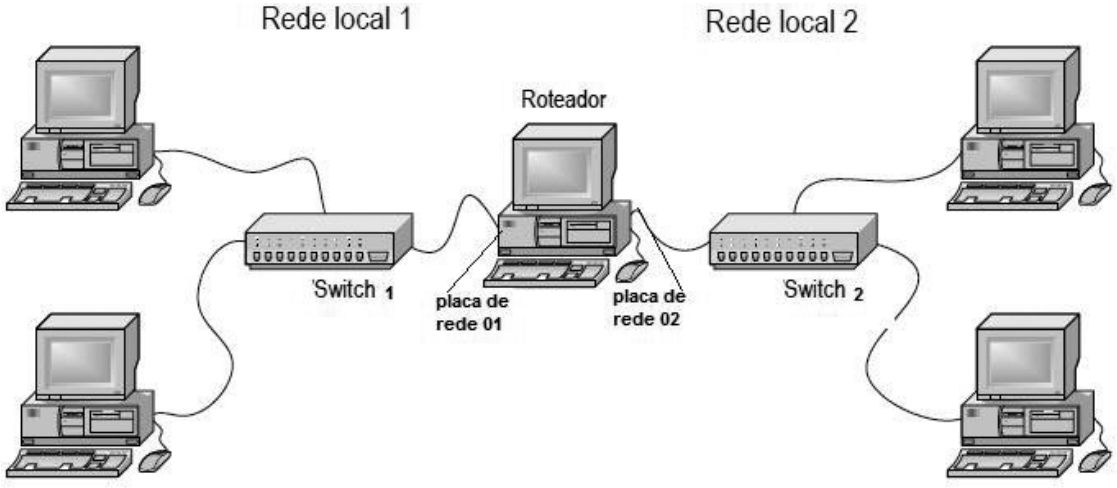



*Figura 6.19 – Roteador interligando dois computadores.*

## 6.4.1 Endereços IP

Um endereço IP é um identificador único para uma interface de rede de uma máquina. Esse endereço é formado por 32 bits (4 bytes). Todo endereço IP possui uma parte que identifica a rede a qual a interface de rede está conectada e outra identifica a máquina dentro dessa rede. O endereço IP é representado por 4 bytes separados por ponto (.). Cada byte é representado por um número decimal (entre 0 e 255), a fim de tornar a identificação do endereço IP mais simples. Como exemplo, temos o endereço IP 11010001.11110101.0011101.10100111 na forma binária, representado na forma decimal por 209.245.29.167.

Como o endereço IP identifica tanto uma rede quanto a estação a que se refere, fica claro que o endereço possui uma parte para a rede e outra para a estação. Dessa forma, uma porção do endereço IP designa a rede na qual a estação está conectada e outra porção identifica a estação dentro dessa rede. O roteador é o equipamento ativo responsável pela interligação dessas duas redes.

Uma vez que o endereço IP tem tamanho fixo, uma das opções dos projetistas no início da especificação do protocolo seria dividir o endereço IP em duas metades, sendo 2 bytes para identificar a rede e 2 bytes para identificar os computadores da rede. Entretanto, isso traria inflexibilidade, pois só poderiam ser endereçados 65.536 redes (2 elevado a 16 bits) e 65.536 computadores para cada rede. Uma rede que possuísse apenas 100 estações estaria utilizando um endereçamento de rede com capacidade de 65.536 computadores, o que também seria um desperdício.

A forma original de dividir o endereçamento IP em rede e estação foi feita por meio de classes, sendo os endereços IPs divididos em cinco classes. Um endereçamento de classe A consiste em endereços que têm uma porção de identificação de rede de 1 byte e uma porção de identificação de equipamentos de 3 bytes. Dessa forma, é possível endereçar até 128 (2 elevado a 7 bits) redes diferentes. Apesar de o primeiro byte possuir 8 bits, para endereços classe A, o bit mais significativo é fixado em 0 (32o bit do endereço IP), logo sobram apenas 7 bits para serem combinados.

Um endereçamento de rede classe B utiliza 2 bytes para rede e 2

bytes para endereçamento dos computadores, enquanto um endereço de classe C utiliza 3 bytes para representar a rede e 1 byte para o endereçamento dos computadores pertencentes às diferentes redes. Endereços classe B possuem os dois primeiros bits setados em 1 e 0 (32o bit e 31o bit do endereço IP), logo a quantidade máxima de redes possíveis para essa classe é de 16.284 (2 elevado a 14 bits).

Já os endereços classe C possuem os 3 primeiros bits setados em 1, 1 e 0 (32o bit, 31o bit e 30o bit do endereço IP), de modo que a quantidade máxima de redes possíveis para essa classe é de 2.097.152 (2 elevado a 21 bits). A tabela 6.5 apresenta um resumo sobre a quantidade possível de redes e computadores ligados a essas redes:

*Tabela 6.5 – Quantidade de redes e de computadores por classe*

| Classe | Descrição |
|---|---|
| Classe A | Possui endereços suficientes para endereçar 128 redes (2 ^ 7) diferentes com até 16.777.216 estações cada uma (2 ^ 24). |
| Classe B | Possui endereços suficientes para endereçar 16.284 redes (2 ^ 14) diferentes com até 65.536 estações (2 ^^16). |
| Classe C | Possui endereços suficientes para endereçar 2.097.152 (2 ^ 21) redes diferentes com até 256 estações (2 ^ 8) cada uma. |

Para diferenciar uma classe de endereço de outra, utilizaram-se os primeiros bits do primeiro byte, entretanto a máscara de rede é quem oficializa a relação entre qual parte do endereço IP representa a rede e qual parte do endereço IP representa o computador. A máscara de rede deve sempre acompanhar o endereço IP quando este for configurado em um equipamento de rede. Como exemplo de máscara de rede para a classe A, temos 255.0.0.0; para a classe B, temos 255.255.0.0; e para a classe C, temos 255.255.255.0.

Nessa forma de divisão, é possível ter um pequeno número de redes, embora muito grandes (classe A), e um grande número de redes, entretanto cada uma delas bem pequenas (classe C). Assim, nas redes classe A, a quantidade de redes é pequena, em

contrapartida, a quantidade de computadores possíveis para cada rede diferente é grande. No caso das redes classe C, acontece o inverso: a quantidade de redes é grande, mas a quantidade de computadores possíveis é pequena. Essa forma de divisão de endereços é histórica, e a Internet utiliza outro mecanismo conhecido por CIDR (*Classless Inter-Domain Routing*), abordado no capítulo 8. É importante observar que se a Internet utilizasse essa forma de distribuição de endereços IP, não estaríamos conseguindo mais acesso, pois, como mencionado, essa forma de distribuição de endereços é predatória.

Para finalizar, temos as classes D e E. A classe D (utilizada atualmente) é uma classe especial para identificar endereços de grupo (*multicast*) e a classe E é reservada. A figura 6.20 apresenta a distribuição dos endereços IP por classes:

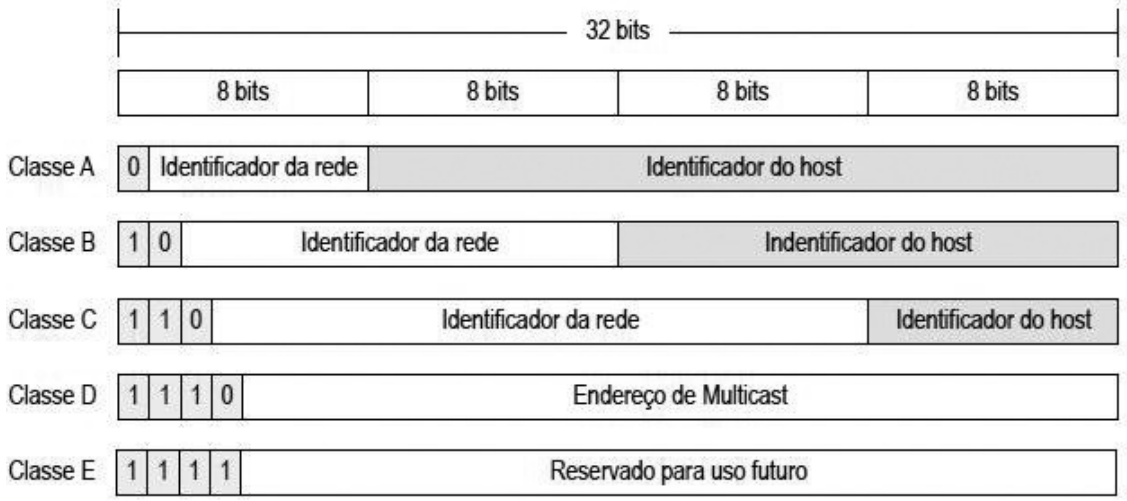



*Figura 6.20 – Divisão das classes de endereçamento IP.*

A seguir, comentaremos alguns endereços IP que não podem ser utilizados na configuração de roteadores ou de computadores. Esses endereços são reservados a funções especiais:

- **Endereço de rede** – Identifica a própria rede e não uma interface de rede específica. A parte do endereço IP que se refere à rede é representada por todos os bits de hosts com o valor zero (10.0.0.0), ou seja, mantém a parte do endereço IP referente à rede com valor e a parte referente ao endereçamento dos

equipamentos fica com zeros. Os roteadores interligam segmentos de rede quando alguma requisição é gerada com endereço de rede diferente do da rede local.

- **Endereço de broadcast** – Identifica todas as máquinas na rede específica, sendo representado por todos os bits de hosts com o valor 1 (o valor 1 representa que o bit esta ligado - 10.255.255.255. 255 O decimal 255 define que os 8 bits do byte estão ligados), ou seja, mantém a parte do endereço IP referente à rede com valor e a parte referente ao endereçamento dos equipamentos fica com 1s.
- **Endereço de broadcast limitado** – Identifica um *broadcast* na própria rede, sem especificar a que rede pertence. Representado por todos os bits do endereço iguais a 1 (255.255.255.255).
- **Endereço de loopback** – Identifica a própria máquina, sendo representado por 127.0.0.1. Serve para enviar uma mensagem para a própria máquina, ou seja, roteia a mensagem para si mesma. Após ser emitida por uma aplicação (p. ex., comando *ping*), essa mensagem fica na camada 3 (camada em que o protocolo IP reside), sem ser enviada à rede.

As figuras 6.20 e 6.21 mostram exemplos de endereçamento de máquinas situadas na mesma rede e em redes diferentes. Pode ser observado que como o endereço começa por 200 (ou seja, os dois primeiros bits são 1 e o terceiro, 0), eles são de classe C. Por isso, os três primeiros bytes do endereço identificam a rede. Conforme apresentado na figura 6.21, as estações possuem o endereço começando por 200.18.171, estando essas estações na mesma rede LAN (200.18.171.0). Na figura 6.22, as estações estão em redes distintas, sendo a primeira rede representada pelo endereço de rede 200.18.171.0 e a segunda representada pelo endereço de rede 200.18.180.0. Nesse caso, torna-se necessária a presença de um roteador para permitir a comunicação entre os computadores das duas redes. É importante observar que é a máscara de rede que oficializa a parte do endereço IP que corresponde à rede.

A figura 6.23 ilustra um diagrama de rede com o endereçamento utilizado. Note que não há necessidade de correlação entre os

endereços utilizados nas redes adjacentes. O mecanismo para que uma mensagem chegue à rede correta é o roteamento. Cada elemento conectando mais de uma rede realiza a função de roteamento IP, baseado em decisões de rotas inseridas de forma manual ou aprendidas por meio de protocolos de roteamento. Note que mesmo os enlaces formados por ligações ponto a ponto são também redes distintas. Nesse diagrama, existem seis redes, identificadas por 200.1.2.0, 139.82.5.0, 210.200.4.0, 210.201.0.0, 10.0.0.0 e 200.1.3.0.

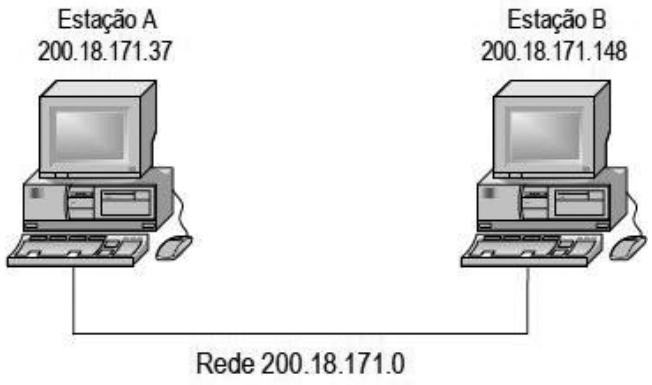



*Figura 6.21 – Rede LAN tradicional com endereços IP.*

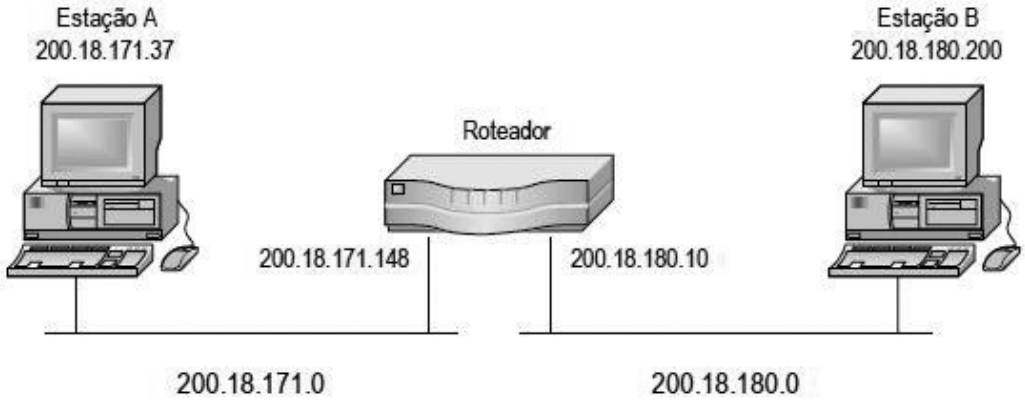



*Figura 6.22 – Rede LAN dividida por um roteador com os respectivos endereços IP.*

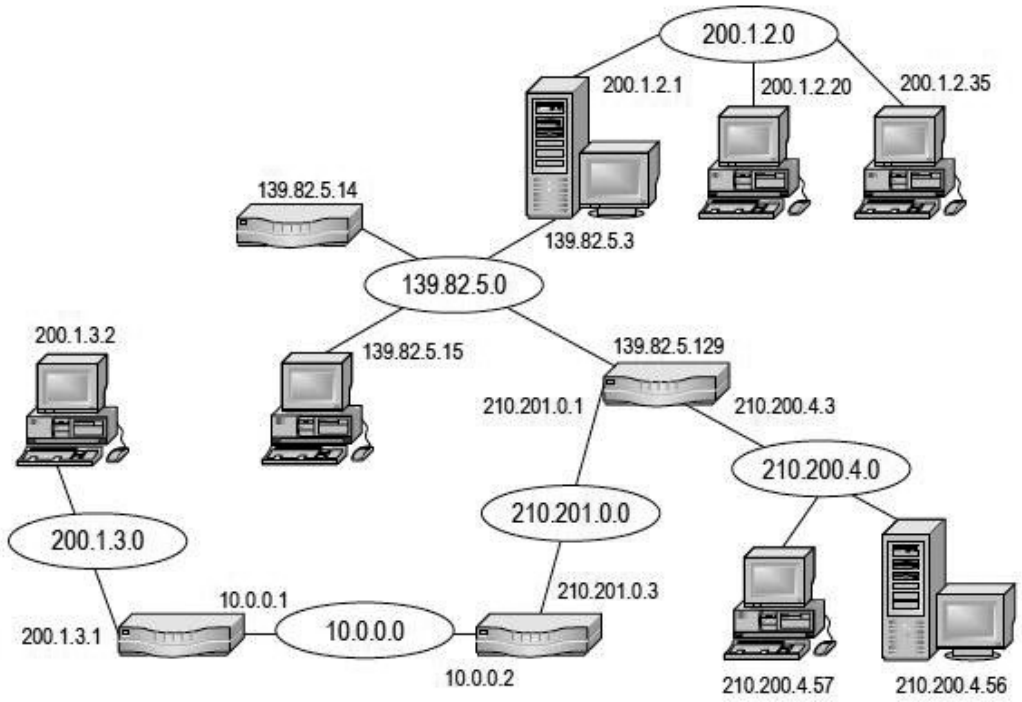



*Figura 6.23 – Diagrama de rede interligada por diversos roteadores.*

## 6.4.2 Mapeamento de endereços IP em endereços de rede

O protocolo Ethernet possui um endereço próprio para identificar as diversas máquinas situadas na rede. No protocolo Ethernet, o endereçamento utilizado é chamado de endereço físico ou endereço MAC (*Media Access Control*), formado por 6 bytes. Esse tipo de endereçamento só é útil para identificar diversas máquinas, não possuindo informação capaz de distinguir redes distintas. Para que uma máquina com o protocolo IP possa enviar um pacote para outra máquina situada na mesma rede, ela deve se basear no protocolo de rede local, já que é necessário saber o endereço físico. Como o protocolo IP só identifica uma máquina pelo endereço IP, deve haver um mapeamento entre o endereço IP e o endereço de rede MAC. Esse mapeamento é realizado pelo protocolo ARP.

A figura 6.24 apresenta as informações contidas no pacote (endereço IP e MAC) quando este está sendo transmitido do computador A para o computador B. Essa figura apresenta a situação desse pacote quando ainda não atingiu o roteador. A figura

6.25 apresenta as informações desse pacote quando ele ultrapassou o roteador. É importante observar que o endereço MAC do pacote, antes de chegar ao roteador, refere-se ao endereço MAC do roteador. Isso acontece para todo pacote direcionado a um endereço IP presente em outra rede. Como ainda não é possível saber qual o endereço MAC do equipamento destino, o pacote gerado possuirá o endereço MAC do roteador (conhecido também por *default gateway*), que representa a porta de saída para alcançar o equipamento destino.

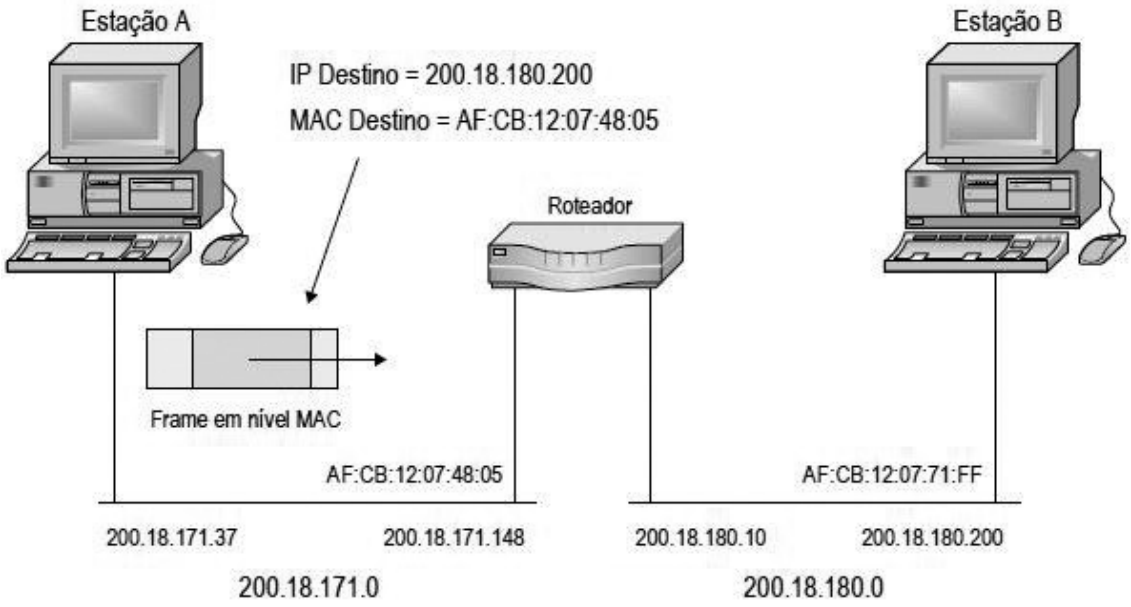



*Figura 6.24 – Comunicação entre duas redes no primeiro estágio.*

A figura 6.24 mostra uma rede com duas estações, na qual uma máquina A com endereço IP 200.18.171.37 deseja enviar uma mensagem para a máquina B, cujo endereço é 200.18.180.200. A mensagem a ser enviada é uma mensagem IP. No caso do exemplo da figura 6.24, antes de efetivamente enviar a mensagem IP, a estação utilizará o protocolo ARP para determinar o endereço MAC da interface cujo endereço IP é o destino da mensagem. A figura 6.25 apresenta o pacote depois de ser repassado pelo roteador. É importante verificar que a informação do MAC destino é alterada no pacote depois de ser remontado pelo roteador.

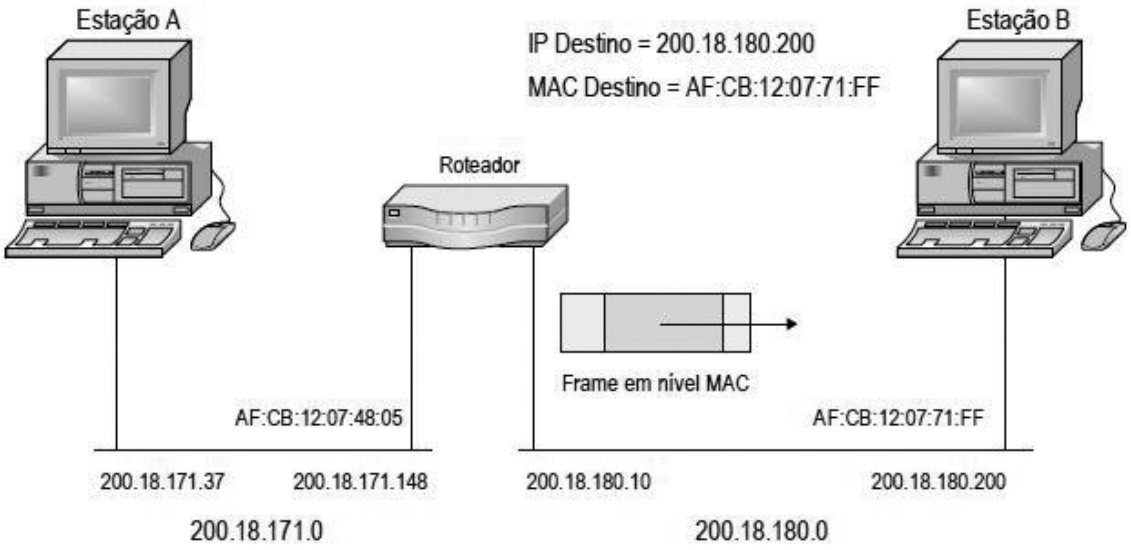



*Figura 6.25 – Comunicação entre duas redes no segundo estágio.*

A seguir, para complementar o assunto de roteadores, descreveremos, de forma sucinta, o funcionamento do protocolo ARP analisando a figura 6.21.

Digamos que o computador A verifique que o computador destino (computador B) está na mesma rede local. Para chegar a essa conclusão, o protocolo IP realiza uma operação lógica & (E) entre o endereço IP origem com sua respectiva máscara e uma operação lógica & entre o endereço IP destino e sua respectiva máscara. Os resultados dessa operação lógica são comparados e, caso sejam iguais, o endereço de rede IP origem e o endereço de rede IP destino pertencem à mesma rede. Na sequência, o protocolo IP do computador A verifica que ainda não possui um mapeamento do endereço MAC para o endereço IP do computador B, assim o protocolo IP solicita ao protocolo ARP o endereço MAC necessário.

Para atender ao pedido do computador A, o protocolo ARP envia um pacote ARP (ARP *Request*) com o endereço MAC destino do pacote igual a *broadcast* (difusão para todas as máquinas – FF:FF:FF:FF:FF:FF). A partir desse momento, todos os computadores recebem o pacote ARP, mas somente aquele que possuir o endereço IP especificado como destino igual ao do pacote enviado responderá. O computador destino guardará por alguns segundos na tabela ARP cache o mapeamento do endereço

200.18.171.37 para o endereço MAC do computador A.

A resposta será enviada no próprio quadro Ethernet, encapsulado, por meio de uma mensagem ARP Reply endereçada diretamente ao computador A. O computador A recebe o pacote e coloca um mapeamento do endereço IP de B e seu endereço MAC respectivo. Essa informação residirá em uma tabela que persistirá durante um certo tempo (ARP *cache*). Por fim, o computador A transmite o pacote IP inicial depois de saber o endereço MAC do computador B.

## 6.5 Exercícios do capítulo 6

Os exercícios 1 a 8 se baseiam na figura 6.26:

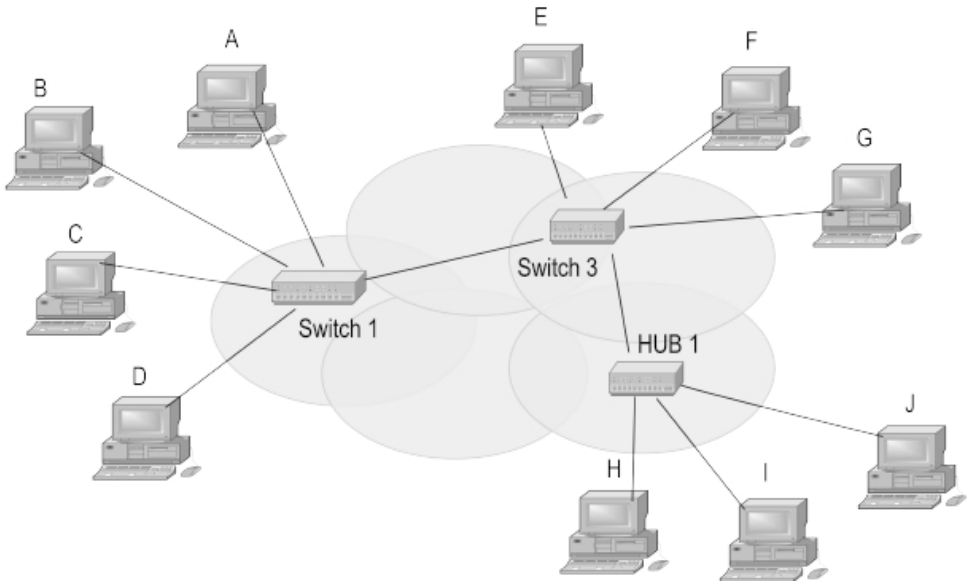



*Figura 6.26 – Rede local.*

**1**. Se o computador A enviar um pedido ao computador D, que computadores também receberão esse pedido?

a) C.

b) B, D.

c) A, D.

d) D.

e) E, F, D.

**2**. Se o computador G enviar um pedido para o computador C, que computadores receberão o pedido?

a) E.

b) B, C, D.

c) A, B, C, D.

d) A, B, C.

e) C.

f) A, B, C, D, E, F.

**3**. Se o computador J enviar um pedido ao computador A, que computadores receberão esse pedido?

a) I, J, A.

b) H, I, A.

c) H, I, A, B, C, D.

d) E, I, J, B.

e) J, A.

**4**. Se o computador F enviar um pedido ao computador E, que computadores receberão esse pedido?

a) E, C.

b) C.

c) E.

d) A, C.

e) F, C.

**5**. Suponha que a máquina A transmita um quadro Ethernet *unicast* para B. Esse quadro Ethernet chegará a quais computadores da rede?

**6**. Suponha que a máquina A transmita um quadro Ethernet em *broadcast*. Esse quadro Ethernet chegará a quais computadores da rede?

**7**. Suponha que a máquina A transmita um quadro Ethernet *unicast* para J. Esse quadro Ethernet chegará a quais computadores da rede?

**8**. Suponha que a máquina A transmita um quadro Ethernet *unicast* para F. Esse quadro Ethernet chegará a quais computadores da rede?

**9**. No máximo, quantos centímetros de cabo devem ser desencapados para realizar a crimpagem, mantendo a qualidade da conexão?

**10**. Cite dois equipamentos ativos e descreva onde se deve utilizar cada um deles.

**11**. No modelo OSI, em qual camada o hub e o switch estão localizados?

**12**. Cite uma vantagem e uma desvantagem do switch.

**13**. Descreva o processo de flooding utilizado pelos switches.

**14**. Em qual situação em uma rede deve-se utilizar um switch no nível de enlace?

**15**. Em quais situações em uma rede deve-se utilizar um roteador?

**16**. Responda sobre equipamentos ativos de rede de computadores:

a) Que equipamento filtra e encaminha pacotes entre segmentos de uma LAN, opera na camada de enlace (camada 2) e, em algumas redes, na camada de rede (camada 3) do modelo de referência TCP/IP, suportando assim qualquer protocolo de pacotes?

b) Que equipamento conecta qualquer número de LANs, usa o cabeçalho e uma tabela de encaminhamento para determinar para onde os pacotes devem ser enviados, usa ICMP para se comunicar com outros e configurar o melhor caminho entre dois hosts?

c) Que equipamento atua como ponto de conexão comum entre dispositivos de uma rede, é comumente utilizado para conectar segmentos de uma LAN, contém múltiplas portas e, quando um pacote é recebido em uma porta, é copiado para as outras portas, de modo que todos os segmentos da LAN podem ver todos os pacotes?

**17**. Temos cinco estações e um servidor em uma rede Ethernet

conectados em fila via cabo coaxial. O cabo se parte entre a 2a e a 3a estação. Quantas estações perderão o acesso ao servidor? No entanto, se as cinco estações e o servidor estivessem conectados via hub 10BASET e o cabo par trançado entre a 2a estação e o hub se partisse, quantas estações perderiam o acesso ao servidor?

a) Duas estações em ambos os casos.

b) Duas estações no cabo coaxial e uma estação no hub.

c) Três estações no cabo coaxial e uma estação no hub.

d) Cinco estações no cabo coaxial, mais o servidor e uma estação no hub.

**18**. Qual dispositivo a seguir opera na camada de rede do modelo OSI?

a) Roteador.

b) Repetidor.

c) Comutador.

d) Ponte.

**19**. O TCP/IP possui um esquema de endereçamento em que é possível definir o endereço da rede e o endereço do host. É dividido normalmente em três classes básicas (A, B e C), além de uma para *multicast* (D) e outra para endereçamento especial. A respeito dos endereços do IP de classes A, B e C, julgue os seguintes itens:

a) Um endereço classe A é caracterizado por ter o seu primeiro bit definido como 0.

b) Um endereço classe B é caracterizado por ter o seu primeiro bit definido como 1 e o segundo bit definido como 1.

c) Um endereço classe C é caracterizado por ter o seu primeiro bit definido como 1, o segundo bit definido como 0 e o terceiro como 1.

d) Um endereço classe C é caracterizado por ter o seu primeiro bit definido como 0, o segundo bit definido como 1 e o terceiro como 1.

**20**. (COPEL, 2010) Um switch Ethernet desempenha a seguinte

função na rede:

a) Distribui endereços IP para os hosts da rede.

b) Realiza a comutação de quadros na camada 2 do modelo OSI.

c) Realiza o encaminhamento de pacotes, processando o endereço IP destino em função de uma tabela de rotas.

d) Gerencia conexões VoIP, fazendo a tradução de padrões quando necessário.

e) Repete todos os quadros recebidos em todas as suas interfaces.

**21**. Como ocorre o processo de eleição no STP?

**22**. O que impacta se ajustarmos o *hellotime* para 5 segundos?

**23**. O que ocorre com um quadro quando for recebido por um switch que acabou de ser ligado?

a) Entra em loop.

b) Gera inundação.

c) Trava a comunicação.

d) Direciona o quadro para somente um destino.

**24**. Qual o parâmetro utilizado pelo switch para definir o switch-raiz?

a) Bridge port.

b) Bridge ID.

c) Custo.

d) Custo e MAC do switch.

CAPÍTULO 7

# Modems

Neste capítulo, apresentaremos as características dos modems utilizados para a conexão entre equipamentos de rede. Citaremos a relação de Nyquist e Shannon, os padrões de modulação e os comandos Hayes utilizados na programação dos modems. Trataremos ainda da diferença entre transmissões síncronas e assíncronas e os tipos de multiplexação.

## 7.1 Introdução

A comunicação entre dois micros via linha telefônica pode ser feita por meio de um periférico chamado modem, que converte os dados gerados pela porta serial do micro transmissor (sinais digitais) em forma de ondas analógicas a serem transmitidas na linha telefônica. No destino, o modem faz o processo inverso, convertendo o sinal analógico em digital. O modem foi criado em 1960 pela AT&T, mas somente em 1979 a Hayes lançou o primeiro modem para microcomputadores. Seu nome é a contração das palavras MOdulador e DEModulador, pois essas são suas principais funções. A figura 7.1 apresenta a comunicação entre dois equipamentos utilizando modems:

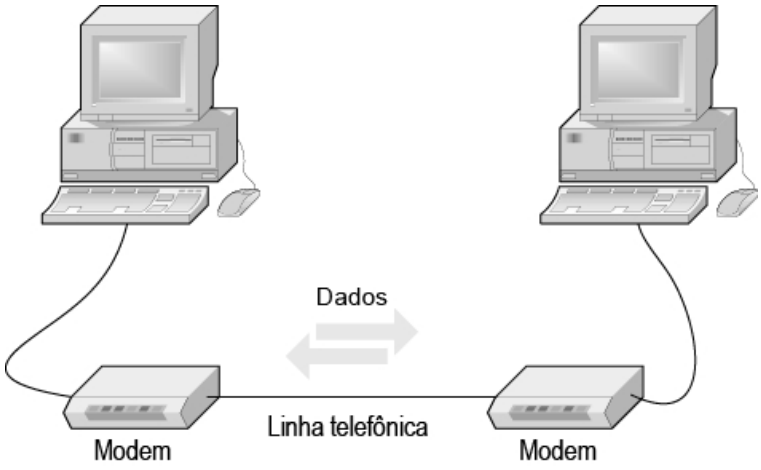


*Figura 7.1 – Conexão entre dois modems.*

O modem executa uma transformação, por modulação (modem analógico) ou por codificação (modem digital), dos sinais emitidos pelo computador, gerando sinais analógicos ou digitais adequados à transmissão sobre uma linha telefônica. No destino, um equipamento igual a este demodula (modem analógico) ou decodifica (modem digital) a informação, entregando o sinal digital restaurado ao equipamento terminal a ele conectado. A codificação e a decodificação são utilizadas quando a linha que interliga os modems é do tipo digital. Nesse caso, os modems funcionam apenas como uma interface para converter os dados gerados pelo computador no formato de transmissão usado pela linha de transmissão. Toda essa tecnologia nos traz alguns benefícios, como:

- Permite o acesso a informações de forma mais rápida e confiável.
- Permite a troca de informações sobre produtos em tempo razoável para seus clientes.
- Oferece maior capacidade de prestação de serviços, eliminando deslocamento de pessoas ao local necessário.
- Permite utilizar o serviço de correio eletrônico, conferências, centro de negócios virtuais e acesso de serviços pela rede.

## 7.2 Modulação e demodulação

As linhas telefônicas operam com sinais analógicos e o computador comunica-se por sinais digitais. Para que o computador se comunique com outro computador utilizando uma linha telefônica, é necessário utilizar um modem e suas propriedades de modulação e demodulação. Vejamos passo a passo como o processo de comunicação entre dois micros acontece:

1. Todas as informações enviadas pelo computador em sinais digitais são transformadas pelo modem, que atua como modulador, em sinais analógicos.
2. Os dados analógicos são transmitidos pela linha telefônica.
3. Quando os dados chegam ao modem receptor (modem remoto),

que atua como demodulador, o sinal analógico é convertido de volta em sinal digital e transferido para o computador receptor, preservando o conteúdo da informação.

O êxito de um sistema de comunicação depende da modulação, de modo que a escolha do tipo de modulação é uma decisão fundamental em projetos de sistemas para transmissão de sinais. A seguir, apresentaremos três técnicas de modulação utilizadas no início da concepção dos modems:

- Modulação por amplitude (AM).
- Modulação por frequência (FM).
- Modulação por fase (PM).

Essas técnicas não são mais utilizadas em decorrência da baixa taxa de transmissão oferecida. Novas técnicas avançadas foram desenvolvidas e estão disponíveis em diversos modems, inclusive os que utilizamos em nossas casas. Como exemplo dessas técnicas, podemos citar o QAM e o PCM. A figura 7.2 apresenta como eram as técnicas de modulação no início da utilização dos modems.

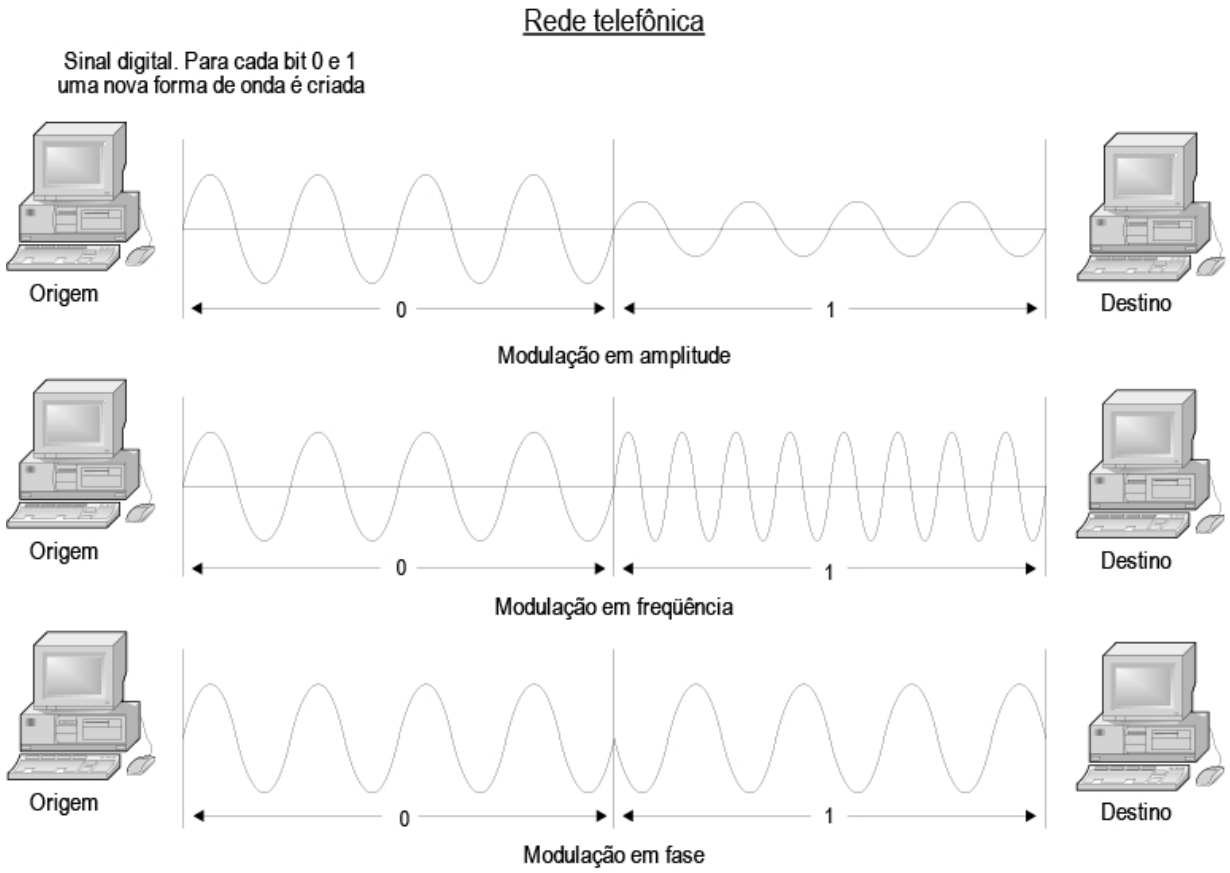



*Figura 7.2 – Técnicas de modulação.*

A seguir, apresentaremos a relação de Nyquist, a qual explicou no início da construção dos modems a relação entre a taxa de transmissão e as formas de modulação.

## 7.3 Relação de Nyquist

A Rede Telefônica Pública (PSTN – *Public Switched Telephone Network*) foi projetada para trabalhar na faixa de frequências de 300 a 3.300 Hz. A diferença entre a maior e a menor frequência resulta na banda de frequência passante (3.000 Hz). As informações são transmitidas por meio da linha telefônica com o uso de variações (modulação) em relação a um determinado sinal, chamado de portadora, ou seja, baseando-se em uma frequência conhecida, aplicam-se variações em cima desse sinal, as quais representarão os bits transmitidos. Quanto maior for o número de variações por segundo, maior será a quantidade de informação transmitida, ou seja, maior será a taxa de bits. A taxa de bits é medida em bps, que significa bits por segundo.

Em 1928, um matemático que trabalhava nos laboratórios da Bell, Harry Nyquist, estabeleceu uma relação entre a banda passante (representado pela letra W) de um canal de dados e a máxima taxa de bits que o canal poderia transportar. É importante observar que, nessa época, para cada frequência (1 Hz = 1 bit) um bit era transmitido. A relação que Nyquist estabeleceu referia-se à taxa máxima em bauds (1 baud = 1 bit = 1 Hz) possível a ser transmitida em um canal telefônico. Nessa época, a taxa de transmissão dos modems era baseada em bauds. Essa relação afirma que, para representarmos um sinal no destino, esse sinal somente poderá ser reconstruído, sem perdas significativas, se forem retiradas amostras com o dobro da frequência máxima desse sinal. Dessa forma, a banda passante de um meio de transmissão de dados deverá também ser, no mínimo, o dobro da frequência máxima do sinal de dados a ser transmitido. Isso é necessário para que este não sofra perdas no momento da recepção.

Assim, esse teorema estabelece que a taxa máxima de bits possível a ser transmitida entre dois equipamentos é igual a 2 x W, em que W refere-se à diferença entre a maior e a menor frequência disponível (3.000 Hz). Como o receptor necessita do dobro da frequência transmitida para recuperar o sinal recebido, a quantidade máxima de bits nesse caso é de 1.500 bps, ou seja, se um modem transmitir dados a 1.500 bps, estes poderão ser reconstruídos no destino em razão de a banda passante ser de 3.000 Hz (1 Hz = 1 bit). Dessa forma, o teorema de Nyquist leva a uma aparente limitação da máxima taxa de bits de transmissão para um canal de dados em 1.500 bps.

Ainda na década de 1980, os modems mais sofisticados transmitiam dados em torno de 1.300 bps e eram vendidos por aproximadamente 500 dólares. Como sabemos, nossos modems possuem a capacidade de transmitir bem mais bits do que o teorema de Nyquist afirma. Ainda neste capítulo, veremos o que foi feito para que os modems atingissem maiores velocidades.

## 7.4 Taxa de transmissão

No caso da linha telefônica, como a frequência máxima que o canal transporta é de 3.000 Hz, temos que esse canal suporta somente 1.500 mudanças de sinal por segundo, ou seja, bits por segundo, conforme comentado no teorema de Nyquist. Assim, ao menos em princípio, a linha telefônica convencional só é capaz de transmitir dados a uma taxa máxima de 1.500 bps. Porém, esse limite de 1.500 bps só existe se convertermos cada bit de informação diretamente em uma tensão a ser transmitida. Por exemplo, converter o bit 0 em 1 volt e o bit 1 em 5 volts. Para romper esse limite, bastaria converter um grupo maior de bits em outros sinais de tensão. Vejamos um exemplo: se usarmos quatro em vez de dois níveis de tensão (1 volt, 1,75 volts, 3,75 volts, 5 volts), poderemos codificar 2 bits por sinal (00, 01, 10, 11). Nesse caso, a taxa de transmissão máxima dobraria, passando de 1.500 bps para 3.000 bps. Em princípio, bastaria aumentar a quantidade de variações de tensão possíveis para que pudéssemos codificar mais *bits* por sinal, aumentando a taxa de transferência.

No entanto, como nem tudo é como imaginamos, surge o seguinte problema a ser analisado: temos que levar em consideração o ruído na linha telefônica, ou seja, chega um ponto em que os níveis de tensão utilizados na transmissão tornam-se tão próximos que qualquer ruído na linha faz que o *modem*-receptor entenda de forma equivocada o dado que está sendo transmitido. Imagine que estamos trabalhando com uma variação de 0,2 volt para codificar cada grupo de 8 *bits*. Se forem transmitidos 4 volts (que representam 11110111) e, em decorrência de um ruído na linha, esse valor cair para 3,8 volts, isso fará com que o *modem*-receptor aceite esse valor (uma vez que está dentro dos valores válidos), mas modulará esse valor como sendo 11110000, já que 3,8 volts representa esse grupo de *bits* por exemplo. O ruído presente nas linhas telefônicas é o responsável pela limitação da taxa de transmissão.

Esse ruído presente nas linhas telefônicas é medido por meio da relação sinal/ruído, também conhecido por *SNR* (*Signal to Noise Ratio*). O *SNR* é medido em decibéis, de modo que a relação sinal/ruído típica da linha telefônica é de 30 dB. A seguir, comentaremos a

relação sinal/ruído.

### 7.4.1 Relação entre o sinal e o ruído

De forma geral, a relação sinal/ruído (S/N – *Signal/Noise*) refere-se a quanto o sinal (propriamente dito) seria mais potente do que o ruído. Quanto maior essa relação, mais eficaz é o meio de transmissão. O valor é obtido dividindo-se a potência do sinal pela potência de ruído, de modo que quanto maior a relação, melhor será a conexão, e uma maior quantidade de dados poderá ser transmitida.

Mesmo sob as melhores circunstâncias, ou seja, mesmo em ambientes com baixo ruído, quando um sinal for submetido à conversão analógica digital, sofrerá com o ruído de quantização que limita a velocidade dos modems a operarem a, no máximo, 33,6 Kbps sempre que existir a conversão entre o sinal analógico em sinal digital. A relação sinal/ruído determina quanto o canal de dados poderá transmitir. Em nossas linhas telefônicas, esse valor é, em média, de 30 dB. O dB (decibel) é uma unidade logarítmica usada, nesse caso, para medir a relação de sinal/ruído.

A figura 7.3 apresenta uma comunicação entre dois equipamentos com os sinais sendo convertidos de analógico para digital e de digital para analógico:

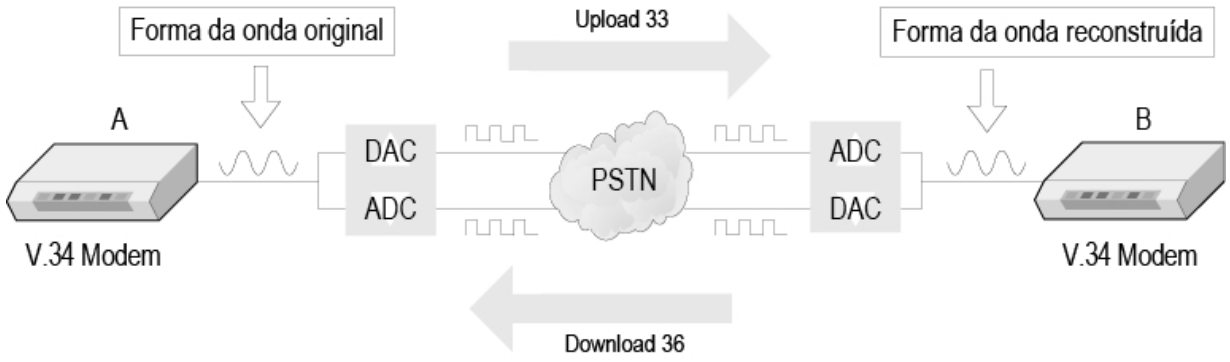



*Figura 7.3 – Conexão entre dois equipamentos via modem.*

A seguir, apresentaremos uma relação do quanto um valor em decibéis se refere à potência do sinal em relação ao ruído.

O valor de 10 decibéis corresponde a um ganho de 10 vezes do sinal em relação ao ruído. Portanto, 30 decibéis correspondem a 10 dB + 10 dB + 10 dB, o que significa 10 * 10 * 10, resultando em

1.000. Assim, o sinal telefônico é da ordem de 1.000 vezes maior do que o ruído da linha telefônica. O ganho de 30 decibéis na linha telefônica foi considerado ideal na década de 1940.

#### 7.4.1.1 Representação do ganho do sinal em decibéis

Por definição, uma quantidade Q em dB (decibéis) é igual a 10 vezes o logaritmo decimal da relação de duas potências medidas em Watts, ou seja, Q(dB) = 10log10(S/N). Para esse exemplo, tomaremos como base a relação sinal/ruído de nossas linhas telefônicas, a qual é dada e vale 1.000.

$Q = 10 * \log_{10} (1.000)$

$Q = 10 * \log_{10} (1.000)$ é igual a 10^x = 10^3, assim x = 3

$Q = 10 * 3$

Q = 30 dB, ou seja, a relação sinal/ruído de uma linha telefônica é, no melhor dos casos, 30 dB.

É importante observar que o termo dB refere-se a uma relação entre unidades iguais e não tem dimensão, ou seja, é um valor adimensional.

## 7.5 Lei de Shannon

Em 1948, Claude Shannon estendeu o trabalho de Nyquist para o caso de canais sujeitos a ruído. Conforme comentamos, o ruído é um dos maiores limitantes dos sistemas de comunicação analógicos/digitais. A quantidade de ruído presente é dada pela relação entre a potência do sinal e a potência do ruído. O teorema de Shannon tem como objetivo informar qual é a máxima taxa de transmissão possível baseada na largura de banda do canal (banda passante) e na quantidade de ruído presente, ou seja, até onde é possível ir com o esquema de modulação, dependendo do ruído do canal. Essa relação definida por Claude Shannon determina a máxima taxa de transmissão de bits teórica para um dado canal. A tabela 7.1 descreve as variáveis apresentadas na figura 7.4, que se refere à fórmula proposta por Shannon.

$$C = W\log_2\left(1 + \frac{S}{N}\right)$$

*Figura 7.4 – Relação de Shanon.*

*Tabela 7.1 – Descrição das variáveis da relação de Shannon*

| Variável | Descrição |
|---|---|
| C | Máxima capacidade do canal em bps. |
| W | Máxima banda passante do canal medida em Hz. |
| S | Potência do sinal em Watts. |
| N | Potência do ruído em Watts. |
| S/N | Relação sinal/ruído. |

### 7.5.1 Aplicação do teorema de Shannon

No sistema telefônico convencional adaptado ao sinal de dados com largura de banda em torno de 3.000 Hz, existe uma relação sinal/ruído que varia entre 30 dB e 35 dB. Assim, segundo Shannon, a capacidade efetiva do canal é dado por:

$3.000 \times (\log_2 1 + \log_2 1000)$

Para resolver esse logaritmo, devemos concluir que: 2 elevado a quanto resultará em 1.000. Como resposta, temos +- 2 elevado a 10.

3.000 x (0 + 10) = ~30.000 bps ou 30 Kbps.

É importante lembrar que a relação sinal/ruído das linhas telefônicas varia entre 30 dB e 35 dB; logo, o teorema de Shanon comprova a banda prática de 33,6 Kbps.

## 7.6 Conclusão dos teoremas

Depois de analisar o teorema de Shannon, concluímos que modems para conexões discadas têm pouca chance de ultrapassar os 33,6 Kbps mantidas a relação sinal/ruído e a taxa de erro mínima. O teorema de Nyquist mostra que codificações com mais bits por ciclo

podem aumentar a taxa máxima de transmissão. O teorema de Shannon mostra que existe um limite para a melhoria que pode ser dado devido às restrições físicas dos sistemas de transmissão reais. Aplicando-se essa fórmula aos dados apresentados pela linha telefônica, observa-se que a linha telefônica convencional tem um limite de transmissão de mais ou menos 34 Kbps. Por isso, os modems mais velozes para linhas telefônicas convencionais são os de 33.600 Kbps no padrão V.34.

## 7.7 Baud rate

Baud rate é a quantidade de elementos analógicos por segundo transmitidos, porém baud não possui o mesmo significado que bits por segundo (bps), uma vez que, em razão da modulação empregada, um elemento analógico representa mais de um bit de informação. Em uma transmissão via linha telefônica a 2.400 bps, a quantidade de elementos sinalizadores por segundo é de 600 bauds, utilizando-se, por exemplo, um esquema de modulação conhecido por Trellis Modulation que converte cada grupo de 4 bits em uma tensão analógica.

## 7.8 Comandos Hayes

Por meio dos comandos Hayes, é possível interagir com o modem submetendo comandos por meio de um terminal disponível no próprio sistema operacional. A string de inicialização de um modem o prepara para a comunicação e configura características, como modo de discagem, tempo de espera para atender, detecção de sinal ocupado etc. A seguir, abordaremos os comandos e suas classificações. Os comandos Hayes estão divididos em quatro grupos, conforme mostram as tabelas 7.2 a 7.5.

A primeira divisão trata dos comandos básicos, que são representados por uma letra maiúscula seguida de um dígito. A tabela 7.2 apresenta exemplos de comandos básicos:

*Tabela 7.2 – Comandos básicos*

| Comando | Descrição |
|---|---|
| ATM1 | Volume do alto-falante. |
| ATW0 | Se o ícone mostrar a velocidade serial, exemplo: 115.2 Kbps ou 38.400, em vez da velocidade de transmissão da linha quando você estiver conectado à Internet, utilize esse comando para alterar a informação (Atw0). |

A segunda divisão trata dos comandos estendidos, que são representados pelo símbolo & (“e” comercial) e uma letra maiúscula seguida por um dígito. A tabela 7.3 apresenta exemplos de comandos estendidos:

*Tabela 7.3 – Comandos estendidos*

| Comando | Descrição |
|---|---|
| AT&F ou AT&F0 | Carrega a configuração original de fábrica. |
| AT&B1 | Faz o modem procurar a melhor taxa para transmissão. |

A terceira divisão trata dos comandos proprietários, que são iniciados por uma contra barra (/) ou por um símbolo de porcentagem (%). A tabela 7.4 apresenta exemplos de comandos proprietários:

*Tabela 7.4 – Comandos proprietários*

| Comando | Descrição |
|---|---|
| AT%C0 | Desabilita a compressão de dados. |
| AT %C1 | Habilita o protocolo MNP5 – compressão de dados. |
| AT %C2 | Habilita o protocolo V.42 bis – compressão de dados. |
| AT %C3 | Habilita o protocolo MNP5 e V.42 bis. |

A quarta e última divisão trata dos comandos de registrador, que são iniciados por Sr = n, em que r é o número de registradores e n é o novo valor a ser atribuído ao registrador. A tabela 7.5 apresenta exemplos de comandos de registrador:

*Tabela 7.5 – Comandos de registrador*

| Comando | Descrição |
|---|---|
| AT S0 = 0 | Desabilita o autoatendimento do modem. |
| AT S0 = 1 | Atende a uma ligação no primeiro Ring. |
| AT S0 = 2 | Atende a uma ligação no segundo Ring. |
| AT S8 = n | Tempo de espera de pausa para discagem, em que n é o tempo em segundos. |

Um registro é uma abstração de um endereço físico de memória, e os modems possuem uma pequena memória incluída. Esse conjunto de instruções serve para alterar o valor de um registro (endereço de memória), o qual armazena uma variável utilizada pelo modem e pelo software de comunicação. A seguir, apresentaremos um exemplo da utilização dos comandos Hayes.

## 7.9. Tipo de modem quanto à sincronização

Existem dois tipos de modems: os síncronos e os assíncronos. A seguir, detalharemos as características de cada um deles.

### 7.9.1 Modem assíncrono

O termo assíncrono também pode ser chamado de transmissão orientada a caractere. A transmissão ocorre caractere a caractere, ou seja, para cada byte transmitido, bits de controle são inseridos entre os bytes. Não é necessário sincronizar o transmissor e o receptor para realizar a transmissão de um caractere, pois o receptor sempre saberá onde começa e onde termina o byte transmitido. Nesse tipo de transmissão, o canal de comunicação permanece em estado de repouso (não há transmissão de informação) até que seja necessário o envio de um caractere (o instante do envio do caractere é arbitrário e definido pelo transmissor). O controle é feito por bits de sinalização chamados de *start bit* e *stop bit* e são necessários um start bit e dois ou mais stop

bits na transmissão de cada byte.

### 7.9.2 Como o método assíncrono é sincronizado

Para o receptor detectar os bits individuais, deve sempre ter um sinal de relógio que esteja em sincronismo com o relógio do transmissor. Tal relógio geraria um tique em sincronismo com cada bit transmitido (ou recebido).

Na transmissão assíncrona, o sincronismo é realizado cercando cada byte com um bit de partida e um ou mais bits de parada (feito por hardware). O receptor escuta na linha por um bit de partida e, quando detecta um bit que caracteriza a partida, dispara os tiques de seu relógio, os quais usa para medir o tempo dos próximos 7, 8 ou 9 bits. Quando o bit de parada é lido, o relógio para e o receptor espera pelo próximo bit de partida. Dessa forma, há sincronismo apenas durante a recepção de um byte, mas não entre os bytes que compõem uma palavra. Assim, a sincronia é estabelecida dentro de cada palavra isoladamente, e cada palavra de um sinal assíncrono é autossuficiente e independente das relações de tempo que possam existir fora de seus limites.

Geralmente, os modems utilizados para comunicação de dados por meio de linhas telefônicas são assíncronos, visto que seria mais caro e mais difícil sincronizar sinais por meio do sistema telefônico, em que os sinais podem ser redirecionados a qualquer momento sem aviso. Esse chaveamento é normal no estabelecimento de uma conexão discada ou no processo de remanejamento de circuitos de dados dedicados.

Na figura 7.5, veja a transmissão de dois bytes em um modem assíncrono.


*Figura 7.5 – Transmissão assíncrona.*

### 7.9.3 Modem síncrono

Nesse tipo de transmissão serial, a informação é continuamente enviada pelo canal de comunicação sem intervalos entre bits ou

grupo de bits. Por meio da transmissão contínua da informação, é possível sincronizar o transmissor e o receptor. Nesse método de transmissão de dados, os modems operam de modo contínuo em frequências iguais, sendo mantidos em uma relação de fase correta por circuitos que monitoram a conexão constantemente, fazendo os ajustes necessários. No modo síncrono, os bits de enquadramento (start bit e stop bit) utilizados no modo assíncrono são desnecessários, o que torna essa modalidade de transmissão mais rápida. Na transmissão síncrona, a sincronia é estabelecida no início da transmissão de cada mensagem por meio de caracteres de sincronização (p. ex., SYN), não sendo necessários os caracteres start/stop. A sincronia, uma vez estabelecida, deve manter-se durante a transmissão de toda a mensagem. Isso significa que deve ser mantido certo ritmo de transmissão. No caso de mensagens longas, são inseridos sinais de sincronização no meio da mensagem.

Esse método possui algumas vantagens, como modems síncronos são mais sofisticados, não possuem a introdução de bits para informar o início e o fim da transmissão, possuem mais eficiência, pois a proporção de dados transmitidos como informação em relação à configuração de sincronização é maior do que durante a transmissão assíncrona. Para finalizar, operam em velocidades maiores em comparação com o modo assíncrono.

Um dos problemas decorrentes do seu uso está em que, antes da troca de informações, as duas extremidades da linha devem estar sincronizadas, assim como a ligação entre o modem e o computador. Como outro problema, temos o recurso de discagem automática que dificilmente funciona com modems síncronos. Isso acontece porque, sem o estabelecimento da conexão, não há quem coordene a sincronização, e esta não pode ser feita sem discagem.

Para finalizar as desvantagens, ainda temos a questão do custo. Os caracteres são enviados em blocos, nunca antes de esses blocos serem formados, obrigando os equipamentos a serem dotados de memória de armazenamento para a coleta dos caracteres, até se formar o bloco com o comprimento usado pelo

equipamento. A memória presente nos modems síncronos refere-se a buffers, o que encarece seu custo. A figura 7.6 representa a transmissão de dados em um modem síncrono:


*Figura 7.6 – Transmissão síncrona.*

A seguir, apresentaremos o conceito de multiplexação presente nas transmissões que utilizam modems.

## 7.10 Multiplexação

A comunicação de dados tem o objetivo de permitir que diferentes componentes de hardware e software interajam entre si. Para isso, o meio de comunicação utilizado deve seguir padrões preestabelecidos de hardware e de software.

O meio de transmissão é, então, utilizado para transportar informações de um dispositivo para outro. Podemos identificar diferentes meios de comunicação utilizados para o transporte de dados, como cabo de cobre, fibras ópticas ou, ainda, ondas magnéticas.

Suponhamos que existam 20 casas em seu condomínio residencial e uma caixa comutadora que receba todos os cabos de cobre (meio de comunicação) e os distribua para a central telefônica. É importante observar que, para cada casa, um cabo individual deve ser instalado até a caixa comutadora e, por sua vez, até a central telefônica. Caso outros condomínios fossem construídos, eles também utilizariam a mesma caixa comutadora.

Se a caixa comutadora estiver no limite, uma nova deverá ser disponibilizada aos novos clientes. Se ainda fossem construídos outros condomínios próximos e para cada residência fosse ligado um novo telefone, a quantidade de cabos interligando as residências à caixa comutadora e, por fim, à central telefônica certamente apresentaria um grande problema de espaço físico para a empresa responsável por essa administração.

A fim de melhorar esse panorama e não tornar a disponibilização de um novo telefone um problema, a interligação entre as caixas

comutadoras e a central telefônica foi multiplexada. A multiplexação de um conjunto de residências significa agrupar em um único meio de transmissão diversas conexões telefônicas. Assim, a quantidade de fios é drasticamente reduzida e há também redução de custos e mais facilidade para disponibilizar novas conexões.

A figura 7.7 apresenta um exemplo de um sistema utilizando multiplexador. O computador A transmitirá dados ao computador D e o caminho seguido será o mesmo utilizado pela comunicação do computador B com o computador C.

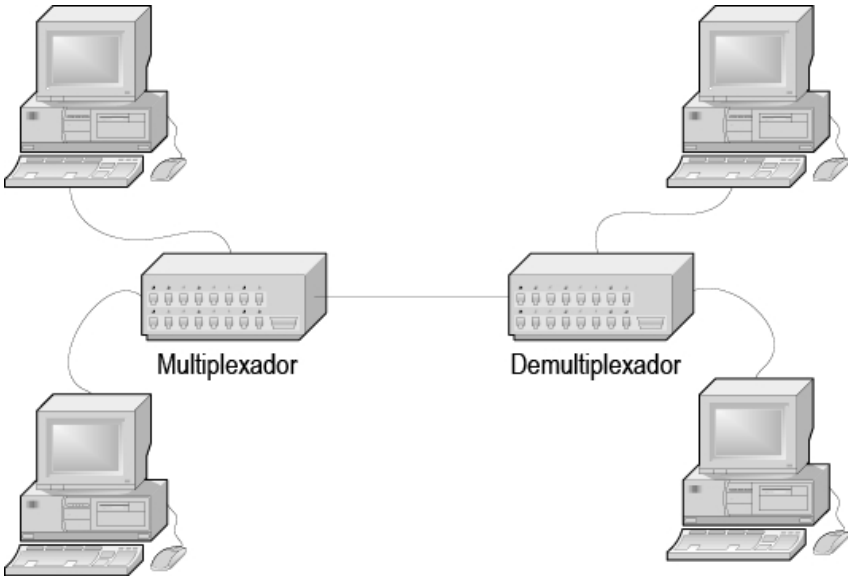



*Figura 7.7 – Sistema utilizando multiplexador.*

Para a transmissão simultânea de diferentes contatos telefônicos ou canais de televisão, devem-se utilizar técnicas adequadas de multiplexação. A seguir, descreveremos a multiplexação por divisão de frequências, por divisão de comprimento de onda e por divisão do tempo.

## 7.10.1 Multiplexação por divisão de frequências

A multiplexação por divisão de frequências (FDM – *Frequency Division Multiplexing*) é utilizada em redes nas quais é necessário transmitir diferentes sinais (diversas portadoras) pelo mesmo meio de comunicação. O termo portadora corresponde ao sinal de frequência contínua capaz de ser modulado.

A multiplexação por divisão de frequências pode transmitir sinais por meio de fios de cobre, fibra óptica ou, ainda, ondas de rádio. Quem gera os sinais na origem é o equipamento chamado de multiplexador, enquanto o que deverá receber o agregado de sinais é o demultiplexador. O multiplexador tem a função de agregar diferentes frequências e transmiti-las por um único canal. Na outra extremidade, o demultiplexador é responsável por receber as diferentes frequências, separá-las e entregá-las ao correto destino.

## 7.10.2 Multiplexação por divisão de comprimento de onda

A multiplexação por divisão de comprimento de onda (WDM – *Wave Division Multiplexing*) é utilizada em rede em que se tem a necessidade de transmitir diferentes comprimentos de ondas ou, de forma mais simpática, diferentes cores. Assim, as portadoras podem ser identificadas como amarela, vermelha, azul etc.

A multiplexação por divisão de comprimento de onda opera enviando inúmeras ondas luminosas em um único par de fibra óptica. Um prisma no emissor combina as diferentes ondas luminosas formando um sinal resultante, o qual é transmitido pelo cabo de fibra óptica até o receptor, sendo este o responsável por separar o sinal recebido. No receptor, existe um segundo prisma utilizado para separar o sinal recebido e, em seguida, entregá-lo ao destino.

## 7.10.3 Multiplexação por divisão de tempo

A multiplexação por divisão do tempo (TDM – *Time Division Multiplexing*) atua como uma alternativa à FDM. Na TDM, além de os dispositivos emissores utilizarem intervalos de tempo para a transmissão de seus dados, existem duas formas de funcionamento: a multiplexação síncrona por divisão do tempo (STDM) e a multiplexação estatística.

Na multiplexação síncrona por divisão do tempo, cada emissor utiliza o meio de transmissão (cabo metálico, fibra óptica ou rádio) por um período conhecido. Cada equipamento possui o seu

momento de transmissão, sempre respeitando a sequência de transmissão, ou seja, antes de um equipamento voltar a transmitir, todos os outros já deverão ter utilizado o seu tempo.

Tomamos, como exemplo, quatro computadores transmitindo dados pela Internet. Inicialmente, o primeiro computador transmite; em seguida, o segundo computador transmite; na sequência, o terceiro transmite e, somente depois de o primeiro, o segundo e o terceiro terem utilizado o meio, o quarto computador inicia sua transmissão. Mesmo que o primeiro, o segundo ou o terceiro computador não tenham nada a transmitir, o quarto computador esperará a sua vez, pois o tempo dos três primeiros computadores já estava reservado, estando esses computadores utilizando o meio ou não.

A multiplexação estatística pode ser utilizada justamente com a finalidade de suprir essa deficiência da STDM, pois também faz a reserva de um tempo para cada equipamento transmitir. Entretanto, caso algum equipamento não tenha nada a transmitir, esse tem o seu tempo otimizado, ou seja, o tempo ocioso será utilizado para que o próximo inicie sua transmissão.

## 7.11 Exercícios do capítulo 7

**1**. Descreva 12 comandos Hayes identificando o resultado que cada um deles causa para o modem depois de ser executado.

**2**. Comente as transmissões síncrona e assíncrona.

CAPÍTULO 8

# Protocolos da camada de inter-rede

Neste capítulo, apresentaremos as características dos protocolos que operam na camada de rede: IP, ARP, RARP, BOOTP, ICMP etc. Além disso, serão abordados endereçamento de rede, máscara de sub-rede e como a Internet está identificada por endereços IP.

## 8.1 Protocolo IP

Quando o IP foi padronizado, no início da década de 1980, foi especificado que para cada equipamento ligado à Internet deveria ser associado um único endereço IP. No caso dos roteadores, deve-se informar um endereço IP diferente para cada interface de rede. Dessa forma, fica claro que na Internet não existem dois ou mais equipamentos com o mesmo endereço IP.

Conforme já comentado, o endereço IP é composto de duas partes. A primeira identifica a rede em que um equipamento está conectado, enquanto a segunda identifica o próprio equipamento na rede. Dessa forma, foi criada a hierarquia de endereçamento de dois níveis. O campo do número de rede composto dos bits mais significativos foi chamado de prefixo de rede, já que essa parte identifica o número da rede. É importante lembrar que todos os equipamentos de uma rede compartilham o mesmo prefixo de rede, mas devem ter um único número que identifica o equipamento dentro da rede. Dessa forma, quaisquer dois equipamentos em diferentes redes devem ter prefixos de rede diferentes, embora possam ter a segunda parte do endereço IP igual.

No momento de instalação e ativação do endereço IP em um determinado equipamento, o sistema de configuração sempre solicitará os números que formam o endereço IP (endereço IP e máscara). Esse número IP tem a extensão de 4 bytes e deve ser único para cada computador da rede conforme comentado. Caso o administrador da rede desconheça as regras de funcionamento do

endereçamento, provavelmente os computadores não estabelecerão comunicação entre si.

### 8.1.1 Endereço IP

Para que os computadores possam ser distinguidos na rede, é necessário que cada um, independentemente do sistema operacional ou hardware utilizado, possua um número único, o qual (endereço) é aplicado em qualquer equipamento que use o modelo de referência TCP/IP. O endereço possui 4 bytes separados por três pontos. Um exemplo de endereço válido seria 140.204.100.200. A figura 8.1 apresenta uma rede com computadores interligados, cada um com seu respectivo endereço IP:

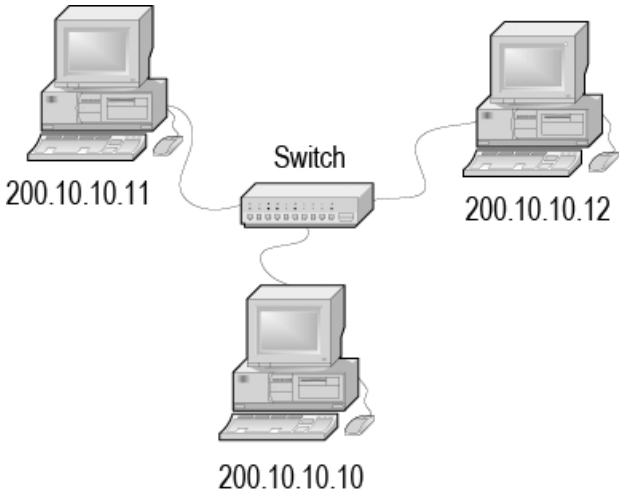



*Figura 8.1 – Rede IP.*

O endereço IP deve ser configurado no momento em que adicionamos a placa de rede ou instalamos o protocolo IP no sistema operacional. A figura 8.2 apresenta uma rede em que os equipamentos possuem endereços IP com parte igual, quando referente à rede, e parte diferente, quando referente à identificação do computador na sub-rede.

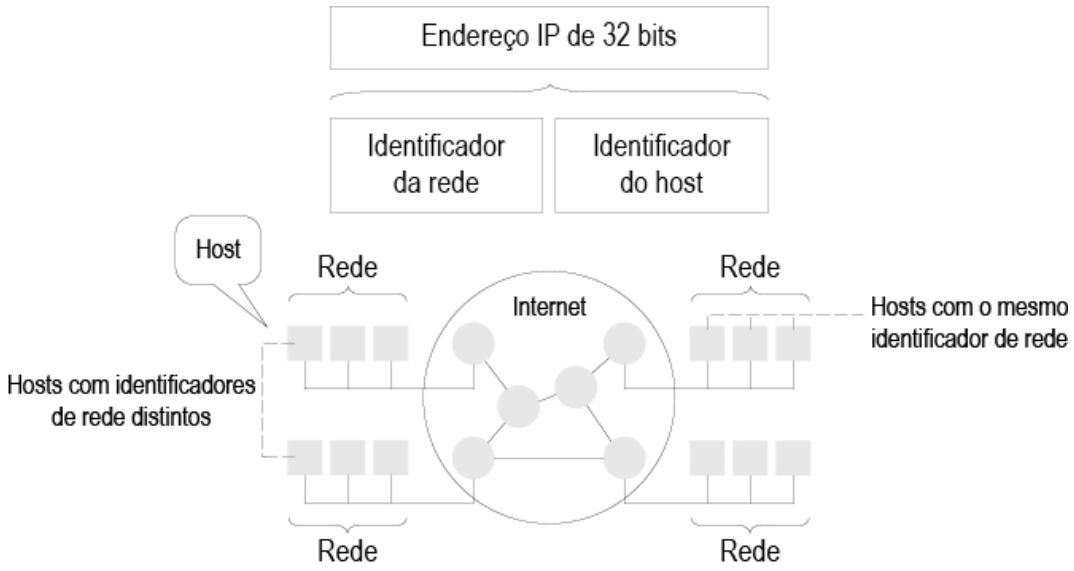



*Figura 8.2 – Rede com realce das partes do endereço IP.*

### 8.1.1.1 Representação do endereço IP

O endereço IP é representado por um número de 32 bits (4 bytes), como já comentado. Como se sabe, cada bit refere-se a um sinal elétrico ou tensão elétrica, podendo ser 0 ou 1 (no formato decimal), o que daria um total de 2 elevado a 32, ou seja, 4.294.967.296 (quatro bilhões duzentos e noventa e quatro milhões novecentos e sessenta e sete mil duzentos e noventa e seis) possíveis endereços IP. Caso tivéssemos que nos referir a endereços IP na sua forma binária, teríamos algo como o endereço IP do meu amigo é 11101111.11101010.10101010.10101010. Números como este não são amigáveis, assim, criou-se a notação chamada de *dot quad* ou ponto quadrante, na qual se divide o número de 32 bits em quatro grupos de 8 bits, representando-os como w.x.y.z., em que w, x, y e z são números decimais variando entre 0 e 255. A figura 8.3 apresenta um endereço IP no formato decimal convertido em binário:

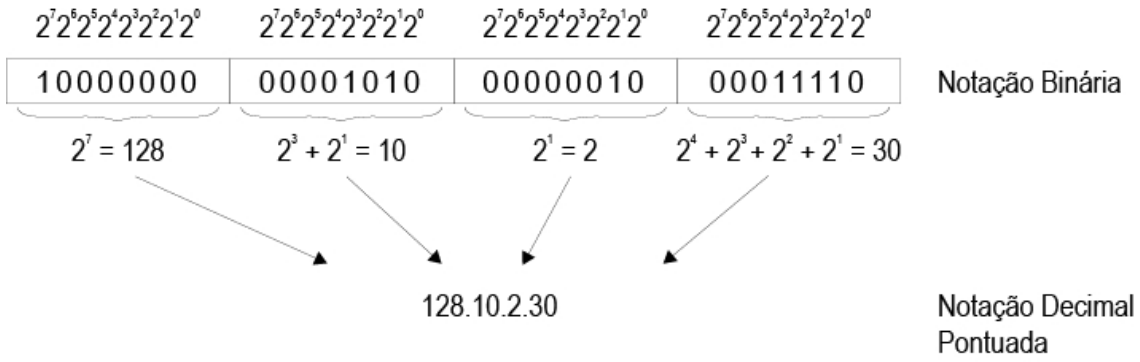



*Figura 8.3 – Endereço no formato binário e decimal.*

Por que de 0 a 255 ?

Com apenas 8 bits em cada parte do endereço (cada parte separada pelo ponto), pode-se conseguir, no máximo, 28 combinações, ou seja, 256 possíveis números. Um endereço IP inicia em 00000000, ou seja, 0 decimal e termina em 11111111, sendo 255 decimal ou FF hexadecimal. Como exemplo, podemos visualizar esses números utilizando a calculadora do Windows ou do Linux.

A seguir, comentaremos como os endereços IP foram divididos na época em que foram padronizados.

## 8.1.2 Classes de endereçamento

É importante observar que, ao configurar uma rede IP, devem-se levar em consideração algumas regras para formar o endereço que será utilizado. Voltamos a lembrar que uma parte do número IP representa a rede e a outra parte, o próprio computador. A seguir, apresentaremos o modo como, no início da utilização do protocolo IP, era representada a parte referente à rede e a parte referente aos hosts.

Na definição do protocolo IP (IPv4), foram estabelecidas cinco classes de endereços que receberam a identificação de A, B, C, D e E. A distribuição dos endereços ou blocos de endereços IP segue os padrões estabelecidos pela IANA, instituição responsável pela atribuição dos endereços a cada computador na Internet. A seguir, detalharemos cada uma das classes de rede definidas na especificação do protocolo IP.

### 8.1.2.1 Classe A

Os endereços classificados como pertencentes à classe A possuem o primeiro número (1o byte ou os 8 primeiros bits) do endereço entre 1 e 127, e os outros 3 bytes podem variar cada um deles entre 0 e 255. Para o protocolo de rede, o qual não conhece números decimais, um endereço é classe A quando o primeiro bit está setado sempre em 0. Os 24 bits restantes (3 bytes) significam que as redes classe A podem ter 2 elevado a 24 ou 16.777.216 computadores diferentes ligados a cada rede.

Como exemplo de endereços classe A, temos 70.35.22.14, 110.25.8.4 e 90.25.25.1. Dessa forma, identificamos a primeira falha da especificação inicial do protocolo IP, ou seja, nunca uma rede poderá ter tantos equipamentos de rede utilizando os diferentes endereços quanto estão disponíveis nessa classe. Assim, uma grande quantidade de endereços IPs foi desperdiçada. A figura 8.4 mostra como um endereço IP classe A é formado:

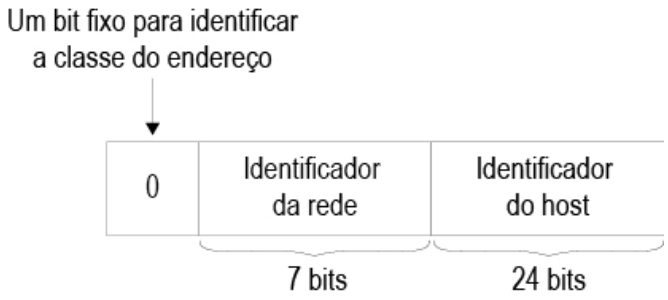



*Figura 8.4 – Representação do endereço classe A.*

É importante observar que os endereços classificados na classe A possuem o primeiro quadrante (8 bits) representando a rede, ou seja, deve ser igual em todos os computadores que compõem a rede local. Os outros três números representam o equipamento (host) e devem ser necessariamente diferentes.

Nenhum endereço de rede pertencente à classe A ou B está mais disponível, ou seja, todos os endereços já foram distribuídos a empresas usuárias da Internet. Somente existem endereços disponíveis para a classe C.

### 8.1.2.2 Classe B

Os endereços classificados como pertencentes à classe B possuem o primeiro quadrante (byte) com valores entre 128 e 191 e o segundo quadrante com valores entre 0 e 255. É possível endereçar até 16.384 diferentes redes. Cada rede pertencente à classe B pode oferecer 65.534 computadores conectados. Para chegarmos ao valor 65.534, fizemos a seguinte operação: [(2 elevado a 16)-2]. Decrescemos dois endereços, pois não existem equipamentos com todos os bits setados em 0 ou em 1 (255). Quando isso acontece, o endereço não se refere a um equipamento, mas a um endereço de rede ou *broadcast*, conforme veremos ainda neste capítulo.

Para o protocolo de rede, o qual não conhece números decimais, um endereço é classe B quando o primeiro bit está setado sempre em 1 e o segundo bit, sempre setado em 0. A figura 8.5 apresenta o formato de um endereço IP classe B:

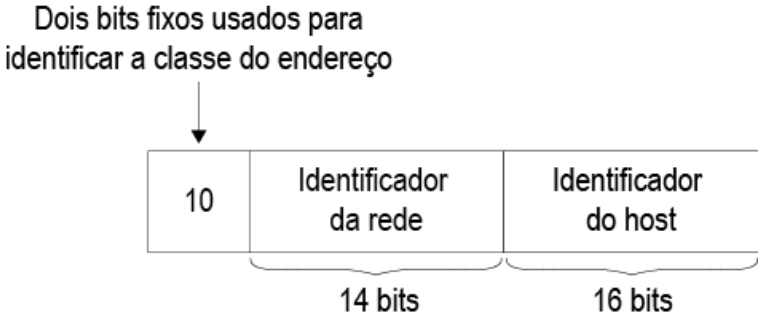



*Figura 8.5 – Representação do endereço classe B.*

Como exemplos de endereços pertencentes à classe B, temos 190.015.014.017, 130.025.008.004 ou 187.025.025.001. Dessa forma, identificamos a segunda falha da especificação inicial do protocolo IP, ou seja, nunca uma rede poderá ter tantos endereços diferentes de equipamentos quanto estão disponíveis nessa classe. Novamente, outra grande quantidade de endereços IP foi desperdiçada.

### 8.1.2.3 Classe C

As redes consideradas pequenas no entendimento da IANA têm os primeiros 24 bits definidos pelo comitê organizador, deixando apenas 8 bits para serem determinados pelos administradores da rede local. Essas redes podem ter, no máximo, 2 elevado a 8, ou

seja, 256 equipamentos conectados na rede. Os endereços IP das redes classe C têm o primeiro quadrante na faixa de 192 até 223.254.255.255.

Como o segundo e o terceiro quadrante podem ter valores entre 0 e 255, a IANA e seus representantes podem trabalhar com 24 bits para distribuir entre as redes classe C, havendo, então, potencialmente 2.097.152 possíveis redes classe C. Para o administrador da rede local, sobram os últimos 8 bits dos endereços IP para serem utilizados em equipamentos.

Para o protocolo de rede, o qual não conhece números decimais, um endereço é classe C quando o primeiro bit está setado sempre em 1, o segundo bit também sempre setado em 1 e o terceiro bit setado em 0.

Como exemplo de endereços classe C, temos o endereço 200.015.014.017, 221.025.008.04 ou 192.025.025.01. Nos endereços classe C, há um maior aproveitamento dos endereços destinados a equipamentos, visto que apenas endereços classe C ainda estão disponíveis na Internet. A figura 8.6 apresenta o formato de um endereço IP classe C:

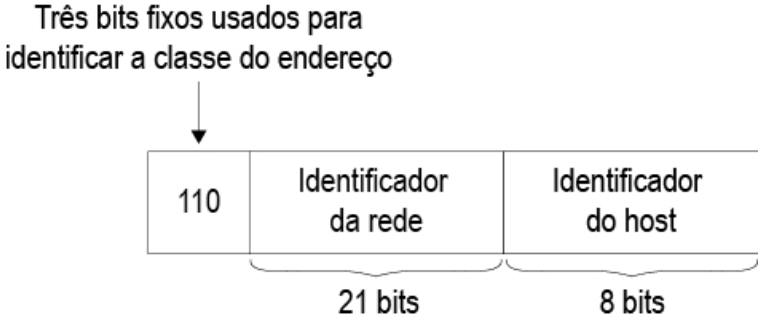



*Figura 8.6 – Representação do endereço classe C.*

A figura 8.7 apresentará a configuração de uma rede IP utilizando os endereços das três classes comentadas até o momento.

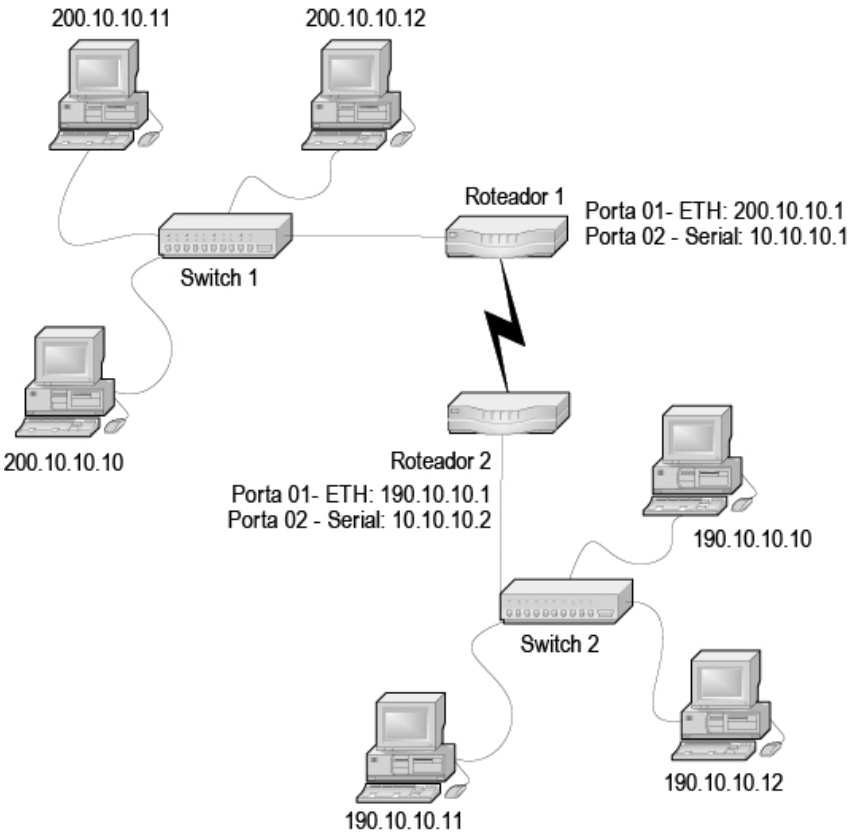



*Figura 8.7 – Rede WAN.*

A primeira rede possui endereços pertencentes à classe C, enquanto a segunda rede possui endereços pertencentes à classe B. Assim, quando precisamos interligar duas redes, devemos utilizar a figura de um roteador. Nesse exemplo, as portas do roteador estão configuradas com endereços pertencentes à classe A. É importante lembrar que, quando interligamos duas redes utilizando linhas telefônicas, elas formam uma rede WAN, assim os endereços dessa rede devem ser independentes das demais.

### 8.1.2.4 Classe D

Os endereços classificados como pertencente à classe D possuem o primeiro byte superior a 224 e variam até 239. Essa classe de endereços está reservada para criar agrupamentos de computadores para o uso em transmissões *multicast* . Endereços IP pertencentes à classe D permitem que um conjunto de computadores com o mesmo endereço IP classe D troque dados entre si.

O protocolo de rede não conhece números decimais. Para identificar um endereço classe D, deve-se ter como base os quatro primeiros bits do primeiro quadrante do endereço IP. Nessa classe de endereços, o primeiro, o segundo e o terceiro bit sempre ficam setados em 1 e o quarto bit fica setado em 0. Portanto, o número é conhecido como classe D quando for identificado que o endereço IP inicia com 3 bits igual a 1 (bits ligados) e o seguinte bit e igual a 0 (desligado). A figura 8.8 apresenta o formato de um endereço IP classe D:

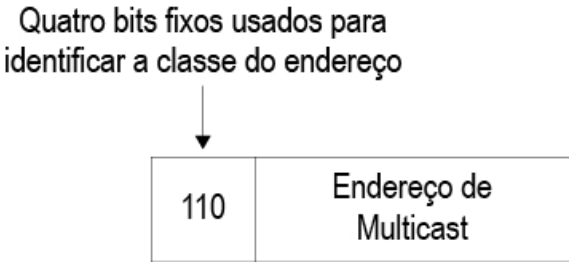



*Figura 8.8 – Representação do endereço classe D.*

A seguir, apresentaremos dois programas escritos em Java, que, utilizando sockets, permitem utilizar endereços classe D. O primeiro programa refere-se ao cliente e o segundo, ao servidor TCP/IP. Esses programas possuem como objetivo apresentar ao leitor uma forma prática de entender e utilizar endereços classe D.

Programa que deverá ser executado no cliente:

```
package redes;
/*Aplicação :
* Função : Criação de cliente que envia um Datagrama para o servidor especificado
* Data de criação: (27/04/04). */
import java.net.*;
import java.io.*;
public class ClienteTCP {
public static void main(String[] args) {
  String tLinha;
  MulticastSocket tServidor;
  byte[] tBuffer;
  InetAddress tEndereco;
  DatagramPacket tPacote;
  try {
    tServidor = new MulticastSocket(6000);
```

```
    tEndereco = InetAddress.getByName("231.0.0.1");
    tServidor.joinGroup(tEndereco);
    tBuffer = new byte[50];
    while (true) {
      tPacote = new DatagramPacket(tBuffer, tBuffer.length);
      tServidor.receive(tPacote);
      tLinha = new String(tPacote.getData());
      System.out.println(tLinha);
    }
  } catch (UnknownHostException e) {
      System.out.println("IP não encontrado.");
      e.printStackTrace();
  } catch (IOException e) {
      System.out.println("Erro na conexão.");
      e.printStackTrace();
    }
  }
}
```

## Programa que deverá ser executado no servidor:

```
package redes;
/* Aplicação :
 * Função    : Criação de um servidor de Multicast que fica enviando pacotes a cada 5
  segundos com o horário.
 * Data de criação: (27/04/04). */
import java.net.*;
import java.io.*;
import java.text.*;
import java.util.*;
class ServerTCP {
  public static void main(String[] args) {
  DatagramSocket tSocket;
  DatagramPacket tPacote;
  byte[] tBuffer;
  String tTexto;
  InetAddress tEndereco;
  DateFormat tFormat;
  tFormat = DateFormat.getDateTimeInstance(DateFormat.LONG, DateFormat.MEDIUM);
  try {
    tSocket = new DatagramSocket(6000);
    tEndereco = InetAddress.getByName("231.0.0.1");
    while (true) {
```

```
        tTexto = tFormat.format(new Date());
        tBuffer = new byte[tTexto.length()];
        tBuffer = tTexto.getBytes();
        try {
          Thread.currentThread().sleep(5000);
        } catch (InterruptedException e) {
        }
        System.out.println("Enviando...");
        tPacote = new DatagramPacket(tBuffer, tBuffer.length,
          tEndereco, 6000);
          tSocket.send(tPacote);
      }
    } catch (IOException e) {
      System.out.println(e);
      e.printStackTrace();
      }
    }
  }
```

Para maiores informações e detalhes sobre os conceitos de orientação a objetos em Java, consulte o livro *Programação Java com Ênfase em Orientação a Objetos*.

#### 8.1.2.5 Classe E

Os endereços classificados como pertencentes à classe E são reservados e foram definidos variando entre 240.0.0.0 e 255.0.0.0. Esses endereços não podem ser utilizados para endereçar os computadores de usuários em redes configuradas no modelo de referência TCP/IP.

A seguir, detalharemos os endereços IPs considerados reservados, endereços que não podem ser configurados em equipamentos IP.

### 8.1.3 Endereços reservados

Os endereços reservados ajudaram a diminuir ainda mais a quantidade de endereços IPs disponíveis na Internet. Quando se analisa a quantidade de combinações possíveis dos números IP em 32 bits, surge uma fascinação em relação aos possíveis 4 bilhões de computadores potencialmente ligados em rede. Como já comentamos, 4 bilhões de endereços IPs podem parecer muito, mas

a impressão não corresponde à realidade. A distribuição, de certa forma predatória, feita considerando o conceito das classes A, B e C, desperdiçou milhões de endereços IP que possivelmente nunca serão utilizados, a não ser que se alterem as regras dessa distribuição. Felizmente, isso aconteceu e abordaremos esse conceito ainda neste capítulo.

A seguir, comentaremos os endereços IPs considerados reservados pela IANA.

#### 8.1.3.1 Loopback address

Endereços IP que iniciam o primeiro byte com o valor 127 foram reservados para receber informações de retorno dos servidores, ou seja, uma mensagem de dados destinada a um servidor 127.x.x.x deverá retornar para o emitente.

Em nossas redes TCP/IP, a tradução literal seria endereço de retorno e, em nossas redes locais, esse endereço é constituído por 127.0.0.1. Todas as vezes que um computador emitir uma requisição a esse endereço, a resposta será dada pelo próprio emitente. Nesse caso, a requisição não passa da camada de rede para a camada de enlace. Ela simplesmente volta direto ao equipamento sem a utilização das camadas inferiores. Quando essa resposta não acontecer, isto indicará um problema de software ou de hardware no computador testado. Essa função é útil para efetuar testes e para otimizar a comunicação entre processos em um mesmo computador.

A utilização desse endereço como endereço reservado leva à perda de 16 milhões de endereços IP, pois um endereço da classe A, conforme já comentado, apresenta essas características.

#### 8.1.3.2 Rota-padrão

O endereço 0.0.0.0 é reservado para uso como a rota-padrão do computador. Todas as vezes que um destino for requisitado e o endereço não estiver presente na rede local (seu endereço IP pertence à outra rede), o protocolo procurará o endereço 0.0.0.0 e avaliará a rota configurada previamente para direcionar a requisição.

### 8.1.3.3 Endereço de broadcast

O endereço 255.255.255.255 é reservado para transmissões de pacotes em *broadcast*. Uma transmissão em *broadcast* indica para todos os computadores da rede local que a informação recebida deverá ser processada independentemente do seu endereço MAC ser ou não igual ao endereço MAC recebido do quadro Ethernet. O endereço MAC utilizado em transmissões *broadcast* é FF:FF:FF:FF:FF:FF.

### 8.1.3.4 Endereços IPs público e privado

A seguir, comentaremos alguns endereços IPs que foram reservados para utilização em redes locais, não sendo possível conectar uma rede à Internet com eles. É importante lembrar que esses endereços podem ser utilizados em redes locais, mas jamais um conjunto deles poderá ser utilizado na Internet. A RFC 1918 sugere um esquema de alocação de endereços IP nas redes privadas. A tabela 8.1 apresenta os endereços definidos na RFC 1918:

*Tabela 8.1 – Classes de endereços IP*

| Endereços IP não roteável | Início | Fim |
|---|---|---|
| Classe A | 10.0.0.0 | 10255255255 |
| Classe B | 172.16.0.0 | 172.31.255.255 |
| Classe C | 192.168.0.0 | 192.168.255.255 |

Qualquer administrador de Intranet ou Extranet pode utilizar esses endereços IP sem precisar pedir para a IANA, pois mesmo que os servidores com esses endereços IP estivessem ligados à Internet, isso não causaria problemas. Tal fato acontece em virtude de os roteadores estarem programados para ignorar pacotes de dados que tenham como endereço de destino ou de origem esses endereços IP, deixando de retransmiti-los, razão pela qual são chamados de endereços não roteáveis.

Muitos falam sobre uma provável segurança apresentada pelos

endereços IPs privados. A impressão de que os IPs privados conferem segurança é um tanto falsa, pois basta que o invasor domine o equipamento de borda (ex.: roteador de borda) e, pronto, ele pode entrar na rede privada por meio dessa máquina. A única malha de proteção é que ele não consegue invadir diretamente sem primeiro colocar uma rota de retorno, o que pode facilitar o controle e a organização da rede. Dessa forma, poderemos ter alguns benefícios de segurança.

Outro fato muito importante relacionado aos endereços privados é quanto a problemas de conectividade, supondo que um administrador de rede use, por exemplo, o endereço 47.160.3.0 (máscara 255.255.255.0 ou /24) na sua rede local para endereçar suas máquinas. Isso é um bloco de endereços IP válidos na Internet. Se fizermos o reverse DNS lookup com essa classe, identificaremos que essa rede pertence à Nortel Networks. Assim, se usarmos esse IP, o NAT (*Network Address Translation*) não conseguirá mascarar essa rede, simplesmente porque ela pertence à sua rede local (a própria rede local não mandaria nada para o gateway NAT). Consequentemente, você não conseguirá navegar em todos os sites da Nortel, mas, sem dúvida, conseguirá navegar em todos os outros sites da Internet sem problema.

A utilização de endereços privados em uma rede local parece não ser um empecilho, desde que não estejamos usando um endereço de um site muito acessado. A seguir, detalharemos os problemas que podem ocorrer caso essa regra seja infringida.

Continuando o exemplo, imaginamos, então, que meu endereço de rede LAN seja 47.160.3.155/24. Quando o pacote IP for montado, o endereço IP origem e o endereço IP destino pertencerão à mesma rede local (47.160.3.0). Logo, o equipamento não enviará esse pacote para o roteador (*default gateway*), que, no nosso caso, seria o equipamento com o NAT. Dessa forma, o usuário receberia a mensagem de página não encontrada, mesmo que a comunicação entre a rede LAN e a Internet estivesse funcionando adequadamente.

### 8.1.4 Máscara de rede

A máscara de rede é chamada, mais propriamente, de máscara de sub-rede. Entretanto, normalmente é referida como máscara de rede, pois determina o comportamento do endereço IP quanto à parte que se refere à rede e qual parte se refere ao equipamento dentro dela.

A máscara de rede é representada na mesma disposição do endereço IP. Os bytes que possuem todos os bits ligados (FF hexadecimal ou 255 em decimal) indicam qual parte do endereço IP refere-se à rede e os bytes que possuem os bits desligados (0 em decimal ou hexadecimal) indicam a parte do endereço IP que se refere à identificação do equipamento dentro da rede. Ainda existem os casos em que a máscara de sub-rede possui quadrantes, e uma parte deles possui bits ligados e a outra parte, *bits* desligados. Trataremos dessas máscaras de sub-rede no tópico CIDR (*Classless Inter-Domain Routing*).

Quando o administrador de rede definir que sua Intranet deverá ter endereços classe A, ele deverá, em todas as máquinas, escolher o endereço de rede 10.0.0.0 e configurar os endereços, também em todas as máquinas, de 10.0.0.1 a 10.0.0.254, por exemplo, com a máscara 255.0.0.0. Se escolher um endereço de rede da classe B (172.16.0.0), deverá utilizar a máscara 255.255.0.0. Finalmente, caso escolha um endereço classe C, deverá utilizar a máscara 255.255.255.0.

Existem dois fatores importantes a serem lembrados sobre a máscara de rede. O primeiro se refere à interpretação. A máscara de rede afeta somente a interpretação local de números IP (de modo que “local” significa “no próprio segmento da rede”). O segundo se refere à sua utilização. A máscara de rede não é um número IP, pois é utilizada para definir qual parte do endereço IP refere-se à parte de rede. Caso o administrador não respeite essas regras, a rede, com certeza, não funcionará corretamente.

### 8.1.5 CIDR (Classless Inter-Domain Routing)

O CIDR é a tendência em roteamento e tem sido bastante utilizada

por todos os administradores de rede. Esse conceito foi apresentado em 1993 para retardar o encolhimento da quantidade de endereços IP até a chegada da próxima geração do IP (IP versão 6, também conhecido como IPng ou IP *next generation*). A especificação CIDR (*Classless Inter-Domain Routing* – Roteamento Interdomínios sem Classe) permite o uso maximizado do limitado espaço de endereçamento na implementação do IP versão 4 (IPv4).

O CIDR foi especificado na RFC 1519 e tem como principal objetivo evitar o desperdício de endereços IP. Sua missão é atribuir endereços IP na forma de blocos contíguos da classe C, distribuídos de modo hierárquico. Assim, consegue-se atender a diferentes necessidades sem desperdiçar milhares de endereços. Vejamos um exemplo:

- Se uma empresa precisar de 500 endereços IPs para equipamentos, ela receberá uma rede da classe C com máscara 255.255.252.0 (/22), ou seja, 2 elevado a 10 é igual a 512. O /22 significa que os 22 bits mais significativos se referem à rede, e ainda sobram 10 bits para endereçamento de equipamentos. Caso utilizássemos a estrutura proposta anteriormente (máscara do tipo 255.255.0.0), estaríamos fornecendo 2 elevado a 16 bits, o que corresponderia a, mais precisamente, 65.534 endereços. Estaríamos desperdiçando milhares de endereços IPs. A Internet está endereçada dessa forma.

Na RFC 1519, também é apresentada uma divisão de endereços IPs em quatro zonas, conforme mostra a tabela 8.2, com o intuito de reduzir o tamanho das tabelas de roteamento. É em virtude disso que, no Brasil, temos endereços IPs iniciando em 200.

A especificação do CIDR inovou no sentido de as redes serem referenciadas usando prefixos em vez das tradicionais classes A, B e C. Por exemplo, um bloco da classe A passa a ser representado pelo prefixo /8 em vez do 255.0.0.0. Na tabela 8.3, relacionaremos alguns prefixos utilizados em redes TCP/IP que seguem a especificação CIDR.

*Tabela 8.2 – Faixas de endereços válidos na Internet*

| Região | Início | Fim |
|---|---|---|
| Europa | 194.0.0.0 | 195.255.255.255 |
| América do Norte | 198.0.0.0 | 199.255.255.255 |
| Américas Central e do Sul | 200.0.0.0 | 201.255.255.255 |
| Ásia e região do Pacífico | 202.0.0.0 | 203.255.255.255 |

*Tabela 8.3 – Prefixos de rede*

| Prefixo CIDR | Equivalente à classe C | Quantidade de hosts |
|---|---|---|
| /27 | 1/8 (um oitavo) da classe C | 32 hosts |
| /26 | 1/4 (um quarto) da classe C | 64 hosts |
| /25 | 1/2 (um meio) da classe C | 128 hosts |
| /24 | 1 classe C | 256 hosts |
| /23 | 2 classes C | 512 hosts |
| /22 | 4 classes C | 1.024 hosts |
| /21 | 8 classes C | 2.048 hosts |

### 8.1.5.1 Funcionamento do CIDR

Apesar de as classificações IP das classes A até a classe D ainda estarem em uso no mundo das redes, esses termos são considerados obsoletos. Com o intuito de manter a situação clara, continuaremos a usá-los para explicar como o CIDR funciona e como poderemos implementá-lo. Com o CIDR vem o conceito de VLSM (*Variable Lenght Subnet Masking* – Máscara de Sub-rede com Comprimento Variável). Note que uma vez que estamos lidando com 32 bits, podemos contar o número de bits com valor igual a 1 a partir da esquerda para direita e usar isso como uma abreviação para endereçamento. A tabela 8.4 apresenta uma relação entre as máscaras de rede no conceito CIDR e a sua respectiva abreviação

em bits:

*Tabela 8.4 – Abreviação entre o endereço IP e sua máscara no formato CIDR*

| Notação de máscara de rede | CIDR |
|---|---|
| 255.255.0.0 | /16 |
| 255.255.128.0 | /17 |
| 255.255.252.0 | /22 |
| 255.255.255.0 | /24 |
| 255.255.255.128 | /25 |
| 255.255.255.192 | /26 |
| 255.255.255.224 | /27 |
| 255.255.255.240 | /28 |

A seguir, apresentaremos uma relação entre o CIDR e as classes de endereçamentos apresentadas no início deste capítulo e que se referem às classes A, B e C. O objetivo da tabela 8.5 é tornar claro o funcionamento do CIDR em relação à teoria comentada sobre as máscaras de rede.

*Tabela 8.5 – Relação entre máscaras, notação CIDR e seu correspondente*

| Máscara | A | B | C | Quantidade | Rede | Broadcast |
|---|---|---|---|---|---|---|
| .0 | /8 | /16 | /24 | 1 | 0 | 255 |
| .128 | /9 | /17 | /25 | 2 | 0 – 128 | 127 – 255 |
| .192 | /10 | /18 | /26 | 4 | 0 – 64 – 128 – 192 | 63 – 127 – 191 – 255 |
| .224 | /11 | /19 | /27 | 8 | 0 – 32–64–96–128–160–192–224 | 31 – 63 – 95 – 127 – 159 – 191 – 223 – 255 |

| Máscara | A | B | C | Quantidade | Rede | Broadcast |
|---|---|---|---|---|---|---|
| .240 | /12 | /20 | /28 | 16 | 0 – 16 – 32 – 48 – 64 – 80 – 96 – 112 – 128 – 144 – 160 – 176 – 192 – 208 – 224 – 240 | 15 – 31 – 47 – 63 – 79 – 95 – 111 – 127 – 143 – 159 – 175 – 191 – 207 – 223 – 239 – 255 |
| .248 | /13 | /21 | /29 | 32 | 0 – 8 – 16 – 24 – 32 – ...176 – 184 ... 200 ...248 | 7 – 15 – 23 – 31 ...175 – 183...199...207...255 |
| .252 | /14 | /22 | /30 | 64 | 0 – 4 – 8 –12 – 16 ...248 252 | 3 – 7 – 11 – 15... 251 – 255 |
| .254 | /15 | /23 | --- | 128 | | |

A primeira linha da tabela 8.5 indica que quando se tem uma máscara de rede final 0, ela pode ser abreviada para um endereço de classe A como /8 (255.0.0.0); como /16 (255.255.0.0), para a classe B; e /24 (255.255.255.0), para a classe C. No caso da classe C, teríamos apenas uma rede, que seria identificada pelo número 0 no final do endereço IP (200.100.100.0).

A segunda linha indica que quando se tem uma máscara de rede final 128, ela pode ser abreviada para um endereço de classe A como /9 (255.128.0.0); como /17 (255.255.128.0), para a classe B; e /25 (255.255.255.128), para a classe C. No caso da classe C, teríamos duas redes, que seriam identificadas pelos números 0 e 128 no final do endereço IP (200.100.100.0 e 200.100.100.128). O valor 128 refere-se ao primeiro bit do quarto quadrante ligado.

Conforme comentamos, a máscara possui todos os bits dos quadrantes referentes à rede ligados, mas isso aconteceria na situação comentada anteriormente (classes A, B e demais). Na especificação do CIDR, apenas parte dos bits referentes à rede ficará ligada.

A terceira linha indica que quando se tem uma máscara de rede final 224, ela pode ser abreviada para um endereço de classe A como /11 (255.224.0.0); como /19 (255.255.224.0), para a classe B;

e /27 (255.255.255.224), para a classe C. Nesse caso, teríamos quatro redes, que seriam identificadas pelos números 0, 64, 128 e 192 no final do endereço IP (200.100.100.0, 200.100.100.64, 200.100.100.128 e 200.100.100.192).

A quarta linha indica que quando se tem uma máscara de rede final 192, ela pode ser abreviada para um endereço de classe A como /10 (255.192.0.0); como /18 (255.255.192.0), para a classe B; e /26 (255.255.255.192), para a classe C. Nesse caso, teríamos oito novas redes, que seriam identificadas pelos números 0, 32, 64, 96, 128, 160, 192 e 224 no final do endereço IP (200.100.100.0, 200.100.100.32, 200.100.100.64, 200.100.100.96 200.100.100.128, 200.100.100.160, 200.100.100.192 e 200.100.100.224).

A tabela 8.5 ainda contém a quantidade de redes para cada máscara, o endereço de rede de cada nova rede criada e o seu respectivo endereço de *broadcast*.

### 8.1.6 Exemplos do uso da especificação CIDR

Em uma tradicional rede configurada com classe C, sempre teremos apenas uma sub-rede-padrão com oito bits disponíveis para endereçar equipamentos de rede e 24 bits para endereçar diferentes tipos de redes. Nesse caso, a máscara-padrão seria 255.255.255.0/24, ou seja, do primeiro ao terceiro quadrante, todos os bits são iguais a 1; no quarto quadrante, todos os bits são iguais a 0. Para tradicionais redes configuradas nas classes A e B, teríamos a seguinte situação: 255.0.0.0 e 255.255.0.0, respectivamente. A seguir, apresentaremos um exemplo do uso mais otimizado do CIDR.

Uma empresa recebeu um endereço de rede classe C completo com o objetivo de comunicar suas 160 máquinas. Com esse conjunto de endereços, a empresa poderia endereçar 256 equipamentos, dos quais dois sempre serão reservados a endereços de rede e de *broadcast* (final 0 - 255.255.255.0 e final 255 - 255.255.255.255), restando, então, 254 para outros equipamentos da rede. Mesmo que precise apenas de 160 endereços, essa empresa estará recebendo 256, desperdiçando, assim, 96

endereços. Quando usamos o conceito definido pelo CIDR, podemos trabalhar esse conjunto de endereços garantindo um formato otimizado e, ainda, distribuí-los de forma mais racional. O uso do endereço sem CIDR ocasionaria um desperdício ainda superior àquele que estamos tendo com o CIDR.

Conforme já apresentado, a parte do endereço IP equivalente à rede é aquela em que, na máscara, todos os bits do quadrante são iguais a 1. Isso significa que um endereço classe C se parece em notação binária com 11111111.11111111.11111111.00000000 e com a notação decimal com 255.255.255.0 (128 + 64 + 32 + 16 + 8 + 4 + 2 + 1 nas três primeiras posições e 0 na última).

Assim, temos um endereço de rede classe C igual a 192.168.1.0/24, disponível para uso. Em nosso exemplo, temos dois escritórios situados em Curitiba e São Paulo com aproximadamente 80 equipamentos cada um. Em razão de esses dois escritórios estarem localizados em cidades diferentes e ser necessário o uso de um roteador, não poderíamos utilizar um esquema de endereços IPs simples como o apresentado nas classes A, B ou C.

Essas duas redes não se encontram porque um computador, para encontrar outro em uma rede, na operação lógica & (E) entre o endereço IP e a máscara de rede dos computadores emissor e receptor, necessita que os resultados sejam iguais. Assim, como a instituição responsável nos forneceu um endereço de rede classe C 192.168.1.0/24, teremos que, a partir dele, criar o ambiente adequado para estabelecer a comunicação entre os dois escritórios.

É importante lembrar que o roteador é um equipamento que possui dois ou mais endereços de rede, pelo menos um na rede local e um ou mais em outras redes. Esse roteador envia qualquer comunicação que não seja para a rede local por meio de seus outros dispositivos de comunicações, dependendo da informação armazenada em sua tabela de roteamento.

Para esse exemplo, precisaríamos de dois endereços de rede classe C, dos quais seriam utilizados 80 para a rede de Curitiba e 80 para a rede de São Paulo, assim somando 160 endereços dos 256 disponíveis. Dessa forma, estaríamos novamente desperdiçando

endereços IP, ainda que em menor escala.

Para otimizarmos a distribuição de endereços IP, estenderemos nossa máscara de rede em mais um bit, ou seja, em vez de 24 bits utilizados para máscara, utilizaremos 25 bits. Essa extensão de um bit para a máscara nos fornecerá duas novas redes ao contrário da situação anterior, na qual tínhamos apenas uma: a rede 192.168.1.0. Isso muda nossa máscara de rede para 255.255.255.128/25, pois o primeiro bit do quarto quadrante ficará ligado e possui valor igual a 128. Ambas as redes de Curitiba e São Paulo deverão utilizar a mesma máscara de rede em todos os equipamentos configurados na rede.

Com a máscara 255.255.255.128/25, criamos duas redes onde havia somente uma. A primeira rede ficará com o endereço IP igual a 192.168.1.0; a segunda rede, com endereço IP igual a 192.168.1.128. É importante lembrar que cada rede deve ter seu próprio endereço de *broadcast*, que, nesse exemplo, seriam 192.168.1.127 e 192.168.1.255 respectivamente. Além disso, em cada nova rede, teremos um roteador conectado à rede LAN e, por boa prática de configuração de rede, devemos assinalar os endereços 192.168.1.1 e 192.168.1.129, respectivamente, para cada porta Ethernet.

Com CIDR, podemos criar tantas redes quantas forem necessárias bastando apenas mudar o formato da máscara de rede, variando de 8 a 30. Atualmente, na Internet, é esse o modelo utilizado. O CIDR também pode oferecer uma forma para isolar departamentos em grandes organizações com o objetivo de melhorar a segurança e diminuir o tráfego de *broadcasts* entre os segmentos de rede.

### 8.1.6.1 Endereço IP especial

Além das faixas de IPs reservados, existem também alguns endereços especiais que só podem ser atribuídos a máquinas destinadas para fins específicos. Esses endereços são default gateway (conhecido como endereço do roteador), endereço de rede e endereço de *broadcast*, ambos comentados anteriormente. Convencionou-se que o primeiro número IP da Intranet seria o

endereço do roteador, ou seja, o endereço da primeira interface do roteador. Como exemplo, temos uma rede classe C com o endereço de rede igual a 192.170.2.0 e máscara 255.255.255.0. O endereço 192.170.2.0 fica reservado para descrever a rede da Intranet, o endereço 192.170.2.255, para o endereço de *broadcast*, e o endereço 192.170.2.1, para a primeira interface de rede do roteador. Nesse ponto, podemos entender o porquê de termos apenas 253 endereços disponíveis para endereçamento de equipamentos.

### 8.1.6.2 Máscara de rede

Quando instalamos ou configuramos o TCP/IP em um computador, independentemente do seu sistema operacional, dois parâmetros são obrigatórios: o primeiro é o endereço IP visto anteriormente e o segundo se refere à máscara de sub-rede (*Subnet Mask*). O endereço do roteador é opcional, mas passa a ser necessário no caso de transporte de pacotes para outras redes diferentes da LAN.

O parâmetro máscara de sub-rede serve para definir o funcionamento da classe do endereço. Essa afirmação parece confusa, porém é possível destacar: quando o endereço é classe A (primeiro byte entre 1 e 127), o parâmetro máscara de sub-rede é 255.0.0.0 por padrão; quando o endereço é classe B, a máscara-padrão é 255.255.0.0; e quando o endereço é classe C, a máscara é 255.255.255.0. Baseando-se nessa situação anterior, podemos definir se duas máquinas estão ou não na mesma rede.

Podemos supostamente atribuir o endereço IP 10.10.0.50 e a máscara de rede 255.0.0.0 ao computador A e 10.10.0.51 e a máscara 255.255.0.0 ao computador B. Quando o computador A necessitar de algum recurso do computador B, gerará uma requisição para este. Nesse momento, o protocolo de rede deverá definir se o endereço IP destino pertence ou não à rede local. Caso pertença, os pacotes IP serão enviados ao computador local; do contrário, os pacotes serão enviados ao roteador para que ele encontre o destino solicitado. Dessa afirmação, surge a seguinte dúvida: como o computador origem identificará se o computador destino pertence ou não à mesma rede? Uma vez que os computadores não entendem os números decimais quando

precisam tomar alguma decisão, para decidir essa questão, o computador origem realiza uma operação lógica entre os endereços IP origem e destino. A seguir, apresentaremos a operação lógica.

Endereço IP origem:

Decimal – 10.10.0.50

Binário – 00001010.00001010.00000000.00110010

Endereço IP destino:

Decimal – 10.10.0.51

Binário – 00001010.00001010.00000000.00110011

Uma vez convertidos os endereços IPs de decimal em binário, realizaremos o & (e) lógico entre os endereços IPs e a máscara de sub-rede.

*Tabela 8.6 – Endereço origem*

| **IP** | **10.10.0.50** | - | **00001010.00001010.00000000.00110011** | | | |
|---|---|---|---|---|---|---|
| Máscara | 255.0.0.0 | - | 11111111.00000000.00000000.00000000 | | | |
| Resultado binário | | | 00001010.00000000.00000000.00000000 | | | |
| Endereço de rede | | | 10 | .0 | .0 | .0 |
| Endereço de broadcast | | | 10 | .255 | .255 | .255 |

*Tabela 8.7 – Endereço destino*

| **IP** | **10.10.0.51** | - | **00001010.00001010.00000000.00110010** | | | |
|---|---|---|---|---|---|---|
| Máscara | 255.255.0.0 | - | 11111111.11111111.00000000.00000000 | | | |
| Resultado binário | | | 00001010.00001010.00000000.00000000 | | | |
| Endereço de rede | | | 10 | .10 | .0 | .0 |
| Endereço de broadcast | | | 10 | .10 | .255 | .255 |

Como podemos verificar nas tabelas 8.6 e 8.7, os endereços de

rede obtidos pela operação lógica entre o endereço IP origem e sua máscara (IP: 10.0.0.0; máscara: 255.0.0.0) e o endereço IP destino e sua máscara (IP: 10.10.0.0; máscara: 255.255.0.0) são diferentes, dessa forma o computador origem enviará esse pacote diretamente para o roteador. É importante observar que, nessa situação, o pacote IP será enviado diretamente ao roteador. Porém, para que essa transmissão ocorra com sucesso, o protocolo na máquina origem deverá substituir, no quadro Ethernet, o endereço MAC do equipamento destino pelo endereço MAC do roteador.

