

Conceitos e Infraestrutura de Redes (online)

Créditos

2

Copyright © TechnoEdition Editora Ltda.

Todos os direitos autorais reservados. Este material de estudo (textos, imagens, áudios e vídeos) não pode ser copiado, reproduzido, traduzido, baixado ou convertido em qualquer outra forma eletrônica, digital ou impressa, ou legível por qualquer meio, em parte ou no todo, sem a aprovação prévia, por escrito, da TechnoEdition Editora Ltda., estando o contrafator sujeito a responder por crime de Violação de Direito Autoral, conforme o art.184 do Código Penal Brasileiro, além de responder por Perdas e Danos. Todos os logotipos e marcas utilizados neste material pertencem às suas respectivas empresas.

"As marcas registradas e os nomes comerciais citados nesta obra, mesmo que não sejam assim identificados, pertencem aos seus respectivos proprietários nos termos das leis, convenções e diretrizes nacionais e internacionais."

Conceitos e Infraestrutura de Redes (online)

Coordenação Geral

Marcia M. Rosa

Coordenação Editorial

Henrique Thomaz Bruscagin

Supervisão de Desenvolvimento Digital

Alexandre Hideki Chicaoka

Produção, Gravação, Edição de Vídeo e Finalização

Bruno de Oliveira Santos

Xandros Luiz de Oliveira Almeida (Impacta Produtora)

Roteirização

Alvaro Salgueiro Monteiro

Aula ministrada por

Alvaro Salgueiro Monteiro

Edição e Revisão final

Alexandre Hideki Chicaoka

Fernanda Monteiro Laneri

Marcos César dos Santos Silva

Luiz Fernando Oliveira

Diagramação

Bruno de Oliveira Santos

Carla Cristina de Souza

Edição nº 1 | 1684/1_EAD
agosto/2014

*Este material é uma nova obra derivada da seguinte obra original, produzida por TechnoEdition Editora Ltda., em Mar/2014: Conceitos e Infraestrutura de Redes
Autoria: Nilson Acacio Ramalho
Nº de registro BN: 664260*

Sobre o instrutor do curso:

Alvaro Salgueiro Monteiro possui formação nas áreas de engenharia eletrônica e física, é consultor em redes, especialista em infraestrutura de redes e telecomunicações e ministra treinamentos na divisão de redes da Impacta Certificação e Treinamento desde 2001. Também é palestrante e autor de artigos e material didático sobre cabeamento estruturado.

Apresentação	08
1. História das redes de computadores	09
1.1. Introdução	10
1.2. Evolução dos modelos de serviços de redes	10
1.3. Virtualização	14
1.3.1. Evolução para virtualização	15
1.3.2. Algumas vantagens da virtualização.....	16
1.4. Computação em nuvem (cloud computing).....	17
1.4.1. Conceitos de computação em nuvem	17
1.4.2. Adoção da computação em nuvem	19
1.4.3. Vantagens da computação na nuvem	19
1.4.3.1. Nuvem pública	19
1.4.3.2. Nuvem privada.....	20
1.4.3.3. Nuvem híbrida	20
1.5. Comunicação unificada	20
Teste seus conhecimentos.....	23
2. Redes de Computadores	27
2.1. Introdução	28
2.2. Infraestrutura de rede	29
2.3. Classificação das redes	31
2.4. Redes sem fio	40
2.5. Storage (Armazenamento).....	44
2.6. Internet, intranet e extranet	48
Teste seus conhecimentos.....	49
3. Modelos, topologias e tecnologias de rede	53
3.1. Introdução	54
3.2. Modelos de rede	54
3.2.2.1. Clientes	58
3.2.2.2. Servidores	59
3.3. Topologias de rede	62
3.3.5.1. Barramento-estrela.....	68
3.3.5.2. Anel-estrela.....	69
3.4. Tecnologias de rede	70
3.4.1.1. CSMA / CD	71
3.4.1.2. Entendendo o funcionamento do CSMA/CD.....	71
Teste seus conhecimentos.....	75

Conceitos e Infraestrutura de Redes (online)

4

4.	Transmissão de dados	79
4.1.	Introdução	80
4.2.	Vias de transmissão	80
4.3.	Modos de transmissão	83
4.4.	Sentidos da transmissão	84
4.5.	Tipos de sinais	86
4.5.2.1.	Modulação de dados	88
4.6.	Problemas na transmissão de sinais	88
4.7.	Tipos de banda	89
	Teste seus conhecimentos.....	93
5.	Meios de transmissão	97
5.1.	Introdução	98
5.2.	Cabos metálicos de par trançado	99
5.2.1.	Blindagem	99
5.2.2.	Desempenho dos cabos metálicos de par trançado	102
5.2.3.	Padrões de conectorização	103
5.3.	Cabos ópticos	105
5.3.1.	Classificação dos tipos de fibras ópticas	106
5.3.2.	Desempenho dos cabos de fibra óptica	109
5.4.	Cabos metálicos x Cabos ópticos	110
	Teste seus conhecimentos.....	111
6.	Componentes de expansão da rede	115
6.1.	Conentes de expansão da rede	116
6.2.	Placas de rede	116
6.2.1.	Placa de rede para estação	116
6.2.2.	Placa de rede para servidor	118
6.3.	Conversores de mídia	119
6.4.	Ativos centrais de redes	120
6.4.1.	Hubs	122
6.4.3.1.	Rede híbrida	126
6.4.3.2.	Controle de fluxo	127
	Teste seus conhecimentos.....	131

7.	Tecnologias para acesso remoto	135
7.1.	Introdução	136
7.2.	Conexão por linha analógica	137
7.3.	Conexão por linha digital	137
7.4.	TDM/PCM	138
7.4.3.1.	AwDSL	140
7.5.	Rádio	143
7.6.	Satélite.....	144
7.7.	Acesso móvel.....	145
7.7.1.1.	2G	145
7.7.1.2.	2.5G	146
7.7.1.3.	3G	147
7.7.1.4.	4G	148
	Teste seus conhecimentos.....	151
8.	Redes wireless.....	155
8.1.	Introdução	156
8.2.	Infravermelho	156
8.3.	Laser.....	158
8.4.	Radiofrequência	159
8.4.1.1.	Equipamentos RFID	160
8.4.2.1.	Redes de dispositivos bluetooth.....	161
8.4.3.1.	Padrão 802.11b	162
8.4.3.2.	Padrão 802.11g	163
8.4.3.3.	Padrão 802.11a.....	163
8.4.3.4.	Padrão 802.11n	163
8.4.3.5.	Padrão 802.11ac	163
8.4.3.6.	Equipamentos WLAN	163
8.4.3.7.	Configuração lógica das redes wireless	167
	Teste seus conhecimentos.....	169

Conceitos e Infraestrutura de Redes (online)

6

9.	Protocolos de rede	173
9.1.	Introdução	174
9.2.	Tipos de protocolos	174
9.2.3.	Protocolos roteáveis.....	175
9.3.	Pilhas de protocolos.....	175
9.4.	Modelo OSI	176
9.5.	Protocolos para conexões à distância.....	181
9.5.2.1.	Tunelamento Camada 2 - Enlace.....	182
9.5.2.2.	Tunelamento Camada 3 - Rede.....	182
9.5.2.3.	MPLS	182
	Teste seus conhecimentos.....	183
10.	Conceitos básicos de TCP/IP	189
10.1.	Introdução	190
10.2.	Camadas do protocolo TCP/IP	190
10.2.1.	Camada de aplicação	191
10.2.2.	Camada de transporte.....	191
10.2.3.	Camada da Internet.....	192
10.2.4.	Camada de interface de rede.....	194
10.3.	Analizando o endereço IP	194
10.3.1.	Classes de endereço	194
10.3.2.	Sub-redes.....	197
10.3.2.1.	Máscaras de sub-rede.....	197
10.3.3.	Atribuindo identificação de rede e de host	199
10.3.4.	Determinando host local ou remoto	200
	Teste seus conhecimentos.....	201

11.	Conceitos básicos de IPv6	205
11.1.	Introdução	206
11.2.	Esgotamento do endereço IPv4.....	206
11.3.	Protocolo IPv6	207
11.4.	Endereçamento IPv6.....	209
11.5.	Cabeçalho do protocolo IPv6	213
11.6.	Coexistência dos protocolos IPv4 e IPv6	214
11.7.	Distribuição dos blocos IPv6	217
	Teste seus conhecimentos.....	219
12.	Convergência digital	223
12.1.	Introdução	224
12.2.	Streaming	224
12.3.	VoIP (Voice over IP)	224
12.4.	IPTV e Web TV.....	227
12.5.	CFTV.....	227
	Teste seus conhecimentos.....	229

Apresentação

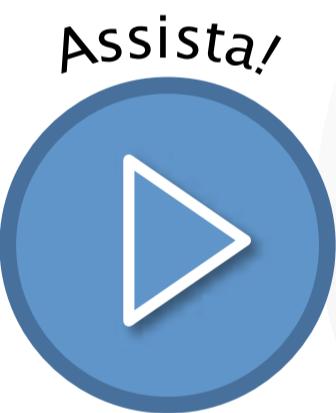
8

Bem-vindo!

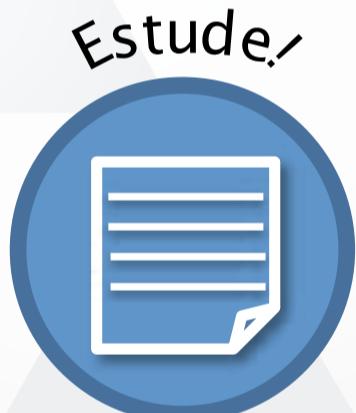
É um prazer tê-lo como aluno do nosso curso online de Conceitos e Infraestrutura de Redes. Este curso é perfeito para você que deseja assimilar os fundamentos e conceitos essenciais envolvidos nas tarefas de implantação e gerenciamento de redes em sistemas operacionais e plataformas específicas. Você verá os tipos, as topologias e as arquiteturas de rede, bem como os componentes e os dispositivos de conectividade de uma rede. Também serão apresentadas informações referentes aos protocolos de rede e às camadas do TCP/IP, entre outras.

Para ter um bom aproveitamento deste curso, é imprescindível que você tenha participado do nosso curso de Ambiente Windows, ou possua conhecimentos equivalentes. Bom aprendizado!

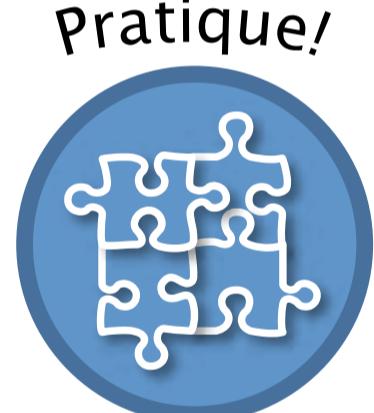
Como estudar?



Assista!



Estude!



Pratique!

Este curso conta com:



Videoaulas sobre os assuntos que você precisa saber no curso online de Conceitos e Infraestrutura de Redes.



Parte teórica, com mais exemplos e detalhes para você que quer se aprofundar no assunto da videoaula.



Exercícios de testes para você pôr à prova o que aprendeu.

História das redes de computadores 1

- ✓ Evolução dos modelos de serviços de redes;
- ✓ Virtualização;
- ✓ Computação em nuvem (cloud computing);
- ✓ Comunicação unificada.

1.1. Introdução

Grandes transformações aconteceram na história das redes de computadores, de tal forma que permitiram avanço significativo e melhorias no modo como as pessoas executavam e ainda executam suas atividades. Com a evolução das redes de computadores, os processos produtivos foram alterados, a velocidade com que as pessoas passaram a fazer seus trabalhos, gerou um aumento quantitativo e qualitativo, elevando os níveis de produção, bem como os resultados financeiros. O começo das redes de computadores aconteceu por volta da década de 1950. Seu tema principal era a rede de comunicação telefônica, e seu objetivo era transmitir voz entre dois pontos, baseando-se em origem e destino.

Tempos mais tarde, viu-se a necessidade da criação de uma rede de dados que teria por objetivo, facilitar a troca de informações entre computadores. Essa rede foi evoluindo juntamente com os computadores, saindo de ambientes restritos, como o militar, o acadêmico e o industrial, para se popularizar em empresas e mais tarde em domicílios. Nessa década, havia o fator do alto custo dos computadores; no entanto, esse quadro evoluiu naturalmente, de modo que foram surgindo computadores menores e cada vez mais baratos, o que potencializou a adoção e rápida assimilação no cenário empresarial e de negócios. Assim, descobriu-se que havia a necessidade de interconectar os computadores para que se pudesse fazer o compartilhamento de recursos, e dados entre diferentes usuários e até mesmo em localizações diferentes. Isso foi resultado natural da grande assimilação que as empresas tiveram do potencial disponível, pois o desenvolvimento dos processos de troca de mensagens e dados entre equipamentos eletrônicos foi de incalculável importância para o desenvolvimento das atividades humanas. O que se iniciou como uma rede de transmissão telefônica local acabou se tornando um serviço de transporte de informações de voz e dados em escala global: a Internet.

Em paralelo ao avanço natural das redes de computadores, os computadores também avançaram desde terminais ligados por meio de cabos a um servidor central até se tornarem dispositivos portáteis como laptops, PDAs, smartphones, telefones celulares, tablets etc., tudo isso ligados a uma rede doméstica, de uma organização ou à Internet, e com armazenamento de dados próprio.

1.2. Evolução dos modelos de serviços de redes

Desde seu advento no meio do século XX, as redes se desenvolveram cada vez mais com o passar dos anos, tendo passado por três fases principais (relacionadas adiante), mas não limitadas a elas.

Tais fases são consideradas como as três gerações da evolução da TI e do modelo de computação:



A partir de agora, vamos ver um pouco mais sobre as principais características de cada fase dessa evolução, como ela tem influenciado a forma de fazer as coisas, o que marcou cada fase e fatores que estão fervilhando no setor de Tecnologia da Informação e Comunicação (TIC), para aumentar a produtividade dos negócios.

- **Modelo de serviços centralizado**



Terminais de mainframe foi o primeiro tipo de rede de troca de dados disponível entre computadores. Consistia em um servidor central e um mainframe, no qual eram ligados diversos terminais, formados por um monitor e um teclado.

Todo o processamento e o armazenamento eram feitos pelo mainframe, de modo centralizado, e os terminais tinham a função apenas de acesso ao servidor, sendo possível que diversos deles se conectassem ao mainframe simultaneamente. Era possível executar todas as operações com grande velocidade e sobre um volume muito grande de dados.

Os mainframes são grandes computadores que, em razão de seu tamanho, ocupavam um considerável espaço e exigiam um ambiente específico e diferenciado para seu funcionamento. No entanto, podemos considerar que, nos dias de hoje, muitas mudanças ocorreram na infraestrutura de mainframe que chega a se comparar com os servidores de hoje, inclusive quanto ao consumo de energia elétrica.

Conceitos e Infraestrutura de Redes (online)

12

No entanto, em sua época, os mainframes surgiram para atender a uma demanda das empresas que precisavam executar tarefas que levavam horas e até dias para serem concluídas. Para solucionar essa questão, foi preciso criar um supercomputador que seria capaz de executar tais tarefas em menor tempo e com mais precisão, elevando a produtividade.

Esse tipo de rede era caro, sendo que apenas grandes corporações tinham condições de possuir uma. Além disso, as conexões de terminais com o mainframe eram feitas localmente, através de cabeamento e remotamente por meio de circuitos de telecomunicações. As principais características desse modelo são:

- Alto custo de hardware;
- Modelo desenhado com capacidade de alta disponibilidade 99.999, baseada em hardware;
- Escalabilidade vertical;
- Concepção de serviços de softwares centralizados;
- Terminais de minicomputadores.

Os minicomputadores tinham a mesma função que o mainframe, porém eram menores e tinham o custo mais baixo, o que possibilitou que empresas menores tivessem condição de dispor de redes desse tipo. Essa rede funciona do mesmo modo que os terminais de mainframe, sendo que os minicomputadores nos quais os terminais se conectam suportam menos usuários simultâneos. As conexões remotas também são feitas por meio de circuitos de telecomunicação, assim como as ligações locais são feitas via cabeamento.

• **Modelo de serviços compartilhado**

Estamos em um processo contínuo de mudança, passando de mainframes para o cliente-servidor, e há uma progressão muito clara a partir de uma para a outra. As redes de computadores no modelo de serviços compartilhados ganham importância, pois as empresas possuem aplicações departamentais que exigem utilização conjunta, a fim de alcançar redução de custo operacional através do compartilhamento de recursos simplificado adotando o uso de correio eletrônico, transferência de arquivos, serviço de impressão para rede, uso de espaço em disco ou mesmo acesso a este a partir de qualquer outro computador sem ter que sair de seu local para copiá-lo, entre outros.

Nesse modelo, as principais características são:

- Desenhado para disponibilidade de 99.9;
 - Escalabilidade vertical/horizontal;
 - Concepção de serviços de softwares descentralizados e compartilhados;
 - Alto consumo de energia, pelo fato de ter seus serviços distribuídos em diversos hardwares.
- **Modelo de serviços baseado no negócio**

Essa é a terceira fase da evolução do modelo das redes de computadores, sendo que, no momento atual, o grande desafio das empresas é simplificar e otimizar a infraestrutura de TI permitindo que seus colaboradores, parceiros e fornecedores colaborem e ofereçam à empresa competitividade no cenário econômico e setor que atuam. Para tanto, é necessário implantar serviços e recursos que potencializem seu sucesso.

Com o grande avanço nas tecnologias de rede e mobilidade, veio também o barateamento dos dispositivos de computação pessoal. Com isso, mais usuários passaram a adotar equipamentos eletrônicos para uso pessoal e profissional. Por outro lado, houve uma elevada necessidade de que as empresas pudessem obter as informações precisas e no tempo certo, de forma que se tornou necessário possuir uma infraestrutura de TI que oferecesse suporte e sustentação às demandas empresariais.



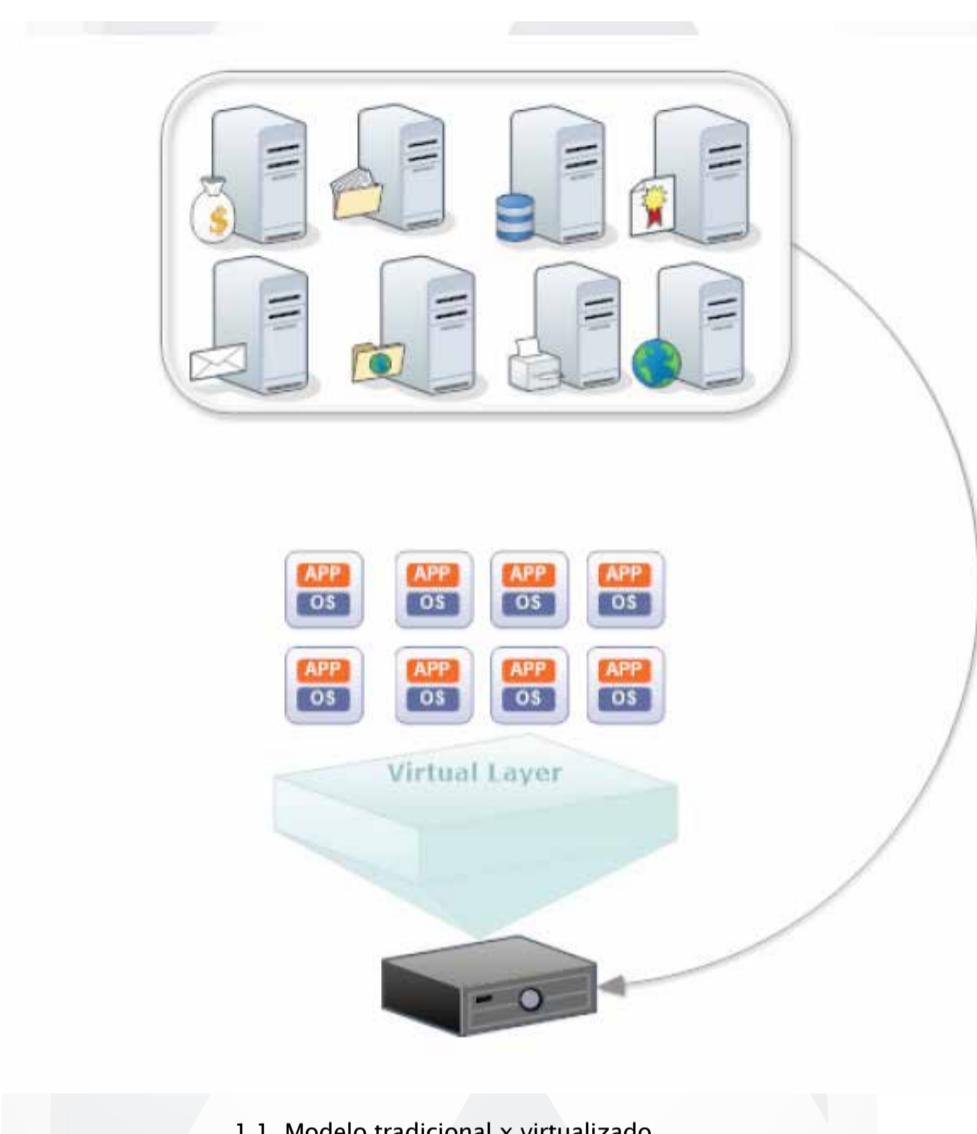
Com o crescente uso da tecnologia na vida das pessoas, a colaboração eleva de forma exponencial a produtividade, enriquecendo os negócios, bem como as tendências globais para a 3^a geração. Um exemplo disso é o **BYOD (Bring Your Own Device)**, que consiste em uma prática na qual o colaborador tem seu próprio dispositivo móvel pessoal e o utiliza para suas funções profissionais com suporte corporativo, ao mesmo tempo em que o utiliza para suas tarefas pessoais e de entretenimento. Compreende, ainda, outras exigências que devem ser garantidas com as redes de computadores de hoje, que são mobilidade e adoção de vídeos para treinamentos corporativos, conferência entre outros.

Uma das características dessa 3^a geração é a oferta de serviços de infraestrutura sob demanda, com capacidade de crescimento como serviço. No passado, havia uma exigência inicial de investimentos elevados em infraestrutura para sua implantação ou ampliação; já atualmente, a contratação de serviços de Cloud Computing permite acesso fácil e escalável com baixo custo de mão de obra e implantação para o cliente. Neste modelo, o cliente paga pelos serviços consumidos, conceito conhecido como pay as you go.

1.3. Virtualização

O conceito sobre virtualização não é novo, no entanto, a tecnologia vem se transformando e amadurecendo de forma significativa. Na década de 1970, o Instituto de Tecnologia de Massachusetts, o MIT, já utilizava o conceito de VMM (Virtual Machine Monitor) com sistema de tempo compartilhado. A VMM roda diretamente sobre o hardware, permitindo a execução de diversas máquinas virtuais, sendo que cada uma possui um sistema operacional diferente.

A adoção da virtualização permite criar várias instâncias do sistema operacional em máquinas virtuais (VM – Virtual Machine) que sejam executadas de forma simultânea em um único servidor de virtualização. Dessa forma, todos os sistemas operacionais que chamamos de guest são gerenciados por uma VM ou pelo hypervisor. Com isso, a virtualização consegue controlar o uso da CPU, da memória e armazenamento dessas VMs convidadas, podendo transferir um sistema operacional de uma VM convidada de uma máquina para outra em caso de indisponibilidade ou quando o ambiente exige escalabilidade para aumento de capacidade.



1.1. Modelo tradicional x virtualizado

1.3.1. Evolução para virtualização

Na história da evolução da TI nas três gerações, pudemos perceber que as mudanças que ocorreram foram significativas e trouxeram desafios quando tratamos de redes de computadores. Nas últimas décadas, o foco foi a descentralização, ou seja, a escalabilidade horizontal. Os serviços e servidores centralizados eram vistos como itens caros de serem adquiridos e mantidos. A partir dessa visão, as aplicações eram transferidas de um grande servidor compartilhado para as suas máquinas físicas.

Uma das razões para a descentralização foi o fato de que não era possível fazer manutenção, aplicar correções, patches de segurança e outras atualizações sem interferir em outros sistemas que estavam sendo executados no mesmo ambiente de produtividade. Além disso, a descentralização contribui com a segurança, pois quando um sistema fica comprometido, ele é isolado dos demais sistemas da rede.

Por outro lado, essa descentralização trouxe aumento do consumo de energia, necessidade de mais espaço físico, sobrecarga de manutenção, número maior de mão de obra especializada, fazendo com que os benefícios elevassem os custos operacionais. Então, com a virtualização, os ganhos são expressivos, pois a implantação centraliza serviços e ao mesmo tempo permite uma separação por meio de VMs mantendo as exigências das aplicações. Dessa forma, em vez de fazer investimentos em vários servidores e prover o gerenciamento e manutenção individual de cada servidor, a implantação permitirá que cada uma das VMs tenha seu próprio sistema operacional e todos esses sistemas podem residir no mesmo hardware, mantendo as vantagens da descentralização e ainda aproveitando melhor todos os recursos da máquina.

1.3.2. Algumas vantagens da virtualização

A principal vantagem está em torno da economia, seja financeira ou de recursos naturais, já que existe uma grande pressão sobre a necessidade de diminuir o desperdício de recursos naturais e sobre o descarte correto dos insumos de TI.

As vantagens são grandes tanto para os usuários como para as empresas que desejam extrair o máximo do desempenho dos servidores com o hardware disponível, a fim de agregar valor ao negócio através da produtividade. Como você pode ver no gráfico, a virtualização permitirá, ao longo do tempo, trazer ótimos resultados, pois vem resolver questões que você não pensava que existissem, com a explosão de novos modelos de equipamentos móveis, usuários cada vez mais remotos e múltiplos sistemas operacionais, ao passo que o conceito de consumerização trará desafios que podem ser atendidos com soluções de virtualização.



A virtualização pode reduzir as despesas operacionais e de capital, e, ainda facilitar a implantação mais rápida de recursos computacionais, facilitando o gerenciamento dos processos de TI e negócios. Veja algumas das vantagens que a virtualização poderá trazer:

- Redução do espaço físico exigido;
- Redução do consumo de energia;
- Melhor gerenciamento e centralização na implantação de servidores com migração rápida;
- Capacidade de escalabilidade e recuperação de desastre;
- Consolidação de servidores e continuidade de negócios;
- Ampla capacidade de suporte a diversos sistemas operacionais;
- Desenvolvimento de testes e compatibilidade de aplicações;
- Melhor aproveitamento os recursos da máquina;
- Redução do custo de hardware;
- Virtualização de servidores, desktop e aplicações.

1.4. Computação em nuvem (cloud computing)

As necessidades de negócios e as tecnologias estão se transformando mais rapidamente do que as empresas podem se adaptar, portanto, uma clara compreensão da computação em nuvem torna-se fundamental para sua assimilação, assim como se torna um fator determinante para realizar um planejamento adequado para adoção das soluções disponíveis com foco em uma implementação segura e aderente em relação às demandas atuais de negócios.

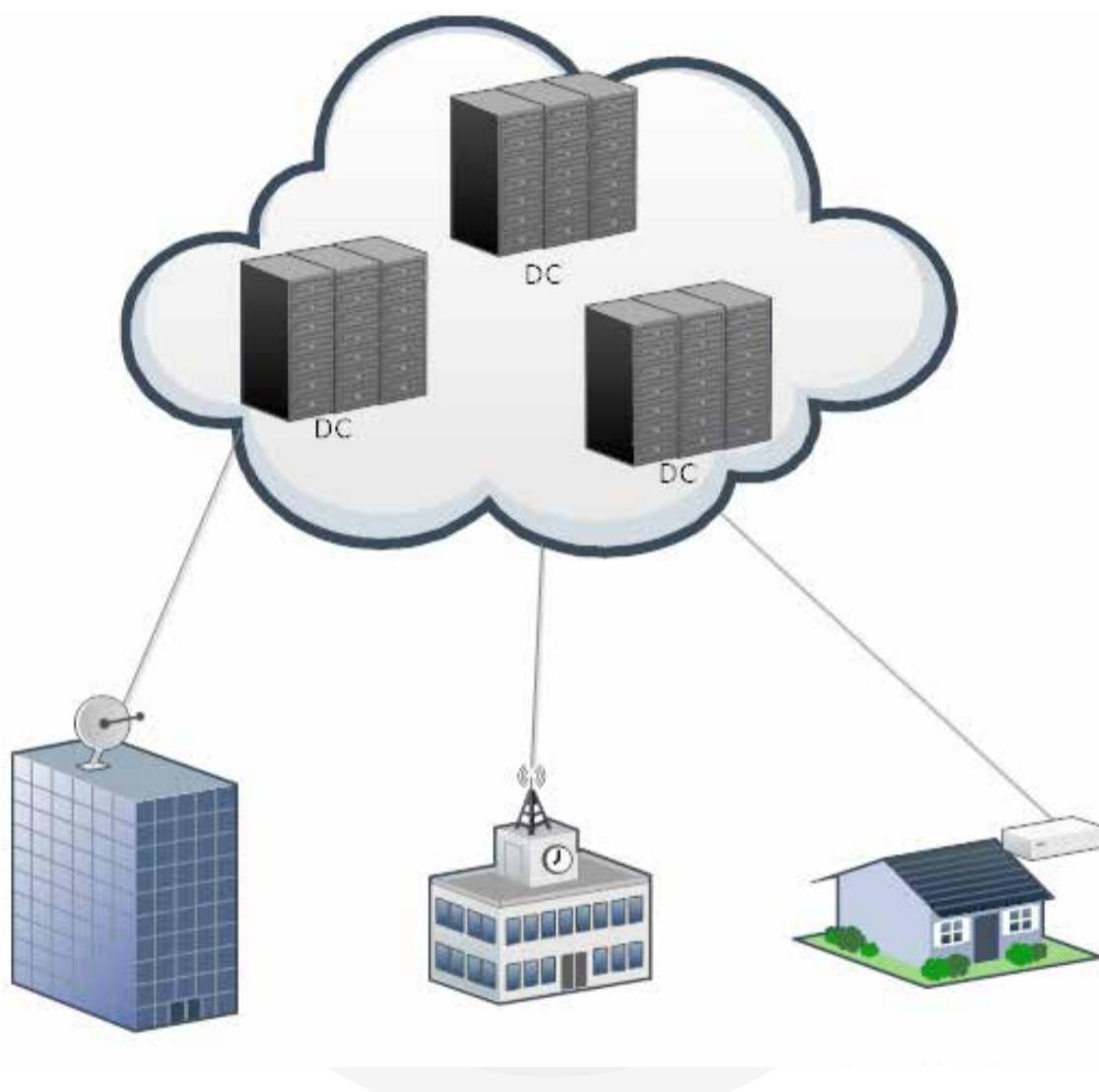
1.4.1. Conceitos de computação em nuvem

O conceito de computação na nuvem vem de cloud computing, que tem por objetivo referenciar-se à ideia de utilizarmos qualquer aplicação em qualquer plataforma ou infraestrutura de TI e em qualquer lugar, sendo tudo acessado por meio da Internet como se estivéssemos acessando em nossos próprios computadores e dispositivos móveis.

Conceitos e Infraestrutura de Redes (online)

18

Normalmente, a instalação de softwares, aplicativos corporativos e arquivos gerados pelos usuários, sejam pessoais ou corporativos, é feita em computadores e servidores locais. Embora, em um ambiente empresarial, seja possível acessar as informações de diversos computadores através da rede local, isso muitas vezes limita o acesso dentro da estrutura de domínio de segurança da rede corporativa, justamente porque esses acessos são locais e não dependem da disponibilidade de acesso à Internet.



Outro fator que temos que considerar é que o custo de hardware, gerenciamento da infraestrutura de TI com mão de obra especializada e de licenças de softwares, em muitos casos, torna-se muito mais elevado em relação a toda a infraestrutura. Por exemplo, empresas com muitos usuários precisam adquirir muitas licenças, sendo uma para cada computador. Com a computação na nuvem, os usuários, independente da plataforma, sistema operacional e de ter ou não aplicativo instalado em seus computadores, poderão obter acesso a diversos softwares e aplicativos de edição de texto, planilhas, criação de slides, armazenamento em discos virtuais entre outros, sem depender da rede local ou de sua localização geográfica, bastando possuir acesso à Internet.

1.4.2. Adoção da computação em nuvem

As transformações que ocorrem com a TIC (Tecnologia da Informação e Telecomunicações) nos últimos anos têm permitido uma evolução significativa nos meios de acesso à internet. A adoção da computação em nuvem foi potencializada com os meios de acesso cada vez mais velozes, links de banda larga domésticos com alta capacidade e com regras de disponibilidade, bem como com links confiáveis e de alta velocidade e SLAs cada vez mais exigentes com os Internet Service Providers (ISPs) no ambiente corporativo.

A computação na nuvem flexibiliza o gerenciamento da infraestrutura de TI, pois sua adoção pelas empresas permite que elas passem a focar em seus negócios, com investimentos razoáveis em infraestrutura de TI transferindo, assim, seus aplicativos de negócios, seus dados e arquivos de uso diário, serviços de correio, ERP, CRM entre outros, pois os fornecedores serão os responsáveis pela disponibilidade dessas aplicações.

1.4.3. Vantagens da computação na nuvem

A computação na nuvem é oferecida pelos fornecedores na modalidade conhecida como SaaS - Softwares as a Service (Software como Serviço), em que a empresa e o usuário não precisam comprar hardwares pesados e licenças de softwares nem proceder com a instalação de aplicações nos computadores locais e com a contratação de uma grande equipe para manter a infraestrutura de TI. Por exemplo, uma empresa que possui 30 colaboradores e precisa de um sistema de gestão de clientes e folha de pagamento teria que contratar uma equipe, fazer os investimentos em hardware e ainda comprar as licenças da aplicação. Com este modelo, a empresa contrata tudo como serviço, ou ainda, se houver empresas que fornecem o software como SaaS, ela pagará apenas pela licença por usuário, o que reduziria ainda mais seus custos.

Há duas modalidades de adoção da computação na nuvem: ela pode ser de um fornecedor, a chamada nuvem pública, que vimos até agora, ou pode ser uma nuvem privada. Veremos as diferenças nos subtópicos a seguir.

1.4.3.1. Nuvem pública

O que vimos de computação na nuvem até agora pode ser classificado como nuvem pública (public cloud), modalidade na qual os serviços de TI estão hospedados fora da empresa, oferecendo às organizações escalabilidade, flexibilização de operações com rápido crescimento sem a necessidade de investimentos e prazos elevados.

1.4.3.2. Nuvem privada

A nuvem privada (private cloud) e as empresas que adotam esse modelo normalmente preocupam-se com regulamentações internas e externas, levando em consideração as políticas de segurança, bem como a cultura organizacional. Essas empresas recebem os benefícios e vantagens de uma computação na nuvem, como disponibilidade e agilidade de processos, mas devem implantá-la dentro do seu próprio data center.

1.4.3.3. Nuvem híbrida

Em diversos setores, há uma série de regulamentações ou até aplicações que tornam a utilização de uma nuvem pública inviável, pois elas funcionam muito bem apenas em uma nuvem privada, por razões de performance. Ou seja, há aplicações que podem ser utilizadas na nuvem pública e há aplicações críticas da operação que normalmente permanecem sob a responsabilidade da corporação em sua nuvem privada. Para esses casos, pode-se adotar um modelo de nuvem que utiliza o melhor da nuvem privada e da pública, a que chamamos de nuvens híbridas (hybrid cloud). Com essa modalidade, as empresas poderão usufruir do que há de melhor na computação em nuvem.

1.5. Comunicação unificada

As empresas procuram continuamente maneiras de acelerar o processo de comunicação entre colaboradores, clientes, fornecedores e sociedade, e existem muitas ferramentas para viabilizá-lo de forma eficiente, seja por meio das mídias sociais, e-mails, mensagens instantâneas, videoconferências, telefone entre outras. No entanto, o uso desses meios de comunicação de forma separada não permite que as empresas utilizem ao máximo o potencial que há quando eles estão sendo utilizados de forma unificada.

Uma forma de as empresas utilizarem o potencial que existe é adotando um sistema único para gerenciar todos os meios digitais de comunicação através de uma única interface de gerenciamento. Isso traz vantagens significativas para a colaboração e gestão do conhecimento, além de melhorar a interação entre equipes em seus trabalhos, sejam presenciais ou virtuais, e dinamizar a comunicação, agregando valor e confiança e reduzindo o tempo. As empresas e seus usuários ainda percebem as seguintes vantagens:

- Com a adoção da comunicação unificada (UC - Unified Communications), você poderá controlar de forma unificada e gerenciar facilmente as soluções em vez de administrar múltiplas interfaces. Dessa forma, o diagnóstico torna-se eficiente, agregando valor ao negócio, assim como a equipe de tecnologia passa a ter razoabilidade para buscar soluções o que agiliza o processo de backup de toda comunicação corporativa;
- A escolha de uma solução de UC requer planejamento sobre sua implantação e investimentos em equipamentos e em treinamento do pessoal que administrará a solução. As vantagens da adoção dessa solução são percebidas quando se detecta a redução de custo, seja a médio ou longo prazo, e o melhor aproveitamento dos recursos, o que dispensa o gerenciamento de várias soluções de comunicação, como: videoconferência, telefonia móvel com conferência individual etc.;
- Normalmente os usuários perdem muito tempo acessando diversas aplicações. Com a UC, eles poderão obter acesso a um único sistema de comunicação, podendo ser via web ou a partir de seus dispositivos móveis ou equipamentos de mesa. Com isso, torna-se possível encontrar facilmente qualquer pessoa de sua equipe, seja os que estão trabalhando em home-office, equipe técnica de campo, visitando clientes ou em projetos externos, com muita facilidade e colaboração.



Teste seus conhecimentos

História das redes de computadores

1

Conceitos e Infraestrutura de Redes (online)

24

1. Qual modelo de computação em nuvem se preocupa com regulamentações internas e externas, levando em consideração as políticas de segurança e a cultura organizacional?

- a) Nuvem privada.
- b) Nuvem pública.
- c) Nuvem híbrida.
- d) Nuvem comunitária.
- e) Nenhuma das alternativas anteriores está correta.

2. Quando a nuvem é disponibilizada ao público geral por uma organização que vende serviços de nuvem, qual é o modelo de implantação?

- a) Nuvem privada.
- b) Nuvem pública.
- c) Nuvem híbrida.
- d) Nuvem comunitária.
- e) Nenhuma das alternativas anteriores está correta.

3. Com o avanço nas tecnologias de rede e mobilidade, veio também o barateamento dos dispositivos de computação pessoal, de forma que mais usuários passaram a adotar equipamentos eletrônicos para uso pessoal e profissional. Essa é uma característica de qual tendência?

- a) BYOD (Bring Your Own Device)
- b) Convergência digital
- c) Mobilidade
- d) Virtualização
- e) Cloud computing

4. Qual(is) das seguintes alternativas apresenta(m) uma vantagem da comunicação unificada?

- a) Melhoria na interação entre equipes em seus trabalhos.
- b) Dinamização da comunicação.
- c) Redução de tempo e custo.
- d) Melhor aproveitamento dos recursos.
- e) Todas as alternativas anteriores estão corretas.

5. Qual das seguintes alternativas não contém uma característica do modelo de serviços centralizado?

- a) Alto custo de hardware.
- b) Modelo desenhado com capacidade de alta disponibilidade 99.999, baseada em hardware.
- c) Escalabilidade horizontal.
- d) Concepção de serviços de softwares centralizados.
- e) Terminais de minicomputadores.

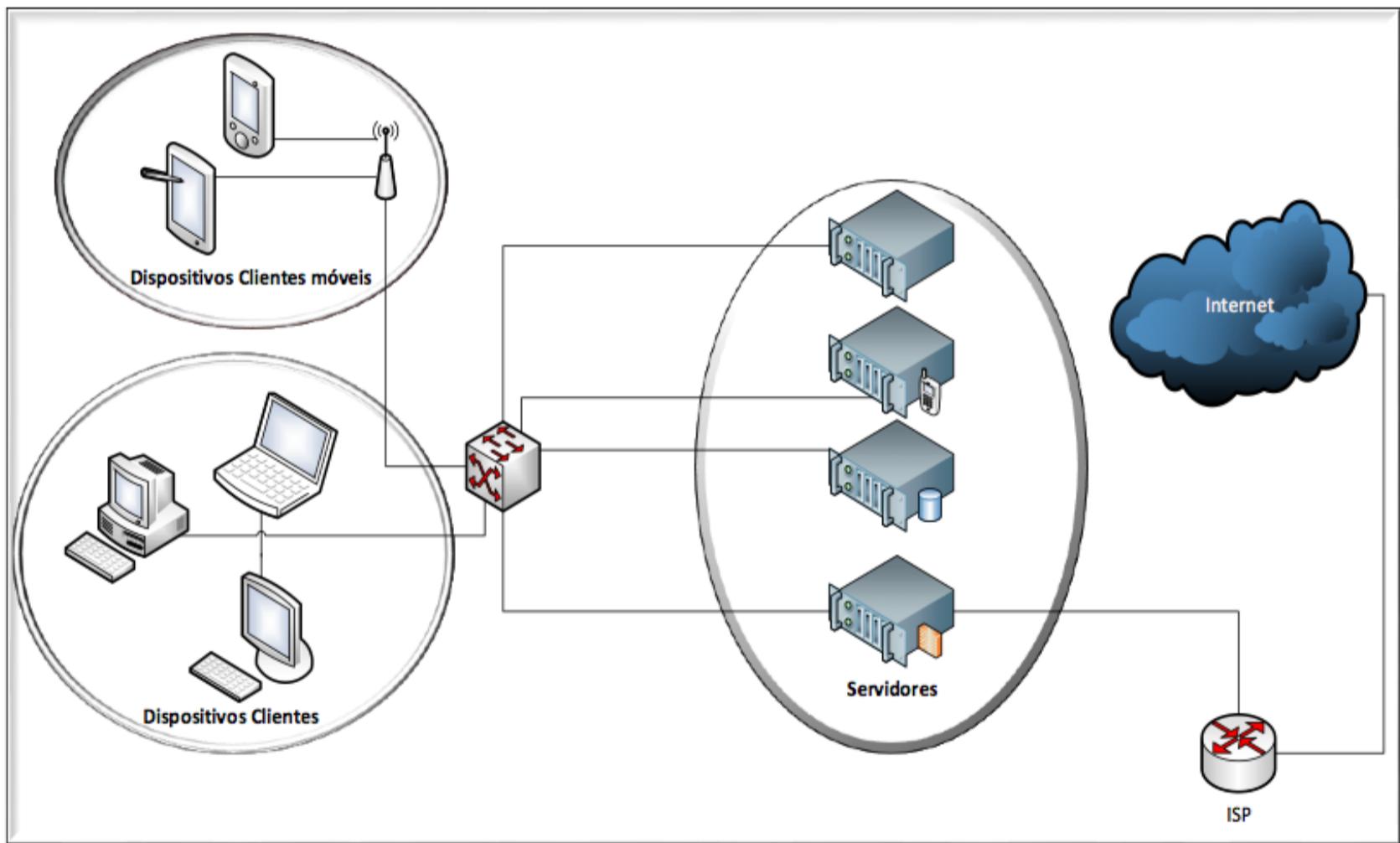
Redes de computadores

2

- ✓ Infraestrutura de rede;
- ✓ Classificação das redes;
- ✓ Redes sem fio;
- ✓ Storage (Armazenamento);
- ✓ Internet, intranet e extranet.

2.1.Introdução

Uma rede de computadores é composta por um conjunto de regras, protocolos, computadores e outros dispositivos de redes que, interconectados, são capazes de trocar informações e compartilhar recursos, com um propósito preestabelecido. A composição da infraestrutura de uma rede de computadores abrange diversos itens, como cabos, conectores, switches, roteadores, protocolos, computadores, servidores, softwares e sistemas, que permitirão a interconexão entre dois ou mais computadores, os quais, ao estabelecerem comunicação, poderão trocar dados entre si, conforme a figura a seguir:



2.1. Exemplo de uma rede de computadores

Uma rede de computadores é composta por diversos componentes, conforme vimos na figura 2.1, e, para que a comunicação aconteça, ela deve possuir um conjunto de regras que garantam o envio seguro de informações. Para que a comunicação seja eficiente, ela necessita que os dados transitem de um computador para outro sem perda e que isso aconteça com a melhor velocidade possível. No próximo tópico veremos quais são os itens que compõe uma rede de computadores.

2.2. Infraestrutura de rede

Uma rede de computadores possui diversas aplicações, seja para fins comerciais ou uso doméstico, e é composta por elementos que permitem o uso de aplicações da linha de negócios que proporcionam maior confiabilidade, agilidade e segurança dos dados, permitindo o compartilhamento de recursos, como impressoras, arquivos de dados, assim como a implantação de soluções de telefonia via IP (VoIP) para fins de redução do custo de comunicação, gerenciamento dos serviços de dados, serviços de web, videoconferência, entre outros.

As redes de computadores podem ser divididas conforme definido a seguir:

- **Infraestrutura física**

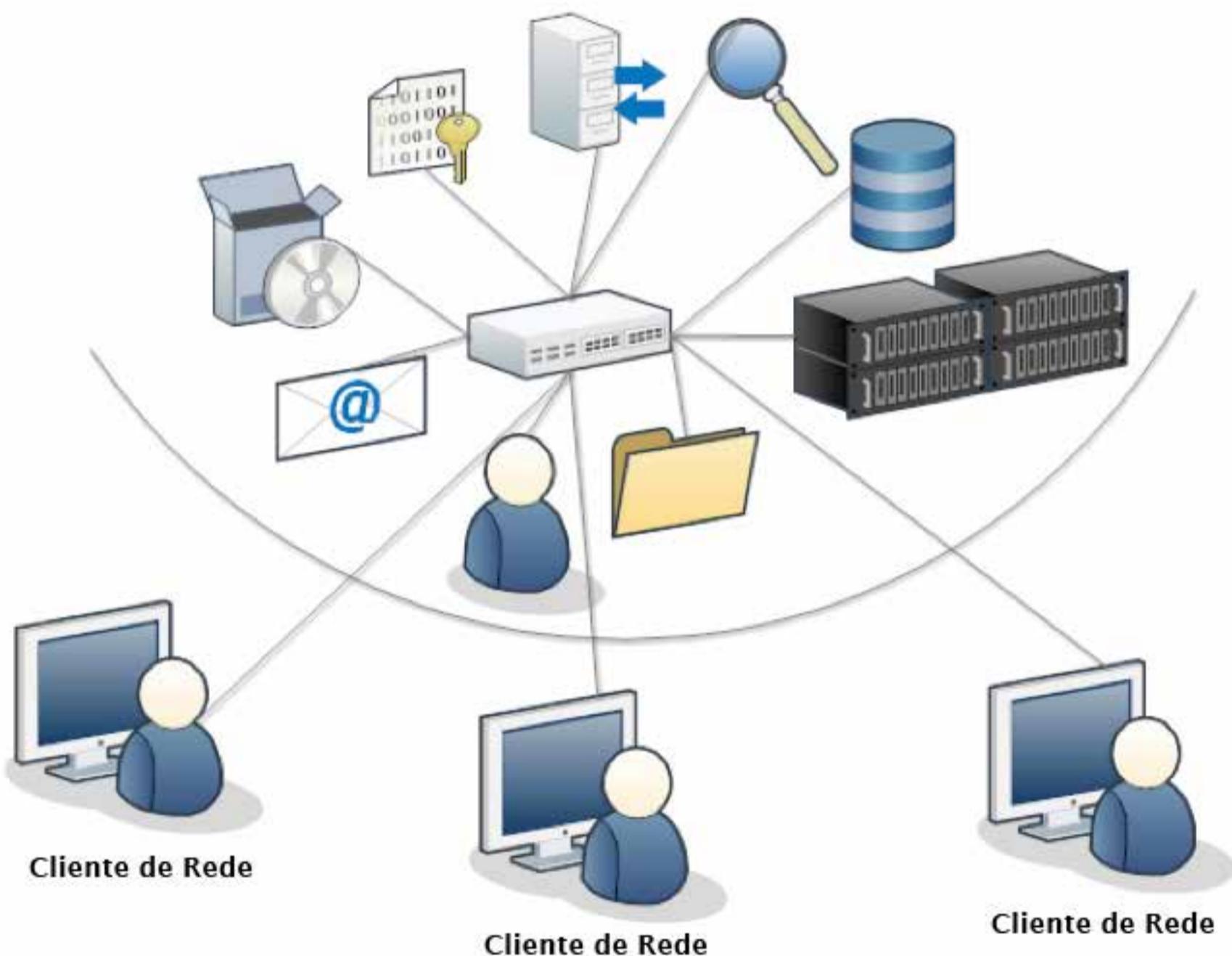
Define como os componentes de hardware de rede (switches, conectores, cabos, fios, placas de rede, computadores) são organizados e interligados. Esta composição e forma de organização é conhecida como Topologia Física, ou seja, é o sistema de comunicação que une os ativos de uma rede, sendo capaz de transportar informações eletromagnéticas, seja por cabo par metálico, cabo coaxial, fibra óptica por meio de feixe de luz ou pelo próprio ar através de spectrum via wireless.

Conceitos e Infraestrutura de Redes (online)

30

- **Infraestrutura lógica**

É um conjunto de regras que permitem um alinhamento entre os componentes de hardware de modo que funcionem quando interligados. Esta composição é organizada e conhecida como Topologia Lógica, pois estabelece um padrão aceito de procedimentos e especificações formais que governam a comunicação entre os ativos de uma rede de computadores.



2.2. Infraestrutura física e lógica de redes

2.3. Classificação das redes

Diversas características podem ser utilizadas para classificar uma rede de computadores. Os critérios adotados para tal classificação podem ser sua escala, o modo como está organizada, seu tamanho físico, bem como seu aspecto geográfico. Ao classificar uma rede, leva-se em consideração se esta é destinada à aplicação para uso pessoal ou empresarial.

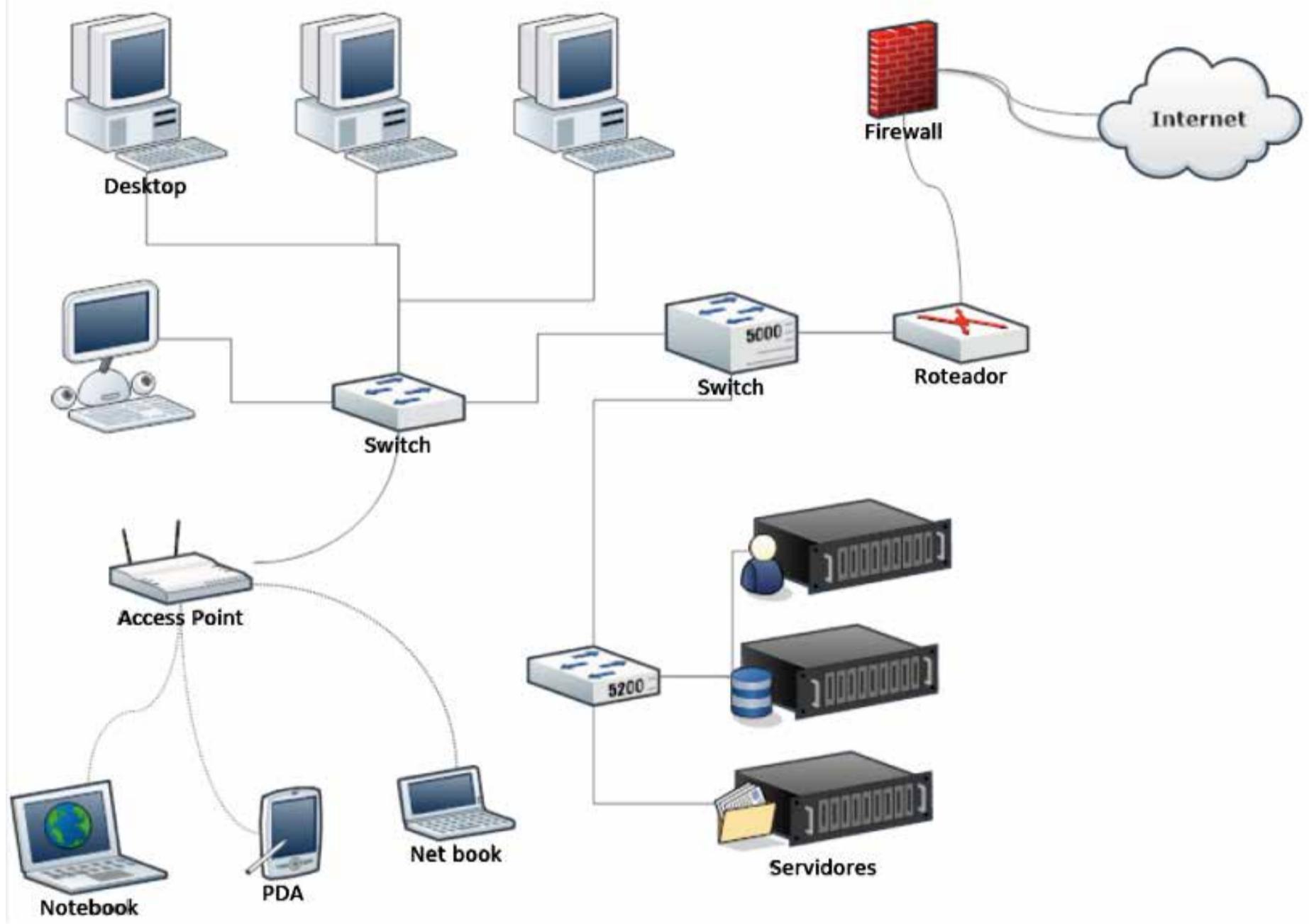
A classificação de redes de computadores baseia-se em sua abrangência. Elas podem ser locais, metropolitanas ou até globais, baseadas em seu aspecto geográfico e na forma como estão distribuídas. Ao passo que uma empresa faz a interligação de dois ou mais escritórios a partir dessa conexão, a sua classificação muda e, nesse contexto, dois fatores, além das tecnologias empregadas, determinarão a sua classificação: a quantidade de usuários que utilizam os recursos dessa rede e a distância que ela pode alcançar. Analisaremos os tipos de rede de acordo com a área física que ela cobre.

