



Redes de Computadores

Roberto Franciscatto

Fernando de Cristo

Tiago Perlin



Frederico Westphalen - RS
2014

Presidência da República Federativa do Brasil
Ministério da Educação
Secretaria de Educação Profissional e Tecnológica

© Colégio Agrícola de Frederico Westphalen
Este caderno foi elaborado em parceria entre o Colégio Agrícola de Frederico Westphalen – CAFW e a Universidade Federal de Santa Maria para a Rede e-Tec Brasil.

Equipe de Elaboração
Colégio Agrícola de Frederico Westphalen – CAFW

Reitor
Paulo Afonso Burmann/UFSM

Direção
Fernando de Cristo/CAFW

Coordenação Geral da Rede e-Tec – UFSM
Paulo Roberto Colusso/CTISM

Coordenação de Curso
Adriana Soares Pereira/CAFW

Professor-autor
Roberto Franciscatto/CAFW
Fernando de Cristo/CAFW
Tiago Perlin/CAFW

Equipe de Acompanhamento e Validação
Colégio Técnico Industrial de Santa Maria – CTISM

Coordenação Institucional
Paulo Roberto Colusso/CTISM

Coordenação de Design
Erika Goellner/CTISM

Revisão Pedagógica
Elisiane Bortoluzzi Scrimini/CTISM
Jaqueline Müller/CTISM
Laura Pippi Fraga/CTISM

Revisão Textual
Carlos Frederico Ruviano/CTISM

Revisão Técnica
Rogério Turchetti/CTISM

Ilustração
Marcel Santos Jacques/CTISM
Rafael Cavalli Viapiana/CTISM
Ricardo Antunes Machado/CTISM

Diagramação
Cássio Fernandes Lemos/CTISM
Leandro Felipe Aguilar Freitas/CTISM

Bibliotecária Nataly Soares Leite Moro – CRB 10/1981

F819r **Franciscatto, Roberto.**
Redes de computadores / Roberto Franciscatto, Fernando de Cristo, Tiago Perlin. – Frederico Westphalen : Universidade Federal de Santa Maria, Colégio Agrícola de Frederico Westphalen, 2014.
116 p. : il. ; 28 cm.
ISBN: 978-85-63573-46-9

1. Redes de computadores. 2. Transmissão de dados. I. Cristo, Fernando de. II. Perlin, Tiago. III. Universidade Federal de Santa Maria. Colégio Agrícola de Frederico Westphalen. III. Título.

CDU 004.7

Apresentação e-Tec Brasil

Prezado estudante,
Bem-vindo a Rede e-Tec Brasil!

Você faz parte de uma rede nacional de ensino, que por sua vez constitui uma das ações do Pronatec – Programa Nacional de Acesso ao Ensino Técnico e Emprego. O Pronatec, instituído pela Lei nº 12.513/2011, tem como objetivo principal expandir, interiorizar e democratizar a oferta de cursos de Educação Profissional e Tecnológica (EPT) para a população brasileira propiciando caminho de o acesso mais rápido ao emprego.

É neste âmbito que as ações da Rede e-Tec Brasil promovem a parceria entre a Secretaria de Educação Profissional e Tecnológica (SETEC) e as instâncias promotoras de ensino técnico como os Institutos Federais, as Secretarias de Educação dos Estados, as Universidades, as Escolas e Colégios Tecnológicos e o Sistema S.

A educação a distância no nosso país, de dimensões continentais e grande diversidade regional e cultural, longe de distanciar, aproxima as pessoas ao garantir acesso à educação de qualidade, e promover o fortalecimento da formação de jovens moradores de regiões distantes, geograficamente ou economicamente, dos grandes centros.

A Rede e-Tec Brasil leva diversos cursos técnicos a todas as regiões do país, incentivando os estudantes a concluir o ensino médio e realizar uma formação e atualização contínuas. Os cursos são ofertados pelas instituições de educação profissional e o atendimento ao estudante é realizado tanto nas sedes das instituições quanto em suas unidades remotas, os polos.

Os parceiros da Rede e-Tec Brasil acreditam em uma educação profissional qualificada – integradora do ensino médio e educação técnica, – é capaz de promover o cidadão com capacidades para produzir, mas também com autonomia diante das diferentes dimensões da realidade: cultural, social, familiar, esportiva, política e ética.

Nós acreditamos em você!
Desejamos sucesso na sua formação profissional!

Ministério da Educação
Setembro de 2013

Nosso contato
etecbrasil@mec.gov.br



Indicação de ícones

Os ícones são elementos gráficos utilizados para ampliar as formas de linguagem e facilitar a organização e a leitura hipertextual.



Atenção: indica pontos de maior relevância no texto.



Saiba mais: oferece novas informações que enriquecem o assunto ou “curiosidades” e notícias recentes relacionadas ao tema estudado.



Glossário: indica a definição de um termo, palavra ou expressão utilizada no texto.



Mídias integradas: sempre que se desejar que os estudantes desenvolvam atividades empregando diferentes mídias: vídeos, filmes, jornais, ambiente AVEA e outras.



Atividades de aprendizagem: apresenta atividades em diferentes níveis de aprendizagem para que o estudante possa realizá-las e conferir o seu domínio do tema estudado.



Sumário

Palavra do professor-autor	9
Apresentação da disciplina	11
Projeto instrucional	13
Aula 1 – Introdução às redes de computadores	15
1.1 Considerações iniciais.....	15
1.2 O surgimento das redes de computadores.....	15
1.3 Tipos de redes de computadores.....	16
1.4 Principais componentes de uma rede de computadores.....	22
Aula 2 – Topologias de redes de computadores	29
2.1 Considerações iniciais.....	29
2.2 Classificação das topologias de rede.....	29
Aula 3 – Arquitetura de redes de computadores	37
3.1 Considerações iniciais.....	37
3.2 O modelo de referência ISO/OSI.....	37
3.3 A arquitetura TCP/IP.....	44
Aula 4 – Protocolos de redes de computadores	49
4.1 Considerações iniciais.....	49
4.2 Protocolos da camada de aplicação.....	50
4.3 Protocolos da camada de transporte.....	55
4.4 Protocolos da camada internet da arquitetura TCP/IP.....	60
4.5 Protocolos da camada física (interface de rede).....	71
Aula 5 – Meios de transmissão de dados	75
5.1 Considerações iniciais.....	75
5.2 Cabeamento.....	75
5.3 Redes de transmissão sem-fio.....	90
Aula 6 – Equipamentos utilizados nas redes de computadores	99
6.1 Considerações iniciais.....	99
6.2 Placas de rede.....	99

6.3 <i>Hub</i>	100
6.4 <i>Switch</i>	102
6.5 <i>Gateway</i>	103
6.6 Roteador.....	103
6.7 <i>Bridges</i>	104
6.8 <i>Transceiver</i>	105
6.9 Repetidores de sinal.....	105
Aula 7 – Redes locais na prática	107
7.1 Considerações iniciais.....	107
Referências	114
Currículo do professor-autor	116

Palavra do professor-autor

Prezado estudante, é com satisfação que chegamos até você através deste caderno didático que trata das redes de computadores. Como técnico em informática para internet é de fundamental importância conhecer os conceitos, características e elementos que compõe uma rede de computadores, bem como, entender seu funcionamento.

Este caderno tem o objetivo de servir como um apoio presencial para a disciplina de Redes de Computadores e seu conteúdo foi pensado de forma que possa ser útil para seu aprendizado durante o curso. Nesse material você conhecerá as topologias, arquiteturas, protocolos, equipamentos que compõe uma rede, além de uma aula que aborda estudos de casos práticos, para melhor absorção dos conteúdos apresentados.

Para que você possa fazer um bom uso deste caderno é de fundamental importância a leitura, resolução de exercícios e acesso às referências extras apresentadas durante esse material.

Desejamos um excelente aprendizado e que você possa utilizar e colocar em prática os conhecimentos relativos às redes de computadores apresentados aqui. Não esqueça de ler constantemente esse material, acompanhar regularmente a disciplina em seu ambiente de aprendizagem, além de interagir com professores, tutores e colegas.

Lembre-se, o seu sucesso depende de seu esforço e dedicação.

Um grande abraço e bons estudos!

Roberto Franciscatto

Fernando de Cristo

Tiago Perlin



Apresentação da disciplina

Na disciplina de Redes de Computadores, você irá estudar sobre os principais conceitos, bem como, terá uma visão geral das tecnologias que permeiam e constituem uma rede de computadores.

O conteúdo dessa disciplina foi dividido em oito aulas, seguindo uma sequência lógica de aprendizado, apresentando desde os conceitos iniciais das redes de computadores até chegarmos aos estudos de caso, que tem por objetivo colocar em prática os conhecimentos básicos apresentados durante todo o caderno.

Na primeira aula, serão introduzidos os principais conceitos relacionados às redes de computadores, a evolução histórica, além de apresentação dos tipos existentes de redes quanto a extensão geográfica. Na segunda aula, são apresentadas as principais topologias de redes, suas classificações, características, vantagens e desvantagens. Na terceira aula, falaremos sobre a arquitetura das redes, onde serão abordados, principalmente, os modelos de referência OSI e TCP/IP, bem como, as funções e detalhamento de cada uma de suas camadas. Na quarta aula, o assunto a ser abordado são os protocolos de rede, onde estudaremos os principais, suas funções e importância de sua utilização em nosso dia-a-dia. Na quinta aula, os meios de transmissão de dados são apresentados, nessa aula aprenderemos sobre os principais meios utilizados nas redes (cabramento metálico, sem-fio e fibras ópticas). Na aula seis, conheceremos os equipamentos que utilizamos para construir uma rede. Neste ponto é necessário conhecer os principais equipamentos, suas funções e importância ao construir uma rede.

Por fim, no capítulo sete, são apresentados os estudos de caso, como forma de mostrar de maneira prática o processo de construção e configuração básica de uma rede local de computadores, fazendo o fechamento da disciplina.



Projeto instrucional

Disciplina: Redes de Computadores (carga horária: 60h).

Ementa: Apresentar as características lógicas dos serviços de redes TCP/IP, equipamentos de comunicação da camada 1, 2 e 3 do modelo OSI, assim como os padrões IEEE 802 e seus meios físicos de comunicação.

AULA	OBJETIVOS DE APRENDIZAGEM	MATERIAIS	CARGA HORÁRIA (horas)
1. Introdução às redes de computadores	Introduzir os principais conceitos relacionados às redes de computadores. Mostrar a evolução histórica das redes. Apresentar os tipos existentes de redes quanto à extensão geográfica.	Ambiente virtual: plataforma Moodle. Apostila didática. Recursos de apoio: <i>links</i> , exercícios.	07
2. Topologias de redes de computadores	Apresentar as principais topologias de redes e suas classificações. Caracterizar as topologias e sua formação. Conhecer as topologias em sua essência. Apresentar as principais características relacionadas às topologias, suas vantagens e desvantagens.	Ambiente virtual: plataforma Moodle. Apostila didática. Recursos de apoio: <i>links</i> , exercícios.	08
3. Arquitetura de redes de computadores	Especificar o modelo de Referência OSI. Entender os objetivos e funções de cada camada que compõe o modelo OSI. Caracterizar a arquitetura TCP/IP. Especificar as camadas da arquitetura TCP/IP e suas diferenças frente ao modelo OSI.	Ambiente virtual: plataforma Moodle. Apostila didática. Recursos de apoio: <i>links</i> , exercícios.	07
4. Protocolos de redes de computadores	Entender o funcionamento dos principais protocolos utilizados nas redes de computadores. Compreender quais protocolos são utilizados em cada camada. Conhecer o funcionamento dos protocolos mais usuais no dia-a-dia dos usuários. Ter o entendimento do endereçamento IP em suas versões 4 e 6.	Ambiente virtual: plataforma Moodle. Apostila didática. Recursos de apoio: <i>links</i> , exercícios.	08

AULA	OBJETIVOS DE APRENDIZAGEM	MATERIAIS	CARGA HORÁRIA (horas)
5. Meios de transmissão de dados	<p>Conhecer os principais meio de transmissão de dados utilizados nas redes de computadores.</p> <p>Compreender as redes de cabeamento metálico, sem-fio e de fibra óptica.</p> <p>Ter o entendimento das principais tecnologias associadas a transmissão de dados.</p> <p>Compreender a utilização dos meios de transmissão no dia-a-dia das redes de computadores.</p>	<p>Ambiente virtual: plataforma Moodle.</p> <p>Apostila didática.</p> <p>Recursos de apoio: <i>links</i>, exercícios.</p>	07
6. Equipamentos utilizados nas redes de computadores	<p>Conhecer os principais equipamentos utilizados nas redes de computadores.</p> <p>Compreender o funcionamento destes equipamentos.</p> <p>Conhecer as características quanto a utilização e função dos equipamentos principais das redes.</p> <p>Ter um entendimento dos equipamentos necessários para montar uma rede local de computadores.</p>	<p>Ambiente virtual: plataforma Moodle.</p> <p>Apostila didática.</p> <p>Recursos de apoio: <i>links</i>, exercícios.</p>	08
7. Redes locais na prática	<p>Aprender a crimpar um cabo de rede do tipo par trançado utilizando os padrões estudados em aulas anteriores.</p> <p>Conhecer os equipamentos básicos necessários para montar uma rede local de computadores.</p> <p>Configurar e testar o funcionamento de uma rede local básica.</p>	<p>Ambiente virtual: plataforma Moodle.</p> <p>Apostila didática.</p> <p>Recursos de apoio: <i>links</i>, exercícios.</p>	15

Aula 1 – Introdução às redes de computadores

Objetivos

Introduzir os principais conceitos relacionados às redes de computadores.

Mostrar a evolução histórica das redes.

Apresentar os tipos existentes de redes quanto à extensão geográfica.

1.1 Considerações iniciais

As redes de computadores constituem-se de um conjunto de dois ou mais computadores interligados com o objetivo de compartilhar recursos e trocar informações.

Cada vez mais presentes no dia-a-dia das pessoas, as redes de computadores estão espalhadas em diversos locais: grandes e médias empresas, pequenos escritórios ou até mesmo em casa.

Um exemplo de uma rede de computadores é a internet. A internet é caracterizada por uma rede de computadores descentralizada que envolve diferentes meios de comunicação, que permite aos seus usuários a troca de informações constante.

1.2 O surgimento das redes de computadores

Instituídas durante a década de 60, as primeiras redes de computadores tinham o propósito de trocar dados entre dois computadores. O cartão perfurado era o meio utilizado para armazenar dados, sendo que o mesmo constituía-se como uma forma demorada e trabalhosa de transportar grandes quantidades de informações.

No período entre 1970 e 1973, com a criação da **Arpanet**, foi possível a criação de uma rede para interligação entre universidades, instituições militares e empresas. Os *hardwares* utilizados nessa época eram os *mainframes*, caracterizados por um poder de processamento baixo e com preços elevados.

A-Z

Arpanet

Rede de comunicação de dados criada pela Agência de Pesquisas em Projetos Avançados (ARPA) dos EUA, que inicialmente conectou algumas universidades e centros de pesquisa, por volta de 1969.

Serviços como *e-mail*, FTP e DNS, foram criados, permitindo aos usuários realizar diferentes tipos de tarefas. Esses recursos serviram de base para o que se tem hoje.

Com a evolução crescente dos meios de comunicação e as tecnologias, a década de 90 ficou caracterizada com a expansão do acesso à internet. Neste caso, redes dos mais variados tipos ganharam seu espaço no mercado. O padrão Ethernet popularizou-se e espalhou-se, sendo utilizado com frequência na construção de redes locais de computadores (LAN's).

Neste período, o acesso à internet através de linha discada era uma realidade comum em empresas, haja vista que era necessário um modem e uma linha telefônica, o que muitas vezes tornava-se uma solução custosa. Como solução a esta alternativa discada, surgiram as linhas de *frame relay* (conexão dedicada com velocidades de 64 *kbits*). Esse tipo de conexão facilitava o acesso à internet em computadores de uma mesma rede, pois permitia compartilhar a conexão entre os computadores da rede, além de permitir que todos estivessem permanentemente conectados.

Hoje é possível construir redes através de inúmeras possibilidades: redes cabeadas (Ethernet, fibra óptica), sem-fio (rádio, **Bluetooth**, Wi-Fi), entre outros. O custo, velocidade entre outros fatores é influenciado pelas tecnologias e dispositivos empregados na construção desta rede.

As redes de computadores apesar da evolução e crescente propagação, mantém seu objetivo primordial: compartilhar recursos (tanto de *hardware* como *software*) e propiciar a troca de informações (MORIMOTO, 2008a).

A-Z

Bluetooth

É o nome dado à tecnologia de comunicação sem-fio de que permite transmissão de dados e arquivos através de dispositivos como telefones celulares, *smartphones*, *notebooks*, câmeras digitais, impressoras, teclados, *mouses* e até fones de ouvido, entre outros equipamentos de maneira rápida e segura.

1.3 Tipos de redes de computadores

As redes de computadores, geralmente, são classificadas de acordo com sua disposição geográfica e hierarquia.

1.3.1 Classificação das redes quanto à extensão geográfica

Neste quesito, as redes são classificadas quanto ao alcance das mesmas, sendo que diversas classificações são propostas como forma de caracterização destes tipos de redes, conforme os tópicos a seguir.

Uma rede local de computadores é utilizada com frequência para conectar computadores em rede, servidores, dispositivos eletrônicos diversos (*tablets, netbooks, notebooks, etc.*). Sua limitação geográfica faz com que as LAN's sejam utilizadas em casas, escritórios, escolas, empresas, entre outros meios locais.

1.3.1.3 MAN

Uma MAN (*Metropolitan Area Network*) rede de área metropolitana, corresponde a uma rede de computadores que compreende um espaço de média dimensão (região, cidade, campus, entre outros). Geralmente uma MAN está associada a interligação de várias LAN's e é considerada uma parte menor de uma WAN (que será descrita no próximo item).

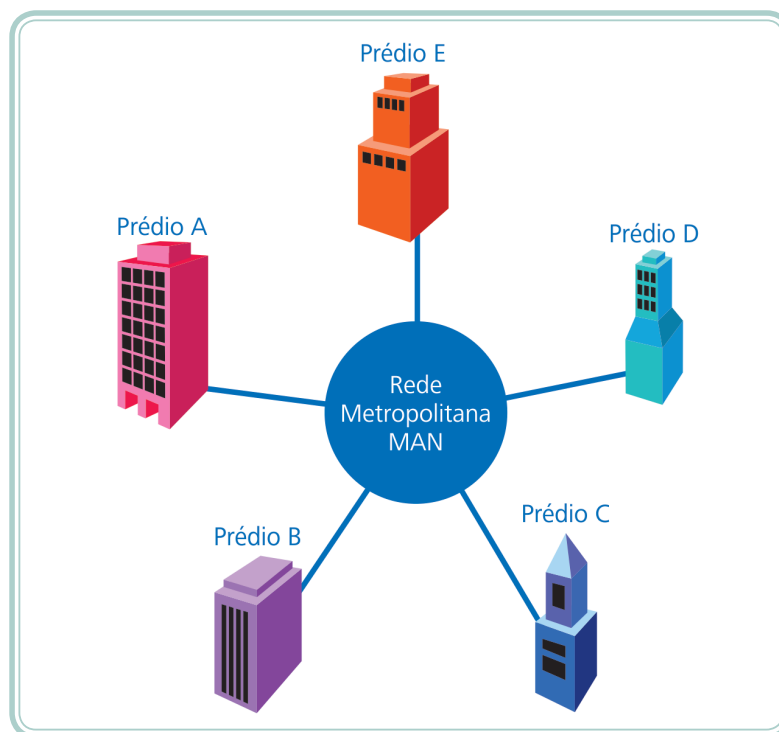


Figura 1.3: Exemplo de uma rede MAN

Fonte: CTISM, adaptado de <http://cyberti54.blogspot.com.br/2010/09/o-que-e-uma-rede-man.html>



Um exemplo de MAN são as redes ISP (*Internet Service Provider*) que em português significa "provedor de serviço de internet". Um ISP nada mais é do que uma empresa (provedor) que fornece acesso à internet e demais serviços de um ISP como: contas de *e-mail*, hospedagem de *sites*, entre outros, mediante o pagamento de uma mensalidade ou taxa. As formas de conexão a esta rede podem ser através de uma linha telefônica (*dial-up*), ou uma conexão de banda larga (*wireless, cabo* ou DSL). As redes ISPs são exemplos clássicos de MAN.

1.3.1.4 WAN

Uma WAN (*Wide Area Network*) ou rede de longa distância, corresponde a uma rede de computadores que abrange uma grande área geográfica, como por exemplo um país, continente, entre outros. As WAN's permitem a comunicação a longa distância, interligando redes dentro de uma grande região geográfica.

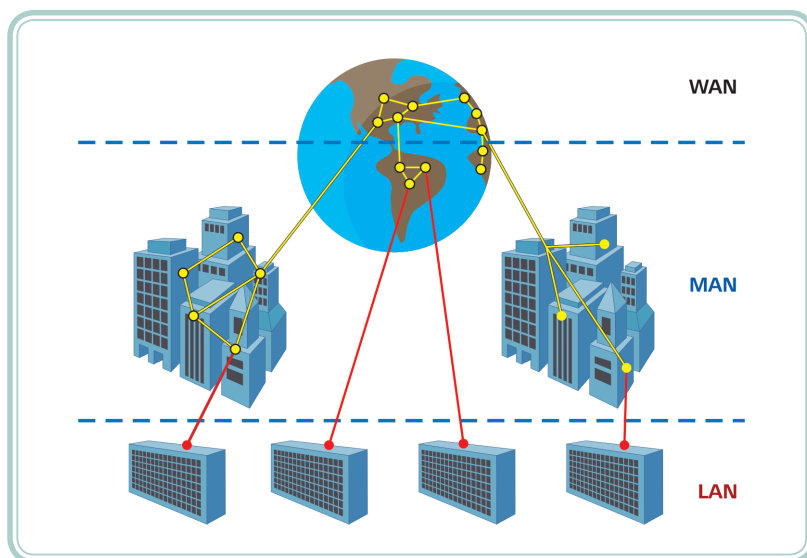


Figura 1.4: Exemplo de uma rede WAN

Fonte: CTISM

1.3.1.5 Demais classificações quanto a extensão geográfica

Uma série de outras nomenclaturas são utilizadas para descrever outros tipos de redes, quanto a extensão geográfica que as mesmas atuam. A seguir é possível conhecer algumas:

- **WMAN** – rede de área metropolitana sem-fio, destina-se principalmente a operadores de telecomunicações.
- **WWAN** – rede de longa distância sem-fio, são comumente utilizadas para criação de redes de transmissão celular.
- **RAN** – considerada uma subcategoria de uma MAN, uma RAN (*Regional Area Network*), corresponde a uma rede de computadores de uma região geográfica específica.
- **CAN** – uma CAN (*Campus Area Network*) corresponde a uma rede de computadores formada por computadores dispostos em edifícios, prédios, campus, entre outros (MENDES, 2007).

1.3.2 Classificação de redes quanto a hierarquia

A classificação das redes de computadores quanto a hierarquia refere-se ao modo como os computadores dentro de uma rede se comunicam. Entre os principais tipos de classificação quanto a hierarquia, estão as redes **ponto-a-ponto** e as redes **cliente-servidor**, que veremos a seguir.

1.3.2.1 Redes ponto-a-ponto

Uma rede ponto-a-ponto normalmente é utilizada em pequenas redes. Neste tipo de rede os computadores trocam informações entre si, compartilhando arquivos e recursos.

Uma rede do tipo ponto-a-ponto possui algumas características pontuais:

- É utilizada em pequenas redes.
- São de implementação fácil e de baixo custo.
- Possuem pouca segurança.
- Apresentam um sistema de cabeamento simples.

Ao citarmos uma vantagem e uma desvantagem deste tipo de rede, podemos considerar como ponto positivo o baixo custo para implementar uma rede do tipo ponto-a-ponto, onde todos os computadores podem acessar diretamente todos os demais computadores e seus recursos compartilhados. Um ponto negativo neste tipo de rede está relacionado a baixa segurança que este modelo proporciona.

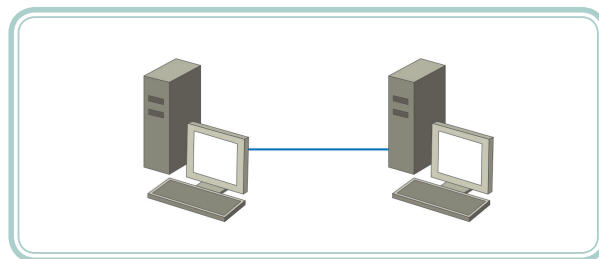


Figura 1.5: Exemplo de uma rede ponto-a-ponto

Fonte: CTISM

1.3.2.2 Redes cliente-servidor

Uma rede de computadores do tipo cliente-servidor possui um ou mais servidores, responsáveis por prover serviços de rede aos demais computadores conectados a ele que são chamados clientes. Cada cliente (computador que

compõe este tipo de rede) que deseja acessar um determinado serviço ou recurso faz essa solicitação ao servidor da rede, por isso o nome cliente-servidor.

Esse tipo de rede surgiu da necessidade de criar uma estrutura que centralizasse o processamento em um computador central da rede (no caso o servidor, com recursos de *hardware* preparados para tal processamento). Como exemplos de serviços de rede que um servidor pode executar estão: servidor de aplicativos, serviço de impressão, hospedagem de *sites*, servidor de *e-mail*, servidor de arquivos, entre outros.

Os computadores clientes, também chamados de “nós” em uma rede de computadores, são as estações de trabalho ou *desktops*. Os computadores clientes são utilizados pelos usuários que acessam as informações armazenadas no servidor e executam aplicações locais.

Como características deste tipo de rede podemos citar:

- Maior custo e implementação mais complexa que uma rede do tipo ponto-a-ponto.
- Existência de pelo menos um servidor da rede.
- Redes do tipo cliente-servidor, apresentam uma estrutura de segurança melhorada, pois as informações encontram-se centralizadas no servidor, o que facilita o controle e o gerenciamento dos mesmos.
- Neste tipo de rede não há tolerância a falhas (como existe em um sistema descentralizado) haja vista um único sistema centralizado de informações (servidor).
- Um servidor de rede é um computador projetado (*hardware*) para suportar a execução de várias tarefas que exigem bastante do *hardware* (como disco rígido e processador), diferentemente de uma estação de trabalho (cliente), que não possui características para realizar o trabalho de um servidor (quando falamos puramente do *hardware* necessário a um computador servidor).
- No contexto do *software* para servidores, deve prover serviços usuais para atender os clientes da rede: autenticação, compartilhamento de recursos, entre outros.

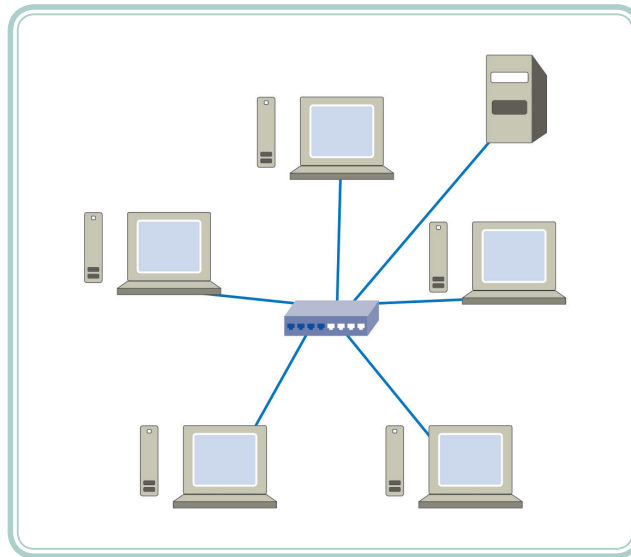


Figura 1.6: Exemplo de uma rede cliente/servidor

Fonte: CTISM

1.4 Principais componentes de uma rede de computadores

Uma rede de computadores é formada por diversos dispositivos, equipamentos, entre outros, para que a mesma possa funcionar corretamente e cumprir o objetivo geral de uma rede: a troca de informações e o compartilhamento de recursos, sejam eles recursos de *hardware* ou *software*. Nos próximos itens faremos uma abordagem inicial dos principais componentes que compõem uma rede de computadores.

