



**GOVERNO DO
ESTADO DO CEARÁ**

Secretaria da Educação

**ESCOLA ESTADUAL DE
EDUCAÇÃO PROFISSIONAL - EEEP**
ENSINO MÉDIO INTEGRADO À EDUCAÇÃO PROFISSIONAL

CURSO TÉCNICO EM INFORMÁTICA

REDES DE COMPUTADORES



GOVERNO DO ESTADO DO CEARÁ

Secretaria da Educação

GOVERNADOR
Camilo Santana

VICE-GOVERNADORA
Maria Izolda Cela de Arruda Coelho

SECRETÁRIO DA EDUCAÇÃO
Rogers Vasconcelos Mendes

SECRETÁRIA EXECUTIVA DA EDUCAÇÃO
Rita de Cássia Tavares Colares

ASSESSORIA INSTITUCIONAL
Danielle Taumaturgo

COORDENADORIA DA EDUCAÇÃO PROFISSIONAL
Jussara de Luna Batista



Disciplina:
Redes de Computadores

*Apostila destinada ao Curso Técnico de Nível Médio em Informática das Escolas Estaduais de
Educação Profissional – EEEP*

Equipe de Elaboração - 2012

*Adriano Gomes da Silva
Cíntia Reis de Oliveira
Evandilce do Carmo Pereira
Fernanda Vieira Ribeiro
Francisco Aislân da Silva Freitas
João Paulo de Oliveira Lima
Juliana Maria Jales Barbosa
Liane Coe Girão Cartaxo
Mirna Geyla Lopes Brandão
Moribe Gomes de Alcântara
Niltemberg Oliveira Carvalho
Paulo Ricardo do Nascimento Lima
Renanh Gonçalves de Araújo
Renato William Rodrigues de Souza
Valbert Oliveira Costa*

Colaboradores

*Maria Analice de Araújo Albuquerque
Maria Danielle Araújo Mota
Sara Maria Rodrigues Ferreira Feitosa*

Atualização – 2018

Paulo Ricardo do Nascimento Lima

SUMÁRIO

APRESENTAÇÃO.....	4
1.0 INTRODUÇÃO ÀS REDES DE COMPUTADORES	5
1.1. O que são e para que servem as redes de computadores.....	6
1.1.1. Dados que podem ser transmitidos	8
1.2. Como a Internet surgiu?	9
1.3. Convergência de tecnologias.....	11
1.3 Redes ponto-a-ponto e cliente-servidor	13
1.5 Como funciona a transmissão	14
1.6 modos de operação	16
2.0 MEIOS DE COMUNICAÇÃO.....	18
2.1. Cabos elétricos, fibras ópticas e ondas de radiofrequência.....	18
2.1.1. Cabos de Par Trançado	18
2.1.2. Cabos Coaxiais.....	20
2.1.3. Fibras Ópticas.....	22
2.1.4. Transmissão via rádio terrestre ou microondas	24
2.1.5. Transmissão via Satélite	26
3.0 TOPOLOGIAS	30
3.1. Topologias de Redes.....	30
3.1.1. Barramento	30
3.1.2. Anel	30
3.1.3. Estrela.....	31
3.1.4. Árvore	33
3.1.5. Híbrida.....	33
3.1.6. Ligação Total – Malha	34
3.8. Sem fio	34
4.0 Escopos de uma rede	37
4.1. Redes divididas geograficamente.....	37
4.1.1. LAN (Local Area Network)	38
4.1.2. MAN (Metropolitan Area Network)	38
4.1.3. WAN (Wide Area Network)	39
4.2 Mainframes, terminais burros e clientes magros.....	40
4.2.1. Mainframes	40
4.2.2. Terminais burros.....	41
4.2.3. Clientes magros (thin clients).....	42
4.3 Arquiteturas cliente-servidor e Peer-to-Peer	44
4.3.1. A arquitetura Cliente – Servidor	44
4.3.2. A arquitetura Peer-to-Peer	45
5.0 MODELOS OSI E TCP	49
5.1. CAMADA DE APLICAÇÃO (Modelos OSI e TCP/IP)	52
5.1.1. Serviços e Funções	52
5.1.2. Protocolo HTTP	53
5.1.3. Protocolo FTP	54
5.1.4. Protocolos SMTP e POP3	54
5.1.5 Encapsulamento	56
5.1.6 Serviços de DNS	61
5.2. CAMADAS DE APRESENTAÇÃO E SESSÃO (Apenas Modelo OSI).....	66
5.2.1. Camada de Apresentação – Serviços e Funções	66
5.2.2. Camada de Sessão – Serviços e Funções	66
5.3. CAMADA DE TRANSPORTE (Modelos OSI e TCP/IP).....	68

5.3.1. Serviços e Funções	68
5.3.2. Protocolo TCP	69
5.3.3. Protocolo UDP	72
5.4. CAMADA DE REDE (Modelo OSI) ou INTERFACE COM A REDE (Modelo TCP/IP)	74
5.4.1. Serviços e Funções	74
5.4.2. Protocolo IP	77
5.4.3. IPv6	80
5.4.5. Protocolo DHCP.....	82
5.5. Camadas de enlace e física (modelo osi) ou interface com a rede (modelo tcp/ip)	85
5.5.1. Endereços MAC	86
5.5.2. Ethernet	88
5.6 Os dispositivos ativos e passivos	91
5.7 Repetidores.....	92
5.7.1. Repetidos Wireless	92
5.8 Hubs	94
5.8.1. Interligando Hubs.....	95
5.9 Placas de redes e o endereço MAC	96
5.9.1. O endereço MAC	97
5.10. Pontes	99
5.11 Switches.....	101
5.11.1. Definição e funcionamento	101
5.11.2. Tipos de Switches	102
5.12 Roteadores	104
6.0. A crimpagem de cabos	110
6.0.1. Utilizar cabo crossover ou direto?.....	110
6.0.2. Padrões T568A e T568B	111
6.1. Wireless	114
6.1.1. O que é uma rede wireless?.....	114
6.1.2. Tipos de redes Wireless	116
6.2 A Tecnologia WI-FI.....	117
6.3. O infravermelho	122
6.4 Tecnologia Bluetooth	124
6.4.1. Redes Bluetooth	125
7.0 Projeto de Redes de Computadores.....	131
7.1. O projeto lógico.....	132
7.1.1. Compreendendo os endereços IP	132
7.1.2. Número IP: identificando rede e máquina.....	133
7.1.3. Classes de endereços IPv4	133
7.1.4. Máscara de rede.....	134
7.1.5. Endereços IP para redes privadas	135
7.2. Serviços utilizáveis na rede	135
7.2.1. Compartilhamento de internet (modens + roteadores sem fio)	135
7.2.2. Configuração de compartilhamento de internet por dispositivos diferentes.....	139
7.3 O projeto físico.....	146
7.3.1 Montagem da infra-estrutura física	147
7.3.2 Tomadas na parede	148
Referências	153

APRESENTAÇÃO

Você, aluno do curso de Técnico em Informática deve estar bastante curioso em relação à sua formação e talvez já tenha se perguntado: “Afinal, o que são Redes de Computadores?”.

Vivendo em uma sociedade na qual, o poder de um indivíduo ou grupo está associado ao nível e volume de informação que este possui, é fácil observar a necessidade de conectividade entre provedores de informação e consumidores destas, visando maior rapidez na aquisição das mesmas e possibilidade de uso desta a seu favor.

Assim gigantes da informação trabalham constantemente interligadas através de redes de dados, permitindo que nos comuniquemos e saibamos cada vez mais e mais rápido uma diversidade de assuntos nunca transmitida antes. Nos bastidores destes processos de transito de informação estão as redes de computadores que trabalham dia e noite afim de otimizar o tempo e qualidade das informações e dos trabalhos realizados sobre estas.

Neste guia trataremos da teoria e prática associada ao funcionamento das redes de computadores, levando em consideração fatores como aplicabilidade, custo, equipamentos e tipos de sistemas que podem ser implantados e que estão em estudos. Por fim, este material cobre os estudos acerca dos processos de conectividade entre equipamentos de rede como computadores, impressoras, switches, modens e roteadores passando pela configuração de redes cabeadas e sem fio chegando a configuração de servidores para compartilhamento de internet, impressoras e arquivos. Observe que, desta forma, estaremos buscando competências e habilidades técnicas que permitirão a realização de trabalhos que vão desde a configuração de um ponto de acesso de rede sem fio domiciliar até a configuração de servidores em laboratórios de informática e lan houses. Assim, buscamos orientar o crescimento em termos de conhecimento técnico complementar, o que o torna um profissional mais completo que consegue exercer atividades tanto na camada de conectividade como na camada de hardware, passando por configuração de serviços essenciais.

Este material teve como grande contribuição e referência para alguns capítulos o material do projeto MEDIOTEC – SEDUC, como apostilas do módulo I, em uma verificação e adaptação do material, por ser um material muito importante e de altíssima qualidade e aproximar bastante a experiência à prática do técnico em informática em abordagens e casos resumidos.

1.0 INTRODUÇÃO ÀS REDES DE COMPUTADORES

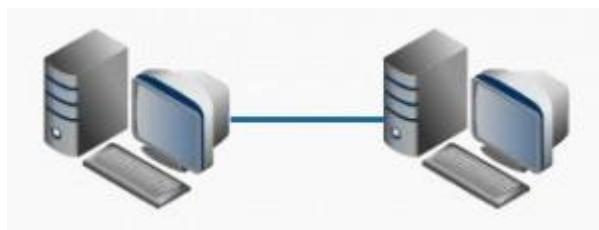
Daqui por diante passa a tratar uma parte do universo da TI que trabalha diretamente com a infraestrutura do sistema de comunicação entre máquinas e por consequência de transmissão de informações entre seres humanos.

Em um bom português, podemos falar que esta área trabalha desde a transferência de dados via bluetooth entre celulares a conexões de banda larga entre países dos 5 continentes. Esta área é conhecida como redes de computadores. Através do estudo dela aprenderemos a fazer computadores acessarem a Internet, celulares copiarem arquivos de um computador, computadores compartilharem impressoras, uma gravadora de DVD ou até mesmo o que está sendo apresentado em seu monitor.



Antes de executar cada configuração aqui citada é necessário aprender sobre as tecnologias e como as comunicações em rede são possíveis para entender como estas tecnologias funcionam. Mas por onde começar?

Tudo precisa começar de algum lugar, então nosso estudo irá começar com foco em uma lição de história. Assim, iremos saber o que é uma rede de computadores. Será interessante entender como nós chegamos onde estamos, mas ela vai ser curta o suficiente para que você não se confunda e possa entrar em detalhes fácil e rapidamente. Se alguns termos não forem familiares para você, não se preocupe, pois se eles forem importantes para aprender redes, serão explicados nos capítulos posteriores.



Hoje em dia fala-se muito em rede, mas afinal de contas, o que é uma rede? Simplificando ao extremo, uma rede nada mais é do que um conjunto de máquinas que se comunicam. Estas máquinas podem ser computadores, impressoras, telefones, aparelhos de fax, etc. Se interligarmos dois computadores de modo que eles possam se comunicar e trocar dados, então teremos uma rede de dois computadores, uma espécie de mini internet. Para fazer com que máquinas se comuniquem é necessário: interligar fisicamente as máquinas; "regular" as máquinas e fazer com que "falem" a mesma linguagem, usando a mesma "gramática". Desse modo, se você tem um computador e uma impressora e as duas máquinas podem se comunicar, então você pode dizer que tem uma rede. Se seu computador está conectado à Internet, então você faz parte de uma rede gigantesca, pois sua máquina pode se comunicar com computadores em qualquer lugar do planeta.

Os meios físicos utilizados para interligar máquinas podem ser simples fios de cobre, fibras óticas ou sofisticados meios de comunicação, através de ondas eletromagnéticas em diversas faixas de frequência (rádio, micro-ondas, bluetooth, wifi, etc) que dispensam fios ou cabos. Independentemente do meio utilizado, o que realmente importa é que as máquinas possuam um canal de comunicação.

1.1. O que são e para que servem as redes de computadores.

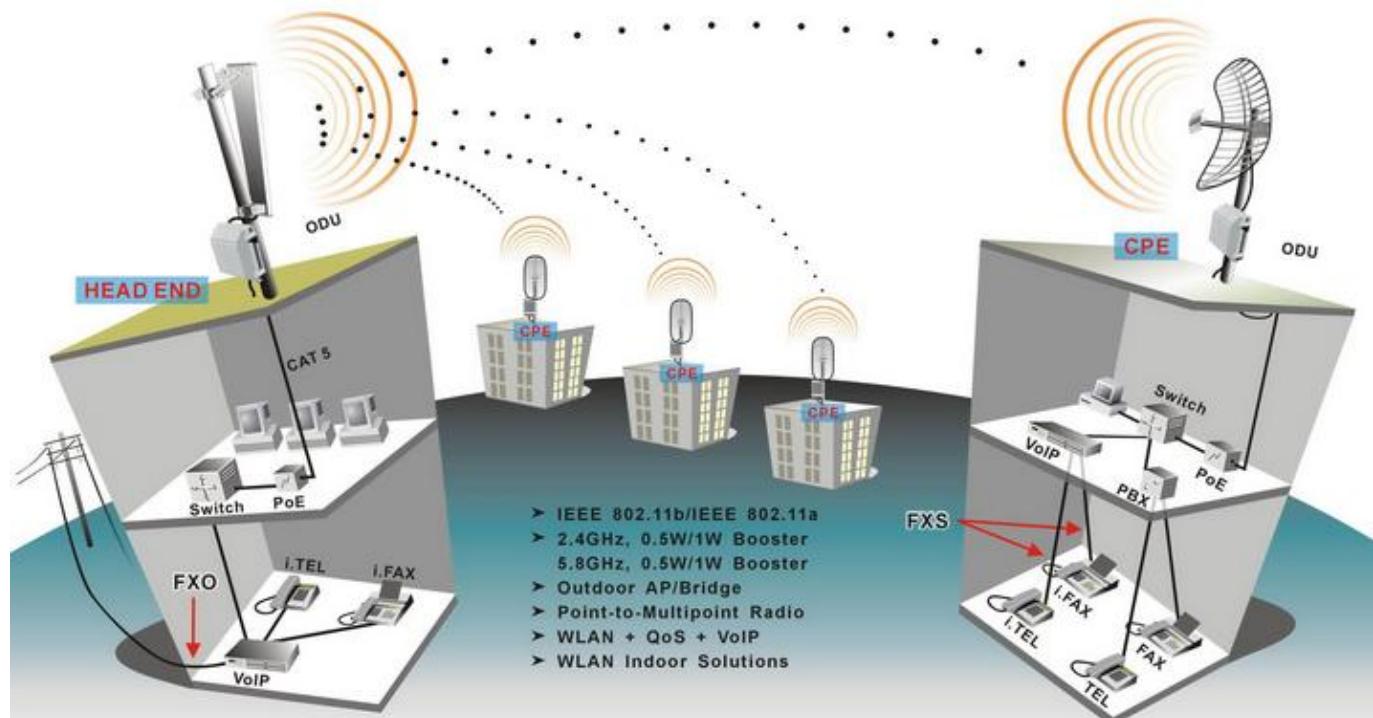
Provavelmente você já foi a uma loja ou supermercado e notou que todos os atendentes utilizam computadores com um sistema, ou programa, para efetuar a venda dos produtos. Para que todos os computadores do estabelecimento utilizem o mesmo programa é necessário que os computadores estejam interligados e se comuniquem. Esta ligação pode ser chamada de Rede.

Uma rede de computadores é a forma de conectarmos equipamentos a fim de que possamos estabelecer uma comunicação entre os mesmos fazendo com que eles troquem dados, informações e serviços.

Sem uma rede, os estabelecimentos do exemplo acima não conseguiriam usar seu sistema de vendas de forma eficiente. Quando um vendedor finaliza a venda de um produto, este produto passa a não constar mais no estoque. Sem uma rede, este mesmo produto ainda iria constar no sistema de outro vendedor, que correria um grande risco de vender um produto que não existe mais na loja.

As redes estão muito mais presentes em nossa vida do que podemos imaginar. Seja em no celular, na

internet, no computador de um hospital ou posto de saúde, no banco, no caixa eletrônico ou no sensor de velocidade. As redes de computadores, apesar do nome, envolvem muito mais que apenas computadores, mas abrangem uma gama de dispositivos e equipamentos como celulares, tablets, impressoras, TVs, carros, videogames e até eletrodomésticos.



Uma rede corporativa, ou seja, uma rede de uma corporação como uma empresa, órgão ou instituição é demasiadamente importante para o bom funcionamento do ambiente de trabalho. Com ela é possível compartilhar arquivos, trocar mensagens, enviar diversos tipos de dados, compartilhar equipamentos como impressoras e aparelhos de fax, distribuir internet, publicar um site interno, gerenciar e-mails, ter acesso ao banco de dados e até mesmo controlar o acesso de usuários na rede. Controle este essencial quando se zela pela segurança, evitando o acesso de intrusos que podem capturar informações sigilosas ou desconfigurar algum serviço.

A segurança em redes é um ponto crucial. Apesar de todos os esforços dos profissionais de Segurança das Informações e de todas as ferramentas já criadas para evitar ataques e intrusões, as nossas redes não são 100% seguras. Você verá este assunto de forma mais aprofundada em disciplinas posteriores, mas fica a dica: os trabalhos que envolvem segurança de redes estão em constante crescimento e é uma ótima área para se especializar.



Então tudo bem, já entendi o que é uma Rede de Computadores, mas que tipos de dados ou arquivos eu posso enviar e receber ao usar uma rede?

1.1.1. Dados que podem ser transmitidos

Provavelmente você já viu uma foto ou uma música serem enviadas de um celular para outro através do Bluetooth. Este é um exemplo de transmissão baseado nas redes de computadores de curta distância.

Sabemos que os computadores processam informações calculando bits que podem ser convertidos em impulsos elétricos, portanto toda informação que pode ser processada em bits, pode ser transmitida em uma rede.

Arquivos de áudio como músicas, arquivos de vídeo, textos e imagens podem ser convertidos em bits, portanto podem ser enviados através de uma rede. Informações como o aroma de uma flor ainda não podem ser convertidas em bits, portanto não podem ser transmitidas, mas já existem pesquisadores desenvolvendo telas que permitem que o usuário sinta a textura das imagens como a aspereza do caule de uma árvore ou a profundidade de um buraco.

Ficou curioso para saber como funciona? Quando tiver um tempo livre, pesquise sobre o assunto na internet!



- Indique e explique o que está errado na seguinte frase: “Uma rede de computadores é a forma de conectarmos equipamentos a fim de que possamos bloquear uma comunicação entre os mesmos.”

- Cite outros locais onde podemos encontrar uma rede de computadores.

3. Diferencie rede corporativa de rede doméstica.

4. Por que devemos zelar pela segurança em uma rede de computadores?

5. Quais tipos de dados podem ser transmitidos em uma rede?

1.2. Como a Internet surgiu?

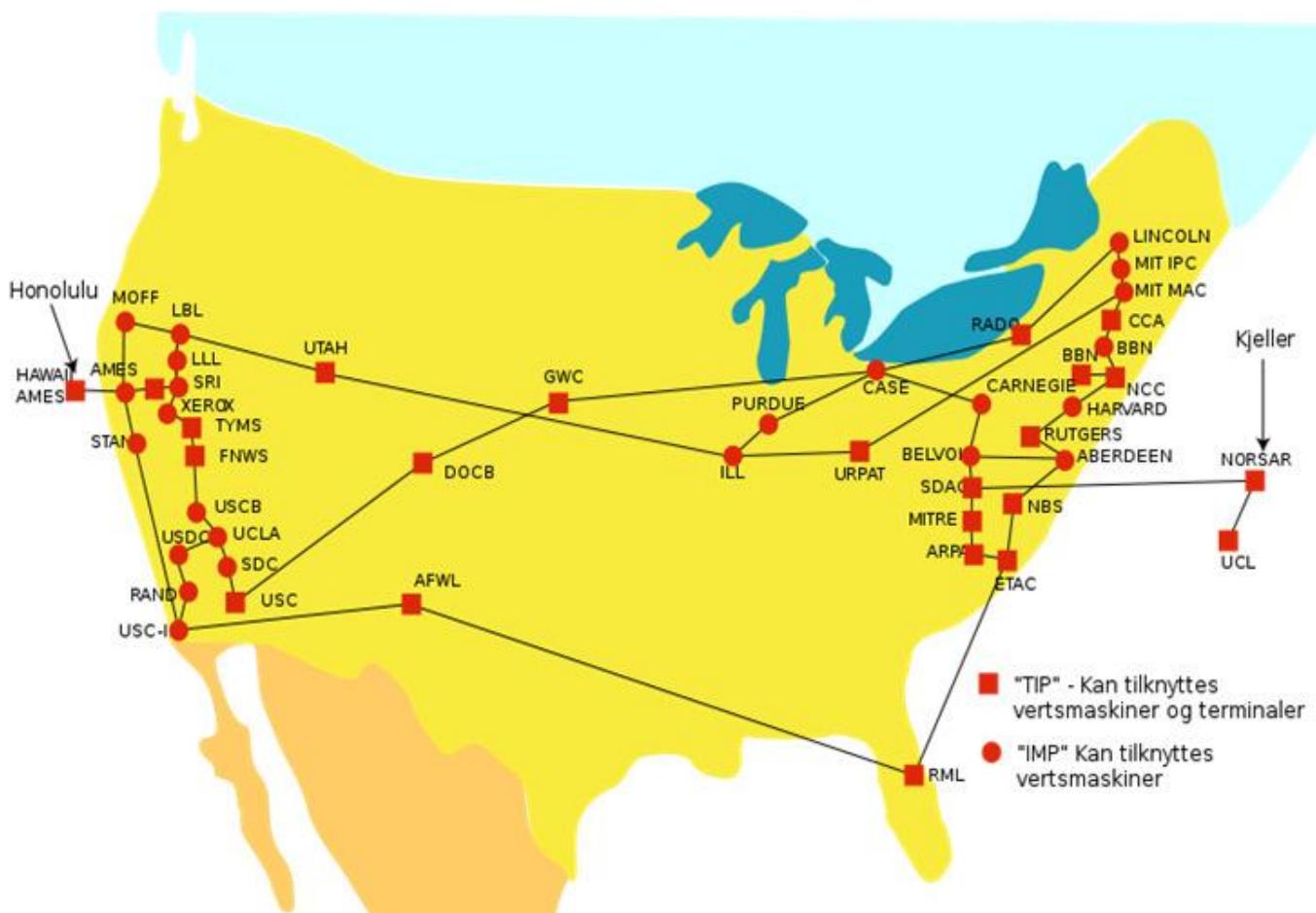
No final de Outubro de 1957 ocorreu um evento que provocaria tamanhas mudanças que alteraria a vida de pessoas em todo o planeta. A União Soviética lançou, com sucesso, o primeiro satélite na órbita da Terra. Após o lançamento desse satélite, denominado “Sputnik 1”, o mundo ficou assombrado, em especial os USA, que possuíam seu próprio programa para lançamentos de satélites, contudo os norte-americanos ainda não haviam lançado um único satélite.

Este evento levou diretamente à criação da Agência de Projetos de Pesquisa Avançada (ARPA) do Departamento de Defesa dos Estados Unidos, devido a uma reconhecida necessidade de uma organização que possa pesquisar e desenvolver ideias e tecnologia avançada para além das necessidades identificadas atualmente. Talvez o seu mais famoso projeto (certamente o mais amplamente utilizado) foi a criação da Internet.

Em 1960, o psicólogo e cientista de computação Joseph Licklider publicou um documento denominado “Relação Homem-Computador”, que articulava a ideia de computadores em rede fornecendo armazenamento e consulta de informações. Enquanto exercia o cargo de chefe do escritório de processamento de informação na ARPA, ele reuniu um grupo para pesquisar computadores, contudo ele abandonou as pesquisas antes que algum projeto tenha sido desenvolvido, o ano era 1962.

O plano para esta rede de computadores (chamada “ARPANET”) foi apresentado em outubro de 1967, e em dezembro de 1969 a primeira rede de quatro computadores estava pronta e funcionando, contudo, havia um grande problema, algumas redes com tecnologias diferentes de comunicação.