- **Local Area Network (LAN)**

Mais comuns em áreas maiores, como um departamento de uma empresa ou andares inteiros de prédios, a rede LAN pode conectar múltiplos grupos entre si e, geralmente, ligá-los a um dispositivo centralizado, como um servidor ou um switch. As redes de computadores que foram criadas, no início de sua composição, limitavam-se a 185 metros de um ponto a outro e considerava-se que suportavam, no máximo, 30 computadores. Com o avanço das tecnologias de comunicação, cabos e equipamentos, essas limitações foram superadas, permitindo maior alcance. A interconexão entre os equipamentos de rede pode ser feita por meio de cabos ou utilizando tecnologia wireless. Esta rede também é conhecida como Rede Local.

Conceitos e Infraestrutura de Redes (online)

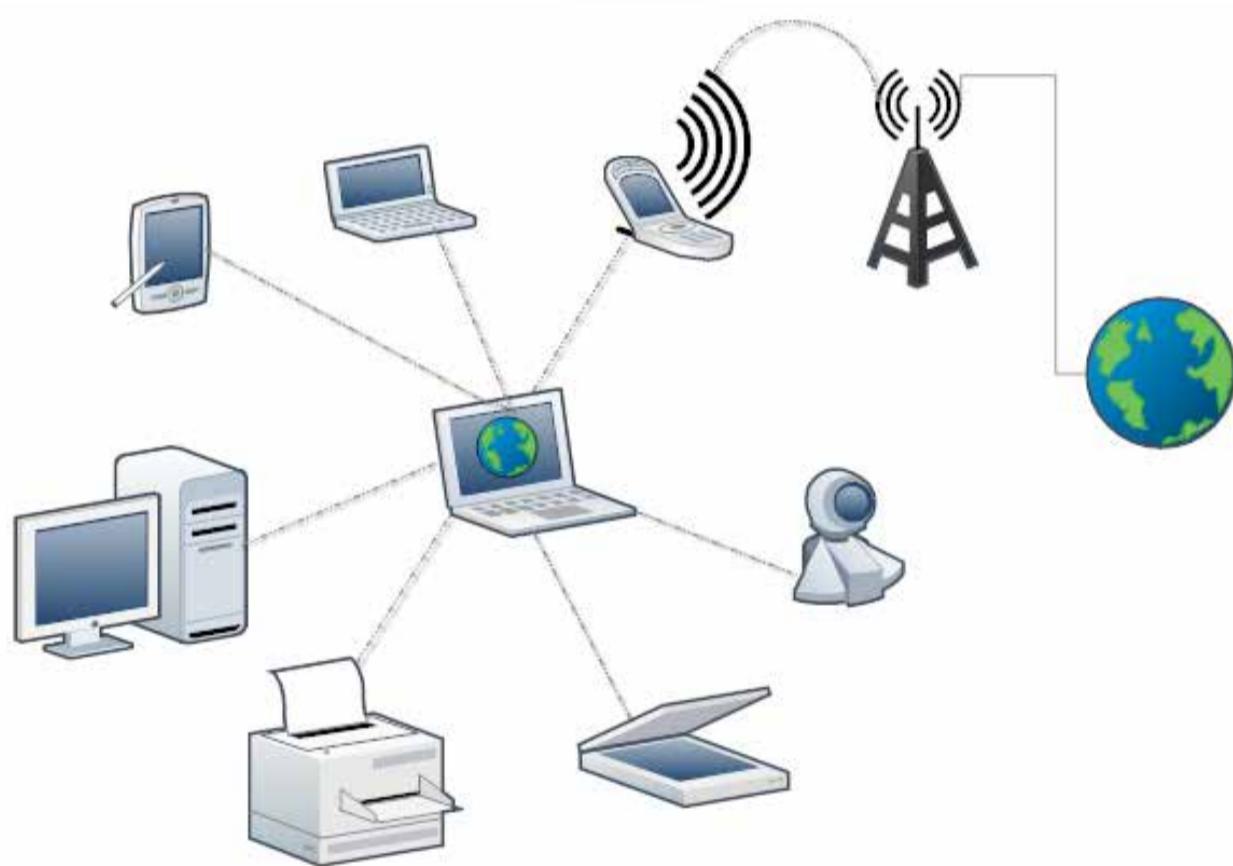
32



2.3. Local Area Network

- **Personal Area Network (PAN)**

A rede PAN é conhecida como uma rede de menor alcance físico, cobrindo geralmente espaços individuais, como um escritório, uma pequena sala ou um cubículo, normalmente em um raio de 10 a 15 metros, pois essa comunicação ocorre normalmente através de frequência de rádio de onda curta, como Home-RF ou Bluetooth, conforme a figura adiante. Esse tipo de rede estabelece a comunicação e realiza a transmissão dos dados através de tecnologias de comunicação sem fio, normalmente para conexão de aparelhos de telefone celular, tablets, smartphones, notebooks, câmeras digitais, consoles de videogame digitais, impressoras, teclados, mouses e até fones de ouvido, entre outros equipamentos.



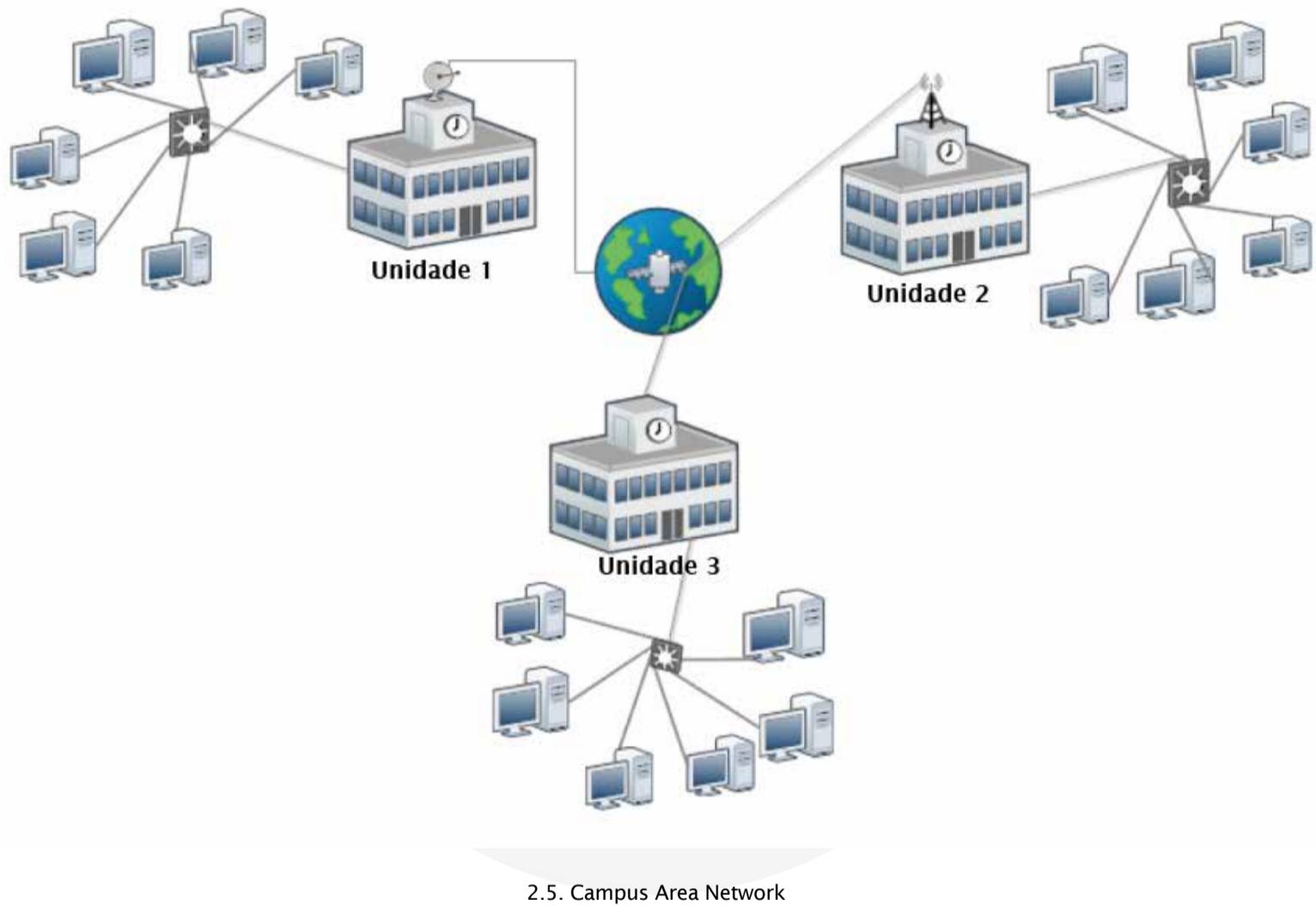
2.4. Personal Area Network

Conceitos e Infraestrutura de Redes (online)

34

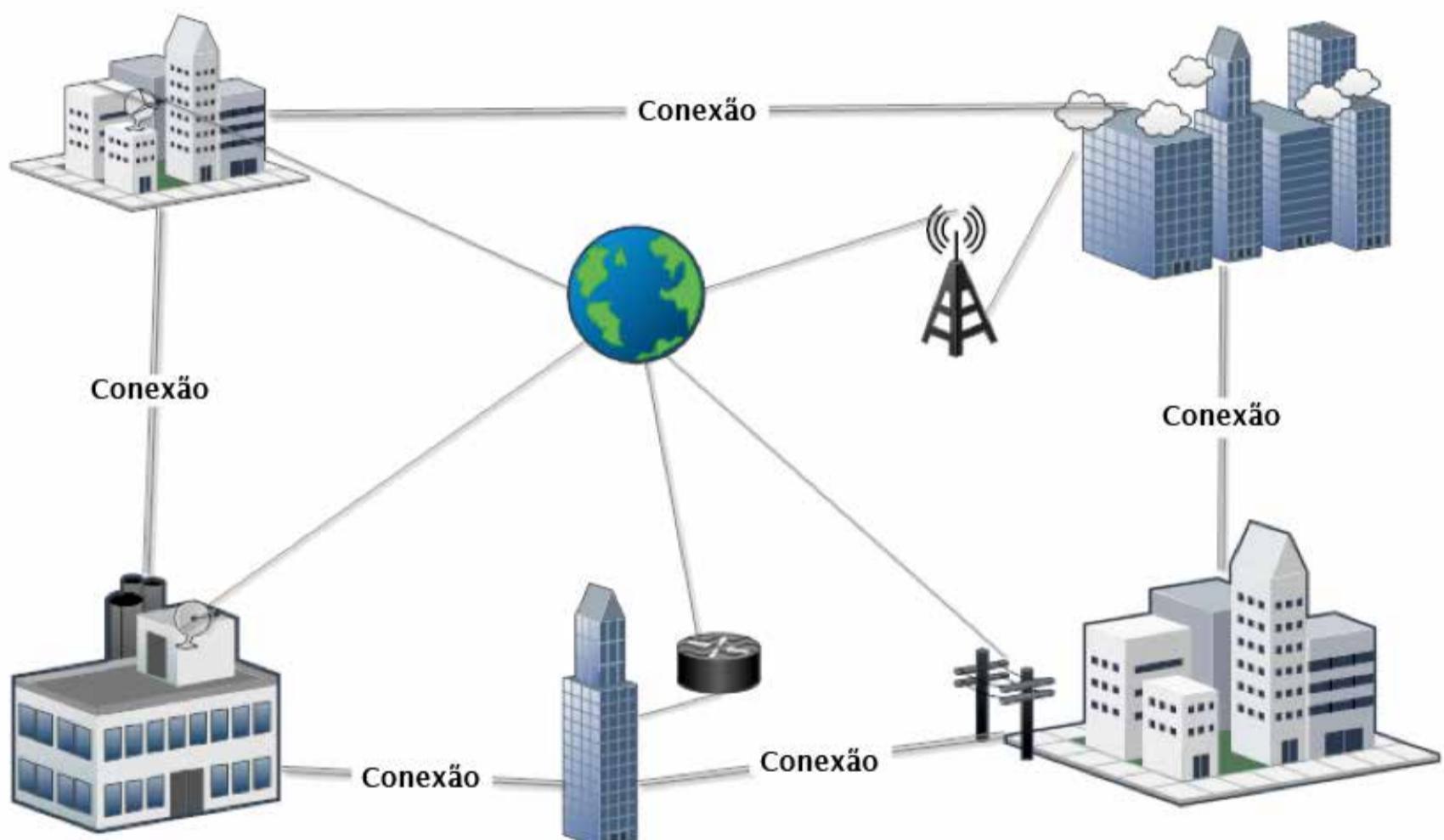
- **Campus Area Network (CAN)**

A classificação de rede que define esta como CAN baseia-se na interligação de duas ou mais redes LAN. As redes CAN são conhecidas como Campus Area Network ou Campus LAN. Essa interligação cria uma área de rede maior que a LAN, conectando, por exemplo, redes de diferentes prédios em uma empresa. Essa conexão pode ser feita por meio de cabos ou tecnologia wireless.



- **Metropolitan Area Network (MAN)**

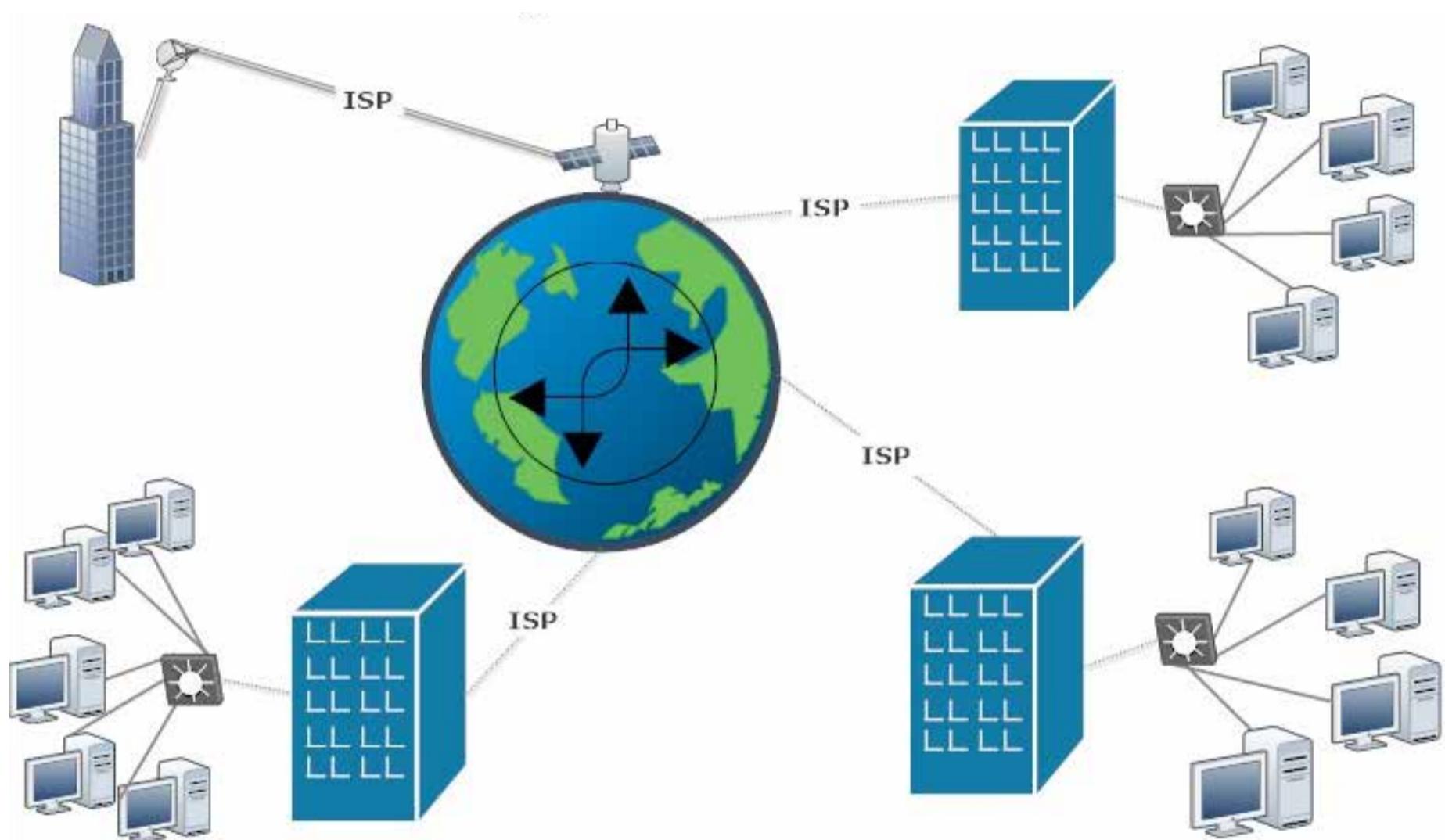
As conexões feitas entre diferentes instalações em uma cidade, como, por exemplo, entre diferentes prédios de uma empresa, formam a rede MAN. As conexões que formam a rede MAN podem ser constituídas por ligações sem fio ou por meio de cabos. O cabeamento de fibra óptica é o método mais comum na ligação de um estabelecimento cliente a uma instalação operada por um provedor de serviço de telecomunicações.



2.6. Metropolitan Area Network

- **Wide Area Network (WAN)**

Redes interligadas que estejam localizadas separadamente por distâncias geográficas maiores que uma área metropolitana são chamadas de redes WAN. Essas redes distantes interligadas podem estar em cidades separadas, países e até continentes, que são os casos de redes WAN globais. Instalações operadas por um provedor de serviço recebem conexões dos estabelecimentos que fazem parte da rede e ligam-se entre si por meio de uma rede de provedores de serviço ou pela própria Internet.



2.7. Wide Area Network

2.3.1. Tecnologias de transmissão

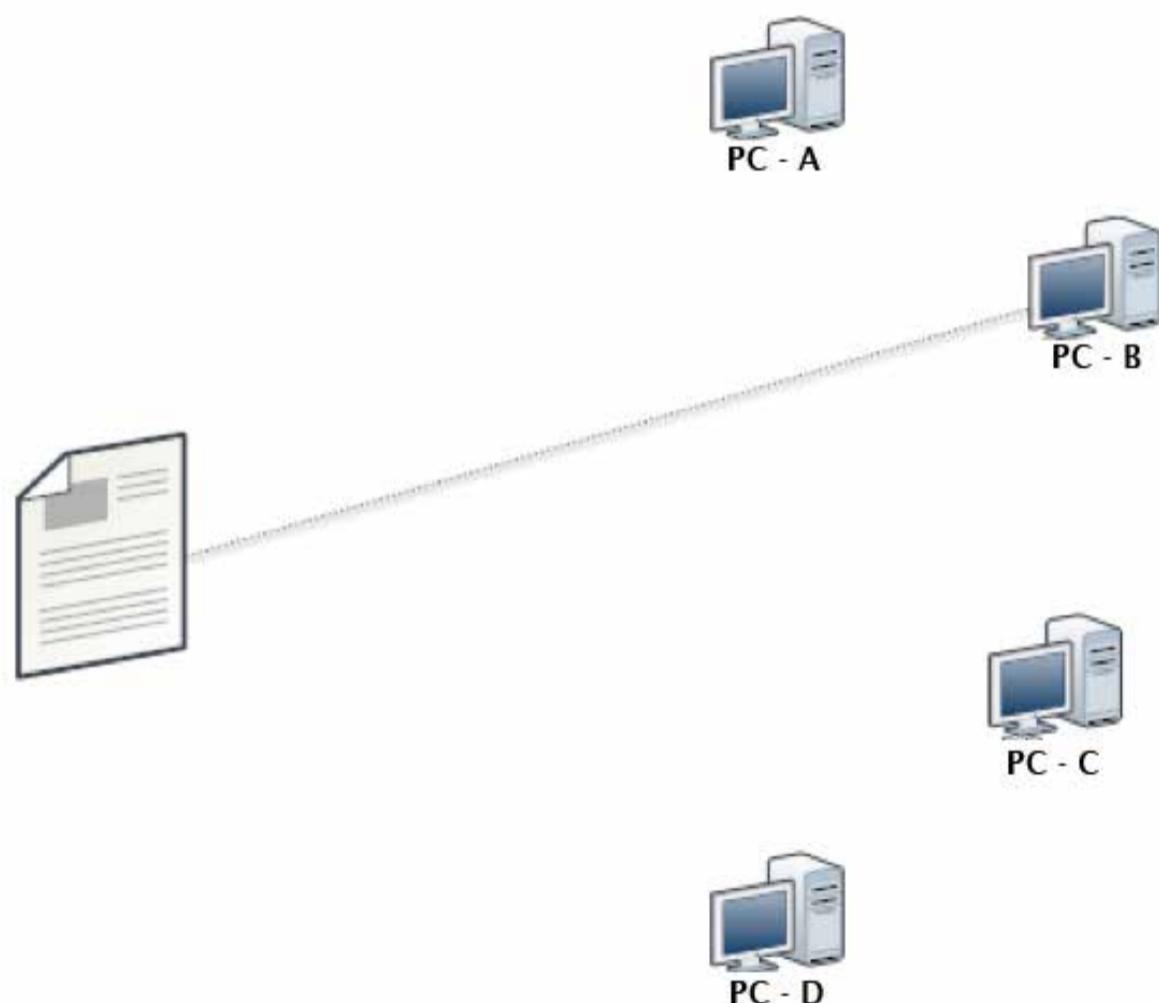
As tecnologias de transmissão de informações eletrônicas presentes na maioria dos dispositivos de rede podem ser de três tipos: unicast, broadcast e multicast. Cada uma delas funciona com um tipo de transmissão diferente, seja em comunicações de um remetente para um receptor único, para múltiplos receptores, direcionados ou não, para grupos específicos de mais de um receptor ou para todos os destinos ligados à rede.

Veremos a seguir as peculiaridades de cada tipo de tecnologia:

- **Transmissão unicast**

A tecnologia unicast funciona enviando dados de um remetente direcionados para apenas um único destino. Não existe risco de enviamos dados para um destino incorreto usando essa tecnologia, pois os pacotes de informações são enviados diretamente apenas ao endereço recipiente.

Caso seja necessário enviar um mesmo pacote de dados para mais de um destino, a mesma transmissão unicast deve ser replicada a quantidade de vezes necessária para cada destino. Porém, a produção de pacotes de dados múltiplos para o envio individual é ineficiente e requer processamento adicional do dispositivo remetente.

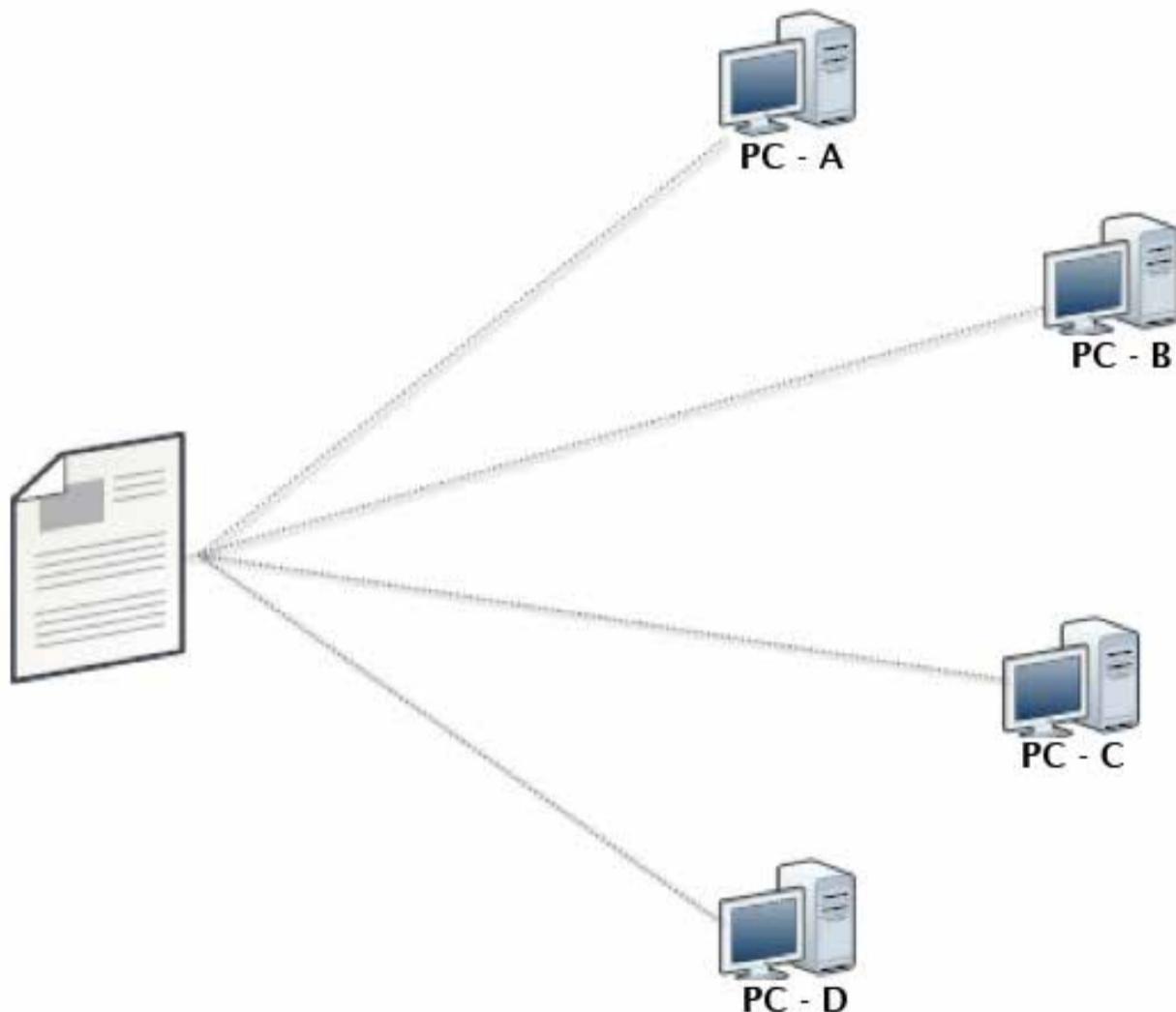


2.8. Transmissão unicast

- **Transmissão broadcast**

Nesse tipo de tecnologia de transmissão, os pacotes de dados possuem uma sequência especial de bits no endereço para indicar que todos os dispositivos do domínio de broadcast serão o destino da informação enviada. Essa tecnologia permite que se envie um pacote de dados apenas uma vez, e ele é replicado para ser enviado aos destinos.

A eficiência da transmissão broadcast se dá nos casos em que todos os dispositivos da rede necessitam receber pacotes difundidos por uma fonte. Se algum dos dispositivos na rede não necessita receber esses dados, ele desperdiça recursos de processamento. Em casos em que o número de dispositivos que não devem receber os dados seja maior do que os que receberão, essa tecnologia torna-se ineficiente por utilizar recursos técnicos desnecessariamente.

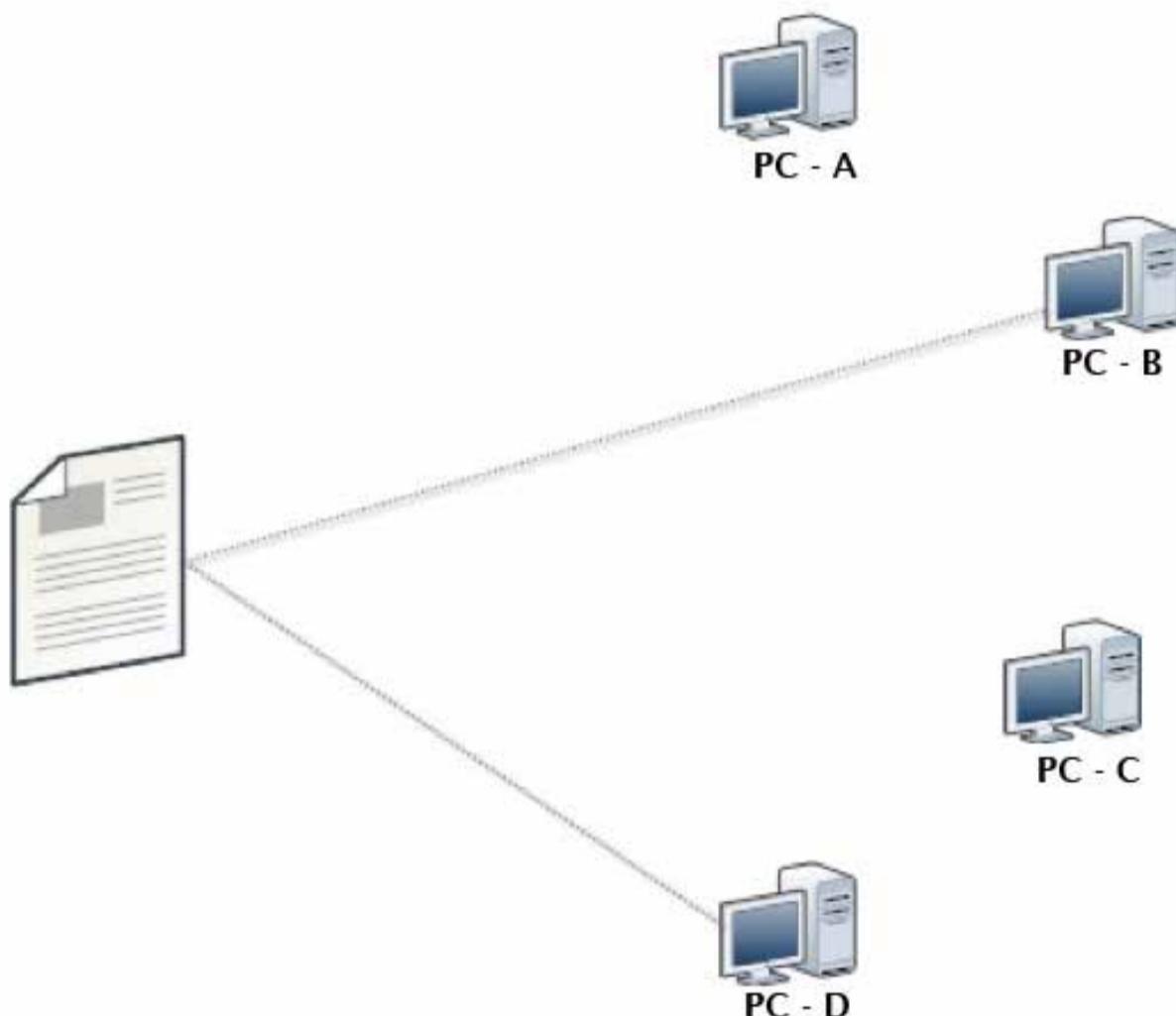


2.9. Transmissão broadcast

- **Transmissão multicast**

Podemos considerar a transmissão multicast como um broadcast seletivo ou direcionado. É a maneira mais recomendada para o envio de um pacote de dados de um único remetente para pontos múltiplos, onde nem todos os dispositivos inseridos na rede devem ter acesso aos dados enviados.

Nessa tecnologia, um pacote de dados enviado por um dispositivo é transmitido para um endereço especial de grupo multicast. A rede redireciona os dados apenas para os dispositivos listados como membros desse grupo multicast.



2.10. Transmissão multicast

2.4. Redes sem fio

O conceito original das redes sem fio é baseado nas transmissões de sinais de telégrafo via rádio, datadas do início do século XX. A transmissão sem fio entre computadores nos dias de hoje funciona por meio do envio e do recebimento de informações em formato binário, assim como nas transmissões de código Morse, porém com um desempenho muito maior.

O que caracteriza uma rede sem fio é qualquer tipo de transmissão de dados, seja por computadores, ativos de rede e/ou quaisquer sistemas que estejam interligados sem a necessidade do uso de fios e cabos. Sua transmissão é realizada através do ar e é chamada de “Wireless”, termo este que vem do inglês “Wire”, que significa “cabo”, e “Less”, que significa “Sem”, ou seja, “Sem Cabos”. Há várias tecnologias que podemos adotar para a comunicação sem fio, tais como: InfraRed (infravermelho), Bluetooth, Wi-Fi e WiMax.

2.4.1. Evolução da tecnologia de rede sem fio

Podemos considerar que há três gerações de tecnologia de rede sem fio, as quais trouxeram avanços significativos para o processo de comunicação e ampliaram a velocidade que os dispositivos de rede utilizam para troca de informação. Hoje, cada uma delas é amplamente utilizada e não houve substituição em razão de qualquer evolução.

O Infravermelho é um dos métodos utilizados para comunicação sem fio, porém possui velocidade limitada e deve estar no mesmo ângulo de visão. Por essa razão, é normalmente utilizada para troca de dados entre dispositivos móveis e interligação de teclados e mouses sem fio.

Outra tecnologia de transmissão de rede sem fio é o Bluetooth, uma tecnologia mais difundida e que trabalha em frequência alta para transmissão de dados entre dispositivos.

A terceira e mais conhecida forma de transmissão de rede sem fio é o Wireless, também chamado de Wi-Fi (Wireless Fidelity), que classifica comercialmente produtos desenvolvidos para atender ao padrão de redes WLAN. No entanto, as tecnologias são padronizadas pelo IEEE (Institute of Electrical and Electronic Engineers), que define padrões de desenvolvimento para atender aos padrões IEEE 802.11 implementados nos rádios dos dispositivos wireless. Os principais padrões são:

- 802.11a, que opera a 54Mbps;
- 802.11b, que opera a 11Mbps;
- 802.11g, que opera a 54Mbps;
- 802.11n, que opera a 300Mbps;
- 802.11ac, que opera a 1Gbps.

2.4.2. Classificação de redes sem fio

Vamos ver abaixo as quatro classificações mais utilizadas:

- **Wireless Personal Area Network (WPAN)**

A rede de interconexão de sistemas WPAN (Wireless Personal Area Network) é um sistema de conexão de pequeno alcance definido pelo padrão 802.15, com a função principal de ligar periféricos, como mouse, teclado, impressoras, entre outros, a um computador, sem a necessidade da utilização de cabos e fios, o que torna a instalação desse tipo de equipamento mais complicada. A tecnologia de interconexão de sistemas chamada Bluetooth é a mais difundida para essas finalidades.

A rede WPAN também é muito útil na conexão de câmeras digitais, scanners, telefones celulares e outros periféricos, sendo necessário, na maioria dos casos, apenas aproxima-los do computador para que funcionem, sem ser preciso instalar drivers ou cabos de conexão. Essa conexão funciona em um esquema master/slave, onde o computador ao qual os dispositivos se ligam age como master, definindo suas configurações e o endereço de conexão, enquanto os periféricos fazem o papel de slaves.

Conceitos e Infraestrutura de Redes (online)

42

- **Rede LAN sem fio (WLAN)**

Para conexões de alcance maior, como, por exemplo, entre computadores em uma sala ou em um departamento de uma empresa, utiliza-se a rede WLAN (Wireless Local Area Network), onde computadores são ligados entre si através de sinal de rádio, por meio de um modem e uma antena. As redes WLAN usam como padrão o IEEE 802.11, que vem sendo bastante usado, já que a maioria dos sistemas é compatível com esse padrão.

Esse tipo de rede sem fio vem se tornando cada vez mais popular nos casos em que é muito dispendiosa a instalação de Ethernet e em locais como cafeteria, salas de conferência etc., pela facilidade de implantação e manutenção.

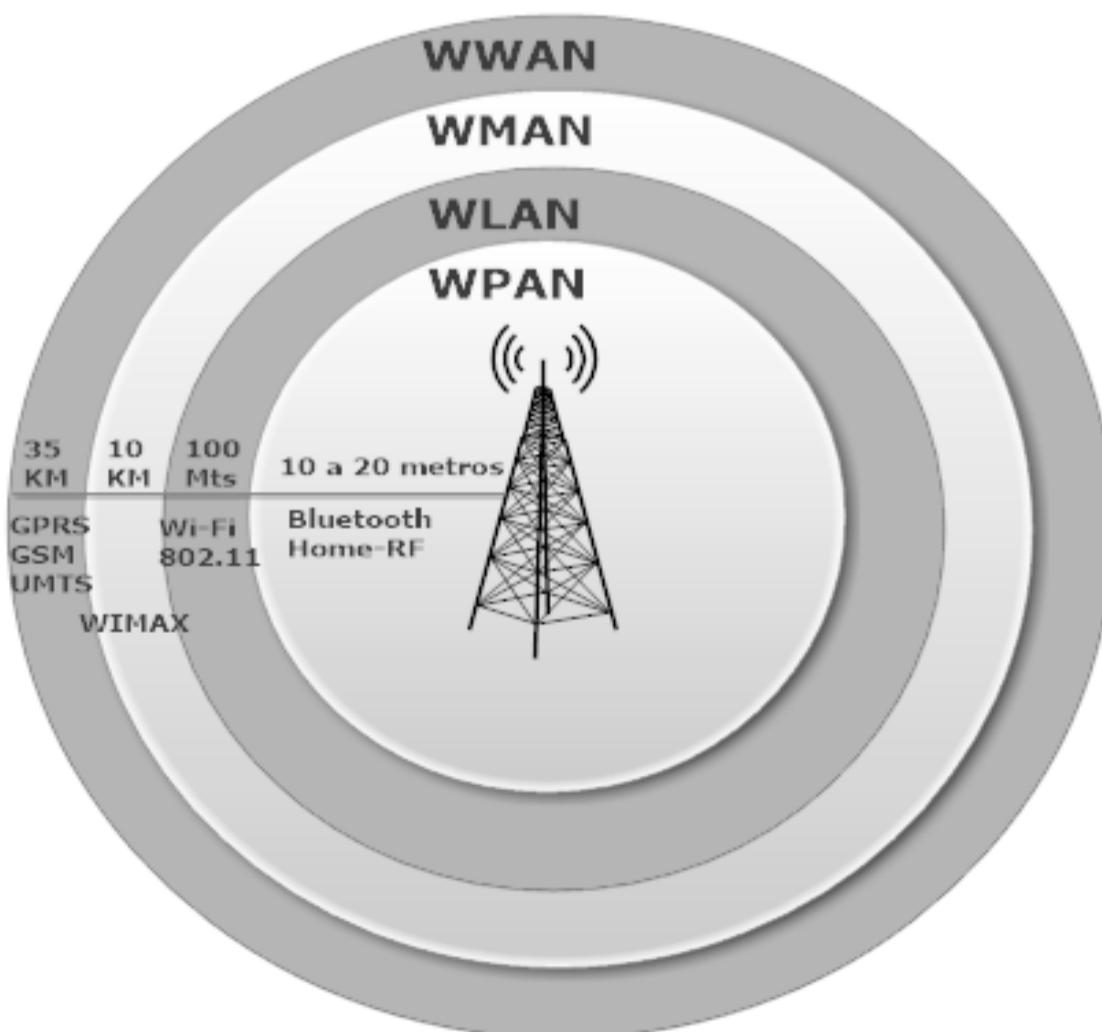
- **Rede MAN sem fio (WMAN)**

Esse tipo de rede é muito similar às Redes MAN, mas em sua implementação não são utilizados fios e cabos para realizar a interligação, e ele é definido pelo padrão de Implementação do IEEE 802.16. Esse modelo de implementação possui como padrão de interconexão o WiMAX (Worldwide Interoperability for Microwave Access), que possui capacidade de promover entrega de sinal e mantém conectividade para uso corporativo, comunitário ou até doméstico, bem como em hotspots através de um único ponto linear. WiMAX é uma tecnologia de comunicação de banda larga que não utiliza fios e cabos e foi projetada para ter um alcance de até 50 km, oferecendo alternativas a tecnologias como cabo e DSL. Ela é utilizada, por exemplo, por operadoras de Telecom (NET, CLARO etc.).

- **Rede WAN sem fio (WWAN)**

O padrão de implementação do WWAN foi definido pelo IEEE 802.20 e os sistemas que utilizam a rede WWAN (Wireless Wide Area Network) são aplicados para grandes áreas que necessitam de ligação de rede sem fio, como, por exemplo, a rede de rádio de telefonia celular. Essa tecnologia já se encontra na quarta geração de seu desenvolvimento, sendo que a primeira trabalhava apenas com a transmissão de voz e funcionava de modo analógico, a segunda geração já se tornou digital, enquanto a terceira e a quarta (mais rápida) são digitais e trabalham com transmissão de voz e dados.

Podemos considerar a rede sem fio de celulares como uma rede LAN sem fio, mas que atinge enormes áreas de funcionamento, sendo possível chamá-las de redes WWAN de baixa largura de banda. Já estão em desenvolvimento redes WWAN com alta largura de banda. Isso permitiria o acesso à Internet em alta velocidade a partir de domicílios e empresas, tornando obsoleto o uso do sistema telefônico. Baseado nos padrões de classificação, a figura a seguir demonstra o raio de alcance de cada padrão:



2.11. Classificação de redes sem fio

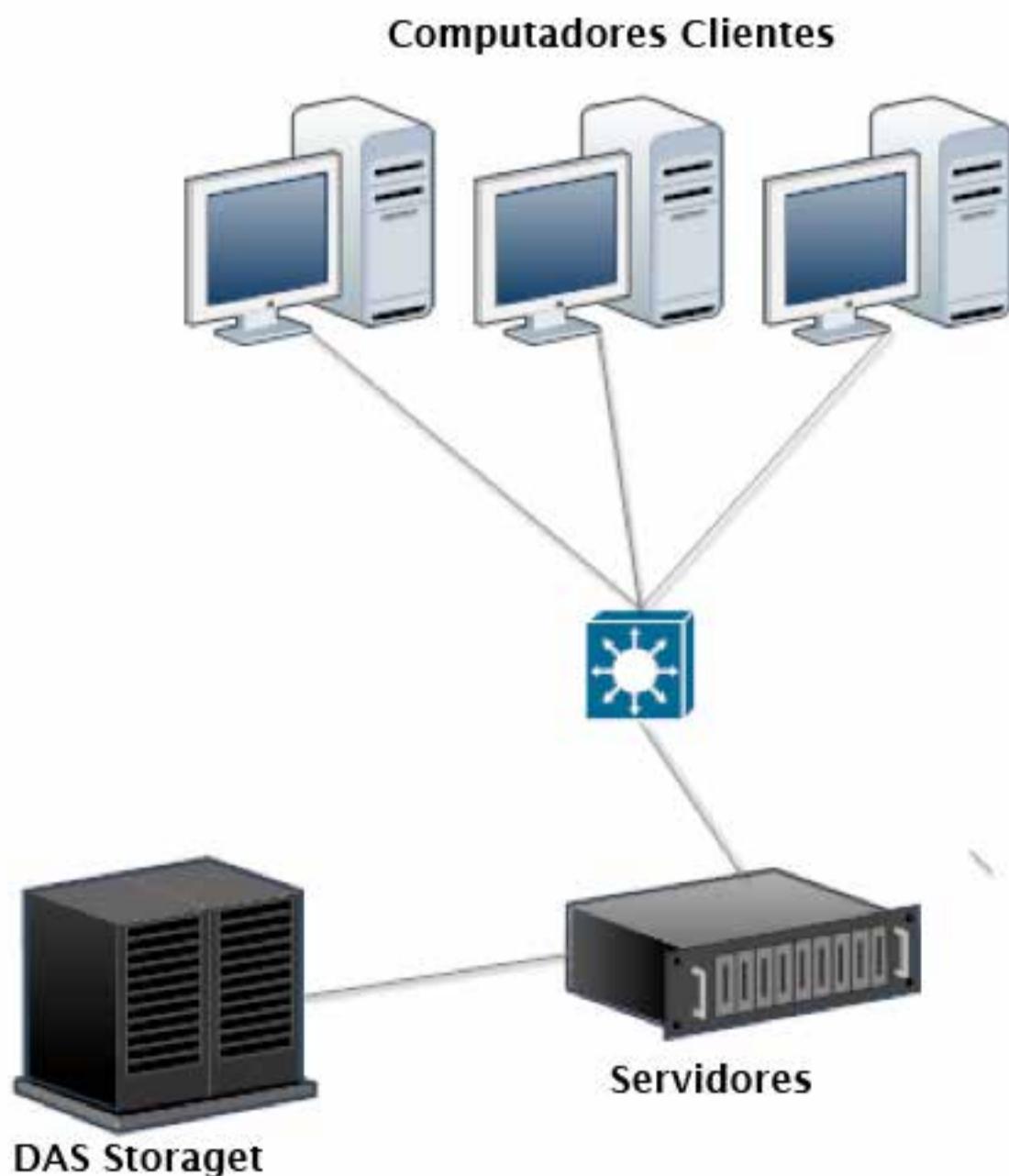
2.5.Storage (Armazenamento)

Com a crescente massa de dados, a necessidade de recuperação de dados e a facilidade para se fazer ou recuperar backup das informações, cada vez mais as empresas criam soluções para o armazenamento de dados. Em empresas de pequeno porte, costuma-se adotar computadores exclusivamente para essa função, e essas máquinas são denominadas servidores de arquivos ou de armazenamento. Mas ao passo que o volume de dados atinge um nível de consumo elevado de espaço em disco e um alto tráfego de acesso e transferência, é provável que seja necessária mais velocidade dos dispositivos de armazenamento. Partindo-se da premissa de que as empresas possuem plano de recuperação de dados, estrutura tolerante para evitar perda das informações, pode-se adotar uma solução de armazenamento que mais se encaixe no perfil de consumo.

Os dados das empresas são recursos valiosos que podem determinar sua continuidade no setor em que atuam ou fazer com que deixem de oferecer produtos, emitir cobrança de serviços prestados, identificar clientes devedores ou mesmo de possuir registros das transações de contas a pagar e receber. Por razões como essas o modelo de armazenamento sofreu uma evolução, para trazer mais segurança e confiabilidade, conforme veremos a seguir:

- **DAS (Direct Attached Storage)**

Uma das soluções de armazenamento é o DAS (Direct Attached Storage). Foi a primeira solução disponível para atender as demandas crescentes de armazenamento de dados corporativos. Este, por sua vez, possui boa capacidade e suporta a combinação de unidades SAS e SATA em um único gabinete, tornando-se ideal para aplicativos de alta capacidade. A principal característica que define um Direct Attached Storage é que este sistema de armazenamento se conecta diretamente a um servidor.



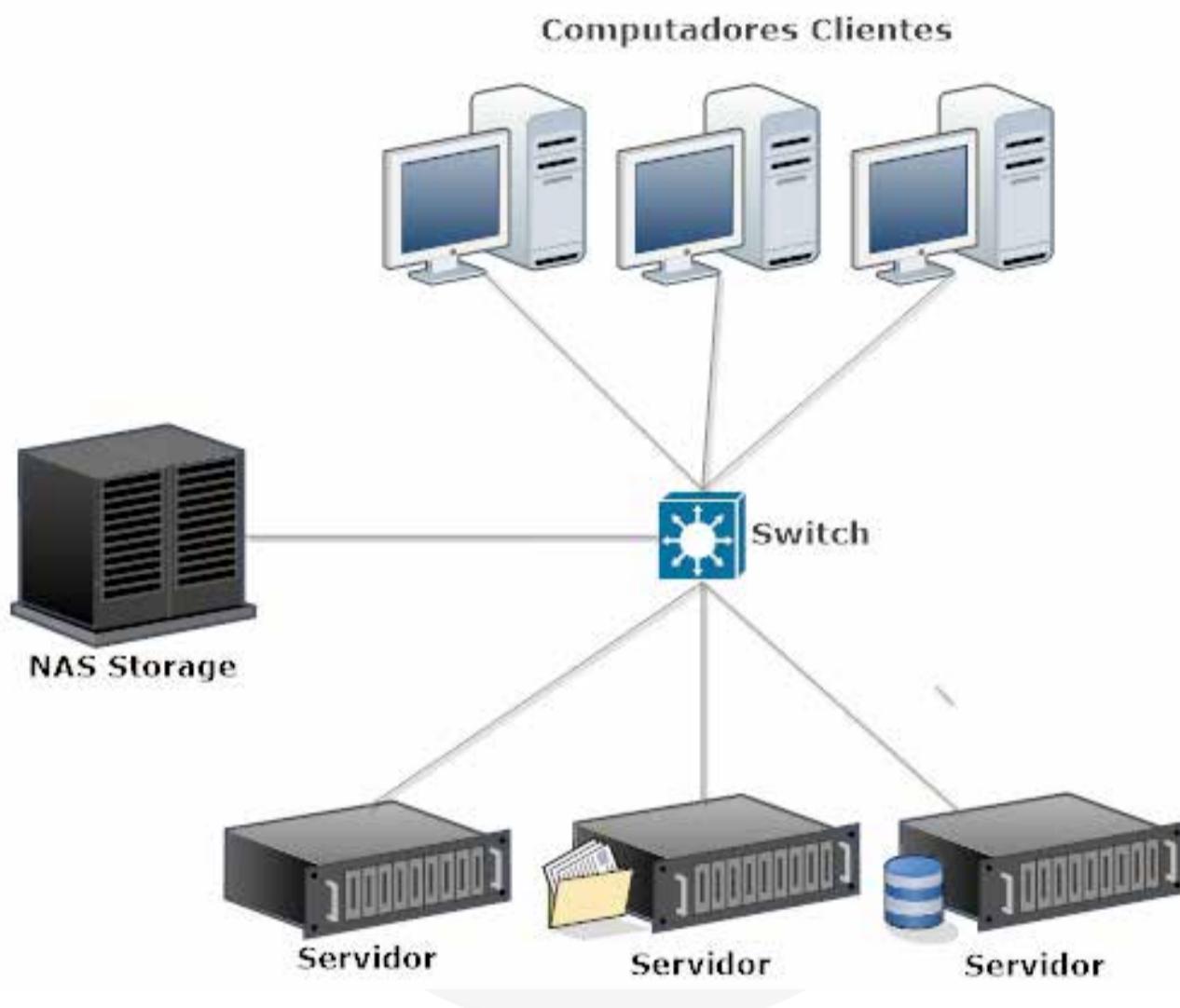
2.12. DAS - Direct Attached Storage

Conceitos e Infraestrutura de Redes (online)

46

- **NAS (Network Attached Storage)**

Elementos de armazenamento que se conectam a uma rede são chamados de NAS, que também têm a função de fornecer serviços de acesso a arquivos para sistemas de computadores. O NAS é constituído normalmente de um mecanismo que oferece os serviços de arquivo, e os dados são armazenados em um ou mais dispositivos.

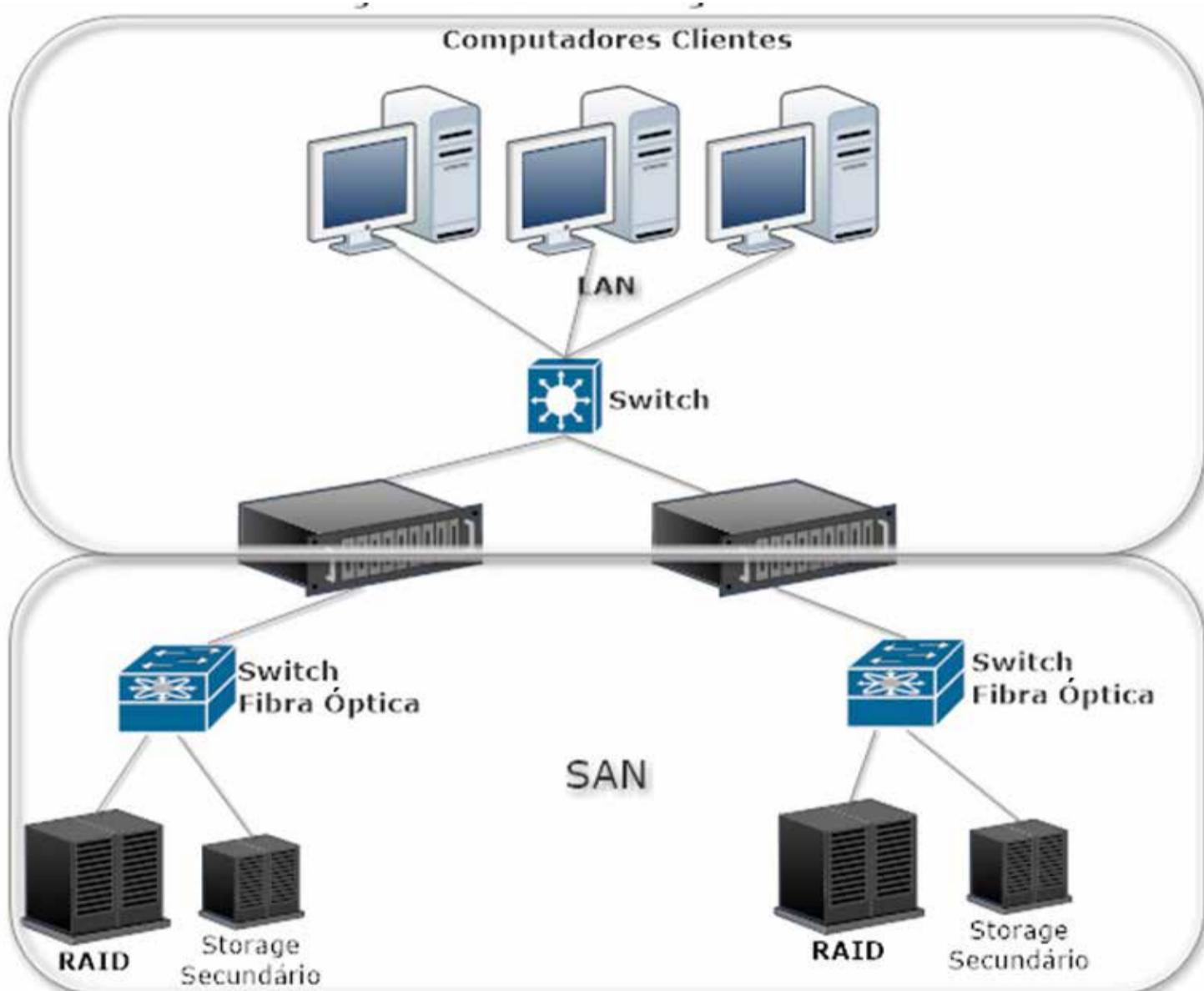


2.13. NAS - Network Attached Storage

- **SAN (Storage Area Network)**

A SAN é uma rede de área de armazenamento cuja principal função é a transferência de informações realizada pelos elementos de armazenamento entre si e sua conexão com sistemas de computador. É um sistema formado por elementos de armazenamento, dispositivos de armazenamento, sistemas de computador, além de todo o software de controle. Esses elementos todos se comunicam através de uma rede.

As conexões físicas são providenciadas pela infraestrutura de comunicação. A organização das conexões, dos elementos de armazenamento e dos sistemas de computadores é realizada por uma camada de gerenciamento, tornando segura e robusta a transferência dos dados. Essa estrutura constitui a área de armazenamento SAN, que é normalmente mais identificada com serviços block I/O do que com serviços de acesso de arquivo.