1.4.1 Servidores

Um servidor, em uma rede de computadores, desempenha diversas tarefas. Entre elas estão: prover diferentes serviços aos computadores que acessam estes servidores, denominados clientes, além de executar serviços como: servidor de arquivos, aplicações, impressão, *e-mail*, *backup*, acesso remoto, entre outros tantos.

Para o bom funcionamento de um servidor, que irá trabalhar com um grande número de requisições, é necessário que o mesmo possua *hardwares* específicos para este fim, ou seja, que o servidor de uma rede possua uma estrutura de *hardware* de servidor e não de um computador comum (*desktop*).

Atualmente, diversas empresas no mercado comercializam servidores, de diferentes tamanhos, estilos e configurações, com preços acessíveis, o que facilita a sua utilização em redes de pequeno, médio e grande porte.

É importante salientar aqui que o servidor deve ser um computador preparado para exercer esta função, tanto no *hardware* com que é composto quanto ao *software* que é empregado no mesmo, ou seja, um servidor deve ter um *hardware* específico para suportar as atividades de servidor e deve também conter um sistema operacional que forneça à máquina capacidade de prover serviços específicos de servidores.

Diversas são as vantagens de se utilizar um servidor em uma rede de computadores, a seguir são citadas algumas delas:

- **Centralização de serviços** – ao utilizar-se um servidor, os serviços de rede (que geralmente são mais do que um) ficam centralizados em um mesmo local, o que facilita a tarefa do administrador do servidor.
- **Backup** – ao centralizar serviços de rede como um servidor de arquivos, *e-mail* e banco de dados, tem-se a facilidade de administrar as cópias de segurança (*backup*), pois todos os serviços, diretórios e arquivos estão centralizados em uma única máquina e não espalhadas por diferentes computadores em uma rede.
- **Acesso remoto** – um servidor pode e, geralmente, tem implementado o serviço de acesso remoto. Dessa forma, usuários podem acessar servidores de uma empresa, por exemplo, de qualquer lugar que tenha acesso à internet, seja em casa, numa praça, etc., como se estivessem na mesma rede local (SILVA, 2010).

1.4.1.1 Tipos de servidores e serviços de rede

Servidores em uma rede de computadores podem executar diferentes serviços em uma mesma máquina física (computador), sendo que, dessa forma, uma única máquina pode prover diferentes serviços para os computadores conectados a essa rede.

Existem, atualmente, diferentes tipos de servidores. Estes servidores são classificados conforme a tarefa que realizam, sendo os principais, listados a seguir:

- **Servidor de arquivos** – tem a função de armazenar os dados que são compartilhados entre os diferentes usuários que compõe uma rede de computadores. Entre estes dados estão o armazenamento de arquivos (texto, planilhas e gráficos). Os programas que manipulam os arquivos são instalados e executados individualmente em cada uma das máquinas, não no servidor, que neste caso é responsável por gerenciar eventuais acessos simultâneos.

- **Servidor de impressão** – um servidor de impressão processa os pedidos de impressão solicitados pelos usuários da rede e gerencia a ordem de impressão em caso de pedidos simultâneos (prioridades podem ser implementadas, caso necessário). Cotas de impressão podem ser implementadas como forma de limitar a quantidade de páginas impressas por usuários.
- **Servidor de aplicações** – é responsável por executar aplicações cliente/servidor, como por exemplo, um banco de dados. Os clientes enviam pedidos ao servidor, que o processa e devolve os dados para serem exibidos em aplicações cliente. A vantagem deste tipo de serviço é que vários usuários podem utilizar uma aplicação ao mesmo tempo.
- **Servidor de e-mail** – responsável pelo armazenamento, processamento de envio e recepção de mensagens eletrônicas (*e-mail*).
- **Servidor de backup** – responsável por executar, armazenar e atualizar cópias de segurança dos dados armazenados no servidor.
- **Servidor WEB** – também conhecido como servidor de hospedagem, armazena as páginas dos usuários que ficarão disponíveis na internet, para acesso pelos clientes via *browsers*. Vale salientar que muitas vezes um servidor WEB está ligado a outros serviços do servidor como banco de dados, servidores de aplicações *server-side*, entre outros.
- **Servidor de DNS** – estes servidores fazem a tradução dos endereços digitados nas URLs dos *browsers* em endereços IP e vice-versa. Este servidor exerce uma tarefa de extrema relevância para as redes de computadores, pois sem eles, cada vez que acessássemos um *site*, por exemplo, teríamos que digitar seu endereço IP correspondente.
- **Servidor proxy** – um *proxy* pode exercer diferentes tipos de serviços a uma rede de computadores. Em geral um *proxy* está associado a *cache*, que nada mais é do que o armazenamento local no servidor das páginas da internet mais visitadas. Dessa forma, cada vez que um novo usuário acessar um *site* já acessado anteriormente, o servidor retornará para este usuário a página armazenada no cache local do servidor, o que se torna muito mais rápido do que abrir uma nova conexão e buscar os dados novamente em um servidor externo.

- **Servidor de FTP** – um servidor de FTP (*File Transfer Protocol*) também conhecido como protocolo de transferência de arquivos tem a função de disponibilizar aos usuários de uma rede um espaço no disco rígido, onde é possível enviar arquivos (*upload*) ou baixar arquivos (*download*), através de um endereço específico.
- **Servidor de virtualização** – bastante utilizado atualmente como forma de reduzir o número de servidores físicos em uma rede de computadores, um servidor de virtualização permite a criação de várias máquinas virtuais em um mesmo computador servidor. Assim, pode-se ter em uma mesma rede, diferentes servidores separados, em um mesmo equipamento, fazendo com que dessa maneira, tenha-se uma maior eficiência em termos de energia despendida a estes serviços, sem prejudicar as funcionalidades de vários sistemas operacionais, sendo executados em mesmo local físico (MORIMOTO, 2008b).

1.4.2 Tipos de sistemas operacionais de servidores

Quanto aos *softwares* utilizados como sistemas operacionais para um servidor em uma rede de computadores, tem-se diversas opções, sendo que algumas delas são soluções pagas (comerciais) e outras livres (quanto a utilização, modificação e alteração).

Os sistemas operacionais para servidores mais utilizados são basicamente os sistemas operacionais Windows, Linux e Mac OS X.

No Quadro 1.1, é possível visualizar os principais sistemas operacionais para servidores, confira:

Quadro 1.1: Sistemas operacionais para servidores		
Windows	Linux	Mac OS X
Windows 2000 Server	Suse	Mac OS X v10.0 Cheetah
Windows 2003 Server	Debian	Mac OS X v10.1 Puma
Windows 2008 Server	Ubuntu	Mac OS X v10.2 Jaguar
Windows 2012 Server	Mandriva	Mac OS X v10.3 Panther
	Red Hat	Mac OS X v10.4 Tiger
	Fedora	Mac OS X v10.5 Leopard
	Slackware	Mac OS X v10.6 Snow Leopard
		Mac OS X v10.7 Lion
		Mac OS X v10.8 Mountain Lion

Fonte: Autores

1.4.3 Principais dispositivos de uma rede

Uma rede de computadores é composta por diferentes dispositivos, cada um com sua função, com o objetivo de dar funcionalidade e organização, bem como, prover a comunicação entre os diferentes componentes de uma rede. A seguir são citados os principais dispositivos de uma rede de computadores, com o intuito de conhecermos um pouco melhor os principais componentes que compõem uma rede (uma descrição completa será apresentada nas próximas aulas):

- **Host** – equipamento utilizado pelos usuários finais para processamento das aplicações e conexão à rede. Enquadram-se nesta descrição os *notebooks*, *netbooks*, computadores pessoais, entre outros.
- **Interface de rede** – cada computador, *notebook*, entre outros dispositivos se conectam à uma rede de computadores através de uma placa de rede. A esta placa de rede é dado o nome de interface de rede. Uma placa de rede pode ser do tipo Ethernet cabeada (na qual um cabo é conectado a esta placa) ou então Ethernet sem-fios (placas que se comunicam via Bluetooth, ondas de rádio, etc.). Características como velocidade, modo de funcionamento e barramento de conexão, podem variar de uma interface para outra.
- **Hub** – o *hub* (concentrador) é um dispositivo cuja função é interligar os computadores de uma rede local. O funcionamento do *hub* se difere de um *switch*, pois o *hub* simplesmente repassa o sinal vindo de um computador para todos os computadores ligados a ele (como um barramento).
- **Switch** – semelhante ao *hub*, um *switch* serve de concentrador em uma rede de computadores com a diferença de que recebe um sinal vindo de um computador origem e entrega este sinal somente ao computador destino. Isto é possível devido a capacidade destes equipamentos em criar um canal de comunicação exclusivo (origem/destino). Esta prática diminui consideravelmente o número de **colisões** e a perda de **pacotes** na rede.
- **Bridge** – ponte de ligação entre duas ou mais redes. Como exemplo, podemos citar uma ponte entre uma rede cabeada e uma rede sem-fio.
- **Gateway** – sinônimo de roteador na arquitetura TCP/IP, é o equipamento que conecta os *hosts* à rede. Em outras arquiteturas de redes, um *gateway* é um dispositivo (*hardware* ou *software*) que converte mensagens de um protocolo em mensagens de outro protocolo.

A-Z

colisões

São perdas de pacotes ocasionadas quando dois ou mais *hosts* tentam transmitir dados simultaneamente utilizando o mesmo meio físico.

pacote

É a forma como é chamado um conjunto de dados enviado através da rede.

- **Roteador** – dispositivo de rede que interconecta duas ou mais redes físicas e encaminha pacotes entre elas.
- **Ponto de acesso wireless (access point)** – equipamento responsável por fazer a interconexão entre todos os dispositivos móveis em uma rede sem-fio. Uma prática comum é a interligação de um *access point* a uma rede cabeada, para, por exemplo, prover acesso à internet e a uma rede local de computadores (ALECRIM, 2004).

Os padrões Ethernet de comunicação de dados possuem diferentes tipos e podem ser tanto cabeados, como sem-fio (*wireless*). Como exemplo de tecnologia Ethernet do tipo cabeada estão os padrões 802.3, 802.4, 802.5, etc. Porém, existem padrões Ethernet sem-fio que são tecnologias bastante utilizadas no dia-a-dia como os padrões 802.11 (b, g, n), 802.15, 802.16, entre outros.

1.4.4 Principais conceitos relacionados às redes de computadores

A seguir, separamos alguns dos principais conceitos relacionados as redes de computadores, como forma de entendermos as principais nomenclaturas e quais suas funções no contexto das redes de computadores:

- **Protocolo** – um protocolo, em uma rede de computadores, nada mais é do que um conjunto de regras e convenções que definem a comunicação dos dispositivos em uma rede. Um dos protocolos mais conhecidos de rede de computadores e da própria internet é o protocolo TCP/IP.
- **TCP/IP** – o protocolo TCP/IP é a junção de dois protocolos diferentes o TCP e o IP. O protocolo TCP (*Transmission Control Protocol*) é o protocolo padrão que define o serviço de circuito virtual da camada de transporte da arquitetura TCP/IP. Já o protocolo IP (*Internet Protocol*) é o protocolo padrão que define o serviço de entrega não confiável e não orientado à conexão da camada de rede do TCP/IP.
- **Endereço IP** – um endereço IP é um identificador de um dispositivo pertencente a uma rede de computadores. Também conhecido como endereço lógico, pode conter endereços reservados, que são utilizados dentro de uma rede local, também conhecidos como não-roteáveis e endereços IP's válidos, utilizados publicamente, inclusive no acesso à internet.
- **Endereço MAC** – um endereço MAC (*Media Access Control*) também conhecido como endereço físico, é atribuído quando da fabricação de



Para conhecer mais e entender o funcionamento destas tecnologias utilizadas nas redes de computadores acesse o endereço:
<http://www.hardware.com.br/livros/redes/padroes-ethernet.html>

uma interface de rede, por exemplo. Este endereço é único para cada dispositivo de rede.

- **Porta** – uma porta em uma rede de computadores corresponde a representação interna do sistema operacional de um ponto de comunicação para envio e recepção de dados. Uma porta é representada por um número, na qual é realizado determinado acesso (TYSON, 2009).

Resumo

Nesta aula, vimos como surgiram as redes de computadores, como se classificam quanto a extensão geográfica (PAN, LAN, MAN, WAN), os principais componentes, entre outros elementos básicos para que você tenha uma ideia inicial das redes e do conteúdo que estudaremos na próxima aula. Para fixar o conteúdo visto em cada aula, é importante que você realize os exercícios de aprendizagem. Em nossa próxima aula, falaremos sobre as topologias das redes de computadores.



Atividades de aprendizagem

1. Qual o objetivo principal de uma rede de computadores?
2. Quais as diferenças entre as redes PAN, LAN, MAN e WAN?
3. Qual a diferença entre uma rede ponto-a-ponto e uma rede cliente-servidor?
4. Cite três tipos de servidores, quanto aos serviços que realizam, explicando a função de cada um deles.

Aula 2 – Topologias de redes de computadores

Objetivos

Apresentar as principais topologias de redes e suas classificações.

Caracterizar as topologias e sua formação.

Conhecer as topologias em sua essência.

Apresentar as principais características relacionadas as topologias, suas vantagens e desvantagens.

2.1 Considerações iniciais

Uma topologia de rede tem o objetivo de descrever como é estruturada uma rede de computadores, tanto fisicamente como logicamente. A topologia física demonstra como os computadores estão dispersos na rede (aparência física da rede). Já a topologia lógica demonstra como os dados trafegam na rede (fluxo de dados entre os computadores que compõe a rede).

2.2 Classificação das topologias de rede

A topologia de uma rede pode ter diferentes classificações. As principais são:

- Barramento.
- Anel.
- Estrela.
- Malha.
- Árvore.
- Híbrida.

2.2.1 Barramento

Na topologia em barramento todos os computadores trocam informações entre si através do mesmo cabo, sendo este utilizado para a transmissão de dados entre os computadores. Este tipo de topologia é utilizada na comunicação ponto-a-ponto. De acordo com Silva (2010), as vantagens da topologia em barramento são:

- Estações de trabalho (nós) compartilham do mesmo cabo.
- São de fácil instalação.
- Utilizam pouca quantidade de cabo.
- Possui baixo custo e grande facilidade de ser implementada em lugares pequenos.

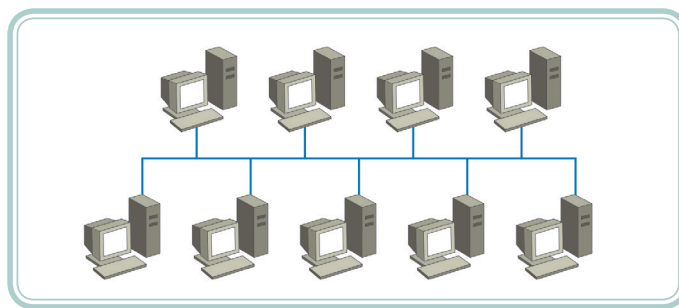


Figura 2.1: Exemplo de uma topologia em barramento

Fonte: CTISM

Como desvantagens deste tipo de topologia, está o fato de que somente um computador pode transmitir informações por vez. Caso mais de uma estação tente transmitir informações ao mesmo tempo, temos uma colisão de pacotes. Cada vez que uma colisão acontece na rede é necessário que o computador reenvie o pacote. Esta tentativa de reenvio do pacote acontece várias vezes, até que o barramento esteja disponível para a transmissão e os dados cheguem até o computador receptor.

Além disso, conforme Silva (2010), outras desvantagens da topologia em barramento são:

- Problemas no cabo (barramento) afetam diretamente todos os computadores desta rede.
- Velocidade da rede variável, conforme a quantidade de computadores ligados ao barramento.

- Gerenciamento complexo (erros e manutenção da rede).

2.2.2 Anel

Uma rede em anel corresponde ao formato que a rede possui. Neste caso, recebem esta denominação pois os dispositivos conectados na rede formam um circuito fechado, no formato de um anel (ou círculo).

Neste tipo de topologia os dados são transmitidos unidirecionalmente, ou seja, em uma única direção, até chegar ao computador destino. Desta forma, o sinal emitido pelo computador origem passa por diversos outros computadores, que retransmitem este sinal até que o mesmo chegue ao computador destino. Vale lembrar aqui que cada computador possui seu endereço que é identificado por cada estação que compõe a rede em anel.

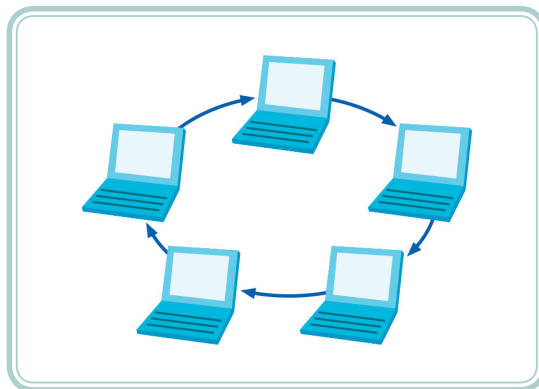


Figura 2.2: Exemplo de uma topologia em anel

Fonte: CTISM

Como vantagens desta topologia estão:

- Inexistência de perda do sinal, uma vez que ele é retransmitido ao passar por um computador da rede.
- Identificação de falhas no cabo é realizada de forma mais rápida que na topologia em barramento.

Como praticamente todas as topologias de rede têm seus pontos positivos e negativos, podemos citar como desvantagens deste tipo de topologia:

- Atraso no processamento de dados, conforme estes dados passam por estações diferentes do computador destino.
- Confiabilidade diminui conforme aumenta o número de computadores na rede.

2.2.3 Estrela

Uma rede em estrela possui esta denominação, pois faz uso de um concentrador na rede. Um concentrador nada mais é do que um dispositivo (*hub*, *switch* ou roteador) que faz a comunicação entre os computadores que fazem parte desta rede. Dessa forma, qualquer computador que queira trocar dados com outro computador da mesma rede, deve enviar esta informação ao concentrador para que o mesmo faça a entrega dos dados.

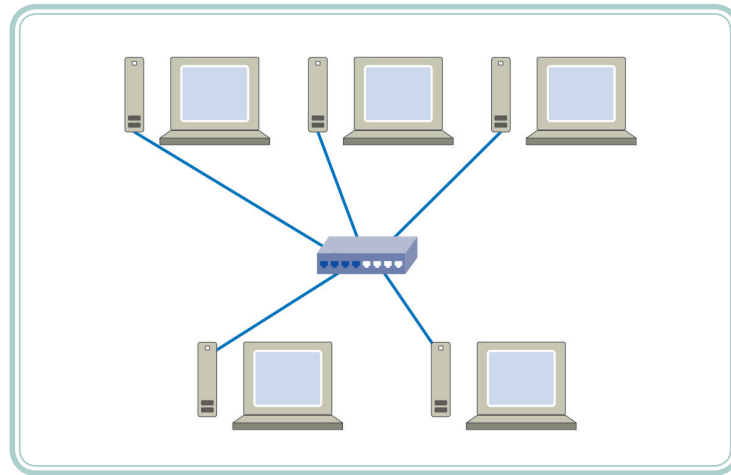


Figura 2.3: Exemplo de uma topologia em estrela

Fonte: CTISM

O concentrador da rede possui a função de realizar o fluxo de dados e o gerenciamento da rede. Concentradores atuais (*switchs* e roteadores) conseguem realizar os procedimentos necessários a rede de forma rápida e sem gerar tráfego a mesma, diferentemente dos antigos *hubs* utilizados neste tipo de topologia, onde os mesmos duplicavam a informação a todos os computadores ligados a ele.

A topologia em estrela apresenta algumas vantagens, as quais são:

- Fácil identificação de falhas em cabos.
- Instalação de novos computadores ligados a rede, ocorre de forma mais simples que em outras topologias.
- Origem de uma falha (cabo, porta do concentrador ou cabo) é mais simples de ser identificada e corrigida.
- Ocorrência de falhas de um computador da rede não afeta as demais estações ligadas ao concentrador.

Como desvantagens ligadas a esta topologia, estão:

- Custo de instalação aumenta proporcionalmente a distância do computador ao concentrador da rede.
- Caso de falha no concentrador afeta toda a rede conectada a ele.

2.2.4 Malha

A topologia em malha refere-se a uma rede de computadores onde cada estação de trabalho está ligada a todas as demais diretamente. Dessa forma, é possível que todos os computadores da rede, possam trocar informações diretamente com todos os demais, sendo que a informação pode ser transmitida da origem ao destino por diversos caminhos.

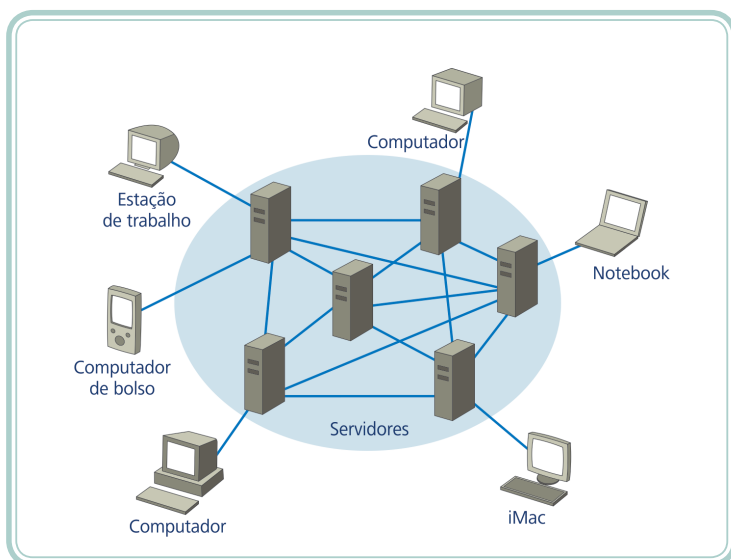


Figura 2.4: Exemplo de uma topologia em malha

Fonte: CTISM

Como vantagens deste tipo de rede, podemos citar:

- Tempo de espera reduzido (devido a quantidade de canais de comunicação).
- Problemas na rede não interferem no funcionamento dos demais computadores.

Uma desvantagem desta topologia está no custo de implementação da mesma, uma vez que para isso, existe a necessidade de instalar uma quantidade de interfaces de rede em cada máquina semelhante a mesma quantidade de computadores existentes na rede em malha.

Exemplo: se tivermos uma rede em malha com seis computadores interligados, será necessário que cada computador tenha cinco placas de rede.

2.2.5 Árvore

Uma topologia em árvore pode ser caracterizada como uma série de barras interconectadas. Esta topologia em árvore nada mais é do que a visualização da interligação de várias redes e sub-redes.

Neste tipo de topologia um concentrador interliga todos os computadores de uma rede local, enquanto outro concentrador interliga as demais redes, fazendo com que um conjunto de redes locais (LAN) sejam interligadas e dispostas no formato de árvore.

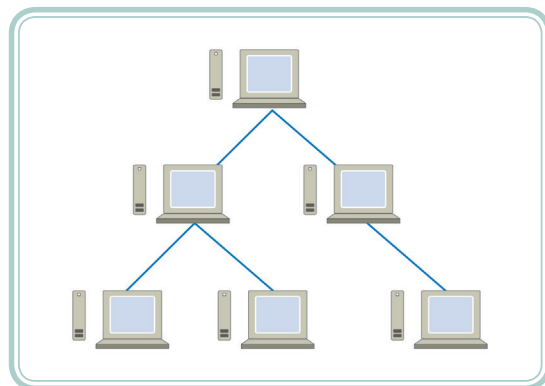


Figura 2.5: Exemplo de uma topologia em árvore

Fonte: CTISM

2.2.6 Híbrida

Este tipo de topologia é aplicada em redes maiores que uma LAN. É chamada de topologia híbrida pois pode ser formada por diferentes tipos de topologia, ou seja, é formada pela união, por exemplo de uma rede em barramento e uma rede em estrela, entre outras.

A finalidade de uma topologia do tipo híbrida está no fato de poder aproveitar o que existe de melhor (custo/benefício) entre os diferentes tipos de topologias, adaptando-as às necessidades de uma empresa, universidade, ou o ambiente onde será aplicada (TYSON, 2009).

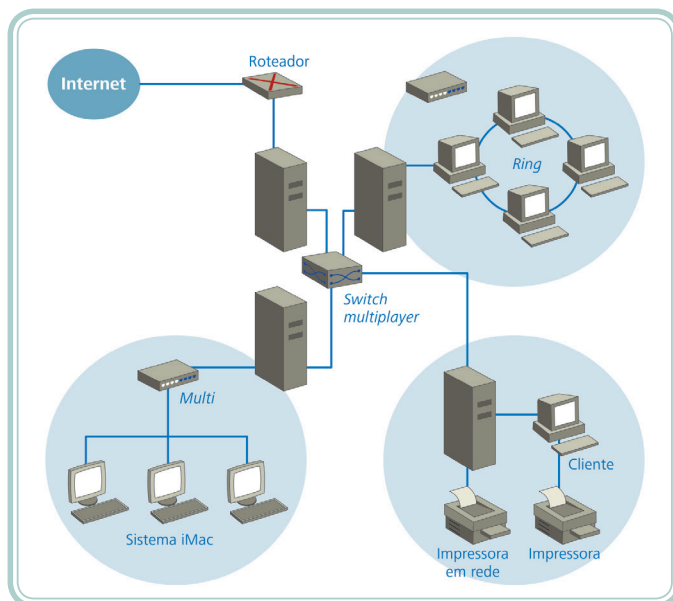


Figura 2.6: Exemplo de uma topologia híbrida

Fonte: CTISM

A seguir é possível visualizar um quadro de comparações entre as principais topologias de rede (estrela, anel e barramento):

Quadro 2.1: Principais topologias de rede e suas características

Topologia/ Características	Estrela	Anel	Barramento
Simplicidade funcional	Melhor	Razoável	Razoável (melhor do que o anel)
Roteamento	Inexistente	Inexistente no anel unidirecionado, simples nos outros tipos	Inexistente
Custo de conexão	Alto	Baixo para médio	Baixo
Crescimento incremental	Limitado à capacidade do nó central	Teoricamente infinito	Alto
Aplicação adequada	Aquelas envolvendo processamento	Sem limitação	Sem limitação
Desempenho	Baixo, todas as mensagens têm de passar pelo nó central	Alto Possibilidade de mais de uma mensagem ser transmitida ao mesmo tempo	Médio
Confiabilidade	Pouca	Boa, desde que sejam tomados cuidados adicionais	A melhor de todas. Interface passiva com o meio
Retardo de transmissão	Médio	Baixo, podendo chegar a não mais do que 1 bit por nó	O mais baixo de todos
Limitação quanto ao meio de transmissão	Nenhuma, ligação ponto-a-ponto	Nenhuma, ligação ponto-a-ponto	Devido à ligação multiponto, sua ligação ao meio de transmissão pode ser de custo elevado

Fonte: Silva, 2010

Resumo

Nesta aula, vimos a classificação das redes quanto as topologias (barramento, anel, estrela, malha, árvore e híbrida) ou seja, a forma com que as redes são distribuídas. Além disso, foi possível entender as características de cada uma, além das vantagens e desvantagens que compõe as mesmas.



