



TECNOLOGIA DA INFORMAÇÃO

Redes de Computadores

Fundamentos e protocolos

SENAI-SP editora

José Wagner Bungart

Redes de Computadores

Fundamentos e protocolos

Dados Internacionais de Catalogação na Publicação (CIP)

Bungart, José Wagner
Redes de computadores: fundamentos e protocolos / José Wagner Bungart
- São Paulo: SENAI-SP Editora, 2019.
200 p., 128 ils.

Inclui referências
ISBN 978-85-8393-765-4

1. Redes de computadores I. Título.

CDD 004.65

Índice para o catálogo sistemático:

1. Redes de computadores 004.65

TECNOLOGIA DA INFORMAÇÃO

Redes de Computadores

Fundamentos e protocolos

José Wagner Bungart

SENAI-SP editora



**Departamento Regional
de São Paulo**

Presidente
Paulo Skaf

Diretor Regional
Ricardo Figueiredo Terra

Diretoria Corporativa
Aprigio Eduardo de Moura Azevedo

*Gerência de Assistência
à Empresa e à Comunidade*
Celso Taborda Kopp

Gerência de Inovação e de Tecnologia
Osvaldo Lahoz Maia

Gerência de Educação
Cassia Regina Souza da Cruz

Apresentação

Com a permanente transformação dos processos produtivos e das formas de organização do trabalho, as demandas por educação profissional multiplicam-se e, sobretudo, se diversificam.

Em sintonia com essa realidade, o SENAI-SP valoriza a educação profissional para o primeiro emprego dirigida a jovens. Privilegia também a qualificação de adultos que buscam um diferencial de qualidade para progredir no mercado de trabalho. E incorpora firmemente o conceito de “educação ao longo de toda a vida”, oferecendo modalidades de formação continuada para profissionais já atuantes. Dessa forma, atende às prioridades estratégicas da Indústria e às prioridades sociais do mercado de trabalho.

A instituição trabalha com cursos de longa duração como os cursos de Aprendizagem Industrial, os cursos Técnicos e os cursos Superiores de Tecnologia. Oferece também cursos de Formação Inicial e Continuada, com duração variada na modalidades de Iniciação Profissional, Qualificação Profissional, Especialização Profissional, Aperfeiçoamento Profissional e Pós-Graduação. Com satisfação, apresentamos ao leitor esta publicação, que integra uma série da SENAI-SP Editora especialmente criada para apoiar os alunos das diversas modalidades.

Sumário

Introdução	9
1. Redes de computadores	11
Definição de redes de computadores	11
Padrões de redes	12
Órgãos normativos	13
Protocolos e serviços de redes	14
Classificação de redes	16
Tipos de redes	21
2. Dispositivos de comunicação de redes	25
Hub	25
Switch	27
Roteador	29
Access point	30
Firewall	32
Modem	33
Switch multcamadas	34
3. Topologias de redes	37
Barramento	37
Anel	38
Estrela	40
Malha	41
Hierárquica	42
4. Arquitetura de protocolos de redes	46
Modelo OSI	46
Arquitetura TCP/IP	58
Correlação entre modelos TCP/IP e OSI	59
5. Camada aplicação	62
Protocolos	62

6. Camada transporte	68
Definição	68
Protocolo TCP – Transmission Control Protocol	70
Protocolo UDP – User Datagram Protocol	75
7. Camada rede	78
Definição	78
Protocolo IPv4	79
Protocolo IPv6	94
Protocolo ICMP – Internet Control Message Protocol	99
8. Camada enlace e camada física	104
Características da camada física	104
Camada enlace	110
Protocolos da camada enlace	110
9. Redes sem fio	120
Definição	121
Classificação de redes sem fio	121
Ondas eletromagnéticas	122
Tipos de transmissão sem fio	124
Órgãos e padrões de redes WLAN	127
Conceitos de redes WLAN	128
Protocolos 802.11	134
10. Serviços de redes	142
Acesso local	142
Acesso remoto	144
Telnet	145
Secure Shell – SSH	145
Dynamic Host Configuration Protocol – DHCP	145
Domain Name System – DNS	149
11. Configurações de equipamentos de redes	152
Switches	152
Roteadores Cisco	173
Funcionamento de uma rede LAN	184
Funcionamento de uma rede WAN	187
Referências	193
Sobre o autor	197

Introdução

Este livro permite ao leitor uma evolução gradativa nos conceitos básicos de redes de computadores, a partir de uma visão geral dos tipos e classificações de redes, até chegar no principal: o alinhamento da linguagem e o conhecimento dos conceitos utilizados pelos profissionais da área. O objetivo central do tema aqui proposto é permitir ao leitor que conheça o funcionamento de uma rede de computadores e consiga, ao final do livro, configurar os equipamentos e protocolos, permitindo a comunicação entre diferentes dispositivos. São apresentados também os principais órgãos normativos, referências de normas e padrões desenvolvidos, que são bastante utilizados entre técnicos.

O Capítulo 1 apresenta os principais equipamentos e as topologias de redes, assunto de fundamental importância para o macroentendimento do funcionamento das redes. Isto é, a primeira abordagem trata do modelo de referência desenvolvido pela ISO, do modelo OSI, e dos conceitos básicos da arquitetura TCP/IP. Esses tópicos são estudados no mesmo capítulo com a finalidade de compará-los, e assim preparar o leitor para a parte seguinte, que trata de maneira mais aprofundada cada uma das camadas da arquitetura TCP/IP. No Capítulo 2, então, são abordadas as características, principais protocolos e utilização da arquitetura TCP/IP nas empresas e nas residências.

Depois de conhecer o básico sobre essa estrutura de rede e as suas duas principais camadas os seus protocolos são estudados com a profundidade e importância que se deve ter. Primeiro é preciso conhecer a camada de transporte com o protocolo TCP, depois a camada de rede com o protocolo IP, inclusive em sua última versão, o IPv6. O livro também trata, em um capítulo específico, das redes sem fio, que ganham importância cada vez maior nas comunicações atuais. Vê-se, então, seus principais conceitos, equipamentos, protocolos e características.

Já na fase final do livro, ao ter permeado todos esses conhecimentos, o leitor conhecerá alguns dos principais serviços de redes, como o DHCP e o DNS, fundamentais para

o funcionamento de qualquer rede de computadores. Também são apresentados os serviços de acesso remoto Telnet e SSH. Ao final, estão as configurações básicas de switches e roteadores para que o leitor consolide os conhecimentos adquiridos ao longo dos capítulos e possa executar a configuração básica de uma rede.

Este livro é destinado a estudantes de cursos técnicos e tecnólogos da área de redes de computadores e informática que estejam em sua fase inicial de formação das bases de conhecimento em redes de computadores, bem como a profissionais da área que necessitem revisitar e atualizar conceitos fundamentais sobre o assunto.

1. Redes de computadores

Definição de redes de computadores

Padrões de redes

Órgãos normativos

Protocolos e serviços de redes

Classificação de redes

Tipos de redes

Atualmente, as redes de computadores permeiam praticamente todas as atividades diárias, sejam elas profissionais ou pessoais. Quando não se está conectado diretamente a alguma rede, certamente faz-se uso de algum serviço provido com a ajuda de alguma rede de algum lugar do mundo.

É comum que haja redes residenciais com poucos dispositivos conectados, como computadores, celulares, videogames e até mesmo controles de funcionalidades residenciais, como, por exemplo: automações de iluminação, acionamento de portas e temperatura de ar-condicionado. Nas empresas e indústrias, a dependência de redes de computadores é ainda maior, e muitas simplesmente não operam caso algum problema ocorra. Quase todas as redes têm alguma interação, ao menos em algum momento, com a internet, ampliando as possibilidades e globalizando as comunicações.

Neste capítulo serão estudados os conceitos fundamentais de redes de computadores, como se comunicam, suas classificações e tipos. A partir dele pode-se comparar definições formais com cenários encontrados no cotidiano.

Definição de redes de computadores

Pode-se definir redes de computadores de maneira muito simples: dois ou mais computadores interconectados por um meio de comunicação que tem por finalidade o

compartilhamento de recursos e informações. Isto é, segundo Andrew Tanenbaum (2001, p. 2) redes de computadores podem ser definidas da seguinte forma:

Utilizaremos a expressão “rede de computadores” quando quisermos mencionar um conjunto de computadores autônomos interconectados por uma única tecnologia. Dois computadores estão interconectados quando podem trocar informações. A conexão não precisa ser feita por um fio de cobre; também podem ser usadas fibras ópticas, micro-ondas, ondas de infravermelho e satélite de comunicações. Existem redes em muitos tamanhos, modelos e formas. Embora possa parecer estranho para algumas pessoas, nem a internet nem a World Wide Web é uma rede de computadores. A resposta simples é que a internet não é uma única rede, mas uma rede de redes, e a Web é um sistema distribuído que funciona na internet.

A definição de Tanenbaum tem um ponto de discussão muito importante: a utilização de uma única tecnologia é o que determina que dois computadores estejam na mesma rede. Isto é, dois computadores só estarão conectados em uma única rede caso possuam a mesma tecnologia. Por exemplo, se os dois computadores de uma determinada comunicação utilizarem somente uma rede sem fio (Wi-Fi), podemos dizer que estão na mesma rede; caso um computador esteja numa rede Wi-Fi e outro numa rede cabeadas, eles não estão na mesma rede. Em diversos pontos deste livro esse assunto será abordado. Também será analisado se dois computadores pertencem ou não à mesma rede: dependendo da resposta, a comunicação entre os computadores será tratada de uma maneira diferente.

Outra definição que aparece na citação e é importante diz respeito à forma como os computadores se comunicam, podendo ser por meios físicos, como cabos metálicos e fibras ópticas, ou por meio do ar, que funciona como transporte, por exemplo as redes Wi-Fi.

Padrões de redes

O termo “padrão” é muito utilizado para se referir às redes de computadores. Ele se refere ao fato de que, para existir comunicação entre dois ou mais computadores deve-se seguir uma grande variedade de regras, acordadas entre as empresas

que desenvolvem tanto o hardware como o software. Em caso contrário, podem ocorrer problemas de compatibilidade e as redes não operarem adequadamente. A esse conjunto de regras dá-se o nome de padrão.

De acordo com a ISO (do inglês, *International Organization for Standardization – Organização Internacional para Padronização*), um padrão é:

Documento aprovado por um organismo reconhecido que provê, pelo uso comum e repetitivo, regras, diretrizes ou características de produtos, processos ou serviços cuja obediência não é obrigatória. (ISO, 2016)

Apesar de a ISO definir “padrão” como elaborado por uma organização, os padrões podem ser de dois tipos:

Quadro 1 – Padrões

Padrão de direito	Padrão de fato
Padrões formais, legais, elaborados e adotados por organizações públicas ou privadas, autorizadas para este fim. Exemplos: Modelo OSI, IEEE 802.	Padrões que existem por causa da grande aceitação do mercado de determinada tecnologia. Exemplos: IBM-PC, UNIX, TCP/IP.

Isto é, também existem os padrões estabelecidos pelo uso, que se firmaram a partir da aceitação e recorrência, sem antes terem sido preestabelecidos por um órgão. Sobre esses padrões, no Capítulo 4 serão dados detalhes. No entanto, veja a seguir algumas das principais organizações que fornecem declaração de padrão para as redes de computadores.

Órgãos normativos

International Organization for Standardization – ISO

É uma organização internacional independente, não governamental, com 163 órgãos nacionais de normatização relacionados com membros que reúnem especialistas para compartilhar conhecimentos e desenvolver normas baseadas em consenso. O objetivo das normas é fornecer soluções para as mais variadas áreas. A ISO desenvolveu diversos padrões para a área de redes de computadores, como padrões para cabeamento, equipamentos, protocolos e segurança de redes.

Institute of Electrical and Electronics Engineers – IEEE

O IEEE é uma organização sem fins lucrativos que possui mais de 370 mil membros no mundo. Criada em 1963 nos Estados Unidos, hoje possui filiais em quase todos os países, abrangendo diversas áreas do conhecimento, como a engenharia elétrica, eletrônica, da computação, ciência da computação e telecomunicações. O objetivo da IEEE é promover o conhecimento nessas áreas, incentivando a pesquisa com publicações técnicas, de jornais e organizando conferências, e além disso, ser um dos mais importantes órgãos padronizadores do mundo.

Internet Engineering Task Force – IETF

O IETF é uma comunidade internacional aberta, composta de projetistas, operadores, fabricantes e pesquisadores com interesse na evolução da arquitetura da internet e sua operação. O seu trabalho técnico é dividido em grupos organizados por tópicos, chamados de ADs (Area Directors). Nela existem ADs de roteamento, transporte, segurança, entre outros. Uma lista completa dos ADs ativos está disponível em: <https://datatracker.ietf.org/wg/>. O IETF também é responsável por desenvolver e manter as RFCs (Request for Comments), documentos que detalham o funcionamento de cada um dos padrões utilizados na internet.

Associação Brasileira de Normas Técnicas – ABNT

A ABNT é uma entidade privada, sem fins lucrativos, responsável pela elaboração das Normas Brasileiras (ABNT NBR), além da avaliação da conformidade e certificação de produtos. Para as redes de computadores existem diversas normas brasileiras, em especial para cabeamento estruturado e infraestrutura.

Protocolos e serviços de redes

Segundo James Kurose e Keith Ross:

Um protocolo define o formato e a ordem das mensagens trocadas entre duas ou mais entidades comunicantes, bem como as ações realizadas na

transmissão e/ou no recebimento de uma mensagem ou outro evento. (KUROSE, 2010, p. 7)

Isto é, a principal função dos protocolos é criar uma maneira de dois dispositivos se comunicarem. Desta forma, computadores, servidores, tablets, celulares e muitos outros equipamentos são capazes de trocar informações e o usuário final pode utilizar os serviços providos por eles.

Os serviços de redes, por sua vez, são as aplicações propriamente ditas utilizadas pelos usuários da rede. Muitas vezes os termos protocolo e serviço de rede são confundidos, isso porque o serviço pode estar associado a somente um protocolo, recebendo assim o nome deste. Mas é importante notar que um serviço de rede também pode estar associado a vários protocolos.

Para compreender melhor o conceito de protocolo, ele pode ser também entendido como a linguagem utilizada entre dois equipamentos. Comparando essa linguagem com uma situação vivida o tempo todo, tem-se o diálogo da Figura 1:

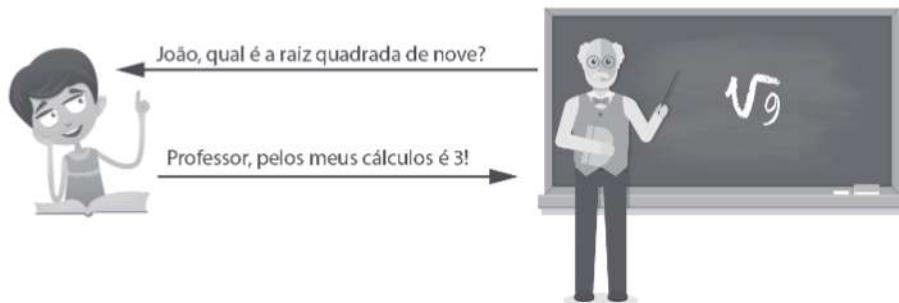


Figura 1 – Protocolo e a comunicação.

Fonte: Thinkstock.

O protocolo utilizado para a comunicação entre o professor e João foi a língua portuguesa oral. O professor conseguiu se expressar, o aluno entendeu e respondeu corretamente. Nesse caso, o serviço final oferecido pelo professor é a aula de matemática.

Se estivessem utilizando protocolos diferentes, por exemplo, se o professor tivesse falado chinês e o aluno, português, a comunicação não teria êxito, conforme a Figura 2.

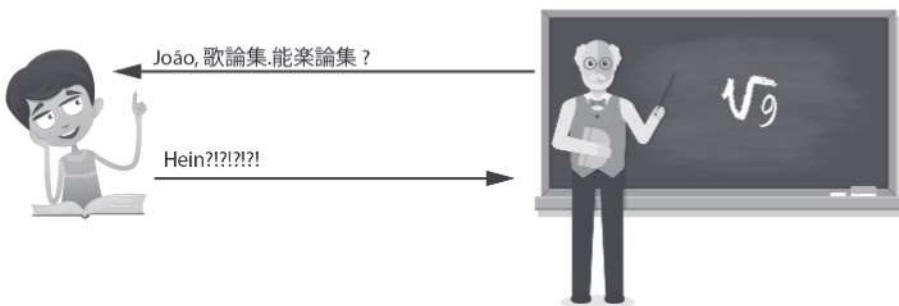


Figura 2 – Protocolos diferentes.

Fonte: Thinkstock.

Apesar de serem fundamentais e necessários para todos os tipos de redes, os protocolos não são definidores destas. Eles caracterizam a comunicação entre as redes, porém a finalidade e os serviços finais que as classificam. Veja a seguir a classificação de redes de computadores.

Classificação de redes

Uma das maneiras mais comuns de classificar as redes de computadores é em relação a sua abrangência ou distribuição geográfica. Conforme já foi mencionado, não importam as tecnologias e os protocolos envolvidos, mas principalmente a finalidade da rede e os serviços que ela oferece. Neste livro serão abordadas as três classificações mais comuns: LAN, MAN, WAN e suas variações sem fio.

Local Area Network – LAN

Podemos definir uma rede de área local, ou simplesmente LAN (do inglês, Local Area Network), como uma rede privada de pequeno alcance. Esse tipo de rede é utilizado geralmente para interconectar computadores, impressoras e servidores dentro de um mesmo prédio ou *campus*, como apresentado na Figura 3. Até quem tem dois computadores interligados ponto a ponto, ou seja, somente os dois computadores interligados por um cabo, sem a conexão com outros equipamentos de rede, possui uma rede de área local. Outra forma de definir uma LAN é por meio da avaliação da presença de altas taxas de transferência, baixos índices de erros e custo relativamente baixo.

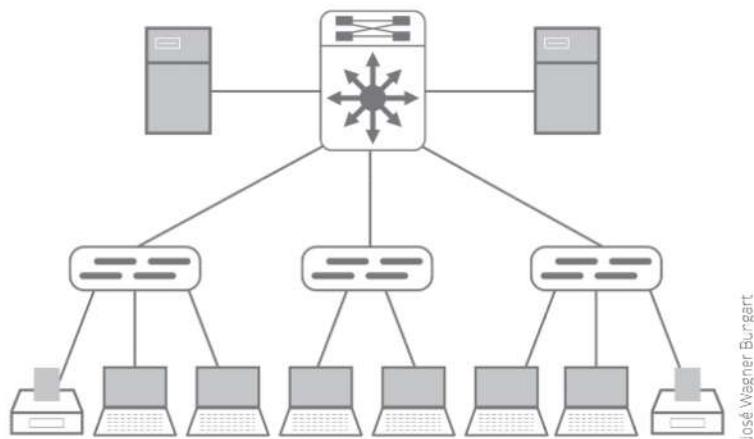


Figura 3 – Local Area Network – LAN.

Há também um outro tipo de rede LAN: as redes WLAN, Wireless LAN. Isto é, WLAN são redes locais sem fio que utilizam alguma tecnologia de interconexão cujo meio de transmissão é o ar. A tecnologia de interconexão mais comumente usada é a WiFi, que será abordada mais adiante neste livro.

É uma forma muito rápida e relativamente barata de prover conectividade entre computadores e outros dispositivos de rede local, pois não dependem de cabeamento metálico ou fibra óptica. As redes Wireless LAN têm crescido muito nos últimos anos, até mesmo para uso doméstico, por serem redes de velocidade relativamente alta se comparadas a outros sistemas sem fio e por permitirem uma pequena mobilidade (Figura 4).

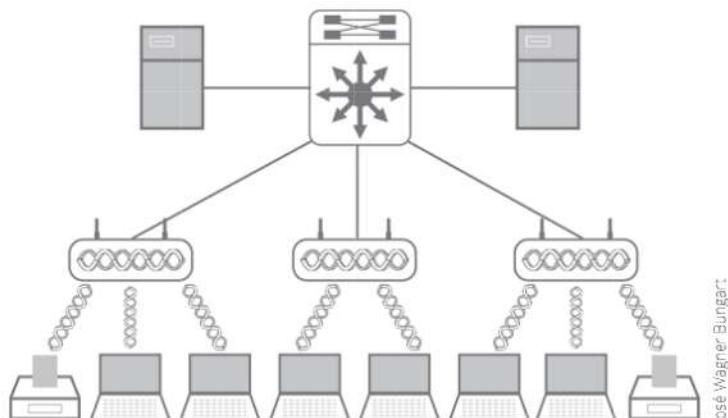


Figura 4 – Wireless LAN.

José Wagner Bürgart

Geralmente as redes WLAN estão conectadas às redes LAN, ou seja, existe também uma conexão por meio físico cabeado, da qual se expande para a rede sem fio.

Metropolitan Area Network – MAN

As redes metropolitanas – como o próprio nome sugere – têm o alcance de uma cidade. Geralmente são utilizadas para interligar empresas e universidades que possuem diversas sedes em uma mesma cidade ou região metropolitana (Figura 5). Outro exemplo de MAN são as redes de televisão a cabo. Elas possuem concessão para prover serviço para uma determinada cidade ou área da cidade, e distribuem seus equipamentos e cabeamento para cobri-las. Se a MAN for maior que os limites de uma cidade será considerada uma WAN, conforme definido a seguir.

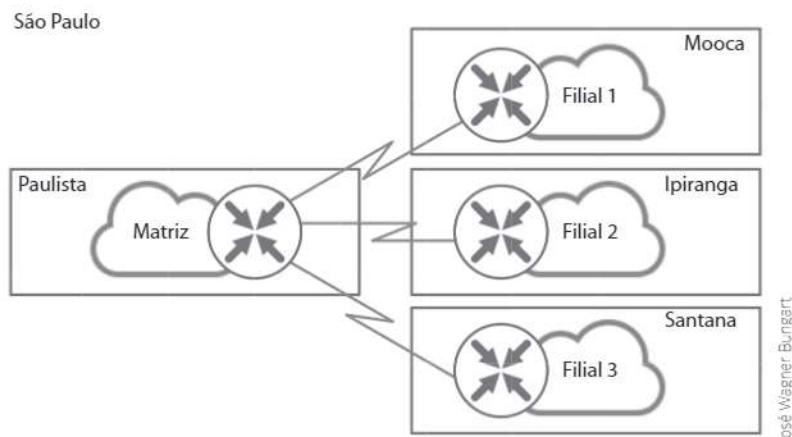


Figura 5 – Metropolitan Area Network – MAN.

Da mesma maneira que funcionam as redes WLAN, também existe a possibilidade de as redes metropolitanas serem conectadas por meio de links sem fio, recebendo o nome de WMAN (*Wireless Metropolitan Area Network*), ilustrada na Figura 6.

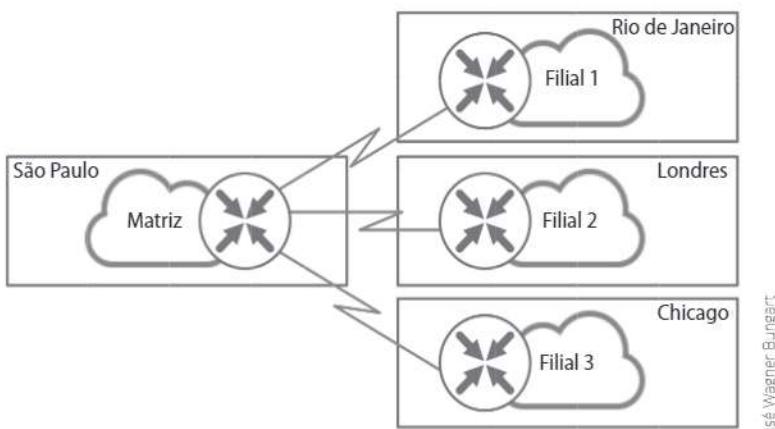


José Wagner Burgart

Figura 6 – Wireless – WMAN.

Wide Area Network – WAN

Redes WAN são redes geograficamente distribuídas, geralmente de grande abrangência. Elas interligam cidades, estados, países e até mesmo continentes. São utilizadas para prover conectividade entre redes locais, como, por exemplo, a matriz de uma empresa a suas filiais, redes de fornecedores e parceiros etc. (Figura 7).



José Wagner Burgart

Figura 7 – Wide Area Network – WAN.

SAIBA MAIS

Para conectar países e continentes utilizam-se fibras ópticas submarinas. Visite o site www.submarinecablemap.com e veja a grande quantidade de cabos submarinos instalados e planejados para os próximos anos.

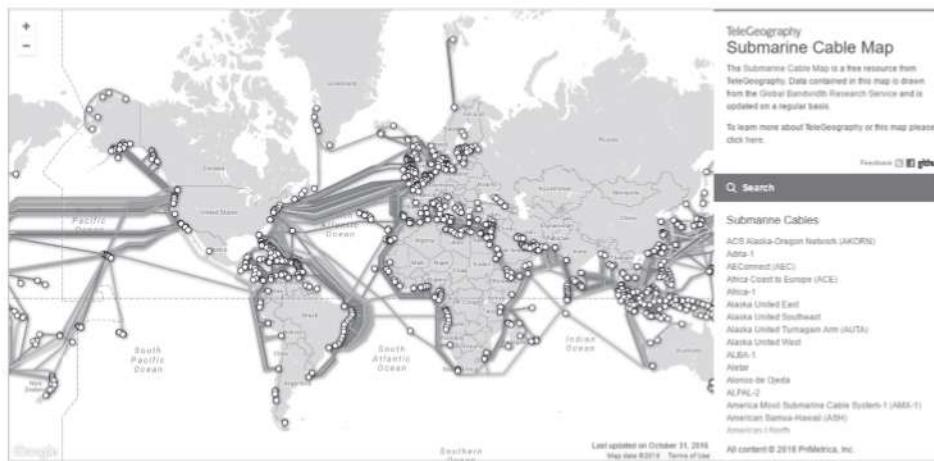


Figura 8 – Mapa de cabos submarinos.

Fonte: Submarine Cable Map.

As redes Wireless WAN (WWAN) são baseadas em redes de telefonia móvel ou em satélites e utilizam sua infraestrutura para transportar dados além de voz. Sua abrangência depende da área de cobertura da operadora de telefonia móvel, mas pode ser ampla o suficiente para ser considerada uma WAN, pois se estende por cidades e até mesmo estados. Quando utilizada por satélites, tem alcance global. A WWAN nasceu da necessidade de se usar dispositivos especiais, como, por exemplo, aparelhos de telemetria de veículos, isto é, rastreamento completo de veículos. Ela possibilita a conexão ininterrupta a uma rede sem a perda de mobilidade, ainda que tenha velocidade mais baixa se comparada às WLANs (Figura 9).

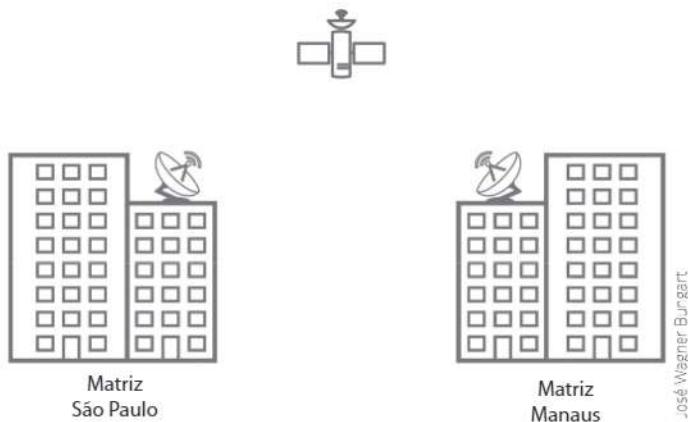


Figura 9 – Wireless WAN.

Além de serem classificadas segundo seu tipo de comunicação (cabeada ou sem fio) e alcance, as redes de computadores se definem por sua arquitetura, isto é, como elas estão montadas. Veja a seguir os diferentes tipos de arquitetura de redes.

Tipos de redes

Cliente-Servidor

Atualmente uma das formas mais comuns de se prestar um serviço de rede é por meio das redes do tipo cliente-servidor. São aquelas em que a arquitetura foi desenhada para um ou mais dispositivos, chamados clientes, utilizarem serviços providos por um outro dispositivo, o servidor, que executará as tarefas ou proverá as informações solicitadas pelo cliente.

Nesse tipo de arquitetura, os clientes iniciam as sessões, esperam uma resposta positiva do servidor e solicitam uma ação. A ação é então executada pelo servidor, que retorna uma resposta ao cliente. Uma característica importante desse tipo de rede é a capacidade de compartilhamento de recursos, ou seja, um único servidor pode atender uma grande quantidade de clientes, reduzindo consideravelmente os custos (Figura 10).

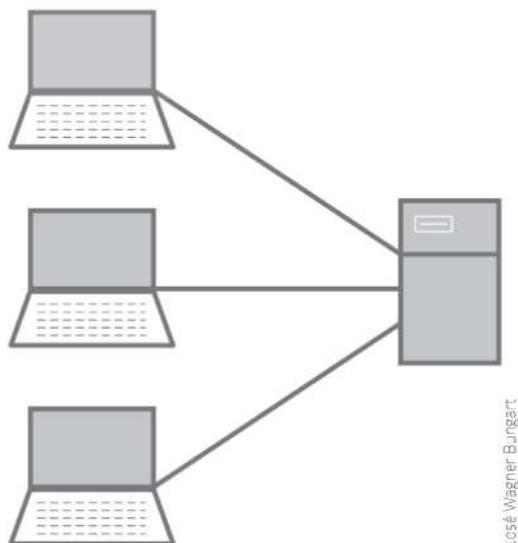
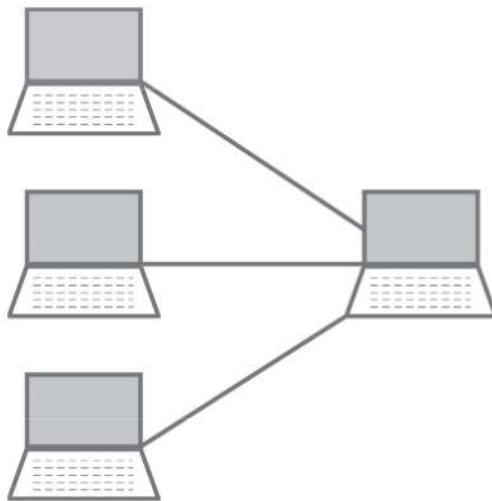


Figura 10 – Rede cliente-servidor.

Peer-to-Peer (P2P)

Chamada de Peer-to-Peer, essa rede também pode ser traduzida por “ponto a ponto”. Conforme o nome indica, os dispositivos de rede se comunicam diretamente sem a necessidade de um servidor. Ao se comparar a arquitetura cliente-servidor com uma rede Peer-to-Peer (P2P), tem-se que a diferença é que nesta cada dispositivo pode solicitar ou processar informações. Atualmente é muito utilizada para compartilhamento simultâneo de informações ou arquivos entre múltiplos dispositivos, como por exemplo nas aplicações de *torrent* (Figura 11). Diferentemente da rede cliente-servidor, a rede P2P não conta com uma hierarquia, uma responsabilidade de um só dispositivo.



José Wagner Burgart

Figura 11 – Peer-to-Peer – P2P.

Redes ubíquas

Redes ubíquas, também conhecidas como redes pervasivas, são aquelas onipresentes, capazes de se espalhar por toda parte sem que haja necessariamente uma conexão física. Uma de suas características primordiais é que devem funcionar de maneira transparente para os usuários, isto é, sem ser percebida. O acionamento de uma rede ubíqua, diferente das outras que envolvem uso direto do dispositivo (mouse, teclado, etc.), deve valer-se de uma maneira natural, como se o usuário não estivesse

dando comandos para uma máquina, mas sim por meio de textos, voz, imagem etc. As interfaces com os usuários devem ser simplificadas, sem exigir deles conhecimentos técnicos para usufruir dos dispositivos e sistemas. Um exemplo de rede ubíqua é o controle de iluminação de uma casa por controle remoto ou gestos humanos, ou um videogame controlado por gestos.

Um grande desafio para os fabricantes de hardware e, principalmente, de softwares de redes é alcançar esse ponto de transparência entre os usuários e os equipamentos de redes, a fim de que a comunicação aconteça da forma mais natural possível para o ser humano e para que ele se sinta totalmente integrado com a rede.

RECAPITULANDO

Neste capítulo foram apresentados a definição de redes de computadores, os padrões, os protocolos e serviços de redes. Foi possível conhecer o que são protocolos de redes e sua importância na comunicação dos computadores, além de aprender a diferenciar os protocolos dos serviços de redes.

Verificou-se que as redes podem ser classificadas quanto a sua abrangência, LAN, MAN e WAN com as suas variações para redes sem fio, WLAN, WMAN e WWAN, mas também por seu tipo. Viu-se que o mais comum deles é o cliente-servidor, as redes ponto a ponto e um conceito relativamente novo: as redes ubíquas, que possuem o objetivo de não serem notadas pelo usuário.

Exercícios

1. Defina o que são redes de computadores.
2. Diferencie padrões de fato de padrões de direito.
3. O que é um protocolo de rede?
4. O que são serviços de rede?

5. Explique o que são as redes do tipo:
 - a) cliente-servidor
 - b) ponto a ponto
 - c) ubíquas
6. Como podemos definir uma rede LAN?
7. Qual a diferença entre uma rede LAN e WLAN?
8. Defina rede MAN. Quando uma rede deixa de ser LAN e passa a ser MAN?
9. Defina rede WAN. Quando uma rede deixa de ser MAN e passa a ser WAN?
10. Explique como são as redes WMAN e WWAN.

As respostas dos exercícios deste livro estão disponíveis para *download* no seguinte *link*: https://www.senaispeditora.com.br/downloads/respostas/redes_computadores_respostas.pdf

2. Dispositivos de comunicação de redes

Hub
Switch
Roteador
Access point
Firewall
Modem
Switch multicamadas

No capítulo anterior foram definidos as redes, os protocolos de comunicação entre os dispositivos de uma rede e os serviços que ela pode prestar. No entanto, como se efetua essa comunicação entre os dispositivos pertencentes a uma rede a fim de realizar o serviço? Para conhecer esse assunto, neste capítulo serão estudados os principais equipamentos de redes, suas funções, principais características e aplicabilidade. As diferenças entre um hub e um switch são apresentadas e é explicado como identificar onde devem ser utilizados access points, roteadores, modems, firewalls e switches multicamadas.

Hub

Os hubs são equipamentos utilizados para redes locais de pequeno porte com a função de interligar computadores, impressoras e outros dispositivos. Ele tem uma estrutura de funcionamento simples e um desempenho baixo, assim como seu custo. Atualmente, seu uso é raro em redes comerciais e industriais, pois ao longo do tempo o custo dos switches, equipamento similar aos hubs,

baixou, apesar do seu desempenho ser muito melhor. Essa substituição tecnológica transformou os hubs em equipamentos obsoletos e com baixo custo-benefício.

Para entender o funcionamento de um hub, pode-se analisar o cenário a seguir, no qual há três computadores (A, B e C) e uma impressora conectados a um hub. Nesse exemplo todos os dispositivos podem se comunicar porque cada um está conectado a uma porta do hub, o qual “concentra” as informações a serem transmitidas. Ele o faz por um procedimento baseado em *broadcast*, ou seja, por um sistema de transmissão de mensagem simultânea para vários dispositivos diferentes. Isto é, quando uma mensagem é enviada por um computador conectado a um hub, este retransmite a mesma mensagem para todos os dispositivos conectados em si, menos para quem originou a mensagem.

No exemplo, quando o computador A transmitir uma mensagem para o computador B, a mesma mensagem será reenviada para o computador C e para a impressora, além do computador B (Figura 1).

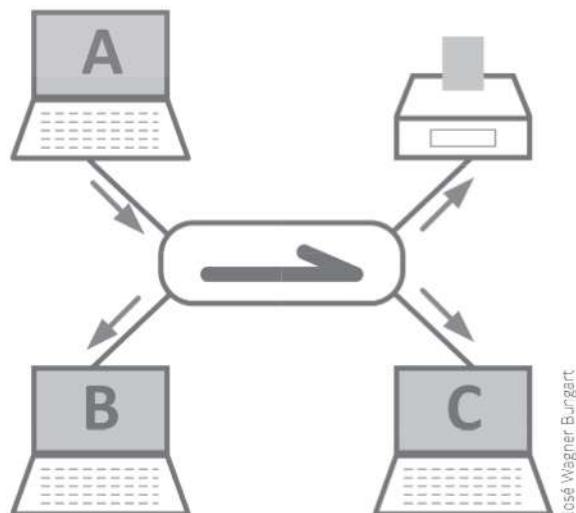


Figura 1 – Funcionamento do hub.

-José Wagner Burgart

SAIBA MAIS

Para entender melhor o funcionamento de um hub, veja a animação no link: www.senaispeditora.com.br/catalogo/informacoes-tecnologicas-tecnologia-da-informacao/redes-de-computadores-fundamentos-e-protocolos/

Os hubs são equipamentos com uma quantidade baixa de portas. Não existe uma padronização, mas é comum encontrar hubs com poucas portas, como seis, oito ou doze (Figura 2), ou equipamentos com uma densidade um pouco maior de portas, como 24 e 48 (Figura 3).



Figura 2 – Hub de oito portas.

Fonte: Omni Secu.



Figura 3 – Hub de 24 portas.

Fonte: Zd Tronic.

Switch

Os switches, assim como os hubs, são equipamentos com a função de conectar dispositivos de rede local. Com o avanço das tecnologias de longa distância, existem switches capazes de conectar dispositivos em localidades remotas, apesar de terem sido originalmente desenvolvidos para redes LAN.

A diferença entre o hub e o switch está na arquitetura e, consequentemente, no desempenho dos dois tipos de equipamentos. Os switches possuem Source Address Table (SAT), ou tabela de endereços MAC (Media Access Control), que é responsável por armazenar informações de endereço relativas a cada dispositivo que está conectado a ele. Isto é, o sistema SAT ou MAC registram os endereços das portas dos

dispositivos e, quando uma mensagem é destinada para um deles, ela só é transmitida para aquela porta e não para todas, como nos hubs. Nesse caso, não existe mais um *broadcast* das mensagens e sim um *unicast*, que é a transmissão somente para um destinatário. Na tabela SAT fica armazenado o número da porta ou sua identificação, e o endereço MAC do dispositivo conectado a essa porta. Utilizando o mesmo exemplo anterior, mas agora substituindo-o por um switch, pode-se observar que a mensagem só é transmitida para o computador B (Figura 4).

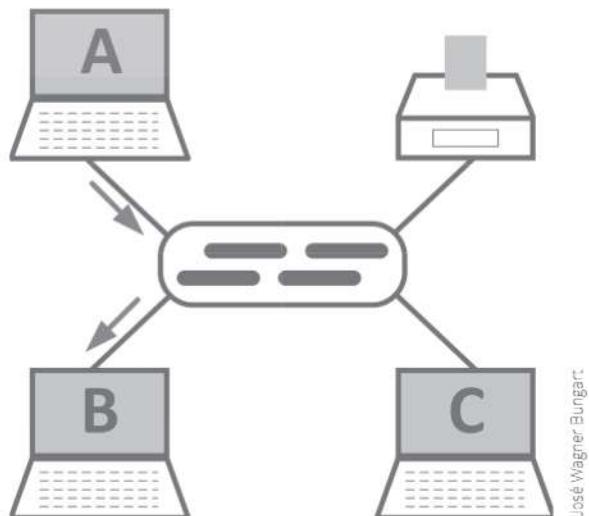


Figura 4 – Funcionamento do switch.

SAIBA MAIS

Para entender melhor o funcionamento de um switch, veja a animação no link: www.senaispeditora.com.br/catalogo/informacoes-tecnologicas-tecnologia-da-informacao/redes-de-computadores-fundamentos-e-protocolos/

Da mesma maneira que para os hubs, não existe uma padronização de quantidade de portas para os switches, somente de tipos. Mais adiante neste livro esse assunto será tratado em detalhes, mas, por enquanto, pode-se dizer que a quantidade de portas de um switch varia desde poucas, para uso residencial e de pequenas empresas, até grandes quantidades, em switches para redes com grande quantidade de usuários e dispositivos de redes. Existem switches com a quantidade fixa de portas (Figura 5) e switches modulares, que utilizam cartões (módulos) com portas de conexão que permitem o crescimento gradativo da rede conforme a necessidade. Assim, com a instalação de mais cartões no switch, a rede pode crescer e continuar a se comunicar (Figura 6).



Figura 5 – Switches com portas fixas.

Fonte: HP – Hewlett-Packard.



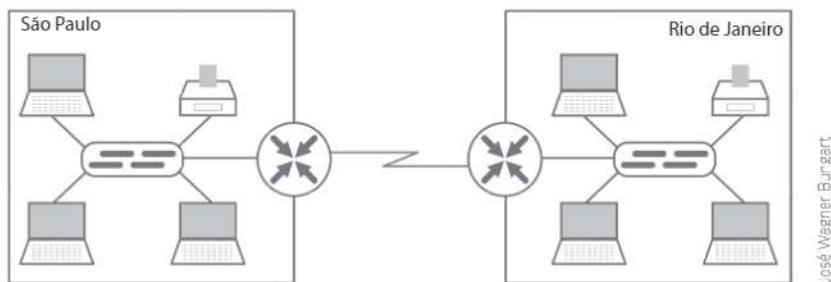
Figura 6 – Switch modular.

Fonte: HP – Hewlett-Packard.

Roteador

Os roteadores são equipamentos com a finalidade de interligar redes, sejam elas locais ou de longa distância. Se houver uma rede local subdividida em várias sub-redes e desejar-se que essas sub-redes se comuniquem entre si, será preciso que um roteador faça essa interconexão. A principal função dos roteadores é prover a comunicação entre redes com lógicas diferentes. No caso dos switches, o tipo de endereçamento utilizado para identificar os computadores é o MAC Address, que é um endereço físico fornecido pelo fabricante do hardware, enquanto um endereço lógico é configurado pelo administrador da rede, sendo o mais comum o endereço IP. Cada rede local deve possuir uma faixa ou conjunto de endereços IPs, chamado de rede ou sub-rede. Mais adiante serão estudados os endereços IPs, suas classes, redes e sub-redes, mas o conceito inicial que se deve ter é que os computadores são agrupados, em suas redes LAN, por faixas de endereços IP e que o roteador é o equipamento responsável por prover a comunicação entre essas redes de lógicas distintas. Uma característica importante dos roteadores é que eles não propagam *broadcasts* por não utilizarem o endereço físico das máquinas, somente o lógico.

Um exemplo típico e de fácil compreensão é a conexão de duas redes geograficamente distantes, como uma rede de uma empresa que possui sua matriz em São Paulo e uma filial no Rio de Janeiro, ambas com suas redes locais. Para que haja comunicação entre as duas redes locais, deve-se utilizar roteadores (Figura 7).



José Wagner Brüggen

Figura 7 – Redes interligadas com roteadores.

SAIBA MAIS

Para visualizar o envio de mensagens e o roteamento de pacotes entre redes, veja a animação no link: www.senaispeditora.com.br/catalogo/informacoes-tecnologicas-tecnologia-da-informacao/redes-de-computadores-fundamentos-e-protocolos/

Existem roteadores de diversos tamanhos, quantidades de portas e funcionalidades de roteamento. Na Figura 8, há quatro modelos de roteadores.



Figura 8 – Roteadores.

Fonte: Cisco Systems.

Access point

Access point – ou ponto de acesso – são equipamentos que têm a função de prover conexão sem fio (wireless) entre as estações da rede como laptops, celulares, tablets, impressoras e outros dispositivos sem fio. Possuem características semelhantes aos switches, pois concentram as conexões de diversos dispositivos

e encaminham suas mensagens para o restante da rede. O Capítulo 9 deste livro trata especificamente de redes sem fio.

Em redes corporativas é comum o uso de access points, enquanto em ambientes residenciais é comum o uso de roteadores wireless, que nada mais são que a junção de diversas funções de rede, como switching, roteamento, rede sem fio, servidores e até mesmo segurança. Por isso é importante não confundir os dois tipos de equipamento.