Desse exemplo, concluímos que caso o endereço de máscara não seja corretamente atribuído aos computadores, a rede não funcionará corretamente. Todos os computadores pertencentes à rede local devem possuir a mesma máscara de rede sob pena de ficarem isolados.

Até o momento, abordamos apenas as máscaras de rede que seguem o padrão tradicional especificado com o IPv4, que são 255.0.0.0, 255.255.0.0 e 255.255.255.0. No próximo tópico, apresentaremos as máscaras de sub-rede efetivamente utilizadas na Internet. As apresentadas anteriormente podem ser utilizadas em Intranets ou Extranets.

### 8.1.6.3 Máscara de sub-rede utilizada pela Internet

Conforme apresentado, todos os computadores devem possuir a mesma máscara de rede e a parte que corresponde à rede (números decimais) igual em todos os equipamentos (computadores e roteadores). Assim, o endereço de rede 10.10.0.0 é diferente do endereço de rede 10.11.0.0, caso ambos sejam configurados com a máscara 255.255.0.0. Nesse caso, a máscara de rede pode até ser a mesma, mas depois da operação lógica, o resultado será diferente (rede 10.10.0.0 é diferente da rede 10.11.0.0), fazendo que o computador emissor envie seus pacotes para o roteador.

Quando alguma empresa solicita uma range de endereços IP à IANA (representada no Brasil pela Fapesp), esta fornece a range, por exemplo: 201.200.171.128 a 201.200.171.192 e, junto, uma máscara de sub-rede. A seguir, apresentaremos um exemplo de

utilização de máscara de sub-rede.

Imaginemos uma empresa configurada na forma tradicional de endereços IP, utilizando ainda o conceito de classes. Para que ela possa dividir sua rede utilizando um roteador e ainda consiga que ambos os segmentos possam acessar a Internet, precisará utilizar dois grupos de endereços IPs diferentes ou poderá utilizar uma máscara de sub-rede para realizar esse objetivo. Na figura 8.9, podemos observar que a empresa FACE possui um endereço de rede 200.220.171.0, registrado na Internet, porém ela possui dois segmentos de rede, e os computadores nos dois segmentos precisam acessar a Internet.

Como a empresa FACE possui apenas uma faixa de endereços, poderíamos apenas ligar um segmento da rede à Internet. Entretanto podemos utilizar o conceito de máscara de sub-rede e configurar todas as máquinas para que estas, apesar de estarem aparentemente com um endereço IP pertencente à mesma rede, apresentem comportamento diferente do anteriormente utilizado.

O exemplo a seguir ilustra a utilização dos seguintes endereços IPs:

IP: 200.220.171.135 Máscara: 255.255.255.0

IP: 200.220.171.10 Máscara: 255.255.255.0

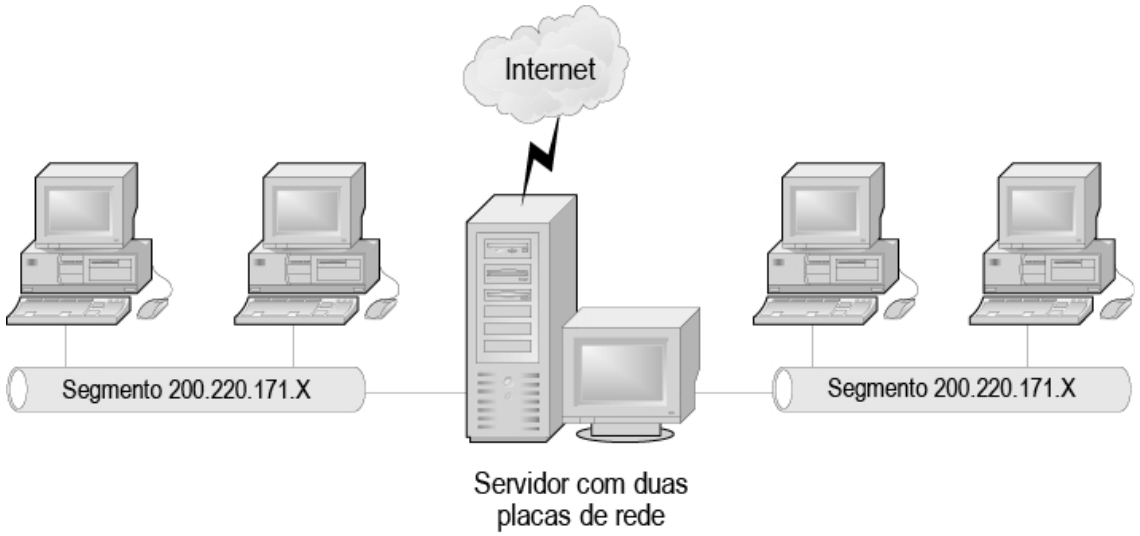



*Figura 8.9 – Servidor com duas placas de rede.*

Nesse caso, o computador configurado com o endereço IP 200.220.171.135 com a máscara 255.255.255.0 será classificado como classe C e estará na mesma rede do endereço IP 200.220.171.10.

Caso consideremos que esses computadores sejam separados nos dois segmentos citados no exemplo, eles não conseguiriam conversar entre si, pois estão logicamente na mesma rede. Para resolvermos esse problema, podemos utilizar a máscara 255.255.255.240 em vez da 255.255.255.0.

Com a máscara 255.255.255.0, o modelo de referência TCP/IP entende que o byte do quarto quadrante será utilizado para representar os computadores. No entanto, quando utilizamos .240, modificamos o significado, informando que apenas uma parte do quarto quadrante (últimos quatro bits menos significativos) será considerada para diferenciar computadores. Nesse momento, nosso exemplo passaria a ser:

IP: 200.220.171.135 Máscara: 255.255.255.240

IP: 200.220.171.10 Máscara: 255.255.255.240

Nesse exemplo, os três primeiros bytes mais a metade do quarto byte do último quadrante representam a rede e a segunda metade do quarto byte (quatro primeiros bits) representa os equipamentos. A tabela 8.8 apresenta o decimal 135, convertido em formato binário.

Em seguida, devemos converter o decimal 240 em seu formato binário. A tabela 8.9 apresenta o decimal 240 no formato binário.

Quando temos uma máscara no formato 255.255.255.240, estamos informando que os quatro primeiros bits que se referem à rede determinarão a que rede esse endereço pertence. A seguir, analisaremos os valores apresentados na tabela 8.9.

*Tabela 8.8 – Procedimento para a conversão de decimal em binário*

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | 2^7 | 2^6 | 2^5 | 2^4 | 2^3 | 2^2 | 2^1 | 2^0 |
| | | 128 | 64 | 32 | 16 | 8 | 4 | 2 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 135 | | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 |
| 135 | = | 128 | | | | | + 4 | + 2 | + 1 |
| | | Total | 128 | | | Total | 7 | | |

*Tabela 8.9 – Valor da máscara convertido em binário*

| | | 2^7 | 2^6 | 2^5 | 2^4 | 2^3 | 2^2 | 2^1 | 2^0 |
|---|---|---|---|---|---|---|---|---|---|
| | | | 128 | 64 | 32 | 16 | 8 | 4 | 2 |
| | | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 |
| 240 | = | 128 | + 64 | + 32 | + 16 | | | | |

Convertendo para decimal os quatro primeiros bits mais significativos, representados por 1 0 0 0, e os quatro últimos bits menos significativos, representados por 0 1 1 1 do decimal 135, teremos os valores decimais 128 e 7. Somando esses números, obtém-se o decimal 135. Na sequência, devemos definir o que efetivamente no endereço representa a rede e o que representa o nó. No endereço IP 200.220.171.135, com a máscara 255.255.255.240, o endereço 200.220.171.128 representa a rede e o endereço 200.220.171.135 é o sétimo equipamento dessa rede.

Assim, além de o segmento de rede possuir um computador configurado com o endereço 200.220.171.135, poderão também fazer parte desse segmento os computadores 200.220.171.136, 200.220.171.137 até 200.220.171.142, pois o endereço 200.220.171.143 refere-se ao endereço de *broadcast* e o endereço 200.220.171.144 já representa a próxima rede, ou seja, um novo segmento (Figura 8.10).

É importante lembrar que quando utilizamos a máscara 255.255.255.240, não podemos, por exemplo, utilizar no mesmo segmento endereços IPs 200.220.171.135 e 200.220.171.200, por exemplo. Com essa máscara, tais endereços aparentemente pertencentes ao mesmo segmento, depois da operação lógica entre

o endereço e a máscara definida, resultariam em endereços de rede diferentes. A seguir, demonstraremos por que esses endereços não são compatíveis. A tabela 8.8 converte o decimal 135 em binário e a tabela 8.10 converte o decimal 200 em binário.

Como já falamos, os 4 primeiros bits caracterizam a rede e, para o endereço 200, a rede seria .192 (128 + 64). Assim, o endereço 200.220.171.135 possui como endereço de rede o endereço 200.220.171.128. O endereço IP 200.220.171.200, por sua vez, possui o endereço de rede 200.220.171.192.

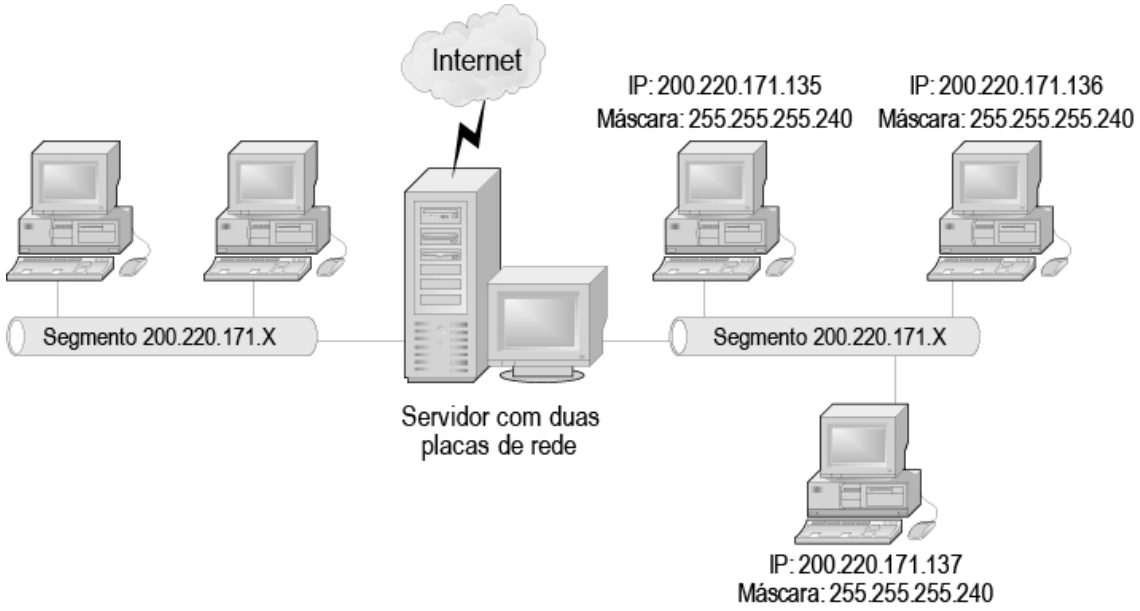



*Figura 8.10 – Servidor com duas placas de rede.*

*Tabela 8.10 – Conversão de decimal em valor binário*

| | | 2^7 | 2^6 | 2^5 | 2^4 | 2^3 | 2^2 | 2^1 | 2^0 |
|---|---|---|---|---|---|---|---|---|---|
| | | | 128 | 64 | 32 | 16 | 8 | 4 | 2 |
| 200 | | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 0 |
| 200 | = | 128 | + 64 | | | + 8 | | | |

Nas tabelas 8.8 e 8.10, percebe-se que os endereços IPs 200.220.171.135 e 200.220.171.200, depois da conversão em formato binário, produzem uma sequência de bits (mais

significativos) diferentes na parte que chamamos de rede (primeiros 28 bits). Dessa forma, tais computadores não conversam entre si, a não ser que exista um roteador configurado entre eles.

Quando utilizamos uma máscara 255.255.255.240, criamos até 16 combinações diferentes de novas sub-redes, as quais estão apresentadas na tabela 8.11:

*Tabela 8.11 – Redes criadas com a máscara final 240*

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 0000 (00) | 0001 (16) | 0010 (32) | 0011 (48) | 0100 (64) | 0101 (80) | 0110 (96) | 0111(112) |
| 1000(128) | 1001(144) | 1010(160) | 1011(176) | 1100(192) | 1101(208) | 1110(224) | 1111(240) |

As 16 combinações permitem que sejam criadas até 16 novas redes. É importante observar que as combinações com todos os bits ligados (todos 1) e todos os bits desligados (todos 0) não são permitidas conforme a norma RFC 950 da IANA. É importante lembrar também que, em uma prova de certificação, caso se questione a possibilidade de subdividir uma rede classe C em duas sub-redes, objetivamente, a resposta é não devido à norma da IANA, mesmo que na prática a divisão funcione perfeitamente.

A tabela 8.12 resume todas as máscaras possíveis, oferecendo todas as informações necessárias para o administrador de rede decidir sobre as suas necessidades:

*Tabela 8.12 – Tabela completa de sub-redes*

| **Nº de sub-redes** | **Máscara de sub-rede** | **Nº da rede** | **Endereço roteamento** | **Endereço de broadcast** | **Nº restante de IP** |
|---|---|---|---|---|---|
| 1 | 255.255.255.0 | w.x.y.0 | w.x.y.1 | w.x.y.255 | 253 |
| 2 | 255.255.255.128 | w.x.y.0 | w.x.y.1 | w.x.y.127 | 125 |
| | 255.255.255.128 | w.x.y.128 | w.x.y.129 | w.x.y.155 | 125 |
| 4 | 255.255.255.192 | w.x.y.0 | w.x.y.1 | w.x.y.63 | 61 |
| | | | | | |

| Nº de sub-redes | Máscara de sub-rede | Nº da rede | Endereço roteamento | Endereço de broadcast | Nº restante de IP |
|---|---|---|---|---|---|
| | 255.255.255.192 | w.x.y.64 | w.x.y.65 | w.x.y.127 | 61 |
| | 255.255.255.192 | w.x.y.128 | w.x.y.129 | w.x.y.191 | 61 |
| | 255.255.255.192 | w.x.y.192 | w.x.y.193 | w.x.y.255 | 61 |
| 8 | 255.255.255.224 | w.x.y.0 | w.x.y.1 | w.x.y.31 | 29 |
| | 255.255.255.224 | w.x.y.32 | w.x.y.33 | w.x.y.63 | 29 |
| | 255.255.255.224 | w.x.y.64 | w.x.y.65 | w.x.y.95 | 29 |
| | 255.255.255.224 | w.x.y.96 | w.x.y.97 | w.x.y.127 | 29 |
| | 255.255.255.224 | w.x.y.128 | w.x.y.129 | w.x.y.159 | 29 |
| | 255.255.255.224 | w.x.y.160 | w.x.y.161 | w.x.y.191 | 29 |
| | 255.255.255.224 | w.x.y.192 | w.x.y.193 | w.x.y.223 | 29 |
| | 255.255.255.224 | w.x.y.224 | w.x.y.225 | w.x.y.255 | 29 |
| 16 | 255.255.255.240 | w.x.y.0 | w.x.y.1 | w.x.y.15 | 13 |
| | 255.255.255.240 | w.x.y.16 | w.x.y.17 | w.x.y.31 | 13 |
| | 255.255.255.240 | w.x.y.32 | w.x.y.33 | w.x.y.47 | 13 |
| | 255.255.255.240 | w.x.y.48 | w.x.y.49 | w.x.y.63 | 13 |
| | 255.255.255.240 | w.x.y.64 | w.x.y.65 | w.x.y.79 | 13 |
| | | | | | |

| Nº de sub-redes | Máscara de sub-rede | Nº da rede | Endereço roteamento | Endereço de broadcast | Nº restante de IP |
|---|---|---|---|---|---|
| | 255.255.255.240 | w.x.y.80 | w.x.y.81 | w.x.y.95 | 13 |
| | 255.255.255.240 | w.x.y.96 | w.x.y.97 | w.x.y.111 | 13 |
| | 255.255.255.240 | w.x.y.112 | w.x.y.113 | w.x.y.127 | 13 |
| | 255.255.255.240 | w.x.y.128 | w.x.y.129 | w.x.y.143 | 13 |
| | 255.255.255.240 | w.x.y.144 | w.x.y.145 | w.x.y.159 | 13 |
| | 255.255.255.240 | w.x.y.160 | w.x.y.161 | w.x.y.175 | 13 |
| | 255.255.255.240 | w.x.y.176 | w.x.y.177 | w.x.y.191 | 13 |
| | 255.255.255.240 | w.x.y.192 | w.x.y.193 | w.x.y.207 | 13 |
| | 255.255.255.240 | w.x.y.208 | w.x.y.209 | w.x.y.223 | 13 |
| | 255.255.255.240 | w.x.y.224 | w.x.y.225 | w.x.y.239 | 13 |
| | 255.255.255.240 | w.x.y.240 | w.x.y.241 | w.x.y.255 | 13 |
| 32 | 255.255.255.248 | w.x.y.0 | w.x.y.1 | w.x.y.7 | 5 |
| | 255.255.255.248 | w.x.y.8 | w.x.y.9 | w.x.y.15 | 5 |
| | 255.255.255.248 | w.x.y.16 | w.x.y.17 | w.x.y.23 | 5 |
| | 255.255.255.248 | w.x.y.24 | w.x.y.25 | w.x.y.31 | 5 |
| | 255.255.255.248 | w.x.y.32 | w.x.y.33 | w.x.y.39 | 5 |
| | | | | | |

| Nº de sub-redes | Máscara de sub-rede | Nº da rede | Endereço roteamento | Endereço de broadcast | Nº restante de IP |
|---|---|---|---|---|---|
| | 255.255.255.248 | w.x.y.40 | w.x.y.41 | w.x.y.47 | 5 |
| | 255.255.255.248 | w.x.y.48 | w.x.y.49 | w.x.y.55 | 5 |
| | 255.255.255.248 | w.x.y.56 | w.x.y.57 | w.x.y.63 | 5 |
| | 255.255.255.248 | w.x.y.64 | w.x.y.65 | w.x.y.71 | 5 |
| | 255.255.255.248 | w.x.y.72 | w.x.y.73 | w.x.y.79 | 5 |
| | 255.255.255.248 | w.x.y.80 | w.x.y.81 | w.x.y.87 | 5 |
| | 255.255.255.248 | w.x.y.88 | w.x.y.89 | w.x.y.95 | 5 |
| | 255.255.255.248 | w.x.y.96 | w.x.y.97 | w.x.y.103 | 5 |
| | 255.255.255.248 | w.x.y.104 | w.x.y.105 | w.x.y.111 | 5 |
| | 255.255.255.248 | w.x.y.112 | w.x.y.113 | w.x.y.119 | 5 |
| | 255.255.255.248 | w.x.y.120 | w.x.y.121 | w.x.y.127 | 5 |
| | 255.255.255.248 | w.x.y.128 | w.x.y.129 | w.x.y.135 | 5 |
| | 255.255.255.248 | w.x.y.136 | w.x.y.137 | w.x.y.143 | 5 |
| | 255.255.255.248 | w.x.y.144 | w.x.y.145 | w.x.y.151 | 5 |
| | 255.255.255.248 | w.x.y.152 | w.x.y.153 | w.x.y.159 | 5 |
| | 255.255.255.248 | w.x.y.160 | w.x.y.161 | w.x.y.167 | 5 |
| | | | | | |

| Nº de sub-redes | Máscara de sub-rede | Nº da rede | Endereço roteamento | Endereço de broadcast | Nº restante de IP |
|---|---|---|---|---|---|
| | 255.255.255.248 | w.x.y.168 | w.x.y.169 | w.x.y.175 | 5 |
| | 255.255.255.248 | w.x.y.176 | w.x.y.177 | w.x.y.183 | 5 |
| | 255.255.255.248 | w.x.y.184 | w.x.y.185 | w.x.y.191 | 5 |
| | 255.255.255.248 | w.x.y.192 | w.x.y.193 | w.x.y.199 | 5 |
| | 255.255.255.248 | w.x.y.200 | w.x.y.201 | w.x.y.207 | 5 |
| | 255.255.255.248 | w.x.y.208 | w.x.y.209 | w.x.y.215 | 5 |
| | 255.255.255.248 | w.x.y.216 | w.x.y.217 | w.x.y.223 | 5 |
| | 255.255.255.248 | w.x.y.224 | w.x.y.225 | w.x.y.231 | 5 |
| | 255.255.255.248 | w.x.y.232 | w.x.y.233 | w.x.y.239 | 5 |
| | 255.255.255.248 | w.x.y.240 | w.x.y.241 | w.x.y.247 | 5 |
| | 255.255.255.248 | w.x.y.248 | w.x.y.249 | w.x.y.255 | 5 |

### 8.1.7 Formato do datagrama IP

O pacote IP apresentado na figura 8.11 é repassado à camada de enlace para que seja enviado ao equipamento destino. A seguir, apresentaremos a descrição de cada parte desse pacote:

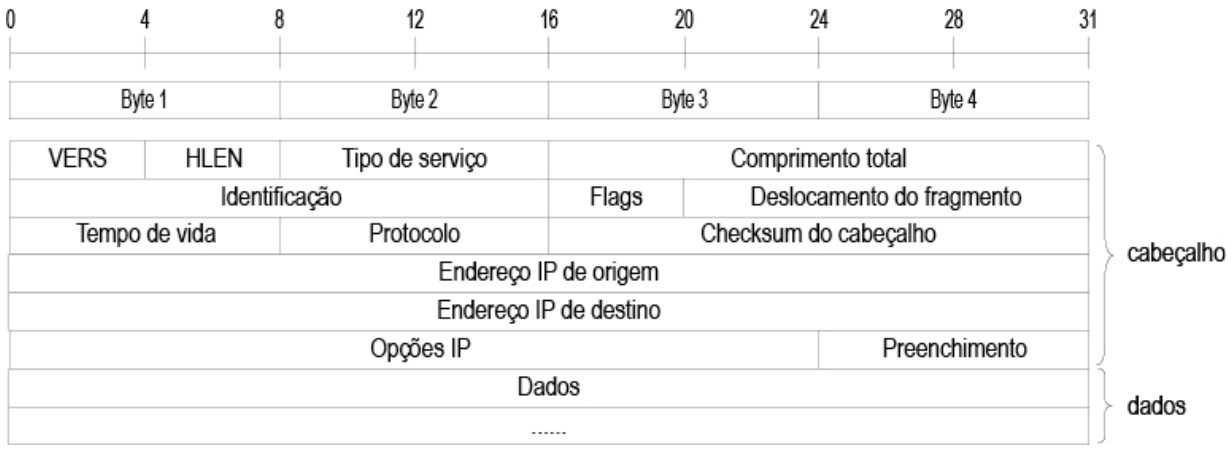



*Figura 8.11 – Formato do pacote IP.*

- **VERS** – Identifica a versão do protocolo IP que montou o pacote.
- **HLEN** – Os quatro bits desse campo determinam o comprimento do cabeçalho do pacote em múltiplos de palavras de 32 bits. O comprimento do cabeçalho é variável, pois os campos opções IP e preenchimento não possuem tamanhos fixos. O tamanho usual do cabeçalho é de 20 bytes, quando os campos opções IP e preenchimento são nulos. Nesse caso, o campo HLEN apresenta comprimento igual a 5 [5 * 32 bits (4 bytes) = 20 bytes].
- **Tipo de serviço** – Contém informações que descrevem a importância do pacote (por meio de oito níveis de prioridade) e a qualidade esperada para o serviço de entrega. A qualidade do serviço é descrita por três bits: D, T e R. O bit D igual a 1 solicita um baixo atraso; o bit T igual a 1 solicita uma alta taxa de transmissão; e o bit R igual a 1 solicita uma transmissão altamente confiável. As informações desse campo são geralmente ignoradas pelos roteadores que transportam o pacote.
- **Comprimento total** – Informa em bytes o comprimento total do pacote, incluindo o cabeçalho e o campo de dados. Como esse campo possui 16 bits, o tamanho máximo de um pacote é 2 elevado a 16 ou 64 Kbytes.
- **Identificação** – Contém um número inteiro que identifica o pacote. Esse campo é utilizado no processo de fragmentação e remontagem dos pacotes. Todos os fragmentos de um pacote contêm o mesmo número de identificação. Dessa forma, o

receptor consegue identificar facilmente os fragmentos que precisam ser reagrupados para remontar o pacote original. Como exemplo de utilização desse campo, temos a interconexão entre duas arquiteturas diferentes, como Token Ring e Ethernet.

- **Flags** – Campo composto dos bits DF (*Don´t Fragment*) e MF (*More Fragments*). A estação transmissora assinala DF igual a 1 para indicar que o pacote não deve ser fragmentado. Nesse caso, se um roteador precisar fragmentar o pacote para adequá-lo à rede de destino, o pacote será descartado. O bit MF igual a 1 é utilizado para indicar que o fragmento é o último pedaço do pacote original. Quando uma estação recebe um fragmento com MF igual a 0, ela sabe que deve esperar a chegada de mais fragmentos para completar a remontagem do pacote.
- **Deslocamento do fragmento** – Esse campo contém a posição relativa do fragmento em relação ao pacote original, medida em bytes. Os fragmentos de um pacote não chegam ao receptor necessariamente na mesma ordem em que foram transmitidos. Utilizando a informação do campo de deslocamento, a estação receptora consegue reordenar os fragmentos recebidos e remontar o pacote original.
- **Tempo de vida (TTL –** *Time to Live***)** – Indica o tempo em segundos que o pacote pode permanecer na rede Internet. Quando uma estação transmite um pacote, ela assinala o valor do TTL. Toda vez que o pacote é processado por um roteador, o TTL é decrescido em uma unidade. Quando ele expira (chega a 0), o pacote é descartado, ainda que o destino final não tenha sido atingido.
- **Protocolo** – O campo protocolo contém um código que especifica o tipo de protocolo de transporte encapsulado no campo de dados do pacote que pode ser o protocolo TCP ou o protocolo UDP.
- **Checksum do cabeçalho** – Esse campo contém o checksum de todos os bytes que compõem o cabeçalho de controle, excluindo apenas o próprio campo de checksum. Além disso, esse campo é utilizado pela estação receptora para verificar a integridade do cabeçalho de controle do pacote recebido.

- **Endereço IP de origem** – Contém o endereço IP que identifica a estação transmissora.
- **Endereço IP de destino** – Contém o endereço IP que identifica a estação de destino. Esse campo reflete sempre o destino final, não importando se o pacote passará ou não por roteadores intermediários.
- **Opções IP** – Campo com tamanho variável de 0 até vários bytes. Esse campo pode conter uma série de códigos em sequência, cada um deles definindo uma opção relativa ao processamento dos pacotes. As opções são geralmente relacionadas a aspectos como segurança, roteamento, relatórios de erro, depuração etc.
- **Preenchimento** – Esse campo completa a sequência do campo opções com bits de preenchimento de valor 0, garantindo que o tamanho total dos campos opções somados ao preenchimento seja múltiplo de 32 bits.
- **Dados** – Contêm os dados transportados pelo pacote, os quais correspondem geralmente à unidade de dados do protocolo de transporte TCP ou UDP.

#### 8.1.7.1 Fragmentação e remontagem

Um pacote IP pode ter um tamanho de até 64 Kbytes (1 k = 1.024 bytes). Entretanto, o IP é um protocolo da camada de rede que deve ser transportado por protocolos das camadas inferiores. O problema é que esses protocolos inferiores podem não suportar o transporte de pacotes desse tamanho. Um exemplo muito conhecido é o caso do IP sobre Ethernet, cujo quadro tem um tamanho máximo (MTU – *Maximum Transmission Unit*) de 1.500 bytes.

Nesse caso, um recurso usado pelo IP e por vários outros protocolos é o de fragmentação (segmentação) e remontagem. O roteador negocia com os periféricos de rede e com o próximo roteador o tamanho máximo que pode ser usado nessa sub-rede. Pacotes com tamanhos maiores deverão ser fragmentados. A operação de fragmentação consiste em quebrar os dados do pacote em unidades transportáveis, copiar o cabeçalho para cada uma delas e, por fim, enviar. Para que o receptor possa remontar o

pacote original, os campos *Identification*, *Flags* e *Fragment Offset* são usados. Cada pacote IP enviado por uma máquina possui um campo *Identification* diferente. Quando o pacote demandar fragmentação, o valor desse campo se manterá o mesmo em cada fragmento.

O campo Flags possui em especial 2 bits. O DF (*Don't Fragment*) informa que o pacote não deve ser fragmentado. Caso o pacote não possa ser transportado sem essa operação, o roteador deverá descartá-lo. Essa opção pode ser usada a fim de determinar o tamanho máximo que pode ser transportado por uma rede. Se o roteador resolver descartar o pacote, precisará informar ao emissor por meio de mensagens geradas pelo protocolo ICMP que o pacote foi descartado.

O campo *More Fragments* indica a existência de mais fragmentos depois da posição desse, ou seja, se esse bit não estiver ligado, esse será o último fragmento da cadeia.

O campo Offset determina a posição relativa do fragmento em relação ao pacote original. Como o campo Flags consumiu três bits (um é reservado), esse campo é utilizado sempre em múltiplos de 8.

Com esses dados, sempre que necessário, é possível fragmentar um pacote de tamanho excessivo em pedaços menores, suportados pela rede, e remontá-lo completamente no seu destino. Cabe lembrar que, por motivos de desempenho dos roteadores, é função única e exclusiva do receptor a reconstrução do pacote.

## 8.2 Protocolo ARP

O protocolo ARP (*Address Resolution Protocol*) é responsável por realizar o mapeamento de endereços lógicos (endereços IP) em endereços físicos (endereços MAC), quando utilizamos o IP sobre redes Ethernet. O protocolo ARP foi proposto e aceito na Internet por meio da RFC 826. Para poder transmitir um pacote, a estação transmissora precisa conhecer todas as informações de endereçamento relacionadas ao destinatário, tanto no que se refere à camada de rede (endereço IP) quanto no que se refere à camada de enlace de dados (endereço físico). No modelo de referência

TCP/IP, todas as referências aos endereços das estações são feitas por meio de endereços IP. O endereço físico do destinatário é descoberto dinamicamente pelo transmissor antes de efetuar a comunicação, utilizando um protocolo auxiliar denominado ARP.

Sua operação segue o seguinte princípio: quando o computador A quer se comunicar com o computador B e não sabe seu endereço físico, envia um pacote ARP em modo *broadcast* pedindo informações. Todos os computadores em operação na rede recebem o pedido. O computador B reconhece que o endereço pedido é o seu e responde, informando qual o seu endereço físico. As figuras 8.13 a 8.16 detalham, de forma mais clara, o comentário apresentado.

Na figura 8.12, apresentamos dois equipamentos que trocarão dados entre si. Nessa figura, são apresentados em alto nível o formato do quadro Ethernet e a parte deste que se refere ao pacote IP:

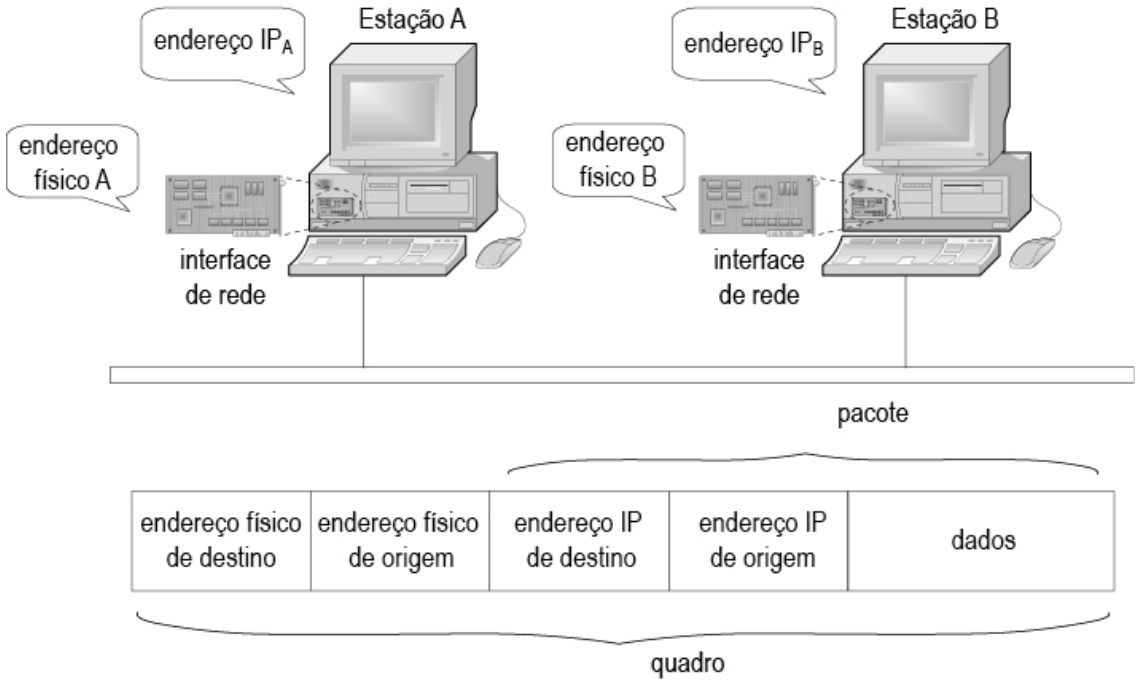



*Figura 8.12 – Protocolo ARP.*

A figura 8.13 apresenta o primeiro passo executado pelo computador A para iniciar a transmissão de um pacote. Nessa figura, também é apresentado o endereço físico (MAC) do

equipamento A (00-60-08-16-85-B3). Como ponto de partida (1), a estação transmissora A envia uma requisição ARP perguntando o endereço físico correspondente ao IP de destino da estação B: 200.17.98.105. Uma requisição ARP é um pacote IP enviado em *broadcast* a todas as estações da rede.

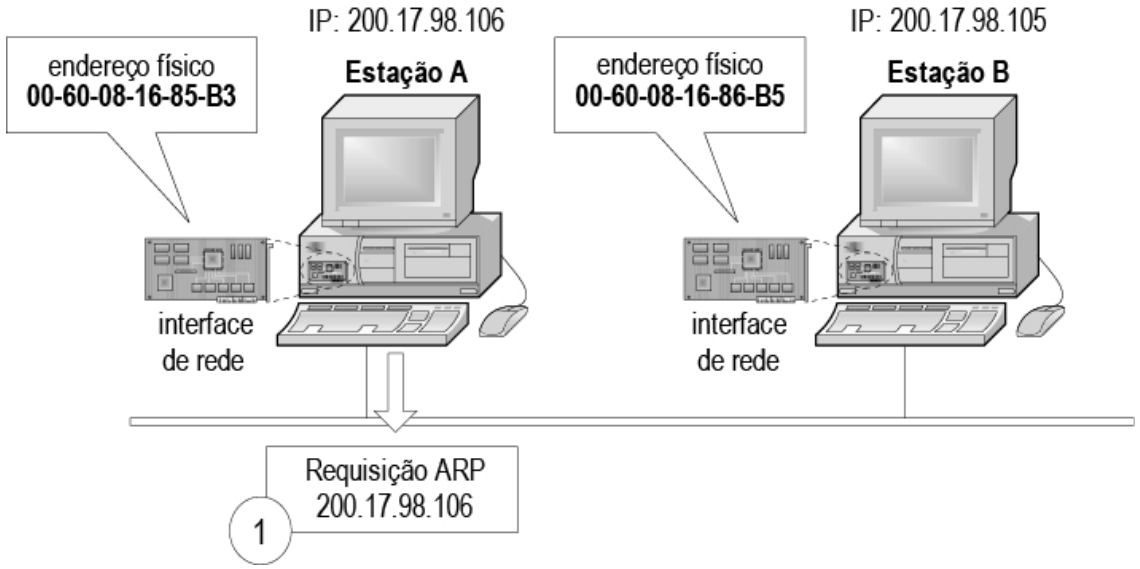



*Figura 8.13 – Protocolo ARP.*

A figura 8.14 apresenta o segundo e terceiro passos executados pela requisição ARP. Também é apresentado o conteúdo da resposta gerada. No segundo passo (2), as estações, ao receberem a requisição ARP, comparam o endereço IP solicitado com o seu próprio. Se os endereços forem diferentes, a requisição será ignorada pelos computadores ligados à rede. No terceiro passo (3), a estação B verifica que o endereço solicitado é o seu e responde enviando uma resposta ARP contendo o seu endereço físico. Essa resposta, um pacote enviado diretamente à estação que gerou a requisição, contém as seguintes informações:

- **Endereço físico de origem** – 00-60-98-16-86-B5.
- **Endereço físico de destino** – 00-60-98-16-86-B3.
- **Endereço IP origem** – 200.17.98.105.
- **Endereço IP destino** – 200.17.98.106.

Observação: o endereço físico solicitado será enviado no campo de dados do pacote IP.

A figura 8.15 apresenta o quarto e quinto passos executados pela requisição ARP. Também é apresentado o conteúdo do pacote depois de a requisição ARP ser encerrada. No quarto passo (4), quando a estação A receber a resposta ARP, determinará o endereço físico da estação destino. No quinto passo (5), já com o endereço físico do destinatário identificado, a estação A envia seus dados diretamente à estação B por meio de uma comunicação ponto a ponto.

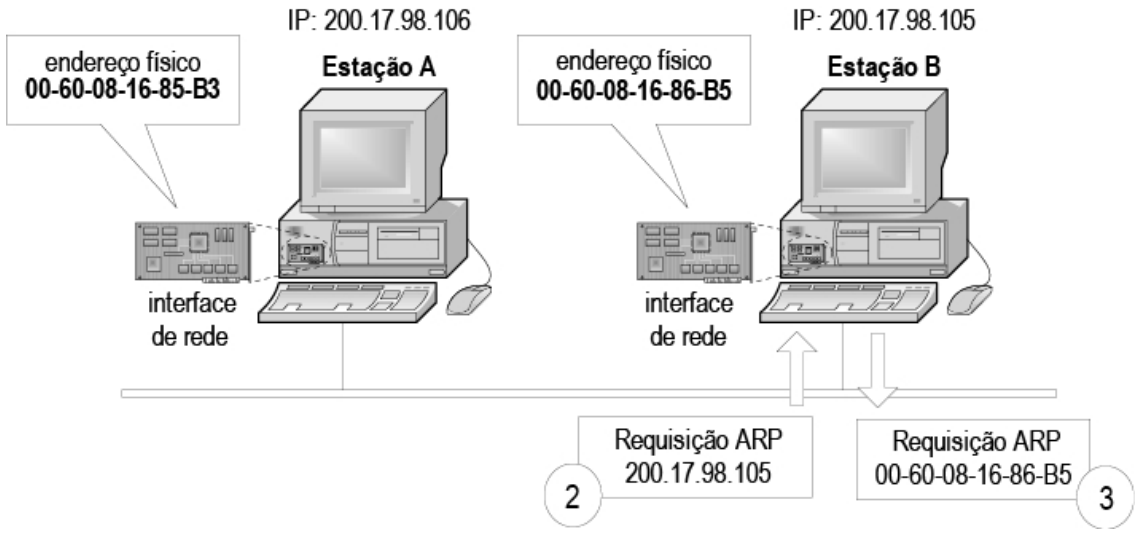



*Figura 8.14 – Segundo e terceiro passos da requisição ARP.*

O pacote enviado pela estação A à estação B contém as seguintes informações:

- **Endereço físico de origem** – 00-60-98-16-86-B3.
- **Endereço físico de destino** – 00-60-98-16-86-B5.
- **Endereço IP origem** – 200.17.98.106.
- **Endereço IP destino** – 200.17.98.105.

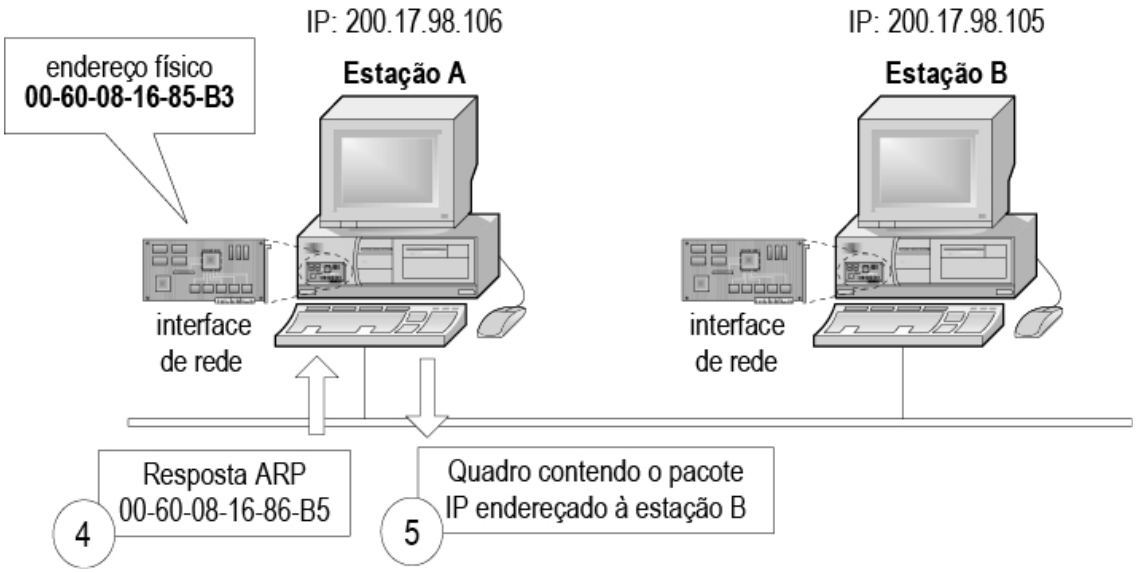



*Figura 8.15 – Quarto e quinto passos da requisição ARP.*

## 8.2.1 Programa arp.exe

O programa arp.exe emcontra-se disponível na maioria dos sistemas operacionais de rede. Esse executável permite visualizar a tabela arp utilizada pelo protocolo IP para identificar o endereço físico do computador destino. O programa arp.exe recebe parâmetros, os quais definem o resultado apresentado pelo programa, conforme mostrado na tabela 8.13. A sintaxe da execução do programa é a seguinte:

arp –a [endereço_IP] [-N endereço MAC]

*Tabela 8.13 – Parâmetros do comando arp.exe*

| Parâmetro | Descrição |
|---|---|
| -a | Exibe as entradas ARP atuais interrogando os dados de protocolo atuais. Se inet_addr (endereço IP) for especificado, somente os endereços IPs e físicos do computador especificado serão exibidos. |
| -g | Mesmo que –a. |
| -d | Exclui o host especificado por inet_addr. |

| Parâmetro | Descrição |
|---|---|
| -s | Adiciona o host e associa o endereço da Internet inet_addr ao endereço físico (eth_addr). O endereço físico é passado com seis bytes hexadecimais separados por hífens. A entrada é permanente e não será removida enquanto o equipamento estiver ligado. |
| If_addr | Caso esteja presente, especifica o endereço da Internet da interface cuja tabela de endereços deve ser modificada. Do contrário, é usada a primeira interface aplicável. |
| Eth_addr | Especifica um endereço físico. |
| Inet_addr | Especifica um endereço de Internet. |
| -N if_addr | Exibe as entradas ARP para a interface de rede especificada por if_addr. |

A seguir, apresentaremos um exemplo da execução do programa arp.exe:

arp -s 175.55.85.212 00-aa-00-62-c6-09 – Adiciona a entrada estática na tabela arp
arp -a – Exibe as entradas da tabela de arp

## 8.2.2 ARP cache

Se para cada vez que enviássemos um pacote IP fosse necessário usar uma sequência de ARP, a rede poderia ficar um pouco carregada, dependendo do tráfego do momento. Para suavizar essa situação, o sistema operacional deve manter em memória uma lista dos últimos endereços descobertos pelo protocolo ARP. Assim, para cada requisição gerada pelo protocolo ARP, guarda-se na ARP cache (memória RAM do emissor) o endereço lógico e físico do equipamento destino, pois provavelmente tal informação poderá ser utilizada em outras requisições.

Todo pedido ARP é enviado em *broadcast*, ou seja, todos os equipamentos que recebem o quadro podem aproveitar o tempo que despenderam para analisar a informação, guardando-a na ARP cache também. Assim, se for necessário transmitir dados novamente para o mesmo equipamento, a informação já estará presente na tabela ARP cache, reduzindo o tempo para

determinação de onde o destino está localizado. Isso é bastante viável, pois as tabelas ARP, em geral, não são muito grandes. Depois de algum tempo, o endereço gravado na ARP cache é removido, independentemente de estar sendo usado ou não. É o que se chama de aging.

Assim que uma máquina iniciar a carga dos serviços de rede, poderá gerar um ARP *broadcast* anunciando seu endereço para as outras, adiantando o processo de detecção e, consequentemente, a comunicação. Isso só é vantajoso se a comunicação for iniciada pelo equipamento remoto, pois, do contrário, será necessário um pacote ARP para pedir o endereço remoto.

### 8.2.3 Formato do pacote ARP

O pacote ARP possui uma estrutura de tamanho variável que segue o formato apresentado na tabela 8.14:

*Tabela 8.14 – Formato do pacote ARP*

| Parâmetro | Descrição |
|---|---|
| HardwareType | Especifica o tipo do hardware. Os tipos conhecidos são definidos pela RFC Assigned Numbers, que recebe uma atualização de tempos em tempos. O hardware Ethernet recebeu o número 1. |
| ProtocolType | Especifica o tipo do protocolo ao qual o endereço lógico se refere. A RFC Assigned Numbers especifica que o tipo deve ser o mesmo que os do MAC Ethernet. No caso do IP, é 0800h. |
| HardwareLen | Determina o comprimento em bytes do endereço de hardware (físico). |
| ProtocolLen | Determina o comprimento em bytes do endereço de protocolo (lógico). |
| Operation | Tipo da operação. Para o ARP, só existem duas: pergunta e resposta. |
| SenderHardwareAddr | Endereço físico de quem está enviando o pacote. |
| SenderProtocolAddr | Endereço lógico de quem está enviando o pacote. |

| Parâmetro | Descrição |
|---|---|
| TargetHardwareAddr | Endereço físico desejado. Na operação de request, vai em branco. Quem responder preenche esse campo. |
| TargetProtocolAddr | Endereço lógico desejado. |

Na operação de resposta, o pacote é copiado, preenchido com a informação desejada e devolvido. Como o endereço físico do requisitante está presente na informação, não háverá problemas no envio.

## 8.3 Protocolo RARP

O ARP resolve o problema de encontrar uma rede Ethernet que corresponda a um determinado endereço IP. Existem situações em que se torna necessário resolver o problema inverso. Isso ocorre especificamente quando uma estação de trabalho sem disco rígido (estação diskless) é reinicializada. Um computador que não possui disco rígido dispara na rede seu endereço MAC e espera que algum servidor responda a ele qual o seu respectivo endereço IP. Para resolver essa questão, utiliza-se o protocolo RARP (*Reverse Address Resolution Protocol*), o qual foi especificado na RFC 903.

Uma desvantagem do RARP é que ele usa um endereço de destino composto somente de 1 (método de *broadcast*) para chegar ao servidor RARP, ou seja, para identificar o servidor RARP, a solução adotada é o envio de *broadcast*, o que pode deixar a rede lenta. Como segunda desvantagem do protocolo RARP, temos que essas difusões em *broadcast* não são encaminhadas pelos roteadores para outras redes, portanto é necessário um servidor RARP em cada rede.

## 8.4 Protocolo BOOTP

Para resolver o problema de *broadcast*, foi inventado um protocolo alternativo chamado de BOOTP. Ao contrário do RARP, que utiliza *broadcast*, o BOOTP usa mensagens UDP, as quais podem ser enviadas entre roteadores. O BOOTP também fornece informações adicionais para as estações de trabalho sem disco, como o

endereço IP do servidor de arquivos que mantém a imagem da memória, ou seja, os endereços IP ligados ao endereço MAC, o endereço IP do roteador-padrão (*default gateway*) e a máscara de sub-rede a ser usada. O BOOTP foi descrito na RFC 951. A utilização desse protocolo se dá em redes que utilizam BOOT REMOTO (muito utilizado em redes Novell). Muitas empresas continuam usando esse tipo de recurso.

Em alguns modelos de roteadores Juniper, a configuração do DHCP relay utiliza o termo BOOTP. O DHCP relay permite que o servidor DHCP seja centralizado em uma localidade, permitindo que redes remotas possam usufruir desse recurso sem a necessidade de ter um servidor de DHCP local.

## 8.5 Protocolo ICMP

O protocolo ICMP está presente em redes em que se utilizam os protocolos do modelo de referência TCP/IP. Qualquer equipamento na rede que utilizar endereço IP, quando não conseguir comunicar-se com outro, reportará seu insucesso emitindo uma mensagem de erro seguindo o padrão do protocolo ICMP. Existem aproximadamente 12 tipos de mensagens ICMP, sendo as mais importantes listadas na tabela 8.15. Cada tipo de mensagem é encapsulado em um pacote IP.

*Tabela 8.15 – Mensagens geradas pelo protocolo ICMP*

| Tipo de mensagem | Descrição |
|---|---|
| Destination unreachable | Pacote não pode ser entregue. Esta é enviada quando a sub-rede ou um roteador não pode localizar o destino. |
| Time exceeded | Campo tempo de vida chegou a 0. Esta é enviada quando um pacote é descartado porque seu contador chegou a 0. Esse evento é um sintoma de que os pacotes estão entrando em loop ou que há um enorme congestionamento. |

| Tipo de mensagem | Descrição |
|---|---|
| Parameter problem | Campo de cabeçalho inválido. Esta é enviada para indicar que um valor inválido foi detectado em um campo de cabeçalho. Esse problema indica a existência de um bug no software IP do host transmissor ou, possivelmente, no software do roteador pelo qual o pacote transitou. |
| Source quench | Pacote regulador. Essa mensagem foi usada para ajustar os hosts que estivessem enviando pacotes demais. Quando recebia essa mensagem, um host deveria desacelerar sua operação. Essa mensagem é raramente usada, pois quando ocorre o congestionamento, esses pacotes tendem a colocar mais lenha na fogueira. O controle de congestionamento da Internet é feito na camada de transporte. |
| Redirect | Ensinar geografia a um roteador. Esta é enviada quando um roteador percebe que o pacote pode ter sido incorretamente roteado. Ela é usada pelo roteador para informar ao host transmissor a respeito do provável erro. |
| Echo request | Perguntar a uma máquina se ela está viva. Esta é enviada para verificar se um determinado destino está ativo. Ao receber a mensagem ECHO, o destino deve enviar de volta uma mensagem ECHO replay. |
| Echo replay | Sim, estou viva. Resposta da mensagem Echo request. |
| Timestamp request | O mesmo que Echo request, mas com timestamp. Semelhante às mensagens já citadas, porém registra o tempo de chegada da mensagem e o tempo de partida da resposta na mensagem de resposta. |
| Timestamp reply | O mesmo que Echo reply, mas com timestamp. |

O programa *ping,* também disponível nos sistemas operacionais em uso, utiliza o protocolo ICMP para determinar se um endereço IP está em uso. Essa é a forma utilizada pelos administradores de rede para determinar se um determinado computador está ou não disponível para ser acessado.

## 8.6 Exercícios do capítulo 8

**1**. Se uma sub-rede tem endereço de rede como 200.201.5.32 com

máscara 255.255.255.224, qual o último endereço válido para um equipamento nessa sub-rede?

a) 200.201.5.61.

b) 200.201.5.62.

c) 200.201.5.63.

d) 200.201.5.64.

**2**. Uma empresa precisa dividir uma classe C em 32 sub-redes. Quantos bits de rede deverão ser setados em 1 na máscara de sub-rede?

a) 24.

b) 21.

c) 29.

d) 25.

e) 27.

**3**. O protocolo IP vem sendo amplamente utilizado há praticamente duas décadas e tem operado de forma adequada, conforme demonstra o crescimento exponencial da Internet. Entretanto o IP vem se tornando uma vítima do próprio sucesso, especificamente no que se refere à escassez crescente de endereços. Acerca do roteamento CIDR, que é uma das soluções utilizadas para minimizar esse problema, identifique a alternativa correta:

a) Uma das ideias básicas do CIDR consiste em dividir a classe E de endereços IP e alocar cada divisão em zonas geográficas distintas do mundo.

b) Em roteadores que empregam CIDR, cada entrada na tabela de roteamento é estendida com a adição de um campo de informação acerca da zona geográfica onde se encontra o ponto de destino.

c) A RFC 1519 descreve o conceito básico de alocação de blocos de tamanho variável de endereços de rede que ainda restam da classe C.

d) O conceito de máscara de sub-rede é suprimida no CIDR.

e) A operação do CIDR não pode ser aplicada a redes antigas com endereços das classes A, B e C.

**4**. Quantas sub-redes serão disponibilizadas se forem utilizados os quatro bits mais significativos de um endereço IP, anteriormente dedicados a equipamentos em um endereço classe C?

a) 6.

b) 8.

c) 10.

d) 14.

e) 15.

**5**. Considerando os endereços IPv4 seguintes 200.17.53.123, 113.8.95.89 e 225.54.33.64, é correto afirmar:

a) Trata-se de um endereço classe C, um endereço classe B e um endereço reservado para uso futuro, respectivamente.

b) Trata-se de um endereço classe C, um endereço classe A e outro endereço classe C, respectivamente.

c) Trata-se de um endereço classe C, um endereço classe A e um endereço classe D (reservado para *multicasting*), respectivamente.

d) Trata-se de um endereço classe C, um endereço sem classe e um endereço de *multicast*, respectivamente.

e) Trata-se de um endereço classe C, um endereço classe B e outro endereço classe C, respectivamente.

**6**. O equivalente binário de 32 bits do endereço IP 200.17.210.11 é:

a) 11000001 00100000 11011000 00001001.

b) 11001000 00010001 11011111 00000011.

c) 11001000 00010011 00000001 00001011.

d) 11001000 00010001 11010010 00001011.

e) 11001000 00010011 11011111 00011011.

**7**. O que é um roteador? Qual é a sua função?

**8**. Sobre a implementação de firewalls, considere as seguintes afirmativas:

I. O sistema de conversão de endereços de rede pode modificar os números de porta de origem e de destino dos pacotes.

II. Em um firewall baseado em regras, é possível identificar o primeiro pacote de uma conexão UDP pelo bit SYN ativo no cabeçalho.

III. O rastreamento de conexões (*connection tracking*) é necessário apenas para manter um registro de atividade (log) das conexões. Um firewall baseado em regras poderia funcionar perfeitamente sem o rastreamento de conexões.

IV. Para liberar o tráfego para um servidor DNS na rede interna, basta abrir a porta UDP 63.

V. Uma das vantagens de utilizar um proxy de aplicação é poder filtrar as requisições do usuário.

Assinale a alternativa correta:

a) Somente as afirmativas I, II e IV são verdadeiras.

b) Somente as afirmativas II, III e V são verdadeiras.

c) Somente as afirmativas I, IV e V são verdadeiras.

d) Somente as afirmativas I e V são verdadeiras.

e) Somente a afirmativa II é verdadeira.

**9**. Considere as seguintes afirmativas sobre firewalls:

I. A função de um firewall é somente impedir que a rede interna seja alvo de ataques externos.

II. Uma política de segurança possível afirma que tudo que não está explicitamente permitido é proibido.

III. Um firewall deve permitir a conversão de endereço via NAT (*Network Address Translation*) e a realização de IP Spoofing.

IV. Um firewall pode ser utilizado para evitar o sniffing dentro da rede interna.

V. Para aplicações como FTP, pode ser necessário que o firewall analise o protocolo no nível de aplicação.

Assinale a alternativa correta:

a) Somente as afirmativas II e V são verdadeiras.

b) Somente as afirmativas III e V são verdadeiras.

c) Somente as afirmativas I e II são verdadeiras.

d) Somente as afirmativas I, II e III são verdadeiras.

e) Somente as afirmativas II e IV são verdadeiras.

**10**. Uma empresa precisa ligar um edifício coligado que se encontra a aproximadamente 250 metros de distância da sede principal. Qual das seguintes tecnologias Ethernet permitirá essa ligação sem a necessidade de repetidores? Escolha a melhor:

a) Cabo-padrão 10BASE2.

b) Cabo-padrão 10BASET.

c) Cabo-padrão 10BASEFL.

d) Cabo-padrão 10BASE5.

**11**. O que é máscara de sub-rede?

a) É uma tecnologia usada para ligar o seu computador em qualquer rede.

b) É uma tecnologia que permite a divisão de uma classe IP em outras classes.

c) É um mecanismo de segurança que impossibilita aos outros descobrirem o seu número IP.

d) É o nome de uma tecnologia de firewalls muito sofisticada.

**12**. O que é classe de endereço IP?

a) É o nível da faixa de preços do provedor a que você se conecta.

b) É o nível de serviço de um número IP (exemplos: A = universidade, B = provedor etc.).

c) É uma divisão dos endereços IP a fim de possibilitar redes de diferentes tamanhos.

d) É uma divisão dos endereços IP por países.

**13**. O que é o endereço de loopback?

a) É um endereço IP usado por seu computador para se desconectar da Internet.

b) É uma falha de projeto no modelo TCP/IP que cria um buraco na

segurança das redes na Internet.

c) É um endereço IP no qual a mensagem é mandada da origem para a origem.

d) É uma falha de projeto no modelo OSI que cria um buraco na segurança das redes na Internet.

**14**. Qual dos seguintes intervalos é uma classe C válida?

a) 192.168.0.0 até 192.168.255.255.

b) 172.17.0.0 até 172.17.255.255.

c) 191.168.0.0 até 191.168.0.255.

d) 10.1.0.0 até 10.1.255.255.

**15**. Quais dos seguintes conjuntos de parâmetros TCP/IP são o mínimo necessário para que um computador possa se comunicar com a Internet?

a) Endereço IP, gateway-padrão.

b) Endereço IP, máscara de sub-rede.

c) Endereço IP, máscara de sub-rede, gateway-padrão.

d) Endereço IP, gateway-padrão, servidor DNS primário.

**16**. Qual é o comando utilizado para realizar o teste de conectividade entre dois sites?

**17**. Quantos bits e quantos bytes possuem o endereço IP?

**18**. Qual o comando utilizado para descobrir a rota seguida por um pacote IP entre a sua casa e um endereço IP?

**19**. Comente sobre endereços IP públicos e privados.

**20**. Dados os endereços IP seguintes: 200.10.80.123, 100.220.90.124, 10.20.30.35, 1.67.95.254, converta-os para o formato binário.

**21**. Nos servidores Windows, qual é o comando que apresenta o endereço IP e o nome do seu computador?

**22**. Como é composto um endereço IP?

a) Identificador de sub-rede + identificador da estação nessa sub-rede.

b) 128 bits.

c) Preâmbulo mais dados.

d) Cabeçalho de dados e número da estação receptora.

**23**. Quais critérios devem ser avaliados para a escolha de uma classe de endereçamento IP?

a) A região de localização.

b) O número de endereços P necessários.

c) Depende da marca dos equipamentos.

d) Nenhuma das alternativas anteriores está correta.

**24**. Qual das seguintes opções descreve uma máscara de rede?

a) Essa camada seta os bits que correspondem à rede para um e seta os bits que correspondem aos equipamentos para zero.

b) É uma sequência de 16 bits.

c) É utilizada para endereçar os computadores na rede.

d) Os roteadores não utilizam esse endereço.

**25**. No modelo de referência TCP/IP, em qual das camadas estão definidos os roteadores?

a) Física.

b) Transporte.

c) Enlace de dados.

d) Redes.

**26**. O endereço IP 200.200.200.10 com a máscara 255.255.248 pertence a qual rede? Qual é o endereço utilizado para *broadcast*?

**27**. Sobre os IPs reservados, é correto afirmar:

a) O endereço 0.0.0.0 é reservado para *broadcast* na rede local.

b) O endereço 1.0.0.127 é conhecido por endereço de loopback.

c) O endereço 169.254.1.1 está na faixa de endereços da classe C.

d) O endereço 255.255.255.255 é reservado como endereço de *broadcast*.

**28**. Para fazer uso do protocolo TCP/IP em um servidor Windows NT, é necessário configurar um endereço IP. Sabendo que a

máscara de sub-rede do servidor deverá ser 255.255.255.224 e que a rota default, definida estaticamente, deve apontar para o roteador 200.250.10.33, indique um endereço IP válido na mesma sub-rede que permita utilizar o servidor para navegar pela Internet:

a) 200.250.10.226.

b) 200.250.10.23.

c) 200.250.10.40.

d) 200.250.10.72.

e) 200.250.10.255.

**29**. Em relação ao protocolo ARP, quando a estação remetente deseja resolver (descobrir) o endereço físico (exemplo: Ethernet) da estação de destino a partir do endereço IP desta última, ela envia uma mensagem de solicitação:

a) Para o endereço de *broadcast* limitado 255.255.255.255. A estação destino responde ao pedido diretamente para a estação solicitante.

b) Diretamente para o servidor ARP, enquanto o servidor ARP responde ao pedido diretamente para a estação solicitante.

c) Para o endereço de *broadcast* limitado 255.255.255.255. O servidor ARP responde ao pedido diretamente para a estação solicitante.

d) Diretamente para o servidor ARP. O servidor ARP responde ao pedido para o endereço de *broadcast* limitado 255.255.255.255.

e) Para o endereço de *broadcast* limitado 255.255.255.255. A estação destino responde ao pedido também para o endereço de *broadcast* limitado 255.255.255.255.

**30**. Considere o endereço de sub-rede IP 15.0.96.0/19. A alternativa que indica, respectivamente, a máscara de rede dessa sub-rede, o número de estações que essa sub-rede pode endereçar e o seu endereço de *broadcast* é:

a) 255.255.240.0, 8190, 15.0.127.255.

b) 255.255.224.0, 8192, 15.0.96.255.

c) 255.255.240.0, 8192, 255.255.255.255.

d) 255.255.224.0, 8190, 15.0.96.255.

e) 255.255.224.0, 8190, 15.0.127.255.

**31**. Se uma rede usa a máscara 255.255.255.224, o endereço da sub-rede a que pertence o endereço IP 195.40.13.131 é?

**32**. (Copel, 2010) Uma máscara de rede 255.255.255.248 foi aplicada sobre o endereço 200.1.1.0/24. Essa operação criará:

a) 248 novos endereços de rede.

b) 3 novos endereços de rede.

c) Em cada nova rede criada, 254 endereços para hosts.

d) Em cada nova rede criada, 14 endereços para hosts.

e) Em cada nova rede criada, 6 endereços para hosts.

**33**. (Copel, 2010) O protocolo IP é um dos protocolos mais utilizados atualmente. Indique a alternativa correta:

a) O protocolo IP é um protocolo baseado em conexão.

b) O protocolo IP é baseado em datagrama não confiável.

c) O protocolo IP realiza o controle de erros.

d) O protocolo IP realiza o controle de fluxo.

e) O protocolo IP envia pacotes de tamanho fixo.

**34**. (UFT, 2005) Na tecnologia Internet, o elemento principal de endereçamento, identificador de uma máquina conectada à rede é:

a) TCP.

b) UDP.

c) IPX.

d) IP.

e) SPX.

CAPÍTULO 9

# Roteamento

Neste capítulo, apresentaremos em detalhes o processo empregado nas redes TCP/IP para o roteamento dos pacotes entre computadores e roteadores. De forma prática, serão apresentados o funcionamento das tabelas de roteamento, a diferença entre roteamento estático e roteamento dinâmico e os tipos de roteadores disponíveis para utilização. Concluíremos o capítulo apresentando os algoritmos utilizados pelo protocolos de roteamento, como também os principais protocolos de roteamento dinâmico, como RIP, OSPF e IS-IS, essenciais à administração de uma rede privada. O protocolo BGP utilizado pela Internet será apresentado no capítulo 18.

## 9.1 Introdução

O roteamento é a forma utilizada na Internet para a entrega de pacotes de dados entre equipamentos de rede, incluindo computadores e roteadores. O modelo de roteamento utilizado é o do salto-por-salto (*hop-by-hop*), no qual cada roteador que recebe um pacote de dados o abre e verifica o endereço de destino no cabeçalho IP. Em seguida, o pacote é entregue ao próximo equipamento conectado, que poderá ser outro roteador ou um computador. Esse processo será repetido até que o pacote alcance o seu destino.

Para que esse processo seja transparente e funcione corretamente, precisamos garantir que o roteador possua uma tabela de roteamento que informará ao roteador o que fazer com os pacotes recebidos. Para montar uma tabela de roteamento, podemos utilizar duas formas, sendo a primeira por meio da criação de rotas estáticas e a segunda por meio da geração automática da tabela de rotas, obtida por meio dos protocolos de roteamento (exs.: RIP, OSPF, IS-IS, entre outros). As tabelas de roteamento são registros de endereços de destino associados ao número de saltos até ele, podendo conter várias outras informações. Os protocolos de roteamento determinam o conteúdo das tabelas de roteamento, ou seja, são eles que ditam a forma como

a tabela é montada e por quais informações ela é composta.

Existem dois tipos de algoritmo em uso pelos protocolos de roteamento: o algoritmo baseado em vetor de distância (*distance-vector routing protocols*) e o algoritmo baseado no estado de link (*link state routing protocols*), os quais serão detalhados neste capítulo. Existe ainda um terceiro algoritmo utilizado pelo protocolo BGP chamado vetor de caminho, abordado no capítulo 18.

## 9.2 Roteamento IP

O roteamento IP é responsável por garantir que um pacote emitido, por exemplo, em Curitiba chegue ao Japão e volte trazendo as informações requeridas. Explicaremos por que o usuário nem percebe quando esse processo todo acontece.

O destino de um pacote IP enviado por uma máquina pode ser a própria estação, situada na mesma rede ou em uma rede diferente (tudo depende da operação lógica entre os endereços IPs). No primeiro caso, o pacote é enviado ao nível IP, que o retorna para os níveis superiores. No segundo caso, é realizado o mapeamento por meio do protocolo ARP, e o pacote é enviado por meio do protocolo de rede. Caso uma estação ou roteador tenha de enviar um pacote para outra rede, o protocolo IP deve enviá-lo para um roteador situado na mesma rede. Por sua vez, o roteador enviará o pacote para outro roteador, na mesma rede que este utilizou, e assim sucessivamente, até que o pacote chegue ao destino final. Esse tipo de roteamento é chamado de *Next-Hop Routing*, já que um pacote é sempre enviado para o próximo roteador no caminho.

Nesse tipo de roteamento, não há necessidade de que um roteador conheça a rota completa até o destino. Cada roteador deve conhecer apenas o próximo roteador para o qual deve enviar a mensagem. Essa decisão é chamada de decisão de roteamento. Uma máquina situada em uma rede que tenha mais de um roteador deve também tomar uma decisão de roteamento escolhendo para qual roteador deve enviar o pacote IP.

Quando uma estação tiver de enviar uma mensagem IP para outra rede, ela deve seguir os seguintes passos:

- Determinar que a estação destino está em outra rede e, em

seguida, enviar a mensagem para um roteador.

- Determinar, por meio da tabela de rotas da máquina origem, qual roteador (*default gateway*) é o correto para enviar a mensagem.
- Descobrir, por meio do protocolo ARP, qual é o endereço MAC do roteador.
- Enviar o pacote IP com o endereço físico (MAC) de destino apontado para o roteador e o endereço IP (no pacote IP) direcionado para a máquina destino.

Uma questão importante no pacote roteado consiste no fato de que o pacote a ser roteado é endereçado fisicamente ao roteador (endereço MAC), mas é endereçado logicamente (endereçamento IP) à máquina destino. Quando o roteador recebe um pacote que não é endereçado a ele, tenta roteá-lo. A decisão de roteamento é baseada na tabela de rotas, que é parte integrante de qualquer equipamento que utilize o protocolo IP.

### 9.2.1 Tabela de roteamento

A tabela de roteamento de um roteador é basicamente composta de endereços IPs (utilizados como meio de acesso a diferentes redes), pela interface física (Ethernet ou serial) e pelo endereço IP que será utilizado para alcançar o endereço da rede informado na primeira opção. Uma vez que possua essas informações, o roteador pode gerar a tabela de roteamento. A tabela deve possuir todos os caminhos de que a rede local precise, para trocar informações com outras redes, locais ou a própria Internet. Caso exista algum pedido cujo destino não esteja na tabela de roteamento, o roteador o direcionará a um caminho-padrão.

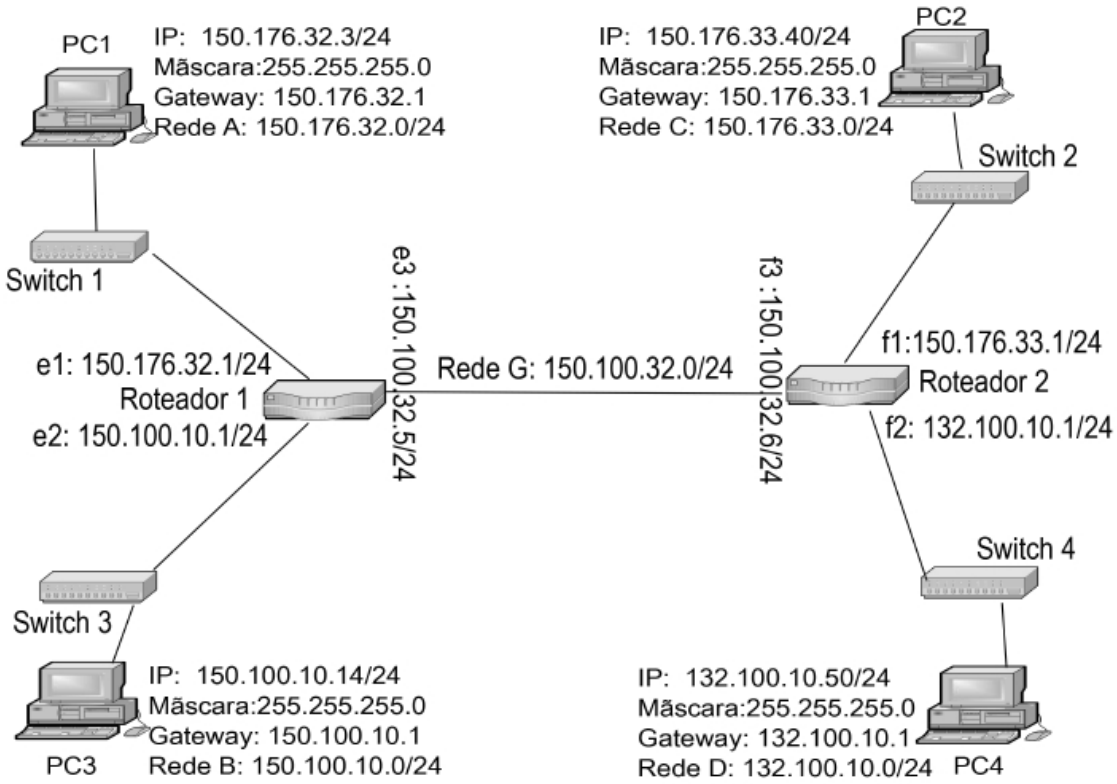
A figura 9.1 será utilizada para entendermos melhor como funciona a tabela de roteamento.

### 9.2.2 Processo de roteamento

Para determinar para onde se destina cada pacote, o roteador deve ler o cabeçalho IP de cada pacote. Cada pacote IP contém o endereço IP destino, que é utilizado pelo roteador para comparar com as entradas da tabela de roteamento e tomar as decisões por onde

rotear. Uma vez que o roteador tenha lido o endereço IP de destino do cabeçalho, ele comparará o endereço de rede, ao qual o endereço pertence, com todos os outros valores na sua tabela de roteamento. Se achar a rede do equipamento destino em sua tabela de roteamento, transmitirá o pacote pela interface associada, e sua tarefa será concluída; do contrário, enviará o pacote para uma rota-padrão.

Para entendermos melhor, tomamos a figura 9.1 como exemplo. O roteador 1 recebe um pacote em sua interface e1 (Ethernet 01) com um endereço de destino 150.100.10.200. Nesse caso, o roteador analisará em sua tabela de rotas se existe alguma interface de rede que possua o endereço de rede 150.100.10.0. Sendo esse o caso, o roteador identificará que a interface de rede que contém esse endereço de rede corresponde a e2 (Ethernet 02).




## Tabela de roteamento

Roteador 1

Interface - e1: 150.176.32.1/24
Interface - e2: 150.100.10.1/24
Interface - e3: 150.100.32.5/24

| Rede | Gateway |
|---|---|
| A | e1 |
| B | e2 |
| G | e3 |
| C e D | f3 |

Roteador 2

Interface - f1:150.176.33.1/24
Interface - f2: 132.100.10.1/24
Interface - f3: 150.100.32.6/24

| Rede | Gateway |
|---|---|
| C | f1 |
| D | f2 |
| G | f3 |
| A e B | e3 |

*Figura 9.1 – Tabela de roteamento.*

Como segundo exemplo, vamos supor que um pacote chegue à interface e1 com um endereço IP destino igual a 150.176.33.100. O roteador 1 procurará em sua tabela de roteamento se possui alguma interface de rede que esteja configurada com esse endereço de rede. Nesse caso, o roteador 1 deverá encontrar em sua tabela de rotas a seguinte sequência: para alcançar a rede 150.176.33.0, deve-se

enviar os pacotes para a interface de rede f3, a qual deverá resolver a requisição com sucesso. Essa rota informa que qualquer pacote com endereço IP de destino que chegue ao roteador 1 igual a 150.176.33.0 ou 132.100.10.0 deve ser enviado ao endereço IP definido por f3.

Caso não existisse rota para as redes C e D presente no roteador 1 e o roteador 1 não possuísse uma rota-padrão, seria remetida ao computador origem uma mensagem gerada pelo protocolo ICMP que, por sua vez, deveria dizer que o destino é inalcançável (*Destination Unreacheable*).

Consideremos que seja emitido um comando *ping* de um computador da rede A para a rede 132.100.10.0 (rede D). De acordo com a tabela de roteamento da figura 9.1, o resultado seria um *ping* com sucesso; Contudo, caso as rotas C e D da interface f3 estivessem presentes e as rotas A e B da interface e3 do roteador 2 não estivessem presentes, o protocolo ICMP geraria uma mensagem de tempo esgotado, pois o pedido chegou ao destino, ou seja, foi alcançado, mas não será possível devolvê-lo ao emissor.

Assim, chegamos à conclusão de que os dois roteadores do exemplo devem ser configurados adequadamente. No entanto, levando-se em conta que a Internet possui milhares de roteadores com milhares de entradas, se fôssemos realizar essa configuração manualmente, teríamos um enorme problema e possivelmente não encontraríamos tempo para concluir essa atividade. Para solucionarmos esse problema, utilizamos os protocolos de roteamento que comentaremos neste capítulo.

A seguir, explicaremos a tabela de roteamento gerada por uma estação conectada a uma rede com acesso à Internet e a tabela de roteamento obtida de um roteador.

### 9.2.3 Exemplos de tabela de roteamento

Depois de ser executado na console de um sistema operacional Windows, o comando route print retorna a uma tabela de rotas, conforme apresentado na tabela 9.1.

*Tabela 9.1 – Tabela de roteamento de um computador*

| Endereço de rede | Máscara | Endereço de gateway | Interface | Custo | Descrição |
|---|---|---|---|---|---|
| 0.0.0.0 | 0.0.0.0 | 167.10.6.1 | 167.10.7.202 | 1 | Essa é a rota para seu gateway-padrão (167.10.16.1) estabelecida via DHCP (dinâmico) ou nas propriedades TCP/IP do sistema operacional de forma manual. |

| Endereço de rede | Máscara | Endereço de gateway | Interface | Custo | Descrição |
|---|---|---|---|---|---|
| 127.0.0.0 | 255.0.0.0 | 127.0.0.1 | 127.0.0.1 | 1 | Endereço do localhost, endereço reservado para teste local de conectividade de driver e outros. Gateway e interface são as mesmas. Essa rota diz para manter interno todo o tráfego para esse destino, em vez de enviá-lo para fora pela rede local, uma vez que simplesmente deverá retornar ao local de origem. |
| 167.10.6.0 | 255.255.254.0 | 167.10.7.202 | 167.10.7.202 | 1 | Essa é a rota para todos os endereços de sua rede local. Perceba que seu Gateway e sua interface são os mesmos. |

| Endereço de rede | Máscara | Endereço de gateway | Interface | Custo | Descrição |
|---|---|---|---|---|---|
| 167.10.7.202 | 255.255.255.255 | 127.0.0.1 | 127.0.0.1 | 1 | Essa é a rota que define que seu localhost é exatamente sua estação. Tudo que for endereçado para o meu endereço IP deverá voltar para o mesmo. |
| 167.10.255.255 | 255.255.255.255 | 167.10.7.202 | 167.10.7.202 | 1 | Essa é a rota para o broadcast da sua rede. Note mais uma vez que o Gateway e o endereço da interface são os mesmos. |
| 224.0.0.0 | 224.0.0.0 | 167.10.7.202 | 167.10.7.202 | 1 | Essa é uma rota para rede reservada. Não se usa. É chamada rede classe D. |

| Endereço de rede | Máscara | Endereço de gateway | Interface | Custo | Descrição |
|---|---|---|---|---|---|
| 255.255.255.255 | 255.255.255.255 | 167.10.7.202 | 167.10.7.202 | 1 | Essa é a rota para broadcast geral, caso o broadcast local não sirva para uma solicitação qualquer. |
| 167.10.6.1 | | | | | Default gateway ou endereço do roteador-padrão. |
| 167.10.7.202 | | | | | Endereço IP da estação. |

A tabela de roteamento obtida de um roteador é apresentada na tabela 9.2.

*Tabela 9.2 – Tabela de roteamento de um roteador*

| Destino | Endereço de gateway | Máscara | Custo | Interface |
|---|---|---|---|---|
| 200.231.191.1 | 0.0.0.0 | 255.255.255.255 | 0 | ppp0 |
| 192.168.0.1 | 0.0.0.0 | 255.255.255.255 | 0 | eth0 |
| 192.168.0.0 | 0.0.0.0 | 255.255.255.0 | 0 | eth0 |
| 127.0.0.0 | 0.0.0.0 | 255.0.0.0 | 0 | Lo |
| 0.0.0.0 | 200.231.191.1 | 0.0.0.0 | 0 | ppp0 |
| lo – Endereço de loopback. | | | | |
| eth0 – Porta serial Ethernet número 0. Um roteador pode ter várias portas Ethernet. | | | | |
| ppp0 – Porta serial que utiliza o protocolo ppp número 0. Um roteador pode ter várias portas configuradas com o protocolo ppp. | | | | |

Na tabela 9.2, percebe-se que, na primeira rota, caso chegue um pacote com o destino 200.231.191.1, deve-se utilizar a interface ppp0 (point-to-point protocol 0 – serial 0), que, no caso, corresponde

fisicamente à porta serial ligada ao modem. No entanto, se o destino for da forma 192.168.0.X, em que X é qualquer octeto (valor inteiro variando entre 0 e 254), segue pela segunda e terceira rotas, sendo utilizada a interface eth0, ou seja, a placa de rede Ethernet do roteador. A diferença entre uma rota para um destino único ou para múltiplos destinos é determinada pela máscara.

A última rota, com destino 0.0.0.0 e máscara 0.0.0.0, é a chamada rota-padrão do roteador, porque satisfaz qualquer destino, ou seja, qualquer pacote cujo roteamento não possa ser enquadrado nas rotas anteriores será enquadrado na rota-padrão. No nosso exemplo, a rota-padrão indica um roteador. Existirá um roteador alternativo sempre que o destino não estiver diretamente acessível a nenhuma porta física do roteador (interface diretamente conectada). É importante considerar que tanto um computador quanto um roteador devem possuir rotas-padrão.

A tabela de rotas é construída automaticamente pelos procedimentos de boot da máquina, mas também pode ser construída e atualizada de forma dinâmica, por meio do recebimento de pacotes de anúncios de rotas nas diversas interfaces da máquina. Serão abordadas as atualizações de tabelas de roteamento de forma dinâmica ainda neste capítulo quando tratarmos dos protocolos RIP, OSPF e IS-IS.

A seguir, será explanada a diferença entre roteamento estático e roteamento dinâmico.

### 9.2.4 Roteamento estático e roteamento dinâmico

A alimentação das informações na tabela de rotas pode ser de modo estático, de modo dinâmico ou ambos simultaneamente. Na alimentação estática, as rotas são preenchidas de forma manual, geralmente pela configuração inicial da máquina ou por um administrador de rede. Na alimentação dinâmica, protocolos como RIP, RIP2, OSPF, IS-IS ou BGP são responsáveis pela aquisição de informações sobre a topologia da rede e sobre a publicação de rotas na tabela de rotas dos roteadores envolvidos.

A criação de rotas é uma atividade que atualmente é bastante solicitada por clientes de operadoras. Apesar da facilidade dos protocolos de roteamento dinâmico, para muitos administradores de

rede a utilização de rotas estáticas ainda é uma opção fácil e rápida para conectar duas redes. Vejamos alguns exemplos sobre como criar rotas estáticas em roteadores Huawei, Cisco e Juniper. Mostraremos ainda como criar rotas estáticas em redes interligadas por VPN MPLS.

- **Roteador Huawei** – Rota estática para acesso à Internet.

  ip route-static 201.194.179.96 255.255.255.248 200.195.179.232

  Em que, 201.194.179.96 é a rede destino, 255.255.255.248 é a máscara de rede da rede destino (/29) e 200.195.179.232 é o endereço IP da interface do outro roteador conectado diretamente ao que receberá essa rota. O endereço IP do roteador que receberá o pacote deve estar diretamente conectado. Também é chamado de *nexthop*.

- Rota estática para acesso a um destino de rede privada configurado sobre VPN MPLS.

  ip route-static vpn-instance vpn00442 10.110.128.208 28 172.35.0.50

  Em que vpn00442 é o nome da VPN utilizada pelo cliente, 10.110.128.208 é a rede destino, 28 é a mascará de rede (equivale a 255.255.255.240) e 172.35.0.50 é o endereço IP da interface do outro roteador conectado diretamente ao que receberá essa rota (*nexthop*). O endereço IP do roteador que receberá o pacote deve estar diretamente conectado.

- **Roteador Juniper** – Rota estática para acesso a um destino de rede privada configurado sobre VPN MPLS.

  set routing-instances vpn00337 routing-options static route 192.168.10.0/24 next-hop 200.1.1.253

  Em que vpn00337 é o nome da VPN utilizada pelo cliente, 192.168.10.0 é a rede destino, /24 é a mascará de rede (equivale a 255.255.255.0) e 200.1.1.253 é o endereço IP da interface do outro roteador conectado diretamente ao que receberá essa rota. O endereço IP do roteador que receberá o pacote deve estar diretamente conectado.

- **Roteador Cisco** – Rota estática para acesso a um destino de rede privada.

  ip route 192.168.0.0 255.255.255.0 10.0.3.2

  Em que, 192.168.0.0 é a rede destino, 255.255.255.0 é a máscara

de rede da rede destino e 10.0.3.2 é o endereço IP da interface do outro roteador conectado diretamente ao que receberá essa rota. O endereço IP do roteador que receberá o pacote deve estar diretamente conectado.

A figura 9.2 apresenta uma rede configurada com rotas estáticas.

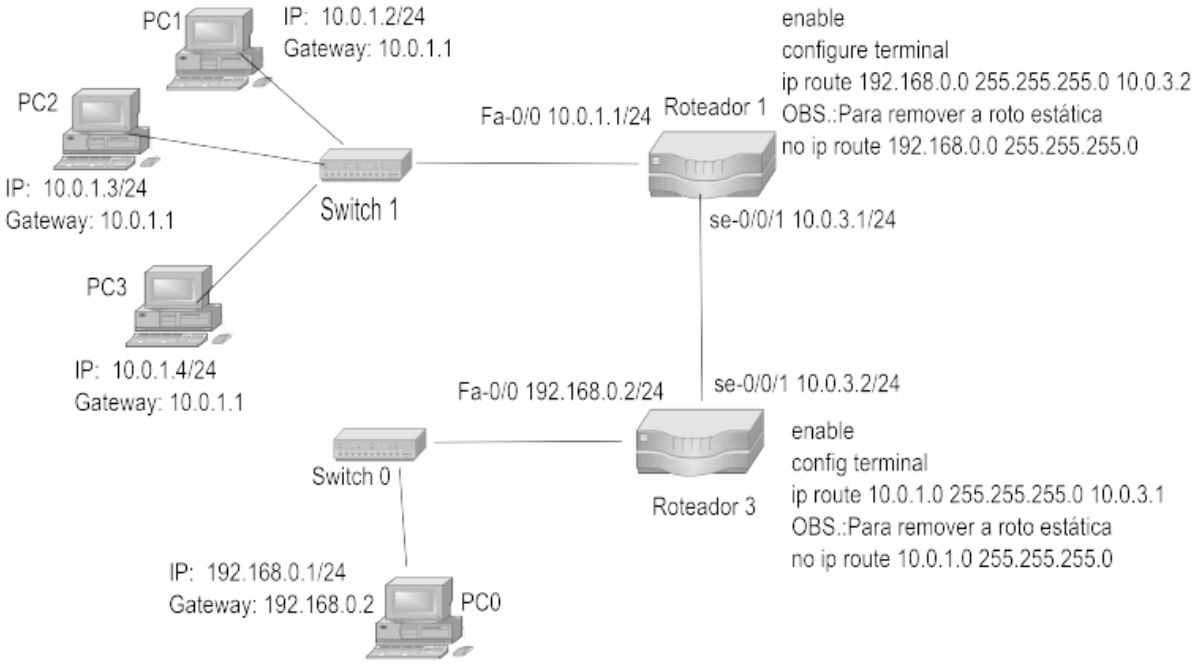



*Figura 9.2 – Exemplo do uso de roteadores configurados com rota estática.*

Conforme podemos observar, o roteador 3 possui, na interface se0/0/1, o endereço IP 10.0.3.2 e, na interface Fa0/0, o endereço IP 192.168.0.2/24. Para que o computador Laptop0 da rede 192.168.0.0/24, com endereço IP 192.168.0.1/24 e *default gateway*: 192.168.0.2/24, consiga acessar os computadores da rede 10.0.1.0/24, o roteador 3 precisa ter uma rota estática com o seguinte conteúdo: ip route 10.0.1.0 255.255.255.0 10.0.3.1, ou seja, para alcançar a rede 10.0.0.1, o roteador repassará o pacote para o endereço IP 10.0.3.1.

Em que 10.0.1.0 é a rede destino, 255.255.255.0 é a máscara de rede destino e 10.0.3.1 é o endereço roteador 1. O comando no ip route 10.0.1.0 255.255.255.0 foi colocado na figura apenas para informar sobre como remover a rota caso necessário.

É importante observar que não é suficiente apenas uma rota estática.

O roteador 1 na interface se0/0/1 possui o endereço IP :10.0.3.1/24. Para que a comunicação ocorra corretamente, esse roteador deverá também definir uma rota estática para que os pacotes saibam retornar. Assim, definimos a seguinte rota: ip route 192.168.0.0 255.255.255.0 10.0.3.2, ou seja, para alcançar a rede 192.168.0.0, o roteador repassará o pacote para o endereço IP 10.0.3.2.

Em que 192.168.0.0 é o endereço IP da rede destino, 255.255.255.0 é a máscara de rede e 10.0.3.2 é o endereço IP do roteador 3.

Conforme observado, as rotas estáticas precisam ser criadas em ambos os sentidos, caso contrário a comunicação não ocorrerá corretamente. Imagine se tivessémos 10 roteadores interligados entre si. Para que conseguíssemos nos comunicar com todas as redes, teríamos que criar inúmeras rotas, tornando essa atividade extremamente complexa. Assim, para reduzir essa administração complexa, devemos optar pelos protocolos de roteamento dinâmico.

Passaremos, agora, aos tipos de roteadores disponíveis para interligação de redes e também aos protocolos e algoritmos de roteamento dinâmico.

## 9.2.5 Tipos de roteadores

Para a interligação de redes, seja em uma residência ou em uma empresa, existem duas formas de realizar essa tarefa, utilizando um roteador interno (computador com duas ou mais placas de rede) ou um roteador externo (equipamento dedicado ao roteamento).

### 9.2.5.1 Roteadores internos

Roteadores internos são compostos pelo hardware do computador e seus componentes, pelo menos duas placas de rede Ethernet e o software de roteamento que normalmente faz parte do sistema operacional Windows ou Linux. Trata-se de uma solução fácil e econômica, porém tem-se um computador não dedicado ao roteamento específico, em que o papel do roteador é compartilhado com outras atividades do computador, como o gerenciamento de disco, do sistema operacional, aplicativos etc. O desempenho, dependendo do tamanho da rede, ficará comprometido, já que a CPU do computador atenderá às funções de roteamento e outras funções

inerentes ao sistema operacional. É importante ressaltar que essa solução deve ser empregada em pequenas e médias redes, em que o processo de roteamento não é crítico. Caso a rede seja grande e necessite de roteamento crítico, deve-se especificar um equipamento dedicado a essa tarefa.

#### 9.2.5.2 Roteadores externos

Roteadores externos são formados por hardware e software dedicados ao roteamento. Como têm funções exclusivamente voltadas ao roteamento, seu desempenho atinge índices superiores, confirmando o porquê de esses roteadores serem mais caros do que os outros. Nesse caso, o produto independe da arquitetura do hardware e software do servidor, uma vez que a ligação ao servidor é feita via portas Ethernet por meio de um hub ou switch. Como exemplo de fabricantes de roteadores dedicados e utilizados em operadoras, temos Cisco, Huawei, Juniper, entre outras.

#### 9.2.5.3 Roteamento dinâmico

Como visto anteriormente, realizar o cadastramento de todas as rotas de um roteador para uma rede de cinco lojas é simples. No entanto, quando pensamos no tráfego da Internet, milhões de rotas podem existir, sendo impossível administrar isso de forma manual. Em razão dessa necessidade, foram desenvolvidos algoritmos e protocolos que realizam essa tarefa de forma dinâmica e muito eficiente. Existem características desejáveis a todos os algoritmos de roteamento. As principais são escolha da melhor rota, simplicidade, robustez, imparcialidade, estabilidade, rapidez, convergência para o caminho ótimo, flexibilidade, aceitar parâmetros de qualidade de serviço (QoS) e ser independente da tecnologia da rede. A principal de todas essas características é, sem dúvida, a robustez. É esperado que uma rede fique funcionando sem interrupções ou falhas por anos. O algoritmo de roteamento deve ser robusto o suficiente para suportar essa grande carga.

Os protocolos de roteamento dinâmico são projetados como ferramentas para realizar várias tarefas. Os dados formatados conforme um protocolo de roteamento específico podem fornecer informações sobre:

- O *throughput* (vazão) e a qualidade dos circuitos entre os roteadores.
- O status operacional de roteadores específicos.
- O número de pontos intermediários (ou *hops*) que um pacote deverá atravessar.
- Os caminhos alternativos disponíveis em caso de falhas na rede.

O software do roteador administra essas e outras informações usando algoritmos especiais e depois determina como enviar um pacote em sua viagem entre os segmentos da rede. Assim, com base nas respostas anteriores, o roteador escolherá um entre outros caminhos possíveis para enviar o pacote. O software do roteador leva em consideração informações como a velocidade de transmissão, o retardo de propagação (o tempo em que um pacote leva para passar de uma rede a outra) e o custo. O custo de um link depende da forma como será desejado realizar o acesso, sendo por aluguel mensal de linhas privadas ou tarifa de linhas telefônicas discadas.

É possível configurar o software do roteador para usar um link redundante como alternativa ao uso do link principal, ou seja, quando o link principal fica inativo, o link redundante assume a comunicação. Esse intercâmbio entre os links ocorre de forma automática, ou seja, quando o link principal é interrompido, o roteador automaticamente pode começar a utilizar o link redundante.

Os roteadores modernos utilizam uma arquitetura adaptativa e distribuída, utilizando softwares que conseguem se adaptar a mudanças no status de um circuito ou de outro roteador em questão de milissegundos. Nesse contexto, os protocolos de roteamento possuem papel fundamental.

Os protocolos de roteamento são divididos em três tipos diferentes: os protocolos de roteamento baseados no algoritmo vetor da distância (RIP), algoritmo estado do link (OSPF e IS-IS) e algoritmo vetor de caminho (*path-vector*) (BGP). A seguir, apresentaremos os protocolos baseados nos algoritmos vetor de distância e estado do link. O protocolo baseado no algoritmo vetor de caminho será apresentado no capítulo 18.

#### 9.2.5.4 Roteamento pelo vetor da distância

Quando um roteador é configurado para operar utilizando o algoritmo

vetor da distância (*distance vector*), periodicamente propagará uma tabela com todas as rotas das redes conhecidas com a distância (saltos) necessária para alcançar cada rede. O valor da distância representa a quantidade de roteadores que estarão envolvidos entre o roteador emissor e o roteador receptor. Cada roteador, ao receber as rotas dos outros roteadores, incrementa o número de saltos e repassa tais valores aos demais roteadores.

O roteamento pelo vetor da distância usa um algoritmo denominado *Bellman-Ford Distribuído* (DBF), que divide o link entre as redes em áreas lógicas. Quando recebe um quadro, um roteador lê o endereço contido no pacote dentro do quadro e o envia em direção à área lógica do destino, baseando-se no menor número de pontos intermediários ou saltos.

O algoritmo discutido trabalha requisitando periodicamente de cada um dos vizinhos suas tabelas de roteamento. Tais tabelas contêm todas as distâncias a partir do equipamento até os outros roteadores da rede. O vetor de distâncias foi o algoritmo de roteamento original da ARPANET e ainda é usado no conhecido protocolo RIP (*Routing Information Protocol*). As vantagens desse algoritmo consistem na simplicidade e na eficiência computacional devido à sua característica distribuída.

Cada roteador mantém apenas uma entrada para qualquer outro roteador da rede e ainda não existem caminhos redundantes. No caso de haver alguma mudança topológica na rede, o algoritmo vetor de distância tem um tempo alto de convergência e tende a criar loops de roteamento. Essa tendência se agrava principalmente em condições em que os links não sejam estáveis, como é o caso das redes *ad-hoc* (redes *wireless*). Esse algoritmo funciona bem na teoria, mas, na prática, tem um sério problema chamado de contagem ao infinito (*count-to-infinity*). Esse problema pode ser resumido no seguinte enunciado: notícias boas andam rápido, notícias ruins demoram a chegar.

Isso significa que se uma nova rota melhor for encontrada, essa informação se propagará rapidamente pela rede, mas, no caso de uma queda de link, por exemplo, essa informação demorará muito para ser propagada. Em redes ad-hoc, o problema de convergência

do vetor de distância torna-se crítico, pois os nodos se movem frequentemente, causando mudanças no estado da rede. Em razão desse motivo, sua simples aplicação não é a solução mais indicada, mesmo tendo uma economia significativa em termos de banda de rede.

Outro aspecto importante é que os protocolos de vetor de distância aprendem as informações de um vizinho e, depois, passam-na para outro vizinho, sem qualquer informação sobre o roteador de origem. Isso se chama roteamento por rumor e pode causar problemas em grandes redes.

Além disso, esses protocolos utilizam atualizações periódicas e de roteamento completo. Isso significa que, em intervalos regulares de tempo (entre 30 e 90 segundos), os protocolos enviam suas tabelas de roteamento por inteiro para cada roteador vizinho, o que pode resultar em um tempo de convergência bastante grande.

A figura 9.3 apresenta uma rede configurada com o algoritmo vetor de distância:

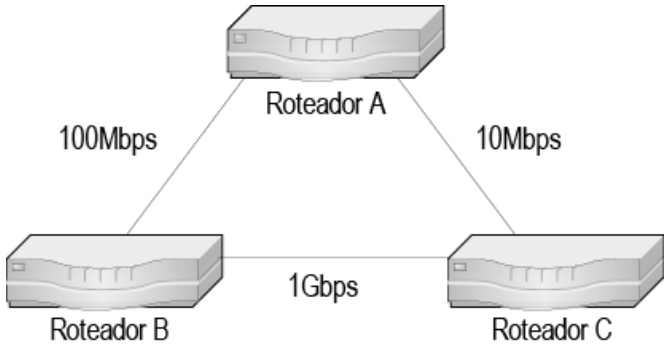



*Figura 9.3 – Rede com o algoritmo vetor de distância.*

Se os roteadores A, B e C estiverem conversando por meio de um algoritmo que segue a especificação vetor de distância, o caminho preferido entre A e C poderia ser o link de 10 Mbps, pois este possui apenas um salto de distância. Entretanto, a rota por meio do roteador B tem dez vezes mais largura de banda, embora esteja a dois saltos de distância. Além da largura de banda, poderiam ser considerados para a definição de uma melhor rota a confiabilidade, o atraso e a carga da rede. Dessa forma, para obter um melhor desempenho, grandes redes optam por utilizar um roteamento pelo estado de link. A seguir, descreveremos essa alternativa.

### 9.2.5.5 Roteamento pelo estado de link

Quando é configurado para operar utilizando o roteamento pelo estado de link, um roteador periodicamente testará se cada enlace está ativo ou não. Quando alguma alteração na topologia da rede ocorrer, um LSA (*Link State Advertisement*) será transmitido para todos os roteadores, informando para que refaçam os cálculos das distâncias. A distância presente em cada rota é calculada utilizando o algoritmo Dijkstra's SPF (*Shortest Path First*). É importante observar que quando a rede envolve vários roteadores, deve-se optar pela configuração utilizando o roteamento pelo estado de link em vez do vetor da distância.

Quando se usa roteamento pelo estado de link, algumas vantagens podem ser obtidas, como o cálculo do melhor caminho é feito localmente e não depende do cálculo de roteadores intermediários, além disso promove a divulgação das rotas de forma mais eficaz entre os roteadores.

Os protocolos codificados com base no algoritmo de roteamento pelo estado do link transportam mais informações entre os roteadores do que os que pertencem ao vetor de distância, de forma que tais protocolos exigem o uso de um processador mais poderoso para analisar as variáveis e realizar a tomada de decisões. A necessidade de hardware avançado não chega a ser um fator complicador, já que os microprocessadores modernos oferecem a capacidade necessária de tratamento de dados a preços razoáveis.

Comparados com os protocolos de vetor de distância, os protocolos de estado de link possuem muitas vantagens, as quais são apresentadas a seguir:

- Cada roteador constrói um mapa da rede distribuído e computa localmente a melhor rota por meio desse mapa. O mapa da rede mantido localmente é regularmente atualizado e permite calcular rotas mais exatas quando comparado com o algoritmo vetor de distância.
- Não possuem classes, ou seja, incluem a máscara de sub-rede com as atualizações de roteamento.
- Rápida convergência sem loops. Logo depois da inundação

(adaptação das rotas às alterações do estado dos enlaces da rede) e da computação das rotas por meio do algoritmo de Dijkstra, não existem mais loops.

- Suporte a múltiplas métricas. Podemos associar várias métricas a um mesmo enlace, diferenciando-as pela mais alta vazão, pelo menor retardo, pelo menor custo e pela mais alta confiabilidade.
- Suporte a múltiplas rotas. Nos protocolos baseados em vetor de distância, quando existem duas rotas possíveis, esse vetor escolhe aleatoriamente uma delas. Os protocolos baseados no enlace de link permitem a distribuição de tráfego por rotas alternativas, ou seja, podem escolher entre uma ou outra rota, baseando-se no congestionamento conhecido.

Os protocolos de estado de link usam atualizações direcionadas a evento, em vez de atualizações periódicas, o que, por inúmeras razões, é extremamente importante. Enviar a tabela de roteamento completo a cada 30 ou 90 segundos é desnecessário e também desperdiça largura de banda, recursos de processador e memória. Os protocolos de estado de link enviam pacotes *hello* em intervalos bastante curtos, em geral de 10 em 10 segundos. Quando um vizinho não responde, é imediatamente enviada uma atualização apenas com as informações modificadas, e não a tabela de roteamento inteira, como acontece com as redes que implementam o algoritmo vetor de distância.

A atualização de link é, então, enviada a todos os roteadores do domínio, na máxima velocidade dos processadores dos roteadores. Quando todos os roteadores na rede tiverem bases de dados idênticas de atualizações, ou seja, estiverem atualizados, eles rodam o algoritmo denominado algoritmo de Dijkstra (cada um deles). Esse algoritmo tem uma importante responsabilidade na consolidação da tabela de roteamento. O algoritmo de Dijkstra encara cada roteador como uma raiz de uma árvore e calcula o melhor caminho entre o roteador em questão e os seus links, definindo, assim, suas rotas. Para essas decisões, o roteador baliza-se na vazão, no congestionamento e na quantidade de roteadores a serem cruzados.

A seguir, detalharemos os protocolos disponíveis nos roteadores que implementam os algoritmos vetor de distância e estado de link.

### 9.2.6 Protocolo RIP

A Internet é formada por um grande número de sistemas autônomos (SA), os quais formam grupos de redes e roteadores, controlados por uma única autoridade administrativa. Os algoritmos de roteamento presentes em um sistema autônomo são chamados de IGP (*Interior Gateway Protocol*) e os algoritmos de roteamento usados entre os sistemas autônomos são chamados de EGP (*Exterior Gateway Protocol*). Com base no algoritmo de Bellman-Ford, foi criado o protocolo de vetores de distância (RIP). Embora não haja um único IGP-padrão, o RIP (*Routing Information Protocol*) é um que pode ser utilizado. Atualmente, prefere-se a utilização do protocolo OSPF, porém, para alguns clientes mais avançados, opta-se ainda pelo uso do prtocolo BGP (Border Gateway Protocol). Esse último é o protocolo utilizado pela Internet.

Os pacotes formados pelo protocolo RIP são transmitidos para uma rede por meio de datagramas UDP (*User Datagram Protocol* – protocolo de datagrama de usuário situado na camada 4 do modelo de referência TCP/IP), carregados em pacotes IP.

O protocolo RIP é do tipo vetor de distância, já que a escolha de rota é feita pela distância em número de roteadores. O funcionamento do protocolo RIP é bem simples, consistindo na divulgação de rotas de cada roteador para seus vizinhos (situados na mesma rede). Cada roteador configurado com RIPv1 divulga sua tabela de rotas por meio do envio de *broadcasts* na rede. Os demais roteadores situados na mesma rede recebem a divulgação e verificam se possuem todas as rotas divulgadas, com, pelo menos, o mesmo custo (custo é a quantidade de roteadores até o destino, de modo que quanto menor o número de pontos intermediários, mais eficiente será o caminho). Se não possuírem rota para determinada rede divulgada, mais uma entrada na sua tabela de rotas deverá ser incluída, colocando-se o roteador que a divulgou como o gateway para aquela rede. Em seguida, sua própria divulgação de rotas já conterá a rota nova aprendida. Esse processo se repete para todos os roteadores em um conjunto de redes, de modo que, depois de várias interações, todos possuirão rotas para todas as redes. Uma rota aprendida é mantida enquanto o roteador que a originou continuar divulgando.

Caso o roteador pare de divulgar a rota ou nenhuma mensagem de divulgação seja recebida dele, o roteador que havia aprendido a rota a mantém por 180 segundos, findos os quais a rota é retirada da tabela de rotas. Nesse caso, se outro roteador divulgar uma rota para aquela rede específica, esta será utilizada. No caso em que um roteador recebe rotas para uma mesma rede divulgada por roteadores diferentes, a que possuir menor custo será usada e as demais serão descartadas.

O RIP não é adaptativo e, embora seja distribuído, os roteadores que o utilizam transferem as tabelas de endereços inteiras entre si a cada 30 segundos, gerando uma *overhead* (sobrecarga) intensa. Essas atualizações frequentes podem por si só causar problemas na rede, pois se um ou mais roteadores não captarem a mensagem de atualização, suas tabelas de roteamento poderão se tornar diferentes, prejudicando a eficiência do sistema. A perda de eficiência resulta em mais atualizações perdidas, o que, por sua vez, agrava ainda mais o problema. A capacidade de retomar o tráfego normal da rede rapidamente, mesmo depois de uma perturbação grave no funcionamento dos circuitos da rede, é conhecida como convergência (o protocolo RIP é considerado um protocolo de pouca convergência).

O RIP divide os participantes da conexão em máquinas ativas e passivas. Os roteadores ativos anunciam suas rotas às demais máquinas. Já as máquinas passivas compreendem e atualizam suas rotas baseadas em anúncio, porém não anunciam como os ativos. Normalmente, os roteadores rodam o RIP em modo ativo, enquanto os computadores utilizam no modo passivo. O roteador que utiliza o RIP no modo ativo emite mensagens em *broadcast* a cada 30 segundos. Essas mensagens contêm informações do banco de dados do roteamento do roteador e consistem em um par, cada um contendo um endereço IP e a distância para a rede destino. Essa distância é calculada por meio de uma contagem métrica entre a origem e o destino.

Tal contagem tem a função de calcular os menores caminhos para agilizar as conexões. Tanto o passivo quanto o ativo da conexão RIP ouvem todas as mensagens de *broadcast* e atualizam as suas tabelas de roteamento de acordo com o algoritmo de contagem métrica. Para

prevenir as rotas de oscilações entre dois ou mais caminhos equivalentes, o RIP especifica que as rotas existentes devem ser retidas, até que uma nova rota tenha um tempo de percurso rigorosamente menor. É importante observar que o protocolo RIP não possui suporte para sub-rede [máscara de rede usando CIDR (*Classless Inter-Domain Routing*)], o que só vem a ser suportado no protocolo RIP versão 2.

Conforme comentado, o custo de uma rota é a quantidade de roteadores que uma mensagem terá de atravessar desde o roteador que possui a rota até a rede destino. O RIP não permite que o número de pontos intermediários seja maior do que 15 (16 representa que a rede é inalcançável). Portanto, os roteadores não poderão transferir pacotes para outros segmentos da rede que fiquem a mais de 16 roteadores de distância.

A figura 9.4 apresenta o formato da mensagem RIP. Nessa mensagem, as rotas divulgadas por cada roteador são incluídas na parte IP ADDRESS OF NET X. Os roteadores divulgam e recebem informações de rotas via RIP, enquanto as estações apenas aprendem as rotas (RIP passivo).

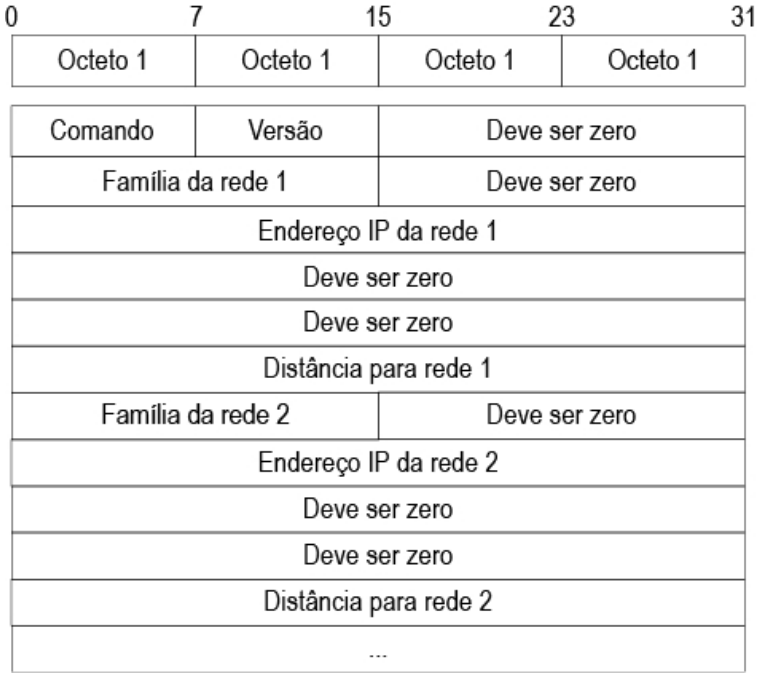



*Figura 9.4 – Mensagem do protocolo RIP.*

### 9.2.6.1 Problemas do protocolo RIP

A simplicidade do RIP (*Routing Information Protocol*) é frequentemente considerada a principal razão de sua grande popularidade. Além disso, a grande simplicidade do protocolo RIP é também a razão que o classifica como um protocolo de roteamento ineficaz.

O RIP é baseado no algoritmo distance-vector (vetor de distância) que funciona bem quando se tem uma rede WAN pequena, entretanto em grandes redes WAN problemas críticos ocorrem. A seguir, abordaremos os seguintes problemas: lenta convergência, loop de rotas/contagem ao infinito e pequena quantidade de hops (limitado a 15).

O algoritmo vetor de distância foi projetado de maneira que todas as rotas sejam compartilhadas regularmente entre os roteadores interligados. O protocolo RIP é também um grande consumidor de largura de banda, pois, a cada 30 segundos, faz um *broadcast* de sua tabela de roteamento, com informações sobre as redes e sub-redes que pode alcançar. O termo lenta convergência significa que leva relativamente muito tempo para que alterações na rede se tornem conhecidas por todos os roteadores interligados. Essa lentidão pode causar loops de roteamento.

O algoritmo distance-vector é bastante lento para identificar o problema de convergência, ou seja, quando há alteração na topologia da rede (p. ex., queda de link), essa informação demora muito tempo para ser percebida pelos roteadores envolvidos. A demora implica um roteador continuar a transmitir dados para outra rede mesmo tendo a informação de que sua conexão foi interrompida. Como o algoritmo vetor de distância demora para perceber a convergência, o roteador que identificou o problema poderá continuar enviando dados para essa rede interrompida, acreditando que um outro roteador tem a conexão ainda válida. Os pacotes de dados ficarão vagando pela rede por um período de tempo e não serão entregues ao destino.

A lenta convergência gera um outro problema: o loop de roteamento (loop entre as rotas recebidas), causado pela falta de sincronia nas informações dos roteadores. Com a figura 9.5, descreveremos como o problema de loop de roteamento ocorre. O roteador R2 recebe inicialmente uma rota para alcançar a rede A por meio do roteador R1.

Em uma situação normal, caso a conexão entre a rede A e o roteador R1 seja interrompida, o roteador R1 deverá colocar que a rota para a rede A possui um custo infinito, ou seja, número de hops (saltos) igual a 16. Quando o roteador R2 receber a tabela de roteamento de R1, identificará que o link entre R1 e a rede A foi interrompido, definindo também sua rota para a rede A através de R1 como infinita.

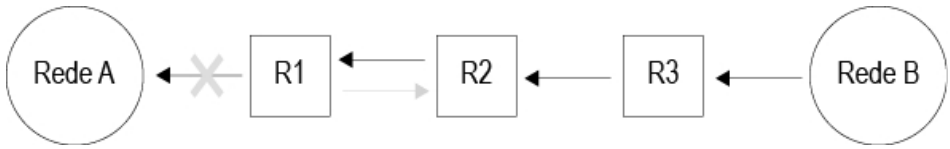



*Figura 9.5 – Trata do problema gerado pelo protocolo RIP na divulgação de suas rotas.*

Entretanto, se ocorrer o contrário, R1 perder sua conexão com a rede A e, antes de informar para R2 sua atual situação, R2 enviar sua tabela de rotas para R1, R1 perceberá que R2 possui uma rota para a rede A com custo 2 (dois roteadores para alcançar a rede A – R1 e o da rede A), assim R1 usará R2 como sua rota oficial para alcançar a rede A registrando-a com custo 3. Esse processo de um roteador usar o outro para acessar uma rede que teve seu link interrompido poderá continuar até que os roteadores percebam que para alcançar a rede interrompida o custo é 16. Quando alcançar o número de hops (saltos) igual a 16, significará que esta é inalcançável.

Para resolver o problema do loop de roteamento, foram criadas algumas alternativas conforme descrito na tabela 9.3.

*Tabela 9.3 – Técnicas para reduzir o problema de convergência*

| Técnica | Descrição |
|---|---|
| Maximum Hop Count | O protocolo RIP permite até 15 hops (saltos) entre 2 roteadores, ou seja, apenas 15 roteadores poderiam estar ligados em série. Acima disso, o RIP classifica a rede como inalcançável. |

| Técnica | Descrição |
|---|---|
| Split Horizons | Especifica que um roteador não pode enviar informações sobre rotas para a interface de onde recebeu a informação de rotas, ou seja, não deve devolver uma rota para quem a mandou. Existe também outro procedimento conhecido por Poison Reverse Update, que difere um pouco do Split Horizon. Nesse procedimento, a propagação de rotas também será feita para as interfaces de onde elas foram recebidas. Entretanto, as rotas terão métrica 16, significando inalcançáveis. Dessa forma, a rota será ignorada, fazendo que a atualização seja feita mais rapidamente. |
| Route Poisoning | Se um roteador conectado a uma determinada rede cair, ele definirá seu contador de hops (saltos) para a rede desconectada com o status de inalcançável (igual a 16). Ao receber tal informação, seu vizinho não usará esse roteador como rota alternativa para acessar outras redes. |
| Hold downs | Não aceita informações sobre uma rede depois de ela ser dada como inalcançável. Previne por um tempo (hold down timer), permitindo que o roteador restabeleça uma rota que foi interrompida com outra rede. Mesmo que o roteador receba de outro roteador uma rota para a rede já classificada como inalcançável, este não restabelecerá tal caminho até o timer chegar ao fim. |

### 9.2.7 Protocolo RIP2

O protocolo RIP é ineficiente e contém poucas informações necessárias para o roteamento de rotas por meio da rede, sendo o RIP um protocolo pouco utilizado pelas empresas configuradas em uma rede WAN. Além disso, o formato do protocolo RIP possui grande quantidade de espaço não utilizado.

No seu formato original, o protocolo RIP não considera sistemas autônomos e interações IGP/EGP, máscara de sub-redes e autenticação. A falta de máscaras de sub-rede, ou seja, utilização do CIDR, é um grande problema, pois atualmente as redes são configuradas levando em consideração esse conceito. Tentando melhorar o RIP, foi desenvolvida uma nova versão que traz as seguintes melhorias:

- Autenticação de cada mensagem trocada entre roteadores.
- *Route Tag* – utilizado para fornecer um método para separar rotas

internas trocadas entre um domínio de roteamento das rotas externas, as quais podem ser importadas de um EGP ou algum outro IGP.

- Máscara de sub-rede (CIDR).
- *Nexthop.*
- *Multicasting*.
- *Queries* – quando uma rota criada pela versão RIP2 receber uma requisição de um roteador configurado na versão RIP, ela deve responder a um pacote contendo informações que a versão original possa processar.

O protocolo RIP2 foi registrado pela RFC 2453 e, em 2007, recebeu uma atualização registrada na RFC 4822.