Atividades de aprendizagem

1. O que é uma rede do tipo malha?
2. O que é uma topologia do tipo híbrida? Como funciona?
3. Cite um ponto positivo e um ponto negativo, quanto às topologias: estrela, barramento e anel.

Aula 3 – Arquitetura de redes de computadores

Objetivos

Especificar o modelo de referência **OSI**.

Entender os objetivos e funções de cada camada que compõe o modelo OSI.

Caracterizar a arquitetura TCP/IP.

Especificar as camadas da arquitetura TCP/IP e suas diferenças frente ao modelo OSI.

A-Z

OSI

Open System Interconnection ou Interconexão de Sistemas Abertos refere-se a um conjunto de padrões da ISO (*International Standard Organization*) relativo à comunicação de dados, utilizado na comunicação em redes de computadores.

3.1 Considerações iniciais

Esta aula tem o objetivo de apresentar a você aluno os conceitos que motivaram a criação da arquitetura padrão da internet, a arquitetura TCP/IP. Você conhecerá o modelo que foi criado, com a finalidade de padronizar a arquitetura de redes de computadores. Nesta aula, daremos atenção especial aos conceitos envolvidos quanto ao modelo de referência OSI da ISO, para, apenas posteriormente, discutirmos o padrão de fato da internet, a arquitetura TCP/IP.

3.2 O modelo de referência ISO/OSI

O modelo de referência ISO/OSI não determina uma arquitetura de rede específica, apenas define um modelo ou padrão que pode ser seguido para a construção de uma arquitetura de rede. A importância da discussão do modelo de referência OSI está, principalmente, na forma como os conceitos estão organizados em camadas com funções bem definidas. Entender o modelo OSI significa compreender o desafio envolvido na comunicação entre computadores com visão de diferentes níveis ou camadas de abstrações envolvidas.

O modelo OSI está organizado em sete camadas bem definidas: **física, enlace, rede, transporte, sessão, apresentação e aplicação**. Cada camada tem como objetivo abstrair a complexidade das camadas inferiores, com funções definidas e formas de usar os recursos da camada imediatamente inferior. Uma camada fornece à camada superior um serviço através de uma interface simplificada.

A Figura 3.1 representa o modelo ISO/OSI na forma de uma pilha de camadas, cada qual com uma função distinta e ligadas a uma camada inferior e a uma camada superior. Nas próximas seções, abordaremos cada uma das camadas, como forma de entender sua função e seu funcionamento.



Figura 3.1: As sete camadas do modelo de referência ISO/OSI

Fonte: CTISM, adaptado de Comer, 2007, p. 245

3.2.1 Camada física

A camada física fornece as características mecânicas, elétricas, funcionais e de procedimentos para manter conexões físicas para a transmissão de *bits* entre os sistemas ou equipamentos (SOARES, et al., 1995).

A camada física trata apenas de permitir transmissão de *bits* de dados, na forma de sinais elétricos, ópticos ou outra forma de onda eletromagnética. Na camada física não há qualquer controle de erros de transmissão.

Estão incluídos na camada física os meios de transmissão: cabos metálicos (transmissão de sinais elétricos), cabos ópticos (transmissão de ondas luminosas), entre outros e os componentes de *hardware* envolvidos na transmissão: interfaces, *hub*, *hardware* para transmissão de ondas no espectro eletromagnético (rede sem-fio), etc. Na camada física são tratadas questões como taxa de transferência de *bits*, modo de conexão (*simplex*, *half-duplex*, *full-duplex*), topologia de rede, etc. Na Figura 3.2 são apresentados os modos de comunicação *simplex*, *half-duplex* e *full-duplex*, como forma de exemplificar o funcionamento de cada um.

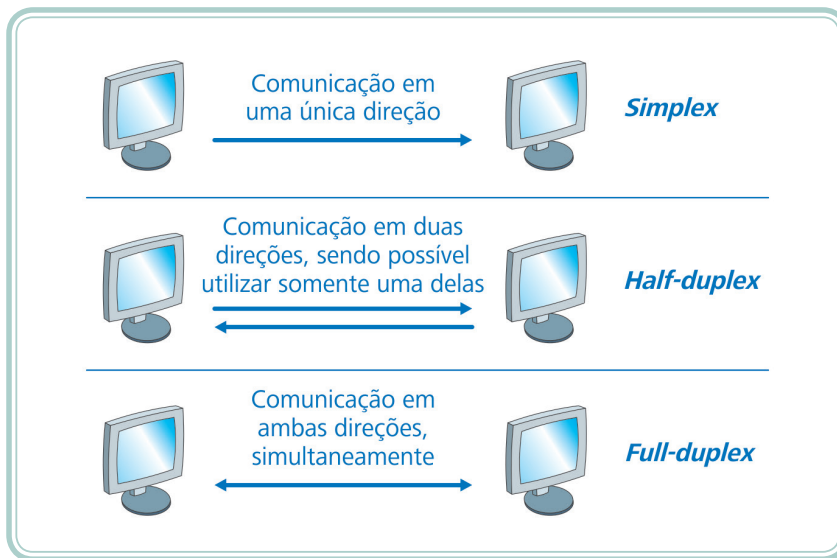


Figura 3.2: Diferenças entre modo de comunicação: simplex, half-duplex e full-duplex
 Fonte: CTISM, adaptado dos autores

3.2.2 Camada de enlace

O objetivo da camada de enlace é detectar e opcionalmente corrigir erros de transmissão da camada física, assim convertendo um canal de transmissão não confiável em um canal confiável, para uso pela camada de rede, logo acima.

Para se conseguir um canal de transmissão confiável na camada de enlace, geralmente são usadas algumas técnicas de identificação ou correção nos quadros de *bits* transmitidos, por meio de inclusão de *bits* redundantes. A correção ou retransmissão de um quadro, quando detectado um erro, é opcional e geralmente é deixada para as camadas superiores do modelo.

A camada de enlace também tem a função de prover um mecanismo de controle de fluxo. Essa função controla o envio de dados pelo transmissor de modo que o receptor não seja inundado com uma quantidade de dados que não consiga processar (SOARES, et al., 1995).

3.2.3 Camada de rede

A camada de rede deve fornecer à camada de transporte um meio para transferir datagramas (também chamados de pacotes dependendo do contexto) pelos pontos da rede até o seu destino. Os datagramas (ou pacotes) são unidades básicas de dados, fragmentos de dados das camadas superiores ou aplicações, com os cabeçalhos necessários para a transmissão. Nessa camada temos o conceito de encaminhamento (ou roteamento) de datagramas, que trata da forma como os datagramas devem ser encaminhados (roteados) pelos nós (roteadores) da rede, de um computador de origem a um computador de destino.

A camada de rede oferece duas classes de serviços: orientados à conexão e não orientados à conexão. No serviço orientado à conexão primeiramente, um transmissor e um receptor estabelecem uma conexão. Todos os pacotes transmitidos posteriormente entre eles são pertencentes àquela conexão (circuito) e normalmente, seguem o mesmo caminho.

No serviço de datagrama não orientado à conexão, cada datagrama enviado é independente dos enviados anteriormente, sem estabelecimento de conexão. Cada datagrama contém em seu cabeçalho a informação do endereço do transmissor (origem, remetente do pacote) e do receptor (destinatário). Os nós intermediários (roteadores) se encarregam de selecionar o melhor caminho e encaminhar (rotear) os datagramas (pacotes) do transmissor (remetente) até o receptor (destinatário) (SOARES, et al., 1995).

3.2.4 Camada de transporte

Até agora, na camada de rede e inferiores, a transferência ocorre, de fato, apenas entre os nós (máquinas) próximos na rede. A camada de transporte, por outro lado, permite que os dados trafeguem em um circuito virtual direto da origem ao destino, sem preocupar-se com a forma que os pacotes de dados viajam na camada de rede e inferiores. A camada de transporte, dessa forma, é responsável pela transferência fim a fim de dados entre processos de uma máquina de origem e processos de uma máquina de destino.

A transferência de dados, na camada de transporte, ocorre de modo transparente, independente da tecnologia, topologia ou configuração das redes nas camadas inferiores. É tarefa da camada de transporte cuidar para que os dados sigam ao seu destino sem erros e na sequência correta, condições para que se crie a ideia de um caminho fim a fim.

Além da detecção e recuperação de erros e controle da sequência dos dados, outras funções desta camada são: multiplexação de conexões e controle de fluxo. A multiplexação permite que vários processos diferentes nas máquinas de origem e destino troquem dados ao mesmo tempo. Os pacotes de dados de vários processos de uma máquina de origem são enviados para vários processos em uma máquina de destino.

Como o meio, usado nas camadas inferiores é compartilhado, os pacotes de dados precisam ser multiplexados (escalonados, embaralhados, misturados), de modo que se tem a impressão de que as transferências ocorrem simultaneamente, em paralelo. O aluno, neste ponto, pode estar se perguntando

como os pacotes multiplexados dos vários processos encontram os processos de destino corretos? Para que isso ocorra, a camada de transporte possui mecanismos para identificar cada pacote ao seu devido fluxo de dados entre os processos. Uma forma de identificação ou endereçamento de pacotes, com relação ao processo de origem e destino, será vista quando tratarmos dos protocolos de transporte da internet.

O controle de erros possui mecanismo para identificar erros de transmissão (pacotes com dados corrompidos, por exemplo) e prover a recuperação desse erro, seja por meio da retransmissão do pacote ou outra forma de reconstrução da informação do pacote. O controle de sequência visa garantir a ordem correta da informação, independentemente da ordem em que os pacotes de dados chegaram ao destino.

Outra função importante da camada de transporte é o controle de fluxo. O destinatário e o emissor dos pacotes podem ter limites diferentes quanto a quantidade de dados que podem receber ou enviar. Um mecanismo de controle de fluxo evita que o destino receba mais dados do que tem condições de receber e processar. Basicamente, o controle de fluxo permite que a máquina de origem ajuste o seu volume de pacotes enviados de acordo com a capacidade do destino em receber pacotes naquele momento, seja aumentando ou diminuindo a vazão do fluxo de pacotes, conforme a reação observada do destino.

3.2.5 Camada de sessão

A camada de sessão possui mecanismos que permitem estruturar os circuitos oferecidos pela camada de transporte. As principais funções da camada de sessão são: gerenciamento de *token*, controle de diálogo e gerenciamento de atividades.

O gerenciamento de *token* é necessário em algumas aplicações, quando a troca de informações é *half-duplex*, ao invés de *full-duplex*. O gerenciamento de *token* permite que apenas o proprietário do *token* possa transmitir dados naquele momento.

O controle de diálogo usa o conceito de ponto de sincronização. Quando a conexão para a transferência de dados de uma aplicação é interrompida, por erro, a transferência pode ser reestabelecida do ponto onde havia parado.

O conceito de atividade permite que as aplicações ou serviços oferecidos aos usuários coordenem as partes constituintes da transferência de dados. Cada atividade possui um conjunto de dados que devem ser trocados entre o serviço na origem e na aplicação de destino. Apenas uma atividade é executada (dados transmitidos) por vez, porém, uma atividade por ser suspensa, é reordenada e retomada.

3.2.6 Camada de apresentação

A camada de apresentação cuida da formatação dos dados, transformação, compressão e criptografia. Não há multiplexação de dados na camada de apresentação. O propósito desta camada é converter as informações que são recebidas da camada de aplicação para um formato “entendível” na transmissão desses dados.

Como exemplo de conversão, estão os caracteres diferentes do padrão usual ASCII que precisam ser “tratados” ou quando os dados recebidos são criptografados sobre diferentes formas de criptografia, desta forma também sendo necessário uma conversão destes dados (SILVA, 2010).

3.2.7 Camada de aplicação

Na camada de aplicação estão os aplicativos, propriamente ditos, dos usuários ou os serviços dos sistemas. Esta camada cuida da comunicação entre as aplicações, sendo que cada aplicação possui protocolos específicos de comunicação.

As aplicações que oferecem recursos aos usuários ou aos sistemas mais conhecidos atualmente são aquelas que oferecem serviços no padrão da internet: aplicação para navegação; transferência de arquivos; transferência de *e-mail*, terminal remoto e outros. A camada de aplicação diz respeito, também, aos protocolos usados na comunicação de dados entre essas aplicações.

No Quadro 3.1, é feito um resumo comparativo entre as principais funções das camadas no modelo OSI. As funções aqui tratadas quanto ao modelo OSI, são consideradas de modo conceitual e separadas uma das outras.

Quadro 3.1: Principais funções das camadas do modelo OSI

Camada	Principais funções
Aplicação	Funções específicas para as aplicações dos usuários: transferência de páginas <i>web</i> ; transferência de arquivos pela rede; envio ou recebimento de correio eletrônico; terminal remoto; etc. Funções especializadas para o sistema: transferência de informações sobre caminhos entre roteadores; serviço de gerenciamento de equipamentos de rede; serviço de tradução de nomes; etc.
Apresentação	Conversão e formatação dos dados.
Sessão	Negociação e conexão entre as máquinas envolvidas.
Transporte	Transporte de dados fim a fim. Fornece um caminho virtual transparente entre um processo em uma máquina da rede com outro processo em alguma outra máquina.
Rede	Encaminhamento (roteamento) de pacotes pelas várias redes.
Enlace	Deteção e correção de erros do meio de transmissão.
Física	Transmissão e recepção dos <i>bits</i> brutos através do meio de transmissão.

Fonte: Tanenbaum, 2003

Na exemplificação (Figura 3.3), como forma de entendimento dos conceitos das camadas de rede pertencentes ao modelo OSI, é caracterizada a trajetória de um pacote de rede, realizada na troca de dados entre dois dispositivos. Isto ajuda a explicar o caminho percorrido por um pacote, passando pelas camadas estudadas anteriormente. Acompanhe!

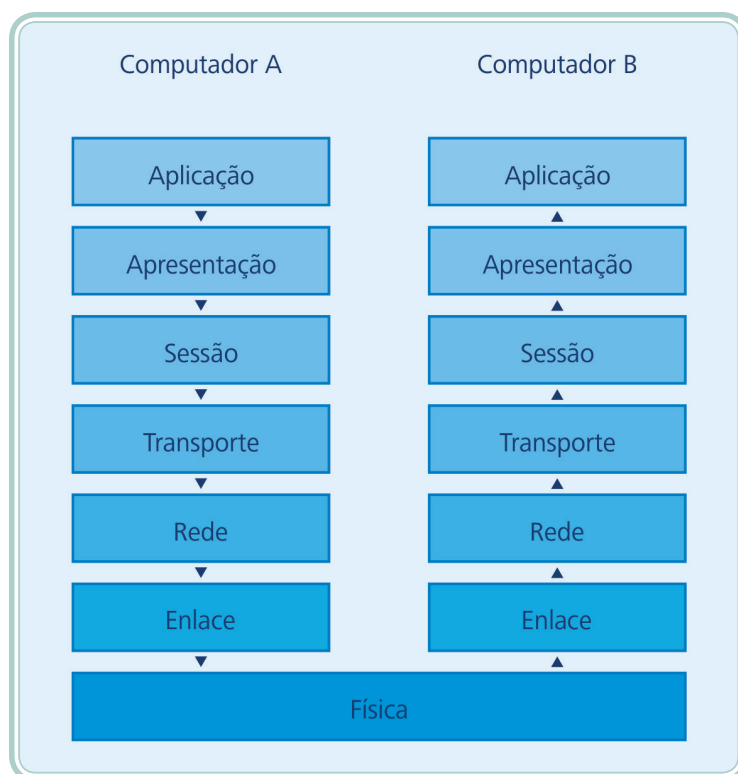


Figura 3.3: Caminho dos dados de um computador para o outro em uma representação do modelo de referência OSI

Fonte: CTISM, adaptado de Tanenbaum, 2003

Na Figura 3.3, traçamos o caminho seguindo pelo tráfego de informações de um computador hipotético “A” até um computador “B”. A informação a ser comunicada encontra-se na aplicação do computador “A” que deve enviá-la à aplicação no computador “B”. Nesse ponto, repare que as únicas funções de interesse da camada de aplicação é a “conversa” (comunicação) entre as aplicações nos computadores distintos, como o que enviar e o que responder. A aplicação em “A” “conversa” apenas com a outra aplicação em “B”. Para a transferência de fato dos dados, a camada de aplicação usará os serviços da camada imediatamente inferior, a camada de apresentação. A camada de apresentação, por sua vez, fará o uso da camada de sessão e assim sucessivamente até a camada física. A transferência de dados (neste caso, codificados em *bits* brutos) ocorre de fato e unicamente na camada física. Ao longo da descida até a camada física, cada camada encapsulou os pacotes de dados e adicionou os seus cabeçalhos de controle e endereçamento, relativo a cada camada.

Quando os pacotes chegam à outra ponta do meio de transmissão da camada física e assim alcançam o computador “B”, o processo inverso acontece. Cada pacote é processado conforme as informações de endereçamento e controle e tem os cabeçalhos da camada removidos e colocados na camada superior. O processo acontece até que o pacote atinge o processo de destino devido (aplicação), na camada de aplicação de “B”.

Historicamente, o modelo OSI não se tornou padrão para a internet, embora muitos protocolos e tecnologias de rede tenham sido desenvolvidos baseados nele. Embora o RM-OSI não tenha se tornado o padrão dominante para a ligação de redes e muitos dos protocolos baseados nele tenham sido suplantados pelo TCP/IP, o estudo do modelo justifica-se pela generalidade dos conceitos adotados na sua construção (TANENBAUM, 2003).

3.3 A arquitetura TCP/IP

O modelo de referência TCP/IP é mais simplificado que o modelo de referência OSI, possuindo quatro camadas principais: **aplicação, transporte, internet e interface de rede**.

A semelhança entre o modelo de referência OSI e o modelo TCP/IP está no fato dos dois estarem baseados no conceito de pilha (contendo protocolos independentes). Como características o modelo TCP/IP possui:

- **Quatro camadas** – sendo as camadas de rede, transporte e aplicação, comum tanto ao modelo de referência OSI, como ao modelo TCP/IP.
- **Adaptativo** – sua criação baseou-se na adaptação para protocolos existentes, enquanto que o modelo de referência OSI (criado antes dos protocolos) apresenta-se como mais genérico e flexível.

Na Figura 3.4, é possível visualizar a diferença de camadas entre o modelo OSI tradicional e o modelo TCP/IP, que na verdade abstrai algumas camadas existentes no modelo OSI. Ao lado das camadas é possível observar também os principais protocolos que trabalham em camadas específicas. Esta associação modelo/camadas/protocolos, ajuda no entendimento de como funciona uma rede de computadores no todo.

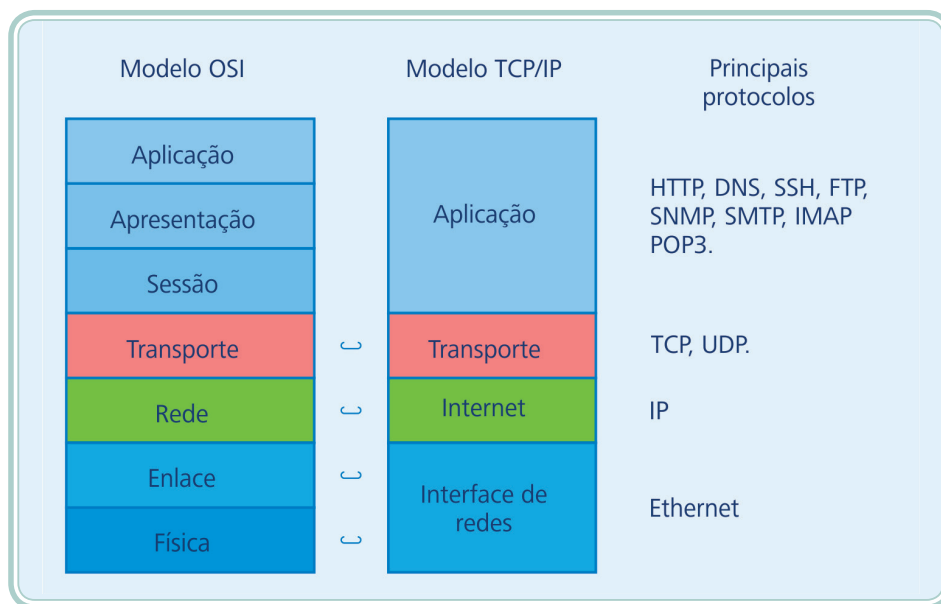


Figura 3.4: Comparativo entre as camadas do modelo OSI com a arquitetura TCP/IP
 Fonte: CTISM, adaptado de Scrimger, 2001

3.3.1 Camada de interface de rede

Esta camada tem como objetivo principal conectar um dispositivo de rede (computador, *notebook*, etc.) a uma rede, utilizando para isso um protocolo. Nesta camada, a exemplo de como ocorre na camada física do modelo OSI, é tratada a informação em mais baixo nível (*bits* que trafegam pela rede) entre as diferentes tecnologias para este fim: cabo de par trançado, fibra óptica, etc. (SCRIMGER, 2001).

3.3.2 Camada de internet

Esta camada tem o objetivo de permitir aos dispositivos de rede enviar pacotes e garantir que estes pacotes cheguem até seu destino. Cabe a camada de

internet especificar o formato do pacote, bem como, o protocolo utilizado, neste caso o protocolo IP (*Internet Protocol*).

Semelhante a camada de rede do modelo de referência OSI, cabe a camada de internet realizar a entrega dos pacotes IP no destino e realizar o roteamento dos pacotes.

3.3.3 Camada de transporte

A camada de transporte do modelo TCP/IP possui a mesma função da camada de transporte do modelo de referência OSI, ou seja, garantir a comunicação entre os dispositivos de origem e destino do pacote. Fazem parte desta camada dois protocolos bastante populares nas redes de computadores: o protocolo TCP (*Transmission Control Protocol*) e o UDP (*User Datagram Protocol*).

- **Protocolo TCP** – considerado um protocolo confiável (devido a quantidade de verificações, confirmações e demais procedimentos realizados), o protocolo TCP garante a entrega dos pacotes aos computadores presentes na rede. O fluxo dos pacotes de rede passa desta camada (depois de fragmentados) para a camada de internet (para onde são encaminhados). No computador destino é feita a verificação e montagem de cada um dos pacotes, para então ser efetivado o recebimento dos mesmos.
- **Protocolo UDP** – protocolo sem confirmação (UDP) é comumente utilizado na transferência de dados, porém, não realiza nenhuma operação de confirmação e verificação de pacotes na estação destino (procedimento realizado pela própria aplicação). Apesar de ser classificado como um protocolo não-confiável, o UDP é mais rápido que o TCP (justamente por ter um mecanismo de funcionamento mais simplificado), sendo utilizado em requisições que não necessitam de confirmação, como é o caso de consultas DNS.

3.3.4 Camada de aplicação

Esta camada tem por objetivo realizar a comunicação entre os aplicativos e os protocolos de transporte, responsáveis por dar encaminhamento a estes pacotes.

Os protocolos da camada de transporte são usualmente conhecidos e desempenham diferentes funções, conforme exemplos a seguir:

- **Protocolo SMTP** – responsável pela comunicação junto ao servidor de *e-mails*, para entrega destes, ao programa cliente que recebe as mensagens.

- **Protocolo HTTP** – acionado cada vez que um usuário abre um *browser* (navegador) e digita um endereço de um *site* da internet.
- **Protocolo FTP** – utilizado cada vez que um usuário acessa um endereço de FTP, para fazer *download* ou *upload* de arquivos (KUROSE, 2010).

Além dos exemplos de protocolos de aplicação citados acima, existem diversos outros que realizam procedimentos importantes para nossas principais atividades do dia-a-dia, como é o caso dos protocolos de aplicação: DNS, SSH, POP3, entre outros que serão descritos com maior riqueza de detalhes na próxima aula.

Resumo

Nesta aula, podemos conhecer em detalhes como uma rede funciona através de sua parte lógica, ou seja, as camadas de rede. Para isso, foi apresentado o modelo de referência OSI e a arquitetura de rede TCP/IP. Foram apresentadas as camadas de cada modelo, suas características e função que possuem na comunicação de dados em uma rede.

Atividades de aprendizagem

1. Quais são as sete camadas do modelo OSI?
2. Das camadas citadas na resposta da questão 1, qual a principal função de cada uma?
3. Quais as diferenças entre os modos de comunicação: *simplex*, *half-duplex* e *full-duplex*?
4. Quais são as camadas do modelo TCP/IP?
5. Qual camada você achou mais importante no modelo OSI e no modelo TCP/IP? Por quê?



Aula 4 – Protocolos de redes de computadores

Objetivos

Entender o funcionamento dos principais protocolos utilizados nas redes de computadores.

Compreender quais protocolos são utilizados em cada camada.

Conhecer o funcionamento dos protocolos mais usuais no dia-a-dia dos usuários.

Ter o entendimento do endereçamento IP em suas versões 4 e 6.

4.1 Considerações iniciais

Protocolos em sua essência são regras e procedimentos de comunicação. Na comunicação em redes de computadores os protocolos definem as regras que os sistemas precisam seguir para comunicar-se entre si. Já, os pacotes são conjuntos de *bits* ou sinais que são agrupados de forma que possam trafegar pelo meio de transmissão (MORAES, et al., 2003).

Os protocolos não dependem da implementação, o que significa que sistemas e equipamentos de fabricantes diferentes podem comunicar-se, desde que sigam as regras do protocolo. Dessa forma, os protocolos da arquitetura TCP/IP estão organizados em uma pilha de protocolos, a exemplo da organização em camadas da arquitetura. No Quadro 4.1 são apresentados os principais protocolos de rede e as camadas de operação onde os mesmos atuam.

Quadro 4.1: Principais protocolos de rede e camadas de operação

Camada	Principais protocolos
Aplicação	HTTP, DNS, SSH
Transporte	TCP, UDP
Internet	IP
Interface de rede	Ethernet

Fonte: Moraes, et al., 2003

4.2 Protocolos da camada de aplicação

Nessa seção serão abordados os principais protocolos da camada de aplicação, bem como, suas características e aplicabilidade. Os protocolos pertencentes a esta camada são responsáveis pela funcionalidade das aplicações utilizadas pelo usuário.

4.2.1 HTTP

O protocolo de transferência de hipertexto (HTTP – *HiperText Transfer Protocol*) é o principal protocolo da *World Wide Web* (WWW) ou simplesmente *web*. O HTTP é usado na *web* para a comunicação e transferência de documentos HTML (*HiperText Markup Language*) entre um servidor *web* e um cliente. O HTTP é um protocolo da camada de aplicação e usa o protocolo TCP para o transporte dos documentos e das mensagens (pedidos e respostas).

Baseado no modelo de arquitetura cliente/servidor e no paradigma de requisição e resposta, o HTTP é responsável pelo tratamento de pedidos e respostas entre um cliente e um servidor. Além disso, utiliza como padrão a porta 80.

O protocolo HTTP é a base da funcionalidade da internet. Construído sob o modelo de referência TCP/IP é caracterizado como um protocolo veloz, leve e orientado à conexão.



As portas utilizadas na comunicação de dados, como por exemplo, a porta 80 para internet (http), a porta 443 para (https), são endereçadas na camada de transporte do modelo de referência OSI.