Na Figura 9 pode-se observar uma rede composta de switch, um roteador conectado à internet e a um access point na rede local. Esse desenho permite que se visualize como funciona o acesso à rede por parte dos usuários sem a utilização de cabos.

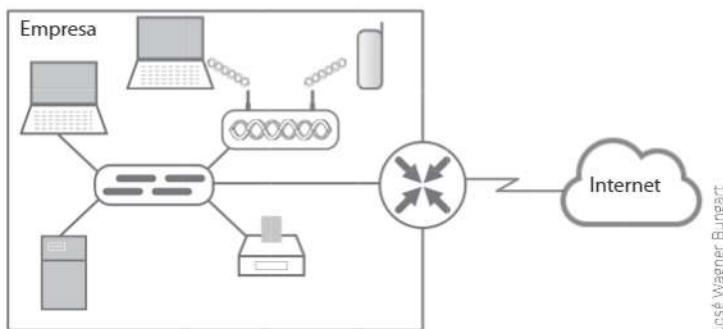


Figura 9 – Rede corporativa com uso de Access point.

Na Figura 10 há a imagem de um access point; um modelo possui antenas externas e o outro, internas.



Figura 10 – Access Point Cisco.

Fonte: Cisco Systems.

Os roteadores wireless são mais comuns em residências. Muito provavelmente o leitor já teve contato com esse tipo de equipamento ou já o viu em alguma rede residencial (Figura 11).



Figura 11 – Roteador Wireless.

Fonte: Tp-link.

Firewall

Firewall é um equipamento de segurança que tem por finalidade controlar o tráfego que passa pela rede, e, principalmente, defendê-la das tentativas de ataque e intrusão vindas da internet e de outras redes externas.

Existem firewalls baseados em hardware ou software, mas ambos têm o mesmo objetivo: servir de barreira para proteger a integridade dos equipamentos e informações, seguindo políticas de segurança preestabelecidas.

Os firewalls físicos, ou seja, baseados em hardware, são equipamentos com a função específica de aumentar a segurança da rede com a inclusão de regras que indicam o tráfego que é permitido ou não na rede (Figura 12). Geralmente, esses equipamentos possuem mais de uma porta de rede para que haja a segmentação física e para que as regras sejam aplicadas em suas portas conectadas à rede externa, por exemplo.

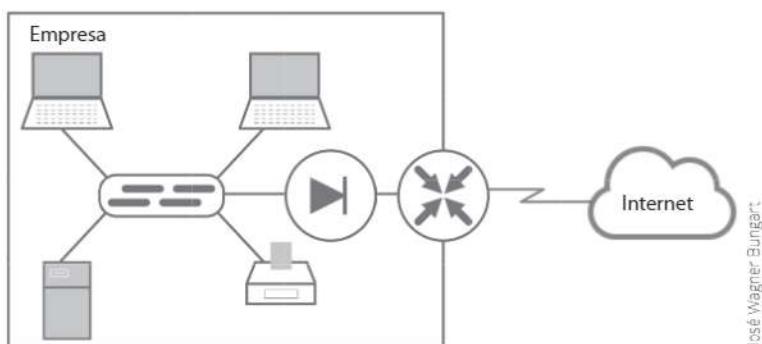


Figura 12 – Firewall baseado em hardware.

José Wagner Bunge Jr.

Na Figura 13 pode-se ver alguns modelos de firewalls em hardware.



Figura 13 – Firewalls.

Fonte: Cisco Systems.

Os firewalls baseados em software – por exemplo o firewall que é fornecido com as versões de Windows para computadores – têm a mesma função: bloquear tráfego indesejado, mas com a diferença de não possuir um hardware dedicado para essa função, tornando o firewall físico mais robusto para empresas com uma grande quantidade de usuários, pois cada transação feita na rede externa será inspecionada pelo firewall; enquanto as soluções baseadas em software podem gerar lentidão na análise dessas transações.

Modem

A palavra “modem” é a contração das palavras modulador e demodulador. Essas palavras e sua consequente denominação advêm da função do aparelho que é transformar sinais analógicos em sinais digitais (modulação) e sinais digitais em sinais analógicos (demodulação). Nas redes de computadores, o modem é utilizado para interligar redes analógicas – normalmente as redes das operadoras de telefonia e dados – às redes internas das empresas e residências, que são digitais. Quando se contrata um link de internet, por exemplo, a operadora instala um modem, que fará a comunicação da rede da operadora com a do cliente, necessitando da transformação do sinal analógico vindo da operadora para um sinal digital da rede interna do cliente. Na Figura 14 pode-se observar um modem instalado em uma rede corporativa. Ele deve estar entre o roteador da empresa e o link de internet.

José Wagner Bürgert

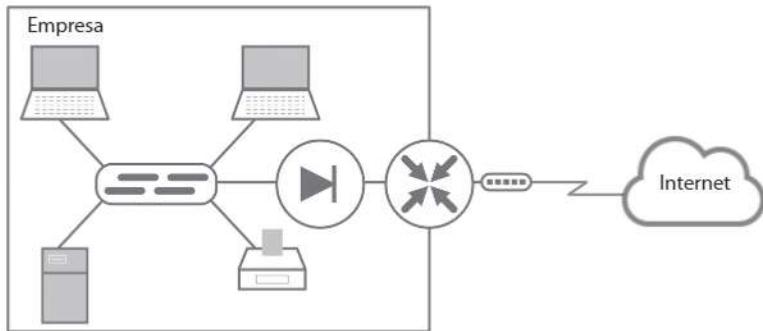


Figura 14 – Modem em uma rede corporativa.

Hoje em dia a função de modulação/demodulação, antes exclusiva aos modems geralmente se encontra em um equipamento único, principalmente em soluções residenciais, ou seja, os roteadores wireless estudados anteriormente também exercem a função de modem. Porém, ainda é possível encontrar instalações exclusivamente com modems, como o da Figura 15. Ele possui apenas duas portas de conexão, uma a que será conectado o link da operadora e outra onde será conectado o roteador da rede local.



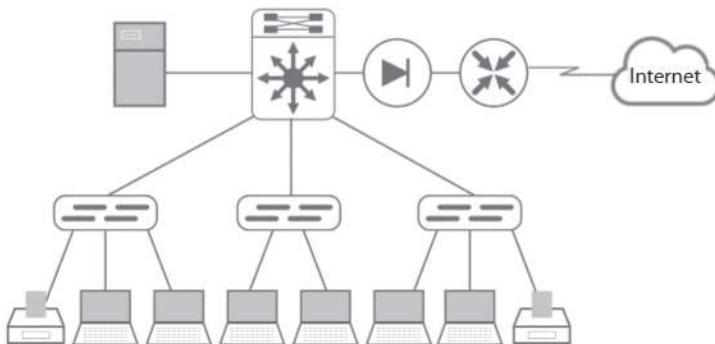
Figura 15 – Modem.

Fonte: Tp-link.

Switch multicamadas

Os switches multicamadas são equipamentos capazes de atuar não só como switch, mas como um roteador e até como firewall em um único equipamento. Os switches multicamadas devem ser utilizados em redes que precisam de mais de uma sub-rede. Em vez de serem instalados roteadores conectados aos diversos switches da rede, instala-se um switch multicamadas capaz de realizar switching e roteamento ao mesmo tempo. Não é somente o porte e a performance desse aparelho que o caracteriza como multicamadas, mas sim as funcionalidades que ele apresenta.

No desenho da rede da Figura 16, o switch multicamadas possui a importante função de interligar os demais switches da rede com o servidor e ainda fazer a interconexão com o firewall para a saída da rede para a internet.



José Wagner Bungart

Figura 16 – Switch multicamadas.

RECAPITULANDO

Neste capítulo foram apresentados os principais equipamentos de redes e suas funções. Foi possível reconhecer que o modo de operação dos hubs inviabiliza seu uso atualmente, por ser baseado em *broadcast*, inundando a rede com mensagens desnecessárias. Já os switches possuem uma maneira de armazenar o endereço dos computadores conectados a ele e, após memorizá-los, envia as mensagens apenas para o destino específico e necessário.

O capítulo tratou também das características e da aplicabilidade dos roteadores e dos access points, que são os equipamentos que fornecem conectividade sem fio para os computadores, laptops e outros dispositivos da rede. Foi estudada também a diferença entre um access point e um roteador wireless.

Foi possível verificar o que é um firewall e a diferença entre um firewall baseado em hardware e um baseado em software. Além disso, viu-se que os modems são equipamentos instalados pelas operadoras com a função de transformar uma transmissão analógica em digital.

Por fim, foi ensinado o que são os switches multicamadas, ou seja, equipamentos com múltiplas funções em um só hardware.

Exercícios

1. Explique a diferença básica no funcionamento de um hub e de um switch.
2. Descreva um cenário onde a utilização de hub em vez de switch não representaria um problema para a rede.
3. O que é a tabela SAT de um switch e o que ela contém?
4. Qual a principal função de um roteador? Onde ele pode ser utilizado?
5. Qual a principal função de um access point? Qual a diferença entre ele e um roteador wireless?
6. O que são firewalls? Explique a diferença entre os softwares e hardwares de firewall e em quais casos cada um deve ser utilizado.
7. O que é um modem? Explique como é utilizado.
8. O que são switches multicamadas? Dê alguns exemplos de uso desse equipamento.

As respostas dos exercícios deste livro estão disponíveis para *download* no seguinte *link*: https://www.senaispeditora.com.br/downloads/respostas/redes_computadores_respostas.pdf

3. Topologias de redes

Barramento

Anel

Estrela

Malha

Hierárquica

Uma topologia de rede é um desenho no qual é possível visualizar localidades, links, equipamentos WAN/LAN, posicionamento dos servidores, aspectos de segurança e grupos de usuários. Enfim, é um desenho que possibilita mapear e ter uma visão geral da rede.

No entanto, nem sempre apenas com uma topologia é possível ter todos os detalhes necessários. Geralmente, a rede é apresentada em uma topologia WAN, mostrando as interligações de filiais, matriz, internet e outros links externos que possam existir. Há também, em outras topologias mais detalhadas, informações sobre a LAN de cada localidade.

É importante ter bom senso ao se desenhar uma topologia. Ela não pode ser simples demais, ocultando informações importantes, nem detalhada demais, tornando o desenho poluído com informações inúteis para quem for utilizá-la.

A seguir tem-se a descrição dos principais tipos de topologias de rede.

Barramento

Em uma topologia em barramento, todos os elementos compartilham um só meio de transmissão, isto é, conforme indica o nome da topologia, os dispositivos são postos em paralelo, como se fossem “barras”. Então, assim como em um circuito elétrico ligado em paralelo, em uma rede dessa forma, caso algum

problema aconteça com uma conexão no barramento, a comunicação de todos os equipamentos será comprometida. Não existe um ponto central e cada elemento trabalha ora como transmissor, ora como receptor (Figura 1). Essa topologia é pouco utilizada atualmente por ser inflexível e muito suscetível a falhas, apesar do seu baixo custo de instalação. Outro problema surgiu com o passar do tempo, resultante do aumento da quantidade de computadores nas redes e da necessidade crescente de comunicação entre os dispositivos. Quando uma transmissão estava sendo realizada, nenhum outro computador poderia transmitir. Dessa forma, o número de retransmissões e, consequentemente, a lentidão na rede se tornaram um fator determinante para o fim desse tipo de ligação de rede, pois as empresas necessitavam de um desempenho melhor e de um menor número de falhas.

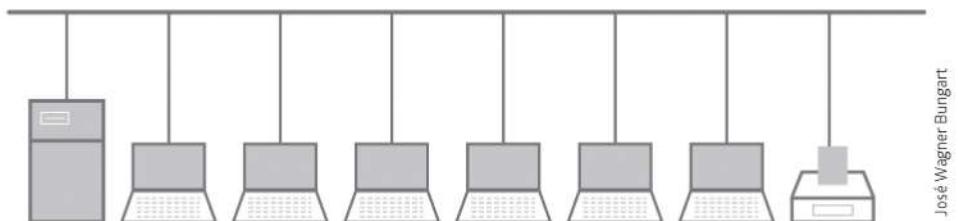


Figura 1 – Barramento.

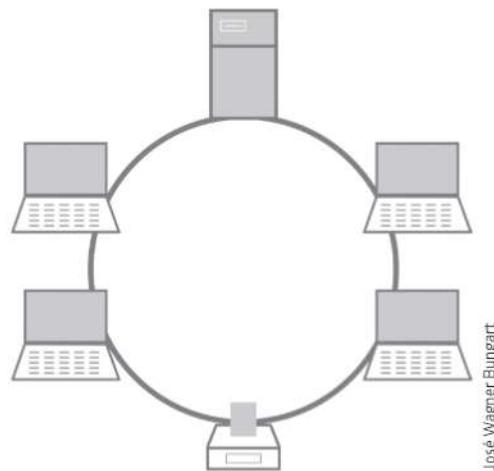
José Wagner Bungart

Anel

Uma topologia em anel é similar à topologia em barramento, mas possui as suas duas pontas conectadas, formando um circuito fechado, conforme pode ser visto na Figura 2. Isso permite redundância e continuidade, fazendo com que, caso algum problema aconteça em um elemento do anel, a comunicação não seja interrompida.

Essa topologia para redes LAN foi muito utilizada no passado com a rede Token Ring, desenvolvida pela IBM para funcionar com base em *tokens*, isto é, mensagens que circulavam pela rede indicando que o meio estava livre para a transmissão. Quando um determinado computador precisava transmitir, ele retirava o *token* do anel, transmitia o que fosse necessário e recolocava o *token* para que outro computador pudesse transmitir. O princípio desse tipo de comunicação teve sua inspiração nos rituais dos índios americanos que utilizavam um bastão, chamado de “bastão da fala”. Esse bastão circulava de mão em mão entre os índios, sentados em um círculo. Caso um dos índios tivesse algo para falar, ele segurava o bastão e falava o que desejava

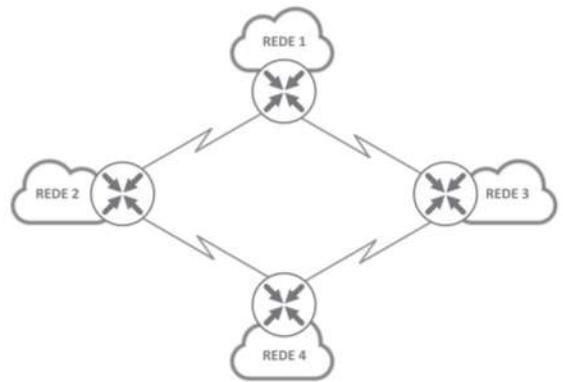
e, após sua fala, passava para o índio ao lado, que se tivesse algo para falar também retinha o bastão e falava. Caso não tivesse, passava para o próximo índio e assim sucessivamente. Para a tecnologia Token Ring, o bastão é uma mensagem do protocolo que informa que o meio de transmissão está livre.



José Wagner Bungart

Figura 2 – Anel: Rede LAN.

A topologia em anel também é utilizada em redes WAN, a diferença é que, em vez de os computadores se comunicarem como anteriormente, a comunicação agora é feita por meio de roteadores que interligam diferentes redes locais (Figura 3). Dessa forma, aumenta-se a disponibilidade da rede por meio de uma redundância de links, ou seja, caso um link fique indisponível, o tráfego pode ser encaminhado por outro link, já que a rede é circular.



José Wagner Bungart

Figura 3 – Anel: Rede WAN.

Estrela

A topologia em estrela possui um elemento central que faz a distribuição dos dados para todos os computadores, tornando-os, assim, independentes. Caso algum problema aconteça com um computador específico ou cabeamento, a comunicação dos demais computadores não é afetada. Porém, como toda informação transmitida passa por esse nó central, chamado também de concentrador, se algum problema acontecer com ele, a comunicação de toda a rede será comprometida (Figura 4).

Os equipamentos que podem ser utilizados nesse tipo de rede são os hubs e switches, sendo que atualmente os hubs quase não são mais utilizados pelos motivos já vistos no capítulo anterior.

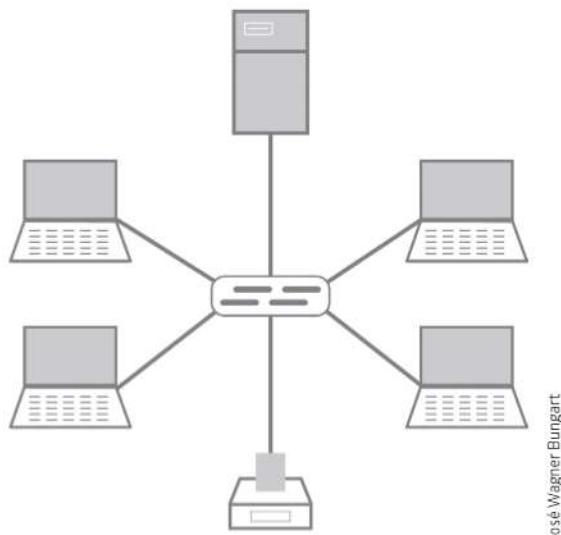


Figura 4 – Estrela.

Há ainda um segundo tipo de topologia em estrela, a chamada estrela estendida. Esse é o nome dado à rede que possui vários segmentos de rede estrela, capaz de aumentar as possibilidades de conexão de computadores e da área de abrangência da rede (Figura 5). A performance de uma rede estrela estendida é maior do que a de uma rede estrela, pois se algum problema ocorrer em um hub ou switch, somente aquele segmento será afetado.

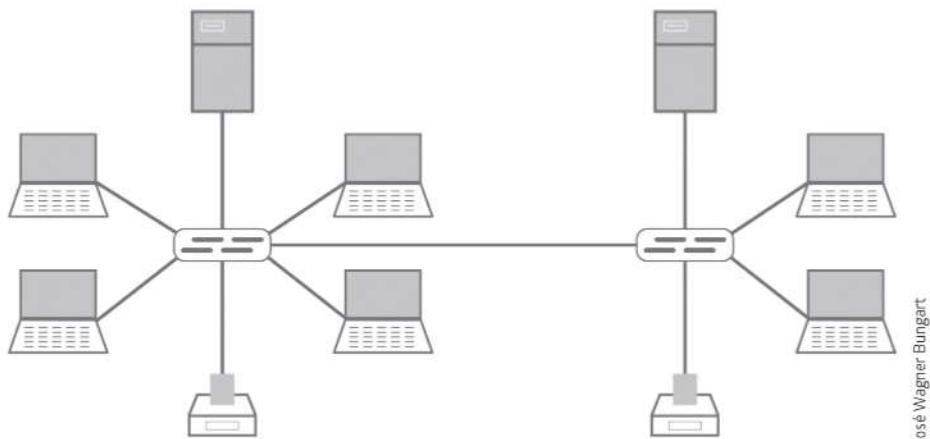


Figura 5 – Estrela estendida.

Essa topologia de rede em estrela é mais comum para redes LAN, já para redes WAN utiliza-se a nomenclatura *hub and spoke*. O princípio é o mesmo: um elemento central se comunica com vários outros elementos (Figura 6). No caso de rede WAN, esse elemento central geralmente é a matriz de uma empresa e os demais elementos, as filiais. São utilizados roteadores para a comunicação desse tipo de estrutura.

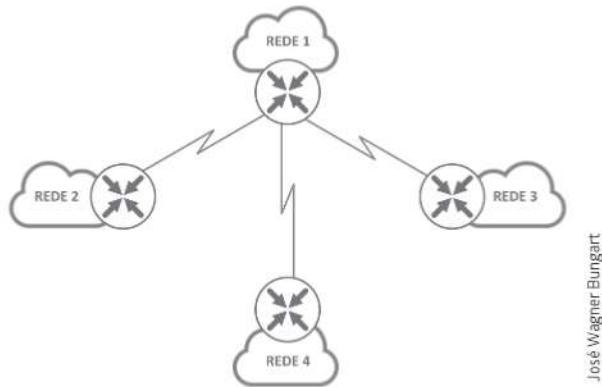


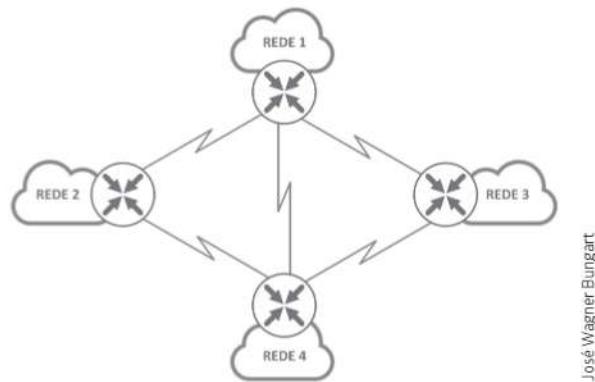
Figura 6 – Hub and Spoke.

Malha

A topologia em malha possui seus dispositivos conectados a mais de um elemento e é geralmente utilizada em redes WAN. Nesse tipo de topologia a disponibili-

dade da rede aumenta, visto que existem mais caminhos alternativos caso algum problema aconteça com a interconexão dos dispositivos. Quanto mais links redundantes ou caminhos alternativos existirem, maior será a disponibilidade da rede e maior o seu custo, consequentemente.

Dá-se o nome de malha parcial quando existem caminhos redundantes, mas nem todos os dispositivos estão conectados entre si. Já a malha total é uma topologia em que todos os elementos são interligados. Somente redes que precisam de uma disponibilidade muito alta, geralmente aplicações de missão crítica, utilizam esse tipo de organização. O custo de instalação e manutenção dessas redes é muito alto. No exemplo a seguir, na Figura 7, há uma rede WAN em malha parcial, pois a rede 2 não está conectada à rede 3.



José Wagner Bungart

Figura 7 – Malha parcial.

Hierárquica

Neste capítulo foi visto que as redes LAN possuem várias formas de conexão, isto é, podem desenhar diferentes topologias e promover um crescimento descontrolado e desestruturado. Com o objetivo de organizar melhor as redes e atribuir funções específicas a determinadas áreas delas, a Cisco Systems criou um modelo hierárquico de rede em camadas, deixando bem claras as funções de cada uma delas. Veja no Quadro 1 a descrição das camadas e sua nomenclatura.

Quadro 1 – Modelo hierárquico em camadas

Camada	Características
Acesso	É a camada onde estão os dispositivos dos usuários, como computadores, laptops e impressoras. Nessa camada também estão os access points. Ela se caracteriza por utilizar switches de baixo custo; suas portas devem suportar a velocidade requerida pelos elementos finais da rede. Sua interligação com a camada de distribuição deverá suportar o tráfego de todos os elementos vindos dela, para que não existam gargalos de capacidade na rede.
Distribuição	É a camada responsável por agregar as conexões dos diversos switches da camada de acesso. Normalmente nessa camada é feita uma segmentação da rede, com a divisão em redes locais virtuais, conceito que será visto mais adiante neste livro. No entanto, é por isso que nessa camada há a necessidade de roteamento entre redes. É um ponto de interconexão com redes externas, podendo ser conectados roteadores que farão links com a internet e outras redes. A camada de distribuição pode conectar os servidores locais da rede, caso a rede não precise de uma camada Core. Porém ela pode se conectar a uma camada Core, se houver. Na camada de distribuição devem ser configurados recursos de segurança por se tratar de um importante ponto de conexão de diversos segmentos da rede.
Core	Deve fornecer conexões de alta velocidade e com um alto grau de confiabilidade, pois fará a interconexão dos switches de distribuição. Deve ser tolerante a falhas e possuir redundância. À camada Core podem ser conectados os servidores da rede. Porém, deve-se avaliar a necessidade dessa camada nas redes, pois o custo dos equipamentos dessa camada é alto. Em grande parte dos casos, o uso somente das camadas de acesso e distribuição é suficiente para suportar todo o tráfego e prover as funcionalidades, segurança e desempenho requeridos.

Na Figura 8 há um exemplo de uma rede hierárquica com as três camadas: Core, distribuição e acesso. O exemplo mostra a redundância oferecida por essa rede.

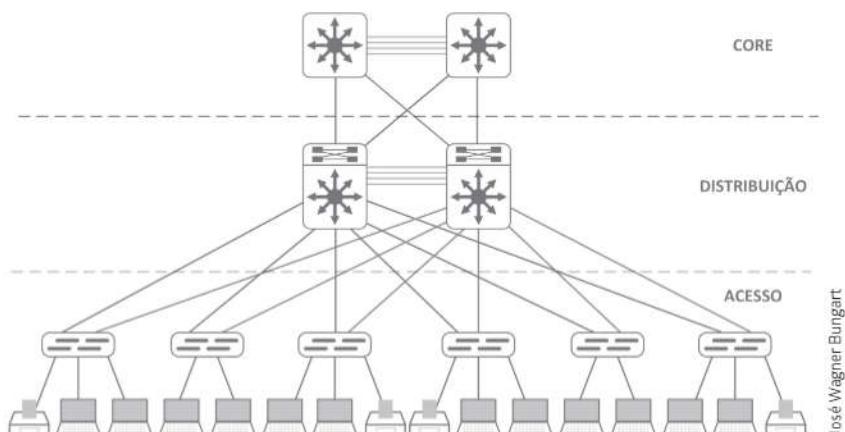


Figura 8 – Rede de topologia hierárquica.

RECAPITULANDO

Neste capítulo pôde-se observar que as topologias em barramento foram utilizadas no início das redes de computadores, mas por suas restrições de desempenho e por causa da grande quantidade de problemas apresentados, a evolução para a topologia em anel foi necessária, garantindo-se mais confiabilidade e aprimoramento do desempenho das redes. No entanto, a capacidade de expansão das redes também se tornou um fator limitador ao longo do tempo, agravado por problemas físicos, pois caso o anel se abrisse, toda a rede LAN seria interrompida.

As topologias em estrela surgiram, então, para resolver essas questões da rede em anel, com o conceito de um elemento central que concentrasse todas as conexões de uma rede LAN e as distribuisse para todos os computadores. Inicialmente, eram utilizados hubs para essa finalidade, mas atualmente são utilizados switches. Esse tipo de topologia não se limita a apenas um dispositivo central, pois pode haver interligações entre switches, configurando topologias em estrela estendida. As redes WAN que possuem esse mesmo conceito de elemento central – neste caso, roteadores – recebem o nome de *hub and spoke*.

Por fim, foi apresentada a topologia hierárquica, muito utilizada atualmente em redes de médio e grande porte. Desenvolvida pela Cisco Systems, apresenta três camadas com funções distintas para organizar melhor a rede e estabelecer características específicas para cada uso.

Exercícios

1. O que são topologias de redes?
2. Qual a principal restrição no funcionamento das topologias em barramento?
3. As topologias em anel podem ser utilizadas tanto para redes LAN como WAN? Explique.
4. Como é uma topologia em estrela? Descreva seu funcionamento e os equipamentos utilizados nas redes LAN e WAN.
5. O que são topologias em malha? Onde são mais utilizadas?
6. Explique o que são as redes LAN hierárquicas e o seu funcionamento básico.

As respostas dos exercícios deste livro estão disponíveis para *download* no seguinte *link*: https://www.senaispeditora.com.br/downloads/respostas/redes_computadores_respostas.pdf

4. Arquitetura de protocolos de redes

Modelo OSI

Arquitetura TCP/IP

Correlação entre modelos TCP/IP e OSI

O estudo de redes de computadores baseia-se no entendimento do modelo de referência OSI (Open System Interconnection) e suas camadas. Com esses conceitos em mente, o profissional de redes entenderá melhor como elas e a interação dos diversos protocolos existentes funcionam. Este capítulo mostra como o modelo OSI foi estruturado e como se dá a comunicação entre as camadas, além da correlação do modelo OSI com a arquitetura TCP/IP, que é o padrão mundialmente utilizado atualmente.

Modelo OSI

O modelo OSI foi formalizado pela ISO, em 1983, para padronizar a indústria de software e hardware de rede. Ele estabelece critérios para orientar os fabricantes e permitir maior compatibilidade e interoperabilidade entre as diversas tecnologias de redes.

O modelo OSI foi desenvolvido em camadas para facilitar a compreensão das funções, protocolos e equipamentos de cada camada. Como modelo de arquitetura de rede, o OSI também facilita a adoção de novas tecnologias, sem o usuário se preocupar em manter sistemas proprietários e restritos a determinados fabricantes. O modelo OSI, apesar de não ser tão usado hoje em dia, serviu como referência para diversas outras arquiteturas de rede. Nos próximos tópicos são descritas as características do modelo e seu funcionamento.

Camadas

As camadas são abstrações criadas no modelo OSI para diferenciar as funções ou partes de uma comunicação. Não se trata de uma separação física, mas sim de uma separação lógica das funcionalidades e protocolos necessários para a comunicação.

A comunicação entre dois sistemas sempre começa no sentido da camada mais alta do sistema transmissor, percorre todas as suas camadas pelo meio (físico ou wireless), e alcança de alguma maneira o sistema receptor pela camada física, percorrendo em seguida todas as outras camadas e alcançando a aplicação do receptor.

Cada camada adiciona o seu cabeçalho com as informações pertinentes ao protocolo utilizado, passando para a camada imediatamente acima ou abaixo as informações necessárias para que a comunicação fluia corretamente, conforme pode se ver a seguir em Encapsulamento de dados.

No modelo OSI foram definidas sete camadas:

- aplicação;
- apresentação;
- sessão;
- transporte;
- rede;
- enlace;
- física.

Cada uma delas representa uma etapa e mecanismo de codificações e interpretações que garantem o funcionamento das redes.

Encapsulamento de dados

A divisão em camadas do modelo OSI cria a necessidade de cada uma delas inserir informações pertinentes a si próprias, por exemplo endereços e controles. Quando uma camada adiciona seu cabeçalho a uma mensagem, dá-se o nome de encapsulamento.

A mensagem de uma determinada camada ainda sem ter aplicado seu cabeçalho é chamada de SDU (Service Data Unit), a qual contém os dados vindos das

camadas anteriores e o cabeçalho da camada imediatamente acima. A partir do momento em que a camada adiciona o seu cabeçalho, chamado de PCI (Protocol Control Information), a mensagem passa a se chamar PDU (Protocol Data Unit). Para ilustrar esse conceito, observe a Figura 1.

A inclusão dos cabeçalhos obviamente aumenta o tamanho dos dados a serem transmitidos. Por isso, uma preocupação constante é criar e utilizar cabeçalhos que sejam pequenos, mas que garantam a confiabilidade da comunicação, pois apesar de cabeçalhos muito curtos poderem ser transmitidos mais rapidamente, eles podem não ser suficientes para garantir a entrega segura dos dados. Por outro lado, cabeçalhos grandes podem ter informações excessivas, tornando-os longos e desnecessários em determinados casos. Dessa forma, a escolha dos protocolos, e consequentemente dos cabeçalhos utilizados, deve ser feita de maneira otimizada para cada necessidade de comunicação.

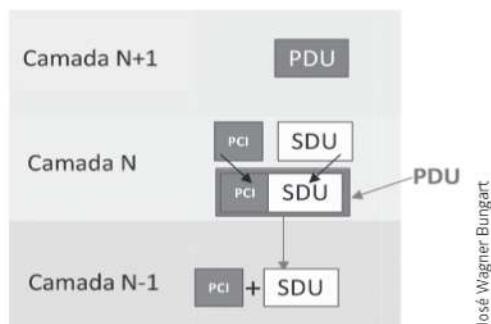


Figura 1 – Encapsulamento de dados.

Comunicação entre camadas

Um princípio básico do modelo OSI é que as camadas devem possuir uma forma padronizada de comunicação entre elas, tanto acima como abaixo, pois isso permite a completa compatibilidade entre os protocolos das camadas vizinhas.

Conforme descrito no tópico anterior, cada camada insere um cabeçalho com as informações pertinentes a ela e que serão utilizadas pela mesma camada no destinatário. Para entender melhor as funções de cada camada e como a comunicação acontece entre elas, analisa-se um exemplo de um computador utilizando uma aplicação muito comum atualmente: uma navegação em um site da internet.

Esse exemplo é de uma arquitetura TCP/IP e não do modelo OSI puramente, mas como se tornou um modelo de referência e é raramente utilizado em sua forma original, será mais fácil a compreensão do procedimento de camadas.

Exemplos

1. A interação do usuário com uma aplicação é o início da comunicação. No exemplo, há a necessidade de o usuário digitar o endereço do site que deseja acessar – por exemplo: www.sp.senai.br – utilizando um navegador de internet, como o Google Chrome, Microsoft Internet Explorer ou Mozilla Firefox. O dado dessa comunicação é, na verdade, o endereço do site, e a função da camada aplicação do dispositivo é inserir seu cabeçalho para que possa ser interpretado pela camada aplicação do servidor (Figura 2). No Capítulo 5 a camada aplicação, alguns de seus protocolos, o funcionamento e o cabeçalho nela inserido para diferentes funções serão estudados.

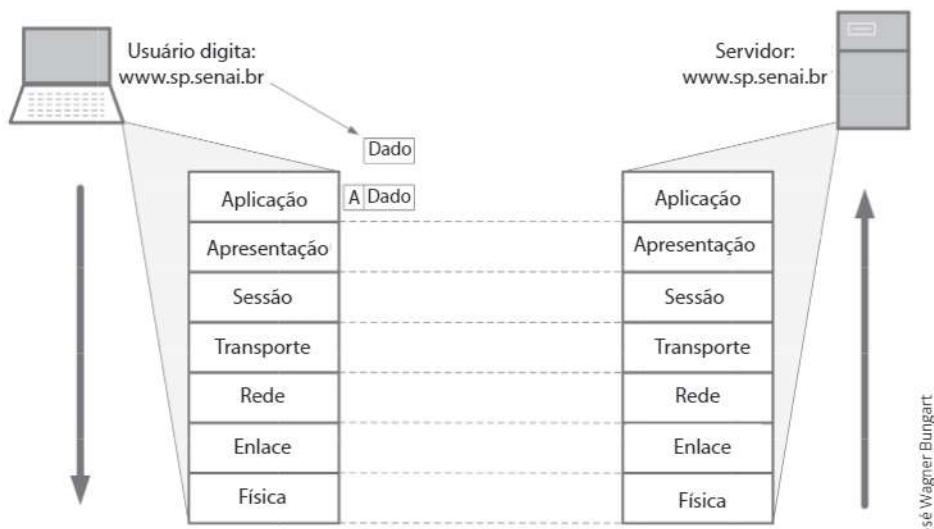


Figura 2 – Camada aplicação (transmissão).

2. A camada apresentação converte os dados da aplicação em uma linguagem menos complexa para o computador. A cada camada que se desce no modelo OSI, maior a facilidade de a máquina interpretar, mas, ao mesmo tempo, mais difícil fica para a compreensão humana. A camada apresentação é responsável por tornar possível a

comunicação entre computadores e estruturas de dados diferentes para que uma mesma aplicação possa ser interpretada por computadores com hardwares diversos. É, por exemplo, a conversão do PDU da camada aplicação em caracteres ASCII: no cabeçalho da camada apresentação deve ser inserido outro cabeçalho que indique o tipo de codificação utilizada (Figura 3).



Figura 3 – Camada apresentação (transmissão).

SAIBA MAIS

Os Caracteres ASCII (American Standard Code for Information Interchange) foram criados em 1960, por Robert W. Bemer, para padronizar a forma como os computadores interpretam os caracteres alfanuméricos (letras, números, sinais e acentos), com o objetivo de que diferentes fabricantes de computadores conseguissem utilizar o mesmo código.

3. A camada de sessão estabelece, gerencia e termina as sessões entre as aplicações de um computador com outros diferentes computadores e servidores. Por exemplo, quando utilizamos um site de um banco, no qual precisamos nos autenticar fornecendo número de agência, conta bancária, senha e outros controles solicitados pelo banco, após a autenticação estabelece-se uma sessão entre o computador-cliente e o servidor do banco, que pode ser interrompida de diversas formas,

seja ela o clique do usuário em um botão que finaliza a sessão, seja o tempo decorrido daquela sessão ou ainda por uma solicitação do servidor. Para isso ocorrer, a camada sessão possui mecanismos de sincronização e segurança das tarefas. Esse controle é inserido no cabeçalho da camada de sessão (Figura 4).



Figura 4 – Camada sessão (transmissão).

4. Na camada transporte ocorre a fragmentação dos dados vindos das camadas superiores, ou seja, a sua divisão em unidades menores, se necessário, para serem transmitidos pela rede. Nessa camada são realizados o controle de fluxo, a ordenação dos pacotes e a correção de erros e é onde o PDU recebe o nome de “segmento”. No Capítulo 6 a camada transporte será estudada a fundo e será possível observar que ela pode garantir o correto recebimento dos segmentos com a implementação de mecanismos de controle, como é o caso do TCP (Transmission Control Protocol), ou simplesmente enviar os dados e não ter a garantia de entrega, no caso do protocolo UDP (User Datagram Protocol). A implementação de uma ou outra forma é posta em prática no cabeçalho dessa camada (Figura 5). No caso de uma navegação web, como um site da internet, o protocolo utilizado é o TCP, pois há a necessidade de uma confirmação de entrega dos pacotes.



Figura 5 – Camada transporte (transmissão).

5. A camada rede tem como função possibilitar a transferência de informações entre redes distintas. Faz a escolha do caminho para alcançar a rede de destino por meio de uma “tabela de roteamento”, que deverá indicar por qual caminho os pacotes, nome do PDU dessa camada, deverão seguir (Figura 6). Na camada rede são utilizados endereços lógicos, sendo o mais comum atualmente o endereço IP. Com base nesse endereçamento, a camada rede poderá escolher o caminho que deverá seguir para chegar ao destino. Por exemplo, para a navegação em um site da internet chegar até o servidor, é necessário o endereço IP de destino, nesse caso o do servidor. Os roteadores são os responsáveis por levar esses dados por um caminho que chegue até o servidor onde o site está hospedado.



Figura 6 – Camada rede (transmissão).

6. O PDU da camada enlace recebe o nome de quadro. Essa camada é responsável pelo estabelecimento e término de conexão sobre a camada física, montagem e delimitação de quadros e controle de erro. A camada enlace recebe os dados vindos da camada rede com seu endereçamento lógico, endereço IP, por exemplo, e o associa a endereços físicos, endereço MAC. Nessa camada existe um campo adicional no final do PDU (Figura 7), e nesse campo são inseridas informações para que sejam possíveis operações de detecção e correção de erros. Vale ressaltar que essa é uma operação que ocorre apenas na rede local, somente para os dados alcançarem o seu destino dentro da mesma rede. No exemplo aqui analisado de um site de internet, o computador de origem não precisa conhecer o endereço MAC do servidor, mas apenas os elementos da sua própria rede, como o roteador de saída para a internet.

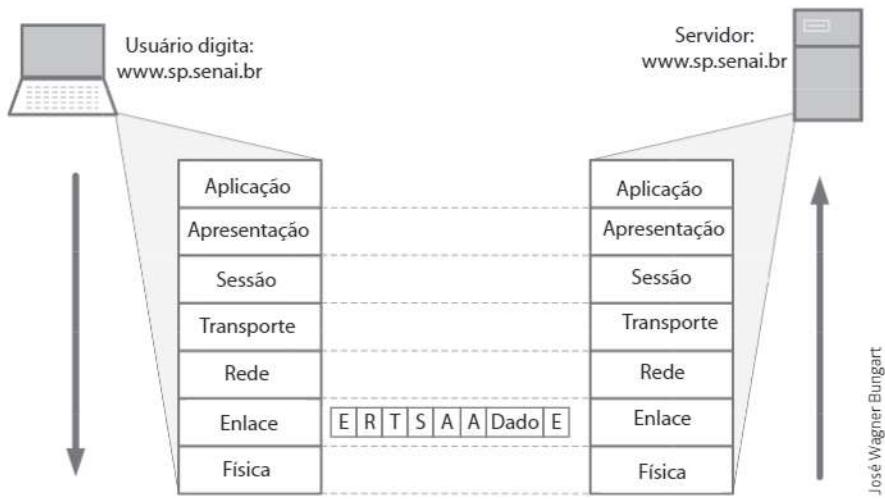


Figura 7 – Camada enlace (transmissão).

7. A camada física trata da transmissão dos dados brutos, em bits, por um determinado meio de transmissão. Essa camada define as características físicas dos meios de transmissão. Da mesma maneira que na camada enlace, existe um campo final utilizado pelos protocolos para realizar a detecção e correção de possíveis erros antes que os bits sejam transmitidos pela rede (Figura 8).

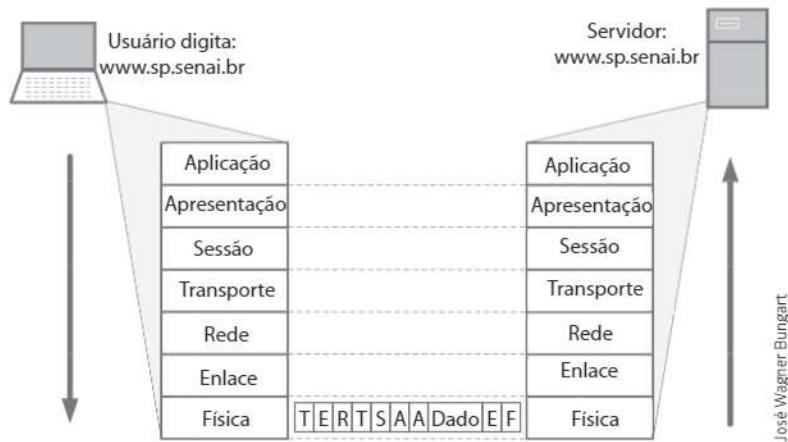


Figura 8 – Camada física (transmissão).

8. Depois de transmitida a sequência binária do originador, o destinatário a recebe por sua camada física, podendo ser por meio de cabos ou pelo ar, e caso seja utilizada uma rede wireless, ele analisa o cabeçalho final enviado para certificar que não houve erros na transmissão (Figura 9), retira ambos, cabeçalho e final do PDU, e encaminha para sua própria camada enlace.

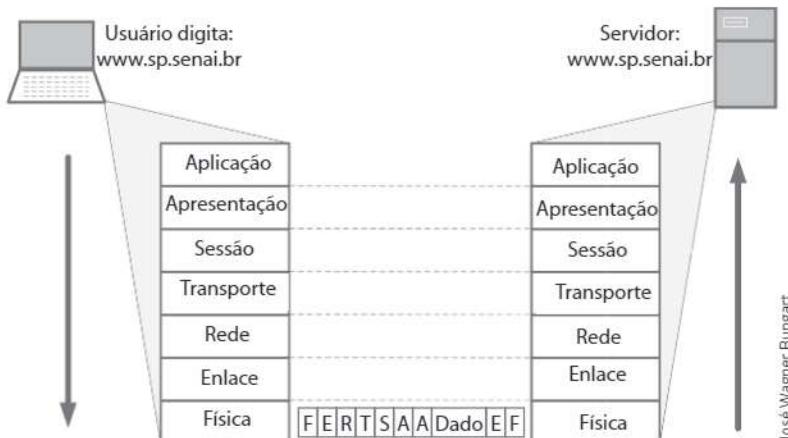


Figura 9 – Camada física (recepção).

9. A principal função é transformar os dados recebidos de um canal de transmissão bruto – a camada física – em um meio livre de erros de transmissão. Analisa se o quadro é destinado a ele, e, caso não

seja, simplesmente ignora o quadro, descartando-o. Caso seja o destinatário correto, verifica a integridade do quadro, retira cabeçalho e mensagem final, encaminhando o PDU para a camada imediatamente acima, a camada rede (Figura 10).

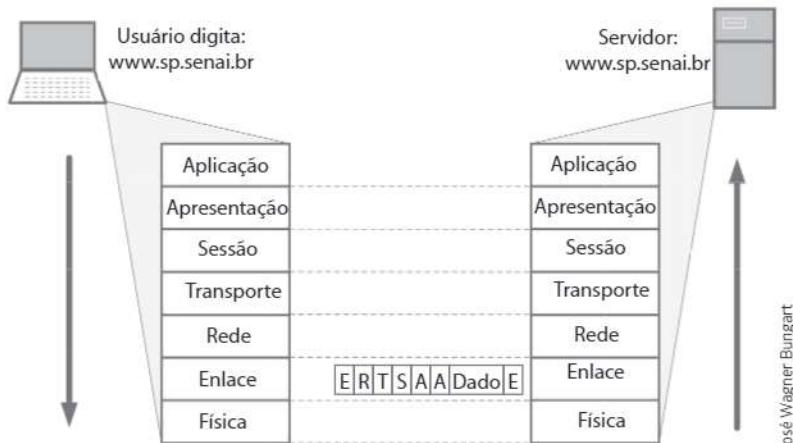


Figura 10 – Camada enlace (recepção).