2.14. SAN – Storage Area Network

2.6. Internet, intranet e extranet

Entende-se por Internet uma coleção de computadores, servidores, gateways e redes relacionadas por meio de um conjunto de protocolos de telecomunicações.

A Internet possibilita acesso mundial a informações e recursos de todos os tipos, como tecnologias recentes, noticiários, fóruns, catálogos, negócios, entre outros. Tudo isso pronto para aprimorar o desempenho do trabalho de milhares de usuários-pesquisadores, ou mesmo de engenheiros de suporte ou administradores de rede.

Em meio ao uso cada vez maior da tecnologia Internet, novos termos e conceitos surgem a uma grande velocidade. Eis os casos de intranet e extranet. A intranet surge como um tipo de rede baseada no modelo da Internet, com a distinção de que ele é empregado para a melhoria da comunicação e da produtividade dentro de uma empresa. Assim, o acesso de funcionários a inúmeras informações, fórum de debates, feedback de clientes, gera um ambiente de maior produtividade e qualidade, garantindo à empresa uma maior competitividade no mercado. Ademais, a intranet assegura benefícios, desde a economia no custo de distribuição de documentos até o desenvolvimento de programas de ensino à distância.

A extranet pode ser vista como parte da intranet de uma empresa, que é estendida a clientes e fornecedores para compartilhar informações de interesse comum e exclusivo. Remete, portanto, a uma rede privada que utiliza o protocolo da Internet para troca de informações de negócios e operações entre uma comunidade restrita. Como resultado, o uso da extranet pode, por exemplo, otimizar a comunicação entre o setor de negócios e os consumidores, agilizando o processo de vendas.



Teste seus conhecimentos Redes de Computadores

2

Conceitos e Infraestrutura de Redes (online)

50

1. Qual padrão, estipulado pelo IEEE através da implementação 802.11 e que define a comunicação de rede sem fio WLAN, opera em taxas de velocidade nominal de Gbps?

- a) Padrão 802.11a
- b) Padrão 802.11c
- c) Padrão 802.11n
- d) Padrão 802.11ac
- e) Padrão 802.11b

2. Qual tecnologia de transmissão permite a replicação do pacote de dados para todos os dispositivos do domínio?

- a) Multicast
- b) Unicast
- c) Broadcast
- d) NAS
- e) SAN

3. Quais classificações de rede, dadas de acordo com a área física que ela cobre, podem ser encontradas?

- a) PAN, LAN, CAN, MAN e WAN.
- b) WPAN, PAN, WLAN, LAN, WCAN, CAN, WMAN, MAN, WWAN e WAN.
- c) Internet, Intranet e Extranet.
- d) SAN e NAS.
- e) Mainframes, minicomputadores e computadores pessoais.

4. Como são conhecidos os dispositivos de armazenamento que podem ser conectados diretamente nas LANs?

- a) SAN
- b) NAS
- c) CAN
- d) WLAN
- e) PAN

5. Quando há ligação entre LANs em um mesmo complexo (por exemplo, blocos ou prédios de uma indústria ou condomínio), sem a necessidade de um provedor de serviços, como é classificada esta rede (ligação)?

- a) WAN
- b) LAN
- c) PAN
- d) CAN
- e) SAN

Modelos, topologias e tecnologias de rede 3

- ✓ Modelos de rede;
- ✓ Topologias de rede;
- ✓ Tecnologias de rede.

3.1.Introdução

Nesta leitura, abordaremos alguns conceitos relativos às redes de computadores. Estes conceitos são fundamentais para o entendimento da disposição e funcionamento das redes para sua implantação.

Para definirmos de forma assertiva qual será o modelo de rede adotado para cada projeto de implantação, primeiramente, é necessário conhecermos os modelos de rede que podem ser empregados e quais os aspectos que devem ser considerados ao escolhermos um deles.

No momento de escolher um modelo de rede, devemos considerar critérios factíveis que tornarão uma rede de computadores confiável e apta a atender com alto padrão de desempenho. Critérios como capacidade, disponibilidade e escalabilidade são alguns dos fatores que tornarão esta rede capaz de suportar qualquer crescimento e de estar preparada para mudanças futuras. A partir da escolha do modelo, partimos então para sua implementação.

Nesta fase do processo, é necessário definir qual será a topologia utilizada, ou seja, de que forma os componentes existentes na rede serão organizados fisicamente. Esta leitura apresenta as principais topologias, expondo suas vantagens e restrições, e oferece, ainda, uma descrição das tecnologias que viabilizam a comunicação efetiva entre os dispositivos presentes na rede.

Por fim, o objetivo é que, ao entendermos o funcionamento da rede e as opções disponíveis para sua implementação, sejamos capazes de fazer a escolha que melhor se ajuste às nossas necessidades.

3.2.Modelos de rede

O processo de comunicação entre computadores tem por finalidade realizar a transferência de arquivos de dados, comunicação por voz ou vídeo e é essencial que isso aconteça com o melhor desempenho possível. Para atender esse objetivo, torna-se necessária a implantação de uma Rede Local (LAN) que atenda todos os requisitos necessários.

A escolha do modelo de rede determinará seu potencial de crescimento, pois ela definirá os dispositivos para suportar as especificações da rede que atenderá demandas de negócios de empresas de pequeno ou médio porte, bem como sua disposição.

Podemos encontrar dois modelos de rede:

- Modelo não hierárquico;
- Modelo cliente-servidor.

Esses modelos têm suas características próprias, que serão estudadas nos tópicos a seguir. A diferença entre elas está na definição e na relação entre os computadores cliente, que recebem dados e serviços, e os computadores servidor, que proveem os dados e serviços.

3.2.1. Modelo não hierárquico

Esse modelo de rede, que também recebe o nome de ponto a ponto, é indicado para redes que possuem uma quantidade limitada de usuários e recursos compartilhados, como as redes domésticas ou pequenos estabelecimentos, onde investimentos em servidores centralizados não são necessários. Nesses casos, não há a necessidade do uso de servidores dedicados que executam software NOS especializado, pois é possível estabelecer um ambiente ponto a ponto em que todas as estações podem agir igualmente. Isso significa que os computadores podem ser configurados para exercer tanto a função de estação quanto de servidor.

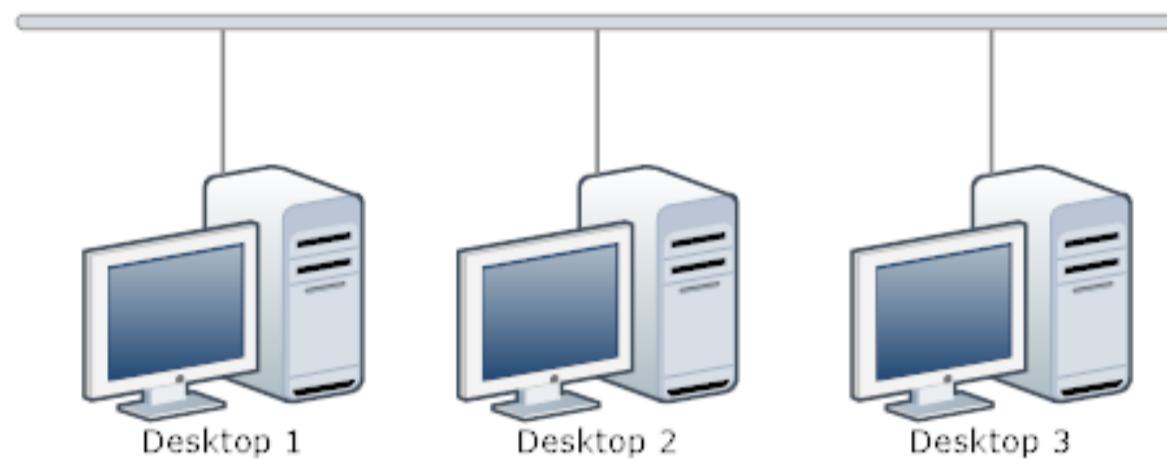


Software NOS (Network Operating System) é o software de sistema de uma rede local responsável por realizar a integração entre os componentes de hardware da rede. Normalmente, é utilizado apenas em redes com grande número de estações de trabalho.

Conceitos e Infraestrutura de Redes (online)

56

Na rede ponto a ponto, os usuários têm o poder de disponibilizar os recursos existentes em seu computador a outros usuários. Para habilitá-la, o computador deve ser equipado com o software NOS ponto a ponto, o que ocorre, geralmente, na forma de um sistema operacional de estação com capacidades limitadas na rede. Esse software promove o gerenciamento de todos os acessos aos recursos designados como compartilháveis naquele computador.



3.1. Modelo não hierárquico

Vejamos algumas características desse tipo de rede:

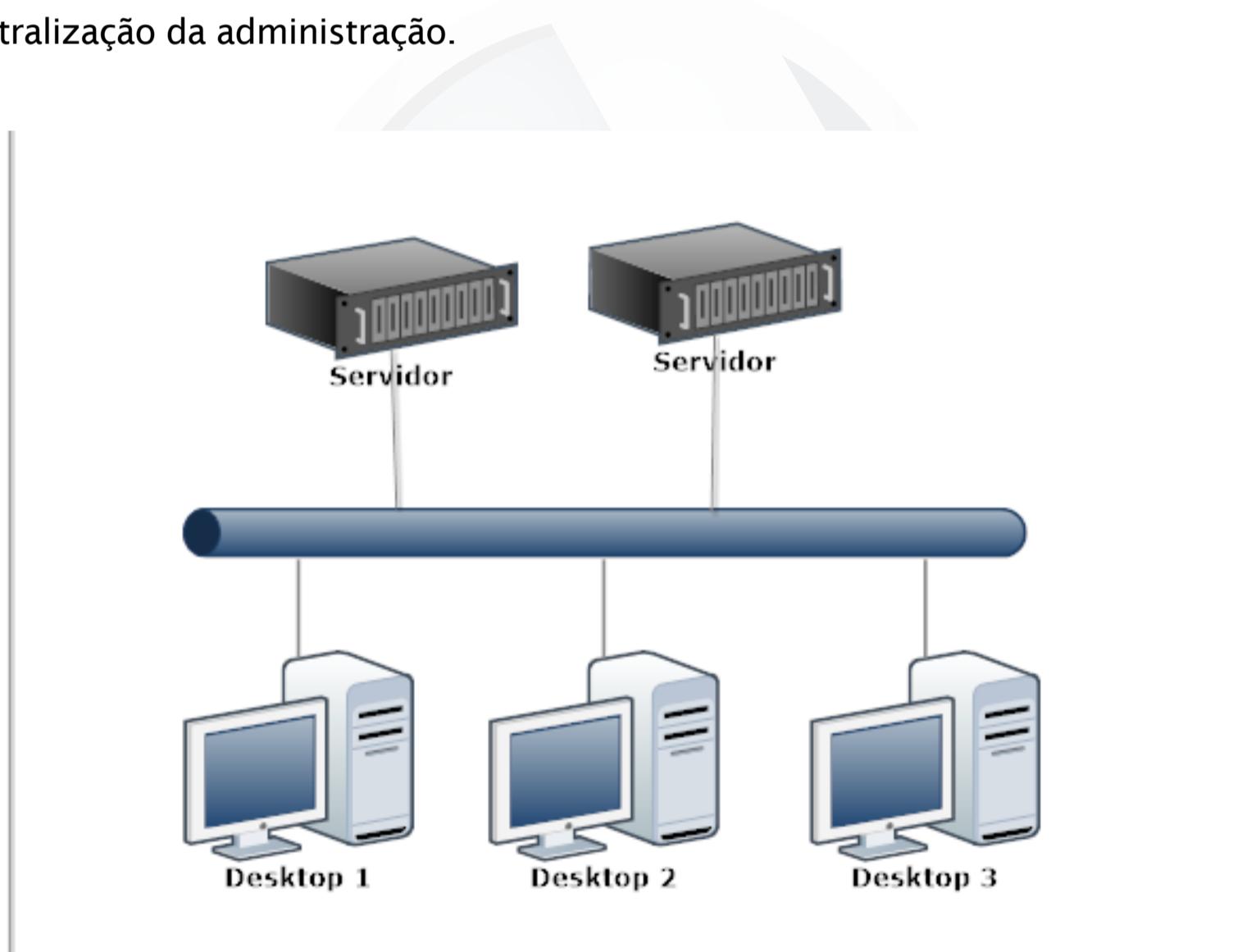
- Ausência de hierarquia entre os computadores e servidores dedicados;
- Ausência de um administrador responsável pela manutenção da rede;
- Dupla funcionalidade, que confere a cada computador a opção de atuar tanto como cliente quanto como servidor;
- Segurança fornecida pelo banco de dados do diretório local de cada computador;
- Compartilhamento de dados presentes em cada computador da rede, determinado pelos usuários de cada micro.

Por essas características, as redes não hierárquicas são propícias a ambientes onde a segurança não representa problema e onde não é necessário um servidor especializado.

3.2.2. Modelo cliente-servidor

Como vimos, uma rede ponto a ponto limita-se a um número pequeno de computadores. Isso significa que, à medida que esse número aumenta, cresce também a demanda por recursos compartilhados na rede, que não são mais suportados por um grupo de trabalho. Daí a necessidade de implantação de redes baseadas em servidores (redes cliente-servidor). Vejamos as suas principais características:

- Presença de servidores dedicados: não atuam como clientes, somente como servidores;
- Configuração otimizada dos servidores dedicados, com o objetivo de processar solicitações de clientes da rede;
- Centralização da administração.



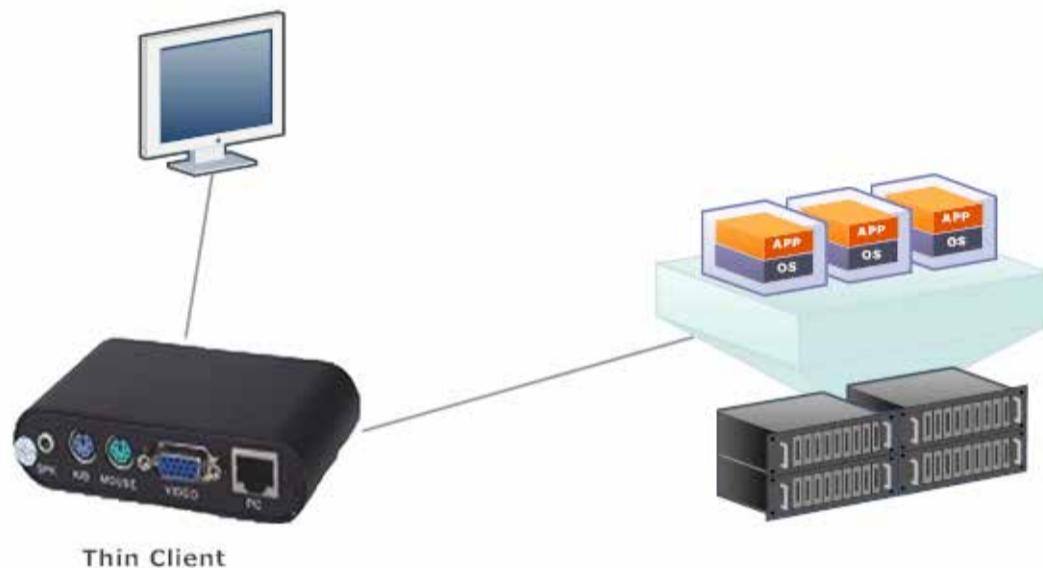
3.2. Modelo cliente-servidor

Nesse modelo de rede, clientes e servidores podem ser classificados de maneiras diferentes, conforme veremos nos tópicos a seguir.

3.2.2.1. Clientes

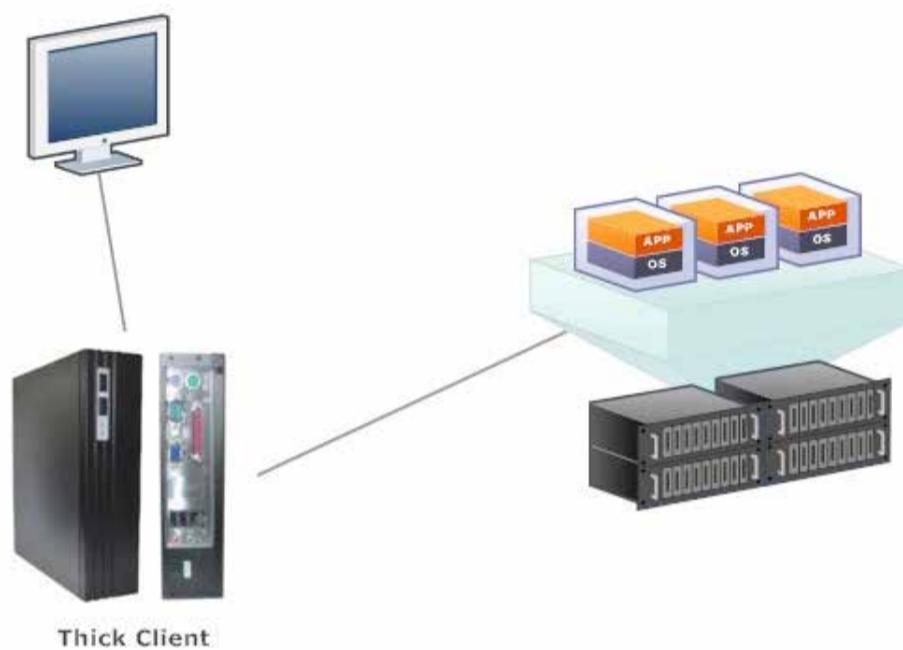
Os clientes podem ser classificados de acordo com sua forma física e configuração. As duas classificações utilizadas são:

- **Thin client:** O thin client (que pode ser literalmente traduzido como “cliente magro”) é um computador cliente que depende de outro computador para realizar a maior parte das tarefas. Por integrar uma rede, o thin client funciona, basicamente, como uma interface e não possui muitos dispositivos e aplicativos. O processamento das tarefas é feito pelo servidor dedicado;



3.3. Thin client

- **Thick client:** O thick client (literalmente “cliente gordo”), ao contrário do thin client, é um computador plenamente funcional, esteja ele conectado ou não a uma rede. Apesar disso, quando conectado a um servidor, ele passa a ser apenas mais um cliente, podendo receber do servidor arquivos e programas que não estão em seu disco local.



3.4.. Thick client

3.2.2.2. Servidores

Com o aumento do número de computadores conectados e a distância física entre eles, as redes cliente-servidor passam a necessitar de mais de um servidor dedicado. Isso possibilita compartilhar tarefas entre os múltiplos servidores (assegurando maior eficiência na execução delas), além de aliviar a carga de trabalho em cada computador individual. Este tipo de rede oferece maior segurança, pelo fato de serem utilizados servidores específicos que centralizam os recursos compartilhados.

Conceitos e Infraestrutura de Redes (online)

60

Vejamos algumas funções que os servidores podem exercer:

- Servidores de arquivos;



- Servidores de banco de dados;



- Servidores de e-mail;



- Servidores de impressão;



- Servidores FTP;



- Servidor de Firewall;



- Servidor WEB;



- Servidor DNS;



- Servidor DHCP.



Assim como os clientes, os servidores também são classificados conforme seu tamanho e forma física. A seguir, podemos conferir as quatro classificações existentes:

- **Servidores torre:** Consistem em unidades autossuficientes, que possuem capacidade interna máxima para compreender diversos drives e cartões de expansão;

- **Gabinetes servidores:** Do ponto de vista funcional, equivalem aos servidores torre, porém, sua projeção requer que sejam armazenados em racks padronizados;



3.5. Modelo de servidores

- **Servidores appliance:** São servidores indicados para locais onde não há muito espaço para racks, já que seu tamanho é de apenas 1U (ou 1RU, de Rack Unit). Como um rack padrão tem capacidade de 42U, é possível armazenar até 42 servidores deste tipo em um único rack. Os servidores appliance são recomendados para os data centers, por exemplo, que precisam lidar com um número muito alto de servidores em um mesmo ambiente;
- **Servidores blade:** Também são indicados para ambientes como os data centers, uma vez que apresentam dimensões ainda menores em relação aos servidores appliance. Um rack padrão, com capacidade de 42U, pode conter até 168 servidores blade. Quando utilizamos servidores blade, um único chassis de rack pode ser equipado com diversas placas add-in, sendo que cada uma delas funciona como um servidor independente. Além disso, os chassis disponibilizam uma fonte de alimentação comum a todos os servidores, que podem ser removidos ou substituídos conforme a necessidade.



3.6. Servidor blade

Vale ressaltar que, para utilizar configurações de alta densidade com servidores appliance e blade, é necessário possuir uma infraestrutura de refrigeração apropriada.

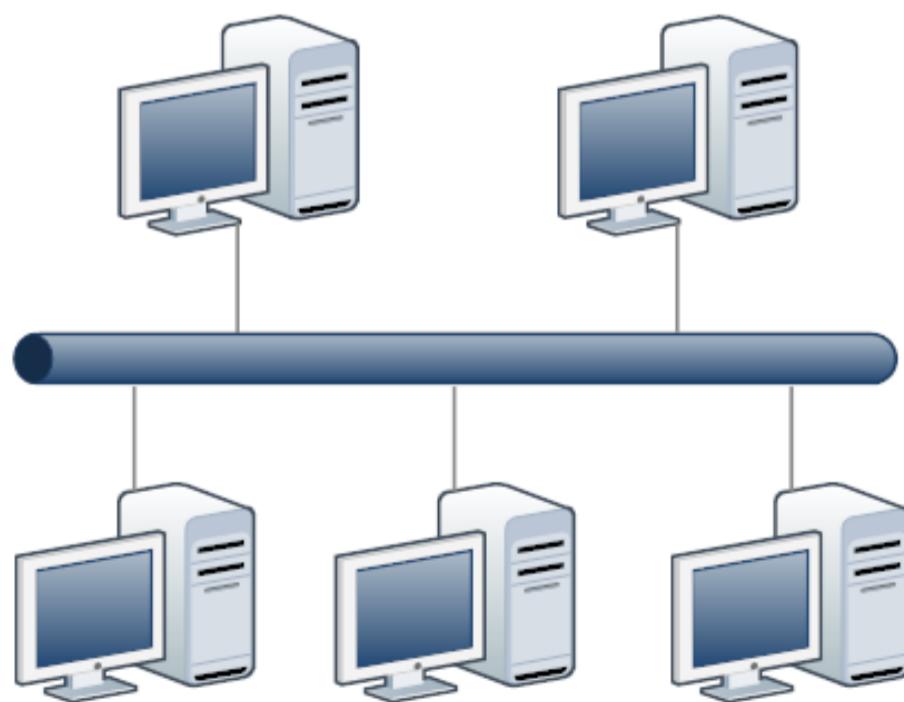
3.3. Topologias de rede

Antes da implantação de uma rede, é necessário, entre outras coisas, definir a topologia a ser utilizada. A topologia de rede consiste na maneira como os dispositivos de uma rede estão dispostos e interligados fisicamente, incluindo o cabeamento utilizado por esses dispositivos e outros componentes pertencentes à rede.

Há três topologias básicas que podem ser utilizadas em uma rede: Barramento, Estrela e Anel. Além dessas, há, ainda, a topologia de malha (mesh) e as topologias mistas, que são combinações feitas a partir das topologias básicas para gerar uma nova. Veremos cada uma delas em detalhes nos tópicos a seguir.

3.3.1. Barramento

Quando uma rede apresenta todos os dispositivos ligados a um cabo contínuo, dizemos que ela emprega uma topologia barramento. Nessa topologia, todos os computadores são interligados através de um único cabo, e neste cabo há conectores que criam elos de comunicação entre os vários dispositivos dessa rede.



3.7. Topologia barramento

Através desse cabo, dados são transmitidos e recebidos pelos vários dispositivos do sistema. O limite deste processo de transmissão e recepção é marcado pelos dispositivos de hardware presentes nas extremidades do cabo, denominados terminadores. A topologia barramento pode ter sua performance afetada se houver:

- Interrupções no cabo ou ausência de terminadores nas suas extremidades. Nesses casos, é possível que ocorra uma paralisação da comunicação entre os dispositivos da rede;
- Um elevado número de dispositivos em comunicação simultânea, o que provoca tráfego na rede, acarretando uma queda na sua eficiência.

Vejamos, então, os benefícios e possíveis prejuízos do uso desse tipo de topologia:

- **Benefícios**
 - Baixo consumo de cabo para sua implantação;
 - Não há complexidade para estruturar uma rede com este tipo de mídia de transmissão;
 - Simples e relativamente confiável;
 - Facilidade de expansão em detrimento do modelo de cabeamento.
- **Prejuízos**
 - Pelo fato de utilizar um único cabo para interligar todos os computadores, a rede pode ficar extremamente lenta em situações de alto tráfego;
 - Um rompimento no único cabo impede a comunicação com a rede;
 - O processo de diagnóstico de um ponto da rede com problema torna-se mais lento e mais difícil de isolar.

3.3.2. Estrela

Em uma rede estruturada segundo a topologia estrela, os segmentos de cabo dos dispositivos encontram-se conectados a um dispositivo central, que pode ser um hub ou um switch. Por meio deste, os dados são transmitidos para todos os dispositivos presentes na rede, conforme exibe a figura a seguir:



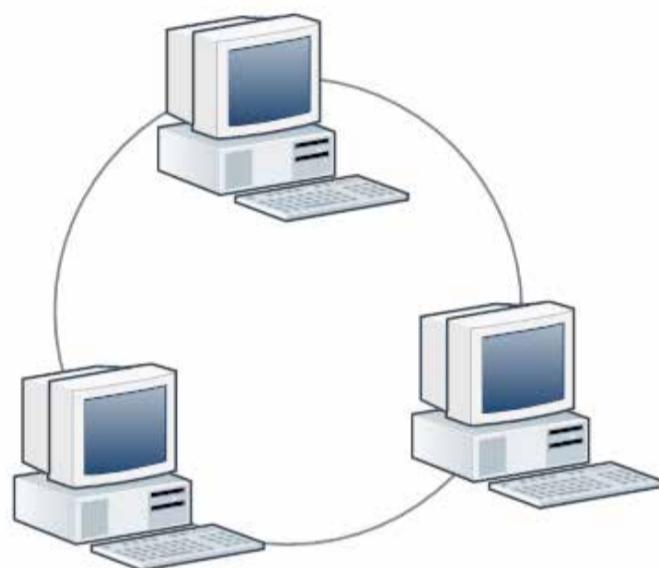
3.8. Topologia estrela

Vejamos, então, os benefícios e possíveis prejuízos do uso desse tipo de topologia:

- **Benefício**
 - Caso um dispositivo falhe, somente ele será impossibilitado de enviar ou receber dados, e não toda a rede;
 - Podemos acrescentar ou remover qualquer dispositivo desta rede sem comprometer a comunicação;
 - Gerenciamento e monitoramento centralizado.
- **Prejuízo**
 - Como toda a comunicação é centralizada em um hub ou switch, se ele falhar, a comunicação de toda a rede será interrompida.

3.3.3. Anel

Uma topologia anel corresponde a dispositivos conectados circularmente por um cabo. Os dados trafegam pelo loop em uma única direção e passam através de cada dispositivo graças à passagem do token.



3.9. Topologia anel

Entendamos melhor esse mecanismo:

1. O dispositivo remetente libera o token (série especial de bits portadores de informações de controle) da rede anelar e envia os dados solicitados ao longo do anel;
2. Cada dispositivo passa os dados adiante, até que o pacote encontre o seu destino;
3. O dispositivo destinatário retorna ao dispositivo remetente uma mensagem confirmando a recepção dos dados;
4. O dispositivo remetente gera um novo token, liberando-o para a rede.

Ainda que possa aliviar o impacto do tráfego intenso gerado na rede, a topologia anel não possibilita que os dados sejam transmitidos a todos os computadores simultaneamente, de forma que o processo deve ser realizado em um micro por vez.

Vejamos, então, os benefícios e possíveis prejuízos do uso desse tipo de topologia:

- **Benefícios**
 - Os computadores têm a mesma prioridade de acesso à rede, porém, apenas acessa quem possui o token;
 - O desempenho da rede não é afetado, mesmo ampliando o número de usuários.
- **Prejuízos**
 - Se houver falha em um único ponto da rede, seja de conector ou computador, afetará toda a rede;
 - Dificuldade para elaborar um diagnóstico e isolar problemas de comunicação.

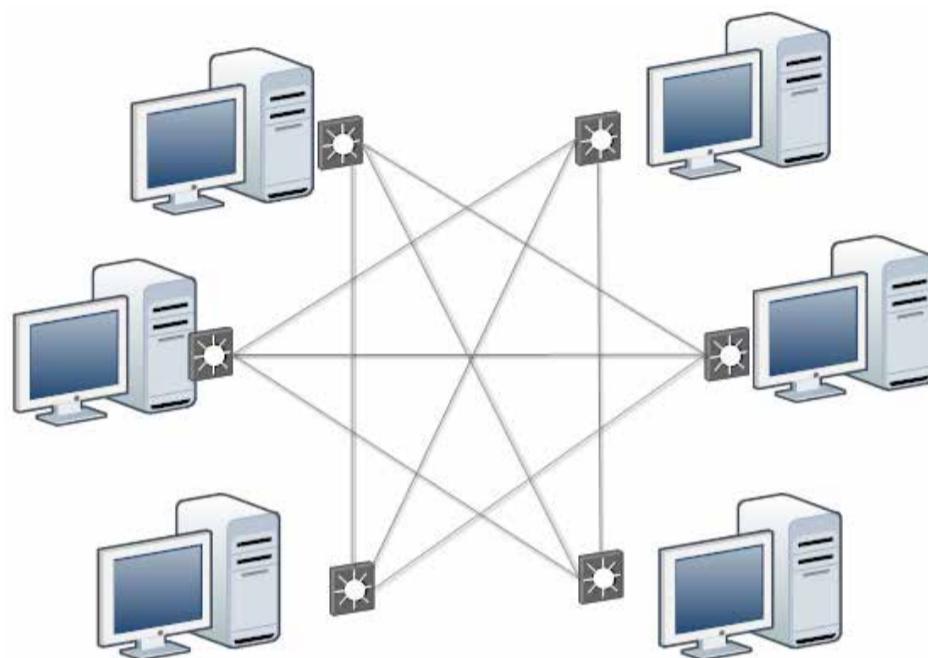
3.3.4. Malha

Na topologia de malha (mesh), é estabelecida uma conexão entre um dispositivo e todos os demais dispositivos da rede. Essa topologia é empregada em situações que requerem estabilidade nas conexões, por exemplo:

- Entre os roteadores;
- Em pontos de acesso de sistemas wireless.

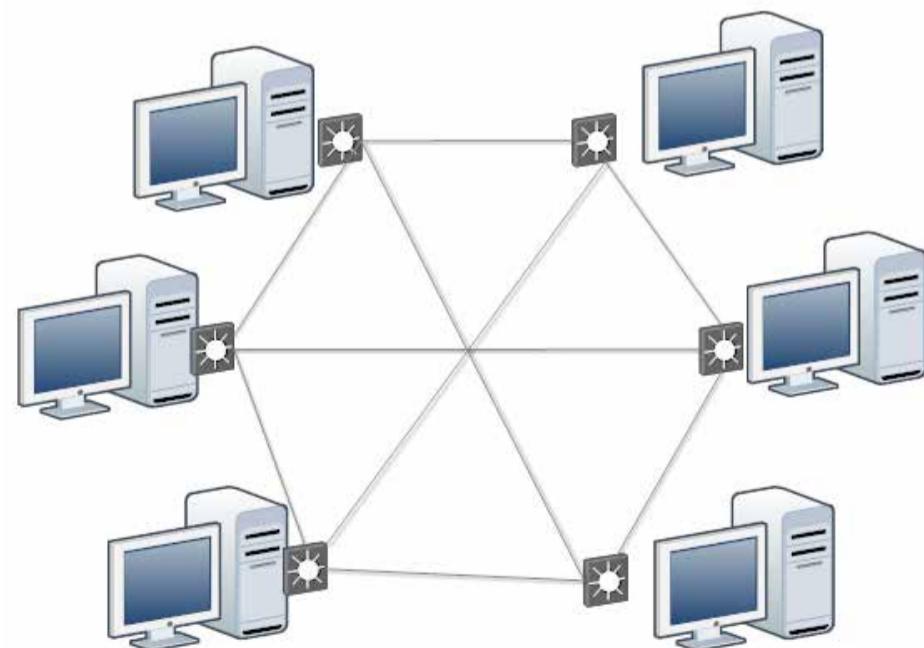
Caso um link falhe, a rede continua funcionando, pois os múltiplos caminhos fornecidos pela topologia de malha disponibilizam rotas alternativas que proporcionam maior tolerância a falhas.

A adoção deste tipo de topologia é para empresas que requerem alto desempenho, bem como disponibilidade. Este modelo é empregado em ambientes que exigem alta disponibilidade, como provedores de acesso à internet, data centers privados ou públicos.



3.10. Topologia malha (mesh)

Contudo, essa estrutura topológica necessita de uma grande quantidade de links, o que torna o seu custo elevado. Para diminuir este custo, temos uma topologia na qual nem todos os dispositivos são interligados entre si. É a chamada malha parcial.



3.11. Topologia malha (mesh) parcial

Vejamos, então, os benefícios e possíveis prejuízos do uso desse tipo de topologia:

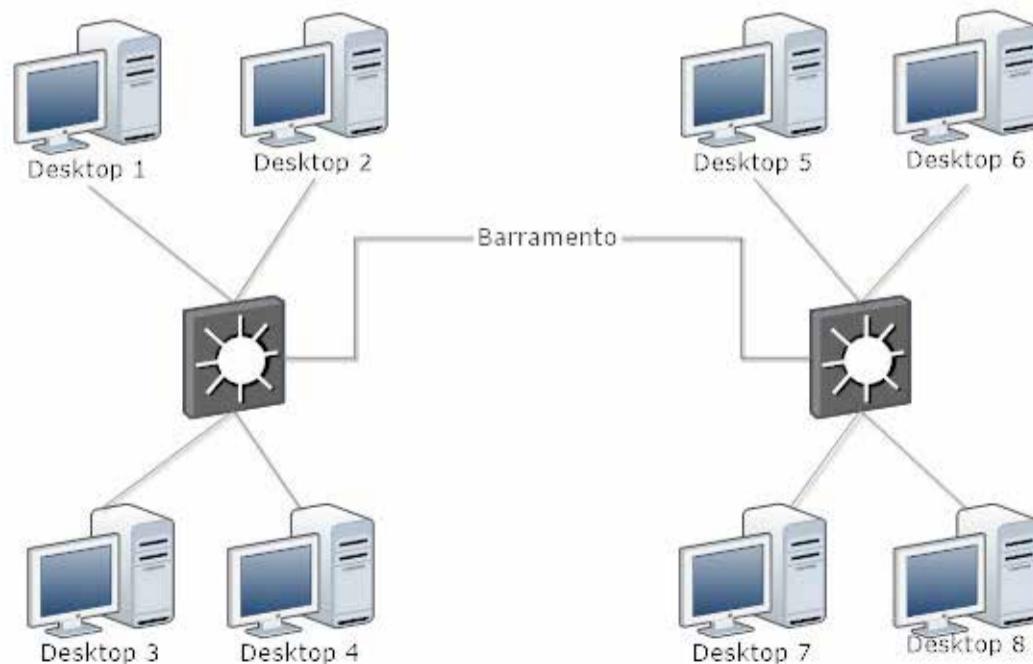
- **Benefícios**
 - Alta disponibilidade;
 - Múltiplos links para trafegar informações, ampliando a velocidade.
- **Prejuízos**
 - Alto custo.

3.3.5. Topologias mistas

Existe a possibilidade de estruturar fisicamente uma rede com a combinação das principais topologias existentes (barramento, estrela e anel). São as denominadas topologias mistas.

3.3.5.1. Barramento-estrela

Duas ou mais redes de topologia estrela podem ser ligadas por intermédio de uma conexão barramento, constituindo uma topologia barramento-estrela.



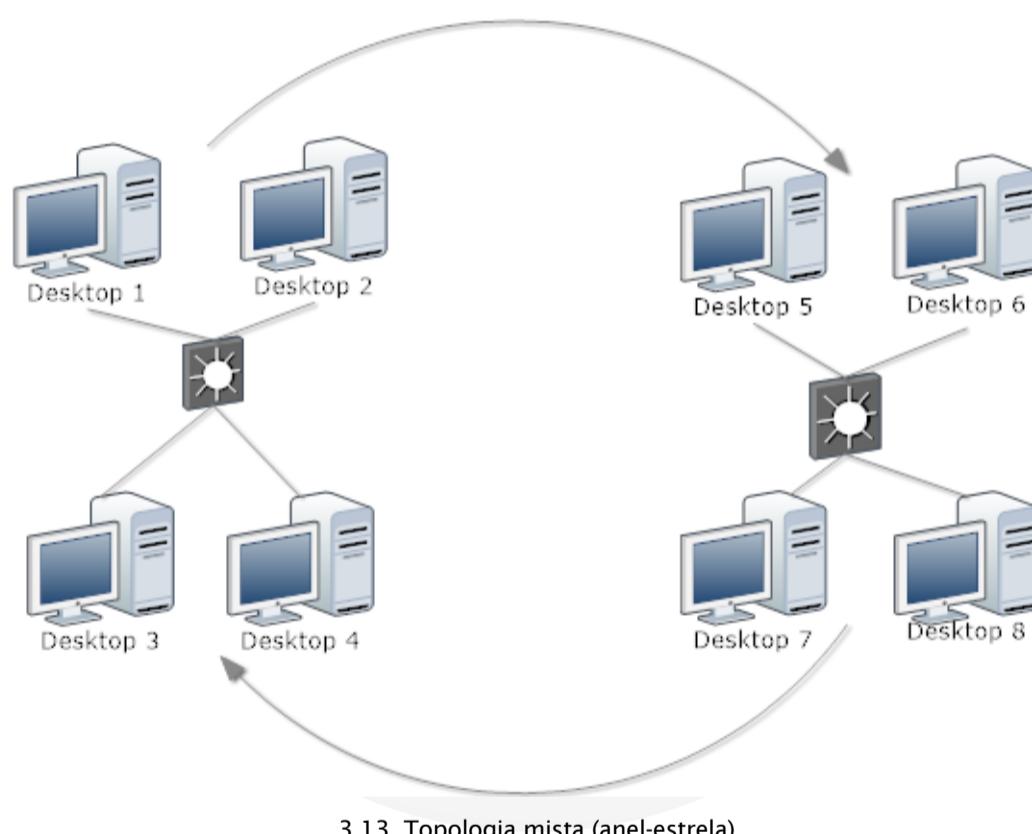
3.12. Topologia mista (barramento-estrela)

Vejamos os pontos positivos e negativos do uso dessa topologia:

- **Positivo:** O restante da rede não é afetado em caso de falha de um dos dispositivos;
- **Negativo:** Caso o hub ou switch de uma das topologias estrela falhe, todos os dispositivos a ele conectados falharão e estarão impossibilitados de estabelecer comunicação com os demais componentes da rede.

3.3.5.2. Anel-estrela

Duas ou mais redes de topologia estrela, dispostas segundo uma rede de topologia anel, constituem uma rede de topologia mista anel-estrela.



3.13. Topologia mista (anel-estrela)

Duas são as vantagens proporcionadas pelo uso dessa topologia:

- O restante da rede não é afetado caso um dos computadores falhe;
- O tráfego através dos cabos da rede é mais eficiente, já que, via passagem token, cada computador possui uma capacidade equivalente de comunicação.

3.4.Tecnologias de rede

Nos tópicos anteriores nós pudemos conhecer as topologias de redes e suas características, entretanto, precisamos conhecer as diferentes tecnologias de rede que podem ser utilizadas para permitir a comunicação de dispositivos entre LANs e WANs. As mais comuns são: Ethernet, X.25, ATM, Frame Relay e SDH. Veremos cada uma delas com mais detalhes nos tópicos a seguir.

3.4.1. Ethernet

A tecnologia Ethernet, também conhecida como IEEE 802.3 e a mais comum em LANs, consiste em uma rede de transmissão que utiliza topologia barramento e apresenta controle descentralizado. Nesse tipo de topologia, ocorre a transmissão de dados entre dois ou mais computadores, sendo que um computador processa as informações, enquanto os demais são programados para rejeitá-las.

Se mais de um computador tentar realizar uma transmissão ao mesmo tempo, utiliza-se um mecanismo arbitrário, que pode ser centralizado ou distribuído, para resolver a questão. No caso da tecnologia Ethernet, os computadores podem enviar seus dados para onde quiserem e se houver uma colisão entre os pacotes de diferentes computadores, estes devem simplesmente aguardar e tentar novamente mais tarde.

O mecanismo utilizado como método de acesso à rede é o Carrier Sense Multiple Access with Collision Detection (CSMA/CD). A tabela a seguir mostra as opções de velocidade em que uma rede Ethernet pode operar:

Topologia	Velocidade
Ethernet	10 Mbps
Fast Ethernet	100 Mbps
Gigabit Ethernet	1 Gbps
10 Gigabit Ethernet	10 Gbps



Nas redes com modo de operação full duplex, o CSMA/CD não é utilizado.

3.4.1.1. CSMA / CD

Quando um computador deseja transmitir uma informação para outro, é necessário que, antes de encaminhá-la, ele saiba se há um canal disponível. Esse processo de encaminhar informações é conhecido como detecção de portadora e obedece a regras que determinam quando o conjunto de informações poderá ser enviado.

Essa regra é conhecida como protocolo de acesso à mídia, que tem a responsabilidade de gerenciar as comunicações em uma rede. Imaginem se, em uma rede com muitos computadores, todos transmitissem informações sem nenhuma regra? Para que não haja perda de performance e a comunicação aconteça com qualidade, o protocolo de controle de acesso à mídia faz esse gerenciamento. Como dito anteriormente, o método utilizado para transmissão pelas redes de computadores Ethernet é o CSMA/CD.

3.4.1.2. Entendendo o funcionamento do CSMA/CD

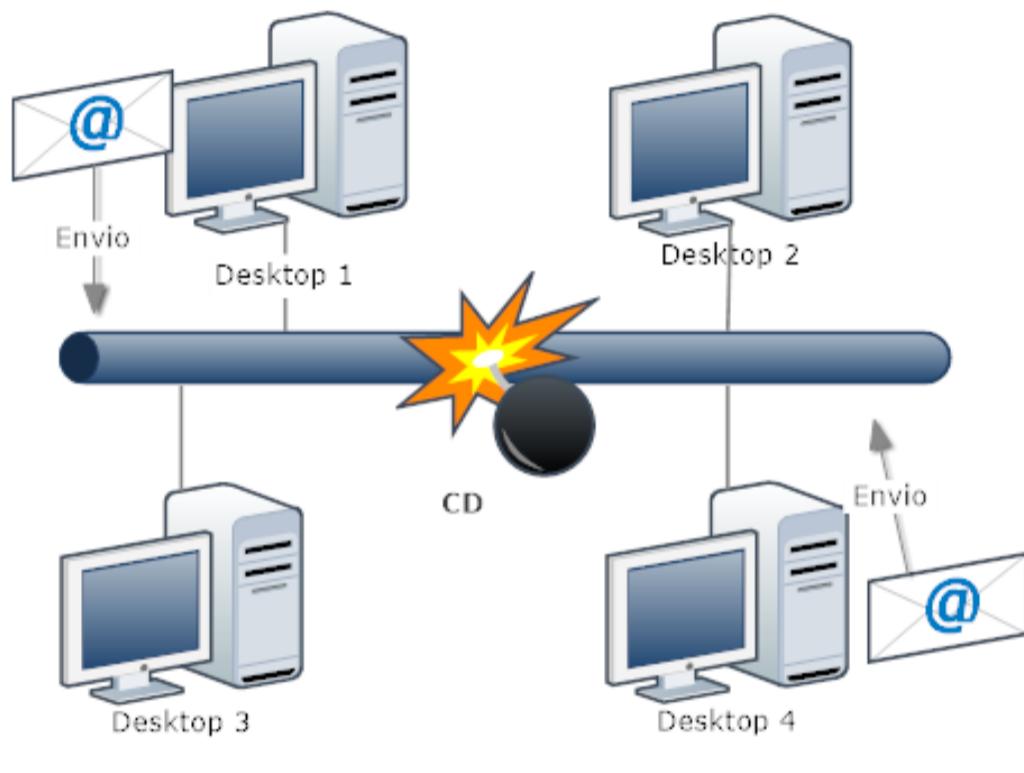
No momento que um computador deseja encaminhar informação, ele faz o processo de Detecção de Portadora Carrier Sense (CS), que tem a responsabilidade de identificar se há canais livres para envio das informações, com a finalidade de mitigar colisões. Se neste processo o canal estiver livre, ele estabelece um tempo preestabelecido para que cada computador envie sua informação em tempos diferentes a fim de evitar colisões.

Já o Multiple Access (MA) foi criado quando ainda tínhamos a rede barramento. O então múltiplo acesso de dados na rede causava a perda de sua integridade, pois gerava colisões. Com o passar do tempo, as redes passaram a utilizar repetidores como Hubs e, finalmente, os switches. Então, o CSMA/CD foi criado para permitir a comunicação de várias máquinas através de um meio compartilhado.

Conceitos e Infraestrutura de Redes (online)

72

O Collision Detection (CD) é o Detector de Colisões. Quando ele entra em cena é porque os sinais de um ou mais computadores, por mais que tenham feito o processo de detecção de portadora e aguardado para transmitir os dados, acabam sendo transmitidos simultaneamente e, como utilizam o mesmo canal, ocorre uma colisão. Os sinais que participaram dessa colisão serão comprometidos e organizados para que sejam encaminhados novamente, mas agora cada um com um tempo novo estabelecido.



3.14. Tecnologia de rede (CSMA/CD)

3.4.2. X.25

O X.25 gera uma rede de extensão mundial apta a destinar pacotes de dados aos endereços determinados. Ele emprega pacotes switching para executar essa transmissão de dados.

Para acessar uma rede X.25, é necessário o emprego do Packet Assembler/Disassembler (PAD) – serviço que possibilita o uso de terminais e modems para efetuar uma conexão, dispensando o hardware do cliente, assim como o plugue de uma linha telefônica na parte traseira do computador. A velocidade de uma rede X.25 varia entre 9,6 Kbps e 2 Mbps.

3.4.3. Frame relay

Trata-se de uma tecnologia de comutação de pacotes que permite a organização de dados através de unidades de tamanho variável conhecidas como frames. Como este protocolo não implementa mecanismos de retransmissão de dados para averiguação de erros, o trânsito de informação pela rede é mais veloz. A velocidade de tráfego dos dados varia entre 64 Kbps e 2 Mbps.

A tecnologia Frame Relay é um padrão desenvolvido pelo American National Standards Institute (ANSI), que define um conjunto de processos para transmissão de dados por uma rede de dados pública (PDN). Nesta tecnologia, a transmissão de dados ocorre de forma eficiente e com alto desempenho. Ela é mundialmente conhecida pela sua capacidade de gerenciamento de canais virtuais.

Com o Frame Relay, a forma de enviar as informações através da WAN ocorre por meio da divisão dos dados em pacotes. Cada pacote é transmitido através de uma série de switches Frame Relay, a fim de que alcancem o destino, operando nas camadas física e de enlace do modelo de referência OSI. Como ele próprio não corrige erros, torna-se dependente de protocolos de camada superior, como o TCP, para efetuar tal correção.

O Frame Relay é um serviço orientado à conexão. Ele utiliza circuitos virtuais para estabelecer a conexão e vários circuitos PVC (Permanent Virtual Circuit, ou circuito virtual permanente), nos quais a largura de banda desejada é definida com base na velocidade média de transmissão, chamada de CIR (Committed Information Rate, ou taxa de informação comissionada). Para alcançar esse objetivo, o processo de encapsulamento entre os dispositivos é realizado por meio do High-Level Data Link Control (HDLC).

A rede que fornece a interface do Frame Relay pode ser uma rede pública de serviços telefônicos ou uma rede de equipamentos privados, que serve a uma única empresa.

Uma rede Frame Relay pode incluir computadores, servidores etc., do lado do usuário, além de dispositivos de rede Frame Relay, como switches, roteadores, CSU/DSUs ou multiplexadores. Ela é representada como uma nuvem de Frame Relay, conforme figura 3.15.

3.4.4. ATM

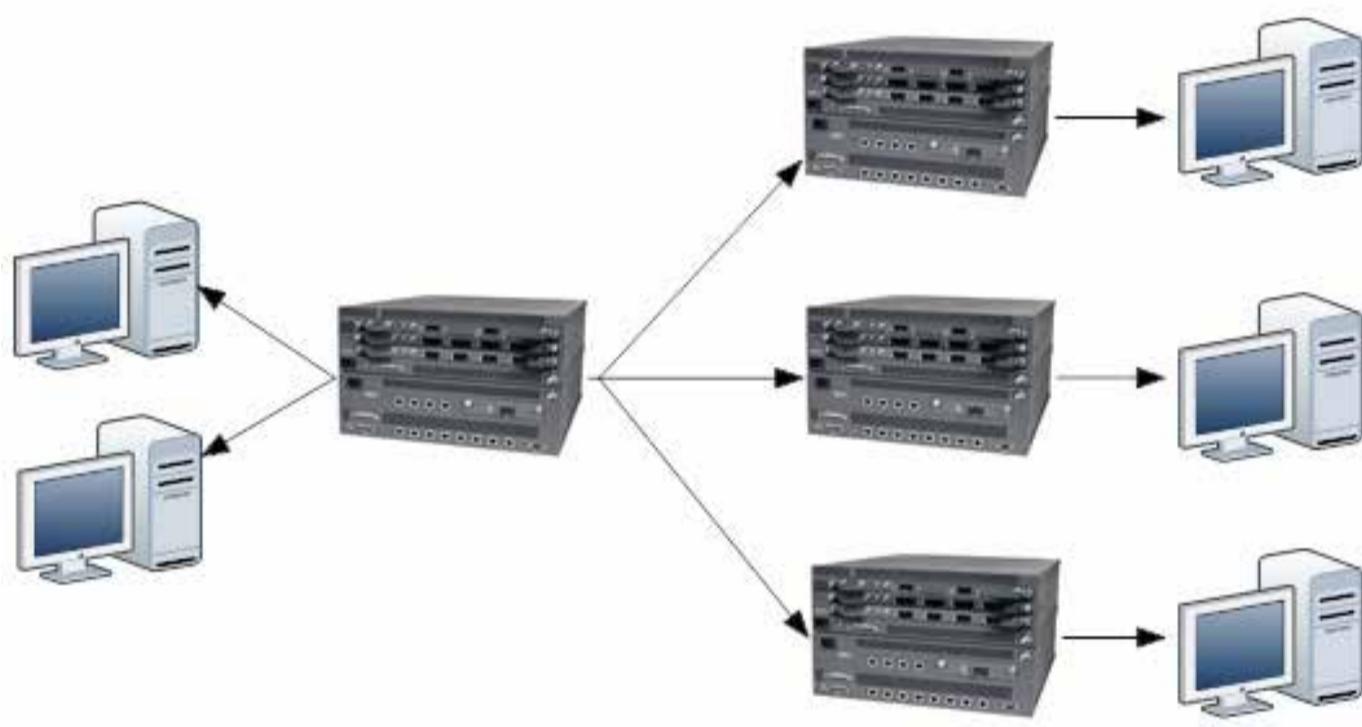
A arquitetura Asynchronous Transfer Mode (ATM) utiliza como método de acesso à rede o processo ponto a ponto, em que a transferência de pacotes de um computador para outro é feita através do dispositivo ATM switch. Essa arquitetura tornou-se uma tecnologia de uso muito significativo nas décadas anteriores em função de sua capacidade de transmissão, pois permite integração de funções de LANs e WANs para transmissão de dados, voz e vídeo com alta performance e escalabilidade.

Conceitos e Infraestrutura de Redes (online)

74

Com a crescente demanda de consumo de rede e a necessidade cada vez mais elevada de transferências de dados, no fim da década de 80 foi criada a tecnologia ATM, que é composta por equipamentos de usuários, equipamentos de acesso com interface ATM e equipamentos de Rede que, somados, permitem uma composição de alta velocidade.

Devemos ressaltar que, ao contrário dos pacotes enviados em outras arquiteturas, os pacotes enviados pela rede ATM possuem tamanho fixo e contêm apenas informações básicas do caminho. Como resultado, temos a transmissão de pacotes compactos de dados em uma velocidade que varia entre 25 Mbps e 622 Mbps.



3.15. Arquitetura ATM

3.4.5. SDH

Uma rede SDH (Synchronous Digital Hierarchy) pode ser definida como uma junção de equipamentos e meios físicos para a transmissão de informações em um sistema digital síncrono, fornecendo uma infraestrutura básica para redes de dados e voz. Atualmente, esse tipo de rede é utilizado em diversas empresas prestadoras de serviços de telecomunicações.

A tecnologia SDH é usada para multiplexação TDM com altas taxas de bits. A fibra óptica é o meio físico preferencial na transmissão de dados para esse tipo de tecnologia. Porém, existem interfaces que permitem o uso de outros meios físicos de transmissão, como, por exemplo, enlaces de rádios.

Além do próprio sistema SDH (nas taxas de 155 Mbit/s, 622 Mbit/s, 2,5 Gbit/s e 10 Gbit/s), essa tecnologia também permite interfaces compatíveis com os sistemas europeu (nas taxas de 2, 8, 34 e 140 Mbit/s) e americano (nas taxas de 1,5 Mbit/s, 6 Mbit/s e 45 Mbit/s).



Teste seus conhecimentos Modelos, topologias e tecnologias de rede

3

1. Suponha que você foi solicitado a montar uma rede para atender seis usuários, que ela deverá ser de baixo custo de implantação, sem a necessidade de um administrador de rede e na qual todos os usuários poderão compartilhar arquivos e periféricos. Qual o modelo de rede a ser implantada?

- a) Cliente-servidor
- b) Não hierárquico
- c) Ethernet
- d) Barramento
- e) Estrela

2. Considere a seguinte afirmação: como toda a comunicação é centralizada, quando um dispositivo falha, somente ele é impossibilitado de enviar e receber dados. Essa é uma característica de qual topologia de rede?

- a) Ethernet
- b) LAN
- c) Estrela
- d) Thick client
- e) Servidor blade

3. Na topologia Fast Ethernet, a que velocidade se pode operar?

- a) 10 Mbps
- b) 100 Mbps
- c) 1 Gbps
- d) 10 Gbps
- e) Todas as alternativas anteriores estão corretas.