Robert Kahn fazia parte de um projeto que visava desenvolver um sistema de comunicações que utilizava pacotes de rede para as transmissões de satélite da ARPA, quem começou a definir algumas regras para uma arquitetura de rede mais aberta para substituir o protocolo até então usado pela ARPANET. Depois, com a chegada de Vinton Cerf, da Universidade de Stanford, os dois criaram um sistema que mascara a diferença entre os protocolos de rede, usando um novo padrão.



Esta especificação reduziu o papel da rede e moveu a responsabilidade de manter a integridade da transmissão para o computador servidor. O resultado final disto foi que ela tornou possível acessar com

facilidade quase todas as redes simultaneamente.

A ARPA financiou o desenvolvimento do software, e em 1977 foi conduzida uma demonstração de uma comunicação entre três redes diferentes. Em 1981, a especificação foi finalizada, publicada e adotada; e em 1982 as conexões da ARPANET para fora dos EUA foram convertidas para usar os protocolos presentes no atual “TCP/IP”, era o embrião do que hoje conhecemos por Internet.

1.3. Convergência de tecnologias

Atualmente vivenciamos a convergência entre as tecnologias das redes de telecomunicações e das redes de computadores, a união dos fatores apresentados anteriormente, aliados aos novos avanços tecnológicos envolvendo a capacidade de transporte das redes de comunicação levou a um campo de atuação comum para ambas que é o fornecimento de múltiplos serviços baseados em uma infra estrutura única, resultado da experiência obtida no desenvolvimento e operação, tanto das redes de computadores quanto das redes de telecomunicações.



Esse conceito de convergência é o que denominamos atualmente como "internetwork", ou seja, um conjunto de dispositivos e procedimentos que viabilizam a interconexão de redes individuais, formando assim redes com capacidades maiores, fortemente baseadas no emprego de computadores e seus recursos de controle, aliadas ao emprego das técnicas de chaveamento de pacotes e transmissão de dados dos sistemas de telecomunicações, sendo, portanto, uma combinação de ambas as tecnologias (redes de telecomunicações e computadores).

O maior exemplo de internetwork é a própria Internet. Um dos atuais desafios dos sistemas de comunicação ainda é a interconexão dos variados sistemas de informação.

Na prática, ainda existem muitas redes de naturezas diferentes, com novos serviços surgindo a cada dia e usando protocolos diferentes que, obviamente, necessitam ser interligadas. Assim, permitir comunicações utilizando a infraestrutura de comunicação existente para prover o intercâmbio desses usuários, proporcionando a todos um suporte eficiente para a comunicação entre tecnologias distintas, com diferentes tipos de mídias e velocidades variadas é um dos objetivos que se quer alcançar com a convergência das tecnologias de redes.

Com certeza, essa evolução das redes de computadores e de telecomunicações é um caminho sem volta que nos levará a total convergência entre as tecnologias, padrões, dispositivos e aplicações para redes de comunicação, presentes e futuras.



1. Explique em poucas palavras o que é uma rede de computadores.

2. Explique resumidamente quais requisitos são necessários para que computadores possam se comunicar em rede.

3. Qual é importância dos protocolos de comunicação em redes de computadores?

4. O que foi o Sputnik?

5. Qual a relação entre a ARPANET e a INTERNET?

6. O que é internetwork?

7. Cite um dos desafios presentes na implantação da internetwork.

1.3 Redes ponto-a-ponto e cliente-servidor

Existem 2 tipos fundamentais de redes. O primeiro tipo é a rede ponto-a-ponto, onde os computadores são ligados entre si para a troca de informações, porém a maioria dos recursos não pode ser compartilhada fazendo com que cada host deva possuir os próprios recursos e aplicações como um programa, por exemplo.



HOST: Palavra inglesa que significa hospedeiro.

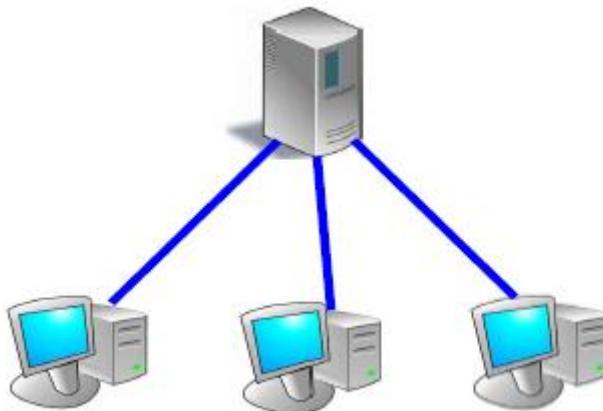
Em informática, um host é um computador ou outro equipamento conectado na rede e que pode compartilhar informações, serviços e recursos.

O segundo tipo é a arquitetura cliente-servidor, onde todos os hosts, chamados de clientes, se comunicam com uma máquina principal, chamada de servidor. O servidor provê todas as aplicações e serviços e

consegue gerenciar o acesso aos recursos da rede como impressoras, por exemplo. Neste tipo de arquitetura os hosts não trocam informações entre si de uma forma direta.

Cada cliente se comunica com o servidor e este devolve respostas atendendo as requisições de cada um. Por exemplo, em um servidor de banco de dados, o cliente pode acessar a aplicação (programa) e alterar um dado. Esta alteração será feita no servidor. Caso outro cliente acesse a aplicação, ele já verá o dado alterado, pois está buscando a informação diretamente no servidor.

Normalmente um servidor é uma máquina mais robusta que as máquinas clientes, pois ela armazena e processa um grande número de informações, além de precisar estar sempre ligada para que haja tráfego de informações na rede.



1.5 Como funciona a transmissão

Nós, seres humanos, usamos diversos meios para nos comunicar. Você, por exemplo, se tiver uma dúvida deverá fazer uma pergunta ao seu professor e este, por sua vez, deverá responder à pergunta de forma a tirar sua dúvida. Neste caso, vocês conseguiram se comunicar e tudo ficou resolvido. Porém, se você não perguntar da maneira correta, ou se houver algum ruído durante a pergunta, talvez o professor não comprehenda bem e acabe respondendo de forma equivocada. Neste caso, houve um problema na transmissão da informação, consequentemente a comunicação ficou comprometida. Simples, não é mesmo?

Em redes de computadores, os princípios são os mesmos. Sempre existe um transmissor, um receptor e uma informação a ser enviada. A transmissão de dados na computação requer alguns componentes essenciais [Ribeiro, 2010]:

- Transmissor: é o dispositivo (computador, telefone, câmera) que envia a informação.

- Receptor: é o dispositivo a quem foi endereçada a informação. O receptor vai receber a mensagem enviada pelo transmissor.
- Mensagem: são os dados e as informações que precisam ser enviados.
- Meio: é o meio físico, ou seja, o caminho pelo qual a mensagem trafegará do transmissor até chegar ao receptor.
- Protocolo: controla o envio e recepção da mensagem e define alguns aspectos como formato da mensagem e ordem de chegada. Tanto o transmissor quanto o receptor devem estar seguindo o mesmo protocolo.

No exemplo anterior, o transmissor é você (o aluno); o receptor é o professor; a mensagem é a pergunta; o meio é o ar, por onde as ondas sonoras da sua voz se propagam e o protocolo é a palavra falada em língua portuguesa.

Para que a comunicação de dados obtenha sucesso ela necessita de três atributos:

- Entrega: os dados devem estar endereçados corretamente. Deve-se ter a certeza de que a informação será entregue ao destinatário correto.
- Confiabilidade: os dados devem chegar ao destino, e mais do que simplesmente chegar, os dados devem estar intactos, sem nenhum tipo de alteração e sem faltar nenhuma parte da informação.
- Controle do Atraso: o tempo que a informação possui para chegar ao destino não pode ser indeterminado. Deve haver um tempo limite para que o destinatário a receba, principalmente no caso de aplicações multimídia em tempo real como áudio e vídeo. Não seria interessante, por exemplo, ao receber um vídeo, ver primeiro as imagens e só depois ouvir o áudio.

TAXA DE TRANSMISSÃO

Ao se transmitir um arquivo, seja ele de que tipo for, pela rede, na realidade estão sendo transmitidos vários bits que, em conjunto, compõem o arquivo depois de processados. A taxa de transmissão de uma rede é a velocidade com a qual esses bits trafegam pelos meios de comunicação e é medida em bps (bits por segundo), ou seja, a quantidade de bits que são enviados em um segundo, portanto quanto maior a taxa de transmissão de uma rede, mais rápido o arquivo consegue ser transmitido do emissor para o receptor.

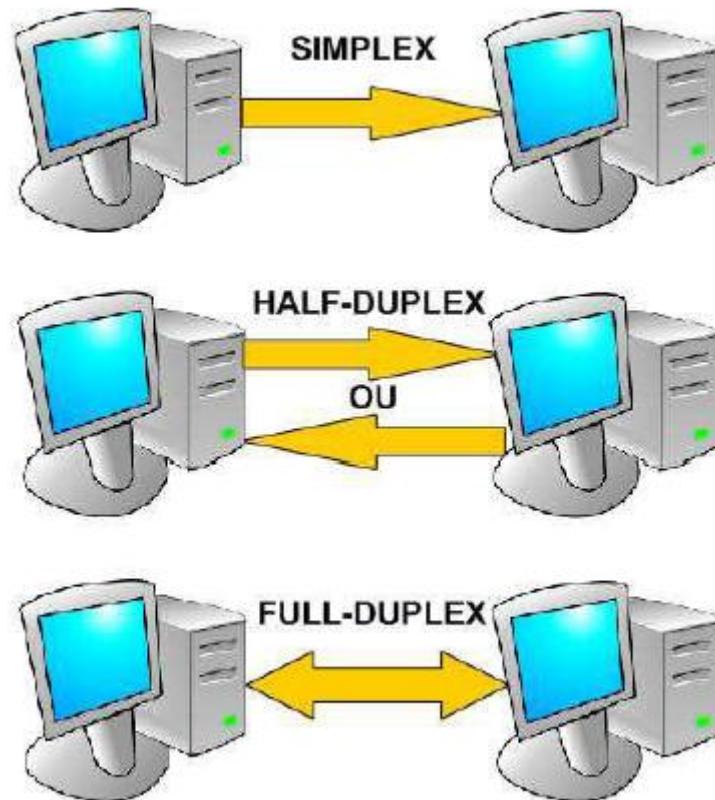


Ah, então é por isso que uma internet de 600kbps é mais rápida que uma de 100kbps! Porque são enviados mais bits, ou seja, mais informação, em um mesmo segundo.

1.6 modos de operação

Existem três tipos de operação na transmissão de dados: simplex, halfduplex e full-duplex. Vejamos como funciona cada uma delas:

- Simplex: a transmissão é unidirecional. Só existe um transmissor e um canal de transmissão. Quaisquer outros componentes que apareçam na comunicação serão receptores. Exemplos: televisão e radiodifusão.
- Half-duplex: a transmissão é bidirecional, ou seja, as duas partes transmitem e também são receptoras, mas, assim como no modo simplex, existe somente um canal de transmissão, portanto só é possível transmitir um por vez. Exemplo: walkie-talkie.
- Full-duplex: é o modo de transmissão mais completo, já que ambas as partes podem transmitir e receber dados simultaneamente, pois existem dois canais de transmissão. Exemplo: telefone.





1. Marque V para verdadeiro e F para falso:

- () Em uma rede ponto-a-ponto cada host deve possuir os próprios recursos e aplicações.
() Em uma arquitetura cliente-servidor, todos os hosts chamados servidores se comunicam com uma máquina principal chamada de servidor.

2. Quais as diferenças no hardware de uma máquina cliente em relação a uma máquina típica para servidores?

3. Qual a importância da taxa de transmissão em uma comunicação?

4. Analise os meios de comunicação abaixo e indique se a transmissão em cada um deles é do tipo (S) simplex, (H) half-duplex ou (F) full-duplex.

- () radioamador
() televisão
() celular
() radiodifusão

2.0 MEIOS DE COMUNICAÇÃO

2.1. Cabos elétricos, fibras ópticas e ondas de radiofrequência.

Já vimos como funciona uma transmissão de dados entre dois equipamentos em uma rede, mas para que a transmissão aconteça é necessário que exista um meio de os dados saírem de um host e chegarem a outro, ou seja, uma forma de propagação.

Uma das formas de se enviar dados é através da eletricidade. As placas de rede com fio são responsáveis por converter dados em bits e bits em impulsos elétricos que podem trafegar por um cabo de energia. Os cabos mais comumente usados são os cabos de par trançado e os cabos coaxiais.

Outra forma é transmitindo através da luz em vez da eletricidade. A transmissão feita por raios luminosos é bem mais eficaz que a feita pela eletricidade, pois o sinal se propaga mais rápido e não sofre com interferências eletromagnéticas. Para transmitir desta maneira utilizamos os cabos de fibra óptica.

Apesar de toda tecnologia no tocante a cabos, existem alguns casos em que eles não são interessantes. Redes com centenas de hosts requerem muito investimento em cabos. Prédios antigos nem sempre possuem tubulação elétrica própria para efetuar a passagem dos cabos. Uma rede cabeada não possui versatilidade suficiente para que o proprietário mude a posição dos computadores sem um pouco de transtorno. Por esses e outros motivos, torna-se desejável o uso de um meio de comunicação versátil, barato, e abundante: o ar. Pelo ar podemos transmitir ondas de radiofrequência através de antenas e efetuar a comunicação entre elementos previamente configurados para este fim. As redes sem fio estão a cada dia mais presentes no nosso cotidiano, nos computadores, celulares, televisores, rádio, entre outros.

Vejamos mais detalhes de cada meio de comunicação de dados:

2.1.1. Cabos de Par Trançado

É o meio de transmissão mais comumente encontrado no nosso dia-a-dia.

Com certeza você já deve ter visto uma série de cabos azuis saindo de computadores em um laboratório de informática, cyber café, agência bancária ou repartições. Esses cabos são compostos por fios de cobre que transmitem através de impulsos elétricos.

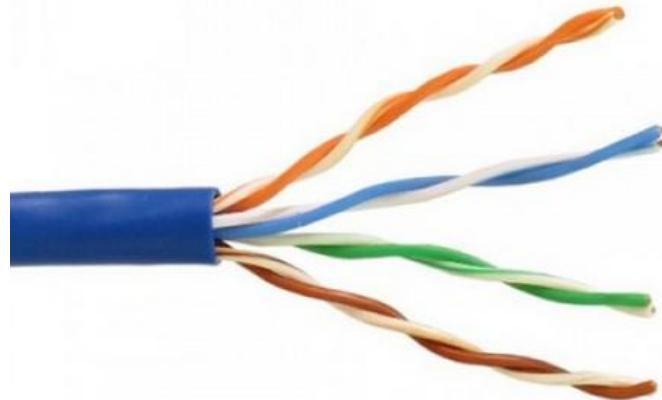


Mas porque "par trançado"???

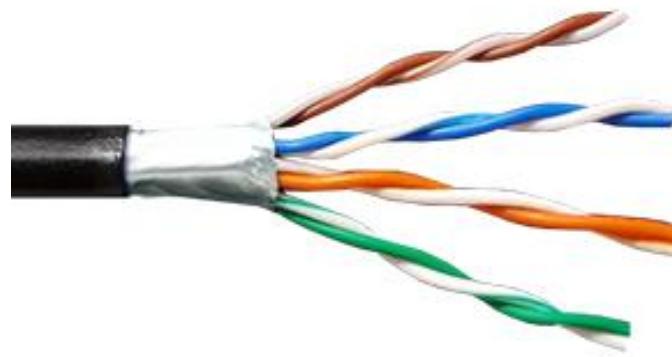
Em todo fio, por onde passa corrente elétrica, cria-se um campo magnético ao redor do mesmo. Esse campo magnético causa interferências eletromagnéticas em fios que estejam próximos e em paralelo. Interferência eletromagnética é uma das grandes causas de problemas em uma rede, podendo fazer com que dados não cheguem ao seu destino e causando instabilidade na rede.

Para tentar diminuir os problemas com a interferência eletromagnética, os fios são enrolados dois a dois, ou seja, em pares. Os pares também são entrelaçados entre si. Este procedimento faz com que diminua a ação da interferência. Além disso, nas redes de até 1000Mb de velocidade, um fio que transmite informação deve ser trançado a um fio que não transmite, ou fio neutro, pela norma EIA/TIA 568 (a qual estudaremos mais adiante).

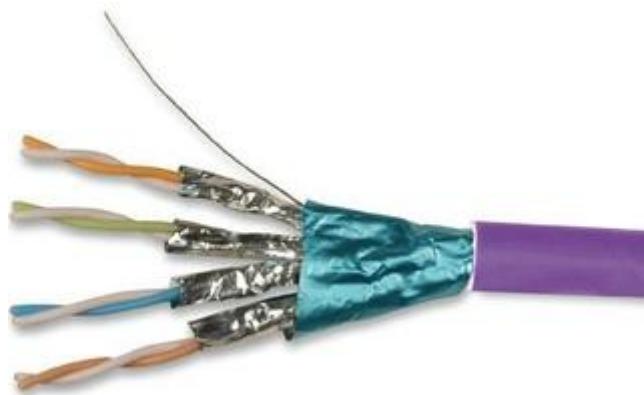
Existem várias categorias de cabo par trançado, onde podem variar a quantidade interna de fios de cobre e a forma de proteção desses fios. Os cabos de par trançado são classificados em três tipos básicos:



- UTP (Unshielded Twisted Pair) – São cabos que não possuem blindagem, ou seja, não existe proteção a interferências externas. Os fios de cobre são protegidos somente por uma capa de plástico (a cor azul não é padrão, mas é a mais comum no mercado). Os cabos UTP possuem taxas de transmissão que vão de 10Mbps a 10Gbps em redes locais.



- FTP (Foiled Twisted Pair) – São cabos que possuem uma blindagem feita com uma folha de alumínio que envolve todos os pares e que protege os fios evitando interferências com cabos da rede elétrica ou motores próximos ao cabo. Essa blindagem é de um tipo mais simples em relação ao STP.



- STP (Shielded Twisted Pair) – São também blindados, mas tornam-se mais eficientes que os FTP, pois sua blindagem é feita a cada par de cabos, ajudando assim a reduzir tanto a interferência externa quanto a interna, ou crosstalk, que é a interferência entre os pares de cabos.

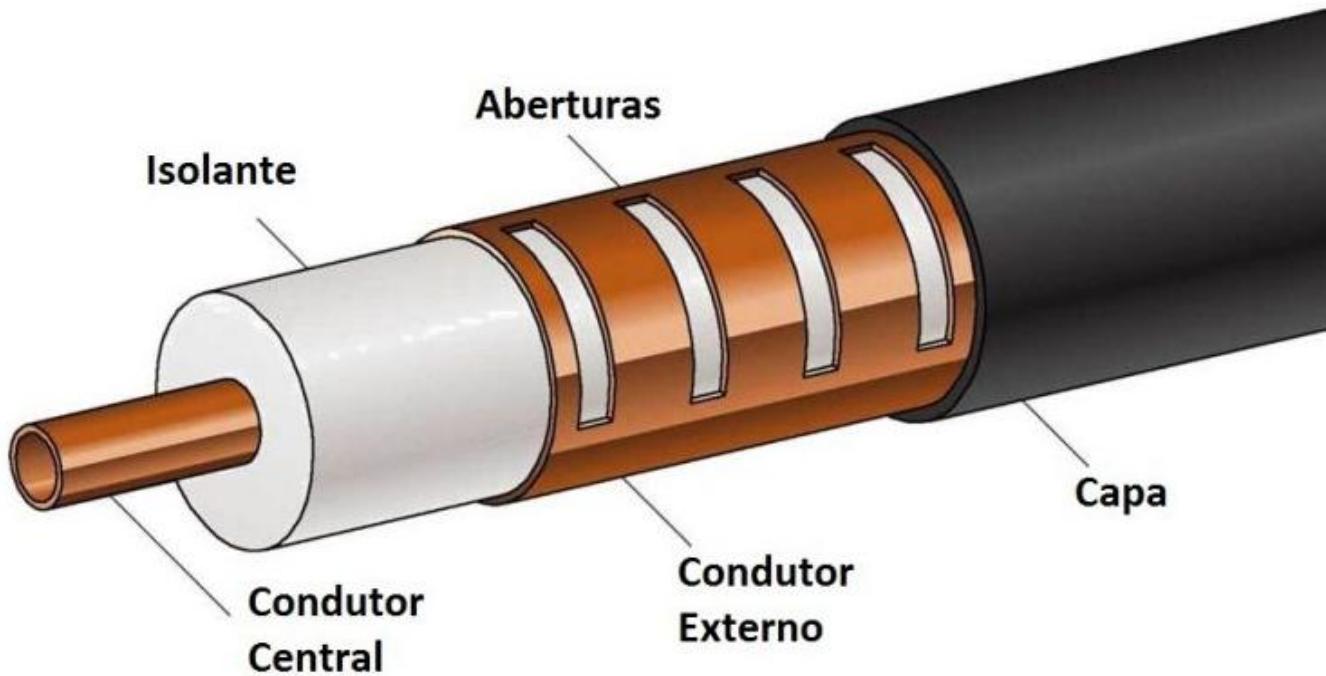
2.1.2. Cabos Coaxiais

Os cabos coaxiais antecederam os cabos de par trançado na conexão de redes, mas hoje são mais utilizados para transmissão de sinal de TV a cabo. O cabo coaxial possui dois condutores e possui uma blindagem entre os condutores permitindo uma boa taxa de transmissão e poucas perdas. Os cabos coaxiais podem ser classificados por sua impedância, ou seja, sua resistência à passagem de corrente elétrica. Quanto menor a resistência, melhor a transmissão pelo cabo, já que o corrente irá fluir mais rapidamente.

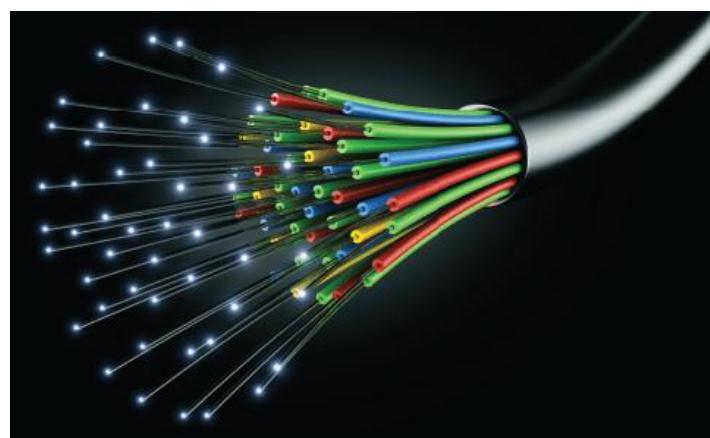
Os mais comuns são os de 75ohms, usados normalmente para antenas de TV

Informática – Redes de Computadores

e os de 50ohms, que possuem resistência menor e portanto são mais utilizados para telefonia celular.