4.2.2 SMTP

Protocolo responsável pelo envio de *e-mails*, o SMTP (*Simple Mail Transfer Protocol*) realiza a comunicação entre o servidor de *e-mails* e o computador requisitante. Este protocolo utiliza por padrão a porta 25.

O protocolo SMTP tem a função de somente enviar *e-mails* (a um destinatário ou mais) fazendo a transmissão do mesmo. Para recebimento das mensagens de um servidor utiliza-se outro protocolo, o POP3 que tem a função de receber mensagens do servidor para o programa cliente de *e-mail* do usuário (Outlook, entre outros).

Para que seja efetivado o envio de *e-mails* através deste protocolo, uma conexão é estabelecida entre o computador cliente e o servidor responsável pelo envio de *e-mails* (servidor SMTP, devidamente configurado).

4.2.3 POP3

Responsável pelo recebimento de *e-mails*, o protocolo POP3 (*Post Office Protocol*) controla a conexão entre um servidor de *e-mail* e o cliente de *e-mail*. De modo geral, sua função é permitir “baixar” todos os *e-mails* que se encontram no servidor para sua caixa de entrada.

O protocolo POP3 realiza três procedimentos básicos durante sua operação de recebimento de *e-mails* que são: **autenticação** (realizada geralmente pelo nome de usuário e uma senha), **transação** (estabelecimento de conexão cliente/servidor) e **atualização** (finalização da conexão cliente/servidor).

Existem duas formas básicas de enviar e receber *e-mails*. A primeira delas é utilizar um cliente de *e-mail* como o Outlook Express, Apple Mail, Kmail, entre outros. Para isso é necessário configurar manualmente os servidores de envio (SMTP) e recebimento de mensagens (POP3). As vantagens deste tipo de serviço são: leitura e escrita de *e-mails* em modo *off-line*, armazenamento de *e-mails* no próprio computador do usuário, entre outros. Em contrapartida existem os chamados *webmails* que utilizam a própria estrutura da internet para acessar os *e-mails* através de um endereço da *web* específico, como: <http://webmail.exemplo.com.br>. As vantagens deste tipo de serviço são a centralização dos recursos de *e-mail* (contatos, *e-mails* enviados, recebidos) bem como a utilização de múltiplas contas e personalizações mais simplificadas que podem ser aplicadas (SILVA, 2010).



4.2.4 FTP

O protocolo FTP (*File Transfer Protocol*) é utilizado na transferência de arquivos cliente/servidor, tanto para *download* quanto *upload* de arquivos. Para tal procedimento este protocolo utiliza as portas 20 e 21. A porta 20 é utilizada para transmissão de dados, enquanto que a porta 21 é utilizada para controle das informações.

Os serviços de FTP subdividem-se em: servidores e clientes de FTP.

Os servidores de FTP permitem criar uma estrutura (serviço) onde é possível acessar via navegador, por exemplo, um endereço específico ao serviço (Ex.: <ftp.exemplo.com.br>) e fazer *upload* e/ou *download* de arquivos de forma *on-line*. Este tipo de servidor de FTP pode ser privado (na qual exige uma autenticação do usuário, mediante nome de usuário e senha) ou público, onde o acesso não necessita autenticação para acesso aos serviços.

Já os clientes de FTP, são programas instalados no computador do usuário, utilizados para acessar os servidores de FTP de forma personalizada. São exemplos destes programas aplicativos: Filezilla, Cute FTP, WS FTP, entre outros.



Vale ressaltar que todos os *browsers* (navegadores) possuem suporte para acesso FTP, dessa forma, a utilização de programas externos de FTP não é obrigatória e sim uma opção caso o usuário achar mais conveniente.

4.2.5 DNS

O Sistema de Nomes de Domínio (DNS – *Domain Name System*) é um esquema hierárquico e distribuído de gerenciamento de nomes. O DNS é usado na internet para manter, organizar e traduzir nomes e endereços de computadores. Na internet toda a comunicação entre dois computadores de usuários ou servidores é feita conhecendo-se o endereço IP da máquina de origem e o endereço IP da máquina de destino. Porém, os usuários preferem usar nomes ao se referir a máquinas e recursos.

Os computadores dispostos em uma rede de computadores são identificados por seu número IP (endereço lógico) e seu endereço MAC (identificação física, designada na fabricação do dispositivo de rede). Os endereços IP na versão 4 (IPv4), compostos de 32 *bits*, geralmente são difíceis de serem memorizados, conforme aumenta a quantidade de computadores na rede, servidores, entre outros. Como forma de facilitar a memorização de computadores, *sites*, servidores e demais dispositivos que trabalham com a numeração IP, foi criado o sistema DNS, que torna possível relacionar nomes aos endereços IP, realizando a troca (endereço por nome). Dessa forma, torna-se mais simples lembrar um determinado endereço (www.exemplo.com.br) do que um número IP relacionado ao domínio (como por exemplo: 200.143.56.76).

O funcionamento do DNS baseia-se em um mapeamento de IPs em nomes. Estes ficam armazenados em tabelas dispostas em banco de dados nos servidores DNS. Nestes servidores são realizadas as trocas de endereços IP em nomes e vice-versa.

A estrutura de nomes na internet tem o formato de uma árvore invertida onde a raiz não possui nome. Os ramos imediatamente inferiores à raiz são chamados de TLDs (*Top-Level Domain Names*) e são por exemplo “.com”, “.edu”, “.org”, “.gov”, “.net”, “.mil”, “.br”, “.fr”, “.us”, “.uk”, etc. Os TLDs que não designam países são utilizados nos EUA. Os diversos países utilizam a sua própria designação para as classificações internas. No Brasil, por exemplo, temos os nomes “.com.br”, “.gov.br”, “.net.br”, “.org.br” entre outros.

Cada ramo completo até a raiz como, por exemplo, “puc-rio.br”, “acme.com.br”, “nasa.gov”, e outros, são chamados de domínios. Um domínio é uma área administrativa englobando ele próprio e os subdomínios abaixo dele. Por exemplo, o domínio “.br” engloba todos os subdomínios do Brasil.

- **Hierarquia de nomes**

Uma hierarquia de nomes é utilizada para caracterizar o uso de cada extensão do domínio. No Quadro 4.2, são caracterizados alguns dos principais domínios utilizados e seu respectivo significado.

Quadro 4.2: Tipos de domínios

Nome do domínio	Significado
com	Organizações comerciais
edu	Instituições educacionais
gov	Instituições governamentais
mil	Agências militares
net	Organizações da rede
org	Organizações não comerciais
int	Organizações internacionais
Código de países	Identificador de 2 letras para domínios de países específicos

Fonte: Tanenbaum, 2003

O registro.br (www.registro.br) é a entidade nacional que trata do registro de domínios para a internet no Brasil, ou seja, que estão sob a faixa “.br”. Dessa forma, ao registrar um novo domínio na internet com a extensão final “.br” é necessário consultar se o domínio em questão não está registrado e se o mesmo é possível de ser registrado (www.registro.br). Para registrar um novo domínio, além de cadastrar-se no portal é necessário informar onde este domínio ficará hospedado (servidor de hospedagem), bem como pagar uma taxa anual para exercer a utilização deste domínio.



4.2.6 DHCP

O protocolo DHCP (*Dynamic Host Configuration Protocol*), possui a função de distribuir e gerenciar endereços IP em uma rede de computadores. Mais do que isso, este protocolo em conjunto com um servidor DHCP é capaz de distribuir endereços, *gateway*, máscaras, entre outros recursos necessários a operação e configuração de uma rede de computadores.

Para que o DHCP possa operar de forma plena é necessário:

- Que o computador cliente (que necessita de um número IP) possua o pacote DHCP cliente instalado.
- A partir deste momento o computador cliente envia uma requisição (pacote) na rede solicitando um número IP (requisição DHCP).
- Cabe a um servidor DHCP disponível na rede responder a requisição do computador solicitante, com um pacote contendo o endereço IP, *gateway* padrão, máscara de rede, servidores de DNS, entre outros.

Um servidor DHCP, utiliza o modelo cliente/servidor, mantendo o gerenciamento centralizado dos IPs utilizados pelos dispositivos conectados a rede.

4.2.7 SNMP

O protocolo SNMP (*Simple Network Management Protocol*), ou Protocolo Simples de Gerência de Rede tem a função de monitorar as informações relativas a um determinado dispositivo que compõe uma rede de computadores.

É através do protocolo SNMP que podemos obter informações gerais sobre a rede como: placas, comutadores, *status* do equipamento, desempenho da rede, entre outros. A obtenção destas informações é possível graças a um *software* denominado agente SNMP presente nos dispositivos de rede, que extrai as informações do próprio equipamento, enviando os mesmos para o servidor de gerenciamento. Este por sua vez recebe as informações, armazena e analisa.

4.2.8 SSH

O protocolo SSH (*Secure Shell*), tem uma função importante na pilha de protocolos da camada de aplicação que é permitir a conexão segura (criptografada) a outro computador (da mesma rede ou de outra rede distinta) e poder controlá-lo (dependendo do nível de acesso e privilégios) remotamente. Esta função de acessar um computador distante geograficamente e poder utilizá-lo/manipulá-lo como se o usuário estivesse presente fisicamente em frente do computador e ainda de forma criptografada, faz com que o protocolo SSH seja utilizado amplamente nas redes de computadores.

Existem diversos programas aplicativos que permitem gerenciar computadores *desktop* e servidores a distância e através de um outro computador ou a partir de seu próprio *smartphone*. A seguir, alguns exemplos destes programas aplicativos de administração remota de computadores.

- OpenSSH (utilizado para a plataforma Linux, tanto para máquinas clientes (que geram a conexão) como máquinas servidoras (que recebem as conexões através da linha de comandos).
- Putty (*software* amplamente conhecido na administração remota de computadores possui versões do aplicativo tanto para Linux quanto para sistemas operacionais Windows).
- WebSSH (aplicativo *on-line* que permite a conexão a um computador remoto sem a necessidade de instalação de aplicativos clientes).

O protocolo SSH opera por padrão na porta 22, sendo possível e indicado a sua modificação (alteração nas configurações do servidor) para operação em uma porta diferente (por questões de segurança).



4.3 Protocolos da camada de transporte

Na arquitetura TCP/IP, a camada de transporte encontra-se logo abaixo da camada de aplicação e diretamente provê um serviço para esta camada. A camada de Transporte oferece um serviço de circuito virtual fim-a-fim entre uma entidade (processo ou aplicação) na máquina de origem e outra entidade na máquina de destino.

Um conceito importante introduzido na camada de transporte da arquitetura TCP/IP é o de portas. As portas provêm um mecanismo interessante para identificação e endereçamento correto dos pacotes aos processos correspondentes nas máquinas de origem e de destino. Cada aplicação, normalmente, está associada a uma porta conhecida pelas máquinas de origem e destino.

Os dois principais protocolos da camada de transporte, o TCP (*Transmission Control Protocol*) e o UDP (*User Datagram Protocol*) oferecem as aplicações em diferentes níveis de serviço e confiabilidade. Normalmente cada aplicação usa um dos dois protocolos, conforme a necessidade de confiabilidade e desempenho, para transporte das mensagens geradas na aplicação do cliente e do servidor. Nessa seção analisaremos mais detalhadamente esses dois principais protocolos.

4.3.1 O TCP (*Transmission Control Protocol*)

O TCP (*Transmission Control Protocol* – Protocolo de Controle de Transmissão) é o protocolo mais importante da camada de transporte e juntamente com o IP (*Internet Protocol*), da camada de rede, forma a dupla de protocolos mais

importantes na arquitetura do TCP/IP. O TCP permite a criação de um canal virtual confiável, livre de erros, fim-a-fim, entre uma aplicação ou serviço na máquina origem e uma aplicação na máquina de destino.

O TCP é um protocolo robusto e confiável, por isso um grande número de aplicações dos usuários faz uso deste para transferência de dados. Algumas características importantes do TCP são:

- **Orientado a conexão** – significa que antes que qualquer transmissão de mensagens ou dados da aplicação seja feita, a camada de transporte, por meio do TCP, deve estabelecer uma conexão. Basicamente, uma conexão é estabelecida após o envio de um pedido de conexão de uma das máquinas envolvidas e a confirmação de ambas. Somente após o estabelecimento da conexão é que as mensagens da aplicação começam a ser enviadas. Todos os pacotes de dados trafegados após o estabelecimento da conexão são associados com uma conexão específica.
- **Ponto-a-ponto** – uma conexão é estabelecida entre duas entidades, mais especificamente, ligando um processo na máquina de origem e um processo na máquina de destino.
- **Confiabilidade** – o TCP usa um mecanismo para tratar erros durante a transmissão, como pacotes perdidos ou pacotes com dados corrompidos. Todos os pacotes transmitidos devem ser confirmados pelo receptor. Simplificadamente, a falta de uma confirmação do receptor, significa que o pacote foi perdido no caminho e deve ser automaticamente retransmitido. O TCP usa uma soma de verificação (*checksum*) em campo de cabeçalho (Figura 4.1), que é verificado pelo receptor. Se a soma de verificação não estiver correta, significa que os dados foram corrompidos no caminho, o pacote é descartado e a origem deve retransmitir o pacote.
- **Full-duplex** – transferência simultânea em ambas as direções, envio e recebimento ao mesmo tempo.
- **Entrega ordenada** – o TCP possui um campo de cabeçalho para identificação da sequência (Figura 4.1) do pacote dentro da conexão. Mesmo que os pacotes cheguem fora de ordem no destino, a mensagem da aplicação é reconstruída na ordem correta.
- **Controle de fluxo** – o TCP usa um campo Janela (Figura 4.1) para determinar a quantidade de dados que o receptor pode receber e processar.

Quando o emissor recebe uma confirmação de um pacote enviado, juntamente ele toma conhecimento do tamanho da janela de dados que o receptor pode trabalhar. Esse mecanismo de controle de fluxo evita que o emissor envie pacotes excessivamente, congestionando o receptor.

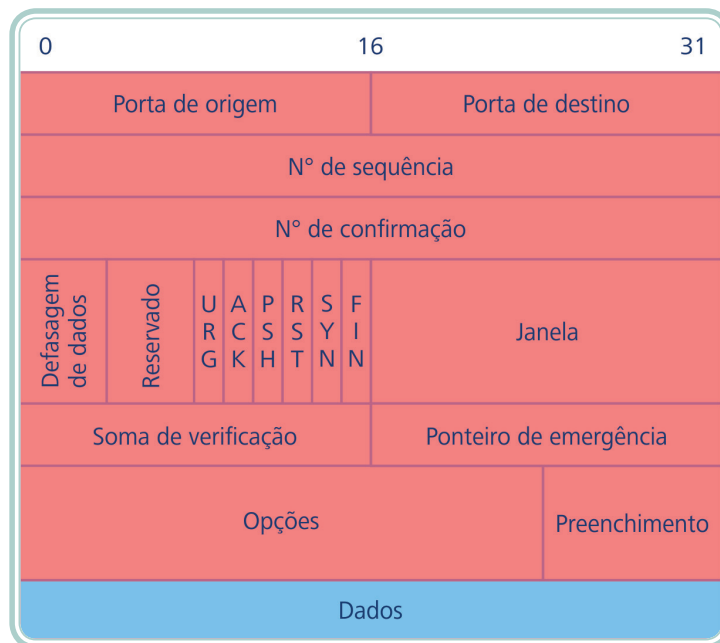


Figura 4.1: Representação dos campos de cabeçalho de um pacote TCP

Fonte: CTISM, adaptado de Tanenbaum, 2003

A Figura 4.1 traz uma representação dos campos de cabeçalhos de um pacote do TCP. Cada campo do cabeçalho tem uma função no funcionamento do TCP.

Para a criação de uma conexão TCP, normalmente são necessários um serviço (processo) rodando em uma máquina servidora, “escutando” em uma porta conhecida e uma aplicação (outro processo) em uma máquina cliente. Um serviço “escutando” em uma porta significa que o processo fica esperando um pedido de conexão nesta porta.

Na outra ponta deverá haver uma aplicação no cliente desejando iniciar uma conexão usando uma porta de origem qualquer. As conexões estabelecidas no cliente ou no servidor são associadas a *sockets*, identificados por: endereço IP de origem (no cabeçalho do protocolo IP), porta TCP de origem (cabeçalho do protocolo TCP, Figura 4.1), endereço IP de destino e porta TCP de destino. *Sockets* permitem a ligação entre a camada de transporte, neste caso pelo protocolo TCP e um processo da camada de aplicação, para o envio e o recebimento de mensagens da aplicação.

Tipicamente, uma conexão TCP envolve três fases: estabelecimento da conexão, transferência de dados e finalização da conexão.

O estabelecimento de uma conexão TCP inicia-se com um cliente desejando estabelecer uma conexão em um servidor já esperando por um pedido de conexão. Uma conexão TCP bem sucedida envolve a troca de uma sequência de pacotes especiais, com *flags* especiais de cabeçalho setadas (*bit* igual a 01) (Figura 4.1):

- O **cliente** requisita uma conexão enviando um pacote TCP especial, com a *flag* **SYN** (*synchronize*) do cabeçalho setada ao servidor. Esse pacote é conhecido simplificadaamente como pacote do tipo **SYN**.
- O **servidor** confirma esta requisição respondendo com um pacote do tipo **SYN-ACK** ao cliente, ou seja, um pacote TCP com as *flags* de cabeçalho **SYN** e **ACK** setadas.
- O **cliente** por sua vez responde com um pacote do tipo **ACK**, *flag* **ACK** setada, e a conexão é estabelecida. Essa sequência é conhecida como **aperto de mão em três etapas** (*Three-Way Handshake*).

Somente após esse processo inicial (*Three-Way Handshake*) a conexão está disponível para a transferência das mensagens das aplicações.

Durante a fase de transferência de dados, cada pacote enviado é identificado com um número de sequência em um campo de cabeçalho e um número de confirmação (**ACK** *nowledgement*). O número de confirmação serve para o receptor informar ao emissor os pacotes que já recebeu. O emissor providenciará a retransmissão do pacote se não receber uma confirmação dentro de um intervalo de tempo estabelecido (*timeout*).

A finalização de uma conexão TCP, por sua vez, ocorre com uma das partes envolvidas enviando um pacote do tipo **FIN**, ou seja, com a *flag* de cabeçalho **FIN** setada, e normalmente com confirmação (**ACK**) do outro lado da conexão, em ambas as direções da conexão.

Continuando a discussão da Figura 4.1, quanto ao cabeçalho TCP, os campos “Porta de origem” e “Porta de Destino” possuem tamanho de 16 *bits*, o que significa que existem 65.536 (0 a 65.535) portas. Os campos “Número de sequência” e “Número de confirmação” são usados para indicar a ordem do

pacote que está sendo enviado e o último pacote recebido, respectivamente. Estes campos possuem tamanho de 32 *bits* cada. O campo “*flags*” (seis *bits*) possui um *bit* para cada *flag*, que é setado (1) ou permanece nulo (0) conforme a função usada durante o funcionamento da conexão no TCP. A “Soma de verificação” (ou *checksum*) é o resultado de uma soma especial nos dados dos cabeçalhos e é usada para verificar a integridade do cabeçalho (SCRIMGER, 2001).

4.3.2 O protocolo UDP

O protocolo UDP (*User Datagram Protocol*) é um protocolo simples da camada de transporte. Diferentemente do TCP, o UDP é um protocolo não confiável, sem controle de sequência em que não há garantia de entrega dos pacotes.

Ainda comparando-se ao TCP, o UDP possui um cabeçalho simplificado como pode ser visto na Figura 4.2. O campo “Soma de verificação” tem função semelhante à função no TCP, porém é opcional. A Figura 4.2, possui um resumo dos campos de um datagrama UDP.

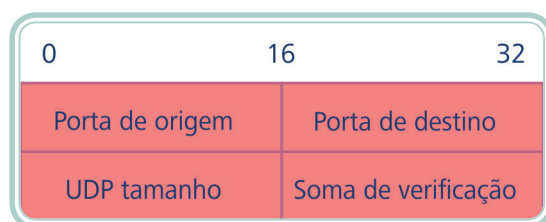


Figura 4.2: UDP

Fonte: CTISM, adaptado de Tanenbaum, 2003, p. 559

Com tantas limitações do UDP é normal nos perguntarmos: Qual a utilidade do UDP, sendo que o TCP faz tudo o que o UDP faz e ainda com confiabilidade?

Apesar da falta de confiabilidade do UDP, ele possui um desempenho melhor que o TCP, pois não há gasto extra (*overhead*) de processamento e de *bits* extras trafegados na rede. Por sua simplicidade o UDP é mais eficiente e rápido. Aplicações em que a confiabilidade na entrega não é tão importante, porém o desempenho é essencial, geralmente, fazem uso do UDP.

Exemplos de aplicação que usa o UDP como protocolo de transporte é o *streaming* de áudio e de vídeo. Nessas aplicações a falta de alguns dados durante a transmissão prejudica apenas a qualidade da imagem ou do áudio quando recebido, sem afetar completamente a transmissão. Na transmissão de áudio ou vídeo em tempo real, a agilidade na entrega dos dados é geralmente o fator mais importante. Outras aplicações podem fazer uso do UDP, por

razões de desempenho e tratar dos possíveis erros de transmissão diretamente dentro da aplicação. No Quadro 4.3 é possível observar algumas das principais características (comparativo) de cada um dos protocolos.

Quadro 4.3: Diferenças entre os protocolos TCP e UDP	
TCP	UDP
Orientado a conexão	Não orientado a conexão
Ponto a ponto	Ponto a ponto
Confiável, controle de erros	Não confiável, sem controle de erros
<i>Full duplex</i>	<i>Full duplex</i>
Entrega ordenada	Não garante entrega ordenada
Controle de fluxo	Sem mecanismo de controle de fluxo

Fonte: Tanenbaum, 2003

O TCP e o UDP usam o protocolo IP, da camada de rede (internet) para a entrega dos pacotes. Os pacotes TCP ou os datagramas do UDP são encapsulados em datagramas IP e encaminhados (roteados) da origem até o destino. Após o encapsulamento, os roteadores usam basicamente os campos do IP.



Vale ressaltar que o protocolo UDP possibilita além da comunicação ponto-a-ponto, realizar a comunicação de um para muitos, o que significa que um computador origem através do protocolo UDP pode entregar pacotes para diversos computadores destino em uma rede. Este é um diferencial bastante relevante do protocolo UDP.

4.4 Protocolos da camada internet da arquitetura TCP/IP

Estudaremos nesta seção os principais protocolos da camada internet (camada de rede no modelo de referência OSI), os protocolos relacionados ou auxiliares e os mecanismos de roteamento.

4.4.1 O Protocolo da Internet – IP

O IP (*Internet Protocol* – Protocolo da Internet) é o protocolo essencial da arquitetura TCP/IP e o principal protocolo da camada de rede. A função principal do IP é a transferência de dados, na forma de datagramas, entre os nós (computador, roteador) da rede.

O serviço oferecido pelo IP não é confiável, também chamado de “melhor esforço”. O protocolo tentará entregar o datagrama no destino, mas não há garantia de que os datagramas cheguem ordenados (pois podem seguir caminhos diferentes na rede e ter a ordem de entrega alterada), duplicados,

não há garantia nem mesmo que o datagrama chegue ao destino. Embora o IP ofereça um serviço de datagrama não confiável, a confiabilidade na transferência dos dados é uma função que pode ser adicionada nas outras camadas da arquitetura, como é estudado nas demais seções. Os roteadores, nesta camada de rede são responsáveis pela escolha do caminho que os datagramas utilizam até chegarem ao seu destino (inter-redes ou internet).

A Figura 4.3, representa os campos do cabeçalho de um datagrama IP, na sua versão 4, a versão mais usada na atualidade. Cada campo do cabeçalho está ligado a uma função dentro do protocolo:

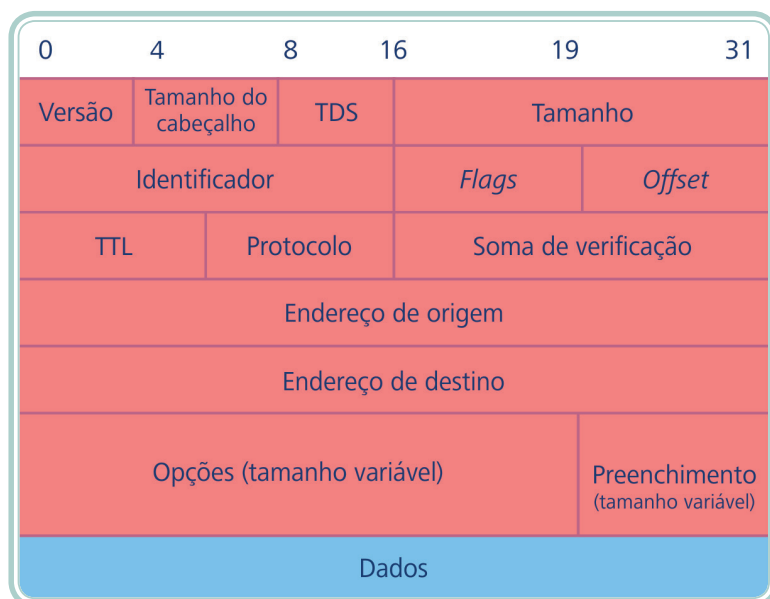


Figura 4.3: Formato de um pacote IPv4

Fonte: CTISM, adaptado de Davie e Bruce, 2004, p. 173

- **Versão** – com quatro *bits* identifica a versão do protocolo. Atualmente a versão 4 (IPv4) é a mais usada, mas a implantação da versão 6 (IPv6) está crescendo rapidamente.
- **Tamanho do cabeçalho** – essencialmente serve para especificar onde começa a porção de dados do datagrama.
- **TDS, tipo de serviço** – basicamente serve para definir diferentes tipos de prioridades aos datagramas de diferentes serviços da internet.
- **Tamanho** – comprimento total do datagrama, incluindo cabeçalho e dados. Quando o tamanho do datagrama é maior que o tamanho máximo de datagrama que a rede suporta, o datagrama é quebrado em fragmentos menores.

- **Identificador** – usado para identificar fragmentos de um mesmo datagrama original.
- **Flags** – usado para controlar e identificar fragmentos.
- **Offset** – permite ao receptor identificar o local de um fragmento no datagrama original.
- **TTL (Time To Live – tempo de vida)** – determina o número máximo de nós que um datagrama pode passar antes de ser descartado. O objetivo desse campo é evitar que um datagrama fique circulando pelas redes (internet) infinitamente. Cada vez que o datagrama passa (roteado) por um nó da rede, o valor do campo TTL é diminuído em uma unidade (decrementado). Quando o valor do TTL chega a zero o datagrama é descartado. Essa situação pode acontecer, por exemplo, quando há algum erro de roteamento e os datagramas são encaminhados indefinidamente (*loop*). Dessa forma o campo TTL evita problemas maiores nas redes.
- **Protocolo** – campo usado para identificar o protocolo usado junto com o IP, por exemplo, TCP (6) ou o ICMP (1).
- **Soma de verificação (checksum)** – usado para a verificação da integridade do cabeçalho IP. Esse valor é recalculado em cada nó (roteador).
- **Endereço IP de origem – endereço IP de destino** – usados para identificar as máquinas de origem e destino respectivamente.
- **Opções** – Campos de cabeçalhos adicionais, normalmente não são usados (DAVIE; BRUCE, 2004).