4. Qual topologia é empregada em situações que requerem estabilidade nas conexões?

- a) ATM
- b) SDH
- c) X25
- d) Barramento
- e) Malha

5. Considere a seguinte afirmação: um único chassis pode ser equipado com diversas placas e cada uma delas funciona como um servidor independente. Qual tipo de equipamento está sendo citado?

- a) Servidores appliance.
- b) Servidores de arquivos.
- c) Servidores de e-mail.
- d) Servidores blade.
- e) Servidores torre.

Transmissão de dados

4

- ✓ Vias de transmissão;
- ✓ Modos de transmissão;
- ✓ Sentidos da transmissão;
- ✓ Tipos de sinais;
- ✓ Problemas na transmissão de sinais;
- ✓ Tipos de banda.

4.1. Introdução

O processo de comunicação entre dois ou mais computadores ocorre através da transmissão de dados. Esse é um dos principais objetivos de uma rede de computadores. Tal processo envolve uma série de análises e devemos decidir sobre como ele ocorrerá, como serão as vias de acesso, o modo de transmissão e o sentido (regras) da transmissão, sendo que, para estes itens, podemos definir os seguintes tipos:

Vias de transmissão	Serial; Paralela.
Modos de transmissão	Síncrona; Assíncrona.
Sentidos da transmissão	Simplex; Half-duplex; Full-duplex.
Banda	Base; Larga.

Ao longo desta leitura, apresentaremos adiante esses conceitos de rede mais detalhadamente, a começar pelas vias de transmissão.

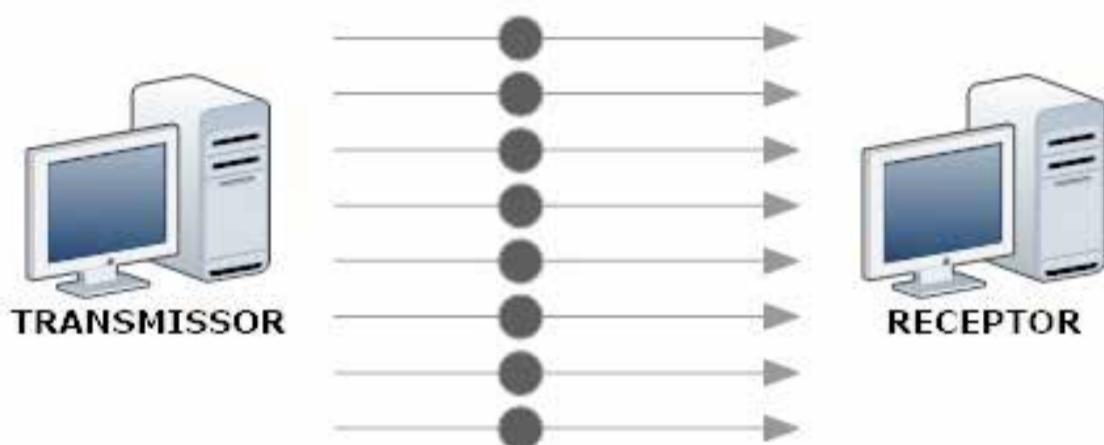
4.2. Vias de transmissão

Em redes de computadores, é possível transmitir dados por duas vias: serial e paralela. Cada uma delas possui características específicas, relacionadas à taxa de velocidade. A seguir, trataremos de cada uma delas.

4.2.1. Transmissão paralela

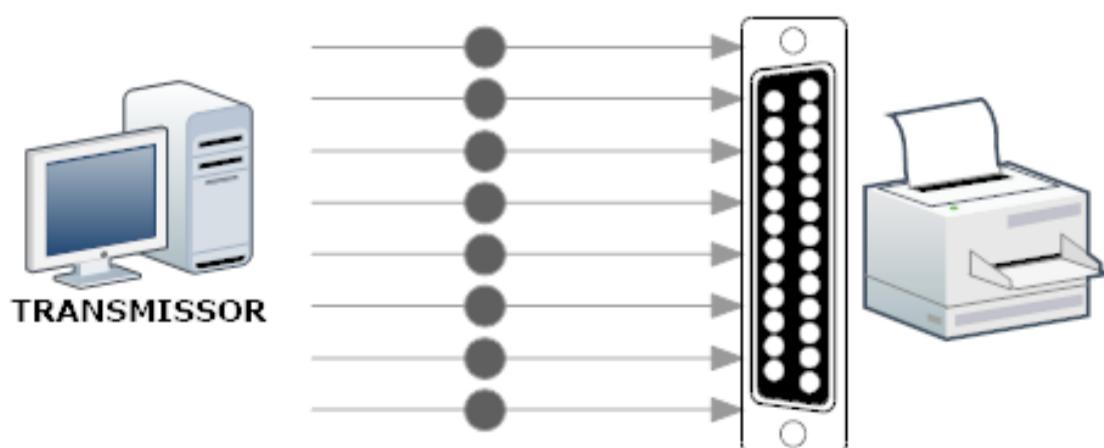
A transmissão paralela é aquela na qual um transmissor envia, de uma só vez, uma determinada quantidade de bits para um receptor. Essa quantidade é definida pela capacidade de transmissão de bits do transmissor, sendo que o receptor deve possuir a mesma capacidade para que aconteça a transmissão.

É importante considerarmos que, na transmissão paralela, cada bit corresponde a um fio. Quanto maior a quantidade de bits, maior será a quantidade de fios necessária em uma transmissão paralela. Dessa forma, no esquema apresentado, são necessários oito fios entre o transmissor e o receptor. Isso faz com que a transmissão paralela seja muito dependente do meio físico utilizado, ou seja, do sistema de fios.



4.1. Transmissão paralela

Esse modelo de transmissão, pela sua característica, é usado por dispositivos que utilizam cabos curtos, e foi amplamente utilizado para conectar dispositivos de impressão através da porta paralela, em que o volume de dados de impressão era encaminhado, de uma única vez, do desktop para a impressora. No entanto, esse modelo de transmissão pode ser utilizado tanto para controlar dispositivos quanto para realizar a comunicação propriamente dita.



4.2. Transmissão paralela

Além disso, devemos considerar que os fios geralmente são dispostos lado a lado, o que pode causar interferência eletromagnética entre eles, corrompendo os dados transmitidos. Para lidar com esse problema, há sistemas de correção de erros. Contudo, isso faz com que a transmissão fique mais lenta, pois, sempre que os dados chegarem corrompidos ao receptor, ele pedirá uma nova transmissão dos dados. Por conta disso, a transmissão paralela deve utilizar fios curtos, evitando degradação de sinal e diminuindo a incidência de erros na transmissão.

No entanto, a transmissão paralela é considerada a mais custosa e mais complexa porque, para executar o processo de transmissão, ela requer mais de um canal de comunicação. Apesar disso, é uma transmissão que possui maior velocidade.

4.2.2. Transmissão serial

A transmissão serial (ou em série) requer apenas um fio para que os dados trafeguem entre o transmissor e o receptor. Nesse modelo de transmissão, o processo ocorre com mais lentidão, pelo fato de utilizar um único canal para realizar a comunicação.

Esse processo de transmissão em série é mais simples, pois utiliza apenas um canal de comunicação para sua transmissão. No entanto, possui menor velocidade de transmissão. Enquanto que na paralela os bits são enviados de uma só vez, na serial eles são enviados um a um.

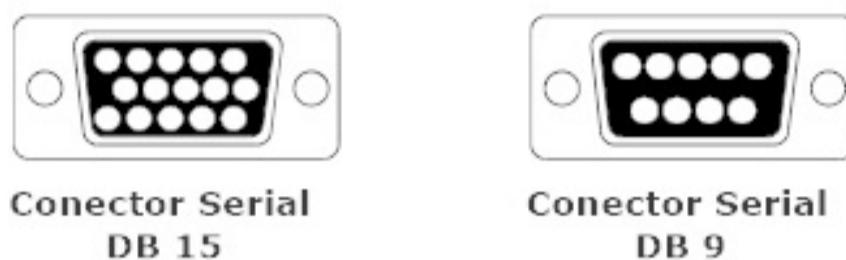
Porém, ao contrário da comunicação paralela, a serial possibilita um maior comprimento de cabo e pode usar apenas um canal de transmissão (fio).



4.3. Transmissão serial

Por essas características, a transmissão serial é utilizada em dispositivos externos, como mouse, teclado e portas USB, que precisam de cabos longos. Ela é também o tipo de transmissão utilizada em redes locais.

A transmissão serial utiliza normalmente conectores do tipo DB 15 ou DB9, conforme exibido na figura a seguir. A velocidade das comunicações seriais é medida em bps (bits por segundo), que indica a quantidade de bits enviados, por segundo, do transmissor ao receptor.



4.4. Conectores (porta serial)

4.3. Modos de transmissão

Os modos de transmissão estão relacionados à sincronização de sinais digitais para transmissão. Os métodos utilizados normalmente são determinados pelo equipamento envolvido. Tais modos são a transmissão assíncrona e a transmissão síncrona, as quais veremos a seguir.

4.3.1. Transmissão assíncrona

Na transmissão assíncrona, não há uma relação precisa de tempo entre os caracteres de informação que são enviados. Além disso, cada um deles carrega sinais de inicialização e finalização.

Como exige que uma combinação de bits de inicialização e finalização seja adicionada a cada stream de dados, a transmissão assíncrona é menos eficiente do que a transmissão síncrona. Contudo, é de fácil implementação em sistemas com menos de 20 Kbps. Esse método possui uma interface padronizada comum e protocolo entre máquinas, o que o torna popular entre usuários de computador.

4.3.2. Transmissão síncrona

Na transmissão síncrona, os bits de dados são sincronizados em fase ou em uníssono, com pulsos ou sinais de clock uniformemente espaçados. Esses sinais impedem a confusão entre os caracteres no fluxo de dados. Para isso, é necessário que o transmissor e o receptor sejam capazes de realizar sincronização e timing.

Esse método é utilizado em sistemas digitais de transmissão em banda base e, diferentemente da transmissão assíncrona, não exige bits de inicialização e finalização, por isso é mais eficiente.

4.4. Sentidos da transmissão

Para que a comunicação ocorra em uma via, deve haver circuitos disponíveis. Nesse circuito há um conjunto de regras que definem o sentido da transmissão, o qual podemos classificar pela forma que ele ocorre, pelo sentido do envio das informações, se é sentido único ou simultâneo e se é sincronizado ou não com o receptor e o transmissor. Essa classificação é conhecida como simplex, half-duplex ou full-duplex.

4.4.1. Simplex

Uma transmissão simplex é caracterizada por ser unidirecional, o que significa que os sinais são transmitidos em apenas uma direção. Os dados trafegam do transmissor para o receptor, mas este não pode responder. Um exemplo disso são os sistemas de transmissão por meio de alto-falantes.



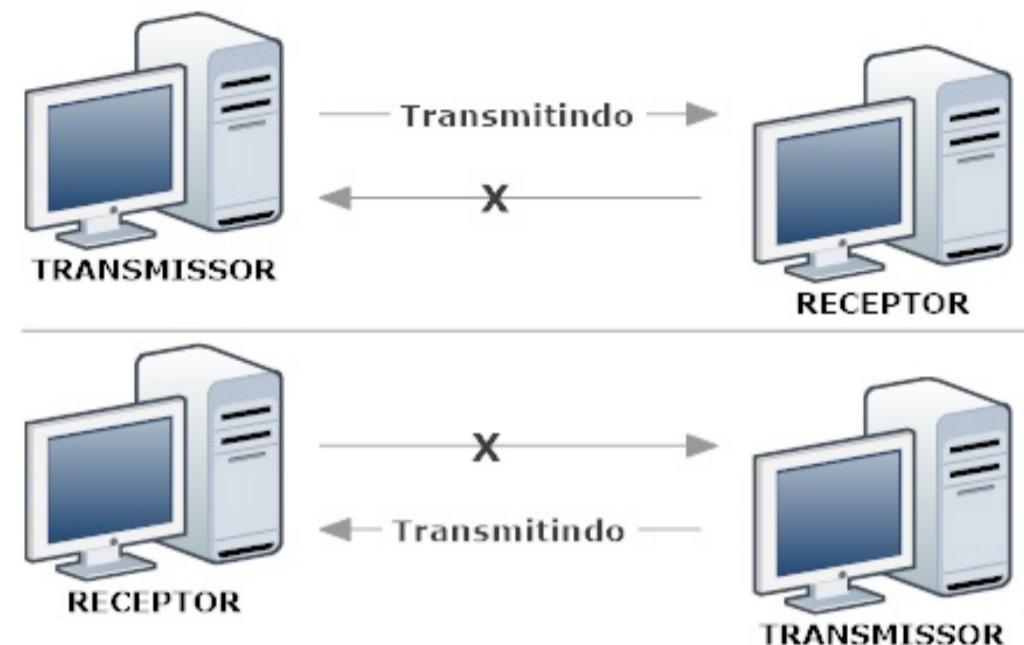
4.5. Transmissão simplex

4.4.2. Half-duplex

A transmissão half-duplex é bidirecional e, portanto, os sinais podem ser transmitidos em ambas as direções. Contudo, eles só são transmitidos em uma direção de cada vez.

Essa característica exige certo consentimento entre as partes que se comunicam. Geralmente, em circuitos de voz, emprega-se um dispositivo que permite iniciar a transmissão (push-to-talk). Além disso, utilizam-se, também, protocolos de sinalização.

Um exemplo desse tipo de transmissão são os intercomunicadores de casa e os walkie-talkies.



4.6. Transmissão half-duplex

4.4.3. Full-duplex

A transmissão full-duplex também é bidirecional. Mas, diferentemente da transmissão half-duplex, permite que os sinais trafeguem simultaneamente em ambas as direções, possibilitando que ambos os envolvidos na comunicação possam enviar e receber ao mesmo tempo. O exemplo mais comum disso é o telefone.

O processo de transmissão, através da comunicação, no modelo full-duplex permite que o fluxo dos dados, que é bidirecional, aumente a carga de transferência de informações, já que os dados podem ser enviados e recebidos ao mesmo tempo. Assim, há um ganho de desempenho significativo em relação aos modelos discutidos anteriormente. Esse ganho pode ser obtido através da redução do tempo de espera entre as transmissões, como ocorre no half-duplex, por exemplo.



4.7. Transmissão full-duplex

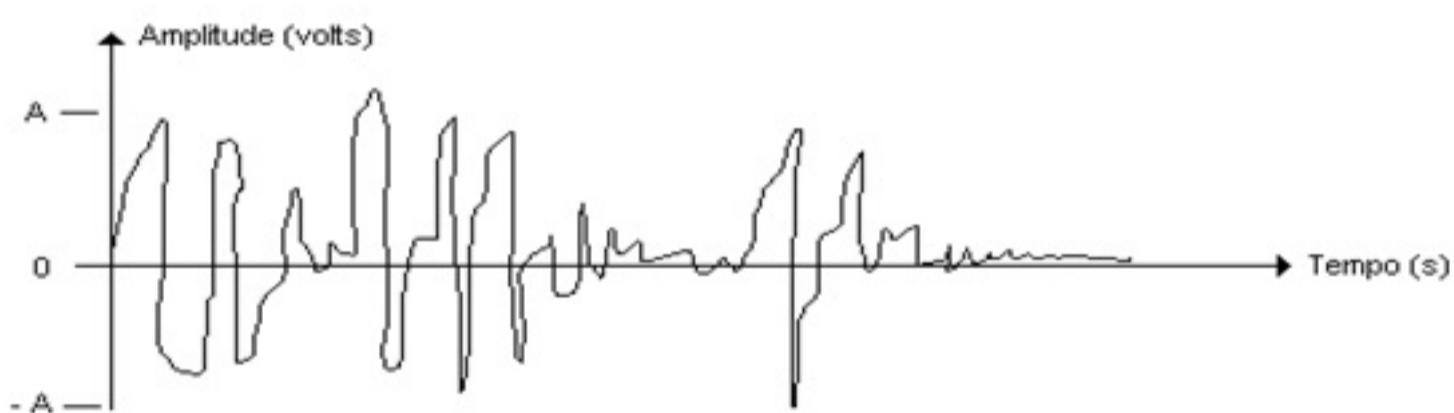
4.5. Tipos de sinais

Os sinais em uma transmissão podem ser de dois tipos: analógicos ou digitais. Vejamos, adiante, uma breve abordagem de cada um deles.

4.5.1. Sinal analógico

As informações analógicas têm valores que podem variar em um intervalo de $-\infty$ a $+\infty$, ou seja, elas podem representar qualquer valor. As informações no mundo real, como som e luz, são informações desse tipo.

Como um sinal analógico pode assumir qualquer valor, conforme visto na figura a seguir, o receptor de uma transmissão não pode verificar se o sinal recebido está ou não correto. Assim, ele pode aceitar como correta uma informação que tenha sido corrompida por um ruído na transmissão (a interferência eletromagnética em um fio, por exemplo).

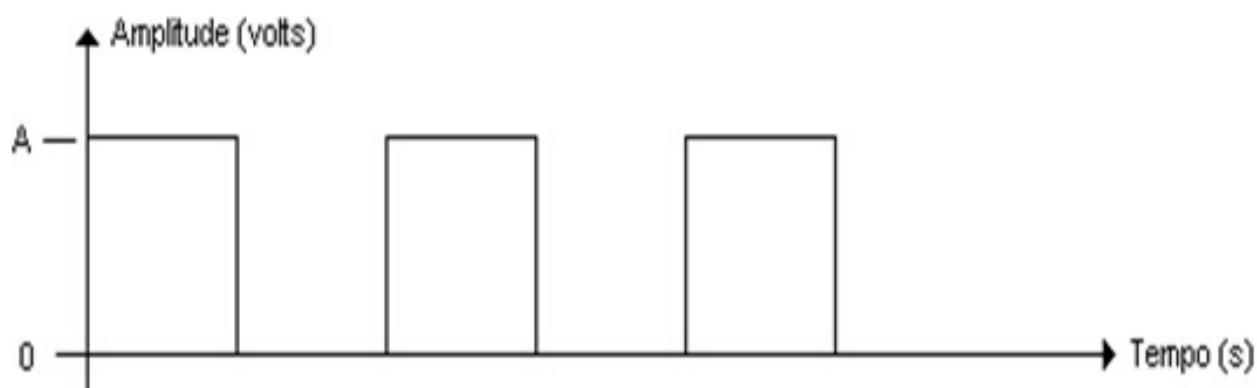


4.8. Sinais analógicos

As fontes que podem gerar interferência são diversas (como, por exemplo, fios situados ao lado de um fio que esteja transmitindo informações), o que torna a transmissão analógica inviável para sistemas de computadores.

4.5.2. Sinal digital

Os computadores utilizam informações digitais que, diferentemente das informações analógicas, só aceitam dois valores, 0 e 1. Qualquer valor diferente disso pode ser descartado pelo receptor.



4.9. Sinais digitais

Fisicamente, os valores 0 e 1 são representados por tensões elétricas, sendo que 0 possui tensão elétrica de 0 volt e 1 possui tensão de 5 volts.

A transmissão digital, na verdade, é feita por meio de números, pois essa é a única linguagem que os computadores entendem. Qualquer tipo de informação transmitida entre computadores, como texto e imagem, é transmitido como uma sequência de números 0 e 1 e transformada novamente em dados comprehensíveis pelo receptor. É justamente por serem números que o receptor pode utilizar mecanismos de correção de erro e verificar se os dados transmitidos estão ou não corretos.

Os valores 0 e 1 usados para informações digitais constituem números chamados binários. Os algarismos que compõem os números binários são chamados bits (contração de binary digit). Como os números binários possuem apenas dois algarismos (0 ou 1), eles são representados na base 2.

As palavras binárias possuem uma nomenclatura própria, que varia de acordo com a quantidade de bits presentes:

Quantidade de bits	Nome
4	Nibble
8	Byte
16	Word
32	Double Word
64	Quad Word

Assim, podemos dizer que uma transmissão de um nibble equivale à transmissão de quatro bits, ou seja uma sequência de quatro algarismos 0 e 1.

4.5.2.1. Modulação de dados

Dependendo do meio utilizado na conexão entre computadores, os números digitais podem ser transmitidos na forma de impulsos elétricos, impulsos ópticos ou ondas de rádio, entre outros. Muitas vezes, eles precisam ser transformados em sinais analógicos para que sejam transmitidos. Isso é chamado de modulação de dados, que é um processo de codificação e decodificação do sinal. Para esse processo há alguns tipos de modulação de pulso. Um dos mais conhecidos é o PCM (modulação por código de pulso – Pulse Code Modulation), que possui algumas variações, como a PAM (modulação por amplitude de pulso – Pulse Amplitude Modulation), PWM (modulação por largura de pulso – Pulse Width Modulation), PPM (modulação por posição de pulso – Pulse Position Modulation) e DM (modulação por atraso de pulso – Delay Modulation).

Ao passo que a modulação é a modificação da amplitude, frequência e/ou fase de uma onda (elétrica, de rádio etc.) para que o sinal possa ser transportado, o processo de demodulação é exatamente o inverso, permitindo que o processo de modulação seja revertido.

Ao receber os dados analógicos (originalmente digitais), o receptor deve demodulá-los, transformando-os novamente em dados digitais. Isso permitirá ao receptor verificar se os dados recebidos estão ou não corrompidos. Caso isso aconteça, o receptor pode solicitar uma retransmissão dos dados.

Esse tipo de transmissão é comumente utilizado em computadores, por meio do modem (Modulador/Demodulador), que transmite os dados digitais através de um canal analógico, a linha telefônica. Em redes locais, a placa de rede é responsável pela modulação e demodulação de dados.

4.6. Problemas na transmissão de sinais

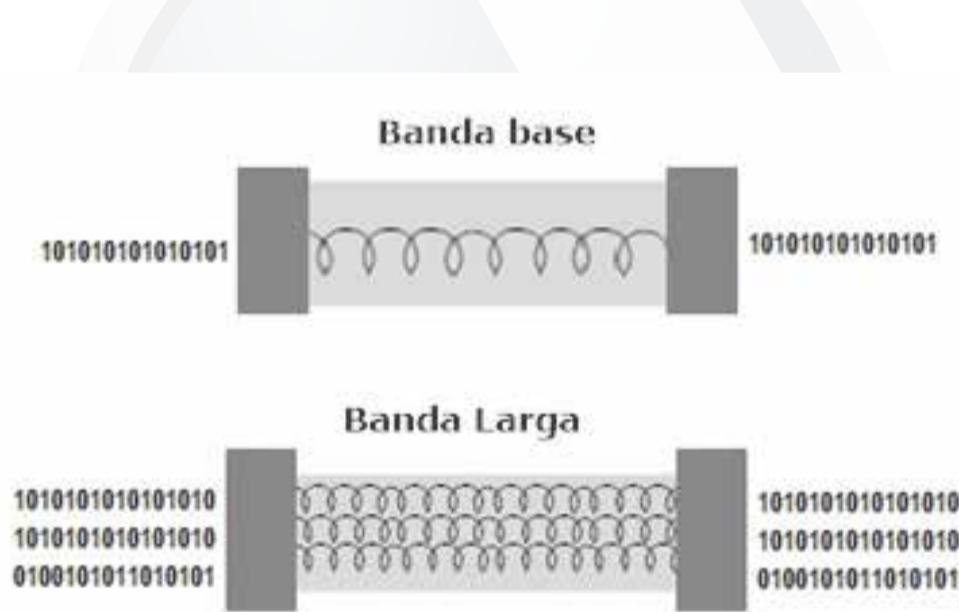
Alguns problemas podem comprometer a transmissão de sinais no meio de comunicação. Nesse contexto, os sinais analógicos e digitais, sendo afetados, tornam o restante do processo irregular. A seguir, listamos os problemas que prejudicam a transmissão, em termos da qualidade e do próprio meio em que ela se dá:

- **Atenuação:** É a diminuição da intensidade ou amplitude do sinal transmitido que é ocasionada pela distância;
- **Distorção:** É a alteração do sinal provocada por uma resposta imperfeita do sistema. Esse fenômeno não deve ser visto como um ruído e menos ainda como uma interferência, mas apenas como o produto de falhas no sistema de transmissão;

- **Interferência:** É a atuação de sinais estranhos ao sistema de transmissão. A influência que eles exercem sobre o sistema se deve ao fato de possuírem o mesmo tipo e frequência do sinal transmitido. Tal fenômeno é recorrente quando o meio de transmissão é o ar;
- **Ruído:** O agente causador do ruído pode estar situado no interior ou no exterior do sistema de transmissão. Às vezes, o ruído bloqueia a comunicação, devido à propriedade que ele tem de ocultar o seu próprio sinal. Por essa razão, é difícil combatê-lo.

4.7. Tipos de banda

Existem duas formas de alocação da capacidade de transmissão de dados, que são conhecidas como banda base e banda larga. A banda base envia um único sinal e este percorre o cabo de cada vez, utilizando a totalidade da largura de banda existente. Já na banda larga, seu sinal é analógico e, em vez de ocupar uma única frequência como a banda base, ela ocupa uma faixa de frequências, como explicado a seguir.



4.10. Banda base x Banda larga

4.7.1. Banda base

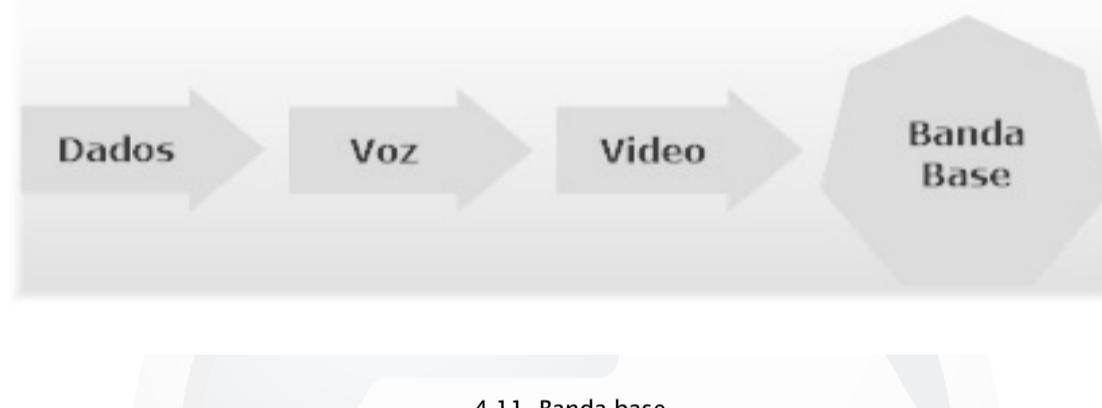
A banda base é utilizada para a transmissão bidirecional de informações, principalmente em LANs, visto que o seu método de transmissão não é o mais adequado para vencer grandes distâncias.

Conceitos e Infraestrutura de Redes (online)

90

Os sinais transmitidos por esse método estão em formato digital e possuem uma só frequência. Um sinal individual percorre o cabo de cada vez, e a totalidade da largura de banda existente nesse cabo é aproveitada.

Quando os dados são transmitidos, pode ocorrer uma certa diminuição na intensidade dos sinais, provocando falhas na comunicação e colocando em risco a confiabilidade da rede, do processo e das informações. Para sanar esse problema, é possível utilizar um ou mais repetidores conectados aos cabos, que recuperarão a intensidade do sinal recebido e farão a retransmissão dos dados com a intensidade que tinham no início da transmissão.



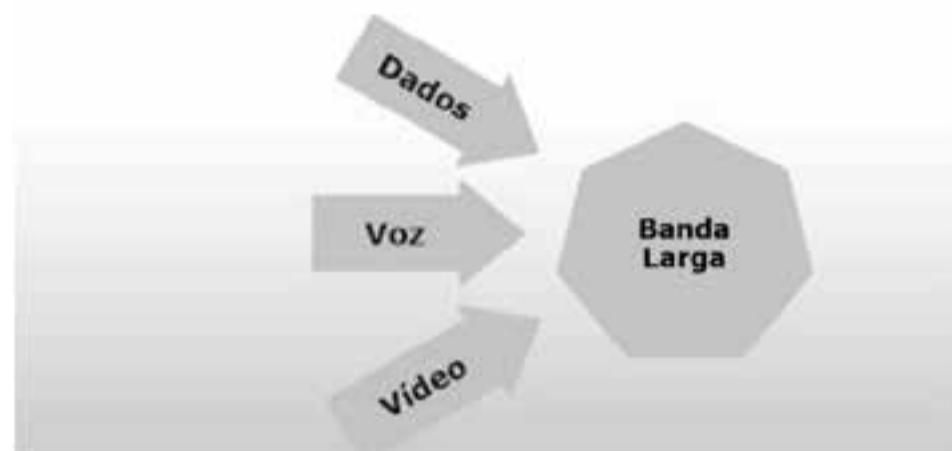
4.7.2. Banda larga

Ao analisarmos os pormenores relativos à transmissão em banda larga, chegamos à conclusão de que esta oferece soluções opostas àquelas oferecidas pela banda base.

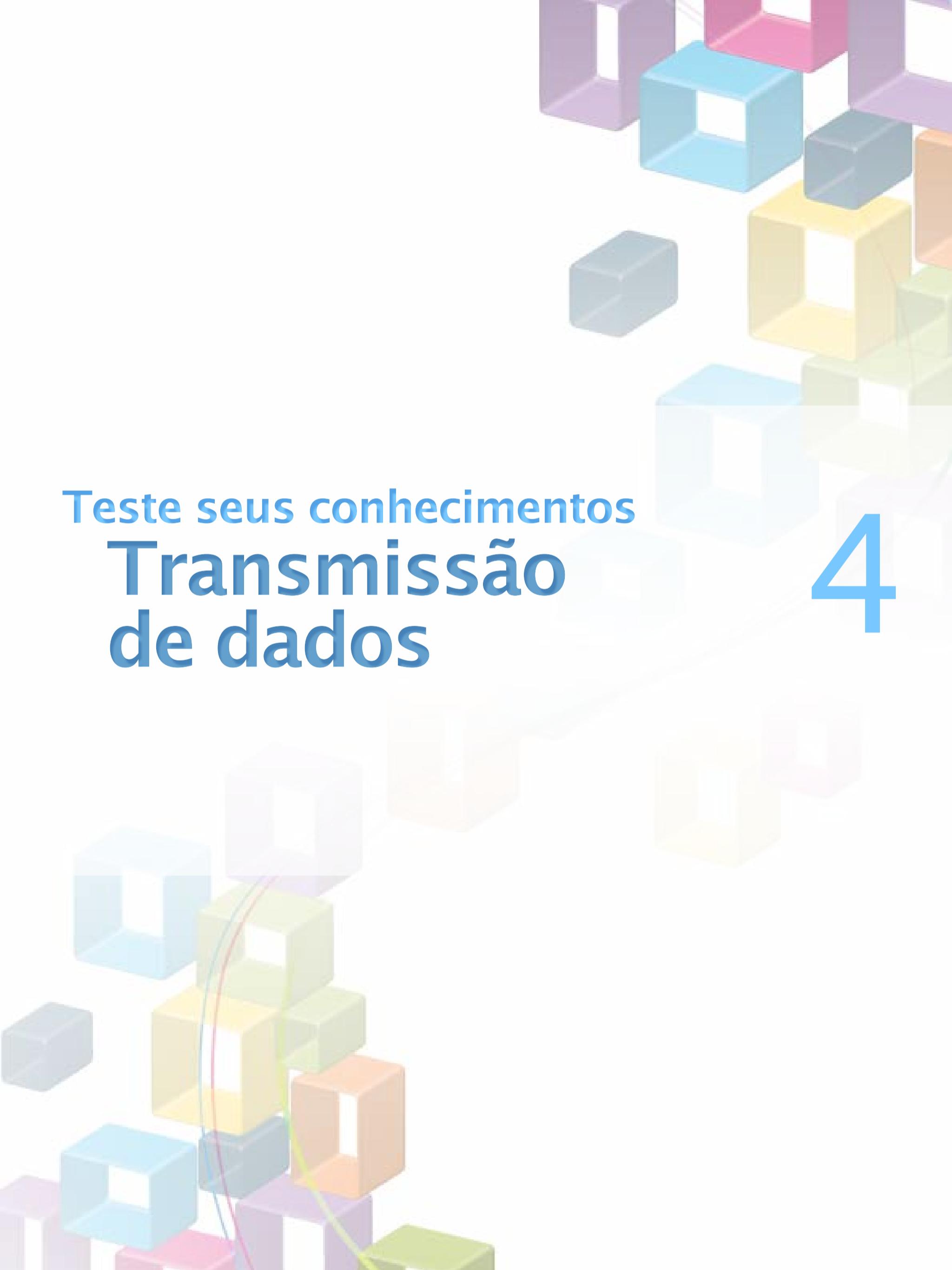
Vamos começar mostrando as diferenças em relação ao sinal transmitido por banda larga, que é analógico e, em vez de ocupar uma única frequência, ocupa uma faixa de frequências. Outro ponto importante que podemos citar é que, em um sistema de banda larga, um sinal pode ser uma onda óptica ou eletromagnética, ao passo que, em um sistema de banda base, um sinal vem a ser um pulso elétrico ou composto por luz.

Ao contrário do sistema de banda base, no sistema de banda larga é necessária a utilização de dois cabos diferentes para que um dispositivo possa enviar e receber sinais, sendo que cada cabo é responsável por uma dessas tarefas, ou que a configuração da banda seja feita de modo que sua largura possa ser dividida. Assim, dois canais poderão ser utilizados, um para cada tarefa. Caso nos decidamos pela segunda opção, estaremos criando dois canais de largura de banda, sendo que, para se diferenciarem entre si, cada um desses canais opera em uma faixa, ou mesmo em uma frequência particular.

Para finalizar, outras duas diferenças a serem lembradas: a intensidade dos sinais transmitidos por meio de sistemas de banda larga também pode enfraquecer ao passo que percorrem os cabos, mas, em lugar de repetidores, são utilizados amplificadores de sinais; por fim, devido à grande velocidade por meio da qual um sinal pode ser transmitido, este sistema pode ser satisfatoriamente utilizado em MANs ou WANs.



4.12. Banda larga



Teste seus conhecimentos Transmissão de dados

4

1. Qual o tipo de alocação de banda utilizada para transmissão de dados em uma rede local?

- a) Simplex
- b) Half-duplex
- c) Full-duplex
- d) Banda base
- e) Banda larga

2. Qual das alternativas a seguir lista características da banda larga?

- a) Sinal analógico, uma só frequência e utilização em LANs.
- b) Sinal digital, normalmente utilizado em MANs ou WANs e largura de banda dividida para transmissão e recepção.
- c) Sinal analógico, uma só frequência e utilização em MANs ou WANs.
- d) Sinal digital, normalmente utilizado em LANs e largura de banda dividida para transmissão e recepção.
- e) Sinal analógico, normalmente utilizado em MANs ou WANs e largura de banda dividida ou cabos diferentes para transmissão e recepção.

3. Considere a seguinte afirmação: os sinais podem ser transmitidos em ambas as direções, porém, não simultaneamente. Ela está relacionada à qual sentido de transmissão?

- a) Full-duplex
- b) Half-duplex
- c) Simplex
- d) Síncrono
- e) Assíncrono

4. Considere a seguinte situação: em uma rede local, todos os dispositivos transmitem e recebem dados através da tecnologia Ethernet e estão interligados utilizando a topologia barramento. Respectivamente, qual a via e o sentido da transmissão, e qual o tipo de banda que estão sendo utilizados?

- a) Serial, full-duplex, banda base.
- b) Paralela, half-duplex, banda base.
- c) Paralela, simplex, banda base.
- d) Serial, half-duplex, banda base.
- e) Serial, half-duplex, banda larga.

5. Qual dispositivo transforma sinais digitais em sinais analógicos, e vice-versa, para serem transmitidos e recebidos através de uma linha telefônica?

- a) NIC
- b) Repetidor
- c) Modem
- d) Amplificador
- e) Nenhuma das alternativas anteriores está correta.

Meios de transmissão

5

- ✓ Cabos metálicos de par trançado;
- ✓ Cabos ópticos;
- ✓ Cabos metálicos x Cabos ópticos.

5.1. Introdução

No decorrer desta leitura, conheceremos as diferenças entre os meios de transmissão de dados e as funções dos diferentes componentes destinados à expansão de uma rede de computadores.

Uma rede pode possuir conectividade através de rede cabeada ou por meio de rede sem fio wireless, para prover serviços de compartilhamento de recursos, entre os quais é possível citar:

- **Controle de acesso:** Este serviço se faz necessário sempre que mais de um dispositivo tenta utilizar um determinado recurso compartilhado ao mesmo tempo;
- **Sincronização:** Este serviço garante que o dispositivo destinatário esteja disponível no momento em que o dispositivo remetente estiver lhe fazendo uma transmissão;
- **Controle de fluxo:** Por meio deste serviço é possível reduzir o tempo de transferência e a perda de dados, pois ele permite monitorar e ajustar a quantidade de dados que é transmitida entre os dispositivos. Com isso, se um dispositivo remetente tentar fazer uma transmissão enquanto o dispositivo destinatário estiver ocupado, este último pode utilizar o controle de fluxo para solicitar ao primeiro uma pausa no processo de transmissão;
- **Controle de erro:** Com este serviço é possível conferir se uma mensagem foi transmitida com sucesso entre os dispositivos. Caso não tenha sido, também é possível utilizá-lo para solicitar uma retransmissão.

Os meios de transmissão são os canais físicos responsáveis pela comunicação de dados, usados tanto em telefonia quanto entre os componentes de uma rede. Os principais tipos de meio de transmissão são os cabos metálicos de par trançado e de fibra óptica. Eles podem ser diferentes quanto a:

- Velocidade e frequência suportada;
- Sensibilidade a ruídos;
- Confiabilidade;
- Atenuação.

Esses fatores podem interferir diretamente na comunicação entre os dispositivos de uma rede. Essas características serão detalhadas nos próximos tópicos.

5.2.Cabos metálicos de par trançado

O cabeamento mais utilizado é aquele no qual o sinal é injetado em um dos pares por meio do transformador existente no dispositivo de rede. Tal sinal é o que chamamos de balanceado. Nesse tipo de cabeamento, os condutores devem ser sólidos, isolados com material plástico dielétrico e trançados em pares.

Ao utilizarmos os cabos metálicos de par trançado, as interferências são reduzidas, pois não há conexão direta. Em vez disso, os condutores são trançados em pares e transmitem o mesmo sinal em direções opostas, de forma que os campos magnéticos gerados também são opostos. Sendo assim, o efeito magnético que poderia interferir em outros pares ou cabos é reduzido ou, em alguns casos, anulado.



Para realizar a transmissão de dados, devemos utilizar cabos metálicos平衡ados de par trançado com impedância de 100 Ohms.

5.2.1.Blindagem

Existem ambientes onde há interferências eletromagnéticas que influenciam e interferem no desempenho de uma rede de computadores. As siglas mais comuns para esse tipo de evento são:

- EME - Electromagnetic Environment (Ambiente Eletromagnético);
- EMI – Electromagnetic Interference (Interferência Eletromagnética);
- EMC - Electromagnetic Compatibility (Compatibilidade Eletromagnética).

Esse ambiente eletromagnético pode ser criado pelos próprios equipamentos elétricos e eletrônicos, bem como por fontes externas. A fim de mitigar riscos de perda de desempenho e interferências nas comunicações, as quais poderão corromper dados, no momento da implantação da rede, podemos utilizar cabos blindados, justamente em áreas onde há grande incidência de eletromagnetismo. A blindagem funciona como uma espécie de proteção contra a interferência eletromagnética (EMI). No entanto, a utilização de um cabo blindado requer que toda a solução do canal, como conectores, patch cords etc., seja blindada e vinculada ao aterramento.

Conceitos e Infraestrutura de Redes (online)

100

As principais fontes de interferências eletromagnéticas são:

- Raios;
- Linhas de força;
- Radares;
- Telefones celulares;
- Ignições de motores;
- Descargas eletroestáticas;
- Transceivers e transmissores de rádio.

O Instituto EIA/TIA é um órgão norte-americano responsável por definições de padrões de sistemas. A sigla EIA significa Electronic Industries Alliance (Aliança das Indústrias Eletrônicas) e a TIA, Telecommunications Industry Association (Associação das Indústrias de Telecomunicações). Esse instituto definiu o padrão de identificação dos cabos baseando-se em suas características. Os nomes dos cabos são compostos por letras separadas por uma barra que indicam o seu tipo, seja ele com blindagem ou não. A letra que vem antes da barra refere-se ao cabo como um todo, indicando se há e qual o tipo de proteção entre a capa protetora e os pares. Já a letra que vem imediatamente após a barra indica se os pares possuem blindagem individual ou não.

A tabela adiante lista os significados de cada letra:

Letra	Significado
U	Não blindado (Unshielded)
F	Blindagem em folha de alumínio (Foil)
S	Blindagem com malha metálica (Shielded)
T	Trançado (Twisted)
P	Par (Pair)

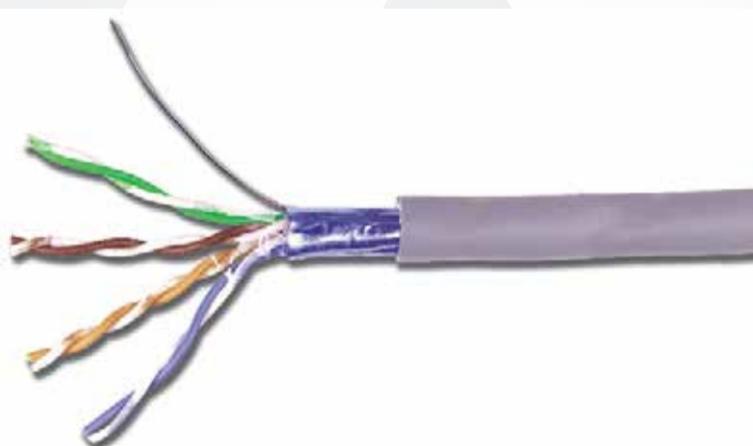
A composição dos cabos metálicos de par trançado é feita por 4 pares de fio de cobre que, conforme seu próprio nome diz, são pares entrelaçados entre si, permitindo, através dessa trança, a criação de uma proteção contra interferências externas eletromagnéticas.

A seguir, temos algumas imagens dos tipos de cabos metálicos de par trançado:

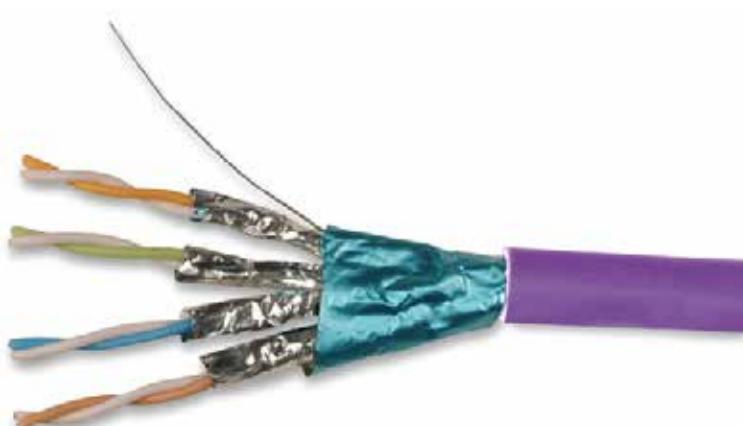
- **U/UTP - Unshielded Twisted Pair:** Cabo de par trançado não blindado;



- **F/UTP - Foil/Unshielded Twisted Pair:** Cabo de par trançado sem blindagem, com revestimento de folha de alumínio;



- **F/FTP ou ScTP – Screened Twisted Pair;**



- S/FTP.



5.2.2. Desempenho dos cabos metálicos de par trançado

Com o objetivo de evitar possíveis incompatibilidades, os cabos metálicos de par trançado são divididos em diferentes categorias conforme o seu desempenho. São levados em consideração fatores como o nível de segurança e a bitola do fio, sendo que os números maiores indicam fios com diâmetros menores. As categorias utilizadas são:

- **Categorias 1 e 2:** Estas categorias não são do padrão trançado e não possuem um padrão definido. Foram os primeiros tipos de cabos criados pela EIA/TIA, instituição responsável pela definição dos padrões dos cabos. Estas categorias foram utilizadas para instalações telefônicas, mas não são mais reconhecidas pela EIA/TIA.
- **Categoria 3:** Foi a primeira categoria de cabos de par trançado desenvolvida especialmente para a transmissão de dados. Suporta a frequência mínima de 16 MHz, permitindo o uso no padrão 10BASE-T, das redes Ethernet de 10 Mbps;
- **Categoria 5e:** O cabo de categoria 5e (de enhanced, ou seja, melhorado) foi desenvolvido com o intuito de reduzir ainda mais a interferência dos ruídos externos. Esses cabos suportam frequência de, no mínimo, 100 MHz e transmissões de até 100 Mbps. A identificação de sua categoria por meio do cabo é fácil, como podemos ver na figura a seguir:



5.1. Cabo UTP CAT 5E

- **Categoria 6:** O cabo cat 6 foi originalmente desenvolvido para ser usado em redes Gigabit Ethernet. Suporta frequência de, no mínimo, 250 MHz e transmissão de 1 Gbps;

- Categoria 6a:** A categoria 6a (de augmented, ou seja, ampliado) foi criada para realizar a transmissão de 10 Gbps e suportar a frequência mínima de 500 MHz;
- Categoria 7:** O cabo de categoria 7 suporta frequência mínima de 600 MHz;
- Categoria 7a:** O cabo de categoria 7a suporta frequência mínima de 1000 MHz.

O comprimento do canal de transmissão estabelecido através dos cabos metálicos de par trançado deve ser de no máximo 100 metros em qualquer uma das categorias descritas.

5.2.3. Padrões de conectorização

As Normas EIA/TIA 568A e 568B são conhecidas como Padrões T568A e T568B. Esses padrões estabelecem a ordem em que os fios dos cabos de par trançado são ligados aos conectores RJ-45. Eles foram os dois padrões estabelecidos para conectorização, como veremos a seguir:

T 568A			T 568B		
Pino RJ45	Cor do Fio	Sinal	Pino RJ45	Cor do Fio	Sinal
1	Branco do Verde	RX+	1	Branco do Laranja	TX+
2	Verde (par 3)	RX-	2	Laranja (par 2)	TX-
3	Branco do Laranja	TX+	3	Branco do Verde	RX+
4	Azul (par 1)		4	Azul (par 1)	
5	Branco do Azul		5	Branco do Azul	
6	Laranja (par 2)	TX-	6	Verde (par 3)	RX-
7	Branco do Marrom		7	Branco do Marrom	
8	Marrom (par 4)		8	Marrom (par 4)	

Identificação do Pino

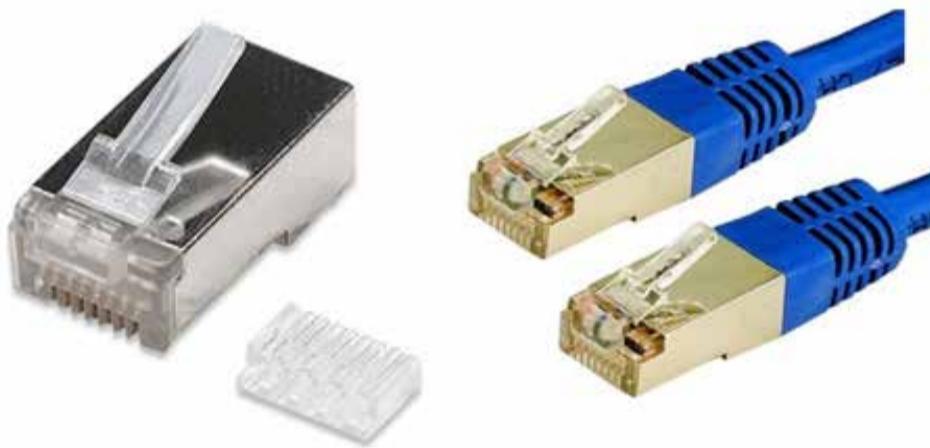
Utilizando esses padrões, podemos criar dois tipos de cabos para tornar a comunicação compatível:

Conceitos e Infraestrutura de Redes (online)

104

- **Cabo direto:** O cabo criado através da referência do padrão T568A também é conhecido como cabo Straight-through e, nesse padrão, sua construção possui as duas pontas iguais. É utilizado para conectar um dispositivo aos demais componentes da rede, como placas de rede e switches;
- **Cabo cruzado:** O cabo criado pelo padrão T568B possui as pontas diferentes, e é mais conhecido como cabo Crossover, ou seja, cada ponta segue um padrão. Sendo que uma ponta deve usar o padrão T568A e a outra, o padrão T568B. É utilizado para interligar dois computadores diretamente (sem a necessidade de um hub ou switch) ou para a tarefa de cascamenteamento de ativos de rede;
- **Tipo de conectores RJ-45:** A fim de ampliar a competição na indústria de telecomunicações, o órgão americano FCC (Comissão Federal de Comunicações) regulamentou por lei este padrão de conectores. Os conectores utilizados para fazer a crimpagem dos cabos dentro dos padrões T568A ou T568B são do tipo RJ 45 (cuja sigla significa Registered Jack e o número 45 identifica sua categoria), que trata da implementação com cabos de rede de 4 pares na categoria 5. Os conectores são do tipo RJ45 Macho ou Fêmea, blindado ou não. Vejamos alguns exemplos de conectores:

- **Conectores RJ45 – Macho blindado:**



- **Conectores RJ45 – Fêmea:**



- **Cabos patch cord:** São cabos criados para manobra ou interconexão, usados em cabeamento estruturado no arranjo físico de conexões (cross connect entre patch panels, interconexão patch panel e switches) e/ou na área de trabalho para ligação entre equipamentos e tomadas de rede.



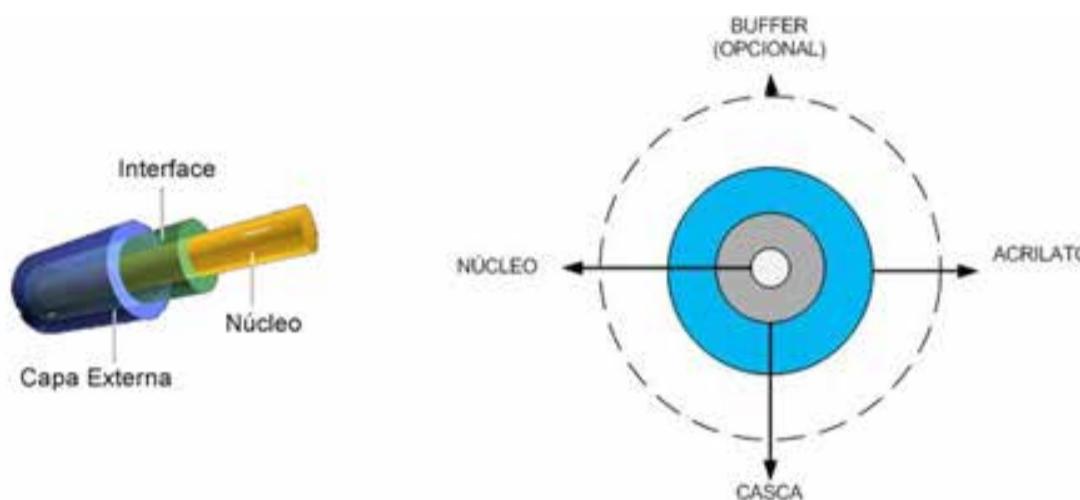
5.3.Cabos ópticos

Os cabos ópticos são completamente diferentes dos cabos metálicos, constituindo-se de, no mínimo, duas fibras ópticas, chamadas de TX e RX, sendo uma para transmissão (TX) e outra para recepção (RX) de informações.

Esses cabos transportam as informações por meio de pulsos de luz, que podemos caracterizar como uma onda eletromagnética, ondas de rádio, radar, raios X ou micro-ondas, e com valores de frequências e comprimentos de onda distintos que podem ser emitidos por um led ou laser.

Os cabos de fibra óptica oferecem muitas vantagens, como imunidade a interferências eletromagnéticas, maior capacidade de transmissão, segurança no tráfego de informações, bem como maiores distâncias.

As fibras ópticas possuem uma estrutura complexa composta por três camadas básicas, podendo apresentar também uma camada adicional, como podemos ver adiante:



5.2. Fibra óptica

O núcleo e a casca são feitos de sílica, sendo que o núcleo apresenta um índice de refração maior que o da casca em decorrência das substâncias dopantes que lhe são adicionadas durante a fabricação da fibra. Essa diferença de refração é o fator responsável por manter o pulso de luz confinado no núcleo, para que, então, possa ser propagado por longas distâncias.

O acrilato é uma película que envolve a fibra de vidro, protegendo-a. Em geral, é colorido, de forma que ambas as suas extremidades possam ser identificadas facilmente.

Já o buffer é uma camada de plástico que oferece maior praticidade no manuseio da fibra, além de possibilitar a terminação direta em conectores.

Normalmente, tanto o núcleo quanto a casca são protegidos com revestimentos plásticos e acondicionados em buffers.

5.3.1. Classificação dos tipos de fibras ópticas

Podemos classificar a fibra óptica de dois modos: Multimodo e Monomodo. Essa classificação tem por objetivo definir a forma como a luz é propagada no interior do núcleo da fibra. Há cabos de fibras para atender as mais diversas necessidades da tecnologia da informação com relação a distância e capacidade, sendo que as fibras podem ser utilizadas tanto para ambiente interno (rede local) como para ambiente externo, seja este por meio submarino ou não.