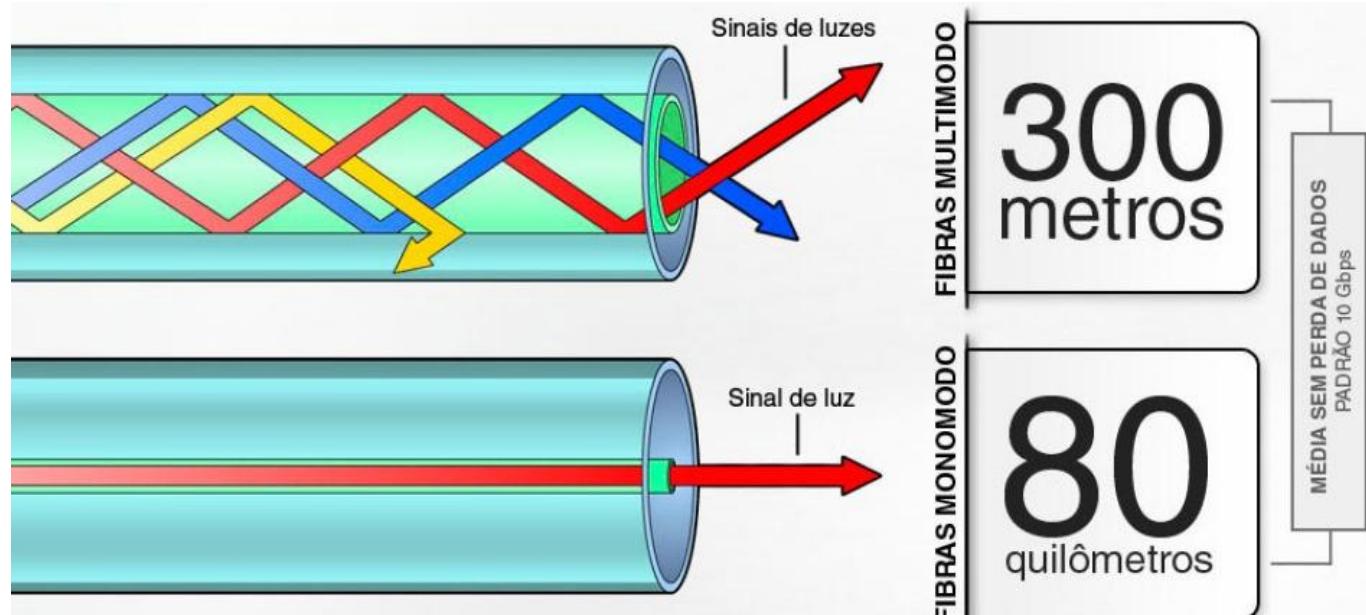


2.1.3. Fibras Ópticas



A fibra ótica é um fino e flexível fio de vidro feito de sílica, componente derivado do silício, que, diferente dos cabos elétricos, transmite dados a partir de feixes de luz. Como a velocidade da luz é bem elevada, a transmissão dos dados é muito melhor na fibra ótica, podendo chegar a 16Tbps. A fibra ótica é preferencialmente utilizada em redes de longa distância e de alta velocidade, pois não sofrem com interferências eletromagnéticas e possui perca mínima, sendo muito utilizada em empresas de telefonia e televisão, onde em ambas existe a necessidade de que o som e/ou a imagem cheguem em tempo real e em perfeita sincronia.

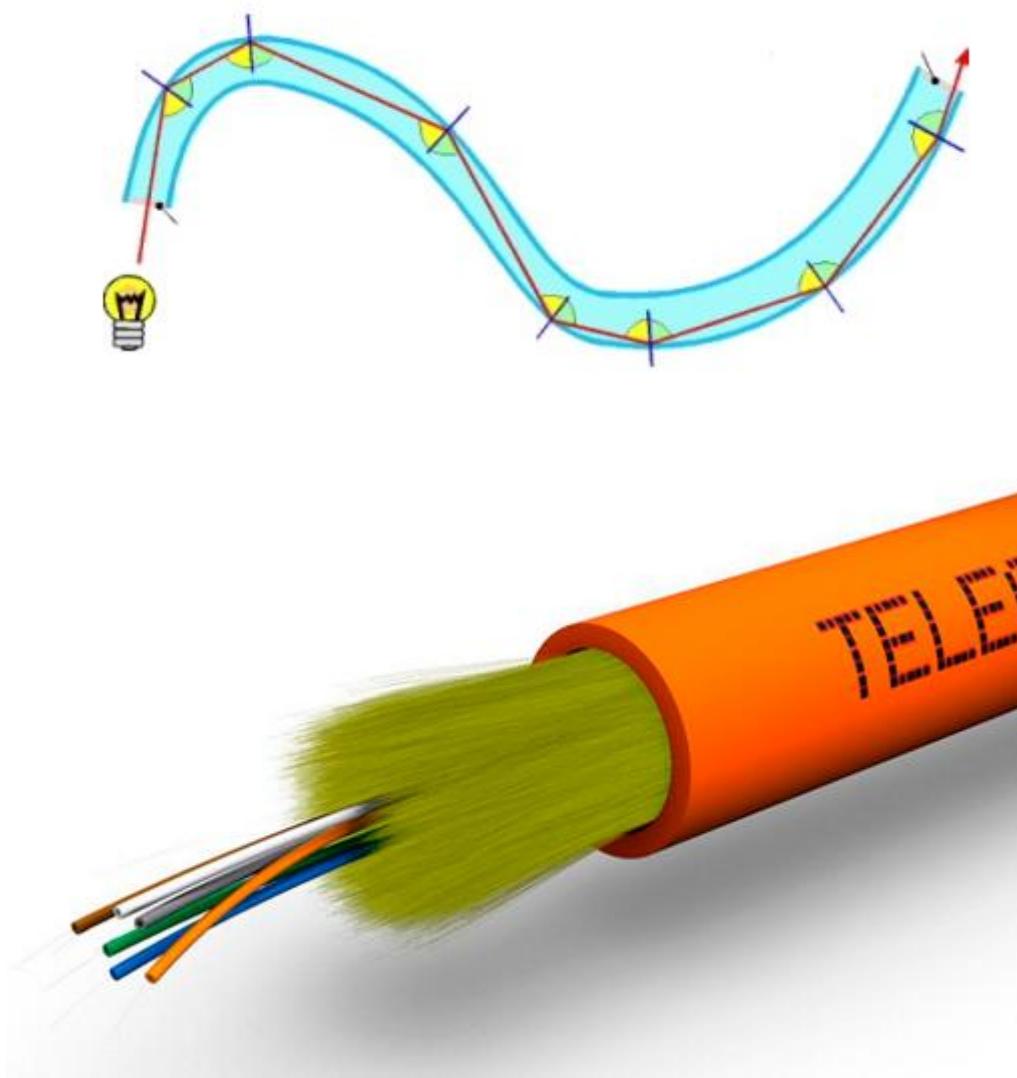
Existem dois tipos de fibras ópticas: as multimodo e as monomodo.



Nos cabos de fibra monomodo, o núcleo da fibra é tão fino que permite que a luz se propague em um único feixe e evitando também muitas reflexões nas paredes internas do cabo. Devido a isso o sinal em uma fibra monomodo pode propagar-se a até 80km de distância, mas fabricar um cabo de fibra tão fino

(cerca de 0,008mm) é muito dispendioso, tornando o cabo muito caro.

Nos cabos multimodo, o núcleo da fibra é mais espesso (cerca de 0,125mm), tornando sua fabricação mais barata, porém a espessura do cabo permite mais reflexões de sinal, e consequentemente mais perdas. A fibra multimodo alcança de até 550m com prováveis perdas de dados em sua transmissão devido seus pontos de reflexão nas paredes do núcleo.



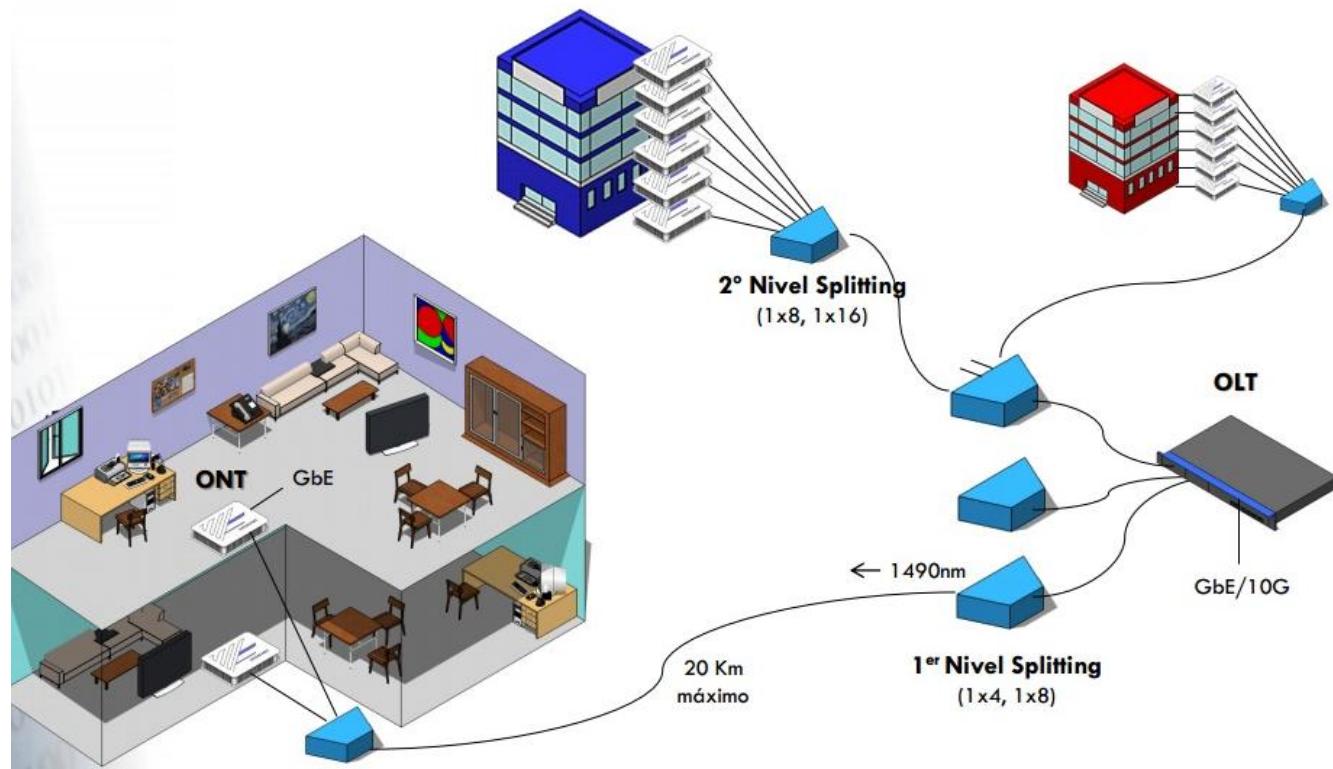
FTTH

FTTH (Fiber-to-the-Home) é a tecnologia que atualmente as operadoras estão utilizando para levar banda larga para o mercado consumidor. O FTTH possibilitará o transporte simultâneo de uma série de serviços, tais como Internet com acesso muito mais rápido, telefonia e televisão, através de uma única fibra óptica. Com o FTTH, a rede de acesso será baseada na fibra e capaz de prover velocidades a partir de 100Mb/s, chegando a até 40Gb/s. Existem novas tecnologias DWDM, com alto controle de PMD – Polarization Mode Dispersion permitem atingir essa incrível marca. Isto criará uma rede de acesso com inúmeras

possibilidades. Esta tecnologia suportará um modelo aberto completo pelo qual o consumidor terá total liberdade de escolha pelo seu fornecedor de serviço.

GPON

GPON (Giga Passive Optical Networks), uma rede óptica passiva com capacidade Gigabit. Está topologia é derivada das redes ópticas passivas (PON – Passive Optical Networks), o qual surgiu em função da redução nos custos de operação e manutenção quando comparadas com as outras arquiteturas. Sua arquitetura é ponto-multiponto e usa um ou mais níveis de acopladores ópticos passivos para distribuir o sinal aos clientes. O acesso ao meio de transmissão é TDMA, ou seja, por meio de multiplexação no tempo. Desta forma é possível compartilhar o mesmo meio físico com vários usuários e diferentes serviços.

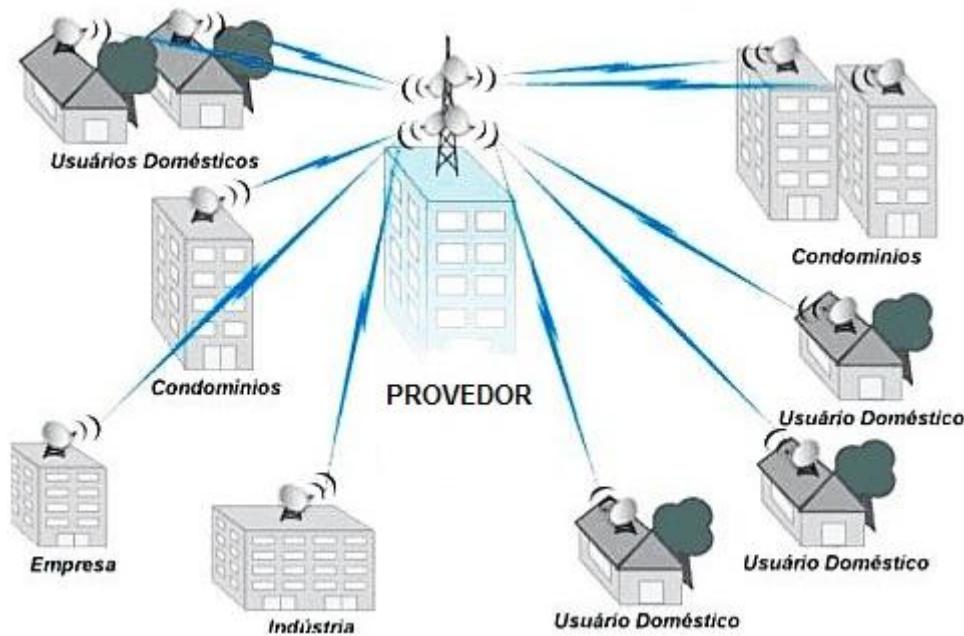


2.1.4. Transmissão via rádio terrestre ou microondas

Os sinais de rádio estão num espectro eletromagnético sem utilização de fios e podem atingir grandes distâncias. Porém estas distâncias variam conforme as condições do local, que pode possuir muitas barreiras físicas ou sinais eletromagnéticos gerando perda e atenuação do sinal, o que pode impedir sua propagação.

Para a propagação são instaladas torres que funcionam como estações repetidoras de microondas. Essas

torres devem sempre estar “enxergando” a próxima, pois a transmissão se dá em linha reta de uma torre à outra. Um exemplo de tecnologia que utiliza freqüências de rádio é a telefonia celular.



- Transmissão de internet via rádio.



- Estação rádio base telefonia celular.

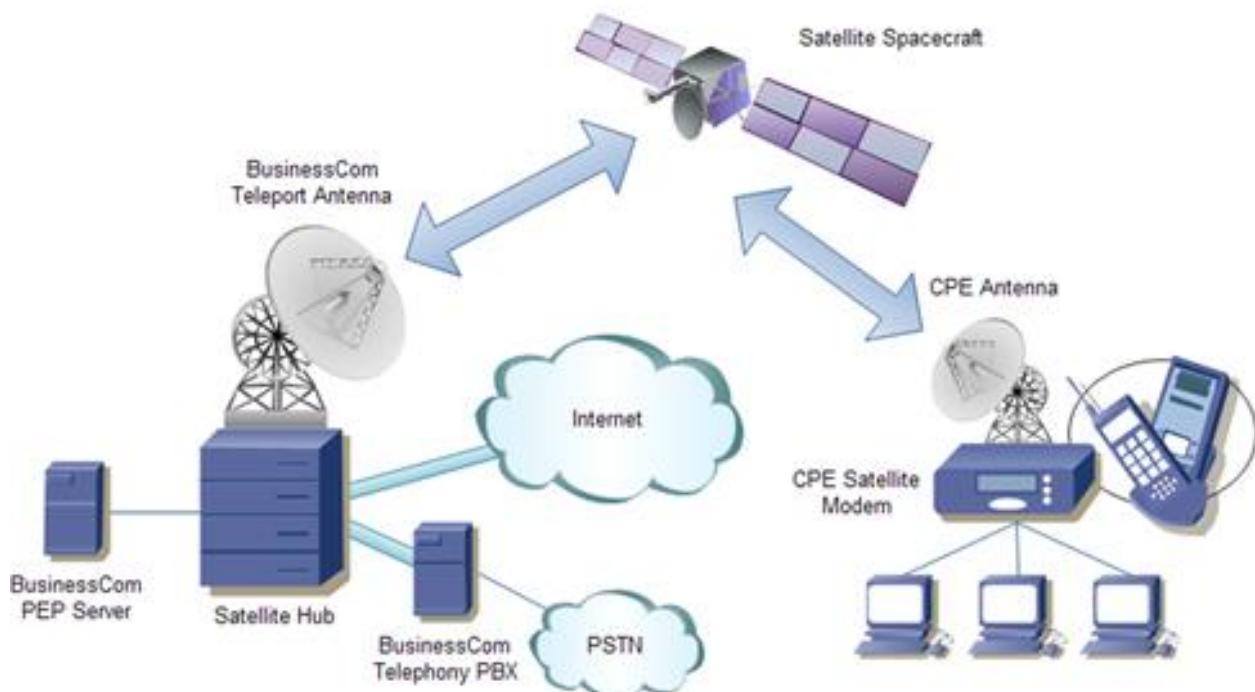
PESQUISA

Pesquise os tipos de equipamentos (não obrigatoriamente meios de comunicação) que utilizam ondas de rádio em seu funcionamento.

2.1.5. Transmissão via Satélite

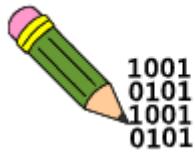
Um satélite liga várias estações repetidoras de microondas as quais citamos anteriormente. Com isso, o satélite é capaz de ligar uma estação terrestre X a outra estação terrestre Y que esteja distante, sem que o sinal tenha que trafegar por todas as estações terrestres vizinhas a X até chegar à estação destino Y. Como isso acontece? Imagine a seguinte situação: Carlos quer fazer uma ligação de Fortaleza, onde reside, para sua prima Joana em Porto Alegre. Ao efetuar a chamada, o sinal do telefone de Carlos procura a estação repetidora terrestre mais próxima em Fortaleza e ao chegar lá, o sinal é enviado ao satélite que por sua vez

localiza e reenvia a chamada para a estação repetidora terrestre mais próxima de Joana em Porto Alegre.



PESQUISA

Existem alguns tipos de satélites: os GEOS, os LEOS e os MEOS. Pesquise a diferença entre eles e que empresas brasileiras usam satélites.



Exercícios

1. Marque V para verdadeiro e F para falso:

- () Em uma rede sem fio o meio pelo qual os dados trafegam é o ar.
- () Nas fibras ópticas a propagação dos dados é feita através da luz.
- () A fibra óptica do tipo monomodo possui o núcleo tão fino que atrapalha a propagação da luz.

2. Cite os meios de transmissão que utilizam a energia elétrica para a propagação dos dados.

3. Que tipo(s) de cabo(s) de par trançado devemos utilizar em ambientes próximos a grandes antenas de transmissão?

4. Por que os cabos UTP, FTP e STP possuem os pares trançados entre si?

5. Onde encontramos mais facilmente uma instalação feita com cabo coaxial?

6. Diferencie fibra óptica monomodo e fibra óptica multimodo.

7. Por que a transmissão na fibra óptica é mais rápida que nos outros meios de transmissão?

8. Suponha que você foi contratado para instalar uma rede de computadores em um prédio tombado como Patrimônio Histórico, onde as paredes não podem ser quebradas. Que meio de transmissão você utilizaria para melhor atender à solicitação? Como você explicaria para seu cliente a vantagem da escolha feita?

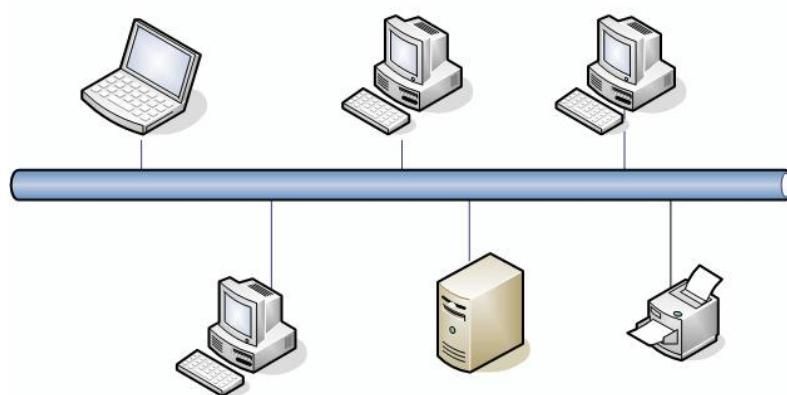
3.0 TOPOLOGIAS

3.1. Topologias de Redes

A topologia de uma rede nada mais é do que a forma como se define o layout da rede, ou como se organiza estruturalmente os computadores, dispositivos de rede e suas conexões. Uma topologia pode física ou lógica. A topologia física é como os computadores e dispositivos se encontram fisicamente, configurando uma espécie de desenho que é caracterizado pela disposição dos equipamentos. A topologia lógica é a forma como os dados trafegam na rede, logo, uma rede pode obedecer a uma determinada topologia apenas de forma lógica, não sendo necessário que os equipamentos estejam organizados de acordo com a topologia física. Há varias formas de se estruturar uma rede, veja as principais:

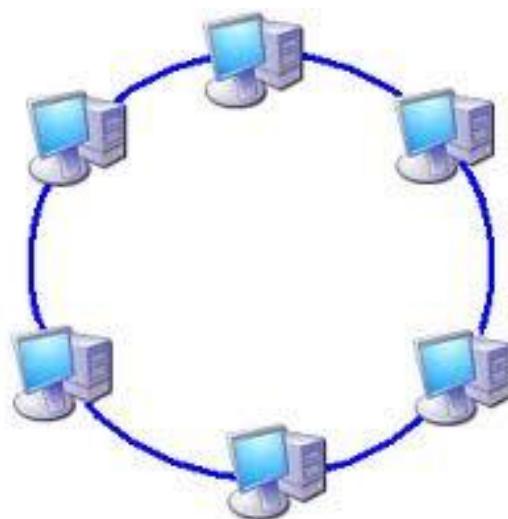
3.1.1. Barramento

Na topologia em barramento cada computador é ligado em série, ou seja, um computador atrás do outro em fila, no mesmo meio físico de transmissão de dados. Devido ao fato de todos os computadores compartilharem o mesmo meio de transmissão, só é possível transmitir os dados de um computador por vez. Quando há algum computador transmitindo dados, o meio fica “ocupado” naquele momento. Durante a transmissão todas as máquinas da rede recebem os dados, mesmo que a mensagem seja destinada a apenas uma. Neste momento, se algum outro computador da rede tentar transmitir, acontecerá uma colisão e todo o tráfego deverá ser refeito.



3.1.2. Anel

Na topologia em anel, assim como em barramento, os computadores também são ligados em série, porém formam um anel, como na figura abaixo:



Na topologia em anel (também chamada de Token-Ring), os dados são transmitidos de computador em computador através de um único meio de transmissão e de forma unidirecional. Ocasionalmente, podem acontecer colisões quando mais de um computador envia dados em um mesmo momento. Para resolver este problema, são usados os Tokens. O Token é como se fosse um passaporte para a transmissão: apenas quem o possui, pode enviar dados. Desta forma cada computador tem sua vez de transmitir e precisa aguardar o Token chegar novamente para continuar transmitindo.

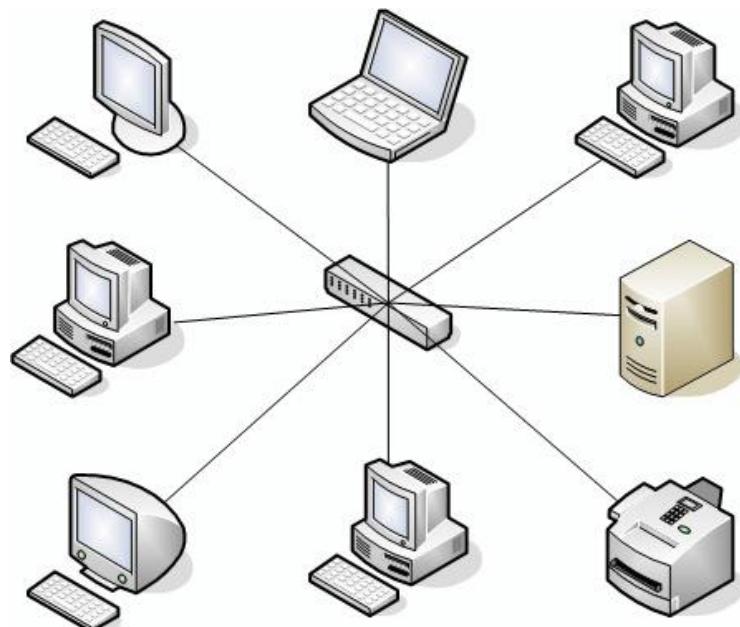
Quando alguma mensagem é transmitida, ela passa por todos os computadores do anel até encontrar o computador de destino. Quando isso acontece o computador que enviou a mensagem passa a vez, ou o Token, para o seu computador vizinho para que ele possa transmitir. Mesmo que o computador não tenha nada a transmitir, ele vai receber o Token e passar determinado período de tempo com ele para em seguida passá-lo ao próximo computador e assim por diante.

A topologia em anel é uma das mais seguras, mas em contrapartida, possui algumas desvantagens:

- caso um dos computadores apresente problemas com a transmissão, toda a transmissão da rede será comprometida.
- Devido o uso do Token, se a rede possuir muitos hosts, estase tornará lenta, já que quanto mais computadores houver na rede, mais o Token vai demorar a chegar a cada host.