A inclusão do uso de *multicast* permitiu ao protocolo RIP deixar de enviar a atualização da tabela de rotas em *broadcast*. Este modo de comunicação repassa a tabela de rotas a todos os equipamentos conectados na rede. Com a utilização de *multicast* por meio do endereço IP 224.0.0.9, somente equipamentos que tenham previamente se unido (*join*) ao grupo, representado pelo endereço 224.0.0.9, receberão a atualização das tabelas de rota. Nesse modelo não haverá condições de roteadores com versões do RIP diferentes interoperarem entre si. Caso seja necessário que roteadores com versões diferentes troquem a tabela de rotas, será essencial configurar o RIP2 para também utilizar *broadcast*.

Embora o protocolo RIP seja útil em redes pequenas, recomendamos que no caso do uso de protocolos dinâmicos seja dada prioridade aos protocolos OSPF ou, ainda, ao IS-IS (*Intermediate System to Intermediate System)*. Esses dois protocolos são do tipo *link state*, isto é, consideram as informações de estado do enlace e mandam atualizações de forma otimizada, apenas quando há mudança de estado. Eles também permitem que se trabalhe com estrutura hierárquica, separando a rede por regiões ou áreas.

Caso se opte por um dos protocolos comentados RIP, OSPF ou IS-IS, a configuração de ambos deve seguir esta filosofia: o roteador somente anunciará as redes (endereço IP de rede) que estão diretamente conectadas em suas portas. Não adianta sair divulgando

inúmeras outras redes que estejam em outros roteadores. A figura 9.6 apresenta uma rede configurada com o protocolo RIP e as redes que devem ser anunciadas por meio do comando *network*.

Conforme podemos observar na figura 9.6, cada roteador anunciou somente os endereços de rede IP que possuem interface diretamente conectada. O roteador 1 anunciou as redes 10.0.1.0, 20.0.1.0 e 30.0.1.0, configuradas em suas três interfaces. O roteador 3 anunciou as redes 192.168.0.0 e 30.0.1.0, configuradas em suas duas interfaces. O roteador 0 anunciou as redes 40.0.0.0 e 20.0.1.0, configuradas em suas duas interfaces. Para configurar o protocolo RIP em roteadores Cisco, deve-se entrar no modo de configuração com os comandos enable e configure terminal. Em seguida, digitar o comando router rip e anunciar as redes com o comando network. Em outros roteadores, segue-se essa mesma filosofia.

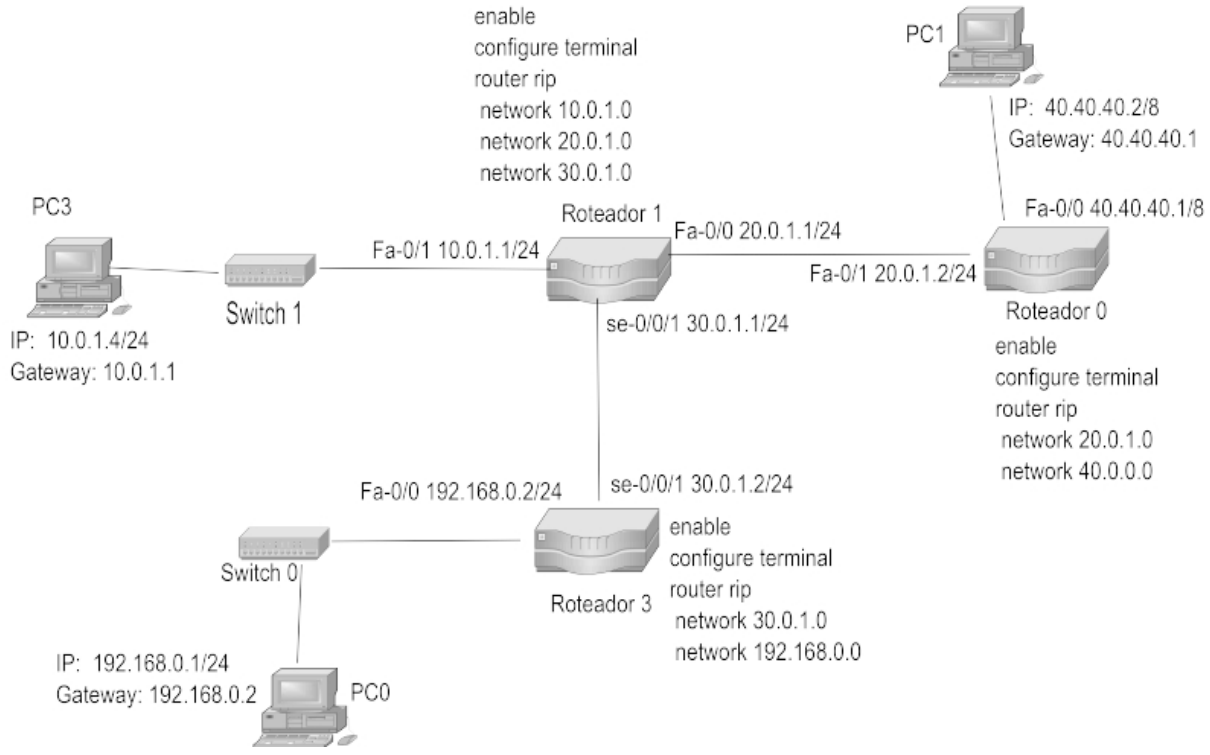



*Figura 9.6 – Rede configurada com o protocolo RIP.*

## 9.2.8 Introdução ao protocolo OSPF

O protocolo OSPF (*Open Shortest Path First*) é classificado como um protocolo *Internal Gateway Protocol* (IGP). Isso significa que o protocolo

distribui informações de roteamento entre roteadores pertencentes a um mesmo sistema autônomo (AS). Um AS se refere a grupos de roteadores que trocam informações de roteamento por meio de um protocolo de roteamento comum. É importante observar que a comunicação por meio da Internet segue por diferentes ASs, sendo cada um responsável por uma parte da comunicação entre dois pontos. Na Internet, o protocolo de roteamento utilizado é o BGP (*Border Gateway Protocol*), comentado no capítulo 18.

O protocolo OSPF é baseado no algoritmo SPF (*Shortest Path First* – primeiro caminho mais curto) e foi desenvolvido pelo grupo de trabalho IETF (*Internet Engineering Task Force*), sendo motivado pelas dificuldades apresentadas pelo protocolo RIP, um dos primeiros protocolos de roteamento. Tal protocolo foi criado para especialmente atender à rede Internet, incluindo total suporte ao protocolo IP. Entretanto, a Internet optou por outro protocolo (BGP), deixando o OSPF para ser utilizado em redes privadas conectadas sobre links dedicados ou por meio de uma VPN MPLS (*Multi-Protocol Label Switching*). As redes que operam sobre VPN MPLS são extensivamente utilizadas pelas operadoras para prover comunicação remota entre dois ou mais pontos de um cliente sob uma VPN (*Virtual Private Network*) exclusiva. Esse modelo de rede garante ao cliente um canal virtual privado sobre a rede da operadora. Nesse ambiente, há a garantia de privacidade dos dados trafegados.

Com a finalidade de suprir as deficiências do protocolo RIP, o protocolo OSPF trouxe em sua primeira versão o suporte a máscara de sub-rede, autenticação no estabelecimento de vizinhança, roteamento baseado em TOS (*Type of Service*) e *multicast* , seja para o anúncio ou recebimento de novas rotas.

Além disso, o OSPF foi especificado para ser um protocolo de roteamento que responde rapidamente a mudanças na topologia da rede, garantindo, ainda, uma pequena quantidade de dados trafegados para as atualizações.

OSPF roteia pacotes IP baseado unicamente no endereço IP destino e no *Type of Service* encontrado no header do pacote IP. Pacotes IP são roteados e não são encapsulados em nenhum outro protocolo enquanto transitam pelo link. Em virtude de ser um protocolo de

roteamento dinâmico, o protocolo OSPF rapidamente identifica uma mudança na topologia de um sistema autônomo e calcula novamente as melhores rotas para que as redes possam se comunicar.

O cálculo das novas rotas depois de uma mudança na rede é baseado no protocolo de roteamento SPF, de modo que cada roteador mantém um banco de dados idêntico descrevendo a topologia do sistema.

Uma característica que permite que o cálculo seja rápido e que exista pouco tráfego de dados entre roteadores é o fato de o protocolo OSPF permitir a criação de áreas. Cada área é formada por um conjunto de redes agrupadas. Cada área é responsável por controlar a sua política de roteamento. A figura 9.7 mostra um exemplo de uma inter-rede com várias áreas.

Na figura 9.7, os roteadores 6, 7 e 8 formam o núcleo do sistema autônomo. Se o equipamento H1 (host 1) da área 1 desejar enviar um pacote ao equipamento H2 na área 2, ele será enviado ao roteador 4, que o encaminhará para o roteador 8; o 8, por sua vez, encaminhará o pacote pelo backbone para o roteador de borda de área 2, que envia o pacote por meio de dois roteadores intra-área (roteadores 2 e 1) para ser encaminhado ao computador H2.

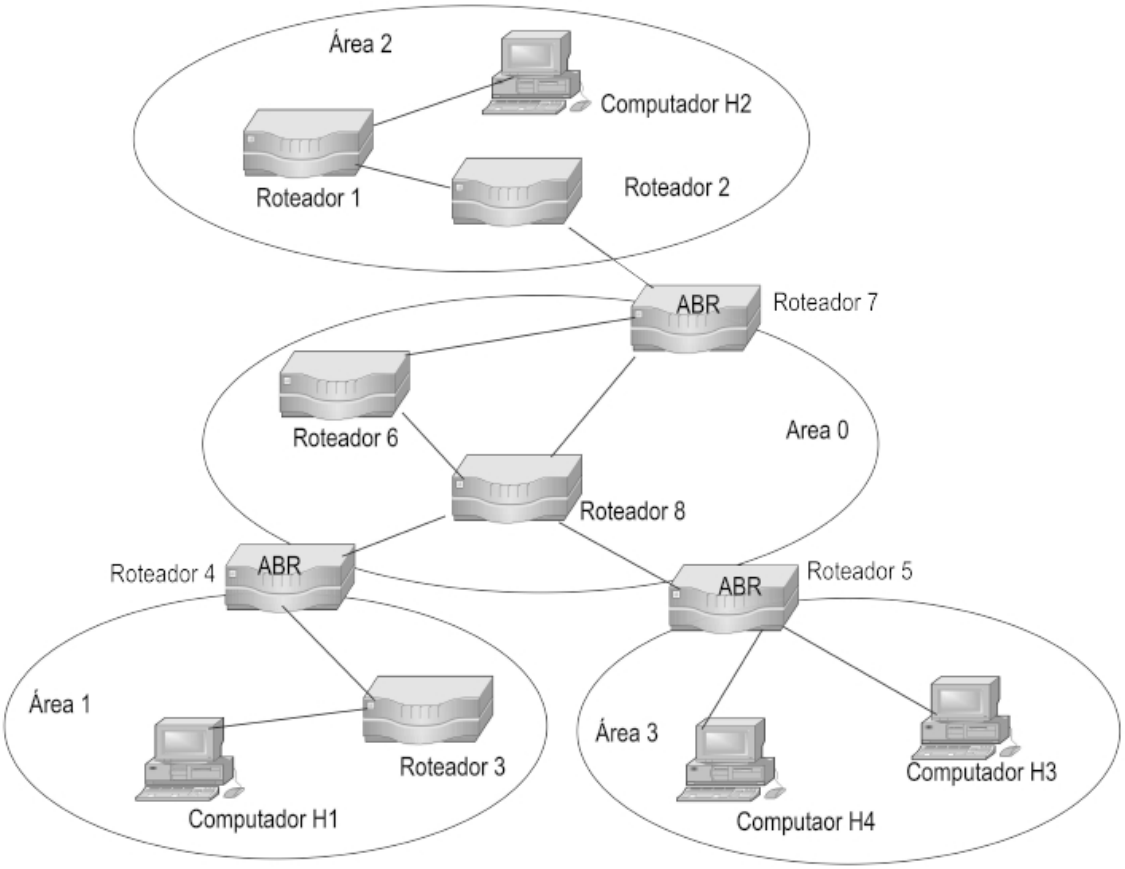



*Figura 9.7 – Múltiplas áreas ligadas por roteadores.*

### 9.2.9 O algoritmo SPF

Conforme descrito, o OSPF é um protocolo de roteamento aberto (*Open*) baseado no algoritmo SPF (*Short Path First* – primeiro menor caminho). O primeiro protocolo baseado no algoritmo de roteamento SPF foi desenvolvido para ser usado na ARPANET, sendo esse o ponto inicial para o desenvolvimento de outros protocolos, entre eles o OSPF. Desde a sua primeira concepção até termos a versão atual, algumas melhorias foram propostas, como:

- Aumento da tolerância a falhas em situações de instabilidade da rede.
- Adição de *checksum* aos pacotes *link state advertisements* (LSAs) permitiu que caso o banco de dados fique corrompido, este possa ser reatualizado; redução de dados trafegados entre o sistema autônomo.

- Capacidade de *multicast* para reduzir ainda mais a quantidade de dados trafegados.

O protocolo SPF define que, dentro de um sistema autônomo, cada roteador enviará periodicamente pacotes *hello* para descobrir e manter as relações de vizinhança, como também pacotes LSAs. O protocolo OSPF se baseia nos pacotes LSAs (*link state advertisements)* para transmitir informações de roteamento entre os roteadores vizinhos. Os LSAs coletados de todos os roteadores e redes referentes ao menor caminho formam o banco de dados de cada roteador. Sobre esse banco de dados, o roteador, através do algoritmo SPF, cria sua tabela de roteamento.

Vejamos os principais LSAs que identificamos durante a configuração de uma rede:

- **Tipo 1** – Representa um router.
- **Tipo 2** – Representa um rotador designado em um link multiaccesso (ex.: Ethernet).
- **Tipo 3** – Network link summary (rota interna), quando temos mais de uma área interligada.
- **Tipo 4** – Representa um ASBR (*Autonomous System Border Router*).
- **Tipo 5** – Representa uma rota externa ao domínio OSPF.
- **Tipo 7** – Usado em áreas NSSA.

Veremos neste capítulo os detalhes e o escopo de cada um dos LSAs apresentados. Para demonstrar os LSAs tipos 1, 2 e 3 na prática, utilizaremos a figura 9.8, que representa uma rede com o protocolo OSPF configurado com duas áreas. Os demais LSAs precisam de um cenário específico para sua visualização.

Antes de avaliarmos se a tabela de rotas foi ou não definida no roteador, precisamos nos certificar se os roteadores configurados com o protocolo OSPF estabeleceram uma relação de vizinhança. Para isso, os roteadores deverão trocar pacotes *hello* em que alguns campos que compõem o pacote serão avaliados para garantir que a vizinhança poderá ser estabelecida entre dois roteadores. O protocolo OSPF possui uma parte do cabeçalho comum a todos os tipos de LSAs seguido dos campos específicos. A figura 9.9 apresenta os

campos da parte comum do pacote OSPF.

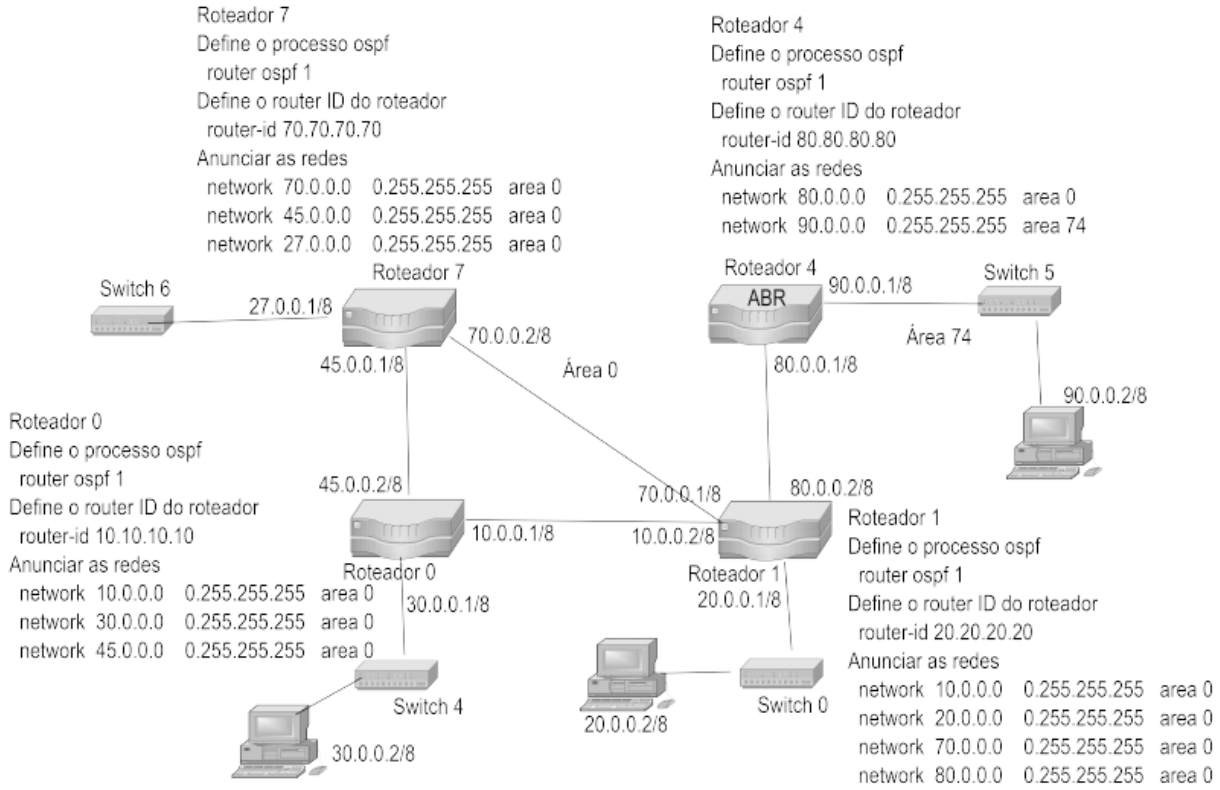



*Figura 9.8 – Rede configurada com OSPF e duas áreas.*

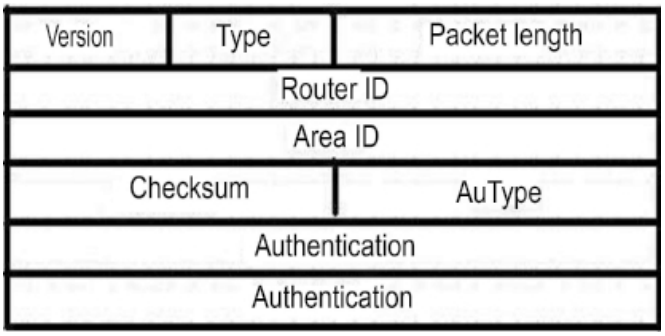



*Figura 9.9 – Pacote OSPF: parte comum.*

Vejamos os campos que compõem o cabeçalho-padrão:

- *Version* – Número da versão do protocolo OSPF.
- *Type* – Informa o tipo do pacote OSPF. Poderá receber os seguintes valores:
  - 1 – *Hello*.
  - 2 – *Database Description*.

- 3 – *Link state Request*.
- 4 – *Link state Update*.
- 5 – *Link state Acknowledgement*.

- *Packet length* – Tamanho do pacote em bytes.
- *Router ID*– Identificador do roteador do qual o pacote foi originado.
- *Área ID* – Número de 32 bits que identifica a área a que o pacote pertence.
- *Checksum* – Checksum-padrão do IP sendo calculado para o conteúdo inteiro do pacote, excetuando-se o campo de autenticação.
- *Autype* – Especifica a autenticação utilizada para o pacote, podendo ser:
  - Tipo 1 – sem autenticação. Esses bytes do pacote não são examinados.
  - Tipo 2 – com autenticação.
- *Authentication* – Campo de 64 bits utilizado para a autenticação.

Os campos que compõem o pacote *hello* seguem os campos que formam o cabeçalho-padrão do protocolo OSPF. A figura 9.10 apresenta o formato do pacote *hello*.

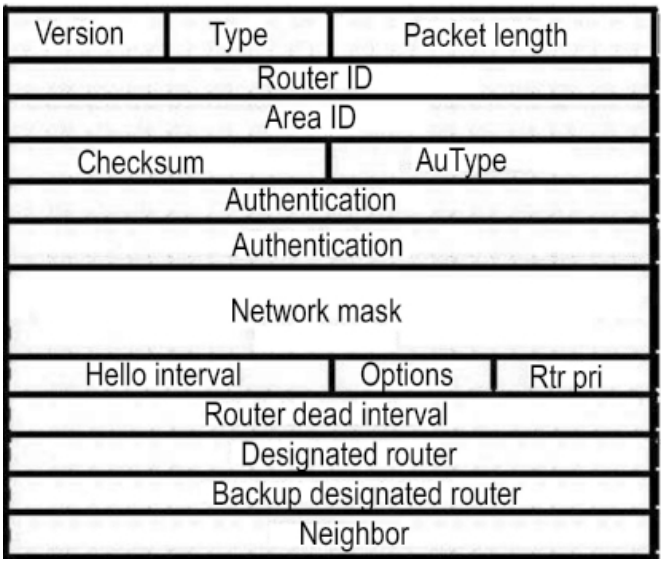



*Figura 9.10 – Itens comuns que compõe o pacote hello.*

Os campos que compõem o pacote *hello* são:

- **Máscara de rede** (*Network Mask*) – Máscara associada às interfaces para as quais se deseja enviar o pacote.
- *Hello Interval* – Número de segundos entre o envio de um e outro pacote de *hello*.
- *Options* – Opções do protocolo.
- *Rtr Pri* – Prioridade do roteador, sendo utilizada na eleição do roteador designado (DR – *Designated Router*) e do roteador designado backup (BDR – *Backup Designated Router*).
- *Router Dead Interval* – Número de segundos antes de considerar que um roteador que está em silêncio saiu fora do ar.
- Endereço IP do roteador designado (*Designated Router*).
- *Neighbor* – São os identificadores de todos os roteadores que mandaram pacotes *hello* válidos no último *RouterDeadInterval*.

Dois roteadores podem ser vizinhos, desde que no pacote *hello*, trocado entre os dois roteadores, os seguintes campos sejam iguais:

- *Area ID* – Representada por um número de 32 bits. Pode ser representada por um inteiro ou no formato de um endereço IP. A área 0 ou 0.0.0.0 é a área de backbone. Para todo processo ou domínio OSPF, terá que existir uma área com ID 0. Cada interface do roteador deverá ser configurada em uma área. Na figura 9.8, o roteador 1 teve suas três interfaces configuradas na área 0. Entretanto, o roteador 4 teve uma de suas interfaces configuradas para a área 0 e uma segunda, para a área 74. Esse campo é conduzido pelo cabeçalho-padrão do pacote OSPF.
- **Autenticação** – Define uma senha em que os roteadores inteligados deverão compartilhar. Caso na configuração de um dos roteadores seja informada uma senha diferente da esperada, a relação de vizinhança não será estabelecida e os LSAs contendo os dados necessários para gerar a tabela de roteamento não serão trocados.
- *Router Dead Interval* – Indica a quantidade de tempo que um roteador aguardará para receber um pacote *hello* do seu vizinho, antes de declarar que o vizinho está com a interface *down*. O valor-padrão definido é 40 segundos.

- *Hello Interval* – O intervalo do envio dos pacotes hello indica com que frequência o roteador OSPF transmitirá seus pacotes *hello*. Por padrão, os pacotes hello são enviados a cada 10 segundos. Caso um roteador não receba um pacote *hello* de seu vizinho em 40 segundos, precisará seguir por outra rota caso queira continuar a comunicação.
- *Stub Area Flag* – No campo opções, o valor do E-bit deve ser igual (para mais detalhes, verificar na RFC – *http://www.rfc-editor.org/rfc/rfc3101.txt*).

É importante não confundir a tabela de rotas dos roteadores com a base de dados (*database*) definida pelo protocolo OSPF. Inicialmente, o protocolo define com quais roteadores será estabelecida a relação de vizinhança e, com isso, serão trocadas informações necessárias para preencher a base de dados. Após fechar a relação de vizinhança, cada roteador poderá individualmente calcular a sua tabela de roteamento utilizando o algoritmo SPF. Para que um roteador formalize quais são seus vizinhos, enviará periodicamente pacotes *hello*. Para conhecer com quais roteadores se estabeleceu a relação de vizinhança, precisamos garantir que o estado entre os roteadores encontra-se em *FULL*. Em equipamentos da fabricante Cisco, podemos digitar o comando:show ip ospf neighbor. Executando esse comando no roteador 0, presente na figura 9.8, teremos o seguinte resultado apresentado na tabela 9.4:

*Tabela 9.4 – Vizinhos do roteador 0*

| Neighbor ID | Pri | State | Dead time | Address | Interface |
|---|---|---|---|---|---|
| 20.20.20.20 | 1 | FULL/DR | 00:00:35 | 10.0.0.2 | FastEthernet0/0 |
| 70.70.70.70 | 1 | FULL/DR | 00:00:35 | 45.0.0.1 | Ethernet1/0 |

Conforme observado, o roteador 0 estabeleceu uma relação de vizinhança com o roteador 1 identificado com *router-id* 20.20.20.20 e com o roteador 7 identificado com router id 70.70.70.70. Executando esse mesmo comando no roteador 1, presente na figura 9.8, teremos o seguinte resultado apresentado na tabela 9.5:

*Tabela 9.5 – Vizinhos do roteador 1*

| Neighbor ID | Pri | State | Dead time | Address | Interface |
|---|---|---|---|---|---|
| 80.80.80.80 | 1 | FULL/DR | 00:00:37 | 80.0.0.1 | Ethernet1/0 |
| 70.70.70.70 | 1 | FULL/DR | 00:00:37 | 70.0.0.2 | Ethernet1/1 |
| 10.10.10.10 | 1 | FULL/BDR | 00:00:38 | 10.0.0.1 | FastEthernet0/0 |

Conforme observado, este roteador fechou uma relação de vizinhança com os roteadores com *router-id* 10.10.10.10, 70.70.70.70 e 80.80.80.80, configurados nos roteadores 0, 7 e 4, conforme demonstrado na figura 9.8. Executando esse mesmo comando no roteador 4, presente na figura 9.8, teremos o seguinte resultado apresentado na tabela 9.6:

*Tabela 9.6 – Vizinhos do roteador 4*

| Neighbor ID | Pri | State | Dead time | Address | Interface |
|---|---|---|---|---|---|
| 20.20.20.20 | 1 | FULL/BDR | 00:00:37 | 80.0.0.2 | FastEthernet0/0 |

Conforme observado, este roteador fecha uma relação de vizinhança com o roteador identificado com *router-id* 20.20.20.20, configurado no roteador 1, conforme demonstrado na figura 9.8.

Executando esse comando no roteador 7, presente na figura 9.8, teremos o seguinte resultado apresentado na tabela 9.7:

*Tabela 9.7 – Vizinhos do roteador 7*

| Neighbor ID | Pri | State | Dead time | Address | Interface |
|---|---|---|---|---|---|
| 20.20.20.20 | 1 | FULL/BDR | 00:00:38 | 70.0.0.1 | FastEthernet0/0 |
| 10.10.10.10 | 1 | FULL/BDR | 00:00:38 | 45.0.0.2 | FastEthernet0/1 |

Conforme observado, este roteador fecha uma relação de confiança com os seguintes roteadores vizinhos: roteador 1 com *router-id* 20.20.20.20 e roteador 0 com router id 10.10.10.10. Podemos

observar na figura 9.8 que o roteador 7 realmente está ligado fisicamente a esses dois outros roteadores. Cada um dos comandos executados apresentou várias colunas. Vejamos o que cada uma delas representa:

- *Neighbor ID* – Esta coluna representa o *router-id* do roteador vizinho. O *router-id* pode ser configurado manualmente. Caso não seja o valor do *router-id*, poderá ser representado pelo endereço de loopback do roteador ou, ainda, pelo maior endereço IP entre as interfaces configuradas. A preferência que os roteadores dão para assumir o valor do *router-id* será o endereço IP atribuído manualmente usando o comando router-id x.x.x.x e, caso não seja, optarão pelo maior endereço IP entre as interfaces do roteador. Podem ainda utilizar o endereço IP de loopback configurado no roteador para ser o rouer-id. É importante observar que após o roteador definir o *router-id*, seu valor não mudará, enquanto o rotedor permanecer ligado. Para perceber a mudança, caso seja feita, o roteador precisará reinicializar o processo ospf com o comando clear ip ospf process 1 (ex.: comando do fabricante Cisco) ou reinicializar o roteador. Outro ponto importante a ser observado é que o endereço do *router-id* não precisa necessariamente ser alcançado por meio do comando *ping*.
- *Pri (Priority)* – Esta coluna formaliza a prioridade atribuída à interface do router vizinho no qual os roteadores estão conectados. Para ajustar a prioridade de uma das interface de um roteador, primeiramente se acessa a interface do roteador com o comando interface ethernet 0/1, por exemplo. Em seguida, ajusta-se a prioridade com o comando ip ospf priority 5 (ex.: comandos-padrão Cisco). Neste caso, definimos que a interface Ethernet 0/1 terá prioridade igual a 5. Esse valor é utilizado para a eleição do roteador designado (DR). O roteador com a maior prioridade será eleito o DR. Caso tenhamos na rede roteadores com o mesmo valor de prioridade, será eleito o DR, o roteador com maior *router-id*. Por padrão, todas as interfaces dos roteadores Cisco e Huawei possuem prioridade igual a 1. Roteadores Juniper possuem prioridade-padrão igual a 128. Caso tenhamos um roteador com prioridade igual a 0, este nunca poderá ser eleito como DR ou BDR

(roteador designado *backup*). Com essa configuração, o roteador será chamado de DROTHER, ou seja, nem será um DR nem BDR. Comentaremos neste capítulo sobre os roteadores designados e roteadores designados backup, como também sobre o termo DROTHER.

- *State* – Quando estiver igual a *FULL,* o estado significará que o roteador e seu vizinho têm bancos de dados (*link state* OSPF) idênticos e o algoritmos SPF poderá ser executado para definir o menor caminho entre os roteadores. É importante observar que até alcançar o estado de *FULL,* o roteador passará por outros sete estados, os quais vemos a seguir:
  - **Estado de** *down* – É o primeiro estado em que dois roteadores ficarão ao estabelecer uma conexão física. Após a conexão física, poderão se tornar vizinhos. Neste estado, nenhum pacote *hello* foi recebido, porém existe a posibilidade de ainda receber. Esse estado também poderá ser visualizado nos casos de um roteador vizinho em estado *FULL* não receber uma pacote hello dentro do tempo definido pelo parâmetro *Dead Interval* (ex.: por padrão, o *Dead Interval* é igual a 4 * o tempo para o envio do pacote *hello*, ou seja, 10 * 4 = 40 segundos). Neste caso, o estado passará de *full* para *down*. Caso a interface de um dos roteadores seja manualmente desconfigurada, o estado também permanecerá em *down*.
  - **Estado de** *attempt* – Está presente em redes do tipo NBMA (*Non-Broadcast Multiple Access*), como X.25, Frame Relay ou ATM. Essas redes são capazes de conectar mais de dois roteadores, mas não possuem a capacidade de broadcast, ou seja, todos os pacotes OSPF são enviados em *unicast* Todos os pacotes devem ser especificamente endereçados a roteadores da rede. Um pacote enviado a um dos roteadores não é recebido pelos demais roteadores. Roteadores OSPF em redes não *broadcast* elegem um roteador designado (DR) e um roteador designado backup (BDR). Redes do tipo NBMA são pouco utilizadas atualmente.
  - **Estado de** *init* – Define que a interface do roteador configurada com OSPF recebeu seu primeiro pacote *hello*, vindo de um potencial roteador vizinho. Ao enviar o pacote hello, o emissor

incluirá seu *router-id*. Ao devolver o pacote *hello*, o roteador destino também incluírá seu *router-id* e mudará para o estado *init*. Com isso, nesta comunicação o pacote *hello* conterá 2 routers-id (obs.: no pacote *hello,* existe um campo do tipo vetor que comporta o transporte de um ou mais *router-id*). Quando o roteador emissor receber o pacote *hello* de volta, visualizará seu próprio *router-id* e mudará seu estado para *two-way*. O mesmo ocorrerá na próxima comunicação com o roteador destino. Caso o roteador destino não devolva um pacote *hello* por 40 segundos (*dead interval*), o roteador origem colocará sua interface em estado de *down*. A figura 9.11 apresenta a interação entre os roteadores nos estados *init* e *down*.

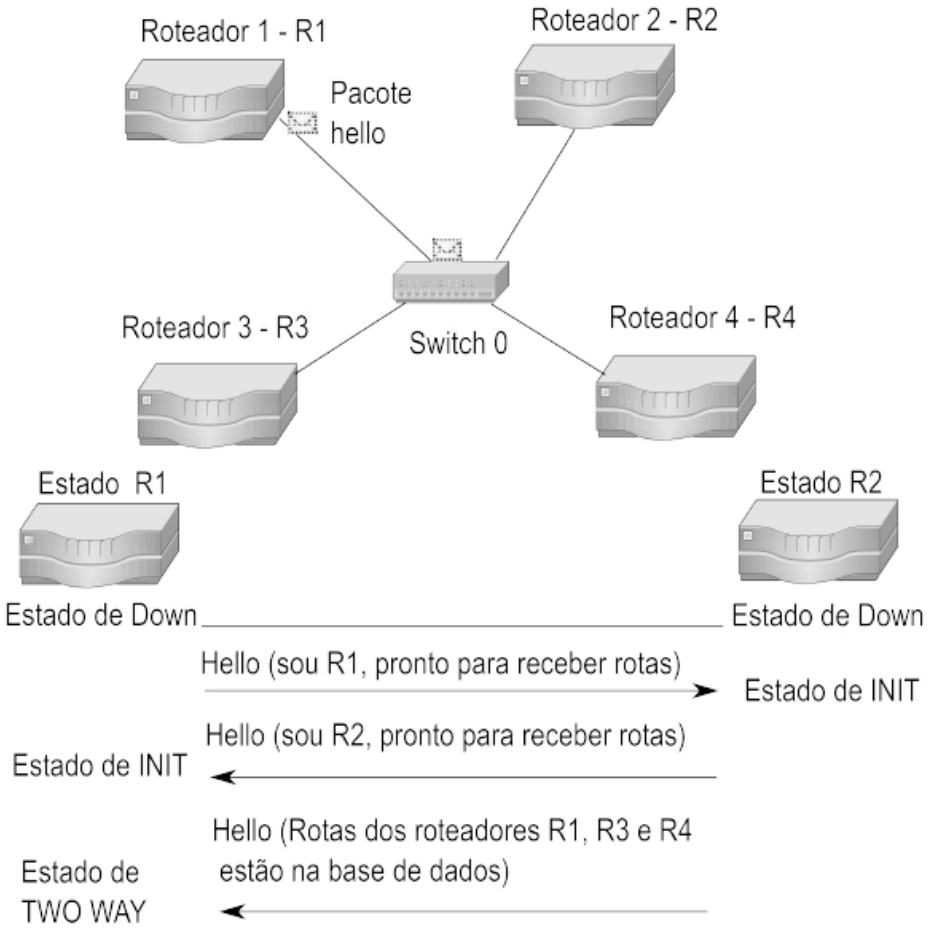



*Figura 9.11 – Trocas de pacotes hello nos estados down e init.*

- **Estado de** *two-way* – Define que existe comunicação bidirecional entre dois roteadores vizinhos. Esse estado ocorre quando o

roteador se vê no pacote *hello* recebido de um roteador vizinho. A passagem desse estado para o próximo marcará o início da troca de LSAs que formarão a base de dados do OSPF.

- **Estado de** *exstart* – Definirá entre dois roteadores vizinhos qual deles será o mestre (*master*) e qual será o escravo (*slave*). O roteador com o maior *router-id* tornar-se-á o *master*. Após essa definição, segue-se para o próximo estado e inicia-se a troca de pacotes DD (*DataBase Descriptor*) contendo os diferentes tipos LSAs.
- **Estado de** *exchange* – Nos estados anteriores foram trocados pacotes do tipo *hello*, e neste estado os roteadores trocarão um segundo tipo de pacote OSPF chamado DD (*DataBase Descriptor*). Esses pacotes trocados conterão diferentes tipos de LSAs que formarão a base de dados utilizada pelo algoritmo SPF para determinar os menores caminhos entre as redes envolvidas.
- **Estado de** *loading* – Neste estado ficarão os roteadores que perceberem alguma nova informação referente a uma nova rede, um novo custo (métrica) ou, ainda, que um dos links foi interrompido. Sempre que um roteador receber um pacote DD, avaliará se existe alguma informação nova. Se houver novidades, o roteador solicitará ao roteador vizinho mais detalhes para compor sua base de dados. Para solicitar tais informações, utilizará um terceiro tipo de pacote OSPF chamado LSR (*Link State Request*). O roteador vizinho devolverá as informações solicitadas utilizando um quarto tipo de pacote OSPF chamado LSU (*Link State Update*).
- **Estado** *full* – Neste estado, a relação de vizinhança estará completa, assim os roteadores vizinhos terão suas bases de dados topológicas exatamente iguais e cada um poderá executar o algoritmo SPF (conhecido também por Dijkstra) para determinar o menor caminho para alcançar todas as redes envolvidas no backbone da rede.

Anexo ao estado, percebemos uma barra (/) seguida dos termos DR (*Designated Router* – Roteador Designado), BDR (*Backup Designated Router* – Roteador Designado Backup) ou DROTHER (não eleito como DR ou BDR). Esse resultado dependerá da forma em que os

roteadores foram interligados. Quando a ligação entre dois roteadores se der na arquitetura ponto a ponto sobre um link Ethernet, uma das portas será eleita DR e a outra, BDR (Figura 9.8). Em uma ligação em que os links forem seriais (Figura 9.16), não teremos a eleição dos roteadores DR e BDR. Perceberemos o termo DROTHER em redes em que as interfaces dos roteadores estiverem sendo interligadas por um switch em uma rede Ethernet (Figura 9.17).

- *Dead Time* – Informa a quantidade de tempo que o roteador esperará para receber um pacote *hello* de seu vizinho antes de considerar o vizinho inativo. Esse valor é redefinido quando a interface recebe um pacote *hello*. Conforme podemos observar no resultado do comando executado no roteador 0, o valor do *dead time* estava em 00:00:35. Esse valor será decrementado até alcançar 0. Quando isso ocorrer, a comunicação ficará no estado *down*.
- *Address* – Informa o endereço IP da interface do roteador vizinho.
- *Interface* – Refere-se à identificação da interface do roteador que possui OSPF habilitado.

É importante observar que basicamente as informações mantidas e utilizadas pelo algoritmo SPF para determinar a melhor rota são endereço IP das interfaces conectadas e custo associado ao link (custo também conhecido por métrica). O custo de uma interface OSPF é uma indicação do esforço necessário para o envio dos pacotes através dessa interface.

A métrica do protocolo OSPF é definida pela RFC 2328 e recomenda que o custo deve ser associado com o lado de saída de cada interface do roteador. Esse custo pode ser configurado pelo administrador da rede. O roteador sempre optará por enviar um pacote para a interface que apresentar menor custo. É importante observar que a RFC 2328 não especifica quais valores devem ser utilizados para determinar o custo. Nos equipamentos da fabricante Cisco, o custo de uma interface é inversamente proporcional à largura de banda dessa interface. Para sabermos o custo de um link, utilizamos:

custo = ((10 ^ 8)/largura de banda em bps), onde 10 ^8 equivale a 100 Mbps. Assim temos 100 Mbps/largura de banda em bps.

Caso o link tenha banda acima de 100 Mbps, utiliza-se 1 ou, ainda, podemos com esse fabricante utilizar a opção custo automático por meio do comando auto-cost reference-bandwidth <VALOR>. Para verificar o custo de uma rota, precisamos avaliar o resultado da tabela de rotas utilizada pelo roteador. Dessa forma, para avaliar o custo, utilizamos o comando show ip route para a fabricante Cisco, display ip routingrouting-table para a fabricante Huawei ou show route table para a fabricante Juniper.

Em um roteador do fabricante Huawei, vejamos como podemos avaliar com quais vizinhos a relação de vizinhança foi estabelecida. Para conferir se as interfaces estabeleceram a relação de vizinhança, executamos o comando:

dis ospf 33 peer brief

O resultado poderá ser observado na tabela 9.8.

OSPF Process 33 with Router ID 172.172.172.172

Peer Statistic Informations

*Tabela 9.8 – Vizinhos de um roteador Huawei*

| Area Id | Interface | Neighbor id | State |
|---|---|---|---|
| 0.0.0.0 | GigabitEthernet1/1/0.1127 | 2.1.1.10 | Full |
| 0.0.0.0 | GigabitEthernet1/1/2.1118 | 2.1.1.1 | Full |
| 0.0.0.0 | GigabitEthernet1/1/2.1139 | 2.1.1.5 | Full |

Conforme comentado, após a relação de vizinhança ser estabelecida, o estado ficará como full. Durante esse processo, os roteadores trocam vários LSAs. Assim, veremos as particularidades de cada um dos LSAs mais observados durante a utilização do protocolo OSPF em redes privadas.

## 9.2.10 LSA – Link State Advertisement

Conforme comentado, antes de o algoritmo SPF ser executado em cada um dos roteadores, cada um que estabeleceu uma relação de vizinhança deverá conter uma base de dados idêntica um ao outro. Essa base de dados será utilizada pelo algoritmo SPF para definir as

melhores rotas. Tais informações serão trocadas através dos pacotes chamados LSAs (*Link State Advertisements*). Os principais tipos que comentaremos serão:

- **Tipo 1** – LSAs trocados entre roteadores de uma mesma área.
- **Tipo 2** – LSAs trocados entre roteadores de uma mesma área com o roteador designado (DR e BDR).
- **Tipo 3** – LSAs trocados entre roteadores classificados como ABR e que pertencem a duas áreas diferentes. Em nosso exemplo, temos como ABR o roteador 4 da figura 9.8.
- **Tipo 4** – LSAs trocados entre roteadores classificados como ASBR (*Autonomous System Border Router*).
- **Tipo 5** – LSAs que transportam rotas externas ao domínio OSPF.

Basicamente, quando avaliamos o resultado do comando show ip ospf database (utilizado pelo fabricante Cisco) em redes configuradas com OSPF envolvendo duas áreas, verificamos quatro tipos de LSAs, os quais abordaremos em detalhes neste capítulo. Para os demais utilizados, precisamos criar um cenário específico para tal.

Todo pacote LSA começa com um cabeçalho-padrão de 20 bytes. Cada roteador durante o estabelecimento da relação de vizinhança originará um ou mais LSAs tipo 1, chamados de router-LSA. Além disso, sempre que o roteador for eleito roteador designado, este originará um LSA tipo 2 chamado network-LSA. Caso a rede possua a interligação de duas áreas diferentes, teremos também a troca de LSAs tipo 3 chamados summary-LSA. Outros tipos de LSAs também poderão ser originados, dependendo da configuração aplicada aos roteadores. Essa coleção de LSAs formará a base de dados dos roteadores vizinhos chamada *link state database* (conforme comentado, essa base será utilizada pelo algoritmo SPF). A figura 9.12 apresenta o formato do cabeçalho LSA sem levar em consideração os campos que compõem os tipos específicos dos LSAs (tipo 1, 2, 3, 4 ou 5). Cada tipo possui uma extensão no cabeçalho.

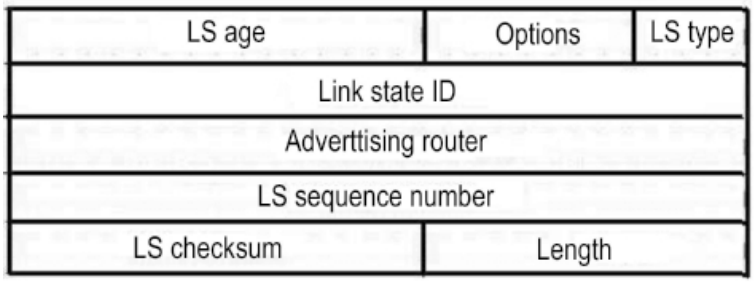



*Figura 9.12 – Itens comuns do cabeçalho do pacote LSA.*

Vejamos o conteúdo do pacote LSA, sem levar em consideração as especifidades dos diferentes tipos que comentaremos neste capítulo:

- *LS age* – Tempo em segundos desde que o LSA foi gerado.
- *Options* – Refere-se às capacidades opcionais do OSPF.
- *LS Type* – Tipo do LSA. Há cinco tipos diferentes de *link state advertisement*:
  - *Router link advertisement* (tipo 1) – São anúncios originários de todos os roteadores de uma determinada área, sendo espalhados pela mesma.
  - *Network link advertisement* (tipo 2) – São anúncios gerados pelo roteador designado em redes multi-acesso, contendo a lista de roteadores numa determinada rede.
  - *Summary link advertisement* (tipos 3, 4) – São gerados pelos roteadores ABR (Area Border Routers) e espalhados para a área associada, descrevendo rotas para destinos fora dessa área, mas pertencentes ao mesmo sistema autônomo (SA). O tipo 3 diz respeito a rotas para redes, enquanto o tipo 4 diz respeito a rotas para roteadores de fronteira do SA.
  - *AS external link advertisement* (tipo 5) – São gerados pelos roteadores ASBR (AS boundary routers) e espalhados para toda o SA. Esse tipo de anúncio descreve rotas para destinos fora do SA.
- *Link State ID* – Identifica um endereço IP que mudará seu conceito, dependendo do tipo do LSA. Esse campo assumirá valores dependendo do tipo do LSA apresentado a seguir:
  - **LSA tipo 1** – Router ID do roteador que gerou o LSA.
  - **LSA tipo 2** – IP do roteador designado da rede.
  - **LSA tipo 3** – ID da rede de destino.

- **LSA tipo 4** – Router ID do ASBR.
- **LSA tipo 5** – IP da rede de destino.

- *Advertising Router* – Identifica o router-is do roteador que gerou o LSA (*link state advertisement*).
- *LS sequence* – Funciona como uma espécie de contador de LSA, sendo utilizado na detecção de LSAs (*link state advertisement*) antigos ou duplicados.
- *LS checksum* – Checksum do conteúdo completo (com exceção do LS *age*) do LSA.
- *Length* – Informa o comprimento do LSA em bytes, incluindo o cabeçalho.

### 9.2.10.1 LSA tipo 1 – Router Links Advertisements

Os LSAs do tipo 1 são gerados e trocados pelos roteadores somente dentro da área que pertencem. A figura 9.13 apresenta o ambiente em que os LSAs do tipo 1 são trocados entre os roteadores.

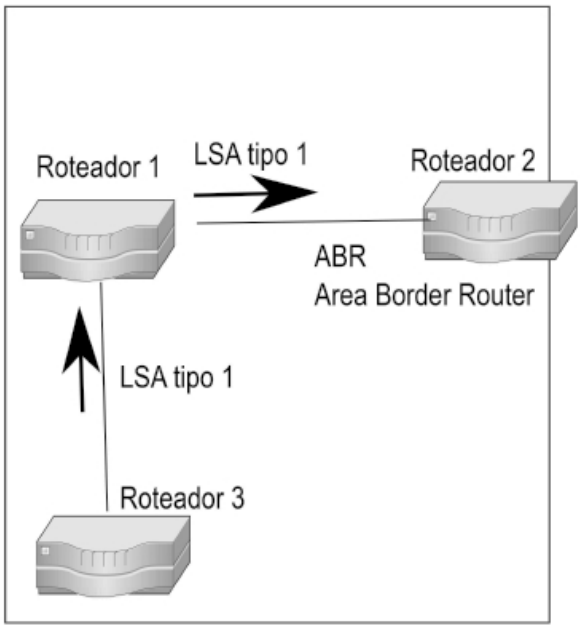



*Figura 9.13 – LSAs do tipo 1 são trocados na área 0.*

Cada roteador em sua área origina um ou mais LSAs do tipo 1. O LSA do tipo 1 descreverá e anunciará, entre outras informações, o estado e o custo das conexões do roteador para a área. Todos as conexões do roteador para a área são concentradas em um único LSA

do tipo 1. A figura 9.14 apresenta o formato do pacote LSA tipo 1. Nela, podemos observar que ao final do pacote existe um vetor em que são registrados os routers-ids dos roteadores contidos na área.

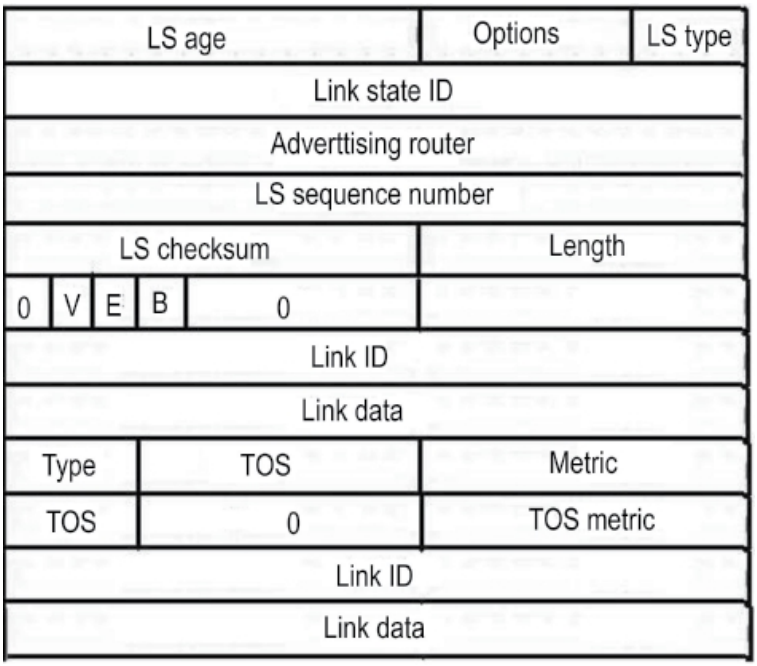



*Figura 9.14 – Formato do pacote-padrão LSA do tipo 1.*

Vejamos o que cada campo do pacote LSA tipo 1 representa: a primeira parte da figura representa os campos do pacote LSA comum. O primeiro campo específco e utilizado pelo LSA do tipo 1 é o campo bit V.

- **Bit V** (em que V representa virtual link) – Se marcado como 1, o roteador que originou o LSA representará um endpoint de um link virtual (*virtual link*).
- **Bit E** (*External*) – Se marcado com o valor 1, o roteador que originou o LSA é um ASBR (*Autonomous System Boundary Router*).
- **Bit B** (*Border*) – Se marcado com o valor 1, o roteador que originou o LSA é um ABR (*Area Border Router*).
- *Number of links* – Inclui o número de links descrito no LSA. Esses links se referem aos vizinhos que o roteador possui com o protocolo OSPF configurado.
- *Link ID* – Seu valor dependerá do campo Type, apresentado a seguir.

- *Link Data* – Seu valor também dependerá do campo Type, apresentado a seguir.
- *Type* – Poderá assumir um dos seguintes valores conforme apresentados na tabela 9.9.
- *Metric* – Custo de uma interface. Obtida automaticamente pelo roteador ou configurada manualmente pelo administrador da rede.

*Tabela 9.9 – Valores para o campo Type*

| Tipo | Descrição | Link ID | Link Data |
|---|---|---|---|
| 1 | Point-to-point numbered. O valor 1 indica uma conexão ponto a ponto com outro roteador. | Conterá o router-id do roteador vizinho | Endereço IP da interface do roteador |
| 2 | Trânsito. O valor 2 refere-se a uma rede de trânsito. | Endereço IP do roteador designado (DR) | Endereço IP da interface do roteador |
| 3 | Stub. O valor 3 indica a conexão com uma rede Stub. | Endereço de rede da interface do roteador. | Máscara de rede |
| 4 | Virtual link. O valor 4 indica a conexão com um link virtual (virtual link). | Conterá o router-id do link virtual do vizinho | Endereço IP do link |

Conforme comentado, os LSAs do tipo 1 são gerados e trocados pelos roteadores pertencentes a uma específica área. Com isso, cada roteador conhecerá quais são os outros roteadores que possuem o protocolo OSPF configurado em sua área e trocará com cada um deles sua base de dados, utilizada para o algoritmo SPF calcular as rotas.

Em equipamentos do fabricante Cisco, podemos avaliar os LSAs do tipo 1 executando o seguinte comando:

```
show ip ospf database
```

No caso do roteador 0 da figura 9.8, as informações trocadas farão parte da base de dados desse roteador. Vejamos na tabela 9.10 o resultado do comando:

*Tabela 9.10 – Router Link States (Area 0)*

| Link ID | ADV Router | Age | Seq# | Checksum | Link count |
|---|---|---|---|---|---|
| 20.20.20.20 | 20.20.20.20 | 1215 | 0x80000008 | 0x00f218 | 4 |
| 10.10.10.10 | 10.10.10.10 | 1215 | 0x80000006 | 0x00ad95 | 3 |
| 80.80.80.80 | 80.80.80.80 | 1215 | 0x80000003 | 0x00d05c | 1 |
| 70.70.70.70 | 70.70.70.70 | 1215 | 0x80000006 | 0x00b338 | 3 |

Vejamos o que cada uma das colunas representa:

- *Link ID* – Identifica o ID do roteador que originou o LSA. A interpretação deste campo dependerá do tipo do LSA. Para a seção que apresenta os LSAs do tipo 1, as colunas Link ID e ADV Router são iguais.
- *ADV Router* – Representa o *router-id* do roteador que criou e anunciou o LSA. Possui mesmo valor que o campo Link ID.
- *Age* – Representa o tempo em segundos em que o LSA foi originado.
- *Seq* – Representa o número de sequência do LSA. Os LSAs recebidos de um roteador vizinho vêm marcados com um número de sequência. Esse número permitirá ao roteador que o recebeu determinar se o LSA recebido é mais novo do que o recebido anteriomente. Um LSA será atualizado quando existir alguma nova informação relacionada aos roteadores da área, como um novo custo, um novo endereço IP ou a queda de um link, por exemplo. Quando um roteador vizinho receber um LSA com número mais novo, o roteador atualizará seu estado para loading e trocará LSRs (*Link State Request*) e LSUs (*Link State Update*) para complementar as informações sobre as novidades geradas na rede.
- *Checksum* – Representa o checksum do pacote LSA. Esse campo é utilizado para avaliar a integridade do pacote em relação a alguma perda durante a transmissão. A verificação da soma (*checksum*) está baseada em todos os campos que compõem o pacote, exceto o campo age. O receptor do pacote avaliará o campo checksum para

garantir que o pacote LSA não está corrompido.

Conforme observado no resultado do comando, o roteador 0 trocou LSAs do tipo 1 com os roteadores representados pelos seguintes routers-id: 80.80.80.80, 20.20.20.20 e 70.70.70.70, além de compor a lista com o seu próprio *router-id* (10.10.10.10). O pacote LSA transportará vários campos, porém basicamente os mais importantes para o algoritmo SPF são os endereços das interfaces envolvidas e o custo de cada uma.

Se executarmos esse mesmo comando nos roteadores 4 e 7 da figura 9.8, teremos o mesmo resultado, apenas a ordem será apresentada de forma diferente. É importante observar que para conferir os LSAs do tipo 1 trocados por um roteador Huawei, executamos o seguinte comando:

```
dis ospf 33 lsdb
```

A tabela 9.11 apresenta o resultado do comando executado em um roteador Huawei com configuração de um de seus clientes.

*Tabela 9.11 – LSAs do tipo 1 gerados em um roteador Huawei*

| OSPF Process 33 with Router ID 152.52.5.58 | | | | | | |
|---|---|---|---|---|---|---|
| Link State Database | | | | | | |
| Area: 0.0.0.0 | | | | | | |
| Type | LinkState ID | AdvRouter | Age | Len | Sequence | Metric |
| Router | 2.1.1.10 | 2.1.1.10 | 771 | 48 | 80000281 | 10 |
| Router | 2.1.1.5 | 2.1.1.5 | 1083 | 48 | 800001AC | 10 |
| Router | 2.1.1.1 | 2.1.1.1 | 842 | 36 | 800003CD | 10 |
| Router | 152.52.5.58 | 152.52.5.58 | 682 | 60 | 800007AD | 1 |

Para analisar a configuração que foi aplicada a esse roteador e conhecer as redes anunciadas, executamos o comando:

```
dis current-configuration configuration ospf 33

ospf 33
  area 0.0.0.0
```

```
network 152.52.5.8.0   0.0.0.7
network 172.20.20.0    0.0.3.255
network 152.52.5.40    0.0.0.7
```

Conforme podemos observar no resultado do comando executado no Huawei, apresenta-se o processo do OSPF que, neste caso, foi 33 e, em seguida, a área 0 e as redes anunciadas seguidas de suas máscaras de rede invetida. A regra para inversão é a máscara de rede tradicional menos 255. No primeiro exemplo, a máscara da rede 152.52.5.8 é 255.255.255.248, que, invertida, ficará 0.0.0.7. As demais seguem a mesma regra.

Conforme comentado, a tabela de rotas dependerá das informaçoes trocadas pelos LSAs. Vejamos na tabela 9.12 a tabela de rotas do roteador 0, apresentado na figura 9.8, executando o comando:

```
show ip route
```

A primeira coluna informa a rede destino. Em seguida, há o custo e para qual endereço IP o pacote seguirá. A última coluna informa a interface física a que o pacote deverá ser enviado para que alcance seu destino. É importante observar que a última rota apresentada traz ao lado do símbolo O o símbolo IA. Este representa uma rota OSPF Inter Area, recebida do roteador 4 (Figura 9.8) configurado para atuar com as áreas 0 e 74.

*Tabela 9.12 – Tabela de rotas geradas pelo OSPF em roteador Cisco*

| **Protocolo** | **Rede destino** | **Como chegar?** | **Interface que dá acesso à rede destino** |
|---|---|---|---|
| C | 10.0.0.0/8 | is directly connected, | FastEthernet0/0 |
| O | 20.0.0.0/8 | [110/2] via 10.0.0.2, 02:15:36, | FastEthernet0/0 |
| O | 27.0.0.0/8 | [110/20] via 45.0.0.1, 02:15:26, | Ethernet1/0 |
| C | 30.0.0.0/8 | is directly connected, | FastEthernet0/1 |
| C | 45.0.0.0/8 | is directly connected, | Ethernet1/0 |
| O | 70.0.0.0/8 | [110/11] via 10.0.0.2, 02:15:26, | FastEthernet0/0 |
| | | [110/11] via 45.0.0.1, 02:15:26, | Ethernet1/0 |

| Protocolo | Rede destino | Como chegar? | Interface que dá acesso à rede destino |
|---|---|---|---|
| O | 80.0.0.0/8 | [110/11] via 10.0.0.2, 02:15:36, | FastEthernet0/0 |
| O IA | 90.0.0.0/8 | [110/12] via 10.0.0.2, 02:15:26, | FastEthernet0/0 |
| Em que C significa interface diretamente conectada e O significa rota aprendida pelo protocolo OSPF. | | | |

### 9.2.10.2 LSA tipo 2 – Network Links Advertisements

Conforme comentado, ao final da troca de LSAs todos os roteadores de uma área OSPF possuem a visão completa dos vizinhos da sua área. A partir dessa visão, cada roteador calculará individualmente qual o melhor caminho para determinado destino.

A intenção dos LSAs tipo 2 é que a troca de informações não ocorra entre todos os roteadores, e sim entre os roteadores e um ponto central. Esse ponto central será um dos roteadores da área eleito como roteador desingnado. Este, por sua vez, receberá as novidades da rede [mudança de endereço IP de alguma interface, alteração do custo, link inacessível (*links down*), entre outras] e fará a divulgação das novidades aos demais roteadores da área. A intenção principal é reduzir a troca de LSAs, que, por sua vez, diminuirá o tráfego da rede. Os LSAs tipo 2 são gerados e encaminhados aos demais roteadores da mesma área pelo roteador eleito como roteador designado (DR).

Conforme observado na figura 9.15, a comunicação com o roteador designado ocorre por meio do endereço *multicast* 224.0.0.6, e o reencaminhamento das atualizações aos demais roteadores ocorre por meio do endereço *multicast* 224.0.0.5.

A troca de LSAs tipo 2 ocorrerá quando os roteadores configurados com o protocolo OSPF estiverem interconectados por interfaces Ethernet. Nesse ambiente, haverá a eleição do roteador designado (DR) e do roteador designado backup (BDR) como redundância. A ideia por trás desse princípio é criar um ponto central na rede multiacesso (rede Ethernet na qual os roteadores estão conectados) para troca de informações, que serão utilizadas pelo algoritmo SPF

para calcular a tabela de rotas. A intenção é evitar que cada roteador troque LSAs com todos os demais roteadores do segmento, gerando tráfego desnecessário. Com esse conceito, cada roteador trocará LSAs apenas com os roteadores DR e o BDR.

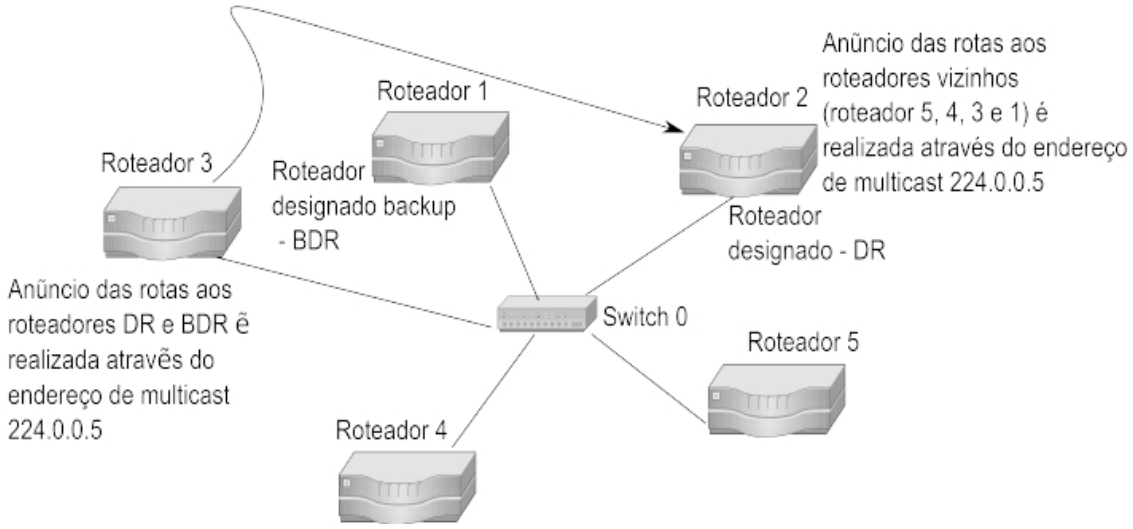



*Figura 9.15 – Comunicação entre os roteadores e o DR.*

Dependendo de como ocorre a interconexão entre os roteadores, poderemos ou não ter a eleição do DR, como também poderemos não observar os LSAs do tipo 2. Assim, apresentaremos três ambientes para análise.

No primeiro caso, analisaremos a interconexão sendo realizada pelas interfaces seriais dos roteadores. Nesse cenário, não teremos LSAs do tipo 2. A figura 9.16 apresenta uma rede com os roteadores interconectados pela interface serial.

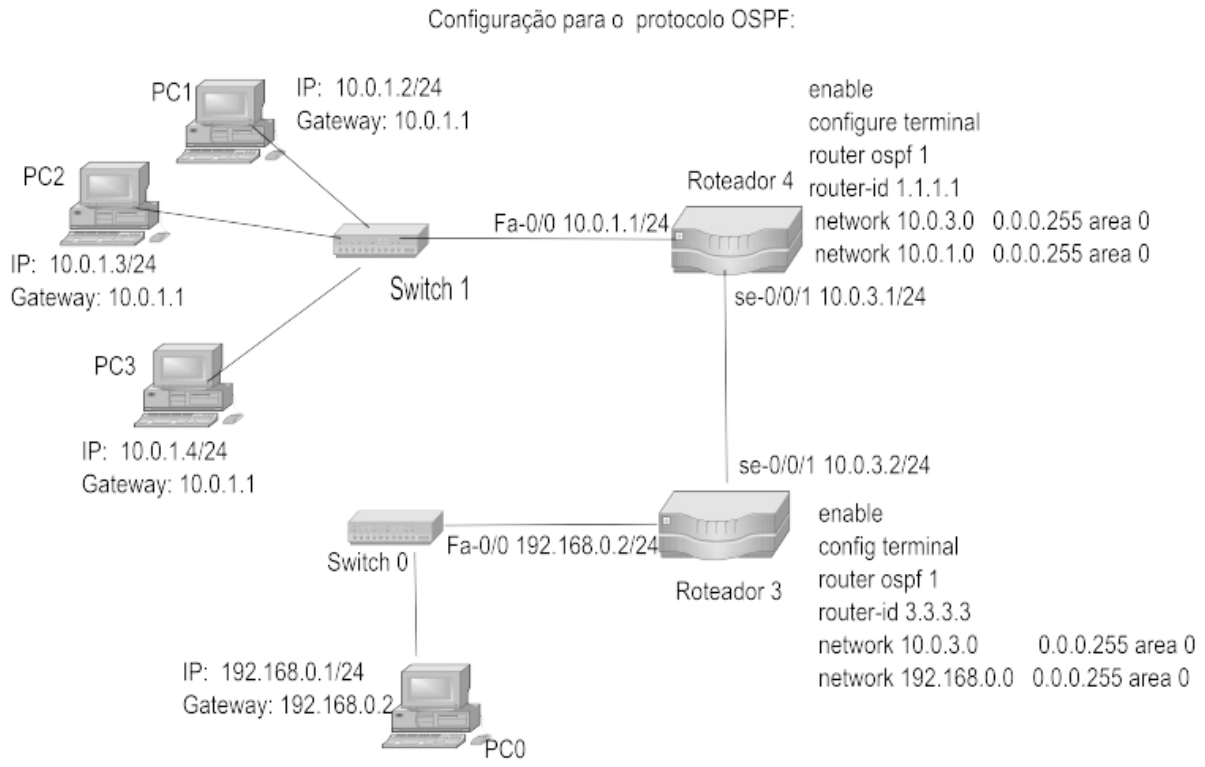



*Figura 9.16 – Roteadores interconectados por uma interface serial.*

Executando o comando show ip ospf neighbor no roteador 1 da figura 9.16, percebemos que não temos a figura do roteador designado, pois, após a barra seguida do estado *FULL,* observamos o símbolo -. Vejamos o resultado da execuçao do comando na tabela 9.13:

*Tabela 9.13 – Vizinhos do roteador 1*

| Neighbor ID | Pri | State | Dead time | Address | Interface |
|---|---|---|---|---|---|
| 3.3.3.3 | 0 | FULL/ - | 00:00:35 | 10.0.3.2 | Serial0/0/1 |

Executando o mesmo comando show ip ospf neighbor, no roteador 3 da figura 9.16, percebemos que também não temos a figura do roteador designado, pois, após a barra do estado *FULL*, observamos o símbolo – (FULL/ -). Vejamos o resultado da execução do comando na tabela 9.14:

*Tabela 9.14 – Vizinhos do roteador 3*

| Neighbor ID | Pri | State | Dead time | Address | Interface |
|---|---|---|---|---|---|
| 1.1.1.1 | 0 | FULL/ - | 00:00:33 | 10.0.3.1 | Serial0/0/1 |

No segundo caso, analisaremos a interconexão dos roteadores pelas interfaces Ethernet. Nesse cenário, teremos apenas duas interfaces relacionadas ao segmento da rede e a eleição ocorrerá entre as duas. Desta forma, uma ficará como DR (roteador com maior *router-id*) e a segunda como BDR. Esse cenário poderá ser observado na figura 9.8, entre, por exemplo, os roteadores 1 e 7.

Executando o comando show ip ospf neighbor no roteador 1 da figura 9.8, percebemos que, para cada vizinho, temos a relação de vizinhança estabelecida e formalizada pelo estado full. Entre as duas interfaces conectadas, o roteador designado (DR) será o roteador com o maior *router-id*.

Assim, entre o roteador 1 com *router-id* 20.20.20.20 e seus vizinhos, teremos a seguinte definição:

- Com o roteador 4 com *router-id* 80.80.80.80, o roteador 4 foi eleito o DR, por possui o maior *router-id*.
- Com o roteador 7 com *router-id* 70.70.70.70, o roteador 7 foi eleito o DR.
- Com o roteador 0 com *router-id* 10.10.10.10, o roteador 1 foi eleito o DR e o roteador 0, o BDR.

Vejamos o resultado do comando comentado na tabela 9.15:

*Tabela 9.15 – Vizinhos do roteador 1 da figura 9.8*

| Neighbor ID | Pri | State | Dead time | Address | Interface |
|---|---|---|---|---|---|
| 80.80.80.80 | 1 | FULL/DR | 00:00:30 | 80.0.0.1 | Ethernet1/0 |
| 70.70.70.70 | 1 | FULL/DR | 00:00:30 | 70.0.0.2 | Ethernet1/1 |
| 10.10.10.10 | 1 | FULL/BDR | 00:00:30 | 10.0.0.1 | FastEthernet0/0 |

Executando o comando show ip ospf neighbor no roteador 7 da figura 9.8, percebemos que, para cada vizinho, temos uma definição única.

O DR é o roteador com o maior *router-id*. Assim, entre o roteador 7 com *router-id* 70.70.70.70 e seus vizinhos, temos a seguinte definição:

- Com o roteador 1 com *router-id* 20.20.20.20, o roteador 7 foi eleito o DR e o roteador 1, BDR.
- Com o roteador 0 com *router-id* 10.10.10.10, o roteador 7 foi eleito o DR e o roteador 0, BDR.

Vejamos o resultado do comando na tabela 9.16.

*Tabela 9.16 – Vizinhos do roteador 7 da figura 9.8*

| Neighbor ID | Pri | State | Dead time | Address | Interface |
|---|---|---|---|---|---|
| 20.20.20.20 | 1 | FULL/BDR | 00:00:36 | 70.0.0.1 | FastEthernet0/0 |
| 10.10.10.10 | 1 | FULL/BDR | 00:00:37 | 45.0.0.2 | FastEthernet0/1 |

No terceiro caso, avaliaremos uma rede em que os roteadores estão interconectados por meio de um switch Ethernet (Figura 9.17). Nesse ambiente, todos os roteadores 0, 1 e 3 estão conectado a um switch e, por isso, criarão uma quantidade significativa de tráfego, pois todos os roteadores trocarão LSAs com todos os seus vizinhos. Para reduzir a quantidade de LSAs trocados, o protocolo OSPF elege um roteador para ser o roteador designado e um segundo para assumir o papel de backup deste, chamado de roteador designado backup. Nesse cenário, percebemos as vantagens do uso do roteador designado. A figura 9.17 apresenta uma rede em que os roteadores estão interconectados por meio de um switch Ethernet.

Conforme podemos observar na figura 9.17, temos os roteadores 0, 1 e 3 interconectados por um switch Ethernet. Assim, entre os três roteadores citados, o roteador com maior *router-id* (roteador 3 com *router-id* 10.10.10.10) será eleito o DR, o segundo maior (roteador 1 com *router-id* 4.4.4.4) será o BDR e os demais serão identificados na rede por DROTHER (roteador 0 com *router-id* 3.3.3.3). Vejamos o resultado da execução do comando show ip ospf neighbor aplicado ao roteador 3 da figura 9.17.

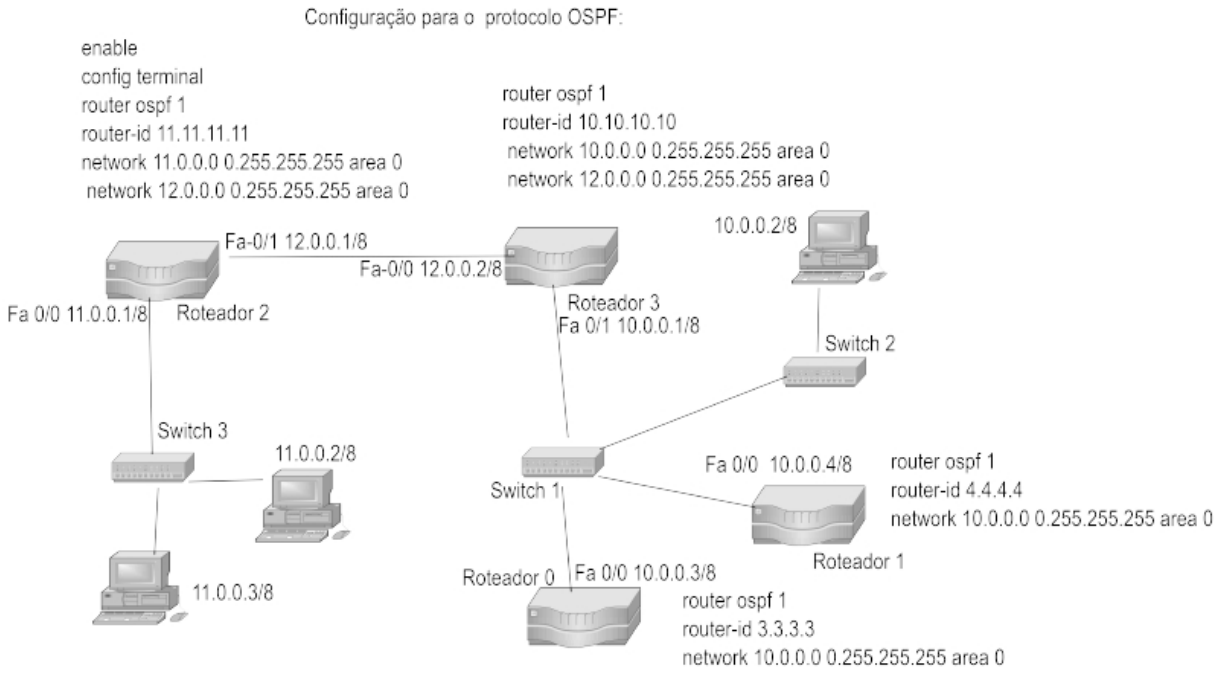



*Figura 9.17 – Roteadores interconectados por um switch Ethernet.*

*Tabela 9.17 – Vizinhos do roteador 3 da figura 9.17*

| Neighbor ID | Pri | State | Dead time | Address | Interface |
|---|---|---|---|---|---|
| 11.11.11.11 | 1 | FULL/DR | 00:00:35 | 12.0.0.1 | FastEthernet0/0 |
| 3.3.3.3 | 1 | FULL/DROTHER | 00:00:35 | 10.0.0.3 | FastEthernet0/1 |
| 4.4.4.4 | 1 | FULL/BDR | 00:00:35 | 10.0.0.4 | FastEthernet0/1 |

Vejamos o resultado da execução do mesmo comando show ip ospf neighbor aplicado ao roteador 1 da figura 9.17. Vejamos o resultado da execução do comando na tabela 9.18.

*Tabela 9.18 – Vizinhos do roteador 1 da figura 9.17*

| Neighbor ID | Pri | State | Dead time | Address | Interface |
|---|---|---|---|---|---|
| 3.3.3.3 | 1 | FULL/DROTHER | 00:00:35 | 10.0.0.3 | FastEthernet0/0 |

| Neighbor ID | Pri | State | Dead time | Address | Interface |
|---|---|---|---|---|---|
| 10.10.10.10 | 1 | FULL/DR | 00:00:35 | 10.0.0.1 | FastEthernet0/0 |

É importante observar que o processo de eleição do roteador designado segue as seguintes etapas:

- Roteador que tenha alguma das suas interfaces pertencentes à área definida com maior prioridade (por padrão, no Cisco e Huawei a prioridade é igual a 1). Esse valor pode ser alterado pelo comando:

  ip ospf priority <valor>

  Uma prioridade com <valor> igual a 0 significa que a interface em questão não é considerada no processo de eleição do DR/BDR. O estado de uma interface com prioridade 0 é DROTHER.

- Em caso de empate, o roteador com maior *router-id* vence a disputa.

Até o momento, apresentamos a relação entre os vizinhos e o roteador designado. Vejamos através do comando show ip ospf database, executado no roteador 0 (Figura 9.17), que este apenas trocou informações com os roteadores designados. Nessa rede, os roteadores 2 e 3 pertencem à área 0. O roteador 3 foi eleito o designado entre os roteadores interconectados ao switch Ethernet. O roteador 2 foi eleito o designado devido a ter uma de suas interfaces conectada a outro roteador no modelo ponto a ponto. Os LSAs do tipo 2 são também chamados de *Net Link States*. Vejamos o resultado do comando show ip ospf database executado no roteador 0 da figura 9.17. Vejamos o resultado da execução do comando na tabela 9.19.

*Tabela 9.19 – LSAs do tipo 2 do roteador 0*

| Net Link States (Area 0) | | | | |
|---|---|---|---|---|
| Link ID | ADV Router | Age | Seq# | Checksum |
| 10.0.0.1 | 10.10.10.10 | 1100 | 0x80000003 | 0x00db9f |
| 12.0.0.1 | 11.11.11.11 | 1099 | 0x80000002 | 0x00d7f5 |

### 9.2.10.3 LSA tipo 3 – Summary Link Advertisements

Os LSAs do tipo 3 são gerados pelos roteadores configurados com duas diferentes áreas chamadas de ABR (*Area Border Router*). Na figura 9.8, o roteador 4 atua como ABR e é responsável por divulgar informações aos demais roteadores da área 0 sobre como alcançar a rede 90.0.0.0 que pertence à área 74. O objetivo será fazer com que os roteadores das áreas 0 e 74 consigam trocar dados entre si. Vejamos o resultado da execução do comando show ip ospf database no roteador 1 da figura 9.8. Os LSAs do tipo 3 também são chamados de *Summary Net Link States*. Vejamos o resultado da execução do comando na tabela 9.20.

*Tabela 9.20 – LSAs do tipo 3 do roteador 1*

| **Summary Net Link States (Area 0)** | | | | |
|---|---|---|---|---|
| Link ID | ADV Router | Age | Seq# | Checksum |
| 90.0.0.0 | 80.80.80.80 | 1225 | 0x80000003 | 0x008f31 |

O roteador 1 receberá apenas uma informação relacionada ao LSA do tipo 3, que trata sobre a rede 90.0.0.0 presente na área 74 configurada no roteador 4. Entretanto, se digitarmos o mesmo comando no roteador 4 (show ip ospf database), que possui configuradas as áreas 0 e 74, perceberemos que todas as redes da área 0 serão recebidas como LSA do tipo 3 pelo roteador 4. Receberá ainda a rede 90.0.0.0 como LSA do tipo 3, pois, para a área 0, essa rede vem de outra área. Vejamos o resultado da execução do comando nas tabelas 9.21 e 9.22.

*Tabela 9.21 – LSAs do tipo 3 da área 0*

| **Summary Net Link States (Area 0)** | | | | |
|---|---|---|---|---|
| Link ID | ADV Router | Age | Seq# | Checksum |
| 90.0.0.0 | 80.80.80.80 | 1198 | 0x80000003 | 0x008f31 |

*Tabela 9.22 – LSAs do tipo 3 da área 74*

| Summary Net Link States (Area 74) | | | | |
|---|---|---|---|---|
| Link ID | ADV Router | Age | Seq# | Checksum |
| 80.0.0.0 | 80.80.80.80 | 1198 | 0x8000000f | 0x00f9c4 |
| 10.0.0.0 | 80.80.80.80 | 1198 | 0x80000010 | 0x00936f |
| 70.0.0.0 | 80.80.80.80 | 1198 | 0x80000011 | 0x00dcdf |
| 45.0.0.0 | 80.80.80.80 | 1198 | 0x80000012 | 0x002ba8 |
| 20.0.0.0 | 80.80.80.80 | 1198 | 0x80000013 | 0x000bea |
| 30.0.0.0 | 80.80.80.80 | 1198 | 0x80000014 | 0x009059 |
| 27.0.0.0 | 80.80.80.80 | 1198 | 0x80000015 | 0x006a6f |

Conforme podemos observar, o roteador 4 possui informações sobre as áreas 0 e 74, as quais foram obtidas via LSA tipo 3

### 9.2.10.4 LSA tipo 4 – AS (Autonomous System) Summary Link Advertisements

Os LSAs do tipo 4 são gerados pelos roteadores ABR (*Area Border Router*), informando os campos *router-id* e o custo para o roteador ASBR (*Autonomous System Border Routers*) fora da área. Essas informações serão utilizadas pelo algoritmo SPF para calcular uma rota para o ASBR. Os roteadores ASBR são responsáveis por redistribuir destinos externos dentro do processo OSPF, como RIP, rotas estáticas, interfaces diretamente conectadas, BGP, entre outras.

O protocolo atualmente utilizado pela Internet e que usa o conceito de AS (*Autonomous System*) é o BGP (*Border Gateway Protocol*). Muitos administradores de rede preferem utilizar o protocolo BGP quando se aplica em suas redes o conceito de AS, deixando o protocolo OSPF para redes sem essa necessidade. Por isso, não aprofundaremos esse assunto neste livro.

### 9.2.10.5 LSA tipo 5 – AS External Link Advertisements

Os LSAs do tipo 5 são gerados pelos roteadores ASBR (*Autonomous System Boundary Router*), informando como alcançar redes que estão fora do AS local. Conforme comentado, os administradores de rede preferem utilizar o protocolo BGP quando se opta por dividir as redes em ASs locais.

### 9.2.11 IS-IS

O protocolo IS-IS (*Intermediate System to Intermediate System*) é um protocolo também baseado no algoritmo SPF, ou seja, após a troca de informações entre roteadores vizinhos, cada roteador conterá informações suficientes para que o algoritmo SPF possa calcular as melhores rotas. Este foi desenvolvido pela ISO (*International Organization for Standardization*) e define em seu nome o termo IS (*Intermediate System*) que denomina o roteador. Vejamos as similaridades com o protocolo OSPF:

- Ambos possuem uma base de dados que, após estar completa, será utilizada pelo algoritmo SPF para calcular as melhores rotas.
- Ambos trocam pacotes *hello* para formação da base de dados nos roteadores.
- Ambos elegem um roteador designado, porém o IS-IS não elege o BDR. No IS-IS, o DR é chamado de DIS (*Designated Intermediate System*).
- Ambos definem áreas que concentram a troca dos pacotes *hello*.
- Ambos oferecem suporte para:
  - *Classless Inter-Domain Routing* (CIDR).
  - Autenticação.
  - Ser divididos em áreas.

Apesar das similaridades, as operadoras utilizam o protocolo IS-IS para a engenharia de tráfego, enquanto seus clientes, que são interligados via VPN MPLS, normalmente optam pelos protocolos OSPF ou BGP. O IS-IS é utilizado no backbone da rede da operadora para redirecionar o tráfego em casos de rompimento de fibra óptica ou necessidade de manutenção nas interfaces dos roteadores ou equipamentos intermediários. O protocolo IS-IS define como métrica o menor valor de um link. Assim, para mudar o sentido do tráfego,

aumentamos o valor do custo de um link de 20 para 200, por exemplo, fazendo que o custo por um determinado link fique tão grande que seja descartado temporariamente como um bom caminho pelo protocolo IS-IS.

Diferentemente do OSPF, o protocolo IS-IS não possui um rígido conceito de área. Apesar de operar com esse conceito, não há necessidade de termos uma área 0 com as demais ligadas a esta. Com o IS-IS, poderemos ter áreas interligadas, porém sem a rigidez do protocolo OSPF.

Conforme comentado, o protocolo IS-IS divide a rede em áreas e, em cada uma delas, podemos ter roteadores classificados em dois níveis, denominados level 1 e level 2. Assim, além de dividirmos nossa rede em áreas como ocorre no protocolo OSPF, ainda dentro de cada uma delas podemos dividir os roteadores em outros dois níveis, garantindo que roteadores em níveis diferentes não estabeleçam relação de vizinhança. É importante observar que os pacotes *hello* trocados entre os roteadores de níveis diferentes serão também diferentes, ou seja, cada roteador do nível 1 enviará seu próprio pacote *hello*. O mesmo ocorre com os roteadores do nível 2.

Por padrão, os roteadores normalmente vêm configurados para atuarem nos dois níveis, porém, na prática, muitos administradores de rede optam por deixá-los todos em um mesmo nível. Neste caso, optou-se pelo nível 2 por ser o nível de backbone. A figura 9.18 apresenta uma relação entre as áreas definidas no protocolo OSPF e sua relação em uma rede que utiliza o protocolo IS-IS.

É importante observar que os roteadores configurados no nível (*level*) 1 somente estabelecerão vizinhança com roteadores que também estejam no nível 1. Os roteadores configurados para o nível (*level*) 2 somente estabelecerão vizinhança com roteadores também configuados no nível 2. Caso o roteador seja configurado para atuar em ambos os níveis L1 e L2, estes estabelecerão vizinhança com quaisquer roteadores. A figura 9.19 apresenta uma rede contendo os elementos do protocolo IS-IS comentados e ainda evidenciando como as áreas são definidas.

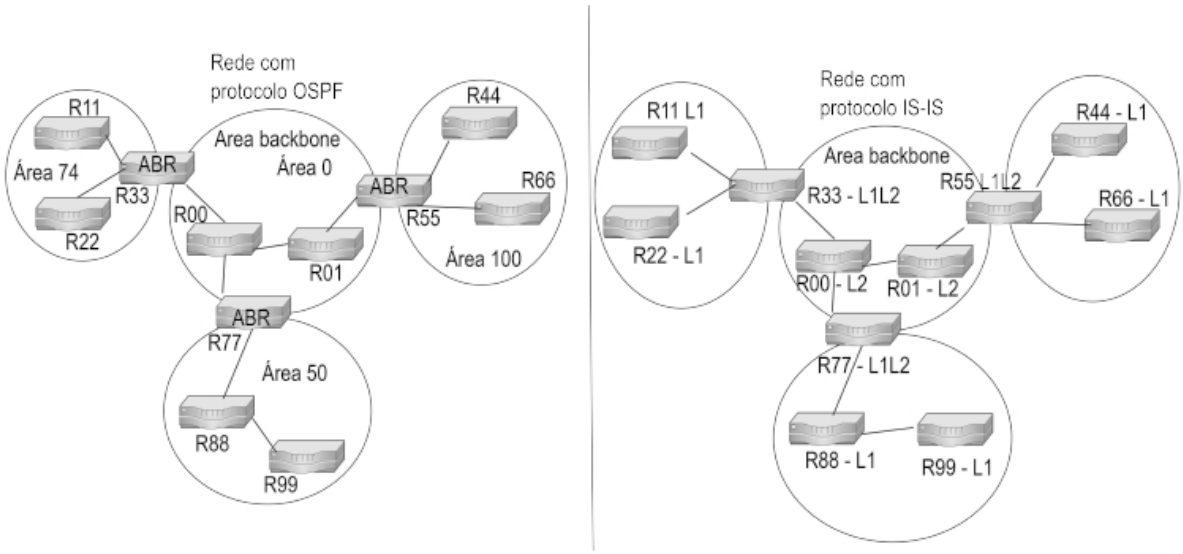



*Figura 9.18 – Elementos que compõem uma rede com IS-IS.*

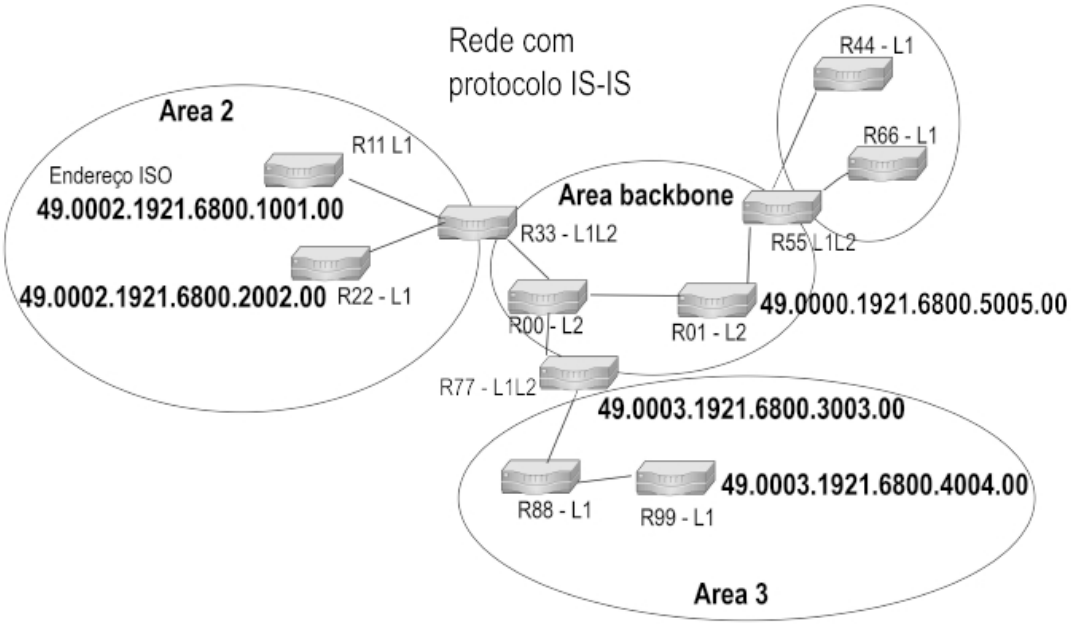



*Figura 9.19 – Elementos que compõem uma rede com IS-IS.*

Conforme podemos observar na figura 9.19, a definição da área em que um roteador está configurado é realizada pelo endereço ISO (49.0002.1921.6800.1001.00) também chamado de NET (*Network Entity Title*). Esse endereço é dividido em quatro partes. Vejamos cada uma das partes que compõem o endereço ISO.

- Primeiros 2 bytes – Geralmente 49 (AFI – Authority and Format Indicator)

- Próximos 4 bytes (Ex.: 0002) – Identificação da área (Area ID)
- Próximos 12 bytes (Ex.: 1921.6800.1001) – Endereço IP de loopback ou endereco MAC.
- Últimos 2 bytes – Ficam com 00.

Exemplo:

Endereço IP do roteador: 192.168.1.1 (endereço de loopback). Deverá atuar na área 1

49.0002.1921.6800.1001.00

A parte relacionada ao AFI representa a competência que o endereço tem. Esse valor pode ser ao nível da rede local, regional ou Internet. Quando AFI for igual a 49, será considerado um endereço privado, como 10.0.0.0/8, assim seria roteado internamente, e não pela Internet. O valor 39 (*Data Country Code*) representa um endereço que poderia ser roteado fora da rede local ao nível da Internet, por exemplo. O valor 47 (*International Code Designator*) representa um endereço que poderia ser roteado fora da rede local, porém dentro de uma organização, como a extranet. A figura 9.20 apresenta a configuração de um endereço ISO em um roteador Juniper. O endereço ISO foi adicionado à interface de loopback do roteador chamada de lo0 (loopback 0).

```
show configuration interfaces lo0
unit 0 {
    family inet {
        address 200.150.95.131/32;
    }
    family iso {
        address 49.0001.2001.5009.5131/32;
    }
}
```

*Figura 9.20 – Configuração do endereço ISO em um roteador Juniper.*

## 9.2.12 Sistemas autônomos

Um sistema autônomo é uma coleção de roteadores e de redes sujeita

a um único controle administrativo, e cada SA possui um código ASN (*Autonomous System Number*) da mesma entidade que fornece endereços IPs públicos para acesso à Internet. Com esses códigos (ex.: COPEL Telecom possui ASN 14868), os SAs trocam suas tabelas de roteamento por meio do protocolo BGP. Como exemplo de empresas brasileiras que possuem códigos com sistemas autônomos, temos TIM, Algar, GVT, Embratel, entre milhares de outras.

Dentro dos sistemas autônomos, as rotas são definidas de forma estática ou por meio de protocolos interiores de roteamento (IGPs), como o protocolo OSPF, IS-IS ou BGP.

## 9.3 Estudo de caso sobre roteamento

A tabela 9.23 apresenta uma rede WAN composta de cinco redes interligadas:

*Tabela 9.23 – Redes*

| Rede | Número da rede | Máscara de sub-rede |
|---|---|---|
| 01 | 10.10.10.0 | 255.255.255.0 |
| 02 | 10.10.20.0 | 255.255.255.0 |
| 03 | 10.10.30.0 | 255.255.255.0 |
| 04 | 10.10.40.0 | 255.255.255.0 |
| 05 | 10.10.5.0 | 255.255.255.0 |

A figura 9.21 apresenta a tabela em formato de uma rede WAN mostrando que qualquer rede poderá enviar pacotes para qualquer outra rede.

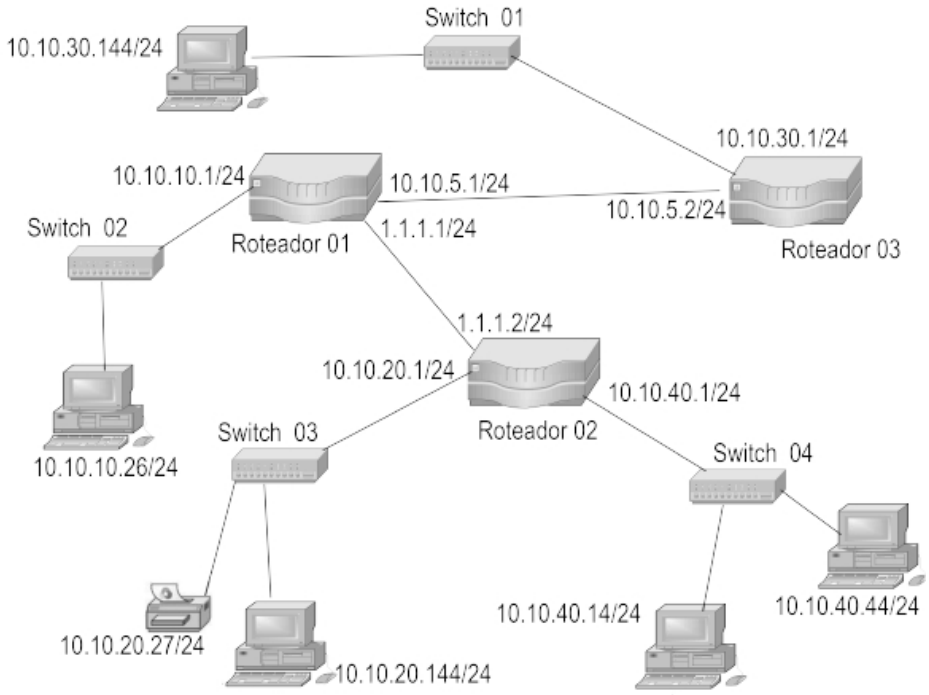



*Figura 9.21 – Rede interconectada por roteadores.*

Nessa rede, caso algum roteador pare de funcionar em razão de algum link ser interrompido, não existem caminhos alternativos e a rede sofrerá problemas. Para os roteadores 1 e 2, o problema será ainda maior, pois interligam duas redes cada um. Essa situação ocorre muito quando os analistas responsáveis não se preocupam com o caminho de backup.

Como boa prática de configuração de roteadores, sugere-se sempre setar na porta LAN do roteador o endereço IP começando com 1. Embora não seja obrigatório, é uma convenção comumente utilizada.

A seguir, analisaremos como seria o tráfego de dados dentro da rede representada pela figura 9.21.

Nessa rede, quando o computador 10.10.30.144 quiser imprimir, enviará sua requisição ao roteador 3 na porta LAN 10.10.30.1, que, por sua vez, repassará a requisição para a porta WAN 10.10.5.2 e, em seguida, para a porta LAN 10.10.5.1 do roteador 1. Depois disso, o roteador 1 repassará a requisição para o roteador 2, que se encarregará de repassar para a rede em que a impressora estiver conectada. Como podemos ver, o uso de uma impressora em uma outra rede afeta drasticamente o tráfego de dados na rede, por isso é sempre recomendável ter uma impressora disponível em cada rede

LAN. O valor gasto com a impressora acaba sendo menor do que os prejuízos causados por impactos em razão da grande quantidade de dados trafegados entre as redes envolvidas.

A impressora está ligada ao computador com o endereço IP 10.10.20.144. De que forma, então, os roteadores sabem que precisam rotear o pedido entre as redes interligadas?

Para que um roteador decida se o endereço IP destino pertence ou não à mesma rede do endereço IP origem, este aplica uma operação lógica entre os endereços, ou seja, cada roteador aplica uma operação lógica E (&) entre o endereço IP e a máscara origem e o endereço IP e a máscara destino envolvidos na comunicação. Caso esses endereços não pertençam à mesma rede, o roteador pesquisará em sua tabela de roteamento e enviará o pedido para onde a rota indicar. Se não possuir uma rota direta, o roteador enviará para a sua rota-padrão. A conclusão a que os roteadores chegam é baseada nas máscaras de cada endereço. As máscaras de cada endereço definem se os equipamentos envolvidos na comunicação estão ou não na mesma rede. Vejamos um exemplo:

| Endereço IP origem | Endereço IP origem |
|---|---|
| 010.010.0.10.144 | 010.010.0.20.144 |
| 255.255.255.000 | 255.255.255.000 |
| _____ | _____ |
| 010.010.010.000 | 010.010.020.000 |

Como podemos verificar, não pertencem à mesma rede, pois a origem está situada na rede 10.10.10.0 e o destino, na rede 10.10.20.0. Por isso, os roteadores precisam usar suas tabelas de roteamento para permitir a comunicação entre equipamentos da rede.

## 9.4 Exercícios do capítulo 9

**1**. (Sanepar, 2004) Avalie as proposições a seguir sobre o roteamento IP:

I. RIP, OSPF e IGRP são protocolos para roteamento interno também conhecidos como IGPs (*Internal Gateway Protocol*) e permitem o roteamento dentro de um mesmo SA (Sistema Autônomo).

II. O protocolo RIP (*Routing Information Protocol*), incluído em distribuições do Unix como *routed*, é baseado no algoritmo de distâncias vetoriais, no qual, a partir dos *hosts* adjacentes, são trocadas as tabelas de roteamento.

III. O OSPF (*Open Shortest Path First*) é um protocolo proprietário da Cisco que executa o roteamento entre diferentes SAs, sendo usado pelos chamados roteadores de borda.

IV. O roteamento entre diferentes SAs pode ser realizado pelo protocolo BGP (*Border Gateway Protocol*).

Assinale a alternativa correta:

a) Somente as proposições I, II e III são verdadeiras.

b) Somente as proposições III e IV são verdadeiras.

c) Somente as proposições I e II são verdadeiras.

d) Somente as proposições I, II e IV são verdadeiras.

e) Todas as proposições são verdadeiras.

**2**. Os protocolos de roteamento mais comuns são:

a) O RIP (*Routing Information Protocol*) que determina a rota mais eficiente para os dados e calcula o número de hops para a rota.

b) O EGP (*Exterior Gateway Protocol*) é usado quando vários roteadores têm de ser interconectados antes de chegar ao seu destino final.

c) O RIP permite caminho com contagem de hops superior a 16.

d) Roteamento estático, que deve ser utilizado quando existem diversas rotas para cada destino.

**3**. O protocolo que utiliza a característica de estado de link é:

a) RIP.

b) OSPF.

c) IGRP.

d) ICMP.

**4**. Todos os protocolos que seguem são protocolos de roteamento, exceto:

a) RIP.

b) OSPF.

c) IGRP.

d) SMTP.

**5**. (Sanepar, 2004) A tabela 9.24 de roteamento RIP foi obtida a partir de um roteador Unix, por meio do comando netstat –rn.

*Tabela 9.24 – Resultado do comando netstat -rn*

| Destination | Gateway | Flags | Iface |
|---|---|---|---|
| 127.0.0.1 | 127.0.0.1 | UH | lo0 |
| 200.17.212. | 200.17.212.5 | U | eth0 |
| 200.17.210. | 200.17.210.6 | U | eth1 |
| 200.19.138. | 200.19.138.1 | U | eth2 |
| default | 200.17.212.161 | UG | |

Com base nos dados da tabela 9.24, é incorreto afirmar:

a) Os endereços das interfaces eth0, eth1 e eth2 são, respectivamente, 200.17.212.5, 200.17.210.6 e 200.19.138.1.

b) O roteador está conectado a três redes por meio das interfaces eth0, eth1 e eth2.

c) A primeira linha corresponde à interface de loopback, que significa: quando um datagrama é enviado para essa interface, o protocolo retorna os dados sem enviá-los por rede.

d) Será enviado ao roteador 200.17.212.161 qualquer datagrama IP que não estiver destinado a (pelo menos) uma das redes listadas explicitamente na tabela de roteamento.

e) O roteador Unix, do qual a tabela 9.24 foi extraída, está endereçado na rede como 127.0.0.1.

CAPÍTULO 10

# Protocolos da camada de transporte

No capítulo 8, analisamos os protocolos residentes na camada 3 do modelo de referência TCP/IP, que tem como principal objetivo endereçar pacotes entre diferentes equipamentos (micro, router etc.) dentro de uma rede. Neste capítulo, apresentaremos os protocolos que compõem a camada de transporte do modelo de referência TCP/IP. Detalharemos os protocolos TCP (*Transmission Control Protocol*) e o protocolo UDP (*User Datagram Protocol*). Esse último não foi definido pelo modelo de referência OSI, estando presente somente no modelo de referência TCP/IP.

## 10.1 Introdução

Os protocolos de transporte são capazes de manipular múltiplas requisições em um mesmo computador, permitindo que várias aplicações (*browser*, email etc.) executadas no mesmo computador possam enviar e receber pacotes independentemente. Dependendo do tipo de serviço de comunicação utilizado, as funções da camada de transporte podem ser executadas pelos protocolos TCP ou UDP. O protocolo TCP (*Transmission Control Protocol*) oferece serviços de comunicação confiáveis e orientados à conexão, enquanto o protocolo UDP (*User Datagram Protocol*) oferece serviços do tipo datagrama, isto é, não orientados à conexão.

A figura 10.1 apresenta como se dá o fluxo de dados dentro das camadas de rede e de transporte. Observe que a camada de rede entrega os dados entre os computadores origem e destino, enquanto a camada de transporte, representada pelos protocolos TCP e UDP, entrega os dados dentro dos computadores às diferentes requisições de aplicativos. O protocolo IP utiliza o endereço IP para diferenciar para qual computador se devem entregar os pacotes, enquanto a camada de transporte utiliza as portas para diferenciar, dentro do computador, para qual aplicação

se deve devolver a requisição.

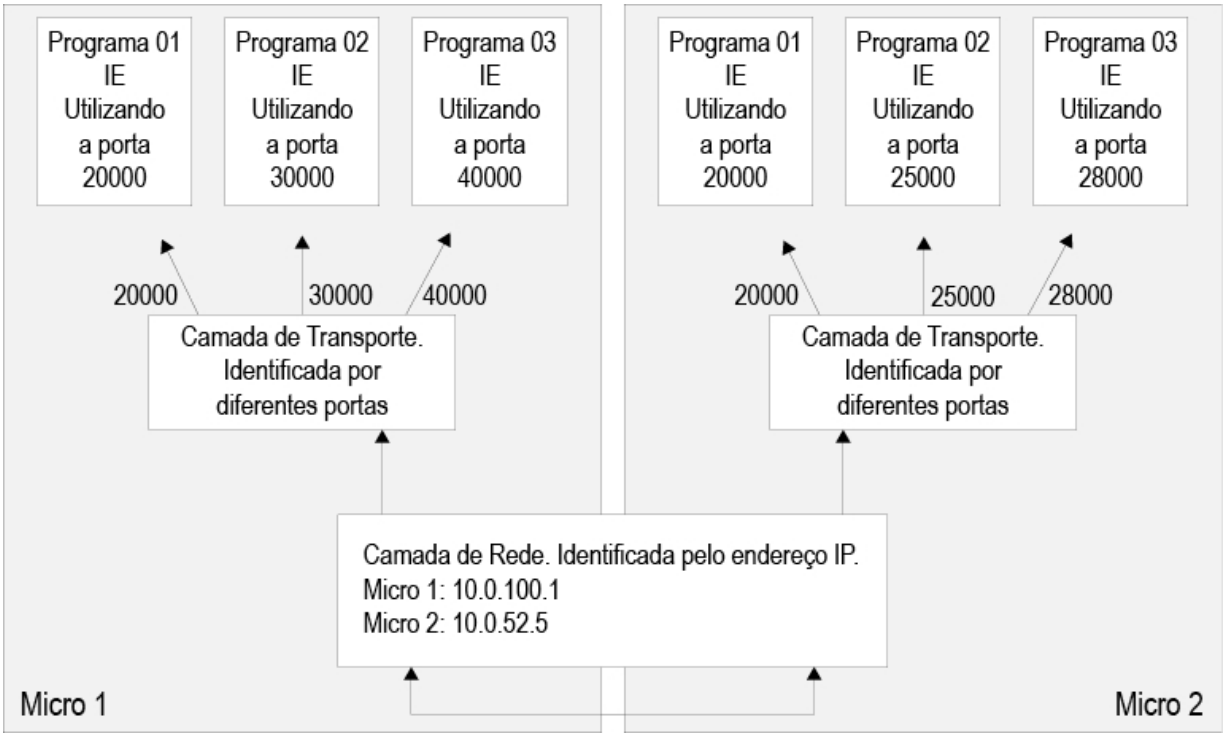



*Figura 10.1 – Representação da relação entre a camada de rede e a camada de transporte.*

## 10.2 Protocolo TCP

O TCP é o protocolo da camada de transporte que oferece o serviço de comunicação confiável, sendo orientado à conexão sobre a camada de rede IP, que tem como objetivo estabelecer uma comunicação ponto a ponto confiável entre o computador origem e o computador destino. O TCP foi desenvolvido por uma entidade fundada pela DARPA (*Defense Advanced Research Projects Agency* – Agência de Desenvolvimentos de Projetos Avançados de Defesa), uma agência militar norte-americana. Esse protocolo tornou-se extremamente difundido por ser utilizado pela Internet. A seguir, veremos como o TCP funciona.

Como já comentado em outros protocolos, cada um apresenta uma forma de identificação. A camada MAC utiliza o endereço físico, a camada LLC possui o SAP LLC e a camada de rede possui o endereço IP. No caso do protocolo TCP, a identificação é realizada

pelas portas. Um endereço de porta é um número inteiro de 16 bits que pode variar entre 1 e 65.536. É importante lembrar que as portas entre 1 e 1.024 são reservadas para protocolos-padrão, como DNS, SMTP, FTP, POP3, SNMP etc. As demais portas são utilizadas para a comunicação entre computadores.

A figura 10.2 apresentará o funcionamento de uma comunicação, utilizando o protocolo TCP. Nesse exemplo, estão três computadores interligados por uma rede. O computador A possui o endereço IP 128.10.2.3, o computador B, o endereço 128.10.2.4, e o computador C, o endereço 128.10.2.5. O computador B fornece o serviço de DNS para os computadores A e C. A requisição gerada pelo computador A possui em seu pacote o endereço destino do computador B e, como o computador A está solicitando um serviço, adiciona ao pacote o número da porta que o computador B utiliza para atender seus clientes nesse serviço específico (128.10.2.4:53). Além do endereço IP de destino e da porta destino, o computador A também precisa compor em seu pacote IP o seu próprio endereço IP e uma porta origem (128.10.2.3:1184). Essa porta (1184) é um valor sorteado entre as portas não consideradas reservadas (portas não reservadas são maiores do que 1.024). A partir desse momento, o protocolo TCP do computador B identificará uma conexão pelo par (IP, porta) de todos os computadores conectados a ele. Dessa forma, uma mesma porta pode ser usada para estabelecer simultaneamente duas ou mais conexões sem nenhuma ambiguidade.

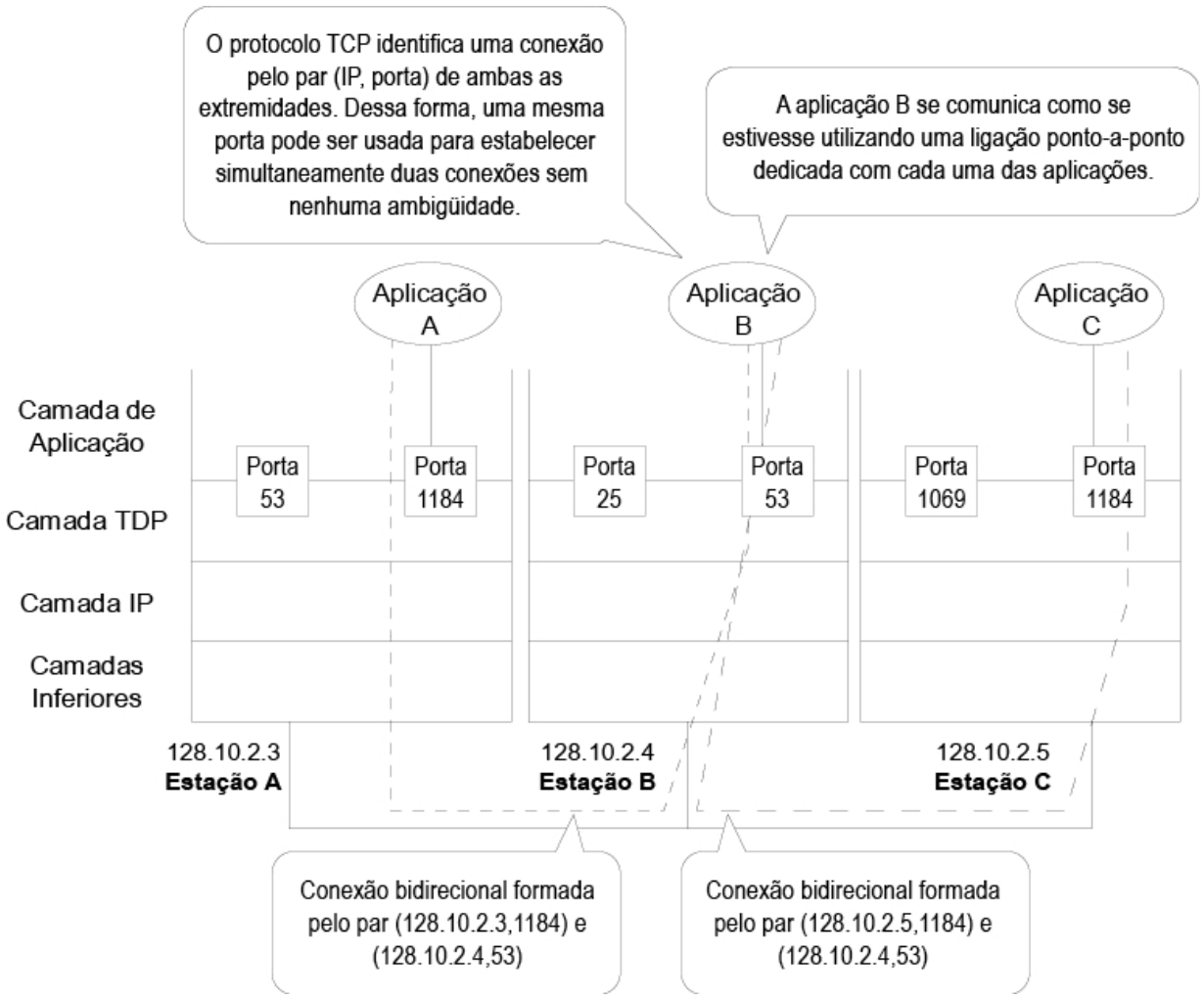



*Figura 10.2 – Funcionamento do protocolo TCP.*

## 10.2.1 Características do protocolo TCP

O protocolo TCP difere-se do IP por oferecer um serviço de entrega de dados confiável – do tipo orientado por conexões. Além disso, assegura uma entrega de dados livre de erros ao seu destinatário, garantindo os fatores integridade e sequenciamento corretos. Para que essa qualidade exista, o protocolo TCP utiliza-se de alguns processos, como processo de handshake, controle de sequências, controle de fluxo e controle e correção de erros. A seguir, detalharemos cada um desses processos.

### 10.2.1.1 Handshake

O processo de handshake significa aperto de mãos. Designa a

habilidade que dois dispositivos que trocam dados entre si têm de estabelecer normas de comunicação que possibilitem a conversação entre si, viabilizando a transmissão de dados. Para tanto, precisam combinar parâmetros como taxa de transferência, largura de banda, tamanho do pacote de dados e, ainda, qual o protocolo de correção de erros será utilizado.

O transmissor e o receptor trocam mensagens entre si, chamadas de acknowledgement messages (mensagens de reconhecimento de recebimento) e representadas de forma abreviada por ACK. Mensagens recebidas com erros causam uma comunicação de falha chamada de NACK, abreviação de not acknowledgement (não acusado o reconhecimento). Em caso de falha na comunicação, cabe ao TCP notificar o emissor para que retransmita os dados. A seguir, apresentaremos um exemplo do processo de uso das mensagens do tipo ACK.

Imagine se você estivesse falando ao telefone com alguém, tentado fazer com que a pessoa do outro lado preenchesse um formulário com seus dados pessoais. A cada informação transmitida, a pessoa do outro lado diria: “OK, entendido”. Se ela não entendesse, diria: “Repita, por favor”. Esse processo se repetiria até que todos os dados fossem transmitidos corretamente.

#### 10.2.1.2 Controle de sequências

Quando uma informação é transmitida por meio de uma rede TCP/IP, os dados são divididos em pequenas partes, embalados para presente em um pacote que contém pequenas porções dos dados, com informações de controle de erro, dados do emissor e do receptor. Também faz parte do pacote uma indicação do número de sequência que indica a ordem desse pacote em relação ao pacote total. O TCP oferece um serviço de comunicação orientado à conexão, garantindo que as mensagens serão recebidas na mesma sequência em que foram transmitidas. Essa característica permite fragmentar as mensagens muito grandes em porções menores, de maneira a compatibilizá-las com o tamanho máximo imposto aos pacotes IP. A mensagem original é reconstituída de maneira transparente pela camada de transporte do receptor. A seguir,

apresentaremos um exemplo dessa característica.

Imagine a necessidade de enviar um livro para alguém, via correio, que só aceita cartas com até dez páginas. Então, dividiríamos o livro em pacotes de dez páginas e mandaríamos cada pacote em um envelope. O destinatário, à medida que recebe as cartas, vai remontando as páginas, baseando-se na numeração que está em cada uma. Pode ocorrer que pacotes viajem por links de comunicação mais lentos em relação a outros, logo existe grande probabilidade de os pacotes chegarem fora da ordem em que foram enviados. Assim, o TCP deve analisar o código de sequência presente no pacote e ordená-lo de forma a apresentar ao usuário a informação na íntegra. O protocolo IP é responsável pelo roteamento dos pacotes e pode alternar os caminhos de acordo com regras de QoS (qualidade de serviço).

#### 10.2.1.3 Controle de Fluxo

Os dados que viajam pela rede seguem os mais diversos tipos de meios de transmissão, como fios de cobre, cabos de fibra ópticas, satélites e cabos telefônicos. Em cada modalidade, pode-se atingir determinada taxa de transmissão de dados, dependendo de vários fatores, como carga no circuito, volume de requisições e características inerentes ao circuito.