10. A camada rede recebe o pacote da camada enlace, confere o endereçamento lógico, retira o cabeçalho e encaminha para a camada transporte (Figura 11).



Figura 11 – Camada rede (recepção).

11. Os pacotes transmitidos da camada rede podem ter sofrido fragmentação na origem ou em algum outro equipamento rede. Cabe à camada transporte reordenar esses pacotes, caso tenham chegado em uma ordem diferente da original. Conforme visto anteriormente, nessa camada também é possível implementar um controle de recebimento dos segmentos, utilizando TCP por exemplo. Dessa forma, a camada transporte do receptor envia uma resposta para o transmissor informando o correto recebimento de cada segmento. Caso algo de errado tenha ocorrido com um dos segmentos, ele pode ser retransmitido individualmente. Essa análise é feita no cabeçalho da camada transporte (Figura 12). Quando todos os segmentos estiverem corretos, são reagrupados em um só e enviados para a camada sessão.

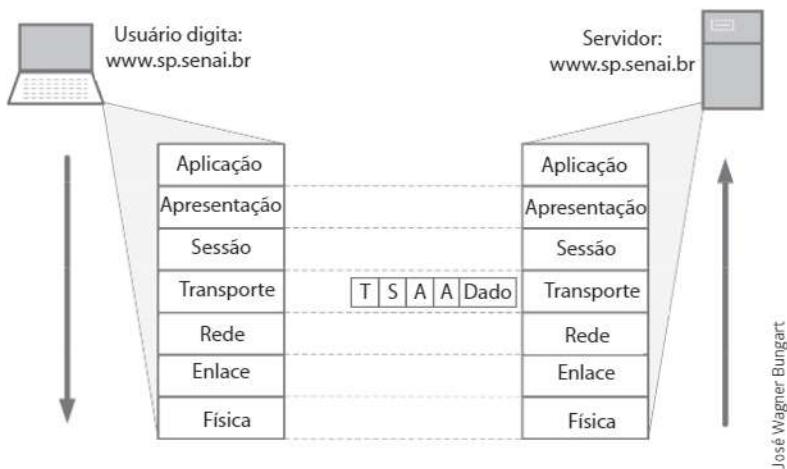


Figura 12 – Camada transporte (recepção).

12. No momento em que a camada sessão recebe os primeiros segmentos da camada transporte, um “círculo virtual” é criado entre origem e destino, estabelecendo uma sessão entre origem e destino, por isso o nome da camada. Em seu cabeçalho, conforme a Figura 13, estão as informações que permitem, além do estabelecimento, a manutenção e a finalização da sessão.



Figura 13 – Camada sessão (recepção).

13. Na camada apresentação do receptor os dados são convertidos de volta para a linguagem da aplicação, seu cabeçalho retirado e o PDU enviado à camada aplicação (Figura 14).



Figura 14 – Camada apresentação (recepção).

14. Finalmente os dados chegam até a camada aplicação do servidor, podendo realizar suas verificações e examinar o cabeçalho da mensagem (Figura 15), respondendo ao originador da transmissão, que, no exemplo, é um servidor web. E então, por fim, a resposta é dada e se concretiza o envio da página requisitada pelo usuário.

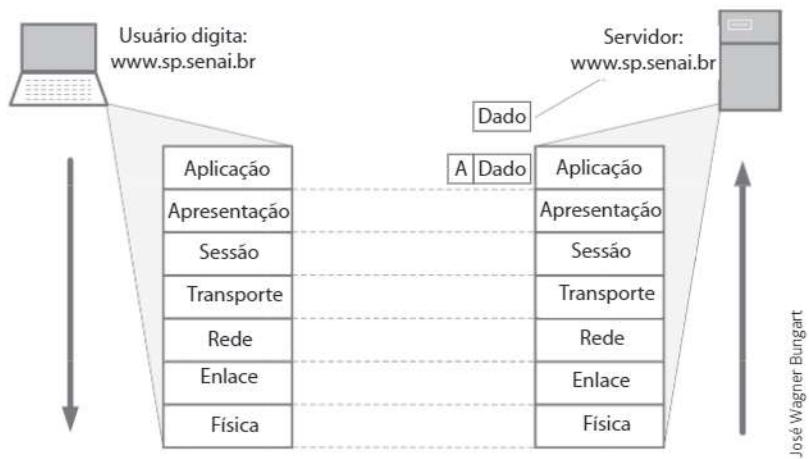


Figura 15 – Camada aplicação (recepção).

Pode-se notar que o simples processo de acessar um site passa por diversas etapas, codificações e processos no modelo OSI. É por isso que ele não é utilizado atualmente. Essa estrutura inicial e o mecanismo de funcionamento foi aproveitado, porém aprimorado, simplificado e hoje tem-se uma rede mais tecnológica e veloz. Essa simplificação pode ser vista no tópico a seguir.

SAIBA MAIS

Para entender melhor a comunicação em camadas do modelo OSI, veja a animação disponível em: www.senaispeditora.com.br/catalogo/informacoes-tecnologicas-tecnologia-da-informacao/redes-de-computadores-fundamentos-e-protocolos/

Arquitetura TCP/IP

A arquitetura TCP/IP teve seu início com a ARPANET, uma rede de pesquisa patrocinada pelo Departamento de Defesa (DoD) que interligava diversas universidades e órgãos públicos dos Estados Unidos. Essa rede tinha a característica de poder conectar várias redes distintas de maneira uniforme, o que deu origem, posteriormente, à arquitetura TCP/IP. O nome TCP/IP vem dos dois principais protocolos utilizados, o TCP da camada de transporte e o IP da camada de rede. Atualmente o TCP/IP é a arquitetura mais utilizada mundialmente, seja em redes locais, seja na internet. Na verdade, a internet surgiu da ARPANET e não seria a grande rede mundial se não fosse pela flexibilidade e facilidade de interconexão existente no TCP/IP.

Segundo Tanenbaum (2011), a arquitetura TCP/IP é definida em quatro camadas:

- aplicação;
- transporte;
- inter-redes (Rede);
- host/rede.

Diferentemente do modelo OSI, as camadas do TCP/IP comportam-se de maneira mais ágil e simplificada, conforme demonstrado no tópico a seguir.

Correlação entre modelos TCP/IP e OSI

A arquitetura TCP/IP agrupa as três camadas mais altas – aplicação, apresentação e sessão – em uma só, chamada de aplicação. Isso ocorre porque geralmente quem programa as aplicações de rede nessa arquitetura já possui a preocupação de, além de desenvolver a aplicação em si, fazer sua conversão de dados e gerenciar as sessões necessárias para o funcionamento da aplicação. Assim, em uma única camada várias etapas se realizam.

A camada transporte do TCP/IP tem as mesmas funções da camada transporte do modelo OSI, da mesma maneira que a camada rede. Alguns autores utilizam a nomenclatura “inter-redes” para denominar essa camada no TCP/IP; no entanto, neste livro será adotado o termo camada rede por ser o termo mais utilizado.

Já para as últimas duas camadas do modelo OSI, enlace e física, há a fusão em uma só camada na arquitetura TCP/IP, tornando-se a camada “host/rede” para alguns autores, ou “acesso à rede” para outros. Host é um termo utilizado em redes de computadores para designar qualquer dispositivo conectado à rede, não importando se é um computador, notebook, impressora e outros. Na verdade, na definição da arquitetura TCP/IP não existe uma especificação clara sobre os protocolos e o funcionamento dessa camada. A seguir, a descrição de Andrew Tanenbaum (2001, p. 47) referente à camada:

Abaixo da camada inter-redes, encontra-se um grande vácuo. O modelo de referência TCP/IP não especifica muito bem o que acontece ali, exceto o fato de que o *host* tem de se conectar à rede utilizando algum protocolo que seja possível enviar pacotes IP. Esse protocolo não é definido e varia de *host* para *host* e de rede para rede. Os livros e a documentação que tratam do modelo TCP/IP raramente descrevem esse protocolo.

Neste livro as camadas física e enlace são descritas juntas, no capítulo 8, assim como na arquitetura TCP/IP, abordando os principais protocolos de cada uma delas.

Na Figura 16 pode-se ver a correlação entre as camadas do modelo OSI e a arquitetura TCP/IP, com especial destaque para a junção das camadas aplicação, apresentação e sessão em uma só nas camadas altas, e da enlace e física nas camadas baixas.

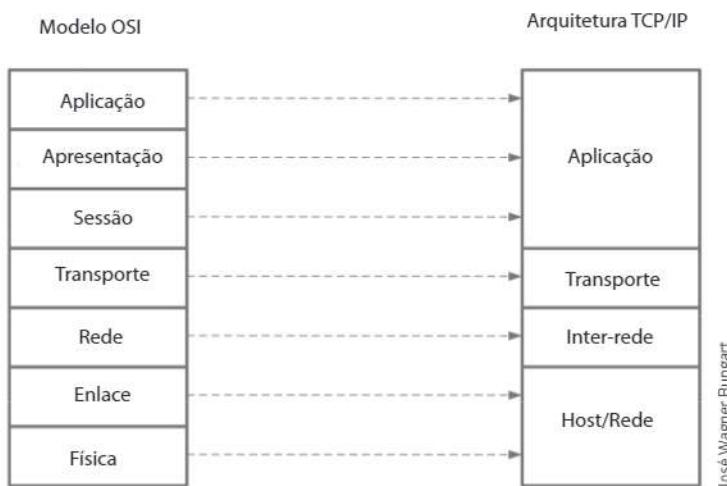


Figura 16 – Correlação OSI x TCP/IP.

RECAPITULANDO

Neste capítulo foi apresentado um importante tema no estudo das redes de computadores, o modelo OSI e a arquitetura TCP/IP. A compreensão desses modelos é fundamental para que o profissional consiga entender o funcionamento das redes, seus equipamentos e protocolos, pois com esses conhecimentos saberá como a informação flui de um computador para outro, como são endereçadas as aplicações e dispositivos. O modelo OSI é atualmente utilizado apenas como referência de arquitetura no estudo das redes, porque o que realmente é utilizado largamente nas redes de todo o mundo é o modelo de arquitetura TCP/IP, a ser detalhado nos capítulos seguintes.

Exercícios

1. O que motivou a criação do modelo OSI?
2. Por que o modelo OSI foi criado em camadas?
3. Cite as sete camadas do modelo OSI.
4. Explique o que é encapsulamento de dados.
5. Explique o que são SDUs, PCIs e PDUs.
6. Por que a arquitetura TCP/IP possui menos camadas do que o modelo OSI e quais são as principais diferenças entre elas?

As respostas dos exercícios deste livro estão disponíveis para *download* no seguinte *link*: https://www.senaispeditora.com.br/downloads/respostas/redes_computadores_respostas.pdf

5. Camada aplicação

Protocolos

O tema de estudo deste capítulo é a camada aplicação. Conforme visto no capítulo anterior, na arquitetura TCP/IP essa camada engloba as três camadas altas do modelo OSI: aplicação, apresentação e sessão. São apresentados a seguir alguns dos principais protocolos, as funções e características, com o objetivo de permitir a execução de alguns experimentos simples de laboratório, consolidando os conhecimentos e agregando uma visão prática do funcionamento dessa camada.

Protocolos

HTTP – Hypertext Transfer Protocol

O protocolo HTTP, Hypertext Transfer Protocol, ou em português, Protocolo de Transferência de Hipertexto, RFC 2616, tem seu funcionamento baseado no procedimento de requisição e resposta. Isto é, o cliente é responsável por enviar as requisições de conteúdo e o servidor, as respostas, como arquivos HTML, por exemplo (Figura 1). Esse protocolo é o maior responsável pela comunicação na internet atualmente, uma vez que codifica endereços escritos em uma linguagem acessível ao computador.



Figura 1 – Requisição HTTP.

O HTTP utiliza o conceito de estabelecimento de sessões, iniciadas pelos clientes por meio de portas (*sockets*) de conexão. Geralmente são utilizadas as portas 80 ou 8080. Essas portas, conforme explicará o próximo capítulo – Camada transporte – permitem que toda a comunicação seja feita por trocas de mensagens, como demonstrado no Exemplo 1. Em várias partes deste livro o Wireshark será utilizado para demonstrar o funcionamento dos protocolos e analisar informações contidas nos cabeçalhos. O Wireshark é um software de captura de pacotes, gratuito, muito utilizado pelos administradores de redes para a captura e análise dos pacotes trafegados na rede. Ou seja, o software identifica os pacotes de informação contidos na rede nas diversas camadas, e permite ao usuário a visualização e análise desses.

No Exemplo 1, pode-se perceber que um usuário está com o IP 192.168.0.3 configurado em seu computador (campo “source”) e está tentando acessar o site www.sp.senai.br localizado no IP 201.16.211.70 (campo “destination”) utilizando o protocolo HTTP. A ação dessa requisição é um “GET”, ou seja, o cliente está solicitando a página HTTP do servidor, a porta TCP do servidor é a 80 “Dst Port”, com uma porta aleatória na sua origem, 52095 “Src Port”. Podemos observar também, no campo “host”, que o site requisitado foi www.sp.senai.br (Figura 2).

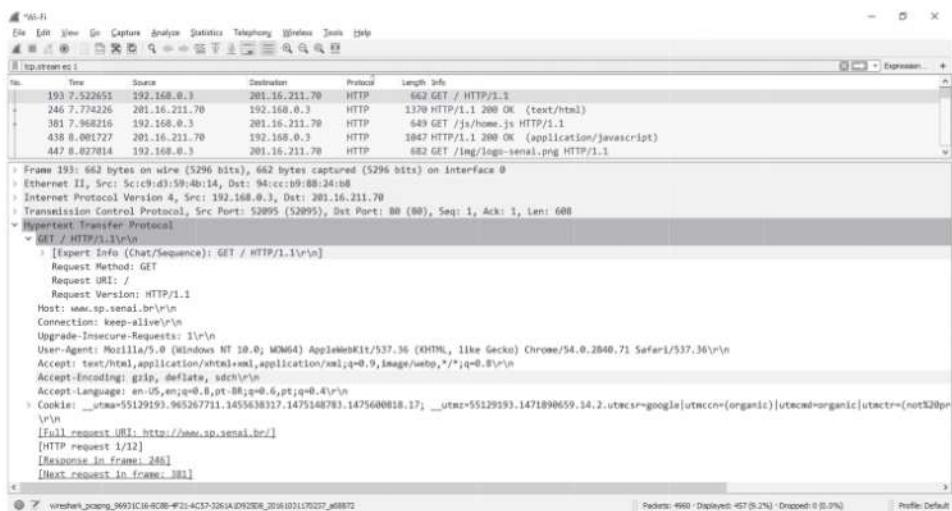


Figura 2 – GET HTTP.

Feita a requisição, a próxima mensagem será enviada do servidor para o cliente, ou seja, do IP 201.16.211.70 como origem (campo “source”) e IP 192.168.0.3 como destino (campo “destination”). Agora, a porta de origem será a 80 e a de destino 52095, a mesma que havia solicitado os dados do site. Dessa forma, tanto o cliente como o servidor trocarão uma série de mensagens até que o site esteja completamente carregado no navegador do cliente (Figura 3).

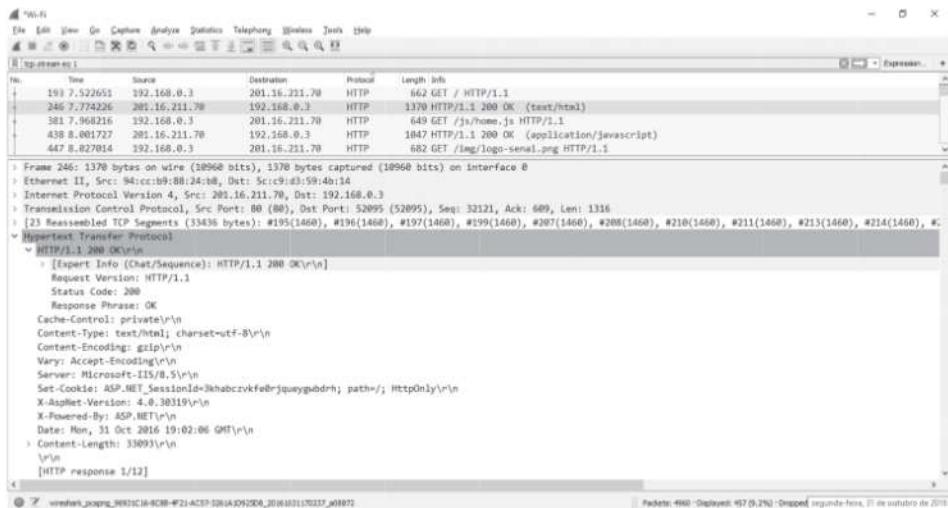


Figura 3 – Resposta HTTP.

Hypertext Transfer Protocol Secure – HTTPS

O protocolo HTTPS, Hypertext Transfer Protocol Secure, ou em português Protocolo de Transferência Segura de Hipertexto, é utilizado para conexões seguras na internet. Ele foi definido pela RFC 2660 e utiliza, por padrão, a porta 443. Um problema crítico do HTTP é que ele pode, quando interceptado, ser facilmente analisado e informações sigilosas, como nomes de usuários e senhas para um determinado sistema, podem cair nas mãos erradas. Por esse motivo foi desenvolvido o protocolo HTTPS com o intuito de prover uma maior segurança nas transações utilizando redes. O servidor insere uma criptografia, ou seja, um código que somente o servidor e o cliente reconhecerão, aumentando muito a segurança daquela comunicação. O HTTP utiliza SSL (Secure Sockets Layer) ou TLS (Transport Layer Security) para criar um túnel criptográfico entre o servidor e o cliente.

Na tela da captura da Figura 4, pode-se verificar a troca de mensagens entre um cliente com o IP 192.168.0.3 e um servidor com o endereço 31.13.80.36. Esse servidor é o site do Facebook. Como o Facebook criptografa o tráfego de dados de seus usuários, é possível ver as mensagens utilizando o protocolo TLS. Inicialmente, o cliente envia uma mensagem para sinalizar que deseja entrar na página segura (Client Hello), recebe um mensagem de resposta (Server Hello) e posteriormente um certificado com as credenciais que devem ser utilizadas. O cliente envia seus dados de acordo com o certificado enviado e é validado pelo servidor. Finalmente, na mensagem identificada com o número 159, a aplicação estará disponível para o usuário receber dados (Application Data). Essa transação é totalmente invisível para o usuário e o único indício que ele recebe, dependendo da versão do navegador que está utilizando, é um cadeado fechado em algum lugar na tela. Isso o informa que se trata de uma conexão segura. Depois desse procedimento, o protocolo encapsulado pelo TLS é o HTTP e os dados estão criptografados.

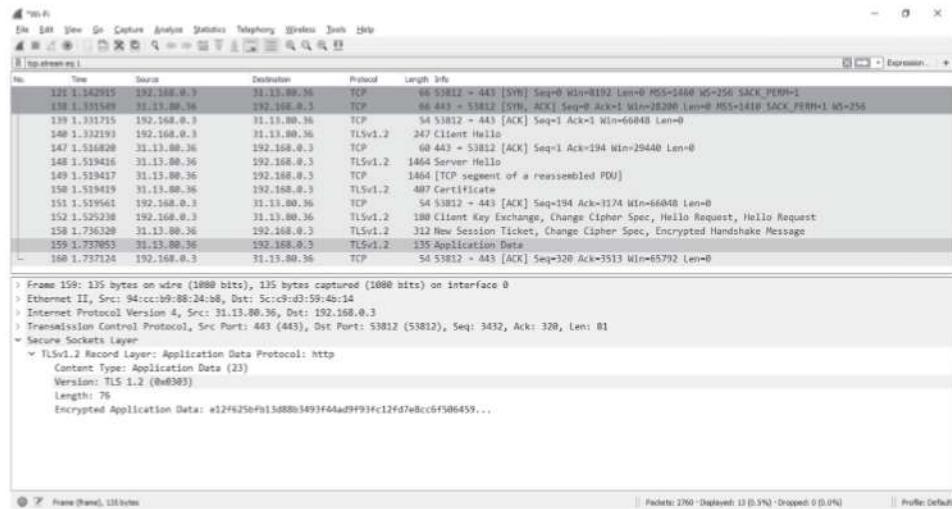


Figura 4 – HTTPS com o uso de TLS.

File Transfer Protocol – FTP

O FTP, File Transfer Protocol, em português Protocolo de Transferência de Arquivo, é um protocolo criado para a transferência de arquivos. Descrito na RFC 959, ele utiliza a porta TCP 20 para a conexão de dados e a 21 para a conexão de controle. Aqui, é importante saber quais são as portas, mas não necessariamente

compreendê-las pois, no Capítulo 6 será apresentada a definição das portas TCP. O FTP é muito utilizado para a transferência de arquivos entre as estações clientes e os servidores que não possuam outros mecanismos para a cópia de arquivos, isto é, que estão longe um do outro ou que sejam impossibilitados de fazer transferência on-line pelo tamanho do arquivo requisitado.

Trivial File Transfer Protocol – TFTP

O TFTP, Trivial File Transfer Protocol, ou Protocolo de Transferência Comum de Arquivo, é um protocolo da camada aplicação também muito utilizado em redes de computadores, principalmente por ser uma maneira de copiar arquivos para equipamentos de redes. Isto é, um servidor TFTP armazena o sistema operacional e arquivos de configuração dos equipamentos instalados, atuando como uma forma simples de backup e recuperação de uma rede em caso de falhas, além de ser muito útil também nas atualizações de software. O TFTP foi definido na RFC 959 e utiliza a porta UDP 1350.

Visto os principais protocolos da camada aplicação, e lembrando que ela, no TCP/IP, equivale às três primeiras camadas do modelo OSI – aplicação, apresentação e sessão – pode-se passar para o conteúdo relativo à camada transporte.

RECAPITULANDO

A camada aplicação é a camada com a qual o usuário interage com mais frequência, desta forma o entendimento do seu funcionamento se torna mais simples. Neste capítulo foram apresentados os quatro protocolos dessa camada, mas na verdade são inúmeras as aplicações e, consequentemente, os protocolos de aplicação. À medida que se aprofundam os estudos em redes de computadores, ampliam-se os conhecimentos dos protocolos dessa camada. Por enquanto, já se sabe que o HTTP é o protocolo mais utilizado para a navegação na internet; a implementação de segurança no HTTP, que é o HTTP com sua criptografia em SSL e TLS, HTTPS; como também os dois protocolos para transferência de arquivos, o FTP e o TFTP, que certamente são muito úteis no dia a dia do profissional de redes de computadores.

Exercícios

1. O protocolo HTTP é muito utilizado na internet. Explique de forma resumida o seu funcionamento, mencionando, principalmente, como são feitas as requisições e a utilização de portas.
2. O que difere o protocolo HTTPS do HTTP?
3. Explique como os protocolos FTP e TFTP são utilizados.

As respostas dos exercícios deste livro estão disponíveis para *download* no seguinte *link*: https://www.senaispeditora.com.br/downloads/respostas/redes_computadores_respostas.pdf

6. Camada transporte

Definição

Protocolo TCP – Transmission Control Protocol

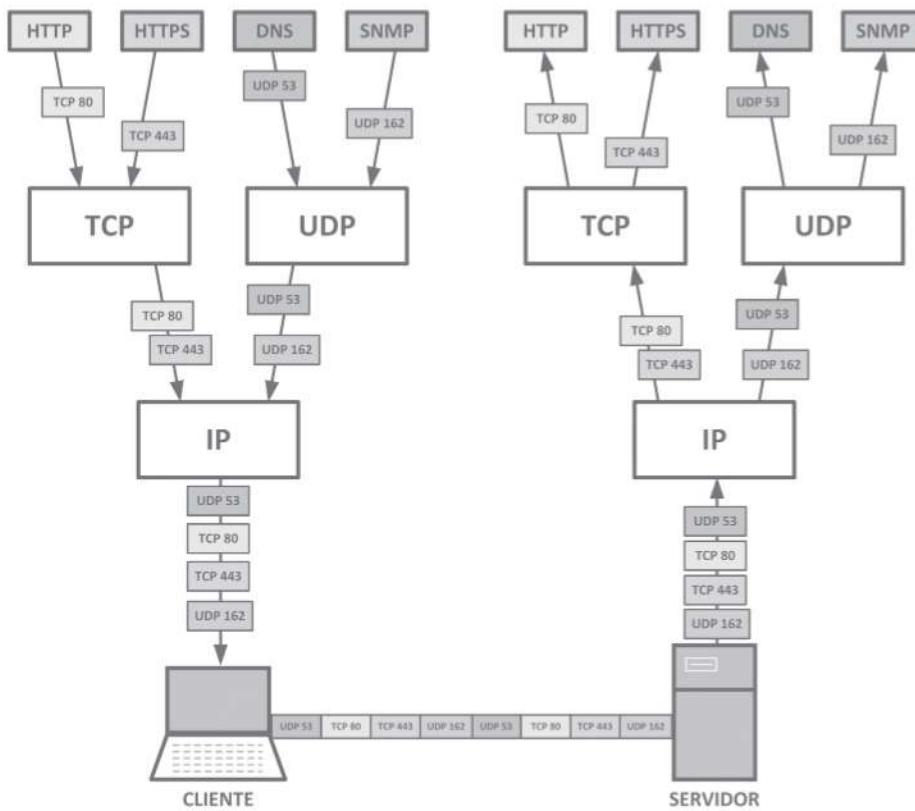
Protocolo UDP – User Datagram Protocol

Neste capítulo será apresentada a camada transporte, muito importante para a arquitetura TCP/IP. Nela existem protocolos orientados à conexão, como o TCP, e protocolos não orientados à conexão, como o UDP. Serão mostrados também detalhes do funcionamento e do cabeçalho desses dois protocolos para melhor compreensão do assunto.

Definição

Na arquitetura TCP/IP, a camada transporte apresenta dois protocolos principais: TCP (Transmission Control Protocol) e UDP (User Datagram Protocol). As principais funções de ambos são fazer o controle fim a fim¹ do fluxo de informações, segmentar os dados vindos da camada aplicação e endereçar uma porta de serviço que esteja associada ao endereçamento lógico (endereço IP), como veremos mais adiante. A identificação de porta associada ao endereço IP de um equipamento e o uso de um dos dois protocolos da camada transporte permitem a localização de um end-point ou socket, que é o ponto por meio do qual os programas de aplicação podem enviar e receber dados (Figura 1).

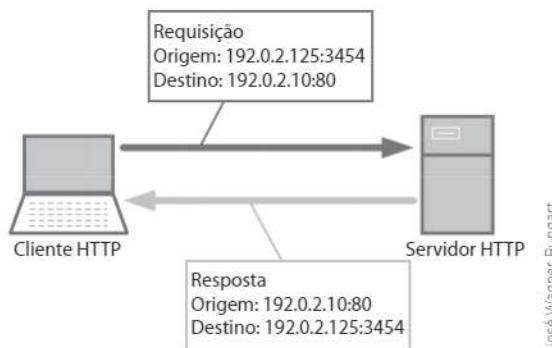
¹ A expressão fim a fim, em redes de computadores, significa uma comunicação estabelecida no nó de origem até o nó de destino, sem interferir em processos ou informações intermediárias.



José Wagner Bungart

Figura 1 – Portas dos protocolos TCP e UDP.

Durante a comunicação entre cliente e servidor, quem requisita a conexão, geralmente o cliente, informa um conjunto de IP e porta, tanto de origem como de destino. Na resposta, a mensagem será entregue exatamente com o mesmo conjunto IP/Porta, conforme a Figura 2:



José Wagner Bungart

Figura 2 – Conjunto IP e porta de conexão.

Protocolo TCP – Transmission Control Protocol

O protocolo TCP é orientado à conexão, ou seja, é um protocolo que estabelece um circuito entre os dispositivos para que haja troca de informações entre duas aplicações e essa transmissão ocorra de forma ordenada. Isto é, o TCP só consegue trabalhar se houver um circuito virtual entre dois equipamentos. Esse circuito é denominado virtual porque não há meio propriamente físico entre eles, mas sim uma rota que pode variar ao longo da transmissão. Depois de estabelecido o circuito virtual, isto é, a conexão, a comunicação se dá de forma bidirecional e ordenada, ou seja, ambos os equipamentos podem receber os dados na mesma ordem que foram transmitidos.

Three-Way Handshake

No entanto, para que uma conexão TCP seja estabelecida, é necessário um processo chamado *Three-Way Handshake*, em português, “aperto de mão em três vias”, no qual o cliente envia uma solicitação de conexão por meio de uma mensagem de sincronismo (SYN). O servidor envia uma resposta do que entendeu à requisição (*acknowledgment*) com uma mensagem SYN+ACK e, por fim, o cliente responde com um ACK. Nesse momento está estabelecida uma conexão entre o cliente e o servidor (Figura 3). Cada uma das requisições e respostas são vias, por isso o nome do processo.

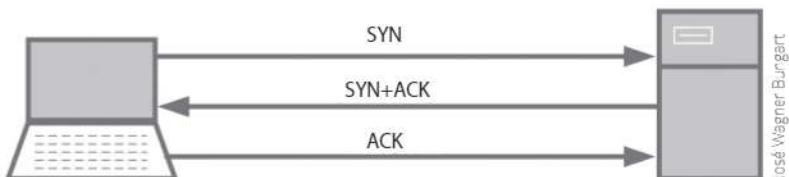


Figura 3 – Three-Way Handshake.

José Wagner Burgart

Na Figura 4 há uma captura de um processo de *Three-Way Handshake*, em que a origem é o cliente 192.168.0.3 e o servidor é 52.204.54.197. Primeiro é enviado um SYN com o valor de sequência igual a zero, logo em seguida o servidor envia o mesmo valor de sequência igual a zero, em números decimais, e um ACK incrementado de 1. O cliente, então, responde com um ACK no valor de 1 e com o número de sequência também 1.

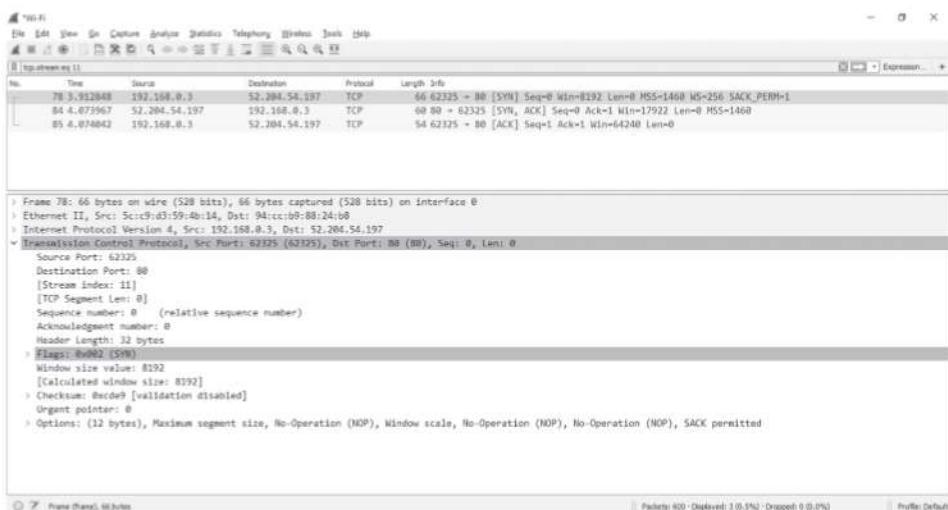


Figura 4 – Captura de pacotes Three-Way Handshake.

No exemplo da Figura 4, após o estabelecimento da conexão, o cliente começa a transmitir mensagens para o servidor. Nesse caso, a comunicação se inicia na camada aplicação com o protocolo HTTP. A linha 81, na Figura 5, é um GET HTTP com a origem no cliente 192.168.0.3 e o destino no servidor 52.204.54.197. A informação *Next sequence number* que está com o número 783 é o número que deve ser enviado pelo servidor como um ACK, ou seja, uma forma de o cliente ter certeza de que o servidor recebeu a mensagem e a entendeu corretamente.

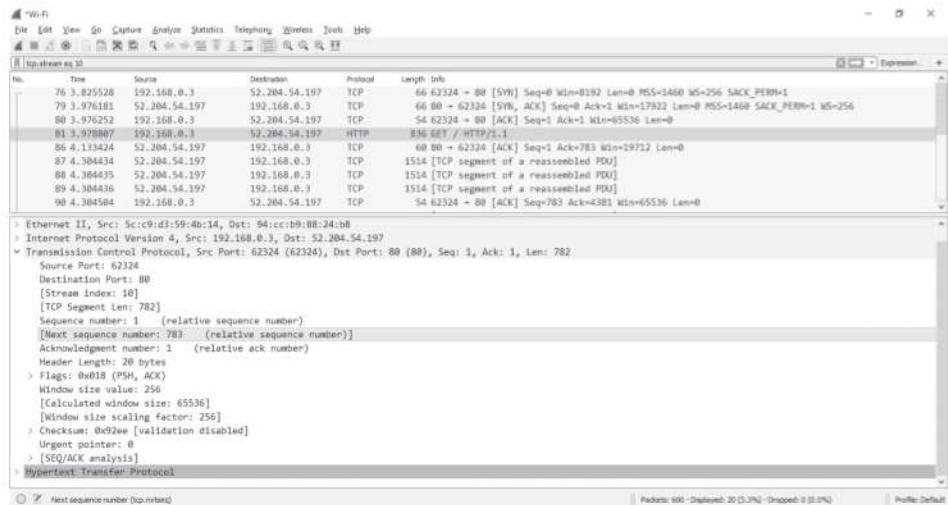


Figura 5 – HTTP com requisição de ACK.

Logo em seguida, na linha identificada como 86, o cliente recebe um ACK do servidor com o número 783, conforme previsto (Figura 6). Caso o ACK estivesse errado ou não retornasse para o cliente, seria enviada uma nova solicitação.

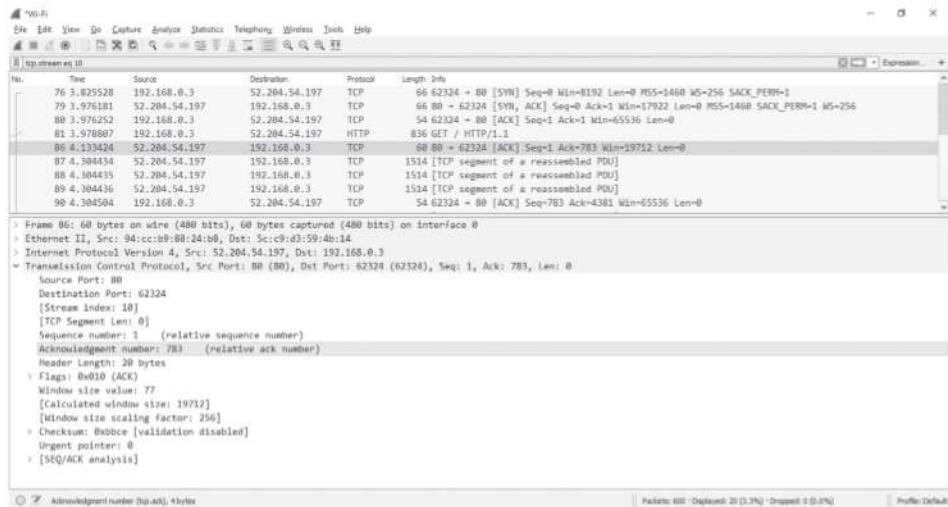


Figura 6 – Recebimento do ACK.

Cabeçalho TCP

Apesar de todas as informações adquiridas serem bastante abstratas, é possível entendê-las de maneira prática por meio do cabeçalho TCP e de seus campos. Esse conhecimento será importante para entender o funcionamento do protocolo e identificar suas funcionalidades (Figura 7).

Porta de origem (16 bits)			Porta de destino (16 bits)							
Número Sequencial (32 bits)										
Número de Confirmação (16 bits)										
HLEN (4 bits)	ZERO (3 bits)	ECN (3 bits)	Controle (6 bits)	Window (16 bits)						
TCP checksum (16 bits)			Apontador de urgência (16 bits)							
Opções										
Dados										

Figura 7 – Cabeçalho TCP.

É importante lembrar que um cabeçalho é um enunciado de mensagens transportadas de um dispositivo para outro na rede de computadores, e entre uma camada e outra dentro do mesmo dispositivo. As portas, na camada transporte, são apenas uma das informações necessárias para a comunicação. Tem-se a seguir, então, alguns dos conceitos e elementos que participam da conexão TCP.

- **Porta de origem (16 bits):** Especifica o número da porta associado ao computador-cliente. As portas TCP são atribuídas pelo IANA (Internet Assigned Numbers Authority), órgão mundialmente responsável pela alocação de endereços IPs que possui o controle da atribuição e distribuição de faixas de endereçamento. Elas foram definidas na RFC 6335. As designações das portas por protocolo podem ser consultadas em www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml. São dividias em três faixas, conforme a seguir:

1. **Portas conhecidas (Well Known Ports):** de 0 até 1023.
2. **Portas registradas (Registered Ports):** de 1024 até 49151.
3. **Portas dinâmicas e/ou privadas (Dynamic and/or Private Ports):** de 49152 até 65535.

As portas conhecidas e registradas não podem ser utilizadas sem o consentimento do IANA, e, para isso existem as portas dinâmicas e privadas.

- **Porta de destino (16 bits):** Especifica o número da porta associado ao *end-point* de destino. Segue as mesmas regulamentações de portas do IANA apresentadas anteriormente.
- **Número de sequência (32 bits):** Controla a ordenação da transmissão de dados no sentido Origem → Destino. Inicializado com um valor aleatório no início da conexão, passa a partir de então a operar como um contador de bytes, que é o agrupamento de oito bits, transmitidos nesse sentido.
- **Número de confirmação (32 bits):** Controla a ordenação da transmissão de dados no sentido Destino → Origem, no sentido inverso do número de sequência, informa o número de sequência esperado na próxima transmissão nesse sentido, indica a confirmação dos dados recebidos até esse número de sequência, adicionando uma unidade.
- **HLEN (4 bits):** Tamanho do cabeçalho TCP.

- **Zero (3 bits):** São três bits reservados que devem ser preenchidos com zeros; não são utilizados.
- **ECN (3 bits):** Do inglês, Explicit Congestion Notification, ou Notificação de Congestionamento Explícito; é um campo opcional destinado a notificar congestionamentos na rede.
- **Window (16 bits):** Informa a disponibilidade em bytes do *buffer*, que é o armazenamento temporário de dados em memória, de recepção de dados do *end-point* local, permitindo a contenção do fluxo de dados no sentido Destino → Origem.
- **TCP Checksum (16 bits):** Número gerado a partir do conteúdo do segmento TCP (cabeçalho + dados) para permitir a verificação da integridade desse segmento na recepção no equipamento de destino.
- **Apontador de urgência (16 bits):** Usado para o envio de dados com prioridade acima do normal.
- **Opções (variável):** Opções adicionais do segmento TCP, usadas para, por exemplo, negociação do tamanho máximo do segmento para essa conexão na fase de estabelecimento da conexão.
- **Dados (variável):** Campo de dados do segmento TCP que contém dados e o cabeçalho da camada aplicação.
- **Controle (6 bits):** Bits que informam a validade de alguns campos do cabeçalho do segmento TCP, bem como indicam funções adicionais do segmento, atuam como *flags* ou marcações para sinalizar o tipo de mensagem. Por exemplo, se o segundo e o quinto bits estiverem com o valor 1 e os demais bits com o valor 0, significa que é uma mensagem SYN + ACK. Ver Figura 8 com cada um dos campos.

URG	ACK	PSH	RST	SYN	FIN
-----	-----	-----	-----	-----	-----

José Wagner Bungar

Figura 8 – Cabeçalho TCP – Flags de controle.

- **URG (Urgent):** Quando ativo, indica que o segmento carrega dados com “urgência” de recepção, localizados pelo campo “apontador de urgência”.
- **ACK (Acknowledgment):** Quando ativo, indica que o campo de confirmação é válido, isto é, pode ser usado como uma confirmação de transmissão no sentido Destino → Origem.

- **PSH (Push):** Quando ativo, indica que os dados desse segmento e os presentes no *buffer* de recepção no equipamento de destino devem ser enviados imediatamente à aplicação associada a esse equipamento.
- **RST (Reset):** Quando ativo, indica que a conexão deve ser cancelada imediatamente e pode ser solicitado tanto pela origem como pelo destino por uma série de motivos, como por exemplo a falta de recursos de hardware ou uma inconsistência encontrada pelo software.
- **SYN (Synchronization):** Quando ativo, indica que o número do campo “número de sequência” deve ser considerado pelo equipamento remoto como o de início de sequência de transmissão. Esse bit é ativado apenas no primeiro segmento do TCP enviado por cada equipamento.
- **FIN (Finalization):** Quando ativo, indica que o equipamento deseja encerrar sua transmissão de dados.

Durante o funcionamento normal de uma rede de computadores, esses *flags* do cabeçalho TCP são ativados ou desativados dependendo das mensagens trocadas. É por meio deles que o estabelecimento e finalização das conexões acontecem. É muito comum a utilização desses *flags* para explorar vulnerabilidades de segurança na tentativa de descobrir portas abertas em servidores e ter sincronização. Ou seja, é comum inundar um servidor com requisições de sincronismo sem completar o processo de *Three-Way Handshake* e até mesmo tentar confundir os protocolos com solicitações sem sentido, como por exemplo o envio de várias requisições com o *flag* FIN ativo, sem que tenha sido estabelecida uma conexão.

Protocolo UDP – User Datagram Protocol

O UDP, do inglês, User Datagram Protocol, é um padrão definido pela RFC 768 e usado por algumas aplicações para o transporte rápido de dados entre *hosts* TCP/IP.

Porém, o UDP não fornece garantia de entrega e nem verificação de dados, como o TCP. O protocolo UDP é utilizado quando a performance nas aplicações é necessária, mas não a confirmação de chegada dos dados, como em uma transmissão de voz ou vídeo. Se os dados não chegarem ao seu destino, não fará mais sentido reenviar a mensagem, pois o momento em que essa informação era preciso e faria sentido já terá passado.

O protocolo UDP não é orientado a conexões, ou seja, ele não se comunica com o destino, mas utiliza a estratégia de *best-effort* – melhor esforço – e entrega os segmentos, sem garantir que haja entrega ou verificação da integridade no destino. Se há necessidade de garantia de entrega, devemos utilizar TCP em vez de UDP.

Seu cabeçalho é muito mais simples que o TCP. Como se pode ver na Figura 9, ele possui apenas porta de origem e destino, um campo para informar o seu tamanho e dos dados, um campo para fazer uma checagem de sanidade do segmento e o campo de dados.

Porta de origem (16 bits)	Porta de destino (16 bits)	- José Wagner Bungart
Comprimento do cabeçalho + dados (16 bits)	UDP checksum (16 bits)	
Dados		

Figura 9 – Cabeçalho UDP.

A captura exibida na Figura 10 mostra uma requisição de resolução de nome DNS (Domain Name System), ou em português, Sistema de Nomes de Domínios, que é a conversão de um nome de um domínio, de um site, por exemplo, para um endereço IP. Mais adiante neste livro o serviço DNS será estudado. As requisições DNS são feitas utilizando o protocolo UDP. Pode-se notar que o cabeçalho é extremamente simples: neste caso, nem a checagem de integridade foi solicitada, uma vez que está desabilitada.



Figura 10 – Captura UDP.

RECAPITULANDO

Neste capítulo foram apresentados os detalhes da camada transporte, principalmente o protocolo TCP, que, por permitir um controle sobre as mensagens enviadas entre transmissor e receptor, se tornou a forma mais utilizada para garantir a entrega dos pacotes no computador ou servidor de destino. Foi visto como é feito o estabelecimento de uma conexão entre dois computadores utilizando o *Three-Way Handshake* do protocolo TCP e estudou-se como são formados os cabeçalhos dos protocolos TCP e UDP.