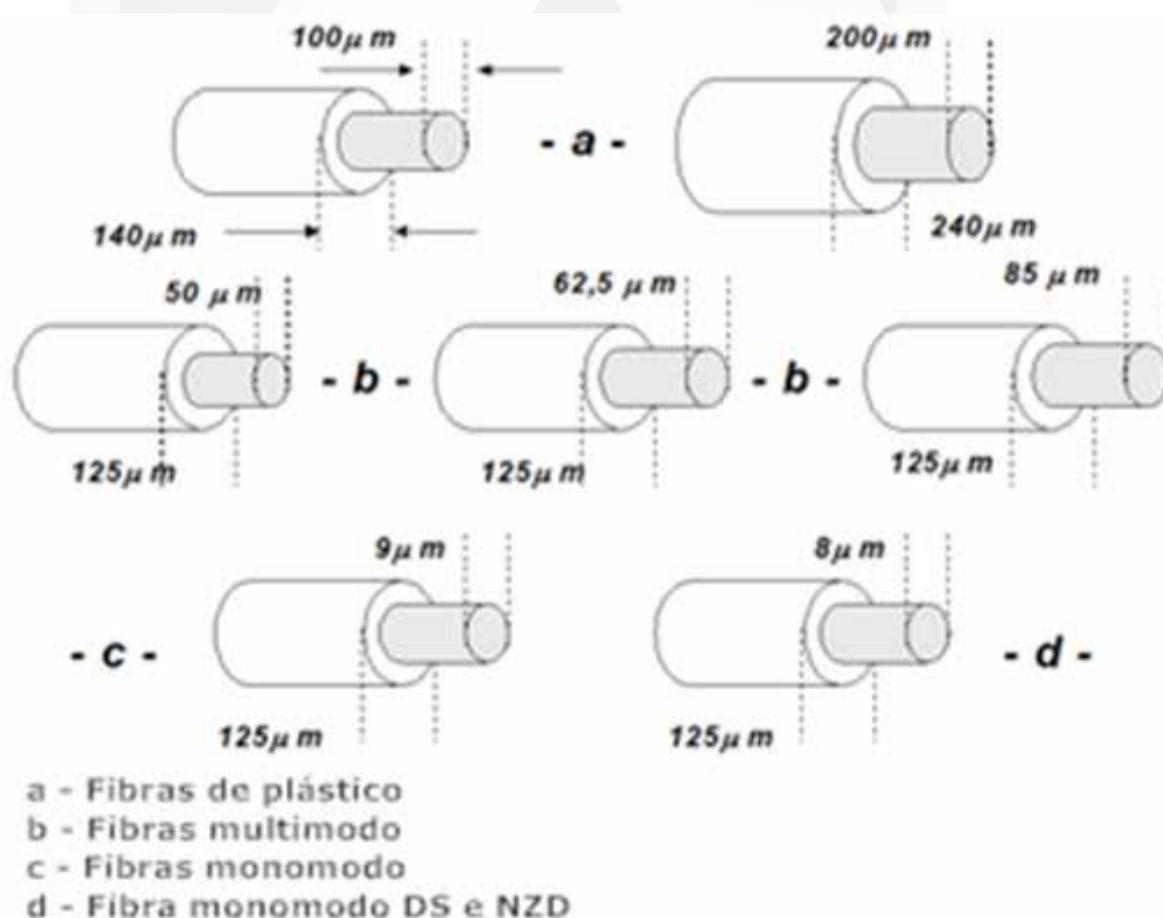
Um dos primeiros tipos de cabo de fibra óptica foi o POF (Polymeric Optical Fiber), que, após sua tradução, ficou conhecido como FOP (Fibras Ópticas Poliméricas). Esse tipo de fibra era muito adotado para implementações de solução de iluminação e no processo de comunicação para transmissão de baixa velocidade, onde as distâncias eram curtas.

Hoje a FOP pode transmitir dados em alta velocidade, com fácil acoplamento e custos reduzidos, quando comparada com as fibras convencionais, podendo ser, como dito anteriormente, do tipo monomodo ou multimodo.

Monomodo e multimodo são classificações decorrentes da variação de diâmetro que o núcleo das fibras apresenta. As fibras multimodo são as que possuem o diâmetro do núcleo maior (na faixa de 50 a 200 μm) e são mais sujeitas à dispersão modal, por permitirem a transmissão de diversos modos. Já as fibras monomodo são as que possuem o núcleo com proporções mais reduzidas.

Suas dimensões são dadas em micrões e podem variar, conforme mostram a tabela e figura a seguir:

Tipo de Fibra	Diâmetro do Núcleo	Diâmetro da Casca
Monomodo OS1 / OS2	8-9 μm	125 μm
Multimodo OM1	62,5 μm	125 μm
Multimodo OM2 / OM3	50 μm	125 μm



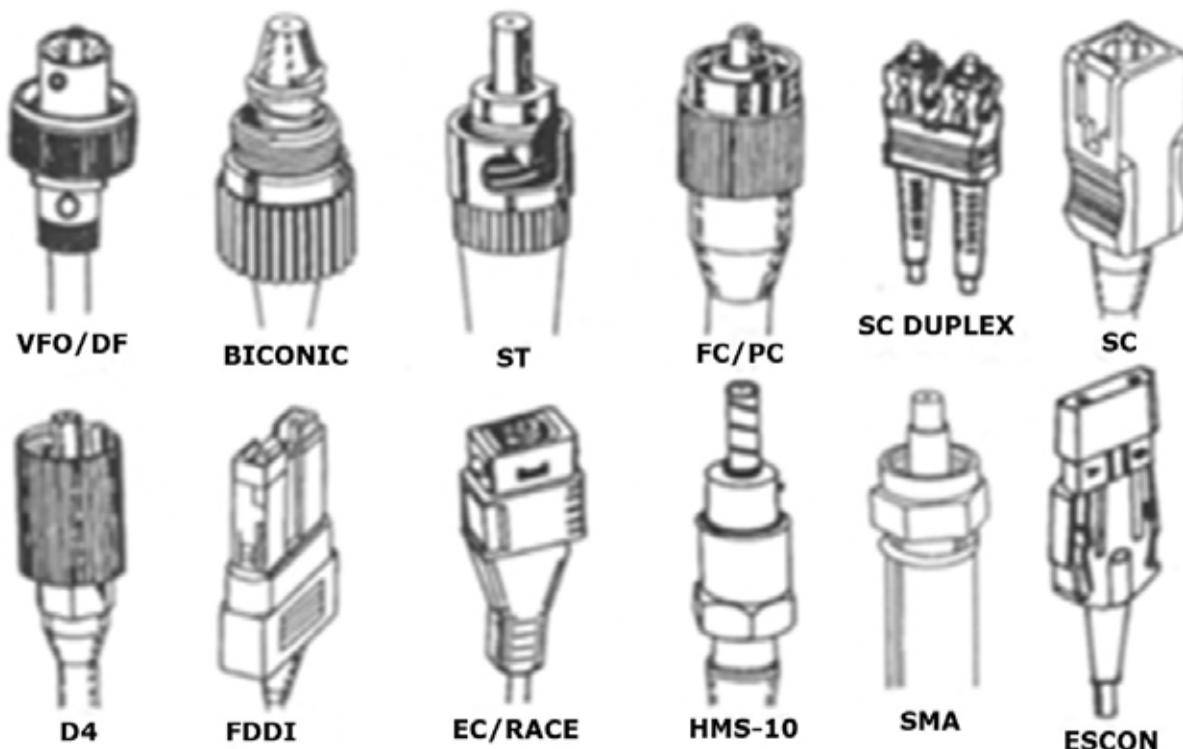
- **Tipo de conectores de fibra de polimento**

Os conectores são componentes importantes para conectar as interfaces ativas e passivas nas redes de computadores. É necessário que sua montagem reúna todos os requisitos de qualidade, a fim de que tenha alinhamento preciso do furo do conector com o núcleo da fibra, pois ele é responsável por proteger as superfícies do ferrolho, entre outros.

- **Tipos de polimento**

- PC (Physical Contact);
- FLAT (plano);
- APC (Angled Physical Contact);
- SPC (Super Physical Contact).

Conectores com polimento PC possuem melhor resposta à perda de retorno e inserção. Já o tipo de polimento APC é utilizado em casos em que a transmissão é em GHz. A perda de retorno é de 50 dB a 70 dB e a de inserção menor do que 0,3 dB.



5.4. Tipos de conectores de fibra óptica

5.3.2. Desempenho dos cabos de fibra óptica

Os cabos de fibra óptica são classificados de acordo com seu desempenho, assim como os cabos de par trançado. Sendo assim, os cabos monomodo subdividem-se em duas classes (OS1 e OS2), enquanto os cabos multimodo são subdivididos em três classes (OM1, OM2 e OM3).

Vejamos, a seguir, as características de cada uma das classes de cabos ópticos existentes:

- **OS1:** São fibras ópticas monomodo genéricas com diâmetros de 8-9 e 125 µm;
- **OS2:** São fibras ópticas monomodo ZWP com diâmetros de 8-9 e 125 µm;
- **OM1:** São fibras ópticas multimodo com diâmetros de 62,5 e 125 µm. Possuem largura de banda mínima de 200 e 500 MHz/KM a 850 e 1300 nm, respectivamente;
- **OM2:** São fibras ópticas multimodo com diâmetros de 50 e 125 µm. Possuem largura de banda mínima de 500 e 500 MHz/KM a 850 e 1300 nm, respectivamente;
- **OM3:** São fibras ópticas multimodo com diâmetros de 50 e 125 µm. Possuem largura de banda mínima de 2000 e 500 MHz/KM a 850 e 1300 nm, respectivamente.

Os cabos ópticos possuem, ainda, um limite máximo de distância para que o atendimento possa ser realizado em uma LAN. Dependendo da classe a que o cabo pertence e da distância entre os dispositivos que ele conecta, podem ocorrer variações na taxa de transferência, conforme podemos ver na tabela adiante:

Backbone	Distância	Taxa
Externo (fibra OM1)	2000 m	155 Mbps
Externo (fibra OM2)	550 m	1 Gbps
Interno (fibra OM1)	2000 m	100 Mbps
Interno (fibra OM2)	300 m	1 Gbps
Interno (fibra OM3)	300 m	10 Gbps
Interno/Externo (fibra OS1)	2000 m	10 Gbps

5.4.Cabos metálicos x Cabos ópticos

Quanto à transferência de um ponto a outro, tanto os cabos metálicos quanto os ópticos produzem resultados semelhantes. Contudo, cada um utiliza uma tecnologia diferente, sendo que a fibra óptica se destaca por apresentar os seguintes benefícios:

- Maior largura de banda;
- Imunidade à interferência eletromagnética, já que a transmissão é feita por meio de pulsos luminosos em vez de elétricos;
- Capacidade de transmitir dados em longas distâncias e de suportar maior velocidade nesse processo. Tal velocidade pode variar dependendo da distância do link e do tipo de fibra utilizada.



Teste seus conhecimentos

Meios de transmissão

5

1. Qual das alternativas a seguir define meios de transmissão?

- a) São os canais físicos responsáveis pela comunicação de dados, usados apenas em telefonia.
- b) São os padrões adotados na conectorização.
- c) São os canais físicos responsáveis pela comunicação de dados, usados apenas entre os componentes de uma rede.
- d) São as sete camadas do modelo OSI.
- e) São os canais físicos responsáveis pela comunicação de dados, usados tanto em telefonia quanto entre os componentes de uma rede.

2. Qual das alternativas a seguir não é um dos benefícios de se utilizar cabos ópticos no lugar de cabos metálicos?

- a) Capacidade de transmitir dados em longas distâncias.
- b) A blindagem dos cabos funciona como proteção contra a interferência eletromagnética.
- c) Imunidade à interferência eletromagnética, considerando que a transmissão é feita por meio de pulsos luminosos em vez de elétricos.
- d) Capacidade de suportar maior velocidade na transmissão de dados em longas distâncias.
- e) Maior largura de banda.

3. Para evitar incompatibilidades, os cabos metálicos de par trançado são divididos em categorias conforme seu desempenho. Qual a categoria que suporta frequência mínima de 1000 Mhz?

- a) Categoria 7
- b) Categoria 7a
- c) Categoria 6
- d) Categoria 6a
- e) Categoria 5e

4. Qual das alternativas a seguir melhor descreve os cabos ópticos?

- a) São constituídos de, no mínimo, duas fibras ópticas para recepção.
- b) São constituídos de, no mínimo, duas fibras ópticas para transmissão.
- c) São constituídos de, no mínimo, duas fibras ópticas, uma para transmissão e outra para recepção.
- d) Nesse tipo de cabeamento, os condutores devem ser sólidos, isolados com material plástico dielétrico.
- e) Nenhuma das alternativas anteriores está correta.

5. Qual das alternativas a seguir não descreve uma característica dos cabos de par trançado?

- a) O sinal é injetado em um dos pares por meio do transformador existente no dispositivo de rede
- b) os condutores devem ser sólidos, isolados com material plástico dielétrico e trançados em pares.
- c) Ao utilizarmos estes cabos, as interferências são reduzidas, pois não há conexão direta.
- d) Os condutores são trançados em pares e transmitem o mesmo sinal em direções opostas, de forma que os campos magnéticos gerados também são opostos.
- e) Transportam as informações por meio de pulsos de luz

Componentes de expansão da rede

6

- ✓ Placas de rede;
- ✓ Conversores de mídia;
- ✓ Ativos centrais de redes.

6.1. Componentes de expansão da rede

Uma rede de computadores é formada por diversos componentes. Para garantir seu crescimento e alto desempenho, torna-se necessário conhecer suas características, a fim de realizar uma implementação que atenda os mais diversos aspectos de uma rede. A seguir conheceremos quais são esses componentes e suas funcionalidades.

6.2. Placas de rede

A placa de rede, também conhecida como NIC (Network Interface Card), consiste em um componente importante que promove a conexão de estações e servidores ao restante da rede. Cada um desses hardwares, no entanto, apresenta características especiais quanto ao uso das placas de rede, conforme podemos ver nas descrições a seguir.

6.2.1. Placa de rede para estação

Podemos classificar as placas de rede de duas formas: OffBoard ou OnBoard. Elas normalmente possuem dois sinais luminosos (LEDs) que indicam seu status de funcionamento. Um dos LEDs, quando verde, indica que na placa há alimentação elétrica, recebida por meio do cabo de rede. O segundo LED indica seu modo de recepção e transmissão de dados, podendo alterar as cores para laranja, que indica uma atuação a 10 Mb/s, ou vermelho, a 100 Mb/s. Vejamos, a seguir, descrições dos dois tipos de placa de rede:

- As placas de rede da categoria OffBoard são dispositivos externos instalados em slots de expansão existentes dentro do computador, conforme podemos ver na figura a seguir:



6.1. Interface de Rede OffBoard

- As placas da categoria OnBoard são aquelas que, ao adquirir seu computador, já vêm embutidas como parte da motherboard (placa-mãe), de modo que a conexão com a LAN pode ser estabelecida a qualquer momento.



6.2. Interface de Rede OnBoard



É comum que o termo LAN na placa-mãe (LOM - LAN On Motherboard) seja utilizado para se referir à placa de rede.

Podemos configurar boa parte das placas de rede com o intuito de aprimorar o desempenho ou até mesmo a segurança do processo de transferência de dados entre estação e rede.

Há uma técnica que pode ser utilizada com o objetivo específico de aprimorar o desempenho do processo: é a priorização de tráfego. Por meio dessa técnica, é possível atribuir diferentes níveis de prioridade às aplicações executadas simultaneamente dentro da estação. Ou seja, a priorização de tráfego nos permite, por exemplo, configurar a placa de rede para transferir os dados de e para uma determinada aplicação, antes de sequer processar as mensagens das demais aplicações.

Quanto ao aprimoramento da segurança, as placas de rede podem ser configuradas para criptografar as mensagens antes de serem transmitidas e verificar a integridade das mensagens de entrada. Algumas placas podem realizar uma checagem de erros avançada. Geralmente, tal checagem, também chamada de offload, é realizada pela CPU da estação.

A maioria das placas de rede de estação podem realizar operações de taxa múltipla. Isso significa que uma certa placa pode ser configurada para identificar, de maneira automática, a taxa de operação máxima da porta do hub ou switch à qual ela se encontra conectada e, então, se configurar para funcionar de acordo com essa taxa. Esse procedimento é o que se conhece como recurso AUTONEG (Autonegotiation).

Quando a placa de rede se encontra conectada a uma porta de switch, é possível configurá-la para operar no modo full-duplex. Com isso, ela fica habilitada a enviar e receber mensagens simultaneamente, o que só é permitido em ambientes que utilizam switches. Sendo assim, quando a placa de rede está conectada a um hub, ela só pode operar em modo half-duplex, o que significa que ela pode enviar e receber mensagens, mas não de maneira simultânea.

Os administradores têm o poder de verificar o status da placa de rede por meio de um software de diagnóstico. Às vezes, esse software permite inclusive testar a integridade da conexão do cabeamento existente entre a placa de rede e seu hub ou switch correspondente.



A placa de rede é um dispositivo que atua na Camada 2 do modelo de referência OSI.

6.2.2. Placa de rede para servidor

Para estabelecer a conexão entre um servidor e a rede geralmente utilizamos uma placa de rede em um ambiente com switches. As placas de rede desenvolvidas para servidores apresentam alguns recursos diferentes daqueles encontrados nas placas de estação, tais como tolerância a falhas, agregação de link, balanceamento de carga, priorização de tráfego e troca quente (hot swap).

- **Tolerância a falhas**

Este recurso requer a presença de duas placas de rede. A segunda fica em stand-by, no modo backup, enquanto as operações realizadas na primeira placa são monitoradas. Com isso, se ocorrer alguma falha na primeira placa de rede, a segunda começa a processar as mensagens de entrada e de saída, garantindo, assim, a continuidade das transmissões.

- **Agregação de link**

Este recurso permite que diversas placas de rede trabalhem juntas como se estivessem em uma mesma conexão. Com isso, há um aumento na taxa de transferência de dados do servidor e o recurso de tolerância a falhas é disponibilizado.

Quando estabelecemos este tipo de conexão entre várias placas, podemos utilizar switches para prover uma tolerância a falhas adicional. Assim, garante-se que a comunicação não seja interrompida caso ocorra falha de alguma placa ou switch.

Este recurso, conhecido também como teaming, trunking e port trunking, possibilita que os recursos do servidor sejam incrementados. No caso de um servidor que possui uma placa de rede operando a 100 Mb/s, por exemplo, é possível adicionar outra placa de configuração similar, de forma que ele poderá contar com 200 Mb/s de tolerância a falhas. Porém, se o servidor não utilizar a agregação de conexão, a placa deverá ser substituída por uma que opere a 1000 MB/s, e o switch correspondente também exigirá uma porta de 1000 Mb/s.

- **Balanceamento de carga**

Com este recurso, o tráfego de mensagens de entrada e de saída é distribuído entre as placas de rede agregadas ao servidor, evitando que algumas fiquem ociosas enquanto outras operam em sua capacidade máxima. Dessa forma, nenhuma placa fica sobrecarregada, o que resulta em melhorias quanto ao desempenho das comunicações da rede do servidor.

- **Priorização de tráfego**

Por meio deste recurso, os administradores de rede podem atribuir níveis de prioridade às aplicações que são executadas no servidor. Quando as aplicações emitem mensagens, estas são colocadas em uma espécie de fila para, então, serem transmitidas. Com este recurso, o processamento e a transmissão das mensagens não seguem a ordem de emissão, mas sim a prioridade estabelecida.

- **Troca quente (Hot swap)**

Por meio deste recurso, é possível substituir qualquer placa de rede sem que seja necessário desligar o servidor.

6.3. Conversores de mídia

Há casos em que a mídia de cabeamento de que dispomos não é correspondente ao transceptor do dispositivo em uso na rede. Tomemos como exemplo uma situação em que é necessário estabelecer uma conexão entre um sistema que usa cabo de fibra óptica e uma placa de rede equipada com um conector para cabo par trançado balanceado. Nesse caso, para que não seja preciso substituir a placa, utiliza-se um conversor de mídia que é ligado tanto ao conector da placa quanto ao sistema de cabo de fibra óptica, promovendo, assim, a conexão entre ambos.

Vejamos o exemplo de um conversor de mídia (transceiver) na figura a seguir:



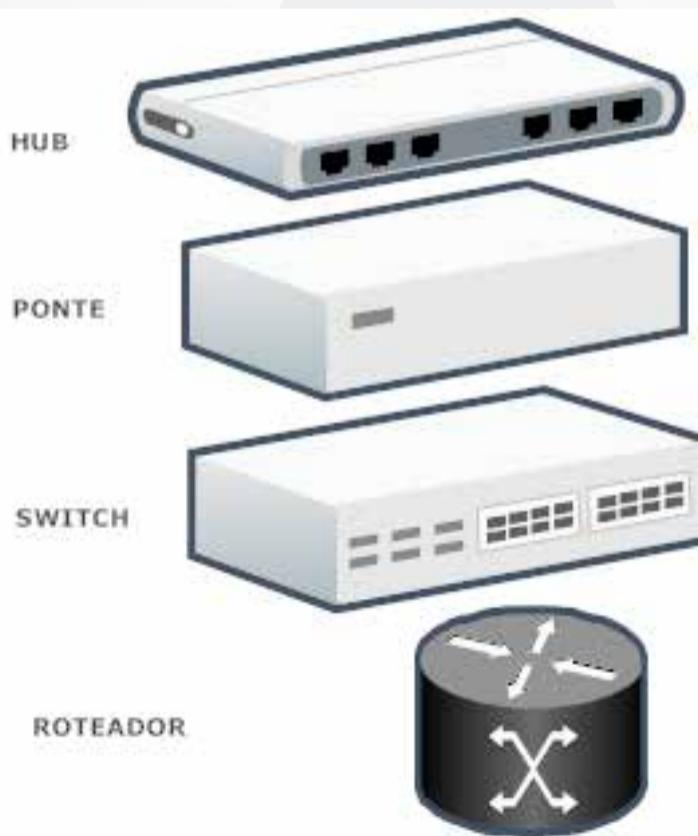
6.3. Transceiver – Conversor de mídia

Os termos filtro e tradutor de mídia também são utilizados para designar os conversores de mídia. Além disso, podemos nos deparar com o termo optoeletrônico em referência ao circuito ou aos componentes das conversões O/E (ópticas e elétricas).

6.4. Ativos centrais de redes

Para fazer a interligação de três ou mais computadores, podemos utilizar equipamentos que gerenciem a troca de informação de forma central. Esses equipamentos também são conhecidos como ativos centrais de redes. Cada tipo de ativo reúne características específicas e é utilizado para atender situações diferentes em uma rede de computadores.

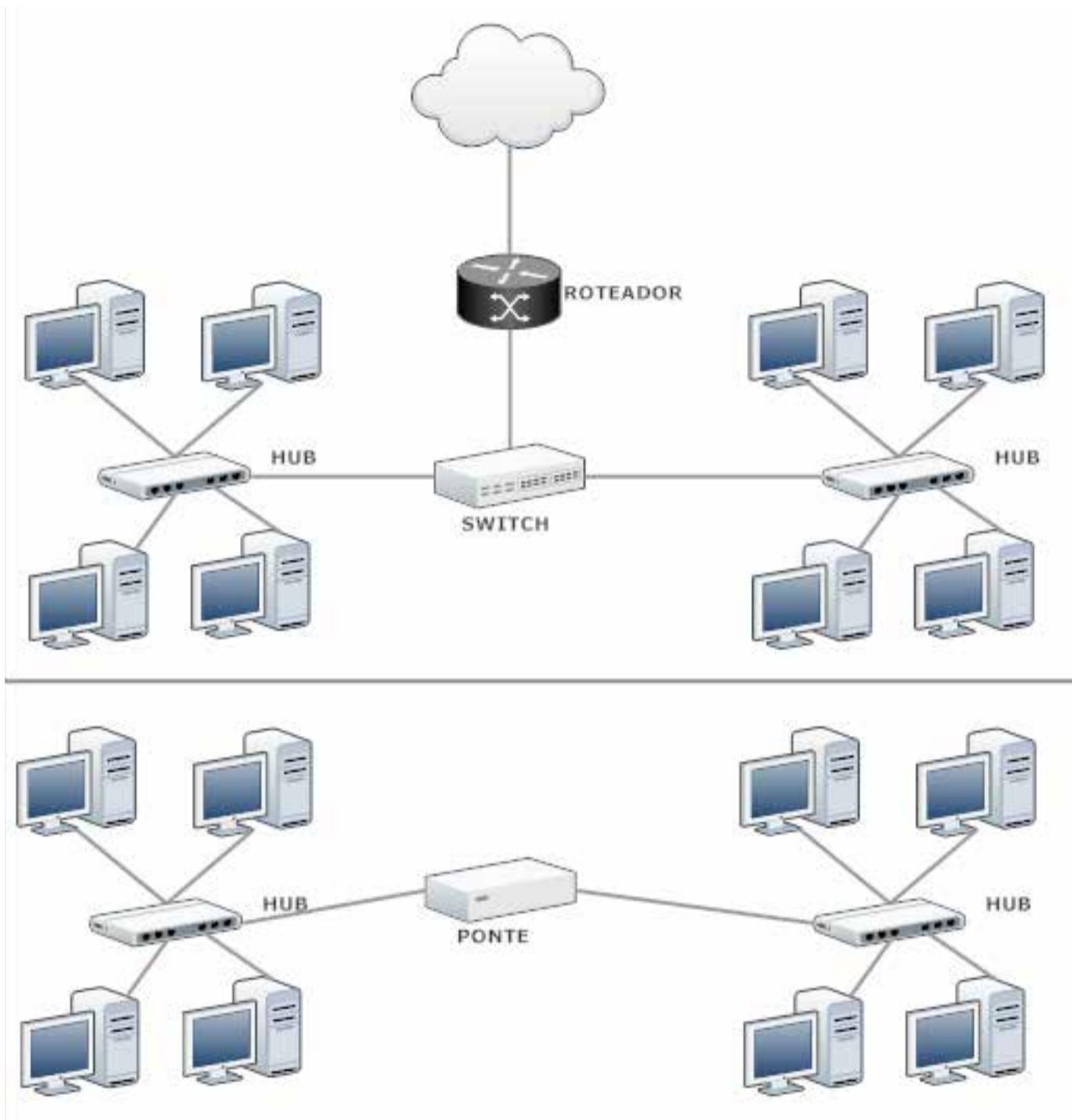
Os ativos são conhecidos como: hub, ponte, switch e roteadores. Vejamos a seguir as características de cada um e sua implementação.



6.4. Tipos de ativos de rede

Componentes de expansão da rede

121



6.5. Tipos de implementações

6.4.1. Hubs

Hub é um dispositivo que concede acesso à rede e consiste em um ponto central para as conexões de mídia e as comunicações da LAN.

É possível equipar o hub com recursos de gerenciamento que ofereçam monitoramento de todos os servidores, estações e demais dispositivos compartilhados, bem como informem os administradores quanto às falhas desses dispositivos, erros e níveis de tráfego da rede. O hub pode, ainda, reforçar o grau de confiabilidade da rede, pois, na maioria das vezes, tem o poder de desconectar dispositivos que apresentam falhas.

Antes dos hubs, a conexão entre os dispositivos de uma LAN era feita por meio de um cabo que funcionava como meio de comunicação compartilhado. O problema dessa configuração é que ela não é confiável, já que, no caso de haver alguma falha de mídia, toda a rede é desabilitada.

O hub é uma espécie de caixa que comporta um cabo curto e funciona como um intermediário no processo de comunicação dentro da rede, pois, em vez de os componentes serem conectados uns aos outros diretamente, eles são conectados aos pontos de conexão do hub, denominados portas. Logo, um hub de 4 portas, por exemplo, tem capacidade de conexão para até 4 dispositivos.



No modelo OSI, o hub é classificado como um dispositivo pertencente à Camada 1.

Em uma rede baseada em hub, as mensagens não são transmitidas diretamente. Ao serem emitidas pelo dispositivo remetente, elas passam primeiro pelo hub, que, então, realiza sua transmissão aos dispositivos receptores conectados.

Há muitos hubs que amplificam ou regeneram os sinais que recebem antes de retransmiti-los com o intuito de aumentar o espaço físico da rede, também chamado de diâmetro máximo de rede permitido. O circuito elétrico que permite essa ação é chamado de repetidor, razão pela qual o hub também é conhecido como repetidor multiporta, já que, além disso, a mensagem recebida por uma porta é transmitida para todas as outras portas disponíveis.

Os dispositivos conectados ao hub só têm permissão para transmitir suas mensagens um por vez, pois há somente um único canal de comunicação compartilhado. Se mais de um dispositivo tentar realizar uma transmissão ao mesmo tempo, suas mensagens se chocarão, interferindo uma na outra de forma que ambas ficarão indecifráveis ou corrompidas.

Muitos dos protocolos da Camada 2 foram desenvolvidos para permitir que os dispositivos disputem, de maneira igualitária, o acesso a um canal de comunicação compartilhado. Entre eles, o mais conhecido é o protocolo que oferece a detecção de colisão. Nesse processo de detecção de colisão, todos os dispositivos que se comunicam por intermédio do hub compartilham um mesmo domínio de colisão, também chamado de domínio de contenção.

Os hubs podem ainda se conectar a outros hubs, expandindo, assim, o seu espaço físico da rede e/ou o número de dispositivos conectados. Para estabelecer uma conexão entre dois hubs, é possível utilizar o mesmo meio que os demais dispositivos utilizam, ou equipar os hubs com conversores de mídia, de forma que o diâmetro da rede seja ampliado. Isso significa que, por exemplo, um hub de 8 portas para conexão com hardwares que utilizam cabo par trançado平衡ado pode ser equipado com uma porta que ofereça conexão a outro hub de 8 portas que, por sua vez, utiliza cabo de fibra óptica.

Há casos em que os hubs se encontram próximos a ponto de poderem ser conectados por meio de um cabo curto, o que lhes permite operar como se fossem um só. Esse fenômeno é chamado de empilhamento de hubs e, por meio dele, a LAN pode ser expandida, envolvendo outros servidores, estações e dispositivos periféricos, conforme a necessidade. Dessa forma, se a rede precisar de mais portas, além das oferecidas pelo hub ao qual se encontra conectada, outros hubs podem ser empilhados sem que, no entanto, o limite máximo permitido seja ultrapassado.

6.4.2. Pontes

Antes de o uso de switches se tornar popular, as pontes eram o recurso utilizado para ampliar a quantidade de dispositivos nas LANs baseadas em hub, sem acarretar prejuízos quanto ao tempo de resposta da rede. Elas possuem, geralmente, duas portas, cuja finalidade é dividir um único domínio de colisão em dois separados. Isso reduz a quantidade de dispositivos usando um mesmo canal de comunicação, o que possibilita uma otimização no tempo de resposta.

As pontes ainda oferecem ampliação do espaço físico da rede. Em princípio, os switches de primeira geração eram comumente chamados de pontes multiportas, uma vez que a tecnologia dos switches se originou nas pontes.

Em geral, quando uma ponte é implementada, os dispositivos da rede continuam a operar da mesma forma, sem que seja necessário fazer nenhuma alteração. Além disso, os usuários conseguem perceber a melhora que as pontes promovem no tempo de resposta. A junção desses dois fatores explica o fato de as operações das pontes serem, muitas vezes, descritas como processos transparentes.

Uma ponte comum de duas portas funciona da seguinte forma:

1. Dois ou mais hubs são conectados entre si, formando um domínio de colisão;
2. Cada hub é, então, conectado a uma porta da ponte, de forma que se tem dois domínios de colisão;
3. Os dispositivos que emitem as mensagens transmitidas em cada domínio de colisão têm seus endereços inspecionados pela ponte;
4. Quando uma mensagem precisa ser transferida de um domínio para o outro, a ponte é que realiza tal transmissão. Já nos casos em que as mensagens não precisam atravessar a ponte, elas são simplesmente descartadas (processo chamado de filtragem).

Vale ressaltar que as pontes criam domínios de colisão e não de transmissão. Por isso, ao receber uma mensagem de entrada endereçada a todos os dispositivos da LAN, ela transmitirá essa mensagem também para os dispositivos do outro domínio.

No modelo OSI, as pontes são classificadas como dispositivos pertencentes à Camada 2, que, por sua vez, lida com as comunicações entre dispositivos de um mesmo domínio de transmissão.

6.4.3. Switches

Assim como o hub, o switch é um dispositivo de acesso à rede que disponibiliza um ponto central para que as comunicações da LAN, as conexões de mídia e as atividades de gerenciamento sejam realizadas. No entanto, enquanto os hubs têm suas portas conectadas a um único canal de comunicação compartilhado por todos os dispositivos, os switches possuem cada porta conectada a um canal de comunicação separado. Com isso, têm-se domínios de colisão diferentes que possibilitam aos dispositivos conectados em portas distintas do switch transmitir suas mensagens simultaneamente.

As portas dos hubs são denominadas conexões compartilhadas, enquanto as portas dos switches são definidas como conexões dedicadas.

O funcionamento do switch é parecido com o das pontes, com a diferença de que o switch é, normalmente, equipado com muito mais portas, razão pela qual também recebe o nome de ponte multiporta. O switch verifica, em cada porta, o endereço dos dispositivos aos quais as mensagens de entrada se destinam. Feito isso, ele transmite as mensagens pela porta que corresponde ao dispositivo destinatário de cada uma delas.

Como os switches funcionam da mesma forma que as pontes, é válido lembrar que os domínios criados são de colisão e não de transmissão, portanto, as mensagens endereçadas a todos os dispositivos, são enviadas aos dispositivos de todos os domínios.

Um hub pode ser conectado a uma porta do switch, da mesma forma que os demais hardwares. Quando essa conexão é feita, todos os dispositivos conectados ao hub disputam pelo acesso à porta do switch. É possível distribuir os hubs e os switches em diversas configurações para formar, assim, uma LAN híbrida que contenha tanto conexões dedicadas quanto compartilhadas.

No modelo OSI, o switch também é classificado como um dispositivo pertencente à Camada 2, que, por sua vez, lida com as comunicações entre os dispositivos de um mesmo domínio de transmissão.

Ao habilitar diversos domínios de colisão em portas individuais, o switch permite que a rede possua mais dispositivos em relação às redes baseadas em hubs. Porém, há uma desvantagem: chega um momento em que os switches não conseguem lidar com o aumento no tráfego de transmissão ocasionado pelos dispositivos adicionais, de forma que isso reflete no tempo de resposta de maneira significativa. Quando esse ponto é atingido, fica impraticável continuar adicionando dispositivos e a solução é implementar uma rede para dividir a LAN em diversos domínios de transmissão, assim como quando se utiliza um switch para criar domínios de colisão.

Os switches surgiram para substituir as pontes e até mesmo os hubs, já que suas portas podem oferecer um canal de comunicação dedicado a cada dispositivo conectado ao hub. Levando em consideração o fator desempenho, é possível dizer que a configuração de LAN ideal é aquela que se baseia em switches para efetivar o acesso à rede, de forma que não seja necessário o compartilhamento de canais de comunicação entre servidores e estações.

As conexões via switch apresentam as seguintes vantagens:

- **Operações em modo full-duplex**

Os dispositivos conectados a um switch no modo full-duplex podem enviar e receber pacotes de maneira simultânea, ao contrário daqueles conectados ao hub, que só opera em modo half-duplex, o que significa que os processos de envio e recebimento só podem ocorrer um por vez.

As redes full-duplex exigem que haja apenas um dispositivo conectado a cada porta do switch, o que chamamos de microsegmentação. Esse tipo de rede é apropriado para aplicações que enviam e recebem um volume semelhante de informações em suas extremidades. O modo full-duplex, quando habilitado, dobra a taxa de transferência de dados da LAN e, além disso, elimina os domínios de colisão, pois estes não podem ocorrer quando ambas as extremidades da conexão enviam e recebem mensagens simultaneamente.

- **Agregação de link**

Também chamada de teaming e port trunking, a agregação de link permite que diversas portas do switch sejam configuradas para trabalhar como um único canal de comunicação, o que corresponde a um meio flexível de aprimorar o desempenho e a tolerância a falhas. Podemos agregar, por exemplo, duas portas full-duplex de 100 Mb/s, para oferecer um canal de 400 Mb/s (lembrando que a taxa de transferência das portas é dobrada no modo full-duplex, logo uma porta de 100 Mb/s passa a ter capacidade de 200 Mb/s).

Caso alguma porta do switch falhe, as demais continuam oferecendo conexão aos dispositivos vinculados. As portas agregadas utilizam somente um endereço, que geralmente é o endereço de uma delas.

6.4.3.1. Rede híbrida

Uma rede híbrida composta por switches e hubs é equipada com:

- Diversas portas que representam um canal compartilhado, o qual pode ser acessado por meio de qualquer uma das portas do hub;
- Um ou mais canais de comunicação dedicados, que podem ser acessados por meio de suas portas correspondentes no switch.

Esse tipo de rede é recomendado para ambientes em que a maioria das estações gera níveis de tráfego moderados, podendo, portanto, compartilhar um único canal de comunicações. Tais estações devem ser conectadas às portas do hub, já que as portas do switch são mais apropriadas para aqueles dispositivos que transmitem informações de forma mais contínua, como servidores e outros switches. Por conta das conexões dedicadas, esses dispositivos podem se comunicar a qualquer momento, não tendo que aguardar pela disponibilidade do canal.

6.4.3.2. Controle de fluxo

Se o switch apresentar distribuição de tráfego desigual, provavelmente será necessário que haja uma grande quantidade de memória intermediária, também chamada de buffer, em cada uma de suas portas.

Tomemos como exemplo um switch de 32 portas que conta com 31 estações e 1 servidor conectados às suas portas. Caso todas as estações enviem dados ao servidor simultaneamente, seus buffers podem armazenar os dados até que seja possível estabelecer conexão com a única porta do servidor. Da mesma forma, se o servidor estiver conectado a uma porta com capacidade superior às portas das estações, as mensagens enviadas por ele excederão a capacidade de recebimento destas estações, resultando em um superfluxo nos buffers. Em situações assim, o receptor deve enviar ao remetente um alerta de que os dados estão se perdendo, solicitando sua retransmissão. Isso configura um desperdício da capacidade dos recursos da rede.

Justamente para garantir que a quantidade de dados aguardando transmissão não exceda a capacidade dos buffers das portas é que existe o controle de fluxo, por meio do qual é possível gerenciar a taxa de transferência entre as portas full-duplex de um switch.

Com o controle de fluxo instaurado, as portas do switch, e até mesmo os dispositivos conectados a elas, podem gerar mensagens de pausa para sinalizar que estão temporariamente indisponíveis para receber dados. Tais mensagens contêm um indicador de retardo que mede a duração da pausa. Ao cessar a pausa, o remetente dá continuidade à transmissão, a não ser que receba outro aviso de pausa. Durante a pausa, a porta emissora da mensagem de pausa libera, pelo menos, parte de seu buffer, processando as mensagens já contidas nele.

Somando a ação dos buffers com o controle de fluxo, é possível que o tráfego dentro dos switches seja equalizado, principalmente quando determinados dispositivos recebem ou enviam a maior parte das mensagens que o switch em questão processa.

A implementação do controle de fluxo depende de a porta do switch estar configurada para modo half-duplex ou full-duplex. Apesar de os switches operarem em modo full-duplex, as portas que estiverem conectadas a hubs, por exemplo, só podem operar em modo half-duplex.

Caso a rapidez do hub em gerar as mensagens exceda a capacidade de transferência da porta do switch, este último pode gerar um ou mais sinais de colisão falsos para interromper as transmissões do hub. Este é um método chamado backpressure, que evita a transmissão de dados por parte de dispositivos half-duplex conectados às portas, o que confere ao switch maior tempo para processar boa parte do conteúdo armazenado em seus buffers. No entanto, este método não faz distinção entre os dispositivos conectados ao hub, de forma que interromperá o fluxo de qualquer dispositivo que tentar enviar dados pela porta à qual o hub estiver conectado.

6.4.4. Roteadores

Os roteadores são, normalmente, dispositivos especializados que combinam hardware e software. Podemos, por exemplo, habilitar um servidor de uso geral para funcionar como um roteador se, simplesmente, instalarmos nele várias placas de rede e um software de roteamento.

A tecnologia de roteamento promove a interconexão de diversos tipos de LAN na Camada 3 do modelo OSI. Com os roteadores, é possível utilizar a atribuição de endereços da Camada 3 para segmentar redes organizacionais em diversos domínios de transmissão, conhecidos também como sub-redes. As interfaces de um roteador podem:

- Utilizar tecnologias comuns de LAN, como as placas de rede;
- Funcionar como um módulo para estabelecer conexão com um canal WAN, no caso de aplicações WAN.

Os roteadores podem utilizar valores de quaisquer campos existentes no datagrama da Camada 3 para processar o tráfego de maneira seletiva. Um exemplo disso é quando uma sub-rede utiliza o processo de filtragem para impedir que o tráfego de transmissão ali gerado chegue a outras sub-redes. Com isso, o processo de filtragem exclui os datagramas de transmissão em vez de transmiti-los, eliminando, assim, uma fonte comum de tráfego desnecessário da rede.

O roteador também pode, por meio da filtragem, conceder ou negar o acesso aos recursos de roteamento tendo como base as informações de endereçamento da rede. É possível, inclusive, programar as interfaces do roteador com listas de controle de acesso (ACLs – Access Control Lists) que definem privilégios de acesso a cada uma dessas interfaces.

No caso de uma organização que possui muitas localidades e LANs, a melhor solução é empregar diversos roteadores para estabelecer uma rede de conexão entre todos os seus componentes. Uma rede complexa apresenta um ou mais roteadores conectados a todos (ou quase todos) os demais, criando, assim, uma configuração mesh total ou parcial, na qual há diversos caminhos possíveis entre duas redes quaisquer conectadas a diferentes roteadores.

Em ambientes como esse, todos os roteadores devem ter conhecimento dos caminhos disponíveis para a rede de destino, bem como do status de cada um. Para que uma mensagem seja roteada para outra rede, o envio pode ser feito por um caminho específico tendo como base uma série de critérios, entre os quais estão inclusos: custo e nível de tráfego de cada caminho e conteúdo da mensagem. Aqui, custo é uma medida que descreve o desempenho ou o grau de confiabilidade de um caminho.

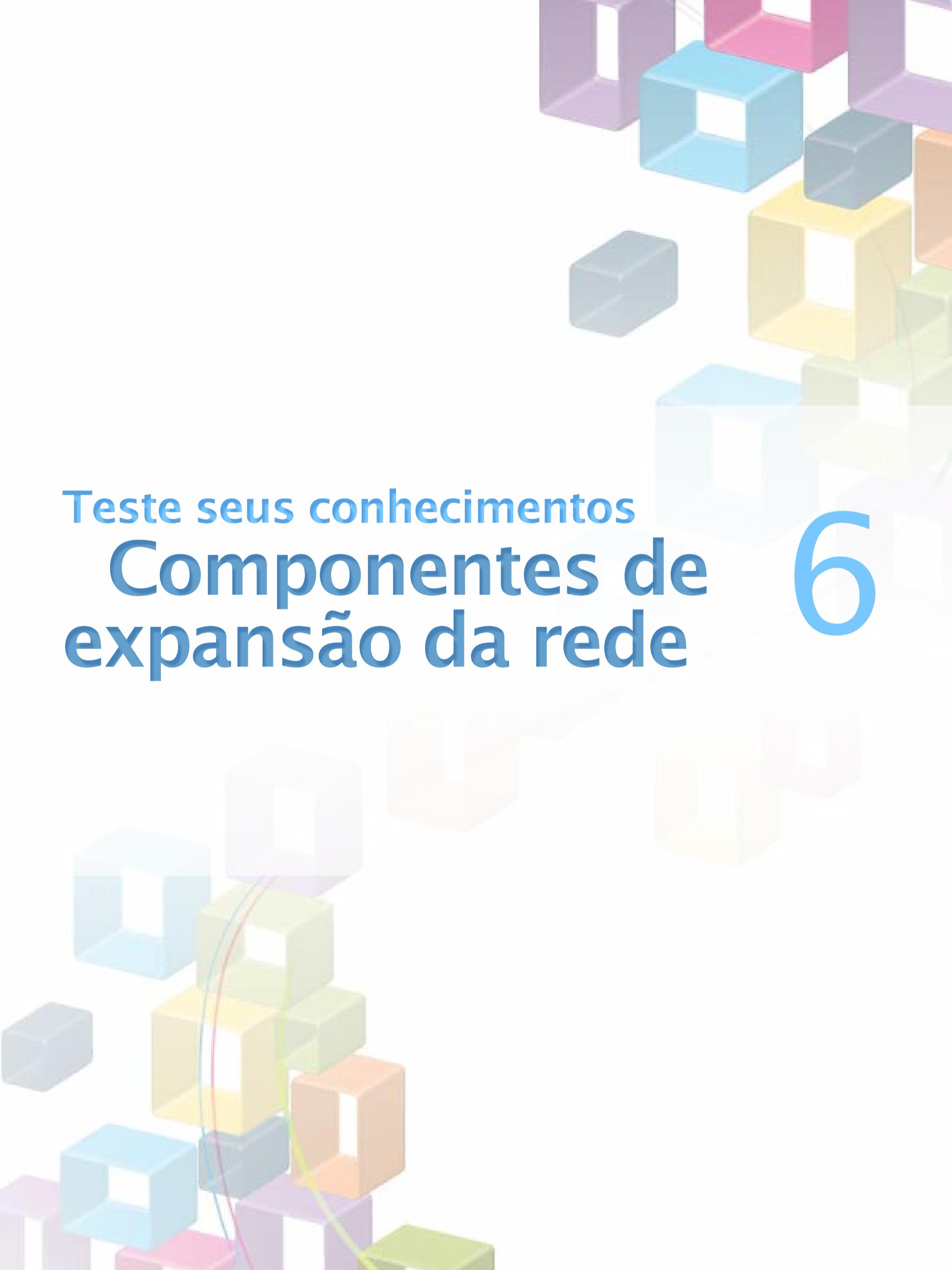
É possível incorporar em um só dispositivo roteamento e LAN baseada em switch, criando, assim, uma unidade híbrida que geralmente é modular. Isso possibilita que diversas combinações de LAN sejam conectadas a outros roteadores para formar uma unidade centralizada, chamada também de roteador backbone. Com o intuito de oferecer conectividade a todas as LANs vinculadas, o roteador backbone pode ser conectado a um roteador operado por um provedor de serviços de Internet (ISP – Internet Service Provider).

As mesmas tecnologias usadas para os switches também foram aplicadas aos roteadores, o que deu origem aos dispositivos chamados de switches de roteamento ou switches da Camada 3.

Os roteadores geralmente utilizam regras e processos baseados em software para transmitir ou filtrar os datagramas da Camada 3, enquanto os switches da Camada 2 utilizam processos e regras parecidos mas que são empacotados na forma de lógica embutida no hardware. Os switches da Camada 3 usam lógica baseada em hardware para desempenhar várias funções de roteamento, o que proporciona um processamento de datagramas muito mais rápido em relação ao roteamento tradicional (baseado em software), mas, em contrapartida, implica em um nível menor de flexibilidade.

Nos switches da Camada 3, o processamento dos pacotes de entrada é feito com base nas informações de endereço desta camada. Tais informações podem ser encontradas no campo de dados do pacote da Camada 2. Às vezes, é possível extrair um nível ainda maior de detalhes para transmitir um pacote. No caso de um switch da Camada 4, por exemplo, os pacotes são direcionados conforme as informações de protocolo desta camada, enquanto em um switch da Camada 7, os pacotes são processados tendo como base as aplicações utilizadas para gerar tais pacotes.

Os administradores de rede obtêm maior flexibilidade ao utilizar switches na camada mais alta do modelo OSI, pois conseguem direcionar, modificar e até mesmo organizar melhor o fluxo de tráfego da rede estabelecendo níveis de prioridade. Podemos nos referir a este processo como engenharia de tráfego ou ajuste de tráfego.



Teste seus conhecimentos Componentes de expansão da rede

6

1. Em determinadas situações, a capacidade de duas ou mais portas de um switch podem ser somadas para trabalhar como um único canal de comunicação. Qual o nome desse recurso?

- a) Controle de fluxo
- b) Soma full-duplex
- c) Agregação de link
- d) Ponte
- e) Bypass

2. Qual a vantagem de configurar uma placa de rede para operar em modo full-duplex onde todos os dispositivos estão interligados por um hub?

- a) Aumentará o desempenho da rede, pois será possível transmitir e receber simultaneamente.
- b) Nenhuma, pois quando conectadas em hub as placas de rede só podem operar em modo half-duplex.
- c) Nenhuma, pois os dados já são transmitidos e recebidos simultaneamente.
- d) Aumentará a capacidade de instalação de novos dispositivos na rede.
- e) Depende da configuração das outras interfaces.

3. Qual das alternativas a seguir não é uma característica que diferencia as placas de rede desenvolvidas para servidores das placas de estação?

- a) Tolerância a falhas.
- b) Agregação de link.
- c) Balanceamento de carga.
- d) Hot swap.
- e) Portas.

4. Com relação aos ativos da rede, qual a alternativa incorreta?

- a) São equipamentos que gerenciam a troca de informações de forma central.
- b) São utilizados para fazer a interligação entre três ou mais computadores.
- c) São conhecidos como hub, ponte, switch e roteador.
- d) As portas dos hubs são denominadas conexões dedicadas, enquanto as portas dos switches são definidas como conexões compartilhadas.
- e) O hub é um ponto central para as conexões de mídia e as comunicações LAN.

5. Qual das alternativas a seguir não é uma característica dos roteadores?

- a) Podem utilizar valores de quaisquer campos existentes no datagrama da Camada 3 para processar o tráfego de maneira seletiva.
- b) Promove a interconexão de diversos tipos de LAN na Camada 3 do modelo OSI.
- c) Suas interfaces podem utilizar tecnologias comuns de LAN, como as placas de rede.
- d) Suas interfaces podem funcionar como um módulo para estabelecer conexão com um canal WAN, no caso de aplicações WAN.
- e) São dispositivos especializados em combinarem softwares.

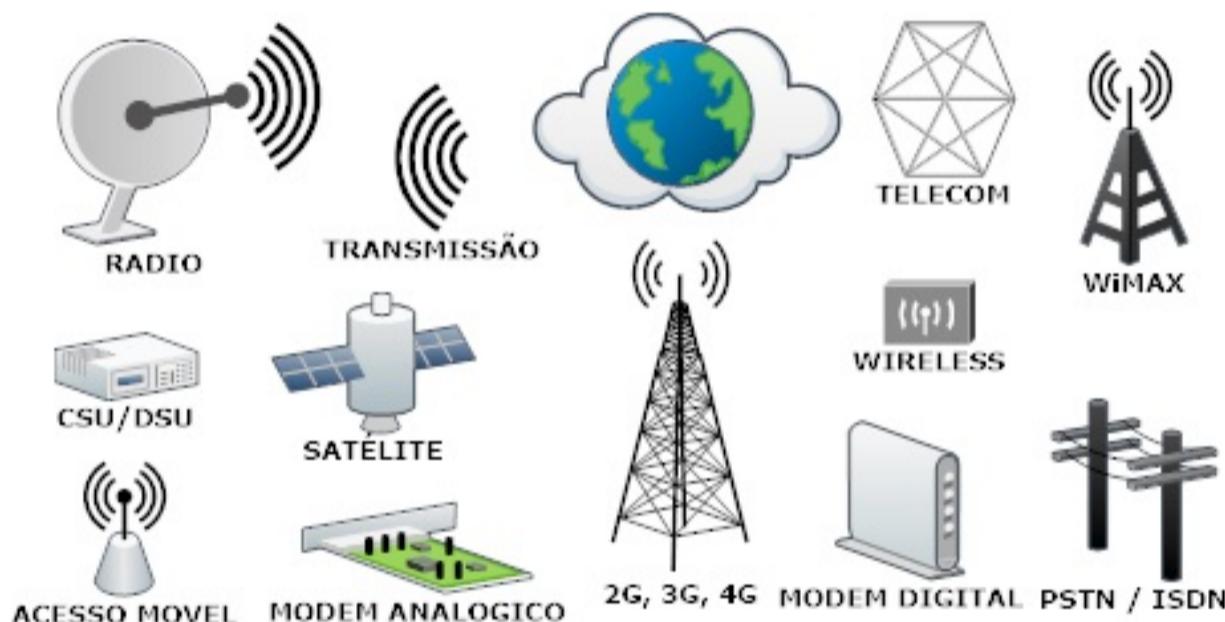
Tecnologias para acesso remoto

7

- ✓ Conexão por linha analógica;
- ✓ Conexão por linha digital;
- ✓ TDM/PCM;
- ✓ Rádio;
- ✓ Satélite;
- ✓ Acesso móvel.

7.1. Introdução

Para realizar a interligação de duas ou mais redes de longa distância, sejam elas locais (MAN) ou globais (WAN), é necessário adotar uma ou mais tecnologias de acesso remoto, a fim de permitir que a comunicação e a transferência de dados entre sistemas sejam estabelecidas. Como apresentado na figura adiante, há diversas opções de tecnologias desse tipo, e os fatores internos e externos de uma organização influenciam na escolha de uma delas.



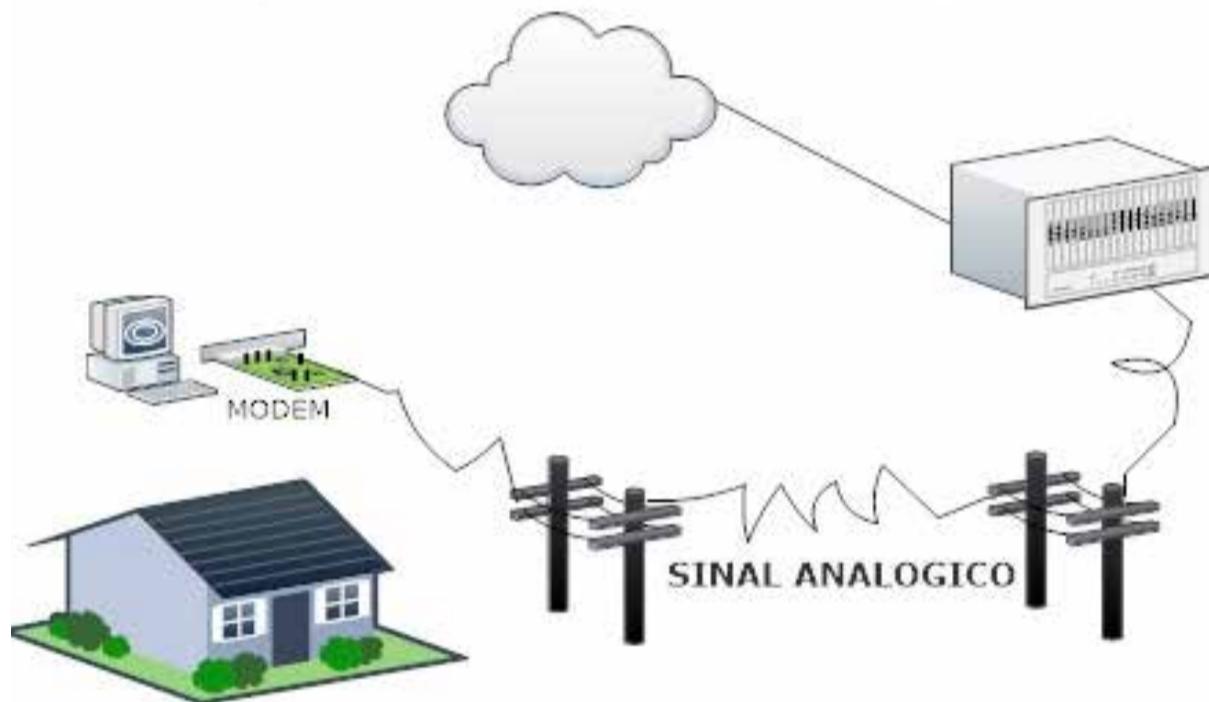
7.1. Tecnologias de acesso remoto

Uma das opções para estabelecer conexões entre redes por meio de acesso remoto é utilizar modems. O nome modem é derivado de modulador e demodulador. Modem é um dispositivo com a função de converter sinais, tornando possível, através de uma linha dedicada, a comunicação entre computadores.