4.4.1.1 Endereçamento IP

O endereçamento IP permite identificar um dispositivo pertencente a uma rede de computadores. Para que isso seja possível cada um destes equipamentos conectados a uma rede (computadores, servidores, *notebooks*, *smartphones*, entre outros) deve possuir um número de identificação único (endereço IP) para que os roteadores possam fazer a entrega de pacotes de forma correta.

a) IPv4

Atualmente o endereçamento IPv4 ainda é o mais utilizado, sendo gradativamente substituído pelo endereçamento IPv6 (que será abordado na sequência).

Os endereços IPv4 são constituídos por 32 *bits*, divididos em quatro octetos, em outras palavras, quatro seções de 08 *bits*, separados por ponto que formam o endereço IP na versão 4 (IPv4). Destes quatro octetos uma parte representa a rede enquanto outra representa a quantidade de computadores que podem estar presentes em cada rede.

Um número IP pode variar do endereço 0.0.0.0 ao endereço 255.255.255.255, embora vejamos que existem algumas particularidades tanto na utilização, quando distribuição dos números IPs nas redes de computadores.

Como forma de organização e funcionamento inicial das redes de computadores, os endereços IPs foram divididos em classes (A, B, C, D e E), conforme a representação no Quadro 4.4.

Quadro 4.4: Classes de endereços IPv4		
Classe	Faixa	Nº endereços
A	1.0.0.0 – 126.255.255.255	16.777.216
B	128.0.0.0 – 191.255.0.0	65.536
C	192.0.0.0 – 223.255.255.0	256
D	224.0.0.0 – 239.255.255.255	<i>Multicast</i>
E	240.0.0.0 – 255.255.255.254	Testes (IETF) e uso futuro

Fonte: Silva, 2010

As classes **A**, **B** e **C** foram distribuídas e são utilizadas por redes de computadores de diferentes tamanhos. Conforme pode ser visualizado no Quadro 4.4, faixas da classe **A**, possuem uma maior quantidade de IPs disponíveis que podem ser utilizados por computadores em uma rede, enquanto nas classes **B** e **C** estes valores decrescem gradativamente (SILVA, 2010).

Os endereços da classe **D** são utilizados para *multicast* em redes de computadores.

Já, os endereços da classe **E**, são utilizados para testes e como reserva futura quando da escassez dos endereços das classes anteriores.

Além dos endereços IPs válidos, citados acima, existem os endereços IPs chamados de não-roteáveis que são reservados para redes privadas (LAN, por exemplo). Dessa forma, é possível montar redes de computadores que funcionam entre si, com a utilização de endereços não-roteáveis. No Quadro 4.5, são apresentados alguns dos endereços reservados a redes privadas.

A-Z

Multicast

Tecnologia que permite que um fluxo de dados seja enviado a múltiplos destinos simultaneamente. Pode ser utilizada tanto em aplicações um-para-muitos, como muitos-para-muitos.

Um exemplo de utilização da tecnologia multicast esta nas aplicações distribuídas, especialmente multimídias, como videoconferências ou ensino a distância, tornando-as mais eficientes e economizando recursos.

Quadro 4.5: Faixas de endereços IPv4 não roteáveis

Classe	Menor endereço	Maior endereço
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

Fonte: Silva, 2010

b) CIDR

Distribuir endereços IP através de classes (A, B, C, D e E) fazia com que inúmeros endereços IPv4 fossem desperdiçados. Como medida para uma melhor utilização dos endereços IPv4 e dada a escassez dos mesmos, foi implementada a notação CIDR (*Classless Inter-Domain Routing*).

Ao utilizar o CIDR ao invés das classes de IPs tradicionais temos a inserção de máscaras de tamanho variáveis, permitindo desta forma uma melhor utilização dos endereços e um menor desperdício de faixas IP.

Outra mudança que ocorre com a utilização do CIDR é a inexistência do conceito de faixas de endereços IP.

Exemplo: uma faixa de endereços IP, com máscara "/24" é equivalente a uma faixa de endereços de classe C, porém esta faixa pode começar com qualquer dígito e não somente de 192 a 223 que era o estipulado para esta faixa antes da utilização da notação CIDR.

É importante salientar que a máscara de rede determina qual parte do endereço IP é destinado a identificar a rede e qual delas endereçam os *hosts*. Em um endereço IP "200.153.132.3", com máscara "255.255.255.0" (/24), os primeiros 24 *bits* (200.153.132) referem-se a rede, enquanto os últimos 08 *bits* (3) referem-se ao *host*.

No Quadro 4.6, é possível visualizar exemplos da aplicação de CIDR e máscaras de tamanho variável, quanto aos endereços de rede e *host* que podem ser formados.

Máscara	Bits da rede	Bits do host	Número de redes	Número de hosts
255.255.255.0 (/24)	Nenhum	00000000	nenhuma	254 endereços (do 1 ao 254)
255.255.255.192 (/26)	11	000000	2 endereços (2 e 3)	62 endereços (de 1 a 62)
255.255.255.224 (/27)	111	00000	6 endereços (de 1 a 6)	30 endereços (de 1 a 30)
255.255.255.240 (/28)	1111	0000	14 endereços (de 1 a 14)	14 endereços (de 1 a 14)
255.255.255.248 (/29)	11111	000	30 endereços (de 1 a 30)	6 endereços (de 1 a 6)
255.255.255.252 (/30)	111111	00	62 endereços (de 1 a 62)	2 endereços (2 e 3)

Fonte: Morimoto, 2007

É importante lembrar que é possível utilizar a notação CIDR a qualquer momento na configuração de placas de rede, servidores e configurações de rede em geral. Ao escrever um *script* de *firewall*, por exemplo, o computador reconhece se escrevermos "192.168.0.0/255.255.255.0", quanto se utilizarmos a notação CIDR, escrevendo "192.168.0.0./24" (MORIMOTO, 2007).

c) IPv6

O IPv6, também conhecido como IP versão 6, é uma espécie de atualização do IPv4, oferecendo inúmeras vantagens para seus utilizadores, como por exemplo, um maior número de endereços IPs disponíveis. A ideia do IPv6 surgiu basicamente por dois motivos principais: a escassez dos endereços IPv4 e pelo fato de empresas deterem faixas de endereços IPv4 classe A, inteiras.

Em um endereço IPv6 são utilizados 128 *bits*, o que permite um total de 340.282.366.920, endereços disponíveis seguidos de mais 27 casas decimais (diferentemente do IPv4, onde são utilizados 32 *bits*, para formar o endereço IP).

Os endereços IPv6 são formados por oito quartetos de caracteres hexadecimais, separados pelo caractere ":" (dois pontos).

Exemplo: **2800 : 03f0 : 4001 : 0804 : 0000 : 0000 : 0000 : 101f**

Considerando o sistema hexadecimal, cada caractere representa 04 *bits*, ou 16 combinações. Ainda, considerando uma base hexadecimal temos a representação de 0 a 9 e a utilização das letras A, B, C, D, E e F, que são as representações das 16 combinações possíveis.



Para saber mais sobre faixas de endereços IP, CIDR e máscara de tamanho variável, acesse: <http://www.hardware.com.br/tutoriais/endereco-ip-cidr/>

No IPv6 os endereços são divididos (assim como no IPv4) em dois blocos: os primeiros 64 *bits* identificando a rede (os primeiros 04 octetos) e os últimos 64 *bits* identificando os *hosts*. Vale lembrar aqui, que diferentemente do IPv4, no IPv6 não existem mais as máscaras de tamanho variável (CIDR) visto anteriormente.

Pode ser um pouco complicado armazenar na memória um endereço IPv6, devido a quantidade de caracteres existentes em cada endereço. Para ajudar nestas situações foram criadas técnicas que permitem abreviar estes endereços, conforme veremos nos exemplos a seguir:

- Exemplo 1: todos os zeros à esquerda (dentro de cada quarteto) do endereço podem ser omitidos. Exemplo: ao invés de escrever "0262", é possível escrever somente "262". Ao invés de escrever "0004", é possível escrever apenas "4" e ao invés de escrever "0000" é possível escrever apenas "0". Todas estas formas de abreviação são válidas e não alteram em nada o significado e funcionamento da rede.
- Exemplo 2: endereços do tipo "0:0:0:0:0:0:1" podem ser reduzidos para "::1".



Para configurar endereços em uma rede local de computadores, existem algumas opções, tais como:

- a) Utilizar endereços sequenciais: "2001:cde1::1", "2001:cde1::2", "2001:cde1::3" e assim sucessivamente para os micros da rede.
- b) Utilizar os endereços MAC das interfaces de rede, para utilizá-los também como endereços IPs. Exemplo: endereço MAC do computador "0C-EE-E6-8D-4D-7D" e tomamos como exemplo que o endereço de rede é "2001:bce4:0:0". A primeira tarefa a ser feita seria a conversão do endereço MAC em um endereço hexadecimal, simplesmente fazendo a inserção dos caracteres "ffff" entre o sexto e sétimo dígito. Desta forma, teríamos no exemplo "0CEE:E6ff:ff8D:4D7D". Fazendo a inserção do endereço de rede, teríamos o endereço IPv6 completo, tal como: 2001:bce4:0000:0000:0CEE:E6ff:ff8D:4D7D. O interessante desta técnica é que agilizamos e simplificamos a tarefa constante de buscarmos saber o endereço MAC e IP da interface da rede, em locais distintos.

Semelhante ao que ocorre no IPv4, no IPv6 temos faixas de endereços reservadas, ou seja, que podem ser utilizadas somente em redes locais, para testes, entre outros. Confira os exemplos no Quadro 4.7:

Quadro 4.7: Endereços IPv6 reservados	
Endereço IP	Utilização
Iniciados por "2001:"	Reservados para provedores de acesso
Iniciados por "3fff : ffff" e "2001 : 0DB8"	Reservados para uso em documentação, exemplos e testes (não são roteáveis)
0:0:0:0:0:0:1	Endereço de <i>loopback</i> (semelhante ao 127.0.0.1 no IPv4)

Fonte: Morimoto, 2007

Para testar a conectividade do IPv6, tanto em sistemas operacionais Windows quanto Linux, basta acessar o *prompt* de comando (Windows) e o terminal (Linux) e digitar respectivamente (MORIMOTO, 2007):

- ping ::1 (Windows)
- ping6 fee::1 (Linux)

4.4.1.2 Máscara de rede

Uma máscara de rede, também conhecida por *netmask*, corresponde a um número de 32 *bits*, semelhante a um endereço IP, com a finalidade de identificar a rede na qual está inserido determinado computador e quantidade de *hosts* (computadores) que podem estar nesta mesma rede.

Os computadores que fazem parte de uma rede possuem além de um número IP que identifica o mesmo, uma máscara de rede e um *gateway* de rede.

As máscaras de rede possuem padrões para cada classe (faixa de endereços IPs), conforme Quadro 4.8:

Quadro 4.8: Classes de endereço IPv4	
Classe	Máscara a ser utilizada
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Fonte: Morimoto, 2007

Para efeitos de exemplificação se tivéssemos um computador com o IP 200.132.36.3 a máscara de rede correspondente seria 255.255.255.0. Computadores que queiram comunicar-se e estejam em uma mesma máscara de

rede, fazendo a comunicação diretamente utilizando o protocolo apropriado para tal procedimento. Computadores que queiram comunicar-se, mas que estão configurados com máscaras diferentes necessitam de comunicação através de roteadores para intermediar a comunicação entre ambos.

4.4.2 O protocolo de controle de erros – ICMP

O protocolo ICMP (*Internet Control Message Protocol*) tem a função de identificar erros em uma rede de computadores. Computadores, servidores, *gateways*, entre outros dispositivos da rede utilizam-se do protocolo ICMP para enviar mensagens e comunicar-se entre si.

Como exemplo da utilização deste protocolo, estão dois comandos bastante conhecidos no contexto das redes de computadores, independente de sistema operacional. Estes comandos são o ping e o traceroute.

- O comando ping, permite saber se determinado computador está acessível, se existe conexão a internet, entre outros.
- O comando traceroute, permite fazer o rastreamento de um pacote na rede, listando os servidores, roteadores, entre outros dispositivos que este pacote “passa” até chegar ao seu destino.

Vale salientar que muitos *firewalls*, servidores e mecanismos de proteção de rede bloqueiam respostas a requisições ICMP (por meio dos comandos ping e traceroute), como forma de proteger estes equipamentos e a rede como um todo de tentativas de mapeamento e posteriormente ataques.

O protocolo ICMP é padronizado pela RFC 792, onde é possível visualizar, por exemplo, as principais funções e características detalhadas do funcionamento deste protocolo.

4.4.3 Tradução de endereços – ARP

Agora que compreendemos como funciona o endereçamento IP, percebemos que teremos duas formas distintas de endereçamento para os computadores da rede local: o endereço da camada de enlace, também conhecido como endereço MAC (corresponde ao endereço físico do computador) e o endereço da camada internet, também conhecido como endereço lógico ou endereço IP. Você pode estar se perguntando agora: “As duas formas de endereçamento são usadas na mesma rede?”. A resposta à pergunta é “Sim!”. Nas redes locais TCP/IP, usamos ambas as formas de endereçamento, em camadas diferentes.

O endereçamento na camada de enlace (o endereço MAC ou endereço Ethernet) é conhecido como endereçamento físico, pois é usado na camada de enlace ou endereço de *hardware*, está gravado no *firmware* da placa de rede e não pode ser alterado. O endereço da camada de rede (o endereço IP) é conhecido como endereço lógico, pois pode ser escolhido arbitrariamente. Sendo mais específico, o endereço físico e o endereço lógico, estão associados a uma mesma interface de rede de um computador conectado na rede, porém usados em camadas diferentes da arquitetura.

A comunicação entre os computadores da rede ocorre realmente na camada de enlace, ou seja, em uma rede local (computadores em uma mesma rede lógica), como a Ethernet, as máquinas se conhecem de fato pelo endereço físico. Por outro lado, na grande rede (internet) para cada computador do usuário é atribuído um endereço lógico distinto, o endereço IP.



Um item importante a ser questionado neste momento é: “Se cada camada usa um padrão de endereçamento diferente, como os protocolos de rede se entendem?”. Percebemos que precisa existir uma forma de associar um endereço lógico a um endereço físico. O protocolo de tradução de endereços mais usado é o ARP (*Address Resolution Protocol* – Protocolo de Resolução de Endereços).

O ARP é um protocolo distribuído, pois não precisa de um computador central gerenciando. Ele está implantado em cada máquina da rede. Conceitualmente, o ARP trabalha na camada de rede, pois traduz endereços da camada de rede em endereços da camada de enlace.

Analisaremos agora o funcionamento do ARP, por meio de um exemplo, passo-a-passo:

- a) O computador A possui o endereço IP 192.168.1.3 e deseja enviar um pacote ao computador B, com o endereço 192.168.1.4.
- b) O computador A, então, envia uma mensagem especial a todos “perguntando”: “Qual o endereço físico (MAC) do computador com endereço lógico (IP) 192.168.1.4?”. A mensagem é enviada a todos (*broadcast*), pois ele não sabe, obviamente, o endereço que está procurando.
- c) O computador B recebe o pedido de A e envia outra mensagem informando seu endereço MAC.

d) O computador A então envia o pacote que estava desejando enviar de início.

No nível de enlace, o endereço de *broadcast* MAC é FF:FF:FF:FF:FF:FF, ou seja, um endereço MAC com todos os 48 *bits* do endereço marcados (setados). Uma mensagem de *broadcast* é recebida por todos os computadores presentes na rede. A Figura 4.4 a seguir mostra os campos existentes em um pacote do tipo ARP.

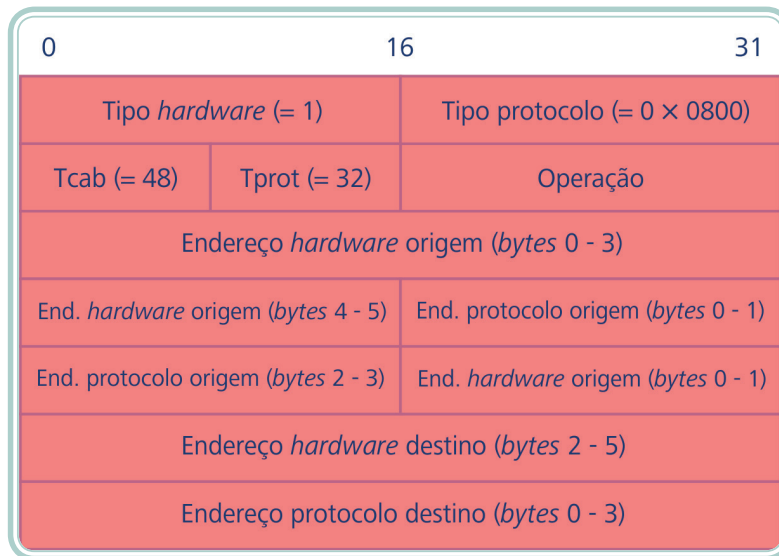


Figura 4.4: Campos de um pacote ARP

Fonte: CTISM, adaptado de Davie e Bruce, 2004, p. 188

No quadro da Figura 4.4 representamos o formato padrão de um pacote do protocolo ARP. O ARP foi projetado para ser genérico e permitir traduzir qualquer endereço lógico em endereço físico, porém na prática, o grande uso é na tradução de endereços IP em endereços MAC (endereço Ethernet). O campo Tipo *hardware* especifica a rede física, o 1 significa rede Ethernet. O campo Tipo protocolo especifica o protocolo da camada superior, neste caso o IP. Tcab significa o tamanho do endereço de *hardware* (endereço MAC) e Tprot determina o tamanho do endereço do protocolo (endereço IP). Operação especifica se o pacote corresponde a uma pergunta ou uma resposta. Os demais campos representam os endereços de origem MAC e IP (do computador que está enviando o pacote) e os endereços de destino MAC e IP (de quem recebe).

Os computadores mantêm uma lista (*cache*) com os endereços MAC associados aos endereços IP dos outros computadores na rede. Assim, o computador não precisa ficar “perguntando” pelo endereço MAC de outro computador, toda vez que quiser enviar um pacote. O ARP é um protocolo onde os computadores

podem “ouvir” os pedidos dos outros computadores, pois as mensagens são enviadas em *broadcast* e usar essas informações para criar sua própria lista de endereços. Um computador pode também responder, consultando sua própria lista, a um pedido de endereço de outro computador.

O ARP está condicionado à rede local. Não há o encaminhamento de pacotes ARP para outras redes, como ocorre com pacotes do nível de rede. No nível de rede, os pacotes são encaminhados aos roteados entre as redes (DAVIE; BRUCE, 2004).

4.4.4 RARP

O protocolo RARP (*Reverse Address Resolution Protocol*) intitulado como Protocolo de Resolução Reversa de Endereços, tem a função de associar um endereço Ethernet (MAC) a um endereço IP. Graças ao protocolo RARP um dispositivo de rede pode fazer uma solicitação a esta mesma rede para saber qual o endereço IP de determinada interface. Diferentemente do protocolo ARP, para dispositivos da rede que utilizam o protocolo RARP é necessário um servidor RARP que responda pelas solicitações encaminhadas a este servidor.

Na Figura 4.5, um esquema simples da diferença e função dos dois protocolos.

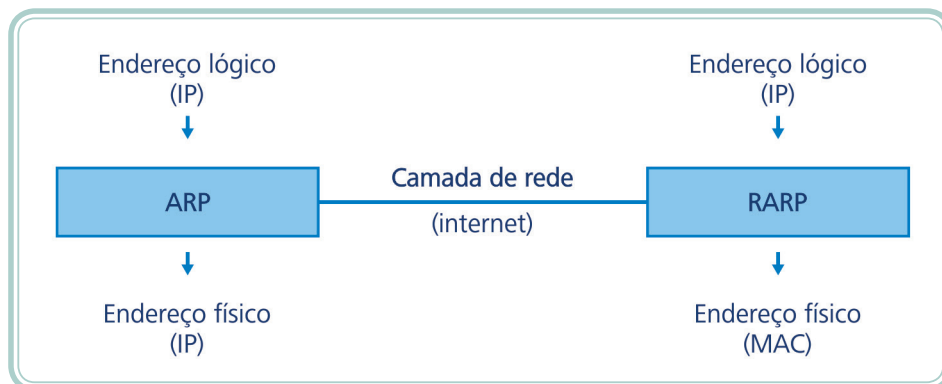


Figura 4.5: Protocolos ARP e RARP

Fonte: CTISM, adaptado dos autores

4.5 Protocolos da camada física (interface de rede)

Nesta quarta e última parte estudaremos os principais protocolos da camada de interface de rede do modelo TCP/IP, também conhecida como camada física. Esta camada aborda protocolos que trabalham no nível mais próximo ao *hardware* (interfaces, periféricos, entre outros).

4.5.1 Ethernet

Padronizada pelo padrão IEEE 802.3, o protocolo Ethernet é amplamente utilizado nas redes locais (LAN). Este protocolo, baseado no envio de pacotes é utilizado na interconexão destas redes. Dentre as características deste protocolo estão:

- Definição de cabeamento e sinais elétricos (camada física).
- Protocolos e formato de pacotes.

O padrão Ethernet baseia-se na ideia de dispositivos de rede enviando mensagens entre si. Cada um destes pontos de rede (nós da rede) possui um endereço de 48 *bits*, gravado de fábrica (endereço único mundialmente), também conhecido como endereço MAC, que permite identificar uma máquina na rede e ao mesmo tempo manter os computadores com endereços distintos entre si.

Um endereço MAC, gravado na memória ROM do computador é um endereço de 48 *bits*, composto por caracteres hexadecimais que vão de 0 à F. Destes 48 *bits* 24 são a representação de um código fornecido pelo IEEE, repassado a cada fabricante de interfaces de rede. Os outros 24 *bits* são atribuídos pela própria fabricante das placas de rede. Dessa forma, tem-se um endereço formado semelhante ao endereço mostrado na Figura 4.6.

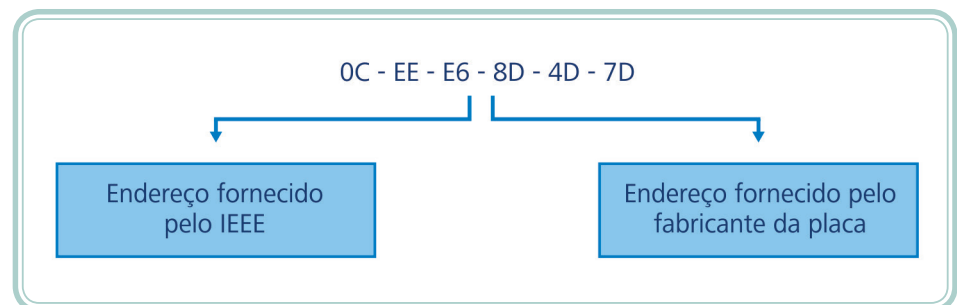


Figura 4.6: Componentes da criação de um endereço MAC

Fonte: CTISM, adaptado dos autores

Vale salientar que para identificar este endereço em um computador com sistema operacional Windows, basta acessar o *prompt* de comando e digitar o comando: "ipconfig /all".

Existem diferentes classificações para o padrão Ethernet, que vão desde padrões para cabeamento metálico, fibra óptica e interfaces *wireless*. Estes variam quanto ao tipo de tecnologia, velocidade, entre outras características. A seguir listamos as principais.

- 10Base-T Ethernet (padronizada pelo padrão IEEE 802.3). Velocidade de 10 *megabits* por segundo, utilizada em redes de par trançado.
- Fast Ethernet (padronizada pelo padrão IEEE 802.3u). Velocidade de 100 *megabits* por segundo, utilizada em redes de par trançado.
- *Gigabit* Ethernet (padronizada pelo padrão IEEE 802.3z). Velocidade de 01 *gigabit* por segundo.
- 10 *gigabit* Ethernet (padronizada pelo padrão IEEE 802.3ae). Velocidade de 10 *gigabits* por segundo.
- 100BASE-FX. Velocidade de 100 *megabits* por segundo, utilizada em redes de fibra óptica.
- 1000BASE-SX. Velocidade 01 *gigabit* por segundo, utilizada em redes de fibra óptica.
- 10GBASE-SR. Velocidade 10 *gigabits* por segundo, utilizada em redes de fibra óptica.
- *Wireless* Ethernet (padronizada pelo padrão IEEE 802.11). Oferece diferentes categorias, com características distintas (velocidade, canal de operação, frequência, etc.):
 - 02 *megabits* por segundo, no padrão 802.11.
 - 11 *megabits* por segundo, no padrão 802.11b.
 - 54 *megabits* por segundo, no padrão 802.11g.
 - De 65 a 300 *megabits* por segundo, no padrão 802.11n.

Resumo

Nessa aula, foi possível conhecer os principais protocolos utilizados nas redes de computadores, bem como, a função de cada um deles. Além disso, foi possível entender como esses protocolos funcionam e em qual camada operam. Como parte principal desta aula foi apresentado em detalhes os protocolos TCP e IP, fundamentais para o funcionamento lógico da rede.



Atividades de aprendizagem

1. Dada as camadas do modelo TCP/IP, liste os principais protocolos que operam em cada uma destas camadas.
2. Diferencie o protocolo TCP do protocolo UDP, citando três diferenças entre eles.
3. Com relação ao IPv4 e ao IPv6, qual a diferença entre estes protocolos? O que muda de um para o outro e como são formados?
4. Para que serve a notação CIDR e porque foi criada?
5. Qual a função do protocolo ICMP?
6. Cite três protocolos da camada de aplicação, o que fazem e para que servem.

Aula 5 – Meios de transmissão de dados

Objetivos

Conhecer os principais meio de transmissão de dados utilizados nas redes de computadores.

Compreender as redes de cabeamento metálico, sem-fio e de fibra óptica.

Ter o entendimento das principais tecnologias associadas a transmissão de dados.

Compreender a utilização dos meios de transmissão no dia-a-dia das redes de computadores.

5.1 Considerações iniciais

Os meios de transmissão de dados em uma rede de computadores são responsáveis pela troca de informação (*bits*) entre os dispositivos que compõe uma rede. Em outras palavras são a parte física da rede.

Diversos equipamentos podem ser utilizados para fazer a comunicação de uma rede, alguns já foram citados em seções anteriores, como uma placa de rede, um roteador, entre outros. Nesse capítulo abordaremos três tipos de meios de transmissão bastante usuais no contexto das redes de computadores: as redes cabeadas (cabos de par trançado e fibra óptica) e as redes sem-fio (*wireless*). Cada uma delas possui suas vantagens e desvantagens (como custo, viabilidade, velocidade, preço de implantação e manutenção) que precisam ser pensadas antes de implementá-las, analisando o custo/benefício e real necessidade de cada ambiente.

5.2 Cabeamento

O meio de transmissão de dados através de cabos possui três tecnologias distintas, porém, importantes no contexto das redes de computadores que são:

5.2.1 Cabos coaxiais

Utilizados em redes de computadores antigas e ainda hoje em cabos de antenas para redes *wireless* e *cable modem*, mas que possuíam uma série de limitações como: mal contato, conectores caros, cabos pouco maleáveis e um limite de velocidade de 10 *Mbits/s*.

O cabo coaxial foi por certo tempo utilizado como cabeamento responsável pela interligação de computadores em uma rede. Um cabo coaxial é basicamente composto por quatro elementos (da parte interna para a externa): um fio de cobre (responsável por transmitir sinais elétricos), um material isolante, com o intuito de minimizar interferências eletromagnéticas produzidas pelo cobre (condutor de energia), um condutor externo de malha e uma camada plástica protetora do cabo. Estes quatro elementos combinados, formam o cabo coaxial, conforme pode ser observado na Figura 5.1 (SILVA, 2010).