Exercícios

1. Quais são os dois principais protocolos da camada transporte?
2. Qual a principal diferença entre o protocolo TCP e o UDP?
3. Explique a função do *Three-Way Handshake* e como são as suas mensagens.
4. Quantos bits são utilizados num cabeçalho TCP para endereçar as portas, sejam elas de origem ou de destino?

As respostas dos exercícios deste livro estão disponíveis para *download* no seguinte *link*: https://www.senaispeditora.com.br/downloads/respostas/redes_computadores_respostas.pdf

7. Camada rede

Definição

Protocolo IPv4

Protocolo IPv6

Protocolo ICMP – Internet Control Message Protocol

Neste capítulo serão estudados os detalhes da camada rede e suas características, método de funcionamento e protocolos. O principal protocolo dessa camada é o IP, então aqui será descrito como é feito o seu endereçamento, sua evolução de *classfull* para *classless*, as máscaras de sub-rede, o CIDR que representou uma evolução e uma sobrevida para o IPv4 e como criar sub-redes com tamanhos variados para melhor aproveitamento do espaço de endereçamento disponível.

Será apresentado em seguida o IPv6, a versão mais recente do protocolo que surgiu da necessidade de se ter um esquema de endereçamento que permitisse a continuidade de crescimento das redes, principalmente da internet, e outras funcionalidades implementadas no novo protocolo, como a possibilidade de cabeçalhos de extensão. Por fim, será apresentado o protocolo ICMP, muito importante para testes e monitoramento de uma rede.

Antes, porém, de se aprofundar no tema, é necessário conhecer a definição básica dessa camada da arquitetura TCP/IP.

Definição

As principais funções da camada rede na arquitetura TCP/IP são: encaminhamento de pacotes, endereçamento, interconexão de redes, tratamento de erros, fragmentação de pacotes, controle de congestionamento e sequenciamento de pacotes.

O endereçamento dos pacotes é uma função de conversão de endereços lógicos em endereços físicos. Isto é, endereçar é fazer com que os pacotes consigam chegar corretamente ao destino pela rede. A camada rede também determina a rota que os pacotes seguirão para atingir o destino, baseada em fatores como condições de tráfego da rede e prioridades.

Essa camada é usada quando a comunicação entre dois equipamentos ocorre em mais de um segmento da rede, ou seja, quando há mais de um caminho pelo qual o pacote pode trafegar até chegar ao destino. Um exemplo muito comum ocorre quando, durante a utilização de qualquer serviço de internet, como a navegação em um site a partir de um computador em uma rede residencial ou corporativa, o computador está em um segmento de rede diferente do site da internet, e, portanto, a escolha do caminho para chegar até o site ocorrerá nessa camada.

Protocolo IPv4

O protocolo IP é responsável pela comunicação entre os computadores pertencentes a redes TCP/IP lógicas diferentes. O protocolo IP provê um serviço sem conexão e não confiável entre equipamentos em uma estrutura de rede. Os protocolos de níveis superiores é que determinam a forma de conexão entre equipamentos, não a camada de rede. Isto é, são as camadas de aplicação e transporte que determinam a arquitetura de conexão que será usada. A camada rede usa o protocolo IP para atribuir um esquema de endereçamento e a capacidade de rotear e tomar decisões sobre o caminho que os pacotes devem seguir para chegar a um determinado destino.

Os equipamentos responsáveis por escolher os caminhos a serem seguidos são os roteadores. Eles podem atuar em redes locais ou de longa distância, e o mecanismo da camada rede será igual.

A principal característica de um roteador é possuir duas ou mais interfaces de rede, cada uma pertencendo a uma rede lógica diferente, conforme visto no Capítulo 2.

Cabeçalho

Na Figura 1 é possível visualizar como é composto o cabeçalho IP, seus campos e suas funções.

Versão (4 bits)	Comp. Cabeçalho (4 bits)	Tipo de serviço (8 bits)	Comprimento total (16 bits)
Identificação (16 bits)		Flags (3 bits)	Deslocamento do fragmento (13 bits)
Tamanho de vida (8 bits)	Protocolo (8 bits)	Checksum do cabeçalho (16 bits)	
Controle (6 bits)			
Apontador de urgência (16 bits)			
Opções			
Dados			

Figura 1 – Cabeçalho IP.

-José Wagner Bürgert

- **Versão (4 bits):** Identifica a versão utilizada.
- **Comprimento do cabeçalho – IHL (Internet Header Length) (4 bits):** Especifica o tamanho do cabeçalho IP.
- **Tipo de serviço (8 bits):** Esse campo é designado para tratar os pacotes e fornecer informações para prover funcionalidades de QoS (Quality of Service). Essa opção nunca foi largamente utilizada da maneira como foi desenvolvida, sendo substituída posteriormente por uma técnica chamada Differentiated Services (DS).
- **Comprimento total (16 bits):** Especifica o tamanho total do pacote IP. Como esse campo possui 16 bits, o tamanho total não ultrapassará 65.535 bytes.
- **Identificação (16 bits):** Esse campo possui um valor comum a todos os fragmentos de uma mensagem em particular. Para pacotes enviados originalmente sem fragmentação, caso tenham que ser fragmentados no caminho até o destino, possuirão o mesmo valor de identificação para que possam ser remontados no seu destino.
- **Flags (3 bits):** São marcações para tratar fragmentação, atribuídos da seguinte forma:
 - **Primeiro bit** – Não utilizado.
 - **Segundo bit: Don't Fragment (DF)** – Quando esse bit possuir o valor 1, nunca deverá ser fragmentado. É muito utilizado para testar o MTU (Maximum Transmission Unit) de uma rede.

- **Terceiro bit: More Fragments (MF)** – Quando possuir o valor 0 significa que esse é o último fragmento da mensagem, quando possuir o valor 1, significa que mais fragmentos ainda estão por vir.
- **Tempo de vida (8 bits)**: Indica o tempo máximo que o pacote poderá trafegar na rede. Esse tempo medido em “saltos” corresponde aos roteadores pelos quais o pacote passou. A cada salto, o valor de TTL (Time to Live) é decrementado de 1. Quando esse valor atingir 0, o pacote é descartado, pois algum *loop* deve ter ocorrido no caminho.
- **Deslocamento do fragmento (13 bits)**: Esse campo indica a posição do fragmento em relação a toda mensagem. O primeiro fragmento terá o valor 0, o segundo terá o tamanho do primeiro (em bytes) mais 1, e assim por diante.
- **Protocolo (8 bits)**: Identifica o protocolo da camada transporte ou encapsulamento da camada rede, como por exemplo TCP ou UDP.
- **Checksum do cabeçalho (16 bits)**: Faz a checagem do cabeçalho IP para certificar que não houve erros na transmissão.
- **Endereço IP de origem (32 bits)**: Informa o endereço IP do originador da mensagem.
- **Endereço IP de destino (32 bits)**: Informa o endereço IP do destinatário.
- **Opções**: Campo não obrigatório que pode conter controles adicionais. É válido observar que todos os elementos de rede envolvidos nessa comunicação devem entender e interpretar corretamente o que for descrito nesse campo.

Endereçamento

Atualmente, existem duas versões de endereçamento IP em uso nas redes: IPv4 e IPv6. O IPv4 é mais popular por ter uma quantidade muito grande de equipamentos e redes que utilizam essa versão. Como toda a base da internet foi criada em IPv4 e uma migração para IPv6 não é tão trivial como se possa imaginar, alguns artifícios foram desenvolvidos para dar uma maior sobrevida ao IPv4, como, por exemplo, a criação de endereçamento privado e a NAT (Network Address Translation). Para entender melhor as diferenças entre eles, é preciso saber que o IPv4 utiliza endereçamento de 32 bits e o IPv6 endereçamento de 128 bits, assunto que será tratado ainda neste capítulo. Os 32 bits de um endereço IPv4 são divididos em 4 partes de oito bits, ou seja, 4 octetos, representados em decimal, conforme exemplo a seguir:

192.168.214.101

Como cada octeto possui oito bits, os números em decimal podem variar de 0 até 255 em cada octeto. Como é possível chegar a esse número? É simples: um octeto possui oito bits, cada bit poderá assumir apenas dois valores, 0 ou 1, já que é uma unidade mínima da linguagem binária. Assim, se 0 e 1 são duas possibilidades, é só fazer o cálculo de potência: 2 elevado à oitava ($2^8 = 256$). Ou seja, são 256 possíveis números. Como começamos a contagem a partir do zero, o último possível número é 255, recomeçando a numeração no próximo octeto.

Sabendo que o IP é um endereço que identifica a rede e o computador a ela pertencente, os números nele contidos são informações sobre esse endereço, ou seja, sobre quantos computadores podem ser conectados nessa rede.

No início das redes TCP/IP, não havia um entendimento sobre o que se tornariam as redes e, principalmente, não se sabia que seriam utilizadas mundialmente e em larga escala, com a internet e todas as redes locais em empresas e residências. Dessa maneira, o endereçamento IP foi dividido em apenas 5 classes, conforme Tabela 1. Talvez, se essa classificação fosse mais recente houvesse mais subdivisões.

Tabela 1 – Classes IPv4

CLASSE	INÍCIO	FIM	MÁSCARA DE REDE
A	1.0.0.0	127.255.255.255	255.0.0.0
B	128.0.0.0	191.255.255.255	255.255.0.0
C	192.0.0.0	223.255.255.255	255.255.255.0
D	224.0.0.0	239.255.255.255	N/A
E	240.0.0.0	255.255.255.255	N/A

A máscara de rede define o tamanho da rede, ou seja, onde ela termina e a quantidade de computadores com endereços de IP atribuídos nela. Neste capítulo foi apresentado o cálculo de potenciação que define o valor de 256 como limite de um IPv4, e por meio dele pode-se descobrir quais são as máscaras de rede, dimensionar o seu tamanho e identificar se dois computadores pertencem à mesma rede lógica ou não. As máscaras de rede foram criadas com base nas classes, e então são chamadas de “máscaras naturais da classe”.

As classes D e E não possuem máscara de rede. O motivo para isso é que a classe D é utilizada para endereços de Multicast, ou seja, endereços utilizados para aplicações específicas, como protocolos de roteamento que não precisam estar, necessariamente, em uma mesma rede local com outros dispositivos, sendo desnecessária uma máscara de rede. A classe E, por sua vez, não possui máscara de rede por ter sido reservada, no momento de sua criação, para “uso futuro” – o que ainda não ocorreu.

As outras três classes, A, B e C, são as principais por serem utilizadas para o endereçamento dos dispositivos das redes locais e internet. Suas máscaras naturais definem a quantidade de computadores. Como pôde ser visto anteriormente, também é utilizado o termo host para indicar qualquer dispositivo ou computadores conectados à rede. Para saber quantos dispositivos podem estar presentes em uma rede, o cálculo é simples: o octeto com 255 indica o número máximo que a rede comporta, não sendo possível alterar esse valor. Assim, somente onde houver 0 no octeto poderão ser endereçados hosts. Um exemplo: a rede de classe C, 192.168.10.0, com a máscara de rede 255.255.255.0 indica que somente o último octeto poderá ser utilizado para endereçar hosts; os outros 3 são da rede. Dessa forma, essa rede de classe C poderá ter 256 IPs.

Uma rede classe B que possui dois octetos para endereçar hosts terá, então, 65.536 IPs ($2^{16} = 65.536$) e uma rede classe A terá 16.777.216 IPs ($2^{24} = 16.777.216$), uma vez que tem 3 octetos livres.

Claramente, esse esquema de endereçamento não funcionaria nos dias de hoje, pois a quantidade de equipamentos na mesma rede, os quais produzem uma quantidade razoável de *broadcasts*, faria com que as redes simplesmente parassem. Só para dar uma ideia dessa quantidade, uma boa prática de mercado indica que as redes locais atuais não devem ter mais do que trezentos hosts, pois a quantidade de *broadcasts* influencia negativamente no desempenho de uma rede desse porte. Quando chegam perto desse número, deve-se considerar a segmentação da rede, criando domínios de *broadcast* menores, os seja, separando em redes lógicas menores com a inclusão de roteadores, isto é, criando sub-redes, tópico a ser estudado adiante.

Endereços reservados

O IANA é o órgão responsável pela alocação dos endereços de IP, conforme visto anteriormente. No site www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml está a reserva de endereços por região. Algumas faixas são reservadas para usos especiais ou futuros, previsto na RFC 5735 e disponível em <https://tools.ietf.org/html/rfc5735>. A Tabela 2 mostra os endereços reservados para uso específico:

Tabela 2 – Endereços reservados

Faixa	Descrição
0.0.0.0/8	Utilizado para a criação de rotas-padrão, ou seja, quando o roteador não possuir um caminho para uma rede específica, enviará os pacotes para uma rota-padrão.
127.0.0.0/8	<i>Loopback</i> . Utilizado para endereçar a própria placa de rede do computador e para outras funções em equipamentos de rede quando se quer criar um endereço virtual.
169.254.0.0/16	APIPA (Automatic Private IP Addressing). Caso um <i>host</i> esteja configurado para receber um IP automaticamente e não encontre um servidor para isso, um IP dessa faixa será automaticamente fornecido.
192.0.2.0/24	Usado como <i>Test-net</i> para documentação e exemplos de códigos desenvolvidos por fabricantes.
192.88.99.0/24	Utilizado para Relay 6to4.
192.18.0.0/24	Testes de <i>Benchmark</i> .

As faixas são representadas por /8, /16 e /24 uma vez que se considera 1 bit para compor as máscaras de rede. Isto é, para a máscara de rede 255.0.0.0 foram necessários oito bits 1 – só um octeto completo –, para 255.255.0.0 foram necessários dezesseis bits 1 e para 255.255.255.0 utiliza-se vinte e quatro bits 1. Daí temos o /8, /16 e /24.

Endereços privados

Como o crescimento da internet estava em patamares incontroláveis e a atribuição de endereçamento para milhares de empresas era inevitável, foi necessária a criação de faixas de endereçamento privadas que devem ser usadas para redes internas, não tendo seus endereços encaminhados para a internet. Desta forma, foram atribuídas faixas de endereços privados conforme a Tabela 3:

Tabela 3 – Endereços privados

FAIXA	INÍCIO	FIM
A	10.0.0.0	10.255.255.255
B	172.16.0.0	172.31.255.255
C	192.168.0.0	192.168.255.255

Endereços públicos

Os demais endereços que não foram descritos como endereços reservados e nem endereços privados são endereços públicos. Ou seja, são atribuídos pelas diversas representações do IANA pelo mundo e encaminhados globalmente para identificar as redes a que pertencem.

Classless Interdomain Routing – CIDR

O CIDR (Classless Interdomain Routing) foi criado, em 1993, pelo IETF com a introdução da RFC 1519 (www.ietf.org/rfc/rfc1519.txt?number=1519) para dar maior granularidade e flexibilidade às redes, sendo hoje largamente utilizado. Como o nome sugere, ele não faz parte das classes A, B e C, uma vez que é praticamente impossível de se imaginar uma rede corporativa que utilize apenas máscaras-padrão. Em vez disso, são criadas sub-redes a partir de uma rede. Com as sub-redes, podemos moldar as nossas redes com tamanhos otimizados para um melhor aproveitamento dos escassos endereços IPs. Antes de calcular faixas de sub-redes IP, é necessário definir alguns importantes conceitos:

- **Endereço de sub-rede:** É o primeiro IP de uma faixa de sub-rede e representará toda a faixa de endereçamento dela. Por exemplo, para os roteadores formarem as tabelas de roteamento, que são a base para a escolha de qual caminho os pacotes deverão tomar para chegar ao destino, é utilizado o endereço de sub-rede (ou rede).
- **Endereço de broadcast:** É o último IP de uma faixa de sub-rede e representa cada um dos endereços IP de uma faixa. Por exemplo, existem protocolos que precisam enviar mensagens para cada *host* na rede, e em vez de endereçar uma mensagem para cada IP, uma única mensagem é enviada para o endereço de broadcast e todas os *hosts* receberão a mesma informação.

- Primeiro endereço de host:** É o IP imediatamente após o endereço de sub-rede; é o primeiro IP que podemos utilizar para endereçar hosts.
- Último endereço de host:** É o IP anterior ao endereço de *broadcast* e o último IP que podemos utilizar para endereçar hosts.

A seguir é apresentado um método para cálculo de endereçamento de sub-redes IP, uma sequência de procedimentos para que se chegue aos endereços de sub-rede, *broadcast*, primeiro e último endereço para host da faixa, bem como para calcular a quantidade de *hosts* e sub-redes com a máscara utilizada.

No Exemplo 1 é usado o IP 192.168.100.40 com máscara 255.255.255.240.

Exemplo 1

- Transformar o endereço IP e máscara de decimal para binário. Para isso deve-se utilizar uma tabela como a da Figura 2:

	128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1	
Endereço IP	192	168	100	40	1	1	0	0	0	0	0	1	0	1	0	1	0	0	0	1	1	0	0	0	
Máscara	255	255	255	240	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0
Sub-Rede																									
Broadcast																									
Próximo Host																									
Último Host																									

José Wagner Bürgart

Figura 2 – Conversão decimal-binário.

- Ao final da sequência de 1 da máscara, passar um traço na vertical. Esse traço servirá como referência para o cálculo dos demais endereços. Do lado esquerdo do traço há a parte sub-rede do endereço e do lado direito a parte host. Na Figura 3 a marcação foi feita com um traço hachurado:

	128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1	
Endereço IP	192	168	100	40	1	1	0	0	0	0	0	1	0	1	0	1	0	0	1	1	0	0	0	0	
Máscara	255	255	255	240	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0
Sub-Rede																									
Broadcast																									
Próximo Host																									
Último Host																									

José Wagner Bürgart

Figura 3 – Marcação da sub-rede.

- Do lado esquerdo do traço deve-se aplicar a função AND, e pode-se observar que os bits do endereço IP se repetirão, pois:

$$1 \text{ AND } 0 = 0$$

$$1 \text{ AND } 1 = 1$$

Assim, pode-se repetir os bits do endereço IP (à esquerda do traço). Isto se aplica também aos demais endereços (*broadcast*, primeiro e último). Do lado direito do traço, deve-se colocar todos os bits 0. Por último, converter o endereço de binário para decimal (Figura 4). Assim se calcula o endereço de sub-rede.

	128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1	
Enderço IP	192	168	100	40	1	1	0	0	0	0	0	1	0	1	0	1	0	0	0	1	0	1	0	0	
Máscara	255	255	255	240	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0
Sub-Rede	192	168	100	32	1	1	0	0	0	0	0	1	0	1	0	0	0	1	1	0	1	1	1	0	0
Broadcast																									
Próximo Host																									
Último Host																									

José Wagner Bürgart

Figura 4 – Endereço de sub-rede.

4. Cálculo do endereço de *broadcast*: assim como no cálculo do endereço de sub-rede, deve-se repetir os bits do endereço IP do lado esquerdo do traço. Do lado direito do traço, colocar todos os bits 1. Por último, converter o endereço de binário para decimal (Figura 5).

	128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1	
Enderço IP	192	168	100	40	1	1	0	0	0	0	0	1	0	1	0	1	0	0	1	0	1	0	1	0	0
Máscara	255	255	255	240	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0
Sub-Rede	192	168	100	32	1	1	0	0	0	0	0	1	0	1	0	1	0	0	1	1	0	1	1	0	0
Broadcast	192	168	100	47	1	1	0	0	0	0	0	1	0	1	0	0	0	1	1	0	1	1	1	1	1
Próximo Host																									
Último Host																									

José Wagner Bürgart

Figura 5 – Endereço de broadcast.

5. Cálculo do primeiro endereço utilizado para host: assim como no cálculo do endereço de sub-rede e *broadcast*, deve-se repetir os bits do endereço IP do lado esquerdo do traço. Do lado direito do traço, colocar todos os bits 0 e o último 1, pois ele é o primeiro endereço depois do endereço de sub-rede que se pode utilizar para endereçar hosts. Por último, converter o endereço de binário para decimal (Figura 6).

	128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1	
Enderço IP	192	168	100	40	1	1	0	0	0	0	0	1	0	1	0	1	0	0	0	1	0	0	1	0	0
Máscara	255	255	255	240	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0
Sub-Rede	192	168	100	32	1	1	0	0	0	0	0	1	0	1	0	0	0	1	1	0	1	1	0	0	0
Broadcast	192	168	100	47	1	1	0	0	0	0	0	1	0	1	0	0	0	1	1	0	1	1	1	1	1
Próximo Host	192	168	100	33	1	1	0	0	0	0	0	1	0	1	0	0	0	1	0	0	1	0	0	0	1
Último Host																									

José Wagner Bürgart

Figura 6 – Endereço do primeiro host.

6. Cálculo do último endereço utilizado para host: assim como no cálculo dos demais endereços, deve-se repetir os bits do endereço IP do lado esquerdo do traço. Do lado direito do traço, colocar todos os bits 1 e o último 0, pois ele é o último endereço antes do endereço de *broadcast*. Por último, converter o endereço de binário para decimal.

	128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1
Endereço IP	192.168.100.40	1	1	0	0	0	0	0	1	0	1	0	0	0	0	1	0	0	0	0	0	1	0	1
Máscara	255.255.255.252	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Sub-Rede	192.168.100.32	1	1	0	0	0	0	0	1	0	1	0	1	0	0	0	1	0	0	0	0	1	0	0
Broadcast	192.168.100.47	1	1	0	0	0	0	0	0	1	0	1	0	0	0	0	1	1	0	0	0	1	0	1
Primeiro Host	192.168.100.32	1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	1	0	0	0	1	0	1
Último Host	192.168.100.46	1	1	0	0	0	0	0	0	1	0	1	0	0	0	0	1	1	0	0	0	1	0	1

José Wagner Bürgart

Figura 7 – Endereço do último host.

7. Para se calcular o número possível de hosts em uma sub-rede, basta aplicar a seguinte fórmula:

$$\text{hosts} = 2^n - 2$$

8. Onde n é o número de bits do lado direito do traço, ou seja, do lado host do endereço. Como não é possível utilizar o endereço de sub-rede e de *broadcast*, subtraí-se 2.

9. No exemplo temos:

$$\text{hosts} = 2^4 - 2 = 14 \text{ hosts}$$

10. Existe uma controvérsia no cálculo do número de sub-redes possível, pois a RFC 950 (www.ietf.org/rfc/rfc950.txt) recomenda que não seja utilizada a primeira sub-rede e a última sub-rede, denominadas “Subnet Zero” e “All-Ones Subnet” respectivamente. O que essa RFC alega é que pode haver alguma confusão na interpretação de um endereço de rede com um endereço de sub-rede. Porém, o que a indústria entende é que se o administrador da rede tiver total controle de como os protocolos entenderão o esquema de rede e sub-rede, poderá também aproveitar essas duas sub-redes, conforme consta no site (www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080093f18.shtml). Dessa forma, é uma escolha do administrador da rede utilizar a primeira e última sub-rede ou seguir a recomendação da RFC 950 do IETF. Dificilmente encontram-se redes que não utilizam a primeira e última sub-rede.

Seguindo a RFC 950, o cálculo ficaria assim:

$$\text{Sub-redes} = 2^m - 2$$

Onde m é o número de bits do lado esquerdo do traço até chegar no bit da máscara padrão da classe que o IP pertence. No exemplo há 4 bits até chegar na máscara 255.255.255.0 da classe C.

$$\text{Sub-redes} = 2^4 - 2 = \mathbf{14 \text{ sub-redes}}$$

Utilizando a Subnet Zero e a All-Ones Subnet, o cálculo ficaria assim:

$$\text{Sub-redes} = 2^m$$

$$\text{Sub-redes} = 2^4 = \mathbf{16 \text{ sub-redes}}$$

Analizando como essa sub-rede (192.168.100.32) se encaixa na divisão da rede *classfull*, ou seja, na sua rede com a máscara natural da classe (192.168.100.0/24), ela é a terceira sub-rede de um total de dezesseis sub-redes, (Tabela 4).

Tabela 4 – Sub-redes de 192.168.100.0/24 com máscara /28

NÚMERO	SUB-REDE
1	192.168.100.0/28
2	192.168.100.16/28
3	192.168.100.32/28
4	192.168.100.48/28
5	192.168.100.64/28
6	192.168.100.80/28
7	192.168.100.96/28
8	192.168.100.112/28
9	192.168.100.128/28
10	192.168.100.144/28
11	192.168.100.160/28
12	192.168.100.176/28
13	192.168.100.192/28
14	192.168.100.208/28

(continua)

NÚMERO	SUB-REDE
15	192.168.100.224/28
16	192.168.100.240/28

FIQUE ALERTA

Existem calculadoras de endereçamento IP que facilitam e agilizam muito o cálculo de endereços de rede. Uma delas está disponível em www.subnet-calculator.com/. Na Figura 8 pode-se observar como ficaria o cálculo do exemplo utilizando essa calculadora. Fique alerta e saiba tirar o melhor proveito da tecnologia.

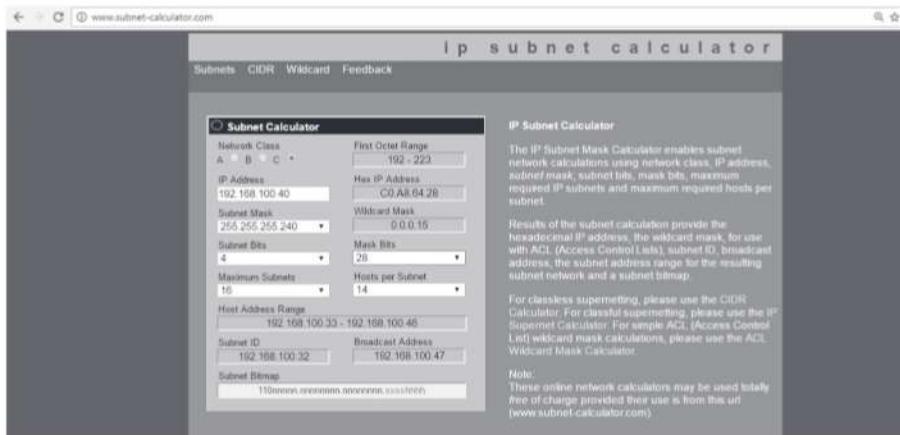


Figura 8 – IP Subnet Calculator

Variable Length Subnet Mask – VLSM

O conceito de VLSM surgiu para otimizar ainda mais o uso do IPv4, pois mesmo com a divisão das redes em sub-redes, seria possível ter um aproveitamento melhor. Por exemplo, uma empresa que possui sua matriz com cem hosts e duas filiais com cinquenta hosts precisaria de duas redes /24 para endereçar todos os hosts. Para demonstrar, tem-se o exemplo de duas redes privadas da classe C:

- Matriz: 192.168.0.0/25
1. Endereço de sub-rede: 192.168.0.0;

2. Endereço de *broadcast*: 192.168.0.127;
3. Quantidade de hosts: 126;
4. Sobrariam 26 IPs.
 - Filial 1: 192.168.0.127/25
 1. Endereço de sub-rede: 192.168.0.128;
 2. Endereço de *broadcast*: 192.168.0.255;
 3. Quantidade de hosts: 126;
 4. Sobrariam 76 hosts, mais do que o dobro necessário.
 - Filial 2: 192.168.1.0/26
 1. Endereço de sub-rede: 192.168.1.0;
 2. Endereço de *broadcast*: 192.168.1.63;
 3. Quantidade de hosts: 62;
 4. Sobrariam 12 hosts e ainda sobrariam mais três redes com 64 IPs em cada, a 192.168.1.64/26, a 192.168.1.128/26 e a 192.168.1.192/26.

Para evitar esse desperdício, utiliza-se VLSM. Ou seja, não é necessário sempre utilizar máscaras de igual tamanho para todas as sub-redes, pode-se pegar, a partir de uma rede ou sub-rede, uma faixa em que caibam todos os IPs com uma divisão mais precisa. Por exemplo, no cenário anterior poderíamos ter:

- Matriz: 192.168.0.0/25
 1. Endereço de sub-rede: 192.168.0.0;
 2. Endereço de *broadcast*: 192.168.0.127;
 3. Quantidade de hosts: 126;
 4. Sobrariam 26 IPs na sub-rede, que poderiam ser utilizados em expansões futuras.
- Filial 1: 192.168.0.127/26

5. Endereço de sub-rede: 192.168.0.128;
 6. Endereço de *broadcast*: 192.168.0.191;
 7. Quantidade de hosts: 126;
 8. Sobrariam apenas 12 hosts na sub-rede, que poderiam ser utilizados em expansões futuras.
- Filial 2: 192.168.0.0/26
 1. Endereço de sub-rede: 192.168.0.192;
 2. Endereço de *broadcast*: 192.168.0.255;
 3. Quantidade de hosts: 62;
 4. Sobrariam apenas 12 hosts na sub-rede, que poderiam ser utilizados em expansões futuras.

Dessa forma, a rede 192.168.0.0/24 seria utilizada totalmente apenas com as sobras em cada sub-rede, mas não seria necessário utilizar uma segunda rede, como foi feito no primeiro cenário com a 192.168.1.0/24, economizando, assim, uma rede classe C inteira.

SAIBA MAIS

Para cálculo de VLSM existe outra calculadora on-line que, além de fazer os cálculos das sub-redes de forma a evitar desperdícios, ainda traz uma estatística do uso dos IPs na rede. Essa calculadora está disponível em www.vlsm-calc.net/. A Figura 9 mostra como ficaria o cálculo do cenário usado como exemplo.

The screenshot shows the VLSM (CIDR) Subnet Calculator interface. The main input is the Major network address 192.168.0.0/24. The user has specified three subnets (A, B, C) with sizes 100, 50, and 50 respectively. The results show the following subnet details:

Subnet	Name	Size	Address	Mask	Net Mask	Assignable Range	Broadcast
A	A	100	192.168.0.0	/25	255.255.255.128	192.168.0.1 - 192.168.0.126	192.168.0.127
B	B	50	192.168.0.128	/26	255.255.255.192	192.168.0.129 - 192.168.0.190	192.168.0.191
C	C	50	192.168.0.192	/26	255.255.255.192	192.168.0.193 - 192.168.0.254	192.168.0.255

References:

- IP Address Classes
- Subnet Masks
- OSI and TCP/IP Network Models
- Power of 2
- Dec/Bin/Hex Conversion

Figura 9 – VLSM Subnet Calculator.

Sumarização de redes

Com a introdução do CIDR, ou seja, o fim das classes de rede, as amarras a elas foram desfeitas totalmente, tanto para a criação de sub-redes, conforme visto anteriormente, como para a criação de “super-redes”, ou seja, com uma quantidade de hosts maior do que a permitida pela máscara natural. Por exemplo, a rede 192.168.0.0/24 inicia em 192.168.0.0 e termina em 192.168.0.255; o próximo IP, 192.168.1.0 já pertenceria à próxima rede, 192.168.1.0/24. Caso se queira juntar as duas redes em uma só, pode-se apenas alterar a máscara, criando uma rede /23 (255.255.255.254), que teria o primeiro IP 192.168.0.0 e o último 192.168.1.255, todos em apenas uma rede CIDR.

A ferramenta on-line IP Subnet Calculator possui essa funcionalidade e pode demonstrar esse mesmo cálculo (Figura 10).

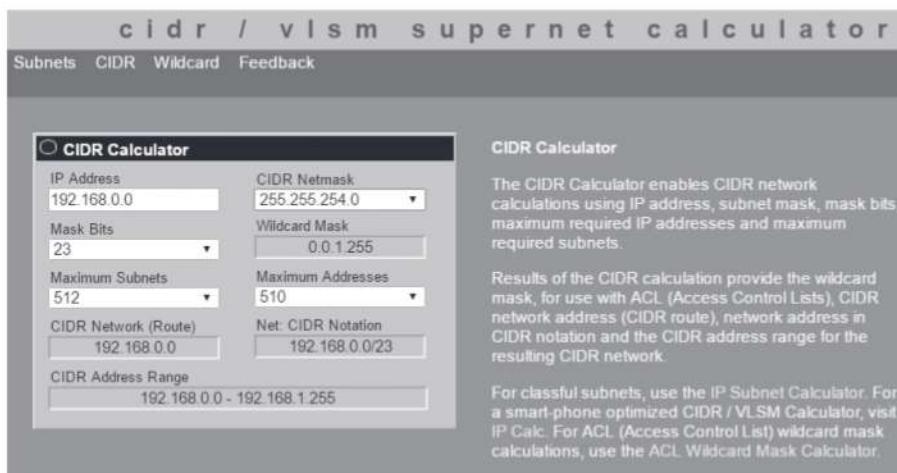


Figura 10 – Cálculo de CIDR.

Esse recurso é muito utilizado também para summarização de redes, ou seja, se um roteador precisa armazenar uma série de rotas para uma sequência de redes, ele pode fazer um resumo dessas redes, não necessariamente sendo sub-redes. Um exemplo disso é o que acontece na internet: por exemplo, o prefixo 201.0.0.0/16 pertence ao Brasil, e engloba várias redes /24. Se fosse necessário rotear cada uma dessas redes, as tabelas de roteamento dos equipamentos ficariam muito maiores do que o necessário.

Protocolo IPv6

O IPv6 é a versão mais recente do protocolo IP e surgiu devido ao esgotamento da disponibilidade de endereços IPv4. Há muitos anos o IANA e seus órgãos regionais – para o caso do Brasil o LACNIC (Latin America and Caribbean Network Information Centre) – vêm trabalhando com a conscientização do uso correto e otimizado dos IPs e administrando sua distribuição. Mas o esgotamento é inevitável, e há apenas poucas reservas técnicas de IPv4 públicos guardadas. O uso do IPv6 na internet está crescendo muito. É possível ver estatísticas tanto da adoção do IPv6 como do esgotamento do IPv4 no site <http://ipv6.br/>. Aproveitando que seria necessária uma nova versão do protocolo IP, algumas melhorias foram introduzidas com o objetivo de deixar o protocolo mais eficiente.

Nas redes privadas, a adoção do IPv6 ainda não foi realizada e demorará um pouco para acontecer. Como existem os IPs privados na versão 4 e as faixas são grandes o suficiente para suportar a quantidade de *hosts* internamente, não há motivos para alterar a infraestrutura interna para IPv6. Assim, essa migração interna pode ocorrer de maneira gradativa e lenta.

Em 1998 o IETF publicou a RFC 2460 (<https://tools.ietf.org/html/rfc2460>) com a introdução do IPv6, destacando as principais mudanças em relação ao IPv4:

- **Aumento na capacidade de endereçamento:** aumento de 32 para 128 bits.
- **Cabeçalho simplificado:** alguns campos do cabeçalho IPv4 se tornaram opcionais ou foram até mesmo removidos com o objetivo de diminuir o processamento dos pacotes nos roteadores.
- **Suporte a cabeçalhos de extensão:** os campos que são opcionais no cabeçalho IPv4 foram retirados do cabeçalho-base. Criou-se o conceito de cabeçalhos de extensão. Caso seja necessária uma funcionalidade específica, o cabeçalho-base aponta para um cabeçalho de extensão.
- **Identificação de fluxo de dados:** pacotes que pertencem a um mesmo fluxo podem ser identificados e terem um tratamento especial, o que antes só poderia ser feito com a ajuda de alguma aplicação externa que enxergasse todos os pacotes.
- **Suporte a autenticação e privacidade:** foram criados cabeçalhos de extensão com o objetivo de permitir autenticação de pacotes.

Cabeçalho

O cabeçalho IPv6 tem tamanho fixo de 40 bytes e tem a característica de ser mais simples em relação ao cabeçalho IPv4, além da flexibilidade inserida com o suporte a cabeçalhos de extensão. Será apresentado a seguir o conteúdo do cabeçalho IPv6 e as funções de cada campo (Figura 11).

Versão (4 bits)	Classe de tráfego (8 bits)	ID de fluxo (20 bits)
Cumprimento dos dados (16 bits)	Próximo cabeçalho (8 bits)	Límite de saltos (8 bits)
Endereço de origem (128 bits)		
Endereço de destino (128 bits)		
Dados		

Figura 11 – Cabeçalho IPv6.

- Versão:** identifica a versão do protocolo IP utilizado. Para o IPv6 esse campo tem o valor em binário 0110 (6 em decimal).
- Classe de tráfego:** identifica os pacotes por classes de serviços ou prioridade; é equivalente ao campo ToS do cabeçalho IPv4.
- ID de fluxo:** identifica um determinado fluxo de dados, definindo os pacotes que pertencem a um mesmo fluxo de comunicação.
- Comprimento dos dados:** indica o tamanho dos campos de dados. Cabe ressaltar que os cabeçalhos de extensão também são contabilizados nesse tamanho.
- Próximo cabeçalho:** identifica o próximo protocolo da camada superior, por exemplo UDP ou TCP, ou indica o próximo cabeçalho de extensão, se houver.
- Límite de saltos:** esse campo é o equivalente TTL do protocolo IPv4. É decrementado toda vez que passa por um roteador, informando então por quantos roteadores o pacote ainda pode passar até que atinja o valor zero e seja descartado.
- Endereço de origem:** indica o endereço IP de origem do pacote.
- Endereço de destino:** indica o endereço de destino do pacote.
- Dados:** são os dados a serem transmitidos, incluindo os cabeçalhos de extensão e de outras camadas.

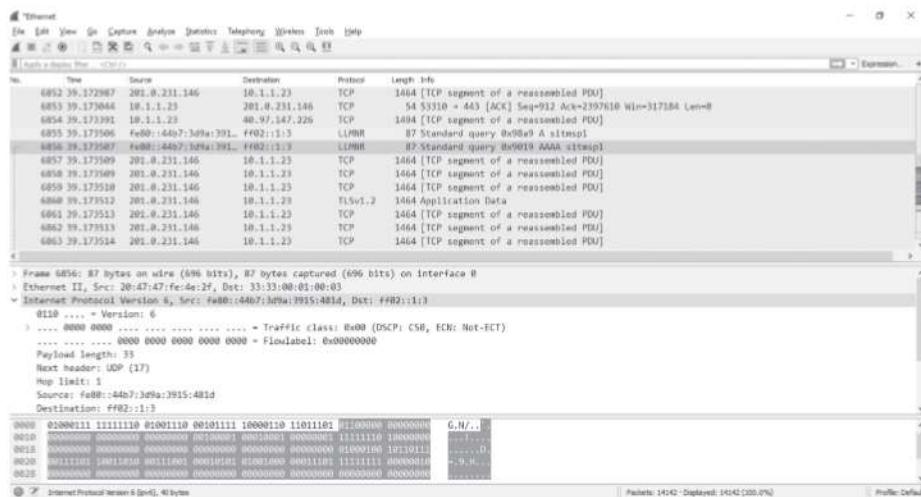


Figura 12 – Captura de pacote IPv6.

Os cabeçalhos de extensão deram flexibilidade ao protocolo, pois apresentam tamanho variável e oferecem a possibilidade de serem criadas cadeias de

cabeçalhos: um cabeçalho de extensão chamando outro cabeçalho. A RFC 2460 define os tipos e valores dos cabeçalhos de extensão conforme a Tabela 5. Essa RFC define também a ordem que os cabeçalhos devem seguir quando estiverem em uma cadeia de cabeçalhos. No cabeçalho-base, os códigos abaixo são inseridos no campo “Próximo cabeçalho”. Como pode-se observar na Figura 12, esse campo está preenchido com o valor UDP (17), ou seja, não há cabeçalho de extensão IPv6 e já é indicado um protocolo de camada superior.

Tabela 5 – Cabeçalhos de extensão

ORDEM	TIPO DE CABEÇALHO	CÓDIGO
1	IPv6 Básico	-
2	Hop-by-Hop Options	0
3	Destination Options (with Routing Options)	60
4	Routing Header	43
5	Fragment Header	44
6	Authentication Header	51
7	Encapsulation Security Payload Header	50
8	Destination Options	60
9	Mobility Header	135
	Sem próximo cabeçalho	59
Camada Superior	TCP	6
Camada Superior	UDP	17
Camada Superior	ICMPv6	58

O cabeçalho de extensão *Hop-by-hop* é uma importante extensão, pois, quando presente, indica que todos os nós da rede devem examiná-lo. Caso não esteja presente, somente o dispositivo final deverá analisar o seu conteúdo. Na ordem indicada pela RFC 2460, ele sempre deve ser o próximo cabeçalho de extensão na sequência do cabeçalho-base. Os demais cabeçalhos de extensão mencionados na Tabela 5 tratam de roteamento, mobilidade, fragmentação, autenticação e segurança.

Endereçamento

O endereçamento no IPv6 foi o grande motivador de sua criação: ele deveria ser capaz de gerar IPs grandes o suficiente para suportar o crescimento da internet, das redes locais e de novas tecnologias que ainda poderiam surgir. Por isso, foi criado um endereçamento de 128 bits, saindo dos limitados 32 bits do IPv4, que suporta 4.294.967.296 endereços de IPs em comparação aos incalculáveis 340.282.366.920.938.463.463.374.607.431.768.211.456 endereços de IPs do IPv6. Para se ter ideia dessa dimensão, considerando que a Terra tenha 6 bilhões de habitantes, um número arredondado, haveria mais de 56 octilhões de endereços por pessoa na Terra.

Como visto anteriormente, o IPv4 utiliza um padrão de números decimais divididos em quatro octetos, como por exemplo 192.168.100.40. Já o IPv6 utiliza um padrão de divisão em oito grupos de 16 bits, escritos em hexadecimal (de 0 a F), como:

2001:ABCD:24F3:FACA:F0CA:CADE:CAFE:0392

A representação das letras é suportada tanto em maiúsculas quanto em minúsculas, sem haver diferenças entre elas. Também é suportado um esquema de abreviação para facilitar a escrita, como por exemplo omitir zeros de um bloco de 16 bits ou zeros à esquerda dentro de um grupo, substituir longas sequências de zeros por “::”, por exemplo, o endereço 2001:0AB7:0000:0000:132A:0000:0000:115B poderia ser escrito como 2001:AB7:0:0:132A::115B ou até mesmo 2001:AB7::132A:0:0:115B.

A representação das sub-redes no IPv6 segue o mesmo critério do IPv4, utilizando a notação da quantidade de bits da sub-rede, com a diferença que agora existem 128 bits. Assim, um endereço de exemplo poderia ser escrito da seguinte forma: 2001:AB8::/32

Estratégias de transição do IPv4 para IPv6

Os protocolos IPv4 e IPv6 não são compatíveis entre si. Para permitir a coexistência dos dois protocolos e viabilizar uma transição sem impactos do IPv4 para o IPv6, foram propostas algumas estratégias:

- pilha dupla;
- túneis;
- tradução.

A estratégia de pilha dupla consiste em estabelecer um suporte para que os dispositivos ofereçam ambos os protocolos simultaneamente, ou seja, estabeleçam uma conexão IPv4 e uma IPv6. Se o dispositivo suportar IPv6, a transmissão é feita por este tipo, caso contrário é utilizado IPv4. Essa foi a solução adotada como padrão.

Porém, quando não é possível a utilização de pilha dupla, caso os dispositivos dos usuários não suportem IPv6 por serem antigos (atualmente, a Anatel só homologa dispositivos de rede no Brasil que suportem IPv4 e IPv6), uma solução é a utilização de túneis que encapsulam o IPv6 em um túnel IPv4. Essa técnica é chamada IPv6-in-IPv4 e descrita na RFC 4213.

A última estratégia de tradução consiste em traduzir endereços IPv6 em endereços IPv4 para redes que já operam em IPv6 suportarem a internet em IPv4. Ou seja, cria-se um mecanismo de conversão de um endereço para outro que é chamado tecnicamente de tradução.