3.1.3. Estrela

Na topologia em estrela é utilizado um ponto central ou ponto concentrador que normalmente é um hub, switch ou roteador. Neste caso o ponto central é responsável por retransmitir os dados vindos do computador de origem para o computador de destino.



Em analogia com a topologia em anel, se algum computador da rede apresentar problemas com a transmissão, somente ele é desativado da rede e o restante dos computadores continua enviando e recebendo dados normalmente. Da mesma forma, quando é necessário adicionar um host, basta fazer a conexão, caso haja espaço no concentrador. Este processo não interferirá no andamento da rede e nenhum equipamento precisará ser desligado. A topologia em estrela, usando um switch, ou equipamento superior, permite mais de uma transmissão ao mesmo tempo caso as transmissões envolvam enlaces diferentes.

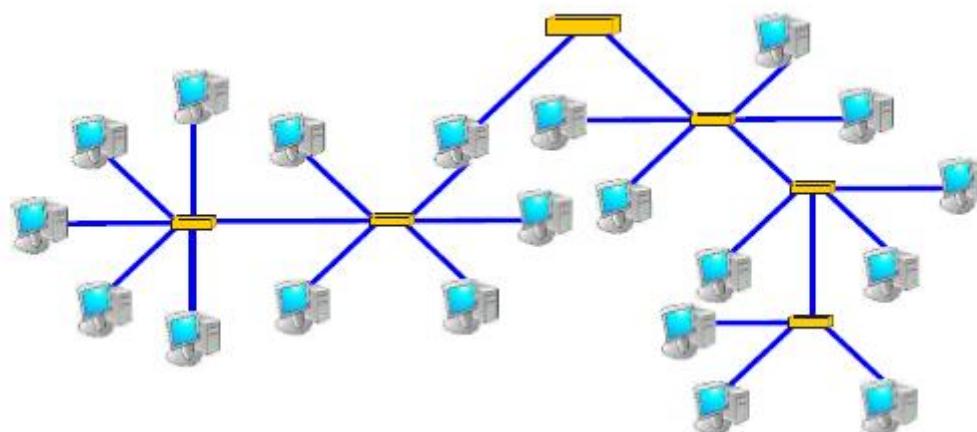


ENLACE

É um link de comunicação, ou uma ligação entre dois sistemas de rede. Por exemplo, a ligação entre um computador e um roteador ou a ligação entre dois roteadores em redes locais diferentes.

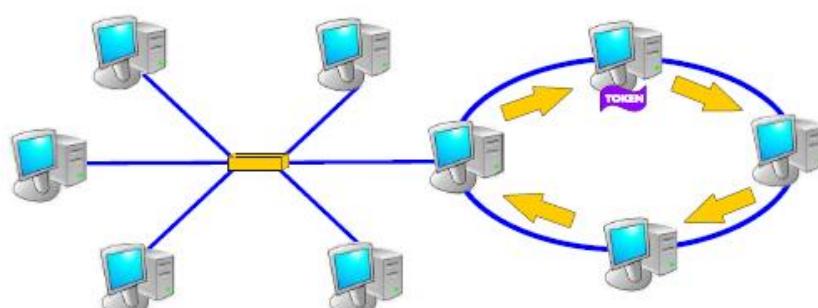
3.1.4. Árvore

A topologia em árvore caracteriza-se por possuir um ponto central onde são conectadas várias ramificações. Nesta topologia existem mais de um concentrador, criando sub-redes, normalmente em forma de estrela. Existem níveis hierárquicos em relação aos concentradores, dado que, em uma transmissão de sinal de internet, por exemplo, acontecendo um problema com um concentrador em um nível mais acima na rede, os concentradores abaixo serão afetados, a não ser que existam estruturas de redundância. Em contrapartida, um problema em um concentrador de nível mais baixo, não afetará a rede por completo, podendo parte dela continuar funcionando normalmente. Provavelmente em sua escola esta topologia seja usada para interligar um ponto central a setores como secretaria, coordenação, laboratórios e etc.



3.1.5. Híbrida

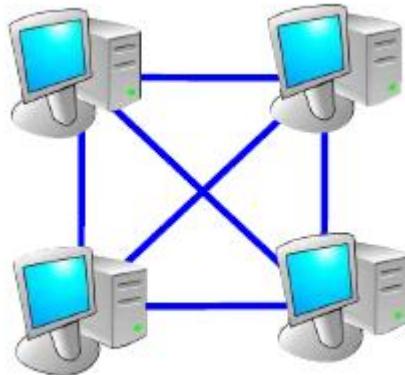
A topologia híbrida é a junção de duas ou mais topologias diferentes. Ela é muito utilizada em empresas em constante crescimento onde a rede pode variar em função do local de trabalho, da quantidade de computadores, dos custos que certa topologia poderia gerar ou do número flutuante de computadores que podem aumentar ou diminuir com a necessidade. Nestes casos vale a pena avaliar as vantagens das outras topologias e utilizar os equipamentos disponíveis naquele momento da empresa.



3.1.6. Ligação Total – Malha

A topologia em Malha, também conhecida como Mesh, tem como característica a formação de uma malha de ligações entre os hosts da rede. Em uma topologia em Malha é possível sair de cada nó da rede, uma ou mais ligações para os outros nós. A quantidade de ligações que saem de um host pode variar de acordo com a rede. É uma topologia mais incomum em relação às outras, porém é a mais segura.

Existem dois tipos de topologias em malha: a Parcial e Total. Na Parcial um ponto da rede possui ligações com vários nós, mas não necessariamente com todos. Na Total, ou Full-Mesh, cada nó da rede possui, obrigatoriamente, uma ligação para cada outro nó da rede, fazendo assim com que, se um rede possui n nós, de cada nó sairá $n-1$ ligações. Este último tipo oferece velocidade e disponibilidade maiores, porém é muito cara.



3.8. Sem fio

A topologia sem fio baseia-se em comunicações através de ondas de radiofrequência. Nela, não é necessário o uso de fios para fazer uma ligação entre dois ou mais nós da rede, fato este que tornou este tipo de rede conhecida como rede wireless, ou seja, sem fios.

Na topologia sem fio, podemos ter a presença de um ponto de acesso, ou access point, que fará a recepção dos sinais enviados pelos hosts e o envio ao receptor de destino. O ponto de acesso faz na rede sem fio, basicamente, a função que um switch faz na rede cabeada. Podemos ter uma topologia de rede sem fio que não utiliza ponto de acesso: a rede ad-hoc. Nas redes ad-hoc, os hosts transmitem dados entre si, utilizando-se de suas próprias placas de rede sem fio. Obviamente, os equipamentos devem estar próximos um do outro, pois a propagação do sinal entre suas antenas é curta. Não é um tipo de rede muito utilizada, pois a transmissão é feita em half-duplex e torna-se muito lenta a medida em que adicionamos equipamentos na rede.

Um exemplo muito comum de rede ad-hoc é a transmissão de arquivos entre aparelhos celulares via Bluetooth.



PESQUISA

- Que topologia de rede é utilizada no laboratório de informática de sua escola?
 - Você considera esta topologia adequada ao local pesquisado?
 - Caso não considere, informe qual topologia você utilizaria e por quê.



Exercícios

1. Em sua opinião, qual a importância de se organizar o layout físico de uma rede?

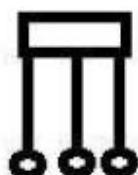
2. Defina e explique os termos abaixo:

a) Topologia física

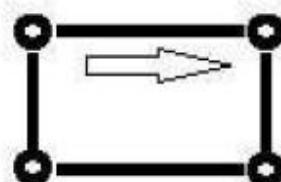
b) Topologia lógica

3. Indique a topologia usada nos esquemas abaixo:

a)



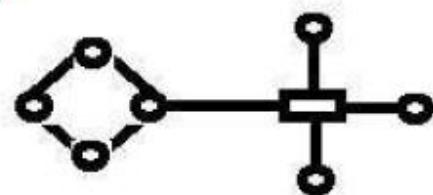
b)



c)



d)



4.0 Escopos de uma rede

LAN's, MAN's, WAN's e PAN's. Nomes que até então eram estranhos, passarão a fazer parte de nosso cotidiano técnico junto aos nomes dos equipamentos utilizados numa topologia de redes de computadores.

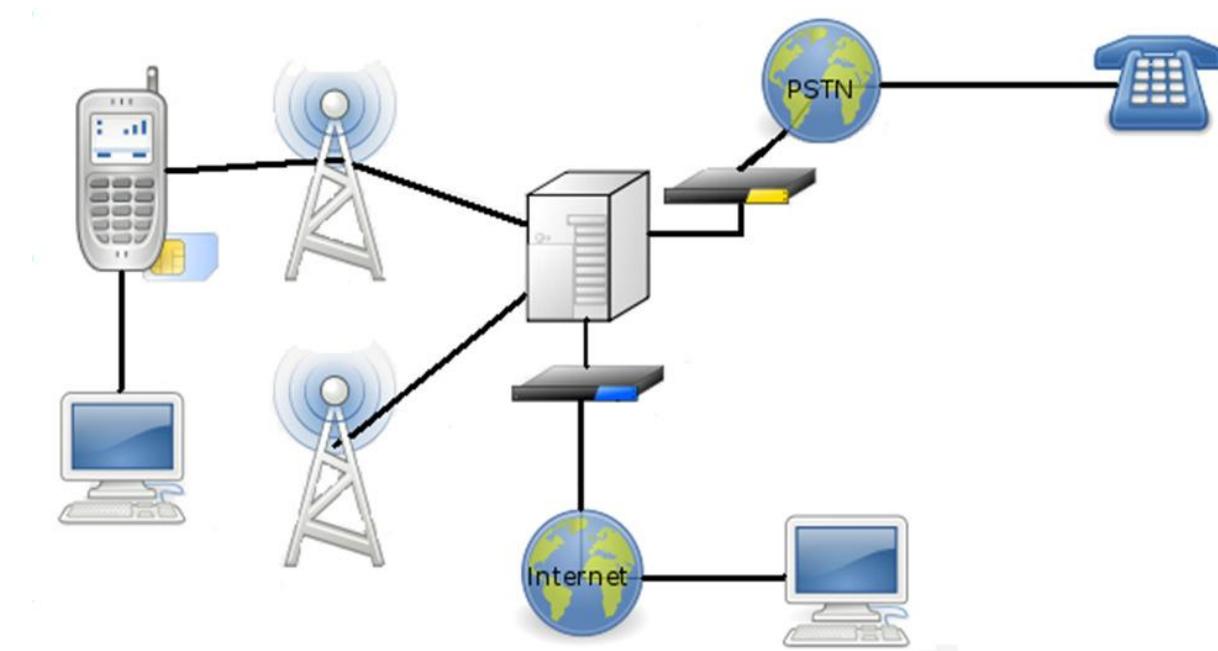
Estudaremos aqui como se classificam as redes e seus componentes em função de suas disposições física/lógicas e tecnologias utilizadas.

As redes de computadores estão presentes em nossa vida diária. Assim, ficamos tão habituados com estas, que muitas vezes as utilizamos automaticamente, sem perceber a complexidade e sofisticação presente nas infraestruturas e das tecnologias responsáveis pela circulação das informações.

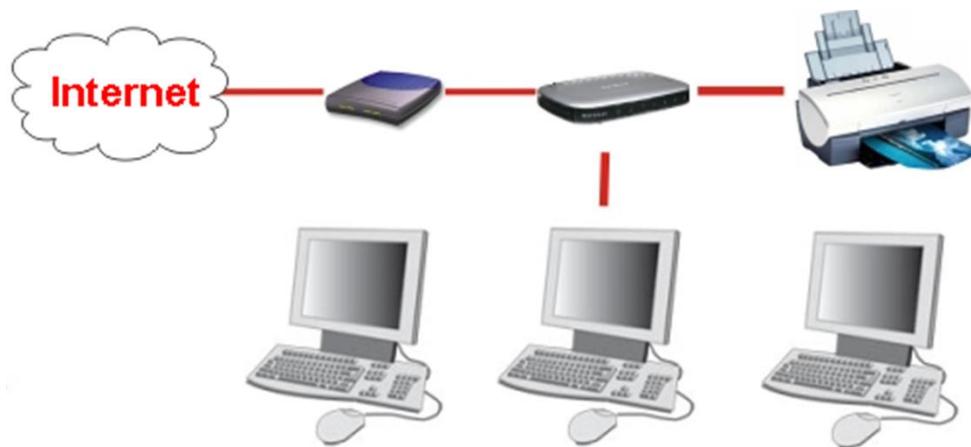
4.1. Redes divididas geograficamente

Analisamos que os componentes que compõem uma rede podem estar numa mesma sala ou espalhados nos andares de um prédio, estando localizados a quilômetros de distância um do outro e conectados através de linhas telefônicas dedicadas, micro-ondas ou qualquer sistema que permita uma troca de dados. Eles podem estar espalhados pelo planeta, sendo interligados por alguma tecnologia para comunicações a longa distância.

Ao analisarmos como as redes de computadores são estudadas e planejadas geograficamente, veremos que estas podem ser classificadas em: LAN, MAN, WAN e PAN.



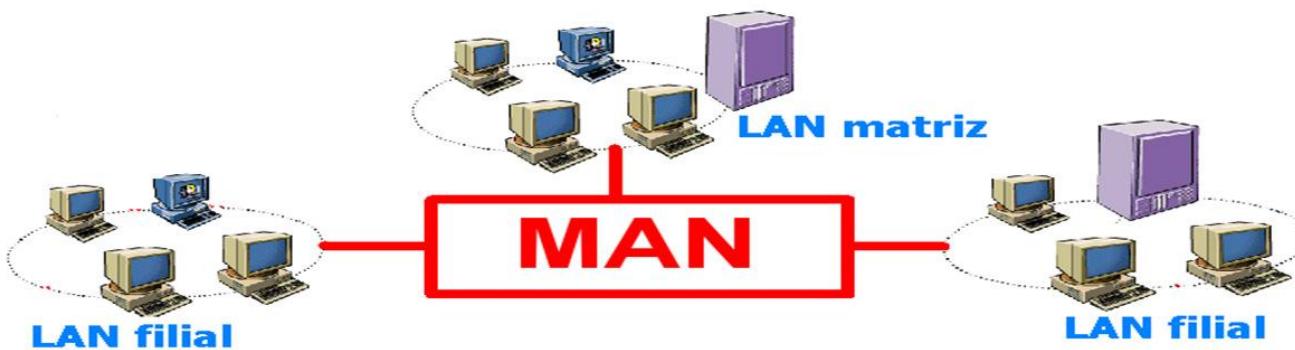
4.1.1. LAN (Local Area Network)



Uma rede de área local é uma rede de computador utilizada na interconexão de equipamentos processadores com a finalidade de troca de dados.

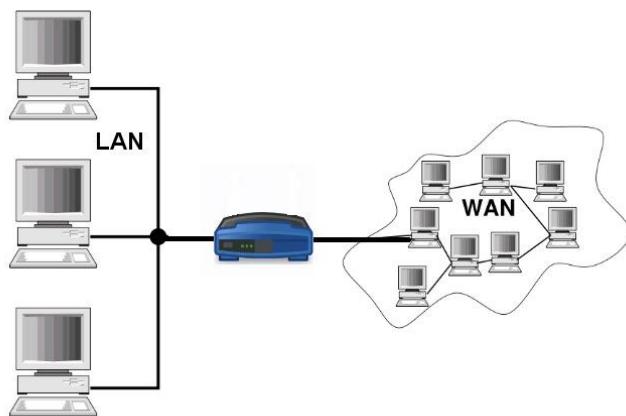
Uma definição mais completa afirma que uma LAN é: uma estruturada de hardware e software que permite a computadores individuais realizarem comunicações entre si, para trocar e compartilhar recursos e informações. Tais redes são denominadas locais, por abrangerem um espaço geográfico limitado (Compreendendo uma área de até 10 Km. Se este limite for alcançado, a rede passa a ser denominada Rede Metropolitana).

4.1.2. MAN (Metropolitan Area Network)



Uma MAN ou rede de área metropolitana são redes que abrangem o perímetro de uma cidade (por isso são chamadas áreas metropolitanas), desse modo são utilizadas por empresas objetivando comunicar-se com suas filiais, quando estas estão localizadas em bairros diferentes. Empresas como grandes grupos de varejo, companhias áreas, bancos, universidades públicas, etc, possuem suas redes internas interligadas por meios de MAN's.

4.1.3. WAN (Wide Area Network)



WAN (Rede de longa distância ou geograficamente distribuída) é uma rede que abrange uma grande área geográfica, sendo uma região, podendo abranger ainda um país ou até um continente. Em geral, as redes geograficamente distribuídas contêm conjuntos de servidores, que formam sub-redes. Essas sub-redes têm a função de transportar os dados entre os computadores ou dispositivos de rede. As WAN tornaram-se necessárias devido ao crescimento das empresas, nas quais as LAN não eram mais suficientes para atender a demanda de informações, pois era necessária uma forma de passar informação de uma empresa para outra de forma rápida e eficiente. Surgiram as WAN que conectam redes dentro de uma vasta área geográfica, permitindo comunicação de longa distância.

WANs utilizam variados meios de transmissão, como: linhas telefônicas, micro-ondas, ou satélites, contudo o mais popular é a fibra óptica. Lembrando que LANs e WANs são redes privadas. Logo, estas interconectam as pessoas dentro de suas organizações.

Agora, se analisarmos a Internet, esta é uma gigantesca WAN pública. A Internet une PC's em universidades, centros de pesquisa e companhias pelo globo.

Como as redes tornaram-se mais poderosas e são conectadas mais empresas e usuários domésticos diariamente, a Internet servirá como um ponto de contato entre a sua companhia, seus fornecedores e clientes.

2.1.4. Personal Area Network e Wireless Personal Area Network



PAN (Personal Area Network) é uma rede caracterizada por estações bastante próximas umas das outras (comumente sem exceder dez metros). Assim, uma rede de área pessoal pode ser formada por exemplo: por um computador portátil, conectando-se a um outro e este a uma impressora. São exemplos de PAN as redes do tipo: Bluetooth e Ultra Wide Band (UWB).

O UWB é uma tecnologia que faz parte das redes Wireless Personal Area Network (WPAN). Uma WPAN é uma rede composta por dispositivos pessoais que usam tecnologias wireless para transmissões de curto alcance.

A topologia física de uma rede descreve como é o layout do meio de transmissão pelo qual ocorre as transmissões das informações, e também como os dispositivos presentes na rede são conectados ao próprio meio. Há várias possibilidades para organizar a interligação entre cada um dos computadores (estações e servidores) numa rede.

Deve-se lembrar que topologias divididas em dois tipos: Topologias física e lógica. A topologia física é o designer da rede ou sua aparência física propriamente dita, já a topologia lógica representa o modo que as transmissões de informações fluem pela rede.

4.2 Mainframes, terminais burros e clientes magros

4.2.1. Mainframes

Mainframes são computadores de grande porte que devido ao seu alto custo são utilizados em atividades

que necessitam de um alto poder de processar grandes volumes de informações. Estes computadores oferecem serviços de processamento para milhares de estações por meio de terminais conectados diretamente a eles ou através de infraestruturas de rede.



4.2.2. Terminais burros



Um terminal burro refere-se a um computador que atua como uma interface entre o usuário e um equipamento responsável pelo processamento requisitado pelo usuário, normalmente este dispositivo é um mainframe.

Desde modo, um terminal burro é um sistema com um hardware simplificado; ele não possui disco rígido,

e todo o processamento depende de um mainframe. Nos modelos mais antigos eram compostos por um monitor e teclados conectados por uma estrutura de rede ao mainframe. Por isso, esse é o nome utilizado no Brasil – Terminal “burro” (o nome deste, em inglês, é: computer terminal ou text terminal).

4.2.3. Clientes magros (thin clients)



Um Cliente magro (“thin client”) é um computador cliente que não possui nenhum ou apenas alguns aplicativos instalados. Assim, estes estão em rede de modo que possam utilizar os recursos de um computador servidor para a grande maioria das atividades de processamento que o cliente magro necessite realizar.

O termo "magro – thin" faz referência a um pequeno programa de boot que os thin clients necessitam, algumas vezes apenas o essencial para conectar-se à rede e executar um navegador da Internet dedicado ou uma conexão para uma Área de Trabalho Remota.

Já o thick (ou fat) client realiza a maior quantidade de processamento e repassa ao servidor apenas as requisições necessárias de operações que o fat client não pode executar. Como os terminais burros os clientes magros são computadores sem disco rígido (diskless), planejados para terem tamanho reduzido e um baixo custo em comparação com os PC's tradicionais. Assim, quase o grosso do processamento dos thin clients é executado no computador com um hardware muito mais potente (server), logicamente o cliente magro executa aplicativos que oferecem recursos de rede.

Assim, clientes magros são conectados a servidores de aplicativos para que estes forneçam os meios requeridos pelos usuários, logo este tipo de PC (thin client) possui apenas o hardware e software para

executar o boot e acessar a Internet.

O servidor de aplicativos normalmente é um computador com o hardware dimensionada para tais tarefas com um sistema operacional de rede para servidores que podem ser alocados numa Wide Area Network (WAN), Metropolitan Area Network (MAN) ou até numa Local Area Network (LAN).

Pode-se citar como vantagens em utilizar clientes magros:

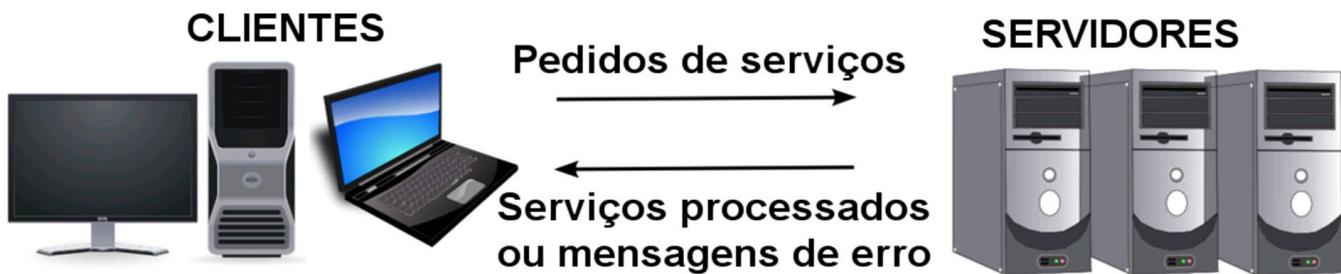
- Mais fácil de mantê-los seguros;
- Possuem um custo de administração menor;
- Gasta-se menos para licenciar os programas por eles utilizados;
- Menores despesas com o hardware;
- Consomem menos energia, dentre outras.

A principal desvantagem presente para aqueles que os utilizam é o fato de que, caso o servidor fique inoperante, todos os computadores conectados a ele ficarão incapazes de processar informações.