Um modem pode ser do tipo analógico (conversão por modulação) ou digital (conversão por codificação). Para que a comunicação remota seja estabelecida, é necessário que haja um modem em cada uma das extremidades da linha dedicada, e eles devem ser semelhantes e compatíveis.

7.2. Conexão por linha analógica

Uma das formas de acesso remoto é a conexão por linha analógica (linha telefônica comum), conhecida como “Rede Pública de Telefonia Comutada”, derivada da sigla PSTN (Public Switched Telephone Network). Sua velocidade de até 56,6 Kb/s é considerada baixa em relação aos demais meios, mas esse é o tipo mais simples e de fácil execução, permitindo interligar redes em regiões não atendidas por outras tecnologias.



7.2. PSTN – Public Switched Telephone Network

Para estabelecer esse tipo de conexão é necessário um modem analógico e uma linha telefônica em cada um dos computadores.

7.3. Conexão por linha digital

A interligação de redes por linha analógica converte o sinal analógico por meio de modems quando uma única linha é utilizada. Várias técnicas podem ser adotadas na transmissão para maximizar o número de canais de comunicação disponíveis. Podemos utilizar mais de um canal ou linha para prover essa interligação – linhas privadas ou até mesmo canais de rádio.

Os equipamentos necessários para converter sinais na conexão por linha digital são roteadores/ multiplexadores CSU/DSU. Por meio deles, podemos utilizar tanto TDM quanto PCM.

7.4.TDM/PCM

A técnica TDM (Time-Division Multiplexing) refere-se ao processo de transmissão por multiplexagem, e a PCM (Pulse Code Modulation) é utilizada para converter sinais analógicos em digitais.

Os níveis de TDM podem ser identificados, tanto na Europa quanto no Brasil, em E1, E2, E3 e E4. A seguir, vamos aprender um pouco mais sobre cada um desses níveis, bem como sobre outras tecnologias digitais.

7.4.1. Níveis E1, E2, E3 e E4

O E1 é o primeiro nível de TDM e é capaz, ao usar um PCM (Pulse Code Modulation) de 64 Kb/s padrão, de lidar com 30 canais de voz análoga padrão que tenha uma largura de banda de 3.100 Hz. Desde que haja recursos de canais adequados, esse nível possibilita que os dados sejam transmitidos por meio de 30 canais de 64 Kb/s. Seu uso é recorrente em transmissões portadoras de curta distância, isto é, de até 320 Km.

Com uma taxa de transmissão de 2.048 Mb/s, esse nível permite que o alinhamento seja executado e a sinalização seja portada por dois canais adicionais de 64 Kb/s. Considerando uma distância específica e certas condições que devem ser respeitadas, são operados, nesse nível, cabos de pares trançados. A separação dos pares de transmissão e recebimento em compartimentos separados ou grupos não adjacentes ocorre comumente.

Podemos lidar com quatro canais E1 (totalizando 120 canais de voz) ao usarmos o nível E2, nível que utiliza um fluxo de pulso de 8.192 Mb/s e que é o segundo nível de multiplexagem. Sinais E2 são portados por sistemas de fibra ótica com baixa velocidade, apesar do caráter obsoleto dos sistemas de par trançado balanceados que usam portadora E2.

No que diz respeito ao fator distância, destacamos a necessidade, por parte da portadora E2, de um par trançado balanceado especial caso a distância ultrapasse os 305 m. Esse cabo possui características diferenciadas de atenuação e linha cruzada, isto é, a interferência de uma linha de comunicação em outra afetando a transmissão. Um exemplo desse cabo é o LoCap. O nível E2 também é usado para cabos coaxiais.

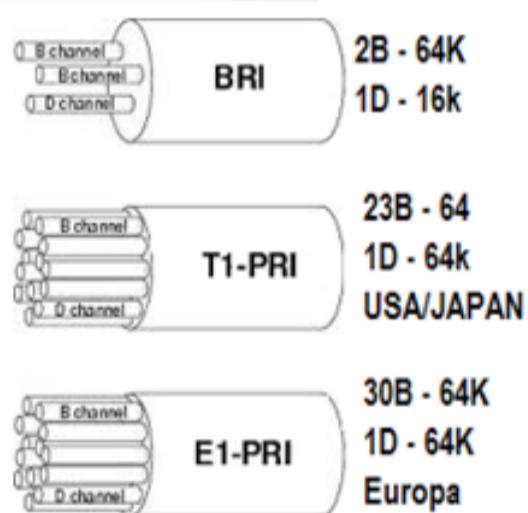
Com o nível E3, por sua vez, quatro sinais E2 podem ser multiplexados (totalizando 480 canais) a 34.816 Mb/s. Nesse nível, há um aumento de uso entre as localizações do consumidor e entre o consumidor e as localizações da instalação da entrada principal.

Para que os fluxos E2 de entrada sejam sincronizados ao terminal multiplexador, é usado o processo bit stuffing, em que são inseridos bits extras no fluxo de dados. Tanto a fibra ótica como os sistemas de rádio digital são usos comuns para a velocidade do nível E3, que também é usado para cabos coaxiais.

O nível E4, quarto nível de multiplexagem, é um sistema de alta densidade e curta distância que pode ser usado para fibra ótica, rádio micro-ondas ou cabo coaxial. Apresenta taxa de 139.264 Mb/s e lida com 1920 canais.

7.4.2. ISDN

Com relação ao ISDN (Integrated Services Digital Network), devemos considerar que a designação canal B pode ser utilizada como referência a um canal único de 64 Kb/s. A tecnologia ISDN utiliza transmissão digital em uma taxa que depende da aplicação, podendo ser taxa básica ou primária, como mostra o exemplo na figura 6.3 a seguir:



7.3. ISDN – Integrated Services Digital Network

A taxa básica (BRI) é indicada para usuários residenciais e de pequenas empresas, enquanto que para usuários de grandes empresas, a taxa primária (PRI) é a taxa adequada. A capacidade de informação total da taxa básica (BRI) é 144 Kb/s e sua taxa de linha, 160 Kb/s. O sinal digital utilizado por ela inclui dois canais B e um canal D (16 Kb/s), que servem, respectivamente, para dados e voz e para dados de pacote e sinalização.

Já a taxa primária (PRI) do ISDN europeu e brasileiro apresenta 1.92 Mb/s de capacidade de informação total, e 2.048 Mb/s de taxa de linha. Os sistemas de transmissão de taxa mais alta podem incorporar essa taxa, assim como sua implementação pode ser feita na portadora repetida E1 ou nas instalações HDSL. Os canais do canal digital da taxa primária operam cada um a 64 Kb/s e contabilizam 30 canais B e um canal D.

7.4.3. DSL

Quando estudamos tecnologias de telecomunicação, é importante termos em mente que as chamadas soluções DSL (Digital Subscriber Line) ou xDSL englobam várias delas. A transmissão por meio dessas soluções é feita por linhas de telefone de par trançado balanceadas. Elas buscam transmitir dados, voz e vídeo com alta velocidade e qualidade.

Algumas de suas variantes são:

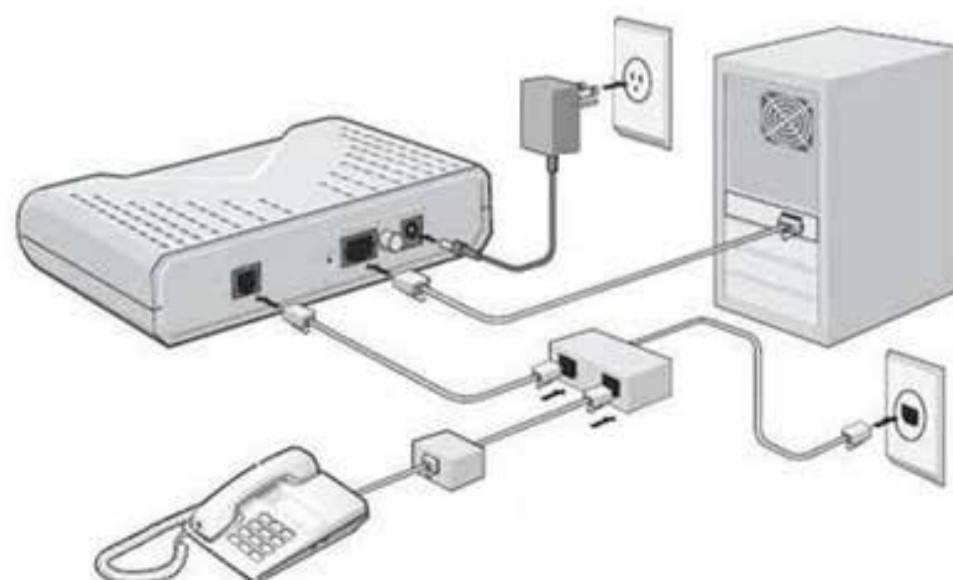
- SDSL (Symmetric Digital Subscriber Line);
- ADSL, ADSL2, ADSL+2 (Asymmetric Digital Subscriber Line);
- HDSL (High Bit Rate Digital Subscriber Line);
- VDSL (Very High Bit Rate Digital Subscriber Line);
- RADSL (Rate Adaptive Digital Subscriber Line).

Dessas, é importante abordarmos um pouco mais profundamente a tecnologia ADSL.

7.4.3.1. AwDSL

Nas tecnologias ADSL (Asymmetric Digital Subscriber Line), o tráfego downstream – aquele em que o fluxo de dados vai do servidor para o cliente – tem maior largura de banda do que o tráfego upstream – caracterizado pelo fluxo de dados na direção contrária, do cliente para o servidor. Essa característica nos permite dizer que a tecnologia ADSL é assimétrica.

Veja na figura a seguir os componentes básicos para montar a estrutura ADSL no lado cliente.



7.4. ADSL – Asymmetric Digital Subscriber Line

O ADSL é usado por muitos aplicativos que encontramos em residências comuns, como vídeos sob demanda, acesso LAN remoto e conexões de Internet – inclusive, para que esta última apresente um bom desempenho, a proporção 10:1 de downstream para upstream é necessária.

Existem três canais de informação formados pelo circuito ADSL. Esse circuito é responsável por conectar, nas extremidades de uma única linha de telefone com par trançado balanceado, um modem ADSL, sendo que cada modem é conectado em uma extremidade.

Os três canais de informação formados dessa maneira são:

- Canal downstream de alta velocidade, cuja abrangência é de 1,5 a 8 Mb/s, sendo que a taxa de upstream vai de 138 Kb/s a pouco a mais que 1 Mb/s;
- Canal duplex de velocidade média;
- Canal POTS (Plain Old Telephone Service), que não é interrompido mesmo que o ADSL apresente falhas, pois os filtros o dividem do modem digital.

Há várias capacitações e gamas de velocidade para os modems ADSL, com os quais o transporte ATM (Asynchronous Transfer Mode) é acomodado, sendo que protocolos IP e cabeçalhos ATM possuem compensação e taxas variáveis. A estrutura hierárquica digital na Europa e nos Estados Unidos coincide com as taxas de dados apresentadas pelos modems ADSL.

Existem alguns fatores que influenciam as taxas de dados com fluxo downstream. Alguns deles são:

- Comprimento do cabo de par trançado balanceado;
- Diâmetro do fio do cabo de par trançado balanceado;
- Interferência de linha cruzada;
- Presença de derivações de ponte.

Os nomes padrão das tecnologias ADSL, junto com seus respectivos tipos e valores de downstream e upstream, são os seguintes:

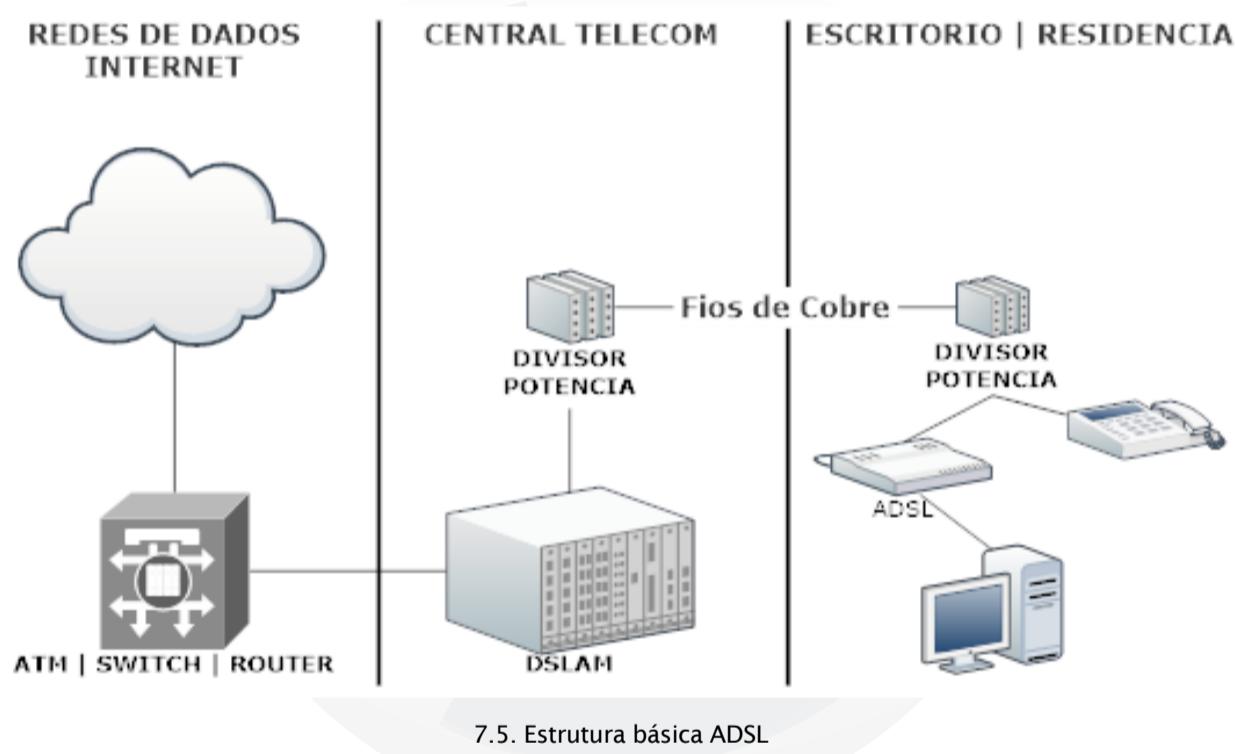
- **ITU G.992.1**: Tipo ADSL (GDMT), com downstream de 8 Mb/s e upstream de 1,0 Mb/s;
- **ITU G.992.2**: Tipo ADSL Lite, com downstream de 1,5 Mb/s e upstream de 0,5 Mb/s;
- **ITU G.992.3/4**: Tipo ADSL2, com downstream de 12 Mb/s e upstream de 1,0 Mb/s;

Conceitos e Infraestrutura de Redes (online)

142

- **ITU G.992.3/4 Anexo J:** Tipo ADSL2, com downstream de 12 Mb/s e upstream de 3,5 Mb/s;
 - **ITU G.992.5:** Tipo ADSL2+, com downstream de 24 Mb/s e upstream de 1,0 Mb/s;
 - **ITU G.992.5 Anexo L:** Tipo ADSL2+, com downstream de 24 Mb/s e upstream de 3,5 Mb/s.
-
- **Estrutura básica do ADSL**

A infraestrutura básica de uma rede ADSL possui diversos componentes, bem como formato de interconexão, como apresenta a figura 6.5 a seguir:



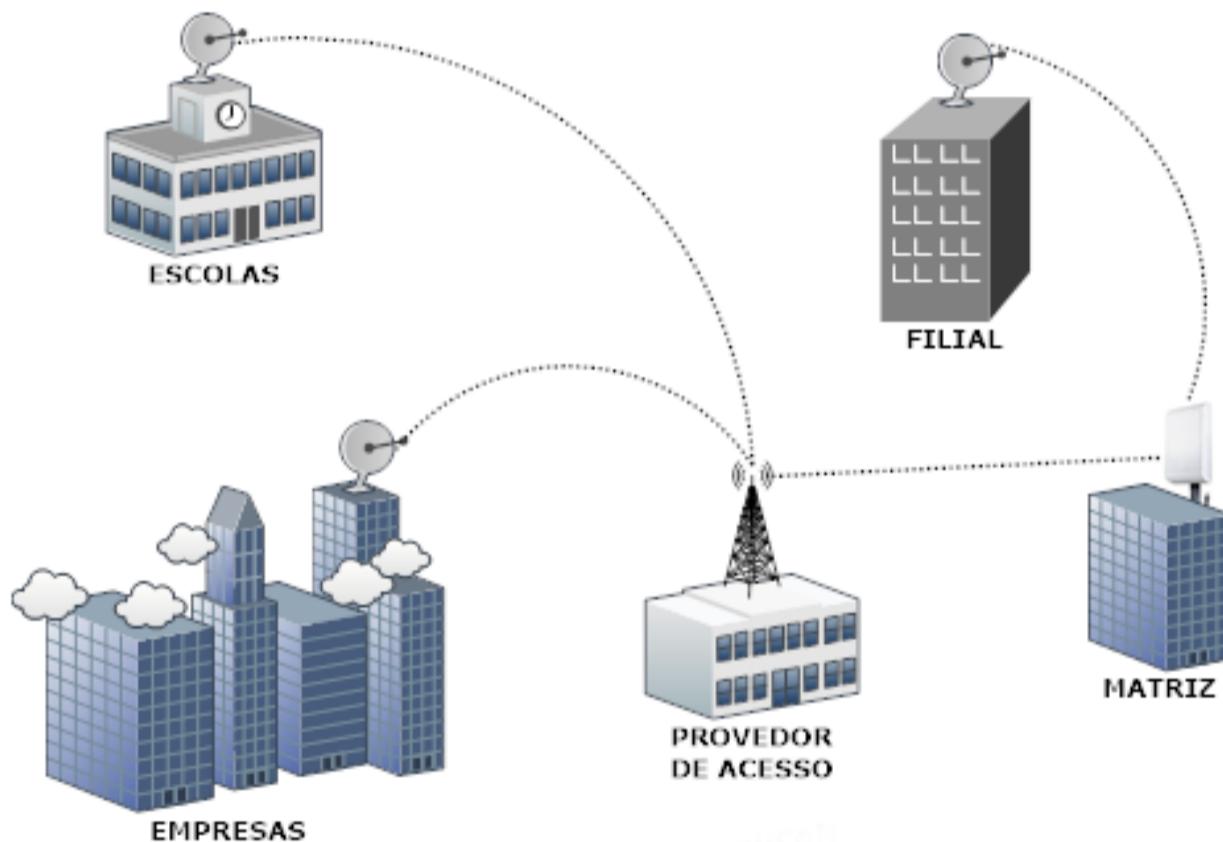
Partindo da infraestrutura da residência ou do escritório, é necessário instalar um **modem ADSL** para estabelecer a conexão ao computador. Geralmente, o modem é conectado a uma placa de rede no micro, que pode funcionar como servidor para uma pequena rede local.

Para fazer a instalação do modem, é necessário um filtro ADSL, conhecido como Divisor de Potência, a fim de fazer a separação do sinal de voz do sinal do tráfego de dados via ADSL.

Nas centrais de TELECOM, os pares de fios são conectados diretamente em um equipamento multiplexador dos sinais DSL, chamado de DSLAM. Sua principal função é centralizar o tráfego de várias linhas e possibilitar a interconexão com a rede de dados. Os circuitos ATM são o tipo de conexão mais adotado para essa interligação.

7.5.Rádio

A conexão via rádio se dá pela instalação de rádio enlaces entre o POP – ponto de presença do provedor do serviço de dados – e pontos remotos. Esses enlaces podem atender a apenas uma localidade (configuração ponto a ponto) ou várias localidades (ponto-multiponto). A solução de rádio oferece facilidade de implantação à empresa e atende locais remotos onde não há infraestrutura para implantação de rede de dados de alta velocidade. Com a tecnologia de rádio, é possível transmitir dados, áudio e vídeo, unificando a infraestrutura e otimizando a implementação.



7.6. Comunicação via rádio

O IEEE (Institute of Electrical and Electronics Engineers) definiu o Padrão IEEE 802.16 criando uma camada física para interligar sistemas em operação com banda larga. Sua finalidade é especificar uma interface sem fio para redes WMAN, a fim de ampliar o raio de cobertura e a abrangência. O padrão 802.16 especifica dois espectros de frequência: a faixa de 2 a 11 GHz para condições NLOS (conhecido como Sub-11), ou de 10 a 66 GHz para condições LOS, cabendo aos órgãos regulamentadores decidir qual frequência as WISPs (Wireless Internet Service Providers) serão utilizadas.

Vamos conhecer os dois tipos de rádios:

- **Line of Sight (LOS) Radio Frequency (RF) Equipment:** Esta faixa de espectro exige que haja visada entre dois ou mais pontos envolvidos, isto é, não deve haver obstáculos entre os rádios. O LOS foi projetado para alcance de até 50 Km por possuir frequências maiores;
- **Non-Line of Sight (NLOS) Radio Frequency (RF) Equipment:** A faixa de frequência NLOS não exige visada entre dois ou mais pontos, ou seja, são equipamentos capazes de superar obstáculos no caminho, projetados para alcance de até 8 Km.

7.6.Satélite

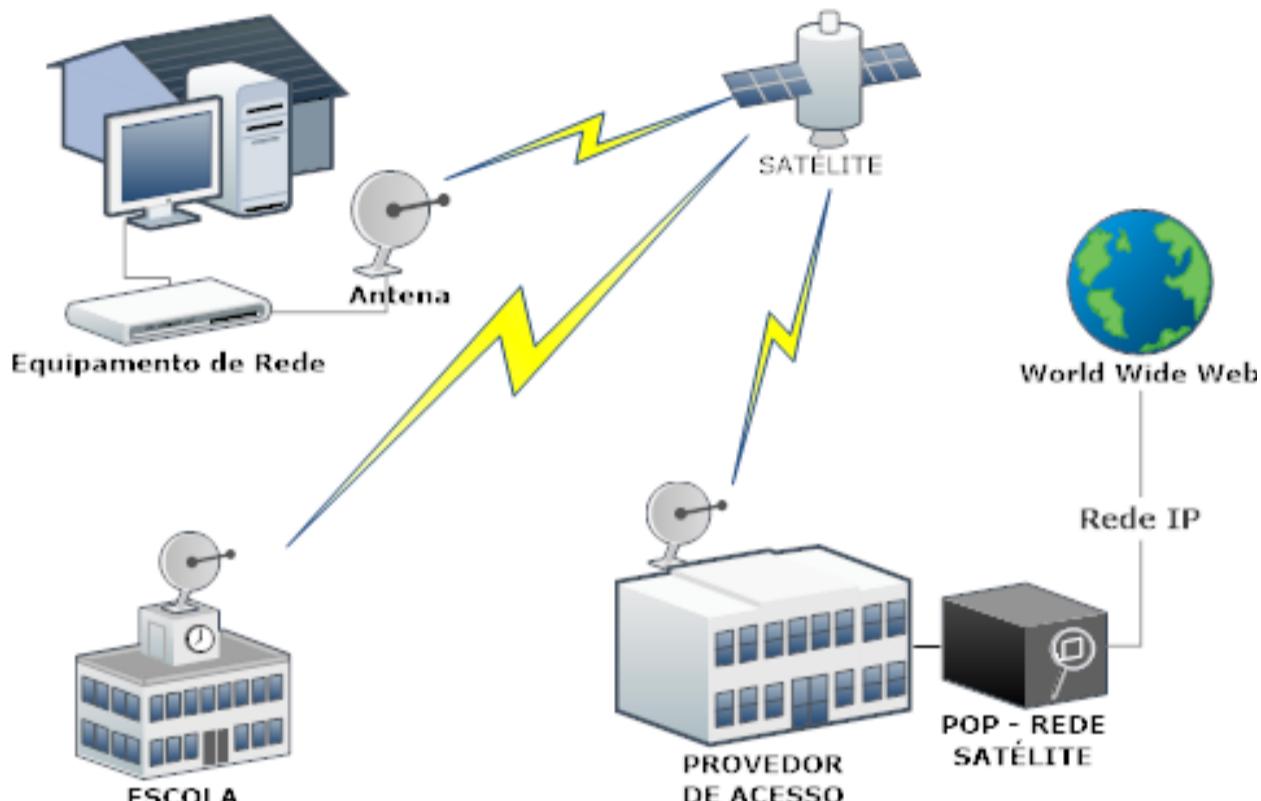
A fim de atender a demandas de conexão de longa distância e distribuição de áudio, vídeo, e imagens pela Internet, podemos utilizar conexão via satélite. Quando utilizamos os meios de transmissão por cabos, há muitos custos envolvidos com infraestrutura, e, em muitos locais, principalmente em áreas rurais ou cidades muito afastadas dos grandes centros, os custos para implantação da infraestrutura cabeada tornam-se muito elevados para as operadoras. A adoção de uma solução de comunicação por satélite elimina altos investimentos em infraestrutura, permite flexibilidade de alteração dos pontos de acesso e oferece alta disponibilidade com abrangência global.

É importante ressaltar que, ao tratarmos de comunicação de redes por rádio em distâncias de centenas de quilômetros, devemos considerar a utilização de equipamentos que tenham a função de repetir o sinal a intervalos regulares e, ao tratarmos de ambientes cabeados por fibras ópticas, torna-se necessário realizar grande investimento em infraestrutura. A conexão por satélite, no entanto, dispensa todos esses investimentos, o que possibilita a instalação em localidades isoladas. A comunicação via satélite pode ser utilizada ocasionalmente (em shows e corridas de automóvel, por exemplo) ou quando queremos que a implantação seja feita de forma rápida.

O satélite funciona da seguinte forma: a Terra emite sinais que, após serem detectados por esses satélites, têm sua frequência deslocada, são amplificados e, em seguida, retornam para a Terra. O satélite é responsável pela repetição desses sinais para que ocorra a transmissão.

Recomenda-se a comunicação via satélite quando o objetivo é fazer com que a mesma informação seja espalhada em uma região geograficamente extensa (TV e Internet, por exemplo) no link de descida, ou com que lugares remotos (como postos em rodovias, campos de mineração e propriedades rurais) sejam alcançados.

A próxima figura exibe o esquema de uma conexão via satélite:



7.7. Comunicação via satélite

7.7. Acesso móvel

O acesso móvel é o tipo de conexão a que se aplicam recursos das redes de dados das operadoras de telefonia celular ou das que são adeptas da tecnologia Wi-Fi.

Conheceremos, a seguir, as tecnologias de acesso móvel mais utilizadas.

7.7.1. Via operadora de telefonia celular

Vejamos as tecnologias de acesso móvel ligadas à operadora de telefonia celular.

7.7.1.1. 2G

Entendemos por 2G sistemas de segunda geração, uma tecnologia desenvolvida na Europa da década de 1980. Diante de dificuldades causadas por incompatibilidades entre seis sistemas celulares distintos, foi formado um comitê entre alemães e franceses que buscavam superar o nível de desenvolvimento em um sistema comum e resolver os problemas por falta de padronização que existiam.

Nesse contexto, surge o que conhecemos como GSM, sigla que designa Global System for Mobile Communications, e, inicialmente, Groupe Spécial Mobile. Ele foi organizado pela CEPT (European Conference of Postal and Telecommunications Administrations), que faz parte do PTT (European Post Telephone and Telegraphs) como seu maior órgão governamental.

A transmissão de dados sem fio foi o objetivo do CDPD (Cellular Digital Packet Data), uma tecnologia cujo protocolo foi padronizado em 1996 e que usava redes análogas de fornecedores de celulares, aproveitando sua capacidade sobressalente e usando a infraestrutura de forma eficiente para realizar a transmissão.

O projeto do CDPD pretendia proteger os dados e a identidade do usuário – que teria acesso a um serviço contínuo no sistema de rede. Além disso, o CDPD buscava o estabelecimento de parâmetros configuracionais, e escalabilidade e crescimento futuro baseado em OSI (Open Systems Interconnection), CLNP (Connectionless Network Protocol) e TCP/IP (Transmission Control Protocol/Internet Protocol).

7.7.1.2. 2.5G

A tecnologia 2.5G é, como o próprio nome sugere, intermediária em relação aos sistemas 2G e 3G. Espécie de fase de transição, ela apresenta recursos aprimorados de dados digitais em relação ao 2G, mas ainda pertence a um grau evolutivo inferior ao 3G.

Esse aprimoramento em relação ao 2G é representado, por exemplo, por recursos como taxas de dados aprimoradas para evolução GSM (EDGE) e conexões de comutação de pacotes.

Outro recurso que demonstra o aprimoramento do 2.5G permite que os usuários dos dispositivos de comunicação portáteis que funcionam em redes sem fio desse tipo, dos quais a GSM e a TDMA são exemplos, recebam serviços de dados sob demanda. Esse protocolo é conhecido como GPRS (General Packet Radio System), foi criado pelo ETSI (European Telecommunications Standards Institute) e opera com as redes sem fio TDMA e GSM que existirem.

A taxa de transmissão e recebimento de dados apresentada pelo GPRS atualmente comprehende de 40 a 60 Kb/s. Ele é capaz, contudo, de realizar essas atividades em até 171.2 Kb/s. Funções de comutação de pacotes podem ser integradas com redes de voz com circuito comutado tradicionais, e podem operar por essas redes também. O GPRS permite essas funções e integração, e suporta IP e X.25.

Com o protocolo GPRS, pacotes de dados são segmentados no que consideramos pedaços de dados, ou seja, quantias grandes de dados. Essa segmentação ocorre a partir de um dispositivo sem fio, e os pedaços de dados podem ser reconstituídos em uma rede remota após serem enviados pela rede sem fio. O dispositivo sem fio, por sua vez, recebe pacotes enviados pelo GPRS a partir da rede de dados remota.

São suportados pelas redes 2.5G:

- Recursos de diretório e pesquisa;
- Protocolo de acesso sem fio (WAP);
- Serviços de mensagens de texto (SMS) e multimídia (MMS);
- Dispositivos móveis para jogos.

7.7.1.3. 3G

Considerado uma evolução da tecnologia 2.5G, o sistema 3G é um sistema de terceira geração. Permitindo uma mobilidade em nível global e com capacidade para incorporar novos serviços e tecnologias, os sistemas 3G oferecem serviços de telefonia, transmissão de mensagens, Internet, banda larga para dados e paginação, além de fornecerem aplicativos multimídia, tais como FMV (Full-Motion Video) e videoconferência.

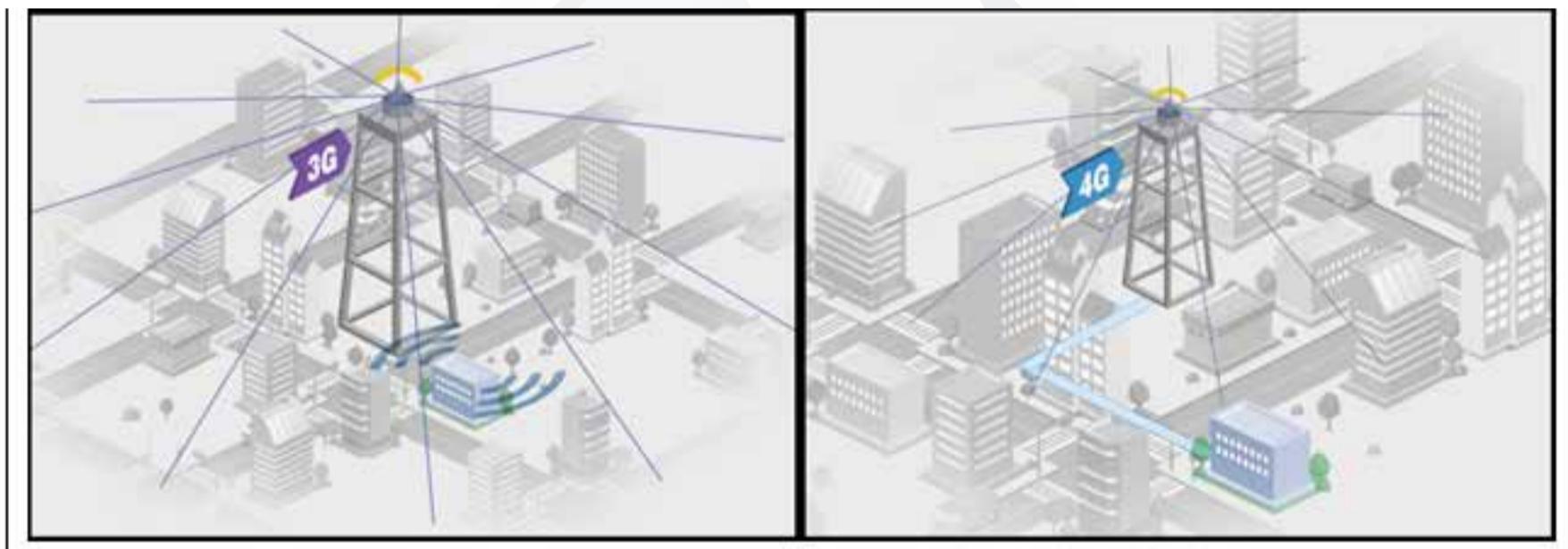
Há uma iniciativa 3G denominada IMT 2000 (International Mobile Telecommunications for the Year 2000), criada pela organização ITU (International Telecommunication Union). Esse padrão para a comunicação 3G proporcionou vários benefícios, que incluem a melhora na eficiência espectral e a alta velocidade na transmissão de dados, que supera 144 Kb/s - quantidade disponível, inclusive, para uso em ambientes abertos.

Além de suportar vários equipamentos portáteis, o sistema 3G concede suporte gradativo para 2.048 Mb/s em uso em recintos fechados – uso fixo – e suporta também serviços de dados por comutação de pacote e comutação de circuito.

Destacamos também as taxas de transmissão de dados simétricas e assimétricas, a interface adaptativa de Internet para tráfego de entrada e de saída, a qualidade de voz (podemos compará-la ao PSTN, isto é, a uma rede pública de telefonia comutada) e os 384 Kb/s disponíveis para telefones que não são muito usados.

7.7.1.4. 4G

4G é o nome utilizado para identificar a quarta geração da tecnologia celular e para agrupar tecnologias suportadas pelo WiMAX. A tecnologia 4G foi definida pela organização ITU (International Telecommunication Union), estabelecendo, para as operadoras, requisitos mínimos para oferecer velocidade de transmissão bem superior à do sistema 3G, pois foi projetada para alcançar até 100 Mbps. Por padrão, as torres de antenas 3G podem compartilhar o sinal com cerca de 60 a 100 telefones celulares; as torres de antenas 4G elevam esse número para atender entre 300 e 400 telefones celulares e, ainda, como apresentado na figura adiante, a conexão entre a torre 4G e a Central é feita por meio de cabos e, no caso da 3G, é por meio de ondas de rádio.



7.8. Tecnologia 3G vs. 4G

7.7.2. WiMAX

Desenvolvidas por um pool de empresas, a WiMAX (Worldwide Interoperability for Microwave Access) é uma tecnologia de banda larga sem fio criada para atuar em MANs, que são redes voltadas para uma metrópole.

O WiMAX, que se baseia no padrão 802.16, da IEEE, apresenta as seguintes características:

- Funciona em uma faixa de frequência entre 2 e 66 GHz;
- Propõe capacidade de banda passante aproximada de 70 Mb/s;
- Não exige que o espaço esteja livre de obstáculos, como edifícios, casas e montanhas, para que a conexão entre dois pontos possa ser efetuada, ou seja, não há necessidade de visada;
- Propõe um alcance aproximado de 50 Km.



Apesar da proposta de banda passante de até 70 Mb/s e alcance máximo aproximado de 50 Km, esses valores podem não ser atingidos na prática. Aspectos como o tipo de equipamento e a frequência utilizada influenciam na banda e no alcance.



Teste seus conhecimentos Tecnologias para acesso remoto

7

Conceitos e Infraestrutura de Redes (online)

152

1. Uma empresa deseja interligar seu prédio administrativo com os demais prédios localizados em uma mesma cidade (centro de distribuição, assistência técnica etc.) via rádio. Não há visada entre eles. Qual o tipo de rádio a ser adotado?

- a) Ponto a ponto
- b) LOS
- c) Multiponto
- d) NLOS
- e) ISDN

2. Quais são, respectivamente, as taxas máximas de upstream e downstream do canal de alta velocidade ADSL?

- a) 8 Mbps, 1 Mbps.
- b) 12 Mbps, 3,5 Mbps.
- c) 500 Kbps, 1.500 Kbps.
- d) 1 Mbps, 12 Mbps.
- e) 1 Mbps, 8 Mbps.

3. Qual tipo de conexão um provedor de Internet via rádio possui com seus clientes?

- a) Ponto-multiponto
- b) Ponto a ponto
- c) POP a POP
- d) POP-NLOS
- e) Nenhuma das alternativas anteriores está correta.

4. Quais são os nomes das taxas disponibilizadas pelo ISDN?

- a) Taxa mínima e taxa máxima.
- b) Taxa de downstream e taxa de upstream.
- c) Taxa básica e taxa primária.
- d) Taxa primária e taxa secundária.
- e) Taxa básica e taxa máxima.

5. Após estudos de tráfego, uma empresa deseja implantar 75 canais de voz em sua nova unidade fabril. De quantos links E1 a empresa precisará?

- a) 2 links E1
- b) 2,5 links E1
- c) 1 link E1
- d) 3 links E1
- e) Não é possível atender a essa necessidade.

Redes wireless

8

- ✓ Redes baseadas em infravermelho;
- ✓ Redes baseadas em laser;
- ✓ Redes baseadas em radiofrequência.

8.1.Introdução

O termo “wireless”, do inglês, pode ser traduzido como “sem fio”. Por esse motivo, redes wireless também são denominadas redes sem fio. São wireless as conexões e transmissões de dados que não utilizem fios e cabos para serem estabelecidas. A principal característica desse tipo de rede é a mobilidade na comunicação. O IEEE (Institute of Electrical and Electronics Engineers) definiu, no padrão 802.11 para WLAN (Wireless Local Area Network), os protocolos para controle de acesso ao meio (ou MAC, Media Access Control) e para o nível físico (PHY, Physical Layer). O método de acesso a mídia é gerenciado pelo CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance), que garante que os dados serão enviados apenas com canal livre. O usuário que deseja transmitir dados envia um RTS (Request to send), solicitando a informação de que o canal está livre, e somente transmite dados ao receber o CTS (Clear to send). Não receber o CTS indica que o canal está ocupado e que o usuário deverá tentar mais tarde.

Há redes wireless projetadas para suportar conexões de longa distância (entre cidades, por exemplo), bem como para atender a necessidades muito menores (para uso doméstico, pequenos escritórios e até conexão entre celulares). Para estabelecer tais conexões, podemos utilizar redes baseadas em laser, radiofrequência ou infravermelho.

Veremos, a seguir, as características de cada uma delas.

8.2.Infravermelho

Uma das tecnologias para transmissão de sinais sem fio é a luz infravermelha. Ela é utilizada, principalmente, em redes sem fio em que notebooks são conectados à rede convencional. Em algumas empresas, por exemplo, funcionários recolhem dados de clientes por meio de um notebook e, depois, precisam transmitir os dados à rede. A conexão do notebook à rede pode ser feita por meio de luz infravermelha.

Os protocolos do infravermelho foram definidos por um grupo de empresas associadas conhecido como IrDA (Infrared Data Association). Esse padrão de comunicação sem fio utiliza sinais de infravermelho emitidos por um LED, os quais são captados por um sensor. Nesse caso, o sensor e o LED são apontados diretamente um para o outro a uma curta distância. O padrão IrDA possui duas derivações: IrDA-D (Data), orientado à conexão entre dispositivos para a troca de dados, e IrDA-C (Control), orientado a comando e controle de periféricos.

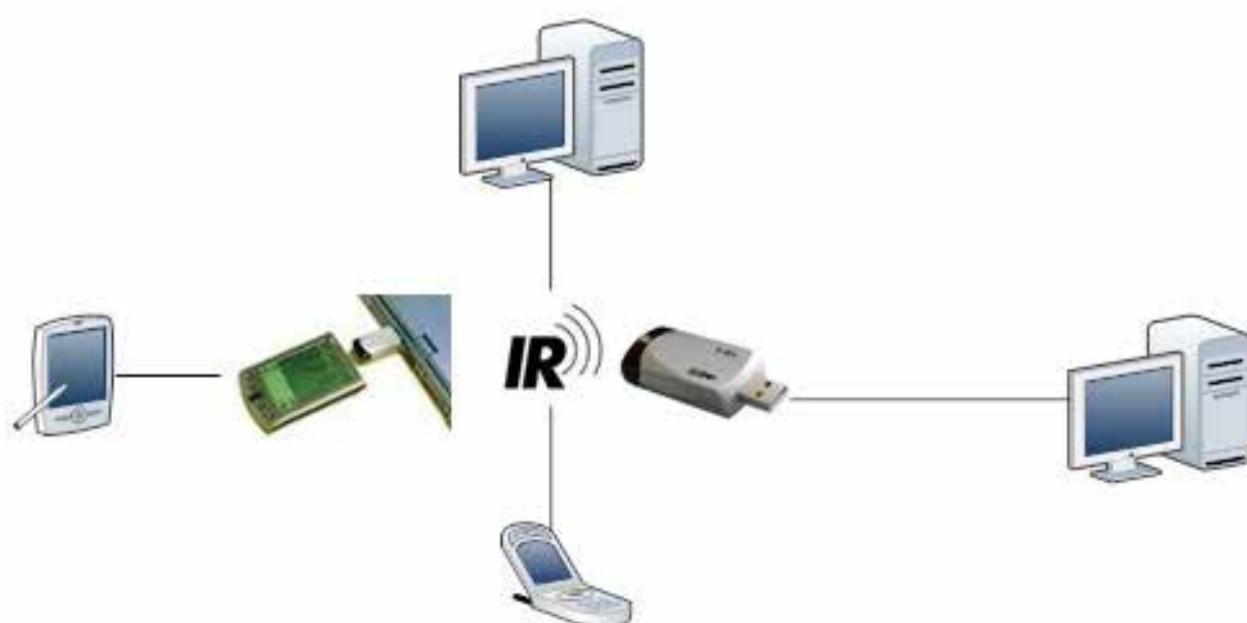
Nessa derivação dos padrões, os equipamentos de enlace, conhecidos como transceivers, são divididos em duas categorias: IrDA-1.0 e IrDA-1.1; em cada uma dessas categorias, há características específicas de codificação e controle de transmissão dos dados e ópticas, como veremos a seguir:

- O padrão IrDA-1.0 possui o modo de conexão SIR – Slow-Speed Infrared Mode, que possui velocidade de dados de até 115.2 Kbps. Ao iniciar o processo de transmissão, cada bit passa por um processo de codificação e, quando chega ao receptor, passa pelo processo de decodificação;
- O padrão IrDA-1.1 possui o modo de conexão FIR – Fast-Speed Infrared Mode, que trabalha com dados na velocidade de até 4 Mbps. Nesse modelo, o transmissor é responsável por montar o frame, anexando no cabeçalho o flag inicial (start flag), o controle de erros e redundância cíclica (CRC-32) e também o flag final (stop flag).

Entretanto, a transmissão por infravermelho possui alguns inconvenientes: não atravessa objetos sólidos (como paredes), não faz curvas e possui alcance muito limitado, praticamente restringindo as transmissões a um mesmo ambiente.

A transmissão por infravermelho é feita por dois métodos:

- **Transmissão direta:** O transmissor e o receptor possuem ângulo de abertura pequeno. Assim, é necessário que eles estejam alinhados para que a transmissão aconteça;
- **Transmissão difusa:** Nesse tipo de transmissão, os sinais infravermelhos são enviados em todas as direções. Possui taxa de transferência e área de alcance menores que as da transmissão direta.



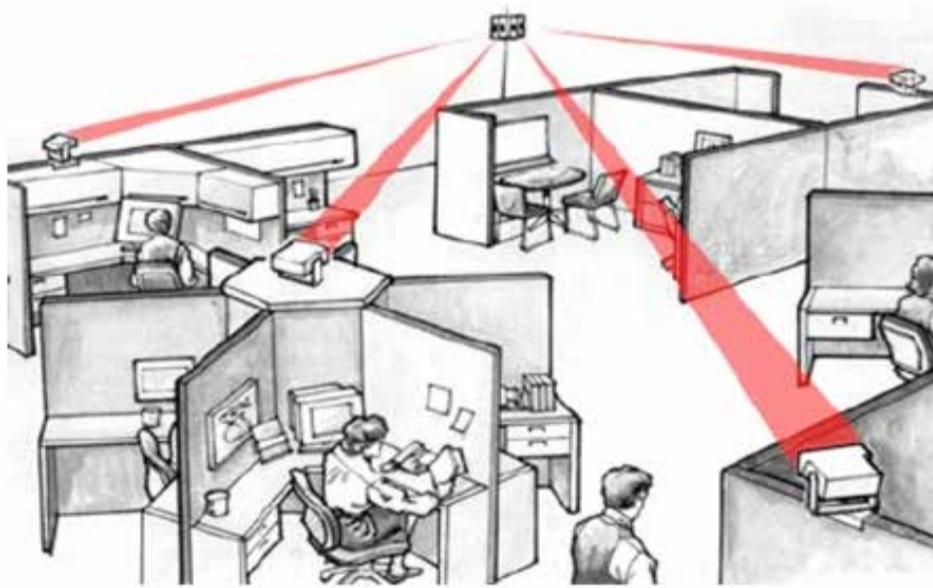
8.1. IrDA – Infravermelho

8.3.Laser

A transmissão por laser também é feita por meio de luz, mas com um comprimento de onda diferente da luz infravermelha. A principal característica da transmissão a laser é ser altamente direcional. Isso significa que os transmissores e receptores devem estar perfeitamente alinhados.

O laser possui um alcance bem maior que o infravermelho, mas possui um grande inconveniente, que é a presença de obstáculos. Qualquer tipo de obstáculo, incluindo chuva e fumaça, impede que a transmissão aconteça.

Por meio de enlaces a laser, é possível transmitir sinais entre dois pontos a uma distância de 1500 m. Para isso, não é necessária a instalação de cabos nem a reserva de espectro de frequência, e a velocidade é compatível com a do padrão Ethernet, ou seja, 10 Mbps. E, nesse caso, o link inclui conversores transmissor e receptor de alta resolução, conforme a figura a seguir:



8.2. Enlace a laser

Algumas características de um enlace a laser:

- Não necessita de instalação de cabos e fibras ópticas;
- Não sofre interferências eletromagnéticas;
- Possui flexibilidade para relocação do enlace óptico;
- Torna a transferência de informação inviolável;

- Possui velocidades de transmissão LAN compatíveis;
- É recomendado para ambientes com ruídos (centrais elétricas, centros urbanos onde o espectro de frequência esteja saturado etc.).

8.4. Radiofrequênciа

A seguir, vamos tratar de três tecnologias de transmissão por radiofrequência.

8.4.1. RFID

A sigla RFID refere-se a Identificação por Radiofrequência, que é uma tecnologia utilizada na coleta de dados. Essa tecnologia utiliza frequências entre 50 KHz e 2,5 GHz. Dependendo da frequência de operação dos sistemas de RFID, eles podem ser classificados como sistemas de baixa, média e alta frequência.

- **Sistemas de banda de frequência baixa:** Com frequências entre 100 e 500 KHz, são caracterizados por terem faixa curta/média de leitura, baixa velocidade de leitura e baixo custo. São utilizados, tipicamente, em controle de acesso, controle de inventário e identificação de animais;
- **Sistemas de banda de frequência média (ou alta):** Com frequências entre 10 e 15 MHz, são caracterizados por terem faixa curta/média de leitura, média velocidade de leitura e potencial de baixo custo. São, geralmente, utilizados em controle de acesso e smart cards;
- **Sistemas de banda de frequência alta (ou ultra-alta):** Com frequências entre 850 e 950 MHz e 2,4 e 5,8 GHz, possuem faixa larga de leitura, alta velocidade de leitura e alto custo, além de exigir linha de visão. É utilizada, por exemplo, em monitoramento de veículos em estradas.

Os sistemas em faixas baixa e intermediária utilizam o princípio de acoplamento indutivo, em que a relação entre a quantidade de energia transferida do transceptor para o tag e o tamanho das antenas de transmissão e recepção é proporcional.

Sistemas em faixa de alta frequência operam de maneira diferente, de acordo com o princípio da comunicação de antenas de radar. Isso significa que o tag se comunica com o transceptor através da modulação do sinal recebido pelo tag e, em seguida, é radiado de volta para o transceptor.

É preciso destacar que a frequência utilizada influencia diretamente a taxa de transferência de dados, de forma que um sistema com alta frequência de faixa permite uma alta taxa de transferência de dados e, consequentemente, um alto número de tags que podem ser lidos de forma simultânea.

8.4.1.1. Equipamentos RFID

A seguir, veremos quais são os elementos básicos dos sistemas RFID:

- **Antena (ou bobina):** A antena é responsável por emitir um sinal para ativar um tag e ler ou escrever dados nele. As antenas possuem formatos e tamanhos diversos. Podem estar presentes em um dispositivo móvel (como um leitor portátil) ou em estruturas fixas (como numa porta de estabelecimento comercial, lendo informações dos tags de mercadorias);
- **Transceptor (ou leitor):** É o componente responsável por realizar a comunicação entre um sistema RFID e sistemas externos de processamento de informações. A depender do tipo de tag e funções a aplicar, pode haver transceptores mais simples ou mais complexos, como os que têm função de verificação de paridade de erro e correção de dados. Quando os sinais do receptor são recebidos e decodificados corretamente, pode-se definir, por meio de algoritmos, se o sinal é uma repetição de transmissão de um tag;
- **Transponder (ou tag):** O transponder (transmitter/responder) tem como função transmitir uma resposta para o transmissor com base em dados armazenados nele. Há dois tipos de transponder ou tag:
 - **Tag ativo:** Típico de leitura/escrita, este tipo de tag é energizado por uma bateria interna. O tamanho da memória de tags ativos é variável, dependendo da aplicação que se dá para o tag;
 - **Tag passivo:** Geralmente, possui memória apenas para leitura (ROM, ou Read Only Memory), ou seja, que não pode ser alterada. Possui vida útil maior que tags ativos, além de custo inferior.

Uma consideração importante a respeito dos sistemas de RFID é que muitos dos que estão à disposição são sistemas proprietários, ou seja, sistemas que não podem ser utilizados com equipamentos de outro fabricante. Desse modo, há uma diversidade muito grande de protocolos de sistemas de RFID, mesmo em uma única planta industrial. Esforços têm sido feitos por diversas organizações no sentido de padronizar protocolos. Entre as mais conhecidas, na área de sistemas RFID, estão a EPC Global e a ISO (International Organization for Standardization).

8.4.2. Bluetooth (802.15 – WPAN)

O bluetooth é um padrão global de comunicação que utiliza radiofrequência para realizar a transmissão de dados entre os dispositivos compatíveis (computadores, telefones celulares, smartphones, teclados, fones de ouvido etc.). A comunicação via bluetooth é feita por meio de uma combinação entre hardware e software. Nesse tipo de comunicação, um dispositivo, independentemente do seu posicionamento, pode detectar outro, desde que esteja dentro do seu limite de alcance.

O alcance é variável entre os diversos dispositivos e é dividido em três classes:

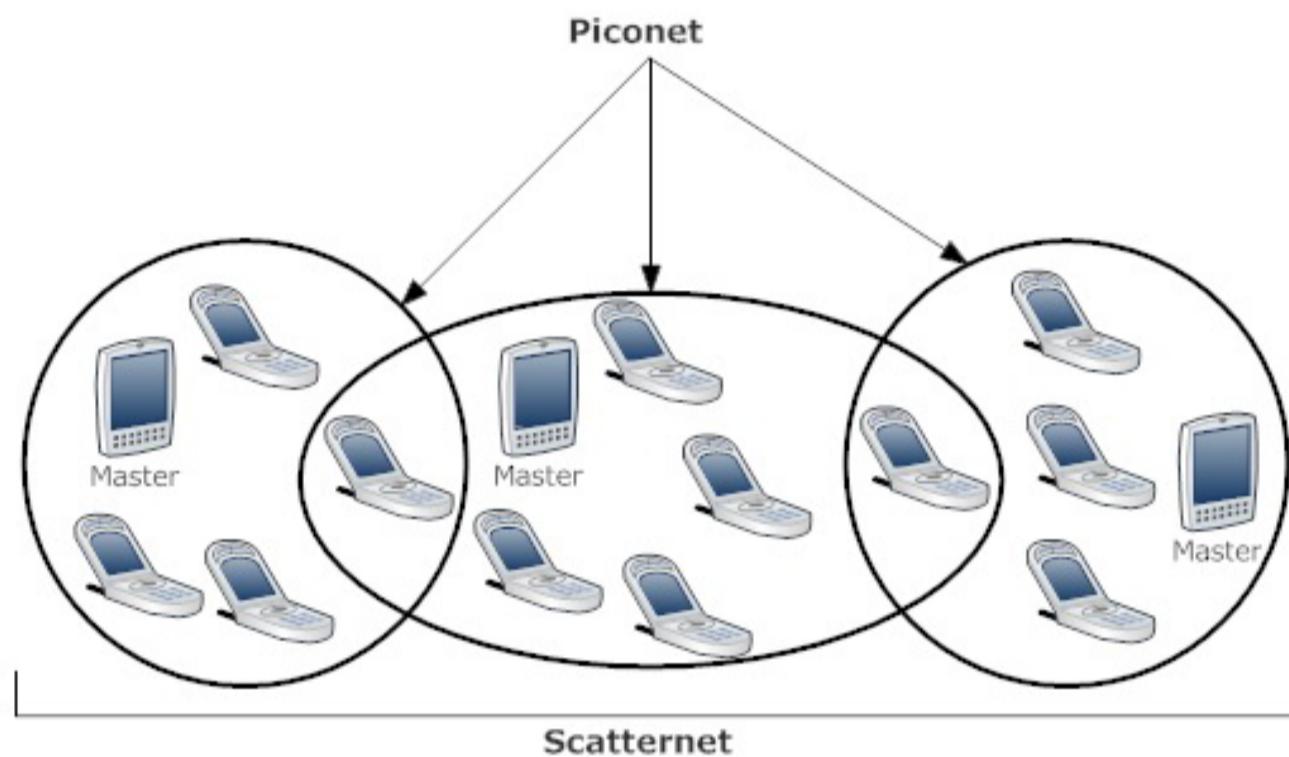
- **Classe 1:** Potência máxima de 100 mW, com alcance de até 100 metros;
- **Classe 2:** Potência máxima de 2,5 mW, com alcance de até 10 metros;
- **Classe 3:** Potência máxima de 1 mW, com alcance de até 1 metro.