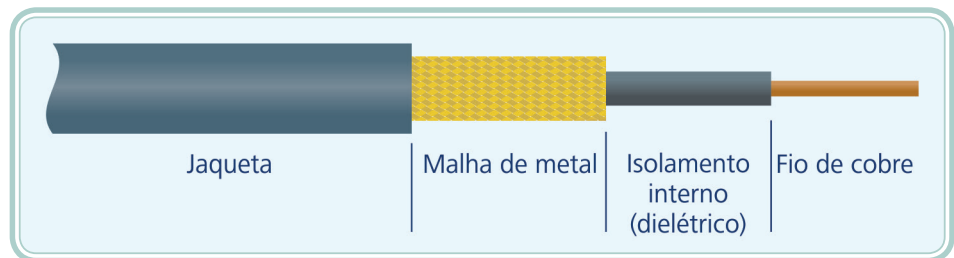


Figura 5.1: Partes do cabo coaxial

Fonte: CTISM

5.2.2 Cabos de par trançado

Os cabos de par trançado são, atualmente, os mais utilizados em uma rede local de computadores. Composto por pares de fios de cobre, trançados entre si, possuem diferentes tipos, categorias e padrões.

Existem algumas nomenclaturas que remetem ao cabo de par trançado, como por exemplo, as expressões 10Base-T ou 100Base-T, que se referem ao tipo de meio utilizado (no caso "T", como par trançado e "10" ou "100", como a taxa de transmissão em *megabits*). Outra expressão que nos remete a ideia de cabo de par trançado é a expressão "Ethernet" (protocolo de interconexão para redes locais), bastante usual, no funcionamento das redes de computadores.

Cabos de par trançado fazem uso de material condutor (cobre) para transmitir sinais elétricos. Associado a isso temos basicamente a frequência que este sinal é transmitido e a quantidade de *bits* que podem ser transferidos por segundo.

Por tratar-se de material condutor de sinais elétricos, os cabos de par trançado estão sujeitos a interferências eletromagnéticas externas de diferentes naturezas.

Uma das maiores vantagens em se utilizar cabos de par trançado para implantar uma rede de computadores é o fato de possuírem baixo custo e flexibilidade em prestar manutenção, corrigir eventuais problemas ou até mesmo expandir o número de computadores ligados a esta rede.

5.2.2.1 Categorias de cabos de par trançado

Os cabos de par trançado são divididos em categorias como uma espécie de classificação e características do mesmo (frequência, velocidade de transmissão, etc.).

As categorias dos cabos de par trançado vão de 1 a 7. Para todas estas categorias a distância máxima permitida entre um ponto e outro onde o cabo é utilizado é de 100 metros. Fatores que influenciam no comprimento máximo do cabo já foram citados anteriormente, como frequência, taxa de transferência de dados e interferência eletromagnética.

No Quadro 5.1 é possível visualizar um comparativo entre as categorias existentes, taxa de transferência possível e frequência.

Quadro 5.1: Categorias de cabos de par trançado		
Categoria do cabo	Taxa de transferência máxima	Frequência
Cat 1	Até 01 Mbps	Até 01 MHz
Cat 2	Até 04 Mbps	Até 16 MHz
Cat 3	Até 10 Mbps	Até 16 MHz
Cat 4	Até 20 Mbps	Até 20 MHz
Cat 5	Até 100 Mbps	Até 100 MHz
Cat 5e	Até 1000 Mbps	Até 125 MHz
Cat 6	Até 1000 Mbps	Até 250 MHz
Cat 6a	Até 10 Gbps	Até 500 MHz
Cat 7	Até 10 Gbps	Até 700 MHz

Fonte: Morimoto, 2007

Os cabos “Cat 1” e “Cat 2” ou categoria 1 e 2, não são mais reconhecidos pela TIA (*Telecommunications Industry Association*), associação responsável pela padronização dos cabos. Usadas em instalações telefônicas no passado, foram sendo automaticamente substituídas por padrões mais novos.

A categoria 3 foi a primeira desenvolvida objetivamente para o uso em redes de comunicações. Como características desta categoria introduziu-se a ideia de entrançamento dos pares de cabo (sendo que cada metro de cabo possuía uma quantidade diferente de tranças), se tornando assim menos suscetíveis a interferências eletromagnéticas externas.

Na categoria 4, padrão não mais reconhecido pela TIA, os cabos possuíam uma qualidade superior aos da categoria 3, porém, não tiveram uma vida útil duradoura no segmento dos cabeamentos de rede.

Os cabos existentes da categoria 5 foram substituídos pelos cabos da categoria 5e (versão aperfeiçoada do padrão, que reduz a interferência e a perda do sinal), bastante usuais em redes locais atuais, principalmente pela taxa de transmissão máxima de 1000 *Mbits*. Os cabos da categoria 5e por sua vez, estão sendo substituídos pelos cabos da categoria 6 e 6a, que podem ser utilizados em redes de 10 *Gbps*.

Na Figura 5.2, é possível observar um cabo cat 5e e um cat 6, haja vista que as informações gerais do cabo como padrão, tipo e categoria já vem rotulados no próprio cabo.

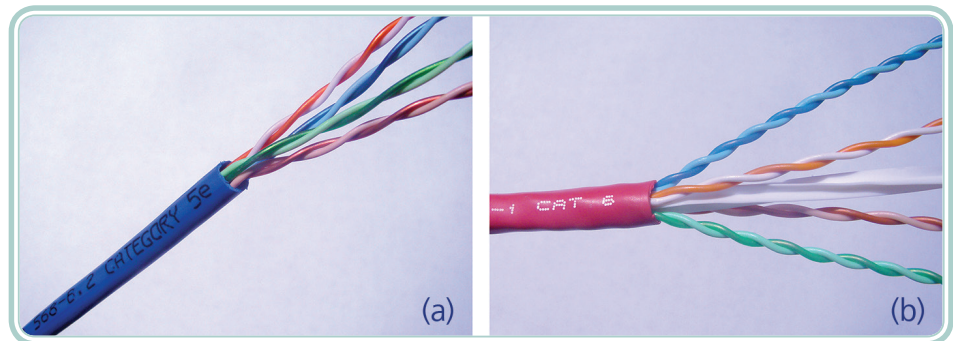


Figura 5.2: Cabos par trançado categoria 5e (a) e categoria 6 (b)

Fonte: CTISM

Os cabos da categoria 6, desenvolvidos para as redes *gigabit* Ethernet, podem ser utilizados em redes de 10 *Gbps*, porém, com uma distância máxima entre dois pontos limitada a 55 metros, diferente dos padrões 5 e 5e que possuem um alcance de 100 metros. Para minimizar este problema foram desenvolvidos cabos com alcance de até 100 metros em redes de 10 *Gbits*, a categoria 6a.

Como medida para reduzir o problema do *crosstalk* (interferência provocada entre os pares de cabo), na categoria 6a foi introduzido no interior do cabo um separador, que nada mais é do que uma espécie de cabo plástico. Apesar dessa medida reduzir o *crosstalk*, ela deixou o cabo mais grosso e menos flexível em comparação aos outros tipos de cabos. Um comparativo entre os dois pode ser visto na Figura 5.3;

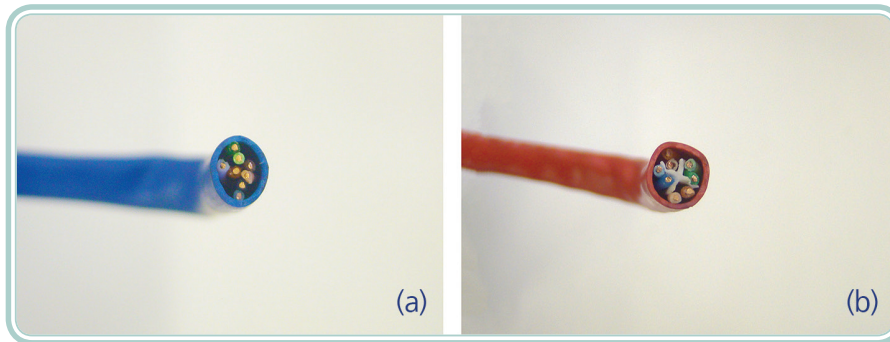


Figura 5.3: Diferenças entre cabos cat 5e (a) e cat 6a (b)

Fonte: CTISM

Os cabos da categoria 7, inicialmente pensados para o padrão de 100 *Gbits*, podem vir a ser utilizados no futuro em substituição a tecnologias anteriores.

5.2.2.2 Conectores de cabos de par trançado

Os cabos de rede geralmente são comercializados por metro. Os cabos de par trançado são compostos de 04 pares de fios, trançados entre si. Quanto aos conectores utilizados nas extremidades dos cabos, temos o conector RJ-45 que é de longe o mais usado em cabos de par trançado. Aqui vale uma ressalva: existem diferentes tipos de conectores RJ-45 para categorias de cabo diferentes. Um conector RJ-45 para cabos cat 5 é diferente de um conector RJ-45 para cat 6. Enquanto o primeiro é disposto lado-a-lado (quanto a sua disposição dos pinos) o outro é disposto em zig-zag, como medida para diminuir a perda de sinal e o *crosstalk*. Na Figura 5.4 é possível visualizar um conector RJ-45 para cat 5 (a) e um conector RJ-45 para cat 6 (b).

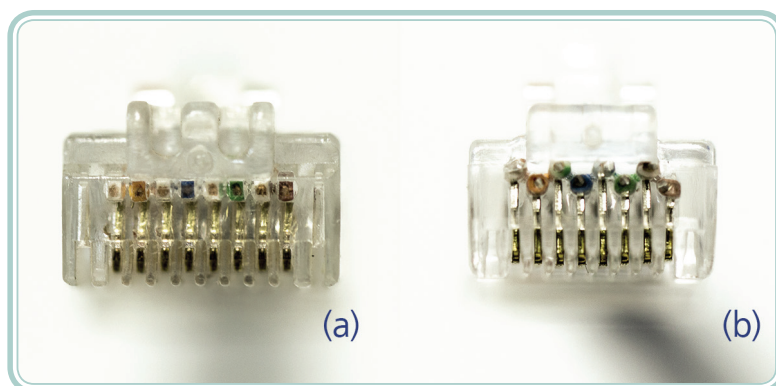


Figura 5.4: Conector RJ-45 cat 5 (a) e cat 6 (b)

Fonte: CTISM

Os conectores TERA são outro tipo de conector que podem vir a ser utilizados nas redes de par trançado em velocidades de 100 *Gbits*. Apesar de ser mais complexo que o conector RJ-45, possui a vantagem de ser blindado o que reduz a possibilidade de mal contato e problemas relacionados.

5.2.2.3 Tipos de cabos de par trançado

Conforme o ambiente onde a rede de computadores será montada, existe a necessidade da utilização de cabos de par trançado específicos para isso. Isto se explica devido os diferentes cenários que podem existir, como por exemplo, ambientes úmidos, áreas externas, ambientes próximos a geradores de energia, entre outros.

Quanto aos tipos de cabos de par trançado, existem basicamente dois: os cabos sem blindagem, conhecidos como **UTP** (*Unshield Twisted Pair*), que por sua vez são mais flexíveis e os cabos com blindagem, chamados de **STP** (*Shielded Twisted Pair*) que se subdividem em: FTP, STP e SSTP.

Os cabos **UTP** (sem blindagem), utilizam o conector RJ-45 e são os mais usuais em redes locais. Estes cabos são padronizados pela TIA/EIA, possuindo um comprimento máximo de 100 metros com uma taxa de transferência que pode mudar conforme a categoria do cabo (categorias apresentadas anteriormente). Na Figura 5.5, é possível visualizar um cabo do tipo **UTP**.

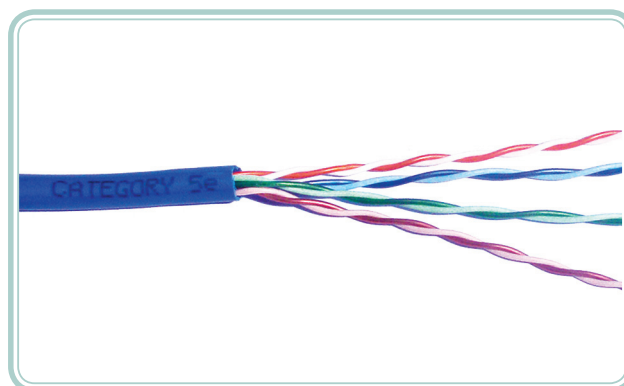


Figura 5.5: Cabo do tipo UTP – par trançado sem blindagem

Fonte: CTISM

Com relação aos cabos de par trançado com blindagem, temos o padrão FTP (*Foiled Twisted Pair*). Neste tipo de cabo, uma camada protetora (produzida de aço ou alumínio) faz uma blindagem simples envolvendo todos os pares de cabo. Este tipo de blindagem simples ajuda a minimizar o problema da interferência eletromagnética, mas não resolve interferências internas, provocadas pelos próprios pares (*crosstalk*). Na Figura 5.6 é possível visualizar um exemplo de cabo do tipo FTP.

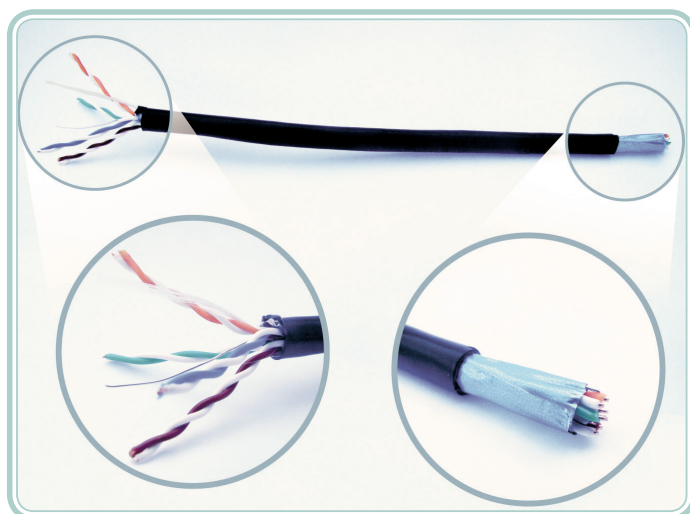


Figura 5.6: Cabo do tipo FTP – par trançado

Fonte: CTISM

Cabos do tipo **STP** (*Shielded Twisted Pair*), fazem uso de uma blindagem que reveste cada par de cabos individualmente. Dessa forma, tem-se um isolamento de cada par de cabos, através de uma cobertura de metal, o que reduz consideravelmente interferências externas e internas, permitindo ainda que o cabo seja utilizado em situações onde se faz necessário utilizar o cabo em distâncias maiores do que 100 metros.

Nos cabos do tipo **SSTP** (*Screened Shielded Twisted Pair*), existe a combinação dos dois tipos de blindagem apresentados anteriormente: o FTP mais o STP. Os cabos do tipo SSTP, são revestidos internamente com uma capa protetora entre cada um dos pares de cabo e mais uma proteção entre todos os pares existentes dentro do cabo, por isso a combinação entre os dois tipos de blindagem apresentados anteriormente. Com estas duas proteções internas, os cabos do tipo SSTP são indicados para casos extremos onde se tem grandes geradores de energia gerando interferência eletromagnética, por onde passam os cabos de rede.

Outra consideração que deve ser levada em conta na utilização de cabos com blindagem é a utilização de conectores especiais para estes cabos. Para isso, existem os conectores RJ-45 blindados. Estes conectores possuem uma proteção metálica que ajuda na blindagem da parte destrançada do cabo. Vale lembrar que as conexões são as partes vulneráveis do cabo (e geralmente as mais propícias a problemas de cabeamento), por isso a importância de manter a blindagem do início ao fim. Na Figura 5.7, é possível visualizar um exemplo de conector RJ-45 blindado (MORIMOTO, 2008a).

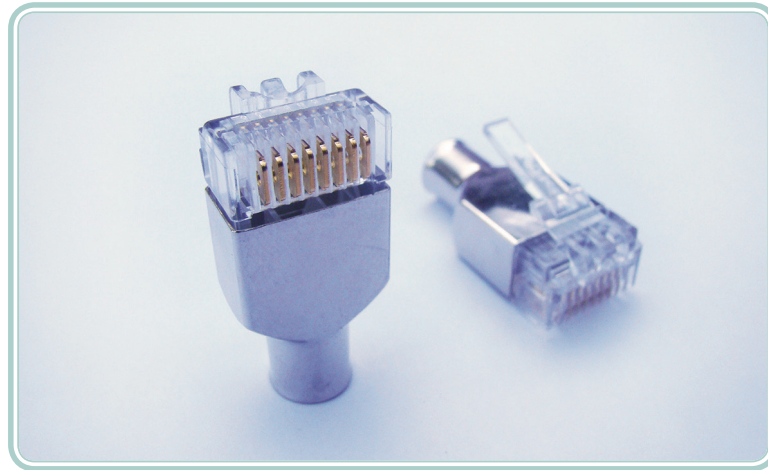


Figura 5.7: Conectores RJ-45 blindados

Fonte: CTISM

5.2.2.4 Padrões de conexão de cabo e pinagem

Conforme descrito anteriormente, um cabo de par trançado dispõe em seu interior de oito fios dispostos em pares, sendo que destes quatro pares somente dois pares são efetivamente utilizados (sendo um para transmitir e outro para receber dados). Os oito fios presentes no cabo possuem cores diferentes, como forma de simplificar a identificação dos mesmos e a crimpagem (ato de conectar o cabo ao conector RJ-45).

Para que seja mantido um padrão quanto a ordem de cores deste cabo junto ao conector, tem-se dois padrões bastante utilizados: os padrões EIA 568A e o padrão EIA 568B. O padrão EIA 568B é o mais comum e segue a ordem quanto a disposição dos fios, conforme apresentado no Quadro 5.2:

Quadro 5.2: Padrão de conexão EIA 568B	
Pino do conector RJ-45	Fio
1	Branco com Laranja
2	Laranja
3	Branco com Verde
4	Azul
5	Branco com Azul
6	Verde
7	Branco com Marrom
8	Marrom

Fonte: Morimoto, 2007

Já o padrão 568A, possui a seguinte ordem, representada no Quadro 5.3.

Quadro 5.3: Padrão de conexão EIA 568A

Pino do conector RJ-45	Fio
1	Branco com Verde
2	Verde
3	Branco com Laranja
4	Azul
5	Branco com Azul
6	Laranja
7	Branco com Marrom
8	Marrom

Fonte: Morimoto, 2007

Os dois padrões possuem grande semelhança, o que ocorre de diferente é a troca de posições entre os cabos laranja e verde.

Ao fazer as conexões dos conectores RJ-45 aos cabos de rede (crimpagem) devemos seguir sempre um dos padrões citados acima (568A ou 568B) nas duas extremidades do cabo, isto serve para ligação de um computador a um *switch*, de um computador a um roteador, enfim, para dispositivos diferentes. Caso exista a necessidade de ligar dispositivos diretamente, como no caso um computador ligado diretamente a outro por um único cabo de rede (chamado neste caso de cabo *crossover*), neste caso é necessário que uma das pontas do cabo seja conectada usando o padrão 568A e a outra ponta o padrão 568B.



É importante salientar a regra a seguir:

- Dispositivos diferentes (ligação de cabo par trançado entre computador/*switch* ou computador/roteador, etc.) cabos com padrões iguais nas duas pontas (568A nas duas pontas ou 568B nas duas pontas).
- Dispositivos iguais (cabo entre computador/computador ou *switch/switch*, etc.) existe a necessidade de uma ponta de conexão ser diferente da outra (uma ponta 568A e a outra ponta 568B).

Com esta regra fica mais fácil a utilização de cada um levando em consideração a necessidade dos mesmos.

5.2.3 Cabos de fibra óptica

Os cabos de fibra óptica popularizaram-se e hoje tem um papel fundamental nas telecomunicações, principalmente em ambientes que necessitam de uma alta largura de banda como é o caso da telefonia, televisão a cabo, entre outros. A redução do preço da fibra, o alcance e quantidade de dados que

é possível trafegar nela são alguns dos motivos da aceitação e utilização das fibras ópticas em longas distâncias, bem como, gradativamente nas redes locais de computadores.

Uma fibra óptica nada mais é do que uma pequena haste de vidro, revestida por materiais protetores, que utiliza-se da refração interna total, para poder transmitir feixes de luz ao longo da fibra por grandes distâncias. Junta-se a capacidade de transmissão da fibra com o fato da perda ser mínima em grande parte dos casos.

Um cabo de fibra óptica é composto por diferentes materiais, conforme pode ser descrito a seguir, da parte interna para a externa da fibra (SILVA, 2010):

- **Núcleo** – geralmente produzido de vidro, possui em média 125 microns (um décimo de um milímetro aproximadamente), por onde passa a luz emitida e refletida por toda a fibra.
- **Casca** – geralmente de plástico serve para revestir a fibra.
- **Capa** – feita de plástico tem o objetivo de proteger tanto a casca como a fibra.
- **Fibras de resistência mecânica** – servem para preservar o cabo evitando que o mesmo seja danificado.
- **Revestimento externo** – camada de plástico externa que protege os cabos de fibra óptica internos.

Os cabos de fibra óptica variam quanto a quantidade de fios existentes em seu interior, podendo ter um ou vários, dependendo do tipo e onde será utilizado. De modo geral, os cabos utilizados para interligação em uma rede de computadores local, geralmente possui um único cabo. Já, os cabos de fibra destinados a interligação de grandes distâncias e *links* de comunicação possuem diversos fios. Um exemplo destes dois tipos de cabo pode ser visto na Figura 5.8.

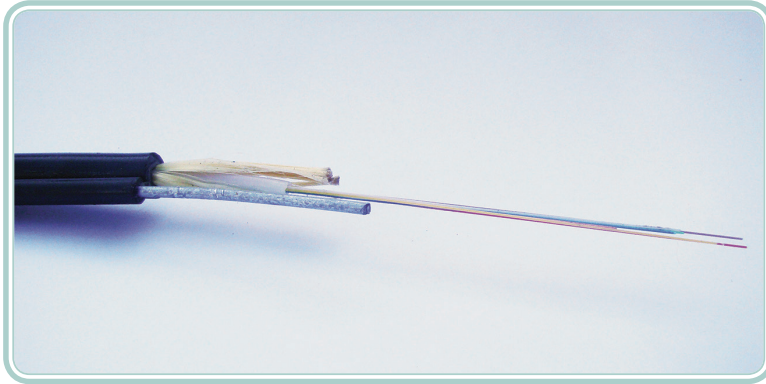


Figura 5.8: Cabo de fibra ótica

Fonte: CTISM

Existe uma série de vantagens em se utilizar cabos de fibra óptica no lugar dos cabos de par trançado citados anteriormente, algumas destas vantagens são:

- Como os cabos de fibra óptica são bastante finos, conforme tamanho mencionado anteriormente é possível incluir uma grande quantidade de fios em um cabo.
- A quantidade de transmissão de dados possível em uma fibra é muito maior do que a capacidade alcançada através de cabos de par trançado.
- Além disso, como as fibras possuem um longo alcance, necessitam de menos repetidores ou equipamentos para expansão do sinal.
- No caso de grandes distâncias a serem interligadas, acaba saindo mais barato o uso de fibras ópticas.
- Por usar refração de luz em seu núcleo a fibra é imune a interferências eletromagnéticas, podendo ser utilizada em diferentes ambientes e situações.

As fibras ópticas fazem uso de luz infravermelha para transmissão de sinais, com um comprimento de onda de 850 a 1550 nanômetros. O uso de LED's era bastante comum nos transmissores, porém, foi sendo gradativamente substituído pelos lasers devido a demanda de velocidade dos novos padrões (01 Gbps e 10 Gbps).

Quanto a classificação das fibras temos duas principais: as fibras **monomodo** e **multimodo**, que serão explicadas na seção seguinte.

5.2.3.1 Tipos de fibras ópticas

As fibras ópticas dividem-se em fibras de monomodo, também conhecidas como SMF (*Single Mode Fibre*) e as fibras de multimodo ou MMF (*Multi Mode Fibre*).

As fibras monomodo, têm as seguintes características:

- Possuem um núcleo de 08 à 10 microns de diâmetro.
- Inicialmente eram bem mais caras do que as fibras multimodo.
- A atenuação do sinal é menor do que nas fibras multimodo.
- São capazes de atingir distâncias de até 50 km sem a necessidade de retransmissores.

Já as fibras ópticas multimodo, possuem como características:

- Núcleos no tamanho de 62,5 microns de diâmetro.
- Inicialmente eram mais baratas que as fibras monomodo.
- Possuem uma atenuação do sinal luminoso maior que as fibras monomodo.
- Podem interligar pontos até 2,5 km sem necessidade de retransmissores.

A diferença entre uma fibra monomodo e uma multimodo é basicamente a forma de propagação do sinal luminoso que cada uma faz. Nas fibras monomodo, por exemplo, dado o núcleo da fibra ser menor, isso faz com que a luz trafegue na fibra mantendo uma constância do sinal, tendo desta forma um número menor de reflexões dentro da fibra, o que torna a mesma menos suscetível a perdas ou atenuação do sinal. Porém, nas fibras multimodo, acontece o inverso, ou seja, devido ao núcleo da fibra ter uma maior espessura, o sinal luminoso ricocheteia dentro da fibra em diferentes direções, fazendo com que o sinal luminoso tenha maior atenuação e maior perda durante a transmissão.

Na Figura 5.9 é possível visualizar como se dá a transmissão do sinal luminoso dentro de cada um dos tipos de fibra (monomodo e multimodo).



Para conhecer mais sobre o processo de fabricação das fibras ópticas assista o seguinte vídeo:

<http://www.youtube.com/watch?v=EK9bbIRKayA>



Figura 5.9: Propagação de sinal dentro da fibra óptica monomodo e multimodo

Fonte: CTISM

5.2.3.2 Conectores para fibras ópticas

Os conectores para as fibras ópticas tem um papel importante, no que diz respeito a permitir a passagem da luz, sem que ocorra um alto nível de perda, neste processo. Existem diferentes tipos de conectores que podem ser utilizados para este fim, entre os mais usuais estão os conectores: ST, SC, LC e MT-RJ.

É possível utilizar qualquer um dos conectores de fibra óptica (inclusive com um padrão diferente em cada ponta do cabo de fibra, por exemplo, um ST numa ponta e um LC na outra ponta do cabo), cada um com suas vantagens e desvantagens. O mais usual é escolher um conector baseado nos equipamentos que se pretende utilizar. A seguir, tem-se uma descrição dos principais conectores para cabos de fibra óptica:

- **Conector ST** – o conector ST, abreviação para *Straight Tip*, bastante utilizado na conexão de fibras multimodo é um dos padrões mais antigos no mercado. Usualmente utilizado na década de 90, foi sendo gradualmente substituído por conectores mais recentes.

O formato do conector ST (estilo baioneta) lembra bastante os conectores BNC utilizados em cabos coaxiais, conforme pode ser visualizado na Figura 5.10.

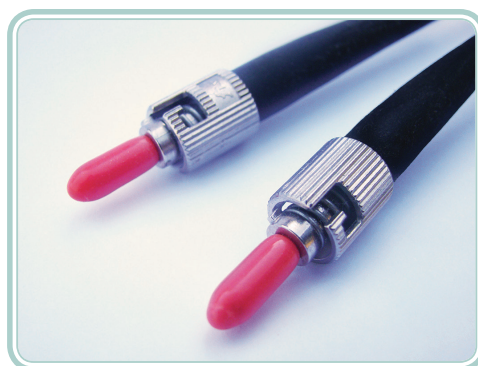


Figura 5.10: Conectores de fibra óptica do tipo ST

Fonte: CTISM

- **Conector SC** – o conector SC, bastante popular em redes *gigabit*, possui como características: facilidade, eficiência e baixa perda de sinal, apesar de perder espaço para os conectores do tipo LC. Como desvantagem o tamanho do conector, que é relativamente grande se comparado aos demais padrões de conectores existentes.