Protocolo ICMP – Internet Control Message Protocol

O ICMP, Internet Control Message Protocol, é um protocolo que foi criado para permitir o controle e relatar condições de erro ou de funcionamento da rede. O ICMP não corrige os erros que encontra, mas informa sobre eles e as condições da rede. O ICMP foi definido na RFC 792 (www.ietf.org/rfc/rfc792.txt) e possui um cabeçalho extremamente simples, conforme pode ser visto na Figura 13. O campo Tipo define o tipo da mensagem, como o próprio nome sugere; o campo Código serve para dar mais granularidade à informação e tem sua utilização em conjunto com o campo Tipo, ou seja, o par formado por Tipo e Código define a mensagem ICMP. O campo Checksum é utilizado para verificar a integridade do pacote, e o campo Mensagem ICMP informa textualmente a mensagem de erro, sendo seu tamanho variável.



Figura 13 – Cabeçalho ICMP.

José Wagner Bungart

O protocolo ICMP possui as versões ICMPv4 e ICMPv6, cada uma para determinado tipo de IP. O formato do cabeçalho de ambos é o mesmo, o que difere são os tipos e códigos utilizados. Uma lista completa dos tipos e códigos pode ser obtida no site do IANA (www.iana.org/assignments/icmp-parameters/icmp-parameters.xhtml).

Pode-se ver na tela de captura da Figura 14 um dos principais usos do ICMP e seus diferentes tipos e códigos: a exibição da mensagem Echo Request e Echo Reply, que são originadas a partir de um comando muito utilizado pelos administradores de redes, o *ping*. Esse comando nada mais é do que um teste de conectividade entre dois dispositivos de uma rede. A mensagem Echo Request possui Tipo=8 e Código=0.

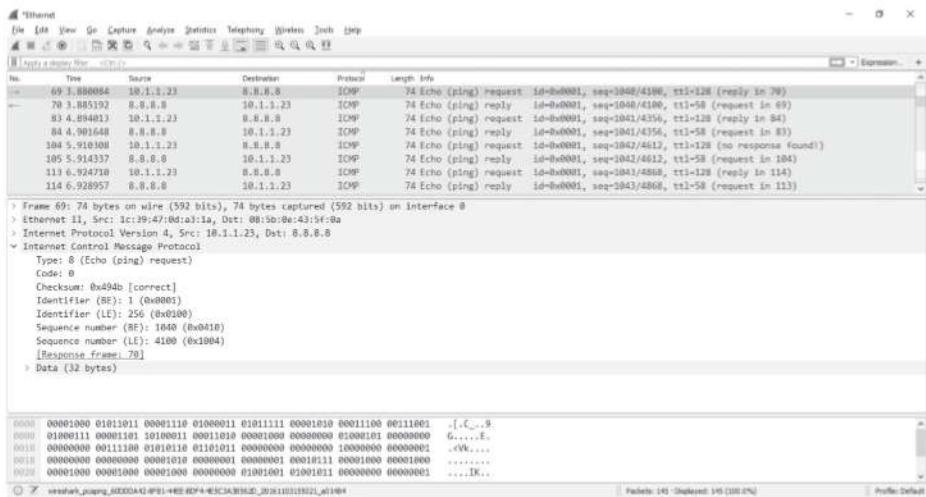
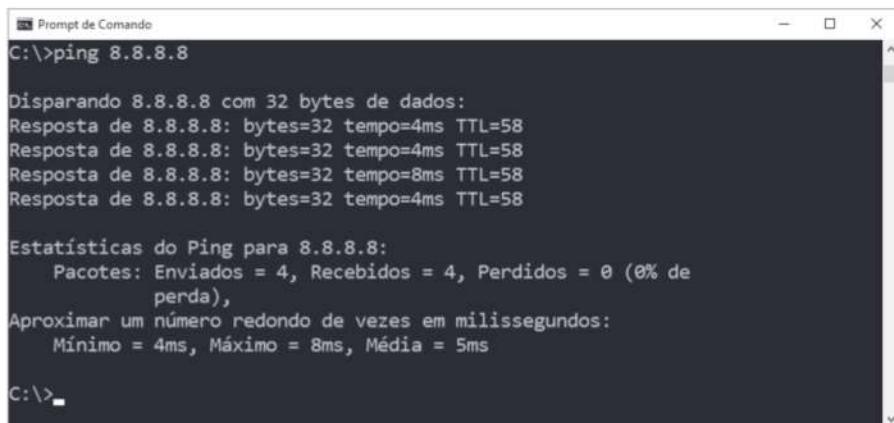


Figura 14 – Captura ICMP.

Conforme pode ser visto na Figura 15, a sintaxe deste comando é “ping [endereço IP]”. Ao digitar isso na tela, o protocolo cria um pacote com 32 bytes de dados e envia para o destinatário. No caso de sistemas operacionais Windows, são enviados 4 pacotes. No exemplo da Figura 15, todos atingiram o seu destino. Além

do teste com resultado positivo ou negativo, uma estatística também é exibida ao final da mensagem.



```
Prompt de Comando
C:\>ping 8.8.8.8

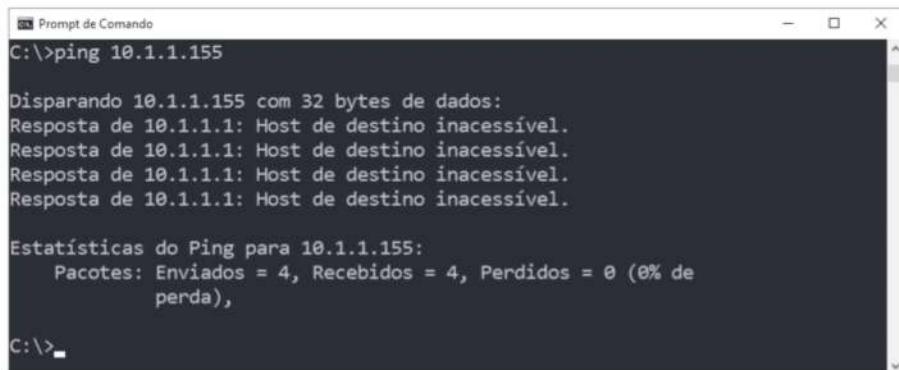
Disparando 8.8.8.8 com 32 bytes de dados:
Resposta de 8.8.8.8: bytes=32 tempo=4ms TTL=58
Resposta de 8.8.8.8: bytes=32 tempo=4ms TTL=58
Resposta de 8.8.8.8: bytes=32 tempo=8ms TTL=58
Resposta de 8.8.8.8: bytes=32 tempo=4ms TTL=58

Estatísticas do Ping para 8.8.8.8:
  Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (0% de
            perda),
Aproximar um número redondo de vezes em milissegundos:
  Mínimo = 4ms, Máximo = 8ms, Média = 5ms

C:\>
```

Figura 15 – Comando Ping.

Caso o IP de destino não esteja disponível ou não exista naquela rede, uma mensagem de erro será exibida na tela do usuário, como pode ser visto na Figura 16.



```
Prompt de Comando
C:\>ping 10.1.1.155

Disparando 10.1.1.155 com 32 bytes de dados:
Resposta de 10.1.1.1: Host de destino inacessível.

Estatísticas do Ping para 10.1.1.155:
  Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (0% de
            perda),

C:\>
```

Figura 16 – Comando Ping: Destino inacessível.

Fazendo uma captura dos pacotes ICMP pode-se notar na Figura 17 que a solicitação Echo Request é enviada para o destinatário, mas uma resposta de erro – Destination Unreachable – é recebida.

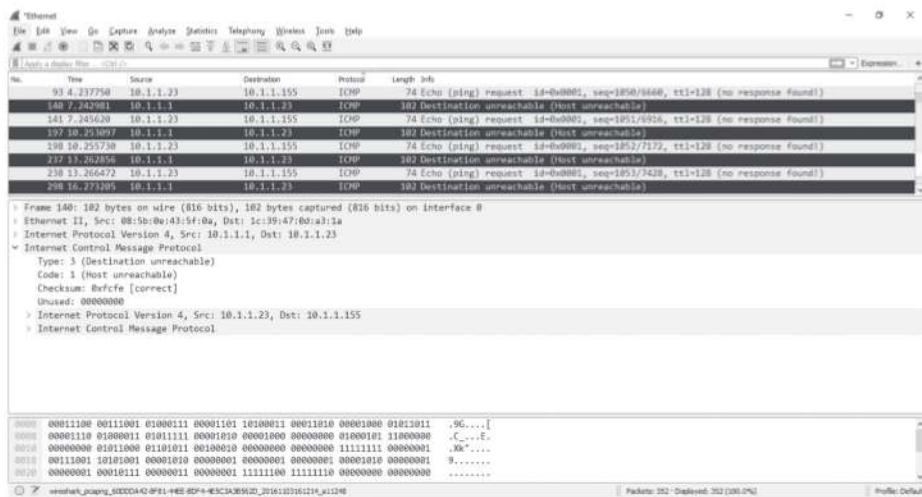


Figura 17 – Captura ICMP: Destino inacessível.

RECAPITULANDO

Neste capítulo foi apresentada uma das partes mais importantes na fundamentação dos conhecimentos de redes de computadores: o protocolo IP e, principalmente, como é feito o seu endereçamento. Pôde-se observar de onde surgiram as classes de endereçamento IPv4, sua evolução de *classfull* para *classless* e as máscaras de sub-rede. Além disso, tomou-se conhecimento do CIDR, que representou uma evolução e uma sobrevida para o IPv4. Foi demonstrado como criar sub-redes com tamanhos variados para melhor aproveitamento do espaço de endereçamento disponíveis.

Na sequência, foi apresentado o IPv6, a versão mais recente do protocolo que surgiu da necessidade de se ter um esquema de endereçamento que permitisse a continuidade de crescimento das redes; principalmente da internet e outras funcionalidades implementadas no novo protocolo, como a possibilidade de cabeçalhos de extensão. Por fim, foi apresentado o protocolo ICMP, muito importante para testes e monitoramento de uma rede.

Exercícios

1. Explique o que são as classes de redes e por que foram criadas.
2. O que são endereços privados, reservados e públicos?
3. Quantos bits possui um endereço IPv4?
4. O que é CIDR e por que ele foi criado?
5. Dado o conjunto IP e máscara de sub-rede, encontre o endereço de sub-rede, endereço de *broadcast*, primeiro host, último host, quantidade de hosts por sub-rede e quantidade de sub-redes:
 - a) 192.168.10.189 – 255.255.255.192
 - b) 192.168.189.10 – 255.255.255.224
 - c) 172.17.200.54 – 255.255.254.0
 - d) 172.29.75.132 – 255.255.240.0
 - e) 10.179.63.5 – 255.255.255.0
 - f) 10.250.18.156 – 255.128.0.0
6. O que é VLSM e por que foi criado?
7. Utilizando VLSM, encontre o endereço de sub-rede e máscara de cada uma das sub-redes, para atender o seguinte cenário: você tem disponível o endereço 172.16.0.0/20 e precisa criar duas redes com 450 hosts, quatro redes com 200 hosts e dez redes com 90 hosts.
8. Explique o principal motivador da criação do protocolo IPv6.
9. Por quantos bits são formados os endereços IPv6?
10. O que são os cabeçalhos de extensão do IPv6? Qual a importância deles?
11. Qual a principal função do protocolo ICMP?
12. Explique o que é um teste de *ping*.

As respostas dos exercícios deste livro estão disponíveis para *download* no seguinte *link*: https://www.senaispeditora.com.br/downloads/respostas/redes_computadores_respostas.pdf

8. Camada enlace e camada física

Características da camada física

Camada enlace

Protocolos da camada enlace

Neste capítulo serão apresentadas as camadas enlace e física, pois, como na arquitetura TCP/IP, elas trabalham juntas. Apresentá-las em conjunto é mais simples e facilita o entendimento, uma vez que elas são muito dependentes uma da outra e até mesmo definidas de forma única em alguns protocolos. Serão estudados primeiro os conceitos básicos da camada física, que serão úteis principalmente para o entendimento dos protocolos de enlace. Além disso, os principais protocolos da camada enlace que são utilizados atualmente serão analisados e, brevemente, também será visto alguns protocolos já obsoletos, somente a título de conhecimento e comparação com os atuais. No entanto, o foco maior será nos protocolos Ethernet e ARP, fundamentais para as redes locais.

Características da camada física

Como já foi visto, pode-se definir comunicação como sendo a transferência de informação de um transmissor para um receptor. O principal objetivo em uma comunicação é fazer informações chegarem ao destino final de forma íntegra, sem perdas ou distorções, com qualidade para que decisões possam ser tomadas, sem que haja dúvidas sobre o conteúdo da informação.

Toda informação precisa de um meio de comunicação para ser transmitida, como o som, por exemplo. Para ser transmitido e alcançar um destino, ele precisa do ar para ser irradiado. Da mesma maneira ocorre a comunicação verbal,

que se propaga e é transmitida pelo ar, justamente por um de seus elementos ser o som, a fala.

Já os equipamentos eletrônicos podem se comunicar por meio de sinais elétricos transmitidos por um condutor metálico, por exemplo um cabo de rede. Nesse caso, o cabo de rede é o meio de transmissão e faz com que o sinal elétrico se propague e transporte as informações.

No caso de redes de computadores, é possível ainda transportar informações entre dois equipamentos por meio de propagação de ondas eletromagnéticas, como por exemplo nas transmissões que se utilizam rádio micro-ondas e satélites.

Uma forma de comunicação muito utilizada atualmente por apresentar excelente performance é a feita por meio óptico, isto é, fibras ópticas.

A camada física, portanto, é justamente o meio físico da comunicação, seja elas ondas eletromagnéticas, cabos de rede, fibras ópticas ou outros. O elemento que necessita da camada física para ser propagado e efetivar a comunicação é chamado sinal elétrico. Nos tópicos a seguir serão apresentados detalhes sobre os tipos de sinais e suas características.

Sinais elétricos

Existem dois tipos de sinais elétricos: analógicos e digitais. O sinal elétrico é sempre variável e pode ser entendido como uma onda gerada pela variação de uma tensão elétrica. Essa onda se propaga por um meio de transmissão, que pode ser metálico, quando transmitida por fios, ou o ar, quando é irradiada por antenas. Isto é, o sinal elétrico variável básico é uma onda analógica que possui variação constante e estável, conhecida como onda senoidal (Figura 1). As variações dessa onda senoidal, por sua vez, produzem os chamados sinais analógicos, que podem ser de diferentes formatos.

Sinais analógicos



Figura 1 – Sinal analógico.

Fonte: Senai-SP.

A onda senoidal básica varia, porém possui um padrão que se repete, chamado de ciclo. Cada ciclo demora um determinado tempo para ocorrer, denominado “período de tempo”. O número de vezes que o ciclo se repete por segundo é chamado de frequência e é medido em Hertz. Existe, então, uma faixa de frequência, ou seja, uma faixa em que há ciclos menores e maiores.

HERTZ = CICLOS POR SEGUNDO

Outro conceito fundamental, relacionado ao sinal elétrico, para se entender o analógico, é sua amplitude de onda, isto é, sua altura. A amplitude de onda é medida em volts no caso de sinais elétricos. Assim, sendo o sinal analógico uma onda que varia continuamente e é transmitida por diversos meios, em frequência e amplitude, ele está sujeito a distorções, atenuações e ruídos ao longo de sua transmissão. Isso faz com que as transmissões analógicas tenham uma qualidade variável de acordo com o meio e com os equipamentos utilizados, uma vez que os aparelhos e meios físicos interferem nas características das ondas.

Sinais digitais

Diferentemente do sinal analógico, que varia continuamente e pode assumir todos os valores entre sua amplitude máxima e mínima, o sinal digital binário só assume

dois valores. Ele salta de um valor para o outro instantaneamente, formando então uma onda que, diferente da do analógico, não é variável, mas é como se fosse quadrada, conforme pode ser visto na Figura 2. Esses dois valores encontraram a representação em caracteres na solução de base binária – também chamada de base 2 – na qual os caracteres são representados por dois dígitos básicos (0 e 1), combinados entre si.

Assim, o sinal elétrico com uma determinada voltagem representa o dígito 1 e com uma outra voltagem representa o dígito 0. Por exemplo, existem equipamentos em que o dígito 1 é representado pela tensão de +15 volts, e o dígito 0, pela tensão de -15 volts.

A leitura do valor do sinal em um determinado instante, no caso digital binário, pode ser somente 1 ou 0. Isso torna a detecção do sinal muito mais fácil, mesmo que ele sofra alguma deterioração ao longo do caminho de transmissão.

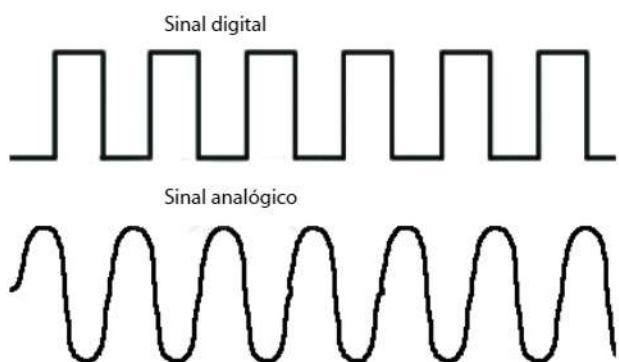


Figura 2 – Comparação sinal analógico x digital.

Agora que já foram apresentados os sinais elétricos de ambos os tipos, pode-se partir para outro conceito relacionado à camada física: os tipos de comunicação que ela efetua. São os chamados “modos de operação da camada física”.

Modo de operação simplex

A comunicação simplex ocorre quando há um dispositivo transmissor e um dispositivo receptor e esse papel de ambos nunca se inverte. A comunicação é unidirecional, ou seja, ocorre somente em uma direção, do transmissor para o

receptor, não havendo retorno do receptor. Pode-se ter um dispositivo transmissor para vários dispositivos receptores, mas nunca há sinalização do receptor que confirme se os dados foram ou não recebidos. Um exemplo de comunicação simplex é a televisão aberta: os transmissores das empresas de TV enviam os sinais e as antenas dos televisores os recebem.

Modo de operação half-duplex

Uma comunicação é chamada de half-duplex ou semiduplex quando há um dispositivo transmissor e outro receptor e ambos podem transmitir e receber dados, porém não simultaneamente. Ou seja, a transmissão tem sentido bidirecional. Por exemplo, o dispositivo A pode transmitir dados para B receber, e, em seguida, o sentido da transmissão é invertido e B passa a transmitir para A.

A operação de troca de sentido de transmissão entre os dispositivos é chamada de *turn-around* e o tempo necessário para os dispositivos chamearem entre as funções de transmissor e receptor é chamado de *turn-around time*. Como exemplo, têm-se as placas de rede e portas de switches que podem operar em half-duplex seguindo as características descritas.

Modo de operação full-duplex

Uma comunicação é chamada de full-duplex quando existe um dispositivo transmissor e outro receptor e os dois podem transmitir dados simultaneamente em ambos os sentidos. Nesse caso a transmissão é bidirecional. Como as transmissões podem ser simultâneas em ambos os sentidos e não existe perda de tempo com o *turn-around*. Uma linha full-duplex pode transmitir mais informações por unidade de tempo do que uma linha half-duplex, considerando a mesma taxa de transmissão de dados. A maioria das placas de rede e switches atuais operam em full-duplex.

Sabe-se agora que os sinais podem ser transmitidos pelo modo simplex, half-duplex ou full-duplex. Porém, há ainda outra característica da camada física a ser estudada: os tipos de transmissão. Como as informações perpassam o meio físico e efetuam a comunicação é o tema dos próximos itens.

Transmissão paralela

A transmissão paralela se caracteriza por agrupar bits e enviá-los simultaneamente por meios de transmissão diversos. Isto é, a cada ciclo, o grupo todo de bits será transmitido ao mesmo tempo por conjunto de condutores, o que, teoricamente, aumenta a taxa de transmissão, uma vez que acontece em um grande fluxo de uma só vez.

Neste tipo de transmissão, o tratamento da informação é mais controlado e complexo. Isso porque as rajadas de informações devem ser recebidas, reagrupadas e verificadas para caso existam erros. Todo esse processo nem sempre é o mais rápido, se comparado a uma transmissão serial. Espera-se sempre que a transmissão paralela seja mais veloz, porém esse é um dos fatores que, na prática, a desaceleram.

Outro fator importante refere-se ao tamanho dos cabos. Quanto maior for o cabo, maiores são as chances de um fio condutor ser maior do que o outro, o que fisicamente poderia trazer problemas para a transmissão. Num condutor maior, a informação levará mais tempo para chegar até o seu destino, e então, dessa forma os dados distribuídos nos diversos fios não chegariam ao destino no mesmo exato momento, o que dificultaria ainda mais o tratamento da informação.

Assim, a transmissão serial, apesar de ser menos adequada em termos de quantidade de informação, acaba por ser mais útil em razão de sua eficácia de processo.

Transmissão serial

A comunicação serial difere da paralela por ter apenas um par de fios condutores e transmitir os bits um a um. No dispositivo receptor, os bits são agrupados em bytes, conjuntos de 8 bits. Desse modo, o controle torna-se mais simples e o problema da diferença de tamanho entre os condutores não existe.

Vistos os principais elementos e características contribuintes para a atuação da camada física, pode-se partir para a descrição do funcionamento da camada enlace.

Camada enlace

A camada enlace é a camada responsável por detectar e corrigir erros da camada física. No caso da recepção dos dados, também é responsável por converter endereços lógicos em endereços físicos, como endereços IP em endereços MAC. Nos próximos itens serão descritos os protocolos pelos quais ela executa essas tarefas.

Protocolos da camada enlace

Token Ring

No Capítulo 3, mencionou-se, ao tratar das topologias de rede, as redes em anel Token Ring, desenvolvidas pela IBM na década de 1980, que apesar de utilizar uma topologia lógica em anel, valia-se de uma topologia física em estrela, contrariando o que muitos pensavam. Eram utilizados hubs Token Ring, (Figura 3) nos quais todos os computadores eram interligados por meio de cabos de par trançado, padronizados pela IBM. As redes Token Ring inicialmente suportavam 4 Mbps e posteriormente 16 mbps, o que na época era uma velocidade muito superior aos 10 Mbps das redes Ethernet. Aqui, porém, trata-se de seu protocolo, que recebeu o mesmo nome.

Conforme visto no Capítulo 3, o protocolo Token Ring funcionava com base em uma tradição indígena, a de utilizar, em reuniões um bastão denominado “bastão da fala”, ou *token*, em inglês. Esse bastão circulava durante a reunião, passando de mão em mão, até que, quando alguém quisesse falar, retinha o bastão consigo, falava e o fazia circular novamente. O protocolo funcionava da mesma forma: um *token*, que era um quadro de 3 bytes, circulava pela rede, passando de computador por computador, e, quando um deles precisava transmitir, retirava o *token* da rede, transmitia e depois disso recolocava o *token* na rede para que outro computador pudesse utilizá-la.



Figura 3 – Hub Token Ring.

Fonte: SellerPro.

X.25

O protocolo X.25 é bem antigo: foi lançado em 1970. Ele tem uma infraestrutura de transmissão baseada em redes de telefonia e cria circuitos virtuais entre os terminais, mantendo a comunicação ativa. Era muito utilizado por operadoras de cartão de crédito por ser um protocolo seguro com a detecção e correção de erros, rápido e com baixa necessidade de recursos. Até hoje algumas operadoras de cartão de crédito utilizam essa tecnologia, apesar de ter sido substituída aos poucos por tecnologias móveis como redes 3G e 4G e redes fixas por conexões de internet ADSL.

Frame Relay

O Frame Relay é um protocolo que surgiu no final da década de 1980, já na fase de implantação de redes de fibra óptica nos Estados Unidos. Como a fibra óptica é um meio de transmissão mais estável do que os cabos metálicos por ser livre de interferências, o Frame Relay foi criado sem controle de fluxo e correção de erros esperando que a quantidade de erros fosse mínima, privilegiando desta forma o desempenho – sem muitos controles que poderiam causar uma carga de processamento maior. Quando um dispositivo transmite por Frame Relay e este detecta um erro, a única ação disponível no protocolo é descartar o quadro. Isso implica a necessidade de sistemas finais mais sofisticados que entendam a perda dos quadros e solicitem uma retransmissão.

O uso de Frame Relay está cada vez menor porque vem sendo substituído gradativamente por tecnologias mais novas como o MPLS ou links dedicados.

Asynchronous Transfer Mode – ATM

Entre o fim da década de 1980 e início da década de 1990 as redes de longa distância precisavam de sistemas com velocidades maiores para suprir as necessidades que a evolução tecnológica trazia. Era preciso realizar, por exemplo, a introdução de interface gráfica nas aplicações e o aumento da capacidade de processamento nos terminais dos usuários.

O ATM surge então para atender a essa demanda. É uma tecnologia que utiliza quadros de tamanho fixo, denominados de células com 53 bytes, sendo 48 bytes para os dados e 5 bytes de cabeçalho. É um protocolo orientado à conexão, ou seja, recebe confirmação dos quadros enviados. As velocidades do ATM começaram em 25 Mbps, depois passaram para 51 Mbps, 155 Mbps em cabeamento metálico até atingirem 622 Mbps com fibra óptica.

Seu uso nos Estados Unidos foi tão popular nas redes de caixas eletrônicos, que por lá e em outros locais do mundo esse tipo de caixa ainda é chamado de ATM, conforme ilustrado pela Figura 4.



Figura 4 – ATM.

Fonte: Thinkstock.

High Level Data Link Control – HDLC

O protocolo HDLC, High Level Data Link Control, foi definido pela ISO no padrão 6256:1981 e é um protocolo de camada enlace para transmissão de longa distância. Foi criado com base no protocolo da IBM SDLC, muito utilizado em todo o mundo pelo uso de meio físico de linhas telefônicas, mas foi substituído pelo PPP com o crescimento da internet.

Point-to-Point Protocol – PPP

O PPP é um protocolo utilizado para estabelecer um enlace direto entre dois dispositivos numa rede. Tem a característica interessante de poder utilizar diversos tipos de redes físicas, como redes de cabeamento metálico com cabo serial ou linha telefônica, fibra óptica e redes sem fio.

Esse protocolo permite autenticação e criptografia entre os dispositivos, aumentando consideravelmente a segurança. O PPP inicialmente foi muito utilizado por provedores de acesso que utilizavam linhas telefônicas discadas e modems para a autenticação dos usuários.

Atualmente, porém, alguns provedores utilizam uma modificação desse protocolo, uma versão mais recente que é o PPPoE (*Point-to-Point over Ethernet*) para autenticar usuários que se valem de tecnologias DSL, como será apresentado ainda neste capítulo.

Asymmetric Digital Subscriber Line – ADSL

Atualmente, o ADSL é o padrão mais utilizado em redes de internet residenciais. No início da popularização da internet, no Brasil havia somente conexões discadas, ou seja, que utilizavam modems conectados a linhas telefônicas e um software “discador”. Esse software realizava a conexão com o provedor. Era uma linha analógica convencional, limitada a 56 kbps, mas tinha um custo muito elevado, pois era tarifada de acordo com os pulsos telefônicos, como se o usuário estivesse em uma ligação. Quando o ADSL foi introduzido pelas operadoras do Brasil houve um grande crescimento da internet residencial, devido aos custos menores e um aumento considerável na qualidade.

Como o tráfego de internet geralmente é mais usado para *download*, ou seja, para transmitir informações no sentido da internet para o usuário, e um pequeno tráfego de *upload* – do usuário para a internet – um padrão assíncrono como o ADSL se encaixa muito bem nesse perfil de uso isso porque o ADSL apresenta uma taxa de transferência – ou velocidade – maior de *download* do que de *upload*.

Apesar do ADSL ser o padrão mais popular, ele não é único. Existem vários outros com o mesmo mecanismo, como por exemplo:

- RADSL – Rate Adaptative DSL.
- HDSL – High bit-rate DSL.
- VDSL – Very High bit-rate DSL.

Ethernet

Em 1972, Robert Metcalfe, um pesquisador que trabalhava na Xerox PARC, desenvolveu o primeiro protótipo experimental de uma conexão do tipo Ethernet para comunicar uma *workstation* até uma interface gráfica. Naquela época, as redes eram do tipo barramento e, conforme foi visto no Capítulo 1, compartilhavam o mesmo meio físico para a transmissão. Além disso, eram baseadas somente em protocolos proprietários. Metcalfe então propôs, em 1973, um novo padrão que pudesse ser utilizado em qualquer tipo de rede, o Ethernet. O nome vem da palavra éter, que em uma tradução informal é um fluido imaterial hipotético que permeia todo o espaço e que, naquele momento, já se supunha ser necessário para a propagação das ondas eletromagnéticas. Apesar dessa teoria ter sido demonstrada falsa, ainda assim o padrão foi batizado com esse nome como uma homenagem a ela. Em junho de 1976, Metcalfe apresentou o padrão na National Computer Conference, quando despertou o interesse da comunidade científica e principalmente do IEEE, que, em 1980, padronizou a Ethernet como protocolo 802.3.

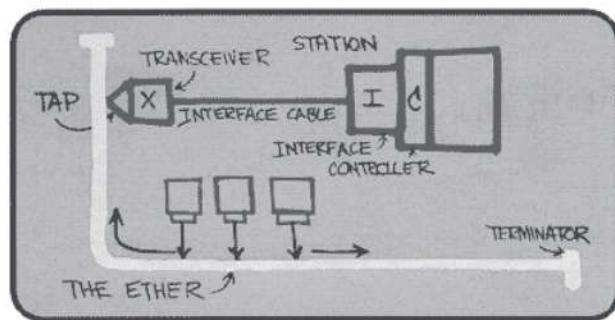


Figura 5 – Rascunho do padrão Ethernet.

Fonte: Senai-SP.

Três elementos compõem o padrão Ethernet: o meio físico, o controle de acesso ao meio e o quadro Ethernet. Isto é, o Ethernet agrupa os dados recebidos das camadas superiores, TCP ou UDP e IP, e os encapsula em quadros Ethernet. O controle do link lógico, (LLC – Logical Link Control) definido pelo IEEE 802.2, informa qual protocolo de nível superior entregou o pacote de dados a ser convertido em quadro,

para manter um link entre camada 2 e camada 3, isto é, entre a camada enlace e sua superior. O controle de acesso ao meio (*MAC – Media Access Control*) monta o quadro de dados que deve ser transmitido pela camada física, encapsulando os dados recebidos da camada LLC, conforme descrito na Figura 6.

Preâmbulo (8 bytes)	Mac de destino (6 bytes)	Mac de origem (6 bytes)	Tipo (2 bytes)	Dados	FCS (4 bytes)
------------------------	-----------------------------	----------------------------	-------------------	-------	------------------

José Wagner Bürgart

Figura 6 – Cabeçalho Ethernet 802.3.

Essas informações podem ser mais bem compreendidas se entendermos os dados contidos no cabeçalho do protocolo Ethernet:

- **Preâmbulo:** é composto por uma sequência de sete bytes que permite sincronizar sua temporização de entrada. Os sete primeiros bytes, na verdade, pertencem à camada física. O sétimo byte é a sequência binária 10101011 que sinaliza o início do quadro Ethernet 802.3.
- **MAC de destino:** indica o endereço MAC do equipamento de destino.
- **MAC de origem:** indica o endereço MAC do equipamento de origem.
- **Tipo:** informa o protocolo utilizado na camada superior, ou seja, na camada rede.
- **Dados:** são os dados vindos das camadas superiores com seus respectivos cabeçalhos. Esse campo é sempre maior do que 46 e de no máximo 1.500 bytes, salvo quando utilizado *Jumbo Frame*.
- **FCS (Frame Check Sequence):** é o campo que faz uma checagem de integridade do quadro.

Carrier Sense Multiple Access with Collision Detection – CSMA/CD

Uma característica estudada anteriormente é a das redes poderem ser half-duplex, ou seja, quando informações estão sendo transmitidas em um meio físico compartilhado, outras estações não podem transmitir simultaneamente. Para controlar e sincronizar transmissões em meios físicos compartilhados, o IEEE desenvolveu um método de controle chamado CSMA/CD. Para explicar o funcionamento do CSMA/CD é apresentada a seguir uma analogia muito criativa de Kurose & Ross (2010):

- **Ouça antes de falar:** se uma pessoa estiver falando, espere que ela tenha terminado. No mundo de redes, isso é denominado **detecção de portadora**: um nó ouve o canal antes de transmitir. Se um quadro estiver correntemente sendo transmitido para dentro do canal, o nó então esperará (se afastará, “back-off”) por um período de tempo aleatório e, então, novamente sondará o canal. Se perceber que o canal está ocioso, o nó então começará a transmissão de quadros. Caso contrário, ele esperará por um período aleatório de tempo e repetirá esse processo.
- **Se alguém começar a falar ao mesmo tempo que você, pare de falar:** no mundo de redes, isso é denominado **detecção de colisão**, um nó que está transmitindo ouve o canal enquanto transmite. Se esse nó detectar que outro nó está transmitindo um quadro interferente, ele para de transmitir e usa algum protocolo para determinar quando deve tentar transmitir novamente. Ao usar essas regras de transmissão, um computador que utiliza o padrão Ethernet sabe quando pode começar uma transmissão e pode detectar colisões, caso elas ocorram.

Como evolução do padrão Ethernet original, que tinha uma velocidade limitada a 10 Mbps e utilizava somente o modo de transmissão half-duplex, surgiram outros padrões, mais utilizados atualmente e com um desempenho superior, conforme listado a seguir:

- **Fast Ethernet IEEE 802.3u:** velocidade limite de 100 Mbps e o modo de operação pode ser tanto half-duplex como full-duplex.
- **Gigabit Ethernet IEEE 802.3z:** velocidade aumentada para 1 Gbps; o tamanho mínimo do quadro também foi aumentado, passando agora para 512 bytes. Foi desenvolvido para manter compatibilidade com os padrões Ethernet e Fast Ethernet e continuar suportando tanto half-duplex quanto full-duplex.
- **TenGigabit Ethernet IEE 802.3ae:** velocidade de 10 Gbps; não suporta mais half-duplex, consequentemente não utiliza CSMA-CD.
- **40 e 100 GigabitEthernet IEEE 802.3bm:** recentemente, em 2015, o IEEE definiu os padrões para transmissões de 40 e 100 Gbps no padrão Ethernet.

Address Resolution Protocol – ARP

O protocolo ARP tem a função de transformar endereços IP em endereços de camada enlace, ou seja, em endereços MAC. O ARP foi definido em novembro de 1982 na RFC 826 (<https://tools.ietf.org/html/rfc826>). Quando dois computadores

se comunicam em uma mesma rede lógica, a codificação do seu endereço IP em um endereço físico de MAC é necessária e então a máquina que precisa descobrir um endereço MAC a partir de um endereço IP envia um *broadcast* para a rede com a solicitação do endereço MAC de quem possui aquele IP.

Para explicar melhor o funcionamento do ARP, há o seguinte exemplo: um computador com IP 10.1.1.23 dispara um comando *ping* para o computador com IP 10.1.1.6. Conforme visto anteriormente, se o computador de destino estiver acessível na rede, ele responderá ao *ping*, mas como ambos os computadores estão na mesma rede lógica, será necessária a tradução do endereço IP no endereço MAC onde este IP de destino está configurado. Antes de enviar o pacote ICMP *Echo Request*, o computador de origem dispara um *broadcast* do tipo ARP *Request* (Figura 7) na linha número 2275, informando que o endereço MAC do computador de origem é 1c:39:47:0d:a3:1a e o endereço MAC de destino é ff:ff:ff:ff:ff:ff, ou seja, um *broadcast*. O que o ARP *Request* faz na verdade é perguntar para todos: “Quem tem 10.1.1.6? Diga para 10.1.1.23”.

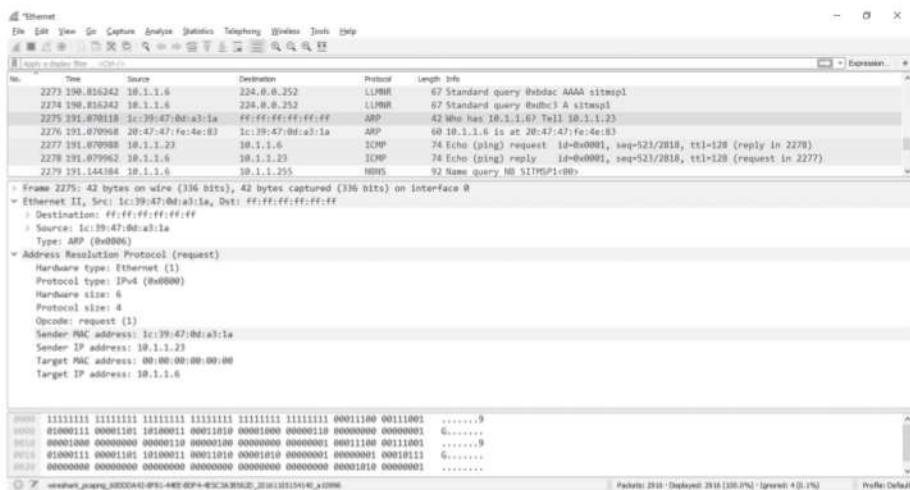


Figura 7 – ARP Request.

Logo em seguida, na linha 2276 vem a resposta da máquina com o IP 10.1.1.6, conforme pode-se observar na Figura 8, em que há o ARP *Reply* do computador 10.1.1.6 informando o seu endereço MAC, 20:47:fe:4e:83. Essa resposta já é um *unicast* direcionado para o computador com o IP 10.1.1.23.

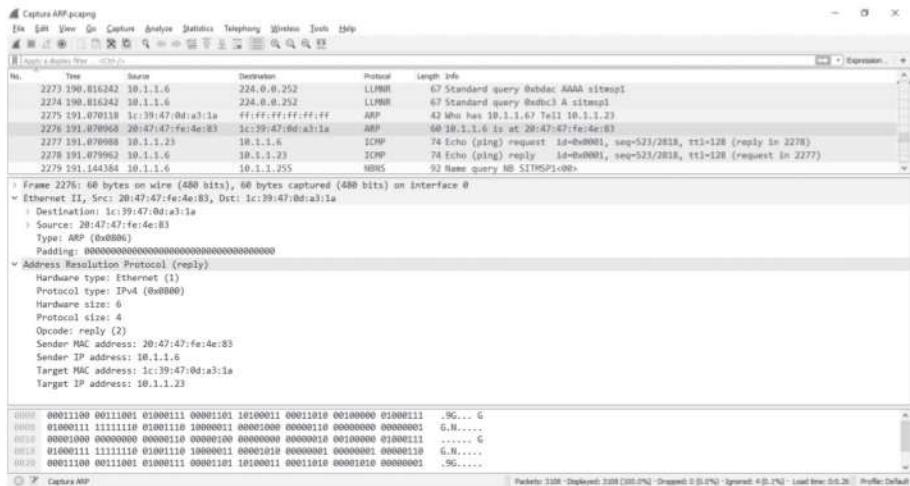


Figura 8 – ARP Reply.

Com a descrição de todos esses protocolos, torna-se possível conhecer todo o mecanismo de funcionamento das redes e os devidos protocolos de suas camadas. No Capítulo 9, o assunto continua com ênfase nas redes sem fio e seu mecanismo.

RECAPITULANDO

Neste capítulo foram apresentadas as principais características da camada enlace e da camada física e os conceitos importantes para o entendimento dos protocolos dessas camadas baixas. Um resumo dos protocolos da camada enlace mais utilizados no passado e atualmente foi apresentado, com uma ênfase maior nos protocolos Ethernet e ARP, pois são muito importantes no estudo das redes de computadores locais, próximo tópico do livro.

Exercícios

1. Explique o que é frequência e amplitude de um sinal elétrico analógico.
2. Explique o que é um sinal digital e o que o difere de um sinal analógico.
3. Explique a diferença entre simplex, half-duplex e full-duplex.
4. O que compõe o padrão Ethernet?
5. Como é o endereçamento no padrão Ethernet?
6. Por que o padrão Ethernet sofre frequentes alterações?
7. Explique de maneira simplificada como funciona o protocolo ARP.

As respostas dos exercícios deste livro estão disponíveis para *download* no seguinte *link*: https://www.senaiseditora.com.br/downloads/respostas/redes_computadores_respostas.pdf

9. Redes sem fio

Definição

Classificação de redes sem fio

Ondas eletromagnéticas

Tipos de transmissão sem fio

Órgãos e padrões de redes WLAN

Conceitos de redes WLAN

Protocolos 802.11

As redes sem fio, wireless, estão presentes na maioria das redes de comunicação, sejam elas empresariais ou residenciais. Graças à facilidade de instalação, redução de custos e mobilidade oferecida, elas estão se tornando cada dia mais populares.

Uma rede sem fio possui a característica de não utilizar um meio guiado de comunicação, como as redes cabeadas utilizam, por exemplo, cabos metálicos ou fibra óptica. No entanto, elas ainda assim possuem um meio físico, pois realizam a transmissão por ondas eletromagnéticas que se propagam pelo ar e podem transportar diversos obstáculos, como a água, paredes e vidro, cada um com características diferentes.

Como se trata de um meio de transmissão naturalmente vulnerável, é necessário entender o funcionamento das tecnologias sem fio as formas de ataques utilizadas e como garantir a segurança ou maximizar a proteção desse tipo de rede.

Este capítulo apresenta as redes sem fio com um foco maior em WLANs. Nele são estudados os conceitos básicos, os protocolos, o funcionamento e a configuração de redes sem fio.

Definição

Uma rede sem fio é como qualquer comunicação existente entre dois computadores. Esses, por sua vez, no âmbito do estudo das redes wireless, são comumente chamados de terminais em redes sem fio. A diferença entre as redes com e sem fio é que estas não utilizam um meio guiado para o transporte das informações. As redes sem fio se caracterizam por utilizar o ar como meio de comunicação e utilizam a transmissão por meio de ondas eletromagnéticas, em vez de elétrons ou luz, como acontece nos meios de transmissão metálicos e ópticos.

Classificação de redes sem fio

As redes sem fio podem ser classificadas em relação a sua abrangência, conforme visto no Capítulo 1. Para relembrar essa classificação, é importante retomar alguns conceitos e apresentar outros novos. Eles facilitam a identificação da abrangência da rede, sua função e a dos demais equipamentos envolvidos em sua arquitetura.

WPAN (Wireless Personal Area Network): as redes PAN possuem uma área de abrangência muito pequena e seu objetivo é atender às necessidades pessoais dos usuários, como, por exemplo, conectar aparelhos celulares a computadores e impressoras. Atualmente, essas redes são muito utilizadas com as tecnologias Bluetooth e UWB (Ultra Wideband). Como exemplo existem as padronizações feitas pelo IEEE 802.15.

WLAN (Wireless Local Area Network): são redes locais sem fio, ou seja, que utilizam alguma tecnologia de interconexão cujo meio de transmissão é o ar. É uma forma muito rápida e relativamente barata de prover conectividade entre computadores e outros dispositivos de acesso local, pois não dependem de cabeamento metálico ou fibra óptica, por exemplo: IEEE 802.11.

WMAN: são redes metropolitanas sem fio para atender uma necessidade intermediária entre as WLANs e WWANs, possuindo uma velocidade alta e uma mobilidade maior. Sempre que uma rede ultrapassar os limites geográficos de um

prédio ou *campus*, mas não sair dos limites de uma cidade, é classificada como uma rede metropolitana.

WWAN: funcionam a partir de redes de telefonia móvel ou por satélites e utilizam sua infraestrutura para também transportar dados. Sua abrangência depende da área de cobertura da operadora de telefonia móvel, mas pode ser ampla o suficiente para ser considerada uma WAN. Nasceu da necessidade de dispositivos especiais, como telemetria de veículos, e demanda a conexão ininterrupta a uma rede sem perder a capacidade de mobilidade, mesmo que com uma velocidade mais baixa se comparada às WLANs. Atualmente, são bastante utilizadas por pessoas e empresas com tecnologias 3G e 4G.

Ondas eletromagnéticas

Uma vez que as redes sem fio não possuem cabeamento para estabelecer conexão entre os dispositivos, é preciso conhecer o meio pelo qual ela é transmitida e realizada. No início deste capítulo viu-se que as redes wireless se propagam por ondas eletromagnéticas, porém o que isso significa? No tópico sobre sinais elétricos pôde-se aprender um pouco sobre elas, mas agora é preciso aprofundar esse conhecimento.