4.3 Arquiteturas cliente-servidor e Peer-to-Peer

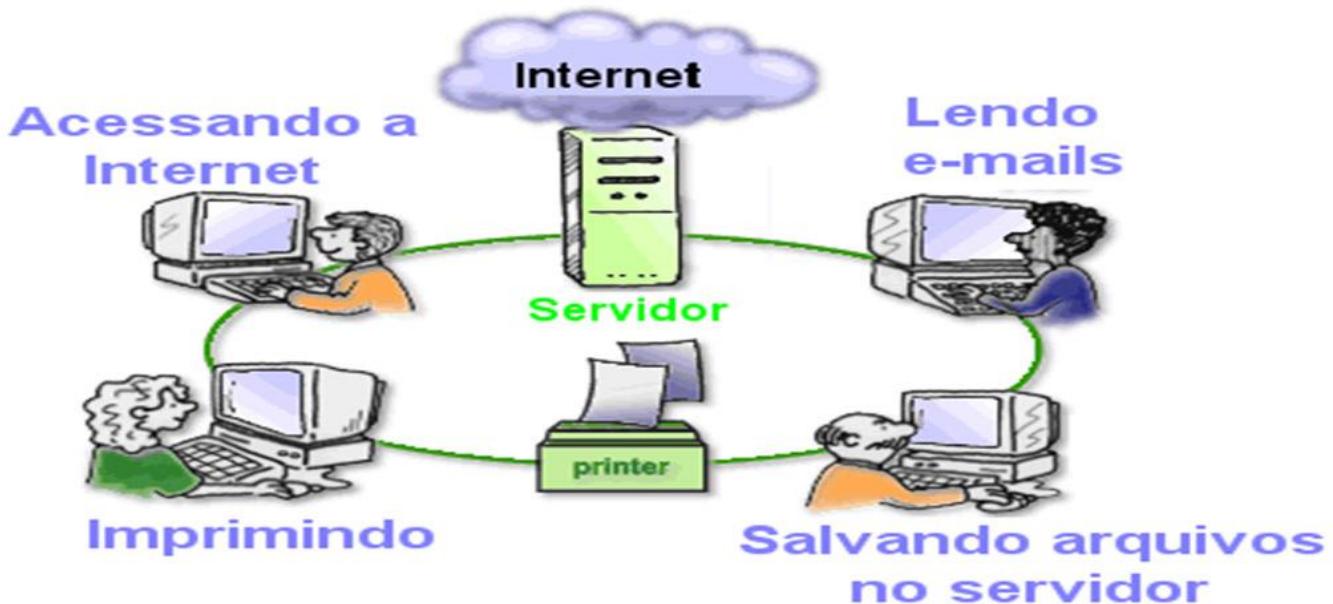
4.3.1. A arquitetura Cliente – Servidor



Cliente-servidor é uma arquitetura utilizada em redes de computadores onde existe uma divisão dos computadores em clientes e servidores. Os clientes enviam requisições de serviços para os servidores e esperam pelas respostas ou mensagens de erros.

Normalmente, os computadores servidores são projetados para atender as requisições, processá-las e retornar o resultado para inúmeros computadores clientes. Esse conceito é usado como várias variações, assim os mainframes (servidores) e terminais burros (clientes), clientes magros (clientes), servidores de e-mail, de páginas da Web, dentre outros são baseados nessa arquitetura para oferecimento de recursos.

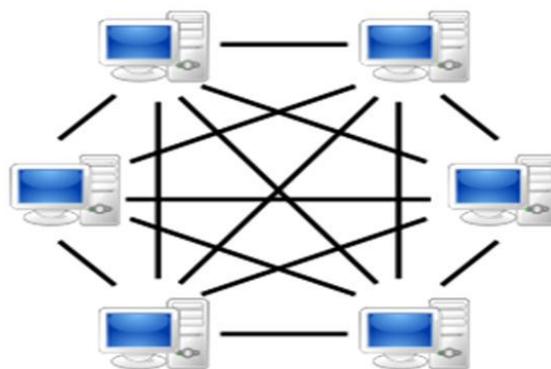
Assim, ao utilizar um navegador da Internet (software cliente) para acessar informações de uma página ou algum serviço, estes estão armazenados em um, ou, mesmo, vários servidores configurados especificamente para executar tais tarefas e repassá-las aos solicitantes.



Agora será que um computador pode ser tanto cliente como servidor? Para responder essa questão vamos

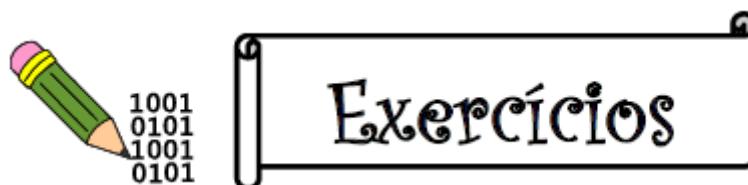
estudar a tecnologia peer-to-peer.

4.3.2. A arquitetura Peer-to-Peer



Na tecnologia Peer-to-Peer (Conhecida no Brasil como ponto-a-ponto ou p2p) cada computador é simultaneamente servidor e cliente, permitindo assim que recursos fossem compartilhados por um grande número de servidores (clientes), tornando dispensável a utilização de servidores específicos. Isso se tornou muito popular graças à diminuição da diferença de desempenho entre computadores, estações e servidores, além do crescimento crescente de pessoas com acesso a banda larga.

A popularização de programas do p2p foi possível devido à softwares como o Gnutella e o Napster que viraram febre para troca de arquivos entre os usuários, como serviços e informações passaram a estar acessíveis em nível global.



1. Quais são os três escopos de rede?

2. Que escopo de rede seria ideal para identificar uma ligação do tipo:

a) Dois computadores em uma residência.

b) Sedes de bancos em vários países.

c) Vários prédios de uma fábrica em um mesmo complexo industrial.

d) Uma loja e seu depósito localizados em bairros diferentes.

3. O que significa LAN?

4. Quais componentes fazem parte de uma LAN?

5. Diferencie MAN, WAN e PAN.

6. O que é WPAN?

7. Comente acerca das topologias em barra, anel e estrela.

8. O que são mainframes?

9. Defina terminal burro?

10. O que são clientes magros?

11. Comente acerca da tecnologia cliente-servidor.

12. O que é peer-to-peer?

Praticando!!!

- 1: Rede LAN ou PAN: Crie diagramas de uma rede pessoal ou de uma rede local (LAN), lembrando que uma rede PAN engloba dispositivo sem fio, como PDA's, Iphones, celulares, smartphones, netbooks, laptops, etc.
- 2: Topologias: Crie diagramas redes segundo as seguintes topologias: Rede em anel, em estrela ou em barra.
- 3: Arquiteturas: Crie esquemas de rede onde estejam representadas redes na plataforma cliente-servidor, peer-to-peer ou mainframe-terminais burros.

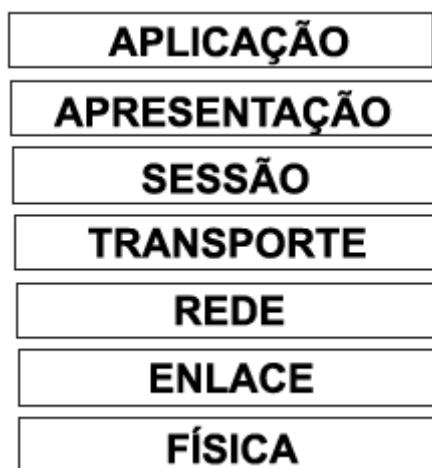
5.0 MODELOS OSI E TCP

Bem, já vimos que com as redes de computadores eu posso comunicar uma empresa, uma pessoa, ou um equipamento a inúmeros lugares do mundo. Todas as pessoas que acessam a internet, por exemplo, fazem parte de uma mesma rede (muito grande por sinal). A internet é uma rede de redes, onde o mapa dessa rede é tão complexo, que nós começamos a chamá-la de nuvem.

Entretanto, se você parar para pensar, a diversidade de marcas e de fabricantes de equipamentos de rede espalhados pelo mundo é descomunal. No início da internet não havia solução para este problema. As redes funcionavam isoladas e cada uma trabalhava com seus tipos de equipamentos do fabricante de sua preferência.

Para solucionar este problema, a ISO (International Organization for Standardization) criou um modelo de referência mundialmente conhecido como Modelo OSI (Open Systems Interconnect). Esse modelo trouxe uma padronização para o fluxo de informações nas redes, fazendo com que os fabricantes lançassem placas de rede, comutadores, roteadores, cabos e conectores de acordo com as normas, assim, todos poderiam se comunicar, pois estariam usando os mesmos protocolos. Trocando em miúdos, é como se todos passassem a falar o mesmo idioma.

Veja, a seguir, como é o modelo de Referência OSI:



Como se pode notar, o modelo OSI é dividido em sete partes, as quais chamamos de camadas, onde:

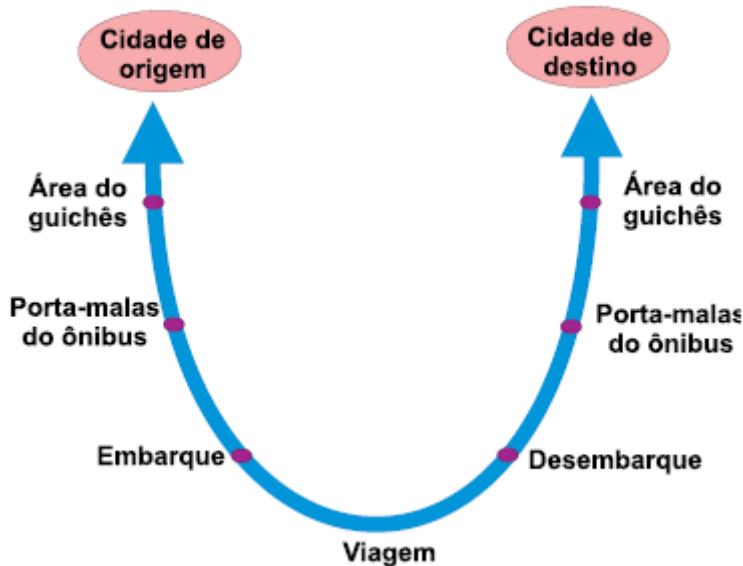
- Cada camada tem a sua função.
- Cada camada necessita dos serviços prestados pelas suas camadas vizinhas.

- Uma camada não sabe como a camada vizinha faz seu trabalho, ela apenas recebe o produto já pronto para ser usado e faz seu trabalho em cima dele, passando-o para a próxima camada. A esta característica damos o nome de encapsulamento.

Vamos entender melhor.

Tomaremos dois exemplos: um você indo para outra cidade de ônibus e o outro, você entrando em um site da Web. No primeiro exemplo você se dirige ao guichê da empresa e compra sua passagem. Nela há a cidade de destino. Depois você pega sua bagagem e se dirige a plataforma. Lá irão verificar sua passagem e indicarão o ônibus correto.

Você guarda sua bagagem no porta-malas do ônibus e recebe um ticket com um código. Depois disso você embarca e o ônibus faz a viagem. Ao chegar à cidade de destino, você desce do ônibus, entrega o ticket ao motorista, pega sua bagagem de volta, sai da plataforma, volta à área dos guichês da rodoviária e vai embora. Se desenharmos seu percurso ele será assim:

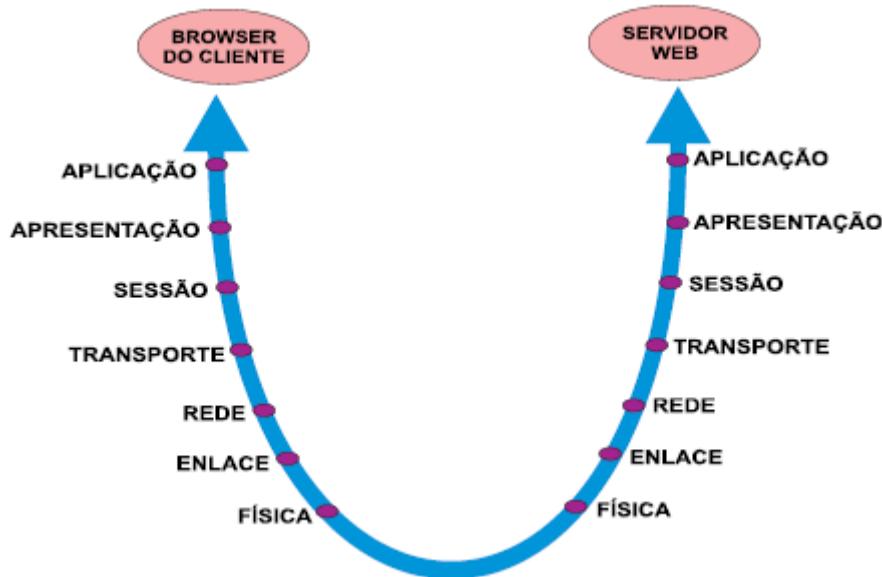


Note que você começa na área dos guichês de uma rodoviária e termina também na área dos guichês de outra rodoviária. Você também se dirige ao porta-malas tanto na saída quanto na chegada. Portanto, o fluxo que é feito no embarque também é feito no desembarque, porém de forma inversa.

Ao voltar à sua cidade de origem, esse fluxo será refeito, invertendo apenas a cidade de origem e a cidade de destino. Já no segundo exemplo, quando quer acessar um site da Web, você abre o browser do seu navegador de internet e digita um endereço, o qual chamamos de URL. Neste momento você está dando um comando à camada de aplicação. Esta solicitação irá ser “empacotada” e enviada para a próxima

camada do seu lado da rede, de cima para baixo, que irá fazer seu trabalho em cima do pacote, colocar outro pacote por cima e passar para a próxima, até chegar à camada física, onde viajará até a camada física do servidor Web em que o site em que você quer navegar está hospedado. Ao chegar à camada

física do servidor, o pacote subirá pelas camadas, onde cada uma delas tira uma das embalagens até chegar à camada de aplicação do servidor Web, que abrirá o último pacote e descobrirá a URL que você solicitou. O servidor irá pegar os arquivos do site que você pediu, colocar em um novo pacote e enviar pelo caminho de volta até chegar ao seu browser, conforme você havia solicitado. Tudo isso em questão de segundos ou milissegundos.



O modelo OSI não é o único modelo de referência. Existe outro modelo chamado de Modelo TCP/IP (Transmission Control Protocol/Internet Protocol).

O modelo TCP/IP surgiu junto com a ARPANET, que era uma rede patrocinada pelo Departamento de Defesa dos EUA, que tinha a intenção de manter comunicantes os órgãos do governo e universidades para enviar avisos sobre catástrofes que pudessem afetar o país. Não por menos, o governo precisava de uma rede robusta, segura e que fosse tolerante a falhas, fazendo surgir então o modelo TCP/IP.

O modelo TCP/IP possui menos camadas que o modelo OSI, pois algumas camadas foram geminadas em uma só, veja:



A camada de Aplicação do TCP/IP inclui as de Aplicação, Apresentação e Sessão do modelo OSI. A de Transporte é a mesma, a de Internet equivale à de Rede e a de Acesso á Rede juntou as de Enlace e Física.

Veremos no decorrer deste manual, especificidades de cada camada dos Modelos OSI e TCP/IP.

Mas não confunda! Modelos de camadas não alteram o funcionamento de uma rede. Eles são apenas referências e padrões a serem seguidos pelos fabricantes ao lançar um novo equipamento no mercado.

5.1. CAMADA DE APLICAÇÃO (Modelos OSI e TCP/IP)

5.1.1. Serviços e Funções

A camada de aplicação é a camada mais acima dos modelos OSI e TCP/IP. Ela é a camada que está mais próxima ao usuário. É nela que acontecem as solicitações dos aplicativos que o usuário manipula, como por exemplo, um browser para acesso a um site da Web, um gerenciador de e mails e um gerente de compartilhamento de arquivos. A camada de aplicação engloba também aplicações que não são apresentadas claramente ao usuário, como os serviços de DNS, que veremos mais adiante.

A camada de aplicação é muito importante porque não existiria lógica na criação de uma rede, sem aplicações que possam servir ao usuário de alguma forma.

As aplicações podem ter dois tipos de arquiteturas: a ponto-a-ponto (ou P2P - peer-to-peer) ou a cliente-servidor. Quando um desenvolvedor deseja criar um aplicativo para ser usado em uma rede, ele antes tem que definir qual dessas arquiteturas ele vai usar. Em arquiteturas P2P não é necessário que os sistemas finais estejam sempre ligados, já na arquitetura cliente-servidor, existirá um host servidor sempre disponível na rede para prover os serviços aos quais ele foi destinado.

Em uma aplicação P2P os hosts comunicam-se entre si, trocando informações. Exemplos de aplicações Informática – Redes de Computadores

P2P são os compartilhadores de arquivos. Neles, um host pode fazer download de arquivos de outros hosts, mas também pode fazer upload, ou seja, disponibilizar seus arquivos para que outro host da rede faça download deles.

Em aplicações cliente-servidor, os clientes não comunicam-se entre si, em vez disso, cada cliente manda sua requisição ao servidor e este se comunica com o cliente destinatário. Ao passo em que o servidor não está disponível, por motivos quaisquer, a aplicação não pode ser finalizada.

5.1.2. Protocolo HTTP

Uma das aplicações mais comuns na rede é o acesso a páginas da Web. Através de um aplicativo chamado browser, podemos solicitar um endereço da Web e receber uma página cheia de conteúdo dos mais diversos tipos e assuntos. Essa uma típica aplicação cliente-servidor, onde o host que solicita a página é o cliente e o host que armazena a página em seu disco é o servidor.

O protocolo que é usado para este fim é o HTTP – HyperText Transfer Protocol ou Protocolo de Transferência de Hipertexto. Este protocolo está presente tanto na máquina do cliente quanto na do servidor, mas atua de forma diferente em cada uma delas.

Uma página da Web é um arquivo, normalmente do tipo HTML, que é constituído por um conjunto de outros arquivos que podem ser texto, imagem, música ou vídeo. Ao hospedar uma página na internet é criado para este arquivo HTML um endereço URL, como por exemplo:

<http://www.cursoderedes.com.br/home.index>, note que o protocolo http usado para o tráfego desta página na rede precede o endereço. Caso essa página possua um texto e duas imagens, a referência a estes 3 objetos estará no arquivo com caminho home.index.

Quando o usuário insere este endereço no browser, o processo cliente HTTP faz uma comunicação com o host responsável pelo endereço cursoderedes.com.br através da porta de conexão 80. Concluída a comunicação, ele envia uma solicitação pedindo o arquivo que está no caminho home.index (que normalmente é a homepage do site). O servidor recebe a solicitação e extrai o arquivo home.index do disco, encapsulando-o e enviando de volta ao cliente. Após o cliente receber o arquivo, o processo HTTP cliente envia uma resposta indicando o recebimento. A comunicação é encerrada e o cliente extrai o arquivo do pacote.

Como vimos, esta página possui três objetos: um texto e duas imagens. Ao receber o arquivo home.index, ele apenas fará referência aos três objetos e o cliente automaticamente reiniciará o processo para receber do servidor cada um dos objetos separadamente.

É claro que cada solicitação e resposta dessa requer um tempo e é por isso que uma página que possui muitos objetos (fotos, vídeos, texto, etc) demora mais a carregar totalmente.

5.1.3. Protocolo FTP

Uma das funções mais primitivas de uma rede de computadores é a transferência de arquivos entre os hosts. O protocolo responsável por este serviço é o FTP – File Transfer Protocol ou Protocolo de Transferência de Arquivos.

Baseado na arquitetura cliente-servidor, o cliente acessa o FTP para fazer login no servidor FTP com usuário e senha e assim autenticar o seu acesso. Quando um cliente deseja compartilhar seus arquivos ele se conecta ao servidor FTP e uma cópia desses arquivos é feita no servidor. Se outro cliente necessita ter acesso a esses arquivos, ele efetua login e visualiza remotamente os arquivos compartilhados. Caso queira, ele pode efetuar uma cópia para seu disco local.

Ao enviar ou receber arquivos do servidor FTP, são usadas duas portas de conexão: a porta 21 para conexão de controle e a porta 20 para conexão de dados. Na conexão de controle é feita a identificação dos usuários com senha e são enviados comandos para adicionar ou capturar um arquivo. Na conexão de dados é que acontece a transferência dos dados realmente, ou seja, é o caminho por onde os dados transitam.

5.1.4. Protocolos SMTP e POP3

Outra aplicação bastante popular na internet é o correio eletrônico, o famoso e-mail. Com o e-mail é possível enviar mensagens a um endereço eletrônico de uma pessoa, onde esta, autenticada com usuário e senha, abre a caixa de mensagens onde lhe for mais apropriado e as lê, quando lhe for conveniente. O protocolo usado para envio de e-mails é o SMTP – Simple Mail Transfer Protocol ou Protocolo de Transferência de Correio Simples.

O e-mail é um tipo de aplicação que parece ser P2P, já que enviamos mensagens diretamente para o destinatário, mas na verdade é uma aplicação cliente-servidor. Quando queremos enviar uma mensagem, ou visualizar nossa caixa de e-mails precisamos nos conectar a um servidor de e-mails e fazemos isso nos autenticando com usuário e senha. Todas as nossas mensagens ficam armazenadas neste servidor. Quando vamos enviar uma mensagem, nem sempre o servidor de e-mail da outra pessoa é o mesmo que nós usamos, portanto o caminho da mensagem é feito da seguinte forma:

- Nos conectamos ao nosso servidor com usuário e senha.

- Uma aplicação chamada de leitor de correio (por exemplo o Outlook Express da Microsoft) permite que tenhamos acesso a nossas mensagens.
- Esta mesma aplicação nos fornece um simples editor de texto para que possamos escrever a mensagem que queremos enviar.
- No cabeçalho da mensagem inserimos o endereço de e-mail do destinatário, em que consta o servidor de e-mail daquela pessoa.
- Ao dar o comando para enviar, o leitor de correio envia a mensagem para o seu servidor de e-mail.
- Ao receber a mensagem, nosso servidor de e-mail inicia um processo cliente SMTP que efetua uma conexão com o servidor SMTP do destinatário e envia a mensagem.
- O processo servidor SMTP entrega a mensagem ao servidor de e-mail do destinatário.
- O servidor de e-mail do destinatário coloca a mensagem na caixa de mensagens.
- Quando o destinatário julgar necessário, ele abrirá seu leitor de correio e visualizará a mensagem que foi enviada.

O SMTP tem como característica ser um protocolo de envio de informações. Ele atua no envio da mensagem do host cliente ao servidor de email e de um servidor de e-mail a outro servidor de e-mail. Entretanto, o momento em que o destinatário abre a caixa de mensagens para visualizá-las é caracterizado como uma recuperação de informações, ação que o SMTP não abrange.

Para recuperar informações é necessário outro protocolo. Um dos mais usados é o POP3 – Post Office Protocol versão 3. É um protocolo muito simples e divide seu funcionamento em três etapas: autorização, transação e atualização.

- Autorização: é o momento em que o leitor de correio autentica o usuário com senha.
- Transação: é o momento em que o protocolo recupera as mensagens do servidor de e-mail e as torna visível no leitor de correio. Nesta fase, o usuário pode marcar mensagens e dar o comando para apagá-las.
- Atualização: é o momento em que o usuário encerra a sessão. Nesta fase, o protocolo realmente apaga do servidor de e-mail as mensagens que foram excluídas.

Bem, se a conta do seu e-mail é Hotmail, por exemplo, você não utiliza os protocolos SMTP e POP3. O Informática – Redes de Computadores

correio eletrônico de empresas como o Hotmail é via Web, portanto o protocolo utilizado para enviar mensagens do host do destinatário ao servidor de e-mail é o HTTP. Porém, o envio de mensagens entre servidores de e-mail é feito pelo SMTP.