Cabe ao TCP fornecer a base para que cada dispositivo negocie a melhor taxa de transmissão, de maneira a realizar a transferência de dados o mais rápido possível, sem que ocorram taxas muito altas de erros, otimizando a largura de banda da rede. Se o buffer de dados no receptor ficar sobrecarregado, o TCP pedirá ao remetente dos dados que reduza a velocidade de emissão, para que ocorram menos erros, garantindo, dessa forma, que os dados realmente cheguem ao destinatário.

#### 10.2.1.4 Controle de erro

O controle de erro fornecido pelo protocolo TCP tem como objetivo garantir que pacotes inconsistentes sejam aceitos pelo receptor. Quando acontece alguma inconsistência, o receptor precisa notificar o transmissor para remeter novamente os dados. Esse processo é

chamado de controle de erros, sendo uma das funções do TCP.

## 10.2.2 Segmento TCP

A unidade de dados do protocolo TCP é denominada segmento. Geralmente, cada segmento TCP é encapsulado no campo de dados de um único pacote. Um segmento TCP é composto de duas partes: um cabeçalho de controle e um campo de dados. O formato do segmento é apresentado na figura 10.3.

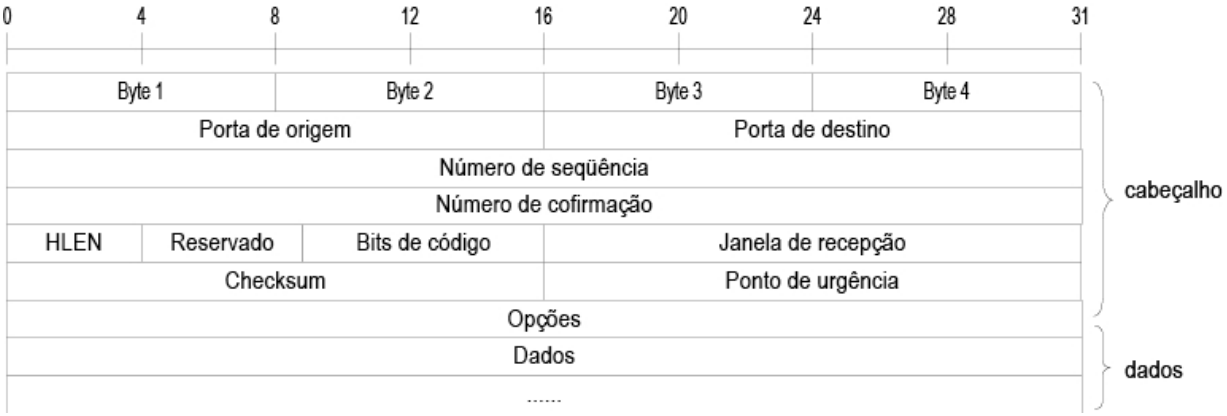



*Figura 10.3 – Formato do segmento TCP.*

Na tabela 10.1, detalharemos cada um dos campos que compõem o segmento TCP.

*Tabela 10.1 – Detalhes dos campos do segmento TCP*

| Campo | Descrição |
|---|---|
| Porta de origem | Identificador de 16 bits que identifica a porta que transmitiu o segmento. |
| Porta de destino | Identificador de 16 bits que identifica a porta para onde o segmento será transmitido. |
| Número de sequência | O protocolo TCP fragmenta mensagens muito longas e as transmite numa sequência de segmentos. O campo número de sequência indica qual porção da mensagem original está sendo transmitida no segmento corrente. Essa informação é utilizada pelo receptor para reordenar os segmentos que cheguem fora de ordem. A figura 10.4 apresenta uma mensagem e sua divisão. |

| Campo | Descrição |
|---|---|
| Número de confirmação | Identifica o número do próximo byte que o receptor espera receber. Essa informação é enviada pelo receptor ao transmissor por meio das mensagens de confirmação de recebimento (ACK). |
| HLEN | Esse campo contém um número inteiro que determina o comprimento do cabeçalho do datagrama em múltiplos de palavras de 32 bits. O comprimento do cabeçalho é variável, pois os campos opções e preenchimento não têm tamanho fixo. |
| Bits de código | Esse campo identifica o tipo de mensagem transportada pelo segmento. Os segmentos podem transportar mensagens de vários tipos, como confirmação (ACK), estabelecimento ou liberação de conexões, dados etc. |
| Janela de recepção | TCP fornece meios para que o receptor cadencie o fluxo de dados enviados pelo transmissor. Toda vez que o receptor confirma o recebimento de uma mensagem (enviando uma mensagem ACK para o transmissor), ele preenche o campo janela de recepção, informando o número de bytes que é capaz de receber na próxima transmissão. O transmissor leva em consideração essa informação para determinar o tamanho do próximo segmento a ser enviado. |
| Ponteiro de urgência | Indica a posição (em bytes) em relação à sequência de dados recebidos em que os dados urgentes poderão ser encontrados. Esse mecanismo é utilizado para que o transmissor possa enviar mensagens de alta prioridade ao receptor. |
| Checksum | Esse campo contém o checksum de todos os bytes que compõem o segmento TCP (cabeçalho de controle e dados). Esse campo é utilizado pela estação receptora para verificar a integridade do segmento recebido. |
| Opções | Campo opcional de tamanho variável, múltiplo de 32 bits. Esse campo foi criado para que o protocolo TCP possa disponibilizar facilidades adicionais que não foram cobertas pelos campos padronizados do cabeçalho de controle. |
| Dados | Contém os dados transportados pelo segmento TCP. |

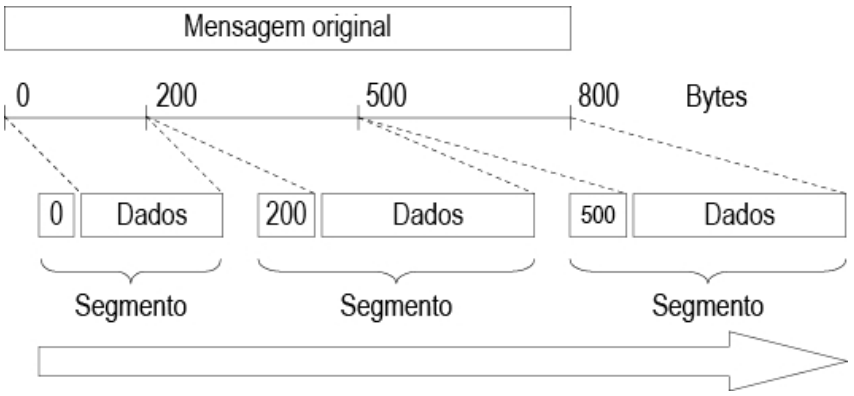



*Figura 10.4 – Divisão de uma mensagem em segmentos com a respectiva identificação da sequência.*

### 10.2.3 Protocolo UDP

O protocolo UDP (*User Datagram Protocol*) oferece aos protocolos da camada de aplicação um serviço não orientado à conexão, ou seja, não confiável. Um serviço é dito não confiável quando o protocolo utilizado não permite o controle de erros, o controle de fluxo ou o controle da sequência dos segmentos.

Os serviços sem orientação por conexão são similares ao correio. Quando se escreve uma carta, é preciso que alguém a leve a seu destinatário, ou seja, o serviço sem orientação por conexão não estabelece uma conexão ponto a ponto. O serviço sem orientação por conexão é muito similar ao da entrega por Sedex. Você deixa a encomenda na agência do correio, de onde é levada por um transportador até a agência central; de lá, a mercadoria é encaminhada até uma agência intermediária, e assim por diante, até chegar ao destino. A entrega chega ao destino, mas pode atrasar devido ao mau tempo, ao excesso de encomendas e a outros fatores. Podem ocorrer situações em que, ao mandar três cartas, uma chegue antes da outra, ficando por conta da pessoa que vai recebê-las colocá-las em ordem.

O protocolo UDP transmite uma mensagem pelos canais de comunicação, igualmente como acontece com o TCP. Entretanto, esse protocolo não se responsabiliza pela ordem em que os segmentos chegarão, como também não oferece garantia de que chegarão. Todos esses controles são repassados aos protocolos da

camada de aplicação que utilizam o UDP como protocolo de transporte. Como exemplos de protocolos que utilizam o UDP, temos o DNS e o BOOTP.

## 10.2.4 Segmento UDP

Um segmento UDP é composto de duas partes: um cabeçalho de controle e um campo de dados. O formato da mensagem é detalhado na figura 10.5.

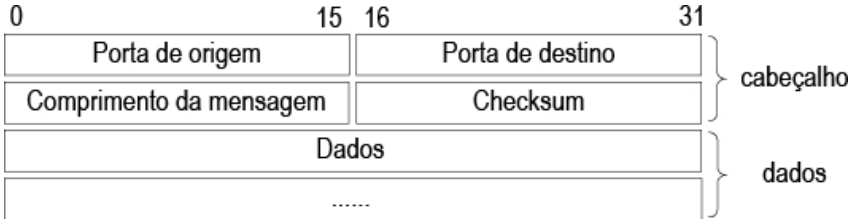



*Figura 10.5 – Formato do segmento UDP.*

Na tabela 10.2, detalharemos cada um dos campos que compõem o segmento UDP e verificaremos que o formato do segmento é bem mais simples.

*Tabela 10.2 – Detalhes dos campos do segmento UDP*

| Campo | Descrição |
|---|---|
| Porta de origem | Identificador de 16 bits que identifica o endereço, ao nível da camada de transporte, para o qual deve ser enviada uma eventual resposta à mensagem transmitida. |
| Porta de destino | Identificador de 16 bits que identifica o endereço do destinatário da mensagem ao nível da camada de transporte. |
| Comprimento da mensagem | Corresponde ao comprimento total da mensagem UDP, em bytes, incluindo o cabeçalho e o campo de dados. |
| Checksum | O preenchimento do campo checksum é opcional. A informação desse campo é usada pelo receptor para verificar a integridade dos dados recebidos. No caso de haver erro, o receptor descartará a mensagem. |
| Dados | O campo de dados contém as informações a serem transmitidas. O comprimento máximo da mensagem UDP, incluindo o campo de dados e o cabeçalho, é de 64 Kbytes. |

## 10.3 Exercícios do capítulo 10

1. Sobre o protocolo TCP, é afirmar que:

a) Os endereços IP identificam tanto um host como uma rede. Para isso, os bits mais significativos identificam a rede e os menos significativos, o host.

b) O ICMP (*Internet Control Message Protocol*) fornece um serviço de mensagens de controle sobre a camada de rede. Essas mensagens podem relatar erros e solicitar ou responder a pedidos de eco (o comando *ping* é uma solicitação de eco do ICMP).

c) O protocolo UDP não estabelece conexões, sendo utilizado em aplicações como DNS, SNMP e FTP.

d) Para controle de erros, o TCP faz uso de um algoritmo chamado janelas deslizantes.

e) O protocolo TCP estabelece conexões por meio de um procedimento chamado aperto de mão de três vias, ou *three-way handshake*.

2. Sobre os protocolos de transporte do TCP/IP, é correto afirmar:

a) Por ser desprovido de algoritmos de controle de fluxo e congestionamento, o protocolo UDP mostrou-se inadequado para aplicações de tempo real, como streaming media, por exemplo.

b) Por ser um protocolo não orientado à conexão e sem garantia de entrega, o UDP não é empregado em nenhuma das aplicações da Internet, sendo de interesse restrito ao uso acadêmico.

c) O protocolo TCP é orientado à conexão, possui algoritmos de controle de fluxo e congestionamento e garante a entrega dos dados sem atrasos.

d) Para estabelecer uma conexão UDP, cliente e servidor trocam sinais de controle em um processo conhecido como aperto de mão (*handshake*).

e) O protocolo TCP é orientado à conexão e, por isso, garante controle de fluxo, controle de sequência e controle de erros.

3. (Sanepar, 2004) Analise as seguintes proposições sobre a arquitetura TCP/IP:

I. Os protocolos de transporte da arquitetura TCP/IP possuem dois tipos de serviço: serviço confiável e orientado à conexão, provido pelo TCP, e serviço não confiável e não orientado à conexão, oferecido pelo UDP.

II. O TCP possui algoritmos de controle de fluxo e congestionamento, bem como detecção e correção de erros e garantia de entrega dos dados sem atrasos.

III. Justamente por não possuir algoritmos de controle de fluxo e congestionamento, o UDP é ideal para aplicações de streaming media.

IV. Aplicações como HTTP, FTP, correio eletrônico e terminal virtual (Telnet) são suportadas pelo protocolo TCP.

Assinale a alternativa correta:

a) Somente as proposições I, II e III são verdadeiras.

b) Somente as proposições I, III e IV são verdadeiras.

c) Somente as proposições I, II e IV são verdadeiras.

d) Somente as proposições I e IV são verdadeiras.

e) Todas as proposições são verdadeiras.

4. (Copel, 2010) O protocolo TCP (*Transmission Control Protocol*) é um dos protocolos que podem ser utilizados na camada de transporte do conjunto de protocolos inter-rede (TCP/IP). Sobre o TCP, é incorreto afirmar que:

a) O protocolo TCP realiza controle de erros fim a fim.

b) O protocolo TCP colabora no controle de congestionamento da rede, reduzindo a taxa de transmissão em caso de erros.

c) O protocolo TCP estabelece um estado de conexão entre cliente e servidor.

d) O protocolo TCP implementa qualidade de serviço fim a fim.

e) O protocolo TCP implementa o controle de fluxo fim a fim.

CAPÍTULO 11

# Resolução de nomes

Neste capítulo, serão explicadas as formas de resolução de nomes utilizados em redes domésticas e pela Internet. Abordaremos os arquivos de hosts e de lmhosts, bem como o protocolo DNS.

## 11.1 Introdução

Não é normal que, ao utilizar nosso *browser* ou outro programa Internet, seja requisitada a comunicação com determinado servidor Internet por meio do seu endereço IP. Ninguém manda um email para *fulano@190.245.123.50*, envia para *fulano@empresa.com.br*. Da mesma forma, ninguém está acostumado a digitar no seu *browser* um endereço 190.245.123.50 para requisitar a comunicação com um site. Os endereços IP foram cuidadosamente planejados para que fossem precisos, fáceis de manusear e de rotear na infinidade de redes locais e públicas que é a Internet. Entretanto, uma vez que não é fácil conseguir memorizá-los, criou-se o sistema de nomes Internet que permite atribuir nomes a um ou mais endereços IP, que passam então a se chamar domínios.

Um dos sistemas de atribuição de nomes a endereços IP é chamado de DNS (*Domain Name Server* – servidor de nomes de domínios). Existem, entre outros, os arquivos de hosts, lmhosts e, ainda, o protocolo WINS (*Windows Internet Name Service*) proprietário da Microsoft. Dentro de um domínio, os servidores terão, além de seus respectivos endereços IP, nomes que os diferenciam uns dos outros. Por exemplo, em um determinado domínio chamado por *empresa.com*, poderão existir os servidores: *micro1.empresa.com*, *micro2.empresa.com*, *fulano.empresa.com*, *servidor.empresa.com*, e assim por diante.

Esses nomes específicos são chamados de *host name* ou nomes de servidor. O processo de fazer a correlação entre os domínios e os host names é chamado de resolução de nomes e, para executá-los,

podemos utilizar os recursos conhecidos como hosts, DNS, lmhost e WINS. A seguir, descreveremos os recursos disponíveis para a resolução de nomes.

## 11.2 Arquivo hosts

Caso não se utilize DNS para resolução de endereços ou o servidor DNS pare de funcionar por algum motivo não identificado, deve-se, então, colocar todas as máquinas da rede no arquivo hosts, o qual é codificado no formato ASCII, com linhas que contêm o endereço IP e o nome dado ao servidor. Assim, ao navegar na Intranet, Extranet ou Internet, pode-se indicar aos programas nomes literais para recuperar os recursos desejados.

No início da antiga ARPANET (precursora da Internet), foi definido que todas as máquinas que fossem conectadas à rede teriam um arquivo hosts, que conteria os endereços de todas as outras máquinas conectadas. Esse arquivo era mantido pela coordenação da ARPANET e distribuído periodicamente como uma atualização. Chegou um momento em que o número de máquinas cresceu tanto que a transmissão do arquivo hosts pela rede começou a se tornar um problema. Foi, então, que surgiu o DNS (*Domain Name Service*), que permitiu que as máquinas não precisassem mais de arquivos hosts com os endereços de todas as outras máquinas, passando, então, a utilizar um processo centralizado de resolução de nomes.

No entanto, isso não acabou com a utilidade do arquivo hosts, que é responsável por permitir a especificação de endereço e domínio da máquina local e o acesso a máquinas quando o serviço DNS não está disponível, ou seja, quando existem problemas com o servidor de DNS. Vejamos um exemplo no qual temos a máquina com o nome de isulpar. Para adicionarmos ao arquivo hosts, precisamos conhecer seu endereço IP, que, nesse caso, será 10.0.0.1. A tabela 11.1 apresenta um exemplo de um arquivo hosts:

*Tabela 11.1 – Exemplo de um arquivo hosts*

| Endereço IP | Nome da máquina | Apelido | Comentário |
|---|---|---|---|
| | | | |

| | | | |
|---|---|---|---|
| 127.0.0.1 | Localhost | | |
| 10.0.0.1 | isulpar.administracaoisulpar | laboratório | #Máquina do laboratório |
| 192.168.0.10 | micro1.empresa.com | | |
| 192.168.0.12 | micro2.empresa.com | | |
| 192.168.0.14 | micro3.empresa.com | | #Máquina do administrador |

O arquivo hosts é composto de várias linhas que identificam máquinas. Cada linha é composta de três colunas, separadas por espaços. Os comentários, se houver, poderão ser inseridos, colocando-se no final da linha mais um espaço, mais o caractere #, mais a nota. Cada servidor fica em uma linha, com seu endereço IP na primeira coluna, separado por um espaço do nome literal do servidor. O arquivo hosts é lido cada vez que uma nova solicitação de resolução de nomes é feita.

Analisando a linha correspondente à máquina isulpar.administracao, a primeira coluna contém o endereço IP (10.0.0.1) associado à nossa máquina. O endereço escolhido faz parte da classe A. A segunda coluna contém o FQDN (*Fully Qualified Domain Name*), que é o nome completo da máquina, ou seja, o nome da máquina associado ao nome do domínio. Em nosso exemplo (isulpar.administração), isulpar é o nome da máquina e administração é o nosso domínio. A terceira e última coluna é a mais interessante. Em nosso exemplo, ela não parece importante, contendo apenas o nome da máquina sem o domínio. Porém, essa coluna especifica apelidos para a máquina. Assim, poderemos nos referir a esse servidor escolhendo a string isulpar.administração, apenas isulpar ou, ainda, laboratório. Isso é útil quando uma máquina é usada por grupos de pessoas diferentes na rede de uma empresa. É importante ressaltar que os nomes devem estar separados por um espaço.

O inconveniente do uso do arquivo hosts é que deve existir em todas as máquinas da sub-rede. Assim, toda vez que for modificado

em uma rede local ou sub-rede, um arquivo hosts deverá ser copiado para todas as estações de trabalho e servidores. Essa atividade tomaria muito tempo do administrador e haveria, ainda, o risco de algum equipamento ser deixado de lado. Para solucionar essa grande dificuldade, utilizamos o protocolo DNS.

## 11.3 Arquivo lmhosts

O arquivo lmhosts mapeia nomes NetBIOS em endereços IP e pode ser usado quando o servidor de WINS (*Windows Internet Name Server*) está indisponível. Se os servidores WINS estiverem disponíveis na rede, o arquivo lmhosts pode ser usado para suportar as sub-redes que não têm um servidor WINS configurado ou para fornecer um serviço de resolução de nomes de reserva, caso o servidor WINS não esteja disponível. O arquivo lmhosts fornece um método de resolução de nomes NetBIOS que pode ser usado em pequenas redes que não usam um servidor WINS.

## 11.4 Protocolo DNS

O DNS (*Domain Name Server*) pode ser visto como um arquivo hosts remoto (não é exatamente assim, mas podemos ver dessa maneira para entender). Sempre que precisar encontrar algum recurso da rede, uma máquina precisará saber qual o endereço IP do recurso requisitado. No entanto, lembrar endereços IP não é muito fácil nem produtivo. Então, para ajudar a encontrar endereços IP, usamos um servidor de nomes, o qual tem como principal objetivo informar o endereço IP de nomes Internet, como *www.empresa.com.br*. A seguir, analisaremos uma consulta DNS.

### 11.4.1 Consulta DNS

Sempre que precisamos acessar determinado site por meio de seu nome Internet (*www.empresa.com.br*), ocorre uma consulta DNS. Nesse momento, é gerado um pacote IP com o endereço IP destino do servidor DNS configurado no sistema operacional que originou o pedido, questionando qual é o endereço IP em que está situado o servidor denominado *www.empresa.com.br.*

Caso o DNS configurado não saiba responder, o pedido é redirecionado aos servidores DNS pertencentes à InterNIC; caso o nome exista, tais servidores informam o endereço IP do servidor DNS, que poderá resolver esse nome. A figura 11.1 apresenta o fluxo de uma requisição e a sua conversão de nomes:

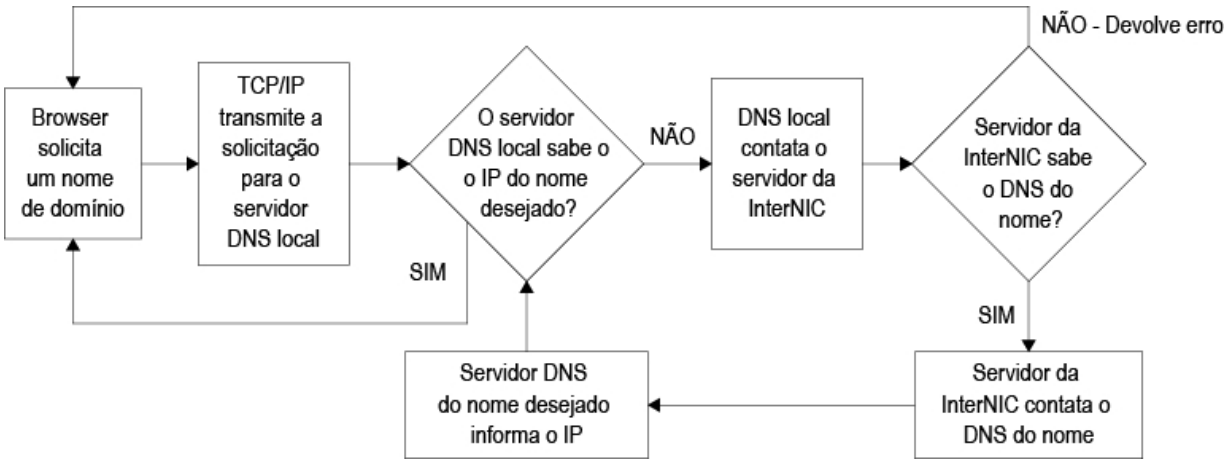



*Figura 11.1 – Fluxo da resolução de nomes.*

## 11.5 Exercícios do capítulo 11

1. Em relação ao serviço de nomes (DNS), assinale a alternativa incorreta:

a) O DNS é um esquema de gerenciamento de nomes hierárquico e centralizado, cuja autoridade central é a zona “.”.

b) O DNS define a sintaxe dos nomes usados na Internet, as regras para delegação de autoridade na definição de nomes, um banco de dados que associa nomes a atributos e um algoritmo para mapear nomes em endereços.

c) Um servidor secundário é uma espécie de cópia de segurança do servidor primário. Quando não é possível encontrar um domínio por meio do servidor primário, o sistema tenta resolver o nome por meio do servidor secundário.

d) Cada administrador de zona que contém dados decide um tempo de vida (TTL) para os dados. Um TTL pequeno garante a consistência, enquanto um TTL grande diminui o tempo que se leva até conseguir determinada informação.

e) Um registro SOA marca o começo de uma zona, um grupo de registros de recursos localizados no mesmo lugar dentro do espaço de nomes do DNS.

CAPÍTULO 12

# NAT – Network Address Translation

Neste capítulo, descreveremos o processo disponível em servidores *multi-homed* (servidores roteadores) e roteadores para o redirecionamento de requisições à Internet, geradas por computadores com IP origem não roteável. Além disso, abordaremos também o processo PAT (*Port Address Translation*), a função de um servidor Proxy e a diferença entre NAT estático e NAT dinâmico. Será comentada ainda a diferença entre o roteador tradicional e o roteador que implementa NAT.

## 12.1 Introdução

O NAT (*Network Address Translation* – Tradução de Endereço de Rede) não é um protocolo nem se refere a um padrão especificado por entidades internacionais. O NAT é apenas uma série de tarefas que um roteador (ou equipamento equivalente) deve realizar para converter endereços IPs entre redes distintas. Um equipamento que tenha o recurso de NAT deve ser capaz de analisar todos os pacotes de dados que passem por ele, além de trocar os endereços desses pacotes de maneira adequada, ou seja, substituir o endereço IP origem do pacote (endereço IP não roteável) pelo endereço IP do roteador (endereço IP roteável). Além dessa substituição de endereço, o roteador que possui NAT ainda cadastra em sua tabela a relação porta origem versus IP origem, a fim de devolver ao emissor o pedido feito.

Vários produtos disponíveis no mercado possibilitam que os endereços IP utilizados internamente nas empresas não precisem ser registrados na InterNIC, ou seja, o administrador da rede poderia atribuir aos computadores da empresa qualquer endereço IP e, ainda assim, permitir que tenham acesso à Internet. No exemplo a seguir, podemos observar que, na rede local da empresa ISULPAR, o endereço de rede utilizado nos computadores é 10.x.x.x, endereço

não registrado (não roteável – IP privado), porém um outro computador que também desempenha o papel de roteador faz a tradução do endereço para que esse endereço possa ser enviado para a Internet. O único endereço registrado pela InterNIC seria o da placa de comunicação externa do roteador. Nesse caso, o roteador faz um serviço de Gateway ao trocar o endereço da máquina que está tentando acessar a Internet por um endereço registrado. A figura 12.1 apresenta uma rede em que o roteador possui a capacidade de fazer NAT.

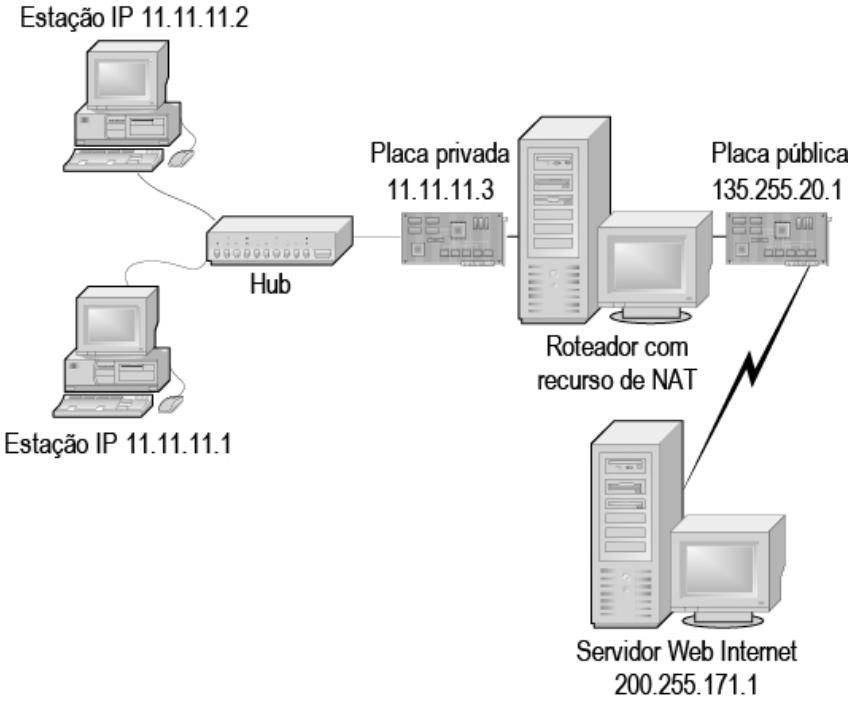



*Figura 12.1 – Rede configurada com NAT.*

O roteador da figura 12.1 (endereço IP 11.11.11.3), ao receber o pacote de dados a ser enviado para a Internet contendo o endereço IP da máquina que está solicitando a conexão 11.11.11.2, por exemplo, cria um outro pacote de dados, porém com o endereço origem associado à sua placa externa (135.255.20.1), o qual é registrado e válido.

Para cada conexão aberta pelo NAT, ele abre um socket com a estação interna, de forma que só deixa passar pacotes para a rede interna que sejam respostas às solicitações das estações. A devolução é identificada pela porta origem e o IP origem da

requisição. Em resumo, todas as estações da rede privada acessam a Internet utilizando um único endereço IP, que seria o da placa pública, ou seja, todos os computadores poderiam acessar a Internet, utilizando apenas um endereço IP registrado.

A figura 12.2 apresenta passo a passo o processo de comunicação de um computador com a Internet utilizando NAT.

O NAT é encontrado de forma nativa em vários sistemas operacionais, sendo normalmente implementado em rede de médio porte (70 estações). Um dos produtos presentes na plataforma Windows que oferece esse serviço é o ICS (*Internet Connection Sharing*). No Linux, o serviço de NAT é encontrado *no IpChains* e *IpTables*.

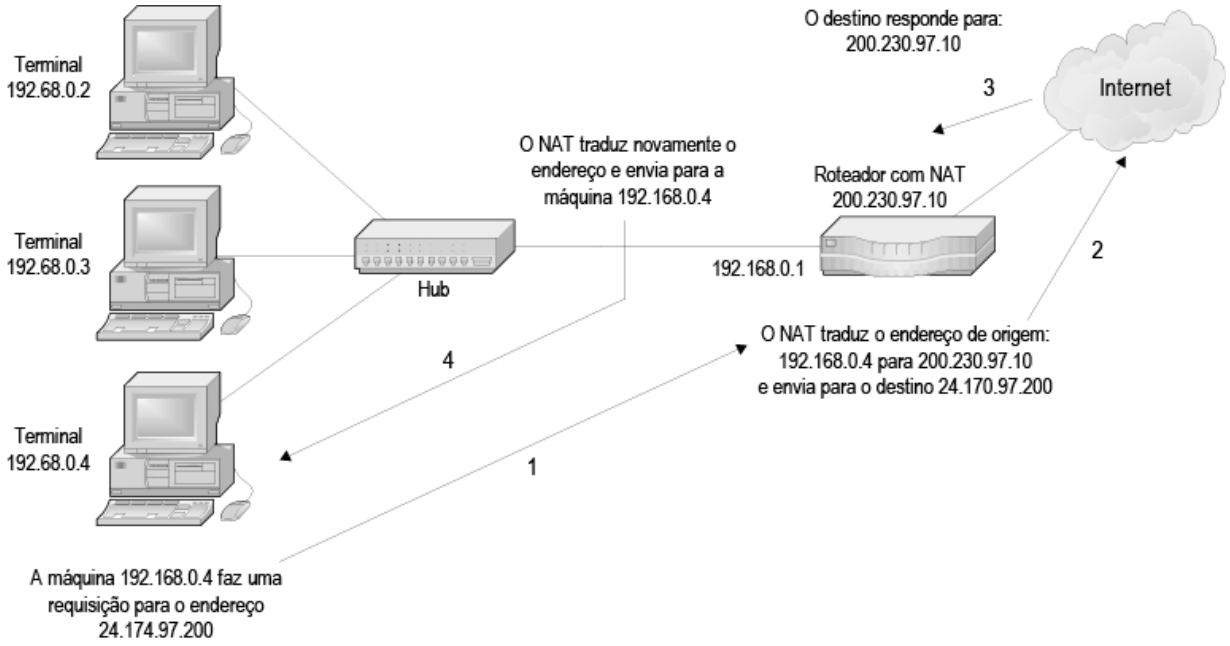



*Figura 12.2 – Sequência entre a emissão e o recebimento da resposta em uma rede utilizando NAT.*

## 12.2 Diferença entre roteador tradicional e um roteador utilizando NAT

Um roteador tradicional difere de um roteador que oferece o NAT na seguinte questão: o servidor ou roteador que oferece NAT substitui o endereço IP origem do pacote (endereço não roteável) pelo seu (endereço roteável) e o envia para a Internet, enquanto um roteador

tradicional, ao receber o pacote, remonta como de prática, mas não substitui o IP origem pelo endereço IP do servidor ou roteador NAT. Dessa forma, redes LANs que aparentemente não conseguiriam acessar a Internet por não possuírem um endereço válido para cada estação podem consegui-lo utilizando esse artifício técnico.

Para que consiga devolver cada requisição ao seu solicitante corretamente, o servidor ou roteador NAT utiliza uma tabela. A seguir, comentaremos a tabela gerada.

## 12.3 Tabela gerada pelo NAT

A utilização de tradução de endereços de rede (e de portas) nos roteadores permite que várias máquinas em uma rede local possam se comunicar com outras sem possuírem endereços IP válidos na Internet. Para isso, é utilizado um equipamento de rede (roteador) que possui, pelo menos, duas interfaces de rede. O roteador realiza a conversão do endereço IP (e das portas) dos pacotes enviados e recebidos. O equipamento que se propõe a fazer NAT internamente gera uma tabela de traduções ativas em cada instante, conforme mostra a tabela 12.1.

*Tabela 12.1 – Tabela interna de um equipamento configurado com NAT*

| Endereço de origem | Porta de origem | Endereço externo | Porta externa | Porta NAT | Protocolo |
|---|---|---|---|---|---|
| 10.0.0.5 | 21023 | 128.1.19.1 | 80 | 14003 | TCP |
| 10.0.0.3 | 1272 | 128.1.19.1 | 80 | 14012 | TCP |

A tabela 12.1 informa que foram iniciadas duas requisições na rede local pelos computadores: 10.0.0.5 e 10.0.0.3. Ambas as requisições possuem como objetivo acessar o servidor web situado na Internet e identificado pelo endereço IP 128.1.19.1:80. Conforme comentado, o roteador NAT armazena em sua tabela os dados que serão utilizados para a devolução do pedido ao emissor e a aplicação devida. É importante ressaltar que todas as conexões estabelecidas pelo protocolo TCP possuem a porta origem e a porta destino, as quais são utilizadas para identificar as aplicações

internamente no computador. O equipamento configurado com NAT baseia-se na porta NAT para devolver a requisição ao computador correto com a respectiva porta.

## 12.4 Tipos de NAT

O NAT possui três formas de funcionamento: o NAT dinâmico, o NAT estático e a junção dos dois. A seguir, descreveremos cada um deles.

### 12.4.1 NAT dinâmico

O NAT dinâmico permite acesso à Internet de dentro da rede local, sendo o mais utilizado. Com o NAT dinâmico, todos os acessos à rede externa terão o endereço da estação substituído pelo endereço da interface pública do servidor ou roteador com o NAT habilitado, de modo que o único endereço a aparecer para a rede externa (Internet) será o endereço da placa pública. A figura 12.3 apresenta a comunicação entre um computador e a Internet, utilizando NAT dinâmico.

Nesse exemplo, as estações possuem os endereços IP 10.0.0.2, 10.0.0.3, 10.0.0.4 não registrados pela InterNIC ou Fapesp. O servidor possui, na placa privada, o endereço 10.0.0.1 e, na placa pública, o endereço 200.231.107.41. Quando necessita acessar a Internet, a estação envia pacotes IPs para o roteador. Cada pacote contém o cabeçalho de controle, o endereço IP origem e o endereço IP do destinatário. O roteador ou servidor que receberá esses pacotes deverá estar configurado para fazer o serviço de NAT. O roteador recebe o pacote IP da estação e substitui apenas o endereço IP do remetente (10.0.0.1), que é um endereço não registrado, pelo endereço da sua placa pública (200.231.107.41), e envia-o para a máquina destino, por meio da Internet. Os pacotes que a máquina destino enviar como resposta serão destinados ao endereço da placa pública do roteador, uma vez que esse é o único endereço válido para trafegar nos roteadores internos da Internet.

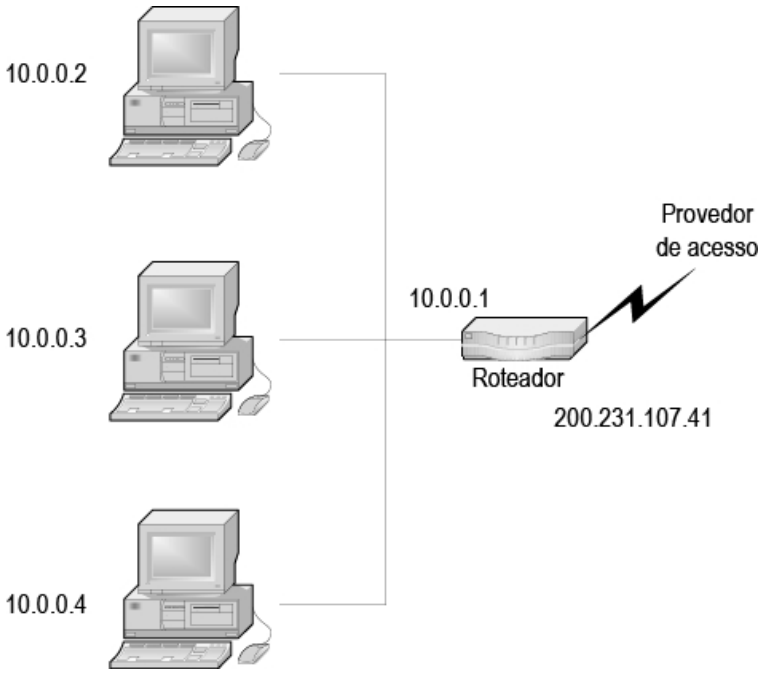



*Figura 12.3 – Rede configurada com NAT.*

O servidor ou roteador recebe o pacote resposta, troca novamente o endereço IP e o envia para a estação que originou a conexão. Com esse sistema, o único endereço IP que aparece e pode ser acessado pela Internet é o endereço da placa pública do servidor ou roteador. Assim, dificulta-se a ação de um hacker que tenta invadir uma estação ou outros computadores dentro da rede privada da empresa, pois o processo de NAT esconde os endereços e os computadores da rede LAN.

## 12.4.2 NAT estático

O NAT estático permite acesso de fora (Internet) para dentro da rede local, sendo utilizado quando se quer esconder o servidor de email ou web dentro da rede local. Todas as requisições serão direcionadas ao servidor com NAT, o qual, depois de pesquisar em sua tabela, repassará a solicitação ao equipamento com capacidade de processar a requisição, ou seja, um servidor que possua o serviço solicitado. A figura 12.4 apresenta um exemplo de rede configurada com NAT estático.

O NAT estático utiliza uma tabela especialmente para relacionar o IP público com o IP privado. Essa tabela possui um endereço

externo e um interno, de forma que o NAT passará qualquer pacote destinado ao endereço IP externo 135.255.20.2 para o IP interno 11.11.11.5. Esse recurso é utilizado quando, por exemplo, a rede privada da empresa possui um servidor web que necessita ser acessado por computadores da rede pública, mas, por questões de segurança, não se quer deixar o servidor com endereço público visível na Internet.

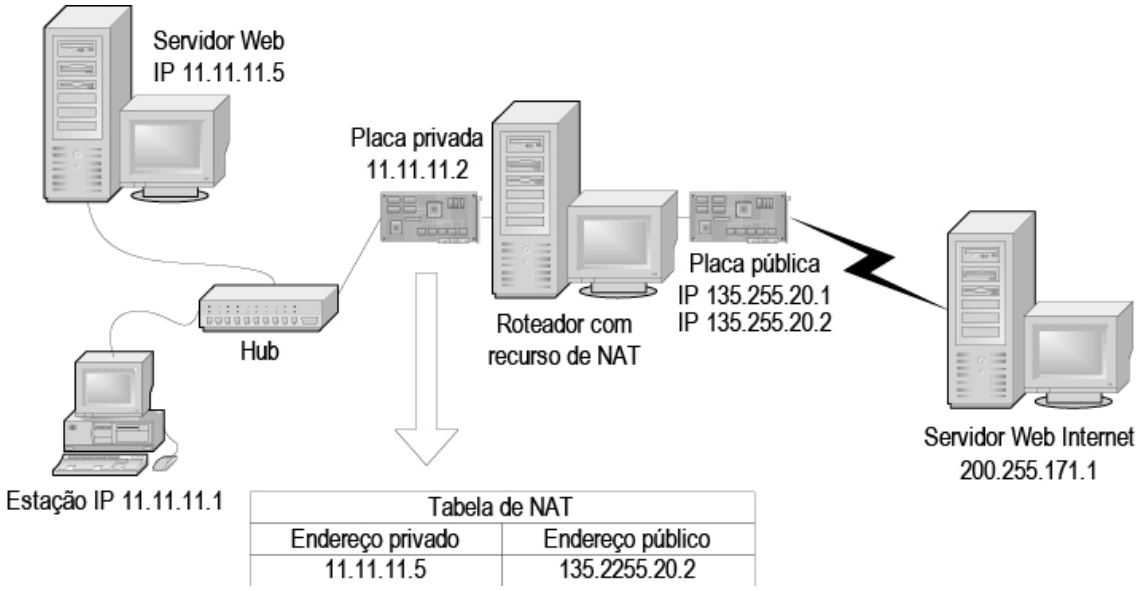



*Figura 12.4 – Rede configurada com NAT estático.*

Na figura 12.4, o endereço privado é 11.11.11.5 e o endereço público correspondente é 135.255.20.2. Para que o processo seja efetuado com sucesso, deve-se configurar no roteador que implementa o NAT uma tabela relacionando o endereço público e o endereço privado.

Podemos observar na figura 12.4 que a placa pública do servidor foi habilitada com dois endereços IPs: o 132.255.20.1 e o 135.255.20.2. O primeiro (132.255.20.1) serve para redirecionar requisições de computadores internos para servidores externos. O segundo (132.255.20.2) serve para redirecionar requisições externas para o servidor web interno (11.11.11.5). No entanto, a partir da tabela NAT estática, pode-se programar que, ao chegar um pacote destinado ao endereço 135.255.20.2, deve ser sempre entregue à máquina da rede privada 11.11.11.5. É importante

lembrar que um servidor que implementa NAT estático deverá possuir um endereço válido para cada redirecionamento.

## 12.5 Diferenças entre NAT, PAT e Proxy

É comum os leitores confundirem o significado e o funcionamento dos servidores NAT com o funcionamento dos servidores que oferecem PAT e Proxy. A seguir, apresentaremos as diferenças entre NAT, PAT e Proxy.

### 12.5.1 Funcionamento do NAT

Vamos comentar o NAT, informando um segundo exemplo baseado na figura 12.4. Vamos supor que nosso objetivo seja montar uma pequena rede em casa utilizando o ICS. Seu servidor que tem o NAT configurado possui o endereço externo 135.255.20.1 e o endereço interno 11.11.11.2. Suas estações possuem os endereços 11.11.11.1 e 11.11.11.5, respectivamente. Suponhamos que a estação 11.11.11.1 faça uma requisição para abrir uma página. O pacote IP que leva a requisição deve obrigatoriamente levar o endereço do solicitante, mas 11.11.11.1 é um endereço inválido, já que se trata de uma range privativa de endereços. Nesse caso, o roteador (software ou hardware) encarrega-se de fazer a conversão adequada que seria algo do tipo: a estação solicitante (11.11.11.1) pede ao gateway (11.11.11.2 – porta LAN do roteador) a abertura da página (TCP, porta 80). O gateway atribui, então, uma porta específica ao solicitante, digamos 135.255.20.1:5000, e envia a solicitação ao host desejado, supostamente 210.210.210.210:80. O pacote, então, retornará ao exato endereço que o gateway enviou ao host, ou seja, 135.255.20.1:5000. Dessa forma, quando o pacote for retornar para a porta 5000, o gateway saberá que este deve ser encaminhado à estação 11.11.11.1.

### 12.5.2 Funcionamento do PAT

O PAT (*Port Address Translation*) age de forma diferente do NAT no sentido de que, baseando-se apenas na porta, realizamos o redirecionamento de uma requisição a um endereço IP específico.

Para facilitar o entendimento, utilizaremos como base a figura 12.4. A rede apresentada possui dois computadores locais representados por 11.11.11.1 e 11.11.11.5, além de um roteador com o endereço 11.11.11.2. Consideremos a hipótese de adicionar um terceiro computador com o endereço 11.11.11.10. Esse computador será utilizado em nossa rede como um servidor de jogos, que estará acessível apenas internamente à rede LAN, já que a range 11.11.11.0 é um endereço de rede não roteável. Nessa configuração, ninguém conseguirá acessar o nosso servidor de jogos, pois o endereço IP do servidor que contém o jogo instalado é privado (endereço IP 11.11.11.10). Assim, utilizando um roteador ou um servidor configurado com PAT (software ou hardware), poderíamos permitir que qualquer requisição recebida pela placa pública (Internet) com uma determinada porta seja encaminhada para o endereço IP do nosso servidor de jogos, ou seja, qualquer requisição ao servidor Internet endereçado por 135.255.20.1 porta 27960 deverá ser redirecionada ao computador 11.11.11.10 porta 27960.

### 12.5.3 Funcionamento do Proxy

Os serviços de Proxy nada mais são do que grandes caches para acelerar o acesso à Internet. Sua principal função é eliminar o tráfego redundante que ocorre quando dois ou mais usuários tentam acessar a mesma página em intervalos curtos de tempo. Basicamente, o que um servidor Proxy faz é checar todas as requisições feitas aos serviços que ele suporta (HTTP, FTP, Telnet etc.) e verificar se a requisição já foi feita. Se não tiver sido feita, o Proxy realizará o download da página para seu cache. Se uma requisição para o endereço já tiver sido feita, o servidor Proxy verificará os arquivos já contidos no cache e comparará a data da página local com a data da página do servidor web destino. Se elas forem idênticas, o Proxy simplesmente enviará a página que está armazenada em seu cache. Caso sejam diferentes, o Proxy atualizará a página em seu cache e, então, a enviará ao usuário solicitante.

## 12.6 Exercícios do capítulo 12

1. Quais os tipos de NAT?
2. Comente o servidor NAT dinâmico.
3. Comente o servidor NAT estático.
4. Comente o PAT.
5. (Copel, 2010) Para realizar configurações de endereçamento IP prevendo o uso do NAT (*Network Address Translation*), deve ser utilizado um endereço de rede que foi previamente reservado para uso privativo, o qual, de acordo com a RFC1918, é dado por:

   a) 0.0.0.0 com máscara 0.0.0.0.

   b) 255.255.255.255 com máscara 255.255.255.255.

   c) 10.0.0.0 com máscara 255.0.0.0.

   d) 192.168.1.0 com máscara 255.255.255.0.

   e) 127.0.0.0 com máscara 255.0.0.0.

CAPÍTULO 13

# Sockets

Neste capítulo, descreveremos a API socket. O socket é responsável por fornecer uma interface de comunicação, a fim de permitir que dois ou mais computadores possam trocar informações. Serão abordadas as funções escritas na linguagem C, explicando onde é possível utilizá-las, além de exemplos de sua utilização na programação para redes.

## 13.1 Introdução

Sockets são abstrações simplificadas, criadas com o intuito de facilitar o desenvolvimento de aplicações que envolvam a comunicação entre dois ou mais computadores interligados por uma rede TCP/IP. A ideia dos sockets foi introduzida inicialmente no sistema operacional Unix BSD da Universidade de Berkeley.

Um socket representa uma conexão entre duas máquinas, de modo que tal conexão funciona como um canal de dados também chamado de *stream* (fluxo), isto é, um canal que permite a transmissão de dados de uma máquina para outra de forma bidirecional. Desse modo, cada socket possui um canal de entrada e outro de saída, e o que é enviado pelo canal de saída de uma máquina é recebido pelo canal de entrada da outra e vice-versa. Quando estabelecido, um socket utiliza endereços IPs para identificar o computador origem e o destino, e ainda utiliza um número de porta para diferenciar as requisições.

Cada endereço IP é único em uma rede, tornando cada máquina identificável como única. Em cada máquina, existem 65.536 números de portas, em que os primeiros 1.024 são reservados para os serviços-padrão (p. ex., FTP, Telnet, SMTP etc.) conforme já comentado. Cada número de porta é como um ramal da máquina, para o qual são direcionadas todas as mensagens, fazendo com que cada aplicação responda apenas pelas mensagens destinadas

a si própria.

Quando se deseja que dois computadores troquem dados, cada um deles deve utilizar um socket, em um processo muito similar às ações de leitura e de escrita de arquivos. A única diferença é que tal arquivo é realmente uma máquina remota que pode decidir o que fazer com os dados enviados ou solicitados.

A comunicação entre computadores em uma rede configurada sob o modelo de referência TCP/IP determina que um deles seja o servidor e o outro, o cliente. O servidor é responsável por abrir um socket e ouvir eventuais pedidos de conexão. O outro computador, denominado cliente, geralmente se conecta ao socket do servidor para obter dados. Para ter sucesso no estabelecimento do socket, o cliente precisa conhecer o endereço IP e saber em qual porta o servidor está ouvindo as requisições. Essa comunicação entre servidor e cliente pode ocorrer de dois modos, os quais serão descritos a seguir.

## 13.2 Modos de operação

Os sockets operam de dois modos, de forma que o modo orientado à conexão opera sob o protocolo TCP e o modo sem conexão opera sob o protocolo UDP.

### 13.2.1 Modo orientado à conexão

Os sockets orientados à conexão, ou stream sockets, operam como um aparelho telefônico, ou seja, estabelecem uma conexão e suspendem a ligação logo em seguida. O mesmo ocorre com as conexões a partir do protocolo HTTP. A partir desse momento, tudo o que flui entre esses dois computadores chegará na mesma ordem em que foi transmitido, além disso, a entrega das mensagens é garantida e livre de erros. Toda garantia e qualidade de entrega é oferecida pelo protocolo TCP (*Transmission Control Protocol*).

### 13.2.2 Modo sem conexão

Os sockets sem conexão, ou datagram sockets, operam como o sistema dos correios. A entrega, além de poder ocorrer em

sequência diferente da enviada pelo emissor, não está garantida. Quando criamos ou usamos um programa desenvolvido utilizando o modo sem conexão, estamos repassando aos protocolos da camada de aplicação toda a responsabilidade pela execução das atividades não executadas pelo protocolo da camada de transporte. O protocolo na camada de transporte que oferece o modo sem conexão é o protocolo UDP (*User Datagram Protocol*).

A opção entre cada modo dependerá das necessidades da aplicação, ou seja, se o objetivo for oferecer maior desempenho, o uso do protocolo UDP será melhor. A troca de dados com garantia de entrega e de sequência se destina a aplicações que não admitem perda de nenhuma mensagem. A troca de dados sem garantia de entrega e de sequência é mais adequada nos casos em que se tolera a perda de uma parte das mensagens, sendo mais rápida do que a troca confiável.

Enquanto aplicações de email sugerem o uso da troca confiável por exigirem garantia de entrega, as requisições geradas pelo protocolo DNS solicitam o uso do mecanismo de troca não confiável, em decorrência da sua necessidade de desempenho. Também se utiliza o modo sem conexão na transmissão de dados entre telefones IP.

Todo socket possui um ciclo de vida independentemente de possuir ou não conexão. As trocas de dados entre programas usando sockets ocorrem em três fases distintas, conforme está descrito na tabela 13.1:

*Tabela 13.1 – Fases da vida do socket*

| Fase | Descrição |
|---|---|
| Criação | Abertura do socket. |
| Leitura e escrita | Recepção e envio de dados por meio do socket. |
| Destruição | Fechamento do socket. |

## 13.3 API socket

Para o desenvolvimento de aplicações TCP/IP, utilizam-se interfaces

conhecidas como APIs socket. O socket é uma abstração desenvolvida pela Universidade de Berkley que estabelece um conjunto de interfaces para uma aplicação acessar os protocolos do modelo de referência TCP/IP. Basicamente, a API socket é constituída por constantes, estruturas e funções C, que são chamadas em uma sequência adequada, definindo algoritmos genéricos para aplicações cliente-servidor. A seguir, trataremos das funções auxiliares, as quais servem de base a outras funções.

### 13.3.1 Funções auxiliares

Nesse tópico, abordaremos a programação para redes nos baseando nas funções-padrão do sistema operacional Unix/Linux, as quais também podem ser utilizadas nos programas no ambiente Windows. O objetivo desse tópico é apresentar, de forma simples, a definição das funções e estruturas utilizadas no desenvolvimento de aplicações cliente/servidor em redes configuradas com o protocolo TCP/IP. Os valores e os ponteiros que serão utilizados como argumentos das funções da API socket (p. ex., socket(), bind(), listen() etc.) são obtidos a partir de funções auxiliares. A seguir, descreveremos as funções auxiliares, as quais devem ser executadas antes das funções da API socket.gethostbyname().

Além do endereço IP e da porta, os computadores também possuem nomes. A tradução de nomes em endereços IPs pode ser realizada em arquivos hosts ou pelo protocolo DNS. A função auxiliar gethostbyname() realiza a tradução do nome, baseando-se no arquivo host ou no protocolo DNS. Essa função tem o objetivo de receber como parâmetro o nome do computador e retornar um ponteiro para uma estrutura com a composição descrita na tabela 13.2:

*Tabela 13.2 – Estrutura hostent*

| Comando | Variável | Descrição |
|---|---|---|
| struct hostent | | |
| | | |

| | | |
|---|---|---|
| { | | |
| Char | *h_name; | /* Nome oficial do host */ |
| Char | **h_aliases; | /* Contém uma lista de nomes alternativos para o host. Caso no arquivo de hosts sejam incluídos apelidos para o host, essa variável conterá todos esses apelidos */ |
| Int | h_addrtype; | /* Retorna o tipo do endereço; geralmente é AF_INET. Indica que o socket será criado para conexões com a rede TCP/IP versão IPv4. Como outros exemplos, temos o AF_IPX para a família dos protocolos da Novell */ |
| Int | h_length; | /* Tamanho em bytes do endereço P */ |
| Char | **h_addr_list; | /* Retorna todos os endereços IPs do computador, caso este possua mais de uma placa de rede instalada */ |
| } | | |

Essa estrutura, além de descrever o computador, obterá dados baseando-se no arquivo de hosts ou no protocolo DNS. A seguir, descreveremos a função getservbyname().

**getservbyname()**

Os serviços oferecidos pelo servidor possuem individualmente um número de porta associado a cada um deles. Como exemplo, temos o SMTP na porta 25, o HTTP na porta 80 e o DNS na porta 53 etc. Também podemos criar serviços e direcioná-los a alguma porta de nossa escolha. O mapeamento entre portas e o serviço oferecido no sistema operacional Unix é listado no arquivo services localizado no diretório */etc/service*. A tabela 13.3 apresenta um exemplo do arquivo services:

*Tabela 13.3 – Relação entre protocolos e portas*

| Serviço | Porta/protocolo | Descrição |
|---|---|---|
| FTP | 21/tcp | |
| Telnet | 23/tcp | |
| SMTP | 25/tcp | Mail |

| Serviço | Porta/protocolo | Descrição |
|---|---|---|
| Domain | 53/udp | Servidor de nomes |
| SNMP | 161/udp | |

A função auxiliar getservbyname() recebe como parâmetros o nome do serviço (SMTP, HTTP etc.) e o protocolo utilizado (TCP ou UDP). Essa função retorna um ponteiro para uma estrutura contendo as informações apresentadas na tabela 13.4:

*Tabela 13.4 – Estrutura servent*

| Comando | Variável | Descrição |
|---|---|---|
| struct servent | | |
| { | | |
| char | *s_name; | /* Nome oficial do serviço */ |
| char | **s_aliases; | /* Lista de todos os apelidos que tratam do mesmo serviço */ |
| int | s_port; | /* Número da porta em que o serviço está configurado */ |
| char | *s_proto; | /* O nome do protocolo utilizado para comunicação com o serviço (TCP ou UDP) */ |
| } | | |

## getprotobyname()

Essa função auxiliar retorna o número do protocolo passado como parâmetro. Baseia-se no arquivo */etc/protocols* para retornar o número especificado. A seguir, apresentaremos um exemplo do arquivo *protocols* (Tabela 13.5).

*Tabela 13.5 – Relação entre os protocolos e o seu respectivo número*

| Protocolo | Número | Descrição |
|---|---|---|

| Protocolo | Número | Descrição |
|---|---|---|
| Ip | 0 | IP # Internet Protocol, pseudo protocol number |
| icmp | 1 | ICMP # Internet Control Message Protocol |
| Tcp | 6 | TCP # Transmission Control Protocol |
| Udp | 17 | UDP # User Datagram Protocol |

A função auxiliar getprotobyname() tem como objetivo receber como parâmetro o nome do protocolo (TCP) e retornar um ponteiro para uma estrutura com as informações apresentadas na tabela 13.6. Essa estrutura descreve o protocolo recebido como parâmetro.

*Tabela 13.6 – Estrutura protoent*

| Comando | Variável | Descrição |
|---|---|---|
| struct protoent | | |
| { | | |
| char | p_name; | /* Nome do protocolo */ |
| char | **p_aliases; | /* Apelidos dados ao protocolo */ |
| short | p_proto; | /* Número do protocolo */ |
| } | | |

A seguir, descreveremos outras funções utilizadas no desenvolvimento de programas cliente-servidor. Essas funções utilizam informações carregadas pelas estruturas das funções auxiliares já descritas.

## 13.3.2 Funções socket

As sintaxes das funções que serão apresentadas devem ser seguidas, a fim de garantir a comunicação entre um computador cliente e o servidor. Depois da apresentação das funções, mostraremos dois exemplos de programas escritos na linguagem C, os quais poderão ser utilizados como exemplos da aplicação prática de cada uma dessas funções.

## Função socket()

Essa função cria o socket, retornando um descritor chamado de *descritor socket*. A sintaxe da chamada dessa função é a seguinte:

```
int socket (int família, int tipo da especificação , int protocolo);
```

O primeiro parâmetro int família (por exemplo: AF_INET) informa que o socket será estabelecido em uma rede configurada sob o modelo de referência TCP/IP. O segundo parâmetro especifica que será usado o TCP como protocolo de transporte (SOCK_STREAM). Como outro exemplo para o segundo parâmetro, teríamos SOCK_DGRAM, caso estivéssemos utilizando o UDP como protocolo de transporte. O terceiro e último parâmetro é o número do protocolo TCP ou UDP, obtido da estrutura protoent definida na função auxiliar getprotobyname().

A função socket() retorna um número positivo que se refere ao descritor de socket ou -1, caso algum erro tenha sido detectado. A tabela 13.7 apresenta um resumo dos parâmetros da função socket():

*Tabela 13.7 – Função socket()*

| Parâmetro | Descrição |
|---|---|
| int família | Informa que o socket será estabelecido em uma rede configurada sob o modelo de referência TCP/IP. |
| int tipo da especificação | Especifica que será usado o TCP ou UDP como protocolo de transporte. |
| int protocolo | Número do protocolo TCP ou UDP. |

## Função bind()

Essa função atribui o número da porta e o endereço IP para um socket recém-criado pela função socket(). A criação de um socket não significa que ele já possua as informações necessárias para poder ser utilizado. A função bind() tem o objetivo de permitir o seu uso. A sintaxe da função é a seguinte:

```
int bind (int s , struct sockaddr * addr , int addrlen);
```

O primeiro parâmetro s é o socket descritor obtido como o retorno da função socket(). O segundo parâmetro é o endereço da estrutura

que contém o endereço IP, a família e o número da porta do computador emissor. O terceiro parâmetro refere-se ao tamanho em bytes da estrutura apontada no segundo parâmetro. A tabela 13.8 apresenta um resumo dos parâmetros da função bind().

Se completou com sucesso, essa função retorna zero; caso algum erro tenha sido detectado, retorna -1.

*Tabela 13.8 – Função bind()*

| Parâmetro | Descrição |
|---|---|
| int s | Descritor de socket obtido da função socket(). |
| struct sockaddr * addr | Estrutura que contém o endereço IP, o número da porta e a família do emissor. |
| int addrlen | Refere-se ao tamanho da estrutura do segundo parâmetro. |

## Função listen()

Quando preparamos uma aplicação para atuar como servidor, precisamos informar qual o tamanho da fila de entrada a que a aplicação pode atender. A quantidade informada refere-se ao valor de conexões permitidas simultaneamente. Caso uma requisição chegue ao servidor com a sua fila cheia, o servidor receberá uma mensagem de conexão negada. A sintaxe dessa função é a seguinte:

```
int listen (int s ,int tamanho da fila);
```

O primeiro parâmetro refere-se ao descritor do socket criado pela função socket(). O segundo parâmetro trata do número máximo de conexões pendentes que podem ser enfileiradas para o socket em um dado momento. A tabela 13.9 apresenta um resumo dos parâmetros da função listen().

Se completou com sucesso, essa função retorna zero, caso algum erro tenha sido detectado, retorna -1.

*Tabela 13.9 – Função listen()*

| Parâmetro | Descrição |
|---|---|
| int s | Descritor de socket obtido da função socket(). |

| Parâmetro | Descrição |
|---|---|
| int tamanho da fila | Refere-se à quantidade máxima de conexões pendentes permitidas para o socket em um dado momento. |

## Função accept()

A função accept() tem como objetivo aceitar e processar a conexão com o computador remoto. Logo depois de ser iniciada, a função accept() continua o processo de conexão e conecta-se ao computador remoto, chamando a função connect() comentada neste capítulo. A função accept() processa todas as conexões pendentes na fila em um socket passivo.

Para concluir as requisições recebidas, essa função cria um novo descritor de socket com as mesmas propriedades do socket s, criado inicialmente pela função socket(). Entretanto, esse novo socket contém ainda as informações do cliente remoto, como o endereço IP e a porta TCP ou UDP. Assim, para cada nova requisição, um novo socket deverá ser aberto. Esse novo descritor de socket será usado na recepção e transmissão dos pacotes entre o servidor e o cliente. Caso não existam conexões pendentes na fila, a função accept() bloqueia sua chamada até que uma nova conexão seja gerada. A sintaxe dessa função é a seguinte:

```
int accept (int s, sctruct sockaddr * addr , int * addrlen);
```

O primeiro parâmetro refere-se ao descritor socket criado pela função socket(), que, subsequentemente, foi ligado ao endereço IP do servidor pela função bind() e que ainda passou a “ouvir” novas conexões depois da execução da função listen(). O segundo parâmetro trata do endereço remoto de nosso cliente que se conectará ao nosso servidor. O terceiro parâmetro refere-se ao tamanho da estrutura ocupada pelo endereçamento do cliente.

Essa função retornará um valor positivo na variável s, referindo-se a um novo descritor de socket. Se completou com sucesso, essa função retorna zero; caso algum erro tenha sido detectado, retorna -1.

A tabela 13.10 apresenta um resumo dos parâmetros da função accept():

*Tabela 13.10 – Função accept()*

| Parâmetro | Descrição |
|---|---|
| int s | Descritor de socket obtido da função socket(). |
| struct sockaddr * addr | Trata do endereço remoto de nosso cliente que se conectará ao nosso servidor. |
| int addrlen | Refere-se ao tamanho da estrutura do segundo parâmetro. |

## Função connect()

A função connect() é responsável por executar a conexão em uma porta informada. Quando um programa vai se comunicar com outro, estejam eles na mesma máquina ou em máquinas diferentes, a função connect() é utilizada para iniciar o processo de comunicação. A sintaxe da função segue:

```
int connect (int s , struct sockaddr * addr , int * addrlen);
```

O primeiro parâmetro é o socket descritor, o segundo refere-se a um ponteiro para a estrutura criada com as informações do computador destino, enquanto o terceiro informa a quantidade de bytes da estrutura informada no segundo parâmetro.

Se completou com sucesso, essa função retorna zero; caso algum erro tenha sido detectado, retorna -1. A tabela 13.11 apresenta um resumo dos parâmetros da função connect():

*Tabela 13.11 – Função connect()*

| Parâmetro | Descrição |
|---|---|
| int s | Descritor de socket obtido da função socket(). |
| struct sockaddr * addr | Contém as informações do computador destino. |
| int addrlen | Refere-se ao tamanho da estrutura do segundo parâmetro. |

## Função recvfrom()

A função recvfrom() é utilizada para receber dados em sockets não

orientados à conexão. Essa função guarda no buffer, representado pela variável buff, os dados recebidos da máquina especificada pelo parâmetro addr (endereço e porta). A sintaxe da função é a seguinte:

```
int recvfrom(int s, const void *buff, int bufflen, unsigned int flags, const struct sockaddr *
  addr, int * addrlen);
```

O primeiro parâmetro (*s*) é o descritor do socket obtido pela função socket(); o segundo parâmetro (*buff*) é um ponteiro para o buffer em que os dados serão armazenados; o terceiro parâmetro (*bufflen*) refere-se ao tamanho do buffer que receberá os dados do socket; o quarto parâmetro (*flags*) pode ser informado como zero, uma vez que é utilizado apenas em opções avançadas; o quinto parâmetro é um ponteiro para uma estrutura (do tipo *sockaddr*) que irá conter o endereço da máquina que enviou os dados (endereço IP e número da porta); por fim, o sexto parâmetro refere-se ao tamanho da estrutura da máquina que enviou os dados. A tabela 13.12 apresenta um resumo dos parâmetros da função recvfrom().

Essa função retorna o número de bytes recebidos, os quais serão colocados na variável buff. Se completou com sucesso, essa função retorna zero; caso algum erro tenha sido detectado, retorna -1.

*Tabela 13.12 – Função recvfrom()*

| Parâmetro | Descrição |
|---|---|
| int sockfd | O descritor do socket obtido pela função socket(). |
| const void *buff | É um ponteiro para o buffer em que os dados serão armazenados. |
| int bufflen | Refere-se ao tamanho do buffer que receberá os dados do socket. |
| unsigned int flags | Utilizado apenas quando se usam opções avançadas. |
| const struct sockaddr * addr | É um ponteiro para uma estrutura do tipo sockaddr_in. |
| int *addrlen | Refere-se ao tamanho da estrutura que conterá o endereço. |

## Função recv()

A função recv() recebe dados de um socket orientado à conexão emitidos pela função sendto(). Os dados recebidos são atribuídos à variável buff e, posteriormente, poderão ser manipulados pelo programa. A sintaxe dessa função é a seguinte:

```
int recv (int s, char * buff, int bufflen, int flags);
```

O primeiro parâmetro (*s*) refere-se ao *socket* descritor obtido da função socket(); o segundo refere-se à variável que receberá os dados do socket; o terceiro refere-se ao tamanho da variável utilizada para receber os dados do socket; o quarto parâmetro (*flags*) pode ser informado como zero pelo fato de ser utilizado apenas em opções avançadas.

Essa função retorna o número de bytes recebidos. Esses bytes serão colocados na variável buff. Se completou com sucesso, essa função retorna zero; caso algum erro tenha sido detectado, retorna -1. A tabela 13.13 apresenta um resumo dos parâmetros da função recv():

*Tabela 13.13 – Função recv()*

| Parâmetro | Descrição |
|---|---|
| int s | Descritor de socket obtido da função socket(). |
| char * buff | Refere-se à variável que receberá os dados do socket. |
| int bufflen | Refere-se ao tamanho da variável utilizada para receber os dados do socket. |
| int flags | Setado com 0 em razão de ser utilizado apenas quando se usam opções avançadas. |

## Função sendto()

Essa função envia o conteúdo do buffer representado pela variável buff para a máquina especificada pelo parâmetro *addr* (endereço e porta). O socket pode ser ou não orientado à conexão. A sintaxe dessa função é a seguinte:

```
int sendto (int s, const void *buff, int bufflen, unsigned int flags, const struct sockaddr *
  addr, int * addrlen);
```

O primeiro parâmetro é o descritor do socket obtido por meio da

função socket(); o segundo é um ponteiro para o buffer que contém os dados a serem enviados para o socket; o terceiro refere-se ao tamanho do buffer utilizado na transmissão dos dados; o quarto recebe o valor zero; o quinto parâmetro (*addr*) é um ponteiro para uma estrutura que conterá o endereço para onde se deseja enviar os dados (endereço IP e número da porta); o sexto parâmetro refere-se ao tamanho da estrutura que conterá o endereço do computador de destino.

Essa função retorna o número de bytes enviados, os quais devem ser iguais a bufflen. Retornará -1, caso algum erro tenha sido detectado. A tabela 13.14 apresenta um resumo da função sendto():

*Tabela 13.14 – Função sendto()*

| Parâmetro | Descrição |
|---|---|
| int s | Descritor de socket obtido da função socket(). |
| const void *buff | Contém os dados a serem enviados para o socket. |
| int bufflen | Refere-se ao tamanho do buffer utilizado na transmissão dos dados. |
| unsigned int flags | Setado com valor 0. |
| const struct sockaddr * addr | Contém o endereço para onde se deseja enviar os dados (endereço IP e número da porta). |
| int * addrlen | Refere-se ao tamanho da estrutura que conterá o endereço do computador de destino. |

## Função send()

A função send() é utilizada para a transmissão de dados em sockets orientados à conexão. A sintaxe dessa função é a seguinte:

```
int send (int s , char *buff, int bufflen, int flags);
```

O primeiro parâmetro é o socket descritor obtido pela função socket(); o segundo é um ponteiro para uma variável que contém os dados a serem enviados para o socket. O terceiro parâmetro (*bufflen*) refere-se ao tamanho do buffer utilizado na transmissão dos dados. O quarto parâmetro (*flags*) recebe o valor 0.

Essa função retorna o número de bytes enviados, os quais devem ser iguais a bufflen. Retornará -1, caso algum erro tenha sido

detectado. A tabela 13.15 apresenta um resumo dos parâmetros da função send():

*Tabela 13.15 – Função send()*

| Parâmetro | Descrição |
|---|---|
| int s | Descritor de socket obtido da função socket(). |
| char *buff | Contém os dados a serem enviados para o socket. |
| int bufflen | Tamanho do buffer utilizado na transmissão dos dados. |
| int flags | Setado com o valor 0. |

### Função close()

Essa função fecha um socket. A sintaxe dessa função é a seguinte:

```
int close (s)
```

Em que o parâmetro s é o descritor do socket obtido pela chamada da função socket().

Se completou com sucesso, essa função retorna zero; caso algum erro tenha sido detectado, retorna -1.

A seguir apresentaremos dois programas que descrevem o formato de um programa cliente e um programa servidor. Ambos estão escritos na linguagem C, utilizando grande parte das funções analisadas neste capítulo.

## 13.4 Arquivo de header

```
/* arqheader.h */
#ifndef ARQHEADER
#define ARQHEADER
#include <sys/socket.h>
#include <netinet/in.h>
#include <netdb.h>
#include <stdio.h>
#include <string.h>
#define PORTAPADRAO  2222  /* Porta-padrão */
#define TAMFILAREQ  5  /* Tamanho da fila de requisições */
int acessos = 0;  /* Quantidade de conexões de clientes */
```

```
char *localhost = "localhost";  /* Este nome refere-se a 127.0.0.1 */
char bufferEnvio[500];
char msg [200];  /* aloca espaço para a mensagem do usuário */
int sock = 0, sock2 = 0;  /* Descritores de socket */
  struct protoent *ptrPort;  /* Ponteiro para o arquivo que contém as portas
                                relacionadas com os protocolos */
  struct  sockaddr_in strAddr; /* Estrutura para suportar o endereço IP */
  struct  hostent *ptrHost; /* Ponteiro para a tabela host*/
  int     numPorta = 0;
  int     qdadeCarac = 0;
  char    *host;
  /* Estrutura responsável por suportar os dados do cliente */
  struct    sockaddr_in cad;
  int       tamEndereco = 0;
  /* Buffer utilizado pelo servidor para enviar mensagens aos clientes */
#endif
```

# 13.5 Programa cliente

```
/*-------------------------------------------------------------------------
Programa: cliente.c
Finalidade: Cria um socket, conecta o socket criado com o servidor e imprime as
  mensagens emitidas no cliente na tela do servidor e ainda aguarda resposta
Como executar: client [ host [port] ], em que o parâmetro host significa o endereço IP
  onde o servidor esta executando e port significa em qual porta TCP o servidor esta
  escutando
/* Compilar: gcc.exe -g cliente.c -DUNIX -o cliente */
#include "arqheader.h"
int main (int argc,char **argv) {
memset (bufferEnvio,'\0',sizeof (bufferEnvio));
  memset((char *)&strAddr,0,sizeof(strAddr)); /*Atribui zero à estrutura strAddr*/
  strAddr.sin_family = AF_INET; /* Seta a família ao atributo da estrutura */
  /* Verifica os parâmetros recebidos */
  /* Caso o número da porta seja informado, teremos mais de três parâmetros */
  if (argc > 2) {
    numPorta = atoi(argv[2]);
  }
  else {
    numPorta = PORTAPADRAO;
  }
  if (numPorta > 0) {
  strAddr.sin_port = htons((u_short)numPorta);
```

```
  }
  else {
    printf("Porta inválida %s\n",argv[2]);
    return (99);
  }
  /*Analisa os parâmetros caso seja informado apenas o nome do host.*/
  if (argc > 1) {
    host = argv[1];
  } else {
    host = localhost;
  }
  /* Converte o nome do servidor para o seu respectivo endereço IP. Após a conversão,
  copia para strAddr.*/
  ptrHost = gethostbyname(host);
  if ( ((char *)ptrHost) == NULL ) {
    printf("Host inválido: %s\n", host);
    return (99);
  }
  memcpy(&strAddr.sin_addr, ptrHost->h_addr, ptrHost->h_length);
  /* Obtém o número do protocolo a partir do seu nome. */
  if ( ((int)(ptrPort = getprotobyname("tcp"))) == 0) {
    printf("Não foi possível mapear o tcp para o seu correto número ");
    return (99);
  }
  /* Cria o socket. */
  sock = socket(PF_INET, SOCK_STREAM, ptrPort->p_proto);
  if (sock < 0) {
    printf("Falha na criação do socket\n");
    return (99);
  }
  /* Conecta o socket ao servidor especificado. */
  if (connect(sock, (struct sockaddr *)&strAddr, sizeof(strAddr)) < 0) {
    printf("Falha na conexão do socket\n");
    return (99);
  }
system ("CMD /c cls"); /* limpa a tela */
printf ("\n\n Entre com sua mensagem a ser transmitida ao servidor: \n");
  memset (msg,'\0',sizeof (msg));
gets (msg);
/* envia a mensagem informada ao servidor */
    send(sock,msg,strlen(msg),0);
    /* Recebe os dados do socket e o atribui a variável buf. */
```

```
    qdadeCarac = recv(sock, bufferEnvio, sizeof(bufferEnvio), 0);
    while (qdadeCarac > 0) {
      printf ("Retorno do servidor: %s",bufferEnvio);
      qdadeCarac = recv(sock, bufferEnvio, sizeof(bufferEnvio), 0);
    }
  /* Fecha o socket. */
  close(sock);
  return(0);
}
```

O programa a seguir deverá ser executado como servidor.

# 13.6 Programa servidor

```
/* servidor.c – Exemplo de um servidor TCP */
/*--------------------------------------------------------------------
* Programa: servidor.c
* Finalidade: Aloca um socket e fica aguardando requisições na porta padrão ou na porta
  recebida como parâmetro.
* Como Executar: servidor [ porta ], em que porta significa o número da porta na qual o
  servidor está ouvindo.
Compilar: gcc.exe -g servidor.c -DUNIX -o servidor
*/
#include "arqheader.h"
int main(int argc , char *argv[]) {
    memset (bufferEnvio,'\0',sizeof (bufferEnvio));
  memset((char *)&strAddr,0,sizeof(strAddr));  /* Limpa a estrutura */
  strAddr.sin_family = AF_INET;              /* Seta a família TCP*/
  strAddr.sin_addr.s_addr = INADDR_ANY;  /* Seta o endereço IP local */
  if (argc > 1) {                    /* Verifica o parâmetro de entrada */
    numPorta = atoi(argv[1]);
  } else { numPorta = PORTAPADRAO;  /* usa porta-padrão */ }
  if (numPorta > 0) {
    strAddr.sin_port = htons((u_short)numPorta);
  }
  else {
    printf("Porta errada %s\n",argv[1]);
    return (99);
  }
  /* Obtém o número do protocolo a partir do seu nome. */
  if ( ((int)(ptrPort = getprotobyname("tcp"))) == 0) {
    printf("Não foi possível mapear o protocolo TCP para o seu correto número ");
    return (99);
```

```
}
/* Cria o socket */
sock = socket(PF_INET, SOCK_STREAM, ptrPort->p_proto);
if (sock < 0) {
  printf( "Problemas na criação do socket \n");
  return (99);
}
/* Liga o endereço local com o socket */
if (bind(sock, (struct sockaddr *)&strAddr, sizeof(strAddr)) < 0) {
  printf("problemas na função bind\n");
  return (99);
}
/* Especifica o tamanho da fila de requisição */
if (listen(sock, TAMFILAREQ) < 0) {
  printf("Problemas na função listen\n");
  return (99);
}
/* Loop principal */
system ("cls"); /* limpa a tela no Sistema operacional Windows */
printf ("Servidor TCP aguardando contato na porta: %d \n", numPorta);
while (1) {
tamEndereco= sizeof(cad);
if ( (sock2=accept(sock, (struct sockaddr *)&cad, &tamEndereco)) < 0) {
  printf("Problemas na função accept\n");
  return (99);
}
system ("cls");
printf ("Servidor TCP aguardando contato na porta: %d \n", numPorta);
int n = recv(sock2, bufferEnvio, sizeof(bufferEnvio), 0);
while (n > 0) {
  write(1,bufferEnvio,n);
  n = recv(sock, bufferEnvio, sizeof(bufferEnvio), 0);
}
printf ("\n Digite uma mensagem para retornar ao cliente: ");
  memset (msg,'\0',sizeof (msg));
gets (msg);
printf ("\n");
acessos++;
sprintf(bufferEnvio,"\n Quantidade de acessos: %d \n",acessos);
strcat (bufferEnvio,msg);
send(sock2,bufferEnvio,strlen(bufferEnvio),0);
  close(sock2);
```

```
    } /* fim while (1) */
    return 0;
}
```

CAPÍTULO 14

# Protocolos da camada de aplicação

Neste capítulo, descreveremos os protocolos que atuam no nível de aplicação do modelo de referência TCP/IP. Dessa forma, serão descritos os protocolos mais utilizados, como: FTP (*File Transfer Protocol*), TFTP (*Trivial File Transfer Protocol*), SSH (*Secure Shell*), Telnet, SMTP (*Simple Mail Transfer Protocol*), HTTP (*Hypertext Transfer Protocol*), DHCP (*Dynamic Host Control Protocol*) e SNMP (*Simple Network Management Protocol*).

## 14.1 Introdução

Em geral, protocolos da camada de aplicação possuem dois componentes conhecidos por cliente e servidor. O cliente é quem inicia o contato com o servidor, enquanto o servidor responde às requisições emitidas pelo cliente. A seguir, serão abordados alguns dos protocolos mais utilizados no dia a dia dos usuários e administradores de rede.

## 14.2 Protocolo FTP

O protocolo FTP (*File Transfer Protocol*) tem o objetivo de transferir programas e arquivos de todos os tipos por meio de redes TCP/IP. Suas principais características são a confiabilidade e a eficiência com que realizam as transferências. Embora seja possível usar outros protocolos para transferir arquivos, como o HTTP e o SMTP, o FTP é o mais adequado para essa tarefa, pois utiliza o protocolo TCP na camada de transporte e escuta as requisições nas portas 20 (dados) e 21 (controle).

A seguir, apresentaremos um exemplo do estabelecimento de uma sessão de FTP, em que objetivamos realizar o login no servidor uccdk001, estando inicialmente logado no servidor dess14. A tabela 14.1 apresenta as mensagens emitidas pelo servidor no processo de login e o resultado de cada linha será detalhado em seguida.

*Tabela 14.1 – Comando de conexão do protocolo FTP*

| Comando | Resultado |
|---|---|
| $ ftp uccdk001 | |
| 1 | Connected to uccdk001.ccp.br.hsbc. |
| 2 | 220 uccdk001 FTP server (Version 4.1 Thu Sep 12 23:46:23 CDT 2002) ready. |
| 3 | Name (uccdk001:douglas): douglas. |
| 4 | 331 Password required for douglas. |
| 5 | Password: |
| 6 | 230-Last unsuccessful login: Mon Jun 14 09:49:05 2004 on ftp from dess14.insurance.br.hsbc. |
| 7 | 230-Last login: Mon Jun 14 10:03:57 2004 on ftp from dess14.insurance.br.hsbc. |
| 8 | 230 User douglas logged in. |
| 9 | Remote system type is UNIX. |
| 10 | Using binary mode to transfer files. |
| 11 | ftp> |

Conectado ao servidor *dess14*, o primeiro comando emitido refere-se a *ftp uccdk001*, ou seja, queremos nos conectar ao servidor *uccdk001* para realizarmos a cópia de arquivos desse servidor para *dess14*. O comando emitido gera três linhas.

A primeira informa que a conexão com o servidor *uccdk001* foi iniciada; a segunda linha, identificada pelo código 220, informa que o servidor *uccdk001* está pronto para receber o login do usuário; a terceira disponibiliza a entrada do login do usuário (douglas). Depois da entrada do nome do usuário, será solicitada a entrada da senha do usuário informado. Essa nova linha, identificada pelo código 331, informa que o nome do usuário foi aceito e que a senha deverá ser informada para o processo de login ser completado. A sexta linha, identificada pelo código 230, informa a data do último acesso – m sem sucesso – do usuário douglas no servidor *dess14*. A sétima linha, também identificada pelo código 230, informa a data do último login desse usuário no servidor *dess14*; a oitava linha, identificada

pelo código 230, informa que o usuário foi logado no servidor *uccdk001* e está liberado para realizar movimentações de arquivos; a nona linha informa que o sistema remoto que estamos utilizando com o protocolo FTP é o Unix; a décima linha, por sua vez, informa que a transferência de arquivos, habilitada por padrão, foi a binária. A partir desse momento, o protocolo FTP está pronto para receber os comandos. Antes de continuarmos com a operação do FTP, apresentaremos, na tabela 14.2, os comandos FTP mais utilizados para a transferência de arquivos.

*Tabela 14.2 – Comandos mais utilizados do protocolo FTP*

| **Comando** | **Descrição** |
|---|---|
| ascii | Altera o modo de transferência para ASCII (texto). |
| binary | Altera o modo de transferência para binário (comum para arquivos do tipo .EXE e .ZIP, entre outros). |
| cd | Muda o diretório na estrutura do servidor remoto. |
| lcd | Muda o diretório na estrutura do servidor local. |
| delete | Apaga um arquivo no diretório corrente do servidor remoto. |
| dir | Lista os arquivos do diretório corrente do servidor remoto. |
| ls | Lista os arquivos do diretório corrente do servidor remoto. |
| get | Realiza o download de um arquivo do diretório corrente do servidor remoto. |
| mkdir | Cria um novo diretório no diretório corrente do servidor remoto. |
| put | Realiza o upload de um arquivo do diretório corrente local (computador do usuário). |
| help | Apresenta todos os comandos possíveis de serem utilizados com o protocolo FTP. |
| quit | Finaliza a conexão FTP. |

Na tabela 14.3, apresentaremos o processo utilizado para a movimentação do arquivo *redes.txt* do servidor uccdk001 para o servidor dess14. Nessa tabela, estão descritos o comando utilizado e a resposta do servidor.

*Tabela 14.3 – Comando de download de arquivo*

| Comando | Resultado |
|---|---|
| ftp> get redes.txt | |
| | 200 PORT command successful. |
| | 150 Opening data connection for redes.txt (560 bytes). |
| | 226 Transfer complete. |
| | 560 bytes received in 0.04 seconds (12.91 Kbytes/s) |
| | ftp> |

Na tabela 14.4, apresentaremos o processo utilizado para a movimentação do arquivo *redes.txt* do servidor dess14 para o servidor uccdk001, depois de ele ter sido alterado. Nessa tabela, estão descritos o comando utilizado e a resposta do servidor.

O processo de movimentação de arquivos utilizando o protocolo FTP é simples e muito útil. A tabela 14.5 mostra os códigos apresentados de acordo com os comandos emitidos e também com a execução dos comandos.

*Tabela 14.4 – Comando de upload de arquivo*

| Comando | Resultado |
|---|---|
| ftp> put redes.txt | |
| | 200 PORT command successful. |
| | 150 Opening data connection for redes.txt. |
| | 226 Transfer complete. |
| | 680 bytes sent in 0.00 seconds (2790.18 Kbytes/s) |
| | ftp> |

*Tabela 14.5 – Códigos emitidos pelo protocolo FTP*

| Comando | Resultado |
|---|---|
| 220 | O servidor está pronto para receber o login de um novo usuário. |
| 331 | O nome de usuário foi aceito e precisa da senha. |

| Comando | Resultado |
|---|---|
| 230 | O usuário foi logado no sistema e pode utilizar os recursos do FTP. |
| 250 | A ação requerida foi completada com sucesso. |
| 200 | O comando foi completado com sucesso. |
| 150 | Início de conexão de transferência de dados. |
| 226 | Fechamento de conexão de transferência de dados ou transferência completada com sucesso. |
| 221 | Fim da conexão FTP. |

## 14.3 Protocolo TFTP

O protocolo TFTP é uma opção para os usuários que não necessitam da robustez do protocolo FTP, de modo que enquanto este utiliza toda a estrutura do TCP como protocolo de transporte, o TFTP utiliza o UDP para transferir seus dados. O protocolo TFTP é utilizado principalmente para transferir arquivos de configuração, ou mesmo do sistema operacional, entre um computador e um equipamento ativo, como roteador, switch, hub ou, ainda, servidor de impressão. O TFTP utiliza o protocolo UDP na camada de transporte e escuta as requisições na porta 69.

## 14.4 Protocolo Telnet

O modelo de referência TCP/IP inclui um protocolo simples de terminal remoto: Telnet. O Telnet é considerado um programa e também um protocolo, e o programa utiliza o protocolo para oferecer uma interface para logins remotos. Uma sessão de Telnet fornece um terminal baseado em caracteres virtuais, em que o usuário pode digitar comandos e outros textos, além de poder verificar a saída de processos na sua máquina remota.

O protocolo Telnet transmite os toques do teclado do usuário diretamente ao servidor, como se estivessem sendo digitados no teclado conectado ao próprio servidor, e retorna o resultado do comando ao cliente que o solicitou. O ambiente oferecido pelo programa e protocolo Telnet é muito utilizado por empresas que

desenvolvem sistemas em ambiente Unix. Nesse ambiente, os servidores possuem o compilador e o banco de dados necessários ao acesso dos desenvolvedores. O Telnet utiliza o protocolo TCP na camada de transporte e escuta as requisições na porta 23.

É importante observar a possibilidade de uso do protocolo SSH (*Secure Shell*) como uma alternativa ao protocolo Telnet. O protocolo SSH oferece a mesma aplicação do protocolo Telnet, com a vantagem de a conexão entre o cliente e o servidor ser criptografada. Esse protocolo utiliza o protocolo TCP na camada de transporte e escuta as requisições na porta 22. Atualmente, muitos equipamentos ativos e servidores são configurados para apenas aceitarem conexões por meio desse protocolo devido à segurança que oferece.

## 14.5 Protocolo SMTP

O SMTP (*Simple Mail Transfer Protocol*), protocolo usado no sistema de correio eletrônico da Internet, utiliza o protocolo TCP na camada de transporte, escutando as requisições na porta 25. Para enviar uma mensagem, um usuário deve utilizar programas que façam a interface entre o protocolo e o usuário. Como exemplo de programas, temos o Sendmail, Lotus Notes ou Outlook. Após o usuário concluir a geração de uma mensagem, esse protocolo solicita ao programa escolhido que realize a entrega da mensagem ao servidor do destinatário. Para executar essa tarefa, o programa escolhido utilizará o protocolo SMTP.

Quando recebe a mensagem do usuário, o sistema de correio eletrônico armazena uma cópia da mensagem com o horário do armazenamento e a identificação do remetente e do destinatário. A transferência da mensagem é realizada por um processo que executa em background, permitindo que o usuário remetente, após entregar a mensagem ao sistema de correio eletrônico, possa executar outras aplicações.

O processo de transferência de mensagens, executado em background, mapeia o nome da máquina de destino, baseando-se no seu endereço IP, e tenta estabelecer uma conexão TCP com o

servidor de correio eletrônico da máquina de destino. Note que o processo de transferência atua como cliente do servidor de correio eletrônico. Se a conexão for estabelecida, o cliente envia uma cópia da mensagem para o servidor, que a armazena em seu SPOOL (*Simultaneous Peripheral Operation Online*). Caso a mensagem seja transferida com sucesso, o servidor emite um aviso ao cliente, informando que recebeu e armazenou uma cópia da mensagem. O SPOOL refere-se a um processo de transferência de dados, colocando-os em uma área de trabalho temporária, o que possibilita que outro programa possa acessar essa cópia e processá-la a qualquer momento.

Quando o cliente recebe a confirmação de recebimento e armazenamento da mensagem, o cliente retira a cópia que mantinha em seu SPOOL local, a fim de liberar espaço. Se a mensagem, por algum motivo, não for transmitida com sucesso, o cliente anotará o horário da tentativa e suspenderá sua execução. Periodicamente, o cliente deve verificar se existem mensagens a serem enviadas na área de SPOOL e deve tentar retransmiti-las. Se uma mensagem não for enviada por um período (p. ex., dois dias), o serviço de correio eletrônico devolverá a mensagem ao remetente, informando que não conseguiu transmiti-la.

Em geral, quando um usuário está conectado, o sistema de correio eletrônico é ativado para verificar se existem mensagens na caixa postal do usuário. Se existirem, esse sistema emite um aviso para o usuário que, quando achar conveniente, ativará o módulo de interface com o usuário para receber as correspondências.

Uma mensagem SMTP divide-se em duas partes, sendo o cabeçalho e o corpo separados por uma linha em branco. O cabeçalho, em que são especificadas as informações necessárias para a transferência da mensagem, é composto de linhas que contêm palavras-chave seguidas de um valor. A tabela 14.6 apresentará as palavras-chave do cabeçalho, cujos exemplos de uso são:

- A identificação do emissor é representada pela palavra-chave MAIL FROM. Essa palavra-chave deve ser seguida de seu

endereço.

- Identificação do destinatário representada pela palavra-chave RCPT TO. Essa palavra-chave deve ser seguida pelo endereço do destinatário.
- Assunto da mensagem representada pela palavra-chave DATA. Essa palavra-chave deve ser seguida pela mensagem a ser enviada ao destinatário. No corpo da mensagem, são transportadas as informações da mensagem propriamente dita, sendo livre o formato do texto.

O SMTP especifica como o sistema de correio eletrônico transfere mensagens de uma máquina para outra, porém não define o módulo interface com o usuário nem a forma como as mensagens são armazenadas.

### 14.5.1 Formato de um endereço SMTP

Os usuários do sistema de correio eletrônico são localizados por meio de um par de identificadores. Um deles especifica o nome da máquina de destino e o outro identifica a caixa postal do usuário. Um remetente pode enviar simultaneamente várias cópias de uma mensagem para diferentes destinatários, utilizando o conceito de lista de distribuição (um nome que identifica um grupo de usuários). O formato dos endereços SMTP é o seguinte: *nome_usuario@computador_dominio*, em que computador_dominio identifica o domínio ao qual a máquina de destino pertence. Esse endereço deve identificar um grupo de máquinas gerenciado por um servidor de correio eletrônico que segue a especificação do SMTP. O nome_usuario identifica a caixa postal do destinatário, que deve ser única para cada usuário.

### 14.5.2 Como enviar uma mensagem SMTP via Telnet

A seguir, descreveremos os passos para a emissão de um email por meio de uma conexão Telnet feita com o servidor de email na porta TCP 25. Esse email será enviado utilizando os comandos no nível de texto, disponíveis pelo protocolo SMTP.

**1.** Inicialmente, o usuário identifica-se para o servidor, informando

seu endereço eletrônico por meio do comando MAIL FROM: douglas@meuservidor.com.br.

**2.** O servidor pode ou não aceitar a origem da mensagem. Se aceitar, enviará ao cliente o código 250 OK.

**3.** O cliente identifica os destinatários, informando os endereços eletrônicos por meio do comando RCPT TO:rubens@destino.com.br, RCPT TO:hey@destino.com.br, e assim por diante.

**4.** Se o servidor for capaz de entregar a mensagem para o destinatário, ele enviará ao cliente o código 250 OK. Do contrário, o cliente receberá a mensagem iniciada pelo código 550, o qual indica que a caixa de mensagens desse usuário escolhido encontra-se indisponível ou inexistente. A mensagem que indica erro será recebida pelo cliente alguns minutos depois do seu envio.

**5.** O cliente envia o comando DATA ao servidor para indicar que está pronto para transmitir.

**6.** O servidor indica que o cliente pode iniciar a transmissão, enviando o código 354 para o cliente, seguido da mensagem *Start mail input*: *end with* <CRLF>.<CRLF>(<enter>.<enter>). O servidor também solicita que a mensagem seja encerrada com a sequência de caracteres <CRLF>.<CRLF>.

**7.** O cliente transmite a mensagem inteira, de uma só vez, acrescentando, no final, a sequência de caracteres <CRLF>. <CRLF>.

**8.** O servidor conclui informando o sucesso da transmissão, retornando ao cliente o código 250 OK.

**9.** O próximo passo é informar ao destinatário que a conexão pode ser encerrada por meio do comando QUIT. Depois da execução desse comando, o cliente receberá a mensagem iniciada pelo código 221.

A tabela 14.6 apresentará os comandos utilizados no protocolo SMTP para o envio de mensagens:

*Tabela 14.6 – Comandos SMTP*

| Comando | Descrição |
|---|---|
| HELO | É o comando com o qual o programa cliente se identifica. |
| MAIL FROM | É o comando para identificar o usuário emissor. |
| RCPT TO | É o comando para identificar o destinatário. É importante notar que esse comando será repetido várias vezes antes de a mensagem ser enviada. Isso permite que seja enviada uma mesma mensagem a um grupo de pessoas. |
| DATA | Esse comando indica que todos os destinatários foram especificados e o emissor está pronto para transferir a mensagem. |
| QUIT | É o comando usado para informar ao destinatário que o remetente terminou e que a conexão pode ser desfeita. |

As respostas recebidas pelos clientes possuem códigos que informam se o comando emitido está ou não de acordo com aquilo que o servidor esperava receber. O primeiro dígito do código informa a categoria geral da mensagem. A tabela 14.7 apresenta uma explicação para os códigos emitidos pelo protocolo SMTP:

*Tabela 14.7 – Descrição dos códigos gerados pelo SMTP*

| Código | Descrição |
|---|---|
| 2xx | É um OK e significa que o comando emitido foi processado com sucesso. |
| 4xx | Refere-se a uma mensagem de erro do tipo servidor temporariamente indisponível. |
| 5xx | Refere-se a uma mensagem de erro do tipo erro de sintaxe. |

Além do SMTP, existem outros protocolos envolvidos no processo de correio eletrônico, os quais passaremos a abordar.

## 14.6 Protocolo POP

O protocolo POP (*Post Office Protocol*) é quem define os mecanismos para o cliente manipular as mensagens depositadas na sua caixa postal do servidor SMTP. Esse protocolo é sempre apresentado seguido da sua versão, que atualmente está na versão 4 (POP4).

O POP utiliza o protocolo TCP na camada de transporte e escuta as requisições na porta 110. Além disso, define os serviços complementares ao SMTP, mas não o substitui. O POP é destinado exclusivamente a estabelecer mecanismos de comunicação entre o cliente e o servidor, não podendo ser utilizado para retransmitir mensagens entre servidores. Ao estabelecer uma conexão com o servidor, cada usuário é capaz de manipular apenas as mensagens de sua própria caixa postal, pois o servidor POP exige que o usuário se autentique por meio de uma senha secreta, sempre que uma conexão for estabelecida.

O protocolo POP define, basicamente, um conjunto de comandos para o usuário ler e apagar mensagens de sua caixa postal, de forma remota. É importante observar que as mensagens lidas do servidor permanecerão armazenadas no sistema de arquivos da máquina do cliente, e não estarão mais disponíveis em computadores de outras localidades.

## 14.7 Protocolo IMAP

O IMAP (*Interactive Mail Access Protocol*) permite ao usuário manipular sua caixa postal remotamente de maneira mais sofisticada do que o POP. O IMAP utiliza o protocolo TCP na camada de transporte e escuta as requisições na porta 143. Esse protocolo é sempre apresentado seguido da sua versão, que atualmente está na versão 4 (IMAP4).

O IMAP foi projetado especialmente para permitir aos usuários acessarem suas mensagens de correio eletrônico a partir de múltiplos computadores, seja em casa, no trabalho ou por meio de computadores portáteis. Para isso, permite ler as mensagens sem copiá-las para o computador do cliente. As mensagens permanecem armazenadas no servidor, podendo ser acessadas pelo cliente de um outro computador em uma conexão futura.

## 14.8 MIME

O MIME (*Multipurpose Internet Mail Extension*) é um padrão de formatação e codificação de mensagens que permite transmitir

informações com conteúdo gráfico e multimídia, codificados como texto. O protocolo SMTP suporta apenas a transmissão de texto puro (ASCII). O padrão MIME, por sua vez, foi desenvolvido para permitir que informações não ASCII, como imagens ou texto formatado, trafeguem por meio das mensagens de correio eletrônico, sendo um complemento ao SMTP e não um substituto. Ademais, especifica como dados arbitrários devem ser codificados em ASCII para serem transmitidos na forma de mensagens de texto.

Basicamente, o padrão MIME define mecanismos para que o receptor possa identificar o tipo de dado que está sendo transmitido (texto, imagem, áudio, vídeo, programas binários etc.) e o padrão de codificação utilizado.

## 14.9 Protocolo HTTP

Até o final dos anos de 1980, as informações compartilhadas na Internet consistiam, primariamente, de trocas de mensagens de correio eletrônico e arquivos de dados de computadores. Nessa época, começaram a surgir os arquivos multimídia que, além de textos, continham figuras, sons e ligações (*hyperlinks*) que permitiam ao usuário saltar dentro de arquivos de um modo não linear ou até mesmo para outros arquivos contendo informações relacionadas. Assim, surgiu a necessidade de criar novos protocolos para atender a esses novos requerimentos.

O padrão de arquivo HTML (*HyperText Markup Language*) e o protocolo HTTP (*HyperText Transfer Protocol*) resultaram de um projeto do CERN (*European Particle Physics Laboratory*) no final da década de 1980.

O protocolo HTTP está presente no nível de aplicação do modelo de referência TCP/IP e utiliza o TCP como protocolo no nível de transporte, escutando as requisições na porta 80. Além disso, é utilizado na World Wide Web para a distribuição e recuperação de informações, em sua maioria documentos hipertexto. A troca de informações entre um navegador e um servidor web é toda feita por meio desse protocolo, o qual define um conjunto de regras simples para a efetiva comunicação entre os dois. De forma simples, esse

protocolo define a forma de conversação e resposta entre os clientes e o servidor web.

### 14.9.1 Funcionamento do HTTP

O programa cliente, geralmente um navegador, estabelece uma conexão com um programa servidor (servidor web) e a ele faz uma requisição. As regras do HTTP definem a sintaxe exata desse pedido, ao qual o servidor retorna uma resposta. Se estiver tudo certo, essa resposta deverá conter a informação desejada pelo cliente em um formato baseado nas regras do protocolo. Um pedido HTTP é composto das seguintes partes:

- Comando – Representa a ação a ser realizada.
- URI (*Universal Resource Identifier*) – Representa a informação requisitada.
- Versão do protocolo HTTP.

A tabela 14.8 apresenta os comandos utilizados pelo protocolo HTTP na interação entre o cliente e o servidor web. É importante destacar que toda essa comunicação é feita de forma transparente para o usuário.

*Tabela 14.8 – Comandos do protocolo HTTP*

| Método | Descrição |
|---|---|
| GET | Recupera todas as informações identificadas no recurso da rede, ou seja, solicitadas na URI passada. Se o recurso for um processo executável, ele retornará a resposta do processo, e não o seu texto. Existe o GET condicional que traz o recurso apenas se este foi alterado depois da data da última transferência. O comando GET http://129.20.27.20:80/kit-corretor/index.html é um exemplo da utilização do método GET. |
| HEAD | Retorna somente informações sobre o recurso procurado, como o tamanho e a data de criação. |
| POST | Envia informações para o servidor web. |
| PUT | Envia uma cópia de um recurso ou informação para ser armazenada no servidor web. |

| Método | Descrição |
|---|---|
| DELETE | Remove um recurso armazenado no servidor web. |

O tipo de URI utilizado pelo protocolo HTTP é chamado de URL (*Uniform Resoure Locator*) e contém três partes: a identificação do protocolo, o endereço do computador servidor e o documento requisitado (podendo incluir subdiretórios). Um bom exemplo de URL seria o documento *index.html* armazenado no diretório */kit-corretor/* em um servidor com o endereço IP 129.20.27.20 e porta 80. A URL para esse exemplo seria *http://129.20.27.20:80/kit-corretor/index.html*. Se for colocado em um navegador, esse endereço fará um pedido HTTP ao servidor web.

Ao receber o pedido, o servidor web faz o processamento de modo a determinar o que deverá ser feito. Em relação ao exemplo, o servidor web deverá procurar o arquivo *index.html* no diretório */kit-corretor* e retorná-lo ao navegador.

## 14.9.2 Resposta HTTP

Toda requisição feita ao servidor web é respondida ao navegador que apresenta o resultado ao usuário. Uma resposta HTTP é formada por três elementos: uma linha de status, indicando sucesso ou falha no pedido, uma descrição da informação contida na resposta e a própria informação que foi requisitada.

A linha de status da resposta consiste na versão do protocolo, seguida de um código de status e sua frase de texto associada. O código de status retornado é um inteiro de três dígitos, resultado da tentativa para entender e satisfazer o pedido. O primeiro dígito define a classe da resposta e os dois últimos dígitos não têm nenhuma categorização. Existem cinco valores para o primeiro dígito, os quais apresentaremos na tabela 14.9:

*Tabela 14.9 – Classes de resposta do protocolo HTTP*

| Código do erro | Descrição |
|---|---|

| Código do erro | Descrição |
|---|---|
| 1xx | Essa classe é apenas informativa. |
| 2xx | Essa classe indica sucesso, ou seja, a ação foi recebida, entendida e aceita. |
| 3xx | Classe de redirecionamento. Algumas ações adicionais devem ser executadas para completar o pedido. |
| 4xx | Classe de erros ocorridos no cliente. Nesse caso, o comando contém algum erro de sintaxe ou não pode ser completado. |
| 5xx | Classe de erros ocorridos no servidor. Nesse caso, o servidor falhou em completar um pedido aparentemente válido. |

A tabela 14.10 apresenta os códigos de erros mais comuns recebidos por um navegador na linha de status.

*Tabela 14.10 – Código e mensagem informativa ao cliente HTTP*

| Código | Descrição |
|---|---|
| 200 | OK. |
| 201 | OK, recurso criado (POST). |
| 202 | O pedido foi aceito para processamento, mas este não foi concluído. |
| 204 | OK, mas não há nada para retornar. |
| 300 | O recurso requisitado está disponível em mais de um local e o local preferido não pode ser determinado via negociação. |
| 301 | O recurso pedido tem uma nova URL. |
| 302 | O recurso pedido está em uma URL diferente temporariamente. |
| 304 | O documento pedido não foi modificado. |
| 400 | Erro de sintaxe no comando. |
| 401 | Não autorizado; para obter acesso, é necessário autenticação. |
| 403 | Acesso proibido. |
| 404 | Arquivo ou URL não encontrado. |
| 500 | Erro interno do servidor. |
| 501 | Recurso solicitado não implementado no servidor. |
| 502 | Servidor sobrecarregado. |
| 503 | Serviço temporariamente indisponível. |

## 14.10 Protocolo DHCP

O protocolo DHCP (*Dynamic Host Configuration Protocol*) é responsável pela configuração dinâmica de endereços IP em uma rede de computadores, ou seja, o protocolo DHCP atribui automaticamente um endereço IP quando um computador é inicializado ou conectado a uma rede de computadores.

A atribuição de endereços IP em uma rede TCP/IP de grande porte, além de ser uma tarefa bastante complexa, pode demandar muito tempo do administrador da rede. O administrador deve certificar-se de que cada computador receberá um endereço IP único, entre todas as máquinas existentes na rede. A configuração manual de endereços IP, além de ser trabalhosa, pode levar à duplicação indesejável de endereços, fato que compromete o funcionamento dos computadores em conflito.

Em redes de grande porte, determinar a localização física de duas máquinas que apresentam conflito de endereços IP pode ser uma tarefa bastante difícil. Para auxiliar a resolver esse problema, foi padronizado um serviço para o auxílio dessa árdua tarefa, conhecido como protocolo DHCP. A seguir apresentaremos o seu funcionamento.

### 14.10.1 Funcionamento do DHCP

O serviço de DHCP funciona na filosofia da arquitetura cliente-servidor, na qual uma máquina (denominada servidor DHCP) é responsável por atribuir endereços IPs às demais máquinas (denominadas clientes DHCP). A atribuição do endereço IP é feita no momento em que o computador cliente é ligado ou, mais especificamente, quando seu serviço de rede é iniciado.

Deve-se observar que o servidor DHCP apenas empresta o endereço IP ao cliente, sendo a renovação do endereço IP de tempos em tempos responsabilidade do cliente. Se o empréstimo não for renovado, o endereço IP será considerado livre e poderá ser atribuído a outra máquina da rede. Essa característica permite reutilizar endereços IP quando um computador é desativado ou desligado por um longo período.

## 14.11 Protocolo SNMP

O protocolo SNMP (*Simple Network Management Protocol*) utiliza no nível de transporte o protocolo UDP para fazer gerência de equipamentos, sendo o protocolo-base de todas as principais plataformas de gerenciamento de diversos fabricantes, como o CiscoWorks, da Cisco, o HPOpenView, da HP, o SunNetManager, da SUN, e o Transcend, da 3COM. O SNMP utiliza o protocolo UDP na camada de transporte e escuta as requisições nas portas 161 (agente) e 162 (*traps*).

As aplicações responsáveis pelo gerenciamento da rede recebem informações emitidas pelos equipamentos ativos configurados com o protocolo SNMP e processam-nas, gerando relatórios e alarmes no momento do atingimento de limites configurados. Esse monitoramento é realizado constantemente, permitindo ao administrador da rede rapidez na identificação e correção de problemas. Todas essas informações são armazenadas em uma base de dados conhecida como MIB (*Management Information Base*).

É possível configurar as aplicações de gerenciamento para enviarem avisos por meio de emails, por sinais visuais ou por sinais sonoros aos administradores da rede quando situações críticas ocorrerem. São exemplos de situações em que um aviso poderia ser enviado: queda de uma porta de um roteador, nível de tráfego fora dos limites, porcentagem de processamento perto do limite, excesso de colisões ou, ainda, uma porta com defeito.

Apesar do alto índice de aceitação, o protocolo SNMP apresenta algumas deficiências, principalmente em relação à segurança e à transferência eficiente de um grande número de informações do agente para o gerente. Além disso, o SNMP não é o protocolo ideal para o gerenciamento de grandes redes de computadores, devido ao fato de apresentar limitações de desempenho para obtenção de requisições explícitas e não dar suporte à comunicação entre gerentes. Assim, na década de 1990, teve início a definição do sucessor do SNMP conhecido por SNMPv2.

## 14.12 Exercícios do capítulo 14

1. (Sanepar, 2004) Sobre o POP (*Post Office Protocol*), assinale a alternativa incorreta:

a) As mensagens encaminhadas por servidores SMTP são armazenadas em servidores de mensagens eletrônicas por meio do POP.

b) O POP utiliza a porta-padrão 110 e opera usando o protocolo TCP.

c) O POP permite o modo de operação offline, no qual um cliente de correio eletrônico solicita ao servidor POP o pacote de novas mensagens, que são, então, transferidas ao programa cliente; em seguida, as mensagens são apagadas do servidor. Nesse modo, todo o processamento de mensagens ocorre no computador que executa o cliente de correio eletrônico.

d) O uso do POP é indicado quando os usuários são estáticos, ou seja, cada um possui seu computador e só acessa seu correio eletrônico a partir dele.

e) O POP permite que diversas pastas sejam mantidas no servidor, auxiliando na organização da mensagens.

2. Avalie as afirmativas a seguir com base no texto que representa a manipulação de um servidor SMTP com uma interface de linha de comando (os números de linha foram inseridos para referência).

```
1  $telnet smtp1.localhost 25
2  220 mail.localhost SMTP
3  helo mail.localhost
4  250 mail.localhost
5  mail from:<teste@teste.com.br>
6  250 Ok
7  rcpt to:<teste2@outrodominio.com.br>
8  250 Ok
9  data
10  Apenas um teste ... até mais!
12  .
13  250 Mail queued for delivery
14  quit
15  221 Closing connection Good bye
```

I. O SMTP utiliza por padrão a porta 25 e opera usando o protocolo

UDP.

II. O SMTP é constituído de duas partes (origem e o destino), e cada uma delas possui acesso a um servidor de armazenamento. Quando a origem envia uma mensagem para o destino, essa mensagem é primeiramente armazenada no servidor de armazenamento da origem, que tenta enviar as mensagens e, se ocorrer algum problema com o destino, tentará posteriormente reenviar a mensagem. Se não conseguir, a mensagem será enviada de volta à origem ou ao post*master*.

III. A linha 12 indica que o corpo da mensagem eletrônica é finalizado.

IV. As linhas 5 e 7 fazem parte do cabeçalho da mensagem, enquanto a linha 10 faz parte do corpo da mensagem.

Assinale a alternativa correta:

a) Somente as afirmativas I e II são verdadeiras.

b) Somente as afirmativas I, III e IV são verdadeiras.

c) Somente as afirmativas II e III são verdadeiras.

d) Somente as afirmativas II, III e IV são verdadeiras.

e) Somente as afirmativas III e IV são verdadeiras.

3. Sobre os protocolos utilizados para envio e recebimento de correio eletrônico (*email*) na Internet, considere as seguintes afirmativas:

I. O protocolo SMTP (*Send Mail Transfer Protocol*), utilizado para enviar correio eletrônico, é um protocolo baseado em codificação ASCII.

II. O POP3 (*Post Office Protocol*) é o protocolo utilizado pelos clientes de correio eletrônico para transferir as mensagens do servidor para máquina local.

III. No protocolo POP3, é possível ler mensagens diretamente do servidor de correio eletrônico, sem fazer sua transferência para máquina local.

IV. As portas do protocolo POP3 e SMTP são, respectivamente, 110 e 25.

V. Os protocolos SMTP e POP3 são capazes de transmitir outras informações, além de texto, como arquivos anexados, sem qualquer tipo de codificação especial.

Assinale a alternativa correta:

a) Somente a afirmativa II é verdadeira.

b) Somente as afirmativas III e IV são verdadeiras.

c) Somente as afirmativas I, II e IV são verdadeiras.

d) Somente a afirmativa V é verdadeira.

e) Todas as afirmativas são verdadeiras.

4. Sobre o POP (*Post Office Protocol*), assinale a alternativa incorreta:

a) As mensagens encaminhadas por servidores SMTP são armazenadas em servidores de mensagens eletrônicas por meio do POP.

b) O POP utiliza a porta-padrão 110 e opera usando o protocolo TCP.

c) O POP permite o modo de operação offline, em que um cliente de correio eletrônico solicita ao servidor POP o pacote de novas mensagens, que são, então, transferidas ao programa cliente; em seguida, as mensagens são apagadas do servidor. Nesse modo, todo o processamento de mensagens ocorre no computador que executa o cliente de correio eletrônico.

d) O uso do POP é indicado quando os usuários são estáticos, ou seja, cada um possui seu computador e só acessa seu correio eletrônico a partir dele.

e) O POP permite que diversas pastas sejam mantidas no servidor, auxiliando na organização da mensagens.

5. Sobre os serviços de rede, considere as seguintes afirmativas:

I. A porta-padrão do protocolo HTTP é 8080 e o protocolo de transporte é TCP.

II. Em caso de falha do DNS, é possível acessar uma máquina da Internet, desde que se conheça seu endereço IP.

III. O DNS é o serviço responsável por transformar o nome de uma

máquina (host) em um endereço IP.

IV. O DNS não é utilizado para transformar o endereço IP em um nome de uma máquina.

Assinale a alternativa correta:

a) Somente as afirmativas II e III são verdadeiras.

b) Somente as afirmativas I e IV são verdadeiras.

c) Somente as afirmativas I, II e III são verdadeiras

d) Somente as afirmativas II e IV são verdadeiras.

e) Somente a afirmativa IV é verdadeira.

6. (Sanepar, 2004) O SMTP (*Simple Mail Transport Protocol*) é um protocolo do TCP/IP para envio de mensagens eletrônicas. Sobre o SMTP, assinale a alternativa <u>incorreta</u>:

a) Diz-se que quando um servidor SMTP processa uma mensagem eletrônica, está com repasse (relay) fechado, pois nem o remetente nem o destinatário são usuários do servidor em questão.

b) Servidores SMTP com repasse constituem uma ameaça na rede, pois são geralmente explorados por spammers.

c) Um servidor SMTP pode utilizar blackhole lists para implementar filtros e, assim, rejeitar mensagens eletrônicas não solicitadas.

d) O SMTP, ao ser projetado, não tem a finalidade de garantir a autenticidade de um remetente de uma mensagem eletrônica.

e) É possível fazer uso direto do SMTP por meio da execução do comando Telnet para a porta 25 de um servidor SMTP em questão.

7. (Copel, 2010) O DHCP (*Dynamic Host Configuration Protocol*) é um protocolo que permite:

a) Resolução de nomes em endereços IP e vice-versa.

b) Ligação entre endereços IP e seu endereço de hardware correspondente.

c) Configuração dinâmica de terminais, com concessão de endereços IP de host e outros parâmetros de configuração para clientes de rede.

d) Gerência de configuração para elementos de rede, permitindo o acesso remoto em interfaces de emulação de terminal.

e) Gerência dinâmica de hosts em redes de gerência de configuração.

8. (Copel, 2010) Suponha que um servidor de nomes (protocolo DNS), responsável pelo domínio "*copel.com.br*", recebeu uma solicitação para resolver o nome "*www.pucpr.br*". Sabendo que o servidor de nomes não tem informações em cache, qual será o primeiro passo para a resolução do nome?

a) Buscar na base de dados e responder com o endereço IP cadastrado.

b) Consultar o servidor-raiz para descobrir o endereço do servidor responsável pelo domínio "br".

c) Consultar o servidor "br" para descobrir o endereço do servidor responsável pelo domínio "*pucpr.br*".

d) Consultar o arquivo host para determinar o endereço do servidor de nomes da rede.

e) Encaminhar a requisição diretamente para o servidor responsável pelo domínio "*pucpr.br*".