As cargas elétricas geram campos elétricos ao seu redor, e seu movimento também gera campos magnéticos (Descoberta de Oersted). Assim, quando aceleradas, as cargas elétricas produzem ondas eletromagnéticas. As estações transmissoras de rádio e TV são exemplos de fontes de ondas EM (eletromagnéticas). A parte fundamental dessas estações é um circuito oscilante que induz na antena uma corrente elétrica oscilante: do topo da antena para a terra e da terra para a antena. Os elétrons livres são fortemente acelerados e retardados emitindo, desta forma, ondas eletromagnéticas cuja frequência é a mesma do vaivém dos elétrons na antena. Uma vez emitida, as ondas EM propagam-se no espaço até serem absorvidas pela matéria ou captadas por antenas receptoras de rádio e/ou televisão.

Na Figura 1 há uma animação demonstrando a formação de ondas eletromagnéticas.

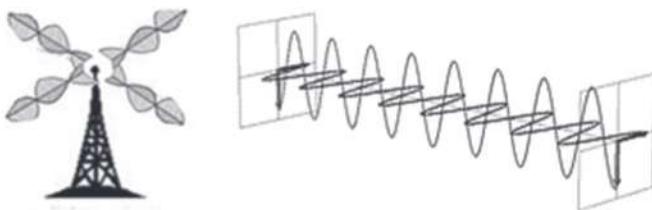


Figura 1 – Ondas eletromagnéticas.

Fonte: Show de física. Instituto de Geociências e Ciências Exatas da Unesp.

A animação está disponível no seguinte link <www.rc.unesp.br/showdefisica/99_Explor_Eletrizacao/paginas%20htmls/Ondas%20EM%20anima%C3%A7%C3%A3o.htm>.

É importante lembrar que uma onda é formada por:

- **Comprimento de onda:** é a distância entre valores repetidos sucessivos num padrão de onda. É usualmente representado pela letra grega lambda (λ). Em uma onda senoidal, o comprimento de onda é a distância entre vales ou cristas (Figura 2).
- **Amplitude:** é a distância da crista até o eixo de propagação.

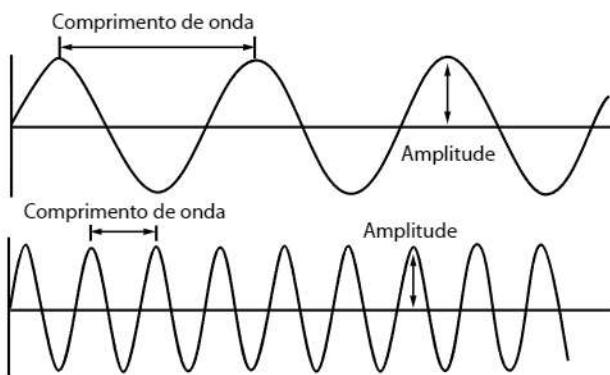


Figura 2 – Características de uma onda.

Fonte: Senai-SP.

- **Frequência:** é o número de oscilações ou ciclos por uma unidade de tempo.

$$f = 1/t$$

Onde:

t (período): intervalo de tempo necessário para a onda caminhar um comprimento de onda.

Conforme já visto, a unidade de medida da frequência da onda é Hertz (Hz), correspondente ao número de oscilações por segundo.

Exemplo 1

Uma determinada onda possui comprimento de onda de 1 milissegundo. Qual é a sua frequência?

$$f = 1/10^{-3} = 1 / 0,001 = 1000 = 1 \text{ KHz}$$

$$f = 1 \text{ KHz}$$

Tipos de transmissão sem fio

Existem basicamente três tipos de redes sem fio para transmissão de dados:

- infravermelho.
- radiofrequência (micro-ondas).
- laser.

O espectro total de frequências desses tipos é composto por:

- ELF: Extremely Low Frequency de 3 Hz a 30 Hz;
- SLF: Super Low Frequency de 30 Hz a 300 Hz;
- ULF: Ultra Low Frequency de 300 Hz a 3 KHz;
- VLF: Very Low Frequency de 3 KHz a 30 KHz;
- LF: Low Frequency de 30 KHz a 300 KHz;
- MF: Medium Frequency de 300 KHz a 3 MHz;
- HF: High Frequency de 3 MHz a 30 MHz;
- VHF: Very High Frequency de 30 MHz a 300 MHz;
- UHF: Ultra High Frequency de 300 MHz a 3 GHz;
- SHF: Super High Frequency de 3 GHz a 30 GHz;
- EHF: Extremely High Frequency de 30 GHz a 300 GHz.

Nos tópicos a seguir tem-se um panorama sobre o que são os tipos e as frequências de ondas no que diz respeito à relevância para os estudos de redes de computadores.

Infravermelho

A radiação infravermelha está em uma faixa de frequência não licenciada, ou seja, os equipamentos que utilizam essa tecnologia podem operar em qualquer lugar do mundo, sem requisitos específicos em cada país. São equipamentos de baixo custo, como por exemplo os controles remotos residenciais. O infravermelho pode ser transmitido com visada direta ou de forma difusa; ou seja, não precisa estar necessariamente apontado para o dispositivo remoto.

Tipicamente ele é utilizado para aplicações *indoor*, ou seja, dentro de ambientes fechados, uma vez que não é capaz de ultrapassar paredes. Porém, pode ser também utilizado *outdoor*, em ambientes externos, desde que seja com visada direta entre os elementos, podendo alcançar até 30 m de distância.

O infravermelho trabalha em frequências acima das radiofrequências, ou seja, as micro-ondas; e abaixo da luz visível. Ele é padronizado pela IrDA (Infrared Data Association), seguindo as especificações IEEE 802.11 Infrared Physical Layer.

Laser

Da mesma maneira que o infravermelho, os sistemas baseados em laser não utilizam frequência licenciada, ou seja, não precisam de outorga ou autorização para uso. Por usar a luz, esses sistemas exigem que os equipamentos possuam visada direta e trabalhem ponto a ponto, tendo um alcance médio de 10 km. A largura de banda pode chegar a 2,5 gbps.

Esses sistemas são chamados de FSO (Free Space Optics) e possuem uma lente que é capaz de duplicar o sinal em ângulos diferentes para que haja uma certa “redundância”. Isso permite que o sinal não seja interrompido facilmente, por exemplo, quando um pássaro passar em frente ao feixe. No entanto, neblina pode ser um problema grave para esse tipo de sistema.

Radiofrequência (micro-ondas)

As faixas de radiofrequência utilizadas para transmissão de dados são conhecidas como micro-ondas em razão do comprimento de onda utilizado. Essas frequências são conhecidas por ISM (Industrial Scientific Medical), são abertas e não

necessitam de autorização para serem utilizadas. No entanto, deve-se observar que apenas algumas frequências dentro do espectro de radiofrequência são classificadas como ISM; são elas 900 mHz, 2,4 GHz e 5 GHz.

Para exemplificar o uso dessas frequências, há o Wireless LAN em 2,4 GHz, com 13 canais na maioria dos países, ou, como no Brasil, 11 canais, conforme a Figura 3.

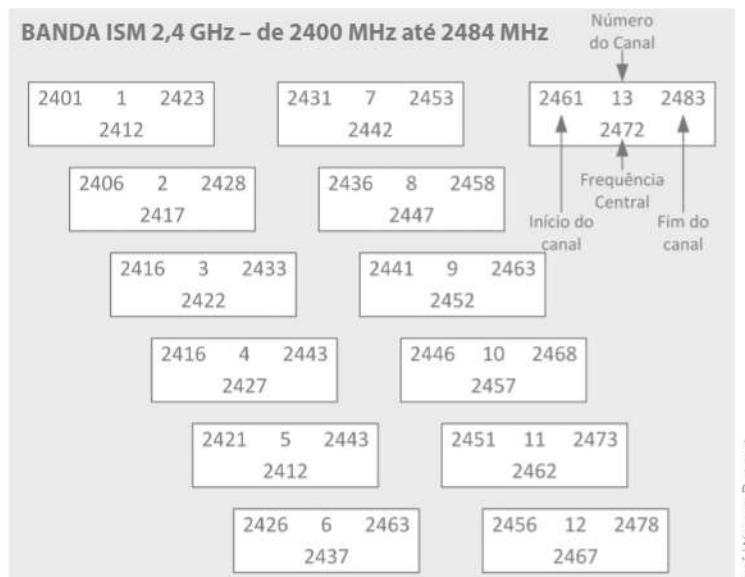


Figura 3 – ISM 2,4GHz.

Apesar de o ar – meio de transmissão de radiofrequência – não poder ser facilmente interrompido, ele está sujeito à absorção, atenuação e reflexão, além de interferências e ruídos.

Os principais fatores que atrapalham a propagação de sinais de radiofrequência são:

- **Frequência:** quanto maior a frequência, menor o alcance e maior a potência necessária.
- **Potência de transmissão:** aumentar a potência de transmissão melhora o sinal, mas ao fazer isso deve-se obedecer às regulamentações locais e estar ciente que isso aumentará o consumo das baterias dos terminais, se for o caso.
- **Antenas:** o posicionamento e o uso correto das antenas é essencial para uma boa transmissão.

- **Tipo de construção:** o tipo da construção do prédio onde o sinal deverá passar interfere diretamente no desempenho. Deve-se então conhecer a composição dos prédios ou paredes que o sinal deve transpor; por exemplo, concreto, gesso, vidro etc.
- **Sinais refletidos:** como acontece um espalhamento dos sinais de rádio, eles também são refletidos pelas superfícies, sem as transpassar, por isso deve-se levar em consideração a reflexão dessas superfícies.
- **Fontes de interferência:** vários aparelhos podem operar na mesma frequência ou em frequências muito próximas das redes WLAN, como telefones sem fio, interferindo diretamente nas redes sem fio.

Órgãos e padrões de redes WLAN

Existem algumas agências e órgãos regulamentadores das redes sem fio locais. São eles:

Agência Nacional de Telecomunicações – ANATEL: é o órgão responsável pela outorga, regulamentação e fiscalização das telecomunicações no Brasil, abrangendo telefonia fixa, telefonia móvel, comunicação multimídia, radiodifusão, TV por assinatura, radiofrequência, satélite e serviços limitados. Também é responsável pela homologação de aparelhos que utilizam qualquer um dos serviços regulamentados.

Federal Communications Commission – FCC: é o órgão regulador de Telecomunicações e Radiodifusão dos Estados Unidos, equivalente à ANATEL no Brasil.

European Telecommunication Standards Institute – ETSI: é o órgão que padroniza e regulamenta as telecomunicações na comunidade europeia.

Institute of Electrical and Electronics Engineers – IEEE: conforme visto no Capítulo 1, é uma organização que, além de promover a pesquisa, estabelece padrões de diversas áreas, inclusive em redes de computadores. O “Wireless Standards Zone” do IEEE é dedicado a padronizar tudo que está relacionado à tecnologia sem fio, como por exemplo:

- 802.11: Grupo de trabalho WLAN.
- 802.15: Grupo de trabalho WPAN.
- 802.16: Grupo de trabalho para padrões de acesso Wireless de banda larga.

Wi-Fi Alliance: é uma associação global da indústria, sem fins lucrativos, cujos participantes são a rede mundial de fornecedores de equipamentos e soluções Wi-Fi. O termo Wi-Fi surgiu de uma brincadeira com o termo Hi-Fi, que significa High Fidelity para definir uma qualidade superior em áudio. Dele surgiu então o termo Wireless Fidelity (Wi-Fi). Os membros do Wi-Fi Alliance trabalham de maneira colaborativa com o objetivo de criar um ecossistema e compartilhar a visão comum de todos os dispositivos conectados, em todos os lugares. Desde 2000, o selo Wi-Fi CERTIFIED de aprovação designa produtos com interoperabilidade comprovada e as proteções de segurança padrão da indústria. A Wi-Fi Alliance já certificou mais de 25 mil produtos, com o objetivo de oferecer a melhor experiência para o usuário e incentivar a ampliação do uso de produtos e serviços. Hoje, milhares de milhões de produtos Wi-Fi realizam uma parte significativa do tráfego de dados do mundo em uma variedade cada vez maior de aplicações.

Conceitos de redes WLAN

No Capítulo 1 e na introdução deste, foi possível conhecer e relembrar os tipos de redes existentes hoje em dia. Dentro da classificação de Wireless Local Area Network, existem alguns outros conceitos que devem ser mencionados:

Ad Hoc ou IBSS

As redes Ad Hoc conectam dispositivos wireless sem a necessidade de um dispositivo central, pois as próprias estações comunicam-se entre si. Isso é feito da seguinte maneira: um dispositivo define um nome para o grupo e os outros dispositivos o utilizam para a comunicação. A esse mecanismo dá-se o nome de Basic Service Set (BSS), que define a área na qual um dispositivo é alcançável. No caso das redes Ad Hoc, recebem o nome de Independent Basic Service Set (IBSS) por não precisarem de um elemento central, portal ou integração com outras redes (Figura 4). As estações recebem o nome de STA (Station).

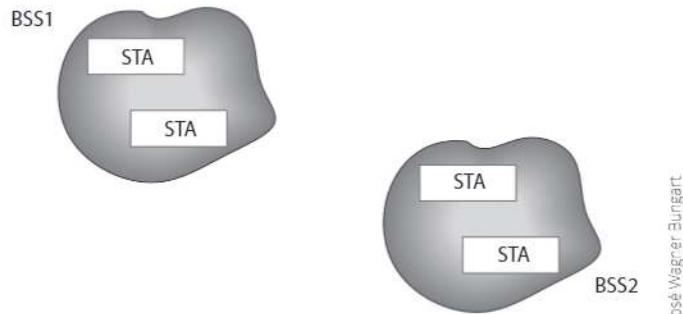


Figura 4 – Independent Basic Service Set.

Fonte: IEEE Std 802.11:2012

Network Infrastructure

As redes denominadas Infrastructure ou, em português, de infraestrutura, recebem esse nome pela indústria por haver um elemento central (ponto de acesso ou access point, conforme visto anteriormente) que será responsável pela conexão, autenticação, segurança e encaminhamento dos pacotes das estações (Figura 5). O padrão IEEE dá o nome de ESS a esse tipo de WLAN, como ver-se-á a seguir. Ele é comparado a um hub de uma rede cabeada, transmitindo os dados de forma half-duplex. Cada ponto de acesso possui seu endereço MAC e a rede ou grupo de trabalho se conecta a ele por meio do Service Set Identifier (SSID).

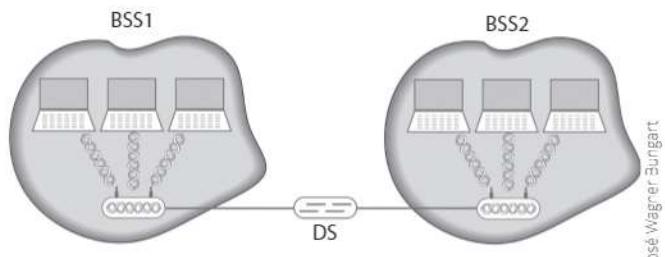


Figura 5 – Network Infrastructure.

Fonte: CCNA Wireless Official Exam Certification Guide – Cisco Press.

Distribution System

Muitas vezes a cobertura de um BSS apenas não é suficiente para uma rede, sendo necessário interligar vários BSSs para se obter a cobertura ideal. O componente utilizado para compor essa arquitetura é chamado de *Distribution System* (DS) (Figura 6). O padrão IEEE 802.11 separa o Wireless Media (WM) de um ponto de acesso (AP) do meio físico do DS, chamado de DSM (Distribution System Media), podendo esse ser o mesmo do AP ou não. Entender essa separação ajudará na compreensão de uma série de outras características e funcionalidades das redes 802.11. O padrão não especifica como deve ser o DSM, então ele pode ser um cabo metálico, fibra óptica ou até uma conexão sem fio.

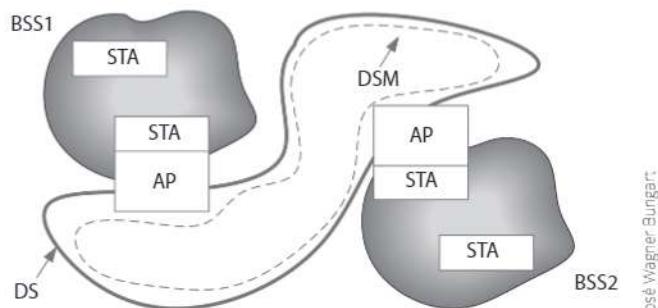


Figura 6 – Distribution System.

Fonte: IEEE Std 802.11:2012.

José Wagner Bungart

ESS sem comunicação externa

Quando dois ou mais BSS se conectam por meio de um DS, formam um ESS (Extended Service Set). O serviço oferecido pelo DS para essa conexão é chamado de DSS (Distribution System Service). Como já foi visto, o padrão não especifica como deve ser essa conexão física do DS, podendo ser cabeada ou wireless. Uma característica importante desse tipo de ESS é não possuir comunicação com outras redes, o que pode ser um pouco difícil de se encontrar atualmente, pois quase todas as redes possuem conexão com a internet.

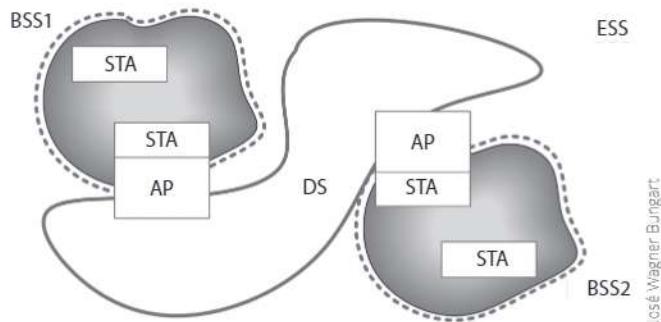


Figura 7 – Extended Service Set.

Fonte: IEEE Std 802.11:2012.

ESS com comunicação externa

Nesse tipo de rede, o ESS – formado pelos BSSs 1, 2 e mais o DS – se conectam a outra rede, o que é definido pelo padrão como portal. Para conexão com o portal, também é utilizado um DSS (Figura 8). Em outras palavras, o portal é o elemento definido pelo padrão IEEE 802.11 responsável pela comunicação com uma rede externa.

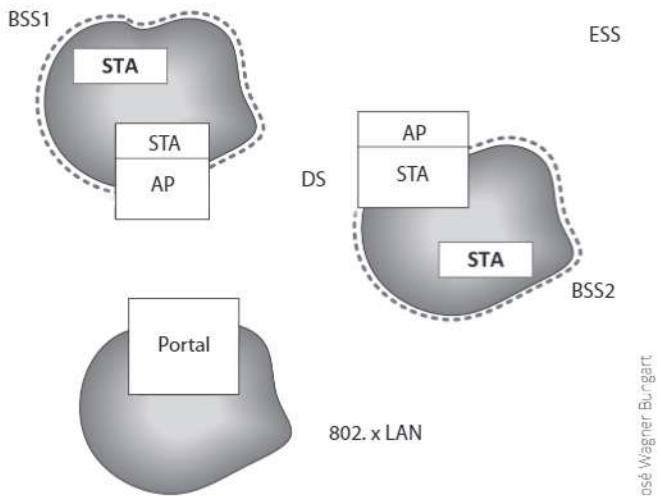


Figura 8 – ESS com comunicação externa.

Fonte: IEEE Std 802.11:2012.

Características dos BSSs, ESSs e DSs

- Os BSSs e DSs permitem criar redes de complexidades e tamanhos variados.
- Conforme foi visto, o ESS é a conexão de BSSs por meio de um DS, mas o ESS não inclui o DS pela definição do padrão 802.11.
- Uma característica importante das estações é que elas aparecem na camada LLC, podendo se comunicar com outras estações no mesmo BSS ou até mesmo de outros pertencentes ao mesmo ESS, somente com o conhecimento dos respectivos endereços MAC. Podem também se mover de um BSS para outro, do mesmo ESS, de forma transparente.
- Os vários BSSs podem ser disjuntos, sobrepostos ou ocuparem exatamente o mesmo espaço.

WorkGroup Bridge

A indústria denomina como WorkGroup Bridge a interligação de uma rede cabeada com uma outra rede cabeada, por meio de dois dispositivos wireless (Figura 9). Utiliza-se um wireless *Bridge* para essa finalidade, que na verdade é um ESS utilizando um DS cabulado.

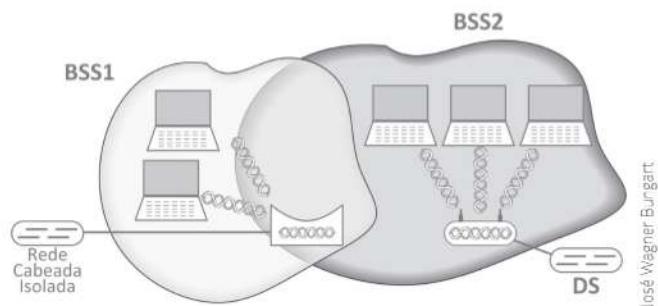


Figura 9 – *Bridge*.
Fonte: CCNA Wireless Official Exam Certification Guide – Cisco Press.

Repetidores

A diferença das redes com repetidores é que o repetidor atua como um access point, mas não se conecta à rede cabeada. Para ter um bom resultado desse tipo de rede é necessário que o repetidor esteja dentro de uma boa cobertura do primeiro access point, que, na verdade, é um ESS utilizando um DS sem fio.

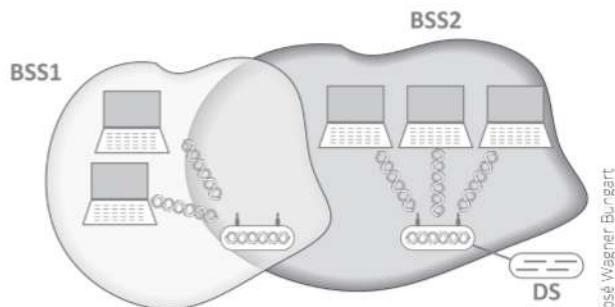


Figura 10 – Repetidores.

Fonte: CCNA Wireless Official Exam Certification Guide – Cisco Press.

Wireless Mesh

Para evitar os problemas da topologia ponto-multiponto, existe a topologia Mesh (Figura 11), na qual todos os pontos de acesso se interconectam formando uma rede mais robusta e redundante. Esse padrão é definido pelo IEEE 802.11s.

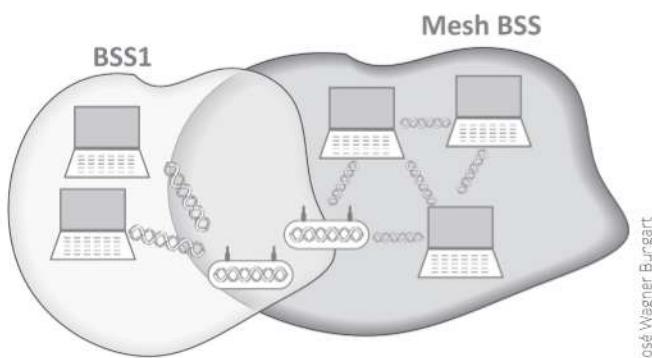


Figura 11 – Wireless Mesh.

Fonte: CCNA Wireless Official Exam Certification Guide – Cisco Press.

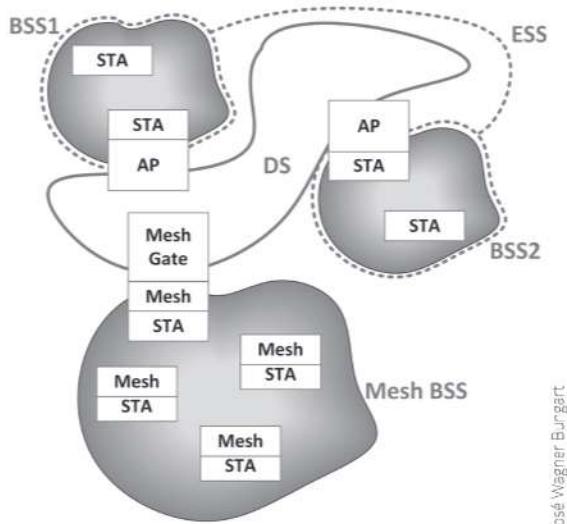
MBSS

As redes Mesh, no padrão 802.11, são chamadas de MBSS (Mesh BSS) e as estações que operam nesse tipo de rede são chamadas de Mesh-STA (Figura 12).

Dentro de um MBSS, todas as estações estabelecem enlaces sem fio com estações vizinhas para troca de mensagens, sendo possíveis também comunicações *multi-hop*.

Outra característica importante é que as estações de um MBSS podem se comunicar entre si em camada enlace.

Da mesma maneira que um ESS, as MBSSs podem ter – e geralmente têm – conexões com redes externas.



José Wagner Burgart

Figura 12 – Mesh BSS.
Fonte: IEEE Std 802.11:2012.

Vistos os principais tipos de redes WLAN, pode-se estudar os protocolos envolvidos para seu funcionamento e comunicação.

Protocolos 802.11

Conforme visto anteriormente, o IEEE define padrões de rede. Para redes WLAN existem uma série de padrões que são frequentemente atualizados com o desenvolvimento da tecnologia e a necessidade de evolução para velocidades de transmissão cada vez maiores. Os protocolos 802.11 são assim numerados pela definição do IEEE para redes WLAN. Eles atuam na camada enlace e possuem uma série de versões, por sua vez distintas por letras e derivadas do padrão inicial simbolizado apenas pelo número 802.11, conforme pode-se ver a seguir.

802.11

O protocolo IEEE 802.11 que deu início às WLANs, em 1997, atualmente não é mais encontrado com frequência em sua versão original, em novos dispositivos.

O 802.11 opera em taxas de 1 e 2 Mbps e utiliza FHSS (Frequency-hopping Spread Spectrum), que é um método de transmissão com base na mudança constante da portadora do sinal, isto é, pelo uso de vários canais de frequência em uma sequência conhecida pelo transmissor e receptor. Esse método dificulta a interceptação dos dados e possui uma alta resistência a interferências e ao compartilhamento de banda, por causa das mudanças constantes de frequência.

O protocolo 802.11 também descreve o DSSS (Direct Sequence Spread Spectrum), que possui características semelhantes ao FHSS, mas com um nível de potência menor, o que causa menos interferências entre redes distintas.

802.11b

O protocolo 802.11b é complementar ao 802.11 original. Na época em que o protocolo foi criado, as redes cabeadas eram majoritariamente de 10 Mbps na camada de acesso dos usuários contra os 1 ou 2 Mbps que se conseguia com o 802.11. Houve então uma corrida dos fabricantes de equipamentos sem fio para aumentar essas taxas e igualar – ou superar – a taxa de transmissão das redes cabeadas. Como o desenvolvimento de um padrão geralmente é mais lento do que os fabricantes, muitos conseguiram atingir maiores taxas rapidamente, mas havia o problema da interoperabilidade entre diferentes fabricantes. Dessa forma, o IEEE simplesmente definiu um padrão que fosse comum a todos os fabricantes da época: o IEEE 802.11b.

O 802.11b oferece taxas de 5,5 e 11 Mbps, mas com a compatibilidade de 1 e 2 Mbps do protocolo 802.11 com a mesma codificação e modulação. Quando opera em 11 Mbps utiliza uma modulação e codificação diferente, a codificação Barker ou CCK (Complementary Code Keying). Para modulação utiliza DBPSK e DQPSK.

802.11a

O protocolo 802.11a é tão antigo quanto o 802.11b, mas há uma grande diferença entre eles. O 802.11a opera na frequência de 5 GHz, fazendo-o incompatível com 802.11, 802.11b e 802.11g. Isso fez com que ele não fosse muito adotado mundialmente como o 802.11b e 802.11g.

Outra importante diferença em relação aos outros dois protocolos mais populares são os canais de *overlapping*: enquanto no 802.11b e 802.11g consegue-se apenas 3 canais sem sobreposição, no 802.11a é possível entre 12 a 23 canais sem sobreposição.

802.11g

O protocolo 802.11g foi publicado em junho de 2003, adicionando 8 faixas de transferência às 4 taxas do 802.11b, sendo a taxa máxima de transmissão de 54 Mbps, na frequência de 2,4 GHz.

É compatível com o 802.11b, pois usa a mesma modulação e codificação para as taxas de 1, 2, 5,5 e 11 Mbps. Para alcançar maiores taxas de transmissão utiliza OFDM.

Convívio 802.11b e 802.11g

Apesar de 802.11g conviver com 802.11b e ser compatível, um ponto importante a ser entendido é que a performance de uma rede com ponto de acesso em 802.11g cai quando recebe um host 802.11b, pois não consegue entender OFDM. Será apresentada a seguir a situação da comunicação quando um ponto de acesso 802.11g recebe um cliente 802.11b.

Na Figura 13 estão representados dois clientes 802.11g conectados a um ponto de acesso 802.11g. O Beacon, que é um quadro enviado pelo ponto de acesso, anunciando os seus serviços e características para associação à rede, informa que um cliente não está presente pela mensagem “Non-ERP” (Extended Rate Physical), ou seja, não existem clientes 802.11b e não é necessário utilizar um mecanismo de proteção.

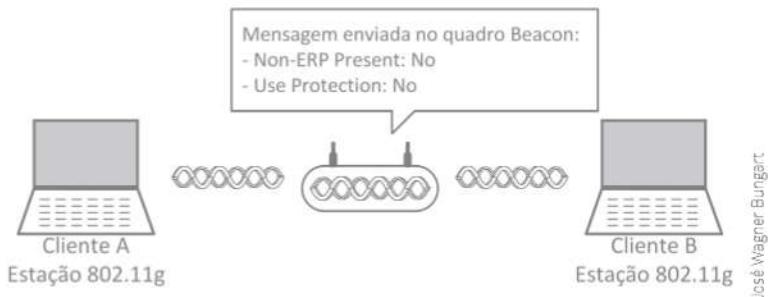


Figura 13 – Mensagem Beacon: Presença de Estações Não ERP = Não.

Fonte: CCNA Wireless Official Exam Certification Guide – Cisco Press.

Agora, ao se associar um cliente 802.11b ao ponto de acesso, o status do Beacon muda, informando os outros clientes e mudando a forma como eles transmitem (Figura 14).

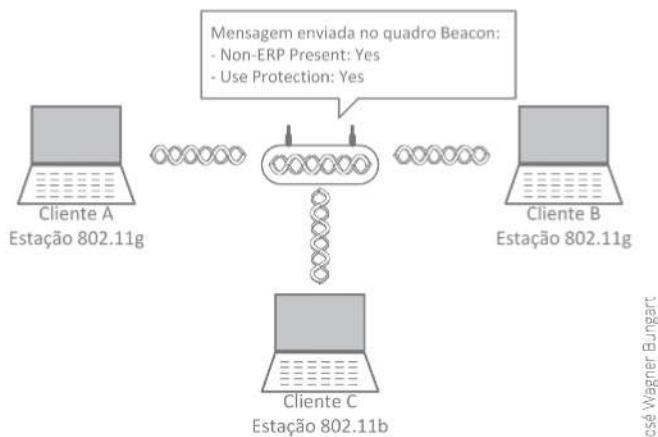


Figura 14 – Mensagem Beacon: Presença de Estações Não ERP = Sim.

Fonte: CCNA Wireless Official Exam Certification Guide – Cisco Press.

A partir desse momento, toda vez que um cliente 802.11g for transmitir para outro cliente 802.11g, ele precisa informar ao cliente 802.11b, na taxa de transmissão do 802.11b, que haverá uma comunicação e ele não conseguirá entender os pacotes trocados. Na Figura 15, o cliente A envia uma mensagem do tipo RTS (Request to Send). Nesse exemplo pode-se observar quanto tempo será necessário para a transmissão.

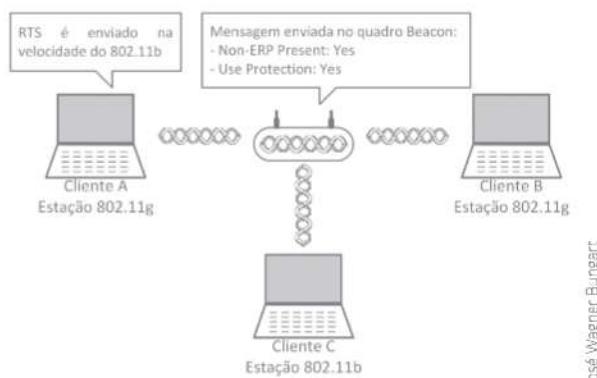


Figura 15 – Mensagem RTS.

Fonte: CCNA Wireless Official Exam Certification Guide – Cisco Press.

O cliente C (802.11b) ouve a informação de RTS e informa os outros clientes. O cliente B também recebe o RTS e envia uma mensagem de CTS (Clear to Send) (Figura 16).

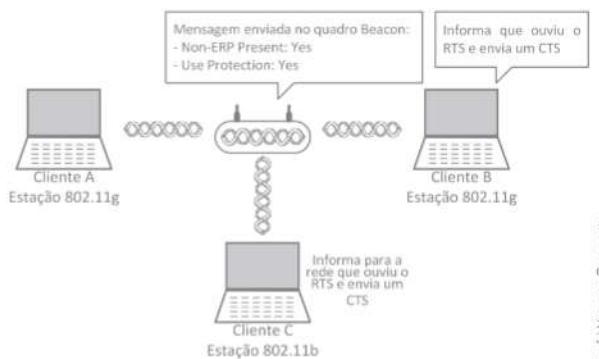


Figura 16 – Mensagem CTS.

Fonte: CCNA Wireless Official Exam Certification Guide – Cisco Press.

Na próxima etapa, o cliente B envia uma mensagem CTS para o cliente A com a duração solicitada para a transmissão. O cliente C ouve a mensagem RTS, que inclui o CTS do cliente B com a duração da transmissão (Figura 17).

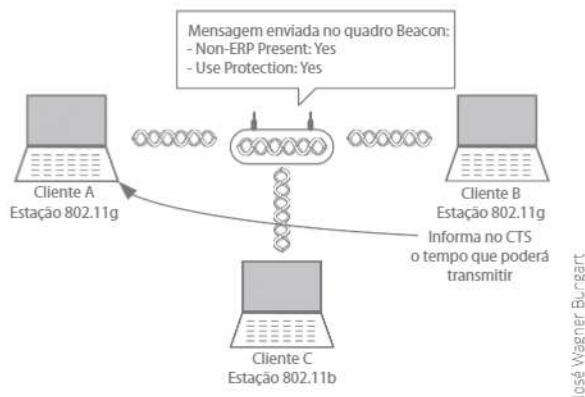


Figura 17 – Mensagem CTS com a duração da transmissão.
Fonte: CCNA Wireless Official Exam Certification Guide – Cisco Press.

Na última etapa, o cliente A envia os dados para o cliente B, na taxa de transmissão do 802.11g (Figura 18); o cliente C não consegue entender mais nada, mas espera o tempo estipulado para fazer uma solicitação de transmissão.

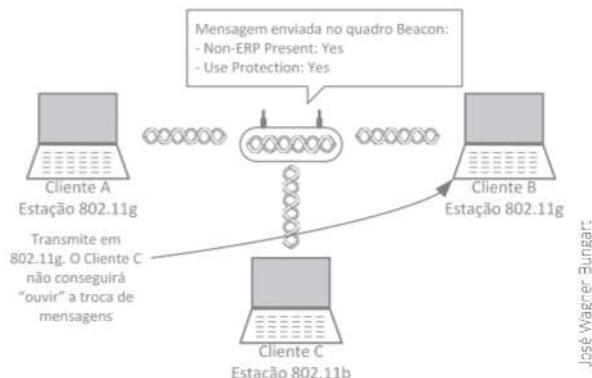


Figura 18 – Envio dos dados entre estações ERP.

802.11n

O protocolo 802.11n foi publicado em 2009 e seu principal objetivo era elevar a taxa de transmissão do 802.11g e 802.11a (54 Mbps) para até 600 Mbps, o que foi alcançado pela utilização de quatro canais de dados com espaçamento de 40 MHz entre eles.

O 802.11n utiliza a tecnologia MIMO (Multiple Input Multiple Output) fazendo a agregação de múltiplos canais na camada MAC. Isso só é possível graças ao uso de múltiplas antenas (tanto no transmissor como no receptor) que agregam mais

informações do que uma única. Utiliza multiplexação SDM (Spatial Division Multiplex). Pode operar tanto em 2,4 GHz como em 5 GHz.

O número de antenas vai determinar a quantidade de fluxos de dados enviada e recebida pelo ponto de acesso. Por exemplo, no equipamento na Figura 19 existem seis antenas, em que quatro podem ser destinadas à transmissão e duas, à receção.



Figura 19 – 802.11n.
Fonte: Aerohive networks.

O 802.11n pode chegar até a 600 Mbps. Existem vários valores intermediários que utilizam diferentes tipos de modulação e taxas de codificação.

802.11ac

O padrão 802.11ac foi o último padrão descrito pelo IEEE para redes locais sem fio. O seu desempenho supera o predecessor, 802.11n, e utiliza a tecnologia MIMO com o acréscimo de mais uma inovação: o MU-MIMO (Multi-user MIMO), suportando até oito fluxos contra os quatro fluxos do 802.11n.

Esse padrão consegue taxas de transferências superiores a 1 Gbps. A largura de banda por canal obrigatória é de 80 MHz, podendo ter, opcionalmente, 160 MHz. Utiliza a faixa de frequência de 5 GHz.

RECAPITULANDO

Neste capítulo foram apresentadas as redes sem fio, com um foco maior em WLANs, seus conceitos básicos, os protocolos, seu funcionamento e configurações.

Exercícios

1. Qual é o órgão regulador das redes sem fio no Brasil?
2. Que órgão definiu os padrões 802.11 e 802.15 de WLAN e WPAN?
3. Descreva as principais características das redes WPAN, WLAN, WMAN e WWAN.
4. O que são faixas de frequência licenciadas e não licenciadas?
5. Infravermelho opera somente se tiver em linha de visada entre transmissor e receptor. Essa afirmação está correta? Justifique sua resposta.
6. Qual a principal diferença entre uma rede sem fio *Ad Hoc* e uma rede Infraestrutura?

As respostas dos exercícios deste livro estão disponíveis para *download* no seguinte *link*: https://www.senaispeditora.com.br/downloads/respostas/redes_computadores_respostas.pdf

10. Serviços de redes

Acesso local

Acesso remoto

Telnet

Secure Shell – SSH

Dynamic Host Configuration Protocol – DHCP

Domain Name System – DNS

Neste capítulo serão estudadas a funcionalidade e as características de alguns serviços básicos de redes com o objetivo de fornecer os conceitos necessários para a instalação de uma rede local com seus principais serviços.

Acesso local

Ao se utilizar o termo “acesso local”, faz-se referência ao acesso a um dispositivo de rede local; ou seja, o administrador ou um técnico tem acesso às configurações de um equipamento conectado diretamente a ele. Geralmente, esse acesso é feito via console, isto é, desktop ou laptop. Alguns dispositivos, como switches e roteadores, não possuem uma forma de conexão com monitor, teclado e mouse, e sim uma porta serial do tipo RS232 ou USB (Figura 1). Isto é, esses dispositivos só permitem que o administrador interaja com ele por meio de algum software de acesso serial, como o Putty, por exemplo, instalado em um laptop ou desktop.



José Wagner Bungart

Figura 1 – Acesso via console.

O acesso local via porta de console deve ser utilizado o mínimo possível, principalmente quando se trabalha em ambientes críticos, isto é, ambientes onde estão instalados os equipamentos de rede e qualquer descuido pode desligá-los ou desconectá-los, causando uma parada no fornecimento dos serviços de rede. Portanto, deve-se evitar que o administrador ou qualquer outra pessoa permaneça nesses ambientes por longos períodos. O administrador, nas primeiras configurações, já deve permitir que o equipamento seja acessado remotamente pela rede, evitando o contato direto com o dispositivo.

Outra maneira de acesso local é via switch KVM (Keyboard Video and Mouse), muito utilizado para acessar servidores que geralmente não possuem monitor, teclado ou mouse, por estarem instalados em *racks* que não dispõem de muito espaço. O objetivo do KVM é permitir uma utilização mais otimizada possível de todos os servidores. Ou seja, em *racks* onde estão instalados diversos servidores, é comum encontrarmos switches KVM e um só console. Assim, esse conjunto permite que o administrador, utilizando somente um console com monitor, mouse e teclado, tenha acesso a vários servidores, bastando escolher o servidor com o qual deseja trabalhar naquele momento.



Figura 2 – KVM em rack.

Acesso remoto

O acesso remoto, como o próprio nome sugere, é a capacidade de acessar um dispositivo de rede, seja ele um roteador, switch, firewall, servidor ou qualquer outro dispositivo, remotamente, sem estar conectado diretamente a ele. Não é necessário sequer que o usuário esteja na mesma rede, podendo acessá-lo de qualquer lugar, até mesmo pela internet, observando sempre as políticas de segurança da empresa para que não seja caracterizada uma invasão.

Existem várias formas de acesso remoto. Cada equipamento ou sistema operacional tem seus protocolos, que podem ser interface texto, também chamada CLI (Command Line Interface) ou interface gráfica. No Capítulo 11 serão estudadas algumas maneiras de acesso remoto e serão feitos alguns exercícios para aplicá-las.

Telnet

O Telnet é um protocolo utilizado para acesso remoto a dispositivos, isto é, para acesá-los sem a necessidade de estar conectado diretamente ao equipamento. O Telnet é um protocolo antigo, inicialmente definido na RFC 15 de setembro de 1969 (<https://tools.ietf.org/html/rfc15>) e depois atualizado em 1983 com a RFC 854 (<https://tools.ietf.org/html/rfc854>). É inseguro, pois não tem qualquer tipo de criptografia dos dados trafegados. Também chamado de *clear text* ou, em português, texto limpo, pode ser facilmente interceptado, facilitando assim que nomes de usuários e senhas sejam descobertos com uma simples captura de pacotes. A porta padrão utilizada é a TCP 23.

Secure Shell – SSH

O SSH, definido pela RFC 4253 de janeiro de 2006 (www.tools.ietf.org/html/rfc4253), é um protocolo de rede que permite acesso remoto a dispositivos de forma segura, diferente do Telnet. O SSH utiliza criptografia entre o computador cliente e o dispositivo remoto, permitindo sua autenticação. Utilizando SSH o administrador pode obter acesso à interface CLI de dispositivos, para digitar comandos, e pode também transferir arquivos com os protocolos SFTP (SSH File Transfer) ou SCP (Secure Copy). A porta-padrão utilizada pelo TCP é a 22.

Dynamic Host Configuration Protocol – DHCP

O DHCP é um protocolo utilizado para a configuração automática de endereçamento de hosts, muito utilizado tanto em redes internas, de maneira a facilitar a configuração de seus computadores, como também pelos provedores de acesso à internet para fornecerem e configurarem o endereçamento de seus clientes de forma automática e dinâmica.

Por meio do DHCP pode-se configurar endereçamento em computadores e outros dispositivos de rede de forma estática, também chamada de manual. Neste caso, as informações

que precisam ser configuradas são basicamente: endereço IP do dispositivo, máscara de rede, *gateway*-padrão e endereço de DNS. O *gateway* padrão é o endereço do roteador da rede local, ou seja, o dispositivo que encaminhará os pacotes para outra rede lógica. Normalmente utiliza-se o primeiro IP do segmento da rede. Alguns administradores utilizam o último endereço, mas não há uma norma para isso. No entanto, por uma questão de organização, adota-se um critério que é utilizado em toda a rede. O endereço de DNS, conforme será apresentado no próximo item deste capítulo, faz as traduções de nomes em endereços IP. Deve-se configurar o endereço IP de um servidor DNS que pode estar na própria rede local ou o DNS externo do provedor de acesso. Na Figura 3 há um exemplo de configuração de IP estático.



Figura 3 – Configuração IP estático.

O uso de DHCP facilita muito a administração da rede, pois não só diminui drasticamente o tempo de configuração dos dispositivos, como também evita que problemas como a duplicidade de endereços aconteça. É possível também com o DHCP realizar reservas de endereços com base em endereços físicos para que um dispositivo sempre receba a mesma configuração caso seja necessário aplicar alguma restrição de acesso baseada em endereço, por exemplo.