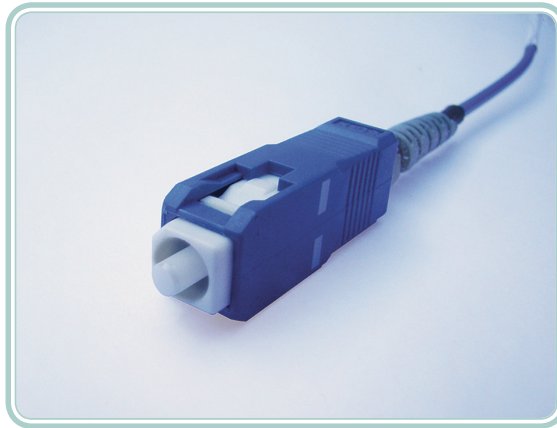


Figura 5.11: Conector de fibra óptica do tipo SC

Fonte: CTISM

- **Conector LC** – conectores do tipo LC (*Lucent Connector*) ganharam bastante popularidade e possuem como características: uso principal em fibras ópticas do tipo monomodo e também em *transceivers* no padrão *Gigabit Ethernet*, além de possuir um tamanho miniaturizado.

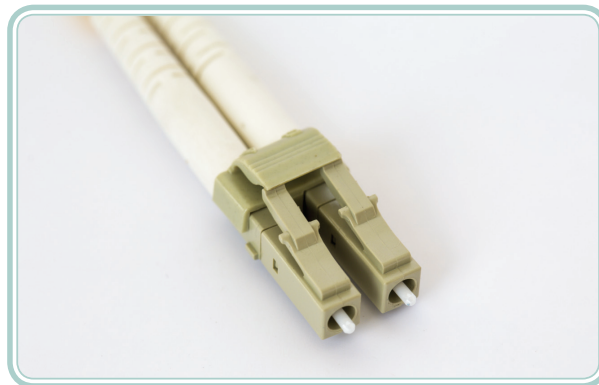


Figura 5.12: Conector de fibra óptica do tipo LC

Fonte: CTISM

- **Conector MT-RJ** – os conectores MT-RJ (*Mechanical Transfer Registered Jack*) permitem combinar duas fibras ópticas em um único conector (através de dois orifícios existentes no conector). Sua utilização é mais indicada para fibras multimodo nas quais vem substituindo gradativamente os conectores SC e ST.

5.2.3.3 Emendas de fibras ópticas

As fibras ópticas podem ser unidas não somente através de conectores, mas também através de dois métodos principais: o processo de fusão e o processo mecânico, os quais serão abordados a seguir:

- **Fusão de fibra óptica**

O processo de fusão da fibra utiliza um arco elétrico para unir (soldar) as duas fibras, formando uma conexão sólida. Apesar de sofrer pequenas atenuações devido a fusão, geralmente o resultado é satisfatório, desde que obedeça aos limites aceitáveis de perda, resultante da fusão da fibra.

Para este processo é utilizada uma máquina de fusão de fibra óptica, onde ocorre um alinhamento das fibras (ficando as mesmas frente-a-frente), aquecendo as extremidades da fibra e aplicando uma pressão para unir as partes.

Cabe uma ressalva de que uma máquina de fusão tem um preço elevado, o que faz sentido para empresas que prestam este tipo de serviço. Ainda, para o processo de fusão, são necessários outros equipamentos como alicates especiais, clivadores, desencapadores, álcool isopropílico (para limpeza das pontas da fibra), entre outros materiais necessários. A emenda por fusão apresenta um dos menores índices de perda de sinal nos processos de fusão.



- **Fusão por emenda mecânica**

O processo de fusão por emenda mecânica apresenta uma emenda de aplicação manual, ou seja, as duas extremidades do fio são unidas e coladas com uma resina especial, permitindo a passagem da luz.

Para evitar que a emenda fique exposta e frágil a novas rupturas, o cabo emendado é reforçado por uma cobertura para assegurar maior proteção ao processo de emenda mecânica (MORIMOTO, 2008b).

5.3 Redes de transmissão sem-fio

As redes de transmissão e comunicação sem-fio, também conhecidas como *wireless*, são, sem dúvida, uma grande alternativa aos meios de transmissão cabeados (par trançado e fibra óptica), pois se utilizam do ar para enviar e receber sinais de comunicação.

A-Z

transceivers ou transceptor
É um equipamento de rede de computadores, que transforma os sinais ópticos recebidos através do cabo em sinais elétricos que são enviados ao *switch* e vice-versa.

Este tipo de comunicação é útil em situações onde a utilização por meio de cabos se torna inviável, porém, como qualquer outra tecnologia, apresenta suas vantagens e desvantagens. Na sequência desse capítulo, abordaremos algumas tecnologias de transmissão sem-fio, como: rádio, Bluetooth, Wi-Fi, infravermelho, *laser*, entre outros.

5.3.1 Rádio

As tecnologias de transmissão via rádio utilizam-se de ondas de rádio para realizar a comunicação. Entre as vantagens deste tipo de tecnologia estão a facilidade na geração das ondas, a possibilidade de comunicação de grandes distâncias, além da flexibilidade em realizar mudanças (inserção de novos pontos de comunicação, entre outros).

Para efeitos de classificação, a transmissão via ondas de rádio pode ser feita de forma **direcional** ou **não direcional**.

Na transmissão direcional a ideia é ter uma antena (geralmente uma parabólica pequena) apontando diretamente para a outra antena (na mesma direção, de forma a ficarem alinhadas, sem obstáculos), para fazer a comunicação entre duas redes distintas, por exemplo. Como vantagem da transmissão direcional está o fato da segurança, uma vez que somente as duas redes se comunicarão, mas como está exposta ao ar livre não está livre dos problemas relacionados ao ambiente externo, como um tempo nublado, chuva, raios, etc.

Com relação a transmissão não direcional, a ideia é que seja colocada uma antena transmissora em um local alto (antena do tipo omnidirecional, que propaga o sinal em diferentes direções a partir da fonte), que propicie aos clientes (antenas que irão se comunicar com a antena servidora) captar o sinal emitido. Este tipo de transmissão por estar exposto (qualquer pessoa com um dispositivo específico poderia captar o sinal) necessita de uma **criptografia** na transmissão dos dados (SILVA, 2010).

Este tipo de comunicação tem como vantagens o fato de ser viável economicamente e eficiente no que se propõe. Fatores como alcance da rede e taxa de transferência estão diretamente relacionados a qualidade e especificações dos equipamentos utilizados na rede.

5.3.2 Bluetooth

O Bluetooth é uma tecnologia de transmissão de dados sem-fio, que permite a comunicação entre computadores, *notebooks*, *smartphones*, *mouse*, teclado,

A-Z

criptografia
É a técnica de usar algoritmos que alterem os dados de forma a impedir ou dificultar acessos indevidos aos mesmos.

impressoras, entre outros dispositivos de forma simples e com um baixo custo, bastando que estes dispositivos estejam em uma mesma área de cobertura.

A tecnologia Bluetooth (padronizada pela IEEE 802.15) possui características como: baixo consumo de energia para seu funcionamento e um padrão de comunicação sem-fio para dispositivos que façam uso desta tecnologia. Dessa forma, a comunicação entre estes dispositivos ocorre através de radiofrequência, independente da posição deste dispositivo, desde que o mesmo se encontre dentro de uma mesma área de abrangência dos demais dispositivos que queiram comunicar-se.

A área de cobertura do Bluetooth abrange três tipos de classes diferentes, conforme Quadro 5.4:

Quadro 5.4: Classes da tecnologia Bluetooth

Classe	Potência (máxima)	Alcance (máximo)
1	100 mW	100 metros
2	2,5 mW	10 metros
3	1 mW	1 metro

Fonte: Alecrim, 2008b

É importante respeitar a distância aceitável de cada dispositivo. A comunicação entre dispositivos de diferentes classes é possível desde que se respeite o alcance máximo de cada classe.

A velocidade de transmissão em uma rede Bluetooth varia conforme a versão da tecnologia, neste caso temos:

- Versão 1.2, com taxa de transmissão de 1 Mbps (taxa máxima).
- Versão 2.0, com taxa de transmissão de 3 Mbps (taxa máxima).
- Versão 3.0, com taxa de transmissão de 24 Mbps (taxa máxima).

Quanto a frequência e operação do Bluetooth, o mesmo opera na frequência de 2,45 GHz, padrão de rádio aberta utilizável em qualquer lugar do mundo. A faixa de operação chamada ISM (*Industrial Scientific Medical*), possui variações de 2,4 à 2,5 GHz.

Quanto às classificações das redes que se formam pela comunicação de dispositivos Bluetooth, temos duas situações: as redes *piconet* e as redes *scatternet*.

Temos uma rede *piconet*, quando dois ou mais dispositivos utilizando Bluetooth se comunicam entre si. Neste caso, o dispositivo que começou a comunicação recebe o papel de *master* ou mestre da rede formada (dispositivo que controla o sincronismo e regula a transmissão dos dados), enquanto os demais dispositivos da rede são denominados *slaves* ou escravos.



Uma rede do tipo *piconet* pode ter no máximo 08 dispositivos se comunicando entre si na mesma rede, sendo um mestre e sete escravos.

Já uma rede *scatternet* é formada quando há uma *piconet* que se comunica com outras redes *piconet* dentro do limite de alcance dos dispositivos. Neste caso há um compartilhamento de dispositivos de diferentes *piconets*, sendo que o dispositivo mestre em cada rede continua o mesmo. Na Figura 5.13, é possível visualizar um exemplo de rede *piconet* e *scatternet* (ALECRIM, 2008b).

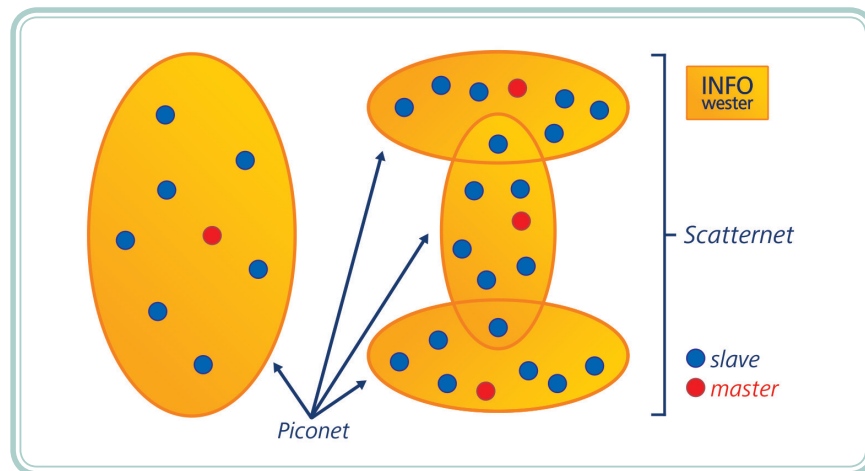


Figura 5.13: Redes Bluetooth do tipo *piconet* e *scatternet*

Fonte: CTISM

5.3.3 Wi-Fi

O termo Wi-Fi (*Wireless Fidelity*), refere-se a um padrão (IEEE 802.11) para redes sem-fio. Através da tecnologia Wi-Fi é possível realizar a interligação de dispositivos compatíveis como *notebooks*, impressoras, *tablets*, *smartphones*, entre outros. Assim como outras tecnologias sem-fio, o Wi-Fi utiliza-se da radiofrequência para transmissão de dados. Esta flexibilidade e facilidade de construir redes utilizando este padrão fez com que o Wi-Fi se tornasse popular, sendo hoje utilizado em diferentes locais como hotéis, bares, restaurantes, hospitais, aeroportos, etc.

A tecnologia Wi-Fi é baseada no padrão 802.11, conforme citado anteriormente, que estabelece regras (normas) para criação e uso das redes sem-fio.

O alcance das redes Wi-Fi variam conforme os equipamentos utilizados, mas em geral cobrem áreas de centenas de metros.

As redes Wi-Fi, são subdivididas em categorias ou padrões, como forma de organização e normatização da tecnologia, conforme descrito a seguir.

- **Padrão 802.11**

Criada originalmente em 1997, opera com frequências definidas pelo IEEE (*Institute of Electrical and Electronic Engineers*) de 2,4 GHz à 2,48 GHz, possuindo uma taxa de transmissão de dados de 1 Mbps à 2 Mbps.

Quanto às formas que o padrão 802.11 utiliza para transmissão do sinal de radiofrequência, tem-se: o DSSS (*Direct Sequence Spread Spectrum*) e o FHSS (*Frequency Hopping Spread Spectrum*). O DSSS faz o uso de vários canais de envio simultâneo, enquanto o FHSS transmite a informação utilizando diferentes frequências.

- **Padrão 802.11b**

Este padrão (802.11b) é uma atualização do padrão 802.11 original. Como característica principal apresenta diferentes velocidades de transmissão, que são: 01 Mbps, 02 Mbps, 5,5 Mbps e 10 Mbps. A taxa de frequência é igual ao padrão anterior (2,4 GHz à 2,48 GHz) sendo que a distância máxima de comunicação neste padrão pode chegar a 400 metros, para ambientes abertos e 50 metros para ambientes fechados (salas, escritórios, etc.).

- **Padrão 802.11a**

Disponível em 1999, esta tecnologia possui as seguintes características:

- Taxa de transmissão de dados: 06, 09, 12, 18, 24, 36, 48 e 54 Mbps.
- Alcance máximo de 50 metros.
- Frequência de operação de 05 GHz.
- Utiliza a técnica de transmissão denominada OFDM (*Orthogonal Frequency Division Multiplexing*), que permite a informação ser trafegada e dividida em pequenos segmentos transmitidos simultaneamente em diferentes frequências.

- **Padrão 802.11g**

Disponível desde 2002, este padrão veio a substituir o padrão 802.11b. Como características este padrão possui:

- Taxas de transmissão de até 54 Mbps.
- Frequências na faixa de 2,4 GHz.
- Técnica de transmissão OFDM.

- **Padrão 802.11n**

Sucessor do padrão 802.11g, o padrão 802.11n teve seu início a partir de 2007. Sua principal característica está no fato de conseguir transmitir utilizando várias vias de transmissão (antenas) em um padrão chamado MIMO (*Multiple-Input Multiple-Output*), propiciando com isso taxas de transmissões na faixa de 300 Mbps.

Com relação a frequência de operação, o padrão 802.11n pode operar tanto na faixa de 2,4 GHz como na faixa de 5 GHz, tornando-se compatível com padrões anteriores. Quanto a abrangência é possível chegar a 400 metros.

- **Padrão 802.11ac**

O padrão 802.11ac, sucessor do padrão 802.11g, faz parte de uma nova geração de padrões de alta velocidade das redes sem-fio. Sua principal vantagem está na velocidade da transmissão de dados entre dispositivos do mesmo padrão: de 450 Mbps à 1 Gbps. Preparada para trabalhar na frequência de 5 GHz, contará com um sistema avançado de modulação chamado MU-MIMO (*Multi User – Multiple Input Multiple Output*) (ALECRIM, 2008a).

Na Figura 5.14, é possível visualizar esta evolução de padrões, mostrando suas principais características.

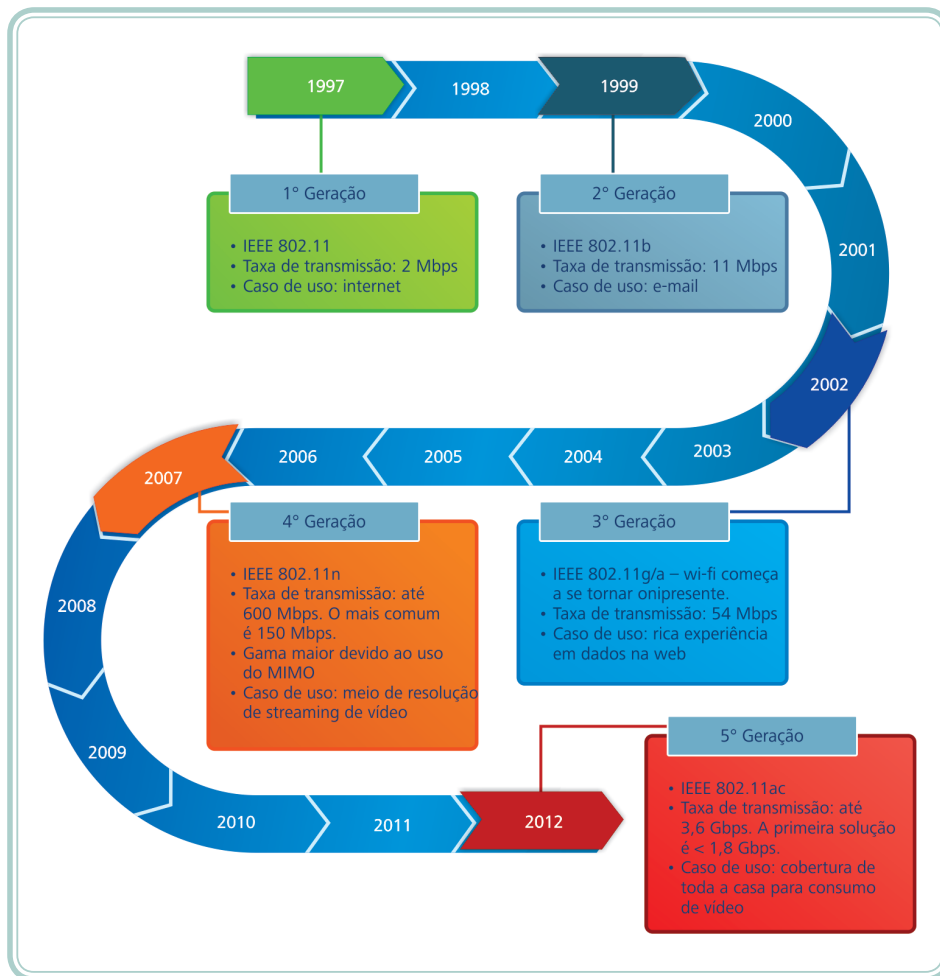


Figura 5.14: Evolução dos padrões de rede sem-fio e suas características

Fonte: CTISM, adaptado de <http://www.dltec.com.br/blog/wp-content/uploads/2012/07/evolu%C3%A7%C3%A3o-do-wifi.png>

5.3.4 Infravermelho

O infravermelho também conhecido como IrDA (*Infrared Data Association*) refere-se a associação de fabricantes criadores do padrão, utilizado comumente em *notebooks*, computadores, impressoras, telefones celulares, entre outros dispositivos.

A comunicação sem-fios, através de infravermelho, faz utilização de sinais de luz, emitidos por um LED (enviados pelo emissor) e captados por um sensor, por parte do receptor.

Esta tecnologia de comunicação tem como características:

- Interface de baixo custo para utilização.
- Capacidade limitada de transmissão (dependendo da versão).

- Capaz de cobrir pequenas distâncias.
- Necessidade de um dispositivo estar diretamente direcionado ao outro dispositivo para início da comunicação.

Quanto à forma de comunicação via infravermelho, tem-se basicamente duas:

- **Comunicação direta** – neste caso, os dispositivos que irão se comunicar devem estar direcionados diretamente um para outro em uma distância curta, para que seja possível a comunicação entre os mesmos.
- **Comunicação difusa** – não existe a necessidade dos dispositivos, a se comunicar, estarem devidamente alinhados (um apontando para o outro), porém, neste caso, a taxa de transmissão é menor e a distância de comunicação entre os dispositivos também diminui.



Importante

Dispositivos que já vem de fábrica com suporte para a utilização do infravermelho, possuem o barramento IrDA incorporado no próprio dispositivo (*notebooks*, telefones, etc.). Demais dispositivos que necessitam deste tipo de comunicação, faz-se necessário a instalação de um transmissor/receptor de infravermelho, que pode ser feita através da conexão em uma porta USB, por exemplo, ou diretamente em um conector da placa-mãe (MORIMOTO, 2005).

Resumo

Nesse capítulo, foi possível conhecer os principais meios de comunicação utilizados nas redes de computadores. Entre eles foram apresentados os cabeamentos metálicos e de fibra óptica, além dos meios de comunicação sem-fio (rádio, Bluetooth, Wi-Fi) importantes na estruturação física de uma rede de computadores.



Atividades de aprendizagem

1. Quais são os principais tipos de cabos de par trançado? Quais as diferenças entre eles e em que lugares são indicados para serem utilizados?
2. Qual a sequência de cores de fios que devo utilizar para montar um cabo, utilizando em uma das pontas o padrão EIA 568A e na outra ponta o padrão EIA 568B?

3. Quais as partes compõem um cabo de fibra óptica? Cite e descreva brevemente sobre cada uma delas.
4. Quais são os tipos de fibras ópticas e quais as diferenças entre elas?
5. Cite e explique três categorias do padrão Wi-Fi.

Aula 6 – Equipamentos utilizados nas redes de computadores

Objetivos

Conhecer os principais equipamentos utilizados nas redes de computadores.

Compreender o funcionamento destes equipamentos.

Conhecer as características quanto a utilização e função dos equipamentos principais das redes.

Ter um entendimento dos equipamentos necessários para montar uma rede local de computadores.

6.1 Considerações iniciais

Existem diversos e diferentes tipos de equipamentos que compõem uma rede de computadores. Eles variam desde uma simples placa de rede a roteadores de alto desempenho. A ideia desta aula é apresentar os principais dispositivos utilizados em uma rede de computadores, bem como descrever suas principais características e sua importância no contexto das redes de computadores.

6.2 Placas de rede

As placas de rede ou interfaces de rede, também denominadas de NIC (*Network Interface Card*) são a comunicação inicial entre um computador ou *notebook*, por exemplo, e os demais dispositivos da rede (*switch*, *hub*, ponto de acesso, etc.), permitindo que este dispositivo conecte-se a outro na rede.

As placas de rede podem ser *on-board*, neste caso já vem integradas ao computador em questão, ou *off-board*, neste caso são placas vendidas separadamente que são encaixadas na placa mãe do computador (*slots*).

Basicamente o que uma placa de rede faz é transmitir e receber dados através da rede. Entre suas principais funções estão: gerar sinais que são captados na rede e controlar o fluxo de dados.



As placas de rede utilizam sinais elétricos para transmitir dados através do cabeamento metálico e sinais luminosos quando transmitem dados por fibras ópticas. Já no caso das placas de rede sem-fio os dados são transmitidos através de ondas eletromagnéticas para outros dispositivos sem-fio.

Ao adquirir uma placa de rede, algumas considerações devem ser analisadas, tais como:

- Esta placa será utilizada para rede cabeada? Rede *wireless*? Para cada tipo de rede necessita-se de um determinado tipo de placa.
- Tipo de barramento: Qual o barramento que esta placa utiliza? PCI, PCI-Express? Outro?
- Qual o tipo de conector necessário para esta placa? RJ, LC, ST?
- Qual a taxa de transmissão da rede (dados os equipamentos que a mesma possui)? 10 Mbps, 100 Mbps, 1 Gbps, 10 Gbps?

Ao responder estas perguntas, é possível conhecer melhor a rede e adquirir, de forma correta, a placa de rede necessária para utilização.

Na Figura 6.1 é possível visualizar um exemplo de placa de rede *wireless*, disponível no mercado.

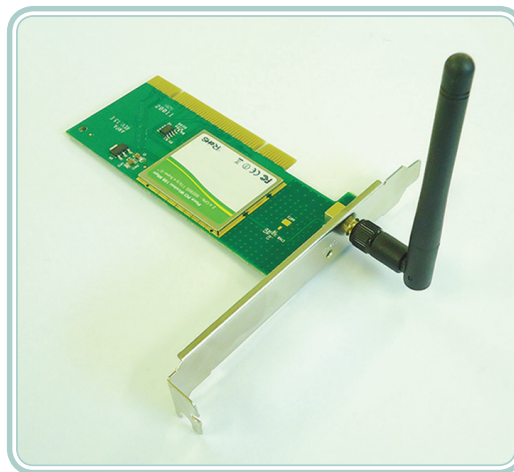


Figura 6.1: Placa de rede wireless

Fonte: CTISM

6.3 Hub

Um *hub* ou concentrador é um dispositivo de rede que como o próprio nome já diz, centraliza os dados que trafegam pela rede. Sua função principal em uma rede é receber o sinal de um dos computadores ligados a ele e difundir este sinal para todos os outros computadores da rede, para que os dados possam ser recebidos pelo computador de destino.

Um *hub* é composto por portas. As portas são as entradas neste *hub* para conexão dos cabos de rede, permitindo desta forma que todos os computadores se comuniquem entre si. Um *hub* pode ter 4, 8, 16, 24, 36, 48 portas ou mais, dependendo do modelo e fabricante. O *hub* está localizado na camada física do modelo OSI, assim como o repetidor de sinal, dessa forma, muitas vezes denominado de repetidor multiportas.

Quanto aos tipos de concentradores (*hub*), estão:

- **Concentrador ativo** – é composto de repetidores presentes em suas portas o que propicia restaurar a amplitude, o sincronismo e a forma do sinal do concentrador às estações de trabalho (computadores da rede).
- **Concentrador passivo** – dispositivo de rede utilizado como concentrador que possui a metade da distância permitida de interligação (*hub*/computador) que um concentrador ativo. Este tipo de concentrador é aconselhável para dispositivos que possuem uma distribuição dentro do limite aceitável da rede.

Em alguns casos é necessário a interligação de *hubs*, para aumentar o alcance e a quantidade de computadores na mesma rede. Este procedimento é perfeitamente possível (desde que respeitado um limite aceitável de até quatro *hubs* interligados) e é denominado como “cascata” ou “cascateamento”. Existem duas formas básicas de realizar tal procedimento:

- a) Através de um cabo cruzado (também conhecido como crossover) ligados em qualquer porta de cada um dos *hubs*.
- b) Interligação através da porta “*uplink*” de cada *hub*. Neste caso, um cabo direto resolve o problema (PINHEIRO, 2005).

Na Figura 6.2 é apresentado um esquema que demonstra tais procedimentos abordados anteriormente:



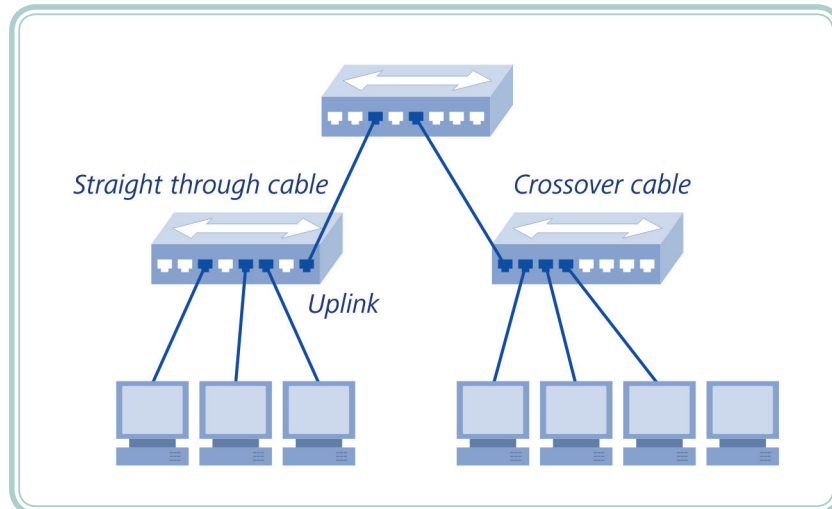


Figura 6.2: Interligação de hubs – forma direta e uplink

Fonte: CTISM

6.4 Switch

Classificado como substituto ao *hub*, o *switch* é um dispositivo de rede que tem o objetivo de interligar os computadores da rede com uma diferença importante com relação ao *hub*. O *switch* recebe um pacote de um computador da rede e entrega diretamente ao computador destino, fazendo uma ligação única entre emissor do pacote e receptor. Já o *hub* conforme visto anteriormente, simplesmente recebe um pacote na rede e distribui a todos os micros da rede para que o destinatário pegue o mesmo, o que gera um grande tráfego na rede.