9. (Copel 2010) O protocolo HTTP (*Hyper Text Transfer Protocol*) possui as seguintes características, <u>exceto</u>:

a) Realiza a transferência de arquivos a partir da mensagem GET.

b) O HTTP versão 1.1 pode manter a conexão TCP aberta e transferir diversos arquivos.

c) Realiza o controle da sessão, controlando autenticações de usuário.

d) O protocolo pode transferir qualquer tipo de arquivo.

e) O protocolo HTTP permite a implementação de transferência de correio eletrônico, podendo substituir o protocolo SMTP (*Simple Mail Transfer Protocol*).

10. (TRT) Um serviço muito utilizado em ambiente Internet, tendo como porta-padrão de funcionamento a TCP 80:

a) DNS.

b) FTP.

c) TELNET.

d) HTTP.

e) GHOST.

11. (TRT) Os softwares de correio eletrônico normalmente utilizam para entrada e saída de emails, respectivamente, os servidores:

a) POP3 + HTTP.

b) POP3 + SMTP.

c) SMTP + POP3.

d) SMTP + HTTP.

e) HTTP + POP3.

CAPÍTULO 15

# Protocolo IPv6

Neste capítulo, abordaremos a nova versão do protocolo IP, conhecida por IPv6. A versão do IP atualmente utilizada (IPv4) apresenta limitações quanto à disponibilidade de endereços IPs, necessários para o endereçamento de equipamentos ligados à Internet. Assim, o objetivo do IPv6 será suprir essa deficiência apresentada pelo IPv4.

## 15.1 Introdução

As empresas que utilizam Internet para realizar negócios vêm encontrando dificuldades para expandir suas atividades, visto que necessitam adicionar endereços IPs a sua rede. Em fevereiro de 2011, a IANA (*Internet Assigned Numbers Authority*), responsável por controlar os endereços em âmbito mundial, promoveu nos Estados Unidos a distribuição dos últimos blocos que estavam em seu estoque, ou seja, o estoque central passou a ser controlado pelos órgãos regionais (RIR – *Regional Internet Registry*) representados nos continentes pelas seguintes instituições:

- Na América Latina e Caribe pelo LACNIC (*Latin America and Caribbean Network Information Centre*).
- Na América do Norte pela ARIN (*American Registry for Internet Numbers*) e na África pela AFRINIC (*African Network Information Center*).
- Na Europa pela RIPE NCC (*Réseaux IP Européens Network Coordination Centre*).
- Na Ásia e Pacífico pela APNIC (*Asia-Pacific Network Information Centre*).

O protocolo IPv6 é a atualização do protocolo IP (IPv4), utilizado em todos os equipamentos que estão conectados à Internet. O modelo de referência TCP/IP adotado pela ARPANET na década de

1980 passou a oferecer o protocolo IP na versão 4 (IPv4). Nessa época, os endereços eram distribuídos, utilizando máscaras de rede seguindo o modelo de classes (exs.: classes A, B, C, D e E), conforme apresentado no capítulo 6. Porém, esse modelo de divisão se mostrou ineficiente, permitindo que inúmeros endereços fossem perdidos devido ao modelo de distribuição baseado em classes.

Na década de 1990, o IETF propôs um novo modelo para determinar a máscara de rede de um endereço IP, chamado de CIDR (*Classless InterDomain Routing*), abordado no capítulo 8. Com esse novo modelo de máscaras de rede, a divisão de endereços IPs deixou de utilizar as classes rígidas (classe A - /8, classe B - /16 e Classe C - /24) e passou a utilizar máscaras com tamanhos variáveis. Desta forma, um bloco IP com máscara /24 que atendia um único cliente passou a atender vários clientes.

Como exemplo de tamanhos utilizados pelo roteadores da Internet, temos:

- /20, em que os primeiros 20 bits são dedicados à rede. Com este, a máscara utilizada ficará com 255.255.240.0.
- /22, em que os primeiros 22 bits são dedicados à rede. Com este, a máscara utilizada ficará com 255.255.252.0.
- /24, em que os primeiros 24 bits são dedicados à rede. Com este, a máscara utilizada ficará com 255.255.255.0. As máscaras anteriormente utilizadas continuam sendo possíveis de serem utilizadas, porém uma nova variedade passou a estar disponível.
- Entre vários outros, como /27 com máscara 255.255.255.224, /28 com máscara 255.255.255.240, /29 com máscara 255.255.255.248 etc.

Com a distribuição de endereços seguindo o modelo CIDR, foi possível criar milhares de redes diferentes e, com isso, gerou-se outro problema, uma quantidade imensa de rotas trocadas entre os roteadores da Internet. Assim, com a chegada do modelo CIDR, foi necessário realizar a agregação de rotas, processo necessário para reduzir a tabela de roteamento trocada entre os roteadores da Internet. Atualmente, existem mais de 520 mil rotas sendo trocadas

entre os roteadores de borda da Internet, ou seja, a ideia de agregação veio ajudar em termos da redução de recursos nos roteadores.

Algumas facilidades foram também criadas para reduzir o consumo de endereços IPs (IPv4) conhecidos por DHCP (*Dynamic Host Control Protocol*) e NAT (*Network Address Translation* – Tradução de Endereço de Rede).

O protocolo DHCP permite distribuir endereços automaticamente, além de manter os endereços IPs recebidos pelo equipamentos por tempo limitado. Caso o equipamento que recebeu o endereço IP deixe de ser utilizado (equipamento desligado, com defeito ou removido do local), o endereço IP voltará à base de endereços válidos (*pool*) e poderá ser novamente utilizado por outro equipamento.

Outro recurso criado para reduzir o impacto da falta de endereços IPs (IPv4) foi o uso de NAT (explicado no capítulo 12). Esse recurso permite que vários equipamentos com endereços IPs privados (explicados no capítulo 8) acessem a Internet com apenas um endereço IP público.

Apesar de todos os esforços comentados, a quantidade de endereços IPs disponíveis permaneceu crítica e, por isso, o protocolo IPv6 ganhou espaço entre os fabricantes de sistemas operacionais de rede, como também entre as operadoras de telecomunicações, provedores de serviços de rede, empresas privadas e usuários domésticos.

O IPv6 deverá substituir o IPv4 progressivamente, pois, como já existem milhares de computadores interligados, essa migração ocorrerá de forma gradual. A grande quantidade de computadores interligados obrigará o IPv6 a operar com o IPv4 durante o processo de migração.

O IPv6 tem como grande vantagem a expansão dos endereços IPs considerados escassos para o acesso à Internet. Com o crescimento exponencial da Internet, em poucos anos não teremos mais endereços IPs livres.

Para termos uma ideia, o protocolo IP disponível é referenciado por

32 bits, enquanto seu sucessor (IPv6) disponibilizará um endereço IP com 128 bits, ou seja, quatro vezes maior em termos de bits, porém, em quantidade de endereços IPs válidos, a diferença é muito maior.

## 15.2 Diferenças entre IPv4 e IPv6

Vejamos as principais diferenças entre os protocolos IPv4 e IPv6 na tabela 15.1:

*Tabela 15.1 – Diferenças entre o IPv4 e IPv6*

| Descrição | IPv4 | IPv6 |
|---|---|---|
| Formato do endereçamento | Endereçamento composto de um endereço com 32 bits separados em quatro partes, e cada uma contém 8 bits. | Endereçamento composto de um endereço com 128 bits separados em oito partes, e cada uma contém 16 bits. |
| Quantidade de endereços IPs possíveis de serem utilizados | São disponibilizados 4.294.967.296 endereços, ou seja, 2 elevado a 32 bits. Uma grande parte acabou sendo desperdiçada com alocações inconsistentes e endereços reservados | Com 2 elevado a 128 endereços, teremos aproximadamente 79 octilhões (7,9 x 10¨28) de vezes a quantidade de endereços IPv4. |
| Configuração | Precisa ser configurado individualmente em cada equipamento ou utilizar o protocolo DHCP que fornece um endereço automaticamente. | Pode usufruir de autoconfiguração, em que os primeiros 64 bits são fixos para a rede local e os outros 64 bits são formados baseando-se no endereço MAC do equipamento de rede. |

| Descrição | IPv4 | IPv6 |
|---|---|---|
| Formato do cabeçalho | Além de oferecer menos endereços IPs, utiliza um cabeçalho maior que o do IPv6. | Cabeçalho simplificado. No IPv6, o cabeçalho é duas vezes menor quando comparado ao IPv4. No IPv6, temos ainda o conceito de cabeçalhos encadeados. A nova versão foi simplificada, tornando-se mais eficiente, reduzindo o processamento dos roteadores. |
| Formato dos endereços | Escritos em formato decimal. | Escritos em formato hexadecimal. Permite que sequências de 0 sejam simplificadas. |
| Protocolos | Os protocolos ARP e RARP são amplamente utilizados para a comunicação entre dois equipamentos. | Os protocolos ARP e RARP foram absorvidos pelo protocolo ICMPv6.<br>O ICMPv6 passa a ser um cabeçalho encadeado do IPv6, e não mais um protocolo em cima do IPv4 (ICMP).<br>O IPv6 é muito dependente do ICMPv6, portanto, recomenda-se não bloquear ICMPv6 nos firewalls. |
| Tipos de tráfego | Permite a transmissão de quadros em broadcast, unicast e multicast. | Excluiu o conceito de broadcast e o substituiu por multicast |
| NAT | Utiliza NAT para reusar endereços IPs. | Não existe NAT no IPv6. Pressupõe-se que cada host terá um IP roteável; |

Mesmo com as diferenças entre os protocolos, estes ainda podem operar de forma conjunta. Há um grande esforço de diversas entidades para que o emprego do IPv6 cresça. Infelizmente, o desconhecimento dos administrradores de rede sobre as características do novo protocolo e a necessidade de investimento em novos equipamentos de rede com suporte ao IPv6 têm feito essa migração ocorrer de forma lenta. A seguir, abordaremos o formato do endereço IPv6.

## 15.3 Formato do endereço IPv6

Uma das novas características desse novo protocolo é o novo formato do endereço. O IPv6 amplia o atual endereço de 32 para 128 bits, tendo sido o endereço dividido em oito partes de 16 bits. Com esse novo formato é possível que qualquer cidadão do mundo tenha um endereço IP individual. O endereço IPv6 possui três formas de representação:

- A primeira segue o seguinte modelo 4DEA:2031:0000:0000:0006:0600:600C:51A7. Nesta forma, as sequências de zeros não foram simplificadas.
- A segunda forma de representação leva em consideração a economia na descrição do endereço IPv6. Como apenas 15% de todos os endereços IPv6 estão previamente alocados, haverá para cada endereço uma quantidade grande de partes com apenas zeros. Com o objetivo de melhorar a representação do endereço IP, é permitida a simplificação da notação seguindo as seguintes regras:
  - Onde houver grupos de zeros, em apenas um deles será necessário constar no endereço IP. Vejamos um exemplo:

  Dado o endereço IPv6: 2001:adba:0000:0000:0000:0000:2709:7474.

  Poderá ser simplificado para: 2001:adba:0:0:0:0: 2709:7474.
- Os zeros à esquerda de grupos com outros valores não necessitam ser representados. Assim, temos que as sequências de zeros poderão ser substituídas pela agregação de "::". É importante observar que essa agregação poderá ser efetuada apenas uma vez em cada endereço IPv6. Vejamos um exemplo:
  - Dado o endereço IPv6: 4DEA:2031:0000:0000:0006:0600:600C:51A7.
  - Poderá ser simplificado para: 4DEA:2031::6:600:600C:51A7. Vejamos a figura 15.1 que apresenta um exemplo de um endereço IP *unicast* e o seu formato simplificado.

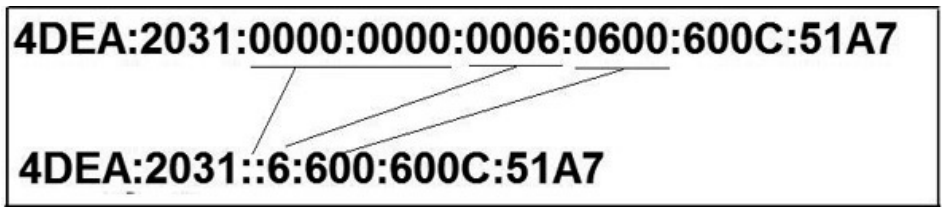



*Figura 15.1 – Formato resumido de um endereço IPv6.*

- A terceira forma refere-se à compatibilização do endereço IPv6 com os endereços utilizados pelo IPv4. Assim, devido ao compartilhamento desses endereços nos mesmos equipamentos, a sua forma de representação é 0:0:0:0:0:0:191.167.10.10 e a forma abreviada é ::191.167.10.10. É importante ressaltar que, mesmo nessa notação, a quantidade de bits é mantida em 128 bits. A tabela 15.2 apresenta exemplos de endereços no formato IPv6 sendo compatibilizados com o padrão IPv4:

*Tabela 15.2 – Endereços IP no IPv6 compatíveis com IPv4*

| Endereço | Forma abreviada | Descrição |
|---|---|---|
| 1180:0:0:0:9:900:100C:417C | 1180::9:900:100C:417C | Endereço ponto a ponto. |
| 0:0:0:0:0:0:0:1 | ::1 | Endereço de loopback. |
| 0:0:0:0:0:0:192.168.100.30 | ::192.168.100.30 | Endereço utilizado em ambientes mistos com IPv4 e IPv6. |

Outro ponto importante a ser observado sobre o protocolo IPv6 é sobre como apresentar a máscara da rede. Com o protocolo IPv4, representamos a máscara usando uma barra (/), seguida pela quantidade de bits que representa a rede do endereço. No IPv6, seguimos o mesmo modelo. Vejamos um exemplo:

- IPv4: 10.1.1.0/24, em que os primeiros 24 bits do endereço são dedicados à rede. Os 8 bits restantes são dedicados aos equipamentos da rede local.
- IPv6: 2001:db8:12::/64, em que os primeiros 64 bits do endereços são dedicados à rede. Os 64 bits restantes são dedicados aos equipamentos da rede local.

## 15.4 Tipos de endereço

O protocolo IPv6 apresenta três tipos de endereço conhecidos por:

- **Endereço** *unicast* – Utilizado para endereçar uma única interface.
- **Endereço** *anycast* – Utilizado para endereçar um conjunto de interfaces, porém entregue para a primeira encontrada.
- **Endereço** *multicast* – Utilizado para endereçar um conjunto de interfaces e entregue a todos os equipamentos que estejam ligados ao grupo do endereço *multicast*.
- O tipo *broadcast*, presente na versão IPv4, não foi implementado no IPv6, e sua utilização pode ser substituída pelo uso dos endereços *multicast*. Os endereços *multicast* que substituem o *broadcast* são:
  - Endereço *multicast* FF02:0:0:0:0:0:0:1 ou no formato simplificado FF02::1 direciona os pacotes a todos os equipamentos da rede IPv6.
  - Endereço *multicast* FF02:0:0:0:0:0:0:2 ou no formato simplificado FF02::2 direciona os pacotes a todos os endereços IPv6 dos roteadores interconectados.

A seguir, descreveremos os detalhes de cada um desses endereços.

### 15.4.1 Endereço unicast

O endereço *unicast* refere-se ao endereçamento ponto a ponto, ou seja, todo pacote enviado a um endereço *unicast* será entregue somente a uma interface de rede específica. Os endereços *unicast* são utilizados para manter a comunicação entre dois equipamentos que poderão ser computadores, impressoras, equipamentos ativos, telefonia VoIP, entre outros.

Um endereço *unicast* pode ser classificado em:

- Endereço *unicast* global.
  - Temos também um tipo especial de endereço *unicast* global conhecido por endereço IPv6 com endereço IPv4 embutido.
- Endereço *unicast* local (*unique local* definido na RFC 4193).
- Endereço *unicast* de *link local* (local de vínculo).

Para facilitar o entendimento sobre o que cada um desses endereços representa, a figura 15.2 apresenta a equivalência que os endereços *unicast* global, local e *link local* possuem com endereços IPv4.

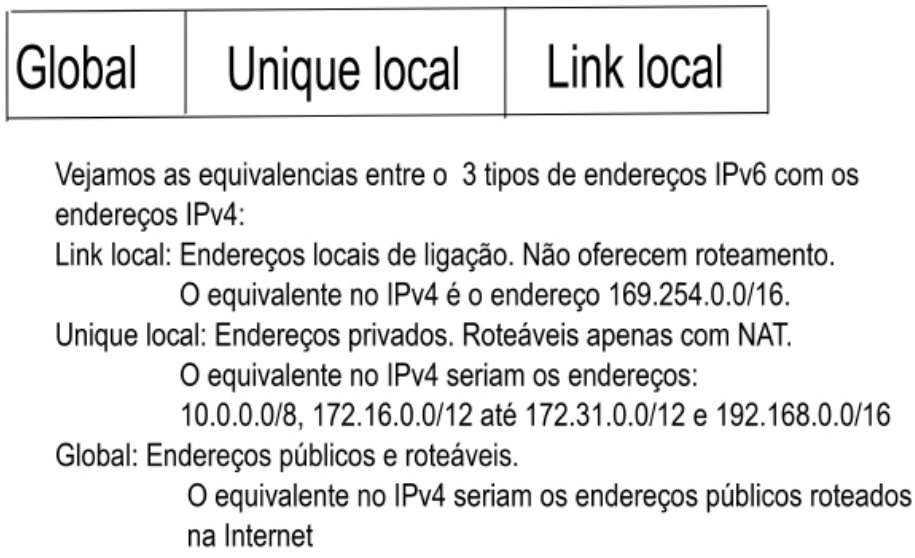



*Figura 15.2 – Equivalência entre um endereço unicast IPv6 e o correspondente IPv4.*

Independentemente do tipo do endereço IP *unicast*, este deverá ser único na rede. A formalização sobre qual é a parte do endereço IPv6 que representa a rede é definida pela sua máscara, entretanto para todos os endereços IPv6 *unicast*, a parte utilizada para endereçar o equipamento, que deve ser única na rede, necessita de 64 bits. Também é chamada de interface ID. Sugere-se que a formação da parte relacionada à interface ID do endereço IPv6 utilize o método EUI-64 comentado neste capítulo. É importante observar que, além dos bits utilizados para endereçar o equipamento, temos também os bits responsáveis por identificar a rede. A parte do endreço IPv6 que define a rede é chamada de Prefix ID. O prefix ID deve conter o mesmo valor para todos os equipamentos da rede local. A figura 15.7 apresenta um exemplo de uma rede em que cada interface do roteador possui um endereço de rede e cada equipamento possui um endereço único.

A regra de usar o método EUI-64 para formar a interface ID não se aplica aos endereços *unicast* que iniciam com os três primeiros bits

em 000. Esses endereços definem endereços IPv4 embutidos no IPv6. Para esses endereços, a parte referente à identificação dos equipamentos não precisará conter 64 bits nem ser gerada a partir do método EUI-64.

O método EUI-64 expande o endereço MAC do equipamento de rede de 48 bits (6 bytes) para 64 bits (8 bytes), inserindo a sequência hexadecimal FFFE no meio do endereço MAC, após o vigésimo quarto bit. Esse método permite que um equipamento de rede sozinho defina seu endereço IPv6. A figura 15.3 apresenta como ficará um endereço IPv6 após a aplicação do método EUI-64. Mostra também a necessidade de inverter o sétimo bit para 1, formalizando que o endereço possui escopo universal.

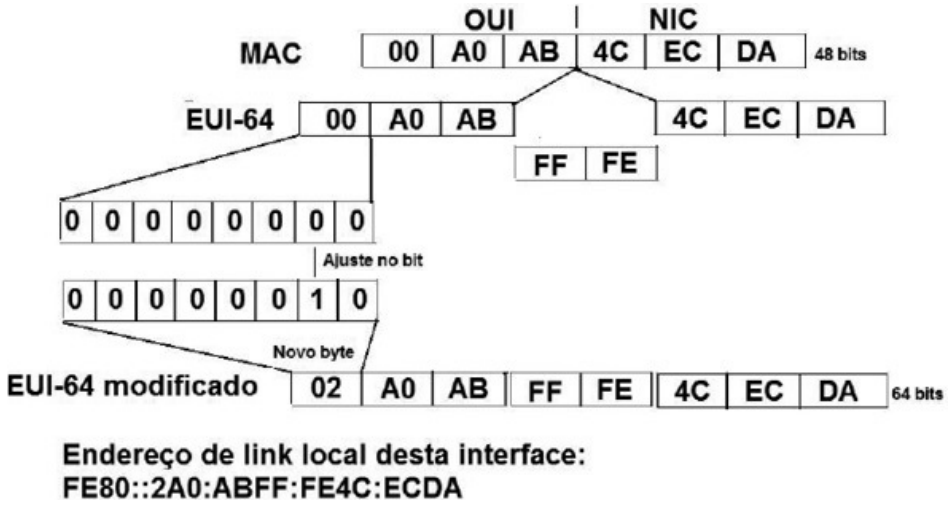



*Figura 15.3 – Formação do endereço IPv6 seguindo o processo EUI-64.*

É importante observar, conforme apresentado na figura 15.3, que, além de adicionarmos a sequência hexadecimal FFFE no meio do endereço MAC, o sétimo bit da esquerda para direita, conhecido por U/L (*Universal/Local*), normalmente é invertido de 0 para 1. Quando 1, esse bit identifica que o escopo do endereço IPv6 é universal, e quando 0, o escopo do endereço IPv6 é local.

Outro ponto importante a ser comentado sobre endereços *unicast* são os endereços reservados, que são formados por zeros e não podem ser atribuídos a nenhum equipamento na rede. Como exemplo de endereços reservados, temos o endereço do default

gateway (rota *default*) e o endereço de loopback. O endereço de loopback (0:0:0:0:0:0:0:1), assim como no IPv4, representa um endereço processado pelo próprio equipamento. A rota default representada por ::/0 também não deve ser utilizada em nenhum equipamento da rede. A seguir, apresentaremos os demais tipos de endereços *unicast* possíveis em uma rede com protocolo IPv6.

### 15.4.1.1 Endereço unicast global

Os endereços *unicast* globais equivalem aos endereços públicos IPv4 e, por isso, são roteáveis entre os roteadores da Internet.

A IANA definiu que os endereços *unicast* globais IPv6 utilizados pelos RIRs (*Regional Internet Registry*) iniciem em 2000::/3 e sigam até 3fff:ffff:ffff:ffff:ffff:ffff:ffff:ffff. Vejamos um exemplo sem a simplicação dos bits zeros:

- De 2000:0000:0000:0000:0000:0000:0000:0000 até 3fff:ffff:ffff:ffff:ffff:ffff:ffff:ffff.

Estes são globalmente roteáveis, similares aos endereços públicos do IPv4. Esse intervalo equivale a 13% dos endereços IPv6 válidos. Atualmente, cada RIR recebeu da IANA um bloco /12 (12 primeiros bits do endereço IPv6) a fim de que cada entidade regional faça a correta distribuição. A IANA reservou 506 prefixos /12 para atribuição mundial, no entanto apenas uma pequena parte desses prefixos foi oficialmente distribuída, o que significa que os estoques da IANA estão carregados. Vejamos as ranges de cada RIR:

- AfriNIC: 2C00:: /12
- APNIC: 2400:: /12
- ARIN: 2600:: /12
- LACNIC: 2800:: /12 – Range alocada em outubro de 2006

No caso do LACNIC que atende o Brasil, existe também a faixa 2001:1200::/23 que foi alocada pela IANA ao LACNIC em novembro de 2002. As primeiras operadoras (ex.: COPEL Telecom) que aderiram ao IPv6 foram identificadas com essa range de endereços.

- RIPE NCC: 2A00:: /12

Uma das vantagens em termos prefixos por região com grande capacidade de expansão é que a tabela dos roteadores pode ser minimizada, uma vez que para rotear um pacote do Japão para o Brasil, o roteador pode encontrar o destino correto com poucas rotas.

O planejamento para alocação dos prefixos IPv6 é responsabilidade de cada autoridade regional (RIR) e cada uma possui suas próprias regras. No contexto do Brasil, o NIC.br recebeu do LACNIC os prefixos 2801:: /16 e 2001:: /16 para coordenar e distribuir no cenário nacional. O NIC.br, por meio do grupo de trabalho IPv6.br, recomenda que as seguintes regras sejam aplicadas:

- Operadoras de telecomunicações (ex.: Algar, GVT) receberam um prefixo /32. Um único prefixo /32 atribuído a uma operadora permite criar um plano de endereçamento com mais de 4 bilhões de sub-redes /64. Cada sub-rede /64, por sua vez, possui mais endereços do que o total do protocolo IPv4. Em algumas situações, as operadoras ainda subdividem o intervalo de /32 até /48 para as regiões onde atendem (por exemplo, subdividem com /40, para atender a regiões do Paraná).

As empresas clientes das operadoras (ex.: provedores de acesso à Internet ou provedores de serviços de rede), quando solicitam, recebem um prefixo /48. Uma empresa, ao receber um prefixo /48, poderá criar 65.536 sub-redes, pois sobram 16 bits entre as posições 48 e 64, o que implica 2 elevado a 16 (65.536) combinações possíveis de novas sub-redes. É importante observar que todo endereço IP após ser designado a um cliente precisará ser registrado no site do Registro.br. Desta forma, sempre que um novo cliente for ativado em IPv6, deveremos associar o endereço IPv6 com seu domínio, CNPJ ou CPF. Essa associação formaliza que um determinado cliente é o responsável pelo endereço em um período de tempo.

Um provedor de serviços de rede poderá ainda repassar a seus clientes regionais um prefixo /56, que permitirá ao provedor comercializar 256 diferentes redes, pois entre a posição 48 e 56

temos 8 bits (2 elevado a 8 = 256 equipamentos).

- Clientes finais residenciais ou até mesmo pequenas empresas devem receber um prefixo /56. Cada um dos /56 poderá ainda ser subdividido em outras 256 redes internas [da posição 56 até 64 (2 elevado a 8 = 256 equipamentos)]. A sugestão apresentada ocorre sobre os primeiros 64 bits, permitindo que o cliente residencial utilize o método EUI-64 para definir seus endereços IPv6 de cada um dos seus equipamentos de rede. Atualmente, um cliente residencial possui inúmeros equipamentos com acesso à rede, como TVs, tablets, smartphones, computadores e, em breve, com a “Internet das coisas”, eletrodomésticos poderão também receber um endereço IPv6. Dessa forma, 256 endereços que aparentemente são muitos poderão ser utilizados em quase toda a sua plenitude.

Algumas operadoras e provedores de serviço podem optar por fornecer um /64 para clientes residenciais. Desta forma, é importante conhecer o protocolo IPv6 e saber negociar para não sofrer com a falta de endereços para os inúmeros equipamentos internos da residência.

A figura 15.4 apresenta o processo de atribuição de um prefixo /48 a uma empresa provedora de serviços de rede por uma operadora que possui um prefixo /32.

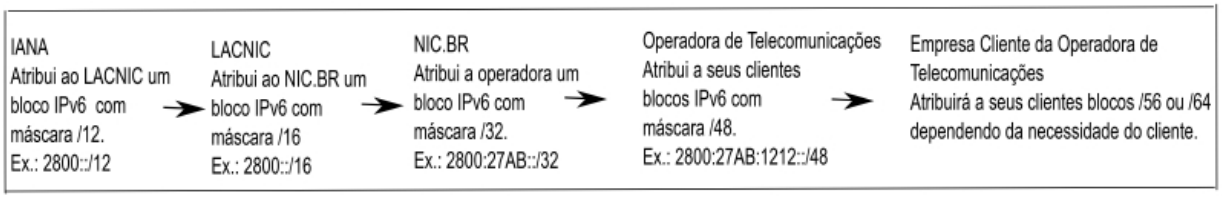



*Figura 15.4 – Exemplo de atribuição dos endereços unicast global.*

Conforme observado na figura 15.4, a IANA repassa ao RIR local (LACNIC) um /12, que, por sua vez, repassa ao NIC.br um /16. Os demais /16 são repassados a entidades de outros países sob administração do LACNIC. O NIC.br, com posse do /16, repassa às operadoras um /32, que será dividido a seus clientes seguindo a sugestão comentada.

De acordo com o modelo de divisão de blocos IPv6 definidos pela

IANA, segue o formato geral de um endereço *unicast* global, apresentado na figura 15.5.

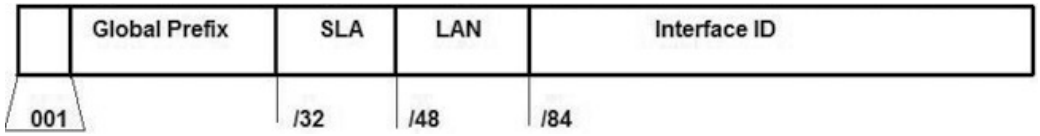



*Figura 15.5 – Formato do endereço unicast global.*

Conforme observado na figura 15.5, os três primeiros bits são reservados e fixados em 001. Esses três bits definem que o bloco de endereços *unicast* global começará com 2. Conforme comentado, o endereço IPv6 é formado por uma base hexadecimal. Assim, todo número ou letra utilizado no endereço é formado por quatro bits. Por exemplo: o número 2 do início 2000 é representado pelos bits 0010. Vejamos outro exemplo:

• O primeiro bit 0 desligado resulta em 0.

• O segundo bit 1 ligado equivale a 2 elevado a 1, que resulta em 2.

• O terceiro bit 0 desligado resulta em 0.

• O quarto bit 0 desligado resulta em 0.

• Caso os 4 bits estivessem ligados, resultaria no decimal 15, que equivale à letra F.

• O primeiro bit 1 ligado equivale a 2 elevado a 0, que resulta em 1.

• O segundo bit 1 ligado equivale a 2 elevado a 1, que resulta em 2.

• O segundo bit 1 ligado equivale a 2 elevado a 2, que resulta em 4.

• O segundo bit 1 ligado equivale a 2 elevado a 3, que resulta em 8.

• Somando os valores, teríamos o decimal 15.

Para o endereço IPv6 2001:1234, são necessários 32 bits, pois, conforme comentado, cada número ou letra utiliza 4 bits. Estes formam juntos o SLA (*Subnet Local Aggregator*) ou conforme definido pela RFC 3587, também chamado de Subnet ID.

A partir do 48o bit até o 63o, os bits são utilizados para endereçar as sub-redes dos clientes das operadoras. Finalizando, os últimos 64 bits endereçam os diferentes equipamentos da rede. É importante observar que para todo endereço IP *unicast* global, recomenda-se utilizar 64 bits para identificar os equipamentos da

rede (computador, TV, smartphone, tablet, impressora, roteador, entre outros). A figura 15.5 apresenta essa parte do endereço IP, denominando-a de interface ID, que será realizada por meio do método EUI-64 comentado neste capítulo.

### 15.4.1.2 Endereço unicast local de ligação (vínculo local)

Todo equipamento de rede IPv6 possui um endereço IP que poderá ser automaticamente gerado assim que o driver IPv6 do sistema operacional for ativado. Esses endereços são designados a equipamentos IPv6 quando na rede local não existir roteador, servidor de DHCPv6 ou, ainda, quando se precisa que a atribuição de endereço IPv6 seja automática. Esse tipo de endereço *unicast* iniciará com FE80::/10, ou seja, os primeiros 10 bits são fixos, os próximos 54 bits são iguais a 0 e os 64 bits restantes serão formatados de acordo com o método EUI-64 comentado neste capítulo. A figura 15.6 apresenta o formato do endereço link local:

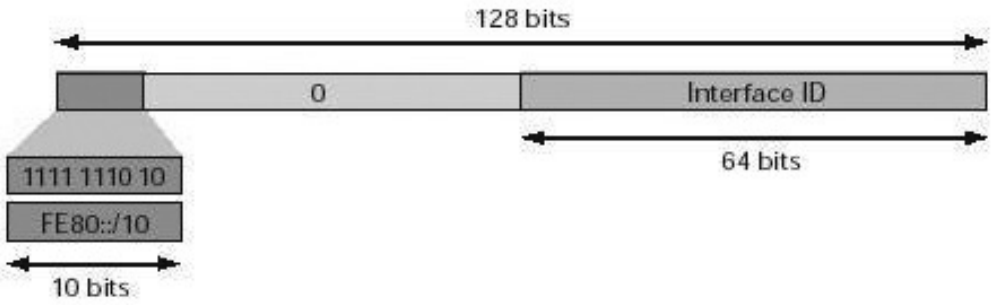



*Figura 15.6 – Formato do endereço link local.*

Conforme comentado, esse endereço é utilizado apenas na rede local onde a interface estiver conectada. Esse grupo de endereços *unicast* equivale aos endereços IPv4 atribuídos automaticamente e conhecidos por endereçamento IP privado automático (APIPA – *Automatic Private IP Addressing*). No padrão IPv4, utiliza-se o prefixo 169.254.0.0/16.

É importante observar que os roteadores não encaminham esses endereços a outras redes, ou seja, apenas serão utilizados entre os computadores que não tenham endereços configurados manualmente nem consigam obtê-los automaticamente por meio do DHCPv6.

### 15.4.1.3 Autoconfiguração

A autoconfiguração de endereços IPv6 permitirá que um equipamento acesse a rede em uma operação plug-and-play. Quando o equipamentos for ligado, automaticamente será associado um endereço IP à sua interface de rede. Com o IPv4, a associação de endereços IP se dava manualmente ou via DHCP.

Em um ambiente IPv6, poderemos usufruir da autoconfiguração em dois momentos:

- **Configuração stateful** – Em que há um servidor DHCPv6, com o qual o equipamento se comunicará.
- **Configuração stateless** – Em que o equipamento construirá seu endereço IP a partir do seu endereço de interface de rede (MAC), que é único, seguindo o método EUI-64.

### 15.4.1.4 Endereço unicast único local (unique local)

Em 1995, a RFC 1884 reservou a range FEC0::/10 para endereços locais e a chamou de endereços *unicast* site-local. Tais endereços tinham a intenção de ser utilizados dentro de um site para uma rede IPv6 privada. Entretanto, o termo site gerou confusão dentro do grupo e, assim, em setembro de 2004, atavés da RFC 3879, foi registrado que o termo site local e o bloco associado estavam obsoletos (*deprecated*).

Em outubro de 2005, por meio da RFC 4193, foi publicado um novo bloco para os endereços privados que passaram a iniciar com FC00::/7. Para esse novo bloco, foi dado o nome de endereço *unicast* local ou unique local. Entretanto, caso o flag Local esteja ligado, ficará FD00 informando que é um endereço local atribuído localmente. Quando utilizar FC00, significará que é um endereço local atribuído por uma organização central ainda a definir.

Os endereços IPv6 classificados como locais (definidos pela RFC 4193) são globalmente únicos, porém devem ser utilizados em uma rede LAN. Tais endereços são capazes de ser roteados entre sites de uma empresa. O bloqueio desses endereços em relação à Internet é realizado por meio de filtros que incialmente inibem todos os endereços IPv6 e, em seguida, liberam os que foram indicados

pela IANA para serem roteáveis.

Cada endereço local tem grande probabilidade de ser globalmente único, pois com a quantidade de endereços oferecidos pelo IPv6 e, ainda, com a utilização do método EUI-64, cada endereço local dificilmente poderá ser duplicado.

Um endereço *unicast* unique local possui a seguinte formatação:

- **7 primeiros bits** – São reservados para formalizar um endereço local. Assim, todo endereço local começará com o seguinte prefixo: FC00::/7 (FC00 equivale ao binário: 1111 (F) 1100 (C) 0000 (0) 0000 (0)).
- **Flag Local** (L) – Conforme comentado, se o valor for 1, significa que se utilizou um procedimento local para definir a parte do endereço IP chamada Global ID (no IPv4, a parte relacionada à rede é igual em todos os equipamentos). Se o valor for 0, seguirá um procedimento diferente do local, porém ainda não definido pela RFC.
- **Identificador global** – Identificador de 40 bits usado para criar um prefixo globalmente único.

  Observação: essas três primeiras partes apresentadas (ex.: FC00:F1D9:6F40) devem ser iguais em todos os equipamentos que compõem a rede LAN. Na figura 15.7, poderemos observar essa regra de configuração.

- **Identificador da interface** – Contém 64 bits dedicados ao endereçamento dos equipamentos.

A figura 15.7 apresenta uma rede configurada com endereços locais.

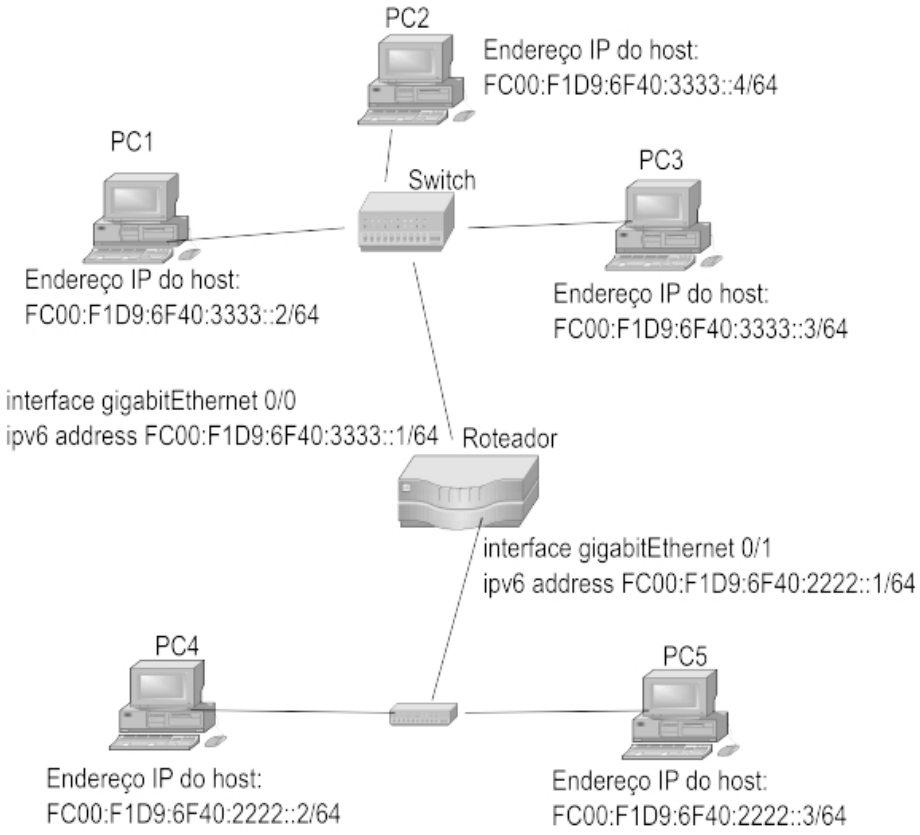



*Figura 15.7 – Rede com endereços locais.*

Nessa rede, os primeiros 64 bits são iguais e identificam a rede. Os últimos 64 bits devem ser diferentes, pois tornam único o equipamento na rede.

## 15.4.2 Endereço anycast

O endereço *anycast* representa um endereços *unicast*, porém com a seguinte particularidade: um mesmo endereço é atribuído a vários roteadores.

Um endereço *anycast* não pode ser utilizado como endereço de origem de um pacote IPv6, ou seja, um endereço *anycast* não pode ser configurado em um computador IPv6; deverá ser associado apenas a roteadores. Um endereço *anycast* tem como objetivo identificar um grupo de roteadores que provê acesso a um determinado domínio em que serviços estão disponíveis, como DNS ou HTTP.

Um pacote direcionado a um endereço *anycast* será enviado para

uma das interfaces identificadas pelo endereço. Especificamente, o pacote é enviado para a interface mais próxima, de acordo com a medida de distância do protocolo de roteamento implementado na rede (ex.: BGP ou OSPF). É importante observar que ao configurarmos um endereço IPv6 classificado como *anycast*, precisamos formalmente informar ao roteador que se trata de um endereço *anycast*. Para isso, utilizamos os seguintes comandos:

- **Em roteadores Cisco** – ipv6 address FC00:F1D9:6F40:2222::1/64 anycast
- **Em roteadores Huawei** – ipv6 address FC00:F1D9:6F40:2222::1 64 anycast

Uma aplicação bastante útil para os endereços *anycast* é a resolução de nomes por equipamentos distribuídos. Nesse caso, quando algum cliente necessitar resolver um nome, ele enviará um pacote para o roteador, o qual determinará o menor caminho para alcançar o servidor DNS. Uma segunda aplicação para o endereço *anycast* é o balanceamente de carga entre servidores. Digamos que em um determinado momento 500 mil pessoas iniciem uma votação pela Internet a fim de eliminar algum participante de um programa de televisão. Como a quantidade de acessos é alta, se tivéssemos um único destino para registrar os votos, com certeza teríamos um problema de congestionamento. Para contornar esse eminente problema, configuramos o mesmo endereço IPv6 em múltiplos roteadores e assim vários servidores atenderão às solicitações. Cada telespectador registrará sua votação em um site mais póximo da sua conexão com a Internet, ou seja, balanceando o tráfego.

É importante entender que um endereço *anycast* identifica um bloco de interfaces, de tal forma que um pacote enviado a um endereço *anycast* será entregue apenas a uma interface do grupo. Os endereços *anycast* são alocados no mesmo espaço de endereçamento *unicast*, utilizando qualquer um dos formatos dos endereços *unicast*. Assim, ambos os tipos de endereços não são distinguíveis sintaticamente. Quando um endereço *unicast* é configurado em mais de uma interface, em um mesmo roteador ou em roteadores diferentes, ele se torna um endereço *anycast*, e o

roteador deve ser explicitamente configurado para reconhecer esse endereço.

### 15.4.3 Endereço multicast

O endereço *multicast* é um tipo de endereçamento do IPv6 que possui a mesma característica dos endereços IPv4 pertencentes à classe D. Um pacote destinado a um endereço *multicast* é entregue a todas as interfaces que fazem parte do grupo de endereços. É importante não o confundir com a transmissão sobre *broadcast*. A diferença existente entre o *multicast* e o *broadcast* é que uma transmissão em *multicast* atinge o seu destino onde ele estiver, além de ser entregue somente aos equipamentos que tenham se unido ao grupo, enquanto uma transmissão em *broadcast* atinge todos os equipamentos em uma rede local.

Conforme comentado, o protocolo IPv6 não oferece suporte a *broadcast*. Para contornar essa falta, existem dois endereços *multicast* que, quando utilizados, atuam como se estivéssemos utilizando *broadcast*.

- Endereço *multicast* FF02::1 direciona os pacotes a todos os equipamentos da rede IPv6.
- Endereço *multicast* FF02::2 direciona os pacotes a todos os endereços IPv6 dos roteadores interconectados.

É importante observar que todos os equipamentos (exs.: computador, encoder, decoder) com endereços *multicast* ligados a um grupo receberão os pacotes, porém, no caso de equipamentos com endereços *anycast*, somente um deles receberá o pacote (o que estiver mais próximo). Outro ponto importante a considerar é que todo equipamento que tem suporte a IPv6 precisará suportar *multicast* em razão de os *broadcasts* serem utilizados como *multicast*. A figura 15.8 apresenta o formato de um endereço IPv6 de *multicast*.

| 8 bits | 4 bits | 4 bits | 112 bits |
|---|---|---|---|
| 1111 1111 | Flags 0RPT | Escopo | Identificador do grupo |

*Figura 15.8 – Formato do endereço de multicast.*

Conforme apresentado na figura 15.8, todo endereço IPv6 *Multicast* começa com o prefixo FF, em que os oito primeiros bits são sempre iguais a 1 (1111 11111, oito primeiros bits). Os próximos quatro bits são flags, que determinam o tempo de vida do pacote, e os próximos quatro bits definem o escopo do endereço *multicast* . Os 112 bits restantes são utilizados para identificar o grupo *multicast* . Vejamos em detalhes as quatro partes que compõem o endereço *multicast* :

1. **Prefixo** – Endereços IPv6 são identificados com o prefixo FF.
2. **Flags** –Estão definidas na RFC 3306. Essa parte do endereço *multicast* é representada por 4 quatro bits, e cada um possui um significado descrito a seguir:
   - O primeiro bit de mais alta ordem é reservado e sempre será igual a 0.
   - O segundo bit (conhecido por R) de mais alta ordem quando for igual a 1 (terá o valor 4 no endereço) significará que o endereço *multicast* é de um ponto de encontro (*Rendezvous Point*). Quando for igual a 0, não representará um endereço de ponto de encontro.
   - O terceiro bit (conhecido por P) de mais alta ordem quando for igual a 0 significará que o endereço *multicast* não está baseado no prefixo da rede. Quando for igual a 1 (terá valor 2 no endereço), representará um endereço *multicast* baseado no prefixo da rede. Quando for igual a 1, o formato do endereço *multicast* seguirá o formato da figura 15.9. Essa figura apresenta um endereço *multicast* gerado a partir de um endereço *unicast*.

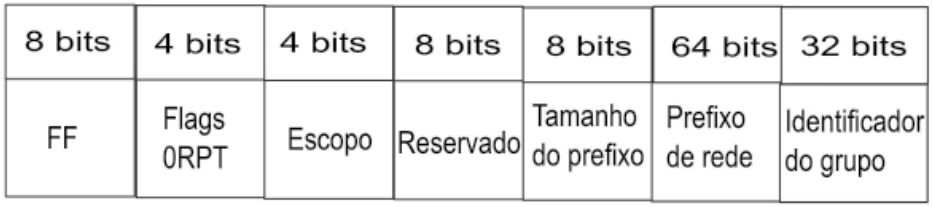



*Figura 15.9 – Formato do endereço de multicast formado a partir de um endereço unicast.*

Comentaremos na seção 15.4.4 como um endereço *multicast* pode ser formado por meio de um endereço *unicast*.

- O quarto bit (conhecido por T) pode variar entre 0 e 1. Quando for 0, significará que o endereço *multicast* foi definido por uma autoridade global da Internet, neste caso a IANA. Os endereços IPv6 *multicast* utilizados pelos protocolos de roteamento possuem o valor 0 nessa posição. Estes foram concebidos para serem utilizados por protocolos de roteamento e sua definição foi formalizada pelas respectivas RFCs. Quando for setado para 1 (terá valor 1 no endereço), significará um endereço IPv6 *multicast* que não é permanente, ou seja, é dinâmico e poderá mudar de acordo com a política de uma operadora (não está sob a administração da IANA). Esse tipo de endereço pode ser chamado de transiente. Esses são endereços utilizados por qualquer operadora para transmitir seus dados de TV, por exemplo. Quando o bit P foi o bit T, também será 1, formando o valor 3 (FF30) no endereço *multicast*

3. **Scope** – Representada por quatro bits, utilizada para limitar o escopo do endereço IPv6 *multicast*. Os quatro bits que representam o escopo do endereço *multicast* são utilizados para delimitar a área de abrangência de um grupo *multicast*. Vejamos as possíveis composições deste campo atualmente utilizadas:

- Quando todos os 4 bits formarem o valor 1 (0001) – Escopo de rede local, por exemplo a rede LAN. Remete a um endereço IPv6 local.
- Quando todos os 4 bits formarem o valor 2 (0010) – Escopo de rede local, por exemplo a rede LAN. Remete a um endereço IPv6 de ligação local, conhecido por endereço de Link-local.

- Quando todos os 4 bits formarem o valor 5 (0101) – Escopo para um rede que atendia a um endereço de site-local. Os endereços de site local tornaram-se obsoletos em 2004 através da RFC 3879.
- Quando todos os 4 bits formarem o valor 8 (1000) – Escopo dedicado a uma rede local de uma organização, por exemplo uma extranet.
- Quando todos os 4 bits formarem o valor E (1110) – escopo global, por exemplo, com abrangência da Internet. Remete a um endereço IPv6 global.

4. **Identificação do grupo** *multicast* – Esta parte é representada por 112 bits. Identifica o grupo *multicast*. Como ocorre na versão IPv4, alguns protocolos de roteamento utilizam endereços *multicast* para ajustarem suas tabelas. Vejamos na tabela 15.3 os endereços IPv6 utilizados pelos principais protocolos de roteamento, como também outros endereços importantes a ser comentados:

*Tabela 15.3 – Endereços multicast utilizados por protocolos de rede*

| Endereço IPv6 | Descrição |
|---|---|
| FF00::/8 | Equivale ao endereço multicast IPv4 224.0.0.0. |
| FF02:0:0:0:0:0:0:1 | Todos os hosts IPv6 escutam o endereço multicast FF02:0:0:0:0:0:0:1. |
| FF02:0:0:0:0:0:0:2 | Todos os roteadores IPv6 escutam o endereço FF02:0:0:0:0:0:0:2. |
| FF02:0:0:0:0:0:0:5 | Utilizado pelo protocolo OSPF entre os roteadores e o roteador designado. |
| FF02:0:0:0:0:0:0:6 | Utilizado pelo protocolo OSPF entre os roteadores e o roteador designado. |
| FF02:0:0:0:0:0:0:9 | Utilizado pelo roteadores configruados com o protocolo RIP. |
| FF02:0:0:0:0:0:0:D | Todos os roteadores que utilizam o protocolo PIM (Protocol-Independent Multica). |
| FF02:0:0:0:0:0:0:12 | Protocolo VRRP (Protocolo de Redundância de Roteador Virtual ou Virtual Router Redundancy Protocol). |

### 15.4.4 Endereço multicast derivado de um prefixo unicast

Conforme observamos na figura 15.9, uma parte do endereço *unicast* poderá ser utilizada para formar o endereço *multicast*. Vejamos um exemplo:

Dados o prefixo *multicast* FF30::/12 [com as flags P = 1 e T = 1, resulta no valor 3 (FF3)] e o endereço *unicast* 2001:DB8::/32, o endereço *multicast* gerado é:

FF3E:0020:2001:DB8:0:0:CADE:CAFE

Em que:

- **FF** – Representa um endereço *multicast*. Até esse ponto, temos 8 bits.
- **3** – O próximo item do endereço tem valor 3 e representa as flags P e T iguais a 1. Até esse ponto, temos os 8 bits e os 4 bits, fechando em 12 bits.
- **E** – O item E do endereço representa um endereço *multicast* com escopo global e roteado pela Internet. Até esse ponto, temos os 12 bits mais 4 bits, fechando em 16 bits.
- **00** – Os próximos oito bits são reservados e fixos em 0. Até esse momento, comentamos sobre os primeiros 24 bits do endereço *multicast*.
- **20** – Os próximos oito bits definem o tamanho do campo Prefixo da rede. É definido pela RFC 3306 como plen. Conforme comentado, cada número ou letra utiliza 4 bits. Assim, o valor 2 é representado pelos bits 0010 e o valor 0, pelos bits 0000. Se unirmos esses bits, teremos o byte 00100000, ou seja, teremos o valor decimal 32 (2 elevado a 5, único bit ligado na sequência de bits), utilizado na máscara do endereço *unicast*. Até esse momento, comentamos sobre os primeiros 32 bits do endereço *multicast* .
- **2001:DB8:0:0** – Os próximos 64 bits contêm o endereço IPv6 *unicast* denominado Prefixo da rede na figura 15.9.
- **CADE:CAFE** – Os próximos 32 bits finais definem o grupo *multicast*.

Vejamos um outro exemplo com o endereço *unicast* (3FFE:FFFF:1::/48) sendo mapeado para um endereço *multicast*.

Prefixo *multicast* com escopo link local: FF32:0030:3FFE:FFFF:0001::/96. Nesse exemplo, percebemos que os bits relacionados ao plen ficaram como 30, ou seja, 0011 (3) e 0000 (0). Unindo esses bits, teremos o byte 00110000. Convertendo para decimal, teremos o decimal 48, pois 2 elevado a 5 vale 32 e 2 elevado a 4 vale 16 (esses são os únicos bits ligados no byte). Somando 32 + 16, teremos 48, valor utilizado na máscara do endereço *unicast*.

### 15.4.5 URLs em IPv6

Conforme comentado, a representação de um endereço IPv6 é dividida em oito grupos de 16 bits, separados por “:” e escritos com dígitos hexadecimais. Vejamos um exemplo:

• 2001:0DB8:0000:0000:130F:0000:0000:140B

Na representação de um endereço IPv6, é permitido utilizar caracteres maiúsculos ou minúsculos, omitir os zeros à esquerda e representar os zeros contínuos por ::”. Assim, o endereço anterior poderia ser representado por: 2001:db8:0:0:130f::140b. É importante observar que a representação com a utilização dupla de :: a seguir é inválida: 2001:db8::130f::140b, pois não podemos ter duas vezes os ::.

Conforme conhecido no IPv4, o sinal de : é utilizado para definir a porta TCP ou UDP utilizada na URL. Dessa forma, com o endereço IPv4, quando digitamos *http://186.202.25.177:8080*, acessamos a página da editora Novatec e a aplicação que responde pela porta 8080.

Como o endereço IPv6 utiliza os : pontos para separar o endereço, precisamos ajustar nos *browsers* sua utilização, a fim de não provocar confusão. Para evitar problemas, utilizamos os colchetes ([ ]) para representar um endereço IPv6. Com isso, ao digitar a URL no *browser,* seguiríamos o seguinte modelo: *http://[2804:49c:319:430::100]/index.html* (ex.: site UOL). Caso seja necesário informar uma porta específica, utilizamos: *http://*

*[2804:49c:319:430::100]:80*.

## 15.4.6 Transição do IPv4 para o IPv6

Atualmente, existem três técnicas de transição entre o padrão IPv4 e o IPv6. Vejamos cada uma delas.

A primeira é a pilha dupla que provê o suporte a ambos os protocolos no mesmo equipamento. Neste modelo, todos os equipamentos envolvidos na rede precisam ter suporte a IPv6, o que atualmente está acontecendo de forma lenta. Muitas empresas e clientes residenciais ainda adquirem equipamentos que apenas suportam IPv4. A utilização dessa técnica permite que equipamentos e roteadores estejam equipados com pilhas para ambos os protocolos, tendo a capacidade de enviar e receber os dois pacotes, IPv4 e IPv6. Com isso, um equipamento pilha dupla (IPv6/IPv4), ao enviar pacotes IPv6, se comportará como um equipamento apenas IPv6, e na comunicação com um equipamento IPv4, se comportará apenas como IPv4. Cada equipamento pilha dupla será configurado com pelo menos dois endereços IPs (um de cada pilha) ou, ainda, poderá utilizar mecanismos IPv4, como DHCP para adquirir seu endereço IPv4, ou mecanismos do protocolo IPv6, como autoconfiguração ou DHCPv6 para adquirir seu endereço IPv6. A figura 15.10 apresenta o modelo de referência TCP/IP quando temos pilha dupla.

A segunda técnica é a tradução, dado que temos uma rede somente configurada com IPv6 e o destino na Internet é somente IPv4. Para que ambos possam trocar dados entre si, utilizamos a tradução. Essa técnica permite a comunicação entre equipamentos que somente suportam IPv6 com equipamentos que somente suportam IPv4. Essa técnica utiliza NAT64, definido na RFC 6146 e DNS64, definido na RFC 6147. A figura 15.11 apresenta um exemplo da utilização do NAT64 e DNS64.

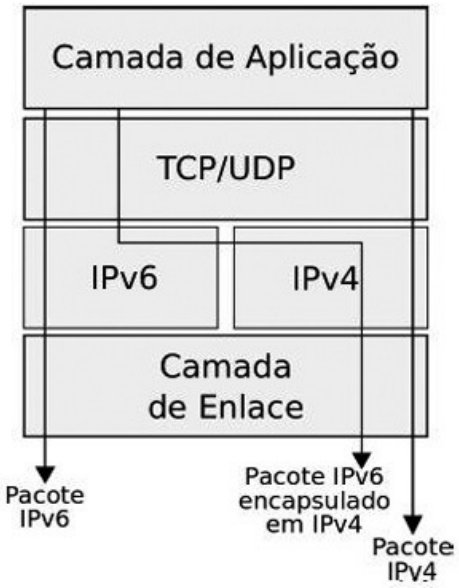



*Figura 15.10 – MR-TCP/IP com pilha dupla.*

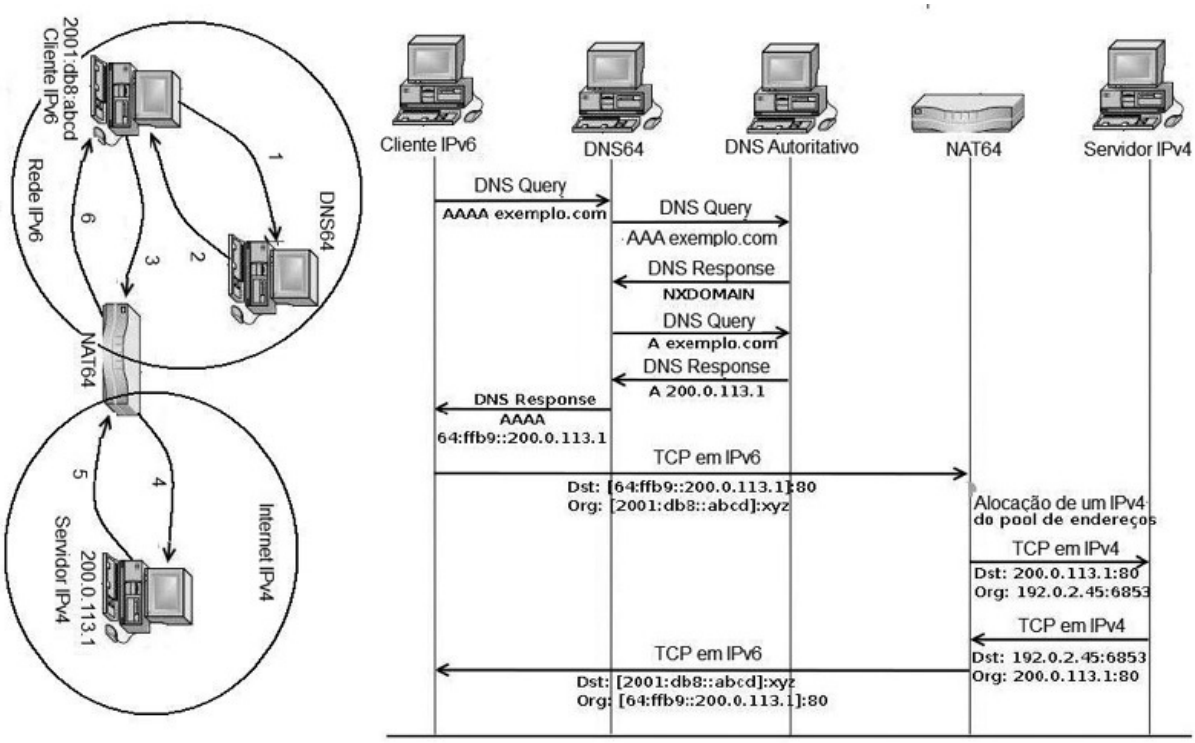



*Figura 15.11 – Uso da técnica de tradução.*

Conforme observado no diagrama de sequência da figura 15.11, verificamos a interação que ocorre para a tradução. O cliente IPv6 inicialmente consulta o servidor DNS64, enviando a URL do equipamento destino. Este, por sua vez, repassa a consulta a um

DNS autoritativo que responderá com o endereço IPv4 do destino consultado. Com posse do endereço informado pelo servidor DNS64, o cliente envia uma consulta ao servidor NAT64, que alocará temporariamente um endereço IPv4 para realizar a comunicação com o destino.

A terceira técnica é o tunelamento. Esta permite o tráfego de pacotes IPv6 sobre a estrutura da rede IPv4 já existente. O tunelamento permite transmitir pacotes IPv6 sobre uma infraestrutura IPv4, sem a necessidade de realizar qualquer mudança nos mecanismos de roteamento, encapsulando o conteúdo do pacote IPv6 em um pacote IPv4. Essa técnica tem sido a mais utilizada na fase inicial de implantação do IPv6, por ser facilmente aplicada. A figura 15.12 apresenta um exemplo de uma rede com tunelamento IPv6 sobre IPv4.

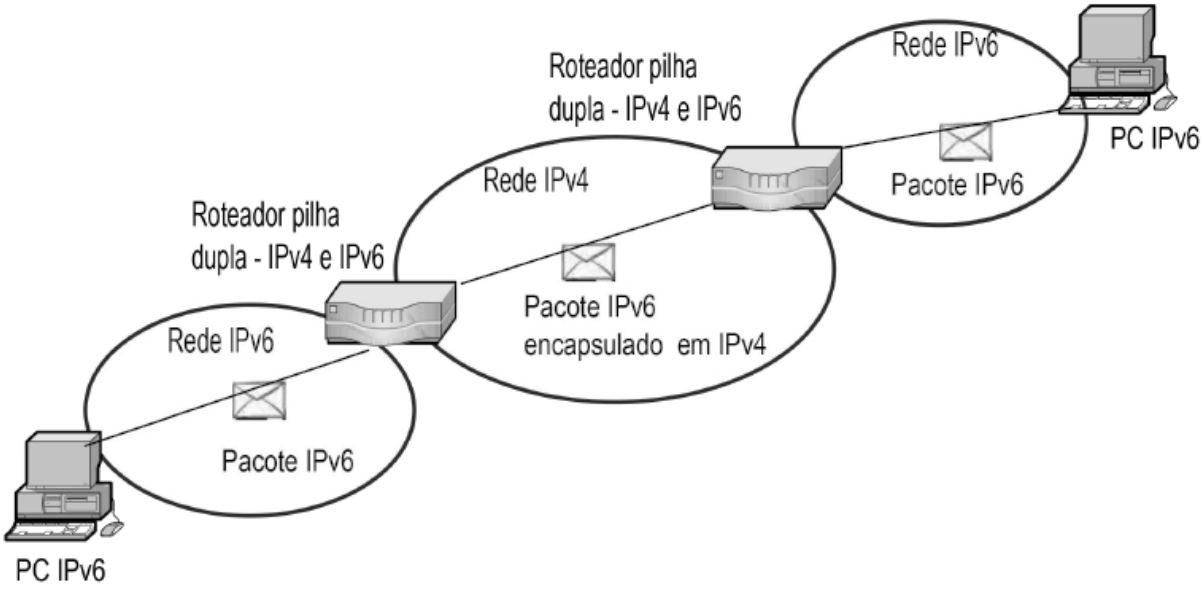



*Figura 15.12 – Rede com tunelamento.*

A seguir, apresentaremos as técnicas de tunelamento mais utilizadas atualmente.

### 15.4.6.1 ISATAP

O ISATAP (*Intra-Site Automatic Tunnel Addressing Protocol*) é um túnel automático IPv6 sobre IPv4 para ser usado dentro das corporações. É importante observar que essa técnica não funciona por meio da

Internet. Definida pela RFC 5214, representa um protocolo de encapsulamento que permite a uma rede com um equipamento IPv6 se comunicar com um equipamento em uma rede IPv4, por meio de um roteador ISATAP, ou seja, permite que equipamentos IPv4 e IPv6 se comuniquem utilizando uma conversão de endereços entre o IPv4 e o IPv6. Essa técnica foi desenvolvida para transportar pacotes IPv6 dentro de redes em que a estrutura IPv6 nativa não se encontra disponível. Por exemplo, quando um equipamento IPv6 for criado para testes. O ISATAP permite que um equipamento IPv6 acesse um equipamento IPv4 cruzando por um roteador configurado com pilha dupla. A figura 15.13 apresenta um exemplo de uma rede que utiliza ISATAP.

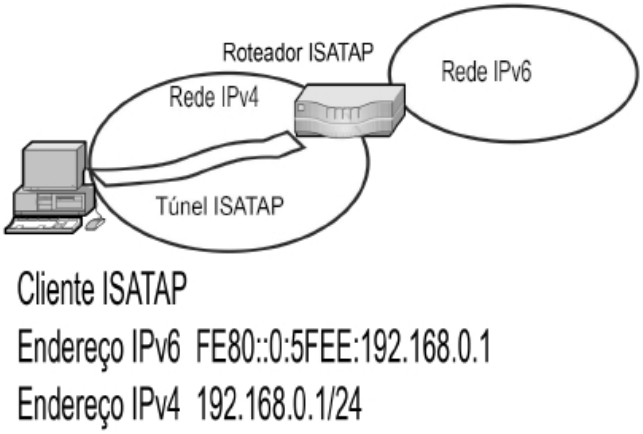



*Figura 15.13 – Rede com tunelamento ISATAP.*

Em um túnel ISATAP os endereços IPv4 dos clientes e roteadores são utilizados como parte dos endereços ISATAP, permitindo a um equipamento determinar facilmente os pontos de entrada e saída dos túneis IPv6, sem utilizar nenhum protocolo ou recurso auxiliar. A figura 15.14 apresenta o formato do endereço ISATAP:

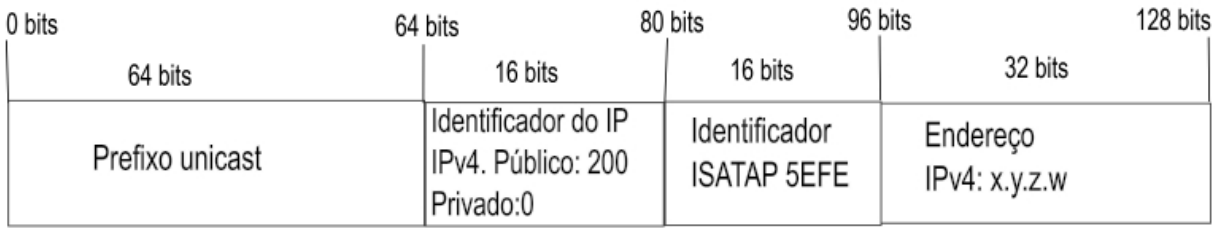


*Figura 15.14 – Formato do endereço ISATAP.*

Conforme observado na figura 15.14, o endereço IPv6 é formado por:

- **Prefixo** *unicast* – É qualquer prefixo *unicast* válido em IPv6, que pode ser link-local (FE80::/64) ou *unicast* global.
- **ID IPv4 público ou privado** – Caso o endereço IPv4 seja público, este campo deve ter o valor 200. Caso seja um endereço IP privado (ex.: 10.0.0.0/8, 172.16.0.0/16 ou 192.168.0.0/24), o valor do campo será 0000.
- **ID ISATAP** – Sempre tem o valor hexadecimal 5EFE.
- **Endereço IPv4** – É o IPv4 do cliente ou roteador em formato IPv4.

### 15.4.6.2 6to4

O 6to4 (RFC 3056) é umas das técnicas de transição mais antigas em uso e que inspirou a criação do 6rd. O objetivo dos túneis 6to4 é permitir que uma rede IPv6 isolada troque pacotes com outra rede IPv6 isolada por meio de uma rede intermediária configurada com IPv4. Um túnel 6to4 pode ser configurado manual ou automaticamente. No caso do uso de túneis automáticos, a comunicação entre as redes IPv6 será ponto a multiponto, enquanto com a configuração manual teremos túneis ponto a ponto. O prefixo IPv6 utilizado para a configuração de túneis 6to4 é 2002::/16. Quando utilizamos a técnica 6to4, os endereços IPv6 possuem uma formação específica, conforme apresentado na figura 15.15.

| 16 bits | 32 bits | 16 bits | 64 bits |
|---|---|---|---|
| 2002 | C8C0:B402 | ID da Subrede | ID da Interface |

*Figura 15.15 – Formato do endereço IPv6 quando usado em túnel 6to4.*

Conforme podemos observar na figura 15.15, temos que:

- A primeira parte do endereço IPv6 possui o prefixo 2002 (definido pela IANA).
- Os próximos 32 bits representam o endereço IPv4 público do cliente, convertido em formato hexadecimal.

- Os próximos 16 bits podem ser utilizados para segmentar a rede IPv6 com túnel 6to4 em até 2 elevado a 16 redes diferentes.
- O ID da interface, que compõe os últimos 32 bits, pode ser igual ao segundo campo, ou seja, poderá ser utilizado o próprio endereço IPv4 do cliente. Essa última parte poderá ainda ser definida por um número sequencial, como 1, 2, 3, 4 ou outro que seja válido.

Vejamos um exemplo da formação de um endereço 6to4:

Dados o endereço IPv4: 200.192.180.002 e o prefixo IPv6 2002::/16.

Primeiramente, convertemos cada número decimal do endereço IPv4 em hexadecimal:

- 200=C8
- 192=C0
- 180=B4
- 002=02

Com isso, o endereço IPv4 convertido será C8C0:B402. O endereço IPv6 utilizado no túnel 6to4 será 2002:C8C0:B402:1::1/64.

Como outro exemplo de conversão de endereço IP para hexadecimal, temos o endereço IP 198.51.100.17. Em hexadecimal, ficará C633 6411. Esse endereço no túnel 6to4 será 2002:C633:6411:1::1/64.

Nessa técnica de tunelamento, o tráfego nas redes LANs utiliza somente o protocolo IPv6 e a comunicação entre as redes LANs IPv6 segue por uma rede IPv4.

Conforme comentado, a técnica 6to4 oferece um tunelamento entre duas redes IPv6 sobre uma rede IPv4. Essa técnica é a mais eficaz depois da técnica de pilha dupla. A figura 15.16 apresenta um exemplo de uma rede com tunelamento 6to4.

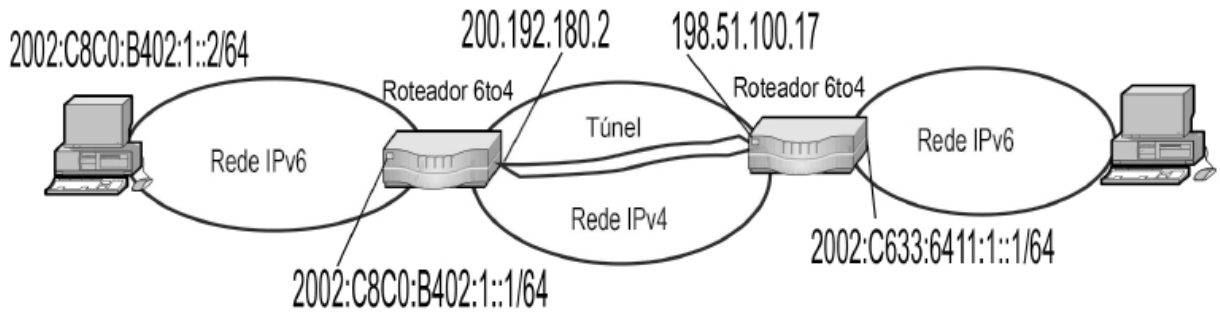



*Figura 15.16 – Rede com túnel 6to4.*

Conforme podemos observar na figura 15.16, as redes das extremidades possuem seus equipamentos configurados com IPv6. Parte do endereço IPv6 utilizado em cada roteador e nos equipamentos é formada pelo endereço IPv4 das interfaces do roteador que realiza o otúnel 6to4. No caso do roteador que conecta as redes, deverá possui endereços IPv4 e IPv6, a fim de garantir que as redes consigam trocar dados entre si. Na rede IPv4, os pacotes IPv6 serão encapsulados em pacotes IPv4 e, após alcançarem seu destino, serão desencapculados e processados pelo destino como IPv6.

Para configurar um túnel 6to4, criamos uma interface tunel no roteador, adicionamos um endereço IPv6 com prefixo 2002::/16, como também criamos uma rota estática para qualquer pacote recebido com destino a 2002::/16, que deverá ser repassado à interface túnel. É importante observar que o endereço IPv6 registrado para a interface túnel deverá ser composto do endereço IPv4 utilizado para configurar a interface do roteador. O modo de configuração seguirá as premissas comentadas, porém a sequência e o formato dos comandos poderão variar de fabricante (ex.: Huawei, Cisco ou Juniper).

### 15.4.6.3 6rd – IPv6 Rapid Deployment

O 6rd tem o objetivo de permitir ao usuário final ter conexão com as redes IPv6, apesar de a rede da operadora continuar funcionando em IPv4. Esse tipo de técnica permite que os provedores utilizem a infraestrutura IPv4 já existente para fazer uma implantação rápida do IPv6. O 6rd (RFC5569) é uma extensão da técnica 6to4. A figura

15.17 apresenta uma arquitetura de rede em que podemos utilizar o 6rd.

Essa técnica de túnel segue o mesmo conceito dos túneis 6to4, porém não é necessário utilizar um prefixo fixo como ocorre com a técnica 6to4 (2002::/16). Outra diferença é que na formação do endereço IPv6 da interface tunel não é obrigatório utilizar os 32 bits do endereço IPv4 configurado no roteador.

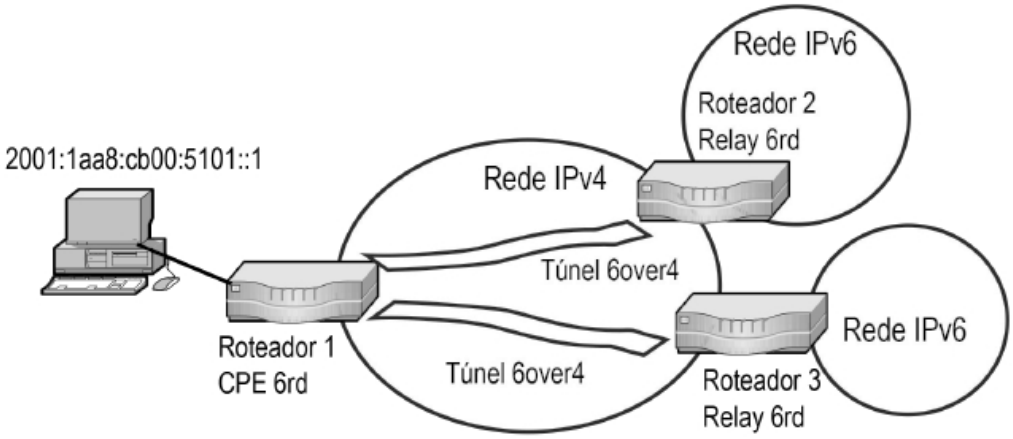



*Figura 15.17 – Rede com túnel 6rd.*

Conforme podemos observar na figura 15.17, temos dois importantes componentes que precisam ser configurados para que o túnel 6rd possa ser utilizado:

- CPE 6rd – Instalado como interface entre a rede da operadora e do usuário.
- *Relay* 6rd – Instalado na interface entre a rede IPv4 da operadora e a Internet IPv6.

O CPE 6rd é um CPE tradicional, como ONU GPON, modem xDSL, cable modem, modem 3G/4G, entre outros. Todos esses equipamentos precisam suportar o uso de túneis 6rd. O CPE 6rd atribui ao cliente um endereço IPv4, como também um endereço IPv6. Esse endereço IPv6 é um endereço IPv6 público válido, mas é construído de maneira específica para que o relay 6rd identifique-o como um endereço 6rd.

O *relay* 6rd é um equipamento que vai encapsular e desencapsular pacotes para trafegarem corretamente nas redes IPv4 e IPv6.

Ambos os equipamentos precisam de configuração específica que dependerá do fabricante.

### 15.4.6.4 IPv4 encapsulado em IPv6

Com as técnicas de tradução atualmente disponíveis, será possível utilizar um roteamento transparente na comunicação entre equipamentos que apresentem suporte apenas a uma versão do protocolo IP ou, ainda, os que utilizem pilha dupla (suporte a IPv4 e IPv6).

A migração do protocolo IPv4 para IPv6 deverá ocorrer de maneira gradual. Para essa migração ocorrer de forma organizada, foram implementados no protocolo IPv6 dois tipos de endereços especiais que podem encapsular os endereços IPv4. Esses endereços possuem seus primeiros 80 bits setados com zeros e os 32 bits finais contêm um endereço no formato IPv4. Os próximos 16 bits do endereço IPv6 indicarão o tipo de endereço utilizado. Quando esses 16 bits estiverem setados com zeros, significará que o endereço é compatível com protocolo IPv4. Quando os 16 bits estiverem setador com 1 (ex.:FFFF), significará que o endereço é do tipo IPv4 mapeado em endereço IPv6. A figura 15.18 apresenta os formatos comentados.

| 80 bits | 16 bits | 32 bits |
|---|---|---|
| 0000.....0000 | 0 | IPv4 |

Endereço IPv6 do Tipo *Compatível-IPv4*

| 80 bits | 16 bits | 32 bits |
|---|---|---|
| 0000.....0000 | FFFF | IPv4 |

Endereço IPv6 do tipo IPv4 Mapeado em IPv6

*Figura 15.18 – Endereço IPV4 encapsulado em IPv6.*

Os endereços compatíveis (*IPv4-Compatible IPv6 address*) estão obsoletos conforme a RFC 4291. Atualmente, o modelo utilizado é o endereço IPv4 mapeado em IPv6 (*IPv4-Mapped IPv6 Address*). Vejamos um exemplo e um endereço IPv4 mapeado em IPv6: ::FFFF:129.144.52.38.

## 15.4.7 Formato do pacote IPv6 em relação ao IPv4

Com o advento da nova versão do protocolo IP, o formato do pacote sofreu vários ajustes. A seguir, apresentaremos os campos que mudaram de nome, como também alguns novos campos que foram incluídos e outros que foram removidos em relação à versão anterior. A figura 15.19 apresenta o formato do pacote IPv4 e a figura 15.20, o formato do pacote IPv6.

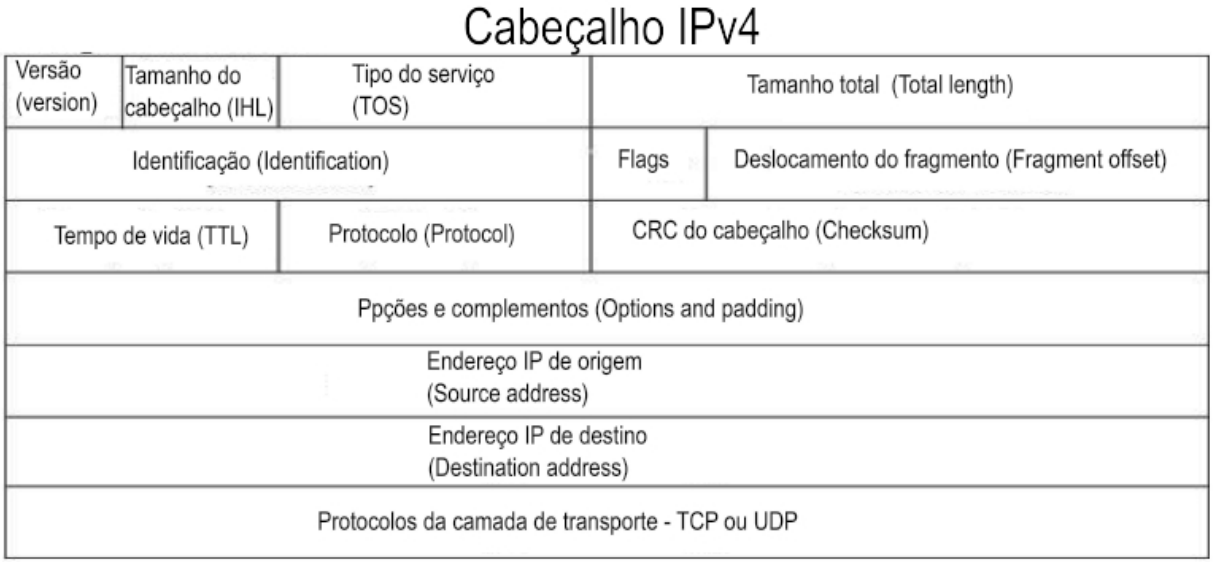



*Figura 15.19 – Formato do pacote IPv4.*

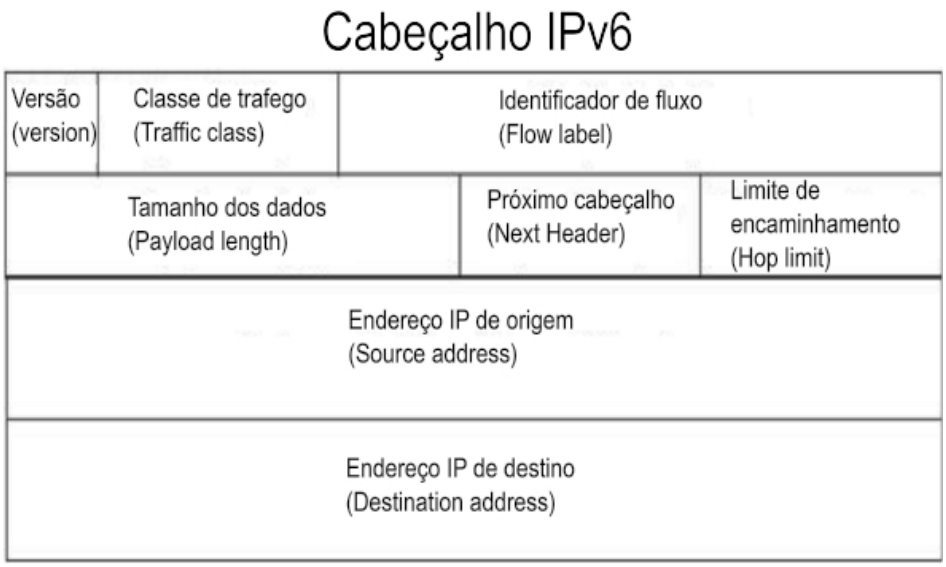



*Figura 15.20 – Formato do pacote IPv6.*

Inicialmente, apresentaremos o formato do pacote IPv4 e, em

seguida, o formato do pacote IPv6, realçando as diferenças entre as duas versões.

### 15.4.7.1 Formato do pacote IPv4

O cabeçalho IPv4, apresentado na figura 15.19, é composto de 12 campos fixos, que podem ou não ser preenchidos. Desta forma, o tamanho do pacote IP poderá variar entre 20 e 60 bytes. Esses campos são destinados a transmitir as características do pacote IP. A seguir, apresentaremos em detalhes os campos do pacote do protocolo IPv4.

- **Versão** – Informa a versão do protocolo a que o pacote pertence. A versão 4 possui tamanho de 4 bits (0100).
- **Tamanho do cabeçalho do pacote IP** (IHL – *Internet Header Length*) – Especifica o tamanho do cabeçalho do pacote. Possui o tamanho de 4 bits. Nesses 4 bits, registra-se o tamanho em bytes do pacote IPv4, em unidades de 4 bytes cada uma. Vejamos um exemplo: caso o tamanho do pacote seja de 20 bytes, o campo IHL conterá o número 5, pois 5 vezes 4 (unidade utilizada por esse campo) resulta em 20. Caso o tamanho do pacote seja de 60 bytes, o campo IHL conterá o número 15 (máximo número decimal possível em ser apresentado com os 4 bits deste campo), pois 15 vezes 4 (unidade utilizada por esse campo) resulta em 60 bytes. É importante observar que o campo tamanho foi removido do pacote IPv6 devido a IPv6 definir esse valor com valor fixo (40 bytes).
- **Tipo do serviço** (TOS – *Type of Service*) – Composto de 8 bits. Também conhecido atualmente pelo nome de serviços diferenciados, é utilizado para indicar a QoS (*Quality of Service* – Qualidade de Serviço) desejada. Seus bits caracterizam os serviços escolhidos para serem considerados pelos roteadores para processar o pacote, como a precedência de um pacote. Um roteador pode, em situações de grande congestionamento, por exemplo, aceitar somente pacotes com um certo nível mínimo de precedência. Geralmente, desejam-se reduzido atraso, alta confiabilidade e alto throughput (vazão). A figura 15.21 apresenta o formato do campo TOS.


*Figura 15.21 – Formato do campo TOS.*

Veja na tabela 15.4 os detalhes do campo TOS. Os bits seguem a estrutura apresentado na figura 15.21.

*Tabela 15.4 – Combinação entre os bits do campo TOS*

| **Bits** | **Descrição** | **Valores – Combinação possível entre os 3 bits** | |
|---|---|---|---|
| 0 1 2 | Precedência | 000: Routine (Rotina)<br>001: Priority (Prioridade)<br>010: Immediate (Imediato)<br>011: Flash (Relâmpago)<br>100: Flash Override (Relâmpago Precedente) | 101: Critic/ECP (Crítico)<br>110: Internetwork Control (Controle entre Redes)<br>111: Network Control (Controle de Rede) |
| 3 | D (Delay – Atraso) | 0: Atraso normal.<br>1: Atraso baixo. | |
| 4 | T (Throughput – Vazão) | 0: Vazão normal.<br>1: Alta vazão. | |
| 5 | R (Relibility – Confiabilidade) | 0: Confiabilidade normal.<br>1: Alta confiabilidade. | |
| 6 7 | Reservados | Obrigatoriamente 00. | |

- **Tamanho total** (*Total length*) – Representa o comprimento total do pacote IP, medido em quantidade de bytes (8 bits). O tamanho total inclui o cabeçalho do pacote e também os dados gerados pela camada de transporte. O tamanho do campo é de 16 bits, o que permite que o tamanho total do pacote chegue a 65.536 bytes ou 64 Kbytes. Entretanto, atualmente esse tamanho de pacote não pode ser transportado entre os roteadores conectados às redes.

  Atualmente, em uma rede Ethernet o tamanho dos quadros transmitidos fica em torno de 1.518 bytes. O limite de 1.518 bytes para o tamanho dos quadros foi criado como parte das especificações dos padrões Ethernet que operavam a 10 Mbps em half-duplex (exs.: 10BASE-T, 10BASE-5). A ideia de definir um tamanho relativamente pequeno foi para evitar que quadros muito grandes agravassem os problemas de colisões, que ocorriam em

redes half-duplex operando com hubs. Um quadro grande poderia ainda permitir que um único equipamento utilizasse o cabo durante um tempo muito longo, tornando o compartilhamento precário, Além disso, quadros maiores demoram mais tempo para serem retransmitidos em caso de perda de dados. O tamanho de 1.518 foi considerado adequado no momento em que foi avaliado.

Atualmente, equipamentos ativos, como roteadores e switches, permitem o transporte de quadros de até 9.000 bytes, chamados de jumboframes. Esse aumento foi possível com o advento das redes que passaram a operar exclusivamente em full-duplex e com velocidades acima de 100 Mbps.

- **Identificação** – Utilizado para permitir que o equipamento de destino determine a qual pacote pertence um fragmento recém-chegado. Todos os fragmentos de um pacote contêm o mesmo valor de identificação. Este campo foi removido do pacote IPv6.
- *Flags* – É formado por três bits, sendo o primeiro reservado e sempre 0. O segundo bit indica se o pacote foi ou não fragmentado. O terceiro bit definido em 1 informa que este não é o último fragmento, ou seja, existem outros fragmentos. Quando definido em 0, significa que esse pacote pode ser o único ou o último de uma cadeia fragmentada. Este campo foi removido do pacote IPv6.
- **Deslocamento do fragmento** – É formado por 13 bits. Um roteador pode precisar fragmentar um pacote ao encaminhá-lo de um meio físico para outro que tenha um MTU menor. Quando ocorre a fragmentação, o pacote IPv4 usa o campo Deslocamento de Fragmento e a flag MF (Mais Fragmentos – terceiro bit do campo flags, comentado) no cabeçalho IP para reconstruir o pacote quando ele chega ao equipamento de destino. O campo deslocamento de fragmento identifica a ordem na qual o fragmento do pacote deve ser colocado na reconstrução, ou seja, determina a posição de um fragmento relativo ao pacote original. Todos os fragmentos de um pacote, com exceção do último, devem ser múltiplos de 8 bytes. Este campo foi removido do pacote IPv6.

  É importante observar que os campos Identificação, Flags e

Deslocamento do fragmento foram removidos do pacote IPv6, porque as informações referentes à fragmentação são indicadas em um cabeçalho de extensão apropriado.

- **Tempo de vida do pacote** (TTL – *Time-to-Live*) – É formado por 8 bits. Este indica o tempo de vida restante do pacote. O valor do TTL é decrementado em uma unidade a cada vez que o pacote é processado por um roteador, ou seja, a cada salto. Quando o valor chega a zero, o roteador descarta o pacote e um novo pacote de advertência é enviado ao equipamento de origem. Esse mecanismo evita que os pacotes que não conseguem chegar a seus destinos sejam encaminhados indefinidamente entre roteadores em um loop de roteamento. Se os loops de roteamento tivessem permissão para continuar, a rede ficaria congestionada com os pacotes de dados que nunca chegariam a seus destinos. O decremento do valor de TTL a cada salto garante que o TTL do pacote chegue a zero, caso viaje sem rumo na rede. Assim, com o campo TTL zerado, o pacote será descartado. Este campo originalmente deveria contar o tempo em segundos, permitindo que um pacote durasse apenas 255 segundos, porém sua utilização foi modificada.
- **Protocolo** – É formado por oito bits. O campo Protocolo possibilita que a camada de rede passe os dados para o protocolo apropriado das camadas superiores. Quando a camada de rede concluir o recebimento de um pacote, precisará repassá-lo ao respectivo protocolo que dará continuidade à requisição realizada. Os códigos de cada protocolo estão listados na página da IANA (*http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xml*). Vejamos alguns exemplos: 01 ICMP, 02 IGMP, 06 TCP, 17 UDP, 89 OSPF, entre outros.
- *Checkcum* (verificação do cabeçalho) – É usado para verificar erros no cabeçalho do pacote. O campo é responsável por detectar inconsistências no pacote IP, realizando uma checagem cíclica de todos os campos do pacote. A intenção é garantir que após percorrer o caminho entre o equipamento origem e destino não exista nenhuma falha. Este campo foi removido do pacote IPv6,

pois esse cálculo ja é realizado pelos protocolos das camadas superiores. Com isso, a velocidade dos roteadores tende a melhorar.

- **Endereço IP origem** – Contém um valor binário de 32 bits que representa o endereço do equipamento de origem do pacote da camada 3.
- **Endereço IP destino** – Contém um valor binário de 32 bits que representa o endereço do equipamento de destino do pacote da camada 3.
- **Opções e complemento** (*padding*) – Campos adicionais ao cabeçalho podem seguir o campo do endereço de destino, mas estes não são normalmente usados. O campo Opções é variável e o campo Complemento é utilizado para fechar os 32 bits caso o campo Opções não o faça. Se faltar para completar os 32 bits, o campo Complemento será preenchido por bits iguais a 0. Dessa forma, com o campo Complemento, garantimos que o cabeçalho do pacote IP seja sempre múltiplo de 32 bits. Este campo foi removido do pacote IPv6, visto que as opções adicionais fazem parte dos cabeçalhos de extensão do IPv6.

### 15.4.7.2 Formato do pacote IPv6

O cabeçalho do pacote IPv6 usa uma estratégia de composição de cabeçalho, ou seja, possui um cabeçalho base com tamanho fixo de 40 bytes distribuídos em 8 campos. Conforme comentado, quando houver necessidade do transporte de informações adicionais, estas serão envolvidas pelos cabeçalhos de extensão. O cabeçalho de base IPv6 é bastante simples e composto dos seguintes campos:

- **Versão (4 bits)** – Versão do pacote IP utilizado. No caso do IPv6, este campo é representado no formato binário pelos bits 0110 (6 em decimal). É utilizado pelos roteadores e demais equipamentos para redirecionar os pacotes IPv6 recebidos para a pilha de protocolos adequada. Equipamentos sem suporte a IPv6 simplesmente descartam os pacotes recebidos, como sendo pertencentes a um protocolo desconhecido.
- **Prioridade (8 bits)** – Ttambém chamado de Classe de Tráfego

(*Traffic Class*). Indica a prioridade com a qual o pacote deve ser tratado pelos roteadores, ou seja, determina a prioridade que um pacote tem. Deve-se utilizar valores de 0 a 7 para dados, que podem sofrer atrasos, e valores de 8 a 15 para aplicações multimídia em tempo real, que não devem sofrer atrasos.

- **Fluxos identificados** (*Flow label*) **(20 bits)** – Identifica, com os campos de endereço de origem e endereço de destino, o fluxo ao qual o pacote pertence. Esse conjunto caracterizado por código do fluxo e os endereços de origem e destino formarão um fluxo com identificação própria que poderá oferecer um QoS específico a um determinado serviço contratado pelo cliente. Esse serviço poderia, por exemplo, ser utilizado para transmitir dados em tempo real, como HD TV. Podemos dizer que o campo Flow Label permite que dois equipamentos IPv6 estabeleçam uma pseudoconexão com características próprias, possibilitando um tratamento diferenciado para diferentes fluxos. Esse novo campo cria a possibilidade de identificar o tipo de tráfego transportado ao nível da camada de rede. Apesar de ainda não o termos utilizado na prática, permite um grande avanço no quesito QoS, sendo tratado pela camada de rede.
- **Tamanho do** *Payload* **(16 bits)** – Tamanho, em bytes, do restante do pacote, após o cabeçalho-padrão. Esse campo indica quantos bytes seguem o cabeçalho-padrão (formado pelos primeiros 40 bytes). De forma similar ao IPv4, o tamanho máximo de um pacote IPv6 é 64 Kbytes.
- **Próximo cabeçalho** (*Next Header*) **(8 bits)** – Indica o tipo do possível cabeçalho de extensão que segue o cabaçalho IPv6 (Figura 15.22). Caso não seja utilizado cabeçalho de extensão, este campo indica a qual protocolo de transporte o pacote deve ser repassado. Este campo tem significado similar ao do campo *Protocol Type* (tipo de protocolo) do IPv4. É utilizado para identificar qual cabeçalho seguirá ao cabeçalho-padrão. Esse campo pode utilizar os códigos da IANA para protocolos conhecidos, como 01 ICMP, 02 IGMP, 06 TCP, 17 UDP, 89 OSPF, entre outros apresentados, mas também poderá utilizar os novos códigos

criados para os cabeçalhos de extensão do IPv6.

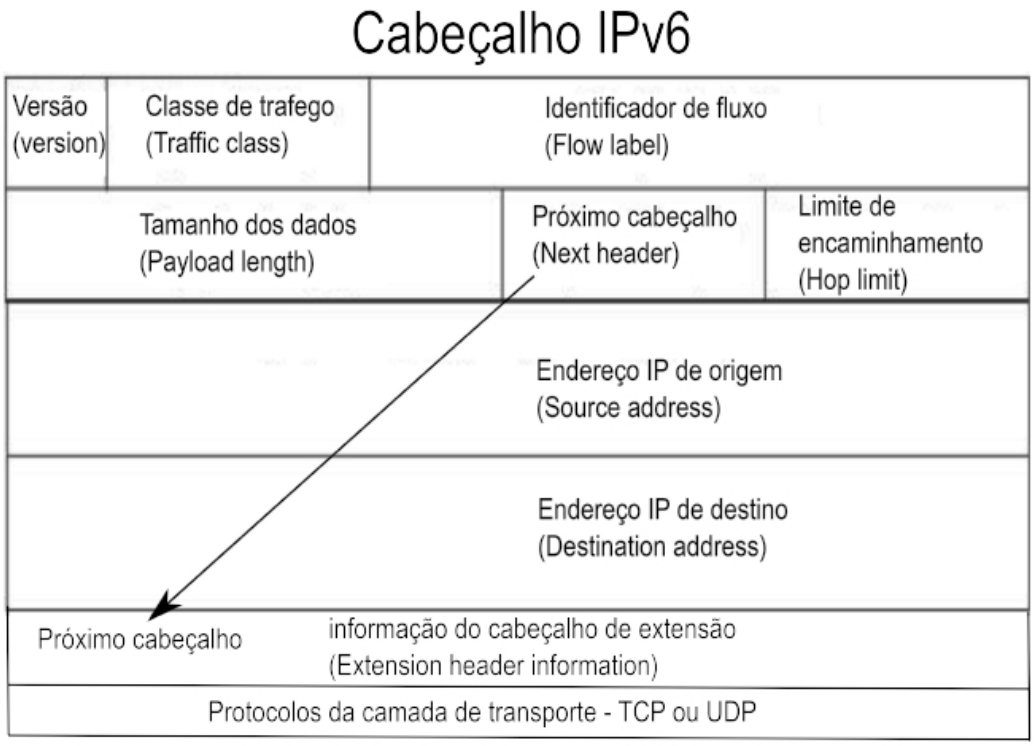



*Figura 15.22 – Formato do pacote IPv6 com ênfase no campo next header.*

- *Hop Limit* **(8 bits)** – Equivale ao campo *Time to Live* (TTL) da versão IPv4. O novo termo é mais adequado, uma vez que o TTL nunca foi medido em tempo, mas sim em número de saltos. O número máximo de saltos em uma rede IPv6 está limitado a 256 saltos (0 a 255), da mesma forma que ocorria na rede IPv4.
- **Endereço de origem (128 bits)** – Endereço IPv6 do equipamento que atua como o remetente dos dados.
- **Endereço de destino (128 bits)** – Endereço IPv6 do equipamento que atua como o receptor dos dados.

### 15.4.7.3 Cabeçalhos de extensão do pacote IPv6

Diferentemente do protocolo IPv4, que inclui no cabeçalho base todas as informações opcionais, o protocolo IPv6 trata as informações opcionais por meio de cabeçalhos de extensão. A definição dos cabeçalhos de extensão foi registrada na RFC 2460. Tais cabeçalhos localizam-se entre o cabeçalho-padrão e o

cabeçalho da camada imediatamente acima (camada de transporte), não havendo nem quantidade, nem tamanho fixo para eles. Caso existam múltiplos cabeçalhos de extensão no mesmo pacote, estes serão adicionados em série.

Conforme comentado, um pacote IPv6 possui uma parte-padrão composta de 40 bytes. Essa parte do pacote inclui apenas as informações básicas para que o pacote possa trafegar pela rede. Entretanto, neste protocolo, todas as informações opcionais são tratadas em cabeçalhos de extensão, ou seja, um transmissor pode optar por escolher quais cabeçalhos de extensão incluirá num determinado pacote e ainda quais omitirá. Assim, os cabeçalhos de extensão fornecem flexibilidade máxima. Outra vantagem oferecida por essa arquitetura é a melhora de velocidade de processamento nos roteadores, uma vez que único cabeçalho de extensão IPv6 processado em cada roteador é o *Hop-by-Hop*. No IPv4, cada opção do pacote é tratada como uma opção salto a salto, causando, assim, diminuição na performance da rede por ter que ser processado em cada roteador intermediário, mesmo não pertencendo a esses roteadores.

É importante observar que os demais pacotes de extensão são tratados apenas pelo nó identificado no campo endereço de destino do cabeçalho base. Além disso, novos cabeçalhos de extensão podem ser definidos e usados sem a necessidade de se alterar o cabeçalho base. Atualmente, o protocolo IPv6 define seis cabeçalhos de extensão conhecidos por:

- *Hop-by-Hop Options* – Identificado pelo valor 0 no campo próximo cabeçalho. Essa extensão permite transportar informações que serão examinadas por cada equipamento ao longo do caminho do pacote. Atualmente, existem dois tipos definidos para o cabeçalho *Hop-by-Hop*: O *Router Alert* e o Jumbograma. O pacote *Router Alert* é utilizado para informar aos equipamentos intermediários que a mensagem a ser encaminhada exige tratamento especial. Essa opção é utilizada pelos protocolos MLD (*Multicast Listener Discovery*) e RSVP (*Resource Reservation Protocol*). O segundo pacote de extensão é o Jumbograma. Esse pacote de extensão é utilizado

para informar a todos os equipamentos do caminho que o tamanho do pacote IPv6 é maior do que 64 KBytes.

- *Destination Options* – Identificado pelo valor 60 no campo próximo cabeçalho. Essa extensão permite transportar informação opcional que deverá ser examinada apenas pelo último equipamento. A RFC 3775 apresenta os detalhes sobre o suporte à mobildiade do protocolo IPv6 e o pacote de extensão comentado.
- *Routing* (Encaminhamento) – Identificado pelo valor 43 no campo próximo cabeçalho. Essa extensão foi inicialmente utilizada para permitir que o emissor do pacote IPv6 possa registrar uma lista de um ou mais equipamentos intermerdiários que deverão ser visitados até o pacote chegar ao destino. Por questões de segurança, a RFC 5095 tornou esse modo de uso obsoleto. Atualmente, utiliza-se esse pacote de extensão como parte do mecanismo de suporte à mobilidade do IPv6. A RFC 3775 apresenta os detalhes sobre o suporte à mobilidade do protocolo IPv6.
- *Fragmentation* – Identificado pelo valor 44 no campo próximo cabeçalho de extensão. Essa extensão é utilizada quando o pacote IPv6 a ser enviado for maior que o MTU do caminho.
- *Authentication Header* – Identificado pelo valor 51 no campo próximo cabeçalho. Utilizado pelo protocolo IPSec para prover autenticação e garantia de integridade aos pacotes IPv6. Este cabeçalho é idêntico ao utilizado no IPv4.
- *Encapsulating Security Payload* – Identificado pelo valor 50 no campo próximo cabeçalho. É também utilizado pelo protocolo IPSec para garantir integridade e confidencialidade dos pacotes.

## 15.5 Exercícios do capítulo 15

1. Descreva as vantagens oferecidas pelo protocolo IPv6 em relação ao protocolo IPv4.
2. Qual a diferença entre um endereço *multicast* e um *broadcast*?
3. A versão do protocolo IP mais utilizada é o IPv4. A nova versão tem como objetivo:

a) Aumento do tamanho dos pacotes transportados pela rede.

b) Aumento da quantidade de pacotes transportados pela rede.

c) Aumento do tipo e da variedade dos pacotes transportados na rede.

d) Necessidade do aumento da capacidade de endereçamento.

4. Quantos bits formam cada uma das oito partes de um endereço IPv6?

a) 24.

b) 4.

c) 3.

d) 16.

5. O protocolo IPv6 permite encapsular pacotes IPv6 dentro de pacote IPv4. Esse mecanismo é chamado de:

a) tunneling.

b) hashing.

c) routing.

d) NAT.

6. O protocolo IPv6 foi designado para substituir o protocolo IPv4. Isso ocorreu em razão de os endereços IPv4 estarem se esgotando. Qual das seguintes sentenças é verdadeira em relação ao protocolo IPv6?

a) A estrutura de endereções não é hierárquica.

b) Pacotes de *broadcasts* foram eliminados e substituídos pelos pacotes de *multicast*.

c) Existem 3,4 bilhões de endereço IPv disponíveis.

d) Uma interface poderá apenas ser configurada com um endereço IPv6.

7. Quais declarações são verdadeiras sobre a representação de um endereço IPv6? (escolha duas):

a) Os primeiros 64 bits são formados pelo método EUI-64.

b) Uma única interface de um equipamento IPv6 pode receber mais

de um endereço IP.

c) Os últimos 64 bits podem ser formados pelo método EUI-64.

d) Um endereço IPv6 somente utiliza caracteres decimais.

8. Marque as opções que sejam mecanismos de transição IPv6 (escolha três):

a) Túnel 6to4.

b) Túnel GREEN.

c) Túnel ISATAP.

d) Túnel 6rd.

e) Túnel VPN.

f) Túnel PPP.

9. Quais das opções são corretas em relação a um endereço *unicast*? (escolha duas):

a) Endereço *unicast* global inicia com 2000::/3.

b) Endereço link-local inicia com FAB0::/10.

c) Endereço link-local inicia com FE00:/12.

d) Endereço de loopback é igual a ::1.

10. Selecione os endereços IPv6 válidos:

a) ::192:168:0:1.

b) 2002:c0a8:101::42.

c) 2003:dead:baaf:4dad:23:46:bb:101.

d) ::1.

e) 2000::.

f) 2001:3452:4952:2837::1.

11. Qual é o endereço *multicast* processado somente pelos roteadores muticast?

a) FF02::4.

b) FF02::3.

c) FF02::2.

d) FF02::1.

12. Qual é o endereço IP *multicast* utilizado pelo protocolo RIP para divulgar suas rotas?

CAPÍTULO 16

# Comunicação sem fio

Neste capítulo, abordaremos a tecnologia de transmissão de dados sem fio, também conhecida como redes *wireless*. Serão apresentadas as topologias de rede sem fio, o padrão 802.11 e suas variações, além da tecnologia bluetooth.

## 16.1 Introdução

O termo *wireless*, que significa sem fio, possui alguns sinônimos que serão apresentados antes das características das redes sem fio. Entre esses sinônimos, temos comunicação sem fio, computação móvel e redes de computadores sem fio.

A comunicação sem fio baseia-se no estabelecimento da comunicação por meio do ar, ou seja, utiliza o espaço como meio de transporte. Um exemplo desse tipo de transmissão é a comunicação via rádios AM e FM e a própria televisão. A comunicação sem fio é considerada o suporte para a computação móvel, a qual se encarrega das transmissões de dados entre computadores, sem o uso de fios e em movimento.

As redes sem fio (*wireless*) possuem como objetivo a conexão entre diferentes pontos com alta taxa de transmissão sem a necessidade do uso de cabos metálicos (telefonia e TV a cabo) ou cabos de fibras ópticas. Redes sem fio transmitem e recebem dados sobre o ar, combinando conectividade dos dados e mobilidade do usuário. Como meio de transmissão, as redes sem fio utilizam as seguintes tecnologias: spread spectrum, infravermelho ou micro-ondas.

Em redes sem fio que utilizam infravermelho, uma célula individual (notebook, notepad) de uma LAN é limitada a uma simples sala, pois a luz infravermelha não penetra em paredes. As demais redes (*spread spectrum* e micro-onda) utilizam o rádio para transmitir dados, e, de forma geral, as redes spread spectrum alcançam distâncias maiores e atuam em frequências mais baixas quando comparadas

com as redes que utilizam micro-ondas.

Como acontece com as redes com cabos metálicos, nas sem fio existem redes LAN e WAN. As redes LANs sem fio (WLAN – *Wireless Local Area Network*) interconectam equipamentos em uma área restrita, com o objetivo de permitir o compartilhamento de recursos de hardware e software. As WAN sem fio (WWAN – *Wireless Wide Área Network*) estão baseadas na tecnologia da telefonia celular, que foi inicialmente desenvolvida para a comunicação de voz e permite a transmissão de dados e imagem.

Uma rede WLAN pode ser usada como ampliação de uma rede com fios para computadores portáteis, como notepads, notebooks ou palmtops. O equipamento móvel sem fio poderá estar em qualquer lugar dentro da empresa ou fora dela (respeitando os limites de alcance), bastando apenas que o equipamento consiga comunicar-se com algum ponto de acesso. Os pontos de acesso possuem como objetivo a interligação entre os equipamentos móveis e a interligação dos equipamentos móveis com a rede cabeada.

## 16.2 Origem das redes sem fio

O primeiro sistema de computadores que empregou as técnicas de radiodifusão em vez de cabos ponto a ponto foi o sistema aloha, na década de 1970. Naquela época, as linhas telefônicas disponíveis eram caras e de péssima qualidade, não oferecendo confiabilidade na transmissão de dados. Entretanto, a necessidade de interligação girava em torno da ligação de sub-redes de universidades (separadas em blocos) aos equipamentos ativos centrais, pois a origem e o destino não estavam muito distantes.

Quando surgiu, o sistema aloha transmitia dados a 9.600 bps, utilizando transmissores e receptores de rádio FM. Nesse sistema, quando tem dados a enviar, uma estação simplesmente faz a transmissão. Se receber os dados corretamente, o ponto central enviará uma mensagem de confirmação para a estação; se não receber tal confirmação dentro de um intervalo de tempo predefinido, a estação fará a retransmissão dos dados.

A largura de banda oferecida pela rede aloha (9.600 bps) limitava a transmissão de dados e vídeo, motivo pelo qual a utilização das redes sem fio não foi amplamente utilizada. Entretanto, com os avanços tecnológicos (miniaturização dos componentes eletrônicos e de comunicações pessoais sem fio), as redes puderam oferecer aos usuários maior qualidade e facilidade de implementação. Devido aos avanços da indústria, foi solicitada ao IEEE a elaboração de padrões a fim de garantir a interoperabilidade entre os equipamentos de redes sem fio. Como resultado do trabalho do IEEE, criou-se o grupo de trabalho 802.11, cujo objetivo consistiu em definir uma especificação para conectividade sem fio entre estações de uma rede local.

## 16.3 Topologia das redes sem fio

As redes sem fio 802.11 podem apresentar-se fisicamente de dois modos: cliente-servidor (infraestrutura) e modo *ad-hoc*.

### 16.3.1 Infraestruturada ou cliente/servidor

As redes cliente/servidor caracterizam-se por possuir dois tipos de elementos: as estações móveis (p. ex., notebook, celular, palm top) e os pontos de acesso. Cada ponto de acesso é responsável pela conexão das estações móveis de uma área de cobertura com a rede cabeada. Esses pontos de acesso desempenham tarefas importantes na coordenação das estações móveis, como aceitar ou não a inserção de uma nova estação à rede, colher estatísticas para melhor gerenciamento do canal e ajudar a definir quando uma estação deve ou não ser controlada por outro ponto de acesso. A figura 16.1 representa uma rede formada na topologia cliente-servidor.

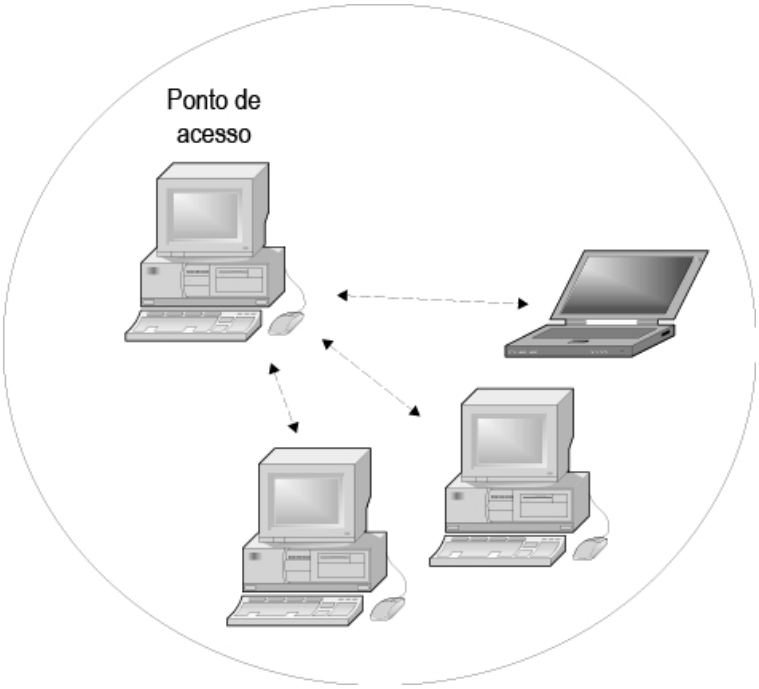



*Figura 16.1 – Rede sem fio na topologia cliente-servidor.*

## 16.3.2 Ad-hoc

Essa topologia caracteriza-se por formar redes simples, em que as comunicações são estabelecidas entre múltiplas estações em uma certa área de cobertura, sem o uso de um ponto de acesso ao servidor.

O padrão especifica os critérios que cada estação deve observar, de modo que todos tenham acesso ao meio sem fio. Um exemplo é a reunião de um grupo de empregados na empresa ou no próprio cliente, em que cada um possui um notebook ou um laptop. Os empregados conectam seus computadores em uma rede temporária e permanecem conectados somente durante o período da reunião. Em uma rede do tipo *ad-hoc*, qualquer um dos equipamentos envolvidos poderá assumir o papel de um roteador e compartilhar o acesso à Internet com os demais equipamentos.

As duas topologias possuem equipamentos padronizados pelo IEEE sob a norma 802.11. A figura 16.2 representa uma rede formada na topologia *ad-hoc*:

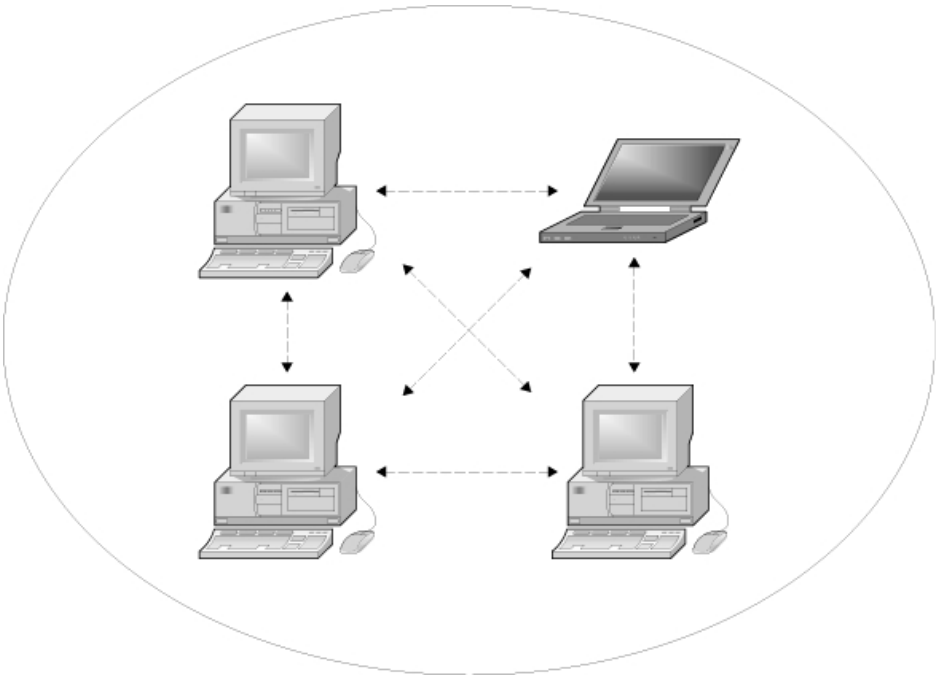


*Figura 16.2 – Rede sem fio na topologia ad-hoc.*

Na topologia cliente/servidor, todo tráfego da rede passa pelo ponto de acesso sem fio, ao passo que na topologia *ad-hoc*, os computadores trocam dados diretamente entre si.

## 16.4 O padrão 802.11

O padrão 802.11 refere-se a uma família de especificações desenvolvidas pelo IEEE para redes sem fio (*wireless*). Seu objetivo é padronizar os equipamentos de redes sem fio, a fim de evitar que cada fabricante produza um equipamento diferente, o que gera incompatibilidade. A especificação do padrão 802.11 foi aceita em 1997 e define uma interface entre um computador sem fio e o seu ponto de acesso, e entre dois computadores sem fio. Fazendo uma analogia com o modelo de referência OSI, o padrão 802.11 define a camada de controle de acesso ao meio (MAC) para transmissões de dados em redes sem fio. Isso quer dizer que a camada LLC não muda, ou seja, esse padrão torna a comunicação transparente para as camadas superiores.

Assim como no padrão Ethernet (802.3), o padrão 802.11 também possui um protocolo no nível MAC para o controle da transmissão, conhecido por CSMA/CA (*Carrier Sense Multiple Access/Collision*

*Avoidance*). O protocolo CSMA/CA foi projetado para reduzir a probabilidade de colisões em uma rede sem fio, composta de múltiplas estações. Uma colisão ocorre quando o meio de transmissão, depois de permanecer um período ocupado, torna-se livre. Durante o tempo em que o meio permanece ocioso, é possível que duas ou mais estações tentem utilizá-lo ao mesmo tempo, causando, assim, uma colisão.

Para evitar esse tipo de problema, um mecanismo de espera randômica é utilizado. Cada estação que deseja transmitir – depois de verificar que o meio está livre –, espera mais um tempo randomicamente determinado e verifica se o meio continua livre; caso esteja, é feita a transmissão.