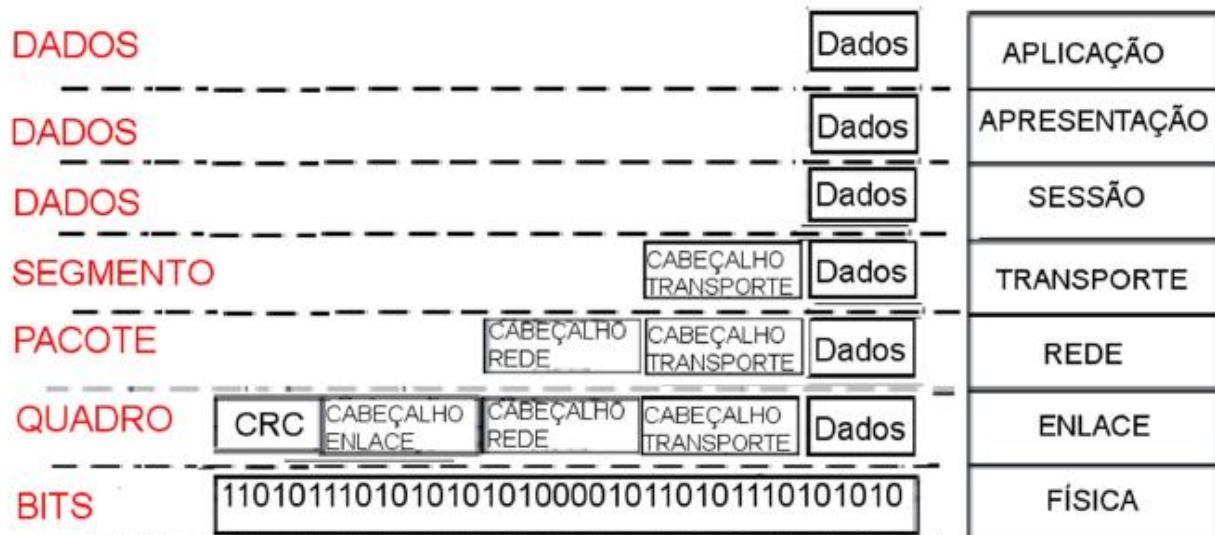
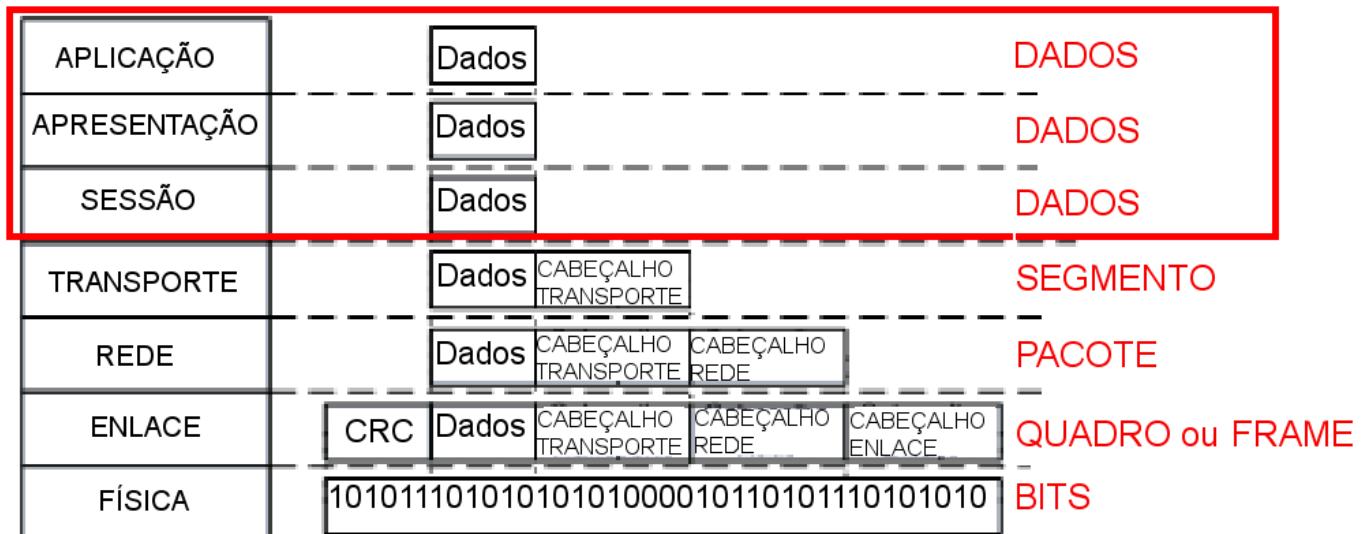
A grande vantagem de se usar um correio eletrônico na Web é a possibilidade de acessar sua caixa de mensagens de qualquer local e em qualquer dispositivo que tenha acesso à internet. Com a popularização dos correios eletrônicos da Web há alguns anos, cada vez menos as pessoas têm utilizado os leitores de correio, que por sua vez só podem ser acessados em computadores previamente configurados com a conta de e-mail.

5.1.5 Encapsulamento

Quando os dados estão sendo tratados pelas camadas, os dados são incrementados por cabeçalhos provenientes dos protocolos na respectiva camada na qual atuam, esse processo é denominado encapsulamento, assim quando esses cabeçalhos são adicionados o conjunto resultante possui um nome adequado.

Os dados vão “passando” de camada em camada, partindo da camada mais alta (Camada 7 – Aplicação) até a camada mais baixa (Camada 1 – Física), vão sendo adicionados cabeçalhos. Assim, esse conjunto (dados da camada superior+cabeçalho) é denominado Protocol Data Unit (PDU) - Unidade de dados do protocolo). Logo, cada PDU possui um nome específico:

1. As camadas de 7 a 5 (Aplicação, Apresentação e Sessão) possuem suas PDU's denominadas dados, assim esta PDU possui os dados quase brutos;
2. Segmento é a PDU da Camada de Transporte (Quarta camada);
3. Pacote é a PDU da Camada de Rede (Terceira camada);
4. Quadro ou frame é a PDU da Camada enlace de dados (Segunda camada);
5. Bits é a PDU da camada Física (Primeira camada).





1. Que solução surgiu para resolver os problemas de incompatibilidade entre os equipamentos de rede de diferentes fabricantes?

2. Complete o modelo OSI com as camadas que faltam:



3. Com a ajuda da explicação de seu professor, explique com suas palavras do que se trata um encapsulamento.

4. Faça uma analogia parecida com a feita na Figura 5b, colocando o percurso de uma correspondência enviada por Cássia que mora no Ceará para Aline que mora em Bruxelas, na Bélgica.

5. Diferencie aplicação P2P e cliente-servidor.

6. Relacione o protocolo ou serviço com a sua função principal:

(1) HTTP

(2) FTP

(3) SMTP

(4) POP3

(5) DNS

() Protocolo que atua na transferência de arquivos entre hosts.

() Serviço que resolve nomes em IPs e IPs em nomes.

() Protocolo que atua no envio de mensagens de e-mail.

() Protocolo que atua na recuperação de mensagens de servidores de email.

() Protocolo que atua no acesso a páginas da Web.

7. Baseado no funcionamento do protocolo HTTP, tente explicar por que a página do Google carrega mais rápido que a página do Facebook.

8. Qual número de porta de conexão é usado pelo HTTP?

9. Por que o FTP utiliza duas portas de conexão?

10. Para que servem os protocolos SMTP e POP3 respectivamente?



SUGESTÃO DE ATIVIDADE PRÁTICA:

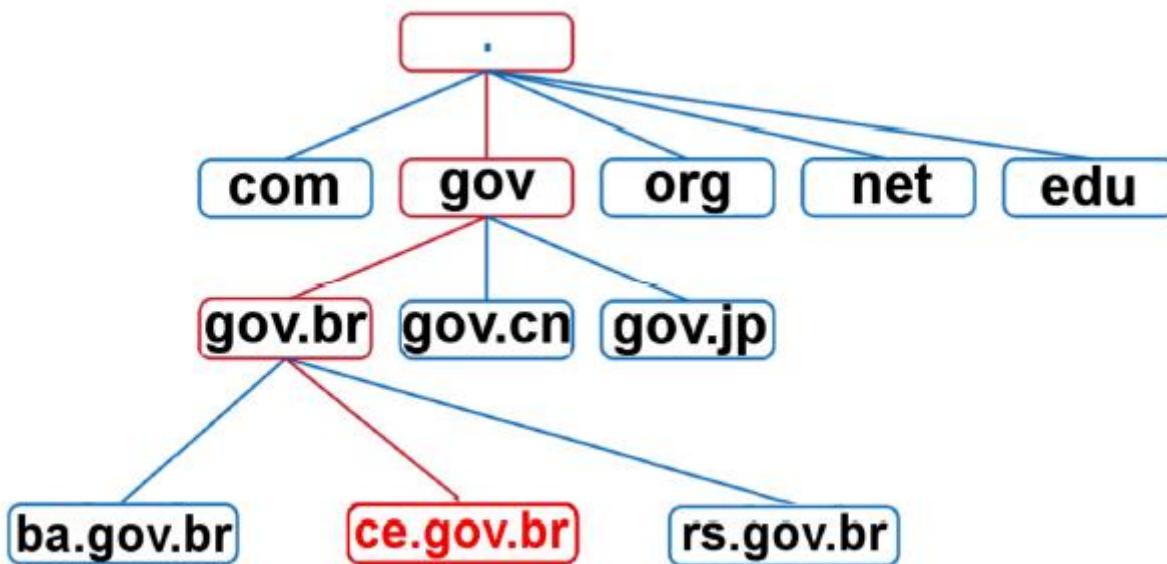
O programa Wireshark é um aplicativo livre e permite que você veja as linhas de cabeçalho de uma requisição HTTP, entre outros pacotes.

5.1.6 Serviços de DNS



Em uma rede, todos os hosts possuem uma identificação. Assim como nós, seres humanos, possuímos um nome e um CPF, os hosts também possuem um nome e um Endereço IP. O endereço IP é um código, que será visto com mais detalhes posteriormente, que identifica cada host em uma rede.

Os equipamentos e protocolos reconhecem um host pelo IP. Entretanto, para as pessoas, torna-se mais complicado decorar números, nem sempre com muito sentido. Imagine que se para cada página da Web que fosse acessar você precisasse digitar na barra de endereços do navegador um código com 12 números! Seria complicado, não?!



Para solucionar este problema, a camada de aplicação está ligada a mais um serviço: o DNS – Domain Name System ou Sistema de Nomes de Domínio. O DNS não é uma aplicação claramente visível para o usuário, mas ele entra em ação sempre que você envia um e-mail, copia um arquivo de um computador da rede, imprime em uma impressora de rede ou acessa uma página da Web.

O DNS é um serviço de tradução (ou resolução) de nomes em IPs e IPs em nomes. Ele possui um software para fazer essa tradução chamado de name resolver.

Vamos ao exemplo:

- Quando o usuário digita uma URL no browser é iniciado na própria máquina o serviço de DNS.
- O cliente DNS faz uma consulta ao servidor DNS mais próximo.
- O servidor DNS responde à solicitação do cliente com o endereço IP correspondente àquela URL.
- O cliente DNS entrega o endereço IP ao browser que, enfim, permitirá ao protocolo HTTP fazer seu trabalho e disponibilizar a página.



Mas como o servidor DNS consegue encontrar o endereço IP correspondente à URL digitada?

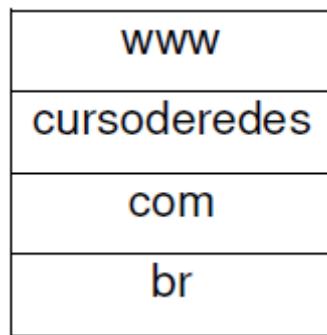
Primeiro você tem que saber que existem alguns servidores DNS específicos:

Servidores DNS raiz: é um conjunto de 13 servidores espalhados em alguns países (não existe nenhum no Brasil) que gerenciam todos os outros servidores DNS. Hierarquicamente estes 13 servidores DNS estão no topo.

Eles possuem o mapa dos servidores DNS de Alto Nível (TLD).

Servidores DNS de Alto Nível: são servidores que são responsáveis por domínios de alto nível como: com, edu, org, gov, entre outros. São responsáveis também por domínios de países como: fr, br, PT, entre outros. Servidores DNS de autoridade: são responsáveis por armazenar os domínios presentes na Web, sejam eles de empresas, escolas, instituições, órgãos e até mesmo pessoais. Todo aquele que quer disponibilizar uma página da Web, deve ter esta ligada a um domínio registrado em um servidor de autoridade, que pode ser próprio ou não.

O DNS recebe a URL e a esmiúça em pequenas partes. O endereço www.cursoderedes.com.br é dividido em:



- O código www, que significa World Wide Web, indica que o endereço refere-se a uma página da Web.
- O cliente DNS faz uma consulta com o endereço completo ao servidor DNS local mais próximo a ele.
- O servidor DNS local faz uma consulta ao servidor DNS raiz para descobrir qual servidor TDL é responsável pelo domínio br.
- O servidor DNS local faz uma consulta ao Servidor DNS de Alto Nível (TLD) responsável pelo domínio .br para descobrir o servidor TDL responsável pelo domínio .com.br.
- O servidor DNS local faz uma consulta ao Servidor DNS de Alto Nível (TLD) responsável pelo domínio .com.br para descobrir o servidor de autoridade responsável pelo domínio cursoderedes.com.br.
- O servidor DNS local faz uma consulta ao Servidor de Autoridade responsável pelo domínio cursoderedes.com.br para descobrir qual endereço IP corresponde a esse domínio.
- O servidor DNS local responde ao cliente DNS fornecendo o endereço IP solicitado.



Ufa!!! O servidor DNS trabalha muito! Mas se minutos depois, o usuário solicitar a mesma página novamente, o DNS vai fazer todo esse percurso de novo?!

Não! Para evitar este retrabalho, é implementado um cache nos servidores locais, ou seja, uma pasta onde ele armazena as consultas já feitas. Assim, quando o usuário anterior, ou até mesmo outro usuário da rede, solicitar a mesma página, o servidor DNS consultará, antes de mais nada, o seu próprio cachê. Se o Informática – Redes de Computadores

registro já existir, o servidor devolve a resposta rapidamente ao cliente. Isso ajuda a deixar o acesso mais rápido.

Como o endereço IP de um host pode mudar a qualquer momento, esse registro é descartado cerca de dois dias depois.



SUGESTÃO DE ATIVIDADE PRÁTICA:
Professor, oriente seus alunos no laboratório para usarem os comandos ping e nslookup.



Exercícios

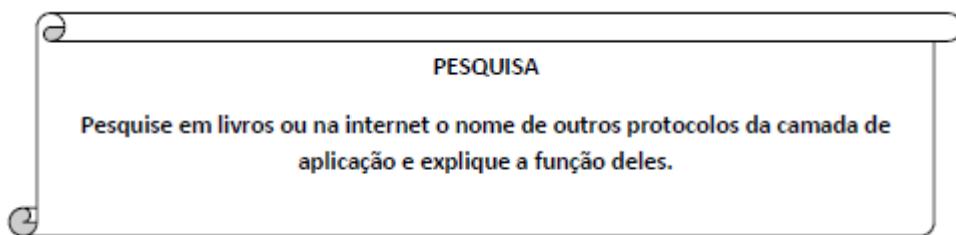
1. Defina:

a) Servidor DNS raiz.

b) Servidor DNS de alto nível.

c) Servidor DNS de autoridade.

2. Qual a importância do cachê para a velocidade da consulta DNS?



5.2. CAMADAS DE APRESENTAÇÃO E SESSÃO (Apenas Modelo OSI)

Como você pôde observar, existem algumas diferenças entre os modelos OSI e TCP/IP. Uma delas é que no modelo OSI existem duas camadas entre a camada de aplicação e a de transporte: a camada de Apresentação e a camada de Sessão. No modelo TCP/IP estas camadas são embutidas na camada de Aplicação. Mas afinal, de que se tratam essas duas camadas?

5.2.1. Camada de Apresentação – Serviços e Funções

Como o nome já sugere. A camada de Apresentação é responsável por apresentar os dados que vem das outras camadas à camada de Aplicação e vice-versa. Podemos dizer também que ela prepara os dados para que sejam lidos pelas outras camadas de forma que sejam entendidos, pois cada camada trata os dados de uma forma bastante específica. Esta camada faz três funções básicas: tradução, compressão e criptografia.

Ao receber os dados de aplicações de um remetente, como palavras escritas em códigos ASCII em uma mensagem de correio eletrônico, por exemplo, a camada de apresentação traduz, ou converte para o padrão usado pelo dispositivo transmissor. Da mesma forma, ao chegar à camada de Apresentação do destinatário, esta vai converter os dados para o padrão a ser usado pela camada de aplicação.

Continuando com o exemplo, ao enviar estes dados, a camada de aplicação entrega-os à de apresentação sem preocupar-se com a forma que estes dados irão trafegar na rede. Para otimizar a transmissão, a camada de apresentação comprime os dados, deixando-os menores. Do outro lado da transmissão, a camada de apresentação do destinatário recebe estes dados comprimidos, faz sua descompressão e entrega-os perfeitamente à camada de aplicação, que nem toma conhecimento de todo este trabalho.

Algumas aplicações exigem uma transmissão mais segura no sentido de evitar que, uma vez que os dados enviados sejam interceptados por alguém não autorizado, estes não possam ser lidos ou entendidos. Para isso podem ser usadas técnicas de criptografia. A aplicação envia os dados totalmente abertos à camada de apresentação e esta, por sua vez, tem a função de criptografá-los com alguma técnica escolhida pelo aplicativo. A partir desta camada, os dados trafegam encriptados até chegar à camada de apresentação do destinatário, onde serão descriptografados e entregues à camada de aplicação da mesma forma que saíram da aplicação do remetente.

5.2.2. Camada de Sessão – Serviços e Funções

A camada de sessão é responsável abrir o canal de comunicação entre dois hosts comunicantes e encerrá-

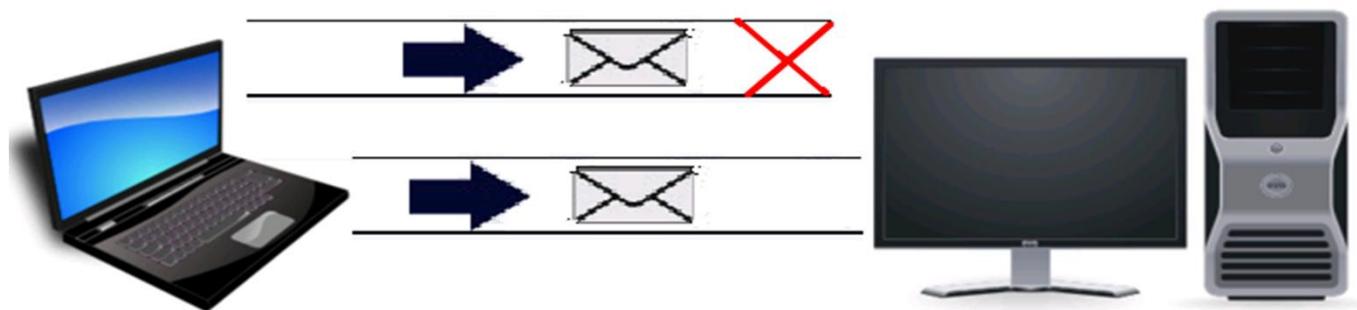
lo. Além disso, ela mantém aberta a conexão entre os hosts até que estes concluam a transmissão. Mesmo que haja algum problema na rede que impeça a comunicação, a camada de sessão consegue reestabelecer a transmissão de forma rápida e do ponto onde foi interrompida, graças à sua técnica de marcação, pois ela vai incluindo marcações nos dados que estão sendo enviados. Sabe aqueles jogos de videogame, onde você faz marcações e caso haja algum problema, é possível voltar o jogo para o último ponto em que foi marcado? A camada de sessão faz mais ou menos isso com a rede!



1. Qual a função da camada de Apresentação e quais serviços ela oferece?

2. Como se dá a técnica usada pela camada de Sessão para conseguir reestabelecer uma transmissão interrompida?

5.3. CAMADA DE TRANSPORTE (Modelos OSI e TCP/IP)



Pelo que estudamos até agora, vimos que em uma transmissão em uma rede, a camada de aplicação “produz” os dados, a de apresentação “prepara” esses dados para serem enviados e a de sessão abre a conexão e mantém seu estado para que os dados possam trafegar. Durante todo este processo as camadas trabalharam com dados Os dados são o PDU das três primeiras camadas.



PDU - Protocol Data Unit, ou seja, Protocolo de Unidade de Dados

O que é o PDU de uma camada?

Cada camada trata a informação transmitida de uma forma. O PDU de uma camada é a unidade em que são tratadas as informações naquele momento.

Na camada de Transporte, o PDU utilizado é o segmento. Ou seja, esta camada receberá os dados da camada de sessão e irá dividi-los em segmentos para serem enviados à camada de rede (ou acesso à rede, no modelo TCP/IP).

5.3.1. Serviços e Funções

Quando usamos uma aplicação de rede, a impressão que temos é que existe uma comunicação direta entre nosso host e o host destinatário. Entretanto existem muitos roteadores de rede fazendo a comunicação física entre os dois hosts, onde muitas vezes centenas de quilômetros os separam.

A camada de transporte faz essa função: comunicar logicamente o processo que roda no host remetente ao processo que roda no host destinatário independente de como esses dados irão chegar até lá, ou seja, independente de por quantos roteadores, enlaces e arquiteturas de rede diferentes eles terão que passar.

Em várias literaturas e até mesmo na internet você encontrará comparações entre uma rede e um serviço de correios. As três primeiras camadas do modelo OSI ou a camada de Aplicações do modelo TCP/IP equivalem ao remetente escrevendo uma carta, colocando-a em um envelope e entregando-a ao carteiro. Quem irá efetuar o transporte da correspondência realmente é o correio, mas se o carteiro não separar as

cartas corretamente e entregá-las na agência em tempo hábil, o correio nada poderá fazer para garantir que sua carta chegue ao destino. Da mesma forma, ao chegar na agência de destino, se o carteiro não separar as cartas corretamente de acordo com o endereço ou demorar a entregar sua carta, de nada adiantou o trabalho dos correios.

Perceba com esta história duas coisas: primeiro, o bom trabalho do carteiro é extremamente importante para o sucesso do serviço dos correios.

Segundo, o carteiro é o elo principal tanto entre o remetente e o correio quanto entre o correio e o destinatário.

Comparando com o nosso modelo de camadas, o carteiro é a nossa Camada de Transporte. Ela faz a ligação entre as camadas a nível de aplicação (Aplicação, Apresentação e Sessão) e as camadas de nível físico (Rede, Enlace e Física no modelo OSI ou Internet e Acesso à Rede no modelo TCP/IP).

Existem dois protocolos usados pela camada de transporte: O TCP – Transmission Control Protocol, ou Protocolo de Controle de Transmissão e o UDP – User Datagram Protocol, ou Protocolo de Datagrama de Usuário.

Estes dois protocolos tem a função de entregar os dados dos processos do host remetente ao host destinatário. Vamos analisar estes dois protocolos com mais detalhes.

5.3.2. Protocolo TCP

O protocolo TCP – Transmission Control Protocol é um protocolo de transporte orientado para conexão, ou seja, antes de começarem a trocar informações, os hosts comunicantes estabelecem uma conexão, que podemos comparar com uma apresentação. É como se o host remetente e o host destinatário efetassem o seguinte diálogo:

- Oi, você está me ouvindo?
- Sim, estou!
- Ok! Então vou começar a transmitir.

Somente depois de ter certeza que o host destinatário está pronto para receber as informações é que o host remetente começa a enviar os dados, sem correr o risco de ficar “falando sozinho”. Esta característica do TCP, entre outras coisas, garante a entrega dos dados ao destinatário de forma íntegra e ordenada. Isso acontece porque, como os hosts estão conectados um ao outro, ao enviar um pacote ao destinatário, o Informática – Redes de Computadores

remetente fica aguardando uma resposta de confirmação. Se o destinatário respondeu confirmado o recebimento do pacote, o remetente envia o próximo pacote, na ordem correta.

Se o destinatário não respondeu, o remetente, após esperar um determinado tempo, reenvia o pacote, presumindo que o que ele enviou antes foi perdido por algum motivo. A essa resposta de confirmação de recebimento damos o nome de acknowledge ou ACK.

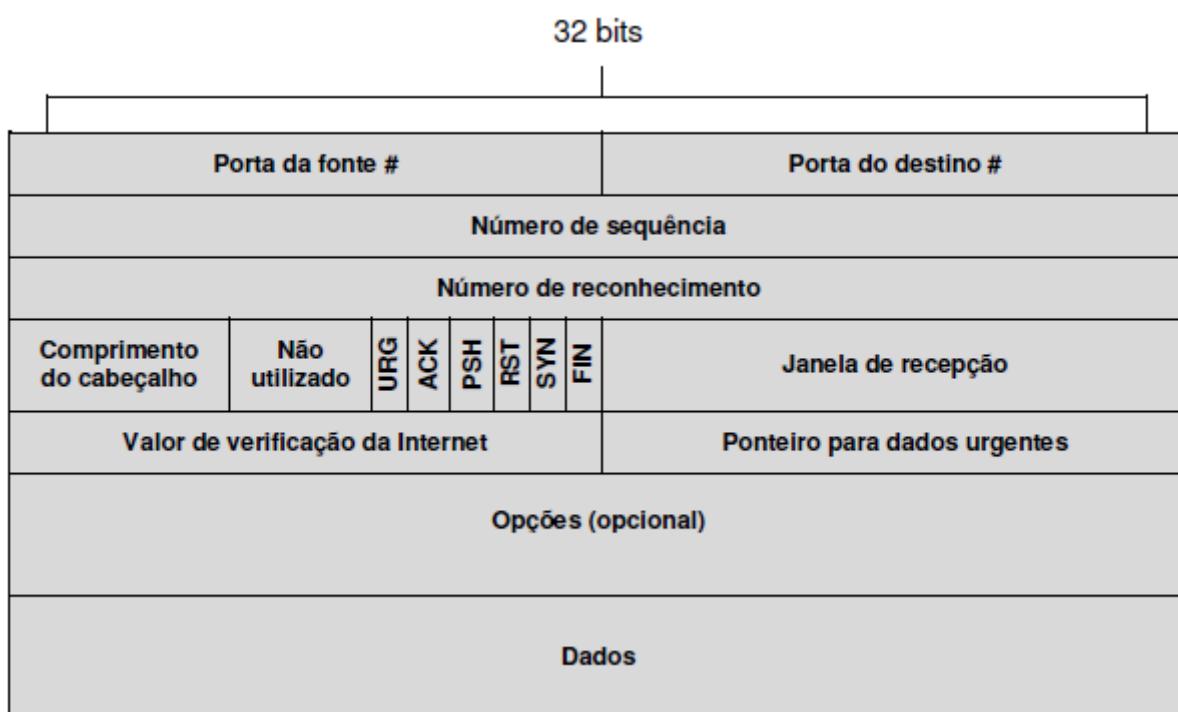
Outra implementação é o controle de congestionamento, onde a taxa de transmissão dos pacotes é diminuída quando existem muitos pacotes trafegando na rede. Assim o TCP evita que aconteça um travamento ou acúmulo de pacotes em caso de congestionamento.