O funcionamento do DHCP é simples, basta seguir este procedimento:

- Um cliente solicita uma configuração de endereçamento IP com uma mensagem DHCP Discover (Figura 4). Essa mensagem é um *broadcast* enviado à rede.

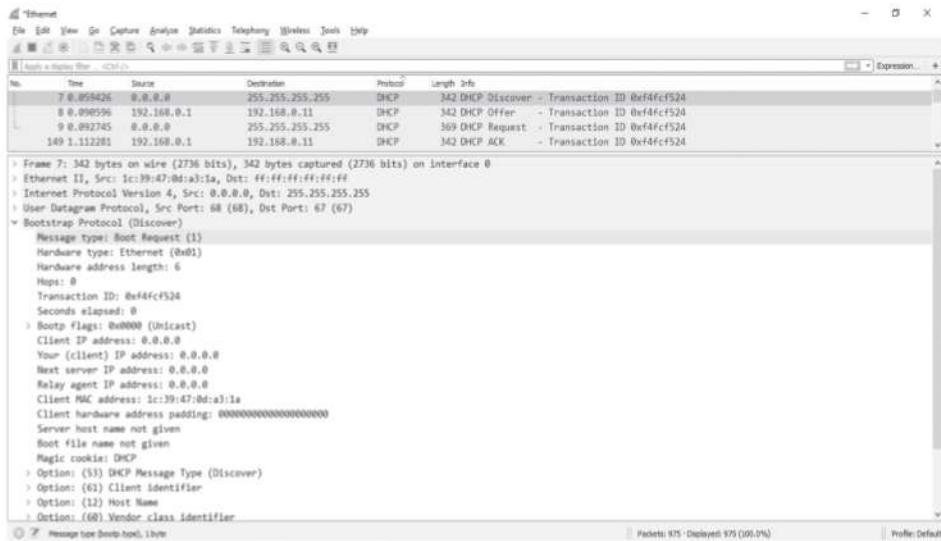


Figura 4 – DHCP Discover.

- Logo em seguida, todos os servidores de DHCP que estiverem na rede fazem uma oferta ao cliente, DHCP Offer (Figura 5). É importante que a rede esteja configurada de maneira que não permita falsos servidores DHCP, pois eles competiriam com os servidores verdadeiros, podendo se tornar potenciais pontos de ataque de uma rede.

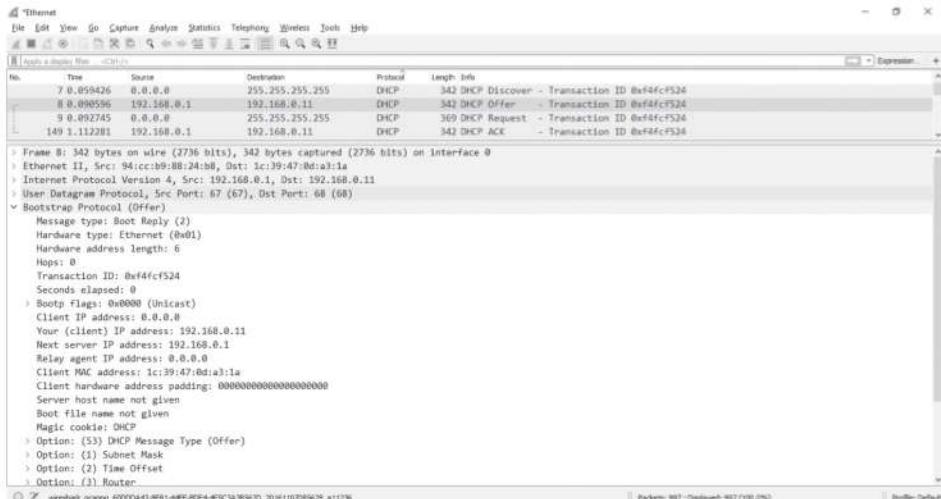


Figura 5 – DHCP Offer.

3. O cliente aceita a oferta e envia um DHCP Request (Figura 6), solicitando que o servidor envie a configuração.

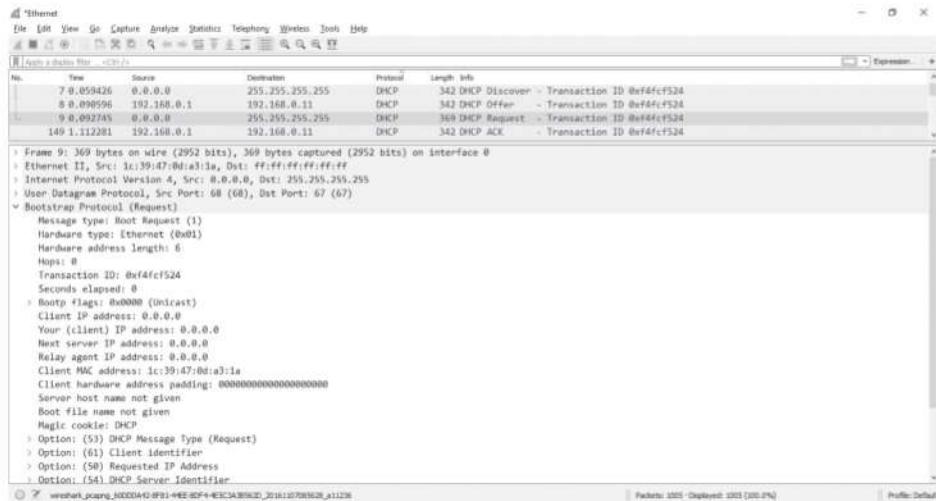


Figura 6 – DHCP Request.

4. Por fim, o servidor envia as configurações em uma mensagem DHCP ACK (Figura 7).

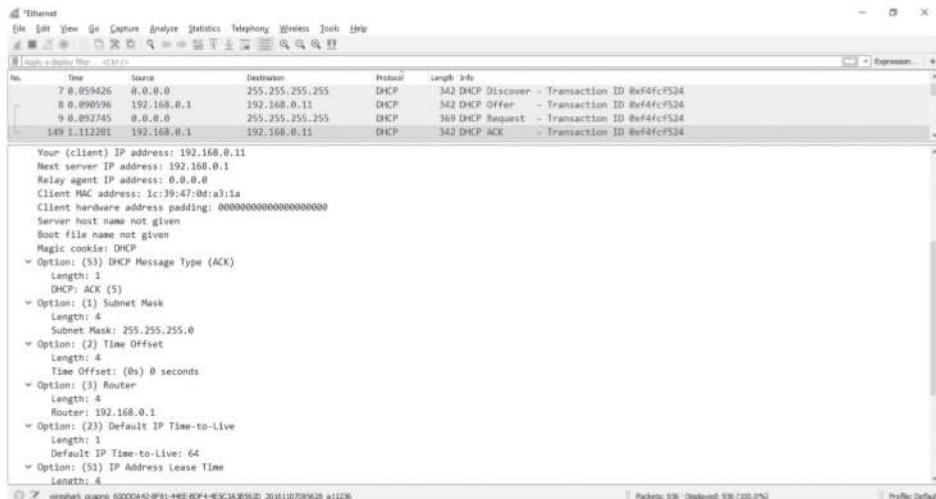


Figura 7 – DHCP ACK.

Domain Name System – DNS

Para os seres humanos é muito mais simples decorar e assimilar nomes de computadores, servidores, equipamentos de redes e sites do que decorar endereços IP, mas para os computadores é mais simples trabalhar com números. Um dos serviços utilizados para traduzir nomes em números e vice-versa é o Domain Name System (DNS).

Pode haver servidores de DNS internos, destinados à resolução de nomes de computadores e outros recursos de rede local ou de uma rede interna de uma determinada empresa. Existem também os servidores de DNS externos, que resolvem endereços de internet. O IANA é o responsável por gerenciar tanto os endereços IP públicos como nomes de domínios, mantendo o Root Zone Database e os Top-Level Domains, que são os registros de mais alto nível. Por exemplo os CCTLD (Country Code Top-Level Domain), os GTLD (Generic Top-Level Domain) e IDN (Internationalised Domain Name), que nada mais são que as indicações de .br, .com, .net, .edu, .uk, .ar e centenas de outros nos nomes de domínios da internet. No site do IANA (<http://www.iana.org/domains/root/db>) é possível ter acesso à lista completa.

O DNS utiliza porta UDP 53 e foi definida na RFC 1035 (www.ietf.org/rfc/rfc1035.txt).

Na Figura 8 pode-se observar uma consulta DNS ao endereço www.sp.senai.br/. Primeiro é feita uma consulta pelo cliente ao seu servidor DNS. Neste caso o cliente é o IP 192.168.0.11 e o servidor DNS 201.6.2.17.



Figura 8 – Consulta DNS.

Logo em seguida vem a resposta do servidor DNS com a resolução do endereço IP, nesse caso 201.16.211.70, como apresentado na Figura 9.

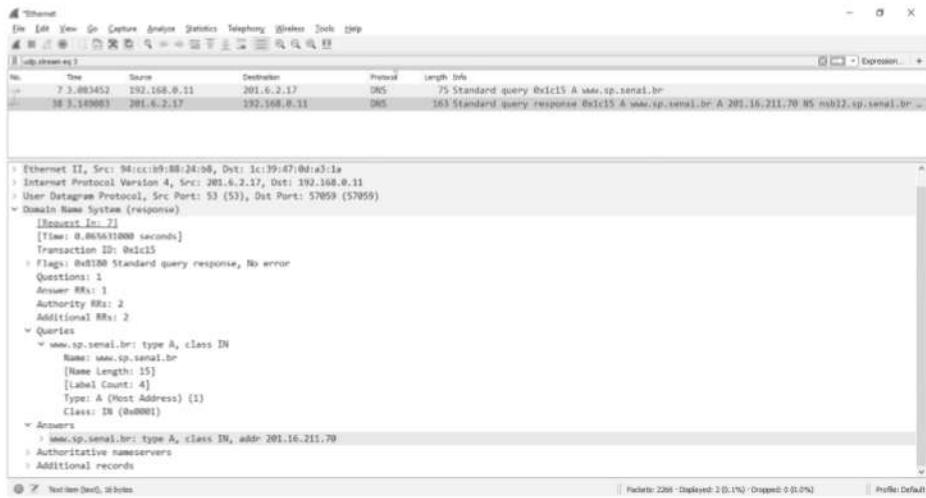


Figura 9 – Resolução DNS.

RECAPITULANDO

Neste capítulo foram apresentados alguns dos principais serviços de redes, a começar pelas formas de acesso local a equipamentos e servidores de rede com o objetivo de mostrar ao administrador como realizar as primeiras configurações. Além disso, foi visto o acesso remoto para que o administrador tenha acesso à distância aos dispositivos. Foram apresentados também os protocolos Telnet e SSH, com o destaque principalmente para a diferença no aspecto de segurança. Estudou-se ainda o funcionamento dos serviços de DHCP para a configuração automática de endereços de hosts e, por fim, o DNS, um importante serviço de rede que transforma nomes de hosts ou nomes de domínios em endereços IP.

Exercícios

1. Explique a diferença entre acesso local e acesso remoto.
2. Qual a função do Telnet?
3. Qual a função do SSH? No que se difere do Telnet?
4. Explique a função do DHCP e como é o processo de configuração automática de endereços.
5. O que é o DNS?

As respostas dos exercícios deste livro estão disponíveis para *download* no seguinte *link*: https://www.senaispeditora.com.br/downloads/respostas/redes_computadores_respostas.pdf

11. Configurações de equipamentos de redes

Switches

Roteadores Cisco

Funcionamento de uma rede LAN

Funcionamento de uma rede WAN

Os procedimentos de configuração básicas de redes são apresentados neste capítulo, além das formas de conexão a switches e roteadores Cisco por meio da porta de console e realização dos procedimentos de configuração desses dispositivos.

Switches

Os switches, conforme visto no Capítulo 2, são equipamentos que trabalham para a camada enlace, sendo responsáveis por conectar hosts à rede cabeada, geralmente composta de computadores, impressoras, access points, servidores, firewalls, roteadores e outros equipamentos.

O switching (comutação de nível 2, camada enlace) é baseado em hardware, ou seja, utiliza o endereço MAC das placas de rede dos computadores e outros elementos de rede para endereçar os hosts de uma rede local. Os switches usam circuitos integrados chamados de ASICs (Application Specific Integrated Circuits) para montar e manter suas tabelas de endereço MAC. Switches de nível 2 são mais rápidos do que roteadores, pois não abrem os cabeçalhos para pesquisar as informações da camada de rede. Em vez disso, examinam os endereços de hardware do *frame* na camada enlace antes de decidir entre encaminhar o quadro ou descartá-lo.

Função

Switches são dispositivos que filtram e encaminham pacotes dentro de segmentos de redes locais (sub-redes). Operam na camada enlace (camada 2) do modelo OSI, devendo ser independentes dos protocolos da camada superior.

Existem três funções distintas de switching nível 2:

- **Descoberta de endereço:** os switches armazenam o endereço de hardware de origem de cada quadro recebido por uma interface e inserem essa informação em um banco de dados MAC chamado Source Address Table (SAT) ou MAC Address Table.
- **Decisões de encaminhar/filtrar:** quando um quadro é recebido em uma interface, o switch examina o endereço de hardware do destino e localiza a interface de saída no banco de dados MAC. O quadro só é encaminhado para a porta de destino especificada.
- **Impedimento de loop:** se várias conexões entre switches forem criadas para criar redundância, poderão ocorrer *loops* na rede. O Spanning Tree Protocol (STP) é usado para impedir esses *loops* de rede, ainda que permita a redundância.

Características

Os switches podem ser classificados quanto ao método de encaminhamento dos pacotes, que são:

- Store and Forward.
- Cut Through.
- Adaptative Cut Through.

Store and Forward

Switches Store and Foward guardam cada quadro em um buffer antes de encaminhá-lo para a porta de saída. Enquanto o quadro está no buffer, o switch calcula o CRC, que é um código para a detecção de erros, e mede o tamanho do quadro. Se o CRC falha, ou o tamanho é muito pequeno ou muito grande (um quadro Ethernet tem entre 64 e 1.518 bytes), o quadro é descartado. Se estiver tudo certo, o quadro é encaminhado para a porta de saída.

O método Store and Forward assegura operações sem erro e aumenta a confiabilidade da rede. Contudo, o tempo gasto para guardar e checar cada quadro adiciona um tempo de latência grande ao processamento dos quadros, isto é, um tempo de espera para que se efetue a verificação de cada quadro.

A latência total é proporcional ao tamanho dos pacotes: quanto maior o pacote, maior a latência.

Cut Through

Os switches Cut Through foram projetados para reduzir a latência alta no Store and Forward, minimizando o atraso ao ler apenas os 6 primeiros bytes do pacote, que contêm o endereço de destino e logo permitem que o pacote completo seja encaminhado. Contudo, esse switch não detecta pacotes corrompidos causados por colisões (conhecidos como *runt*s) e nem erros de CRC. Quanto maior for o número de colisões na rede, maior será a largura de banda gasta com o encaminhamento de pacotes corrompidos.

Existe um segundo tipo de switch Cut Through chamado Fragment Free, que foi projetado para evitar os problemas inerentes ao Cut Through. Nesse tipo de switch os primeiros 64 bytes de cada pacote são lidos, assegurando que o quadro tenha pelo menos o tamanho mínimo e, assim, evitando o encaminhamento de *runt*s pela rede.

Adaptative Cut Through (Fragment Free)

Os switches que processam pacotes no modo adaptativo suportam tanto Store and Forward quanto Cut Through. Qualquer um dos modos pode ser ativado pelo administrador da rede, ou o switch pode ter inteligência e tecnologia o bastante para escolher entre os dois métodos, baseado no número de quadros com erro que passam pelas portas. Quando o número de quadros corrompidos atinge certo nível, o switch pode mudar do modo Cut Through para Store and Forward, voltando ao modo anterior quando a rede se normalizar.

Apenas os switches Store and Forward ou Adaptative Cut Through funcionam no modo Store and Forward e possuem a capacidade de suportar mais de um tipo de LAN (como por exemplo Ethernet e FastEthernet), pois são os únicos com capacidade de “bufferização” dos quadros, ou seja, de armazenar temporariamente dados em sua memória, condição necessária para a posterior conversão do formato do quadro MAC ou do método de sinalização.

Interfaces de switches

Uma das principais funções dos switches é a de conectar diversos dispositivos, trabalhando como um concentrador de conexões. Para que essa concentração ocorra são utilizadas as interfaces de conexão, que podem ser metálicas ou ópticas, ou seja, são as portas físicas onde os cabos são conectados. Para cabeamento metálico, o tipo de interface mais comum é RJ-45, e para cabeamento óptico existem alguns tipos de interface, sendo os mais utilizados atualmente o SC, LC e MT-RJ.

As principais configurações normalmente feitas em interfaces de switches são:

- **Velocidade:** podendo ser 10 Mbps, 100 Mbps, 1 Gbps, 10 Gbps e 40 Gbps.
- **Modo de operação Duplex:** half-duplex ou full-duplex.
- **Descrição:** o administrador escreve uma descrição de qual dispositivo está conectado àquela porta, muito útil para documentar a rede.

Funcionamento básico

É importante entender como um switch constrói a tabela de endereços MAC, que será utilizada para o encaminhamento dos *frames* para as portas corretas. Para isso será utilizado um exemplo simples, com apenas quatro computadores e um switch, conforme Figura 1.

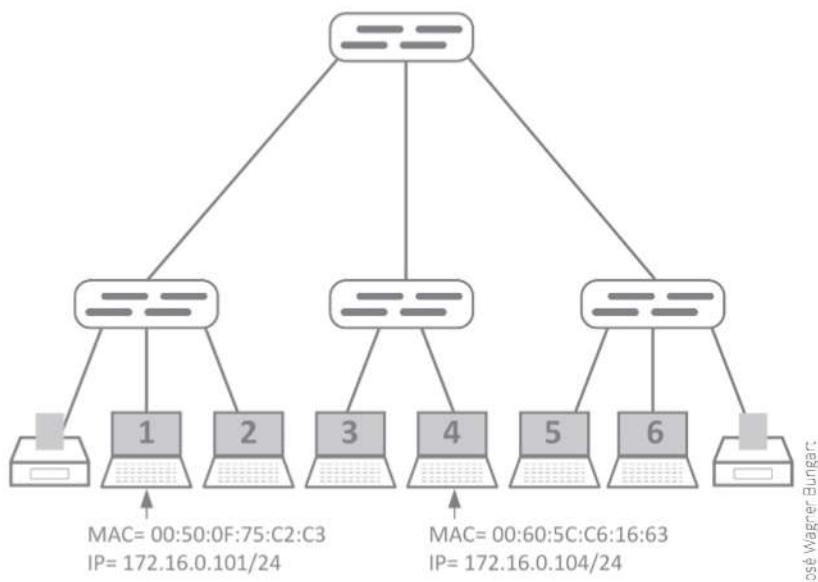


Figura 1 – Topologia com switch.

Quando a rede é iniciada, nenhum host tenta transmitir pela rede, uma vez que o switch não possui entradas em sua tabela de endereços MAC. Para demonstrar o que acontece na rede será realizado um *ping* do Host1 para o Host4 e será acompanhado o que acontece com os *frames* e, principalmente, o comportamento do switch.

A Tabela 1 é uma tabela de endereços MAC do switch, e está vazia, conforme previsto.

Tabela 1 – Tabela MAC do switch

```
Switch#show mac-address-table
Mac Address Table
-----
Vlan Mac Address Type Ports
-----
Switch#
```

Como se trata de um ping, ou seja, de uma mensagem do tipo ICMP Echo Request, que é disparada para um endereço IP no qual tanto origem como destino estão na mesma rede IP (172.16.0.101 e 172.16.0.104), será necessário o MAC Address de destino para que os hosts se comuniquem. Como o Host1 ainda não possui o MAC Address do Host4, é realizado um ARP Request para que ele possa ser descoberto.

No momento em que o ARP Request do Host1 chega ao switch, seu MAC Address é armazenado na tabela de MAC Address do switch. A tabela de endereços MAC agora possui uma entrada.

Tabela 2 – Tabela MAC com entrada

```
Switch#show mac-address-table
Mac Address Table
-----
Vlan Mac Address Type Ports
-----
Switch#
Switch#show mac-address-table
Mac Address Table
-----
Vlan Mac Address Type Ports
-----
1 0001.97d6.71cd DYNAMIC Fa0/1
Switch#
```

Conforme visto anteriormente, o ARP Request é uma mensagem do tipo broadcast, ou seja, ela será enviada para todos os hosts conectados aos switches. No cabeçalho do quadro Ethernet o MAC de destino é FF:FF:FF:FF:FF, isso significa um *broadcast*.

Todos os hosts conectados aos switches receberão o ARP Request, menos quem o originou, e todos os outros hosts ignorarão a mensagem, pois consultam o IP de destino e constatam que não é o seu IP, portanto não devem responder à requisição. O Host4 identifica que o ARP Request é para o seu IP e responde à mensagem, gerando um ARP Response, com o seu IP e MAC como sendo os endereços de origem e o IP e MAC do Host1 como endereços de destino.

Quando o switch recebe o ARP Response, o MAC Address do Host4 é inserido em sua tabela MAC.

Tabela 3 – Tabela MAC com MAC Address do Host4

```
Switch#show mac-address-table
Mac Address Table
-----
Vlan Mac Address Type Ports
-----
Switch#
Switch#show mac-address-table
Mac Address Table
-----
Vlan Mac Address Type Ports
-----
1 0001.97d6.71cd DYNAMIC Fa0/1
1 000d.bda9.698b DYNAMIC Fa0/2
Switch#
```

Como o switch possui o MAC Address de destino (Host1) em sua tabela, o *frame* é encaminhado exclusivamente para a sua porta correspondente (FastEthernet0/1).

Dessa forma o switch “aprende” o MAC Address que está conectado em cada uma de suas portas, diminuindo a quantidade de *broadcasts* propagados na rede.

Acesso via console

Os switches Cisco possuem, normalmente, interface por linha de comando (CLI – Command Line Interface) e alguns modelos possuem interface gráfica. Dessa forma, a familiaridade com as linhas de comando, os modos de operação e as formas de acesso são muito importantes para aprender a operá-lo.

Para uma primeira configuração dos switches Cisco, é preciso de uma configuração local via porta de console (Figura 2). Para isso utiliza-se algum aplicativo de acesso serial, sendo o Putty o mais comum atualmente.



Figura 2 – Porta de console.

Fonte: Blog Router Switch.

A configuração do Putty para uma conexão pela porta serial deve ser conforme a Figura 3. Pode-se observar que a velocidade de conexão deve ser 9.600 bps e deve-se escolher qual porta está ativa e configurada no computador em questão. Caso não se saiba, deve-se consultar o Gerenciador de Dispositivos do Painel de Controle do Windows, se o Windows estiver sendo utilizado:

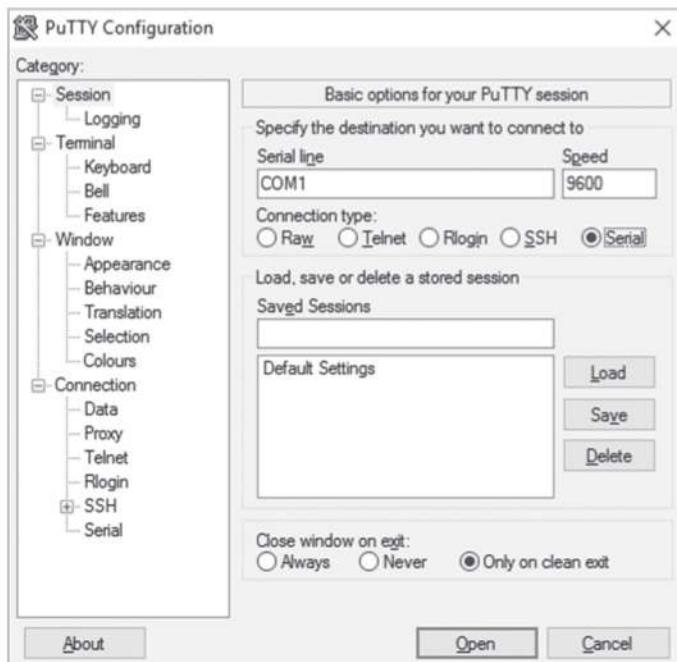


Figura 3 – Putty: Conexão serial.

Após configurado o acesso via Putty, basta pressionar “enter” para que a conexão seja feita com o switch, assim a tela a seguir aparecerá. Durante o processo de inicialização do switch são exibidas informações de hardware, como a quantidade, o tipo de portas e informações da versão do sistema operacional do equipamento.

Pressione “enter” novamente e receberemos o prompt de comando do switch.

Tabela 4 – Prompt de comando do switch

```
C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)FX, RELEASE SOFTWARE (fc4)
Cisco WS-C2960-24TT (RC32300) processor (revision C0) with 21039K bytes of memory.
2960-24TT starting...
Base ethernet MAC Address: 0001.977E.1D23
Xmodem file system is available.
Initializing Flash...
flashfs[0]: 1 files, 0 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 64016384
flashfs[0]: Bytes used: 4414921
flashfs[0]: Bytes available: 59601463
flashfs[0]: flashfs fsck took 1 seconds.
...done Initializing Flash.
Boot Sector Filesystem (bs:) installed, fsid: 3
Parameter Block Filesystem (pb:) installed, fsid: 4
Loading "flash:/c2960-lanbase-mz.122-25.FX.bin"...
```

(continua)

```
#####
# [OK]
# Restricted Rights Legend
# Use, duplication, or disclosure by the Government is
# subject to restrictions as set forth in subparagraph
# (c) of the Commercial Computer Software - Restricted
# Rights clause at FAR sec. 52.227-19 and subparagraph
# (c) (1) (ii) of the Rights in Technical Data and Computer
# Software clause at DFARS sec. 252.227-7013.
# cisco Systems, Inc.
# 170 West Tasman Drive
# San Jose, California 95134-1706
Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 12.2(25)FX, RELEASE
SOFTWARE (fc1)
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 12-Oct-05 22:05 by pt_team
Image text-base: 0x80008098, data-base: 0x814129C4
Cisco WS-C2960-24TT (RC32300) processor (revision C0) with 21039K bytes of memory.
24 FastEthernet/IEEE 802.3 interface(s)
2 Gigabit Ethernet/IEEE 802.3 interface(s)
    63488K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address : 0001.977E.1D23
Motherboard assembly number : 73-9832-06
Power supply part number : 341-0097-02
Motherboard serial number : FOC103248MJ
Power supply serial number : DCA102133JA
Model revision number : B0
Motherboard revision number : C0
Model number : WS-C2960-24TT
System serial number : FOC1033Z1EY
Top Assembly Part Number : 800-26671-02
Top Assembly Revision Number : B0
Version ID : V02
CLEI Code Number : COM3K00BRA
Hardware Board Revision Number : 0x01
Switch Ports Model SW Version SW Image
-----
* 1 26 WS-C2960-24TT 12.2 C2960-LANBASE-M
Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 12.2(25)FX, RELEASE
SOFTWARE (fc1)
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 12-Oct-05 22:05 by pt_team
Press RETURN to get started!
Switch>
```

Modos de acesso

Os equipamentos Cisco, trabalhando em interface CLI, possuem diferentes níveis de acesso, também chamados de modo. Observando o prompt de comando pode-se visualizar em qual modo atuar. Essa é uma atenção que o administrador deve ter sempre que estiver utilizando a interface CLI.

O primeiro prompt de comando é chamado de “Modo Usuário” e permite que apenas comandos básicos do equipamento sejam executados. Para visualizar os comandos e funcionalidades disponíveis no equipamento pode-se digitar o caractere “?” a qualquer momento para obter ajuda sobre o comando, como no exemplo a seguir:

Tabela 5 – Obter ajuda no prompt de comando do switch

Switch>?	
Exec commands:	
connect	Open a terminal connection
disable	Turn off privileged commands
disconnect	Disconnect an existing network connection
enable	Turn on privileged commands
exit	Exit from the EXEC
logout	Exit from the EXEC
ping	Send echo messages
resume	Resume an active network connection
show	Show running system information
telnet	Open a telnet connection
terminal	Set terminal line parameters
traceroute	Trace route to destination
Switch>	

Ao digitar “Enable”, o “Modo Usuário” é abandonado e muda-se para o “Modo Privilegiado”, que possui, como o próprio nome afirma, mais privilégios do que o “Modo Usuário”. Veja que o prompt de comando mudou e que agora a lista de comandos é bem maior do que no “Modo Usuário”.

Tabela 6 – Modo Privilegiado

Switch>enable	
Switch#?	
Exec commands:	
clear	Reset functions
clock	Manage the system clock
configure	Enter configuration mode

(continua)

connect	Open a terminal connection
copy	Copy from one file to another
debug	Debugging functions (see also 'undebbug')
delete	Delete a file
dir	List files on a filesystem
disable	Turn off privileged commands
disconnect	Disconnect an existing network connection
enable	Turn on privileged commands
erase	Erase a filesystem
exit	Exit from the EXEC
logout	Exit from the EXEC
more	Display the contents of a file
no	Disable debugging informations
ping	Send echo messages
reload	Halt and perform a cold restart
resume	Resume an active network connection
setup	Run the SETUP command facility
show	Show running system information
<hr/> -More-	
ssh	Open a secure shell client connection
telnet	Open a telnet connection
terminal	Set terminal line parameters
traceroute	Trace route to destination
undebbug	Disable debugging functions (see also 'debug')
vlan	Configure VLAN parameters
write	Write running configuration to memory, network, or terminal
<hr/> Switch#	

Quando há muitas informações para serem exibidas na mesma tela, a Cisco pausa a exibição e no final da tela aparece a informação – More –, indicando que existem mais informações a serem exibidas. Para dar continuidade na exibição dos

comandos o administrador pode pressionar a tecla “enter”, que exibirá mais uma linha a cada tecla digitada, ou poderá pressionar a barra de espaços do teclado, que exibirá mais uma tela de comandos.

No “Modo Privilegiado” não é possível configurar o switch, mas somente visualizar configurações, status e testar configurações. Para ter acesso às configurações deve-se digitar “Configure terminal”.

É importante ressaltar que é possível utilizar a tecla “Tab” para completar comandos. O sistema operacional Cisco também suporta comandos resumidos, como “conf t”, por exemplo.

Tabela 7 – Comando de configuração do switch

```

Switch#conf
Switch#configure ter
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#

```

Esse modo é denominado “Modo de Configuração Global”, no qual é possível realizar configurações que afetam todo o equipamento e também entrar em outros modos de configuração, como, por exemplo, configuração de interfaces. Os comandos e os prompts são apresentados na tela da Tabela 8:

Tabela 8 – Comandos e prompts

Switch(config)#?	Configure commands:
access-list	Add an access list entry
banner	Define a login banner
boot	Boot Commands
cdp	Global CDP configuration subcommands
clock	Configure time-of-day clock
crypto	Encryption module
do	To run exec commands in config mode
enable	Modify enable password parameters
end	Exit from configure mode
exit	Exit from configure mode
hostname	Set system's network name

(continua)

interface	Select an interface to configure
ip Global	IP configuration subcommands
line	Configure a terminal line
logging	Modify message logging facilities
mac	MAC configuration
mac-address-table	Configure the MAC address table
mls	mls global commands
no	Negate a command or set its defaults
port-channel	EtherChannel configuration
privilege	Command privilege parameters
service	Modify use of network based services
snmp-server	Modify SNMP engine parameters
spanning-tree	Spanning Tree Subsystem
username	Establish User Name Authentication
vlan	Vlan commands
vtp	Configure global VTP state

A partir do “Modo de Configuração Global”, podemos entrar nas configurações de interfaces de rede. No exemplo da Tabela 9, o prompt de comando mudará novamente, indicando que agora se está configurando uma porta do switch.

Tabela 9 – Configuração global e porta do switch

Switch(config)#interface fastEthernet 0/1	
Switch(config-if)#?	
cdp	Global CDP configuration subcommands
channel-group	Etherchannel/port bundling configuration
channel-protocol	Select the channel protocol (LACP, PAgP)
description	Interface specific description
duplex	Configure duplex operation.
exit	Exit from interface configuration mode
ip	Interface Internet Protocol config commands
mdix	Set Media Dependent Interface with Crossover
mls	mls interface commands

(continua)

no	Negate a command or set its defaults
shutdown	Shutdown the selected interface
spanning-tree	Spanning Tree Subsystem
speed	Configure speed operation
storm-control	storm configuration
switchport	Set switching mode characteristics
tx-ring-limit	Configure PA level transmit ring limit
Switch(config-if) #	

Configuração de portas

Serão apresentados a seguir alguns comandos básicos para a configuração de portas de switches. Normalmente, quando se faz configurações de switches de acesso, ou seja, aqueles que serão utilizados para a conexão com os equipamentos dos usuários finais, deixa-se as configurações das portas do switch no modo automático, pois os terminais dos usuários finais podem ter diferentes configurações de velocidade e de duplex, facilitando assim a administração da rede e dando maior flexibilidade no uso dos switches. Mas quando se configuram portas de interconexão entre switches, entre switches e roteadores, servidores, firewalls e outros equipamentos de rede que dificilmente serão alterados, é uma boa prática fixar as configurações de velocidade e duplex. No exemplo a seguir, na Tabela 10, estão os comandos para essas configurações:

Tabela 10 – Comandos para configurações fixas

```

Switch(config-if)#speed ?
10 Force 10 Mbps operation
100 Force 100 Mbps operation
auto Enable AUTO speed configuration
Switch(config-if)#speed 100
Switch(config-if)#duplex ?
auto Enable AUTO duplex configuration
full Force full duplex operation
half Force half-duplex operation
Switch(config-if)#duplex full
Switch(config-if)#

```

Caso algum comando tenha sido digitado errado, uma mensagem será exibida para indicar o erro, assim como uma breve descrição do que pode ter ocorrido.

No exemplo anterior, na Tabela 10, os comandos foram aceitos normalmente, pois, após o “Enter”, o prompt foi exibido normalmente na linha abaixo.

Uma boa prática é escrever uma descrição em cada porta do switch, pois isso facilitará a administração, indicando o que está conectado à cada porta. Caso seja muito difícil administrar cada um dos computadores, impressoras, laptops e outros equipamentos dos usuários finais, é comum utilizar indicações de onde aquela porta está conectada, por exemplo, “Segundo Andar – Sala 2 – Ponto 15”. Essa descrição de porta suporta até 240 caracteres.

Tabela 11 – Descrição de porta para o switch

```
Switch(config-if)#description ?
LINE Up to 240 characters describing this interface
Switch(config-if)#description Segundo Andar - Sala 2 - Ponto 15
Switch(config-if)#+
```

Quando existem muitas portas a serem configuradas com as mesmas características, pode-se utilizar o recurso de especificar uma faixa sequencial de portas e configurá-las simultaneamente. No exemplo a seguir serão configuradas as portas FastEthernet de 0/1 até 0/9, todas com 100 Mbps de velocidade, full-duplex e com a descrição “Portas reservadas para uso futuro”.

Tabela 12 – Configuração de múltiplas portas simultaneamente

```
Switch(config)#interface range fastEthernet 0/1 - fastEthernet 0/9
Switch(config-if-range)#speed 100
Switch(config-if-range)#duplex full
Switch(config-if-range)#description Portas reservadas para uso futuro
Switch(config-if-range)#+
```

Para verificar as configurações aplicadas no equipamento, utiliza-se o comando *show running-config*. Esse comando exibe as configurações atuais e que estão em execução pela memória RAM (Random Access Memory) do equipamento. Como esse tipo de memória é do tipo volátil, ou seja, quando o dispositivo é desligado o seu conteúdo é perdido, somente informações temporárias são armazenadas, como por exemplo a tabela de endereços MAC e as configurações em execução. Para armazenar as informações que não podem ser perdidas quando o equipamento é desligado, a Cisco utiliza memórias NVRAM (Non-volatile RAM), onde devem ser salvas todas as configurações dos equipamentos. O comando para salvar as configurações é: *copy running-config startup-config*.

Na verdade, o que ele executa é uma cópia das configurações que estão na RAM (*running-config*) para a NVRAM (*startup-config*).

Para executar tanto o comando *show running-config* como o *copy running-config startup-config*, deve-se estar no “Modo Privilegiado”. No último exemplo, nas Tabelas 11 e 12 foi apresentada a configuração de portas do switch. A partir daquela tela, para voltar para o “Modo Privilegiado” utilizou-se o comando *exit*, que volta um nível do modo em que se está, ou seja, ela sairá do “Modo de Configuração de Interfaces” e passará para o “Modo de Configuração Global”. Digitando *exit* novamente ele sairá do “Modo de Configuração Global” e passará para o “Modo Privilegiado”.

Uma forma de passar diretamente do “Modo de Configuração de Interface” para o “Modo Privilegiado” é digitando o comando *end*. Na sequência de comandos a seguir, o “Modo de Configuração de Interface” é abandonado, passa-se para o “Modo Privilegiado” diretamente e visualiza-se as configurações aplicadas.

Tabela 12 – Passagem direta para o Modo Privilegiado

```

Switch(config-if-range)#end
%SYS-5-CONFIG_I: Configured from console by console
Switch#show running-config
Building configuration...
Current configuration : 1682 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
!
!
spanning-tree mode pvst
!
interface FastEthernet0/1
description Portas reservadas para uso futuro
duplex full
speed 100
!
```

(continua)

```
interface FastEthernet0/2
description Portas reservadas para uso futuro
duplex full
speed 100
!
interface FastEthernet0/3
description Portas reservadas para uso futuro
duplex full
speed 100
!
interface FastEthernet0/4
description Portas reservadas para uso futuro
duplex full
speed 100
!
interface FastEthernet0/5
description Portas reservadas para uso futuro
duplex full
speed 100
!
```

Essa é somente uma amostra da saída do comando, mas já é suficiente para entender que as configurações de *description*, velocidade e duplex foram aplicadas corretamente.

Agora, para salvar as configurações, pode-se utilizar o comando *copy running-config* ou o comando resumido *wr*, conforme pode-se verificar no exemplo abaixo, na Tabela 13. Na primeira vez em que o switch copiará as configurações da memória RAM será solicitado o nome do arquivo de destino na NVRAM, o padrão é utilizar *startup-config*.

Tabela 13 – Comando resumido wr e aplicação das configurações

```
Switch#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Switch#
Switch#wr
Building configuration...
[OK]
Switch#
```

Configuração de Telnet

Foi apresentada a maneira como um administrador de rede pode ter acesso a um equipamento via console. Essa é uma conexão local, ou seja, o administrador deve ter condições de conectar um cabo de console diretamente ao seu compu-

tador e utilizar um software como o Putty para ter acesso às configurações. Mas nem sempre essa é a realidade do administrador, pois em um ambiente operacional o administrador geralmente está fisicamente distante do equipamento, e deve realizar uma conexão remota.

Para os acessos remotos, dois protocolos são utilizados com maior frequência, o Telnet e o SSH. Como visto anteriormente, o Telnet não é uma forma segura por não criptografar os dados que são transmitidos, enquanto o SSH possui essa funcionalidade.