### 16.4.1 Funcionamento do protocolo CSMA/CA

Quando deseja enviar um pacote, a estação emissora verifica se o meio de comunicação está livre e, se estiver, faz a transmissão. Depois de a estação transmitir seu pacote de dados, espera da estação receptora um pacote de confirmação chamado ACK (*Acknowledgment*). A estação receptora, depois de verificar que o pacote está consistente, envia o pacote ACK para a estação emissora. Porém, se a estação emissora não receber o ACK ou se a estação receptora não o enviar por qualquer motivo, fica evidenciado que houve uma colisão, e após um tempo randômico de espera, a estação novamente transmite o pacote. Ainda, no caso de o pacote ACK chegar corrompido, também ficará evidenciado que houve uma colisão e o mesmo procedimento será aplicado.

Depois de a primeira transmissão ter ocorrido com sucesso em uma rede sem fio, cada computador da rede será configurado para transmitir em um determinado período de tempo. Assim, a partir desse momento, não ocorrerá colisão, pois cada computador possui um momento certo para iniciar a sua transmissão. Quando a rede permanece ociosa, isto é, se passar o tempo e nenhuma das máquinas quiser transmitir, o meio de comunicação deixa de ser utilizado, e a rede volta ao estado anterior da primeira transmissão.

É importante observar que o tempo de transmissão de cada

máquina só será definido depois de uma primeira transmissão ter sido efetuada. Assim, só poderá haver colisão na primeira transmissão, isto é, quando dois ou mais dispositivos sem fio verificam que o canal está livre e tentam transmitir ao mesmo tempo. A seguir, apresentaremos as diferentes versões do padrão 802.11.

## 16.4.2 Padrão 802.11b

O padrão 802.11b foi o primeiro desenvolvido pelo IEEE especificamente para redes Ethernet sem fio. Esse padrão foi desenvolvido a fim de suprir as necessidades e as expectativas das empresas. Esse padrão pode operar tanto na topologia *ad-hoc* quanto na topologia cliente/servidor. Nesta, todo o tráfego da rede passa pelo ponto de acesso sem fio, enquanto na topologia *ad-hoc*, os computadores trocam dados diretamente entre si.

O padrão 802.11b opera na frequência de 2,4 GHz conhecida como ISM (*Industrial Scientific and Medical*) e utiliza a técnica DSSS (*Direct Sequency Spread Spectrum*). Em razão de atuar em uma frequência mais baixa, esse padrão está mais suscetível a interferências de outros tipos de fontes de ruído, como aparelhos de telefone sem fio e fornos micro-ondas, os quais trabalham na mesma faixa de frequência. O padrão 802.11b possui alcance de aproximadamente 100 metros e a sua taxa de transmissão pode chegar a 11 Mbps.

## 16.4.3 Padrão 802.11a

O padrão 802.11a foi o segundo desenvolvido pelo IEEE e é, em média, cinco vezes mais rápido do que o padrão 802.11b, chegando a transmitir dados a 54 Mbps. Esse padrão opera na frequência de 5.8 GHz e utiliza a técnica OFDM (*Orthogonal Frequency Division Multiplexing*). Além disso, disponibiliza até oito canais por ponto de acesso, o que possibilita maiores taxas de transmissão para uma quantidade maior de usuários simultâneos. Visto que o padrão 802.11a opera na banda conhecida como UNII (*Unlicensed National Information Infrastructure*) com frequências mais elevadas, possui

maior imunidade a interferências eletromagnéticas, embora apresente mais dificuldade em ultrapassar paredes. É importante observar que o padrão 802.11a possui alto custo e não é compatível com dispositivos do padrão 802.11b.

### 16.4.4 Padrão 802.11g

O IEEE publicou também o padrão 802.11g, que objetivou combinar o melhor dos padrões 802.11a e 802.11b, transmitindo dados a 54 Mbps e utilizando a frequência de 2,4 GHz. Essa frequência é liberada sem necessidade de pedir licença à Anatel para ser utilizada. O padrão 802.11g é totalmente compatível com o padrão 802.11b, ou seja, pontos de acesso 802.11g podem transmitir dados de placas de rede-padrão 802.11b.

### 16.4.5 Padrão 802.11e

O padrão 802.11e foi desenvolvido como o objetivo de melhorar a qualidade do serviço (QoS) em ligações telefônicas, transmissão de vídeo de alta resolução e outras aplicações multimídia. Com esse padrão, será possível que certos tipos de tráfego em redes sem fio sejam prioritários em relação a outros. Uma rede sem fio poderá garantir que ligações em telefones IP e conteúdo multimídia sejam devidamente acessados tanto em redes sem fio como em redes cabeadas.

### 16.4.6 Padrão 802.11i

A especificação de segurança 802.11i é baseada no padrão de encriptação avançada (AES) que suporta chaves de criptografia de 128, 192 e 256 bits. Esse padrão objetiva resolver o problema de segurança existente nas redes sem fio. O padrão de segurança utilizado nas redes sem fio, conhecido por WEP (*Wired Equivalent Privacy*), utiliza técnicas simples de criptografia, não garantindo privacidade na transmissão de dados nesse meio.

### 16.4.7 Padrão 802.11n

Com o objetivo de aumentar a velocidade de transmisão de dados

em redes sem fio, o IEEE deu continuidade às pesquisas e publicou o padrão 802.11g. Esse padrão permite que um roteador sem fio transmita dados a até 300 Mbps, porém o desempenho dependerá do modelo adquirido. Atualmente, as operadoras vêm oferecendo conexões cada vez mais rápidas para o acesso à Internet residencial, chegando em algumas regiões com produtos de 150 Mbps ou mais. Dessa forma, para atender a esse mercado que não para de crescer, foi necessária a criação de um novo padrão que realmente permitirá altas velocidades na transmissão de dados sem fio. A seguir, apresentaremos o padrão 802.11ac.

### 16.4.8 Padrão 802.11ac

Este é o padrão mais atual neste momento. Esse novo padrão traz um ganho de desempenho por meio de várias melhorias, permitindo que o tráfego de dados seja transmitido por canais operando a 80 MHz, chegando até 160 MHz, contra os 40 Mhz do padrão 802.11n. Esse padrão oferece uma melhora na técnica de modulação de sinal, utilizando o 256 QAM (*Quadrature Amplitude Modulation*) contra o padrão 64 QAM utilizado pelo padrão 802.11n. Uma outra razão para o 802.11ac ser mais rápido é que ele opera exclusivamente na faixa de frequência de 5 GHz, que tem mais canais e é menos concorrida que a faixa dos 2.4 GHz comumente usada pelas tecnologias *wireless* atuais.

Outra caracterísitca que permite que o padrão 802.11ac alcance velocidades maiores é sua forma de transmissão inteligente. Em vez de propagar as ondas de modo uniforme para todas as direções, os roteadores *wireless* reforçam o sinal para os locais em que há equipamentos *wireless* conectados. Essa tecnologia é chamada de *beamforming* e garante comunicação direta entre os dispositivos sem fio da rede. A figura 16.3 apresenta uma comparação entre a comunicação do atual e quando se utiliza beamforming.

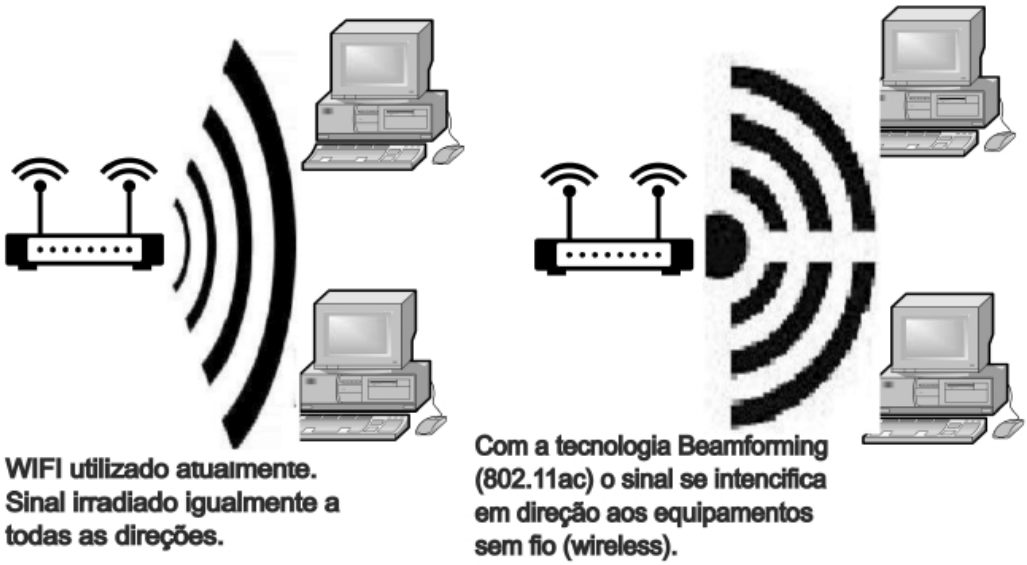



*Figura 16.3 – Tecnologia beamforming.*

## 16.5 Bluetooth

O Bluetooth é uma tecnologia também utilizada em redes sem fio que seguiu um caminho de desenvolvimento diferente do da família 802.11. Opera na topologia *ad-hoc* em frequências de 2,4 GHz (mesma do 802.11b e 802.11g) que possibilitam a transmissão de dados em curtas distâncias entre telefones sem fio, celulares, rádios automotivos, GPS, notebooks, teclados e joysticks, ou seja, qualquer aparelho digital que use um chip bluetooth. O bluetooth tem o objetivo de simplificar a comunicação e a sincronização entre esses aparelhos que hoje utilizam cabos para conectarem e sincronizarem entre si.

O bluetooth foi otimizado para permitir que um número elevado de comunicações ocorra dentro da mesma área, ou seja, por ser utilizado na topologia ad-hoc, oferece melhores condições para a sua utilização quando comparado com outras tecnologias ad-hoc. Nessa tecnologia, existe um grande número de canais independentes e não sincronizados, os quais servem somente a um número limitado de participantes. Em outras soluções ad-hoc, todos os equipamentos compartilham o mesmo canal.

### 16.5.1 Como surgiu o Bluetooth

O Bluetooth é uma tecnologia de rádio de curto alcance criada pela Ericsson em meados da década de 1990 e desenvolvida por diversas companhias. Essa tecnologia sem fio possibilita a transmissão de dados em curtas distâncias entre telefones, computadores e outros aparelhos eletroeletrônicos.

Seu principal objetivo é eliminar o cabeamento entre os equipamentos móveis, facilitando a comunicação de dados e voz, além de criar um meio de conexão universal. O sucesso de bluetooth foi alcançado depois de uma união entre empresas que impulsionaram a tecnologia, como IBM e Intel.

Para o desenvolvimento do Bluetooth, foi criada uma organização chamada Bluetooth Special Interest Group, que pode ser acessada por meio do site *www.bluetooth.org*.

## 16.5.2 Funcionamento do Bluetooth

A comunicação ocorre sempre que um equipamento compatível com o padrão detecta outro equipamento, também compatível com o padrão bluetooth, dentro da área de seu alcance. O alcance de operação do bluetooth, atualmente na versão 4, melhorou e pode chegar a 61 metros. Outro ponto positivo dessa última versão foi o baixo consumo de energia.

No momento em que os equipamentos bluetooth se encontram dentro das distâncias suportadas pelo padrão, forma-se uma rede piconet. A piconet é uma pequena rede pessoal conhecida por PAN (*Personal Area Network*), na qual um dos equipamentos interligados recebe a função de mestre e os demais, a função de escravos. O mestre é responsável por controlar as comunicações entre o mestre e os escravos, além de controlar as transferências de dados entre os equipamentos escravos, pois uma rede ad-hoc permite a comunicação sem a presença de um ponto central.

Uma rede piconet é formada por, no máximo, oito equipamentos, todos interconectados entre si. Quando duas ou mais piconets são interligadas, forma-se uma scatternet, a qual pode conter até 80 equipamentos, sendo esse o limite para que a rede funcione bem. É importante observar que uma piconet tem a capacidade de se

conectar tanto a uma rede cabeada como à Internet.

Os equipamentos que seguem o padrão bluetooth 1.0 transmitem dados a 1 Mbps e, para a transmissão de voz, a especificação determina três canais síncronos de 64 Kbps cada um. A versão 1 ainda evolui para as versões 1.1 e 1.2. A partir da versão 1.1, o IEEE foi envolvido e padronizou este como IEEE 802.15. Outras versões vieram e atualmente esse padrão está na versão 4.1. É importante observar que, na versão 3.0, o bluetooth passou a transmitir dados na mesma frequência do padrão 802.11, sendo possível alcançar a velocidade de até 24 Mbps.

## 16.6 Precauções em redes sem fio

Para que seja possível utilizar as redes sem fio em sua plenitude, alguns cuidados devem ser tomados. A seguir, relacionaremos as situações em que se deve ter cuidado para que o investimento em uma rede sem fio não cause problemas.

A primeira precaução refere-se à altura da antena, que não pode ser instalada ao nível do computador. Quanto mais alta a sua localização, melhor será a comunicação entre os equipamentos da rede sem fio. Os computadores que fazem parte da rede também devem ser instalados em lugares altos, a fim de facilitar a comunicação com as antenas. Jamais se deve instalar computadores com placas sem fio ao nível do chão, pois, nesses casos, ainda existe o campo magnético gerado pelo contato com tapetes ou carpete.

A segunda precaução refere-se aos equipamentos domésticos que operam na mesma frequência das placas de rede sem fio, como os telefones sem fio e o forno de micro-ondas.

A terceira precaução refere-se a paredes de concreto entre os equipamentos de rede. Esse problema se agrava quando as paredes estão revestidas com plantas. Outro inimigo da boa propagação são os grandes recipientes com água e vidros (aquários) utilizados para separar os ambientes.

## 16.7 Exercícios do capítulo 16

**1**. Qual o significado do termo *wireless*?

**2**. As redes sem fio operam em quais topologias?

**3**. Cite as diferenças entre o CSMA/CD e o CSMA/CA.

**4**. Em qual camada do modelo de referência OSI o padrão 802.11 opera?

**5**. Descreva o padrão 802.11a.

**6**. Descreva o padrão 802.11b.

**7**. Qual a diferença entre o padrão 802.11a e o padrão 802.11b?

**8**. Descreva o padrão 802.11g.

**9**. Descreva o padrão 802.11e.

**10**. Descreva o padrão 802.11i.

**11**. Descreva o padrão de segurança WEP.

**12**. O padrão bluetooth opera em qual topologia?

**13**. Descreva a rede piconet e a rede scatternet.

**14**. Para o transporte de voz entre equipamentos bluetooth, quantos canais podem ser utilizados ao mesmo tempo e em qual taxa de transmissão?

CAPÍTULO 17

# Redes GPON

Neste capítulo, abordaremos a tecnologia de transmissão de dados sobre fibra óptica, conhecida por GPON (*Gigabit Passive Optic Network*). Serão apresentados suas características, uma comparação com o padrão EPON (*Ethernet Passive Optic Network*), os equipamentos ativos e passivos utilizados, a relação com o padrão Ethernet, seus principais conceitos e a utilização dos T-CONTs, algoritmo DBA (*Dynamic Bandwidth Allocation* – Alocação Dinâmica de Banda), entre outras importantes características dessa nova tecnologia que garante acesso à Internet em alta velocidade a um baixo custo.

## 17.1 Introdução ao padrão PON

Com a necessidade cada vez maior de o mundo se manter conectado, o mercado de novas tecnologias de rede de transporte vem crescendo rapidamente, seja para a interligação de clientes à Internet ou mesmo para a interligação dos escritórios de uma empresa sobre links de alta velocidade. Nesse cenário, apresentaremos uma nova tecnologia conhecida por PON (*Passive Optic Network*). O termo PON é um acrônimo para *Passive Optical Network*, e o termo *passive* se caracteriza pela ausência de alimentação elétrica (*unpowered*).

Como principais atrativos financeiros de uma rede PON, temos a possibilidade de atender múltiplos clientes em uma infraestrutura reduzida (rede ponto a multiponto) e, ainda, transmitir dados, voz e vídeo sobre essa mesma infraestrutura, ou seja, a tecnologia PON suporta *triple-play* (Internet, VoIP e TV). Devido ao baixo custo de implementação, aliado ao alto desempenho, as operadoras e empresas provedoras de serviços de rede têm direcionado esforços e investimento para essa nova tecnologia. Vejamos algumas das principais vantagens em investir em uma infraestrutura de rede

sobre a tecnologia PON:

- Não necessita de armários, presentes nas ruas, com alimentação elétrica.
- Permite que múltiplos clientes compartilhem uma grande parte da rede de fibra óptica, reduzindo a quantidade de cabos estendidos de forma subterrânea ou aérea. Uma rede PON oferece a capacidade de comunicação ponto a multiponto.
- Os *splitters* (divisores ópticos) podem ser instalados de forma aérea em postes ou em caixas de emendas subterrâneas. Não utilizam energia elétrica.
- Redução do uso de energia elétrica e espaço, pois um OLT (*Optical Line Terminal* – Terminal de Linha Óptica) substitui inúmeros switches e patch pannels. A necessidade de energia elétrica presente na tecnologia DSL (*Digital Subscriber Line*) exige que as operadoras instalem armários nos grandes centros urbanos para concentrarem os cabos e demais equipamentos. Atualmente, está cada vez mais difícil instalar um armário, seja pela questão ambiental, custo do espaço ou licenciamento dos municípios. Esses armários exigem baterias para o caso de falta de energia.
- Não há problemas com interferências externas ou queima dos elementos por descarga elétrica.
- Hoje o custo da fibra óptica já é menor do que o custo dos cabos de cobre.
- Oferece taxas de download e upload maiores do que as oferecidas pelo padrão DSL.
- Maiores distâncias. A distância entre o OLT e ONUs pode chegar a 20 km.
- Podemos classificar uma infraestrurura de rede PON como uma tecnologia verde. O termo verde (*green*) remete a tecnologias que atendem aos seguinte parâmetros:
  - Tecnologia com sustentabilidade: o PON ofecere baixo custo e reutilização de recursos.
  - Preservação do meio ambiente: uma rede PON exige menos

cabos, switches e pacth pannels.

- Uso consciente dos recursos naturais e energéticos: parte da rede PON não utiliza energia elétrica.

Atualmente, os serviços de acesso à Internet oferecidos pelas operadoras vêm mudando sua arquitetura, ou seja, em vez de utilizar as tecnologias tradicionais, como DSL (Linha Digital para o Assinante – *Digital Subscriber Line*), cable modem ou HFC (*Hibrid Fiber Coax*), formadas por cabos de cobre, as operadoras estão investindo em redes excencialmente compostas de fibra óptica. Nesse contexto, com a intenção de aumentar as altas taxas de transmissão em um meio físico com alta qualidade, as operadoras passaram a levar a fibra óptica até a residência dos clientes (FTTH – *Fiber to the Home*), ou, ainda, vêm investindo em prumadas de prédios (FTTB – *Fiber to the Builder*).

Em uma rede PON, as operadoras estendem uma fibra óptica saindo de uma base central (POP – Ponto de Presença) que poderá atender inúmeros clientes, reusando uma parte dessa fibra óptica. É importante observar que apesar de uma fibra ser estendida do ponto central da operadora até um determinado bairro, exigirá ainda uma pequena parte de fibra que seja estendida do divisor óptico (*splitter*), situado em um ponto estratégico do bairro atendido, até a residência do cliente. A figura 17.1 apresenta uma rede PON em que poderemos observar a reusabilidade de sua infraestrutura.

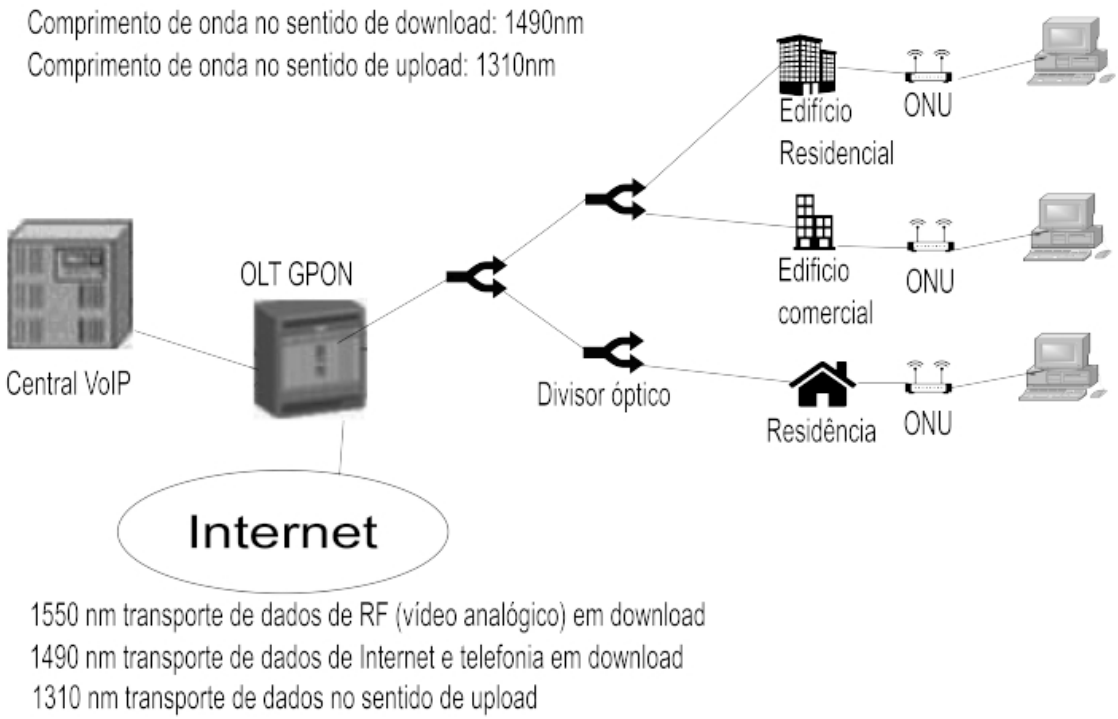



*Figura 17.1 – Estrutura de uma rede PON.*

Neste cenário, atendemos múltiplos clientes reusando uma parte da fibra e, assim, conseguimos redução da quantidade de fibras, energia, equipamentos ativos e infraestrutura, permitindo que os serviços comercializados sejam acessíveis (baixo custo) a um maior número de clientes. Conforme observamos na figura 17.1, uma rede PON possui alguns equipamentos estratégicos conhecidos por:

- OLT (*Optical Line Terminal* – Terminal de Linha Óptica).
- *Splitter* (divisor óptico ou *optical distribution network* (ODN)).
- ONU (*Optical Network Unit*) também chamada de ONTs (*Optical Network Terminals*).

Esses equipamentos estão dispostos em uma arquitetura ponto a multiponto (*Point-to-Multipoint* – P2MP) usando fibra óptica fim a fim. Quando utilizamos a rede PON, podemos estender a fibra óptica por 10 ou 15 km, seguindo por um caminho estratégico e, ao final, atender múltiplos clientes (em torno de 128 clientes) com apenas um par de fibra óptica, chegando a 20 km. A redução de esforço e custo é considerável. Assim, temos que em uma comunicação ponto a ponto um par de fibra óptica atende um cliente, enquanto em uma

topologia ponto a multiponto o mesmo par de fibra óptica poderá atender até 128 clientes.

## 17.2 Equipamentos de uma rede PON

Conforme comentado, em uma rede PON temos a presença dos seguintes equipamentos:

- OLT posicionado em um local central. Normalmente, instala-se o OLT em um POP, com capacidade de redundância de energia e total segurança. O OLT concentra o recebimento de todo o tráfego PON. Esta, em seguida, o repassará a uma interface Ethernet em que estará conectado o roteador.
- *Splitter* posicionado em um ponto estratégico no caminho seguido em um determinado bairro. Esse equipamento permitirá que o par de fibra óptica seja dividido e passe a atender os 128 clientes comentados.
- ONU posicionada no endereço do cliente. Este equipamento realiza a conversão do sinal óptico para uma interface RJ-45 que opera com sinais elétricos.

O OLT atua como elemento central e normalmente fica instalado em um ponto de presença (POP) da operadora. Esse equipamento, além de conectar os clientes da rede PON, também faz a conexão com os roteadores (ex.: Huawei, Juniper, Cisco etc.) do backbone. A conexão com os roteadores deve ocorrer por meio de uma porta Ethernet normalmente de 1 ou 10 Gbps em razão de o OLT canalizar múltiplas portas PON, que, por sua vez, recebem dados de centenas de clientes. Os pacotes enviados pelo roteador a uma das portas do OLT serão repassados a todas as ONUs ligadas a essa porta. Cada ONU acede à informação que lhe é endereçada e a descodifica. Neste capítulo, apresentaremos como os quadros são transmitidos no sentido de download e upload entre as ONUs e o OLT.

Em uma posição intermediária na rede, temos o *splitter* (divisor óptico), responsável por permitir que com um par da fibra óptica, conectada a uma das portas PON do OLT, esta seja subdivida e

atenda aos múltiplos clientes. A quantidade de clientes atendidos dependerá da implementação da tecnologia PON que poderá ser de até 128 clientes, caso se utilize GPON. A figura 17.2 apresenta o formato de um *splitter*, modelos 1:2 (uma fibra se subdivide em 2 fios), 1:4 (uma fibra se subdivide em 4 fios) e 1:32 (uma fibra se subdivide em 32 fios). Existem ainda outros modelos, como 1:8 e 1:16.

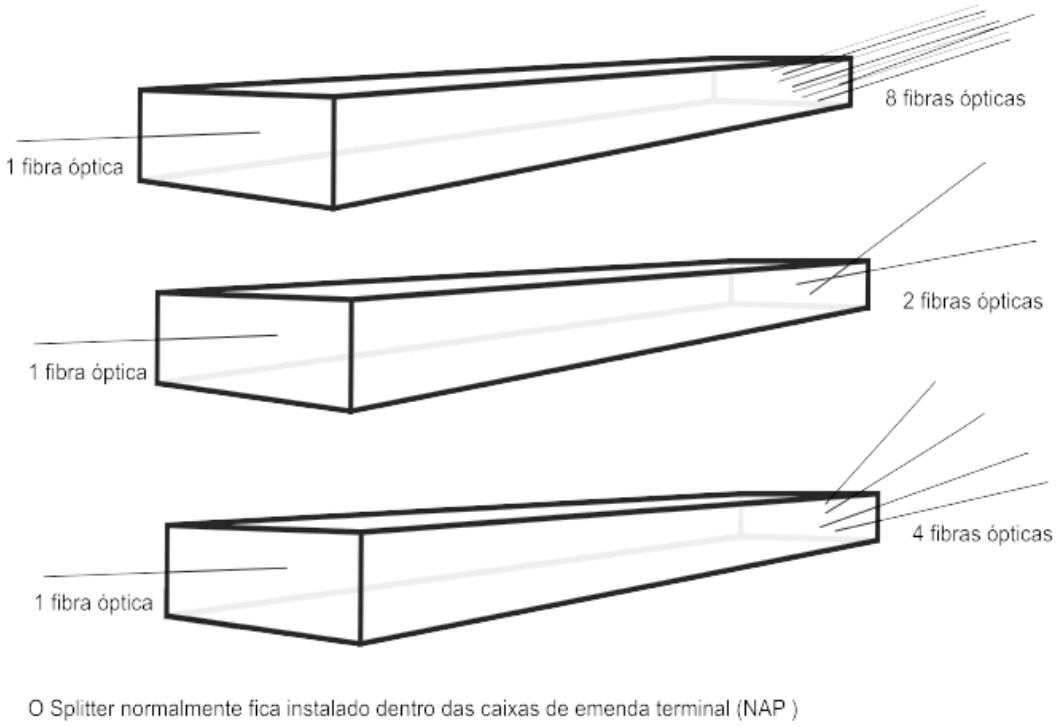



*Figura 17.2 – Modelo do splitter.*

Na prática, para a instalação de clientes residenciais, procura-se utilizar *splitters*, inicialmente o modelo 1:2, em que a fibra óptica, após chegar a um ponto estratégico na região do cliente (ex.: seu bairro), é dividida em duas fibras, e em cada uma instalamos dois novos *splitters* com suporte de 1:32, ou seja, para cada fio da fibra óptica, teremos a possibilidade de instalar até 32 clientes. Essa divisão poderá variar, dependendo da estratégia da área de engenharia responsável.

É importante observar que sempre que utilizamos *splitters*, temos perda de potência. No caso do *splitter* de 1:2, a perda ficou em torno

de 3,5 dB e, no caso do *splitter* 1:32, a perda foi de em torno de 15 dB. Dessa forma, em cada perda do *splitter* 1:2, teremos, no mínimo, uma perda de 18,5 dB (3,5 dB + 15 dB). Para que uma ONU tenha qualidade na comunicação, deverá operar abaixo de -28 dB (ONUs classe B+). Os 9,5 dB restantes poderão aparecer pela distância que a fibra ainda seguirá até o endereço do cliente, como também pela fusão que precise ser feita no caminho e na casa do cliente. Em prédios, costuma-se utilizar inicialmente *splitters* 1:8, em que cada perna poderá receber mais um *splitter* 1:8, fechando o total de 64 clientes. É importante observar que não se precisa necessariamente utilizar os 128 possíveis. A decisão de ter 128 ou 64 será confirmado pela área de engenharia responsável.

Ao final da rede, temos as ONUs, responsáveis por efetuar a conversão do sinal óptico em sinal elétrico e entregá-lo no endereço do cliente. Esse equipamento também converte os quadros do padrão PON para o padrão Ethernet presente nos equipamentos de rede dos clientes.

## 17.3 PON e WDM

Em uma rede PON, toda a informação será transmitida bidirecionalmente sob o mesmo caminho. Para que múltiplos serviços sejam multiplexados em uma mesma fibra óptica, precisamos aplicar alguma tecnologia que nos permita tal utilização. No caso das redes PON, utilizamos WDM (*Wavelength Division Multiple* – Multiplexação por Divisão de Comprimento de Onda).

Para a transmissão de dados e voz, utilizam-se dois comprimentos de onda diferentes, um para download (do OLT para a ONU) com comprimento de onda de 1.490 nm (*nanometer*) e um para upload (da ONU para o OLT) com comprimento de onda de 1.310 nm. Existe ainda o comprimento de onda de 1.550 nm, que atende à transmissão do sinal de TV. A figura 17.1 apresenta as diferentes frequências presentes na tecnologia PON.

A tecnologia WDM utiliza o conceito de multiplexação por comprimento de onda, em que cada comprimento de onda pode ser associado a uma cor ou a um valor diferente. O WDM permite a

transmissão de vários feixes de luz em frequências diferentes numa mesma fibra óptica, possibilitando que em um mesmo meio físico consigamos compartilhar dados, VoIP e vídeo. Além dos múltiplos serviços oferecidos em um mesmo meio físico, temos ainda a possibilidade de garantir que os dados de upload (1.310 nm) e download (1.490 nm e 1.550 nm) sigam pelo mesmo caminho físico em *full-duplex*. O sistema funciona como um multiplexador que agrega os vários comprimentos de onda dos transmissores ópticos e disponibiliza uma saída para ser transmitida por uma única fibra óptica. Na outra extremidade da fibra óptica, que pode estar a dezenas de quilômetros de distância (no GPON, a distância máxima é 20 km), utiliza-se um demultiplexador que separa os vários comprimentos de onda em saídas diferentes para serem conectadas nos receptores ópticos e atender a diferentes serviços.

## 17.4 Implementações da tecnologia PON

Atualmente, existem duas diferentes implementações da tecnologia PON conhecidas por GPON (*Gigabit Passive Optical Network*) e GEPON (*Gigabit Ethernet Passive Optical Network*) ou simplesmente EPON. Neste capítulo, descreveremos o padrão GPON e faremos uma comparação com o padrão EPON.

### 17.4.1 Rede GPON

A tecnologia GPON (*Gigabit Passive Optical Network* ou rede Gibabit Óptica Passiva) foi padronizada pelo ITU-T G.984 (*International Telecommunication Union Telecommunication Standardization Sector*), por meio de quatro documentos conhecidos pelos padrões ITU-T 984.1 a ITU-T 984.4. O GPON surgiu como uma solução no mercado de redes de acesso ponto a multiponto, oferecendo suporte sem precedentes para alta velocidade e múltiplos serviços (Internet, VoIP e TV).

Conforme comentado, devido às frequências utilizadas, a tecnologia GPON utiliza fibra óptica monomodo. As fibras ópticas monomodo são caracterizadas por:

• Maior alcance e maior taxa de dados.

• Manuseio/emendas mais delicados.

• Utiliza as frequências comentadas iniciando em 1.310 nm e seguindo até 1.550 nm.

Outro modelo de fibra óptica utilizado em redes, porém não pela rede GPON, são as fibras multimodo. As fibras ópticas multimodo são caracterizadas por:

• Menor taxa de dados e alcance.

• Uso de fonte de luz mais barata.

• Fisicamente ser mais robustas.

• Utiliza as frequências comentadas iniciando em 850 nm e seguindo até 1.300 nm.

O GPON foi desenvolvido a partir das necessidades das próprias operadoras de telecomunicações por maiores taxas de tráfego de download e upload, maior eficiência de banda, redução de custo e maior variedade de serviços, ou seja, as operadoras buscaram uma atualização para as tecnologias de transmissão existentes, como Cable Modem e xDSL. Como exemplo de implementações de rede xDSL, temos ADSL (*Asymetric* DSL) e VDSL (*Very high-speed* DSL).

O GPON adota a tecnologia WDM (*Wavelength Division Multiplexing*), a fim de permitir que o tráfego de download e upload ocorra em uma mesma fibra óptica. Para que o tráfego não se misture, cada sentido transmite em diferentes comprimentos de onda, e o comprimento de onda 1.310 nm atende ao sentido de upload, enquanto 1.490 e 1.550 nm atendem ao sentido de download.

É importante observar que download e upload na arquitetura GPON utilizam mecanismos de comunicação diferentes. A seguir, abordaremos os detalhes sobre como o download e upload ocorrem.

## 17.4.2 Download em redes GPON

O mecanismo de transporte dos quadros de uma rede GPON no sentido de download é totalmente ponto a multiponto, transmitindo os quadros em *broadcast* (difusão do OLT para a ONU). Com isso, cada quadro transmitido pelo OLT será recebido por todas as ONUs. Vejamos na figura 17.3 um exemplo de como ocorre a comunicação

no sentido de download.

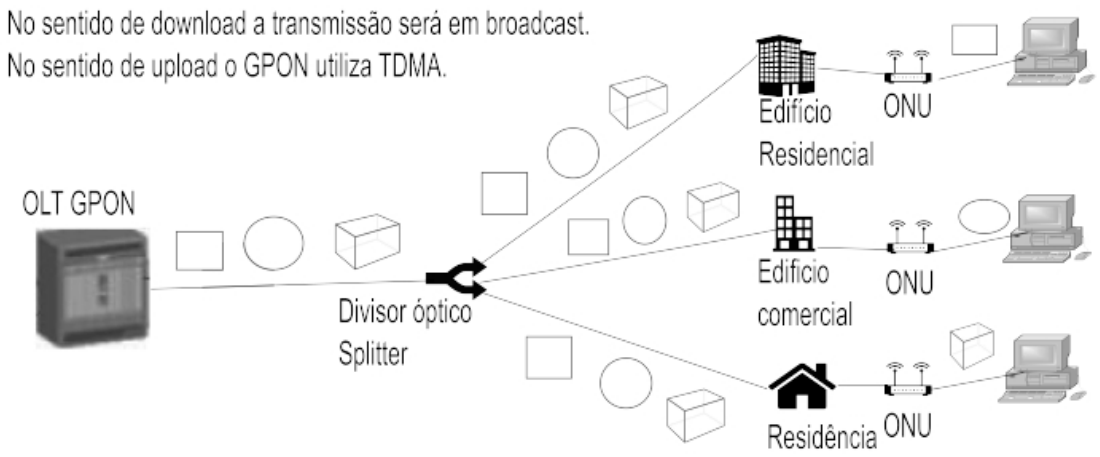



*Figura 17.3 – Download em redes GPON.*

Com a finalidade de garantir segurança durante a transmissão no sentido de download, o GPON permite que sejam utilizados mecanismos que assegurem que a ativação de uma nova ONU seja segura e ainda garante que os quadros enviados em *broadcast* sejam apenas recebidos pela correta ONU. Vejamos cada um dos mecanismos citados.

Para garantir que nenhuma ONU não homologada pela operadora seja conectada à rede e, pior, venha receber dados clandestinamente, o GPON disponibiliza um processo de ativação que garante tal segurança. No momento da ativação da ONU, o GPON apresenta dois mecanismos que podem ser utilizados a fim de garantir que a ONU conectada seja a homologada pela operadora e seja de seu conhecimento.

O primeiro elemento utilizado durante a ativação pode ser o número serial presente na ONU. No momento que conectamos a ONU no endereço do cliente, informamos o número serial previamente conhecido e a ONU inicia sua comunicação com o OLT. A inserção do número serial é realizada por meio de um cabo serial pelo técnico responsável pela ativação.

Uma segunda opção de ativação é com o uso de uma senha pré-definida com o OLT. Essa senha é informada durante a configuração na ferramenta de gerência (ex.: U2000 da Huawei ou NetHorizhon

(*ZMS – Zone Management Systems*) da Zhone). Não é recomendado, apesar de possível, permitir que o OLT aceite ONUs sem nenhum elemento de segurança. Caso isso seja permitido, alguém poderá instalar uma ONU falsa (obtida aleatoriamente) e receber sinal clandestinamente. A figura 17.4 apresenta o ambiente, da plataforma Huawei, em que a equipe de ativação escolhe o modo que será utilizado na autenticação da ONU.

Conforme podemos observar na figura 17.4, na opção *Authentication Mode*, escolhemos o modo que será utilizado pelo OLT para concluir o processo de ativação da ONU. Nesse exemplo, a senha utilizada foi 27091974.

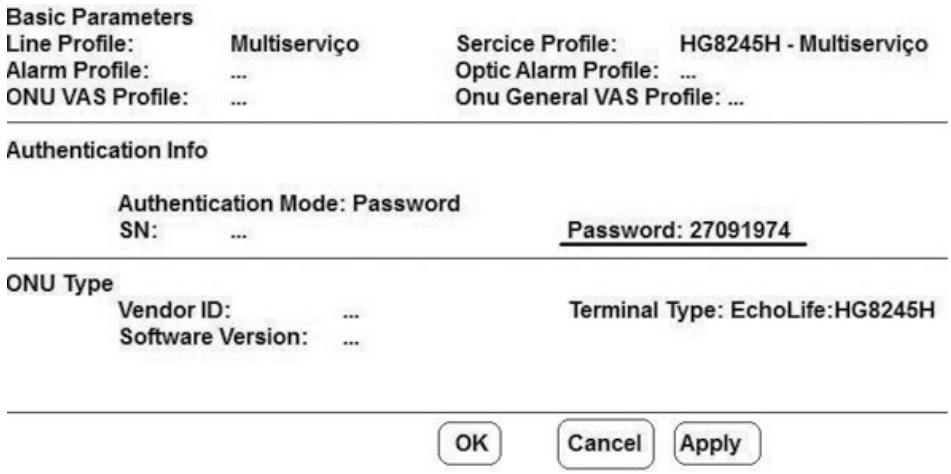



*Figura 17.4 – Ambiente em que definimos o modo de autenticação.*

Devido à natureza de *broadcast* presente no sentido de download, uma rede GPON naturalmente carece de falta de privacidade, pois cada ONU poderia acessar os dados de download relativos a outras ONUs. Conforme comentado no sentido de download, o OLT envia os dados a todas as ONUs, ou seja, como evitar que uma ONU não receba os dados das outras? No GPON, a resposta está baseada na implementação do algoritmo AES-128 (*Advanced Encryption Standard* – Padrão de Criptografia Avançada – 128 bits). O GPON fornece codificação de dados e usa o algoritmo AES (*Advanced Encryption Standard*) para encriptar a carga útil (*payload*) somente no sentido de download. A chave de encriptação associada a cada ONU é enviada três vezes (devido à robustez) pela ONU ao OLT. O

envio da chave escolhida, pela ONU, ocorre no sentido de upload por meio do campo PLOAM (*Physical Layer Operations, Administration and Management*) abordado neste capítulo. Uma vez que o OLT recebe essa chave, utiliza-a para a comumicação com a respectiva ONU. É importante observar que, além de a chave ser enviada no início da comunicação entre a ONU e o OLT, esta será periodicamente enviada para que a segurança não seja quebrada.

O AES utilizado pelo GPON utiliza criptografia simétrica, ou seja, a mesma chave usada para criptografar, também é usada para decriptografar os quadros. Por utilizar 128 bits, é possível termos 3.4 * 1038 diferentes chaves, ou seja, para quebrar uma chave, levaria muito tempo. No caso do quadro GEM (*GPON Encapsulation Method*), explicado neste capítulo, o mecanismo de encriptação do GPON mantém encriptado apenas o GEM *payload*, pois assim os dados Ethernet encapsulados no quadro GEM ficarão totalmente protegidos. Com isso, cada uma das ONUs somente conseguirá extrair os dados Ethernet direcionados diretamente para si. As chaves utilizadas para encriptação, conforme comentado, são transportadas por mensagens PLOAM, presentes no campo PLOAM do quadro do GPON. Apresentaremos neste capítulo as mensagens PLOAM e o campo PLOAM.

Conforme comentado, entre o OLT e todas as ONUs, haverá troca de mensagens PLOAM em que cada ONU definirá sua própria chave e acordará com o OLT para que os quadros trafegados carreguem tal chave. Desta forma, cada ONU abrirá somente os quadros que tenham sido endereçadas a ela. Assim, após o processo de ativação da ONU ser concluído, o OLT envia uma mensagem PLOAM conhecida por *Request_Key* à ONU que deverá criar, armazenar e enviar a chave ao OLT. A ONU enviará a chave três vezes consecutivas para o OLT. Nessa transmissão, os dados são enviados sem criptografia, pois considera-se que o tráfego em upload é seguro. A figura 17.5 demonstra a negociação entre o OLT e a ONU para definir a chave.

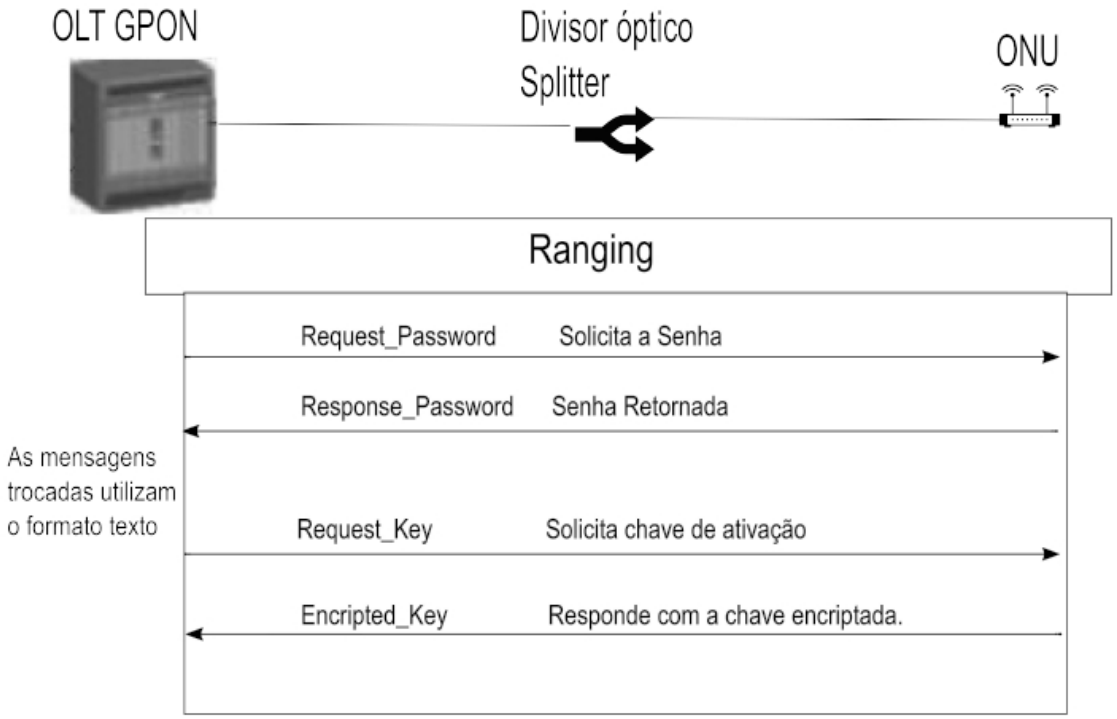



*Figura 17.5 – Processo de ativação e ranging.*

Conforme observamos na figura 17.5, o primeiro procedimento executado entre o OLT e a ONU é conhecido por *ranging,* que ocorre ao mesmo tempo que o processo de ativação. O processo de *ranging* executado entre o OLT e todas as ONUs busca medir a distância lógica entre estas, a fim de garantir que a ONU, no sentido de upload, consiga o espaço e tempo necessário para transmitir na velocidade que tenha sido configurada sem colisões. Esse procedimento garantirá que o OLT, por meio do campo *BWmap* enviado no sentido download, defina corretamente o período que a ONU terá para transmitir no sentido de upload. Comentaremos neste capítulo o modo de transmisão em upload que difere do download por utilizar o conceito de TDMA (*Time Division Multiple Access*).

Em paralelo ao processo de *ranging*, ocorre o processo de ativação. Durante a ativação, o OLT solicita uma senha por meio da mensagem PLOAM (*Physical Layer Operations, Administration and Management*) conhecida por *Request_Password*. Em um segundo momento, o OLT solicita à ONU que envie a chave criptografada pelo algoritmo AES por meio da mensagem PLOAM *Request_Key*.

### 17.4.3 Modelo de referência OSI e a estrutura do GPON

É importante observar que uma rede GPON atua na última milha e fica em uma posição intermediária, ou seja, entre o roteador da operadora e os equipamentos do cliente, ambos operando sobre o padrão Ethernet. As requisições geradas pelo cliente (notebooks, desktops, roteadores) são encaminhas pela rede GPON até alcançar o roteador que dará acesso à Internet. Dessa forma, apenas a parte final do caminho percorrido será sobre a rede GPON e, assim, consideramos o caminho GPON como última milha.

A arquitetura do GPON é composta de camadas como o modelo de referência OSI e o modelo de referência TCP/IP. No caso do GPON, as camadas que atendem a essa tecnologia se posicionam paralelas às camadas 1 e 2 do MR-OSI. A figura 17.6apresenta uma comparação entre o modelo de referência OSI e o GPON.

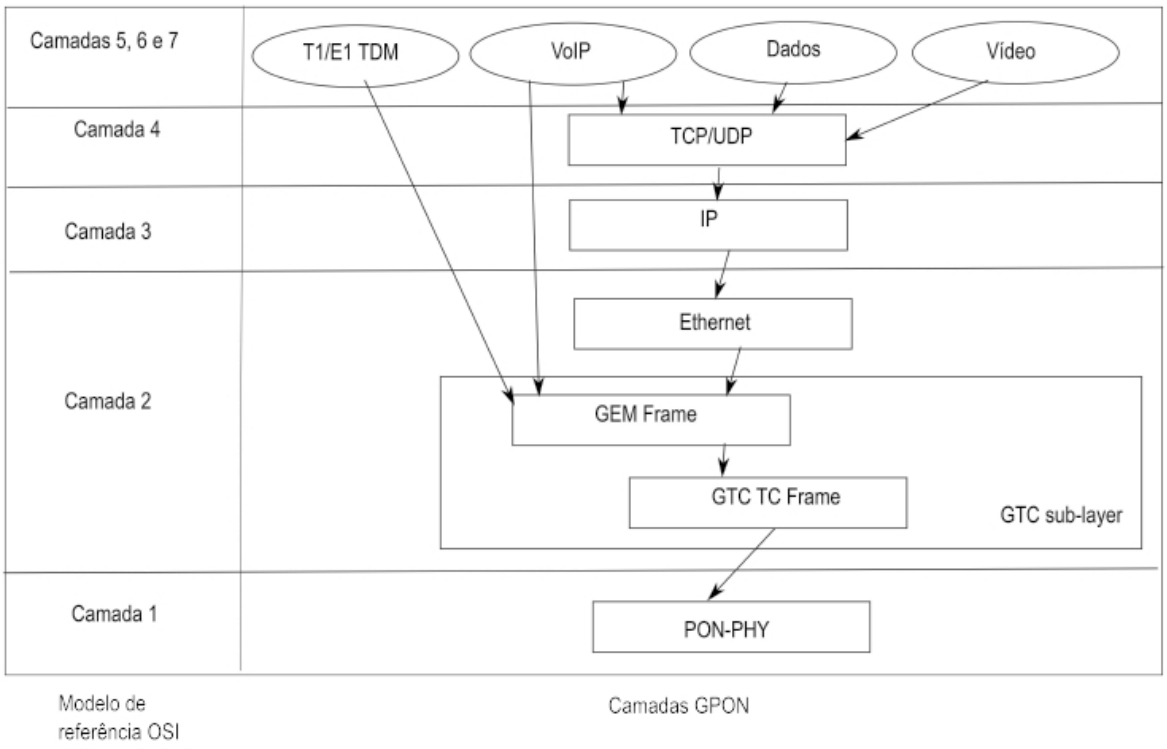



*Figura 17.6 – Relação emtre o MR-OSI e o GPON.*

#### 17.4.3.1 Camada física da arquitetura GPON – PON-PHY

A camada 1 (PON-PHY), especificada pelo ITU-T, por meio da

recomendação G.984.2, é responsável por gerenciar os parâmetros relacionados à interligação entre OLT, *splitter* e ONUs. Entre os parâmetros gerenciados, temos:

- Atenuações máxima e mínima da porta do OLT e ONUs. Os valores dependerão dos modelos do equipamento, que poderão ser:
  - Classe A, variando de - 5 a - 20 dB.
  - Classe B, variando de - 10 a - 25 dB.
  - Classe B+, variando de - 10 a - 28 dB. Atualmente muitas operadores utilizam esse modelo.
  - Classe C, variando de - 15 a - 30 dB.

É importante observar que existem outros fatores que impactam na atenuação e, se não observados, podem causar problemas na comunicação. A tabela 17.1 apresenta os principais elementos e seus valores:

*Tabela 17.1 – Valores de atenuação*

| **Elementos que causam atenuação** | **Detalhes da mensagem** |
|---|---|
| Atenuação por km (1.310 nm) | Entre 0,35 dB/km e 0,37 dB/km |
| Atenuação por km (1.550 nm) | Entre 0,20 dB/km e 0,23 dB/km |
| Cordão óptico por km (1.310 nm) | 0,40 dB/km |
| Cordão óptico por km (1.550 nm) | 0,30 dB/km |
| Conectorização (unidade) | 0,507 dB/km |
| Splitter 1:2 | 3,7 dB/km |
| Splitter 1:4 | 7,3 dB/km |
| Splitter 1:8 | 10,5 dB/km |
| Splitter 1:16 | 13,7 dB/km |
| Splitter 1:32 | 17,1 dB/km |
| Splitter 1:64 | 20,5 dB/km |

- Distância fisica entre o OLT e cada uma das ONUs. Atualmente, os

equipamentos não podem ter mais de 20 km de distância. Os modelos de ONUs que aceitam ficar até 20 km de distância devem ser classificadas nas classes B+ ou C.

- Quantidade de ONUs conectadas a cada uma das portas PON do OLT. Atualmente, uma porta PON permite até 128 ONUs.
- Taxa nominal de download. Atualmente, podemos usufruir de 2.488,32 Mbps (2,5 Gbps) para download.
- Taxa nominal de upload. Atualmente podemos usufruir de 1.244,16 Mbps (1,25 Gbps) para upload.
- Padrão de codificação dos bits. Utiliza-se o padrão de codificação NRZ para converter bits em sinais luminosos. No GPON, adotaram-se alto nível de luz representando o bit 1 e baixo nível de luz para representar o bit 0.
- Parâmetros de tolerância a falhas e tempos de acesso, como o valor do *jitter*.

A figura 17.8 apresenta a posição da camada física na arquitetura GPON.

### 17.4.3.2 Camada de enlace da arquitetura GPON

A segunda camada da arquitetura GPON é conhecida por GTC (*GPON Transmission Convergence*). É especificada pelo ITU-T, por meio da recomendação G.984.3. A camada GTC é composta de duas subcamadas, sendo uma camada para enquadramento chamada de GTC *framing* e uma de adaptação para outras tecnologias (ex.: Ethernet) chamada de GTC *adaptation*. A figura 17.8 apresenta a posição que ocupam as subcamada comentadas. De outro ponto de vista, a camada GTC pode ser analisada como uma camada responsável pelos planos de controle e gerenciamento (*C/M-plane*) e o plano do usuário (*U-plane*).

O plano U é responsável por transportar os dados dos usuários. O plano C/M gerencia o fluxo de dados do usuário, elementos de segurança entre o OLT e ONUs e, ainda gerencia, as mensagens OAM e PLOAM. Vejamos alguns detalhes de cada um dos planos comentados

**Plano C/M**

O plano de gerenciamento e controle (*C/M plane*) é responsável por controlar informações relacionadas ao controle e gerenciamento da rede GPON. É composto de três mensagens:

- Mensagens *embedded* OAM (*Operations, Administration and Management*): representam mensagens com alta prioridade na rede GPON. Como mensagens que se classificam como OAM *embedded*, temos, por exemplo, as trocadas pelos campos DBRu e US *BWmap*.
- Mensagens PLOAM (*Physical Layer Operations, Administration and Management*).
- Mensagens enviadas pelo canal OMCI (*ONT Management and Control Interface*): basicamente enfocam informações utilizadas no provisionamento de cada ONU. Esse canal permite que as tecnologias posicionadas nas camadas superiores troquem mensagens pela arquitetura GPON.

As mensagens *embedded* OAM são transportadas pelo *header* da camada GTC e possuem prioridade na rede GPON, sendo processadas imediatamente pelo plano de gerenciamento e controle (C/M). Essas mensagens possuem baixa latência por tratarem mensagens classificadas como urgentes para a operação entre as ONUs e o OLT. Quando uma ONU sinaliza uma mensagem urgente, o OLT alocará espaço específico para a mensagem, que deverá ser recebida em um tempo inferior a 5 milissegundos. Como exemplo de mensagens classificadas como urgentes, temos:

- A troca de senhas entre cada ONU e o OLT. Essas senhas serão utilizadas para a comunicação no sentido de download. Essas mensagens são trocadas durante o processo de *ranging* e, posteriormente, para garantir que a segurança não será prejudicada.
- Mensagens relacionadas a sinalização e alocação de banda dinâmica utilizada pelo algoritmo DBA (*Dynamic Bandwidth Allocation* – Alocação Dinâmica de Banda). Cada ONU, ao ser ativada, negociará com o OLT seu espaço para transmissão, levando em

consideração sua distância e banda alocada. Essas mensagem são formatadas e transmitidas através dos campos DBRu e US *BWmap*.

- Mensagens relacionadas ao monitoramento de falhas (ex.: BER – *Bit Error Ratio* – Taxa de Erros de Bits).

A alocação de espaço específica para as mensagens urgentes se justifica devido à concorrência do meio físico durante a transmissão dos quadros no sentido de upload. Nesse sentido, apesar do eficiente gerenciamento de banda do algoritmo DBA (*Dynamic Bandwidth Allocation*), cada ONU disputará os espaços livres para transmissão. Caso o canal no sentido de upload esteja congestionado, uma mensagem urgente poderá aguardar um tempo maior que o suportado pela tecnologia. No sentido de upload, cada porta do OLT oferecerá apenas 1,25 Gbps de banda. Caso tenhamos 128 ONUs ativas em uma porta, a possibilidade de congestionamento será real.

As mensagens PLOAM são transportadas pelo campo PLOAM. A figura 17.8 apresenta a interface PLOAM. Por esse campo são transportadas mensagens relacionadas ao processo de ativação de cada uma das ONUs, como também as demais mensagens de alarme (logs) emitidas pela camada física e de enlace. Vejamos algumas das mensagens que seguem pelo campo PLOAM:

- Contador de mensagens PLOAM.
- Mensagens de erro de CRC.
- Total de mensagens recebidas.
- Total de mensagens *unicast* recebidas.
- Total de mensagens *broadcast* recebidas.
- Total de mensagens descartadas.
- Total de mensagens transmitidas.
- Mensagens relacionadas à ativação de cada ONU.
- Notificação de alarmes.

A figura 17.7 apresenta o formato do quadro GTC no sentido de download. Nessa figura, podemos observar os detalhes do campo

PLOAM. Abordaremos os detalhes desse campo neste capítulo.

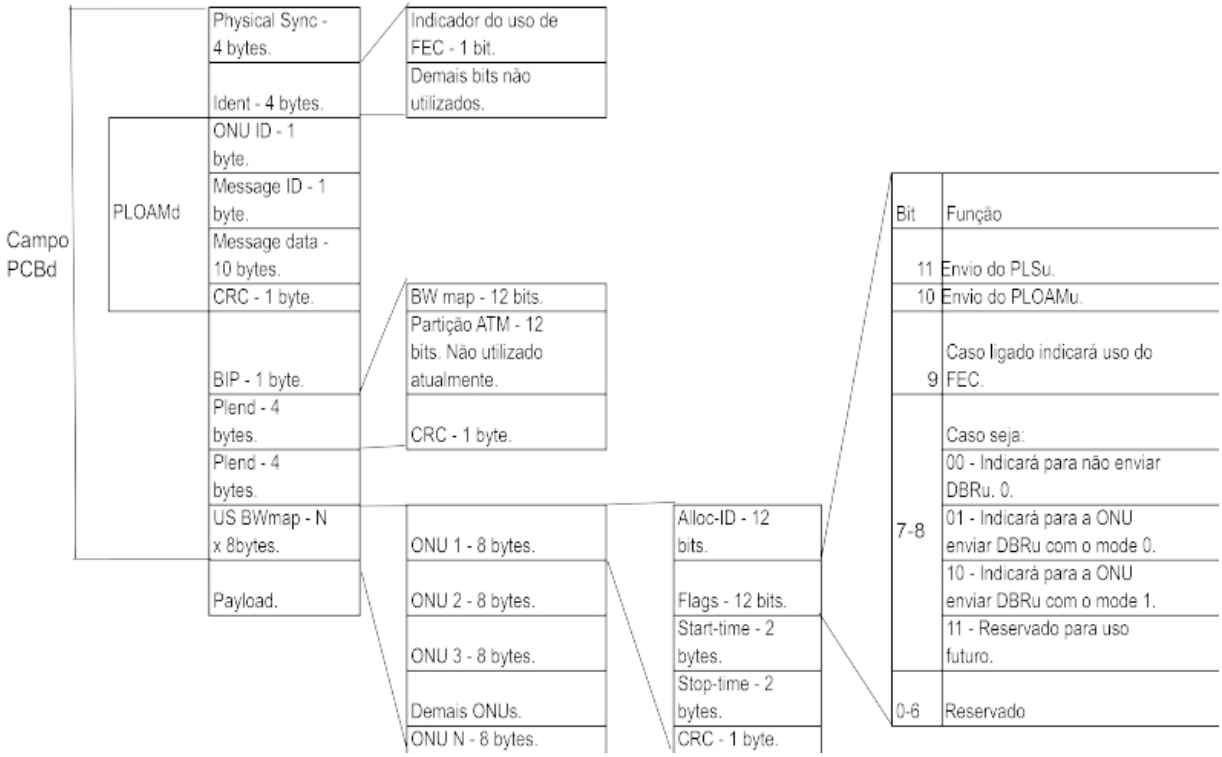



*Figura 17.7 – Formato do quadro GTC no sentido de download.*

O canal OMCI trata das mensagens enviadas e analisadas por camadas superiores à camada GTC. Por esse canal, segue toda a configuração aplicada a uma determinada ONU. Essas mensagens são necessárias e utilizadas pela arquitetura GPON para se autogerenciar. Tais mensagens são trocadas entre cada uma das portas PON presentes no OLT e as ONUs.

As ferramentas de gerência, como U2000, da Huawei, e NetHorizhon, da Zhone, são responsáveis por interagir com as ONUs por meio do canal OMCI. Como consequência dessa comunicação, poderemos rapidamente em um ambiente gráfico analisar o que ocorreu ou ocorre com uma específica ONU. É importante observar que o plano C/M entrega à interface OMCI as mensagens para que possam ser processadas pelas camadas superiores à camada GTC. A camada de adaptação GEM (*GPON Encapsulation Method*) atua de forma intermediária entre a camada GTC e a interface OMCI. Essa camada de adaptação no sentido de

download recebe os dados do canal OMCI e os repassa à camada GTC, que o enviará à ONU. No sentido de upload, a camada de adaptação GEM faz o processo inverso: recebe os quadros da camada GTC e os repassa à camada de adaptação OMCI. A figura 17.8 apresenta as camadas da arquitetura GPON:

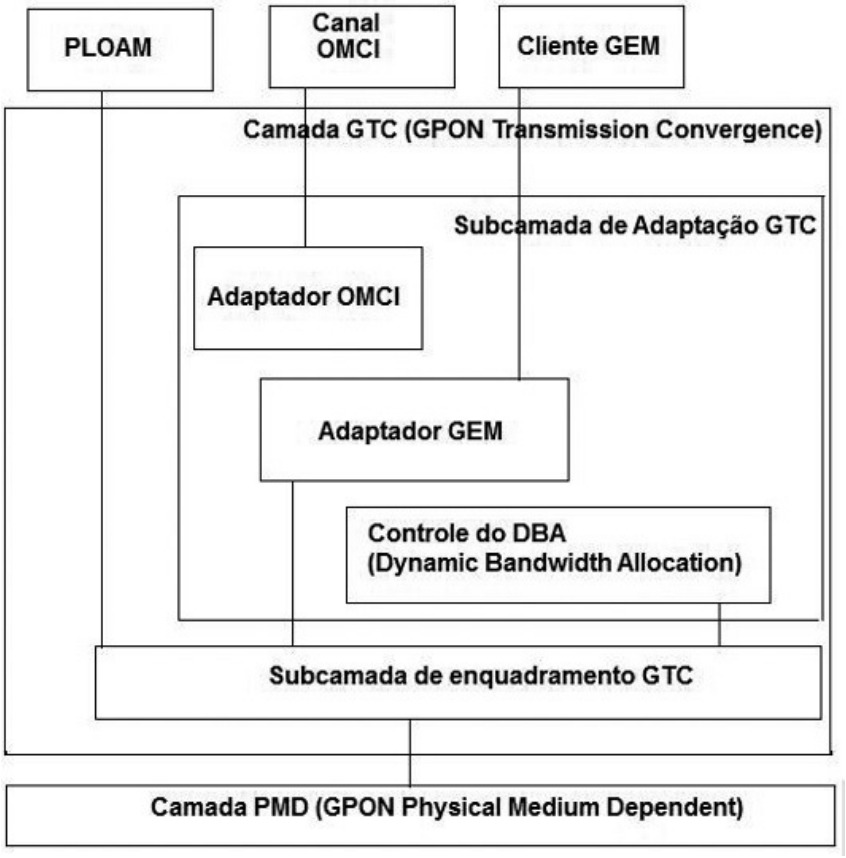



*Figura 17.8 – Camada física, camada GTC e suas interfaces.*

**Plano U**

O plano de usuário (*U-plane*) é responsável por transportar os dados dos clientes sobre a rede GPON. Os fluxos de dados de cada cliente serão relacionados a um GEM *port* ID. Baseando-se na plataforma Huawei, ao adicionarmos o *service port* à ferramenta U2000, teremos que escolher o GEM *port* ID, previamente configurado pelo administrador da rede. Com isso, o fluxo de dados de cada cliente será identificado da seguinte forma: *Frame* ID/*slot* ID/*port* ID/ONU ID/GEM *port* ID (ex.: 0/2/45/60/10). Vejamos o que cada item representa:

- *Frame* ID – Identifica a caixa (*shelf*) e normalmente vale 0.
- *Slot* ID – Representa a posição em qua a placa foi instalada no OLT. Inicia em 1 e pode serguir até a quantidade de slots disponíveis no OLT.
- *Port* ID – Representa a porta da placa utilizada. Na plataforma Huwei, temos em torno de sete portas por placa.
- ONU ID – Representa a posição lógica da ONU na porta do OLT. Pode variar entre 0 e 127.
- GEM *port* ID – Representa um identificador e pode variar entre 1 e 4.095. Esse identificador ficará associado a um T-CONT fixo ou dinâmico. Para cada T-CONT, teremos uma banda associada definida por um DBA *profile* (perfil DBA). Abordaremos os detalhes do T-CONT e do algoritmo DBA neste capítulo. Em um caso prático utilizado por um operadora estadual, vejamos a relação entre o GEM *port* ID, T-CONT e DBA.
  - Para o serviço de acesso à Internet, foram definidos para utilizar o GEM *port* ID 10 e T-CONT dinâmico com banda de 100 Mbps (a banda é definida por um DBA *profile*). O termo dinâmico significa que caso uma ONU esteja inativa ou com pouco tráfego, o espaço utilizado para transmissão dos dados no sentido de upload poderá ser alocado para outra ONU.
  - Para o serviço de acesso ao VoIP, foram definidos para utilizar o GEM *port* ID 20 e T-CONT com banda de 1 Mbps fixo. O termo fixo significa que teremos 1 Mbps alocado para cada uma das ONUs, para transmitir seus dados no sentido de upload. Se a ONU usar ou não o espaço reservado de 1 Mbps, este sempre ficará reservado.
  - Nos demais serviços oferecidos na rede GPON, como RAVs (Redes de Alta Velocidade que interligam duas ou mais extremidades das rede de um cliente), foram definidos para utilizar GEM port ID 30 e T-CONT de 100 Mbps variável. É importante observar que caso tenhamos algum cliente que utilize uma banda maior, como 400 Mbps (simétrico, com download e upload iguais), precisaremos criar um GEM *port* ID específico e

relacioná-lo a um T-CONT e DBA *profile* também específicos. Nesse caso, a utilização de um cliente poderá prejudicar os demais, pois, conforme comentado, a velocidade de upload é de 1,25 Gbps. Poderemos associar múltiplas ONUs com um único GEM *port* ID ou criar identificadores específicos (para isso, existem 4.095 possíveis) para clientes que possuam necessidade de banda específica. É importante observar que cada GEM *port* ID está intimamente relacionado a um T-CONT e, por sua vez, a um DBA *profile*.

O campo *port* ID está contido no cabeçalho do quadro GEM. Conforme observamos, o campo *port* ID é composto de 12 bits, assim podemos criar até 4.096 diferentes identificadores (de 0 até 4.095). A figura 17.9 demonstra o cabeçalho do quadro GEM e a posição do campo *port* ID.

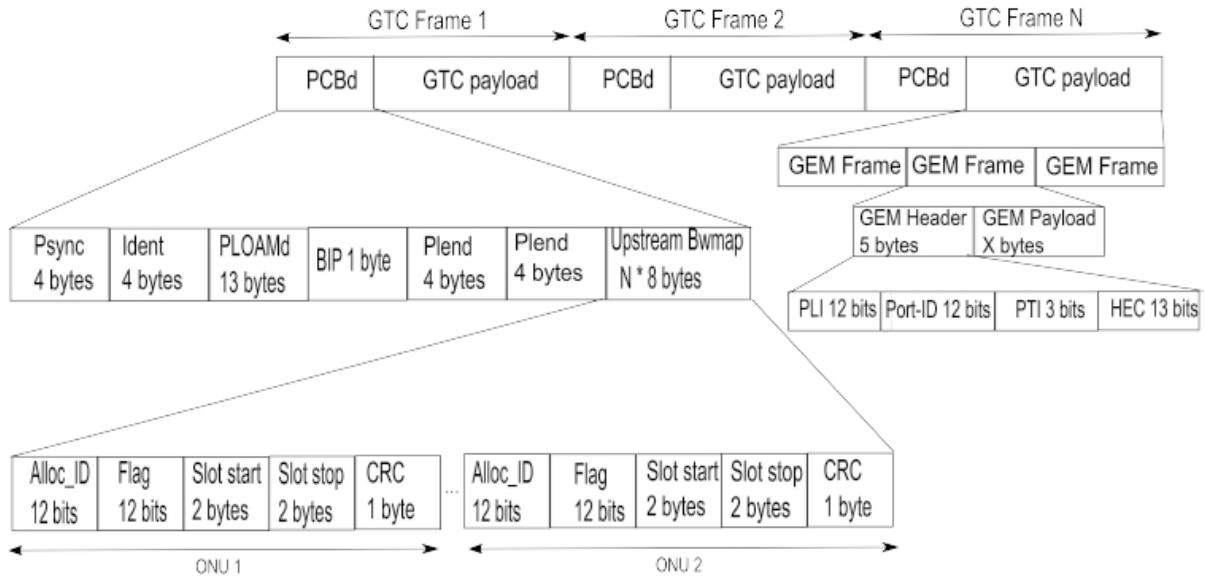



*Figura 17.9 – Cabeçalho do quadro GEM.*

### 17.4.3.3 T-CONT – Transmission Containers

Cada ONU instalada na rede GPON passa a ser identificada por um identificador conhecido por ONU-ID. Durante a ativação de um novo cliente, para cada serviço oferecido pela ONU, define-se um GEM *port* ID, que, por sua vez, sempre estará relacionado a um T-CONT e a um DBA *profile*.

Os T-CONTs são utilizados para relacionar o GEM *port* ID com o

DBA *profile*. Com isso, cada um dos serviços oferecidos pela ONU utilizará uma banda previamente configurada e negociada com o OLT durante o processo de *ranging*. A figura 17.10 apresenta a relação entre o T-CONT e o GEM *port* ID.

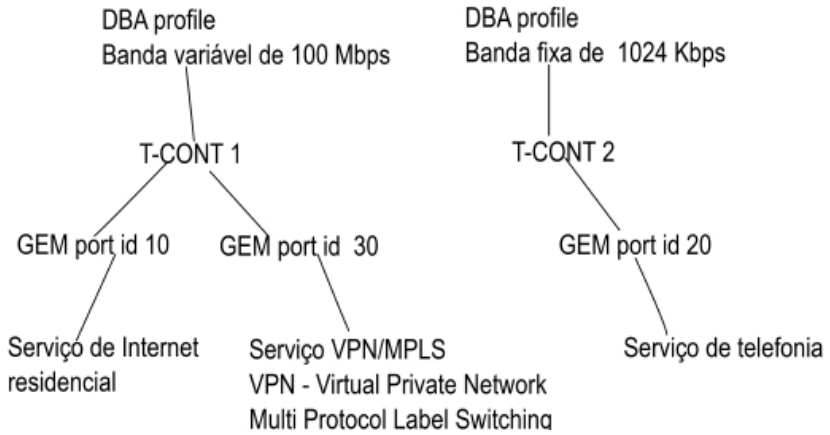



*Figura 17.10 – Relação entre T-CONT e GEM port ID.*

Na prática, utilizamos o T-CONT para o tráfego de upload e este deverá ser criado no OLT. Utilizando a plataforma Huawei como exemplo, veja como formamos o T-CONT.

Primeiramente, criamos um DBA *profile* (15 representa 400 Mbps) com os seguintes comandos:

dba-profile add profile-id 15 profile-name "400Mbps" type1 fix 410000

- Mensagem recebida de retorno do OLT: *Attention: DBA-profile bandwidth value 410000 has been adjusted to 409984*.

dba-profile add profile-id 13 profile-name "gerencia" type1 fix 1024

Ao criar o DBA *profile*, podemos utilizar a velocidade que for necessária. Caso a operadora comercialize serviços de 100 Mbps, podemos substituir a velocidade de 400 Mbps por 100 Mbps. Outro elemento a que devemos prestar atenção é o parâmetro *type*. Quando utilizamos *type4 max* 410000, a alocação do DBA será dinâmica, enquanto se utilizarmos *type1 fix* 410000, a alocação do DBA será fixa. Quando se utiliza dinâmica, os slots de tempo não utilizados por uma ONU para transmitir dados no sentido de upload poderão ser utilizados por outras ONUs que possuam rajadas. Caso sejam fixos, os *slots* de tempo no sentido upload ficarão reservados continuamente, não podendo ser utilizados por outras ONUs.

Em seguida, criamos os T-CONTs e os relacionamos com o DBA *profile*. Na plataforma, a criação do T-CONT ocorre dentro de um *ont-lineprofile*. Na tabela 17.2, apresentamos a criação de 2 T-CONTs, sendo um para gerência da rede e um segundo para atender a um cliente específico que trafegará sobre 400 Mbps.

*Tabela 17.2 – Configuração de um line profile para receber 400 Mbps de banda*

| Comando | Descrição |
|---|---|
| ont-lineprofile gpon profile-id 3 profile-name “EHSN400M” | Acessa o modo de configuração do profile 3. |
| tcont 1 dba-profile-id 13 | Utilizado para gerência com banda de 1 Mbps. |
| tcont 2 dba-profile-id 15 | Utilizado para o tráfego do cliente de 400 Mbps. Associado ao dbaprofile com id 15, apresentado no comando anterior. |
| Gem add 80 eth tcont 2 encrypt on | Relaciona o GEM port ID 80 com o TCONT 2. |
| Gem mapping 80 0 vlan 80 | Relaciona o GEM port ID com a VLAN 80. |
| Commit | Confirma para o OLT os comandos. |
| Quit | Sai do prompt da criação do ont-lineprofile. |

Para finalizar, precisamos relacionar a VLAN criada no *ont-lineprofile* com as portas da ONU que ficará instalada no cliente. Dado que a ONU tenha quatro portas Ethernet, precisaremos informar que poderão ser utilizadas pela VLAN 80. Para isso, criamos um *ont-srvprofile*. Vejamos os comandos na tabela 17.3.

*Tabela 17.3 – Configuração de um server profile para receber 400 Mbps de banda*

| Comando | Descrição |
|---|---|
| ont-srvprofile gpon profile-id 11 profile-name “HG863 – EHSN400M” | Acessa o modo de configuração do ont-srvprofile. |
| Ont-port eth 4 | Informa que a ONU possui quatro portas Ethernet. |

| Comando | Descrição |
|---|---|
| multicast-forward untag | Libera o tráfego multicast. |
| port vlan eth 1 translation 80 user-vlan 80 | Relaciona a porta 1 a VLAN 80. |
| port vlan eth 2 translation 80 user-vlan 80 | Relaciona a porta 2 a VLAN 80. |
| port vlan eth 3 translation 80 user-vlan 80 | Relaciona a porta 3 a VLAN 80. |
| port vlan eth 4 translation 80 user-vlan 80 | Relaciona a porta 4 a VLAN 80. |
| Commit | Confirma os comandos. |
| Quit | Sai do ambiente de ont-svrprofile. |

Os comandos anteriores foram utilizados para criar um ambiente para um cliente com 400 Mbps poder transmtir seus dados. O DBA *profile* (identificado como 15) foi configurado para oferecer 400 Mbps. Entretanto, normalmente para os clientes Internet, criamos um DBA *profile* de 100 Mbps e os respectivos T-CONTs. Vejamos o comando para este caso:

```
dba-profile add profile-id 11 profile-name "100MbpsDinamico" type4 max 100032
```

- Acessa o ambiente *dba-profile*. Os T-CONTs de usuários de acesso à Internet precisarão se relacionar com o DBA *profile* específico. Vejamos na tabela 17.4 os comandos necessários.

*Tabela 17.4 – Configuração de um dba profile para receber 100 Mbps de banda*

| Comando | Descrição |
|---|---|
| ont-lineprofile gpon profile-id 1 profile-name “Internet” | |
| tcont 1 dba-profile-id 13<br>tcont 4 dba-profile-id 11 | DBA profile com banda 1 Mbps alocado para gerência.<br>DBA profile com banda 100 Mbps alocado dinamicamente. |
| Gem add 10 eth tcont 4 encrypt on | |
| Gem mapping 10 0 vlan 10 | |
| Commit | |

Para finalizar, precisamos relacionar a VLAN criada no *ont-lineprofile* com as portas da ONU que ficará instalada no cliente. Dado que a

ONU tenha quatro portas Ethernet, precisaremos informar que poderão ser utilizadas pela VLAN 10. Para isso, criamos um *ont-srvprofile*. Vejamos os comandos na tabela 17.5:

*Tabela 17.5 – Configuração de um server profile para receber 100 Mbps de banda*

| Comando | Descrição |
|---|---|
| Ont-srvprofile gpon profile-id 1 profile-name “HG850a – VoIP e Internet” | Acessa o ambiente de ont-svrprofile. |
| Ont-port pots 2 eth 4 catv 1 | ONT possui duas portas para VoIP, quatro portas de rede Ethernet e uma interface para TV. |
| multicast-forward untag | Libera tráfego multicast. |
| port vlan eth 1 translation 10 user-vlan 10 | Relaciona a porta 1 a VLAN 10. |
| port vlan eth 2 translation 10 user-vlan 10 | Relaciona a porta 2 a VLAN 10. |
| port vlan eth 3 translation 10 user-vlan 10 | Relaciona a porta 3 a VLAN 10. |
| port vlan eth 4 translation 10 user-vlan 10 | Relaciona a porta 4 a VLAN 10. |
| Commit | Confirma os comandos. |
| quit | Sai do ambiente de ont-svrprofile. |

É importante observar, na especificação ITU-T, que existem cinco tipos de T-CONTs disponíveis para utilização. O uso desses conceitos poderá ou não ser aplicado em um ambiente prático. Vejamos os cinco tipos citados pela especificação:

- O T-CONT tipo 1 conduz dados com uma banda fixa. Utilizado por aplicações sensíveis ao tempo, como transmissão de voz. Em nosso exemplo, utilizamos o T-CONT 1 para o tráfego de dados de gerência.
- O T-CONT tipo 2 conduz dados com uma banda assegurada. Utilizado para aplicações que necessitam de alta prioridade, como transmissão de vídeo. Em nosso exemplo, utilizamos o T-CONT 2 para o tráfego de dados de um cliente estratégico para a operadora.
- O T-CONT tipo 3 conduz dados com uma banda não assegurada. Utilizado para aplicações que podem ter certo atraso que não

afetam sua qualidade, como transmissão de arquivos de dados. Pouco utilizado na prática.

- O T-CONT tipo 4 conduz dados com uma banda seguindo modelo de melhor esforço. Utilizado para aplicações que não tenham problemas com atraso, como acesso a Internet e email. Em nosso exemplo, utilizamos o T-CONT 4 para o tráfego de dados de um cliente estratégico para a operadora.
- O T-CONT tipo 5 mescla todos os tipos citados. É pouco utilizado na prática.

É importante observar que na plataforma Zhone, o T-CONT é chamado de GTP (*GPON Traffic Profile*). A configuração dele é realizada pela ferramenta de gerência e integra também a criação do *profile* do DBA.

#### 17.4.3.4 Funções-chave da camada GTC

A camada GTC é responsável por controlar o acesso ao meio físico entre as ONUs e o OLT no sentido de download e upload. No sentido de download, o fluxo segue o modelo de *broadcast* e, assim, todas as ONUs recebem o mesmo tráfego, porém, devido às chaves de segurança, somente processam o que for devido. Entretanto, no sentido de upload, permite-se que múltiplos usuários compartilhem o mesmo meio físico sem problemas de colisão ou atrasos. É imporntante observar que os quadros enviados no sentido de download contêm dentro do campo *BWmap* (Mapa de Banda – *Bandwidth map*) todas as posições que cada ONU utilizará durante o tráfego de upload.

### 17.4.4 Detalhes do quadro GTC no sentido de download

O quadro enviado pela rede GPON no sentido de download (do OLT para as ONUs) é composto dos campos PCBd (*Physical Control Block download*) e *payload* (contêm os headers das camadas superiores e os dados propriamente ditos) conforme demonstrado pela figura 17.7.

#### 17.4.4.1 Campo PCBd

O tamanho do campo PCBd dependerá da quantidade de ONUs instaladas na porta PON do OLT. Dentro do campo PCBd, temos o campo *BWmap* que transporta parâmetros de cada uma das ONUs instaladas, ou seja, dependendo da quantidade de ONUs, o tamanho do campo PCBd poderá variar. O campo PCBd contém diversos campos e, conforme comentado, a ONU transmite o campo PCBd no sentido de download em *broadcast* a todas as ONUs. Cada ONU receberá interiramente o campo PCBd e fará o recebimento apenas dos quadros que tiverem uma chave igual a sua. A figura 17.7 apresenta os detalhes que compõem o campo PCBd.

É importante observar que podemos dividir esse campo em uma parte fixa e em uma variável. A parte fixa contém os campos *Physical Sync*, *Ident* e PLOAM. Esses campos são protegidos por um byte chamado BIP (*bit-interleaved parity check*). Vejamos o que cada um representa:

- *PSync* (*Physical Synchronization* – 4 bytes) – Informa à ONU que o receberá o início do quadro GTC. Como ocorre com o preâmbulo do padrão Ethernet que é composto de 7 bytes contendo os bits 10101010, este campo contém formato hexadecimal igual a 0xB6AB31E0.
- *Ident* (Identificador – 4 bytes) – É composto de 4 bytes, porém atualmente se utiliza apenas o primeiro bit que informa à ONU se o quadro transmitido utiliza ou não *Forward Error Correction* (FEC).
- **PLOAM** (*Physical Layer Operations, Administration and Management* – 13 bytes) – Tem a função de transportar mensagens necessárias para a configuração e gestão das ONUs. A tabela 17.6 apresenta em detalhes as principais mensagens PLOAM. O campo PLOAM está dividido em:
  - **ONU ID** (1 byte) – Representa um valor inteiro que o OLT definirá à ONU, durante o processo de *ranging*, por meio da mensagem PLOAM. Essa identificação será utilizada pelo OLT quando o quadro seguir no sentido de upload. Na prática, esse valor inicia em 1 e segue até 64, ou, ainda, poderá se estender até 128, caso a operadora opte por instalar 128 clientes em uma única porta do OLT. Quando o quadro for enviado no sentido de download, o

campo ONU ID será definido com o valor 255 (hexadecimal igual a 0xFF), que o identifica como *broadcast*.

- **Message ID** (1 byte) – Identifica o tipo da mensagem que está sendo enviada. Na tabela 17.6, apresentamos os tipos de mensagens transportadas pelo campo PLOAM.
- **Message Data** (10 bytes) – Contêm o texto da mensagem enviada.
- **CRC** (1 byte) – Utilizado para validar se o campo PLOAM não foi recebido com erro no destino.

O campo PLOAM, conforme comentado, transporta mensagens relacionadas às camadas físicas e de enlace de uma rede GPON. As mensagens transportadas podem ser relacionadas ao sentido download e outras, relacionadas ao sentido upload. A tabela 17.6 apresenta as mensagens PLOAM enviadas no semtido de download.

*Tabela 17.6 – Mensagens PLOAM enviadas no sentido de download*

| Seq | Nome da mensagem | Detalhes da mensagem |
|---|---|---|
| 1 | Upstream_ Overhead | Função: no momento da instalação da ONU, algumas informações precisam ser assumidas para que a comunicação ocorra. Assim, o OLT envia a ONU que esta deverá pré-indicar um valor de delay e um valor em bytes para o preâmbulo, quando esta gerar um quadro de resposta no sentido de upload. Nesta mensagem, a ONU também ajusta a potência óptica. |
| | | Enviada no início do processo de ativação da ONU. |
| | | Quantidade de vezes que é enviada: três vezes, por questões de robustez da arquitetura GPON. |
| | | Efeitos ao ser recebida: a ONU define os parâmetros para que um quadro de retorno possa ser devolvido ao OLT. |

| Seq | Nome da mensagem | Detalhes da mensagem |
|---|---|---|
| 2 | Assign_ ONU-ID | Função: esta mensagem relacionará um identificador (ONU ID) livre com o número serial da ONU. |
| | | Enviada quando o OLT identifica um novo número serial de uma ONU, ou seja, quando o OLT recebe um quadro com número serial sem um identificador (OT-ID), o OLT efetua o relacionamento. |
| | | Quantidade de vezes que é enviada: três vezes. |
| | | Efeitos ao ser recebida: a ONU com o respectivo número serial seta o campo ONU-ID e o campo Alloc-ID com o identificador escolhido. |
| 3 | Ranging_ Time | Função: após o OLT confirmar a relação do número serial e o ONU ID, o OLT informará por meio da mensagem Ranging Time o tempo de equalização entre o OLT e a ONU. Primeiramente, o OLT calcula o RTD (Round Trip Delay) durante o processo de ranging. Em seguida, define o tempo de equalização. O tempo de equalização, conhecido por EqD, é definido a cada uma das ONUs. Esse valor é calculado por Teqd - RTD, em que Teqd é um valor fixo que dependerá da distância máxima entre as ONUs e a porta PON. Digamos que a distância máxima seja 20 km, assim Teqd será 200 milissegundos. |
| | | Enviada pelo OLT inicialmente após concluir o relacionamento entre o número serial e o ONU ID. Será enviada também em outros momentos caso o OLT perceba que o delay precisa ser atualizado. |
| | | Quantidade de vezes que é enviada: três vezes. |
| | | Efeitos ao ser recebida: a ONU define seu EqD. |
| 4 | Deactivate_ONU-ID | Função: informa a uma ONU identificada com um ONU ID para de enviar dados no sentido de upload e, ainda, reinicia a ONU. |
| | | |

| Seq | Nome da mensagem | Detalhes da mensagem |
|---|---|---|
| | | Enviada quando a ONU percebe alarmes relacionados a LOS (Loss of Signal), LOF (Loss of Frame), LCD (Loss of Channel Delineation), LOA (Loss of Acknowledgement) e SUF (Start Up Failure). |
| | | Quantidade de vezes que é enviada: três vezes. |
| | | Efeitos ao ser recebida: a ONU com o respectivo ONU ID desliga o laser; o ONU ID, OMCI Port-ID e todos os Alloc-ID definidos são descartados e a ONU move-se para o estado de standby. |
| 5 | Disable_ Serial_ Number | Função: habilitar e desabilitar uma ONU com seu respectivo número serial. |
| | | Enviada por meio de um comando a partir da console do OLT ou de forma gráfica por meio do NetHorizhon, da Zhone, ou U2000, da Huawei. |
| | | Quantidade de vezes que é enviada: três vezes. |
| | | Efeitos ao ser recebida quando for para desabilitar: move a ONU para o estado de Emergency Stop. A ONU não responderá ao OLT por alocação de banda para transmitir no sentido de upload.<br>Efeitos ao ser recebida quando for para habilitar: move a ONU para o estado de standby. A ONU reinicia o processo de ativação. |
| 6 | Encrypted_Port-ID | Função: mensagem enviada para informar quais canais estão ou não encriptados. |
| | | Enviada quando um novo canal deve ou não ser encriptado. |
| | | Quantidade de vezes que é enviada: três vezes. |
| | | Efeitos ao ser recebida. Marca ou desmarca um determinado canal como encriptado ou sem encriptação. Ao receber uma menagem e considerando-a correta, retorna um acknowledge. |

| Seq | Nome da mensagem | Detalhes da mensagem |
|---|---|---|
| 7 | Request_ Password | Função: mensagem utilizada para solicitar a senha armazenada por uma ONU a fim de ser verificada pelo OLT. O OLT possui uma tabela local com todas as senhas de suas ONUs conectadas. |
| | | Enviada após a ONU concluir o processo de ranging. Esta mensagem é opcional do ponto de vista do OLT em solicitar e mandatória do ponto de vista da ONU em enviar. |
| | | Quantidade de vezes que é enviada: uma vez. |
| | | Quando a senha é solicitada pelo OLT, será enviada três vezes pela ONU. |
| 8 | Assign_ Alloc-ID | Função: indica à ONU que um Alloc-ID será relacionado a esta. |
| | | Enviada quando o OLT identifica que múltiplos T_CONTs são suportados pela ONU. |
| | | Quantidade de vezes que é enviada: três vezes. |
| | | Como efeito, enviará um quadro de acknowledge após cada mensagem que for recebida corretamente. A ONU responderá a sua alocação de banda com seu respectivo Alloc-ID. Até que o T-CONT esteja corretamente mapeado ao Alloc-ID, idle GEM frames deverão ser enviados. |
| 9 | No message | Indica que quando o campo PLOAM está sendo transmitido não existem mensagens disponíveis. |
| | | Enviada quando a fila de mensagens está vazia. |
| 10 | POPUP | Função: o OLT, quando envia esta mensagem em broadcast, força todas as ONUs que estejam no estado de POPUP e não estejam nos estados de LOS (Loss of Signal)/LOF (Loss of Frame) a alternarem para o estado de ranging. Pode ainda direcionar uma específica ONU para o estado de operação caso a mensagem de POPUP venha direcionada a um ONU ID. |
| | | Enviada para acelerar a ativação de ONUS que estejam no estado de LOS. |
| | | |

| Seq | Nome da mensagem | Detalhes da mensagem |
|---|---|---|
| | | Quantidade de vezes que é enviada: três vezes. |
| | | Como efeito, ao ser recebida, temos que a ONU mudará seu estado para ranging ou para estado de operação. |
| 11 | Request_ Key | Função: o OLT requisita à ONU para gerar uma nova chave de segurança encriptada e enviá-la no sentido de upload. |
| | | Enviada sob demanda. |
| | | Quantidade de vezes que é enviada a solicitação: uma vez. |
| | | Quantidade de vezes que é enviada a chave encriptada pela ONU: três vezes. |
| 12 | Configure Port-ID | Função: esta mensagem relaciona um canal interno gerado na camada OMCI com o valor do GEM port ID utilizado pela ONU para transportar seus dados entre a arquitetura GPON e a Ethernet. O GEM port ID é anexado ao header do quadro GEM e utilizado como um mecanismo de endereçamento para relacionar um canal da camada OMCI com um canal da camada GEM. |
| | | Enviada quando uma nova ONU é configurada por uma plataforma de configuração, como U2000 ou NetHorizhon. |
| | | Quantidade de vezes que é enviada a solicitação: três vezes. |
| | | Cada GEM port ID é relacionado pelo OLT a um canal lógico provido pela camada OMCI por meio do OMCC (ONU Management and Control Channel). Esse canal é utilizado pelo OLT para interagir com cada ONU, respeitando as suas características de configuração. Após cada mensagem ser recebida com sucesso, a ONU retorna um acknowledge. |
| 13 | Physical_ Equipment_ | Função: indica às ONUs que o OLT é incapaz de enviar quadros GEM e quadros OMCC. |
| | | |

| Seq | Nome da mensagem | Detalhes da mensagem |
|---|---|---|
| | Error (PEE) | Enviada quando o OLT detecta que não consegue enviar quadros à ONU. |
| | | Enviada uma vez por segundo. |
| | | Mensagem é processada pela ONU que registra um alarme de erro. |
| 14 | Change_Power_Level | Função: OLT informa à ONU para aumentar ou diminuar seu nível óptico de transmissão. |
| | | Enviada quando o OLT detecta que o nível óptico da ONU está abaixo ou acima dos limites definidos no estado de ranging. |
| | | Enviada uma vez. |
| | | Quando recebida, a ONU ajusta sua potência óptica. |
| 15 | PST message Passive optical network Section Trace message | Função: verificar se a conectividade entre a ONU e a OLT está adequada. Caso perceba alguma anormalidade, esta mensagem poderá disparar um chaveamento automático de proteção (APS – Automatic Protection Switching). |
| | | Enviada periodicamente, como também após uma falha ser identificada. |
| | | Enviada uma vez por segundo. |
| | | Uma rede GPON tem a capacidade de automaticamente alternar para uma outra fibra caso a comunicação por uma das fibras venha apresentar problemas. Assim que uma ONU detecta a perda de sinal do sentido de download, a ONU envia um alarme de perda de janela (LOW – Loss of Window) para o OLT. Como resultado, o OLT automaticamente chaveia todas as ONUs para a fibra de proteção que será atendida por outra porta PON. |
| 16 | BER Interval Bit Error Ratio Interval | Função: define o tempo que uma determinada ONU acumulará erros relacionados aos quadros recebidos do sentido de download. |
| | | |

| Seq | Nome da mensagem | Detalhes da mensagem |
|---|---|---|
| | | Quantidade de vezes que é enviada a solicitação: três vezes. |
| | | Ao ser recebida, a ONU inicia um contador de tempo e acumula os erros que tenham sido recebidos dos quadros de download. Para cada mensagem recebida com sucesso, um acknowledge é enviado. |
| 17 | Key_Switching_Time | Função: o OLT informa a ONU quando deverá utilizar uma nova chave de segurança encriptada. |
| | | Enviada quando o OLT estiver pronta para trocar a chave de segurança. |
| | | Quantidade de vezes que é enviada a solicitação: Enviada 3 vezes |
| | | Quando recebida a ONU prepara-se para chavear e utilizar a nova chave. Será enviado 1 acknowledge após cada mensagem recebida com sucesso.. |

A seguir, abordaremos os demais campos utilizados pelo quadro GTC no sentido de download.

- BIP (*Bit Interleaved Parity* – 1 byte) – Utilizado para detectar erros. Cada ONU, ao enviar um quadro ao OLT, calcula o bit de paridade. Quando o OLT recebe o quadro, refaz o cálculo e compara com o recebido da ONU, a fim de medir o número de erros do link. Caso exista diferença, será incrementada a variável ERR na ONU e no OLT. O valor do campo BIP será utilizado pelo monitoramento de bits errados chamado BER (*Bit Error Rate*). O BER serve para indicar a taxa de bits errados (quantidade enviada/bits com erro) transmitidos. O GPON, quando configurado pelo administrador de rede, poderá utilizar uma técnica chamada FEC (*Forward Error Correction*) que melhora o desempenho do BER. Para isso, com os bits trafegados, seguem bits redundantes que serão utilizados para corrigir os bits errados, ou seja, com o FEC será possível detectar e corrigir bits errados sem solicitar retransmissão.

Conforme comentado, o tamanho do campo PCBd dependerá da quantidade de ONUs instaladas na porta PON do OLT. Até o momento, abordamos os campos que formam a parte fixa do campo PCBd. A seguir, analisaremos os campos que compõem a parte variável conhecidos por *Plend* e *BWmap*.

- Plend (*Payload Length Downstream* – Indicador de comprimento do *payload* – 4 bytes (duas vezes)): este campo transporta o comprimento do campo *BWmap* (mapa de largura de banda), o tamanho da partição ATM (não utilizado atualmente) e o CRC. O *PLend* é enviado duas vezes por motivos de robustez da arquitetura GPON. Devido à importância desse campo, segue junto um campo para CRC que validará no receptor sobre se o que foi gerado foi recebido corretamente.
- US *BWmap* (*Upstream Bandwidth map* – Mapa de largura de banda – N * 8 bytes): este campo transporta o intervalo de tempo que cada ONU utilzará para transportar seus quadros no sentido de upload. Para isso, esse campo implementa um vetor, e cada coluna do vetor, contendo 8 bytes, carrega os dados de uma ONU. O termo N * 8 significa que teremos uma ou mais ONUs (de 1 a 128) e as informações relacionadas a cada uma delas serão transportadas em 8 bytes. A figura 17.11 apresenta um exemplo do formato do campo *BWmap*.

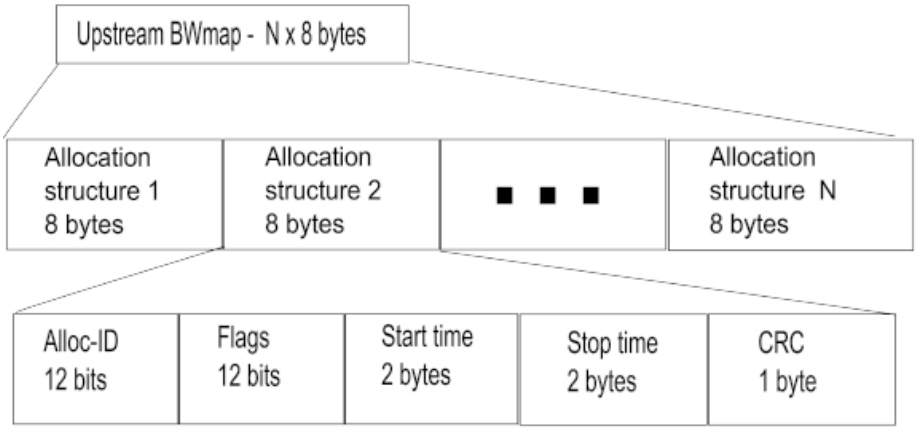



*Figura 17.11 – Formato do campo BWmap.*

Conforme observado no campo *BWmap*, cada coluna do vetor contém dados relacionados a uma única ONU. Para essa

identificação, o campo transporta o campo *Alloc-ID* que contém a identificação da ONU, o campo *flags* e, ainda, os campos *start time* (momento de início da transmissão) e *stoptime* (momento de fim da transmissão). Ao final, ainda transporta um campo de CRC para avaliar a integridade dos dados transmitidos. Os campos *start* e *stop time* são medidos em bytes e utilizados para o tráfego da ONU no sentido de upload.

No campo *flags* serão transportadas informações relacionadas à utilização ou não da técnica FEC presente no quadro enviado. Caso seja utilizado FEC, OLT e ONU precisarão se preparar para sua utilização. Conforme comentado no sentido de download, a utilização ou não do FEC segue pela variável *Ident*; no caso do sentido de upload, o OLT ligará o bit 9 do campo *flags*. Esse bit correponde à varíavel *Use*_FEC conforme registrado pela especificação ITU-T G984.3. Com o campo *flags*, podemos, ainda, permitir que o OLT requisite que a ONU envie informações do campo PLOAMu no sentido de upload. Para isso, utiliza-se o bit 10 ligado. O campo PLOAMu conterá a informação se o FEC está ou não habilitado, além de outras informações importantes ao gerenciamento do OLT com as ONUs.

O OLT pode também requisitar que a ONU envie informações relacionadas à alocação dinâmica de banda (DBRu – *Dynamic Bandwidth Report*). Caso a combinação entre os bits 7 e 8 seja:

- 00, o OLT informa à ONU para não enviar o campo DBRu no quadro GTC no sentido upload.
- 01, o OLT informa à ONU para enviar o campo DBRu no quadro GTC no sentido upload. Com essa combinação, utiliza-se o *Mode* 0, aplicada a *Alloc-Ids* sem limitação. Esse é o modo-padrão.
- 10, o OLT informa à ONU para enviar o campo DBRu no quadro GTC no sentido upload. Com essa combinação, utiliza-se o *Mode 1*, aplicada a *Alloc-Ids* com tráfego em melhor esforço.
- 11, é reservado neste momento.

Conforme comentado, dentro do campo PCBd temos o campo *BWmap*. Dentro do campo *BWmap,* o OLT envia apontadores

informando a cada ONU o momento de início e fim da sua transmissão. Dessa forma, a cada período de tempo, somente uma ONU terá acesso ao meio e não existirá colisão durante a transmissão no sentido de upload. Os apontadores de início e fim são dimensionados em bytes. A figura 17.12 apresenta um exemplo sobre como ocorre a comunicação no sentido de download e upload, informando valores para os campos que compõem o *BWmap*.

O quadro de download tem duração de 125 μs para qualquer taxa de download. Atualmente, as operadoras têm optado pelas redes GPON com taxa de 2.48832 Gbps (2,5 Gbps). Caso não existam dados a serem enviados, o quadro de download será enviado a fim de manter o tempo de sincronismo. A quantidade de bits que podem ser transferidos por cada quadro dependerá da velocidade do link.

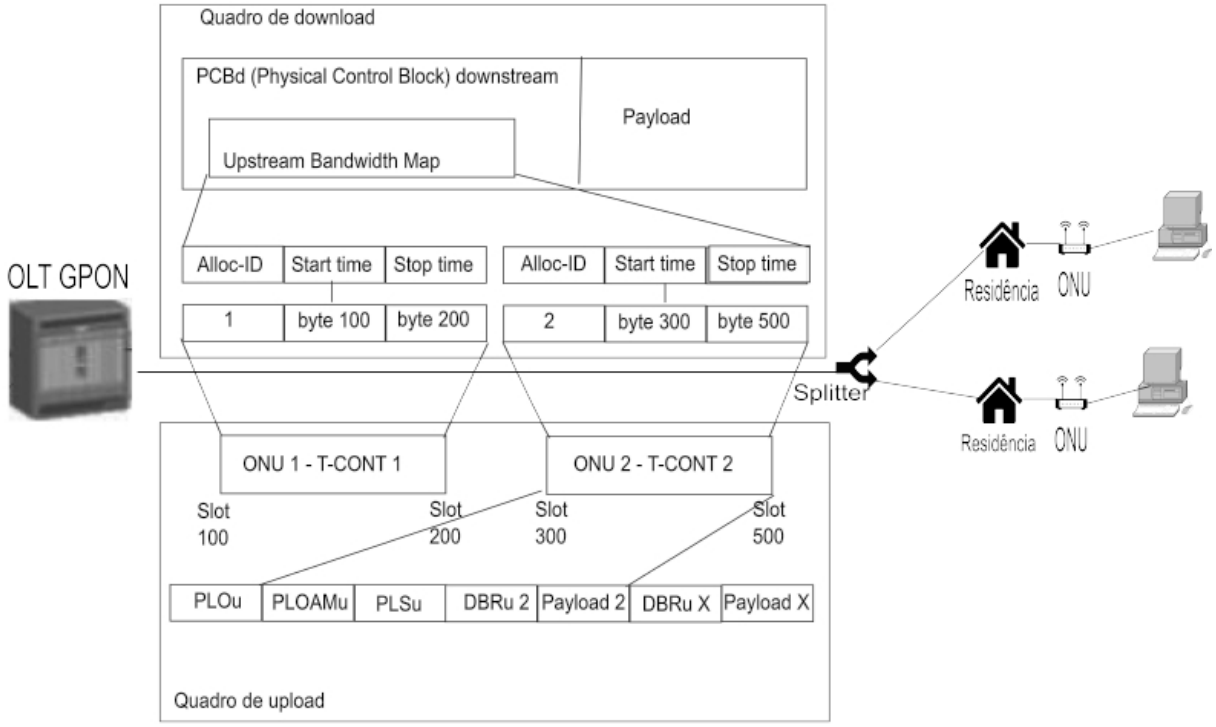



*Figura 17.12 – Quadro de download com campo BWmap.*

Levando-se em consideração que a taxa de download na rede GPON é exatamente 2.48832 Gbps, podemos transmitir 38.880 bytes por quadro. Para chegar ao valor de 38.880 efetuamos o

seguinte cálculo:

- Taxa de download em Gbps é igual a 2.488.320.000 bps.
- Converter a taxa de download em Gbps para bytes/s
  - Valor em bytes/segundo = 2.488.320.000 bps/8 bits
    - 2.488.320.000/8 = 311.040.000 bytes/s
  - Valor em bytes/s = 311.040.000 bytes/s
- Valor em bytes/s * 125 µs
  - Converter 125 µs em s = 0,000125 s
- 311.040.000 bytes/s * 0,000125 s = 38.880 bytes.

Assim, a cada 125 µs, uma porta GPON pode transmitir 38.880 bytes. O quadro de download, formado na camada GTC com duração de 125 µs e capacidade para transmitir 38.880 bytes, é composto de duas partes, sendo a primeira o campo PCBd (*Physical Control Block Downstream*) e a segunda o campo Payload. A figura 17.13 apresenta o formato do quadro GTC de download e o seu tempo.

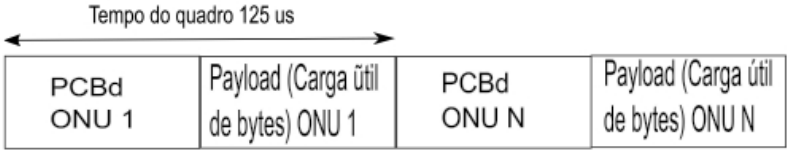



*Figura 17.13 – Composição do quadro de download e seu tempo.*

Conforme comentado e apresentado na figura 17.7, o tamanho do campo PCBd dependerá da quantidade de ONUs instaladas na porta PON do OLT. Até esse momento, apresentamos os campos que compõem o PCBd, levando-se em consideração a sua parte fixa e variável. A seguir, comentaremos sobre o campo *payload* presente no quadro GTC.

### 17.4.4.2 Campo payload

Ao final do campo *BWmap,* inicia-se o transporte do campo de *payload* do quadro GTC. O *payload* do quadro GTC é formado por uma série de quadros GEM (*GPON Encapsulation Method*) que têm as seguintes funções:

• Delinear os dados recebidos e enviados ao cliente.

• Relacionar o fluxo de dados as GEM *port* IDs.

A figura 17.14 apresenta os detalhes do campo *payload* e de sua composição através dos quadros GEM.

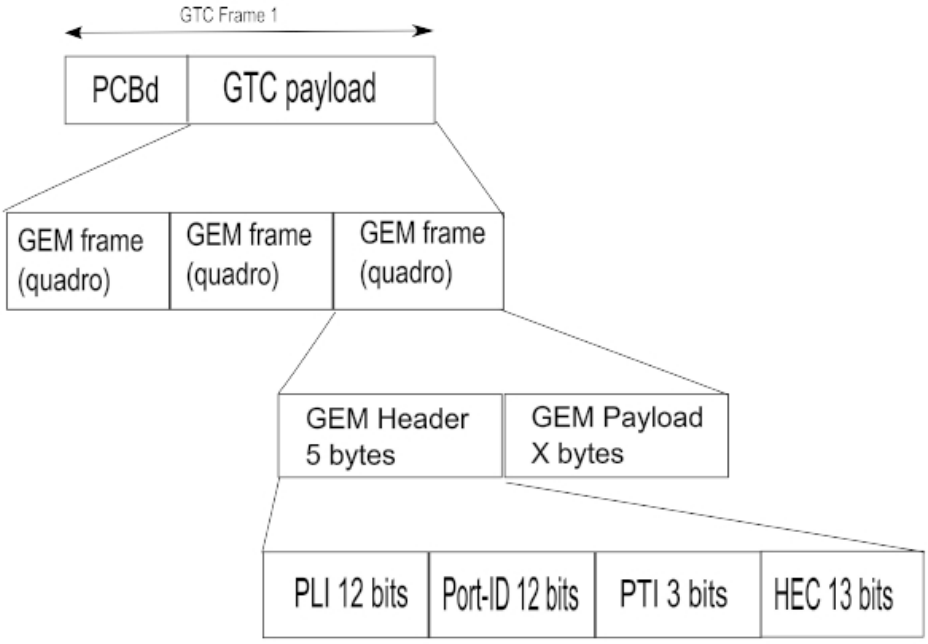



*Figura 17.14 – Composição do campo payload.*

O quadro GEM possui um *header* composto dos campos PLI (*Payload Length Indicator*), *Port-ID*, PTI (*Payload Type Indicator*) e HEC (*Header error Control*). Esse último é utilizado para avaliar se houve erro na transmissão do quadro GEM. Veja os detalhes de cada campo:

• **PLI** (*Payload Type Indicator*) – Indica o tamanho em bytes do campo GEM *payload* que seguirá o campo GEM *header*. Esse campo possui 12 bits, ou seja, podemos ter campos GEM *payload* com tamanhos de, no máximo, 4.096 bytes. Caso o quadro do cliente a ser transmitido seja maior que esse valor, o quadro do cliente será fragmentado em múltiplos quadros GEM. Ao informar o tamanho em bytes do campo GEM *payload,* será possível delinear onde começará o próximo header (*GEM header*). Essa informação será importante nos casos em que for necessário fragmentar. No processo de fragmentação, a rede GPON utiliza o campo PTI

(*Payload Type Indicator*) que informa se, após o primeiro quadro, existem ou não outros quadros sendo transmitidos.

- *Port* ID (GEM *port* ID) – Fornece identificadores de tráfego a fim de permitir que múltiplos serviços (Internet, VoIP, vídeo) sejam multiplexados pela mesma porta PON. Este campo é formado por 12 bits, permitindo termos 4.096 diferentes portas. Conforme comentado, cada GEM *port* ID está relacionado a um T-CONT, que, por sua vez, està relacionado a um DBA *profile*.
- **PTI** (*Payload Type Indicator*) – Composto de 3 bits. Este campo é utilizado para identificar caraterísticas do quadro GEM. Veja o que cada combinação dos bits desse campo pode informar:
  - **000** – Indica que o quadro do cliente está fragmentado e que não é o último, ou seja, existem outros quadros.
  - **001** – Indica que o quadro do cliente está fragmentado e que é o final do quadro.
  - **010** – Reservado.
  - **011** – Reservado.
  - **100** – Indica um quadro GEM OAM e que este não é o último.
  - **101** – Indica um quadro GEM OAM e que este é o último.
  - **110** – Reservado.
  - **111** – Reservado.

#### 17.4.4.3 Ethernet sobre o quadro GEM (GPON Encapsulation Method)

O GPON *Encapsulation Method* (GEM) fornece um mecanismo de mapeamento que permite transportar diferentes formatos de pacotes em uma rede GPON. O GEM permite que em uma rede GPON sejam transportados sobre o mesmo caminho físico quadros Ethernet e tráfego TDM contendo pacotes de voz. A figura 17.15 apresenta o formato do quadro comparando a transmisão de um quadro TDM e Ethernet.

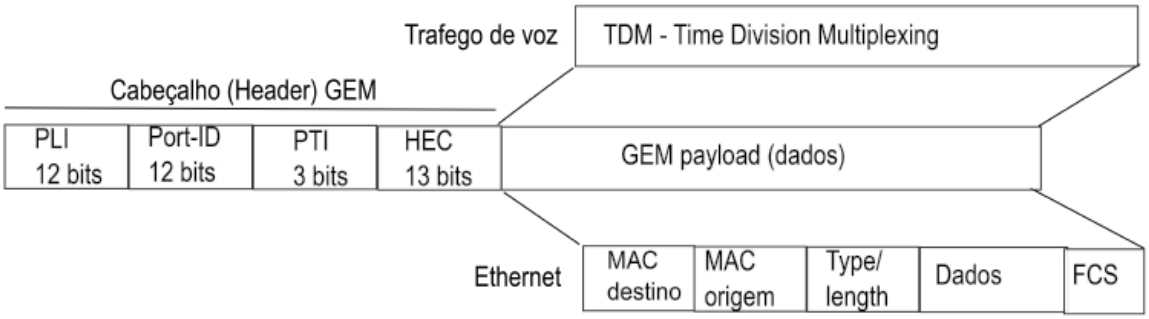



*Figura 17.15 – Diferentes pacotes sobre GEM.*

Conforme comentado e apresentado na figura 17.7, a segunda parte do quadro GTC (*payload*) será composta pelos dados de cada uma das ONUs conectadas à porta PON. Cada ONU transmitirá uma quantidade específica de dados que dependerá da banda alocada pela porta do OLT (ex.: 20 Mbps, 40 Mbps ou 100 Mbps). No caso da transmissão de um quadro Ethernet, os bytes que compõem os campos preâmbulo e SFD são descartados antes do encapsulamento feito pela camada GEM. Cada quadro Ethernet é mapeado para um ou múltiplos quadros GEM, dependendo da quantidade de bytes solicitada pelo usuário. A figura 17.16 apresenta a relação entre os campos do quadro Ethernet e os equivalentes no quadro GEM.

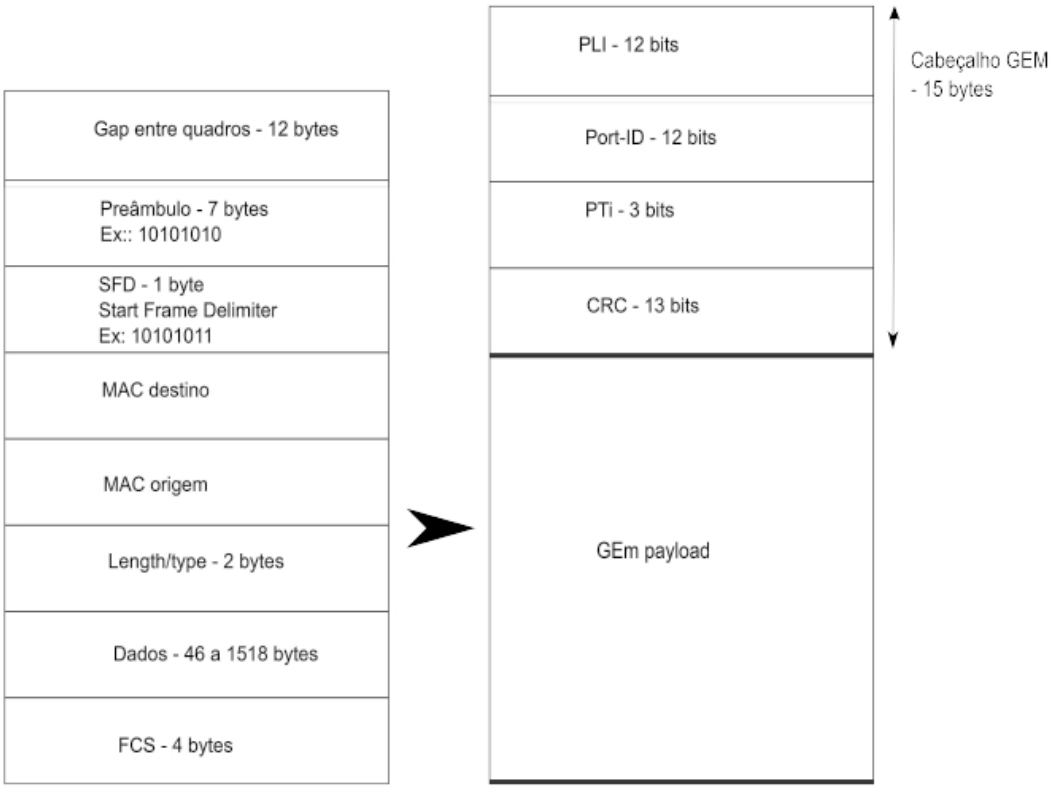



*Figura 17.16 – Relação entre o padrão Ethernet e o quadro GEM.*

## 17.4.5 Detalhes do quadro GTC no sentido de upload

O quadro GTC no sentido de upload também possui duração de 125 µs. Com uma banda de 1,24416 Gbps, cada quadro GTC poderá conter 19.440 bytes (a operação matemática é a mesma apresentada para o sentido de download). Cada quadro de upload contém a transmissão de dados de uma ou mais ONUs. O padrão GPON permite outras velocidades no sentido upload, porém, por padrão, muitas operadoras optaram por 1,24416 Gbps (1,25 Gbps).

O formato do quadro GTC no sentido de upload dependerá basicamente dos bits do campo *flag* pertencentes ao campo *BWmap* enviado pelo OLT a cada uma das ONUs. A figura 17.17 apresenta um exemplo dos campos do quadro GTC no sentido de upload. Nela, temos o quadro em dois formatos, demonstrando que dependendo do campo *flag,* esse quadro ficará modificado. Para a ONU A, foram transmitidos os campos PLOu (*Physical Layer Overhead*), PLOAM (*Physical Layer Operations, Administration and*

*Management*), PLS (*Power Leveling Sequence*) (não mais utilizado, conforme a especificação ITU T 984.3), DBRu (*Dynamic Bandwidth Report*) e Payload. Para a ONU B, apenas os campos PLOu, DBRu e *payload* foram necessários. Conforme comentado é por meio do campo *flag* que serão determinados os campos que serão enviados no sentido de upload.