O TCP também implementa o controle de fluxo, ou seja, ele não permite que um remetente envie, ao mesmo tempo, mais dados do que o destinatário pode receber. Isso acontece porque são estabelecidos tanto no host remetente quanto no destinatário um valor de MTU – Maximum transmission unit, ou unidade máxima de transmissão. É o MTU quem diz a quantidade máxima de dados que podem ser enviados/recebidos em um segmento TCP.



E como é um segmento TCP?

Vamos analisar com detalhes o segmento TCP abaixo:



- Porta da fonte e porta do destino: Um processo envia dados para a camada de transporte ou recebe dados da camada de transporte através de portas, por exemplo as portas 20 e 21 do protocolo FTP, ou a porta 80 do HTTP, entre outras. Ao enviar dados em um segmento TCP, devem ser informadas a porta da fonte dos dados e a porta do destino destes dados.
- Número de sequência: é a cadeia de 32 bits que indica a ordem de envio dos segmentos oriundos de um conjunto de dados.
- Número de reconhecimento: devido o TCP ser full-duplex, pode ocorrer de um host ser remetente e destinatário ao mesmo tempo, em uma mesma conexão TCP com outro host. Para que não haja confusão entre os segmentos que estão sendo enviados, são implementados números de reconhecimento que especificam o número do próximo byte que o receptor espera receber. Isso faz com que, em uma transmissão full-duplex, o host A saiba se o segmento que ele está recebendo é um segmento dos dados que o host B está transmitindo, ou se é um segmento de acknowledge (confirmação de recebimento) de um segmento enviado pelo host A.
- Comprimento do cabeçalho: são 4 bits que informam o comprimento do cabeçalho. Quase todos os campos do segmento TCP possuem tamanho predefinido, exceto o campo Opções, que é opcional, portanto o comprimento do cabeçalho pode variar caso o campo Opções esteja preenchido.
- Não utilizado: é realmente um campo que ainda não é utilizado pelo TCP, mas fica reservado para uso no futuro.
- Flags: são marcações do tamanho de um bit. Onde houver bit 1 nesses campos, estes devem ser levados em consideração:

URG - Campo de ponteiro Urgente é válido

ACK - Campo de Reconhecimento é válido

PSH - Este segmento solicita um PUSH

RST - Reset da conexão

SYN - Sincroniza números de sequências

FIN - O transmissor chega ao fim do fluxo de bytes.

- Dados: é no campo Dados que pedaços do conjunto de dados que devem ser enviados são

colocados. O tamanho do campo Dados varia de acordo com o MTU preestabelecido.

O protocolo TCP é muito mais complexo, mas estudos mais aprofundados não vêm ao caso neste momento. O importante é você saber que o TCP é confiável e ideal para aplicações orientadas à conexão, que precisam enviar e receber todos os dados, sem percas e em perfeita ordem.

Consequentemente, devido aos procedimentos que devem ser feitos para garantir a entrega dos segmentos, a transmissão demora um pouco para acontecer, mas é o preço que se paga pela qualidade do serviço.

5.3.3. Protocolo UDP

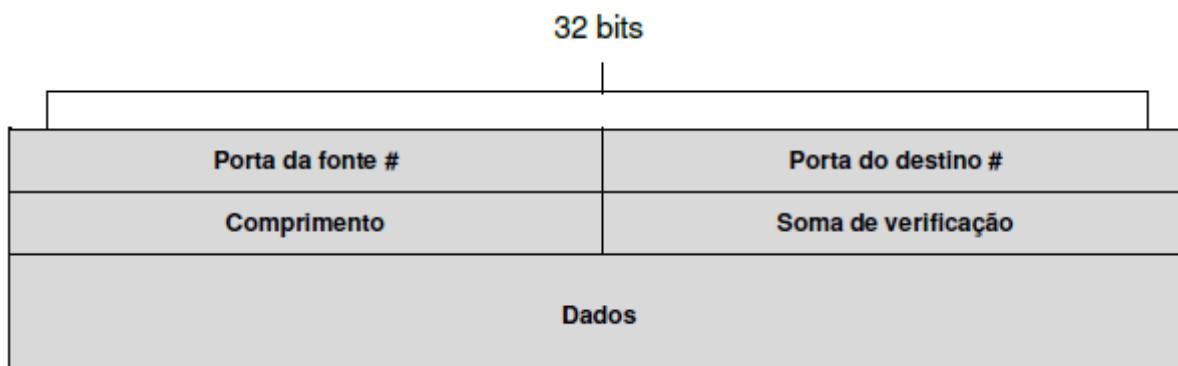
Diferente do TCP, o UDP – User datagram Protocol, ou Protocolo de Datagrama de Usuário, não é orientado para conexão, ou seja, quando o processo do remetente precisa enviar dados, ele simplesmente envia, sem se preocupar se o processo do destinatário está ativo. Sendo assim, o protocolo UDP não garante a entrega dos dados enviados.



Então, qual a vantagem do UDP em relação ao TCP?!

Existem várias vantagens em se usar o protocolo UDP. A primeira delas é que como não existe nenhuma apresentação entre os hosts, ou estabelecimento de conexão, a transmissão no UDP é mais rápida. A segunda é que, como não existe controle de congestionamento, em nenhum momento a taxa de transmissão é reduzida. E por último, o cabeçalho do segmento UDP é bem menor que o cabeçalho do segmento TCP, evitando assim a sobrecarga de cabeçalho.

Veja abaixo um segmento UDP:



A soma de verificação é uma forma de detectar erros dentro do segmento, que podem acontecer devido a alguma interferência no meio da transmissão. Nela é implementado um algoritmo que efetua sequências de adições sobre os bits que compõem o segmento. O resultado deste cálculo é colocado no campo Soma de verificação. Ao receber o segmento, o protocolo UDP do destinatário usa o mesmo algoritmo nos bits do segmento recebido e compara o resultado com o que está no campo Soma de verificação. Se o resultado for igual significa que o segmento chegou intacto, caso contrário o UDP destinatário descobre que há um erro nos dados do segmento.

Como podemos ver, o UDP é um protocolo muito mais leve e rápido que o TCP, por isso é amplamente usado em aplicações multimídia e em tempo real, que toleram algumas falhas e percas de pacotes, mas necessitam primordialmente de rapidez na entrega dos mesmos, sem atrasos, que prejudicariam a essência da aplicação.

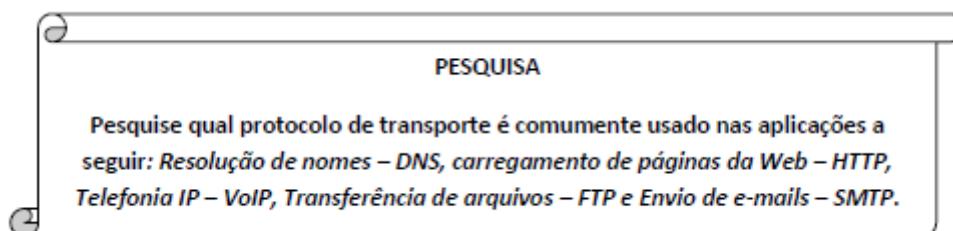


1. Explique o que é uma transmissão orientada para conexão.

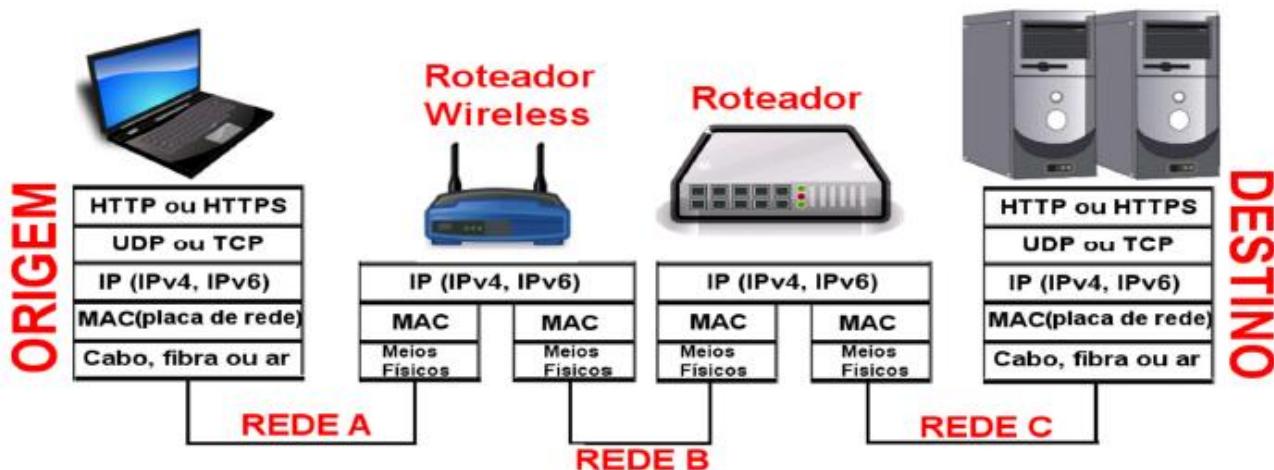
2. Qual a função de um acknowledge?

3. Qual a relação entre o MTU e o serviço de controle de fluxo TCP?

4. Cite uma vantagem e uma desvantagem dos protocolos TCP e UDP.



5.4. CAMADA DE REDE (Modelo OSI) ou INTERFACE COM A REDE (Modelo TCP/IP)



5.4.1. Serviços e Funções

Na camada anterior, vimos os principais protocolos de transporte de informações na rede. Esses protocolos recebem dados das camadas mais acima e os dividem em segmentos para que possam ser transportados. Cada segmento possui um cabeçalho com todas as especificidades daquele protocolo de transporte, seja TCP ou UDP, e contém também os dados que serão enviados.

Um segmento da camada de transporte é como se fosse um envelope, onde externamente temos as informações daquela camada e internamente temos as informações. Ao enviar para a próxima camada, a camada de Rede, ou Interface com a Rede, este envelope será colocado dentro de outro envelope (até porque uma camada não se importa como a outra manipulou os dados), onde externamente constarão as Informática – Redes de Computadores

informações relevantes dos protocolos daquela camada.

O envelope da camada de rede é chamado de datagrama e será a PDU desta camada.



Mas afinal, qual é a função da Camada de Rede?

A camada de rede possui duas funções principais: a função de repasse e a função de roteamento. Antes de esmiuçarmos cada uma das funções, vamos entender primeiro que, a partir desta camada, estaremos mais diretamente ligados a meios físicos na rede, ou seja, equipamentos. O equipamento fundamental, sem o qual a camada de rede não teria sentido é o roteador.

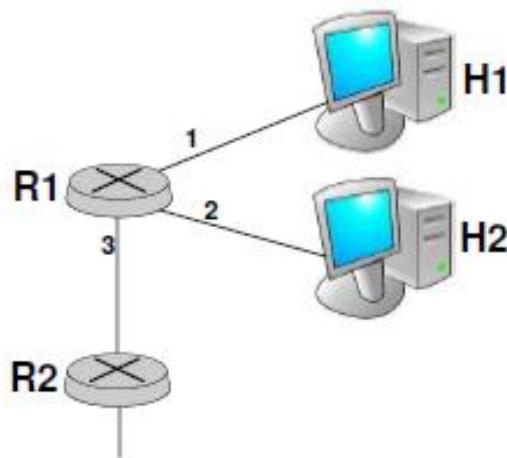
O roteador de rede é a porta de entrada ou saída de uma rede qualquer. Ele tem a função de encaminhar os datagramas da camada de rede até um host diretamente ligado a ele ou até outro roteador vizinho. Sabemos que ao solicitarmos no browser um site da internet, esta solicitação percorrerá inúmeros roteadores até chegar ao servidor Web que hospeda aquela página.

Portanto, mais do que apenas repassar os datagramas ao próximo nó da rede, um roteador tem a função de roteamento, ou seja, ele faz um mapeamento de todos os roteadores existentes do ponto onde ele está até um host de destino (como o servidor Web que hospeda o site, por exemplo) e, além disso, ele decide qual a melhor rota a ser percorrida até o destino, com o caminho que demore menos tempo para ser percorrido, seja ele o menor ou o menos congestionado.

5.4.1.1. Função de Repasse

Um roteador pode possuir várias portas as quais chamamos de interfaces. Para cumprir sua função de repasse, o roteador deve ter ciência de qual interface deverá ser usada para repassar um determinado datagrama.

Essa escolha irá depender do destino daquele datagrama. Essa informação que constará no cabeçalho do datagrama será comparada com uma tabela de repasse que estará presente no próprio roteador. Veja e analise a imagem abaixo:



Como você pode notar, temos um roteador R1 ligado a dois hosts H1 e H2 e a um segundo roteador R2, portanto o roteador R1 possui três interfaces ativas, cada uma comunicando-se com uma interface de outro equipamento através de um enlace. O roteador R1 do exemplo acima possui a seguinte tabela de roteamento:

TABELA DE REPASSE	
VALOR DO CABEÇALHO	INTERFACE DE SAÍDA
1111	1
1010	2
0011	3

Podemos concluir que, se o host H1 enviar um datagrama ao roteador R1, com o valor 0011 no cabeçalho, o roteador R1 deverá encaminhar este datagrama à interface 3, que possui um enlace de comunicação com o roteador R2. Da mesma forma, quando o roteador R2 quiser responder à solicitação do host H1, ele deverá enviar um datagrama para o roteador R1 com o valor 1111 no cabeçalho. Assim R1 verificará na tabela de repasse e encaminhará o datagrama corretamente até H1.

Perceba também que, apesar de a tabela de repasse indicar interface de saída, as interfaces de um roteador também são de entrada. Lembre-se que a transmissão neste nível é full-duplex.

5.4.1.2. Função de roteamento

Cumprir a função de roteamento envolve todos os roteadores desde o de origem até o de destino. Como já falamos, nesta função o roteador irá traçar o melhor caminho até chegar ao host destinatário. Qualquer host, em qualquer rede, que esteja ligada à internet, ao enviar uma solicitação para fora da rede local, precisa encaminhar seus datagramas ao roteador de borda de rede (também chamado de roteador default, ou roteador de primeiro salto) que é o roteador mais próximo; aquele que faz a comunicação da rede local

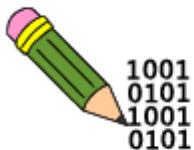
com as demais redes. O host destinatário também possui um roteador default mais próximo a ele. É entre estes dois roteadores de borda que acontece o roteamento.



Como o roteador consegue determinar qual a melhor rota a ser percorrida pelos pacotes de informações?

O roteador utiliza-se de algoritmos de roteamento, que mapeiam todos os roteadores no caminho até o roteador destino e faz algumas mensurações como: a quantidade de enlaces existentes no caminho; a distância física dos enlaces entre os roteadores e a velocidade dos enlaces. Baseados nesses dados os algoritmos de roteamento verificam o caminho de menor custo ou caminho mais curto. Além disso os algoritmos de roteamento podem mensurar a carga de um enlace, ou seja, o nível de congestionamento daquele enlace.

Em resumo, os algoritmos de roteamento verificam o caminho mais curto, porém se o mais curto for, ao mesmo tempo, muito congestionado (o que será bem provável), o algoritmo irá verificar uma segunda opção de caminho que não seja tão longo, mas que não possua congestionamento. O importante é achar o caminho mais rápido em um determinado momento!

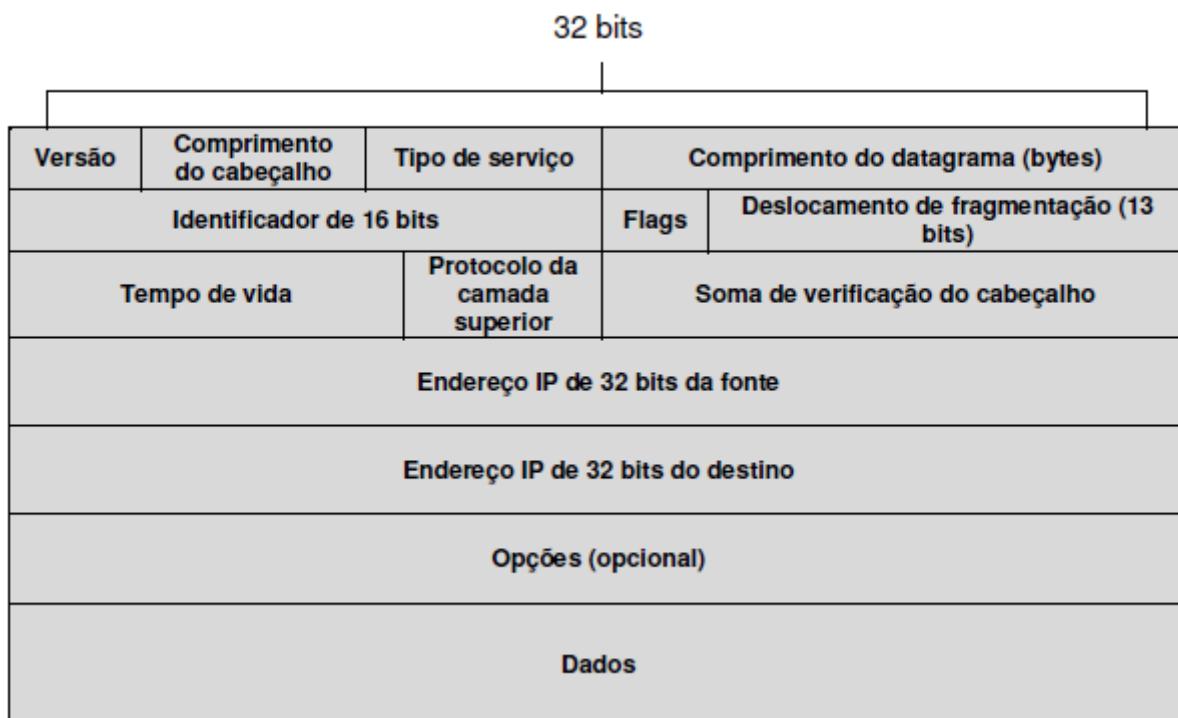


SUGESTÃO DE ATIVIDADE PRÁTICA:
Usar o Traceroute (Linux) ou Tracert (Windows) para visualizar a rota do host local a qualquer site no mundo e o tempo de viagem de ida e volta.

5.4.2. Protocolo IP

O protocolo mais importante da camada de Rede é o IP – Internet Protocol, ou Protocolo de Internet. O IP é responsável pelo endereçamento dos hosts e equipamentos em uma rede. Todo host em uma rede deve ter um endereço lógico que chamamos de endereço IP. Falamos um pouco de endereços IP na seção 5.1.5 quando estudamos sobre Serviços de DNS, lembra?

Bem, como já sabemos, a camada de rede recebe os segmentos da camada de transporte e os transforma em datagramas., que é o tipo de pacote da camada de rede. Esses datagramas possuem um cabeçalho com uma forma predefinida pelo protocolo que os utiliza: o protocolo IP. Estudaremos duas versões de IP, o IP versão 4 (IPv4) e o IP versão 6 (IPv6). A primeira versão, IPv4, é ainda a mais utilizada atualmente. Veja como é a estrutura de um datagrama IPv4:



- Versão: indica de o protocolo usado é o IPv4 ou o IPv6.
- Comprimento do cabeçalho: este campo é necessário devido a existência do campo Opções, que pode fazer com que o tamanho do cabeçalho varie.
- Tipo de serviço: indica se o datagrama possui alguma particularidade, como se é de uma aplicação em tempo real, se requer baixo atraso, etc.
- Tempo de vida: para que o datagrama não corra o risco de ficar viajando de roteador a roteador “eternamente” é inserido neste campo um valor onde, a cada roteador pelo qual o datagrama passa, é decrementado o valor 1 do tempo de vida, assim quando este valor for 0 o datagrama deverá ser descartado.
- Protocolo de camada superior: qual a camada superior em relação à camada de rede? A de transporte, não é mesmo? Neste campo é informado qual protocolo da camada de transporte deverá ser usado neste pacote, TCP ou UDP.
- Soma de verificação do cabeçalho: como já vimos em cabeçalhos de outras camadas, a soma de verificação é uma forma de detecção de erros no cabeçalho.
- Endereços IP de fonte e de destino: trazem, respectivamente, o endereço IP do host remetente e o endereço IP do host destinatário.

- Identificador de 16 bits, Flags, Deslocamento de fragmentação: estes 3 campos servem para auxiliar em uma propriedade do protocolo IP: a fragmentação. Ao enviar um datagrama abaixo na pilha de camadas, ou seja para a camada de enlace, corre-se o risco de os quadros da camada de enlace possuírem uma MTU (unidade máxima de transmissão) menor que o tamanho do datagrama e não suportarem a carga de bits, obrigando a camada de rede a fragmentar seu datagrama em datagramas menores e, só assim, enviá-los pela rede. Os campos Identificador, Flags e Deslocamento servem para identificar cada fragmento e ajudar na reconstrução destes datagramas menores no datagrama original ao chegarem no host destinatário.

Bem, falamos de datagramas IP, mas fica a questão: como surgem os endereços IP nos hosts da rede?

O endereço IPv4 é formado por 32 bits, separados por pontos em 4 conjuntos de 8 bits, que chamamos de octetos. Apesar de serem essencialmente números binários, o endereço IP é tratado por nós em notação decimal. Portanto o endereço IP 192.168.10.56 em notação decimal é formado na verdade por 4 conjuntos de 8 bits:

11000000.10101000.00001010.00111000.

Os endereços IPv4 são divididos em duas partes. A parte mais à esquerda serve para identificar a qual rede o host pertence e a parte mais à direita serve para identificar os hosts daquela rede. É como usar o nome e o sobrenome: o sobrenome identifica a qual família uma pessoa pertence e o nome identifica os membros daquela família.

Se eu usar os 3 primeiros octetos do endereço IP acima para identificar a rede e o último octeto para identificar o host, dessa forma:

11000000.	10101000.	00001010.	
REDE			HOST

O endereço ficará assim:

192.168.100.56/24

Onde o /24 indicará a máscara de sub-rede, ou seja, a quantidade de bits que foram usados no endereço para identificar a rede a qual pertence este host. Podemos concluir que, este host especificamente, está na sub-rede 192.168.10 e o código dele é o 56.

É claro que podemos usar diferentes máscaras de sub-rede para identificar uma sub-rede e um host, mas

para facilitar as coisas foram criadas as classes de endereços IP:

- **Classe A**

Na classe A usamos 1 octeto para identificar a sub-rede e 3 octetos para identificar o host:

Prefixo		Sufixo	

Esta classe é mais usada em sub-redes com grande número de hosts, onde é necessária uma variedade maior de endereços. Neste caso a máscara de sub-rede será /8, pois apenas os 8 primeiros bits do endereço serão usados para identificar a rede. Você também verá a máscara de sub-rede representada assim: 255.0.0.0.

- **Classe B**

Na classe B usamos 2 octetos para identificar a sub-rede e 2 octetos para identificar os hosts:

prefixo		Sufixo	

Nesta classe, a quantidade de endereços reservados para as sub-redes é igual a de endereços reservados para os hosts. A máscara de sub-rede será /16 ou 255.255.0.0.

- **Classe C**

Na classe C usamos 3 octetos para identificar a sub-rede e 1 octeto para identificar os hosts:

prefixo		Sufixo	

Esta classe é a mais usada em redes de pequeno porte, onde o número de hosts na rede não ultrapassem os 253 hosts. A máscara de sub-rede é /24 ou 255.255.255.0.