Os comandos que configuram Telnet em equipamento Cisco são simples. No “Modo Privilegiado” deve-se digitar *line vty* para entrar no modo de configuração das “linhas” de Telnet que podem ser configuradas. No exemplo iniciado na Tabela 14, serão configuradas dezesseis linhas, ou seja, serão permitidos dezesseis acessos simultâneos. Pode-se estabelecer uma senha para o Telnet com o comando *password* e, por fim, o comando *login*, conforme pode-se ver a seguir:

Tabela 14 – Configuração de Telnet

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#line vty 0 15
Switch(config-line)#password senai123
Switch(config-line)#login
```

Para verificar a configuração, utiliza-se o comando *show running-config*, que pode ser executado mesmo estando no modo de configuração de interface. Para isso, ele deve ser precedido do comando *do*, conforme pode-se observar abaixo. Para a saída do comando não ficar muito longa, omitiu-se a parte inicial e apresentou-se apenas a configuração pertinente ao Telnet:

Tabela 15 – Descrição da configuração do Telnet (resumida)

```
Switch(config-line)#do show running-config
Building configuration...
!
line vty 0 4
password senai123
login
line vty 5 15
password senai123
login
!
end
Switch(config-line)#

```

Foram criadas as linhas *vty* de 0 a 4 no primeiro bloco e de 5 a 15 no segundo bloco, totalizando os dezesseis acessos simultâneos. Para o acesso ao switch via Telnet é necessária a configuração de uma senha para entrar no “Modo Privilegiado”, também conhecida como “senha de *enable*”. Para isso é necessário o seguinte comando no “Modo de Configuração Global”:

Tabela 16 – Tela do Modo de Configuração Global: senha de *enable*

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#enable secret senai123
Switch(config)#
```

Uma boa prática é configurar uma senha também para a porta de console, assim, caso alguém tenha acesso fisicamente ao equipamento, poderá fazer uso da porta de console para entrar nas configurações do switch. Para isso deve-se configurar a porta de console da seguinte maneira:

Tabela 17 – Tela do Modo de Configuração Global: senha de porta de console

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#line console 0
Switch(config-line)#password senai123
Switch(config-line)#login
Switch(config-line)#
```

Ainda falta realizar uma configuração no switch para que ele possa receber conexões Telnet. Ainda não se configurou um IP no switch, para isso utiliza-se a VLAN 1 (Virtual LAN), que é a VLAN nativa dos equipamentos Cisco, para configurar um endereço IP.

VLAN é uma tecnologia que permite ter, no mesmo equipamento, de maneira virtual, mais de uma rede LAN. Ou seja, pode-se configurar portas dos switches como se estivessem em domínios de *broadcasts* diferentes, isolando completamente as redes em camada 2.

Para que uma VLAN se comunique com outra é necessário haver roteamento. Essa técnica de utilização de VLANs é utilizada para duas finalidades: primeiro, para aumentar a segurança da rede, pois quando se quer isolar partes da rede, ou fazer um controle maior utilizando um roteador, pode-se criar diferentes VLANs; segundo, para melhorar o desempenho, como visto anteriormente, pois criando-se grandes domínios de *broadcast* a quantidade de interrupções nos dispositivos

aumenta consideravelmente, e diminuir o tamanho dos segmentos melhora o desempenho da rede, pois o roteador não propaga os *broadcasts* gerados.

Voltando à configuração do endereço IP no roteador, é necessário colocar um endereço IP na interface VLAN 1. A VLAN 1 já vem configurada por padrão nos switches Cisco, bastando apenas configurar o seu endereço IP e máscara de rede, por exemplo, *ip address 192.168.1.20 255.255.255.0*, e ativar a interface VLAN com o comando *no shutdown*. A seguir, na Tabela 18, estão os comandos para essa configuração:

Tabela 18 – Ativação da interface VLAN

```

Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface vlan1
Switch(config-if)#ip address 192.168.1.20 255.255.255.0
Switch(config-if)#no shutdown
%LINK-5-CHANGED: Interface Vlan1, changed state to up
Switch(config-if)#

```

Para testar o funcionamento do Telnet, deve-se utilizar um computador na mesma rede do switch, ou se existir acesso de outras redes, utilizar um software de Telnet, como o Putty, por exemplo. Deve-se digitar o endereço IP do switch e sua porta (23), conforme Figura 4:

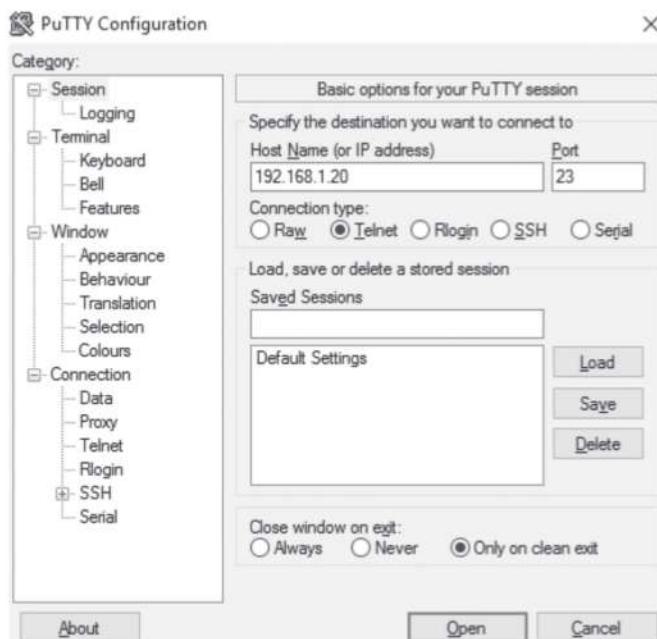


Figura 4 – Telnet utilizando Putty.

Configuração de SSH

Em switches Cisco, as configurações do SSH são um pouco mais complexas do que para o Telnet. É necessário observar alguns pontos importantes nessa configuração:

1. O nome do switch não pode ser o padrão. É necessário alterar com o comando *hostname*. No exemplo da Tabela 19 há o *hostname SW.SP.01*.
2. O comando *aaa new-model* faz com que o equipamento utilize usuários locais caso não encontre um servidor AAA (Authentication, Authorization, and Accounting). Esse tipo de servidor é criado para que faça a autenticação de usuários utilizando os protocolos RADIUS ou TACACS+, por exemplo. Neste livro não serão abordados servidores AAA, mas serão feitas as autenticações locais.
3. Para criar usuários locais, utiliza-se o comando *username admin password 0 senai123*, que cria o usuário admin. com a senha senai123.
4. Como o SSH é um protocolo criptografado, é necessária a criação de uma chave. Para isso existe o comando *cry key generate rsa*. No exemplo da Tabela 19 criou-se uma chave de 512 bits. Colocou-se um tempo de expiração da sessão de 60 segundos e uma quantidade máxima de duas tentativas de autenticação.
5. Por fim, dentro da configuração de Telnet, coloca-se o comando *transport input ssh*, que limita o acesso remoto ao switch somente por SSH e não permite a forma insegura de Telnet.
6. A configuração do endereço IP na VLAN é o mesmo visto na configuração do Telnet.

Tabela 19 – Configuração de SSH

```

Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
(config)#hostname SW.SP.01
SW.SP.01(config)#ip domain-name teste.testandossh.com
SW.SP.01(config)#aaa new-model
SW.SP.01(config)#username admin password 0 senai123
SW.SP.01(config)#cry key generate rsa
The name for the keys will be: SW.SP.01.teste.testandossh.com
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

```

(continua)

```

How many bits in the modulus [512]: 512
% Generating 512 bit RSA keys ...[OK]
*Mar 1 00:00:52.535: %SSH-5-ENABLED: SSH 1.99 has been enabled
SW.SW01(config)#ip ssh time-out 60
SW.SW01(config)#ip ssh authentication-retries 2
SW.SW01(config)#line vty 0 15
SW.SW01(config-line)#transport input ssh
SW.SW01(config-line)#exit
SW.SW01(config)#interface vlan1
SW.SW01(config-if)#ip address 192.168.1.20 255.255.255.0
SW.SW01(config-if)#no shutdown
%LINK-5-CHANGED: Interface Vlan1, changed state to up
SW.SW01(config-if)#

```

Para testar o acesso via SSH utilizou-se o aplicativo Putty, conforme Figura 5:

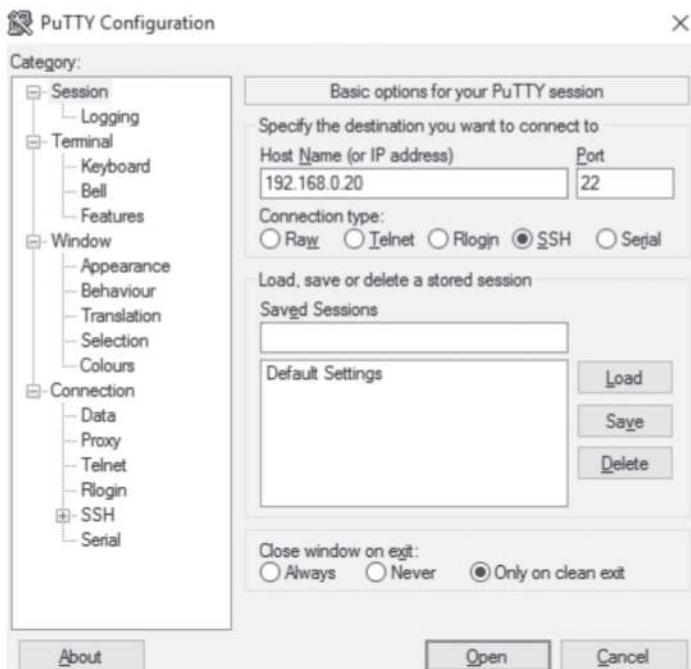


Figura 5 – SSH utilizando o Putty.

Roteadores Cisco

Conforme visto no Capítulo 2, roteadores são equipamentos de redes cuja função principal é encaminhar o tráfego de uma rede IP para outra. Um roteador deve possuir, no mínimo, duas interfaces de rede, cada uma pertencendo a uma rede

diferente. Nele são armazenadas as configurações do próprio equipamento, como por exemplo as configurações das interfaces de rede, e também as configurações de roteamento, que são as possibilidades de o roteador interagir com os demais roteadores da rede. Será apresentado mais adiante três maneiras de um roteador “aprender” as redes da topologia em que está inserido: redes diretamente conectadas (redes em que o roteador possui uma interface de rede conectada à ela), estaticamente (um administrador insere manualmente as rotas) ou dinamicamente (um administrador configura um protocolo de roteamento dinâmico e os roteadores trocam informações sobre as redes que conhecem).

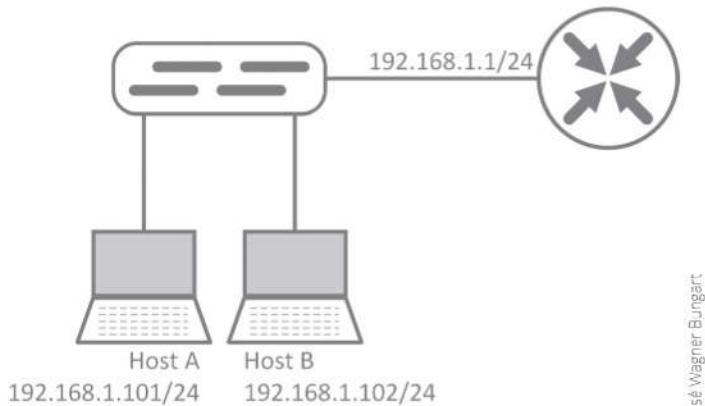
Com isso os roteadores conseguem preencher com dados suas tabelas de roteamento as quais são responsáveis por essa comunicação acontecer. Esse procedimento é chamado de “popular”. As tabelas de roteamento armazenam as informações de rotas “aprendidas” pelos roteadores. É pela tabela de roteamento que um roteador toma a decisão de qual rota é mais adequada para se chegar até o destino. No exemplo a seguir, na Tabela 20, há uma tabela de roteamento de um equipamento Cisco.

Tabela 20 – Tabela de roteamento de um roteador Cisco

```
R1#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2
      i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
      ia - IS-IS inter area, * - candidate default, U - per-user static route
      o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
      + - replicated route, % - next hop override
Gateway of last resort is not set
      172.16.0.0/16 is variably subnetted, 6 subnets, 2 masks
C    172.16.1.0/24 is directly connected, FastEthernet0/0
L    172.16.1.1/32 is directly connected, FastEthernet0/0
R    172.16.2.0/24 [120/1] via 192.168.1.2, 00:00:15, Serial1/0
R    172.16.3.0/24 [120/1] via 192.168.1.6, 00:00:07, Serial1/1
R    172.16.4.0/24 [120/2] via 192.168.1.6, 00:00:07, Serial1/1
                  [120/2] via 192.168.1.2, 00:00:15, Serial1/0
S    172.16.5.0/24 [1/0] via 192.168.1.2
      192.168.1.0/24 is variably subnetted, 6 subnets, 2 masks
C    192.168.1.0/30 is directly connected, Serial1/0
L    192.168.1.1/32 is directly connected, Serial1/0
C    192.168.1.4/30 is directly connected, Serial1/1
L    192.168.1.5/32 is directly connected, Serial1/1
R    192.168.1.8/30 [120/1] via 192.168.1.6, 00:00:07, Serial1/1
R    192.168.1.12/30 [120/1] via 192.168.1.2, 00:00:15, Serial1/0
R1#
```

Rotas diretas

Apesar de não haver roteamento quando dois hosts estão na mesma rede, existe o termo “rota direta” que denomina esse tipo de comunicação. Como pode-se ver no exemplo da Figura 6, Host A e Host B pertencem à mesma rede IP. Desta forma, diz-se que entre eles há uma rota direta.

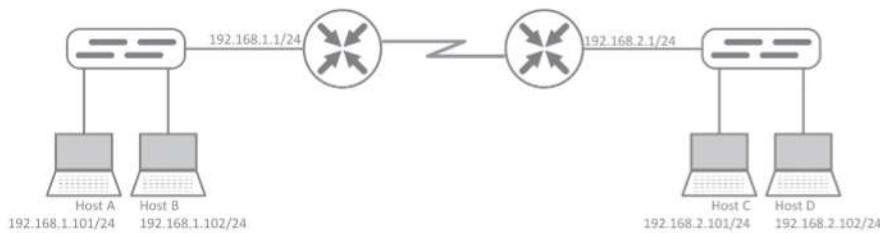


José Wagner Büngart

Figura 6 – Rotas diretas.

Rotas indiretas

Rotas indiretas são aquelas que precisam de um roteador para fazer o encaminhamento do tráfego entre redes. No exemplo abaixo pode-se ver duas redes IP diferentes interligadas por dois roteadores (Figura 7).



José Wagner Büngart

Figura 7 – Rotas indiretas.

Redes diretamente conectadas

Redes diretamente conectadas são aquelas que possuem uma interface configurada no roteador. Em outras palavras, toda vez que se configura uma interface de rede em um roteador, automaticamente a rede à qual aquela interface pertence será inserida na tabela de roteamento como diretamente conectada.

Roteamento estático

As rotas estáticas são aquelas inseridas manualmente por um administrador. Cada entrada deve ser adicionada por meio de comandos específicos para que o roteador conheça o caminho para uma determinada rede. Esse tipo de roteamento só deve ser usado em redes pequenas e cuja topologia não seja complexa. Quanto maior e mais complexa a rede, mais difícil será administrar uma rede somente com rotas estáticas. Um outro ponto que deve ser observado é que, quando existir caminhos redundantes para um determinado destino, as rotas estáticas devem ser configuradas com custos distintos e a administração dos caminhos preferenciais se torna difícil se há uma rede muito dinâmica. A escolha do melhor caminho é feita pelo roteador com base em custos, ou seja, o caminho que tiver o menor custo será o preferencial para o roteador encaminhar os pacotes.

Configuração de roteamento estático

Para explicar a configuração de um roteamento estático simples, utiliza-se a topologia da Figura 8. Nela há três roteadores, R1, R2 e R3, cada um com uma rede LAN e dois links que interligam R1 e R3 à R2 numa topologia *hub and spoke*.

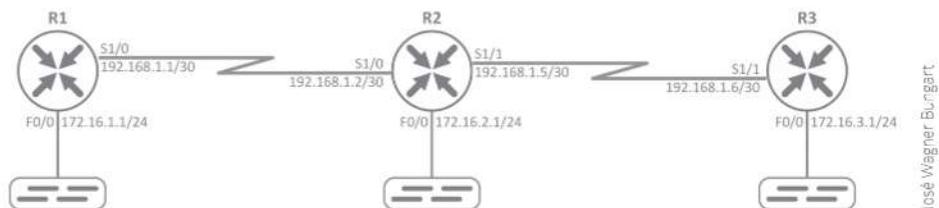


Figura 8 – Roteamento estático.

As configurações desse tipo de roteamento são simples. Basicamente, o que se faz é configurar cada uma das interfaces de cada roteador e criar uma rota estática para cada destino que se quer alcançar a fim de criar conectividade lógica com uma rede ao se comunicar com outra. No roteamento estático é necessário criar rotas manualmente, tanto de ida como de volta. Em outras palavras, cada roteador deve ter uma rota para cada destino.

Os comandos para configurar interfaces já foram vistos anteriormente no tópico sobre switch, porém há um único comando novo específico para criação de rota estática, que segue sempre a sintaxe a seguir, no Modo de Configuração Global:

IP ROUTE [IP DA REDE DE DESTINO] [MÁSCARA DA REDE DE DESTINO] [IP DO PRÓXIMO ROTEADOR]

Deve-se ter cuidado com alguns pontos importantes:

- **IP da rede de destino:** sempre deve ser colocado um endereço de rede ou sub-rede, a não ser que se esteja criando uma rota para um único host de destino.
- **Máscara da rede de destino:** a máscara que deve ser inserida é da rede de destino. Deve-se ter cuidado para não errar a máscara, senão alguns hosts podem ficar fora do intervalo declarado.
- **IP do próximo roteador:** também conhecido como *next-hop*, é o IP do outro roteador conectado ao que estiver sendo configurado. Esse IP nunca poderá ser do próprio roteador e nem de um roteador ao qual ele não tenha uma rede diretamente conectada.

Veja agora como demonstrar as configurações de cada roteador:

Tabela 21 – Configuração do roteador R1

```
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface fastethernet 0/0
R1(config-if)#ip address 172.16.1.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface serial 1/0
R1(config-if)#ip address 192.168.1.1 255.255.255.252
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#ip route 172.16.2.0 255.255.255.0 192.168.1.2
R1(config)#ip route 172.16.3.0 255.255.255.0 192.168.1.2
R1(config)#ip route 192.168.1.4 255.255.255.252 192.168.1.2
```

Tabela 22 – Configuração do roteador R2

```
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#interface fastethernet 0/0
R2(config-if)#ip address 172.16.2.1 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#interface serial 1/0
R2(config-if)#ip address 192.168.1.2 255.255.255.252
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#interface serial 1/1
R2(config-if)#ip address 192.168.1.5 255.255.255.252
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#ip route 172.16.1.0 255.255.255.0 192.168.1.1
R2(config)#ip route 172.16.3.0 255.255.255.0 192.168.1.6
```

Tabela 23 – Configuração do roteador R3

```
R3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#interface fastethernet 0/0
R3(config-if)#ip address 172.16.3.1 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#interface serial 1/0
R3(config-if)#ip address 192.168.1.6 255.255.255.252
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.5
```

No roteador R3 foi feita uma configuração de roteamento estático um pouco diferente, pois utilizou-se o recurso de “rota *default*”. Esse recurso encaminha os pacotes destinados a qualquer rede que não esteja na tabela de roteamento pelo caminho que esteja apontando a “rota *default*”, isto é, uma rota padrão. No exemplo, poderia ter sido aplicada também no roteador R1. Essa prática é muito utilizada nas redes, apontando em direção para onde estiverem os links de internet. As tabelas de roteamento dos três roteadores ficarão da seguinte forma:

Tabela 24 – Tabela de roteamento de R1

R1#sh ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2
 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
 ia - IS-IS inter area, * - candidate default, U - per-user static route
 o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
 + - replicated route, % - next hop override

Gateway of last resort is not set

C	172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
C	172.16.1.0/24 is directly connected, FastEthernet0/0
L	172.16.1.1/32 is directly connected, FastEthernet0/0
S	172.16.2.0/24 [1/0] via 192.168.1.2
S	172.16.3.0/24 [1/0] via 192.168.1.2
	192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C	192.168.1.0/30 is directly connected, Serial1/0
L	192.168.1.1/32 is directly connected, Serial1/0

R1#

Tabela 25 – Tabela de roteamento de R2

R2#sh ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2
 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
 ia - IS-IS inter area, * - candidate default, U - per-user static route
 o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
 + - replicated route, % - next hop override

Gateway of last resort is not set

S	172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
S	172.16.1.0/24 [1/0] via 192.168.1.1
C	172.16.2.0/24 is directly connected, FastEthernet0/0
L	172.16.2.1/32 is directly connected, FastEthernet0/0
S	172.16.3.0/24 [1/0] via 192.168.1.6
	192.168.1.0/24 is variably subnetted, 4 subnets, 2 masks
C	192.168.1.0/30 is directly connected, Serial1/0
L	192.168.1.2/32 is directly connected, Serial1/0
C	192.168.1.4/30 is directly connected, Serial1/1
L	192.168.1.5/32 is directly connected, Serial1/1

R2#

Tabela 26 – Tabela de roteamento de R3

R3#sh ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2
 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
 ia - IS-IS inter area, * - candidate default, U - per-user static route
 o - ODR, P - periodic downloaded static route, H - NHRP, I - LISP
 + - replicated route, % - next hop override

Gateway of last resort is 192.168.1.5 to network 0.0.0.0

```
S* 0.0.0.0/0 [1/0] via 192.168.1.5
  172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C   172.16.3.0/24 is directly connected, FastEthernet0/0
L   172.16.3.1/32 is directly connected, FastEthernet0/0
  192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C   192.168.1.4/30 is directly connected, Serial1/0
L   192.168.1.6/32 is directly connected, Serial1/0
R3#
```

Para verificar a conectividade da rede, pode-se utilizar o comando *ping* de dentro dos roteadores, conforme Tabela 27:

Tabela 27 – Uso do comando *ping* para roteamento de R1

```
R1#ping 172.16.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/8 ms
R1#ping 172.16.3.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.3.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/36/64 ms
R1#ping 192.168.1.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/40/64 ms
R1#
```

Roteamento dinâmico

Com roteamento dinâmico o trabalho de configuração manual é reduzido, limitando-se apenas às configurações iniciais, pois as rotas das redes são trocadas automaticamente pelos roteadores. Isto é, nesse processo cada roteador anuncia tanto suas rotas diretamente conectadas como as outras rotas que “aprenderam” estática ou dinamicamente. Assim, os vizinhos “aprendem” as rotas enviadas e as armazenam na tabela de roteamento.

Esse tipo de roteamento facilita bastante o trabalho de configuração em redes grandes e complexas. Seus protocolos podem ser classificados em dois tipos: os IGPs (Internal Gateway Protocol) e os EGPs (External Gateway Protocol). O primeiro deles é uma classificação utilizada para uso interno de uma rede, o segundo para redes externas, tais como a internet. Existem outras duas classificações para os protocolos de roteamento, dessa vez em relação ao modo operacional do protocolo: Distance Vector e Link State.

Antes de conhecê-los melhor, no entanto, é importante entender o que são os saltos.

Os protocolos do tipo Distance Vector utilizam o número de saltos como métrica para atingir o destino desejado, ou seja, a quantidade de roteadores que o pacote passa até chegar ao seu destino, sendo que cada roteador conta um salto. Em alguns casos também é utilizada a banda para calcular a métrica de escolha do melhor caminho. Uma outra característica desse modo operacional do roteamento dinâmico é o anúncio das rotas: são enviadas atualizações periódicas e com toda a topologia da rede, e não apenas as alterações de topologia.

Já os protocolos do tipo Link State utilizam uma atualização incremental da topologia da rede, ou seja, as atualizações não são enviadas completas para os vizinhos, mas somente suas alterações. Além disso, esse envio ocorre somente quando algo foi alterado, isto é, não é periódico como acontece no Distance Vector. Dessa forma, os protocolos do tipo Link State possuem uma convergência mais rápida do que os Distance Vector. A métrica para tomada de decisões do melhor caminho é baseada num custo que pode ser a largura de banda, menor caminho ou a menor perda de pacotes.

Acesso via console

As configurações em roteadores Cisco são muito semelhantes às aqui já estudadas para switches. A Cisco padroniza os comandos o máximo possível, de maneira que não possa haver diferença entre equipamentos e versões de sistemas operacionais, o que facilita a administração da rede e acelera o aprendizado de configuração e manutenção.

Então, por uma questão de organização e de facilidade para o leitor, as configurações já estudadas serão apresentadas apenas em forma de comandos, sem a necessidade de se repetir as explicações. Caso haja alguma dúvida, deve-se voltar aos capítulos anteriores para revisar as explicações.

Para acessar via console um roteador Cisco, deve-se utilizar o aplicativo Putty e escolher a opção Console, com as configurações padrão ativadas. Assim, o usuário terá acesso à interface CLI do roteador.

Por motivos de segurança, é uma boa prática configurar uma senha de acesso ao console, conforme pode ser visto na Tabela 28:

Tabela 28 – Configuração de senha de acesso ao console

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#line console 0
Router(config-line)#password senai123
Router(config-line)#login
Router(config-line)#+
```

Configuração de Telnet

As configurações de Telnet para roteadores são as mesmas já vistas em relação ao switch. A seguir, os comandos para configuração de Telnet em roteadores:

Tabela 29 – Resumo de configurações de Telnet em roteadores

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#line vty 0 15
Router(config-line)#password senai123
Router(config-line)#login
```

Até aqui tudo foi semelhante às configurações do switch, porém, uma diferença dos roteadores é a não obrigatoriedade de se fazer a configuração de endereço IP na VLAN. Como as interfaces dos roteadores devem possuir endereços IP, pode-se utilizar esses IPs para o acesso remoto.

Configuração de SSH

Para configurar o SSH de um roteador, deve-se seguir a Tabela 30. Caso haja dúvidas, deve-se retomar os procedimentos de configuração de SSH do switch, pois eles são exatamente iguais.

Tabela 30 – Configuração de SSH em roteadores

```

Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname SW.SP.01
RT.SP.01(config)#ip domain-name teste.testandossh.com
RT.SP.01(config)#aaa new-model
RT.SP.01(config)#username admin password 0 senai123
RT.SP.01(config)#cry key generate rsa
The name for the keys will be: RT.SP.01.teste.testandossh.com
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 512
% Generating 512 bit RSA keys ...[OK]
*Mar 1 00:00:52.535: %SSH-5-ENABLED: SSH 1.99 has been enabled
RT.SP.01(config)#ip ssh time-out 60
RT.SP.01(config)#ip ssh authentication-retries 2
RT.SP.01(config)#line vty 0 15
RT.SP.01(config-line)#transport input ssh
RT.SP.01(config-line)#exit

```

Configuração de portas

Os roteadores possuem algumas características diferente dos switches. Uma delas trata-se de configuração das portas: enquanto nos switches todas as portas vêm habilitadas por padrão, nos roteadores elas vêm desabilitadas. Outra diferença é a necessidade de configurar endereços IP nas portas que queremos utilizar, com cada uma delas pertencendo a redes lógicas diferentes, para que o roteador possa encaminhar os pacotes para as redes corretas.

A seguir é apresentada uma configuração simples de uma interface FastEthernet, por meio da inserção do endereço IP e habilitação da porta:

Tabela 31 – Configuração de portas

```
R5#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface fastethernet 0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#
*Nov 7 17:28:31.499: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0, changed state to up
Router(config-if)#

```

É possível observar que após a interface ter sido configurada, o estado muda para *up*, indicando que agora ela está habilitada e que existe algum equipamento conectado a ela, o que permite existir conectividade com outro elemento.

Funcionamento de uma rede LAN

A topologia apresentada na Figura 9 exemplifica o funcionamento de uma rede LAN. É uma rede local típica de uma pequena empresa, que apresenta três switches interligados para prover conectividade entre os computadores da empresa, com um servidor de DNS (172.16.0.10) e um roteador para acesso à internet.

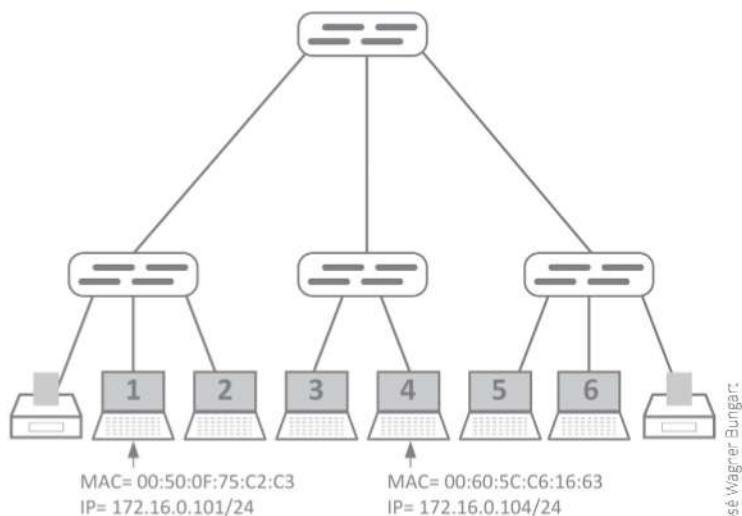


Figura 9 – Topologia LAN.

Considera-se que todos os hosts já possuem os endereços IP configurados e que todos os switches estão com suas tabelas de endereço MAC vazias. Nesse caso, o fluxo dos dados durante o funcionamento da LAN é:

1. O Host1 (172.16.0.101) envia um *ping* para o Host4 (172.16.0.104), ou seja, *ping* 172.16.0.104.
2. Como ambos estão na mesma rede lógica, é necessário que o Host1 conheça o endereço MAC do Host4; então é enviado um ARP Request para a rede.
3. Quando o ARP Request chegar até o switch, ele armazenará o MAC do Host1 em sua tabela de endereços MAC e enviará o *broadcast* para todas as suas portas, menos para a porta de origem, ou seja, para a impressora, para o Host2 e para o SW1. A impressora e o Host2 ignorarão a mensagem.
4. O SW1 enviará o *broadcast* para todas as suas portas, menos para o SW2, ou seja, para o servidor DNS, para o roteador, SW3 e SW4. O servidor e o roteador ignoram a mensagem, pois não é destinada a eles.
5. O SW3 e SW4 fazem o *broadcast* da mensagem para todas as suas portas, menos a porta do SW1.
6. No SW4 a mensagem é ignorada por todos, pois não possui o computador de destino.
7. No SW3 o Host4 responde o ARP Request com um ARP Reply, pois ele possui o IP solicitado na mensagem, respondendo com o seu endereço MAC.
8. Quando o ARP Reply chega ao SW3, o endereço MAC do Host4 é armazenado em sua tabela de endereços MAC e é enviado para o SW1. É importante lembrar que o ARP Reply é um *unicast*, e, portanto não é enviado para todas as portas.
9. O SW1 armazena o endereço MAC do Host4 e envia o ARP Reply para o SW2.
10. O SW2 armazena o endereço MAC do Host4 e envia o ARP Reply para o Host4.
11. O Host1 armazena a relação IP/MAC e agora está apto a enviar a mensagem ICMP diretamente para o Host4, assim como todos os switches do caminho entre as duas estações.

Considera-se agora o seguinte cenário: nenhum computador ou switch conhece qualquer endereço da rede, a não ser os que estão configurados estaticamente em suas interfaces. Nesse cenário, o mesmo Host1 envia um ping para o Host4, mas dessa vez não utiliza o endereço IP do computador de destino e sim o seu nome, para que o DNS resolva o nome:

1. O Host1 (172.16.0.101) envia um *ping* para o Host4 utilizando o seu nome, ou seja, *ping* Host4.
2. Antes de mais nada, o Host1 precisa que o nome seja traduzido em um endereço IP. Para isso ele deve enviar uma mensagem DNS Query para o servidor de DNS, consultar sua configuração de interface de rede e descobrir que o IP do DNS está na mesma rede lógica. Então, antes do DNS Query, é necessário um ARP Request para encontrar o endereço MAC do servidor DNS.
3. Quando o ARP Request chega até o switch SW2, ele armazena o MAC do Host1 em sua tabela de endereços MAC e envia o *broadcast* para todas as suas portas, menos para a porta de origem. Ou seja, a impressora, o Host2 e o SW1 recebem a mensagem, mas a impressora e o Host2 a ignoram.
4. O SW1 envia o *broadcast* para todas as suas portas, menos para o SW2, ou seja, para o servidor DNS, para o roteador, SW3 e SW4. Os switches SW3 e SW4 enviam seus *broadcasts*, mas não retornam uma resposta. O roteador ignora a mensagem, pois não é destinada a ele.
5. O servidor DNS responde o ARP Request com um ARP Reply, pois ele possui o IP solicitado na mensagem. A resposta é o seu endereço MAC.
6. Quando o ARP Reply chega ao SW1, o endereço MAC do servidor DNS é armazenado em sua tabela de endereços MAC e reenviado para o SW2. Deve-se lembrar que o ARP Reply é um *unicast*, portanto não é enviado para todas as portas.
7. O SW2 armazena o endereço MAC do servidor DNS e envia o ARP Reply para o Host1.
8. O Host1 armazena a relação IP/MAC do servidor DNS e agora estará apto a enviar a mensagem DNS Query para o servidor.
9. O DNS Query é enviado para o SW2, que a envia na sequência para SW1 e chega ao servidor.

10. O DNS faz a consulta em sua base de dados e responde com um DNS Query Response que o IP do host4 é 172.16.0.104.

11. A mensagem retorna para o Host1, que analisa o seu endereço e compara com o endereço de destino. Nesse caso, eles pertencem à mesma rede lógica, iniciando novamente um ARP Request, exatamente da mesma forma do exemplo anterior.

Funcionamento de uma rede WAN

Utilizando a mesma topologia do exemplo anterior, mas agora com um cenário de comunicação de um computador da rede LAN se comunicando com um site da internet, como exemplo ao tentar acessar o site do Senai São Paulo, www.sp.senai.br. Como nesse cenário há um servidor DNS e considera-se que ele já tenha em sua base a tradução do nome do site para o endereço público, o procedimento descrito nos dois cenários anteriores será utilizado, mas agora com a diferença de que a interface do roteador será utilizada para enviar a mensagem. Assim, considerando um estado inicial da rede em que nenhum endereço é conhecido, exceto os configurados estaticamente, têm-se:

1. O Host1 (172.16.0.101) envia um HTTP GET para o site www.sp.senai.br.
2. O Host1 precisa que o nome seja traduzido em um endereço IP. Para isso ele deve enviar uma mensagem DNS Query para o servidor de DNS, consultar sua configuração de interface de rede e descobrir se o IP do DNS está na mesma rede lógica. Então, antes do DNS Query é necessário um ARP Request para encontrar o endereço MAC do servidor DNS.
3. Quando o ARP Request chega até o switch SW2, ele armazena o MAC do Host1 em sua tabela de endereços MAC e envia o *broadcast* para todas as suas portas, menos para a porta de origem, ou seja, para a impressora, para o Host2e para o SW1. A impressora e o Host2 ignoram a mensagem.
4. O SW1 envia o *broadcast* para todas as suas portas, menos para o SW2, ou seja, para o servidor DNS, para o roteador, SW3 e SW4. Os switches SW3 e SW4 enviam seus *broadcasts*, mas não retornam uma resposta. O roteador ignora a mensagem, pois não é destinada a ele.

5. O servidor DNS responde o ARP Request com um ARP Reply, pois ele possui o IP solicitado na mensagem. A resposta é o seu endereço MAC.
6. Quando o ARP Reply chega ao SW1 o endereço MAC do servidor DNS é armazenado em sua tabela de endereços MAC e é enviado para o SW2. Deve-se lembrar que o ARP Reply é um *unicast*, portanto não é enviado para todas as portas.
7. O SW2 armazena o endereço MAC do servidor DNS e envia o ARP Reply para o Host1.
8. O Host1 armazena a relação IP/MAC do servidor DNS e agora está apto a enviar a mensagem DNS Query para o servidor.
9. O DNS Query é enviado para o SW2, que a envia para SW1 e chega ao servidor.
10. O DNS faz a consulta em sua base de dados e responde com um DNS Query Response traduzindo o domínio do site www.sp.senai.br para seu IP público.
11. A mensagem retorna para o Host1, que analisa o seu endereço e o compara com o endereço de destino. Nesse caso eles não pertencem a mesma rede lógica. Dessa forma, a mensagem HTTP GET deve ser enviada para seu *gateway* padrão, pois ele deverá encaminhar as requisições para outras redes. Obrigatoriamente o *gateway* padrão deve estar na mesma rede lógica do Host1, dando início a um processo de ARP Request para encontrar o endereço MAC do roteador. Após o processo de descoberta do endereço MAC do roteador ser finalizado, será possível encaminhar a solicitação para ele. Assim, o HTTP GET seguirá para a internet, passando por alguns ou vários roteadores até chegar ao seu destino.

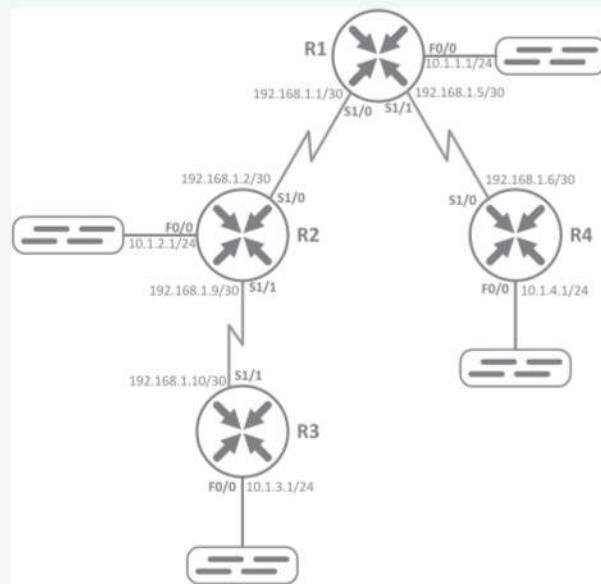
RECAPITULANDO

Neste capítulo estudou-se como são feitas as primeiras configurações de equipamentos Cisco, desde suas configurações básicas e comuns até switches e roteadores, passando por particularidades de configurações de portas de switches, pela configuração de interfaces, e, por fim, roteamento de uma rede simples. Foi possível obter uma visão geral da configuração desses dois importantes equipamentos em uma rede de computadores e de como é o fluxo de dados numa comunicação em rede LAN ou WAN. Foi possível analisar todos os passos que devem ocorrer para que as mensagens originadas em um computador da rede cheguem a seu destino.

Exercícios

1. Escreva os comandos necessários para a configuração de um switch com as seguintes características:
 - a) Configuração de senha para acesso à interface de console. A senha utilizada deve ser @cess0.
 - b) Configuração de 16 conexões simultâneas de Telnet. A senha utilizada deve ser @cess0.
 - c) Deve ser configurada uma “senha de enable”. A senha utilizada deve ser @cess0.
 - d) As portas FastEthernet de 0/1 até 0/12 devem estar com full-duplex e 100 Mbps.
 - e) As portas FastEthernet de 0/13 até 0/20 devem estar com half-duplex e 10 Mbps.
 - f) As portas FastEthernet de 0/21 até 0/24 devem permanecer em modo automático, mas desabilitadas.
2. Escreva os comandos necessários para a configuração de um switch com as seguintes características:
 - a) Configuração de senha para acesso à interface de console. A senha utilizada deve ser @cess0.
 - b) Configuração de SSH, escolha os nomes que desejar para usuário e outras configurações.
 - c) As portas FastEthernet de 0/1 até 0/24 devem ter a descrição “Switch Prédio 10 Sala 15”.

3. Escreva os comandos necessários para a configuração da rede a seguir utilizando roteamento estático. Todos os roteadores devem ser configurados de maneira que cada um seja capaz de se comunicar com todas as outras redes da topologia:



As respostas dos exercícios deste livro estão disponíveis para *download* no seguinte *link*: https://www.senaispeditora.com.br/downloads/respostas/redes_computadores_respostas.pdf

Através da leitura desse livro foi possível conhecer os conceitos gerais de redes de computadores e os seus principais protocolos de comunicação, desde a terminologia básica utilizada na área de infraestrutura de redes até configurações simples de dispositivos, com o objetivo de entender o fluxo de dados e os protocolos utilizados.

Uma importante parte no estudo de redes é o entendimento da arquitetura em camadas do TCP/IP, pois esse modelo permite entender facilmente as funções e as particularidades da comunicação em redes. Cada camada possui o seu conjunto de protocolos, e no livro foram apresentados os principais, que, em conjunto, possibilitam a comunicação.

Foram abordadas também as duas versões do protocolo IP usadas atualmente: a versão IPv4 e IPv6. Viu-se que, hoje em dia, ocorre uma fase de transição entre as duas versões, daí a importância de se conhecer as características de cada uma, para que se possa utilizá-las da melhor maneira possível e assim promover uma transição segura e suave.

Após a conceituação de redes e protocolos, foram estudadas as configurações de dois importantes equipamentos de redes, os switches e roteadores. Viu-se como são configurados equipamentos do fabricante Cisco, atualmente o líder de mercado nessa área. Por fim, foi apresentado de maneira simplificada como funciona o fluxo de dados em redes LAN, WLAN e WAN para consolidar os conhecimentos adquiridos em todos os capítulos do livro.

Com essas informações, o leitor estará apto a aprofundar-se mais na área de infraestrutura de redes, abrindo caminho para diversas áreas do conhecimento. São inúmeras as possibilidades, como, por exemplo, configuração e administração de dispositivos, de serviços e servidores de redes, segurança e gerenciamento de redes. Esta é uma área que cresce exponencialmente e da qual as empresas e pessoas dependem cada vez mais. Continuar os estudos e se especializar nessa área poderá, certamente, trazer boas oportunidades profissionais.

Referências

CARROLL, Brandon James. **CCNA Official Certification Guide**. MacMillan Technical, 2008.

COMER, Douglas. **Interligação de redes com TCP/IP - Volume 1**. 6 ed. Rio de Janeiro: Campus. 2015.

IANA – Internet Assigned Numbers Authority. **Internet Control Message Protocol (ICMP) Parameters**. Disponível em: <<http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xhtml>>. Acesso: 10 set. 2016.

_____. **IPv4 Address Space Registry**. Disponível em: <<http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml>>. Acesso: 12 ago. 2016.

_____. **Root Zone Database**. Disponível em: <<http://www.iana.org/domains/root/db>>. Acesso: 20 set. 2016.

_____. **Service Name and Transport Protocol Port Number Registry**. Disponível em: <<http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml>>. Acesso: 04 ago. 2016.

IEEE, Institute of Electrical and Electronics Engineers. **802.11 Wireless Local Area Networks - The Working Group for WLAN Standards**. Disponível em: <<http://www.ieee802.org/11/>>. Acesso: 26 out. 2016.

IETF – Internet Engineering Task Force. **Basic Transition Mechanisms for IPv6 Hosts and Routers**. Disponível em: <<https://www.ietf.org/rfc/rfc4213.txt>>. Acesso: 09 out. 2016.

_____. **Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy**. Disponível em: <<https://www.ietf.org/rfc/rfc1519.txt?number=1519>>. Acesso: 04 out. 2016.

_____. **Domain Names: Implementation and Specification**. Disponível em: <<https://www.ietf.org/rfc/rfc1035.txt>>. Acesso: 03 nov. 2016.

- _____. **An Ethernet Address Resolution Protocol.** Disponível em: <<https://tools.ietf.org/html/rfc826>>. Acesso: 28 out. 2016.
- _____. **File Transfer Protocol (FTP).** Disponível em: <<https://www.ietf.org/rfc/rfc959.txt>>. Acesso: 15 out. 2016.
- _____. **Hypertext Transfer Protocol.** Disponível em: <<https://www.ietf.org/rfc/rfc2616.txt>>. Acesso: 19 out. 2016.
- _____. **Internet Assigned Numbers Authority (IANA) Procedures for the Management of the Service Name and Transport Protocol Port Number Registry.** Disponível em: <<https://www.ietf.org/rfc/rfc6335.txt>>. Acesso: 19 set. 2016.
- _____. **Internet Control Message Protocol.** Disponível em: <<https://www.ietf.org/rfc/rfc792.txt>>. Acesso: 25 out. 2016.
- _____. **Internet Protocol, Version 6 (IPv6).** Disponível em: <<https://tools.ietf.org/html/rfc2460>>. Acesso: 8 out. 2016.
- _____. **Internet Standard Subnetting Procedure.** Disponível em: <<http://www.ietf.org/rfc/rfc950.txt>>. Acesso: 24 ago. 2016.
- _____. **Network Subsystem for Time Sharing Hosts.** Disponível em: <<https://tools.ietf.org/html/rfc15>>. Acesso: 28 out. 2016.
- _____. **The Secure HyperText Transfer Protocol.** Disponível em: <<https://www.ietf.org/rfc/rfc2660.txt>>. Acesso: 21 out. 2016.
- _____. **The Secure Shell (SSH) Transport Layer Protocol.** Disponível em: <<https://tools.ietf.org/html/rfc4253>>. Acesso: 03 nov. 2016.
- _____. **Special Use IPv4 Addresses.** Disponível em: <<https://tools.ietf.org/html/rfc5735>>. Acesso: 07 set. 2016.
- _____. **Telnet Protocol Specification.** Disponível em: <<https://tools.ietf.org/html/rfc854>>. Acesso: 03 nov. 2016.
- _____. **User Datagram Protocol.** Disponível em: <<http://www.ietf.org/rfc/rfc768.txt>>. Acesso: 04 ago. 2016.
- ISO, International Organization for Standardization. **Standards.** Disponível em: <<http://www.iso.org/iso/home/standards.htm>>. Acesso: 26 set. 2016.

KOZIEROK, Charles M. **TCP/IP Guide: A Comprehensive, Illustrated Internet Protocols Reference.** 1 ed. E. São Francisco: No Starch, 2005.

KUROSE, James F.; ROSS Keth W. **Redes de computadores e a internet: uma abordagem top-down.** 5 ed. São Paulo: Pearson, 2010.

ODOM, Wendell. **CCENT/CCNA ICND 1: 640-822 Guia oficial de certificação do exame.** 3 ed. Rio de Janeiro: Alta Books, 2013.

ROSS, John. **O livro do wireless: um guia definitivo para Wi-fi redes sem fio.** 2 ed. São Paulo: Alta Books, 2009.

RUFINO, Nelson Murilo de O. **Segurança em redes sem fio.** 4 ed. São Paulo: Novatec, 2015.

SILVA, César Felipe Gonçalves. **Configurando switches e roteadores Cisco: Guia para certificação CCENT/CCNA.** 1 ed. São Paulo: Brasport, 2013.

TANENBAUM, Andrew S. WETHERALL, David J. **Redes de computadores.** 5 ed. São Paulo: Pearson, 2011.

Sobre o autor

José Wagner Bungart é engenheiro de Telecomunicações, especialista em Informática empresarial, especialista em Redes corporativas – voz e dados, possui MBA em Gestão de Tecnologia da Informação e é mestrando em Engenharia da Computação, na área de Infraestrutura Computacional. Nessa pesquisa segue a linha de otimização de redes de sensores sem fio com o uso de redes definidas por software.

Desde 1996 trabalha como engenheiro especialista em grandes empresas de Telecomunicações, consultor e gerente de Engenharia e Infraestrutura de Tecnologia da Informação. Em sua carreira acadêmica, atua como professor em cursos técnicos, de graduação e pós-graduação nas áreas de Redes de Computadores, Segurança da Informação, Telecomunicações, Ciência da Computação e Gestão de TI.

SENAI-SP editora

Coordenação geral

Raimundo Ernando de Melo Junior

Coordenação editorial

Glaucê Perusso Pereira Dias Muniz

Direitos autorais

Aldrey Barbosa

Edilza Leite

Viviane Medeiros de Souza Guedes

Edição

Monique Gonçalves

Tania Mano

Eloah Pina

Assistência editorial

Mariane Cristina de Oliveira

Preparação

Débora Donadel

Revisão

Alexandra Maria Misurini

Olivia Yumi Duarte

Capa

Inventum Design

Diagramação

Robson Santos | Tikinet

Produção gráfica

Ana Carolina Almeida de Moura

Rafael Zemantauskas

© SENAI-SP Editora, 2019

A SENAI-SP Editora empenhou-se em identificar e contatar todos os responsáveis pelos direitos autorais deste livro. Se porventura for constatada omissão na identificação de algum material, disponibilizaremos a efetuar, futuramente, os possíveis acertos.

Esta publicação integra uma série da SENAI-SP Editora especialmente criada para apoiar os cursos do SENAI-SP.

O mercado de trabalho em permanente mudança exige que o profissional se atualize continuamente ou, em muitos casos, busque qualificações. É para esse profissional, sintonizado com a evolução tecnológica e com as inovações nos processos produtivos, que o SENAI-SP oferece muitas opções em cursos, em diferentes níveis, nas diversas áreas tecnológicas.

ISBN 978-85-8393-765-4