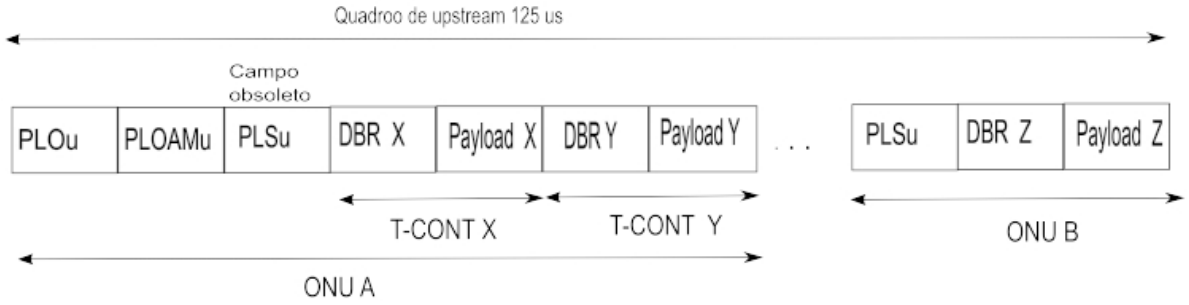



*Figura 17.17 – Formato do quadro GTC utilizado no sentido de upload.*

Conforme podemos observar na figura 17.17, a ONU A demonstra que está transmitindo dados relacionados a 2 T-CONTs, como Internet e VoIP, por exemplo. Por isso, possui os campos DBRu Y e *Payload* Y

Cada ONU utilizará um espaço do quadro GTC, envolvendo os campos PLOu, PLOAMu, DBRu e *payload* ou parte deles. O campo PLOu sempre estará presente, entretanto a transmissão ou não dos campos PLOAMu e DBRu, pela ONU, dependerá, conforme comentado, do campo *flag* definido pelo OLT no campo *BWmap*, ou seja, o OLT é quem determinará qual dos campos fará parte do quadro de upload. Conforme comentado, o campo *BWmap* enviado no sentido de download a cada uma das ONUs determinará o formato do intervalo de alocação de cada uma das ONUs. A figura 17.18 apresenta o formato do quadro GTC no sentido de upload contendo os detalhes de cada um dos campos principais.

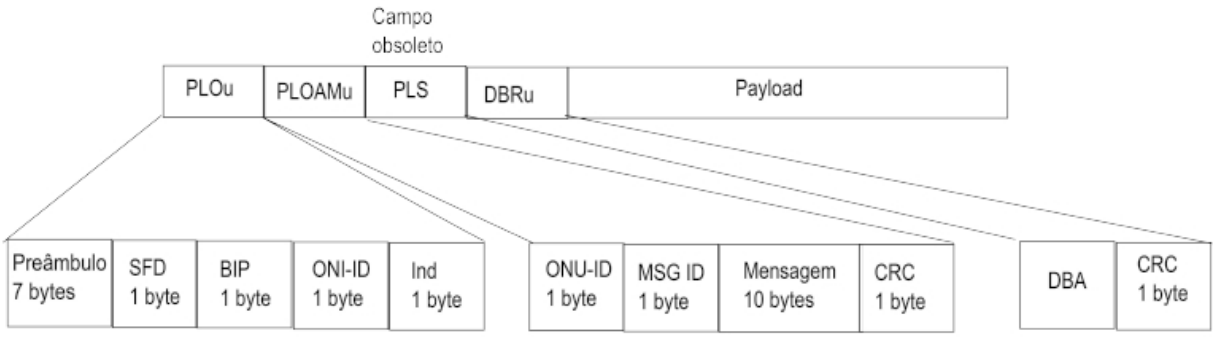



*Figura 17.18 – Detalhes do quadro GTC utilizado no sentido de upload.*

Conforme observado na figura 17.18, vejamos os detalhes de cada campo:

- O campo PLOu (*Physical Layer Overhead upstream*) inicia com um preâmbulo, utilizado para informar o OLT, que atua como receptor, para sincronizar o recebimento dos dados com o emissor (ONU). O recebimento do campo preâmbulo delimita o início do quadro GTC no sentido de upload.
- O delimitador que segue o preâmbulo complementa a informação sobre o início e significa o início de uma rajada de upload.
- O campo BIP tem a mesma função já descrita pelo quadro em sentido de download.
- O campo ONU-ID identifica a ONU que está transmitindo em um dado momento.
- O campo *Ind* fornece informações em tempo real do status da ONU para o OLT. Esse status informa se a ONU possui dados em espera de um *time slot* para enviar o OLT. A figura 17.19 apresenta os difentes tipos de espera que podem ocorrer em relação ao T-CONT em utilização.

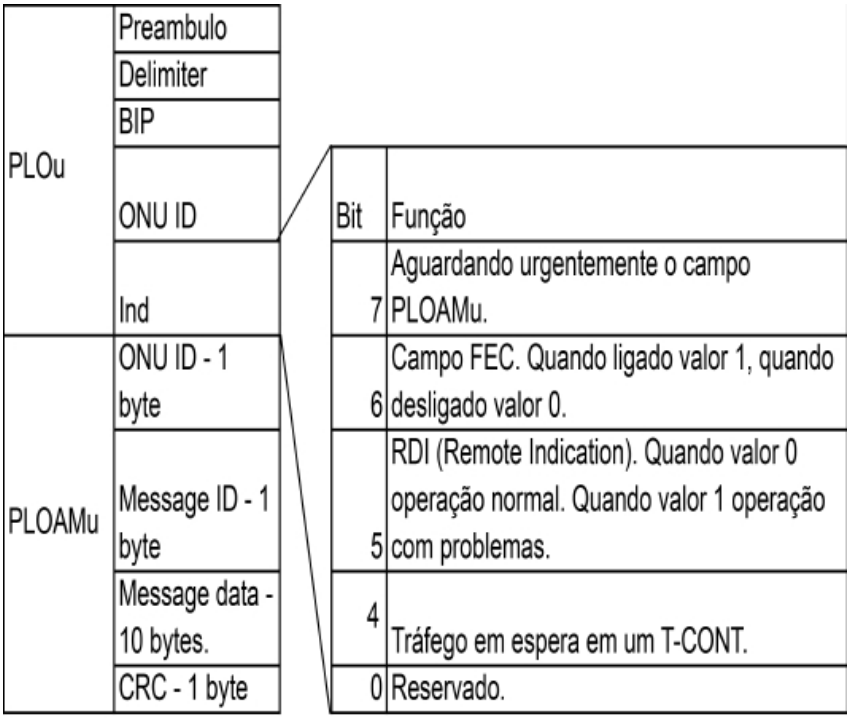



*Figura 17.19 – Variações do campo Ind.*

Seguindo o campo PLOu, conforme comentado, existem alguns campos opcionais que poderão compor a rajada de uma ONU ou não. Os campos opcionais são PLOAMu, PLSu (*Power leveling sequence upstream*), já obsoleto, e DBRu. A transmissão desses campos é controlada pelo OLT por meio das *flags* contidas no campo *BWmap* enviado no quadro GTC, campo PCBd, no sentido de download.

O campo PLOAMu é responsável por gerenciar funções, como *ranging*, ativação da ONU e notificações de alarmes que precisam ser informadas à ONU para tomada de decisão ou para demonstrar em uma ferramenta de gerência alguma anormalidade da rede. Na tabela 17.7, apresentamos as mensagens transportadas pelo campo PLOAMu no sentido upload.

*Tabela 17.7 – Mensagens PLOAM enviadas no sentido de upload*

| Seq | Nome da mensagem | Detalhes da mensagem |
|---|---|---|
| 1 | Serial_Number_ONU | Função: esta mensagem transporta o número serial da ONU no sentido de upload. |

| Seq | Nome da mensagem | Detalhes da mensagem |
|---|---|---|
| | | Esta mernsagem é enviada pela ONU em dois momentos. A primeira mensagem é enviada em resposta ao OLT durante a definição dos dados do campo BWmap. Em um segundo momento, é respondida ao OLT durante o processo de ranging. |
| | | Enviada uma vez a cada solicitação. |
| | | Ao ser recebida, o OLT extrairá o número serial da ONU e o relacionará com um novo ONU ID. |
| 2 | Password | Função: esta mensagem é enviada da ONU para o OLT durante o processo de ativação. A senha, ao ser informada pelo técnico no ato da ativação, será enviada ao OLT para registro e comparação com a declarada durante a configuração. |
| | | Enviada quando o OLT requisitar a senha por meio da mensagem Request_Password enviada no sentido de download. |
| | | Enviada três vezes da ONU para o OLT. |
| | | Caso o OLT receba três senhas idênticas, esta declará a senha como válida. |
| 3 | Dying_Gasp | Função: informa ao OLT que a ONU foi desligada em uma operação normal, por exemplo, sem o corte de energia de forma abrupta. Essa mensagem é enviada para informar o OLT que, apesar da interrupção da ONU, esta não deverá gerar alarmes desnecessários. |
| | | A ONU enviará esta mensagem quando for desligada normalmente. |
| | | Poderá ser enviada pelo menos três vezes. |
| | | Ao ser recebida pelo OLT, esta descartará quaisquer mensagens de alarme subsequente. |
| 4 | No message | Indica que a fila de mensagem permanece vazia. |

| Seq | Nome da mensagem | Detalhes da mensagem |
|---|---|---|
| 5 | Encryption key | Função: esta mensagem transporta, no sentido de upload, a chave encriptada criada pela ONU e que deverá ser registrada pelo OLT. A chave será enviada em fragmentos devido ao seu tamanho e também por questões de segurança. |
| | | Será enviada pela ONU após receber do OLT a mensagem key request message. |
| | | Envia três vezes para cada fragmento enviado. |
| | | O OLT verifica se existem erros em cada fragmento e, caso não os identifique, armazena a chave. |
| 6 | Physical_ Equipment_ Error (PEE) | Função: indica ao OLT que a ONU é incapaz de enviar quadros GEM e OMCC entre as camadas GEM e TC (Transmission Convergence – Camada de Enlace da Arquitetura GPON). |
| | | Será enviada quando a ONU perceber que é incapaz de enviar quadros GEM e OMCC entre as camadas GEM e TC. |
| | | Enviada uma vez por segundo. |
| 7 | PST message Passive optical network Section Trace message | Função: verificar se a conectividade entre a ONU e o OLT está adequada. Caso perceba alguma anormalidade, esta mensagem poderá disparar um chaveamento automático de proteção (APS – Automatic Protection Switching). |
| | | Enviada periodicamente, como também após uma falha ser identificada. |
| | | Enviada uma vez por segundo. |

| Seq | Nome da mensagem | Detalhes da mensagem |
|---|---|---|
| | | Uma rede GPON tem a capacidade de automaticamente alternar para uma outra fibra caso a comunicação por uma das fibras venha apresentar problemas. Assim que uma ONU detecta perda de sinal do sentido de download, enviará um alarme de perda de janela (LOW – Loss of Window) para o OLT. Como resultado, o OLT automaticamente chaveará todas as ONUs para a fibra de proteção que será atendida por outra porta PON. Essa é uma característica indispensável de ser utilizada por uma operadora ou provedor de serviços. |
| 8 | Remote error indication (REI) | Função: informar o número de erros identificados durante o intervalo definido por BER Interval. |
| | | Será enviada quando o tempo definido por BER Interval tiver sido alcançado. |
| | | Enviada uma vez a cada BER Interval. |
| | | O OLT pode determinar o BER relacionado a cada uma das ONUs. |
| 9 | Acknowledge | Função: utilizada pela ONU para indicar que uma mensagem de download foi recebida. |
| | | Enviada sempre após ter recebido uma mensagem de download com sucesso e que requeira uma confirmação (acknowledgement). |
| | | Enviada uma vez. |
| | | Ao ser recebida, demonostrará que o meio utilizado para o transporte dos dados de download é confiável. |

A seguir, analisaremos os demais campos que compõem o quadro de upload.

O campo PLSu, já obsoleto pelas últimas redes GPON, informa ao OLT o nível de potência do laser da ONU.

O campo DBRu está relacionado aos T-CONTs utilizados pela ONU. O campo DBRu possui comprimento variável, dependendo do

resultado da alocação dinâmica de banda realizada pelo mecanismo DBA e, ainda, da quantidade de T-CONTs configurados para a ONU. O campo DBRu transporta internamente informações relacionadas aos resultados do mecanismo DBA para a respectiva ONU. Digamos que a ONU em algum momento demonstre interesse em incrementar sua transmissão devido a uma situação de transmissão de dados em rajada. Essa necessidade será informada ao OLT que, dinamicamente, alocará *time slots* livres para que a ONU em sobrecarga consiga dar uma melhor vazão a seus dados. Dessa forma, dinamicamente, o OLT ajustará as necessidades da ONU, a fim de garantir que as necessidades dos clientes sejam atendidas adequadamente. Sempre que houver *time slots* livres, uma ONU poderá utilizá-los temporariamente.

Finalizando, temos o campo *payload*, que é responsável por transmitir os dados dos clientes. A figura 17.20 apresenta os detalhes do campo payload.

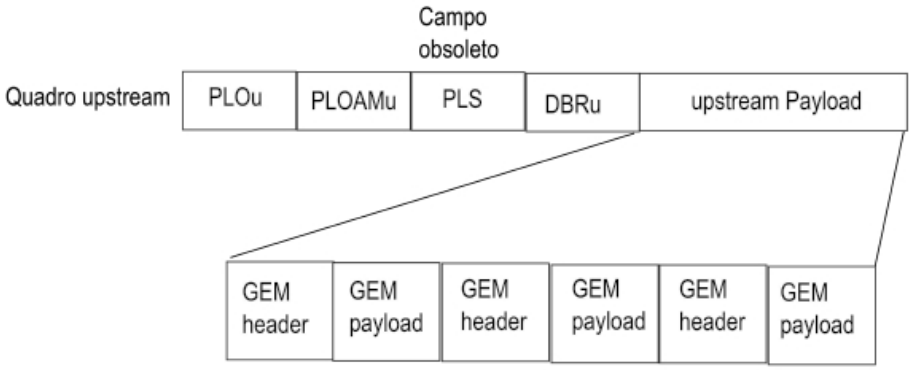



*Figura 17.20 – Campo payload do quadro GTC no sentido de upload.*

Conforme observado, o campo *payload* no sentido de upload é composto de inúmeros quadros GEM, e para cada um temos um *header* (*GEM Header*) e os dados propriamente ditos (*GEM Payload*).

## 17.4.6 DBA – Dynamic Bandwidth Allocation

Uma das principais vantagens das redes GPON sobre redes ponto a ponto é que uma simples fibra óptica pode ser compartilhada com muitos clientes, reduzindo os custos de implantação e manutenção.

Como vantagem, temos ainda que uma rede GPON mantém as características de uma rede *broadband*, em que podemos transmitir múltiplos serviços (Internet, VoIP, vídeo) simultaneamente. Conforme comentado, podemos compartilhar uma porta PON com até 128 clientes. Todavia, compartilhar uma única fibra com múltiplos clientes exige uma cuidadosa atenção com a questão de alocação de banda a cada um dos clientes conectados, pois, entre os 128 clientes, muitos optam por serviços diferentes (Internet ou VoIP) com velocidades diferentes (20 Mbps, 40 Mbps, 60 Mbps ou 160 Mbps).

Conforme comentado, uma rede GPON oferece uma variedade de serviços, o que fez do GPON uma arquitetura amplamente utilizada pelas operadoras e provedores de serviços de Internet. Alguns serviços oferecidos por uma rede GPON, como VoIP, requerem uma banda de upload constante. Assim, nesse caso, o OLT poderia alocar uma banda estática para esse tipo de serviço. Para isso, utilizaríamos o seguinte comando na plataforma Huawei:

```
dba-profile add profile-id 15 profile-name "VoIP" type1 fix 1000
```

Esse comando está definindo um DBA *profile* com banda fixa de 1 Mbps (*type1 fix* 1000).

É importante observar que navegação na Internet, jogos online, transmissão de TV, compartilhamento de arquivos e até mesmo upload de arquivos, são serviços que operam, por natureza, em formato de rajadas (*burst*), características de uma rede IP, ou seja, a banda utilizada é totalmente variável por natureza. Se criássemos perfis fixos para esses serviços, a banda de upload da rede GPON seria muito mal utilizada e, com isso, os clientes seriam prejudicados com essa política.

Em uma rede GPON, os dados transmitidos no sentido de download seguem em *broadcast* e seu comportamento é parecido com o de uma rede Ethernet. Porém, no caso do upload, o modelo de transmissão é diferente, ou seja, não se utiliza *broadcast*, e sim o conceito do TDMA (*Time Division Multiple Access*). Nesse sentido, o OLT é quem controla a transmissão de cada uma das ONUs. Assim, para que a rede fique otimizada para atender a esse tipo de

transmissão no sentido de upload, o OLT precisa alocar banda dinamicamente às ONUs, pois, conforme comentado, os serviços transmitem, em algum momento, alta taxa de quadros sob o modelo de rajadas. Para criar um DBA *profile* com característica de alocação de banda diâmica, utilizaríamos o seguinte comando na plataforma Huawei:

```
dba-profile add profile-id 15 profile-name "Internet" type4 max 100000
```

Esse comando está definindo um DBA *profile* com banda variável de 100 Mbps (*type4 max* 100000).

### 17.4.6.1 Utilizando o mecanismo/algoritmo DBA

Em uma rede GPON, o OLT é responsável por controlar e informar, por meio do campo *BWmap* (*Bandwidth Mapping*), a alocação de banda de cada uma das ONUs. Cada alocação de banda feita pelo OLT define o intervalo no qual a ONU transmitirá seus quadros de upload. A essência do DBA é dinamicamente calcular os valores dos intervalos a fim de alocar a correta banda para cada ONU. No campo *BWmap*, determina-se dinamicamente o período que cada ONU transmitirá e determinará em que momento deverá iniciar e terminar sua transmissão.

Nesse intervalo, serão consideradas também as características dos diferentes serviços contratados e configurados nas ONUs. Dessa forma, concluímos que a essência do mecanismo DBA é calcular de forma eficiente o campo *BWmap*, responsável por transportar, no sentido de download, todas as informações necessárias a cada ONU para transmissão no sentido de upload.

Conforme comentado, o mecanismo DBA otimiza os *slots* de tempo de ONUs que param de transmitir dados. Com essa gestão, uma ONU poderá transmitir rajadas e, caso necessário, ultrapassar a banda contratada. A figura 17.21 apresenta um exemplo do reuso de *slot* de tempo.

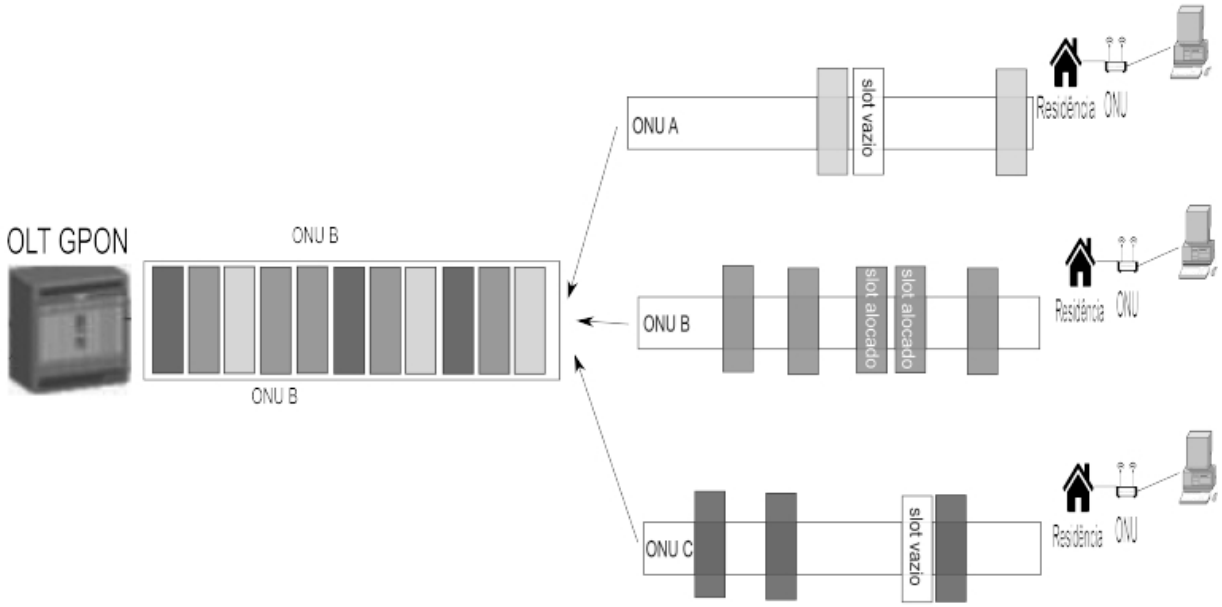



*Figura 17.21 – Atuação do mecanismo DBA.*

Na figura 17.21, observamos que a banda não utilizada pelas ONUs A e C foi alocada à ONU B. Esses casos ocorreriam quando a ONU B, além de utilizar suas coordenadas, faria também uso de espaço livre para transmitir seu excedente no formato de rajadas.

### 17.4.6.2 Alocação de banda estática

As versões anteriores do GPON alocavam a banda de cada ONU de forma estática, ou seja, cada ONU recebia uma banda fixa que utilizava para transmitir seus quadros. Essa aplicação é adequada para o uso do serviço de VoIP que utiliza uma banda fixa de transmissão, porém para outros serviços que utilizam rajadas, como upload de arquivos ou navegação na Internet, este modelo de alocação não é muito eficiente. Neste modelo, cada ONU recebe uma banda fixa, usando-a ou não. Enquanto o tráfego gerado pela ONU permanece constante, a utilização do canal fica bom. Uma vez que a ONU pare de transmitir dados, conforme apresentado na figura 17.22 pelas ONUs B e C, essa banda não poderá ser

reutilizada por outra ONU. Dessa forma, caso alguma outra ONU precise de uma banda um pouco maior, não terá condições de receber e as rajadas serão totalmente comprometidas.

O fato de a banda reservada e não utilizada por uma ONU não poder ser utilizada por outras ONUs impede que a rede GPON seja eficiente quando existam serviços que utilizam rajadas para transmissão.

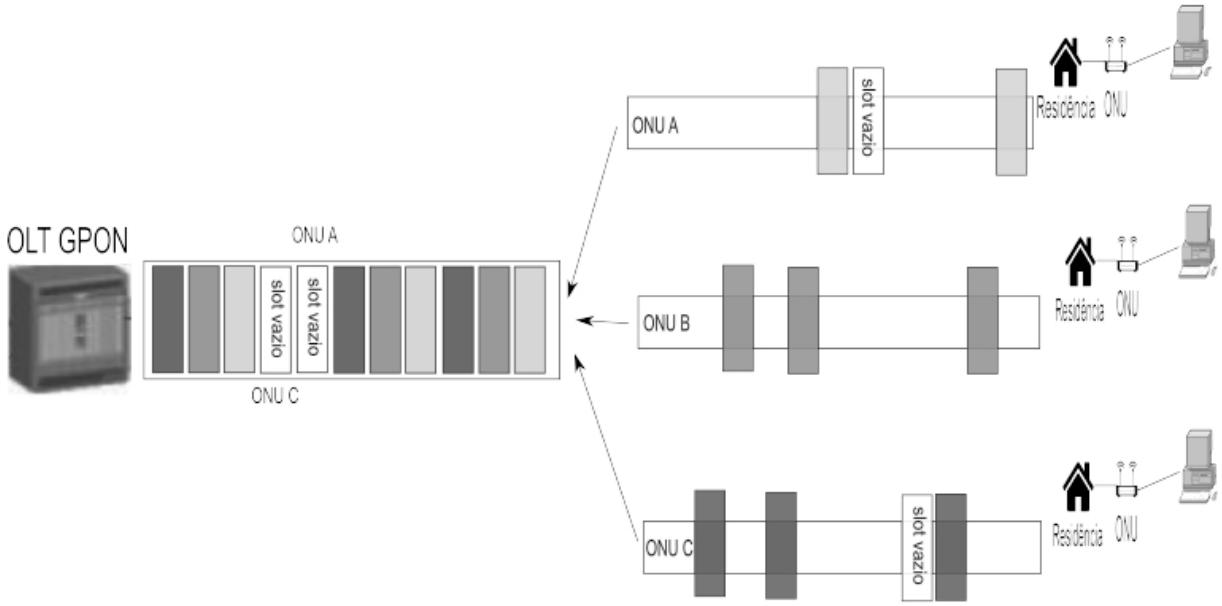



*Figura 17.22 – Alocação estática de banda.*

Conforme observamos na figura 17.22, houve três momentos em que as ONUs B e C ficaram sem transmissão e o time slot ficou vazio, não sendo reutilizado por nenhuma outra ONU.

### 17.4.6.3 Categorias do DBA (Dynamic Bandwidth Allocation)

O mecanismo DBA pode ser dividido nas seguintes categories: *Status Reporting* (SR DBA) ou *Non Status Reporting* (NSR DBA).

No caso do uso de SR-DBA, todas as ONUs reportam sua ocupação de banda de upload para ser utilizado pelo processo otimizado de cálculo do OLT. Cada ONU pode ser configurada com diversos T-CONTs (*Transmission Containers*). Combinando as informações de ocupação da fila e o provisionado de cada T-CONT,

o OLT pode otimizar a alocação de banda da ONU para upload.

No caso do uso de NSR-DBA, as ONUs não reportam sua ocupação de banda de upload para ser utilizado pelo processo otimizado de cálculo do OLT. Neste caso, o OLT estima a ocupação de banda de upload baseando-se nas últimas transmissções realizadas pela ONU. Por exemplo, se uma ONU não possui tráfego para enviar, esta transmitirá *idle frames* durante seu tempo de transmissão, ou seja, transmite algo sem valor, apenas para ocupar seu tempo. Neste caso, o OLT observará esse comportamento de *idle frames* e decrementará a alocação de banda dessa ONU no próximo ciclo. No caso de a ONU transmitir quadros ao OLT, este, por sua vez, aumentará a banda da ONU para atender às rajadas, até que encontre *idle frames*. Nesse modelo não existe um ponto ótimo, pois tudo ocorre de forma subjetiva. Nesse modelo, o *delay* poderá aumentar. É importante observar que um ciclo representa o tempo para transmissão dos quadros de todas as ONUs.

O uso do SR DBA em relação ao NSR DBA somente traz beneficios aos clientes. No caso do uso do SR DBA, o OLT não subestimará nem superestimará o uso da ONU, oferecendo a banda que realmente precisa no momento que precisar. O *delay* no modelo SR DBA é menor em razão de o OLT poder fornecer à banda necessária a ONU no momento que venha requisitar. Com essa implementação (SR DBA), mesmo que todos os clientes façam upload ao mesmo tempo, necessitando de uma banda maior que a oferecida pelo GPON (1,25 Gbps), todos terão seus dados entregues em um tempo adequado.

### 17.4.7 FEC (Forward Error Correction)

A FEC é utilizada para detectar e corrigir erros durante a transmissão dos dados em uma rede GPON. Com a opção FEC habilitada, transmitem-se bytes adicionais (16 bytes a cada 239 bytes) que serão utilizados para recuperar outros bytes que venham a ser perdidos durante a transmissão. É importante observar que os principais objetivos da FEC são:

• Evitar a retransmissão de bits perdidos.

• Aumentar de 3 a 4 dB o nível de potência óptica na recepção da ONU. Em valores normais, não deverá ser maior que -28 dB.

Como desvantagem de habilitar a FEC, haverá redução em torno de 6,5% do espaço para transporte dos dados do usuário. O valor de 6,5% refere-se aos bytes adicionais que precisarão ser enviados para permitir a recuperação caso haja perda durante a transmissão.

A recomendação ITU-T recomenda que os equipamentos GPON implementem o modelo de decodificação RS (255,239), em que RS representa *Reed-Solomon*. Quando se habilita FEC nos sentidos de download ou upload seguindo o padrão de decodificação RS (255,239), adicionam-se a cada 239 bytes 16 bytes para futura recuperação. A soma entre os dados do usuário e os bytes de paridade totalizam 255 bytes e dá-se o nome de *codeword*. Assim, o quadro GTC de 38.880 bytes permitirá que sejam transportados 36.432 bytes, ou seja, 6,5% do total será utilizado pelos diferentes blocos de 16 bytes de paridade adicionados ao quadro GTC. A figura 17.23 demonstra a inclusão dos bytes de paridade ao quadro GTC.

A utilização ou não de FEC na comunicação entre o OLT e a ONU, sentido download, será informada pelo campo Ident (Identificador). Conforme comentado, esse campo é composto de 4 bytes, porém, no momento, utiliza-se apenas o primeiro bit que informa à ONU se o quadro transmitido utiliza ou não FEC. A utilização ou não de FEC na comunicação entre a ONU e o OLT, sentido upload, será informada pelo campo flag por meio do bit *Use*_FEC.

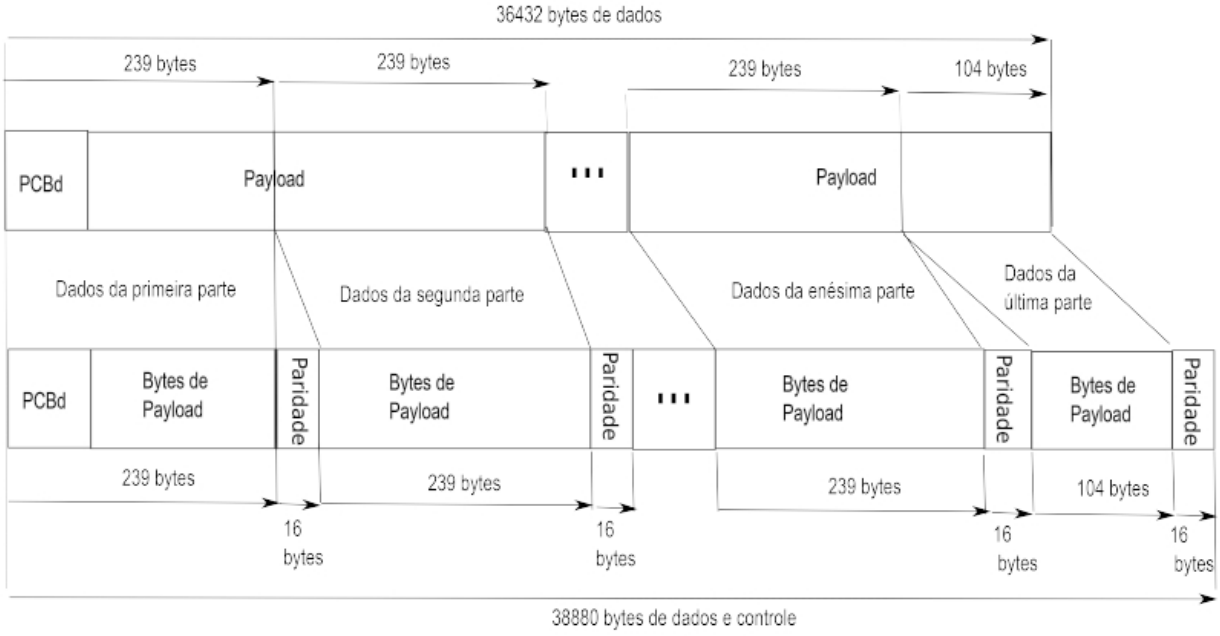



*Figura 17.23 – Utilização do mecanismo FEC.*

## 17.4.8 OMCI (Optical network termination Management and Control Interface)

A ONU, uma vez adicionada (ou confirmada) ao OLT, é gerenciada por este por meio do canal de controle chamado OMCI. Por esse canal de controle, é possível enviar informações para configurar a ONU, ou seja, mesmo que o cliente desligue ou altere a configuração da ONU, esse canal se encarregará de atualizar a configuração realizada pela operadora. Por meio do OMCI, é possível configurar os seguintes dados da ONU:

- T-CONTs utilizados.
- VLANs utilizadas para as portas LAN e WAN.
- Alterar a VLAN da WAN.
- Definição do uso ou não do QinQ na ONU.
- Configuração necessária para fechar a sessão PPPoE.
- Atualizar o dia e a hora na ONU. Muito utilizado para acompanhar eventos na rede do cliente.
- Alterar o modo de obtenção de IP da WAN (IP fixo, DHCP,

PPPoE).

- Habilitar o acesso remoto por meio de HTTP, TELNET ou SSH.
- Alterar o usuário e a senha-padrão da ONU.
- Gerenciamento de segurança no momento da ativação.
- Gerenciamento do status, permitindo observar se a ONU está:
  - Conectada a suas mensagens.
  - Transmitindo dados.
  - Com as portas utilizadas.
  - Com velocidade das portas e fechando a conexão (ex.: 100 *full-duplex*), entre outras opções.
- Gerenciamento de falhas, *traps* e alarmes gerados pela ONU que poderão auxiliar na solução de problemas. Como exemplo de alarmes e falhas, temos falta de energia, bateria baixa/faltando/com problemas, *dying gasp* (ONU desligada iminentemente), nível óptico, temperatura alta ou média e voltagem alta ou média.
- Gerenciar uma reinicialização e novo registro (*re-register/resync*) dos dados na ONU.
- Gerenciamento de desempenho: solicitar à ONU informações e particularidades de funcionamento.
- Várias outras opções que poderão ser observadas nas ferramentas gráficas, como U2000 e NetHorizhon.

O protocolo OMCI executa sobre uma conexão GEM presente na camada GTC. A figura 17.8 apresenta a relação entre o canal OMCI e a camada GTC. A especificação ITU-T G.984.4 especifica como os fabricantes deverão prover mecanismos para o gerenciamento e configuração das ONUs. Esses mecanismos podem ser relacionados a ferramentas gráficas ou por meio de comandos emitidos no OLT para gerenciar uma ONU. O OLT utilizará o protocolo OMCI para as seguintes atividades:

- Com o gerenciamento da configuração das ONUs, podemos instalar e utilizar aplicações gráficas, como U2000 ou Nethorizhon para configurar as ONUs, seguindo cacterísticas específicas de

cada serviço (Internet, VoIP). Com tais ferramentas, garantimos ainda que toda a configuração ficará armazenada em uma base de dados e, caso seja necessário, a ONU será trocada e o próprio OLT enviará novamente a configuração à ONU recém-instalada. Podemos ainda atualizar o firmware de uma ONU, ressincronizar uma ONU, resetar a ONU remotamente, analisar os valores de RX e TX, por meio de gráficos de desempenho, mudar o status de uma porta de ligada para desligada, ajustar VLAN, configurar elementos de segurança, entre outras possibilidades com ferramentas gráficas, web ou com envio de comandos por meio de console.

- Obter estatísticas de desempenho ou informações do status de funcionamento da ONU. A análise de indicadores facilitará um futuro suporte remoto.
- Receber alarmes gerados pela ONU facilitará a indentificação do porquê a comunicação não ocorre normalmente ou conforme contratada.

## 17.5 Tecnologias GPON e EPON

Atualmente, muitas operadores e provedores de serviços de redes vêm buscando tecnologias que permitem transmitir dados em alta velocidade a um baixo custo. Conforme comentado, a tecnologia PON trouxe essa possibilidade. Entretanto, da tecnologia PON derivaram-se duas implementações: a GPON já apresentada neste capítulo e o EPON. Assim, na tabela 17.8 apresentamos uma comparação entre essas duas implementações:

*Tabela 17.8 – Comparação entre GPON e EPON*

| Características | EPON | GPON |
|---|---|---|
| Recomendação | IEEE 802.3ah | ITU-T G.984 |
| Protocolo | Ethernet | Ethernet, TDM |

| Características | EPON | GPON |
|---|---|---|
| Taxa de bits | 1 Gbit/s é a taxa de transferência de dados para download e upload<br>1,25 Gbit/s é a taxa de bits física do acesso devido à codificação 8b/10b | 2488 Mbit/s para download e 1.244 Mbit/s para upload |
| Distância máxima entre o OLT e as ONUs | 10 km | 20 km |
| Quantidade de ONUs suportadas por uma porta do OLT | 32. Caso se utilize FEC, pode-se chegar até 64 ONUs | 128 ONUs |

## 17.6 Exercícios do capítulo 17

1. Descreva as vantagens de uma rede GPON.
2. Qual é a função do T-CONT?
3. Qual é a função do algoritmo DBA?
4. Quais equipamentos são utilizados em uma rede GPON?

CAPÍTULO 18

# BGP – Border Gateway Protocol

Neste capítulo, apresentaremos o protocolo BGP (*Border gateway Protocol*) envolvendo as principais características, mensagens trocadas e os possíveis estados assumidos durante o estabelecimento de uma sessão BGP. Abordaremos o conceito de sistemas autônomos públicos e privados, a diferença entre protocolos IGP e EGP, a diferencça entre iBGP e eBGP, e também os principais atributos utilizados para escolher entre dois destinos (rotas) com mesmo prefixo de rede.

## 18.1 Introdução ao protocolo BGP

O protocolo BGP é responsável pela gestão das rotas da Internet, ou seja, representa a cola que mantém a Internet unida e permite a inter-conexão universal. Vejamos algumas das características do protocolo BGP:

- Esse protocolo é baseado no algoritmo vetor de caminho. Os protocolos comentados, como RIP, baseiam-se no algoritmo vetor de distância, enquanto os protocolos OSPF e IS-IS, no algoritmo SPF.
- As tabelas de roteamento completas são trocadas entre roteadores pares (*peer*) após a sessão BGP ser estabelecida (estado *established*). Atualmente, a quantidade de rotas trocadas entre os rotadores da Internet supera 520 mil rotas.
- Atualizações adicionais são enviadas imediatamente por meio de mensagens de update. As mensagens de update trocadas entre os roteadores serão abordadas neste capítulo. Quando uma nova rota é criada, o roteador divulga imediatamente para seus pares (*peers*) BGP. Entretanto, na prática, estabelece-se um tempo mínimo (*Minimum Route Advertisement Interval* – MRAI) entre cada uma das atualizações.

• Utiliza a porta 179 do protocolo TCP.

O protocolo BGP percebe a Internet como uma coleção de sistemas autônomos [*Autonomous Systems* (AS)]. Um AS trata-se de um grupo de redes IP que é gerenciado por uma operadora (ex.: COPEL Telecom, GVT) ou provedor de serviço que possui uma clara e única política de roteamento. Cada sistema autônomo (AS) tem associado a si um número (exs.: COPEL Telecom – AS14868, Tim – AS16232, Telebrás – AS53237) que é utilizado como um identificador do AS para a troca de rotas com outros ASs. Os identificadores podem representam AS públicos ou privados. Vejamos algumas características sobre ASs públicos e privados:

• O intervalo utilizado para ASs privados, representados por 16 bits, inicia em 64.512 e segue até 65.534.

• O intervalo utilizado para ASs privados, representados por 32 bits, inicia em 4.200.000.000 e segue até - 4.294.967.294.

• O intervalo utilizado para ASs públicos, representados por 16 bits, inicia em 1 e segue até 23.455. O identificador 23.456 é reservado pela IANA

• O intervalo utilizado para ASs públicos, representados por 32 bits, inicia em 131.072 e segue até 4.199.999.999.

A figura 18.1 apresenta uma rede composta de ASs privados.

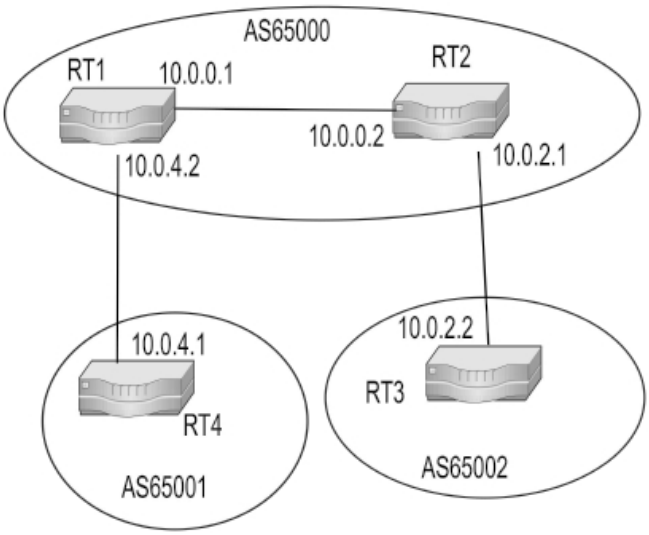



*Figura 18.1 – Rede segmentada por ASs.*

O BGP atualmente na versão 4 (especificada na RFC 1771) possibilita o intercâmbio de informações de roteamento entre os diversos sistemas autônomos (ASs), que, em conjunto, formam a Internet. Quando um roteador receber um pacote pertencente a uma rede diferente das diretamente conectadas a ele, este consultará sua tabela de rotas e repassará a requisição para o próximo AS, que direcionará a requisição para o destino correto, ou seja, o BGP permite que os dados trafeguem entre os ASs até chegar ao AS de destino e, dentro dele, siga até o seu destino final (equipamentos de rede). É importante observar que na Internet para um cliente do Brasil alcançar um site hospedado nos EUA, será necessário seguir por diferentes ASs. Vejamos um exemplo de rota BGP na tabela 18.1:

*Tabela 18.1 – Rota BGP*

| Network | NextHop | LocPrf | PrefVal | Path/Ogn |
|---|---|---|---|---|
| 31.13.85.0/24 | 201.48.54.58 | 100 | 0 | 16735, 32934 |

Essa rota atende à rede do Facebook. Esta foi obtida de um roteador Huawei de uma operadora estadual.

Essa rota nos informa que para alcançar a rede 31.13.85.0/24, o roteador de borda (ligado diretamente a uma segunda operadora que dá acesso à Internet em âmbitos nacional e internacional – operadora de trânsito) repassa os pacotes ao roteador com endereço IP 201.48.54.58, presente na operadora de trânsito. Essa rota formaliza que o roteador com endereço IP 201.48.54.58 responde pelo AS 16735 (ALGAR Telecom). Essa operadora, por sua vez, repassará os pacotes para o AS 32934 (Facebook – Facebook, Inc.), que corresponde ao AS do Facebook, destino que precisamos alcançar.

## 18.2 Algoritmo vetor de caminho (path vector)

Como os protocolos RIP e OSPF, o protocolo BGP também se baseia em um algoritmo para definir o melhor caminho a seguir

entre o emissor e o receptor. Este é chamado de vetor de caminho. A figura 18.2 apresenta o funcionamento do algoritmo.

Conforme observado na figura 18.2, temos três sistemas autônomos: AS65001, AS65002 e AS65003. Considere, no exemplo, que o roteador de borda do AS65003 (Z) deseja divulgar para os demais ASs (AS65001, AS65002) que é possível chegar à rede 200.195.1.0/24 através dele. A divulgação de rota é feita para o roteador E do AS65002 e para o roteador F do AS65001. A divulgação inclui o vetor de caminho, que é uma lista de sistemas autônomos em vez de uma lista de roteadores. Quando um roteador de borda recebe uma divulgação, ele passa a rota recebida para frente, incluindo os ASs recebidos e, ainda, adiciona o seu AS ao vetor de caminho. Dessa forma, o acesso à rede 200.195.1.0/24 é repassado para o roteador F do AS65001 por dois roteadores. O primeiro é enviado pelo roteador Z (AS65003) e a segunda, pelo roteador E (AS65002).

Com as divulgações comentadas, o roteador F terá duas rotas para chegar ao roteador Z. A primeira seguirá pelo roteador E e terá dois ASs (como ocorreu no caso do Facebook apresentado). A segunda rota será a melhor, pois para o roteador F alcançar a rede 200.195.1.0/24 configurada no roteador Z, seguirá por apenas um AS.

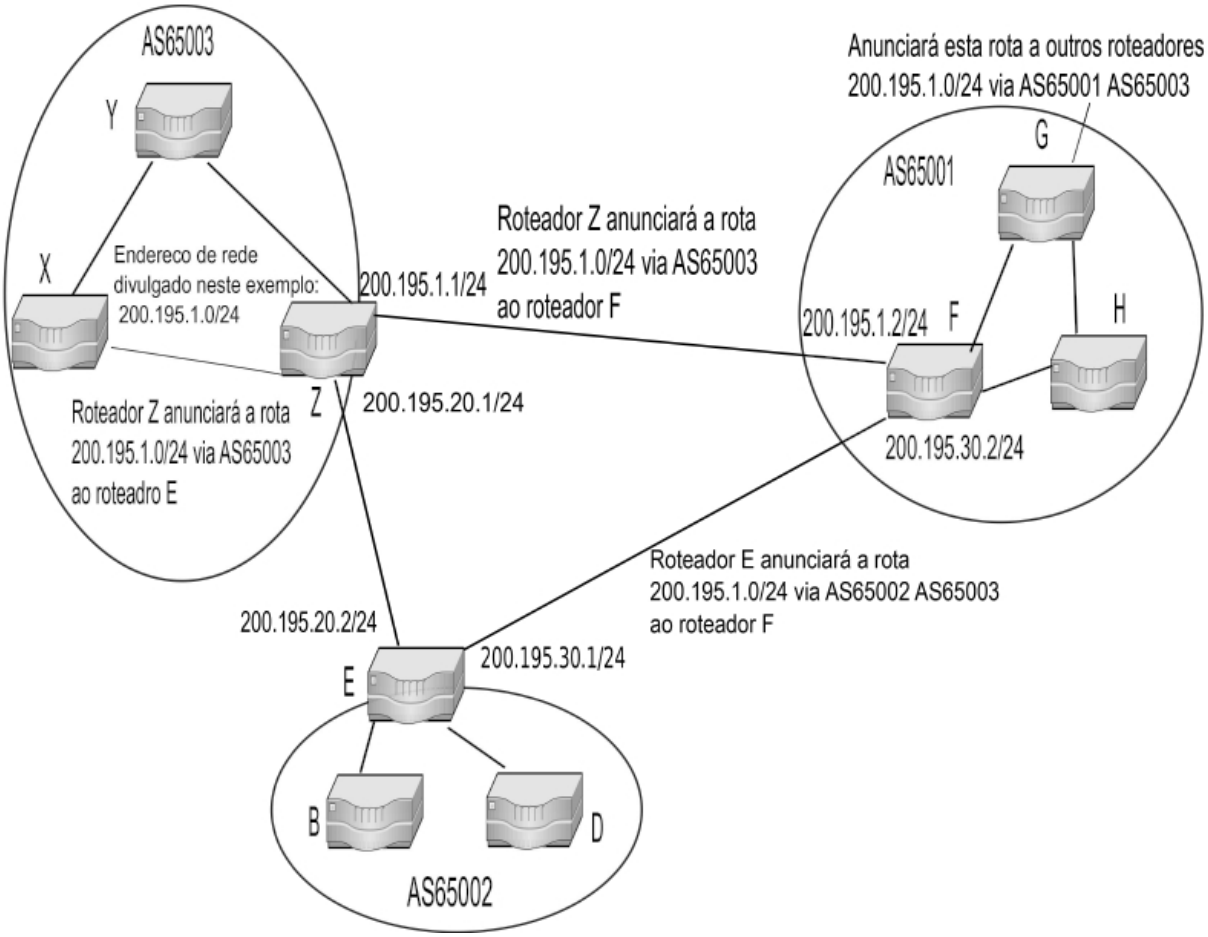



*Figura 18.2 – Funcionamento do algoritmo vetor de caminho.*

Baseando-se na figura 18.2, a tabela de rotas do roteador F montada pelo BGP ficará de acordo com a tabela 18.2:

*Tabela 18.2 – Rotas BGP do roteador F*

| Network | NextHop | LocPrf | PrefVal | Path/Ogn |
|---|---|---|---|---|
| 200.195.0.0/24 | 200.195.0.1/24 | 100 | 0 | 65003 |
| 200.195.0.0/24 | 200.150.0.1/24 | 100 | 0 | 65002,65003 |

O método do algoritmo vetor de caminho é bastante similar ao método do algoritmo vetor de distância utilizado pelo RIP, contudo, nesse método, uma lista completa de saltos da origem até o destino é incluída nas ofertas de rotas trocadas entre os roteadores. O

objetivo principal dessa lista é evitar a criação de loops, ou seja, quando um roteador receber uma rota BGP e perceber que seu AS consta no vetor de caminho, o roteador identificará que essa rota já foi recebida e a descartará.

É importante observar que quando um roteador receber duas rotas BGP para o mesmo destino, será escolhida a que tiver o melhor custo. A rota que for considerada a melhor de acordo com os critérios do protocolo BGP ficará na FIB (*Fowarding Information Base*). As demais rotas serão gravadas na RIB (*Router Information Base*), ou seja, as rotas que não foram consideradas melhores ficarão guardadas na RIB e serão utilizadas caso a rota principal fique indisponível. O protocolo BGP somente divulgará a outros roteadores as rotas que estiverem gravadas na FIB.

## 18.3 IGP e EGP

Os protocolos de roteamento são classificados em dois tipos conhecidos: protocolos IGP (*Interior Gateway Protoco*l – Protocolo de Gateway Interior) e protocolos EGP (*Exterior Gateway Protocol* – Protocolo de Gateway Exterior). Os protocolos IGP atuam como protocolos de roteamento entre os roteadores internos ao AS, enquanto os protocolos EGP atuam como protocolos de roteamento entre sistemas autônomos (AS).

Como exemplos de protocolos IGP, temos OSPF, IS-IS e RIP. Para uma operadora, pode-se definir, por exemplo, que os protocolos OSPF e RIP atendem clientes externos, enquanto o protocolo IS-IS atende à engenharia de tráfego do backbone da rede. Conforme comentado, os protocolos IGP permitirão que todos os roteadores da empresa consigam trocar dados entre si. Existem ainda empresas que por definição interna utilizam o protocolo BGP para integrar suas redes internas. São poucas, mas, quando isso ocorre, utilizam números de AS contidos entre os valores privados (de 64.512 até 65.534).

Uma outra forma menos prática, para garantir que os roteadores troquem dados entre si, seria criar rotas estáticas, porém quando há mais de cinco roteadores, essa tarefa torna-se complexa.

Enquanto temos vários protocolos IGP, atualmente o único protocolo EGP utilizado pela Internet é o BGP. A principal finalidade do BGP é permitir que os IPs dos ASs apareçam na Internet. A figura 18.3 apresenta uma rede que utiliza o protocolo BGP nos roteadores de borda e protocolos IGP nos roteadores internos ao AS. Este seria o caso de um provedor de serviço que fecha sessão BGP com uma operadora.

Conforme podemos observar na figura 18.3, os roteadores de borda do provedor fecham sessões BGP, por exemplo, com duas operadoras, como COPEL Telecom e Telebrás. Internamente a essa rede, os roteadores espalhados utilizam o protocolo OSPF. Nessa figura, as operadoras citadas atuam como operadoras de trânsito entre o cliente e a Internet. Esse cliente poderá, dependendo do destino, ter seus pacotes seguindo por uma ou outra operadora, como também esses pacotes poderão voltar por qualquer uma das duas. É importante observar que, além dos protocolos IGP configurados internamente em um AS, temos, ainda, em algumas situações, que configurar o protocolo BGP para também atuar internamente ao AS. Assim, apresentaremos dois importantes conceitos do protocolo BGP chamados de iBGP (BGP interno) e eBGP (BGP externo).

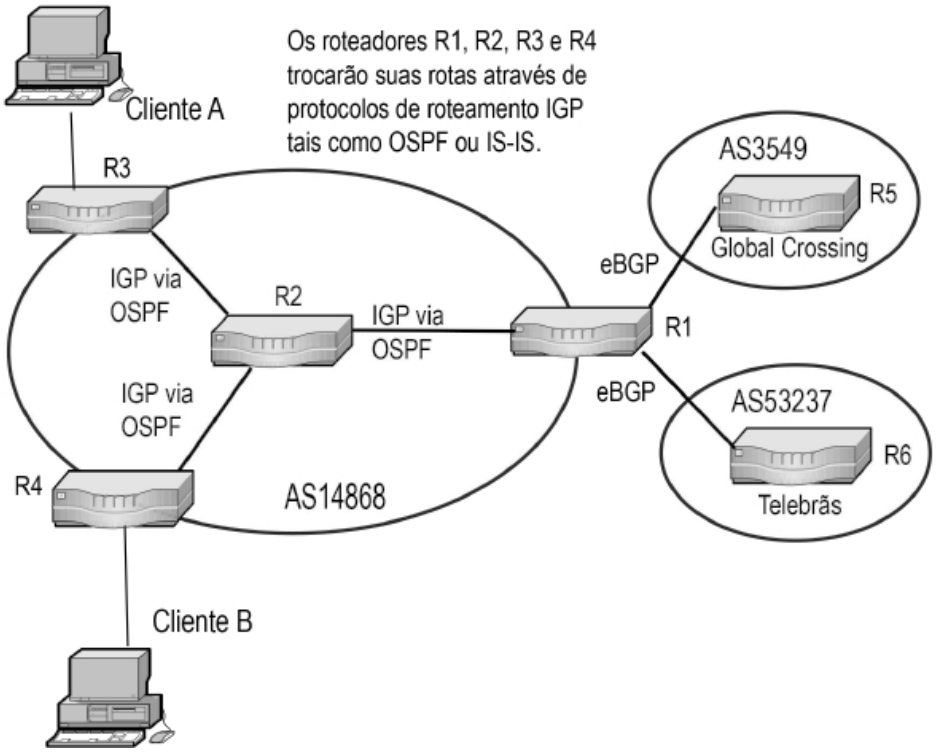



*Figura 18.3 – Rede com BGP apenas nos roteadores de borda.*

## 18.4 iBGP e eBGP

Existem empresas que possuem clientes que também possuem AS conectados a elas. A figura 18.4 apresenta uma rede com essa característica. Neste caso, será indispensável a utilização do BGP com o cliente em uma extremidade e com operadoras de trânsito em outra extremidade. Nesse cenário, além da utilização de um protocolo IGP, para garantir que os roteadores se conheçam internamente no AS, será necessário também configurar os roteadores internos para estabelecerem sessões iBGP (BGP interno). O iBGP permite estabelecer sessões BGP com roteadores que fazem parte do mesmo sistema autônomo. Porém, é importante observar que para o iBGP funcionar necessariamente, devemos utilizar um protocolo IGP (ex.: IS-IS).

A utilização de sessões iBGP deve ser evitada dentro do AS, a menos que as extremidades precisem trocar rotas com ASs externos, como apresentado na figura 18.4, ou seja, se houver realmente a necessidade de entregar para um cliente externo da

operadora as rotas BGP recebidas do fornecedor de trânsito, precisaremos configurar sessões iBGP. Vejamos um exemplo dessa situação.

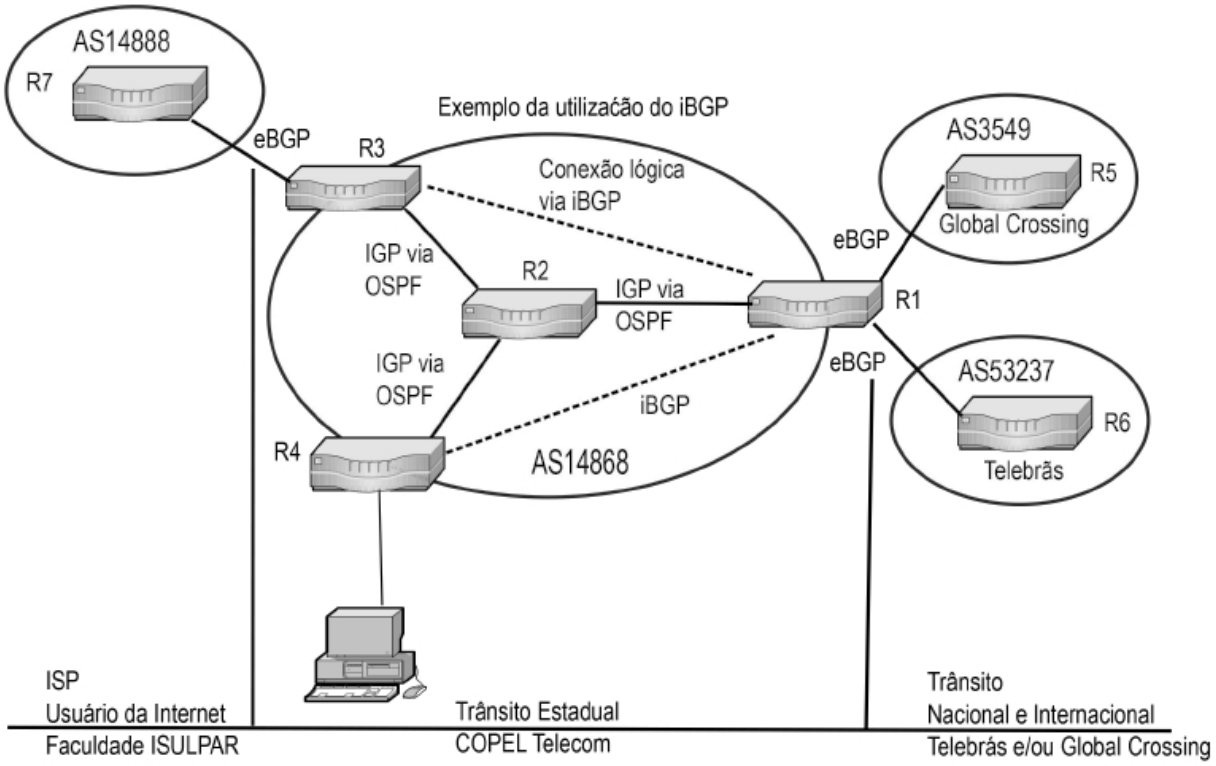



*Figura 18.4 – Rede que exige a utilização do iBGP.*

Digamos que a operadora COPEL Telecom (com AS14868) feche sessão BGP com a empresa Isulpar (AS14888). A empresa Isulpar optou por receber todas as rotas (*full routing*) da operadora (em torno de 520 mil rotas) estadual. As rotas que serão repassadas à Isulpar foram obtidas pela operadora de seus fornecedores de trânsito. Na figura 18.4, a operadora COPEL Telecom tem trânsito com as empresas Global Crossing e Telebrás (operadoras com atuações nacional e internacional).

Para entender o termo trânsito, vamos analisar a figura 18.1. Num primeiro momento, a única forma de AS65001 chegar a AS65002 (e vice-versa) seria passando por dentro do AS65000. Dizemos que, neste caso, o AS65000 faz trânsito para os outros dois ASs.

Neste caso, para a empresa Isulpar acessar à Internet, deve seguir pela operadora COPEL Telecom que atua como trânsito da Isulpar.

As operadoras Telebrás e Global Crossing atuam como trânsito para a operadora COPEL Telecom.

É importante observar que para um roteador estabelecer uma sessão BGP, este precisará conhecer onde o seu destino (par - *peer*) estará. No caso de uma sessão eBGP, os roteadores poderão ou não estar com suas interfaces diretamente conectadas. Caso estejam, estabelece-se a sessão normalmente, entretanto, é importante observar que caso o roteador destino não esteja diretamente conectado, será necessário utilizar o conceito de eBGP *multihop*. Abordaremos neste capítulo o conceito de sessão eBGP *multihop*.

No caso das sessões iBGP, em que os roteadores estão distribuídos dentro de um mesmo AS, nem sempre estarão conectados diretamente. Assim, para que uma sessão iBGP seja estabelecida entre dois roteadores distantes, será necessário que na rede, interna ao AS, tenhamos algum protocolo IGP configurado, como OSPF ou IS-IS. Esses protocolos informarão o caminho para que os roteadores possam se encontrar dentro da rede, ou seja, o protocolo BGP estabelece uma sessão ponto a ponto e, por isso, precisará de ajuda para que sua sessão possa ser estabelecida. A figura 18.5 apresenta uma rede em que temos dois roteadores que, mesmo não conectados diretamente, estabelecem uma sessão iBGP.

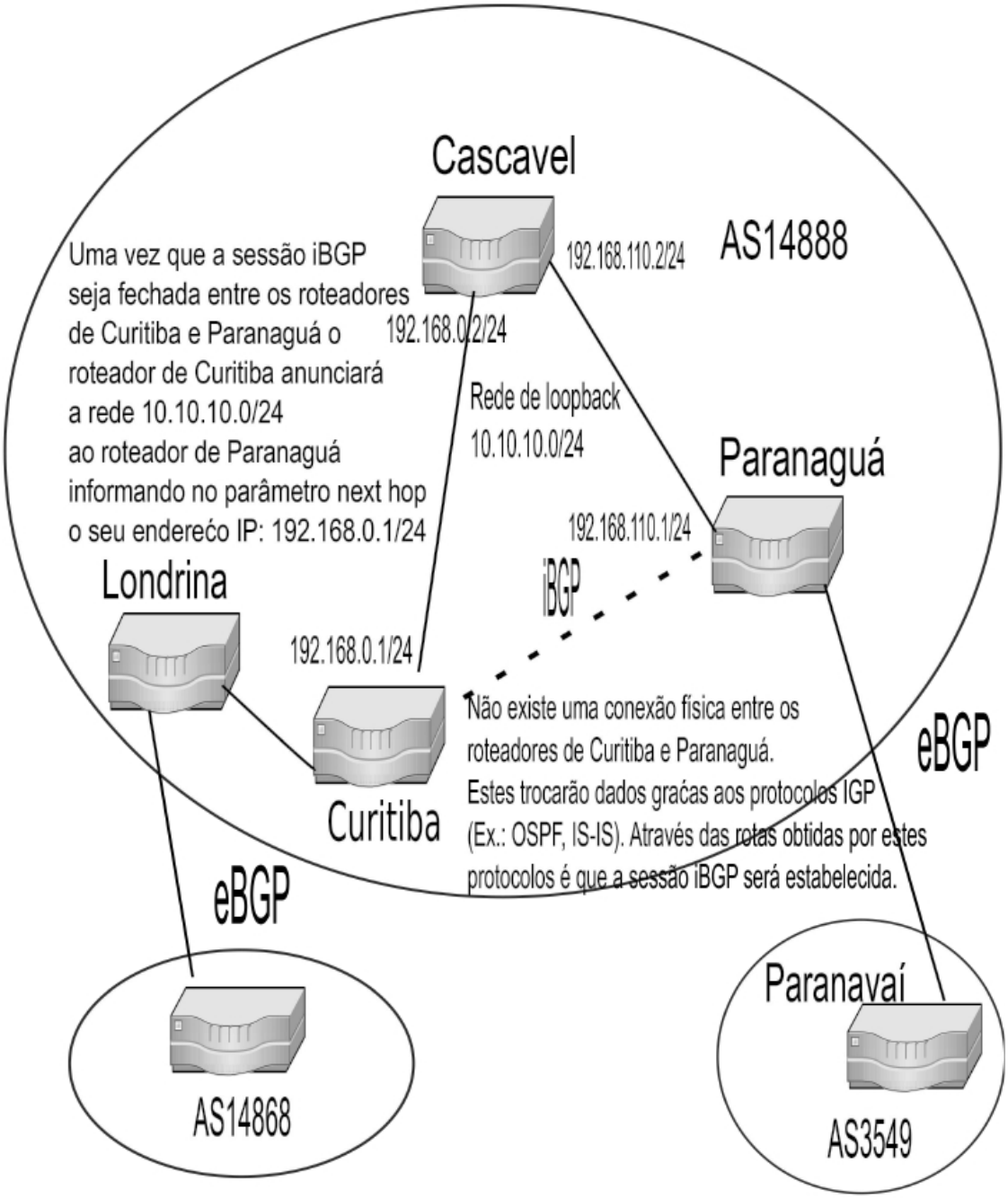



*Figura 18.5 – Conexão iBGP e eBGP.*

Conforme observado na figura 18.5, os roteadores Curitiba e Paranaguá fecham uma sessão iBGP, porém não estão diretamente conectados. Entretanto, os roteadores de Paranaguá e Paranavaí fecham uma sessão eBGP por estarem diretamente conectados. A diferença entre estabelecer uma sessão iBGP ou eBGP dependerá do AS destino. Para o fabricante Huawei, se os ASs utilizados nos

comandos forem iguais, os roteadores entenderão que é uma sessão iBGP. Se forem diferentes, identificarão que é uma sessão eBGP. No caso do fabricante Juniper, poderemos utilizar um parâmetro chamado *internal* ou *external* para determinar o tipo da sessão.

Utilizando a figura 18.1 como base e roteadores Juniper como exemplo, para estabelecer uma sessão iBGP, usamos os seguintes comandos:

• Comandos executados em rt1:

- set routing-options autonomous-system 65000
- set protocols bgp group ibgp-lab type internal
- set protocols bgp group ibgp-lab neighbor 10.0.0.2
- set protocols bgp group ibgp-lab local-address 10.0.0.1

• Comandos executados em rt2

- set routing-options autonomous-system 65000
- set protocols bgp group ibgp-lab type internal
- set protocols bgp group ibgp-lab neighbor 10.0.0.1
- set protocols bgp group ibgp-lab local-address 10.0.0.2

Os endereços IPs utilizados para estabelecer a sessão foram os endereços das interfaces de loopback, configuradas nos roteadores rt1 e rt2. Para fechar sessão iBGP, não importa se os roteadores estão diretamente conectados e, por isso, podemos utilizar o endereço IP de loopback. É importante observar que o que diferencia iBGP de eBGP é o comando *internal* ou *external*, no caso dos roteadores Juniper.

Caso o roteador utilizado seja Huawei, a formalização da sessão ser iBGP ou eBGP dependerá do valor do AS utilizado no comando *peer*. Se for igual ao do AS interno, então o roteador o identificará como uma sessão iBGP. Se diferentes, o roteador o identificará como uma sessão eBGP. Vejamos um exemplo com roteadores Huawei:

- bgp 65001
- peer 202.155.182.178 as-number 65001

- peer 202.155.182.178 description ## ISULPAR.edu.br ##
- peer 202.155.182.178 connect-interface Gigabitethernet1/0/0.1555

No caso do roteador Huawei, a tabela de rotas de um roteador interno ao AS com iBGP será apresentada conforme a execução do comando:

dis ip routing-table protocol bgp.

Vejamos na tabela 18.3 o resultado do comando:

*Tabela 18.3 – Resultado do comando aplicado ao Huawei*

| Destination/Mask | Proto | Pre | Cost | Flags | NextHop | Interface |
|---|---|---|---|---|---|---|
| 0.0.0.0/0 | IBGP | 255 | 0 | RD | 200.150.95.220 | GigabitEthernet1/0/18 |
| 10.0.0.0/24 | IBGP | 255 | 22 | RD | 200.150.95.43 | GigabitEthernet1/0/18 |

Conforme observado na tabela de rotas do iBGP, para cada rede destino o *next hop* é um dos roteadores internos ao AS.

Utilizando a figura 18.1 como base e roteadores Juniper como exemplo, para estabelecer uma sessão eBGP, utilizamos os seguintes comandos:

- Comandos executados em rt1:
  - set protocols bgp group ebgp-as65001 type external
  - set protocols bgp group ebgp-as65001 local-address 10.0.4.2
  - set protocols bgp group ebgp-as65001 peer-as 65001
  - set protocols bgp group ebgp-as65001 neighbor 10.0.4.1
- Comandos executados em rt2:
  - set protocols bgp group ebgp-as65002 type external
  - set protocols bgp group ebgp-as65002 local-address 10.0.2.1
  - set protocols bgp group ebgp-as65002 peer-as 65002
  - set protocols bgp group ebgp-as65002 neighbor 10.0.2.2
- Comandos executados em rt3:
  - set routing-options autonomous-system 65002

- set protocols bgp group ebgp-as65000 type external
- set protocols bgp group ebgp-as65000 local-address 10.0.2.2
- set protocols bgp group ebgp-as65000 peer-as 65000
- set protocols bgp group ebgp-as65000 neighbor 10.0.2.1

• Comandos executados em rt4:

- set routing-options autonomous-system 65001
- set protocols bgp group ebgp- as65000 type external
- set protocols bgp group ebgp- as65000 local-address 10.0.4.1
- set protocols bgp group ebgp- as65000 peer-as 65000
- set protocols bgp group ebgp- as65000 neighbor 10.0.4.2

Os endereços IPs utilizados foram os endereços das interfaces diretamente conectadas, configuradas em cada um dos roteadores. No caso da sessão eBGP, os endereços IPs devem ser das interfaces diretamente conectadas.

Conforme comentado, o protocolo BGP precisa estabelecer sessões com seus pares (*peers*) para que seja possível a troca de rotas. Dentro do AS de uma operadora, podem existir centenas de roteadores e, com isso, fechar sessão iBGP entre todos os roteadores pode ser uma atividade muito complexa. Sessões iBGP precisam formar uma malha completa (*full mesh*) para que todos os roteadores possam trocar a tabela de rotas entre si. A figura 18.6 apresenta uma rede com uma arquitetura *full mesh*.

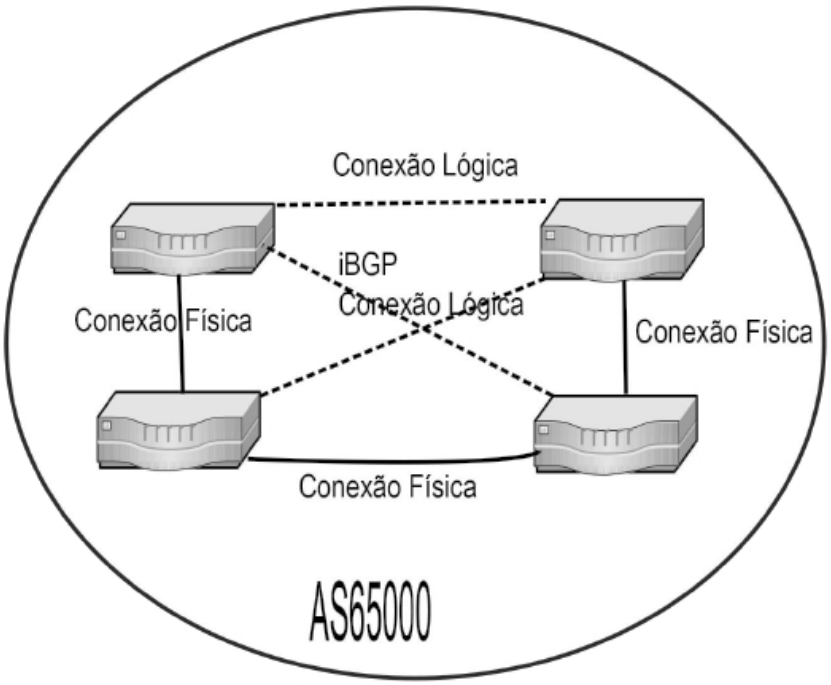



*Figura 18.6 – Conexão iBGP entre todos os roteadores do AS.*

Conforme observado na figura 18.6, a quantidade de sessões iBGP ficará grande e trará esforço adicional aos administradores da rede Assim, com a finalidade de remover essa dificuldade, o protocolo BGP oferece a possibilidade de se configurar um roteador classificado de *route reflector*. Esse roteador centralizará as atualizações de rotas na rede e as repassará aos roteadores conectados. O papel do *route reflector* é muito parecido com o roteador designado do protocolo OSPF.

## 18.5 Atributos BGP

O processo de decisão sobre a melhor rota no protocolo BGP baseia-se nos valores dos atributos de cada anúncio. Para esse cálculo, são utilizados em torno de nove atributos de decisão, classificados em quatro categorias:

- **Conhecidos** *(Well-known*) – Atributos classificados nesta categoria são obrigatórios em todas as implementacões do protocolo BGP. São subclassificados em outras duas categorias chamadas de *mandatory* e *discretionary*.

- **Conhecidos obrigatórios** (*Well-known mandatory*) – Precisam estar em todas as mensagens de update trocadas entre roteadores pares (*peers*). Vejamos alguns atributos que se classificam nessa categoria: *Next hop* – caso não seja alcançável, a rota é ignorada e AS_PATH (o mais curto).
- **Conhecido discricionário** (*Well-known discretionary*) – Estão presentes em todas as implementações do protocolo BGP, porém não precisam constar em todas as mensagens de update. Vejamos dois atributos que se classificam nesta categoria: local preference (o maior) e rotas agregadas atômicas.

• **Opcional** – Parâmetros classificados como opcionais não precisam estar presentes em todas as implementação do protocolo BGP, ou seja, a Huawei pode implementar um atributo específico que a Cisco não implementa. São classificados em outras duas categorias, chamadas de transitivo e não transitivo.

- **Opcional transitivo** (*Optional transitive*) – Mesmo que o atributo não seja suportado por um fabricante, este deverá ser aceito e repassado por meio das mensagens de update a seus pares (*peers*). Vejamos os atributos que se classificam nesta categoria: rotas agregadas e comunidades.
- **Opcional não transitivo** (*Optional non-transitive*) – Para atributos não suportados por um fabricante, estes poderão ser ignorados e não repassados por meio das mensagens de update para seus pares (*peers*). Vejamos um atributo mais comum que se classifica nesta categoria: MED (*Multi-Exit Discriminator*) (o menor valor).

## 18.6 Prefixo de rede mais específico

É importante observar que o protocolo BGP apenas analisará os atributos de uma rota (*Next hop*, AS-PATH, *Origin*, entre outros) para definir qual a melhor entre duas ou mais rotas recebidas, caso o prefixo da rede destino seja igual, ou seja, pelo caminho A, eu consigo acessar a rede destino e o prefixo anunciado é um /20. Pelo caminho B, consigo acessar a rede destino e o prefixo anunciado é um /21. Com isso, o caminho preferido será o que tiver o /21,

independentemente dos valores dos atributos. Sempre que tivermos uma rota com prefixo mais específico, esta sempre será preferida independentemente dos seus atributos. Vejamos um exemplo sobre como ajustar um prefixo de rede para que possar ficar mais específico.

Conforme comentado, um prefixo mais específico será a primeira opção para que o protocolo BGP assuma com o melhor caminho e direcione os pacotes. É importante observar que quando divulgamos uma rota via BGP, essa divulgação impactará a volta dos pacotes, enquanto as rotas recebidas dos pares impactarão a saída dos pacotes, ou seja, se quero que um determinado cliente chegue a minha rede por um fornecedor específico, poderei divulgar para esse preferido um prefixo mais específico e para o que apenas quero que fique de backup um prefixo menos específico.

Dado que uma empresa tenha sob sua responsabilidade um bloco IP /20 e utilize o endereço de rede 10.10.0.0, esse bloco IP /20 (os 20 primeiros bits são definidos para formalizar a parte rede do endereço IP) poderá atender até 16 diferentes clientes. Vejamos as cinco primeiras redes que com um /20 podemos utilizar:

- **10.10.0.0** – Primeira rede, em que o terceiro byte teve os 4 bits mais significativos mantidos em 0 (0000 0000).
- **10.10.16.0** – Segunda rede, em que o terceiro byte teve o quinto bit ligado (0001 0000). O valor do quinto bit ligado equivale a 2 elevado a 4 igual a 16.
- **10.10.32.0** – Terceira rede, em que o terceiro byte teve o sexto bit ligado (0010 0000). O valor do sexto bit ligado equivale a 2 elevado a 5 igual a 32.
- **10.10.48.0** – Quarta rede, em que o terceiro byte teve o quinto e o sexto bit ligados (0011 0000). O valor do quinto bit ligado equivale a 2 elevado a 4 igual a 16. O valor do sexto bit ligado equivale a 2 elevado a 5 igual a 32. A soma dos dois resulta em 48.
- **10.10.64.0** – Quinta rede, em que o terceiro byte teve o sétimo bit ligado (0100 0000). O valor do sétimo bit ligado equivale a 2 elevado a 6 igual a 64.

• Entre várias outras, totalizando 16, que poderão ser criadas combinando os 4 bits mais significativos do terceiro byte.

É importante observar que quando realizamos a quebra de um bloco, temos que respeitar os limites do bloco escolhido. Por exemplo, para o bloco 10.10.0.0/20 (máscara /20 equivale a 255.255.240.0), devemos observar que o intervalo será válido entre 10.10.0.0/20 e 10.10.15.254/20, ou seja, 10.10.0.0/20 representa o endereço de rede, 10.10.0.1/20, o endereço do *default gateway* e 10.10.15.255/20, o endereço de *broadcast*. Os endreços válidos seriam entre 10.10.0.1/20 e 10.10.15.254/20.

Digamos, para o cliente 10.10.0.0, que seja necessário quebrar seu bloco /20 para permitir divulgar prefixos mais específicos para um fornecedor de trânsito preferido. Apresentaremos a quebra em dois blocos /21.

A máscara do bloco /20 para o endereço IP 10.10.0.0 seria 255.255.240.0. A quebra seria realizada entre as redes 10.10.0.0, primeira rede e 10.10.16.0, segunda rede. Vejamos como ficará:

Dada a rede 10.10.0.0 com máscara 255.255.240.0 (/20), teremos as seguintes redes com bloco /21:

• **10.10.0.0 255.255.248.0 (/21)** – Neste exemplo, o terceiro byte manteve o quarto bit desligado (0000 0000). Lembrando que um /21 equivale aos primeiros 21 bits dedicados à rede. No primeiro byte, temos 8 bits, no segundo byte, outros 8 bits. No terceiro byte, em vez de utilizar 4 bits e ter um /20, optamos por utilizar 5 bits e ter um /21, pois 8 + 8 + 5 é igual a 21.

• **10.10.8.0 255.255.248.0 (/21)** – Neste exemplo, o terceiro byte teve o quarto bit ligado (0000 1000). O valor do quarto bit ligado equivale a 2 elevado a 3 igual a 8.

Lembrando que a rede 10.10.16.0 /20 pertence à segunda rede do bloco /20, rede que não nos pertence nesse exemplo. Essa rede seria repassada a uma outra empresa, por exemplo. Assim, poderemos anunciar os dois blocos /21 pelo fornecedor de trânsito preferido e o bloco /20 pelo fornecedor de trânsito backup.

Vejamos o impacto que cada um dos atributos gera sobre a decisão do melhor caminho a seguir, ou seja, como o BGP

escolherá a melhor rota caso tenhamos duas ou mais rotas para um mesmo destino com prefixos iguais (mesma máscara de sub-rede). O protocolo BGP colocará na FIB a melhor rota de acordo com a seguinte ordem:

- *Next hop* – Caso a rota não seja alcançável, a rota será ignorada.
- Weight – Atributo proprietário da Cisco. Opta-se pela rota com maior valor para o atributo weight.
- *Local preference* – Rota com maior valor de local preference terá preferência. Por padrão, o valor é 100.
- AS_PATH – Rota com o menor AS_PATH terá preferência.
- *Origin* – Rota com menor tipo de origem. IGP (i) < EGP (e) < INCOMPLETE (?).
- MED – Rota com menor valor para MED (*multi-exit discriminator*) terá preferência.
- Escolhe a rota recebida por (eBGP) em relação a (iBGP).
- Rota com a menor métrica IGP para o *next hop* BGP. Ex.: O next-hop aprendido via OSPF vai vencer um next-hop aprendido via IS-IS.
- Rota recebida de um router com menor *router ID*.

É importante observar que a análise segue para o próximo critério apenas quando houver empate no critério anterior.

## 18.7 Características dos atributos BGP

Os atributos são utilizados pelo protocolo BGP para desempatar entre duas rotas quando houver duas ou mais opções para o mesmo destino. Vejamos na tabela 18.4 como as rotas BGP são apresentadas em um roteador Huawei. Esse resultado foi obtido executando-se o comando:

```
dis bgp routing-table
```

Vejamos o resultado na tabela 18.4:

*Tabela 18.4 – Resultado do comando dis bgp routing-table*

| Network | NextHop | MED | LocPrf | Path/Ogn |
|---|---|---|---|---|
| *> 14.200.200.0/21 | 208.178.245.65 | 1 | 100 | 3549 2828 7545 7545 7545 7545i |
| *> 31.200.200.0/24 | 208.178.245.65 | 1 | 100 | 3549 6762 3216 12418i |
| *>i 177.200.200.0/24 | 200.219.144.21 | 1 | 300 | 18881 28343i |
| *>i 189.200.200.0/24 | 200.150.95.221 | 1 | 100 | 3549 3491 13591i |
| *>i 193.200.200.0 | 200.150.95.221 | 1 | 100 | 3549 6762 9050 35584i |

Em que * significa uma rota válida, >, a melhor rota (*best*) e i, *internal*.

- A próxima coluna chamada *Network* registra a rede destino.
- A coluna *NextHop* representa o endereço IP do roteador que receberá o pacote para avaliá-lo. Caso não tenha o destino como uma interface diretamente conectada, consultará sua tabela de rotas e repassará ao próximo roteador.
- A coluna MED apresenta o valor do atributo *Multi-Exit Discriminator* aplicado à rota. Apresentaremos o funiconamento desse atributos neste capítulo.
- A coluna *LocPrfr* apresenta o valor do atributo *local preference* aplicado à rota. Apresentaremos o funiconamento desses atributos neste capítulo.
- A coluna *Path/Ogn* representa o valor dos atributos AS-PATH e *origin*. O atributo AS-PATH representa uma lista de AS que os pacotes seguirão até alcançar o destino. O valor do AS-PATH é seguido do valor do atributo *origin*, e, em nosso exemplo, i significa que a rota foi aprendida de um protocolo IGP.

As rotas são trocadas entre os roteadores pares (*peers*) por meio das mensagens update. Nestas são conduzidos os valores dos atributos de cada uma das rotas conhecidas. Vejamos os detalhes dos principais atributos do protocolo BGP.

### 18.7.1 Atributo Next Hop

O atributo next-hop indica o endereço IP do próximo salto para encaminhamento de pacotes. Usualmente, utiliza-se o endereço IP do roteador externo do BGP (eBGP). A figura 18.7 mostra como o atributo é utilizado.

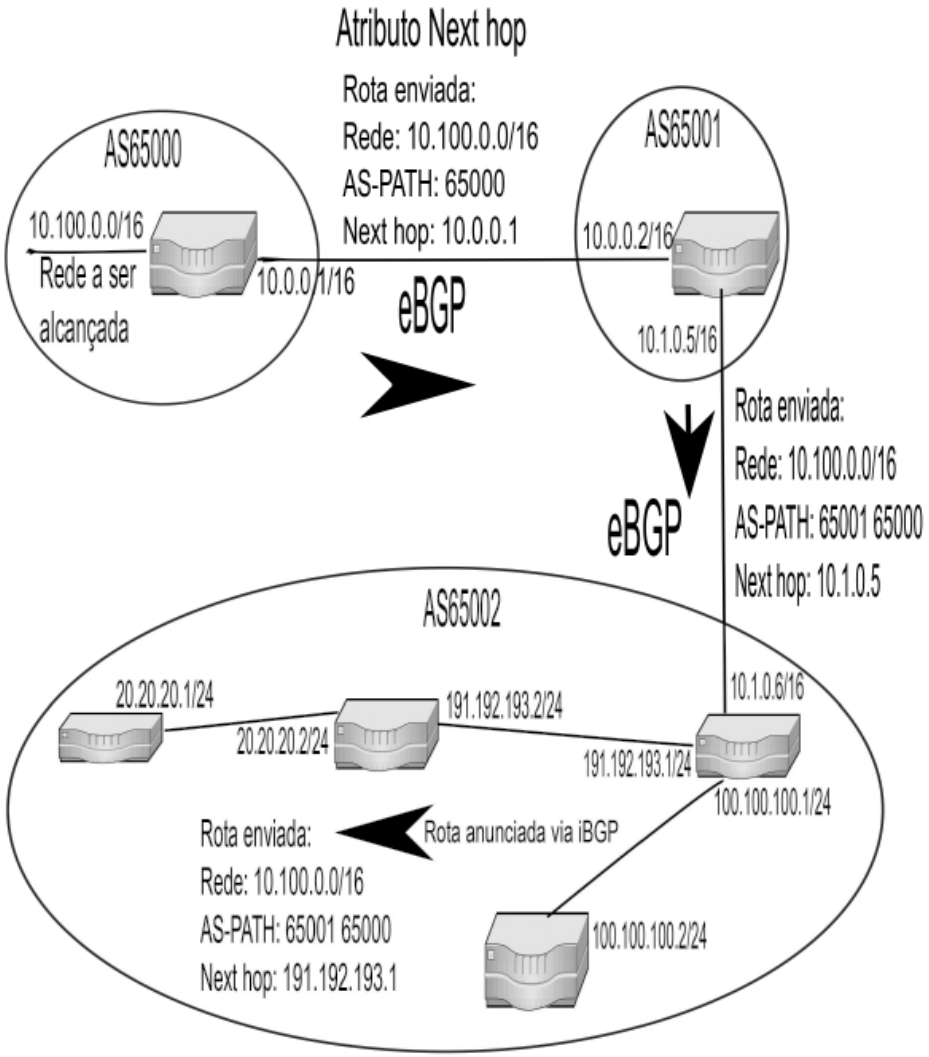



*Figura 18.7 – Atributo next hop.*

O atributo next-hop em sessões eBGP apresenta algumas particularidades. Por padrão, o roteador que origina a rota coloca seu endereço IP como next-hop. Caso a interface do roteador atenda múltiplos clientes, o endreço IP da rota será o endereço da respectiva subinterface. Observando a figura 18.7, temos que o roteador do AS65000 repassa para o roteador do AS65001 o seu

endereço IP (10.0.0.1/16) como next-hop. Esse endereço foi utilizado para estabelecer a sessão BGP com o par (*peer*) do AS65001. O roteador do AS65001 repassa para o roteador do AS 65002 o seu endereço IP (10.1.0.5/16) como next-hop. Esse endereço IP foi utilizado para estabelecer a sessão BGP com o par do AS 65002. Assim, vemos que o next-hop é o endereço IP de quem ensinou a rota. O roteador do AS65002 divulgará internamente a seus roteadores que, para alcançar a rede 10.100.0.0/16, o next-hop deve ser 10.1.0.5.

Assim, o roteador interno presente na rede 191.192.193.0/24 que fechou a sessão iBGP utilizando os endereços 191.192.192.1/24 e 191.192.192.2/24 aprenderia que para alcançar as redes do AS65000, o next-hop deveria ser 10.1.0.5, ou seja, é importante observar que quando a rota segue via iBGP para dentro do AS65002, o next-hop repassado será o do AS65001 (10.1.0.5/16), e não o do AS 65002 (ex.: 191.192.193.1), como ocorre nos casos das sessões eBGP. Para garantir que o next-hop trocado internamente via iBGP seja o endereço IP do roteador do AS 65002 (191.192.193.1), devemos configurar a interface de nosso roteador de borda com o parâmetro *next-hop self*. Assim, para os roteadores internos do AS65002, as rotas aprendidas do AS65001 serão divulgadas internamente aos roteadores do AS65002 contendo o correto next-hop. Na plataforma Huawei, o *next-hop self* é chamado de *next-hop-local*.

A figura 18.8 apresenta de forma simplificada como fica o atributo next-hop quando utilizamos o parâmetro *next hop self*.

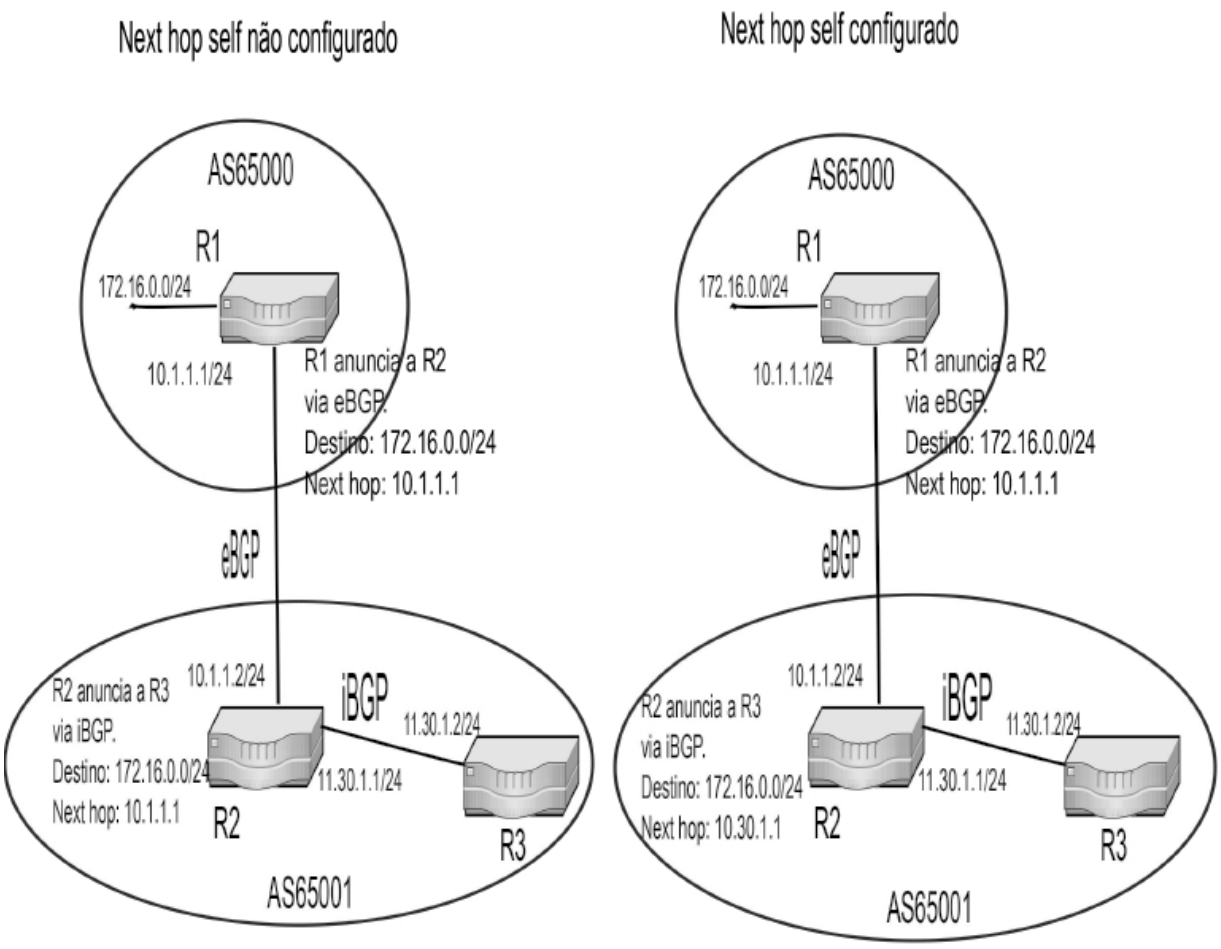



*Figura 18.8 – Atributo next hop quando configurado o next-hop self.*

## 18.7.2 Atributo local preference

O atributo *local preference* é importante no contexto de um AS se considerarmos um AS com múltiplas conexões iBGP entre si, ou seja, é usado para selecionar a melhor rota de saída a partir de um determinado AS usando iBGP. A rota que possuir o maior valor será a escolhida para constar na FIB (registra as melhores rotas). O valor-padrão desse atributo é 100. Em roteadores Huawei, o valor do *local preference* será associado ao *peer* durante o estabelecimento da sessão BGP. Para ajustar o valor do parâmetro, utilizamos uma política de roteamento (*route-policy*). Vejamos os comandos para configurar o protocolo BGP no Huawei e os comandos utilizados para o ajuste do atributo apresentado:

• system – Entra no modo de configuração.

- bgp 14868 – Entra no modo de configuração do protocolo BGP AS 14868.
- peer 211.111.112.178 as-number 15000 – Informa o endereço IP do roteador vizinho e o ASN (*Autonomous System Number*) do AS vizinho.
- peer 211.111.112.178 connect-interface Gigabitethernet1/0/0.122 – Relaciona o endereço IP do roteador vizinho e a subinterface ao qual pertence.
- ipv4-family unicast – Formaliza que a sessão utilizará o protocolo IPv4.
- peer 211.111.112.178 enable – Habilita a troca de mensagens entre os *peers*.
- peer 211.111.112.178 route-policy 318860-IN import – Relacionamos o *peer* com a política.
- Na política 318860-IN, informaremos o valor do atributo *local preference*. Ex.:
  - route-policy 311110-IN permit node 10
    - apply local-preference 300

Assim, o *local preferente* para o *peer* 211.111.112.178 qure representa uma das minhas saídas para Internet terá valor igual a 300. Internamente, no AS, quando um roteador tiver que avaliar o destino de um pacote, optará pela saída com maior local preference. Esse atributo, quando configurado em um roteador, será enviado a todos os roteadores pertencentes ao mesmo AS. A figura 18.9 apresenta uma rede com essa característica.

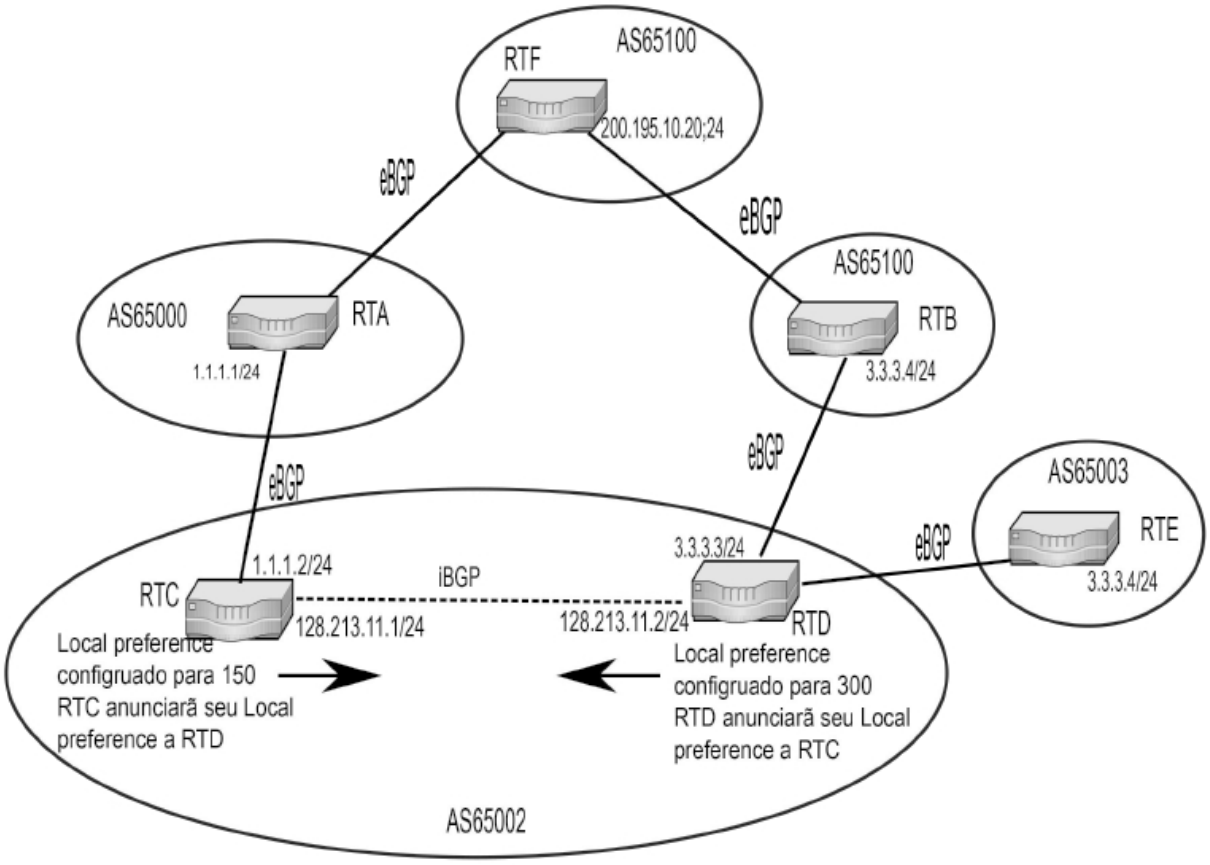



*Figura 18.9 – Atributo local preference.*

Conforme observamos na figura 18.9, os roteadores do AS65002 poderão alcançar a rede 200.195.10.20/24 pelos AS65000 e AS65001. Como a sessão BGP com o AS65001 considerou um *local preference* maior (300), os roteadores do AS65002 sempre darão prioridade para sair pelo roteador RTD.

## 18.7.3 Atributo AS-PATH

O atributo AS-PATH é conhecido e mandatório (*well-known mandatory*), ou seja, estará presente nas mensagens de update trocadas entre sessões BGP. O conteúdo desse atributo conterá uma lista de ASs por meio dos quais o destino pode ser alcançado. Além de conter a lista dos ASs que o pacote seguirá até alcançar seu destino, esse parâmetro evita também a ocorrência de loop, ou seja, caso um roteador receba uma rota e verifique seu AS, este simplesmente descartará a rota, pois identificará que já foi recebida

e trata-se de um loop. A figura 18.10 apresenta um exemplo do uso do atributo AS-PATH.

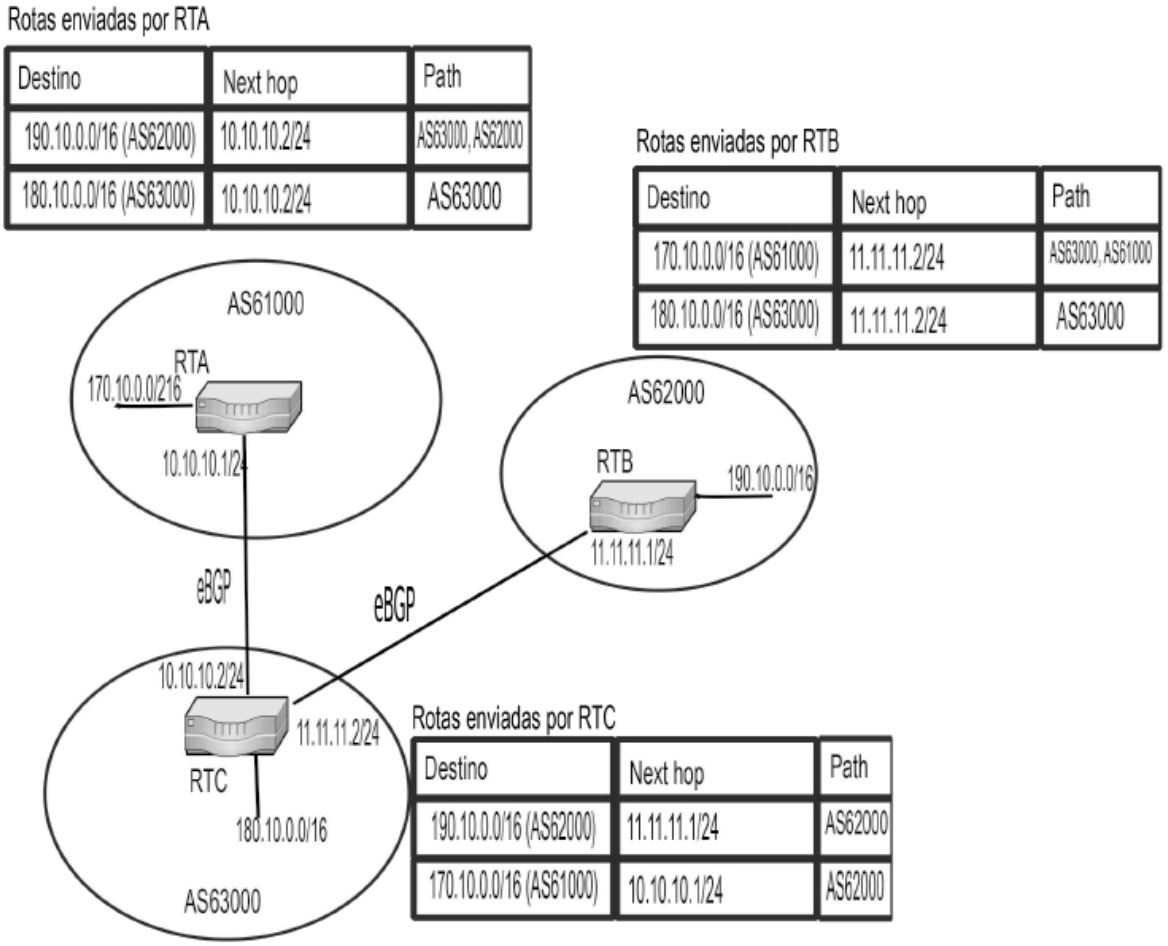



*Figura 18.10 – Atributo AS-PATH.*

Com o atributo AS-PATH, podemos realizar a operação de *prepend*, que se caracteriza por piorar o AS-PATH para determinado destino, forçando que outros caminhos possam ser escolhidos por possuírem um caminho com menor AS-PATH. Com essa operação, adicionamos o mesmo AS mais de uma vez, fazendo que a lista de ASs aumente e torne uma determinada rota pior que outra. Na tabela 18.4, vemos que para alcançar o destino 14.200.200.0/21, o caminho a ser seguido sofreu ajustes com o comando prepend (3549 2828 7545 7545 7545 7545i). O AS 7545 foi adicionado algumas vezes para piorar a rota divulgada. É importante observar que as rotas recebidas de AS vizinhos impactarão o envio de pacotes,

enquanto as rotas enviadas a AS vizinhos impactarão como a Internet as acessará.

### 18.7.4 Atributo origin

O atributo *origin* define a origem da informação de roteamento. Pode assumir um dos seguintes três valores:

- 1 origem IGP (i).
- 2 origem EGP (e).
- Origem INCOMPLETE (?).

Quando receber o valor 1, significará que a rota foi recebida de um protocolo IGP, como OSPF, RIP ou IS-IS. Quando receber o valor 2, significará que a rota foi recebida do protocolo BGP, que é um protocolo EGP. Quando receber o valor 3, significará que a rota foi recebida de uma fonte desconhecida. No Huawei, qualquer rota injetada no BGP, seja estática, interface diretamente conectada, RIP, IS-IS ou OSPF, ficará com ?. Na tabela 18.4, percebemos que as rotas aprendidas foram via protocolo IGP.

### 18.7.5 Atributo MED

O atributo MED (*Multi-Exit Discriminator*) é utilizado para determinar por qual de duas ou mais saídas o roteador enviará seus pacotes. A figura 18.11 apresenta um exemplo do uso do atributo MED.

Conforme podemos observar na figura 18.11, a comunicação entre o roteador de Curitiba situado no AS65004 e o AS65003 ocorrerá pelo link com atributo MED definido com 50 (o menor torna uma rota a preferida).

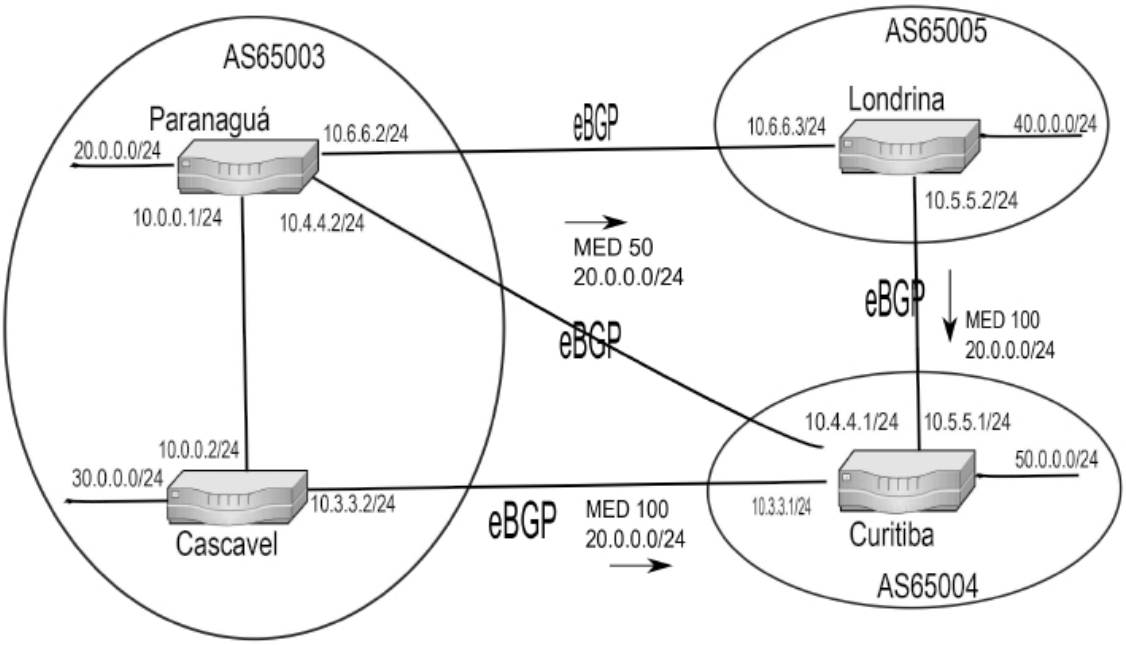



*Figura 18.11 – Atributo MED.*

O roteador de Curitiba no AS65004 pode alcançar a rede 20.0.0.0/24 no AS65003, diretamente pelo roteador de Paranaguá, ou seguir por um link redundante, passando pelos roteadores de Cascavel e, em seguida, pelo roteador de Paranaguá. Pode ainda alcançar a rede 20.0.0.0/24 pelo roteador de Londrina, porém vamos dar ênfase na comunicação com o AS65003, em que modificamos o atributo MED.

O roteador de Curitiba compara o valor do atributo MED recebido dos dois roteadores do AS65003. O roteador de Cascavel anuncia a rota com valor do MED igual a 100, enquanto o roteador de Paranaguá anuncia a rota com valor do MED igual a 50. Nesse caso, o roteador de Curitiba adicionará a rota recebida do roteador de Paranaguá à FIB, pois esta, em nosso exemplo, foi considerada a melhor rota.

É importante observar que por padrão o BGP compara o atributo MED de rotas aprendidas de um mesmo AS. Nesse caso, o roteador de Curitiba poderá comparar somente o atributo MED da rede 20.0.0.0/24 que foi recebida dos roteadores de Cascavel e Paranaguá. Por padrão, o roteador de Curitiba somente avaliará o atributo entre roteadores localizados em um mesmo AS. No caso do

roteador de Londrina, por estar em um AS diferente, não avaliará o atributo MED, pois, por esse caminho, só existe uma opção.

Entretanto, podemos usar o parâmetro *always-compare-med* para configurar o roteador de Curitiba, considerando o atributo MED do roteador de Londrina. Em roteadores Juniper, podemos utilizar o comando set protocols bgp path-selection always-compare-med, que fará que o roteador sempre compare o atributo MED independentemente do AS. Com isso, caso tenhamos duas rotas para um determinado destino e o prefixo de rede das duas opções e o local preference sejam iguais, caso possuam o mesmo AS-PATH, então o atributo MED será utilizado na decisão da melhor rota.

Em roteadores Huawei, podemos utilizar os seguintes comandos para permitir que o atributo MED seja avaliado independentemente do AS: acessar o modo de configuração do roteador com o comando system. Acessar o ambiente de configuração do AS com o comando: bgp 14868, em que 14.868 representa o AS da operadora utilizada nos exemplo. Estando no nível do AS, devemos digitar o comando: compare-different-as-med. Com isso, apesar de o atributo MED do AS65005 ser menor (valor 10), para alcançar a rede 20.0.0.0/24, a melhor rota ainda será através do AS65003, devido a possuir um AS-PATH menor.

Conforme comentado, os atributos BGP são enviados entre os roteadores pela mensagem update. Porém, além dessa mensagem, o protocolo BGP utiliza outras mensagens para sua operação. Assim, veremos a seguir os detalhes das mensagens trocadas pelo protocolo BGP.

## 18.8 Mensagens BGP

O protocolo BGP utiliza mensagens para estabelecer a sessão e atualizar rotas que tenham sido alteradas. Temos quatro tipos de mensagens conhecidas por *open*, *update*, *notification* e *keepalive*. Vejamos cada uma delas com mais detalhes:

- **Mensagem open** (abertura) – Será enviada após a conexão TCP entre os roteadores estar concluída. Possui como finalidade iniciar o processo do estabelecimento de uma conexão BGP. É a primeira

mensagem enviada por um roteador que deseja estabelecer uma sessão BGP com seu par (*peer*). Durante o estabelecimento da sessão, ambos trocam mensagens *open* para que os parâmetros importantes para o BGP sejam reconhecidos e a sessão alcance o estado de *established*. Como parâmetros trocados, temos versão do BGP, número do AS, *router-id*, tempo de espera (*hold time*) e parâmetros opcionais. A figura 18.12 demonstra que uma mensagem *open* será trocada durante vários estados entre o início e a conclusão do estabelecimento de uma sessão BGP

- **Mensagem update** (atualização) – É utilizada para os anúncios propriamente ditos, incluindo rotas que devem ser incluídas na tabela e também que devem ser removidos da tabela BGP, devido a terem ficado indisponíveis. É dentro dessas mensagens que seguem informações sobre cada prefixo de rede que está sendo anunciado. Essas mensagens serão trocadas após a sessão BGP encontrar-se no estado *established*. A figura 18.12 apresenta o momento (estado *established*) em que as mensagens *updates* começam a serem trocadas.
- **Mensagem notificação** (*notification message*) – São enviadas para os seguintes fins:
  - Reportar erros de algumas das mensagens enviadas.
  - Informar possíveis problemas nas conexões BGP.
  - Encerrar uma sessão ativa e informar a todos os roteadores conectados o motivo do encerramento da sessão.
  - Informar que o tempo de *hold time* expirou.

Sempre que um roteador enviar uma mensagem do tipo *notification,* finalizará a sessão BGP correspondente. Na figura 18.12, podemos observar que em todos os casos em que houver uma mensagem *notification*, o estado será direcionado para o estado *idle*.

- **Mensagem keepalive** (ainda estou aqui) – São utilizadas para garantir que a conexão entre dois roteadores se mantenha ativa. Dois roteadores, após alcaçarem o estado *established,* precisam manter-se vivos e, para isso, podem trocar mensagens update caso exista alguma novidade quanto às rotas. Caso não sejam

trocadas mensagens update, as mensagens *keepalive* formalizarão que ambos continuam conectados e que nenhum problema foi identificado. As mensagens *keepalive* são utilizadas inicialmente para confirmar o estabelecimento da sessão BGP (mudança do estado *openconfirm* para *established*) e, em seguida, para mantê-la ativa.

As mensagens *keepalive* são enviadas por um período previamente configurado nos roteadores que fecham sessão. Assim, a cada período de tempo previamente acordado, cada roteador enviará uma mensagem *keepalive* para que o seu par (*peer*) saiba que há conectividade. Caso o *keepalive* atrase, o roteador começará a contagem de *hold time* e, se nesse período não for recebido nenhum *keepalive*, a sessão BGP será finalizada. É importante observar que o tempo de *keepalive* como o de *hold time* podem ser configurados para mais ou menos tempo. O valor-padrão de *keepalive* é 60 segundos e o de *hold time*, 180 segundos. Alguns administradores de rede optam ainda por hold time em 90 segundos e *keepalive* em 30 segundos. É importante observar sempre que o valor de *hold time* deve ser o triplo do valor do *keepalive*.

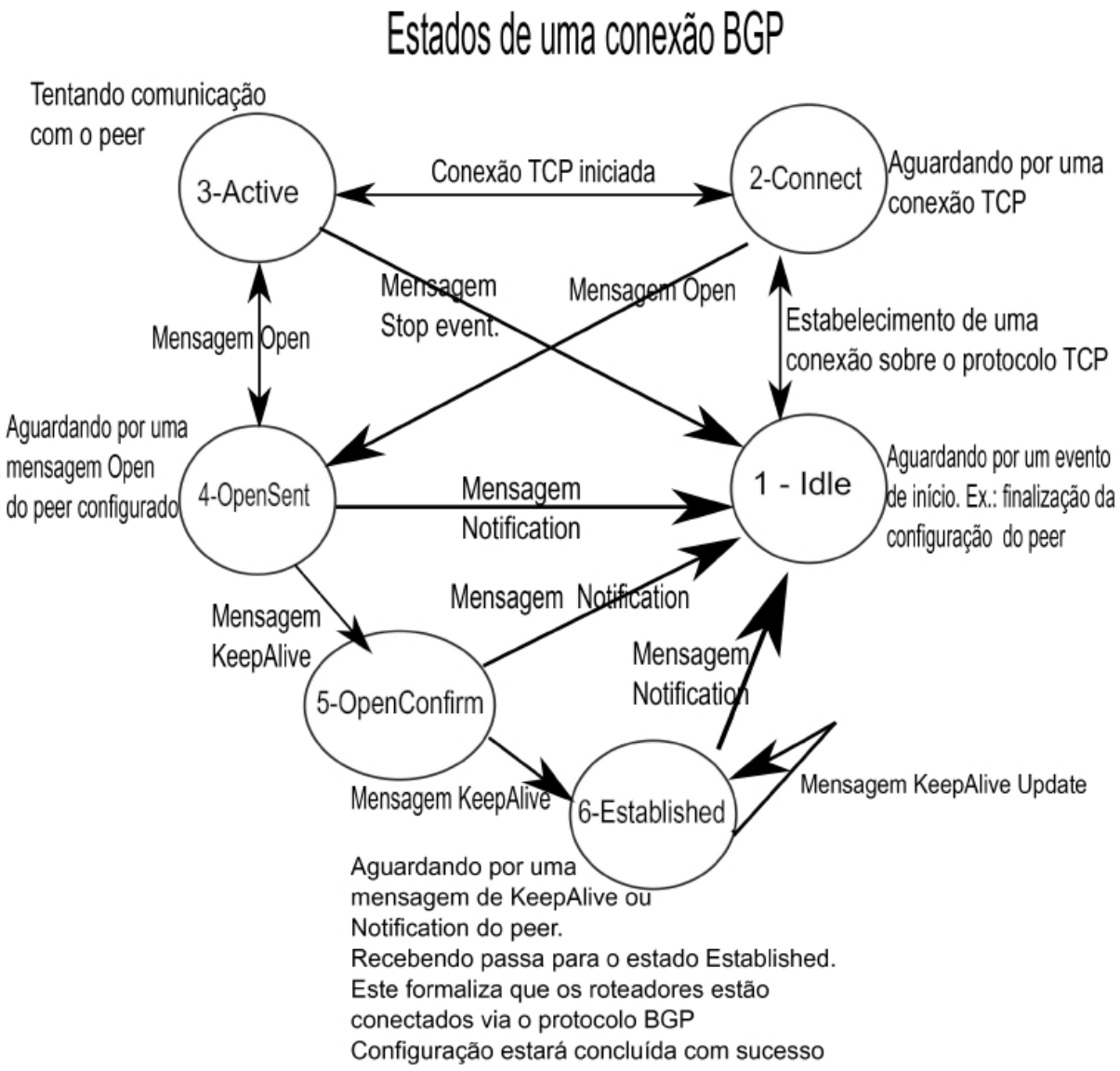



*Figura 18.12 – Mensagens e estados BGP.*

Conforme observado na figura 18.12, entre o início e o fim do estabelecimento da sessão BGP, temos seis estados. Vejamos o que cada um representa:

- *Idle* – Identifica o primeiro estágio de uma conexão BGP, em que o protocolo está aguardando uma conexão de um *peer* remoto. Este é o estado em que a sessão BGP permanece quando é interrompida por uma mensagem de notificação ou intervenção do administrador de rede. Caso se perceba esse estado durante muito tempo, isso apontará algum problema de conectividade IP ou, ainda, que o BGP nao foi configurado corretamente em algum dos

lados. O próximo estado é chamado de *connect*. Caso exista falha durante esse estado, a sessão voltará para o estado *idle*.