Um dispositivo Classe 3, portanto, só consegue se comunicar com dispositivos situados a menos de 1 metro de distância. É o suficiente para conectar um teclado ao computador, ou um fone de ouvido ao celular, por exemplo. É importante ressaltar que dispositivos de diferentes classes podem se comunicar, desde que respeitado, é claro, o limite do dispositivo de menor alcance.

8.4.2.1. Redes de dispositivos bluetooth

Uma rede formada por dois ou mais dispositivos que se comunicam por meio de bluetooth é chamada de piconet. Nesse tipo de rede, a relação master/slave entre os dispositivos é definida pelo dispositivo que iniciou a comunicação. Ele é o master, responsável por regular a transmissão de dados e o sincronismo entre os dispositivos. Os outros dispositivos são definidos como slave.

Uma piconet suporta até oito dispositivos (um master e sete slaves). É possível, ainda, sobrepor piconets, ou seja, estabelecer conexão entre duas ou mais piconets. Isso é denominado scatternet. Neste caso, um dispositivo slave pode fazer parte de mais de uma piconet ao mesmo tempo. Um master, contudo, só pode ocupar essa posição em uma única piconet.



8.3. Rede bluetooth

8.4.3. WLAN – 802.11

A especificação IEEE 802.11 é o principal padrão de comunicação utilizado em redes WLAN. Esse padrão define os protocolos para controle de acesso ao meio (ou MAC, Media Access Control) e para o nível físico (PHY, Physical Layer).

Os padrões e suas extensões determinam uma quantidade de opções para a comunicação em redes de fio. Os produtos para redes WLAN voltados para consumidores e empresas possuem apenas algumas dessas extensões adequadamente implementadas. As faixas de frequência em que operam os produtos para redes WLAN, conhecidas como ISM (Industrial, Scientific, Medical), são as seguintes: 900 MHz, 2,4 GHz e 5 GHz.

8.4.3.1. Padrão 802.11b

O padrão 802.11b, o primeiro a ser utilizado em larga escala, foi responsável por popularizar as redes sem fio. A faixa de frequência em que esse padrão opera é de 2,4 GHz. A velocidade de conexão é de até 11 Mbps.

8.4.3.2. Padrão 802.11g

Disponível desde 2003, esse padrão é considerado sucessor do 802.11b, sendo totalmente compatível com ele. Opera em faixa de frequência de 2,4 GHz. A velocidade de conexão é de até 54 Mbps.

8.4.3.3. Padrão 802.11a

Disponibilizado depois do 802.11b, esse padrão opera em faixa de frequência de 5 GHz e possui velocidade de transmissão de até 54 Mbps.

8.4.3.4. Padrão 802.11n

Esse padrão opera em faixa de frequência de 2,4 GHz e/ou 5 GHz e possui velocidade de transmissão acima de 300 Mbps.

8.4.3.5. Padrão 802.11ac

Esse é o novo padrão de conexão WLAN para alto desempenho desenvolvido pelo IEEE. O padrão 802.11ac é considerado a próxima geração da tecnologia wireless e tem vantagens como melhores técnicas de modulação de sinal e canais mais amplos para o tráfego de dados. Além disso, por operar somente na faixa de frequência de 5 GHz, que tem mais canais e menor concorrência (em relação à faixa de 2.4 GHz usada pelas tecnologias Wi-Fi atuais), o padrão 802.11ac é mais rápido.

Na especificação 802.11ac, o número máximo de streams é oito, e a largura máxima por stream é 433 Mbps. Os aparelhos de primeira geração, no entanto, usarão apenas duas ou três antenas para recepção e transmissão, com largura de banda máxima de 866 Mbps, ou 1.3 Gbps.

8.4.3.6. Equipamentos WLAN

O equipamento mínimo em uma rede wireless constitui-se de dois dispositivos de rede, equipados com placas de interface de rede (NICs) sem fio, além do software cliente adequado.

Conceitos e Infraestrutura de Redes (online)

164

Adiante, abordamos os componentes de redes wireless:



8.4. Equipamentos WLAN

- **Placas de interface de rede (ou NICs, network interface cards)**

Esses componentes são responsáveis por habilitar um dispositivo autônomo a funcionar como estação (ou cliente) em uma rede wireless. O dispositivo pode ser tanto um notebook ou desktop quanto um dispositivo mais especializado, como um leitor de código de barras.

- **Software cliente**

Para ser conectado a uma rede wireless, o software cliente pode ser incluído com uma placa de interface de rede ou desenvolvido no sistema operacional do dispositivo.

O mínimo que um software cliente deve incluir são os drivers, responsáveis pela conexão entre a placa de interface de rede e o sistema operacional. É por meio dos drivers que o sistema operacional pode configurar e utilizar a placa de interface de rede nas comunicações sem fio.

- **Pontos de acesso**

Os pontos de acesso se comunicam com estações, redes cabeadas e outros pontos de acesso, além de serem o destino inicial de todas as mensagens enviadas por estações, o que permite que sejam configurados para fornecer, de forma centralizada, diversos serviços de rede para as estações presentes. Os pontos de acesso constituem um ponto central de configuração e gerenciamento em uma rede wireless.

Entre os serviços fornecidos pelos pontos de acesso, destacamos:

- Segurança, impedindo o acesso de estações sem fio não autorizadas e criptografando todas as mensagens;
- Gerenciamento, fornecendo informações sobre status e permitindo manutenção remota sobre a rede organizacional ou a Internet;
- Configuração, direcionando identificadores para estações autorizadas;
- Roaming, permitindo às estações moverem-se entre zonas cobertas controladas por outros pontos de acesso.

Podemos classificar um ponto de acesso, genericamente, como residencial ou organizacional. Os do segundo tipo normalmente oferecem recursos de gerenciamento e segurança adicionais em relação aos residenciais. Esses recursos podem estar embutidos no ponto de acesso ou serem inclusos, com um custo extra, pelos fornecedores, que geralmente oferecem caminhos de migração para atualização dos pontos de acesso.

A alimentação elétrica e a conexão de pontos de acesso a uma rede cabeada podem ser feitas por meio de um único cabo Ethernet, o que confere flexibilidade aos projetistas e administradores de redes wireless. Em um cabo de quatro pares trançados平衡ados, dois pares são utilizados para o sinal de Ethernet e os outros dois podem ser usados para fornecer voltagem.

É preciso ressaltar que, além de permitir comunicação entre estações sem fio, os pontos de acesso também podem operar em pontes wireless.

- **Antenas**

Tanto os pontos de acesso quanto as placas de interface de rede possuem antenas embutidas para transmitir e receber sinais para os dispositivos. Em alguns casos, podem-se utilizar antenas externas. As antenas de ambientes wireless podem ser unidirecionais, direcionais ou omnidirecionais.

- **Pontes**

As pontes realizam ligação entre dispositivos de acesso, aumentando a zona de cobertura, ou amplitude física, de uma rede. Podem ser utilizadas em ambientes wireless ou cabeados.

Conceitos e Infraestrutura de Redes (online)

166

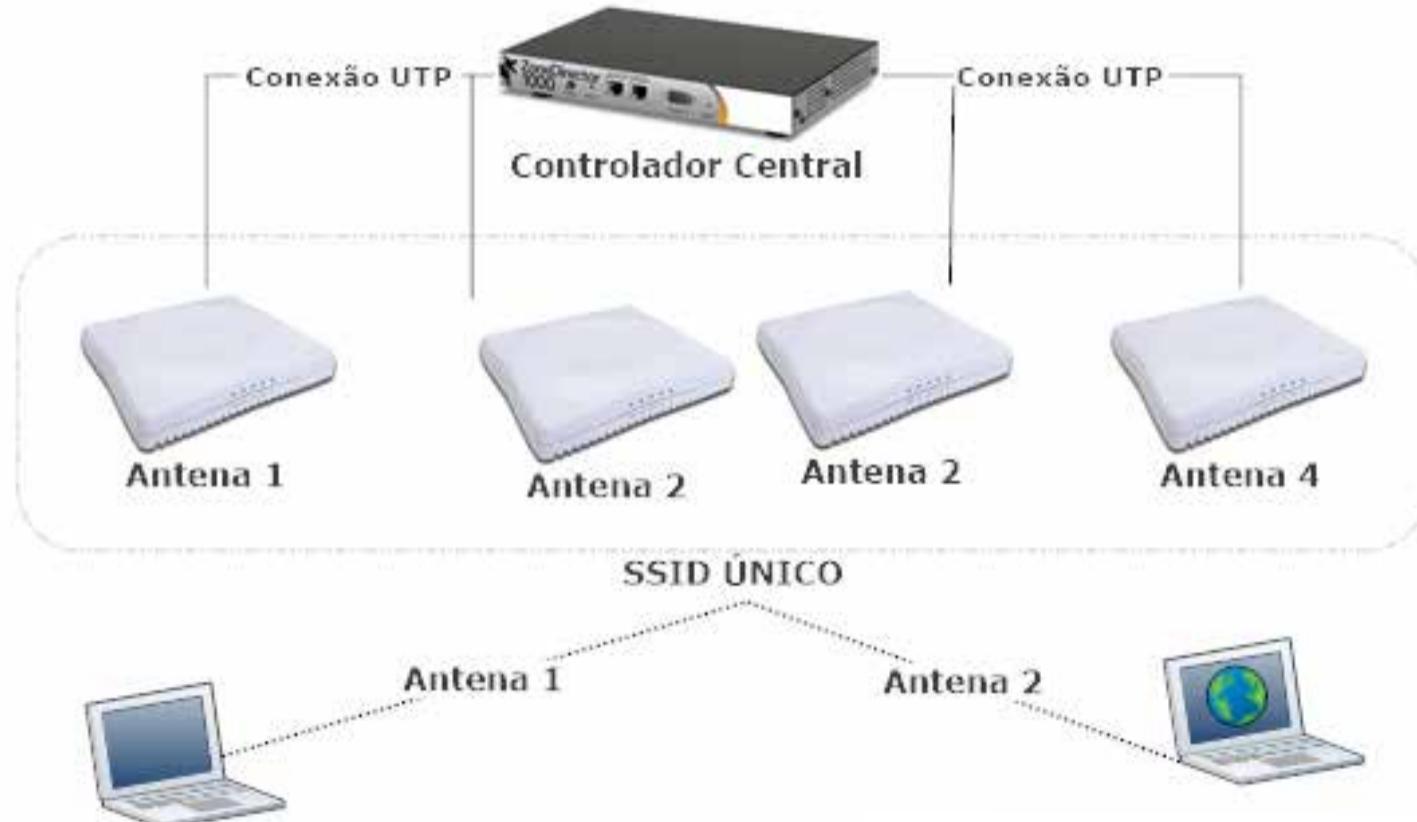
Em ambientes wireless, há dois tipos de ligação entre pontos de acesso:

- **Ligaçāo ponto a ponto:** Dois pontos de acesso, cada um deles conectado a uma rede cabeada, são ligados entre si;
- **Ligaçāo ponto a multiponto:** Ligação entre um ponto de acesso conectado a uma rede cabeada e pontos de acesso que oferecem acesso de rede a diversas estações.

Também podemos utilizar pontes wireless para estender a amplitude de uma conexão ponto a ponto. Uma ponte é colocada entre os dois pontos de acesso, tendo como função transmitir todos os sinais enviados entre eles. Esse mecanismo também é conhecido como ponte de repetição ou extensor de alcance.

- **WLAN com controle centralizado**

Ambientes de grande tráfego ou que possuem muitas pessoas acessando ao mesmo tempo, como universidades, campus, aeroportos etc., exigem um número maior de antenas. O controle administrativo, no entanto, pode ser centralizado. Em alguns modelos de equipamentos de fabricantes específicos, até 25 antenas podem ser implementadas para um único controlador, cada antena pode suportar até 200 conexões e todo o ambiente poderá responder por um único SSID (Service Set Identifier).



8.5. Gerenciamento centralizado

- **Switches**

Em redes wireless com quantidade limitada de pontos de acesso, o gerenciamento e a comunicação são feitas pelos próprios pontos de acesso, que podem ser monitorados e configurados individualmente. Em ambientes de rede com uma quantidade de pontos de acesso que torna inviável seu gerenciamento individual, podemos usar switches. Eles são dispositivos cuja função é gerenciar, de forma centralizada, os pontos de acesso conectados. Assim, não é necessário conectar cada um deles a um switch que está ligado à rede cabeadas. As conexões são dirigidas a um switch wireless.

- **Roteadores**

Um roteador wireless é um dispositivo que reúne funções de hardware e software, como serviços de impressão, recursos de segurança (como firewall), uma interface para conexão com um dispositivo de rede provedor de serviços de Internet (como um modem DSL) e um hub interno, ou portas switch para conectar certa quantidade de dispositivos cabeados (como um switch 4 portas 10/100 Mbps). Os roteadores wireless são associados a redes residenciais ou escritórios domésticos, que possuem poucos dispositivos para conectar e priorizam baixo custo.

- **Gateways**

Os gateways permitem aos administradores de rede gerenciar de maneira centralizada uma grande quantidade de pontos de acesso. Funcionam, portanto, de modo similar aos switches wireless. São diferentes, porém, com relação aos recursos administrativos, que são mais sofisticados nos gateways.

8.4.3.7. Configuração lógica das redes wireless

A configuração lógica das redes wireless depende do tipo de rede exigida. Podemos identificar três tipos de configuração lógica para redes WLAN. Esses tipos são definidos em padrões IEEE e serão abordados a seguir:

- **Redes ad hoc (ou IBSS, Independent Basic Service Set)**

Uma rede desse tipo é constituída quando temos duas ou mais estações equipadas com placas de interface de rede que se comunicam entre si. É apropriada para um pequeno número de dispositivos em uma área comum, geralmente configurada para uma duração determinada de tempo. Em redes ad hoc, os dados são transferidos entre os dispositivos diretamente, sem necessidade de ponto de acesso. Dessa forma, o tempo de configuração é menor e a conexão é mais simples e conveniente para os usuários.

Conceitos e Infraestrutura de Redes (online)

168

- **Redes de infraestrutura básica (ou BSS, Basic Service Set)**

Nesse tipo de rede, a comunicação entre duas ou mais estações com placas de interface de rede sem fio é gerenciada de forma centralizada por um único ponto de acesso, que permite aumentar a quantidade de estações e a amplitude física da rede. Em redes BSS, a comunicação não pode ser feita antes da instalação de um ponto de acesso, o qual pode ser uma unidade independente ou estar conectado a uma rede cabeada.

- **Redes de infraestrutura (ou ESS, Extended Service Set)**

Nesse tipo de rede, temos dois ou mais pontos de acesso de diferentes redes BSS em conexão, que pode ser cabeada ou sem fio. Esse tipo de configuração é utilizado quando a área da rede ou o número de estações ultrapassa a capacidade de um único ponto de acesso. É importante ressaltar que, quando as áreas de cobertura de duas redes BSS se interseccionam, é possível que uma estação na rede ESS se mova de uma rede BSS para outra sem perder conexão de rede.

A rede utilizada para ligar os pontos de acesso é chamada de sistema de distribuição. Quando os pontos de acesso estiverem conectados por cabos, eles serão descritos como gateways. Eles convertem os sinais entre a rede baseada no padrão IEEE 802.11 e o sistema de distribuição.

Devemos considerar que, ao contrário de uma rede wireless pequena e independente, que demanda apenas placas de rede e pontos de acesso, redes wireless em larga escala e conectadas a uma rede organizacional ou à Internet podem, frequentemente, demandar componentes adicionais.



**Teste seus conhecimentos
Redes wireless**

8

1. Uma empresa de logística pretende implantar um sistema de auxílio nas operações de recebimento, separação, transporte, armazenamento e expedição de materiais em seus depósitos e armazéns. Qual a melhor tecnologia a ser indicada?

- a) 802.11
- b) Bluetooth
- c) Infravermelho
- d) Laser
- e) RFID

2. O padrão 802.11a é compatível com o padrão 802.11g?

- a) Sim, ambos possuem transmissão de até 54 Mbps.
- b) Não, pois trabalham em frequências diferentes.
- c) Sim, todos os padrões 802.11 são compatíveis.
- d) Não, cada padrão é único.
- e) Nenhuma das alternativas anteriores está correta.

3. Qual o número máximo de dispositivos que podem ser encontrados em uma rede piconet?

- a) 7
- b) 9
- c) 8
- d) 6
- e) 5

4. Qual é o dispositivo de uma rede wireless padrão 802.11g responsável por impedir o acesso de dispositivos não autorizados, criptografar todas as mensagens e fazer a interligação com a rede cabeada?

- a) Roteador wireless
- b) Switch wireless
- c) Ponto de acesso
- d) Gateway
- e) Ponte

5. Quando uma estação se move de um ponto de acesso a outro sem perder a conexão, qual o nome da configuração lógica implantada?

- a) Rede ad hoc
- b) BSS
- c) Rede de infraestrutura básica
- d) IBSS
- e) ESS

Protocolos de rede 9

- ✓ Tipos de protocolos;
- ✓ Pilhas de protocolos;
- ✓ Modelo OSI;
- ✓ Protocolos para conexões à distância.

9.1. Introdução

Entendemos como protocolo um conjunto de regras preestabelecidas destinadas a organizar o modo pelo qual os computadores de uma rede comunicam-se uns com os outros.

A comunicação entre duas máquinas diferentes é possível somente no momento em que elas têm o mesmo protocolo, ou seja, os protocolos devem apresentar compatibilidade entre si. Apesar disso, cada tipo de protocolo possui sua própria função e promove a execução de tarefas diferentes.

9.2. Tipos de protocolos

Há diversos tipos de protocolos que podem ser encontrados; eles podem ser abertos, proprietários, roteáveis e não roteáveis. Nos tópicos a seguir, veremos quais são suas características, bem como as diferenças entre eles.

9.2.1. Abertos

Protocolos abertos são aqueles de domínio público, ou seja, que não são de propriedade privada. Os protocolos abertos são compatíveis entre si, uma vez que todos seguem os mesmos padrões. Um exemplo muito conhecido desse protocolo é o TCP/IP, utilizado para a troca de informações na Internet.

9.2.2. Proprietários

Os protocolos proprietários, ao contrário dos abertos, são de propriedade privada, uma vez que seus fornecedores os desenvolvem para que sejam utilizados apenas em seus ambientes específicos.

Podemos citar como exemplos os seguintes protocolos:

- **IPX/SPX:** Desenvolvido pela Novell para intercâmbio dos pacotes das redes na arquitetura NetWare;
- **AppleTalk:** Empregado por sistemas de computadores Apple.

Dessa forma, podemos concluir que os protocolos proprietários são desenvolvidos para que sejam utilizados apenas para a troca de informações entre computadores cujos ambientes sejam aqueles especificados por seu fornecedor.

9.2.3. Protocolos roteáveis

Os protocolos roteáveis oferecem suporte para a transmissão de dados entre segmentos diferentes de rede, seja esta rede de pequeno porte – cuja área de envolvimento pode ser apenas um prédio –, ou de grande porte, como a Internet. Os protocolos **TCP/IP** e **IPX/SPX** também são exemplos de protocolos roteáveis.

9.2.4. Protocolos não roteáveis

Os protocolos não roteáveis não suportam a transmissão de dados entre os segmentos de rede diferentes. Eles apenas podem promover a transmissão de dados entre computadores que estejam dentro do mesmo segmento de rede. O **NetBEUI**, desenvolvido pela **Microsoft**, é um bom exemplo desse tipo de protocolo: é um protocolo de transporte utilizado nos sistemas operacionais de rede.

9.3. Pilhas de protocolos

Uma pilha de protocolos é um conjunto de protocolos dispostos em camadas. A pilha de protocolo mais conhecida é o **TCP/IP**. De acordo com a sua função, cada protocolo trabalha em uma camada específica. Esses mesmos protocolos utilizam a pilha de protocolos para promover a transmissão de dados e estão classificados de acordo com a tarefa que desempenham na rede:

- **Protocolos de aplicativo:** Um exemplo desse tipo de protocolo é o **FTP**, responsável pela transferência de arquivos dentro da rede. Esses protocolos promovem a troca de dados entre os aplicativos disponíveis em uma rede;
- **Protocolos de transporte:** Esses protocolos são responsáveis por uma transmissão de dados confiável durante a comunicação entre computadores diferentes. O **TCP** é um exemplo de protocolo de transporte responsável pelo controle das transmissões;
- **Protocolos de rede:** Esse tipo de protocolo define os preceitos para que haja comunicação apenas em um ambiente da rede. O protocolo **IP** é considerado um protocolo de rede.

9.4. Modelo OSI

Em razão da evolução das redes de computadores, muitos fabricantes de equipamentos e sistemas passaram a criar soluções proprietárias de arquitetura fechada para atender as crescentes demandas do mercado. Entretanto, essa diversidade criou uma incompatibilidade, pois os fabricantes desenvolviam equipamentos com características e funcionalidades específicas, o que tornava as implementações de softwares e hardwares exclusivas e muito distintas de outros fabricantes. Por essa razão, muitas redes de computadores tornaram-se incompatíveis, exigindo que existissem equipamentos e softwares de fabricantes específicos para que houvesse total interoperabilidade.

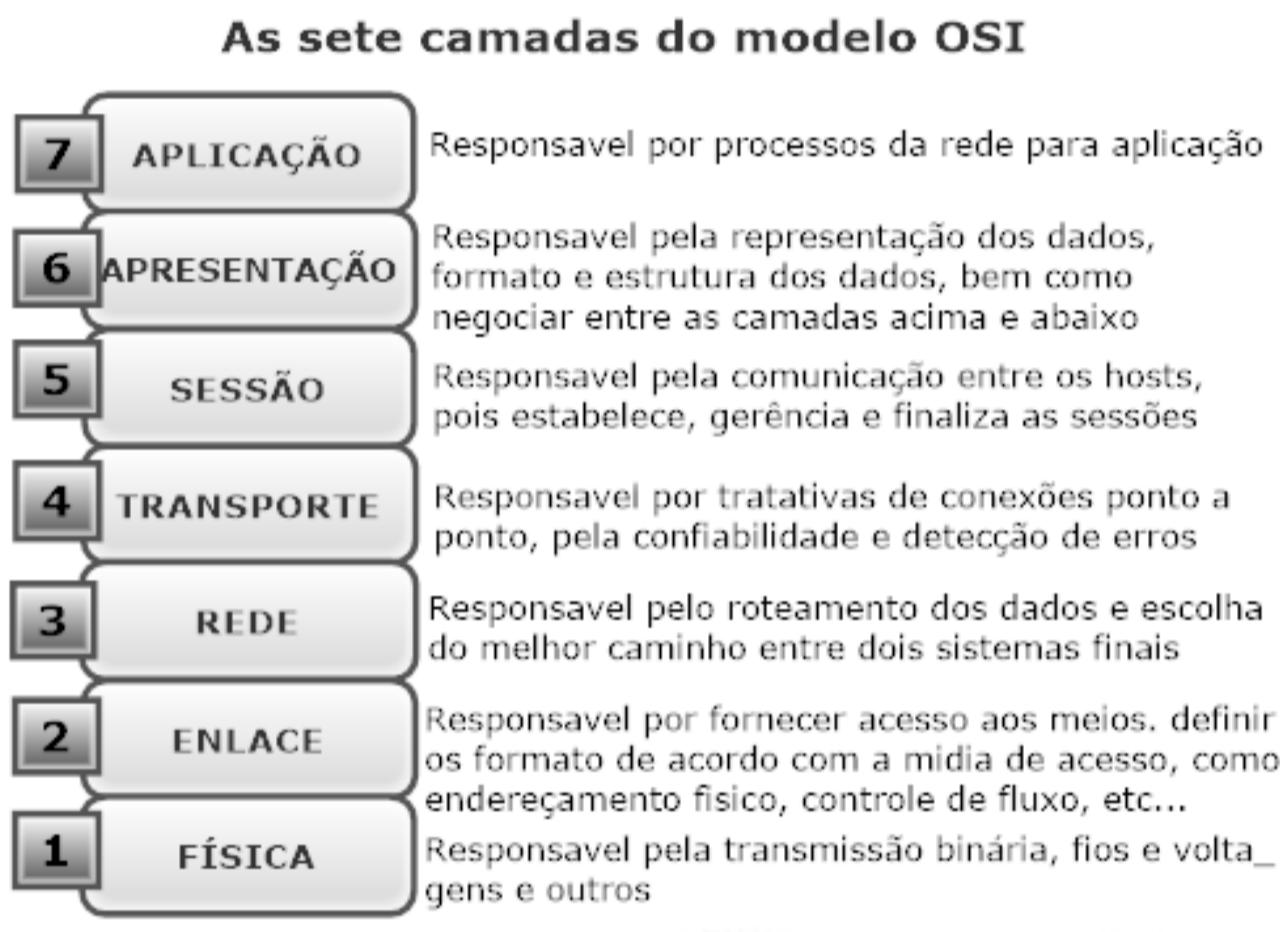
Em vista disso, a Organização Internacional de Padronização (ISO – International Organization for Standardization) estudou uma solução para que houvesse um padrão de interconexão entre padrões abertos de comunicação. Então, a ISO criou o modelo de Referência OSI (Open Systems Interconnection), fazendo com que, independentemente de fabricante e funcionalidades, as redes de computadores pudessem conversar entre si, passando, então, a adotar um padrão de arquitetura aberta, facilitando para as organizações, que não ficariam presas a um único fabricante.

9.4.1. As camadas do modelo OSI

Há diversos níveis em que a comunicação pode ocorrer dentro de uma rede e, por essa razão, uma estrutura básica foi estabelecida pela ISO com o intuito de classificar os processos de troca de informações. Tal estrutura é o que se chama formalmente de Modelo de Referência para Interconexão de Sistemas Abertos, mais conhecida como modelo OSI.

O modelo OSI visa oferecer uma comunicação estruturada para promover o desenvolvimento dos diferentes tipos de rede. Sendo assim, esse modelo define uma sequência de processos necessária para que seja possível transmitir mensagens entre aplicações executadas em diversos sistemas da rede.

Aqui, o termo sistema engloba todos os elementos envolvidos, desde o software até o meio utilizado para processar e transferir os dados. Tendo esse conceito de sistema como referência, o modelo OSI pode ser utilizado para definir qualquer tipo de rede. Veja, a seguir, a definição de cada uma das camadas do modelo de referência OSI:



9.1. Modelo OSI

9.4.2. Definição das camadas

O modelo de referência OSI está dividido em camadas, que têm por finalidade organizar o processo de interoperabilidade entre os sistemas. Essa divisão se dá por sete camadas: Aplicação, Apresentação, Sessão, Transporte, Rede, Enlace e Física. Essas camadas são relacionadas de forma vertical, onde cada uma delas tem uma função nessa estrutura de comunicação e serviços que oferecem à rede.

Todas elas possuem duas denominações: uma por nome e outra por número. Vejamos quais são essas camadas e os serviços oferecidos por cada uma delas:

- **Camada 7 (Camada de Aplicação):** Os serviços desta camada permitem que as aplicações (idênticas ou não) executadas em sistemas diferentes utilizem a rede para a troca de mensagens. Encontram-se nesta camada serviços como a transferência de arquivos, a manipulação de mensagens e o gerenciamento remoto;

Conceitos e Infraestrutura de Redes (online)

178

- **Camada 6 (Camada de Apresentação):** Esta camada oferece diversas formas de conversão de dados, negociando e estabelecendo uma representação comum para todos eles. Isso inclui a tradução do código de caractere, a compressão dos dados e a criptografia da mensagem;
- **Camada 5 (Camada de Sessão):** São agrupados nesta camada os serviços que sincronizam e gerenciam a transferência de dados na rede. Sendo assim, um protocolo desta camada tem o poder de determinar, por exemplo, que um dispositivo interrompa o processo de transferência;
- **Camada 4 (Camada de Transporte):** Por meio dos serviços desta camada, é possível atribuir níveis de qualidade para a transferência de dados. Com isso, no momento em que os dispositivos estabelecem uma conexão, é possível utilizar o protocolo desta camada para selecionar um tipo específico de serviço. Além disso, a camada 4 permite monitorar a transferência para fins de faturamento, manter a qualidade de serviço mais adequada e emitir um alerta caso haja a suspeita de que tal qualidade esteja em risco;
- **Camada 3 (Camada de Rede):** Os serviços da Camada 3 têm como função realizar a transferência de dados de redes interligadas. Caso haja diversos roteadores entre as redes, um protocolo desta camada pode ser utilizado para escolher qual deles é o mais adequado para realizar a transferência. Essa escolha envolve diversos fatores, tais como o congestionamento dos roteadores, a prioridade da mensagem etc.;
- **Camada 2 (Camada de Ligação de Dados):** Os serviços desta camada têm por objetivo realizar a transferência de dados sobre uma conexão física de maneira confiável dentro de uma rede local. Os protocolos da Camada 2 podem ser utilizados para identificar dispositivos e gerenciar o acesso ao canal de transmissão compartilhado, provendo funções e regras que permitam ativar, manter, detectar e controlar erros e, ao final do processo, desativar um enlace físico;

- Camada 1 (Camada Física):** Uma das responsabilidades desta camada é realizar a transmissão dos bits através de um canal de comunicação que interconecte dois ou mais ativos de redes, definindo os métodos, sejam eles eletrônicos ou não. Assim, os serviços que pertencem a esta camada têm a função de transmitir bits por diversos meios, sendo que o modelo OSI não especifica se os meios devem ser cabeados ou wireless. O modelo de sete camadas OSI permite criar um mapeamento de referências em relação aos serviços de interconexão de rede, como exibido na figura a seguir:

As sete camadas do modelo OSI como referência

Camada 7 Aplicação	Camada 6 Apresentação	Camada 5 Sessão	Camada 4 Transporte	Camada 3 Rede	Camada 2 Enlace	Camada 1 Física
Correio eletronico	POP/SMTP	110/25	TCP	IP v4 IP v6		RS X, CAT 1 ISDN ADSL ATM
Grupo de noticias	Usenet	532				
Aplicativos da Web	HTTP	80			SLIP/PPP	
Transferencia de arquivos	FTP	20/21			SNAP 802.2	
Sessões de hosts	Telnet	25	UDP		Ethernet II	FDDI CAT 1 - 6 Cabos Coaxiais
Serviços de Diretorio	DNS	53				
Gerenciamento de rede	SNMP	161/162				
Serviços de arquivos	NTS	RCP Maper				

9.2. Modelo OSI e suas sete camadas

A estrutura do modelo OSI funciona da seguinte forma: cada camada oferece serviços para as camadas que estão acima, de forma que as camadas superiores não tomam conhecimento dos procedimentos necessários para a implementação dos serviços oferecidos pelas camadas inferiores.

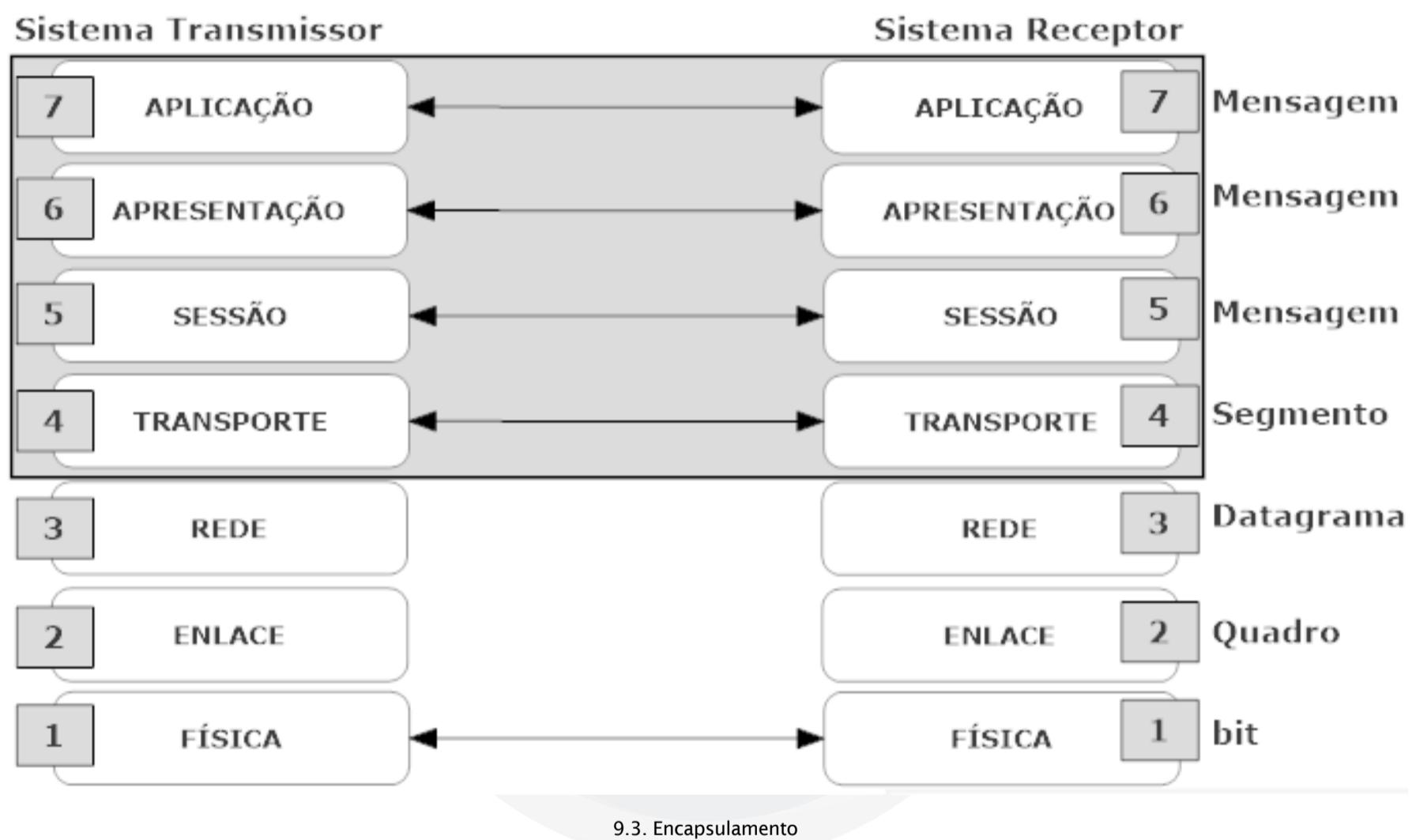
É possível fazer alterações em uma camada sem que seja necessário aplicá-las às demais, mas, para isso, as entradas e saídas da camada modificada devem permanecer as mesmas. Com isso, pode-se tirar proveito de novas tecnologias dentro de uma camada específica sem prejuízos para o restante da rede ou para outras redes.

A conexão entre as camadas é normalmente descrita de forma vertical, razão pela qual recebe o nome de pilha de protocolo. Essa pilha especifica como será a interação entre software e hardware em diversos níveis para possibilitar aos dispositivos de uma LAN, ou de diferentes LANs interligadas, a transmissão de suas mensagens.

Conceitos e Infraestrutura de Redes (online)

180

Durante o processo de comunicação entre dois sistemas, cada camada tem a responsabilidade de fornecer serviços para a camada imediatamente ligada a ela, seja superior ou inferior. Assim, enquanto os dois sistemas transferem informações, um circuito virtual é estabelecido e cada uma das camadas cria circuitos virtuais para manter comunicação direta com sua camada par no outro computador. Em cada etapa do processo de transmissão de dados, ao transferir entre as camadas, o pacote recebe um nome diferente em função da camada de origem, que passa pelo processo conhecido como encapsulamento dos dados, como vemos na figura a seguir:



As pilhas de protocolo possuem algumas características. Como já vimos anteriormente, cada camada do modelo OSI oferece um conjunto de serviços específicos para as camadas que se encontram acima. Tais serviços, assim como a pilha em si, são definidos pelos protocolos. Além disso, as camadas são conectadas por pontos denominados SAPs (Service Access Points), onde cada uma possui uma interconexão com outra camada.

Quando é necessário transferir uma mensagem entre dois sistemas, é possível estabelecer uma relação ponto a ponto entre as camadas correspondentes na pilha de protocolo de cada sistema, promovendo, assim, a comunicação através da rede. Essa transmissão funciona da seguinte forma: a mensagem vai passando da camada em que está para as camadas inferiores até atingir a Camada 1 da pilha. A partir daí, ela é enviada para a Camada 1 da pilha de destino, de onde é transmitida para as camadas superiores até atingir a camada correspondente àquela de onde foi enviada.

9.5. Protocolos para conexões à distância

Para estabelecer conexões ponto a ponto entre computadores e servidores de acesso remoto, é necessária a utilização de protocolos para que seja efetuado o enquadramento, o controle de erros e outras funções da camada de enlace. A seguir serão apresentados os protocolos principais.

9.5.1. PPP

O PPP (Point-to-Point Protocol) é um protocolo de enlace de dados para conexões ponto a ponto, usando linhas seriais ou discadas. Comumente utilizado para transmitir pacotes IP na Internet, o PPP padronizou o método de envio de dados em conexões ponto a ponto, permitindo assim o acesso a qualquer servidor que utilize um método compatível.

9.5.2. Protocolos VPN

As VPNs (Virtual Private Network) permitem que, entre usuários remotos e redes corporativas, sejam transferidas informações de maneira segura. As VPNs são os túneis de criptografia que permitem essa transferência segura.

A implementação das redes corporativas é feita com o uso de uma rede pública – como a Internet – em detrimento de linhas privativas. As redes públicas e/ou privadas criam pontos autorizados entre os quais as VPNs promovem a transmissão.

Para compreender melhor as VPNs é preciso entender o tunelamento, pois essa tecnologia é tomada como base para as redes virtuais privadas. No tunelamento, um protocolo é encapsulado dentro de outro. A tecnologia de tunelamento aplicada às VPNs não requer que o protocolo dos pacotes que serão encapsulados e o protocolo dos pacotes nos quais aqueles serão encapsulados sejam iguais; eles podem ser protocolos diferentes. Assim, pacotes de protocolo TCP/IP, por exemplo, podem encapsular e transportar pacotes de protocolo IPX.

Ao usarmos o tunelamento nas VPNs, temos o seguinte procedimento:

1. O pacote é criptografado para que mesmo com uma possível interceptação do pacote ele não possa ser lido;
2. O pacote é encapsulado;
3. O pacote navega pela Internet em direção ao seu destino, sendo que está então criptografado e encapsulado;
4. O pacote retorna ao seu formato original, isto é, ele sofre um processo de desencapsulação e descriptografia assim que chega ao seu destino.

9.5.2.1. Tunelamento Camada 2 - Enlace

Nesse tipo de tunelamento, os quadros funcionam como unidade de troca. Os protocolos encapsulam os pacotes da Camada 3, dos quais o IP e o IPX são exemplos, em quadros PPP, tendo por finalidade o transporte desses protocolos na Internet.

Alguns desses protocolos são descritos na tabela a seguir:

Protocolo	Fabricante	Descrição
PPTP (Point-to-Point Tunneling Protocol)	Microsoft	A criptografia e o encapsulamento dos tráfegos IP, IPX e NetBEUI são permitidos para que estes sejam enviados.
L2TP (Layer 2 Tunneling Protocol)	IETF (Internet Engineering Task Force)	Canais de comunicação de datagrama ponto a ponto (IP, X25, Frame Relay ou ATM, por exemplo) são usados como meio para o envio dos tráfegos IP, IPX e NetBEUI - que também são criptografados.
L2F (Layer 2 Forwarding)	Cisco	Usado para VPNs discadas.

9.5.2.2. Tunelamento Camada 3 - Rede

Antes de sua transmissão, os pacotes IP privados passam por procedimentos, realizados pelo IPSec da IETF, que visam sua proteção (criptografia, autenticação e integridade, por exemplo), e então são encapsulados em outros pacotes IP.

No caso de tunelamento na camada de rede, antes que os pacotes IP sejam enviados na rede, eles são encapsulados com um cabeçalho adicional do mesmo protocolo.

9.5.2.3. MPLS

Com o protocolo de roteamento MPLS (Multiprotocol Label Switching), cada VPN tem tabelas exclusivas, possibilitando que o tráfego seja completamente isolado. Ele baseia-se em pacotes rotulados, também chamados de labels. O índice na tabela de roteamento do próximo roteador é representado por um rótulo.

O tráfego entre os pontos da VPN é beneficiado na medida em que o QoS (Quality of Service) pode ser realizado, dando prioridade às aplicações críticas. Com ele, o tráfego de voz e de vídeo é permitido, e os recursos da rede encontram melhores condições de utilização.



Teste seus conhecimentos Protocolos de rede 9

1. Quais características tornam o TCP/IP uma das pilhas de protocolo mais utilizada?

- a) Ser proprietário e não roteável.
- b) Ser aberto e não roteável.
- c) Ser aberto e roteável.
- d) Ser proprietário e roteável.
- e) Todas as alternativas anteriores estão corretas.

2. Qual recurso é citado na seguinte afirmação: prioriza o tráfego de determinadas aplicações, tais como voz e vídeo?

- a) IPSec
- b) L2TP
- c) PPTP
- d) QoS
- e) MPLS

3. Dos itens abaixo, qual representa um protocolo de VPN do tipo tunelamento Camada 2?

- a) IPSec
- b) PPP
- c) L2F
- d) TCP
- e) MPLS

4. É possível trocar dados entre dispositivos com protocolos diferentes entre duas LANs?

- a) Sim, desde que sejam protocolos abertos.
- b) Não, pois necessitam de uma comunicação ponto a ponto.
- c) Sim, desde que exista um Gateway para conversão.
- d) Sim, desde que sejam protocolos proprietários.
- e) Não, para haver troca de informação os dispositivos devem possuir o mesmo protocolo.

Conceitos e Infraestrutura de Redes (online)

186

5. Considere a seguinte afirmação: esse tipo de protocolo define os preceitos para que haja comunicação apenas em um ambiente da rede. Qual tipo de protocolo está sendo citado?

- a) Protocolo de rede
- b) Protocolo aberto
- c) Protocolo proprietário
- d) Protocolo VPN
- e) Protocolo de transporte

6. Em qual camada do modelo OSI operam os roteadores?

- a) Camada 3
- b) Camada 2
- c) Camada 4
- d) Camada 1
- e) Camada 5

7. Quando há necessidade de promover a interconexão entre LANs utilizando a camada de rede do modelo OSI, obrigatoriamente, qual equipamento deve ser instalado em cada segmento?

- a) Switch
- b) Ponte
- c) Conversor de mídia
- d) Roteador
- e) Nenhuma das alternativas anteriores está correta.

8. Quais itens a seguir apresentam em sua totalidade os dispositivos de rede pertencentes à camada 2 do modelo OSI?

- a) Placa de rede, hub e switch.
- b) Hub, switch e ponte.
- c) Placa de rede, switch e roteador.
- d) Placa de rede, hub e ponte.
- e) Placa de rede, ponte e switch.

Conceitos básicos de TCP/IP 10

- ✓ Camadas do protocolo TCP/IP;
- ✓ Análise do endereço IP.

10.1. Introdução

Entendemos por protocolo TCP/IP (Transmission Control Protocol/Internet Protocol) um agregado formado por uma série de protocolos utilizados para a comunicação em redes de grandes proporções.

O TCP/IP é dividido em quatro camadas, dentro das quais estão localizados os diferentes protocolos que o compõem. Tal método tende a maximizar a agilidade no que diz respeito à comunicação. Esses protocolos possuem responsabilidades distintas, e as transações na rede somente poderão ser efetuadas com sucesso quando todos cumprirem seu papel de modo satisfatório.

10.2. Camadas do protocolo TCP/IP

Como já dissemos, o TCP/IP é composto por quatro camadas, nas quais estão dispostos todos os outros protocolos. Vejamos a tabela a seguir:

Camada	Exemplos de protocolo
Aplicação	HTTP FTP
Transporte	TCP UDP
Internet	IP ARP ICMP IGMP
Interface de Rede	ATM Ethernet Token Ring Frame Relay

Nos subtópicos a seguir, conferiremos uma descrição das camadas TCP/IP e dos seus principais protocolos.

10.2.1.Camada de aplicação

Esta camada, que está no nível mais alto, é responsável por alocar utilitários e aplicativos que, por meio dela, comunicam-se com a rede.

Há dois protocolos importantes na camada de aplicação:

- **HTTP**

Por meio do Hyper Text Transfer Protocol, ou protocolo de transferência de hipertexto, é que obtemos acesso aos sites da Internet.

- **FTP**

Por meio deste protocolo, File Transfer Protocol, ou protocolo de transferência de arquivo, como o próprio nome sugere, podemos proceder com a transferência de arquivos por meio da Internet.

10.2.2.Camada de transporte

Esta camada possui três funções distintas: a primeira delas é definir, por meio de um identificador, os dados sendo transmitidos; a segunda é agir como intermediária entre as camadas da Internet e de aplicação, no que se refere ao envio de dados; a terceira e última é proceder com o gerenciamento das transmissões de dados, assegurando-se de que elas ocorram de maneira satisfatória. Há dois protocolos na camada de transporte que merecem destaque:

- **TCP**

A função deste protocolo é solicitar que o recebimento dos dados seja confirmado, uma vez que eles tiverem alcançado o seu destino. É um protocolo confiável e orientado à conexão, a qual é estabelecida por dois computadores utilizando o processo handshake de três vias, que envolve as seguintes etapas:

1. Inicialização e transmissão de dados pelo computador de origem;
2. Resposta com informações de conexão pelo computador de destino;
3. Confirmação e aceitação do recebimento pelo computador de origem.

- **UDP**

Este protocolo agiliza o processo de envio dos dados por meio da entrega de pacotes sem conexão. Apesar de ser rápido, não é confiável, pois não existe a confirmação dos pacotes recebidos e nem a retransmissão de dados perdidos. Por isso, este protocolo é utilizado para a transmissão de dados em que a perda de alguns pacotes não será um problema.

10.2.3. Camada da Internet

Quando se tornar necessário proceder com o envio de dados por meio de uma rede, eles precisam ser roteados, endereçados e empacotados. Tais ações são realizadas na camada da Internet, cujos protocolos mais importantes serão detalhados a seguir:

- **IP**

Se for necessário o envio de pacotes de dados por meio de uma rede, é preciso proceder com o endereçamento desses dados. Em seguida, é necessário proceder com o roteamento deles. Nesse caso, temos de recorrer ao protocolo denominado Internet Protocol, mais conhecido como IP.

O IP é um protocolo sem conexão e não confiável que, para ser efetivamente utilizado com o intuito de direcionar os pacotes de dados ao seu destino, precisa que todos os pacotes enviados contenham, em seu interior, tanto o endereço IP do computador remetente quanto o do destinatário. Enquanto um pacote de dados estiver sendo enviado pela rede, podemos nos deparar com duas situações distintas: na primeira, remetente e destinatário encontram-se em segmentos de rede distintos. Desse modo, o envio do pacote de dados é realizado com o auxílio de um roteador. A segunda situação é oposta à primeira, ou seja, o remetente e o destinatário encontram-se em um único segmento de rede. Sendo assim, o envio do pacote de dados é realizado de forma mais direta.

Outra responsabilidade do IP é determinar o tempo de vida (TTL) dos pacotes, para que estes não trafeguem na rede indefinidamente.

- **ARP**

Antes que um pacote de dados possa ser enviado por meio de uma rede, é preciso que o protocolo ARP faça um mapeamento dos endereços IP (endereços lógicos) alocados nesse pacote para endereços MAC (endereços físicos). Esse procedimento recebe o nome de resolução de endereços.

Para que o mapeamento citado possa ser realizado, existe uma tabela alocada em uma área de memória, denominada cache ARP, que contém os endereços MAC correspondentes aos endereços IP das máquinas existentes em um mesmo segmento de rede.

Por meio desse mapeamento é que os adaptadores de rede farão a identificação do destino de um pacote, processando as seguintes etapas:

1. No computador de origem, o cache do ARP é verificado;
2. Caso não seja encontrado o endereço MAC no cache, uma solicitação do **ARP** é enviada pelo segmento por meio de uma transmissão por difusão, a fim de encontrar o computador de destino;
3. Identificado o computador de destino, a entrada do **ARP** é adicionada a ele, contendo o seu endereço;
4. O computador de destino envia uma solicitação do **ARP**;
5. A entrada do **ARP** é adicionada ao computador de origem;
6. Feita a verificação, o pacote **IP** é enviado.

- **ICMP (Internet Control Message Protocol)**

A função deste protocolo é enviar mensagens ao computador remetente caso ocorra alguma falha no momento em que um pacote de dados estiver sendo enviado através de uma rede. Por meio de tais mensagens, podemos analisar os erros ocorridos, bem como utilizar as informações retornadas para solucionar eventuais problemas.

- **IGMP (Internet Group Management Protocol)**

Antes de falarmos sobre o protocolo IGMP, é interessante discorrermos sobre o conceito de difusão seletiva IP. Quando é necessário que uma mensagem qualquer seja enviada a mais de um destinatário simultaneamente, utilizamos a difusão seletiva IP. Esses usuários formam um conjunto ou grupo para o qual um pacote de dados é enviado utilizando-se um endereço IP de difusão seletiva.

Os destinatários de diferentes grupos como esse, conhecidos como grupos de difusão seletiva, são alocados em listas. A função do protocolo IGMP é administrar essas listas.

10.2.4.Camada de interface de rede

Por meio desta camada, podemos obter acesso físico ao ambiente de rede. Dois protocolos presentes nesta camada são o ATM (modo de transferência assíncrona) e o Ethernet. O adaptador de rede é um exemplo de componente de hardware encontrado na camada de rede.

10.3.Analisando o endereço IP

Podemos definir como endereço IP um número de identificação responsável por assegurar a individualidade de identificação de um micro na rede. Esse tipo de endereço deve ser composto por quatro números, entre 0 e 255, dispostos da seguinte maneira: xxx.xxx.xxx.xxx.

Os endereços IP são organizados em classes com o intuito de determinar o local de um host de destino em relação ao computador de origem. Um host remete a qualquer dispositivo em uma rede TCP/IP (como micros, impressoras e roteadores) que utilize o endereçamento IP como meio de transmissão e recepção de informações.

É possível atribuir endereços IP a todos os computadores conectados à rede por meio da sua divisão em sub-redes.

É preciso destacar que alguns endereços IP possuem funções especiais e, por isso, não podem ser utilizados como endereços de host. São eles:

- **Endereço com todos os bits destinados à identificação da máquina iguais a 0:** Representa o endereço da rede. Por exemplo: 192.168.1.0;
- **Endereço com todos os bits destinados à identificação da máquina iguais a 1:** Representa o endereço de broadcast. Por exemplo: 192.168.1.255;
- **Endereços da rede 127.0.0.0:** Usados como alias que faz referência à própria máquina. O endereço 127.0.0.1, associado ao nome do host local, é normalmente utilizado.

10.3.1.Classes de endereço

As identificações de rede são atribuídas com a utilização das classes de endereço. Esse processo é feito com o objetivo de permitir que computadores conectados nas diferentes redes de uma empresa possam estabelecer uma comunicação com a Internet.

Uma classe de endereço é determinada de acordo com a estrutura de um endereço IP. Este, como já vimos, possui quatro segmentos numéricos cujos valores variam entre 0 e 255. O valor do byte do endereço IP irá definir a sua classe, conforme o intervalo de valores ao qual se enquadra. Vejamos a tabela a seguir:

Intervalo	Classe
1 - 126	A
128 - 191	B
192 - 223	C
224 - 239	D
240 - 255	E

Estão descritas, nos subtópicos adiante, as diferentes classes de identificação de rede com as suas respectivas características.

Para calcular a quantidade de redes possível em uma classe e a quantidade de hosts possível em cada rede, aplicamos a fórmula $2^n - 2$, em que n equivale à quantidade de bits que podem ser alterados.

- **Classe A**
 - Em redes que possuem uma grande quantidade de hosts, são atribuídos endereços de Classe A;
 - Possibilita a existência de 126 redes;
 - Cada rede pode possuir 16.777.214 hosts.



Para identificação de rede, é utilizado o primeiro byte menos o primeiro bit. Os outros três bytes são utilizados para identificação do host.

- **Classe B**

- Em redes médias e pequenas, são atribuídos endereços de Classe B;
- Possibilita a existência de 16.382 redes;
- Cada rede pode possuir 65.534 hosts.



Para identificação de rede, são utilizados os dois primeiros bytes menos os dois primeiros bits. Os outros dois bytes são utilizados para identificação do host.

- **Classe C**

- Em pequenas LANs, são atribuídos endereços de Classe C;
- Possibilita a existência de, aproximadamente, 2.097.150 redes;
- Cada rede pode possuir 254 hosts.



Para identificação de rede, são utilizados os três primeiros bytes menos os três primeiros bits. O outro byte é utilizado para identificação do host.

- **Classes D e E**

- Ambas as classes não se destinam a hosts;
- A classe D tem os seus endereços utilizados para multicast;
- A classe E tem os seus endereços reservados para uma futura utilização.

10.3.2. Sub-redes

É possível evitar o aumento da colisão de dados e a redução do desempenho de uma rede baseada na tecnologia Ethernet, em caso de alto número de computadores e grande volume de tráfego. Basta que os computadores dessa rede sejam agrupados em segmentos separados por um dispositivo físico, como um roteador ou uma ponte.

Os segmentos de uma rede TCP/IP são conhecidos como sub-redes e encontram-se separados por roteadores. Em uma sub-rede, todos os endereços IP dos computadores são portadores da mesma identificação de rede. Por outro lado, para que as sub-redes se comuniquem, cada uma deve possuir uma identificação de rede distinta. A identificação de rede permite, então, que as sub-redes especifiquem as divisões lógicas de uma rede.

10.3.2.1. Máscaras de sub-rede

Vimos que uma rede única pode ser segmentada em sub-redes, cada qual com uma identificação de rede diferente, ou seja, com uma identificação de sub-rede. Essa divisão de uma única identificação de rede em identificações de rede menores é realizada via máscara de sub-rede.