Através de um *switch* é possível chavear conexões entre os computadores que desejam se comunicar, permitindo que diversos computadores conversem entre si ao mesmo tempo (algo impossível com um *hub*), além de aumentar a taxa de transmissão da rede.



Figura 6.3: Exemplo de um switch de 24 portas

Fonte: CTISM

Um *switch* pode ter diversas portas (8, 24, 48, etc.) assim como um *hub*. Definido como um elemento ativo de rede, trabalha na camada 2 (enlace) do modelo OSI.

6.5 Gateway

Um *gateway* de rede é um dispositivo que permite a comunicação entre redes. De um modo genérico podemos classificar os *gateways* em dois tipos: os *gateways* conversores de meio e os tradutores de protocolos. Os *gateways* conversores de meio são os mais simples. Como funções básicas estão: receber um pacote do nível inferior, tratá-lo (ler cabeçalho, descobrir roteamento, construir um novo pacote inter-redes) e enviá-lo ao destino.

Já os *gateways* tradutores de protocolos ou *gateways* de aplicação, basicamente traduzem mensagens de uma rede para outra rede, como, por exemplo, converter *e-mails* em mensagens de texto para *smartphones*.

De forma geral, um *gateway* pode ser visto como um dispositivo complexo para conexão de redes que combina diferentes funções de pontes, roteadores e repetidores, possibilitando desta forma a interligação de redes distintas. O *gateway* trabalha na camada de transporte do modelo de referência OSI.

6.6 Roteador

Trata-se de um dispositivo de rede semelhante a um *hub* ou *switch* (com as mesmas funções), além de possuir a função de interligar diferentes redes de computadores (independente da quantidade e das distâncias destas redes). São características de um roteador:

- Escolher o melhor caminho para um pacote chegar até o computador destino.
- Escolher o caminho mais curto ou com menor tráfego para encaminhar pacotes.
- Interligar redes diferentes.
- Trabalhar na camada de rede do modelo de referência OSI.

Existem basicamente dois tipos de roteadores: estáticos e dinâmicos.

- **Roteadores estáticos** – escolhem entre os caminhos disponíveis para enviar um pacote, o menor caminho possível, porém, não verificam se este caminho está mais ou menos congestionado do que outro, por exemplo.
- **Roteadores dinâmicos** – estes sim verificam o melhor caminho disponível para tráfego dos dados na rede. Dessa forma, pode-se escolher, por exemplo, um caminho livre mais longo para comunicação ou um caminho mais curto congestionado.

Os roteadores em sua origem trabalham baseados nas tabelas de roteamento. Esta tabela é consultada pelo roteador, toda a vez que um pacote chega a ele, como forma de verificar a existência de um caminho para destinar este pacote e assim realizar o seu trabalho de roteamento (rota que o pacote deve seguir). Quanto aos tipos de roteamento tem-se basicamente dois: roteamento estático e dinâmico:

- **Roteamento estático** – neste tipo de roteamento a tabela de roteamento é criada manualmente (pela inserção de comandos), ou seja, o administrador da rede insere as rotas possíveis que o pacote pode seguir, o que se torna viável apenas para pequenas redes.
- **Roteamento dinâmico** – neste caso a tabela de roteamento é criada dinamicamente. Isto é possível pelo fato dos roteadores se comunicarem constantemente, através de protocolos para atualização de suas tabelas o que se torna viável para redes grandes, como a internet (SILVA, 2010).

6.7 Bridges

As *bridges*, também conhecidas como pontes, são dispositivos com o objetivo de segmentar uma rede em várias sub-redes, diminuindo o tráfego de dados. Como função principal de uma *bridge* está o fluxo de pacotes entre segmentos de uma rede local. Por exemplo, se uma estação envia um sinal somente os computadores que estão no mesmo segmento recebem este sinal. Somente quando o destino está em outro segmento de rede é permitida a passagem do sinal, o que torna o papel da *bridge* de fundamental importância no contexto das redes de computadores.

Apesar de uma função semelhante ao de um repetidor, as *bridges* se diferem no fato de trabalhar com pacotes ao invés de sinais elétricos. Desta forma, não retransmitem frames mal formados ou com erros, pelo contrário, é necessário que o pacote esteja apto para então ser retransmitido por uma *bridge*.

Uma *bridge* trabalha nas camadas 1 e 2 (física e enlace) do modelo de referência OSI (PINHEIRO, 2005).

6.8 Transceiver

A função básica de um transceiver é transformar sinais ópticos (recebidos pelo cabo) em sinais elétricos (enviados ao *switch*) e vice-versa. Geralmente um transceiver tem um preço elevado se comparado com outros dispositivos de rede, porém é a solução dos problemas em muitos casos.

Outra característica importante a ser frisada é que *switchs gigabit*, incorporam (em sua grande maioria) duas, quatro ou mais portas para *transceivers*, o que faz do *switch* (quando necessário) uma utilização como *bridge*, unindo segmentos de par trançado e fibra óptica, formando uma única rede (MORIMOTO, 2008a).

6.9 Repetidores de sinal

Um repetidor de sinal, do inglês *repeater*, é um equipamento de rede, que permite aumentar um sinal, entre dispositivos da rede, com o propósito de aumentar a distância de uma rede (seja ela cabeada ou *wireless*). O repetidor de sinal, trabalha na camada 1 do modelo OSI (camada física), isso quer dizer que seu papel é simplesmente amplificar o sinal em nível binário, mas não interpretar os pacotes que por ali trafegam.

O propósito de sua utilização está no fato de que, em uma transmissão, o sinal enfraquece e sofre distorções, conforme a distância entre os dispositivos conectados. Esta distância é limitada (por exemplo, centenas de metros numa rede local), fazendo com que seja necessária a utilização de um repetidor de sinal, para que a comunicação seja efetivada, onde os limites locais já foram ultrapassados.

Como exemplo de utilização de um repetidor de sinal estão:

- Ligar dois segmentos de redes distintos, como por exemplo, um segmento de rede do tipo par trançado com um segmento do tipo fibra óptica.
- Amplificar as ondas eletromagnéticas oriundas de uma rede *wireless* (neste caso, fazendo com que um ponto de acesso tenha seu sinal amplificado para cobrir uma área maior).

Na Figura 6.4, é possível visualizar um modelo de repetidor *wireless*.



Figura 6.4: Exemplo de repetidor de sinal *wireless*

Fonte: CTISM

Resumo

Nessa aula foram apresentados os principais equipamentos utilizados nas redes de computadores. Como forma de entendê-los melhor, foi descrito como cada um funciona, suas características e importância na utilização em uma rede de computadores.



Atividades de aprendizagem

1. Para que serve e qual a função de uma placa de rede? Quais são os tipos mais usuais encontrados no mercado?
2. Qual a diferença entre um *hub* e um *switch*? Ainda, é possível interligar redes locais com estes equipamentos? Explique.
3. Qual a diferença entre um *gateway* e um roteador?
4. O que é roteamento? Quais as diferenças entre roteamento estático e dinâmico?
5. O que faz um repetidor de sinal e como funciona?

Aula 7 – Redes locais na prática

Objetivos

Aprender a crimpar um cabo de rede do tipo par trançado utilizando os padrões estudados em aulas anteriores.

Conhecer os equipamentos básicos necessários para montar uma rede local de computadores.

Configurar e testar o funcionamento de uma rede local básica.

7.1 Considerações iniciais

Nessa aula iremos aprender de maneira prática, através de dois estudos de caso, como devemos preparar os cabos metálicos e posteriormente como montamos, configuramos e testamos uma rede local de computadores.

7.1.1 Estudo de caso 1: montar um cabo de rede do tipo par trançado

Neste estudo de caso vamos montar (também chamado de “crimpar”) um cabo de rede com os devidos conectores RJ-45 (necessários neste processo). Para esse estudo vamos precisar dos seguintes materiais:

- Alguns metros de cabos de rede metálicos do tipo par trançado, CAT5 ou CAT6.
- Vários conectores do tipo RJ-45.
- Um alicate de crimpar.
- Um testador de cabos.

Com os cabos colocados no local desejado, vamos seguir os seguintes passos:

- a) Corte o cabo de rede com o alicate no comprimento desejado (para essa atividade aproximadamente 1,5 metros). Uma dica é sempre deixar alguns

centímetros a mais além do tamanho desejado, para os casos em que precisar refazer as pontas.

- b) Em cada uma das duas pontas do cabo, retire cerca de dois centímetros da capa externa de isolamento do cabo. Para essa tarefa use o compartimento adequado no alicate de crimpar, pressionando levemente contra o cabo e girando. Tome muito cuidado para não cortar os fios internos do cabo. Se acontecer de cortar alguns dos fios, descarte a parte danificada e repita este passo.
- c) Desenrole totalmente os oito fios (quatro pares) nas pontas desencapadas do cabo. Deixe os fios totalmente lisos para facilitar a inserção no conector. Escolha a sequência de cores desejada e organize os fios um do lado do outro conforme o esquema de cores. Você poderá usar qualquer um esquema de cores, o T568A ou o T568B, porém, deverá usar o mesmo esquema nas duas pontas do cabo, pois estamos construindo um cabo direto. Caso desejássemos confeccionar um cabo do tipo *crossover* usaríamos um esquema de cores diferente em cada ponta do cabo. Veja na Figura 7.1, a ordem das cores dos fios, conforme o padrão T568A ou T568B.

EIA/TIA T568A			EIA/TIA T568B		
Pino	Cor		Pino	Cor	
1	Branco e verde		1	Branco e laranja	
2	Verde		2	Laranja	
3	Branco e laranja		3	Branco e verde	
4	Azul		4	Azul	
5	Branco e azul		5	Branco e azul	
6	Laranja		6	Verde	
7	Branco e marron		7	Branco e marron	
8	Marron		8	Marron	

Figura 7.1: Esquemas de cores dos pares de fios nos padrões T568A e T568B para cabos de par trançado

Fonte: CTISM

- d) Mantendo todos os fios nas suas posições corretas conforme o esquema escolhido, segure firmemente os fios com os dedos. Usando o espaço correto (lâmina de corte) do alicate de crimpar, com cuidado, corte a ponta de todos os fios de uma única vez, na distância de um centímetro da posição onde foi desencapado o cabo. Os fios cortados devem ficar todos alinhados após o corte para facilitar a colocação no conector.

- e) Segure firme com os dedos os fios alinhados e insira-os cuidadosamente no conector. Todos os fios devem chegar até a porção final do conector, nas suas posições corretas. Se algum dos fios não for inserido corretamente no conector, repita os passos anteriores. Veja o alinhamento correto dos fios na Figura 7.2.

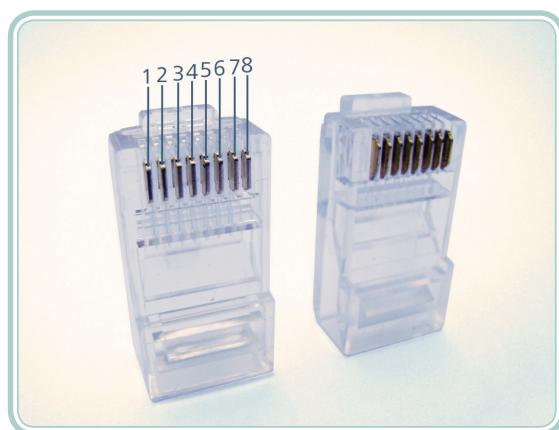


Figura 7.2: Conector RJ-45

Fonte: CTISM

- f) Insira o conector no compartimento adequado no alicate de crimpar. Tome cuidado para que os fios não saiam das suas posições. É importante que uma parte da capa externa do cabo também entre do conector. Verifique se todos os fios estão chegando até o final do conector e com força, aperte o alicate. Tome cuidado apenas para não quebrar o conector.
- g) Após repetir os passos para as duas pontas do cabo é hora de testar o cabo criado. Para o teste utilize um testador de cabos. Os testadores possuem pelo menos duas portas RJ-45 (*jacks*), normalmente em módulos separados, para a colocação de cada ponta (conector) do cabo. Coloque as pontas do cabo nas portas do testador e acione o procedimento de teste. O testador vai informar (por meio de leds indicativos ou por um sinal sonoro) se o cabo foi aprovado ou não no teste. Caso o cabo não tenha passado no teste, corte o conector com defeito e repita todo o processo.

7.1.2 Estudo de caso 2: montar e configurar uma rede local básica

Nesta atividade vamos montar uma pequena rede de computadores usando cabos metálicos de par trançado. Vamos usar os seguintes materiais:

- Um mínimo de dois computadores do tipo PC (*Personal Computer*) com configuração básica, com o SO (Sistema Operacional) devidamente instalado. Para esta atividade podemos usar o SO Windows 7 ou o Ubuntu Linux.

- Um concentrador de rede que pode ser um *hub* ou um *switch*.
- Cabos de rede UTP CAT5 ou CAT6.

Para montar a rede vamos seguir os passos:

- a) Primeiramente, vamos lançar os cabos ligando todos os computadores até o *hub* ou *switch* de rede. Vamos usar uma topologia de rede do tipo estrela, com o *hub* ou *switch* no centro, conforme a Figura 7.3.

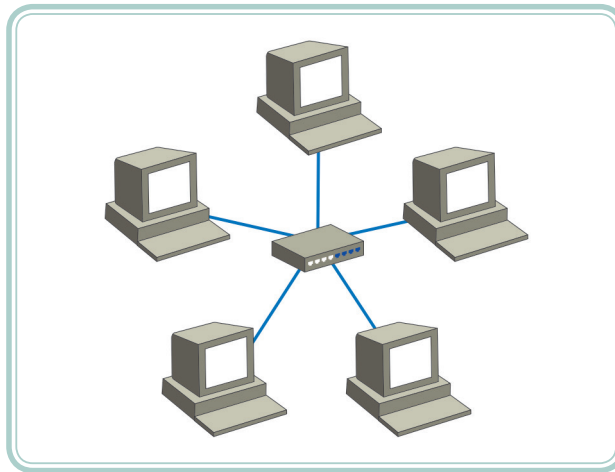


Figura 7.3: Topologia de rede em estrela

Fonte: CTISM

- b) Faça todas as conexões (crimpar) nas pontas dos cabos, conforme aprendemos no estudo anterior.
- c) Com os cabos de rede já com seus conectores RJ-45, ligue-os todos nos computadores e no *hub* ou *switch*. Ligue todos os computadores e equipamentos de rede. Verifique se os leds indicativos nas placas de rede dos computadores e nas portas do *hub* ou *switch* estão acesos. Caso o led indicativo de alguma porta não acender, verifique possíveis problemas de cabos mal conectados ou problemas no cabo. Use o testador de cabos para encontrar cabos com defeito.
- d) Agora vamos escolher uma faixa de endereços IP para atribuir a cada computador. Reveja a aula que trata do endereçamento IPv4, principalmente a seção que trata de endereços de rede privadas. Para esse estudo vamos usar a faixa de endereços 192.0.2.0/24. Atribua manualmente o endereço 192.0.2.1, máscara 255.255.255.0, para o primeiro computador, o endereço 192.0.2.2, máscara 255.255.255.0 para o segundo computador e assim para os demais computadores.

e) Para a configuração da rede:

- No SO Windows 7, abra o “Painel de Controle”, após “Rede e Internet”, procure e abra o item “Conexões de Rede”. Encontre o ícone com a descrição “Conexão Local” e abra as suas propriedades (clique com o botão direito do *mouse* sobre o ícone e selecione “Propriedades”). Caso o computador possua mais de uma porta de rede, haverá mais de um ícone para rede local (“Rede local 2”), neste caso deve-se encontrar a conexão correspondente à porta que está sendo usada (o Windows indica as conexões que estão ativas ou desconectadas). Selecione o item “Protocolo TCP/IP versão 4” e clique em “Propriedades”. Na janela que se abriu, atribua o endereço IP e a máscara de rede para o computador, veja a Figura 7.4. Os demais campos (*gateway*, DNS) não precisam ser configurados para este estudo específico.

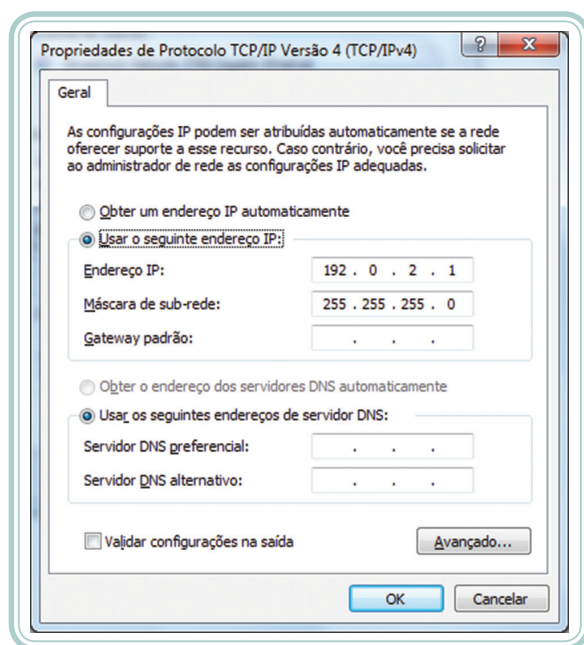


Figura 7.4: Configuração de endereço IPv4 no Windows 7

Fonte: Windows 7

- No Ubuntu Linux, vamos editar o arquivo: `/etc/network/interfaces`. Abra o terminal e digite o comando para editar o arquivo de configuração:

`nano/etc/network/interfaces`

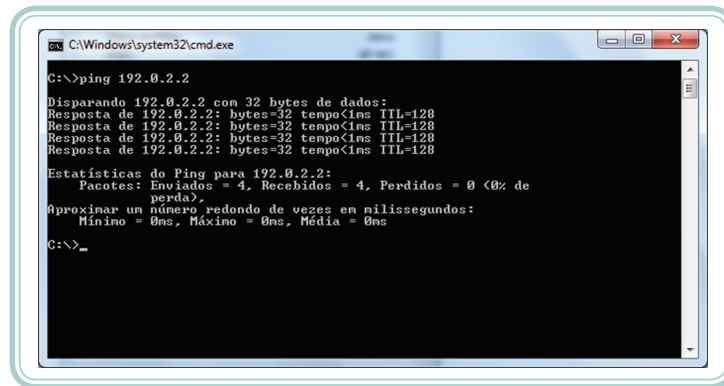
Edite o arquivo, substituindo as linhas que forem necessárias. Após a edição, o arquivo deverá ter as seguintes configurações:

```
auto eth0
iface eth0 inet static
address 192.168.1.10
netmask 255.255.255.0
```

f) Agora vamos testar a comunicação de rede entre nossos computadores.

Para testar a conectividade de rede vamos usar o utilitário ping. O ping envia um pacote para o endereço IP passado com parâmetro e espera por uma resposta, exibindo estatísticas de pacotes enviados e pacotes recebidos (respostas).

No primeiro computador vamos “pingar” (disparar pacotes com o utilitário ping) para o segundo computador, Figura 7.5.



```
C:\Windows\system32\cmd.exe
C:\>ping 192.0.2.2
Disparando 192.0.2.2 com 32 bytes de dados:
Resposta de 192.0.2.2: bytes=32 tempo<ms TTL=128
Resposta de 192.0.2.2: bytes=32 tempo<ms TTL=128
Resposta de 192.0.2.2: bytes=32 tempo<ms TTL=128
Resposta de 192.0.2.2: bytes=32 tempo<ms TTL=128

Estatísticas do Ping para 192.0.2.2:
    Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (0% de
    perda),
    Aproximar um número redondo de vezes em milissegundos:
    Mínimo = 0ms, Máximo = 0ms, Média = 0ms

C:\>_
```

Figura 7.5: Teste de rede usando utilitário ping

Fonte: Windows 7

Caso os testes com o ping falharem, vamos procurar pelos problemas de conexão. Verifique se todos os cabos estão conectados e se os leds indicativos estão acesos. Verifique se os endereços IP atribuídos em cada computador estão corretos. Se o problema persistir, verifique possíveis problemas de configuração do SO e *drivers* das placas de rede.

Resumo

Nessa aula foram apresentados os procedimentos básicos para crimpar um cabo metálico de rede, bem como montar e configurar uma rede local básica de computadores. É importante lembrar que os procedimentos presentes nessa aula devem ser feitos de forma prática para que os conhecimentos acumulados nesta e nas aulas anteriores, sejam efetivamente praticados.

Atividades de aprendizagem



1. Quais são as cores (sequência de fios) para os padrões 568A e 568B que devem ser configurados ao crimpar um cabo de rede do tipo:
 - a) Cabo direto
 - b) Cabo *crossover*
2. Quais equipamentos seriam necessário para montar uma rede local básica com três computadores se comunicando entre si?
3. Para esta mesma rede citada acima no exercício 2, quais deveriam ser as configurações para cada um dos três computadores a fim de que possam se comunicar entre si, para os seguintes itens:
 - a) Endereço IP
 - b) Máscara de rede
 - c) *Gateway* padrão
4. Procure e informe o que fazem e para que servem os seguintes comandos:
 - a) ipconfig
 - b) ping
 - c) tracert
 - d) nslookup
 - e) netstat

Referências

ALECRIM, Emerson. **Diferenças entre hub, switch e roteador**. Info Wester. [Online] 08 nov. 2004. Disponível em: <<http://www.infowester.com/hubswitchrouter.php>>. Acesso em: 14 fev. 2013.

_____. **O que é Wi-Fi (IEEE 802.11)?**. Info Wester. [Online] 19 mar. 2008a. Disponível em: <<http://www.infowester.com/wifi.php>>. Acesso em: 05 mar. 2013.

_____. **Tecnologia Bluetooth: o que é e como funciona?** Info Wester. [Online] 30 jan. 2008b. Disponível em: <<http://www.infowester.com/bluetooth.php>>. Acesso em: 03 mar. 2013.

COMER, Douglas E. **Redes de computadores e internet**. Porto Alegre: Bookman, 2007. 85-60031367.

DAVIE, Larry L. Peterson; BRUCE, S. **Redes de computadores: uma abordagem de sistemas**. Rio de Janeiro: Campus, 2004. 8535213805.

KUROSE, Keith W. Ross; JAMES F. **Redes de computadores e a internet: uma abordagem top-down**. [S.l.]: Addison-Wesley, 2010. 8588639971.

MENDES, Douglas Rocha. **Redes de computadores – Teoria e prática**. São Paulo: Novatec, 2007. 9788575221273.

MORAES, Alexandre Fernandes de; CIRONE, Antonio Carlos. **Redes de computadores – Da Ethernet a internet**. São Paulo: [s.n.], 2003. 8571949573.

MORIMOTO, Carlos Eduardo. **Faixas de endereços IP, CIDR e máscaras de tamanho variável**. Guia do Hardware. [Online] 26 set. 2007. Disponível em: <<http://www.hardware.com.br/tutoriais/endereco-ip-cidr/pagina2.html>>. Acesso em: 25 fev. 2013.

_____. **IrDA**. Guia do hardware. [Online] 26 jun. 2005. Disponível em: <<http://www.hardware.com.br/termos/irda>>. Acesso em: 07 mar. 2013.

_____. **Redes, guia prático**. 2. ed. Guia do hardware. [Online] 01 abr. 2008a. Disponível em: <<http://www.hardware.com.br/livros/redes/categorias-cabos.html>>. Acesso em: 07 mar. 2013.

_____. **Servidores Linux, guia prático**. Guia do Hardware. [Online] 01 ago. 2008b. Disponível em: <<http://www.hardware.com.br/livros/servidores-linux/>>. Acesso em: 20 fev. 2013.

PINHEIRO, José Maurício dos Santos. **Equipamentos para redes – 2ª parte**. Projeto de redes. [Online] 11 fev. 2005. Disponível em: <http://www.projetedoredes.com.br/tutoriais/tutorial_equipamentos_de_redes_02.php>. Acesso em: 09 mar. 2013.

SCRIMGER, Rob. **TCP/IP a bíblia**. Rio de Janeiro: Campus, 2001. 8535209220.

SILVA, Camila Ceccato da. **Redes de computadores** – Conceito e prática. Santa Cruz do Rio Pardo-SP: Viena, 2010.

SOARES, Luís Fernando; LEMOS, Guido; COLCHER, Sérgio. **Redes de computadores**: das LANs, MANs e WANs às redes ATM. Rio de Janeiro: Campus, 1995. 9788570019981.

TANENBAUM, Andrew S. **Redes de computadores**. São Paulo: Campus, 2003. 8535211853.

TORRES, Gabriel. **Redes de computadores**. [S.l.]: Nova Terra, 2009. 9788561893057.

TYSON, Jeff. **Como funcionam os switches LAN** (rede de comunicação local). Como Tudo Funciona. [Online] 23 maio 2009. Disponível em: <<http://informatica.hsw.uol.com.br/lan-switch1.htm>>. Acesso em: 21 fev. 2013.

Currículo do professor-autor



Roberto Franciscatto é natural de Frederico Westphalen -RS. Graduado em Informática pela URI-FW (Universidade Regional Integrada do Alto Uruguai e das Missões campus de Frederico Westphalen) e Mestre em Computação Aplicada pela UNISINOS-RS (Universidade do Vale do Rio dos Sinos). Atualmente é professor em regime de dedicação exclusiva da Universidade Federal de Santa Maria, lotado no Colégio Agrícola de Frederico Westphalen. Atua nos cursos: Técnico em Informática, Graduação Tecnológica em Sistemas para Internet e Especialização em Gestão de Tecnologia da Informação. Atua principalmente nos seguintes temas: sistemas operacionais, segurança da informação, projeto e instalação de servidores, redes de computadores e desenvolvimento de aplicativos para dispositivos móveis.



Fernando de Cristo possui graduação em Informática pela Universidade Regional Integrada do Alto Uruguai e das Missões (URI) e mestrado em Engenharia de Produção na área de Tecnologia da Informação pela Universidade Federal de Santa Maria (UFSM). Atualmente, é avaliador do Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (INEP) e professor da Universidade Federal de Santa Maria (UFSM). Tem experiência na área de Automação, Robótica e Otimização Combinatória com ênfase em Heurísticas e Metaheurísticas. Atua principalmente nos seguintes temas: suporte ao usuário, redes de computadores, manutenção de computadores, instalação de *software* e configuração de periféricos.



Tiago Perlin é natural de Pejuçara -RS, possui graduação em Ciência da Computação, pela Universidade de Cruz Alta -RS (Unicruz) e possui mestrado em Computação pela Universidade Federal de Santa Maria (UFSM). Atualmente é Analista de Tecnologia da Informação na Universidade Federal de Santa Maria (UFSM). Possui experiência em: redes de computadores, sistemas distribuídos, segurança em redes de computadores. Tem interesse nos temas: segurança da informação, detecção de intrusão, tolerância a falhas.