- *Connect* – Neste estado, o BGP aguarda para estabelecer uma conexão TCP (protocolo da camada de transporte) através da porta 179. Quando a conexão TCP estiver estabelecida, assume-se o estado *connect*, envia-se uma mensagem *open* e passa-se ao estado de *opensent*. Se a conexão ao nível da camada de transporta não for bem-sucedida, o estado irá para *active*. No caso de o tempo de espera (*hold time*) ser alcançado, o estado voltará para *connect* e será reiniciada nova tentativa para estabelecer uma nova conexão. Em qualquer outro evento, retorna-se para o estado *idle*.
- *Active* – Este estado será alcançado quando não for possível estabelecer ou manter a sessão TCP através da porta 179. O BGP continuará tentando estabelecer uma sessão TCP com o seu par (*peer*). Ao conseguir, enviará uma mensagem *open* e mudará o estado para *opensent*. Se essa tentativa não for bem-sucedida, pelo motivo de expiração do tempo, por exemplo, o estado passará para *connect*. Em caso de interrupção pelo sistema ou pelo administrador de rede, volta-se ao estado *idle*. Geralmente, as transições entre o estado de *connect* e *active* refletem problemas no estabelecimento de uma conexão TCP.
- *Opensent* – Neste estado, o BGP aguarda a mensagem de *open* de seu par (*peer*) e faz uma checagem de seu conteúdo após o receber. Caso seja encontrado algum erro, como número de AS incoerente ao esperado ou a própria versão do BGP, envia-se uma mensagem de *notification* e volta-se ao estado *idle*. Caso não ocorram erros na checagem, inicia-se o envio de mensagens *keepalive* e segue-se ao estado de *openconfirm*.

  Em seguida, negocia-se o tempo de *hold time* e *keepalive* entre os pares (*peers*). Caso os pares possuam valores diferentes, optar-se-á pelo menor tempo entre os dois pares. Depois desse acerto, compara-se o número do AS local e o número do AS enviado pelo *peer*, com o intuito de detectar se se trata de uma conexão iBGP (números de AS iguais) ou eBGP (números de AS diferentes). Em

caso de desconexão ao nível do protocolo de transporte, o estado passa para *active*. Para as demais situações de erro, como expiração do tempo de *hold time*, envia-se uma mensagem *notification* com o código de erro correspondente e retorna-se ao estado *idle*. No caso de intervenção do administrador, também se retorna ao estado *idle*.

- *Openconfirm* – Neste estado, o BGP aguarda a mensagem de keepalive do seu par (*peer*). Quando for recebida, o estado seguirá para *established* e a negociação com o par será finalmente concluída. Com o recebimento da mensagem de *keepalive*, é confirmado o valor de *hold time* entre os *peers*. Se o sistema receber uma mensagem *notification*, retorna-se ao estado de *idle*. O sistema também envia periodicamente, seguindo o tempo negociado, mensagens de *keepalive*. No caso da ocorrência de eventos como desconexão ou intervenção do administrador da rede retorna-se ao estado de *idle*.
- *Established* – Neste estado, o BGP inicia a troca de mensagens *update* ou *keepalive*, de acordo com a periodicidade negociada. Caso seja recebida alguma mensagem *notification*, retorna-se ao estado *idle*. No recebimento de cada mensagem de *update*, aplica-se uma checagem nos atributos, observando se existem atributos incorretos, atributos duplicados ou ainda se há a falta de algum. Caso algum erro seja detectado, envia-se uma mensagem *notification*, retornando ao estado *idle*. Por fim, se o *hold time* negociado expirar ou for detectada desconexão ou intervenção do administrador, também se retorna ao estado de *idle*.

## 18.9 eBGP multihop

Normalmente, uma sessão eBGP é fechada entre dois roteadores conectados diretamente ponto a ponto, com endereço de rede com máscara /30. Por exemplo, dado que a operadora definiu o endereço IP 167.220.155.248/30, o endereço IP 167.220.155.249 seria configurado no roteador da operadora e o endereço IP 167.220.155.250, no roteador do cliente. A figura 18.13 apresenta um exemplo em que a sessão BGP será estabelecida entre dois

roteadores conectados ponto a ponto.

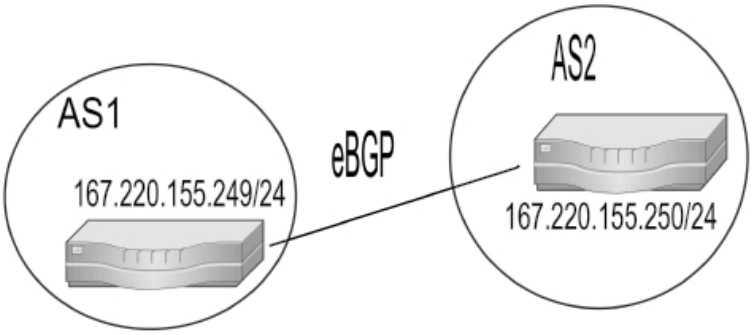



*Figura 18.13 – Sessão eBGP com interfaces diretamento conectadas.*

Entretanto, digamos que o cliente precise que a sessão BGP seja estabelecida com um endereço IP público de sua propriedade, ou seja, o endereço IP 157.124.176.3. Esse é o endereço de um roteador interno do cliente, ou seja, não está diretamente conectado ao roteador da operadora. Nesse caso, utilizaremos o conceito de eBGP *multihop*, ou seja, a sessão eBGP não será estabelecida entre dois roteadores com as interfaces diretamente conectadas, e sim com um segundo roteador. A figura 18.14 apresenta um ambiente em que a sessão será estabelecida com um roteador interno ao AS (AS2) do cliente.

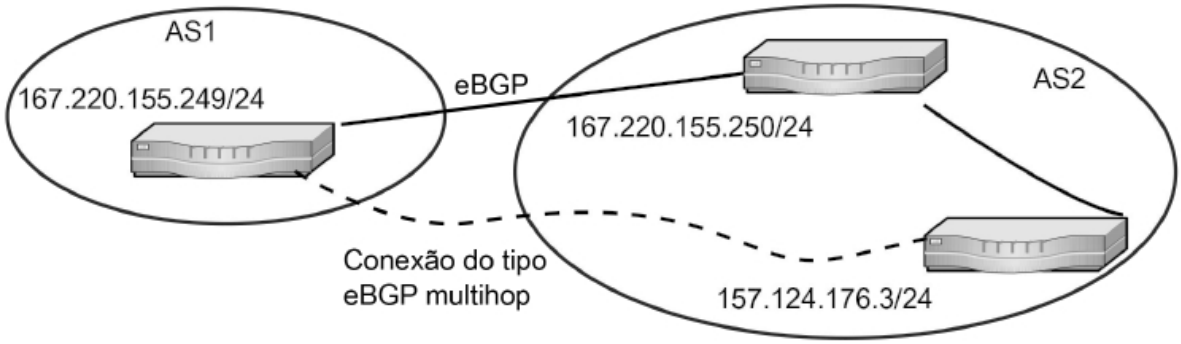



*Figura 18.14 – Sessão eBGP multihop.*

Para que essa atividade seja concluída, além dos comandos

necessários para configurar uma sessão BGP, precisará, ainda, permitir que o roteador da operadora consiga alcançar a rede do endereço IP escolhido pelo cliente. Nesse caso, criamos uma rota estática no roteador da operadora para permitir que o endereço IP (157.124.176.3) seja alcançado. No caso de roteadores Huawei, podemos utilizar o seguinte comando para a criação da rota estática: ip route-static 157.124.176.3 32 167.220.155.250. Com essa rota, o roteador da operadora conseguirá alcançar o endereço IP interno do cliente. Em seguida, devemos formalizar que o endereço IP do *peer* utilizará o conceito de eBGP *multihop*. Para isso, na plataforma Huawei, utilizamos o comando: peer 157.124.176.3 ebgp-max-hop. Se o roteador fosse Cisco, utilizaríamos o comando neighbor 157.124.176.3 ebgp-multihop.

## 18.10 Exercícios do capítulo 18

1. Descreva as caraterísticas do protocolo BGP.
2. Qual é a diferença entre protocolos classificados como IGP e EGP?

APÊNDICE A

# Estudo de caso

## A.1 Título

Desenvolvimento do sistema de comunicação de dados e redes de computadores de uma instituição de ensino com campos em três capitais: Rio de Janeiro, São Paulo e Curitiba.

## A.2 Objetivo

O objetivo deste trabalho é desenvolver a capacidade de resolver projetos de rede de computadores no que concerne a avaliação do problema, treinamento de funcionários da instituição de ensino até a escolha de equipamentos, tecnologias, configurações e planejamento da instalação.

## A.3 Ambiente a ser utilizado para o desenvolvimento do projeto

No Rio de Janeiro, os cursos ofertados são Oceanografia, Geografia, Engenharia Cartográfica, Engenharia Civil, Engenharia Elétrica, Engenharia Mecânica e Engenharia da Computação. Observe as características de cada disciplina, pois os laboratórios deverão acompanhar o estilo do curso. Cursos de Engenharia, por exemplo, devem ter um laboratório mais sofisticado para a execução do CAD.

Em São Paulo, os cursos ofertados são Bacharelado em Informática, Ciência da Computação, Matemática e Física. Em Curitiba, os cursos ofertados são Administração de Empresas, Sistemas de Informação, Marketing, Pedagogia, História, Direito, Biologia, Farmácia, Medicina e Robótica.

Todos os cursos são distribuídos em blocos relacionados às áreas Exatas, Biológicas e Humanas. Além disso, a instituição possui um centro para controles administrativos e uma biblioteca que deverá

disponibilizar acesso à Internet.

## A.4 Proposta para o desenvolvimento do projeto

**1.** Identificar uma estimativa do número de laboratórios disponíveis para os cursos.

**2.** Determinar os seguintes equipamentos para cada cidade: servidores, equipamentos ativos (router e switches), circuitos de comunicação, cabeamento estruturado, proteção da rede elétrica (*No-break*), sistema de backup, contingência, segurança, impressoras, acesso à Internet e configuração dos protocolos necessários à comunicação.

**3.** Levantar o Backbone local (LAN) da instituição em cada cidade.

**4.** Levantar o Backbone remoto (WAN) necessário à interligação da instituição entre as capitais. Identificar alternativas de protocolos WAN e justificar a sua escolha.

**5.** Avaliar as necessidades dos administradores locais. O que o seu cliente espera que você forneça a ele.

**6.** Dividir os núcleos específicos de cada sub-rede (blocos, laboratórios, biblioteca, centro administrativo etc.).

**7.** Diagramar o projeto (desenhos esquemáticos da distribuição dos laboratórios, centros de computação, sistemas de comunicação, centro administrativo etc.). No diagrama, deverão ser apresentados o endereço IP e a máscara de rede para cada equipamento.

**8.** Apresentar as possíveis soluções com sistemas operacionais diferentes.

**9.** Apresentar planilha de custos de compra, instalação, configuração e treinamento.

**10.** Determinar cronograma de implantação.

**11.** Elaborar o treinamento

## A.5 Observações finais

Este é um trabalho didático, mas que se aproxima muito de uma possível realidade futura de qualquer um dos profissionais dessa

área. Assim, é o momento ideal para aprender os conceitos relacionados a esse assunto disponível e discutir qualquer ponto ou necessidade que se encontre no caminho profissional.

# APÊNDICE B
# Respostas dos exercícios

## Capítulo 1

**1. Cite sete recursos que podem ser compartilhados em uma rede.**

- Impressora
- Scanner
- Unidade de CD-ROM e DVD
- Placa de Fax/Modem
- Conexão com a Internet e a Extranet
- Conexão com outras arquiteturas e plataformas como Mainframe.
- Disco rígido
- Arquivos

**2. O que levou as redes de computadores a se tornarem tão acessíveis?**

A principal razão está relacionada à atitude tomada por quem iniciou as pesquisas sobre as redes. A empresa que inventou o padrão Ethernet não quis tornar tal descoberta um produto de um único dono, liberando o padrão para o mercado.

**3. Qual é o objetivo do padrão OSI? Por que esse padrão foi concebido?**

Foi criado com o objetivo de oferecer um padrão para as redes de computadores. No início das redes, cada fabricante possuía o seu próprio padrão, não permitindo que um cliente migrasse para outro fornecedor sem ter de investir em hardware e software novamente. No começo, o software e o hardware também estavam totalmente dependentes um do outro. Tal atitude gerou benefícios em relação à padronização de equipamentos de rede.

**4. Qual a influência da IBM no processo de definição do modelo**

**de referência OSI?**

Como representava uma das maiores empresas de informática e fornecedora de equipamentos de rede, a IBM praticamente ditou o formato do modelo de referência OSI, o qual ficou muito semelhante ao padrão da IBM conhecido por SNA.

**5. Comente o modelo de referência TCP/IP.**

Esse padrão foi criado pelo Departamento de Defesa americano com o objetivo de uso militar. Devido ao seu grande sucesso, tornou-se um padrão aberto e tem sido utilizado em todo o mundo. A Internet está baseada nesse padrão.

**6. Qual é a diferença entre LAN, MAN e WAN?**

- **LAN** – *Local Área Network*. Trata-se de uma rede local, por exemplo, uma rede montada dentro de um escritório de informática, ou uma rede criada dentro de uma empresa que interligue todos os departamentos. Fisicamente, uma rede LAN está situada no mesmo local físico.
- **MAN** – *Metropolitan Area Network*. Trata-se de uma rede metropolitana, por exemplo, uma rede montada dentro de um escritório de informática sendo interligada ao segundo escritório localizado na área metropolitana de uma grande cidade.
- **WAN** – *Wide Area Network*. Trata-se de uma rede global, por exemplo, uma rede montada dentro de um escritório de informática, sendo conectada a outra rede localizada em outra cidade ou país. A Internet é um exemplo de uma rede WAN.

**7. Onde surgiu a Internet? Descreva a sua origem.**

A rede Internet teve seu início nas décadas de 1960 e 1970, em função da necessidade de o governo americano, representado pelo Departamento de Defesa, querer transmitir dados entre suas bases militares na Guerra Fria, a qual envolveu os Estados Unidos e a extinta União Soviética. A rede criada foi chamada de ARPANET.

A rede ARPANET utilizou o conceito de transmissão de dados divididos em pequenos pacotes, exatamente como acontece com a rede Internet atualmente. Essa divisão teve como objetivo garantir

que, em caso de ataque, a base poderia rotear esses pacotes por outros caminhos, sem causar prejuízo na entrega da informação.

Com o passar dos anos, essa rede bem-sucedida foi também utilizada pelas universidades americanas e continua sendo por todos os que acessam a Internet.

**8. Qual é a diferença entre Intranet e Extranet?**

- Intranet: trata-se de uma rede LAN distribuída dentro de uma empresa, executando os protocolos do modelo de referência TCP/IP.
- Extranet: segue o mesmo conceito, mas as redes se comportam como uma MAN ou WAN.

**9. Cite as vantagens e desvantagens das redes de computadores.**

As vantagens são:

- A possibilidade de compartilhar dados, conseguir informações em pequeno espaço de tempo, poder comunicar-se com amigos ou parentes em lugares distantes, sem gastar com caríssimas ligações telefônicas, facilidade de movimentar arquivos e a integração entre empresas diferentes.

As desvantagens são:

- Possibilidade da perda de informações sigilosas, alteração de dados sigilosos, vírus de computador, pirataria, assédio em todos os sentidos e negociação irregular.

**10. Quais são os componentes de uma rede?**

Placa de rede, conectores, concentradores, equipamentos ativos, modems, cabos e software especializado.

**11. Qual é a arquitetura de rede local utilizada pela maioria das redes no mundo? A rede em que você trabalha possui qual arquitetura?**

No mundo, utiliza-se fortemente o modelo Ethernet. Em minha empresa, utilizamos o padrão Ethernet 100Mbps para a LAN e 10 Gbps entre centros administrativos.

**12. Qual é a largura de banda da rede em que você estuda ou trabalha? Que largura de banda você considera ideal para o seu ambiente de estudo ou trabalho?**

Em minha empresa, utilizamos 100 Mbps, 1.000 Mbps e 10 Gpbs. O melhor custo-benefício seria o das redes 100 Mbps.

**13. Cite e comente quatro entidades de padronização.**

- **IANA** – A sigla significa *Internet Assigned Numbers Authority*. Essa entidade supervisiona a distribuição e o uso dos endereços IPs e de zonas DNS. Na Internet, cada rede possui um endereço de rede IP, o qual não será utilizado por nenhuma outra rede interligada à Internet. Quem garante isso é a entidade IANA.
- **ISO** – A sigla significa *Open Systems Interconnection Basic Reference Model*. A ISO desenvolveu o padrão OSI, com o objetivo de oferecer às empresas um modelo de referência único para a construção de *softwares* e equipamentos de rede.
- **IETF** – A sigla significa *Internet Engineering Task Force*. Trata-se de uma entidade que tem o objetivo de garantir a evolução da Internet e desenvolver e promover padrões para a Internet, registrando-os em documentos conhecidos por RFCs (*Request for Coments*). Todo novo conceito empregado em redes de computadores poderá ser mais bem entendido analisando sua RFC respectiva.
- **IEEE** – A sigla significa *Institute of Electrical and Electronics Engineers*. Trata-se de uma organização sem fins lucrativos, cujo objetivo é definir o avanço da teoria e da prática da ciência da computação e das telecomunicações.

**14. Qual entidade é responsável pela distribuição de endereços IP e nomes de domínio no Brasil?**

A distribuição dos endereços IP no Brasil fica sob a responsabilidade da Registro.br, que está vinculada à entidade Fapesp (Federação de Amparo à Pesquisa do Estado de São Paulo).

**15. Descreva a URL (Uniform Resource Locator) da empresa**

**onde você trabalha.**

Exemplo: *protocolo://equipamento/caminho/recurso ou http://www.banco.com.br/index.html*

O item protocolo pode conter HTTP ou FTP. O item equipamento refere-se ao servidor que responderá ao pedido solicitado. O caminho refere-se ao diretório pertencente ao servidor em que o recurso está gravado.

**16. Descreva como foi composto seu endereço de email.**

*nomeusuario@seudominio.com.br*.

Exemplo: *douglas@novatec.com.br*.

**17. Quais são os equipamentos ativos que sua empresa possui instalados?**

Exemplos: hubs, switches e roteadores.

**18. Qual é o sistema operacional de rede instalado nos servidores de sua empresa?**

Exemplos: UNIX IBM/AIX e HPUX, Linux e Windows XP.

**19. Quais são o sistema operacional e o modelo da placa de rede do seu computador?**

Exemplos: Windows XP e placa 3COM 100 Mbps.

**20. Qual é o modelo do cabo de rede que o seu computador utiliza?**

Exemplo: Cabo par trançado categoria 5.

**21. Qual é a largura de banda da rede em que você trabalha ou estuda?**

Exemplo: 100 Mbps.

**22. Uma Intranet tradicional é:**

a) Uma rede-padrão LAN que utiliza o protocolo TCP/IP para comunicação.

b) Uma rede corporativa que utiliza o protocolo IPX da Internet para seu transporte fundamental.

c) Composta de inúmeras redes de empresas distintas.

d) Uma rede privativa que permite fácil acesso à Internet, utilizando o protocolo TCP/IP, diferentemente de uma Extranet.

e) Uma rede na qual não podemos ter servidores, existindo apenas máquinas de usuários.

Alternativa correta: a.

# Capítulo 2

**1. Qual é a arquitetura de redes mais usada em projetos de redes?**

Arquitetura Ethernet, responsável pelas camadas físicas e de enlace, e o modelo de referência TCP/IP, responsável por definir as camadas de rede, transporte e aplicação.

**2. Como são conhecidas as redes que transmitem dados a 100 Mbps?**

São conhecidas como redes Fast Ethernet, as quais utilizam cabo par trançado, ou redes FDDI, que utilizam cabo de fibra óptica.

**3. Como são conhecidas as redes que transmitem dados a 1 Gbps?**

São conhecidas como redes Gigabit Ethernet.

**4. Qual é a função do protocolo CSMA/CD nas redes Ethernet? Qual é sua importância?**

O CSMA/CD é responsável por controlar as colisões das redes Ethernet. Esse protocolo é muito importante, pois sem ele não obteríamos sucesso no uso das redes Ethernet.

**5. Quais são os meios de comunicação utilizados pelo padrão Ethernet para transmitir dados?**

Cabo par trançado, cabo coaxial e fibra óptica.

**6. O que acontece quando duas estações transmitem dados ao mesmo tempo em uma rede Ethernet?**

Ocorre o problema de colisão. Após uma colisão ser identificada pelo protocolo CSMA/CD, as máquinas envolvidas na colisão deverão esperar um tempo aleatório para voltar a transmitir os

dados.

**7. Quando mais equipamentos são inseridos em um segmento de rede utilizando um hub, qual é o comportamento da rede?**

A rede tende a ficar mais lenta, pois é natural das redes Ethernet o problema de colisão. Quanto mais equipamentos na rede, maior é a probabilidade de colisões ocorrerem.

**8. Qual protocolo Ethernet faz a detecção de colisão?**

O protocolo CSMD/CD.

**9. Que topologia de rede você utiliza na escola/trabalho?**

Exemplos: topologias anel, barramento e estrela.

**10. Defina o processo de reflexão apresentado nos cabos coaxiais.**

Quantidade duplicada de tensão trafegando pelo segmento da rede.

**11. (Sanepar, 2004) Assinale a alternativa que descreve corretamente o comportamento do protocolo Ethernet na ocorrência de uma colisão:**

a) O protocolo retransmite imediatamente.

~~b) O protocolo aguarda um tempo aleatório e retransmite.~~

c) O protocolo aguarda um tempo aleatório, verifica se há portadora no meio e, caso não haja, retransmite.

d) O protocolo aguarda o meio ficar livre e retransmite.

e) O protocolo aguarda o meio ficar livre e retransmite com uma probabilidade p, definida pelo padrão IEEE802.3.

Alternativa correta: b.

**12. (Sanepar, 2004) Uma colisão pode ocorrer em alguns protocolos quando duas máquinas compartilham o mesmo meio de transmissão e tentam utilizá-lo ao mesmo tempo. Considere as afirmativas a seguir relativas às colisões em redes locais:**

I. Colisões podem ocorrer em redes Fast Ethernet não comutadas, ou seja, utilizando um hub.

II. Uma colisão pode ocorrer em redes com topologia anel, como a rede Token Ring.

III. Colisões nunca ocorrem em redes Ethernet comutadas, ou seja, utilizando um switch.

IV. O número de colisões está diretamente relacionado ao desempenho da rede.

a) Somente as afirmativas I, III e IV são verdadeiras.

~~b) Somente as afirmativas I e IV são verdadeiras.~~

c) Somente as afirmativas II e III são verdadeiras.

d) Somente as afirmativas II, III e IV são verdadeiras.

e) Somente as afirmativas III e IV são verdadeiras.

Alternativa correta: b.

**13. (Enade, 2008 _ Computação) Em redes locais de computadores, o protocolo de controle de acesso ao meio define um conjunto de regras que deve ser adotado pelos múltiplos dispositivos para compartilhar o meio físico de transmissão. No caso de uma rede Ethernet IEEE 802.3 conectada fisicamente a um concentrador (hub), em que abordagem se baseia o protocolo de controle de acesso ao meio?**

a) Na passagem de permissão em anel.

b) Na ordenação com contenção.

c) Na ordenação sem contenção.

~~d) Na contenção com detecção de colisão.~~

e) Na arbitragem centralizada.

Alternativa correta: d.

# Capítulo 3

**1. Qual foi o principal objetivo do modelo de referência OSI?**

Oferecer uma interface para padronizar os equipamentos e softwares utilizados em redes de computadores.

**2. Quantas e quais são as camadas do modelo de referência OSI?**

No modelo de referência OSI, são sete camadas: aplicação, apresentação, sessão, transporte, rede, enlace e física.

**3. Qual camada do modelo OSI é responsável pelas funções de criptografia, conversão de códigos e formatação?**

~~a) Apresentação.~~

b) Sessão.

c) Transporte.

d) Física.

Alternativa correta: a.

**4. O modelo de referência OSI é:**

a) Padrão direcionado para interconexão homogênea.

b) Padrão de arquitetura proprietária.

c) Exemplo de sistema fechado.

~~d) Exemplo de sistema aberto.~~

Alternativa correta: d.

**5. Que camada do modelo OSI suporta diretamente as aplicações do usuário final?**

~~a) Aplicação.~~

b) Sessão.

c) Apresentação.

d) Rede.

Alternativa correta: a.

**6. A camada do modelo OSI que atua como um dispositivo de chaveamento (switch) para rede local é conhecida pela camada:**

a) Física.

~~b) Enlace.~~

c) Rede.

d) Transporte.

Alternativa correta: b.

**7. A camada OSI de comunicação de dados que atende às funções de criptografia, compreensão de textos e conversão de padrões de terminais é a camada de:**

a) Sessão.

b) Aplicação.

~~c) Apresentação – camada responsável por prover independência aos processos de aplicação das diferenças na representação dos dados (sintaxe). Entra EBCDIC e essa camada converte para ASCII. Nessa camada, ocorrem a criptografia e a compressão de dados.~~

d) Transporte.

Alternativa correta: c.

**8. Em qual camada do modelo OSI atua o dispositivo bridge:**

a) Física – É a única camada que possui acesso físico ao meio de transmissão da rede. Cuida de diversos fatores, como especificações elétricas, mecânicas, funcionais e de procedimento de interface física entre o equipamento e o meio de transmissão. Como exemplo, temos o controle da distância máxima dos cabos. Sua principal tarefa é adaptar o sinal ao meio de transmissão sem levar em conta o significado dos dados. Aqui não importa a sequência dos bits que são tratados individualmente.

~~b) Camada de enlace – Tem o objetivo de fornecer uma conexão confiável com o meio físico. Deve detectar e, em alguns casos, corrigir erros que possam ter ocorrido no nível físico, como as colisões de dados, por exemplo. Essa camada, diferentemente da camada física, gerencia o acesso ao meio de transmissão, o fluxo de dados em frames e sua sequência. Outro controle efetuado por essa camada é a sincronização de dados transmitidos entre o receptor e o emissor. Em geral, isso ocorre quando os dados são transmitidos a taxas mais elevadas do que as suportadas pelo receptor, o que provocaria o esgotamento do~~

~~buffer de recepção existente na placa de rede do receptor.~~

c) Rede – A tarefa da camada de rede é preparar o modo como os recursos existentes nas camadas inferiores serão utilizados para implementar conexões de rede, ou seja, aqui é reconhecida a existência de vários computadores conectados em rede, o que não ocorre nas camadas física e de enlace. É nessa camada que eventuais sub-redes com diferentes sistemas operacionais terão suas diferenças compatibilizadas, já que, para o usuário, o que interessa é o serviço a ser realizado, independentemente do sistema utilizado. Nesse nível, ocorrerão o roteamento e a escolha dos melhores caminhos.

d) Transporte – Nessa camada, encontramos os mecanismos para transferência de dados fim a fim. Sua principal função é negociar o *throughtput* (taxa de transferência de dados na rede). O tamanho dos pacotes trocados pelas camadas também deve ser compatibilizado, já que diferentes camadas trabalham com pacotes de tamanhos diversos. Ainda nessa camada, os pacotes são colocados em ordem e checados para confirmar se formam a sequência completa dos dados enviados. Na camada de transporte, leva-se em conta a existência de inúmeras tarefas resultantes de diversos aplicativos em uso na rede. A camada de transporte cuida para que os dados sejam destinados à tarefa correta, ou seja, à aplicação correta.

Alternativa correta: b.

**9. A camada de enlace de dados é responsável por fornecer uma transmissão livre de erros à camada de rede. Dentre as funções apresentadas a seguir, identifique qual** não **é executada pela camada de enlace:**

a) Enquadramento.

b) Controle de erros.

~~c) Controle de congestionamento.~~

d) Controle de fluxo.

Alternativa correta: c.

**10. O modelo de referência OSI é dividido em sete camadas. Qual das camadas a seguir preocupa-se com a comunicação fim a fim?**

a) Camada física.

b) Camada enlace.

c) Camada rede.

~~d) Camada transporte (protocolos de transporte são chamados de protocolos fim a fim. Sua principal função é negociar o throughtput, taxa de transferência de dados na rede).~~

Alternativa correta: d.

**11. Assinale a camada do modelo de referência OSI responsável por funções como controle de congestionamento e encaminhamento de pacotes:**

~~a) Transporte.~~

b) Rede.

c) Sessão.

d) Apresentação.

Alternativa correta: a.

**12. Na arquitetura IEEE 802, o controle de enlace lógico (LLC) com o controle de acesso ao meio (MAC) é uma adaptação de qual camada do modelo de referência OSI?**

a) Sessão.

b) Transporte.

c) Rede.

~~d) Física.~~

e) Enlace de dados.

Alternativa correta: d.

**13. (Sanepar, 2004) No que concerne ao modelo ISO/OSI, é <u>incorreto</u> afirmar:**

a) A camada de transporte implementa um mecanismo de controle de fluxo, de forma a evitar que um host rápido possa

sobrecarregar um host mais lento.

~~b) A arquitetura descrita pelo modelo OSI é amplamente utilizada pela maioria dos protocolos de redes atuais.~~

c) Cada camada intermediária do modelo OSI, ao receber dados da camada superior, anexa um cabeçalho à informação recebida e transmite o item resultante à camada inferior.

d) Os padrões definidos para as camadas do modelo OSI são de difícil implementação e de operação ineficiente.

e) No modelo OSI, funções como controle de fluxo e detecção de erros são especificadas em mais de uma camada, o que é desnecessário.

Alternativa correta: b.

**14. Acerca do modelo OSI, definido pela ISO, avalie as seguintes afirmativas:**

I. Os protocolos da Internet foram originalmente concebidos de acordo com o modelo OSI, mas em razão de o OSI ter se tornado obsoleto, esses protocolos passaram a seguir o modelo TCP/IP.

II. O modelo OSI propõe uma pilha de protocolos, organizados em camadas hierarquicamente distribuídas, e foi criado com o propósito de padronizar protocolos de redes de computadores.

III. Os protocolos do modelo OSI somente se aplicam a redes de tecnologia local, também chamadas de LANs (*Local Area Networks*).

IV. O modelo de referência OSI é seguido por todos os protocolos de domínio público. Apenas protocolos proprietários não utilizam esse modelo.

Assinale a alternativa correta:

a) Somente as afirmativas I, II e III são verdadeiras.

b) Somente as afirmativas I e IV são verdadeiras.

c) Somente as afirmativas II e IV são verdadeiras.

~~d) Apenas a afirmativa II é verdadeira.~~

e) Apenas a afirmativa I é verdadeira.

Alternativa correta: d.

**15. (Sanepar, 2004) Relacione as camadas citadas do modelo ISO/OSI às funcionalidades correspondentes, enumerando a coluna da direita com base nas informações da esquerda:**

| | |
|---|---|
| 1. Física | ( ) Responsável pelo roteamento. |
| 2. Enlace | ( ) Responsável pela representação sintática, compressão e criptografia dos dados. |
| 3. Rede | ( ) Controla a comunicação entre duas máquinas, sincronização. |
| 4. Sessão | ( ) Especifica interfaces mecânicas e elétricas. |
| 5. Apresentação | ( ) Protocolos de controle de acesso ao meio. |

Assinale a sequência correta, de cima para baixo:

a) 5, 3, 2, 1, 4.

b) 2, 1, 4, 3, 5.

c) 3, 4, 5, 1, 2.

d) 3, 5, 2, 1, 4.

~~e) 3, 5, 4, 1, 2.~~

Alternativa correta: e.

**16. (Copel, 2010) Marque a opção que indica funções executadas pelo protocolo de camada de rede do modelo OSI:**

a) Multiplexação lógica e controle de fluxo.

~~b) Endereçamento lógico e roteamento.~~

c) Enquadramento e controle de erros.

d) Gerência de sessões de rede e autenticação.

e) Conversões de padrões e criptografia.

Alternativa correta: b.

**17. (Enade, 2008 – Computação) Uma arquitetura de rede é usualmente organizada em um conjunto de camadas e protocolos com o propósito de estruturar o hardware e o software de comunicação. Como exemplos, têm-se as arquiteturas OSI e TCP/IP. A arquitetura TCP/IP, adotada na**

**Internet, é um exemplo concreto de tecnologia de interconexão de redes e sistemas heterogêneos usada em escala global. Com relação à arquitetura TCP/IP, assinale a opção correta:**

a) A camada de interface de rede, também denominada intrarede, adota o conceito de portas para identificar os dispositivos da rede física. Cada porta é associada à interface de rede do dispositivo e os quadros enviados transportam o número das portas para identificar os dispositivos de origem e de destino.

~~b) A camada de rede, também denominada inter-rede, adota endereços IP para identificar as redes e seus dispositivos. Para interconectar redes físicas que adotam diferentes tamanhos máximos de quadros, a camada de rede adota os conceitos de fragmentação e remontagem de datagramas.~~

c) A camada de transporte é responsável pelo processo de roteamento de datagramas. Nesse processo, a camada de transporte deve selecionar os caminhos ou rotas que os datagramas devem seguir entre os dispositivos de origem e de destino, passando, assim, através das várias redes interconectadas.

d) A camada de aplicação é composta de um conjunto de protocolos, que são implementados pelos processos executados nos dispositivos. Cada protocolo de aplicação deve especificar a interface gráfica ou textual oferecida pelo respectivo processo para permitir a interação com os usuários da aplicação.

e) A arquitetura TCP/IP é uma implementação concreta da arquitetura conceitual OSI. Portanto, a arquitetura TCP/IP é também estruturada em sete camadas, que são as camadas: física, de enlace, de rede, de transporte, de sessão, de apresentação e de aplicação.

Alternativa correta: b.

**18. (Enade, 2008 – Tecnologia em Redes de Computadores) A técnica de encapsulamento utilizada em arquiteturas de redes tem como objetivo prover a abstração de protocolos e**

**serviços e promover a independência entre camadas, porque o encapsulamento esconde as informações de uma camada nos dados da camada superior.**

Analisando as afirmações anteriores, conclui-se que:

a) As duas afirmações são verdadeiras e a segunda justifica a primeira.

b) As duas afirmações são verdadeiras e a segunda não justifica a primeira.

~~c) A primeira afirmação é verdadeira e a segunda é falsa.~~

d) A primeira afirmação é falsa e a segunda é verdadeira.

e) As duas afirmações são falsas.

Alternativa correta: c.

**19. (Enade, 2008 – Tecnologia em Redes de Computadores) As atuais arquiteturas de redes de computadores são baseadas em dois conceitos fundamentais: modelo em camadas e protocolos de comunicação. Com relação a esses conceitos, qual descrição a seguir aborda de modo consistente um aspecto da relação entre camadas e protocolos?**

a) O uso de camadas em redes de computadores permite o desenvolvimento de protocolos cada vez mais abrangentes e complexos, em que cada camada adiciona, de maneira transparente, uma nova característica a um protocolo. A estruturação de várias funções no mesmo protocolo dá origem à expressão “pilha de protocolos”.

b) Os protocolos IP e TCP foram padronizados pela ISO para as camadas de rede e transporte, respectivamente. A estruturação do protocolo IP sobre o TCP dá origem à expressão “pilha de protocolos”.

c) Os protocolos atuam como um padrão de comunicação entre as interfaces das camadas de uma arquitetura de redes e se comunicam por meio da troca de unidades de dados chamadas de PDU. O uso de protocolos para a comunicação entre camadas sobrepostas dá origem à expressão “pilha de protocolos”.

d) As camadas das arquiteturas de redes de computadores foram concebidas para separar e modularizar a relação entre protocolos nas topologias lógica em barramento e física em estrela. A estruturação dos protocolos lógicos sobre os físicos dá origem à expressão “pilha de protocolos”.

~~e) As arquiteturas de redes de computadores são organizadas em camadas para obter modularidade e as funções abstratas dentro de cada camada são implementadas por protocolos. A estruturação com vários protocolos usados em camadas distintas dá origem à expressão “pilha de protocolos”.~~

Alternativa correta: e.

# Capítulo 4

**1. O padrão Ethernet foi um padrão que deu certo. Explique o porquê de todo esse sucesso.**

Seu grande sucesso se deve ao seu criador, Robert Metacalf, que, quando trabalhava na Xerox, optou por tornar sua descoberta um padrão aberto, permitindo que fosse possível a qualquer empresa desenvolver hardware e software seguindo sua especificação.

**2. Descreva os modos de transmissão simplex,** *half-duplex* **e** *full-duplex***.**

*Simplex* – Nesse modo de transmissão, somente há um transmissor e diversos receptores, como ocorre com o sinal de TV.

*Half-duplex* – Nesse modo de transmissão, há um transmissor e um receptor envolvidos na comunicação. Enquanto um está transmitindo, o outro deve ficar em modo de espera. Esse modo de operação, por ser mais barato, está presente na maioria das redes, operando a 10 ou 100 Mbps.

*Full-duplex* – Nesse modo de transmissão, há um transmissor e um receptor envolvidos na comunicação. Ambos podem transmitir e receber dados ao mesmo tempo. Dessa forma, o padrão operando nesse modo terá um desempenho duas vezes maior.

**3. Apesar de a sinalização analógica não ser utilizada para a**

**transmissão de dados entre computadores interligados em rede local, essa técnica é utilizada para a transmissão de dados entre redes fisicamente separadas. Comente o porquê da utilização da sinalização analógica nesses ambientes.**

Utiliza-se uma conexão analógica, muitas vezes, por limitação física do local ou quando as distâncias são muito grandes.

**4. O modelo de referência TCP/IP não define regras para as camadas física e de enlace. Qual é o padrão que atua nessas camadas no modelo de referência TCP/IP?**

Padrão Ethernet.

**5. (Sanepar, 2004) Em relação à tecnologia Ethernet, são feitas as seguintes proposições:**

I. No que diz respeito à topologia lógica das redes Ethernet, é possível afirmar que são redes em estrela, pois necessitam de concentradores conhecidos como hubs.

II. As taxas de transmissão para redes Ethernet eram inicialmente de 10 Mbps; com o advento do Fast Ethernet, passaram a atingir velocidades de até 100 Mbps; e com o Gigabit Ethernet, uma taxa de até 1 Gbps é possível.

III. O Ethernet faz uso do protocolo de acesso ao meio conhecido por CSMA/CD, que consiste em verificar se há portadora no meio e, caso não haja, transmitir.

IV. As redes Ethernet permitem *broadcasting*.

Com base nas afirmativas anteriores, é correto afirmar:

~~a) Somente as afirmativas I, II e III são verdadeiras.~~

b) Somente as afirmativas II e III são verdadeiras.

c) Somente as afirmativas II, III e IV são verdadeiras.

d) Somente a alternativa II é verdadeira.

e) Todas as alternativas são verdadeiras.

Alternativa correta: a.

**6. Descreva a forma de endereçamento própria da camada MAC.**

Na camada MAC, o endereçamento é controlado pelo endereço MAC Address presente na placa de rede. Esse número deve ser único dentro da rede local.

**7. As redes locais (ou LANs – *Local Area Networks*) são redes privadas que podem ter, no máximo, alguns quilômetros de extensão. São amplamente usadas para conectar computadores pessoais e estações de trabalho em escritórios e instalações industriais. Entre os padrões populares para redes locais, estão o padrão IEEE 802.3 (mais conhecido como Ethernet), o padrão IEEE 802.5 (mais conhecido como Token Ring) e o padrão IEEE 802.3u (mais conhecido como Fast Ethernet). Considere as afirmativas a seguir relativas às LANs:**

I. A rede Ethernet deve utilizar uma topologia em anel.

II. A rede Fast Ethernet utiliza uma topologia em barramento.

III. A rede Token Ring utiliza uma topologia em anel.

IV. A rede Fast Ethernet nada mais é que uma melhoria do padrão Ethernet, permitindo velocidade de até 100 Mbps.

a) Somente as afirmativas I, II e III são verdadeiras.

b) Somente as afirmativas I e IV são verdadeiras.

c) Somente as afirmativas II e III são verdadeiras.

d) Somente as afirmativas II, III e IV são verdadeiras.

~~e) Somente as afirmativas III e IV são verdadeiras.~~

Alternativa correta: e.

# Capítulo 5

**1. (Sanepar, 2004) Considere o padrão IEEE 802.3 para redes locais, mais conhecido como Ethernet. O tipo de cabeamento mais comum para esse padrão é o 10BASET, usando cabo par trançado. Dessa maneira, várias máquinas são conectadas a um hub ou switch. Qual é o alcance máximo de um cabo desse tipo?**

a) Aproximadamente 1 metro.

b) Aproximadamente 10 metros.

~~c) Aproximadamente 100 metros.~~

d) Aproximadamente 1.000 metros.

e) Não existe limite para o alcance desse tipo de cabo.

Alternativa correta: c.

**2. (Sanepar, 2004) Sobre a especificação 10BASET, é correto afirmar que:**

a) O meio de transmissão é um cabo coaxial fino de 300 ohms.

b) A maior taxa de transmissão suportada é de 100 Mbps a distâncias de até 200 metros.

~~c) No caso de a rede possuir mais de dois dispositivos conectados, o uso de repetidores multiporta (hubs) torna-se obrigatório.~~

d) O conector especificado é o BNC.

e) Para conexão ao cabo, são necessários conectores vampiros, ligados a transceivers AUI/TP.

Alternativa correta: c.

**3. Sobre o cabo coaxial, é correto afirmar:**

a) O cabo coaxial é composto de dois condutores montados um dentro do outro, um central e outro externo, ambos separados por um isolante e revestidos por uma capa plástica para isolação e proteção. Atinge 100 metros de distância e permite a ligação de redes broadband. Possui alta flexibilidade.

b) O cabo coaxial é composto de dois condutores montados um dentro do outro, um central e outro externo, ambos separados por um isolante e revestidos por uma capa plástica para isolação e proteção. Atinge 100 metros de distância e permite a ligação de redes broadband e baseband. Possui alta flexibilidade.

~~c) O cabo coaxial é composto de dois condutores montados um dentro do outro, um central e outro externo, ambos separados por um isolante e revestidos por uma capa plástica para isolação e proteção. Atinge 185 metros de distância e permite a ligação~~

~~de redes broadband e baseband. Possui baixa flexibilidade.~~

d) Atinge velocidades de até 100 Mbps em topologia linear.

Alternativa correta: c.

**4. Sobre o cabo par trançado, é correto afirmar:**

a) Basicamente existem três tipos de cabo par trançado conhecidos por UTP, FTP e STP.

b) Basicamente existem dois tipos de cabo par trançado conhecidos por UTP e STP, mas nenhum deles têm blindagem.

~~c) Basicamente existem dois tipos de cabo par trançado conhecidos por UTP e STP. Ambos possuem formas para garantir a imunidade a ruídos.~~

d) Os cabos STP são divididos em categorias, sendo a 1 e a 2 utilizadas na telefonia.

Alternativa correta: c.

**5. Sobre a técnica utilizada pelo cabo par trançado para oferecer imunidade a ruídos, é correto afirmar:**

a) Utiliza a técnica de emplacamento para garantir a imunidade a ruídos.

b) Utiliza a técnica de encapsulamento para garantir a imunidade a ruídos.

~~c) Utiliza a técnica de cancelamento para garantir a imunidade a ruídos.~~

d) Esse tipo de cabo não possui técnica para garantir a imunidade a ruídos.

Alternativa correta: c.

**6. Sobre a nomenclatura do padrão 10BASET, 10BASE2 e 100BASET, é correto afirmar que:**

a) O padrão 10BASET refere-se à velocidade de 10 Mbps, transmissão baseband, atinge, no máximo, 10 metros de distância e utiliza o cabo coaxial. O padrão 10BASE2 refere-se à velocidade de 10 Mbps, transmissão baseband e atinge até 185 metros de distância. O padrão 100BASET se refere à velocidade

de 100 Mbps, transmissão baseband, atinge, no máximo, 100 metros de distância e utiliza cabo coaxial.

b) O padrão 10BASET refere-se à velocidade de 1000 Mbps, transmissão baseband, atinge, no máximo, 10 metros de distância e utiliza o cabo par trançado. O padrão 10BASE2 refere-se à velocidade de 10 Mbps, transmissão baseband e atinge até 185 metros de distância. O padrão 100BASET refere-se à velocidade de 10 Mbps, transmissão broadband, atinge, no máximo, 100 metros de distância e utiliza cabo par trançado.

c) O padrão 10BASET refere-se à velocidade de 10 Mbps, transmissão broadband, atinge, no máximo, 100 metros de distância e utiliza o cabo par trançado. O padrão 10BASE2 refere-se à velocidade de 100 Mbps, transmissão broadband e atinge até 185 metros de distância. O padrão 100BASET refere-se à velocidade de 100 Mbps, transmissão baseband, atinge, no máximo, 100 metros de distância e utiliza cabo par trançado.

~~d) O padrão 10BASET refere-se à velocidade de 10 Mbps, transmissão baseband, atinge, no máximo, 100 metros de distância e utiliza o cabo par trançado. O padrão 10BASE2 refere-se à velocidade de 10 Mbps, transmissão baseband e atinge até 185 metros de distância. O padrão 100BASET refere-se à velocidade de 100 Mbps, transmissão baseband, atinge, no máximo, 100 metros de distância e utiliza cabo par trançado.~~

Alternativa correta: d.

**7. Sobre o processo de flooding, é correto afirmar que:**

~~a) Os hubs fazem flooding em todas as suas transmissões.~~

b) O switch faz flooding independentemente da quantidade de tempo que esteja ligado.

c) Os roteadores fazem flooding somente nos primeiros minutos depois de serem ligados.

d) O processo de flooding não é mais implementado por nenhum equipamento ativo.

Alternativa correta: a.

**8. (Sanepar, 2004) Assinale a única alternativa correta sobre cabeamento:**

~~a) A especificação 10BASE5 permite comunicação em banda básica, a uma velocidade de 10M bps, com comprimento máximo do segmento de 500 metros.~~

b) A especificação 10BASE2 faz uso de cabo par trançado, categoria 5, com conectores RJ-45 e terminadores nas extremidades do cabo.

c) A comunicação por fibra óptica faz uso de um cabo híbrido coaxial duplamente blindado com fibras de vidro, capaz de conduzir luz, definindo um canal upstream, que usa tecnologia eletrônica, e outro canal downstream, que usa tecnologia óptica.

d) A tecnologia mais popular para cabeamento e presente na maioria das redes locais é o bluetooth, nome recebido em razão do famoso cabo par trançado azul usado para conectar computadores aos hubs.

e) Os cabos par trançado categoria 5 são blindados, por isso estão imunes à interferência eletromagnética, podendo ser colocados em eletrodutos compartilhados com cabos da rede elétrica.

Alternativa correta: a.

**9. O que deve ser feito em um cabo par trançado padrão T-568A para que ele se torne um cabo *cross-over*?**

Para criar cabos *cross-over*, deve-se ligar o pino 1 da ponta A do cabo ao pino 3 da ponta B do cabo, e também o pino 2 da ponta A ao pino 6 da ponta B. Assim, do lado do computador A, o que for transmitido pelo pino 1 será recebido pelo computador B na outra ponta no pino 3.

**10. Qual é a correta sequência de cores dos fios quando for "*crimpar*" um cabo par trançado no padrão T-568A?**

1. Branco com listras verdes.
2. Verde com listras brancas.
3. Branco com listras laranjas.
4. Azul com listras brancas.

5. Branco com listras azuis.
6. Laranja com listras brancas.
7. Branco com listras marrons.
8. Marrom com listras brancas.

**11. (Copel, 2010) O sistema de cabeamento estruturado prevê que a topologia física da rede em um ambiente de cabeamento secundário (ou horizontal) será:**

a) Barramento.
b) Anel simples.
c) Anel duplo.
d) Ponto a ponto (ou *peer-to-peer*).
~~e) Estrela.~~

Alternativa correta: e.

# Capítulo 6

Os exercícios 1 a 8 se baseiam na figura 6.26:

**1. Se o computador A enviar um pedido ao computador D, que computadores também receberão esse pedido?**

a) C.
b) B, D.
c) A, D.
~~d) D.~~
e) E, F, D.

Alternativa correta: d.

**2. Se o computador G enviar um pedido para o computador C, que computadores receberão o pedido?**

a) E.
b) B, C, D.
c) A, B, C, D.
d) A, B, C.

~~e) C.~~

f) A, B, C, D, E, F.

Alternativa correta: e.

**3. Se o computador J enviar em pedido ao computador A, que computadores receberão esse pedido?**

a) I, J, A.

~~b) H, I, A.~~

c) H, I, A, B, C, D.

d) E, I, J, B.

e) J, A.

Alternativa correta: b.

**4. Se o computador F enviar um pedido ao computador E, que computadores receberão esse pedido?**

a) E, C.

b) C.

~~c) E.~~

d) A, C.

e) F, C.

Alternativa correta: c.

**5. Suponha que a máquina A transmita um quadro Ethernet *unicast* para B. Esse quadro Ethernet chegará a quais computadores da rede?**

Somente para o computador B.

**6. Suponha que a máquina A transmita um quadro Ethernet em *broadcast*. Esse quadro Ethernet chegará a quais computadores da rede?**

Para todos os computadores interligados.

**7. Suponha que a máquina A transmita um quadro Ethernet *unicast* para J. Esse quadro Ethernet chegará a quais computadores da rede?**

Para os computadores H, I e J.

**8. Suponha que a máquina A transmita um quadro Ethernet *unicast* para F. Esse quadro Ethernet chegará a quais computadores da rede?**

Somente para o computador J.

**9. No máximo, quantos centímetros de cabo devem ser descascados para realizar a crimpagem, mantendo a qualidade da conexão?**

Poder-se-á descascar, no máximo, 3 centímetros.

**10. Cite dois equipamentos ativos e descreva onde se deve utilizar cada um deles.**

- hub, para interligar computadores a impressoras dentro de uma rede local.
- Switch, para interligar departamentos de uma empresa, como marketing com contabilidade. Essas áreas poderiam ter seus computadores interligados usando um hub, entretanto isso apresentaria menos qualidade na comunicação dos dados.

**11. No modelo OSI, em qual camada o hub e o switch estão localizados?**

Camadas física e de enlace, respectivamente.

**12. Cite uma vantagem e uma desvantagem do switch.**

Vantagem: direciona os quadros diretamente a porta destino. Disponibiliza ligação em anel para garantir redundância. Desvantagem: pode apresentar alto custo quando exigir recursos avançados.

**13. Descreva o processo de flooding utilizado pelos switches.**

Um switch só fará flooding imediatamente após ter sido ligado e utiliza essa técnica até ter sua tabela que relaciona endereço MAC e porta criada.

**14. Em qual situação em uma rede deve-se utilizar um switch no nível de enlace?**

Deve-se utilizá-lo quando o objetivo é buscar desempenho na rede.

**15. Em quais situações em uma rede deve-se utilizar um**

**roteador?**

Quando há necessidade de dividir a rede em duas redes diferentes. Entenda diferente como o caso de os endereços de máscara de rede serem diversos ou começarem com números diferentes.

**16. Responda às seguintes questões sobre equipamentos ativos de rede de computadores:**

**a)** Qual equipamento filtra e encaminha pacotes entre segmentos de uma LAN, opera na camada de enlace (camada 2) e, em algumas redes, na camada de rede (camada 3) do modelo de referência TCP/IP, suportando, assim, qualquer protocolo de pacotes?

Switch atuando na camada de rede.

**b)** Qual equipamento conecta qualquer número de LANs, usa o cabeçalho e uma tabela de encaminhamento para determinar para onde os pacotes devem ser enviados, usa ICMP para se comunicar com os outros e configurar o melhor caminho entre dois hosts?

Roteador.

**c)** Qual equipamento atua como ponto de conexão comum entre dispositivos de uma rede, é comumente utilizado para conectar segmentos de uma LAN, contém múltiplas portas e, quando um pacote é recebido em uma porta, é copiado para as outras portas, de modo que todos os segmentos da LAN possam ver todos os pacotes?

hub.

**17. Temos cinco estações e um servidor em uma rede Ethernet conectados em fila via cabo coaxial. O cabo se parte entre a segunda e a terceira estação. Quantas estações perderão o acesso ao servidor? No entanto, se as cinco estações e o servidor estivessem conectados via um hub 10BASET, e o cabo par trançado entre a segunda estação e o hub se partisse, quantas estações perderiam o acesso ao servidor?**

a) Duas estações em ambos os casos.

b) Duas estações no cabo coaxial e uma estação no hub.

c) Três estações no cabo coaxial e uma estação no hub.

~~d) Cinco estações no cabo coaxial, mais o servidor e uma estação no hub.~~

Alternativa correta: d.

**18. Qual dispositivo a seguir opera na camada de rede do modelo OSI?**

~~a) Roteador.~~

b) Repetidor.

c) Comutador.

d) Ponte.

Alternativa correta: a.

**19. O TCP/IP possui um esquema de endereçamento em que é possível definir o endereço da rede e o endereço do host. É dividido normalmente em três classes básicas (A, B e C), além de uma para *multicast* (D) e outra para endereçamento especial. A respeito dos endereços do IP de classes A, B e C, julgue os seguintes itens:**

~~a) Um endereço classe A é caracterizado por ter o seu primeiro bit definido como 0.~~

b) Um endereço classe B é caracterizado por ter o seu primeiro bit definido como 1 e o segundo bit definido como 1.

c) Um endereço classe C é caracterizado por ter o seu primeiro bit definido como 1, o segundo bit definido como 0 e o terceiro como 1.

d) Um endereço classe C é caracterizado por ter o seu primeiro bit definido como 0, o segundo bit definido como 1 e o terceiro como 1.

**20. (Copel, 2010) Um switch Ethernet desempenha a seguinte função na rede:**

a) Distribui endereços IP para os hosts da rede.

~~b) Realiza a comutação de quadros na camada 2 do modelo OSI.~~

c) Realiza o encaminhamento de pacotes, processando o endereço

IP destino em função de uma tabela de rotas.

d) Gerencia conexões VoIP, fazendo a tradução de padrões quando necessário.

e) Repete todos os quadros recebidos em todas as suas interfaces.

Alternativa correta: b.

**21. Como ocorre o processo de eleição no STP?**

Primeiramente, elege-se o switch-raiz. Este será o switch com menor bridge ID.

Em segundo, elegem-se as portas-raiz. Serão as portas dos switches que compõem o loop com menor custo até a switch root. Caso o custo seja o mesmo, será escolhida a porta que recebe o menor BID do switch vizinho.

Em seguida elegem-se as portas designadas. Estas serão as portas com menor custo até o switch-raiz. Caso o custo seja o mesmo, será escolhida a porta do switch que contiver menor BID. Caso sejam iguais, a porta escolhida será a que tiver a menor identificação.

Ao final, será bloqueada uma das portas que compõem o anel. Entre duas portas designadas, a porta que estiver em um switch com maior BID ficará bloqueada.

**22. O que impacta se ajustarmos o *hellotime* para 5 segundos?**

Teremos menos BPDUs sendo trafegados pela rede. Porém, poderão ocorrer convergência caso um switch não receba o BPDU dentro do tempo definido por *maxage.*

**23. O que ocorre com um quadro quando for recebido por um switch que acabou de ser ligado?**

a) Entre em loop.

~~b) Gera inundação.~~

c) Trava a comunicação.

d) Direciona o quadro para somente um destino.

Alternativa correta: b.

**24. Qual o parâmetro utilizado pelo switch para definir o switch-**

**raiz?**

a) Bridge port.

~~b) Bridge ID.~~

c) Custo.

d) Custo e MAC do switch.

Alternativa correta: b.

# Capítulo 7

## 1. Descreva 12 comandos Hayes identificando o resultado que cada um deles causa para o modem depois de ser executado.

| Comando | Descrição | Comentários |
|---|---|---|
| A0 ou A | Responde a uma chamada. | |
| A/ | Repete o último comando. | Não anteceder com o comando AT. |
| ATD | Discar. | Disca o número a seguir e, então, negocia em modo origem.<br>P: Discagem usando o modo Pulse.<br>T: Discagem usando o modo Tom.<br>T0: Usado dentro de empresas em que é necessário digitar o 0 para obter uma linha. Espera pelo tempo especificado no registrador S8.<br>!: Equivale à tecla Flash do aparelho telefônico (interrompe a ligação por meio segundo, permitindo transferir uma chamada). |
| ATL0 | Define o nível do alto-falante para modems internos, pois os externos possuem controle manual. | Desligado ou volume baixo. |
| L1 | | Volume baixo. |
| L2 | | Volume médio. |
| L3 | | Máximo ou volume alto. |

| Comando | Descrição | Comentários |
|---|---|---|
| AT M0 ou M | Alto-falante desligado. | |
| M1 | | Alto-falante ligado. |
| M2 | | Alto-falante sempre ligado (os sons dos dados serão ouvidos depois de a conexão ser estabelecida). |
| Z0 ou Z | Reiniciar. | Reinicia para a configuração armazenada de fábrica. |

**2. Comente as transmissões síncrona e assíncrona.**

A transmissão síncrona é mais complexa e cara quando comparada com a transmissão assíncrona. Na transmissão síncrona, utiliza-se um sinal de clock para sincronizar a transmissão. A transmissão assíncrona não usa o sinal de clock; opera em circuitos menos complexos, além de ser muito mais barata. Os modems mais comuns usados em residências de forma discada utilizam a transmissão assíncrona.

# Capítulo 8

**1. Se uma sub-rede tem endereço de rede como 200.201.5.32 com máscara 255.255.255.224, qual o último endereço válido para um equipamento nessa sub-rede?**

a) 200.201.5.61.

~~b) 200.201.5.62.~~

c) 200.201.5.63.

d) 200.201.5.64.

Alternativa correta: b.

**2. Uma empresa precisa dividir uma classe C em 32 sub-redes. Quantos bits de rede deverão ser setados em 1 na máscara de sub-rede?**

a) 24.

b) 21.

~~c) 29.~~

d) 25.

e) 27.

Alternativa correta: c.

**3. O protocolo IP vem sendo amplamente utilizado há praticamente duas décadas e tem operado de forma adequada, conforme demonstra o crescimento exponencial da Internet. Porém, o IP vem se tornando uma vítima do próprio sucesso, especificamente no que se refere à escassez crescente de endereços. Acerca do roteamento CIDR, que é uma das soluções utilizadas para minimizar esse problema, identifique a alternativa correta:**

a) Uma das ideias básicas do CIDR consiste em dividir a classe E de endereços IP e alocar cada divisão para zonas geográficas distintas do mundo.

b) Em roteadores que empregam CIDR, cada entrada na tabela de roteamento é estendida com a adição de um campo de informação acerca da zona geográfica em que se encontra o ponto de destino.

~~c) A RFC 1519 descreve o conceito básico de alocação de blocos de tamanho variável de endereços de rede que ainda restam da classe C.~~

d) O conceito de máscara de sub-rede é suprimida no CIDR.

e) A operação do CIDR não pode ser aplicada para redes antigas com endereços das classes A, B e C.

Alternativa correta: c.

**4. Quantas sub-redes serão disponibilizadas se forem utilizados os 4 bits mais significativos de um endereço IP, anteriormente dedicados a equipamentos em um endereço classe C?**

a) 6.

b) 8.

c) 10.

d) 14, pois estamos desconsiderando as redes com todos os bits desligados e com todos os bits ligados.

e) 15.

Alternativa correta: d.

**5. Considerando os endereços IPv4 seguintes 200.17.53.123, 113.8.95.89 e 225.54.33.64, é correto afirmar:**

a) Trata-se de um endereço classe C, um endereço classe B e um endereço reservado para uso futuro, respectivamente.

b) Trata-se de um endereço classe C, um endereço classe A e outro endereço classe C, respectivamente.

c) Trata-se de um endereço classe C, um endereço classe A e um endereço classe D (reservado para *multicasting*), respectivamente.

d) Trata-se de um endereço classe C, um endereço sem classe e um endereço de *multicast*, respectivamente.

e) Trata-se de um endereço classe C, um endereço classe B e outro endereço classe C, respectivamente.

Alternativa correta: c.

**6. O equivalente binário de 32 bits do endereço IP 200.17.210.11 é:**

a) 11000001 00100000 11011000 00001001.

b) 11001000 00010001 11011111 00000011.

c) 11001000 00010011 00000001 00001011.

d) 11001000 00010001 11010010 00001011.

e) 11001000 00010011 11011111 00011011.

Alternativa correta: d.

**7. O que é um roteador? Qual é a sua função?**

É um equipamento ativo que interliga duas redes com endereços IP diferentes.

**8. Sobre a implementação de firewalls, considere as seguintes afirmativas:**

I. O sistema de conversão de endereços de rede pode modificar os números de porta de origem e de destino dos pacotes.

II. Em um firewall baseado em regras, é possível identificar o primeiro pacote de uma conexão UDP pelo bit SYN ativo no cabeçalho.

III. O rastreamento de conexões (*connection tracking*) é necessário apenas para manter um registro de atividade (log) das conexões. Um firewall baseado em regras poderia funcionar perfeitamente sem o rastreamento de conexões.

IV. Para liberar o tráfego para um servidor DNS na rede interna, basta abrir a porta UDP 63.

V. Uma vantagem de utilizar um proxy de aplicação é poder filtrar as requisições do usuário.

Assinale a alternativa correta:

a) Somente as afirmativas I, II e IV são verdadeiras.

b) Somente as afirmativas II, III e V são verdadeiras.

c) Somente as afirmativas I, IV e V são verdadeiras.

~~d) Somente as afirmativas I e V são verdadeiras.~~

e) Somente a afirmativa II é verdadeira.

Alternativa correta: d.

**9. Considere as seguintes afirmativas sobre firewalls:**

I. A função de um firewall é somente impedir que a rede interna seja alvo de ataques externos.

II. Uma política de segurança possível afirma que tudo que não está explicitamente permitido é proibido.

III. Um firewall deve permitir que sejam efetuadas a conversão de endereço via NAT (*Network Address Translation*) e a realização de IP Spoofing.

VI. Um firewall pode ser utilizado para evitar o sniffing dentro da rede interna.

V. Para aplicações como FTP, pode ser necessário que o firewall analise o protocolo no nível de aplicação.

Assinale a alternativa correta:

~~a) Somente as afirmativas II e V são verdadeiras.~~

b) Somente as afirmativas III e V são verdadeiras.

c) Somente as afirmativas I e II são verdadeiras.

d) Somente as afirmativas I, II e III são verdadeiras.

e) Somente as afirmativas II e IV são verdadeiras.

Alternativa correta: a.

**10. Uma empresa precisa ligar um edifício coligado que se encontra a aproximadamente 250 metros de distância da sede principal. Qual das seguintes tecnologias Ethernet permitirá essa ligação sem a necessidade de repetidores? Escolha a melhor:**

a) Cabo-padrão 10BASE2.

b) Cabo-padrão 10BASET.

~~c) Cabo-padrão 10BASEFL.~~

d) Cabo-padrão 10BASE5.

Alternativa correta: c.

**11. O que é máscara de sub-rede?**

~~a) É uma tecnologia usada para ligar o seu computador em qualquer rede.~~

b) É uma tecnologia que permite a divisão de uma classe IP em outras classes.

c) É um mecanismo de segurança que impossibilita aos outros descobrirem o seu número IP.

d) É o nome de uma tecnologia de firewalls muito sofisticada.

Alternativa correta: a.

**12. O que é classe de endereço IP?**

a) É o nível da faixa de preços do provedor a que você se conecta.

b) É o nível de serviço de um número IP (exemplo: A = universidade, B = provedor etc.).

~~c) É uma divisão dos endereços IP a fim de possibilitar redes de~~

~~diferentes tamanhos.~~

d) É uma divisão dos endereços IP por países.

Alternativa correta: c.

**13. O que é o endereço de loopback?**

a) É um endereço IP usado por seu computador para se desconectar da Internet.

b) É uma falha de projeto no modelo TCP/IP que cria um buraco na segurança das redes na Internet.

~~c) É um endereço IP em que a mensagem é mandada da origem para a origem.~~

d) É uma falha de projeto no modelo OSI que cria um buraco na segurança das redes na Internet.

Alternativa correta: c.

**14. Qual dos seguintes intervalos é uma classe C válida?**

~~a) 192.168.0.0 até 192.168.255.255.~~

b) 172.17.0.0 até 172.17.255.255.

c) 190.168.0.0 até 190.168.0.255.

d) 10.1.0.0 até 10.1.255.255.

Alternativa correta: a.

**15. Quais dos seguintes conjuntos de parâmetros TCP/IP são o mínimo necessário para que um computador possa se comunicar com a Internet?**

a) Endereço IP, gateway-padrão.

b) Endereço IP, máscara de sub-rede.

~~c) Endereço IP, máscara de sub-rede, gateway-padrão.~~

d) Endereço IP, gateway-padrão, servidor DNS primário.

Alternativa correta: c.

**16. Qual é o comando utilizado para realizar o teste de conectividade entre dois sites?**

Para realizar o teste de conectividade entre dois sites, utiliza-se o comando *ping*.

**17. Quantos bits e quantos bytes possuem o endereço IP?**

O endereço IP possui 32 bits e 4 bytes.

**18. Qual é o comando utilizado para descobrir a rota seguida por um pacote IP entre a sua casa e um endereço IP.**

Utiliza-se o comando tracert.

**19. Comente sobre endereços IP públicos e privados.**

IPs públicos são aqueles utilizados pela Internet para o roteamento dos pacotes entre roteadores.

IPs privados são aqueles que não são utilizados pela Internet para o roteamento dos pacotes entre roteadores, por exemplo o endereço iniciando com 10.x.y.z.

**20. Dados os endereços IP seguintes: 200.10.80.123 e 100.220.90.124, converta-os para o formato binário.**

200.10.80.123 – 11001000.00001010.01010000.01111011.

100.220.90.124 – 01100100.11011100.01011010.01111100.

**21. Nos servidores Windows, qual é o comando que apresenta o endereço IP e o nome do seu computador?**

Trata-se do comando Ipconfig /all.

**22. Como é composto um endereço IP?**

~~a) Identificador da rede + identificador da estação nessa rede.~~

b) 128 bits.

c) Preâmbulo mais dados.

d) Cabeçalho de dados e número da estação receptora.

Alternativa correta: a.

**23. Quais critérios devem ser avaliados para a escolha de uma classe de endereçamento IP?**

a) A região de localização.

~~b) O número de endereços IP necessários.~~

c) Depende da marca dos equipamentos.

d) Nenhuma das alternativas anteriores está correta.

Alternativa correta: b.

**24. Qual das seguintes opções descreve uma máscara de rede?**

~~a) Essa camada seta os bits que correspondem à rede para 1 e seta os bits que correspondem aos equipamentos para zero.~~

b) É uma sequência de 16 bits.

c) É utilizada para endereçar os computadores na rede.

d) Os roteadores não utilizam esse endereço.

Alternativa correta: a.

**25. No modelo de referência TCP/IP, em qual das camadas estão definidos os roteadores?**

a) Física.

b) Transporte.

c) Enlace de dados.

~~d) Redes.~~

Alternativa correta: d.

**26. O endereço IP 200.200.200.10 com a máscara 255.255.255.248 pertence a qual rede? Qual é o endereço utilizado para *broadcast*?**

Endereço IP: 200.200.200.10.

Máscara: 255.255.255.248, convertida em binário:

255.255.248.0 – 11111111.11111111.11111111.11111000 = /29.

200.200.200.10 – 11001000.11001000.11001000.00001010.

Executando a operação lógica:

& Lógico _____

Resultado 11001000.11001000.11001000.00001000

Rede – 200.200.200.8

Como a próxima rede é 200.200.200.16, o endereço de *broadcast* ficaria 200.200.200.15.

**27. Sobre os IPs reservados, é correto afirmar:**

a) O endereço 0.0.0.0 é reservado para *broadcast* na rede local.

b) O endereço 1.0.0.127 é conhecido por endereço de loopback.

c) O endereço 169.254.1.1 está na faixa de endereços da classe C.

~~d) O endereço 255.255.255.255 é reservado como endereço de *Broadcast*.~~

Alternativa correta: d.

**28. Para fazer uso do protocolo TCP/IP em um servidor Windows NT, é necessário configurar um endereço IP. Sabendo que a máscara de sub-rede do servidor deverá ser 255.255.255.224 e que a rota default, definida estaticamente, deve apontar para o roteador 200.250.10.33, indique um endereço IP válido na mesma sub-rede que permita utilizar o servidor para navegar pela Internet:**

a) 200.250.10.226.

b) 200.250.10.23.

~~c) 200.250.10.40.~~

d) 200.250.10.72.

e) 200.250.10.255.

11111111.11111111.11111111.11100000 = /27 = 224

Máscara: 255.255.255.224

Rota Default: 200.250.10.33

Endereço de rede: 200.250.10.32

Endereço da próxima rede: 200.250.10.64

Alternativa correta: c.

**29. Em relação ao protocolo ARP, quando a estação remetente deseja resolver (descobrir) o endereço físico (exemplo: Ethernet) da estação de destino a partir do endereço IP dessa última, ela envia uma mensagem de solicitação:**

~~a) Para o endereço de *broadcast* limitado 255.255.255.255. A estação destino responde ao pedido diretamente para a estação solicitante.~~

b) Diretamente para o servidor ARP, enquanto o servidor ARP responde ao pedido diretamente para a estação solicitante.

c) Para o endereço de *broadcast* limitado 255.255.255.255. O servidor ARP responde ao pedido diretamente para a estação solicitante.

d) Diretamente para o servidor ARP. O servidor ARP responde ao pedido para o endereço de *broadcast* limitado 255.255.255.255.

e) Para o endereço de *broadcast* limitado 255.255.255.255. A estação destino responde ao pedido também para o endereço de *broadcast* limitado 255.255.255.255.

**30. Considere o endereço de sub-rede IP 15.0.96.0/19. A alternativa que indica, respectivamente, a máscara de rede dessa sub-rede, o número de estações que essa sub-rede pode endereçar e o seu endereço de *broadcast* é:**

a) 255.255.240.0, 8190, 15.0.127.255.

~~b) 255.255.224.0, 8192, 15.0.96.255.~~

c) 255.255.240.0, 8192, 255.255.255.255.

d) 255.255.224.0, 8190, 15.0.96.255.

e) 255.255.224.0, 8190, 15.0.127.255.

11111111.11111111.11100000.00000000 = /19

Máscara: 255.255.224.0

Número de estações igual a 2 elevado a 13 = 8192.

Alternativa correta: b.

**31. Se uma rede usa a máscara 255.255.255.224, o endereço da sub-rede a que pertence o endereço IP 195.40.13.131 é?**

11111111.11111111.11111111.11100000 = /27

195. 40. 13. 10000011

_____

195. 40. 13. 10000000 = 128.

Rede 195.40.13.128

**32. (Copel, 2010) Uma máscara de rede 255.255.255.248 foi aplicada sobre o endereço 200.1.1.0/24. Essa operação criará:**

a) 248 novos endereços de rede.

b) 3 novos endereços de rede.

c) Em cada nova rede criada, 254 endereços para hosts.

d) Em cada nova rede criada, 14 endereços para hosts.

~~e) Em cada nova rede criada, 6 endereços para hosts.~~

Alternativa correta: e.

**33. (Copel, 2010) O protocolo IP é um dos protocolos mais utilizados atualmente. Indique a alternativa correta:**

a) O protocolo IP é um protocolo baseado em conexão.

~~b) O protocolo IP é baseado em datagrama não confiável.~~

c) O protocolo IP realiza o controle de erros.

d) O protocolo IP realiza o controle de fluxo.

e) O protocolo IP envia pacotes de tamanho fixo.

**34. (UFT, 2005) Na tecnologia Internet, o elemento principal de endereçamento, identificador de uma máquina conectada à rede, é:**

a) TCP.

b) UDP.

c) IPX.

~~d) IP.~~

e) SPX.

Alternativa correta: d.

# Capítulo 9

**1. (Sanepar, 2004) Avalie as proposições a seguir sobre o roteamento IP:**

I. RIP, OSPF e IGRP são protocolos para roteamento interno também conhecidos como IGPs (*Internal Gateway Protocol*) e permitem o roteamento dentro de um mesmo SA (Sistema Autônomo).

II. O protocolo RIP (*Routing Information Protocol*), incluído em distribuições do Unix como routed, é baseado no algoritmo de

distâncias vetoriais, no qual, a partir dos *hosts* adjacentes, são trocadas as tabelas de roteamento.

III. O OSPF (*Open Shortest Path First*) é um protocolo proprietário da Cisco, que executa o roteamento entre diferentes SAs, sendo usado pelos chamados roteadores de borda.

IV. O roteamento entre diferentes SAs pode ser realizado pelo protocolo BGP (*Border Gateway Protocol*).

Assinale a alternativa correta:

a) Somente as proposições I, II e III são verdadeiras.

b) Somente as proposições III e IV são verdadeiras.

c) Somente as proposições I e II são verdadeiras.

~~d) Somente as proposições I, II e IV são verdadeiras.~~

e) Todas as proposições são verdadeiras.

Alternativa correta: d.

**2. Os protocolos de roteamento mais comuns são:**

~~a) O RIP (*Routing Information Protocol*), que determina a rota mais eficiente para os dados e calcula o número de hops para a rota.~~

b) O EGP (*Exterior Gateway Protocol*) é usado quando vários roteadores têm de ser interconectados antes de chegar ao seu destino final.

c) O RIP permite caminho com contagem de hops superior a 16.

d) Roteamento estático, que deve ser utilizado quando existem diversas rotas para cada destino.

Alternativa correta: a.

**3. O protocolo que utiliza a característica de estado de link é:**

a) RIP.

~~b) OSPF.~~

c) IGRP.

d) ICMP.

Alternativa correta: b.

**4. Todos protocolos que seguem são protocolos de roteamento,**

exceto**:**

a) RIP.

b) OSPF.

c) IGRP.

~~d) SMTP.~~

Alternativa correta: d.

**5. (Sanepar, 2004) A tabela 9.24 de roteamento RIP foi obtida a partir de um roteador Unix, por meio do comando** netstat –rn**.**

*Tabela 9.24 – Resultado do comando netstat -rn*

| Destination | Gateway | Flags | Iface |
|---|---|---|---|
| 127.0.0.1 | 127.0.0.1 | UH | lo0 |
| 200.17.212. | 200.17.212.5 | U | eth0 |
| 200.17.210. | 200.17.210.6 | U | eth1 |
| 200.19.138. | 200.19.138.1 | U | eth2 |
| default | 200.17.212.161 | UG | |

Com base nos dados dessa tabela, é incorreto afirmar:

a) Os endereços das interfaces eth0, eth1 e eth2 podem ser, respectivamente, 200.17.212.5, 200.17.210.6 e 200.19.138.1.

b) O roteador está conectado a três redes, por meio das interfaces eth0, eth1 e eth2.

c) A primeira linha corresponde à interface de loopback, que significa: quando um datagrama é enviado para essa interface, o protocolo retorna os dados sem enviá-los por rede.

d) Será enviado ao roteador 200.17.212.161 qualquer datagrama IP que não estiver destinado a (pelo menos) uma das redes listadas explicitamente na tabela de roteamento

~~e) O roteador Unix de onde a tabela 9.24 foi extraída está endereçado na rede como 127.0.0.1.~~

Alternativa correta: e.

# Capítulo 10

**1. Sobre o protocolo TCP, é incorreto afirmar que:**

a) Os endereços IP identificam tanto um host como uma rede. Para isso, os bits mais significativos identificam a rede e os menos significativos, o host.

b) O ICMP (*Internet Control Message Protocol*) fornece um serviço de mensagens de controle sobre a camada de rede. Essas mensagens podem relatar erros e solicitar ou responder a pedidos de eco (o comando *ping* é uma solicitação de eco do ICMP).

c) O protocolo UDP não estabelece conexões, sendo utilizado em aplicações como DNS, SNMP e FTP.

d) Para controle de erros, o TCP faz uso de um algoritmo chamado janelas deslizantes.

~~e) O protocolo TCP estabelece conexões por meio de um procedimento chamado aperto de mão de três vias ou three way handshake.~~

Alternativa correta: e.

**2. Sobre os protocolos de transporte do TCP/IP, é correto afirmar:**

a) Por ser desprovido de algoritmos de controle de fluxo e congestionamento, o protocolo UDP mostrou-se inadequado para aplicações de tempo real, como streaming media, por exemplo.

b) Por ser um protocolo não orientado à conexão e sem garantia de entrega, o UDP não é empregado em aplicações da Internet, sendo de interesse restrito ao uso acadêmico.

~~c) O protocolo TCP é orientado à conexão, possui algoritmos de controle de fluxo e congestionamento e garante a entrega dos dados sem atrasos.~~

d) Para estabelecer uma conexão UDP, cliente e servidor trocam sinais de controle em um processo conhecido como aperto de mão (*handshake*).

e) O protocolo TCP é orientado à conexão, por isso garante

controle de fluxo, controle de sequência e controle de erros.

Alternativa correta: c.

**3. (Sanepar, 2004) Analise as seguintes proposições sobre a arquitetura TCP/IP:**

I. Os protocolos de transporte da arquitetura TCP/IP possuem dois tipos de serviço: serviço confiável e orientado à conexão, fornecido pelo TCP; e serviço não confiável e não orientado à conexão, oferecido pelo UDP.

II. O TCP possui algoritmos de controle de fluxo e congestionamento, bem como detecção e correção de erros e garantia de entrega dos dados sem atrasos.

III. Justamente por não possuir algoritmos de controle de fluxo e congestionamento, o UDP é ideal para aplicações de streaming media.

IV. Aplicações como HTTP, FTP, correio eletrônico e terminal virtual (*Telnet*) são suportados pelo protocolo TCP.

Assinale a alternativa correta:

a) Somente as proposições I, II e III são verdadeiras.

~~b) Somente as proposições I, III e IV são verdadeiras.~~

c) Somente as proposições I, II e IV são verdadeiras.

d) Somente as proposições I e IV são verdadeiras.

e) Todas as proposições são verdadeiras.

Alternativa correta: b.

**4. (Copel, 2010) O protocolo TCP (*Transmission Control Protocol*) é um dos protocolos que podem ser utilizados na camada de transporte do conjunto de protocolos inter-rede (TCP/IP). Sobre o TCP, é incorreto afirmar que:**

a) O protocolo TCP realiza controle de erros fim a fim.

b) O protocolo TCP colabora no controle de congestionamento da rede, reduzindo a taxa de transmissão em caso de erros.

c) O protocolo TCP estabelece um estado de conexão entre cliente e servidor.

~~d) O protocolo TCP implementa qualidade de serviço fim a fim.~~

e) O protocolo TCP implementa o controle de fluxo fim a fim.

Alternativa correta: d.

# Capítulo 11

**1. Em relação ao serviço de nomes (DNS), assinale a alternativa incorreta:**

~~a) O DNS é um esquema de gerenciamento de nomes hierárquico e centralizado, cuja autoridade central é a zona ".".~~

b) O DNS define a sintaxe dos nomes usados na Internet, as regras para delegação de autoridade na definição de nomes, um banco de dados que associa nomes a atributos e um algoritmo para mapear nomes em endereços.

c) Um servidor secundário é uma espécie de cópia de segurança do servidor primário. Quando não é possível encontrar um domínio por meio do servidor primário, o sistema tenta resolver o nome por meio do servidor secundário.

d) Cada administrador de zona que contém dados decide um tempo de vida (TTL) para os dados. Um TTL pequeno garante a consistência, enquanto um TTL grande diminui o tempo que se leva até conseguir determinada informação.

e) Um registro SOA marca o começo de uma zona, um grupo de registros de recursos localizados no mesmo lugar dentro do espaço de nomes do DNS.

Alternativa correta: a.

# Capítulo 12

**1. Quais os tipos de NAT?**

É possível utilizar três formas de tradução de endereços IP: NAT dinâmico, NAT estático e PAT (*Port Address Translation*).

**2. Comente o servidor NAT dinâmico.**

O NAT dinâmico é muito utilizado para permitir que a máquina de

uma rede Intranet com endereço privado tenha acesso à Internet normalmente, como se estivesse utilizando um endereço público.

**3. Comente o servidor NAT estático.**

Como o nome indica, um NAT estático utiliza um endereço fixo para a tradução de uma máquina da rede local para a rede Internet. Esse tipo de NAT é muito utilizado quando se quer ocultar o endereço IP interno de uma máquina para o acesso externo via Internet e, ao mesmo tempo, torná-la visível para a rede mundial.

**4. Comente o PAT.**

O PAT (*Port Address Translation*) é um tipo de NAT que utiliza um único endereço IP como endereço público para conversão. Para atender a diferentes clientes com um único endereço público, o PAT utiliza as portas da camada de transporte para saber devolver as requisições aos clientes corretos.

**5. (Copel, 2010) Para realizar configurações de endereçamento IP prevendo o uso do NAT (*Network Address Translation*), deve ser utilizado um endereço de rede que foi previamente reservado para uso privativo. A alternativa que indica um endereço de rede IP reservado para uso privativo, de acordo com a RFC1918, é dada por:**

a) 0.0.0.0 com máscara 0.0.0.0.

b) 255.255.255.255 com máscara 255.255.255.255.

~~c) 10.0.0.0 com máscara 255.0.0.0.~~

d) 192.168.1.0 com máscara 255.255.255.0.

e) 127.0.0.0 com máscara 255.0.0.0.

Alternativa correta: c.

# Capítulo 14

**1. (Sanepar, 2004) Sobre o POP (*Post Office Protocol*), assinale a alternativa** incorreta:

a) As mensagens encaminhadas por servidores SMTP são armazenadas em servidores de mensagens eletrônicas por meio

do POP.

b) O POP utiliza a porta-padrão 110 e opera usando o protocolo TCP.

c) O POP permite o modo de operação offline, no qual um cliente de correio eletrônico solicita ao servidor POP o pacote de novas mensagens, que são, então, transferidas ao programa cliente; em seguida, as mensagens são apagadas do servidor. Nesse modo, todo o processamento de mensagens ocorre no computador que executa o cliente de correio eletrônico.

d) O uso do POP é indicado quando os usuários são estáticos, ou seja, cada um possui seu computador e só acessa seu correio eletrônico a partir dele.

~~e) O POP permite que diversas pastas sejam mantidas no servidor, auxiliando na organização da mensagens.~~

Alternativa correta: e.

**2. Avalie as afirmativas a seguir com base no texto que representa a manipulação de um servidor SMTP com uma interface de linha de comando (os números de linha foram inseridos para referência).**

```
1  $telnet smtp1.localhost 25
2  220 mail.localhost SMTP
3  helo mail.localhost
4  250 mail.localhost
5  mail from:<teste@teste.com.br>
6  250 Ok
7  rcpt to:<teste2@outrodominio.com.br>
8  250 Ok
9  data
10 Apenas um teste ... até mais!
12 .
13 250 Mail queued for delivery
14 quit
15 221 Closing connection Good bye
```

I. O SMTP utiliza por padrão a porta 25 e opera usando o protocolo UDP.

II. O SMTP é constituído de duas partes: a origem e o destino, e

cada uma delas possui acesso a um servidor de armazenamento. Quando a origem envia uma mensagem para o destino, essa mensagem é primeiramente armazenada no servidor de armazenamento da origem, que tenta enviar as mensagens e, se ocorrer algum problema com o destino, tentará posteriormente reenviar a mensagem. Se não conseguir, a mensagem será enviada de volta à origem ou ao post*master*.

III. A linha 12 indica que o corpo da mensagem eletrônica é finalizado.

IV. As linhas 5 e 7 fazem parte do cabeçalho da mensagem, enquanto a linha 10 faz parte do corpo da mensagem.

Assinale a alternativa correta:

a) Somente as afirmativas I e II são verdadeiras.

b) Somente as afirmativas I, III e IV são verdadeiras.

c) Somente as afirmativas II e III são verdadeiras.

~~d) Somente as afirmativas II, III e IV são verdadeiras.~~

e) Somente as afirmativas III e IV são verdadeiras.

Alternativa correta: d.

**3. (Sanepar) Sobre os protocolos utilizados para o envio e recebimento de correio eletrônico (email) na Internet, considere as seguintes afirmativas:**

I. O protocolo SMTP (*Send Mail Transfer Protocol*) é utilizado para enviar correio eletrônico; é um protocolo baseado em codificação ASCII.

II. O POP3 (*Post Office Protocol*) é o protocolo utilizado pelos clientes de correio eletrônico para transferir as mensagens do servidor para máquina local.

III. No protocolo POP3, é possível ler mensagens diretamente do servidor de correio eletrônico, sem fazer sua transferência para máquina local.

IV. As portas do protocolo POP3 e SMTP são, respectivamente, 110 e 25.

V. Os protocolo SMTP e POP3 são capazes de transmitir outras informações, além de texto, como arquivos anexados, sem qualquer tipo de codificação especial.

Assinale a alternativa correta:

a) Somente a afirmativa II é verdadeira.

b) Somente as afirmativas III e IV são verdadeiras.

~~c) Somente as afirmativas I, II e IV são verdadeiras.~~

d) Somente a afirmativa V é verdadeira.

e) Todas as afirmativas são verdadeiras.

Alternativa correta: c.

**4. Sobre o POP (*Post Office Protocol*), assinale a alternativa incorreta:**

a) As mensagens encaminhadas por servidores SMTP são armazenadas em servidores de mensagens eletrônicas por meio do POP.

b) O POP utiliza a porta-padrão 110 e opera usando o protocolo TCP.

c) O POP permite o modo de operação offline, no qual um cliente de correio eletrônico solicita ao servidor POP o pacote de novas mensagens, que são, então, transferidas ao programa cliente; em seguida, as mensagens são apagadas do servidor. Nesse modo, todo o processamento de mensagens ocorre no computador que executa o cliente de correio eletrônico.

d) O uso do POP é indicado quando os usuários são estáticos, ou seja, cada um possui seu computador e só acessa seu correio eletrônico a partir dele.

~~e) O POP permite que diversas pastas sejam mantidas no servidor, auxiliando na organização das mensagens.~~

Alternativa correta: e.

**5. Sobre os serviços de rede, considere as seguintes afirmações:**

I. A porta-padrão do protocolo HTTP na Internet é 8080 e o

protocolo de transporte, TCP (errada, pois o certo seria 80).

II. Em caso de falha do DNS, é possível acessar uma máquina na rede local, desde que se conheça seu endereço IP.

III. O DNS é o serviço responsável por transformar o nome de uma máquina (host) em um endereço IP.

IV. O DNS não é utilizado para transformar o endereço IP em um nome de uma máquina (errada, pois o DNS converte um nome de uma máquina em endereço IP).

Assinale a alternativa correta:

~~a) Somente as afirmativas II e III são verdadeiras.~~

b) Somente as afirmativas I e IV são verdadeiras.

c) Somente as afirmativas I, II e III são verdadeiras

d) Somente as afirmativas II e IV são verdadeiras.

e) Somente a afirmativa IV é verdadeira.

Alternativa correta: a.

**6. (Sanepar, 2004 ) O SMTP (***Simple Mail Transport Protocol***) é um protocolo do TCP/IP para envio de mensagens eletrônicas. Sobre o SMTP, assinale a alternativa** incorreta**:**

~~a) Diz-se que quando um servidor SMTP processa uma mensagem eletrônica, está com repasse (relay) fechado, pois nem o remetente nem o destinatário são usuários do servidor em questão.~~

b) Servidores SMTP com repasse constituem uma ameaça na rede, pois são geralmente explorados por spammers.

c) Um servidor SMTP pode utilizar blackhole lists para implementar filtros e assim rejeitar mensagens eletrônicas não solicitadas.

d) O SMTP, ao ser projetado, não tinha a finalidade de garantir a autenticidade de um remetente de uma mensagem eletrônica.

e) É possível fazer uso direto do SMTP por meio da execução do comando Telnet para a porta 25 de um servidor SMTP em questão.

Alternativa correta: a.

**7. (Copel, 2010) O DHCP (***Dynamic Host Configuration Protocol***) é um**

**protocolo que permite:**

a) Resolução de nomes em endereços IP e vice-versa.

b) Ligação entre endereços IP e seu endereço de hardware correspondente.

~~c) Configuração dinâmica de terminais, com concessão de endereços IP de host e outros parâmetros de configuração para clientes de rede.~~

d) Gerência de configuração para elementos de rede, permitindo o acesso remoto em interfaces de emulação de terminal.

e) Gerência dinâmica de hosts em redes de gerência de configuração.

Alternativa correta: c.

**8. (Copel, 2010) Suponha que um servidor de nomes (protocolo DNS) responsável pelo domínio "***copel.com.br***" recebeu uma solicitação para resolver o nome "***www.pucpr.br***". Sabendo que o servidor de nomes não tem informações em cache, qual será o primeiro passo para resolução do nome?**

a) Buscar na base de dados e responder com o endereço IP cadastrado.

~~b) Consultar o servidor raiz para descobrir o endereço do servidor responsável pelo domínio "br".~~

c) Consultar o servidor "br" para descobrir o endereço do servidor responsável pelo domínio "*pucpr.br*".

d) Consultar o arquivo host para determinar o endereço do servidor de nomes da rede.

e) Encaminhar a requisição diretamente para o servidor responsável pelo domínio "*pucpr.br*".

Alternativa correta: b.

**9. (Copel 2010) O protocolo HTTP (***Hyper Text Transfer Protocol***) possui as seguintes características,** <u>exceto</u>**:**

a) Realiza a transferência de arquivos a partir da mensagem GET.

b) O HTTP versão 1.1 pode manter a conexão TCP aberta e

transferir diversos arquivos.

~~c) Realiza o controle da sessão, controlando autenticações de usuário.~~

d) O protocolo pode transferir qualquer tipo de arquivo.

e) O protocolo HTTP permite a implementação de transferência de correio eletrônico, podendo substituir o protocolo SMTP (*Simple Mail Transfer Protocol*).

Alternativa correta: c.

**10. (TRT) É um serviço muito utilizado em ambiente Internet, tendo como porta-padrão de funcionamento a TCP 80:**

a) DNS.

b) FTP.

c) TELNET.

~~d) HTTP.~~

e) GHOST.

Alternativa correta: d.

**11. (TRT) Os softwares de correio eletrônico normalmente utilizam para entrada e saída de emails, respectivamente, os servidores:**

a) POP3 + HTTP.

~~b) POP3 + SMTP.~~

c) SMTP + POP3.

d) SMTP + HTTP.

e) HTTP + POP3.

Alternativa correta: b.

# Capítulo 15

**1. Descreva as vantagens oferecidas pelo protocolo IPv6 em relação ao protocolo IPv4.**

O IPv6 tem como principal vantagem a expansão dos endereços IPs, hoje considerados escassos para o acesso à Internet, ou seja,

com o crescimento exponencial da Internet, em poucos anos, não teremos mais endereços IPs livres.

Para se ter uma ideia, o protocolo IP disponível é referenciado por 32 bits, enquanto o seu sucessor (IPv6) disponibilizará um endereço IP com 128 bits, ou seja, quatro vezes maior em quantidade de bits e muito maior em quantidade de endereços. Com o IPv6, teremos 2 elevado a 64 possíveis endereços IPs.

**2. Qual é a diferença entre um endereço *multicast* e um *broadcast*?**

O endereço *multicast* é um tipo de endereçamento do IPv6 que possui a mesma característica dos endereços IPv4 pertencentes à classe D. Um pacote destinado a um endereço *multicast* é entregue a todas as interfaces que fazem parte do grupo de endereços ao mesmo tempo, assim como ocorre nas transmissões do tipo *broadcast*.

A diferença existente entre o *multicast* e o *broadcast* é que uma transmissão em *multicast* atinge o seu destino onde ele estiver; uma transmissão em *broadcast*, por sua vez, atinge somente computadores em uma rede local.

**3. A versão do protocolo IP mais utilizada é o IPv4. A nova versão tem como objetivo:**

a) O aumento do tamanho dos pacotes transportados pela rede.

b) O aumento da quantidade de pacotes transportados pela rede.

c) O aumento do tipo e variedade dos pacotes transportados na rede.

~~d) A necessidade do aumento da capacidade de endereçamento.~~

Alternativa correta: d.

**4. Quantos bits formam cada uma das oito partes de um endereço IPv6?**

a) 24.

b) 4.

c) 3.

d) 16.

Alternativa correta: d. O formato do endereço IPv6 é X:X:X:X:X:X:X:X, em que X é um campo hexadecimal de 16 bits. Por exemplo: 110A:0192:190F:0000:0000:082C:875A:132C.

**5. O protocolo IPv6 permite encapsular pacotes IPv6 dentro de pacote IPv4. Esse mecanismo é chamado de:**

a) Tunneling.

b) Hashing.

c) Routing.

d) Nat.

Alternativa correta: a.

**6. O protocolo IPv6 foi designado para substituir o protocolo IPv4. Isso ocorreu por os endereços IPv4 estarem se esgotando. Qual das seguintes sentenças é verdadeira em relação ao protocolo IPv6?**

a) A estrutura de endereções não é hierárquica.

b) Pacotes de *broadcasts* foram eliminados e substituídos pelos pacotes de *multicast*.

c) Existem 3,4 bilhões de endereço IPv disponíveis.

d) Uma interface poderá apenas ser configurada com um endreço IPv6.

Alternativa correta: b.

**7. Quais das declarações são verdadeiras sobre a representação de um endereço IPv6? (escolha duas)**

a) Os primeiros 64 bits são formados pelo método EUI-64.

b) Uma única interface de um equipamento IPv6 pode receber mais de um endereço IP.

c) Os últimos 64 bits podem ser formados pelo método EUI-64.

d) Um endereço IPv6 somente utiliza caracteres decimais.

Alternativas corretas: b e c.

**8. Marque as opções que são mecanismos de transição IPv6: (escolha três)**

a) Túnel 6to4.

b) Túnel GREEN.

c) Túnel ISATAP.

d) Túnel 6rd.

e) Túnel VPN.

f) Túnel PPP.

Alternativas corretas: a, c e d.

**9. Qual das opções são corretas em relação a um endereço *unicast*? (escolha duas)**

a) Endereço *unicast* global inicia com 2000::/3.

b) Endereço link-local inicia com FAB0::/10.

c) Endereço link-local inicia com FE00:/12.

d) Endereço de loopback é igual a ::1.

Alternativas corretas: a e d.

**10. Selecione endereços IPv6 válidos:**

a) ::192:168:0:1.

b) 2002:c0a8:101::42.

c) 2003:dead:baaf:4dad:23:46:bb:101.

d) ::1.

e) 2000::

f) 2001:3452:4952:2837::1.

Alternativas corretas: a, b, c, d e f.

**11. Qual o endereço *multicast* processado somente pelos roteadores muticast?**

a) FF02::4.

b) FF02::3.

c) FF02::2.

d) FF02::1.

Alternativa correta: c.

**12. Qual é o endereço IP *multicast* utilizado pelo protocolo RIP**

**para divulgar suas rotas?**

Resposta: FF02::9.

# Capítulo 16

**1. Qual é o significado do termo *wireless*?**

Redes sem fio.

**2. Em quais topologias as redes sem fio operam?**

As redes sem fio operam em Ad-hoc e cliente/servidor.

**3. Cite as diferenças entre o CSMA/CD e o CSMA/CA.**

O protocolo CSMA/CA (*Carrier Sense Multiple Access/Collision Avoidance*) foi projetado para reduzir a probabilidade de colisões em uma rede sem fio, composta de múltiplas estações. O CSMA/CD é utilizado para reduzir colisões em redes Ethernet utilizando cabos.

**4. Em qual camada do modelo de referência OSI o padrão 802.11 opera?**

Esse padrão opera na camada física.

**5. Descreva o padrão 802.11a.**

O padrão 802.11a foi desenvolvido pelo IEEE após o padrão 802.11b e é, em média, cinco vezes mais rápido que o padrão 802.11b, chegando a transmitir dados a 54 Mbps. Ademais, opera na frequência de 5.8 GHz e utiliza a técnica OFDM (*Orthogonal Frequency Division Multiplexing*), disponibilizando até oito canais por ponto de acesso, o que possibilita maiores taxas de transmissão para uma quantidade maior de usuários simultâneos.

**6. Descreva o padrão 802.11b.**

O padrão 802.11b foi o primeiro desenvolvido pelo IEEE especificamente para redes Ethernet sem fio. Foi criado a fim de atender às necessidades e às expectativas das empresas. Pode operar tanto na topologia ad-hoc, na qual os computadores trocam dados diretamente entre si, quanto na topologia cliente/servidor, na qual todo o tráfego da rede passa pelo ponto de acesso sem fio.

**7. Qual é a diferença entre o padrão 802.11a e o padrão**

**802.11b?**

A tabela a seguir representa a diferença entre as tecnologias:

| Padrões | 802.11a | 802.11b |
|---|---|---|
| Taxa máxima de transmissão | 54 Mbps | 11 Mbps |
| Taxa de transmissão | 20 Mbps | 5 Mbps |
| Banda | 5.8 GHz | 2.4 GHz |
| Canais | 8 | 3 |

**8. Descreva o padrão 802.11g.**

Recentemente, o IEEE publicou o padrão 802.11g, que tem o objetivo de combinar o melhor dos padrões 802.11a e 802.11b, transmitindo dados a 54 Mbps e utilizando a frequência de 2,4 GHz. Essa frequência é liberada, não sendo necessário pedir licença à Anatel para ser utilizada. O padrão 802.11g é totalmente compatível com o padrão 802.11b, ou seja, pontos de acesso 802.11g podem transmitir dados de placas de rede-padrão 802.11b.

**9. Descreva o padrão 802.11e.**

O padrão 802.11e foi desenvolvido com o objetivo de melhorar a qualidade do serviço (QoS) em ligações telefônicas, transmissão de vídeo de alta resolução e outras aplicações multimídia. Com esse padrão, será possível que certos tipos de tráfego em redes sem fio sejam prioritários em relação a outros. Assim, uma rede sem fio poderá garantir que ligações em telefones IP e conteúdo multimídia sejam devidamente acessados tanto em redes sem fio como em redes cabeadas.

**10. Descreva o padrão 802.11i.**

A especificação de segurança 802.11i é baseada no padrão de encriptação avançada (AES) que suporta chaves de criptografia de 128, 192 e 256 bits. Esse padrão tem como objetivo resolver o problema de segurança existente atualmente nas redes sem fio. O atual padrão de segurança utilizado nas redes sem fio, conhecido

por WEP (*Wired Equivalent Privacy*), utiliza técnicas simples de criptografia, não garantindo privacidade na transmissão de dados nesse meio.

**11. Descreva o padrão de segurança WEP.**

O atual padrão de segurança utilizada nas redes sem fio conhecido por WEP (*Wired Equivalent Privacy*) utiliza técnicas simples de criptografia, não garantindo privacidade na transmissão de dados nesse meio. Esse padrão foi disponibilizado na tentativa de oferecer segurança na autenticação, proteção e confiabilidade na comunicação entre dispositivos sem fio, porém é inseguro devido à sua arquitetura.

**12. O padrão bluetooth opera em qual topologia?**

O bluetooth opera na topologia ad-hoc em frequências de 2,4 GHz (mesma do 802.11b e 802.11g), que possibilitam a transmissão de dados em curtas distâncias entre telefones sem fio, celulares, impressoras, PDAs, notebooks, fax, teclados, joysticks, ou seja, qualquer aparelho digital que use um chip bluetooth.

**13. Descreva as redes piconet e scatternet.**

Uma piconet é uma pequena rede pessoal conhecida por PAN (*Personal Area Network*). Na piconet, um dos equipamentos interligados recebe a função de mestre e os demais recebem a função de escravos. O mestre é responsável por controlar as comunicações entre o mestre e os escravos e também as transferências de dados entre os equipamentos escravos, afinal, uma rede ad-hoc permite a comunicação sem a presença de um ponto central. Uma rede piconet é formada por, no máximo, oito equipamentos, todos interconectados entre si. Quando duas ou mais piconets são interligadas, formamos uma scatternet.

Uma scatternet pode conter até oitenta equipamentos, sendo esse o limite para que a rede funcione bem. É importante observar que uma piconet tem a capacidade de se conectar tanto a uma rede cabeada quanto à Internet.

**14. Para o transporte de voz entre equipamentos bluetooth, quantos canais podem ser utilizados e em qual taxa de**

**transmissão?**

Os equipamentos que seguem o padrão bluetooth 1.0 transmitem dados a 1 Mbps e, para a transmissão de voz, a especificação determina três canais síncronos de 64 Kbps cada um. A nova versão do padrão bluetooth (versão 1.1) permitirá a comunicação entre equipamentos a 100 metros, utilizando um rádio com uma frequência maior.

# Capítulo 17

**1. Descreva as vantagens de uma rede GPON.**

Baixo custo de instalação e manutenção

**2. Qual é a função do T-CONT?**

Relacionar o DBA profile com o GEM port ID.

**3. Qual é a função do algoritmo DBA?**

Garantir que a comunicação entre o OLT e as ONUs seja otimizada.

**4. Quais os equipamentos que são utilizados em uma rede GPON?**

Para o funcionamento de uma rede GPON, utilizamos o OLT, instalado em um ponto central, o *splitter* e a ONU instalada no endereço do cliente.

# Capítulo 18

**1. Descreva as caraterísticas do protocolo BGP.**

O protocolo BGP é baseado no algoritmo *path vector* (vetor de caminho).

As tabelas de roteamento completas são trocadas entre roteadores peers após a sessão BGP ser estabelecida (estado *established*).

Utiliza a porta 179 do protocolo TCP.

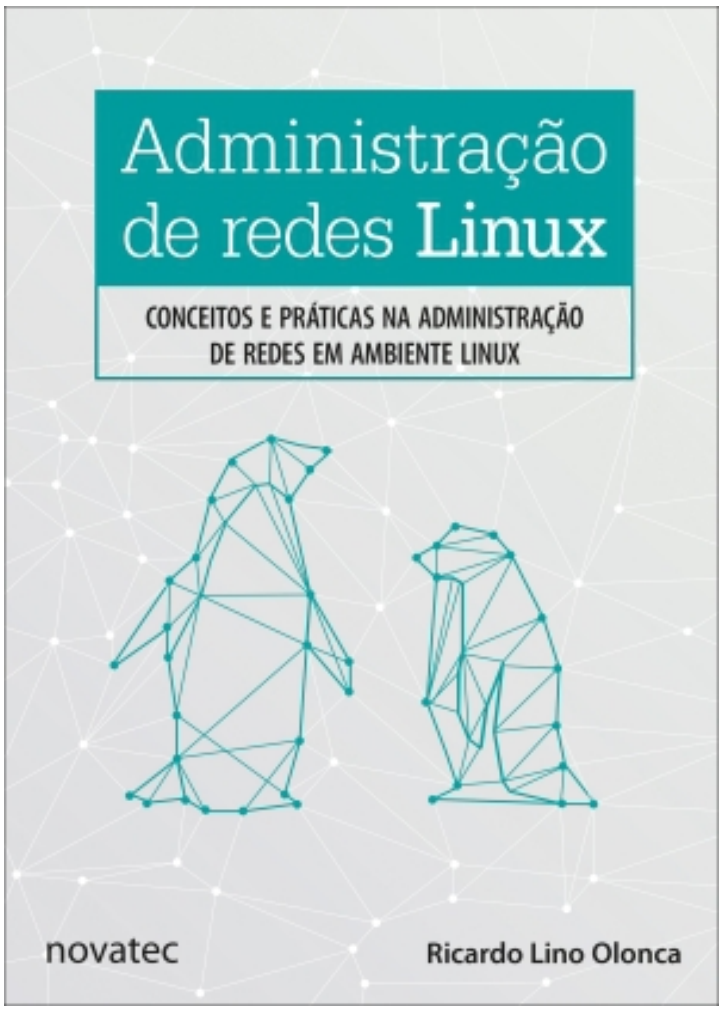
O protocolo BGP percebe a Internet como uma coleção de sistemas autônomos.

**2. Qual é a diferença entre protocolos classificados como IGP e**

**EGP?**

Os protocolos IGP atuam como protocolos de roteamento entre os roteadores internos ao AS. Como exemplos, temos RIP, OSPF e Is-IS.

Os protocolos EGP atuam como protocolo de roteamento entre sistemas autônomos (AS). Como exemplo, temos o BGP.



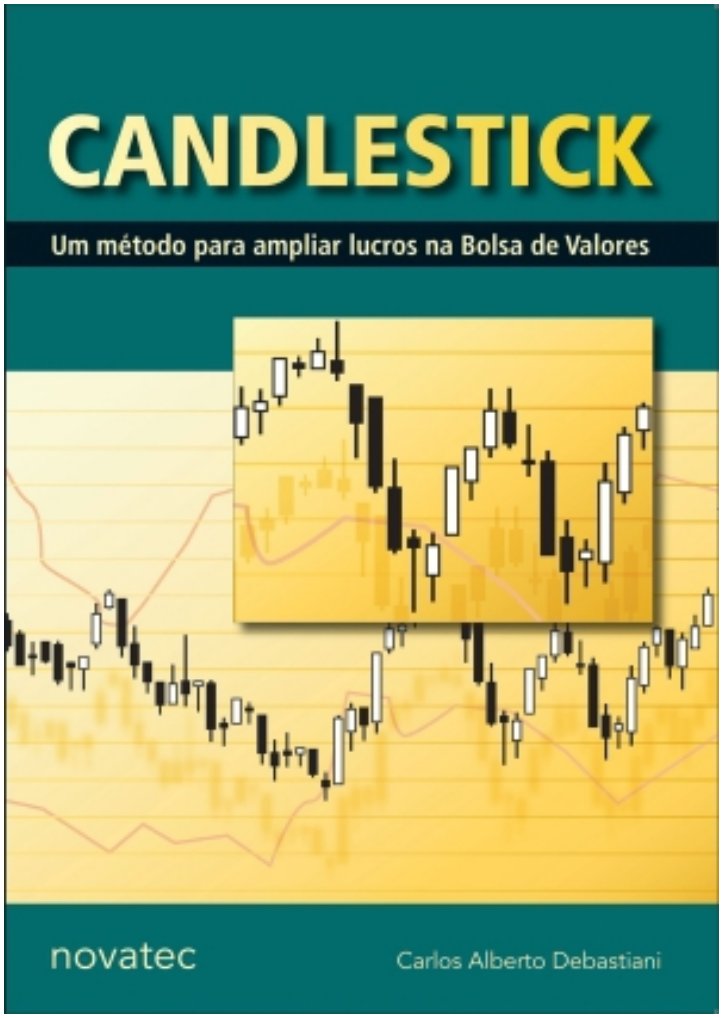

# Administração de redes Linux

Olonca, Ricardo Lino
9788575226506
256 páginas



Como um firewall funciona? Como configurar o Squid? Como funciona um proxy? O que é possível fazer com o iptables? Como calcular a máscara de sub-rede? São perguntas que todo profissional que trabalha na administração de redes deveria saber

responder. O assunto é muito amplo, não se resumindo apenas à configuração das interfaces. Rotas, bloqueios, limitações, filtros e alta disponibilidade são apenas alguns dos milhares de assuntos da área de redes, e dominar seus conceitos, suas práticas e possibilidades requer estudo, treino e tempo. Este livro mostra os conceitos fundamentais, as configurações e como fazer análises de desempenho e de problemas envolvendo redes. Também ensina o funcionamento dos principais serviços de rede, como roteamento, DNS, DHCP, firewall, NAT e proxy e como configurá-los em um ambiente Linux. Destina-se a profissionais de informática que já tenham conhecimentos em Linux e que desejam dominar os fundamentos da rede TCP/IP. O livro, ao estilo mão na massa, começa com assuntos simples e vai aumentando a complexidade conforme mostra exemplos práticos do dia a dia, que darão ao leitor o conhecimento necessário para administrar com eficiência e segurança uma rede em ambiente Linux. Administração de redes Linux aborda: Conceito de protocolo e uma breve explicação sobre o protocolo TCP/IP. Como calcular a máscara de sub-rede. Roteamento. Instalação e configuração do Bind9. Funcionamento do DHCP e a função de Relay. Funcionamento do iptables. Conceito de NAT e como configurá-lo no iptables. Funcionamento de um sniffer. Funcionamento de um proxy e instalação do Squid. Ferramentas de segurança.



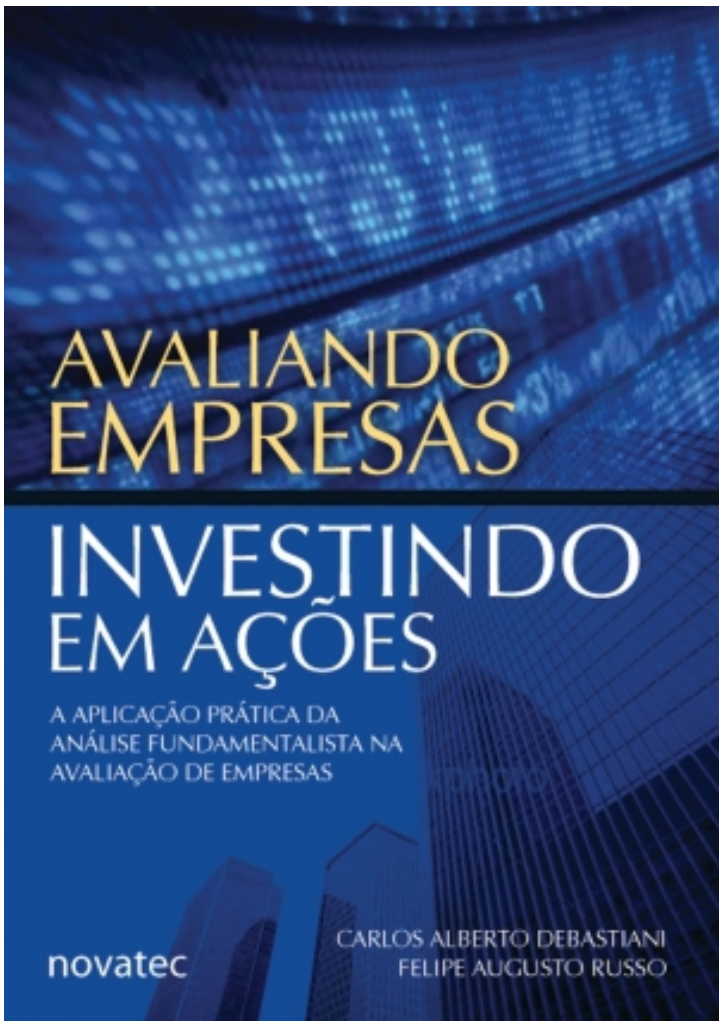

# Candlestick

Debastiani, Carlos Alberto
9788575225943
200 páginas

Compre agora e leia

A análise dos gráficos de Candlestick é uma técnica amplamente utilizada pelos operadores de bolsas de valores no mundo inteiro. De origem japonesa, este refinado método avalia o comportamento

do mercado, sendo muito eficaz na previsão de mudanças em tendências, o que permite desvendar fatores psicológicos por trás dos gráficos, incrementando a lucratividade dos investimentos. Candlestick – Um método para ampliar lucros na Bolsa de Valores é uma obra bem estruturada e totalmente ilustrada. A preocupação do autor em utilizar uma linguagem clara e acessível a torna leve e de fácil assimilação, mesmo para leigos. Cada padrão de análise abordado possui um modelo com sua figura clássica, facilitando a identificação. Depois das características, das peculiaridades e dos fatores psicológicos do padrão, é apresentado o gráfico de um caso real aplicado a uma ação negociada na Bovespa. Este livro possui, ainda, um índice resumido dos padrões para pesquisa rápida na utilização cotidiana.




# Avaliando Empresas, Investindo em Ações

Debastiani, Carlos Alberto
9788575225974
224 páginas



Avaliando Empresas, Investindo em Ações é um livro destinado a investidores que desejam conhecer, em detalhes, os métodos de análise que integram a linha de trabalho da escola fundamentalista,

trazendo ao leitor, em linguagem clara e acessível, o conhecimento profundo dos elementos necessários a uma análise criteriosa da saúde financeira das empresas, envolvendo indicadores de balanço e de mercado, análise de liquidez e dos riscos pertinentes a fatores setoriais e conjunturas econômicas nacional e internacional. Por meio de exemplos práticos e ilustrações, os autores exercitam os conceitos teóricos abordados, desde os fundamentos básicos da economia até a formulação de estratégias para investimentos de longo prazo.


# Manual de Análise Técnica

Abe, Marcos
9788575227022
256 páginas



Este livro aborda o tema Investimento em Ações de maneira inédita e tem o objetivo de ensinar os investidores a lucrarem nas mais diversas condições do mercado, inclusive em tempos de crise.

Ensinará ao leitor que, para ganhar dinheiro, não importa se o mercado está em alta ou em baixa, mas sim saber como operar em cada situação. Com o Manual de Análise Técnica o leitor aprenderá: - os conceitos clássicos da Análise Técnica de forma diferenciada, de maneira que assimile não só os princípios, mas que desenvolva o raciocínio necessário para utilizar os gráficos como meio de interpretar os movimentos da massa de investidores do mercado; - identificar oportunidades para lucrar na bolsa de valores, a longo e curto prazo, até mesmo em mercados baixistas; um sistema de investimentos completo com estratégias para abrir, conduzir e fechar operações, de forma que seja possível maximizar lucros e minimizar prejuízos; - estruturar e proteger operações por meio do gerenciamento de capital. Destina-se a iniciantes na bolsa de valores e investidores que ainda não desenvolveram uma metodologia própria para operar lucrativamente.


# Microsserviços prontos para a produção

Fowler, Susan J.
9788575227473
224 páginas



Um dos maiores desafios para as empresas que adotaram a arquitetura de microsserviços é a falta de padronização de arquitetura – operacional e organizacional. Depois de dividir uma

aplicação monolítica ou construir um ecossistema de microsserviços a partir do zero, muitos engenheiros se perguntam o que vem a seguir. Neste livro prático, a autora Susan Fowler apresenta com profundidade um conjunto de padrões de microsserviço, aproveitando sua experiência de padronização de mais de mil microsserviços do Uber. Você aprenderá a projetar microsserviços que são estáveis, confiáveis, escaláveis, tolerantes a falhas, de alto desempenho, monitorados, documentados e preparados para qualquer catástrofe. Explore os padrões de disponibilidade de produção, incluindo: Estabilidade e confiabilidade – desenvolva, implante, introduza e descontinue microsserviços; proteja-se contra falhas de dependência. Escalabilidade e desempenho – conheça os componentes essenciais para alcançar mais eficiência do microsserviço. Tolerância a falhas e prontidão para catástrofes – garanta a disponibilidade forçando ativamente os microsserviços a falhar em tempo real. Monitoramento – aprenda como monitorar, gravar logs e exibir as principais métricas; estabeleça procedimentos de alerta e de prontidão. Documentação e compreensão – atenue os efeitos negativos das contrapartidas que acompanham a adoção dos microsserviços, incluindo a dispersão organizacional e a defasagem técnica.