Definimos como máscara de sub-rede um recurso que distingue, em um endereço IP, a identificação de rede de uma identificação de host. Essa máscara é representada por um conjunto de quatro números, organizados segundo valores máximos contíguos seguidos por valores mínimos contíguos. Nesse sentido, cada um dos quatro números pode considerar um valor máximo de 255 ou mínimo de 0. Os valores máximos remeterão à identificação de rede, enquanto os mínimos, à identificação de host.

Podemos definir dois tipos de máscaras de sub-rede: o padrão e o personalizado. O primeiro tipo é comum às classes de endereços IP. Sua configuração se dá da seguinte maneira:

Classe de endereço IP	Endereço IP	Máscara de sub-rede	Identificação de rede	Identificação de host
A	w.x.y.z	255.0.0.0	w.0.0.0	x.y.z
B	w.x.y.z	255.255.0.0	w.x.0.0	y.z
C	w.x.y.z	255.255.255.0	w.x.y.0	z

Já o segundo tipo, personalizado, é utilizado no caso de precisarmos dividir as redes em sub-redes sem adicionar equipamentos adicionais.

Conceitos e Infraestrutura de Redes (online)

198

Há três passos que devem ser seguidos para a definição de uma sub-rede:

1. Uma vez determinado o número de segmentos físicos necessários na rede local, é necessário converter esse valor para binário;
2. Conta-se, então, o número de bits necessários para representar o valor binário do número de segmentos físicos. Por exemplo: precisamos de quatro sub-redes. O valor binário de 4 é 100. Assim, para representar o valor 4 no sistema binário, são usados 3 bits;
3. Por fim, converte-se o número necessário de bits para decimal, no sentido da esquerda para a direita.

Por exemplo: em uma rede classe C, se forem necessários 5 bits, é preciso configurar os primeiros 5 bits (à esquerda) do Host ID como 1, passando a fazer parte do Network ID. O valor binário será, então, 1111 1000, o qual, no sistema decimal, equivale a 248. Nesse caso, a máscara de sub-rede será 255.255.225.248.

A seguir, temos as tabelas de conversões possíveis de máscaras de sub-rede para as classes A, B e C:

- **Classe A**

Número de sub-redes	Bits necessários	Máscara de sub-rede	Computadores por sub-rede
2	2	255.192.0.0	4.194.302
6	3	255.224.0.0	2.097.150
14	4	255.240.0.0	1.048.574
30	5	255.248.0.0	524.286
62	6	255.252.0.0	262.142
126	7	255.254.0.0	131.070
254	8	255.255.0.0	65.534

- **Classe B**

Número de sub-redes	Bits necessários	Máscara de sub-rede	Computadores por sub-rede
2	2	255.255.192.0	16.382
6	3	255.255.224.0	8.190
14	4	255.255.240.0	4.094
30	5	255.255.248.0	2.046
62	6	255.255.252.0	1.022
126	7	255.255.254.0	510
254	8	255.255.255.0	256

- **Classe C**

Número de sub-redes	Bits necessários	Máscara de sub-rede	Computadores por sub-rede
2	2	255.255.255.192	62
6	3	255.255.255.224	30
14	4	255.255.255.240	14
30	5	255.255.255.248	6
62	6	255.255.255.252	2

10.3.3. Atribuindo identificação de rede e de host

Um endereço IP é dividido em dois segmentos distintos: identificação de rede e identificação de host.

Um micro qualquer que faça parte de uma rede encontra-se alocado em um segmento de rede. Definir em que segmento esse micro está localizado é de responsabilidade da identificação de rede, sendo que esta é comum a todos os micros do segmento.

Além da identificação de rede, todos os micros ou outros componentes presentes em uma rede possuem uma identificação de host diferente. Jamais dois hosts em uma rede possuirão identificação de host igual.

10.3.4. Determinando host local ou remoto

Um host local é aquele cuja identificação de rede é similar à de outro host, ou seja, que se encontra na mesma sub-rede que o micro (host) com o qual está trocando informações. Um host remoto é aquele cuja identificação de rede difere da de outro host, ou seja, que se encontra em uma sub-rede diferente da do micro (host) com o qual está trocando informações.





Teste seus conhecimentos Conceitos básicos 10 de TCP/IP

1. Uma rede classe C com máscara padrão comporta quantos hosts?

- a) 16.534
- b) 254
- c) 2.097.150
- d) 02
- e) 121

2. A qual endereço de identificação da rede pertence o host 192.168.1.37 com máscara padrão?

- a) 192.168.0.0
- b) 192.168.0.1
- c) 192.168.1.255
- d) 192.168.1.0
- e) 192.168.0.255

3. Qual é a máscara padrão para um host com o IP 172.16.4.3?

- a) 255.0.0.0
- b) 255.255.0.0
- c) 255.255.255.0
- d) 0.255.0.0
- e) Nenhuma das alternativas anteriores está correta.

4. Qual é o protocolo responsável pelo gerenciamento do tempo de vida (TTL) dos pacotes nas redes?

- a) IGMP
- b) HTTP
- c) ICMP
- d) IP
- e) UDP

5. Qual classe de IP é destinada a multicast?

- a) Classe A
- b) Classe B
- c) Classe C
- d) Classe D
- e) Classe E

Conceitos básicos de IPv6 11

- ✓ Esgotamento do endereço IPv4;
- ✓ Protocolo IPv6;
- ✓ Endereçamento IPv6;
- ✓ Cabeçalho do protocolo IPv6;
- ✓ Coexistência dos protocolos IPv4 e IPv6;
- ✓ Distribuição dos blocos IPv6.

11.1. Introdução

Para entender a importância do IPv6, é necessário conhecer um pouco a história da Internet e analisar informações sobre o desenvolvimento do protocolo IP. Ainda, é importante entender quais foram os impactos causados pela forma de distribuição dos endereços IP devido ao rápido crescimento da Internet.

11.2. Esgotamento do endereço IPv4

Quando a Internet foi projetada, não se previa que a rede de computadores mundial viria a ser como é hoje. Ela foi projetada, inicialmente, para interligar centros de pesquisas com foco em estudos militares, mas, pelo potencial que apresentava, seu uso foi rapidamente adotado por universidades americanas. A partir da década de 1990, quando a Internet passou a ser utilizada comercialmente, seu crescimento foi acelerado. Nos dias atuais, falamos sobre a “Internet das Coisas”, cuja finalidade é facilitar a vida, colaborando e conectando pessoas, dispositivos eletroeletrônicos, eletrodomésticos, carros, possibilitando o rastreamento de transportes, casas, animais, enfim, de tudo em que se pode colocar uma etiqueta eletrônica. Estima-se que, nos próximos anos, 50 bilhões de coisas estarão conectadas à Internet.

O IPv6 (IP versão 6) representa a nova versão do protocolo de Internet. A iminente exaustão do espaço de endereços da versão anterior, o IPv4 (IP versão 4), fez surgir a necessidade de adotar a conversão de endereços de rede por meio do NAT (Network Address Translation), alternativa desenvolvida pela RFC 1631 (que foi definida em 1994 e ficou obsoleta em 2001 pela RFC 3022), que tinha a finalidade de oferecer técnicas para mapear vários endereços particulares para um único endereço IP público. Acreditava-se que o NAT pudesse ser a solução para o esgotamento do endereço IPv4. Havia, entretanto, limitações significativas que não seriam eliminadas a partir dessa proposta, principalmente em relação à segurança, pois a adoção do NAT cria uma quebra da conexão fim a fim, gerando a necessidade de intermediários para fechar as conexões, o que cria vulnerabilidades; além disso, esse mecanismo não possui escalabilidade, e o gerenciamento da tabela exige grande poder de processamento, bem como impossibilita a adoção de técnicas de segurança como a oferecida pelo IPSec (Internet Protocol Security).

Além do crescimento exponencial da Internet, vimos anteriormente como ocorreu a distribuição dos endereços IPs através das classes de endereço. Se houvesse a necessidade de endereçar 270 computadores, por exemplo, seria necessário utilizar uma classe B, gerando um grande desperdício de endereços. Outro fator que contribuiu com o desperdício de endereços foi

o método inicial adotado de distribuição de faixas classe A, com 16.777.216 milhões de endereços, de forma integral a grandes instituições como Xerox, HP, IBM, AT&T, Apple, MIT, Departamento de Defesa Americano, entre muitas outras.

O esgotamento do endereço IPv4 foi percebido e tornou-se necessária, então, sua substituição. Portanto, a partir da década de 1990, o IETF (Internet Engineering Task Force) passou a elaborar projetos para a nova versão do protocolo de Internet.

Como vimos, torna-se indispensável a adoção de uma solução definitiva a fim de apoiar o crescimento da rede, atendendo novos projetos de aplicações de Internet, o crescente número de usuários e regiões que estão sendo atendidas através de projetos de inclusão digital, novas redes corporativas que ainda surgirão etc. O protocolo IPv6 foi projetado para oferecer uma solução definitiva para essas questões, além de prover os avanços que veremos a seguir.

11.3. Protocolo IPv6

A partir da década de 1990, o IETF iniciou o desenvolvimento do novo protocolo, formalizado pela RFC 1550, criando uma versão que foi chamada de IPv5 e que ficou conhecida como IP Next Generation (IPng). O projeto deveria prever as seguintes necessidades:

- Distribuição adequada do endereço IP;
- Redução do tamanho das tabelas de roteamento;
- Simplificação da estrutura do protocolo para permitir processamento mais ágil;
- Suporte ao recurso de QoS;
- Suporte à mobilidade;
- Suporte a maior número de hosts na Internet;
- Segurança no nível do protocolo, com privacidade e autenticação;
- Interoperabilidade entre protocolos em ambas as versões;
- Facilidade do multicasting.

No entanto, a partir dos avanços do projeto do novo protocolo, foram estabelecidas novas RFCs com definições específicas sobre esses avanços. Uma delas foi a RFC 1883 (que foi definida em 1995 e ficou obsoleta em 1998 pela RFC 2460), que definiu regras e especificações do IPv6.

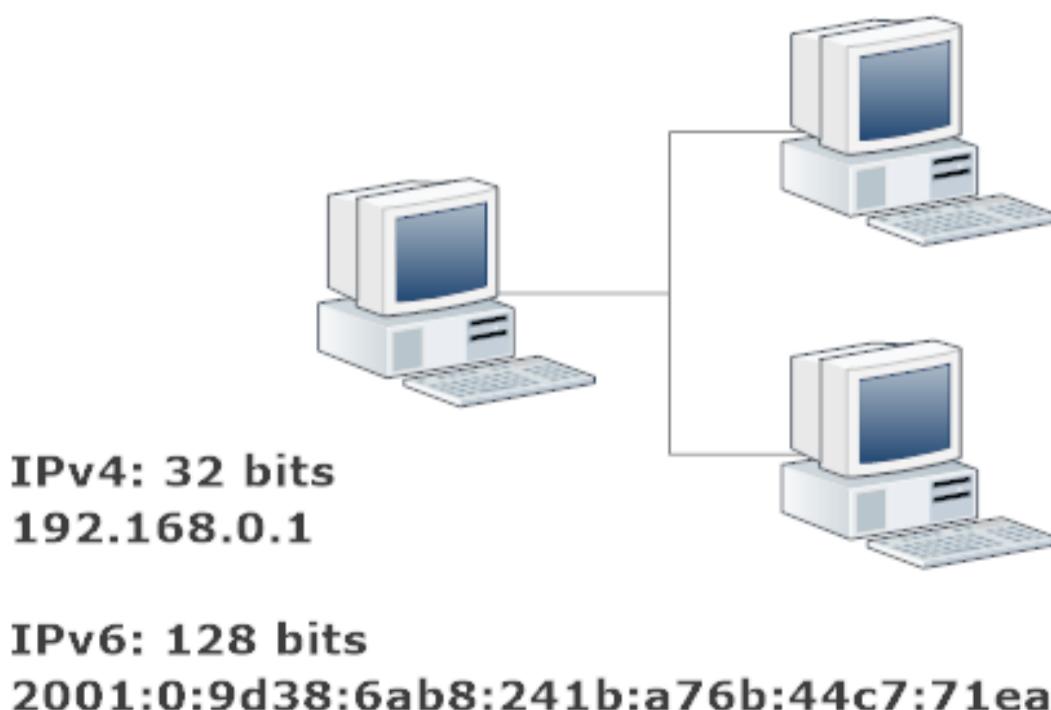
Com as alterações no protocolo IPv6, o espaço para endereços IPs foi elevado de forma significativa, garantindo-se, assim, alta disponibilidade com capacidade de crescimento e escalabilidade global. Veja duas implementações importantes:

- **Segurança:** O protocolo IPv6 oferece suporte obrigatório ao IPSec, sendo possível a ativação em todos os processos de comunicação, garantindo, assim, autenticidade, privacidade e integridade dos dados;
- **ICMP:** O protocolo ICMP foi alterado para oferecer mecanismos de autoconfiguração de endereços, com recurso de descoberta de vizinhança e gerenciamento de multicast.

11.3.1. Estrutura do Protocolo IPv6

Como vimos, o protocolo IPv6 (Internet Protocol version 6), substituto do IPv4, é uma evolução, e sua principal alteração é que nessa nova versão são utilizados endereços de 128 bits em vez de 32 bits. O IPv6 não é apenas uma atualização, é um novo protocolo.

O número de um endereço IPv6 é significativamente maior, com muito mais casas decimais do que o modelo anterior (IPv4), visando justamente evitar que uma nova substituição seja necessária no futuro.

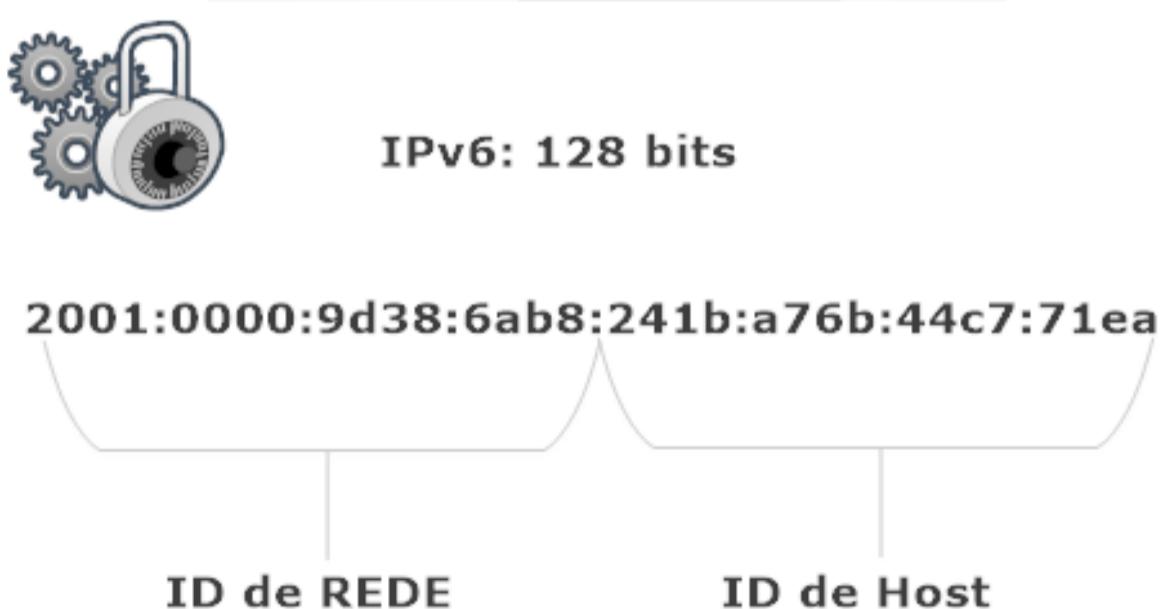


O endereçamento IPv4 é representado por um conjunto de quatro octetos separados por pontos (.), sendo w.x.y.z. Já a representação dos endereços IPv6 se dá por meio de 32 caracteres, que ficam ordenados em oito quartetos, cada um separado por dois pontos (:). Esses endereços, por serem mais extensos, são representados por meio de caracteres em conjunto hexadecimal. Em tal conjunto, cada caractere representa 4 bits, isto é, 16 combinações. Isso significa que, em um endereço IPv6, é possível utilizar os caracteres A, B, C, D, E e F, além de qualquer número de 0 a 9. Os caracteres A, B, C, D, E e F representam, respectivamente, os números 10, 11, 12, 13, 14 e 15.

A adoção da nova versão do protocolo IP elimina qualquer chance de esgotamento de endereços, pois ela possibilitará a disponibilidade de endereços IPs conforme a seguir: 340.282.366.92 0.938.463.463.374.607.431.768.211.456. Isso representa 79 trilhões de trilhões de vezes a quantidade que há disponível na versão IPv4.

11.4. Endereçamento IPv6

Os endereços IPv6 são divididos em dois blocos, tal qual o IPv4. Já vimos que, no total, há oito quartetos. Os quatro primeiros quartetos – que consistem na primeira parte de 64 bits – são responsáveis pela identificação da rede, ao passo que os quatro últimos quartetos – aqueles que representam a outra parte de 64 bits, totalizando os 128 bits do IPv6 – são aqueles que identificam o host, como mostra a figura a seguir.



11.2. Estrutura do IPv6

Conceitos e Infraestrutura de Redes (online)

210

IPv4	IPv6
O protocolo IPv4, com um cabeçalho de 32 bits, possibilita a criação de 4 bilhões de endereços IP diferentes para dispositivos na Internet.	O protocolo IPv6, com um cabeçalho de 128 bits, possibilita a criação de $3,4 \times 10^{38}$ endereços diferentes. Isso é equivalente a 56 octilhões de endereços por ser humano na Terra.
O endereço IPv4 é dividido em 4 grupos de 8 bits separados por pontos (.) e escritos com dígitos decimais.	O endereço IPv6 é dividido em 8 grupos de 16 bits, separados por dois pontos (:) e escritos com dígitos hexadecimais.

É importante ressaltar que os endereços IPv6 permitem que as letras no endereço sejam maiúsculas ou minúsculas, e podemos abreviá-los de várias formas, deixando-os extremamente compactos. Em cada quarteto, é possível omitir quaisquer zeros que estiverem à esquerda de um número. Assim, em vez de escrever o número 0675, por exemplo, pode-se simplesmente digitar 675. Se o número for 0000, basta deixar apenas 0 (omitindo os outros três à esquerda). Tudo isso não altera em nada o significado; os zeros à esquerda são apenas omitidos. Portanto, é comum se deparar com endereços IPv6 que tenham, em seus quartetos, apenas três, dois ou um dígito só.

Até mesmo sequências do número 0 podem ser omitidas em um endereço IPv6. Para isso, são utilizados dois pontos seguidos (::). Ao utilizar o endereço, o sistema sabe disso e, sem ter problemas, faz a conversão internamente.

Zeros contíguos podem ser abreviados apenas uma vez no mesmo endereço, para evitar que haja ambiguidades na representação dos endereços. Veja o exemplo a seguir:

Endereço IPv6: 2001:0000:0000:0058:0000:0000:0000:0320

Formatos de abreviação corretos:

Formato 1: 2001::58:0:0:0:320

Formato 2: 2001:0:0:58::320

Formato de abreviação errado:

2001::58::320

Existem duas possibilidades para configurarmos endereços em uma mesma rede. Podemos utilizar endereços sequenciais ou utilizar a atribuição automática de endereços no IPv6, que consiste em utilizar os endereços MAC das placas de rede para atribuir os endereços dos hosts.

Os endereços MAC, porém, contêm apenas 12 dígitos hexa, ao passo que, no IPv6, o trecho em que está identificado o host (a segunda metade, conforme vimos) contém 16 dígitos. Atualmente, uma extensão dos endereços MAC das placas de rede é estudada, contudo, enquanto não há algo definitivo, é possível converter endereços de 12 dígitos em endereços de 16 dígitos por meio de um método simples: acrescentar, entre o sexto e o sétimo dígito do endereço (no meio), os dígitos ffff, como no exemplo: **0018e7ffff4929cf**.

O endereço IPv6 ficará ainda mais extenso se adicionarmos o endereço da rede, pois, desta vez, há o acréscimo dos dígitos ffff.

Vale lembrar que os zeros sequenciais do endereço sempre podem ser omitidos por dois pontos seguidos (::). Assim, **2002:0:0:0:0:176.16.10.1** ficaria **2002::176.16.10.1**.

Nessa nova versão de protocolo IPv6, há três tipos de endereçamento em razão do novo espaço de endereços, que são o unicast, o multicast e o anycast. Vamos ver como é a estrutura de cada um desses tipos de endereços.

11.4.1. Unicast

O tipo de endereço unicast identifica somente uma interface, logo, um pacote enviado a um endereço unicast é entregue a uma interface apenas. No entanto, há tipos de endereços unicast, como veremos a seguir:

- **Global unicast:** Representa um endereço IP equivalente aos endereços IP públicos IPv4. É um endereço roteável e acessível na Internet IPv6;
- **Link-local:** Endereço atribuído de forma automática e válido apenas dentro do mesmo espaço de endereço; utiliza-se prefixo FE80::/64, e, com esse espaço de endereço, 64 bits são reservados para a identificação da interface de rede;
- **Unique-local:** Endereço globalmente único e utilizado apenas para comunicações locais; implantado dentro do mesmo enlace e não roteável para Internet. Endereço identificado pelo prefixo FC00::/7, sempre seguido de um ID global único de 40 bits, gerado de forma aleatória;
- **IPv4 mapeado em IPv6:** O endereço do tipo IPv4 mapeado em IPv6 possui um formato de implementação específico e é considerado um endereço especial, pois, geralmente, é utilizado para mapear um endereço IPv4 em um endereço IPv6 de 128 bits;

- **Loopback:** É representado pelo unicast 0:0:0:0:0:0:0:1 ou ::1. Esse endereço equivale ao endereço da versão IPv4 loopback 127.0.0.1. Bastante utilizado em testes internos, o endereço é usado para referenciar a própria máquina. Também é um endereço especial;
- **Unspecified:** É considerado um endereço especial e é representado pelo endereço 0:0:0:0:0:0:0:0 ou ::0. No endereço IPv4, equivale ao unspecified 0.0.0.0. Ele nunca deve ser atribuído, pois indica somente ausência de endereço, seja de forma automática ou dinâmica.

11.4.2. Multicast

Os endereços multicast são derivados do bloco FF00::/8. O octeto que segue o prefixo FF contém flags que determinam o tempo de vida do pacote, e um valor de 4 bits define o escopo do grupo multicast. Endereços multicast são utilizados para identificar grupos de interfaces, sendo que cada interface pode pertencer a mais de um grupo, e os pacotes são encaminhados para o grupo, logo, quem participa do grupo recebe os dados encaminhados.

 Na versão IPv6, o multicast assume várias funcionalidades, inclusive substituir a função de broadcast que havia na versão IPv4, cuja tarefa é encaminhar pacotes a todos os sistemas interligados na mesma rede. Para isso, utiliza o endereço de multicast chamado de All nodes on link FF02::1.

11.4.3. Anycast

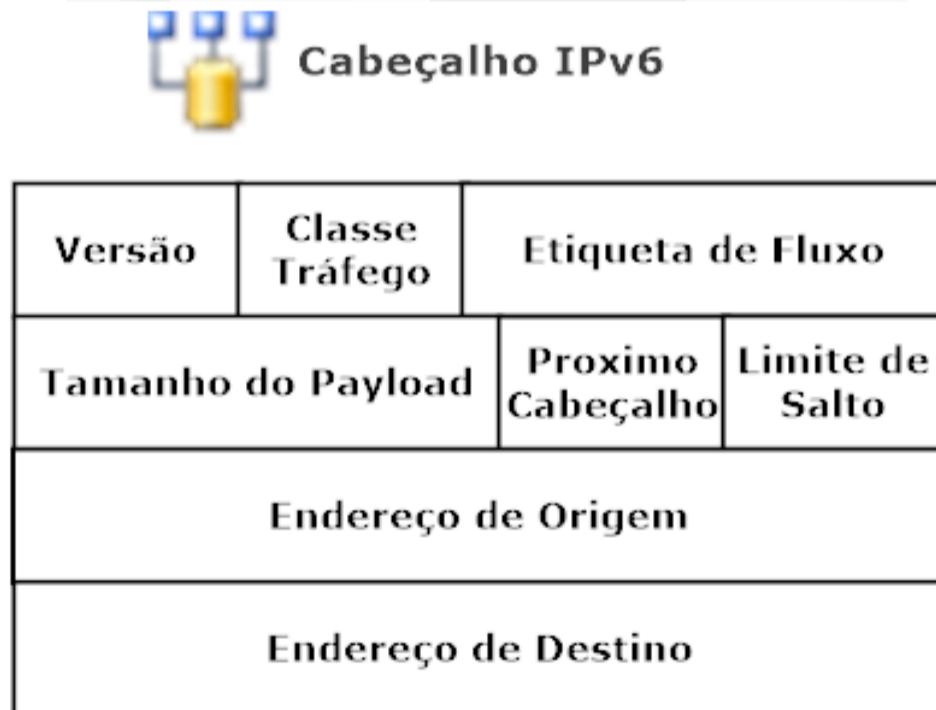
Endereços IPv6 do tipo anycast são utilizados para identificar um grupo de interfaces, e são atribuídos a partir da faixa de endereços unicast. Geralmente, não há diferenças sintáticas entre eles, portanto, quando atribuído a mais de uma interface, um endereço unicast transforma-se em um endereço anycast, devendo-se, nesse caso, configurar explicitamente os sistemas a fim de que saibam que um endereço anycast foi atribuído a eles. Além disso, esse endereço deve ser configurado nos roteadores como uma entrada separada (prefixo/128 - host route).

Devemos ressaltar que podemos atribuir múltiplos tipos de endereços em uma interface de rede. Vejamos:

- Tipo Global: 2001:....
- Tipo Unique Local: FC07:....
- Tipo Link Local: F800:....
- Tipo Loopback: ::1

11.5. Cabeçalho do protocolo IPv6

Uma das mudanças mais importantes em relação ao protocolo IPv6 está no cabeçalho. Nessa versão, o IETF conseguiu um grande avanço em relação à versão anterior. Embora o endereço IPv6 seja de 128 bits, quatro vezes maior que o IPv4, que é de 32 bits, seu cabeçalho é apenas duas vezes maior. Nessa versão, o cabeçalho ficou mais simplificado, o que trouxe mais velocidade e resultou em menor tempo para o processamento, sendo fundamental para redes de alta velocidade.



11.3. Cabeçalho do protocolo IPv6

Conceitos e Infraestrutura de Redes (online)

214

Cada um dos campos no cabeçalho IPv6 possui características específicas. Vamos apresentar cada um deles a seguir:

Nome do campo	Tamanho do campo	Descrição do campo
Versão	4 bits	Esse campo informa qual a versão do protocolo, que pode ser v4 ou v6. No caso, apresentamos apenas a versão 6.
Classe de tráfego	8 bits	Utilizado para identificar um pacote por classe de serviço ou por prioridade. Esse campo serve de base para o serviço de QoS, por exemplo.
Etiqueta de fluxo	20 bits	Adiciona tags de identificação aos pacotes. Esses dados são utilizados em conjunto com a Classe de tráfego para tratamento do pacote.
Tamanho dos dados (payload)	16 bits	Representa o tamanho em bytes dos dados encaminhados pelo protocolo IPv6 junto com o cabeçalho. Entretanto, o tamanho do cabeçalho de extensão também é somado nesse novo campo.
Próximo cabeçalho	8 bits	É responsável por identificar o tipo de cabeçalho que está sendo encaminhado, considerando o processo de transição ou de coexistência de versões.
Limite de salto	8 bits	Esse campo define a quantidade de roteadores pelos quais o pacote pode passar até que seja descartado. A cada nó que o pacote é encaminhado, é reduzido o número de saltos, o que reduz o tempo de vida de um pacote. Se o número de saltos chegar a zero, o pacote será descartado.
Endereço de origem	128 bits	Representa o endereço de origem do pacote.
Endereço de destino	128 bits	Representa o endereço de destino do pacote, no entanto, pode não ser o endereço final, em razão do processo de roteamento.

11.6. Coexistência dos protocolos IPv4 e IPv6

Embora a migração do protocolo IPv4 para o IPv6 seja muito importante, em razão do esgotamento do espaço de endereços, ainda é necessário que, por um tempo, ambas as versões de protocolos coexistam. Dessa forma, será necessário manter a interoperabilidade das versões para que o processo de transição ocorra com sucesso. Existem alguns mecanismos para manter a compatibilidade, como os recursos chamados de Pilha Dupla, Tradução e Tunelamento.

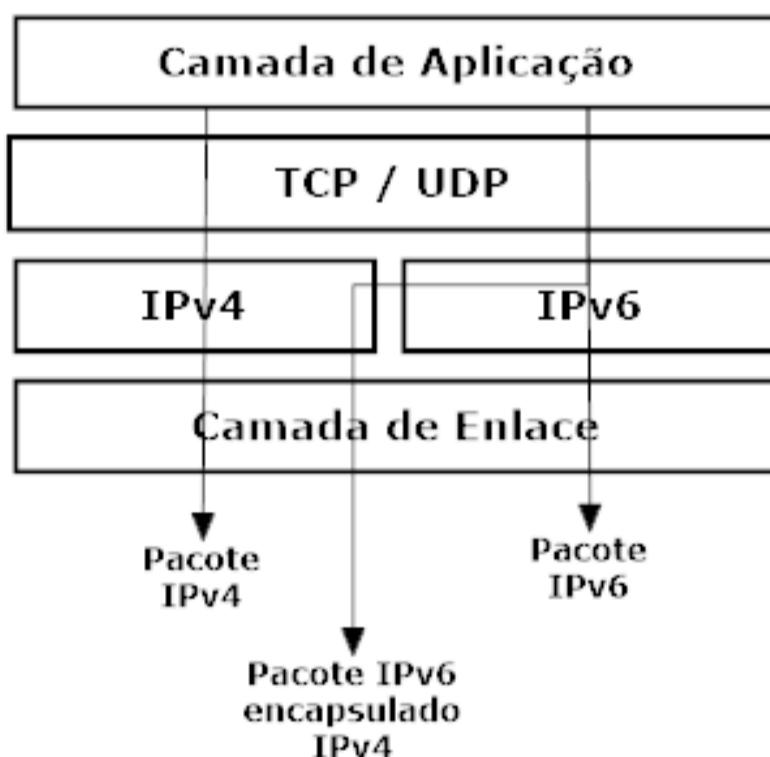
Uma das metas do IPv6 é estar compatível com ambientes que ainda utilizem o IPv4, uma vez que, em tais ambientes, existem sistemas que não são mais atualizados. Mas há computadores que possuem o IPv4 já configurado e vão migrar para o IPv6. Nesses, é possível adicionar um endereço IPv6 sem que haja queda na rede, de forma que o computador continue respondendo normalmente ao endereço IPv4 e, agora, também ao endereço IPv6.

Uma forma de manter a compatibilidade entre ambos os protocolos é um recurso oferecido pelo IPv6. Basta acrescentar **ffff:** antes do endereço IPv4 que atualmente estiver em utilização. Com isso, poderemos continuar utilizando os mesmos endereços ao migrar para o IPv6.

Vamos conhecer esses recursos disponíveis para a transição.

11.6.1. Pilha Dupla (Dual-Stack)

Esse mecanismo de coexistência chamado Dual-Stack oferece ao IPv6 suporte de interoperabilidade. Internamente, ele possui suporte das duas pilhas TCP/IP (IPv4 e IPv6). Com isso, durante o processo de roteamento e transferência de dados, o nodos TCP, com base na versão do protocolo, decide qual pilha processará o quadro de dados, ou seja, provê suporte a ambos os protocolos no mesmo dispositivo.



11.4. Pilha dupla - Dual-stack

Com o mecanismo Dual-Stack, o pacote de dados utiliza o mesmo endereço para encaminhamento em ambas as versões de protocolos, assim, mesmo que tenha sistemas já atualizados com IPv6, ele garantirá que se comuniquem com sistemas que tenham a versão do IPv4. Com esse mecanismo, sistemas que possuem apenas o protocolo IPv4 podem encaminhar pacotes para dual-stack que possuam IPv4; o mesmo caso para sistemas IPv6.

11.6.2. Tradução

Os mecanismos e técnicas de tradução tornam possível que o processo de roteamento seja transparente na comunicação entre dois sistemas que apresentem suporte apenas a uma versão do protocolo IP, ou até mesmo que utilizem pilha dupla. A grande vantagem desses mecanismos é que eles podem atuar em múltiplas camadas, realizando a tradução de cabeçalhos de protocolo na versão 4 para cabeçalhos na versão 6, e realizar o processo de tradução reverso. Também realiza o processo de tradução endereços de APIs de linguagens de programação, ou atuando na troca de tráfego dos protocolos TCP ou UDP.

11.6.3. Tunelamento

O mecanismo de tunelamento tem a finalidade de permitir a transmissão de pacotes IPv6 com parte de dados de um pacote IPv4, a fim de que dois sistemas possam comunicar-se por meio de uma rede que só suporte IPv4. Essa técnica tem sido amplamente utilizada a fim de facilitar o processo de transição e implantação do protocolo IPv6. Esse formato de utilização está definido pela RFC 4213, em razão da facilidade de adoção da nova versão. O tunelamento permite o tráfego de pacotes IPv6 em uma estrutura de rede existente IPv4, sem realizar nenhuma alteração no mecanismo de roteamento, pois ele realizará o encapsulamento de pacotes IPv6 em pacotes IPv4.

Isso vem a ser uma vantagem em situações nas quais, por exemplo, houver um grande êxodo do IPv4 para o IPv6, e o provedor de acesso oferecer suporte somente ao IPv4. Esse tipo de situação já é prevista pelo IPv6, o qual, por meio de redes IPv4, oferece suporte ao tunelamento de pacotes IPv6. Isso funciona da seguinte forma:

1. O roteador, antecipadamente, percebe a necessidade dos pacotes IPv6 passarem por uma rede IPv4;

2. Os pacotes IPv6, então, serão empacotados pelo roteador, que os coloca dentro de pacotes IPv4 para que possam ser roteados normalmente através da rede IPv4;



Vale ressaltar que o IPv6 possibilita que sistemas configurados com endereços IPv4, como máquinas executando o Windows 95 ou o Windows 98, por exemplo, continuem acessando a Internet, mesmo após essa migração descrita nos passos anteriores.

3. Um roteador IPv6 estaria do outro lado da conexão, com a função de remover o cabeçalho IPv4 dos pacotes, obtendo, assim, os pacotes IPv6 originais.

No processo de tunelamento, existem algumas técnicas para a criação do túnel de compatibilidade para o roteamento dos pacotes e, comumente, pode ser adotado um dos seguintes: 6to4, TunnelBroker, Teredo e ISATAP. Isso exigirá do administrador, no entanto, uma análise das diferenças entre os modelos.

11.7. Distribuição dos blocos IPv6

A distribuição dos blocos de endereços IPv6 é realizada de forma hierárquica e é coordenada da seguinte forma:

1. O instituto conhecido como IANA (Internet Assigned Numbers Authority) é uma organização sem fins lucrativos responsável pela coordenação global dos endereços IP, bem como pelos endereços liberados para roteamento na Internet. Ela define os critérios de como os endereços serão utilizados e distribuídos pelo Regional Internet Registry, conhecido apenas como RIR, responsável pelos Registros Regionais de Internet de cada parte do globo, como mostra a figura a seguir. Assim, o IANA entrega a cada RIR um bloco de endereços /12;

Conceitos e Infraestrutura de Redes (online)

218



RIRs	Área de Cobertura
ARIN	Região da América do Norte
AFRINIC	Região da África
RIPE NCC	Região da Europa, Ásia Central
APNIC	Região da Ásia/Pacífico
LACNIC	Região da América Latina e Caribe

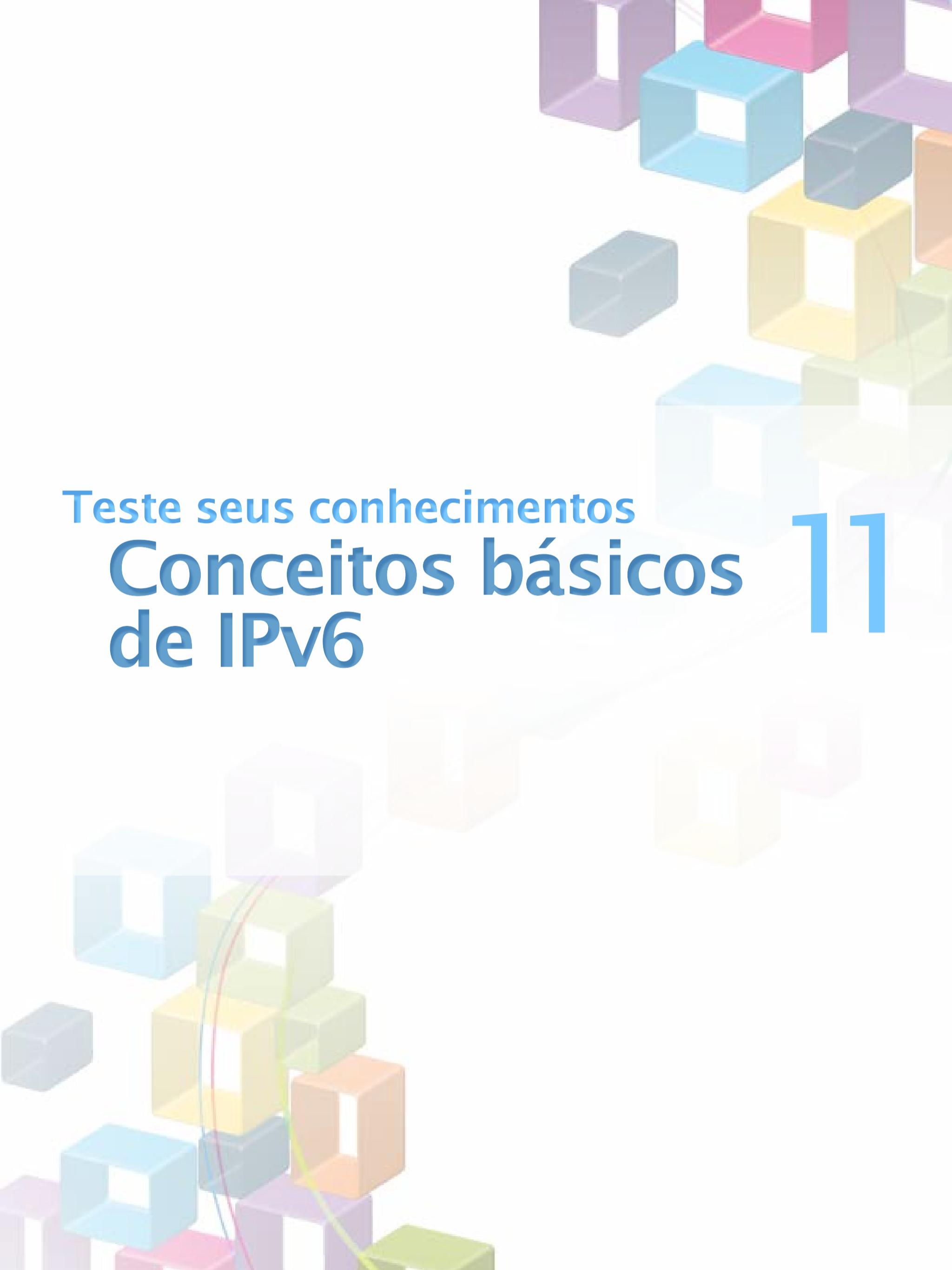
11.5. RIR – Regional Internet Registry

O formato de apresentação do endereçamento IP continua utilizando a Notação CIDR para identificação da Rede e Host.

2. Os RIRs são responsáveis por distribuir os blocos de endereços recebidos pelo IANA aos provedores de acesso à Internet de suas regiões. Embora o IANA tenha uma política global de distribuição e organização de endereços IPs, os RIRs têm certa autonomia para criar estratégias de distribuição de forma que seja mais eficiente em sua região de atuação. Os RIRs entregam aos provedores de acesso blocos de endereços IPs /32;

3. Os provedores de acesso à Internet também são conhecidos como ISPs. Eles são contratados para fornecer acesso à Internet aos usuários finais e devem entregar aos seus clientes blocos de endereços IPs /48 ou /56. Com esses blocos, os clientes podem ter respectivamente 65.536 ou 256 redes diferentes, cada uma delas com 18.446.744.073.709.551.616 endereços IPs diferentes. Já os usuários domésticos poderão receber um bloco /64.

Todas as distribuições de Linux atuais, bem como o Windows XP com SP2 e o Windows Vista, já dão suporte ao endereçamento IPv6.



Teste seus conhecimentos Conceitos básicos de IPv6 11

1. Qual campo no cabeçalho IPv6 é responsável por determinar por quantos roteadores os pacotes de dados serão encaminhados?

- a) Classe de tráfego
- b) Etiqueta de fluxo
- c) Versão
- d) Limite de salto
- e) Tamanho dos dados (payload)

2. Qual o tamanho do endereço com o protocolo IPv6?

- a) 192 bits
- b) 180 bits
- c) 32 bits
- d) 128 bits
- e) 129 bits

3. Como é representado um endereço IP com o protocolo IPv6?

- a) É representado por quatro octetos.
- b) É representado por dezesseis quartetos.
- c) É representado por oito octetos.
- d) É representado por dezesseis octetos.
- e) É representado por oito quartetos.

4. Quais são os tipos de endereços IPv6?

- a) Broadcast, multicast e unicast.
- b) Unicast, multicast e simplex.
- c) Unicast, broadcast, anycast.
- d) Multicast, unicast e anycast.
- e) Multicast, unique-local e global.

5. Em relação ao modo de distribuição dos endereços IP, qual é o RIR responsável pela organização na América Latina?

- a) ARIN
- b) AFRINIC
- c) APNIC
- d) LACNIC
- e) RIPE NCC

Convergência digital

12

- ✓ Streaming;
- ✓ VoIP (Voice over IP);
- ✓ IPTV e Web TV;
- ✓ CFTV.

12.1. Introdução

Desde a invenção do telégrafo, cada meio de comunicação necessita de uma infraestrutura, de uma rede adequada que permita sua difusão aos usuários. Atualmente, com a enorme migração das tecnologias para IP, faz-se necessário criar uma solução única de infraestrutura de transporte e distribuição de mídias e serviços. Há uma necessidade de convergência dos vários serviços para uma única conexão de rede.

No caso dos serviços de voz e imagem, é necessário que estes ocorram em tempo real. Para isso, deve ser considerada a qualidade de serviço (QoS - Quality of Service) em toda a rede.

Adiante, abordaremos algumas tecnologias importantes na convergência de redes.

12.2. Streaming

O método de distribuição de dados multimídia até os usuários é chamado de streaming. Essa tecnologia permite que usuários acessem dados em tempo real, sem a necessidade de aguardar um download completo.

Podemos considerar três classes de streaming:

- **Streaming armazenado:** Os dados são armazenados em servidores e, quando necessário, os clientes requisitam as informações;
- **Streaming em tempo real:** Os dados são transmitidos em tempo real pela rede;
- **Streaming interativo em tempo real:** Os dados são transmitidos em tempo real e há interatividade entre os dispositivos.

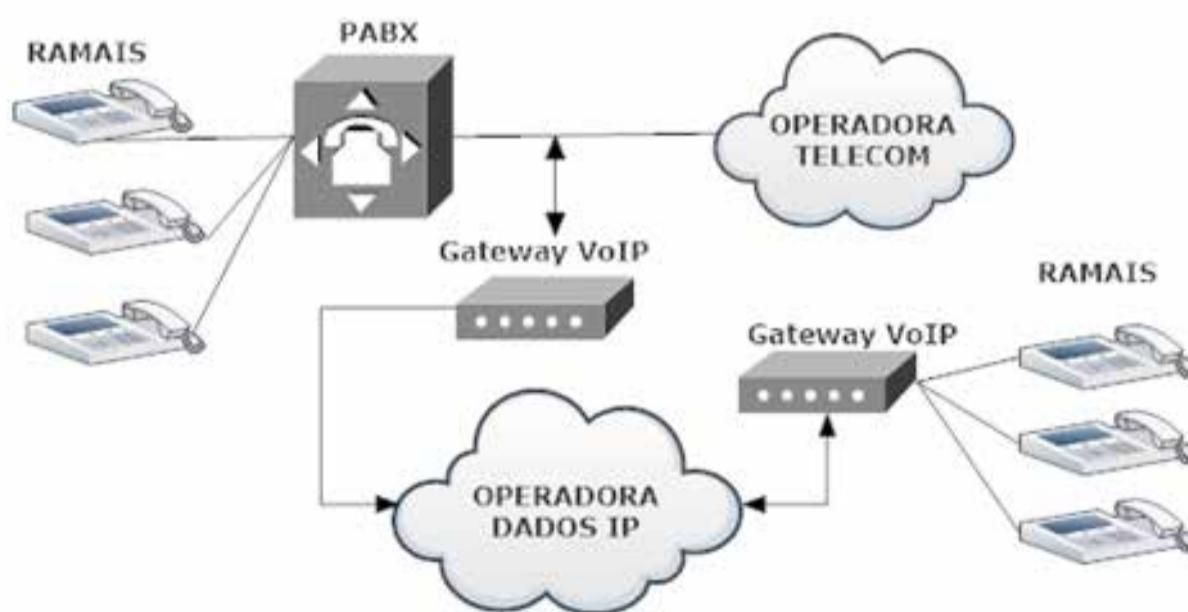
12.3. VoIP (Voice over IP)

Atualmente, a tecnologia VoIP (Voice over Internet Protocol) ocupa posição de destaque entre as tecnologias do setor de telecomunicações. Através dela, é possível efetuar comunicação de voz por meio da Internet ou de redes IP. A tecnologia VoIP consiste basicamente na conversão de sinais de voz em pacotes de dados, que são transmitidos, então, pela rede.

Entretanto, desde o advento da tecnologia ISDN, busca-se uma solução para realizar a transmissão de voz sobre canais de dados já existentes. Com a evolução da tecnologia VoIP para as NGNs (Next Generation Networks), houve a integração de dois mundos: a rede de dados IP e a telefonia. Com o uso da Internet, a ampla disponibilidade de canais de dados acabou criando uma infraestrutura que trouxe também a redução de custos como uma das grandes vantagens dessa integração.

Com a tecnologia VoIP, torna-se possível a realização de chamadas telefônicas por meio da internet, pois ela cria uma interconexão entre as redes de telefonia e de dados. Assim, é possível que usuários domésticos possam realizar ligações de baixo custo para telefones convencionais (tanto locais como internacionais) por meio de seu computador.

Além dos usuários domésticos, as empresas se beneficiam muito dessa tecnologia, pois, através de uma central telefônica interna (PABX – Private Automatic Branch Exchange), elas podem integrar seus sistemas de ramais telefônicos, permitindo assim que as ligações de sentido OUT (ou saída) sejam feitas por meio de canais de custo mais baixo, deixando o sistema de IN (ou entrada) para operadoras de telefonia, como mostra a figura a seguir. Além disso, mesmo com a possibilidade dessa integração (PABX com VoIP), muitas empresas estão deixando de ter gastos com centrais telefônicas, pois estão substituindo-as por servidores IP específicos para sistemas VoIP, chamados de SIP Servers.



12.1. VoIP (Voice over IP)

As redes em que se realizam comunicações VoIP são classificadas em dois tipos:

- **Privadas:** Como exemplo de redes privadas, temos as redes corporativas de empresas. Contudo, as redes privadas usadas para comunicação VoIP podem ser de diversos tamanhos, desde grandes redes corporativas até pequenas redes locais;
- **Públicas:** Como representante de rede pública para comunicações VoIP, temos a Internet. Para utilizar o serviço VoIP, o usuário, preferencialmente, deve possuir um acesso de banda larga, como cabo, ADSL e rádio, entre outros.

O modo mais simples de utilização de VoIP é a comunicação feita computador a computador, a partir da Internet. Nesse tipo de comunicação, o programa mais utilizado é o Skype.

12.3.1. Telefonia IP

A tecnologia VoIP pode ser usada para estabelecer chamadas com a rede pública de telefonia, seja telefonia fixa ou celular. Essa aplicação da tecnologia VoIP é conhecida como telefonia IP.

Há dois tipos de serviços de telefonia IP:

- Para fazer chamadas para a rede pública, em que o usuário completa a chamada discando o número convencional do telefone de destino;
- Para fazer e receber chamadas da rede pública, em que o usuário completa a chamada discando o número convencional do telefone de destino e recebe um número para receber as chamadas da rede pública.

É preciso destacar que os dois tipos de serviço podem receber e fazer chamadas para um usuário que utilize o mesmo prestador de serviços VoIP, o que normalmente é feito sem custo. Não podem, porém, realizar chamadas para usuários de outros provedores VoIP.

O sistema VoIP apresenta os seguintes componentes básicos:

- **Telefone IP:** Telefone com os recursos necessários para o serviço VoIP. Para que possa receber e fazer ligações VoIP, basta apenas que seja conectado a uma rede IP;
- **Adaptador para Telefone Analógico (ATA):** Dispositivo responsável por converter um telefone analógico convencional para um telefone IP. Quando conectado a um telefone analógico e a uma rede IP, permite ao telefone analógico receber e fazer ligações VoIP;

- **Softphone:** Programa interligado a um servidor VoIP, realiza chamadas para ATAs, telefones IP e outros softphones que estejam conectados ao mesmo servidor VoIP;
- **Gatekeeper (GK):** Controla o acesso e a banda utilizada pela rede. Além disso, gerencia as chamadas dos terminais e realiza o endereçamento dos terminais na rede. Em outras palavras, o Gatekeeper efetua o gerenciamento dos telefones IP;
- **Gateway (GW):** Este dispositivo torna possível a conexão entre uma rede VoIP e a rede de telefonia pública, já que ele efetua a conversão da voz analógica para voz digital comprimida (em tempo real) e a conversão de sinalização para as chamadas telefônicas da rede VoIP;
- **Application Server (AS):** Os variados serviços adicionais que uma rede VoIP pode oferecer (como caixa postal, agenda telefônica, entre outros) são fornecidos pelo Application Server.

12.4. IPTV e Web TV

A IPTV ou TVIP é um método de transmissão de sinais televisivos que utiliza o protocolo IP como meio de transporte do conteúdo. É diferente, entretanto, de uma Web TV, em que os conteúdos de televisão podem ser distribuídos via streaming, mas não há garantia de qualidade do sinal.

Na IPTV, o conteúdo é apenas enviado em streaming e há garantia de qualidade na entrega, pois a rede é fechada. O sinal passa, a seguir, para um receptor, que é um aparelho set-top box conectado à televisão (semelhante ao decodificador utilizado na TV a cabo).

Na Web TV, o receptor é normalmente um computador e o conteúdo é quase sempre visto em um monitor. Normalmente uma programação é enviada via streaming armazenado, pois como o meio de acesso é a rede pública, podem ocorrer pausas e interrupções no envio do conteúdo devido à disponibilidade e tráfego, principalmente se o meio utilizado for o streaming em tempo real.

12.5. CFTV

CFTV refere-se aos circuitos fechados de televisão. Eles são utilizados como mecanismos de prevenção e controle de segurança. Eles permitem ver e gravar imagens de locais situados em ambientes residenciais, públicos e corporativos. Os CFTVs utilizam novas tecnologias que os tornam mais versáteis e completos. Podemos destacar os gravadores digitais, que substituíram as fitas, e os softwares que permitem a transmissão de imagens ao vivo, via Internet, para um dispositivo remoto. Sistemas digitais de CFTV são fáceis de administrar, além de serem flexíveis e expansíveis. Eles podem, ainda, ser integrados às estruturas existentes.

As imagens em um CFTV podem ser captadas através de câmeras analógicas ou câmeras IP.

O armazenamento e acesso de imagens em um CFTV podem ser feitos através de dois dispositivos, os quais veremos a seguir.

12.5.1. DVR

O gravador de vídeo digital (ou DVR, digital video recorder) grava vídeo analógico em formato digital, armazenando-o em um disco rígido ou outro dispositivo de memória. Podemos também considerar como DVR programas para computador que possibilitam captura de vídeo para um disco rígido, bem como reprodução de vídeos.

As imagens analógicas de cada câmera são enviadas para uma entrada do DVR, que possui, no mínimo, uma saída para monitor. O software residente no DVR possibilita enviar para a saída do monitor a imagem de uma única câmera ou de várias simultaneamente.

O DVR pode possuir uma porta Ethernet e se conectar à rede, onde usuários podem acessar, de qualquer microcomputador, as imagens em tempo real ou armazenadas.

12.5.2. NVR

O gravador de vídeo para rede (ou NVR, network video recorder) é um software de gerenciamento e controle de vídeo. Por meio dele, podemos monitorar, gravar, reproduzir e controlar câmeras em uma rede.

Nesse esquema, cada câmera possui um endereço IP e estão conectadas na rede local. O microcomputador que possui o NVR instalado grava, gerencia, monitora e controla as câmeras através da rede local.



Teste seus conhecimentos
Convergência
digital

12

Conceitos e Infraestrutura de Redes (online)

230

1. O gerenciamento, controle e armazenamento de imagens em um CFTV que utiliza câmeras IP são feitos por qual dispositivo?

- a) Gateway
- b) DVR
- c) PC
- d) NVR
- e) Todas as alternativas anteriores estão corretas.

2. Qual dos itens a seguir é responsável por oferecer serviços tais como agenda telefônica, caixa postal, fila de espera, distribuidor automático de chamadas em sistemas VoIP?

- a) Telefone IP
- b) Application Server
- c) Gateway
- d) Gatekeeper
- e) NVR

3. Controlar o acesso e a banda utilizada pela rede, gerenciar as chamadas dos terminais e realizar o endereçamento dos terminais na rede são funções de qual dispositivo?

- a) DVR
- b) NVR
- c) Gatekeeper
- d) Gateway
- e) Application Server

4. Qual é a classe de streaming que normalmente é utilizada em Web TV?

- a) Streaming armazenado.
- b) Streaming em tempo real.
- c) Streaming interativo em tempo real.
- d) Não se utiliza streaming em Web TV.
- e) Nenhuma das alternativas anteriores está correta.

5. Qual o nome de um programa que realiza chamadas para ATAs e telefones IP conectados ao mesmo servidor VoIP?

- a) Set-top box
- b) NVR
- c) Gatekeeper
- d) Gateway
- e) Softphone