5.4.3. IPv6

No início da sessão anterior comentamos que existem duas versões do protocolo IP, o IPv4 e o IPv6.

Vimos a estrutura tanto do endereçamento IPv4 quanto do datagrama IPv4. Vamos conhecer então, um pouco do IPv6.

Antes de mais nada vamos entender um pouco o motivo da existência do IPv6.

Se você calcular bem, o endereço IPv4 possui 32 bits, o que equivale a 232 possibilidades de endereços, que corresponde a 4.294.967.296 de endereços possíveis. Cada roteador e cada host da rede mundial, ou internet, deve possuir um endereço IP único, o que consequentemente faz com que os mais de 4 milhões de endereços IPv4 possíveis estejam esgotando.

Antes que isto realmente aconteça, grupos de trabalhos de instituições ligadas à internet se dedicaram na criação de uma nova versão do protocolo IP que permitisse a continuação do crescimento da internet possuindo um tipo de endereçamento com um número imensamente maior de possibilidades. A essa versão foi dado o nome de IPv6 (Internet Protocol versão 6).



Agora fiquei curioso! Como seria então um endereço IPv6?

Enquanto o endereço IPv4 possui apenas 32 bits, o endereço IPv6 possui 128 bits, ou seja 2128 endereços possíveis. Este cálculo resulta em um número tão grande que dizem que se cada grão de areia no mundo quisesse, poderia ter um endereço IP [Kurose, 2007].

O endereço IPv6 é dividido em 8 conjuntos de 16 bits representados por 4 dígitos em hexadecimal, veja o exemplo:

2051:0fb6:45d2:48d0:9312:5ad9:a340:5217



Muito interessante! Mas se é uma maravilha tão grande, por que ainda não usamos o IPv6?

Toda a rede mundial funciona hoje usando o protocolo IPv4. Migrar para outra versão, que altera o modo como os dados trafegam na rede é um processo bem complicado, principalmente porque são bilhões de equipamentos ligados em rede no mundo todo. Não se pode simplesmente ir dormir usando o IPv4 e acordar usando o IPv6.

Foi cogitado, inclusive, implementar um “dia da conversão”, onde em um determinado dia e em uma determinada hora todas os computadores, impressoras de rede, roteadores, celulares, tablets, enfim, todos os equipamentos ligados à internet teriam que ser desligados e atualizados, migrando do IPv4 para o IPv6. Um técnico em Redes ganharia muito dinheiro fazendo atendimentos para atualizar as máquinas dos clientes, mas provavelmente ele enlouqueceria antes do fim do dia! =)

De fato que não é viável proceder desta forma (até porque ainda existem equipamentos e sistemas operacionais funcionando por aí que não possuem suporte ao IPv6, portanto eles não poderiam mais ter acesso à internet) essa migração será feita aos poucos.

Os novos sistemas operacionais, drivers de placas de rede, roteadores e demais equipamentos de rede possuem suporte tanto ao IPv4 quanto ao IPv6. Hoje em dia é possível que um host habilitado para IPv6 envie datagramas IPv4 para não interferir no restante da rede, portanto gradativamente o IPv6 será introduzido, de forma bem menos traumática.

5.4.5. Protocolo DHCP

Já está devidamente entendido que cada host, roteador, impressora de rede, ou qualquer outro equipamento que envie e receba pacotes da rede deve ter um endereço IP para ser localizado, mas quem é o responsável por configurar estes números de IP nos hosts? A princípio seria o técnico administrador da rede que faria isso manualmente em cada host, executando uma tarefa repetitiva.

Uma tarefa repetitiva, normalmente pode ser executada por um software. A tarefa de inserir números de IP, máscara de sub-rede, gateway e DNS nos hosts de uma rede pode ser executada por um software em um servidor baseado no protocolo DHCP – Dynamic Host Configuration Protocol, ou Protocolo de Configuração Dinâmica de Hospedeiro.



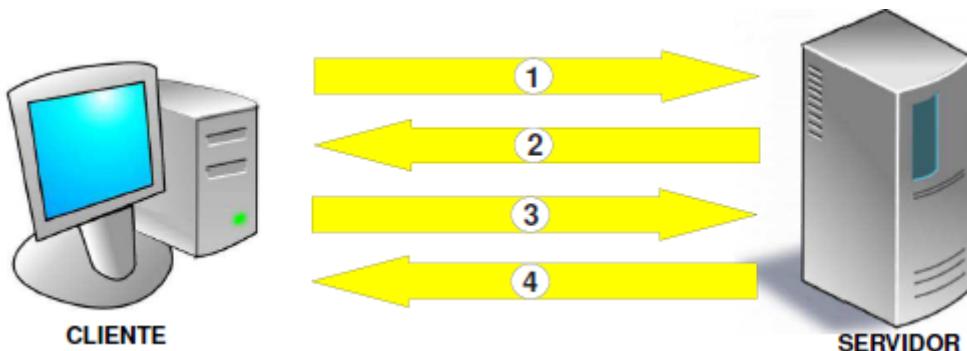
E qual é a vantagem em se usar o DHCP?

Quando temos uma pequena rede, com poucos hosts, normalmente desktops, é realmente interessante que se configure os IPs manualmente para um maior controle. Agora imagine uma rede em que haja muitos computadores e dentre eles muitos notebooks que entram e saem da rede com frequência. Tome como exemplo um hotel, onde cada hóspede pode usar a internet acessando a rede sem fio do estabelecimento em seu notebook, tablet, celular ou afim. Seria muito complicado para o administrador da rede, configurar os equipamentos de todos os hóspedes tendo em vista a rotatividade de pessoas no local.

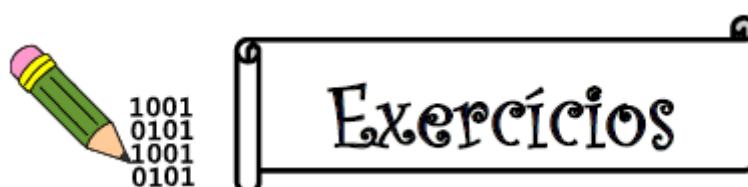
Neste caso, a melhor solução seria usar o protocolo DHCP para, a partir de um servidor DHCP, que pode ser um computador ou um ponto de acesso sem fio, atribuir IPs, máscaras, números de gateway e DNS nos hosts, de forma dinâmica, ou seja, variável.

Voltando ao exemplo, imagine o hóspede que estava usando a rede sem fio do hotel se dirigindo ao aeroporto para voltar à sua cidade de origem. Ao chegar ao aeroporto, este também precisa acessar a rede sem fio para se conectar à internet. Também neste momento, o servidor DHCP do aeroporto irá configurar o computador com os códigos da rede local. Note que para que o viajante consiga se conectar em ambas as redes sem precisar atribuir endereços de rede manualmente, em seu computador deverá rodar um software cliente DHCP.

Veja como funciona o processo:



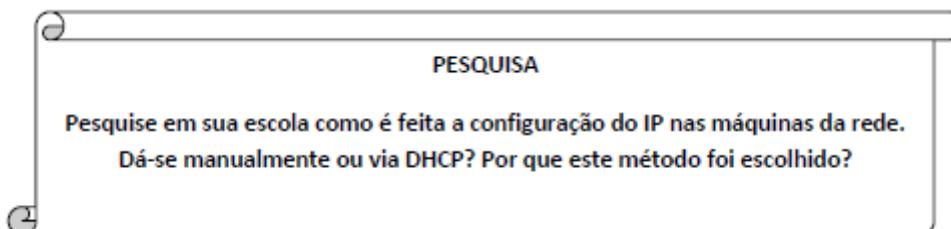
1. Descoberta DHCP: o cliente, que acaba de entrar na rede, não sabe qual host poderá fornecê-lo um IP, portanto envia uma mensagem através do protocolo UDP a todos os hosts da rede para o IP 255.255.255.255, que é o endereço de broadcast.
2. Ofertas DHCP: ao receber a mensagem de descoberta do cliente, o servidor DHCP responde enviando ao solicitante ofertando um IP disponível. Se houverem mais de um servidor DHCP na rede, todos eles enviam uma mensagem de oferta ao cliente.
3. Requisição DHCP: ao receber a(s) oferta(s), o cliente seleciona o IP que do servidor ao qual deseja se conectar e envia uma mensagem de requisição.
4. Confirmação DHCP: o servidor envia um acknowledge – ACK, confirmando a requisição.



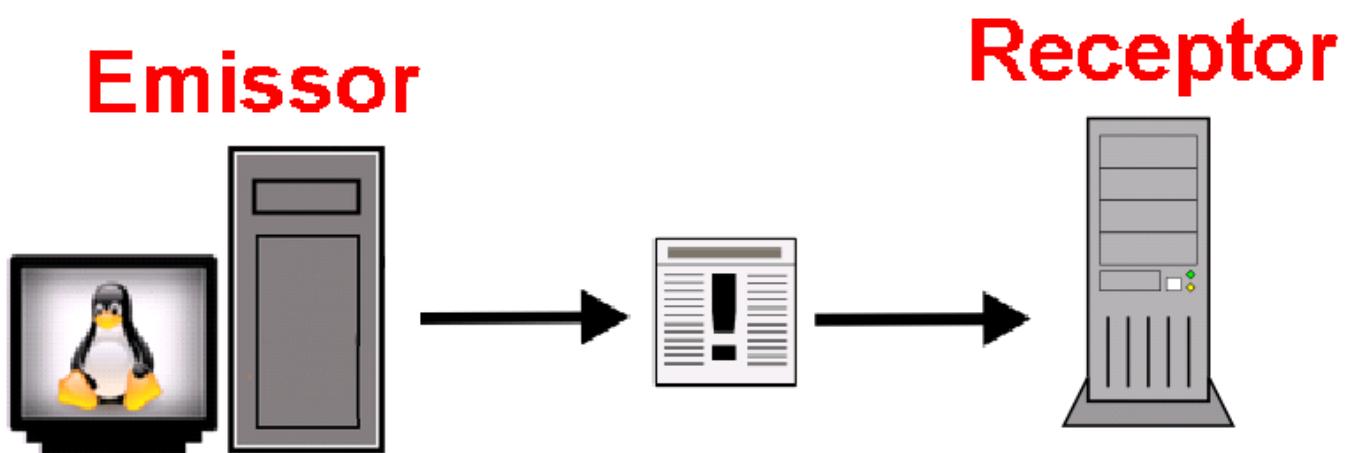
1. Explique brevemente as duas funções básicas da camada de Rede.

2. Retorne à Figura 5g e responda: “Se o host H2 quiser se comunicar com o host H1, qual valor de cabeçalho deverá conter no datagrama enviado ao roteador R1?”.

3. Se a versão 4 do IP está funcionando tão bem, por que as redes deverão migrar para a versão 6?



5.5. Camadas de enlace e física (modelo osi) ou interface com a rede (modelo tcp/ip)



Chegamos aos níveis mais baixos dos modelos de camadas. Níveis mais baixos também, pois são os que mais se distanciam da interação com o homem.

Antes de qualquer coisa, vamos lembrar o que é um enlace:



ENLACE

É um link de comunicação, ou uma ligação entre dois sistemas de rede. Por exemplo, a ligação entre um computador e um roteador ou a ligação entre dois roteadores em redes locais diferentes.

Por muito tempo, o enlace foi visto apenas como o fio que liga um host ou roteador a outro host ou roteador, mas com o advento das redes wireless, o fio deixou de ser o principal integrante de um enlace. Sendo assim, podemos ver, ou imaginar, um enlace como um canal de comunicação entre um host ou roteador a outro host ou roteador.

O PDU da camada de enlace é o quadro. Após receber o datagrama IP, a camada de enlace o coloca dentro de uma estrutura chamada quadro. Estes quadros viajam do host remetente ao host destinatário por uma sequência de enlaces. Ao chegar à camada de rede no destinatário, esta irá retirar o datagrama IP de dentro do quadro da camada de enlace.

Agora pense bem, quando vamos nos conectar a um site da Web, este pode estar em qualquer local do mundo, concorda? Imagine então quantos enlaces existirão no caminho entre o computador local e o servidor Web. Imagine também os mais diferentes tipos de enlaces neste caminho.

Você pode estar usando um notebook e se comunicando com um roteador wireless em uma rede sem fio, isto já é um enlace. Na sequência, o roteador da sua casa pode estar se comunicando com seu provedor de

internet via cabo de par trançado, num protocolo Ethernet ou usando uma linha telefônica, outro enlace. Ao chegar ao seu provedor, este poderá se comunicar com outro servidor usando protocolos WAN através de fibras ópticas, depois antenas Wi-Max, passar por outro cabo de par trançado num protocolo PPP (Protocolo Ponto-a-Ponto) e etc.

Em resumo, existem vários tipos de enlaces e a função fundamental da camada de enlace é fazer o datagrama IP passear pelos variados enlaces sem sentir a diferença entre eles e chegar ao destino, assim como prover alguns serviços, como: garantia de entrega, controle de fluxo, detecção e correção de erros.

5.5.1. Endereços MAC

Desde a camada de aplicação até a camada de rede, quem implementa os serviços e os protocolos é o host. Na camada de enlace, a implementação é feita por adaptadores. Adaptadores são as conhecidas placas de rede, tanto para redes com fio, quanto sem fio. O adaptador deve existir tanto no host remetente, pois é por onde o quadro da camada de enlace sai, quanto no host destinatário, que é por onde o quadro chega.

Neste adaptador é inserido um endereço de camada de enlace, ou endereço físico, mas é mais conhecido como endereço MAC – Media Access Control, ou Controle de Acesso ao Meio. Cada adaptador de rede do mundo tem seu próprio endereço MAC. É chamado de endereço físico porque fica gravado na ROM do adaptador e não deve ser alterado.



Mas se já existe um endereço IP, qual a necessidade de existir também um endereço MAC?

Veja bem, o endereço IP é um endereço lógico e deve ser inserido de acordo com a distribuição dos hosts pelas redes, e pode ser alterado, dependendo da necessidade. O endereço físico MAC acompanhará o adaptador do host aonde quer que ele vá. É como se o MAC identificasse o host e o IP identificasse onde mora o host.



E se a placa de rede (adaptador) de um host ficar defeituosa e for trocada por outra, o que acontece com o endereço MAC do host?

Como já dissemos, o MAC acompanha a placa de rede, ou adaptador.

Se ela for retirada, o MAC é retirado junto, e ao inserir uma nova placa, consequentemente o host terá um Informática – Redes de Computadores

novo endereço MAC.

Em algumas redes, o administrador cadastrá e gerencia os endereços MAC dos computadores, para que somente os MACs cadastrados possam ter acesso à rede, evitando o acesso de intrusos com outros computadores.

Assim como o DNS resolve nomes em IPs para um host, os endereços MAC também tem que ser resolvidos em IPs e o responsável por fazer tudo isto é o protocolo ARP – Address resolution Protocol, ou protocolo de Resolução de Endereços.

O ARP faz um mapeamento na rede de todos os endereços MAC à medida que eles vão enviando ou recebendo dados na rede e coloca estes endereços em uma tabela, chamada de tabela ARP.



1. O que é um enlace?

2. O que é um Endereço MAC?

3. Relacione os PDUs com as camadas:

(1) Camada de Aplicação.

(2) Camada de Transporte.

(3) Camada de Rede.

(4) Camada de Enlace.

() quadro

() segmento

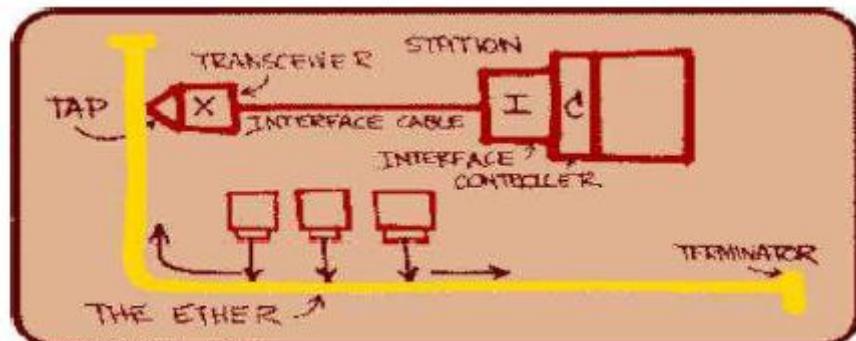
() dados

() datagrama

5.5.2. Ethernet

Existem muitas tecnologias de rede, mas de longe, a mais conhecida e usada de todas é a Ethernet, que surgiu dos termos ether: cabo coaxial e net:redes. Pode-se dizer então que o padrão Ethernet é usado em redes cabeadas, já que se estendeu também aos outros tipos de cabo além do coaxial, como o par trançado e a fibra óptica. Alguns autores afirmam que as redes wireless também fazem parte do padrão Ethernet, mas como a maioria discorda, não vamos entrar nessa discussão neste momento.

Este padrão começou a ser desenvolvido em meados da década de 70 por Bob Metcalfe que fez o seguinte desenho de seu projeto:



O padrão original da Ethernet possuía 2.94 Mbps e usava cabos coaxiais. Este padrão deu origem a outros dois: o 10BASE-5 e o 10BASE-2.

Logo em seguida surgiram os padrões 10BASE-T e o 10BASE-F.



O que todos estes padrões têm em comum?

A velocidade. Todos eles transmitiam dados a 10 Mbps, daí o significado do número 10 no início dos

nomes. O termo BASE vem de baseband modulation, o que significa que o sinal é percorrido de forma digital e não mais de forma analógica, dispensando o uso de modems telefônicos.

Vejamos as características:

- 10BASE-5: usava cabos coaxiais pesados e pouco flexíveis do tipo thicknet, transmitia a 10 Mbps e o sinal poderia chegar a até 500 metros de comprimento.
- 10BASE-2: surgiu em seguida, usando cabos coaxiais mais leves e flexíveis do tipo thinnet, transmitia a 10 Mbps e o sinal poderia percorrer uma distância de até 185 metros pelo cabo.
- 10BASE-T: é a evolução do Ethernet do cabo coaxial para o cabo de par trançado. A letra T no fim do nome vem de twisted pair, ou par trançado. Este padrão também transmite a 10 Mbps e o sinal percorre até 100 metros.
- 10BASE-F: neste padrão já é utilizada a fibra óptica, indicada pela letra F de fiber optic. É um padrão com custo muito elevado, portanto não foi muito utilizado. O sinal podia chegar a 2000 metros de distância.

Todos estes padrões de 10 Mbps tornaram-se obsoletos e não são mais utilizados. A grande evolução dos padrões Ethernet fez surgir o Fast Ethernet, um padrão que aumentava em 10 vezes a velocidade da transmissão. Dentre os padrões Fast Ethernet lançados os principais são:

- 100BASE-TX: É o padrão mais popular entre todos. Possui taxa de transmissão de 100 Mbps, uma boa evolução em relação ao 10BASE-T, seu correspondente Ethernet. Ele usa o cabo de par trançado e nele o sinal percorre até 100 metros. O cabo UTP mais utilizado no 100BASE-TX é o de categoria 5, onde dos 4 pares apenas dois são utilizados, um para enviar e outro para receber. [MORIMOTO, 2010]. Os outros dois pares não utilizados para transmissão ficam fazendo o papel de isolamento contra interferências eletromagnéticas, uma grande vantagem neste padrão.
- 100BASE-FX: é o Fast Ethernet para uso com fibra óptica e transmite a 100 Mbps.

No caminho da evolução surgiu o padrão Gigabit Ethernet que eleva a velocidade de transmissão de 100 Mbps (Fast Ethernet) para 1000 Mbps, ou 1 Gbps, daí o nome Gigabit.

- 1000BASE-LX: padrão para cabos de fibra óptica, utiliza lasers que são mais rápidos que leds, porém muito mais caros. Seu alto nível qualidade oferece um alcance de sinal de até 10 km, portanto é um padrão muito utilizado para redes de longa distância.

- 1000BASE-SX: também feito para uso com fibra óptica, porém usa lasers de curta distância, barateando os custos, o que leva a uma redução do alcance para no máximo 275 metros.
- 1000BASE-CX: este padrão já passa a usar cabos de par trançado, porém apenas os STPs ou SSTPs, ou seja, cabos blindados. Chagou a ser mais utilizado logo após seu lançamento, por ser mais barato que a fibra óptica, mas com o aparecimento do 1000BASE-T, ele praticamente caiu em desuso.
- 1000BASE-T: é o padrão para cabos de par trançado e ainda por cima, UTPs, ou seja, sem blindagem. Este padrão fez o Gigabit Ethernet começar a se popularizar, pois além de diminuir e muito os custos, seu complexo sistema de transmissão permitiu manter a distância de propagação do sinal em 100 metros, os mesmos usados no 10BASE-T e no 100BASE-FX.

Por último, mas não menos importante, temos o surgimento do mais atual padrão Ethernet: o 10 Gigabit Ethernet. É isso mesmo que você está pensando, ele multiplica por 10 o Gigabit Ethernet. Possui taxa de transmissão de 10Gbps (10 gigabits por segundo), ou 10.000 Mbps. É de longe o padrão mais veloz, porém ainda não muito popular. Para uso com fibras ópticas temos

Por último, mas não menos importante, temos o surgimento do mais atual padrão Ethernet: o 10 Gigabit Ethernet. É isso mesmo que você está pensando, ele multiplica por 10 o Gigabit Ethernet. Possui taxa de transmissão de 10Gbps (10 gigabits por segundo), ou 10.000 Mbps. É de longe o padrão mais veloz, porém ainda não muito popular. Para uso com fibras ópticas temos vários padrões como os 10GBASE-LR, 10GBASE-ER, 10GBASE-ZR, 10GBASE-SR e 10GBASE-LRM. A princípio imaginou-se que com este padrão não seria possível o uso de cabos de par trançado e que obrigatoriamente, quem quisesse aumentar a velocidade de transmissão usando este padrão teria que migrar para a fibra óptica, mas como podíamos prever, os pesquisadores estudaram várias formas até conseguir criar um padrão que usasse o par trançado, foi então que surgiu o 10GBASE-T, onde o cabo ideal para uso é o categoria 6.

No 10GBASE-T, surgiram algumas condições para que fosse possível usar os cabos categoria 6: os 4 pares do cabo são utilizados para transmissão de dados, extinguindo assim os cabos que faziam o isolamento contra interferências eletromagnéticas. A distância percorrida pelo sinal passou de 100 para 55 metros, pois a partir daí o sinal começa a atenuar. Ao utilizar o 10GBASE-T, deve haver um cuidado especial com a crimpagem dos cabos e evitar ao máximo os ruídos que gerem interferências, como antenas e cabos elétricos próximos aos cabos de dados.

PESQUISA

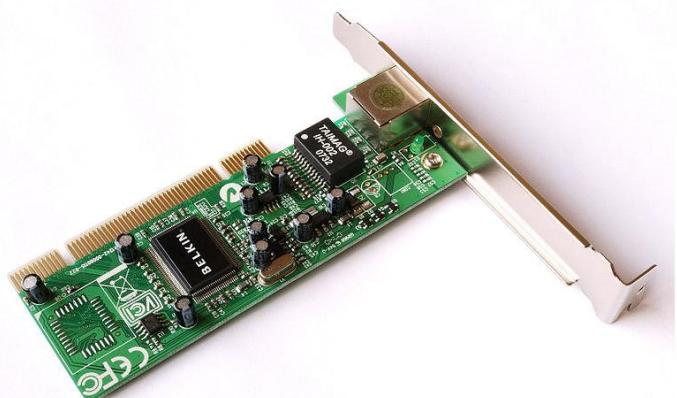
Pesquise na rede de sua escola se é usado algum padrão Ethernet. Qual deles é utilizado?

5.6 Os dispositivos ativos e passivos

As redes de computadores sejam LAN's, MAN's, WAN's, PAN's são concebidas para garantir aos clientes acesso aos mais variados serviços e compartilha uma ampla gama de recursos, como impressoras, scanners, softwares e demais informações com simplicidade e eficiência.

Estas redes utilizam dispositivos para permitir que as transmissões/recepções ocorram. Assim, os componentes são divididos em dois grupos:

Passivos – Garantem o transporte através do meio físico (como exemplos temos: antenas, cabos, demais acessórios para cabeamento e tubulações). São denominados passivos pois não necessitam de uma alimentação elétrica e não realizam nenhum “trabalho” mais aprimorado.

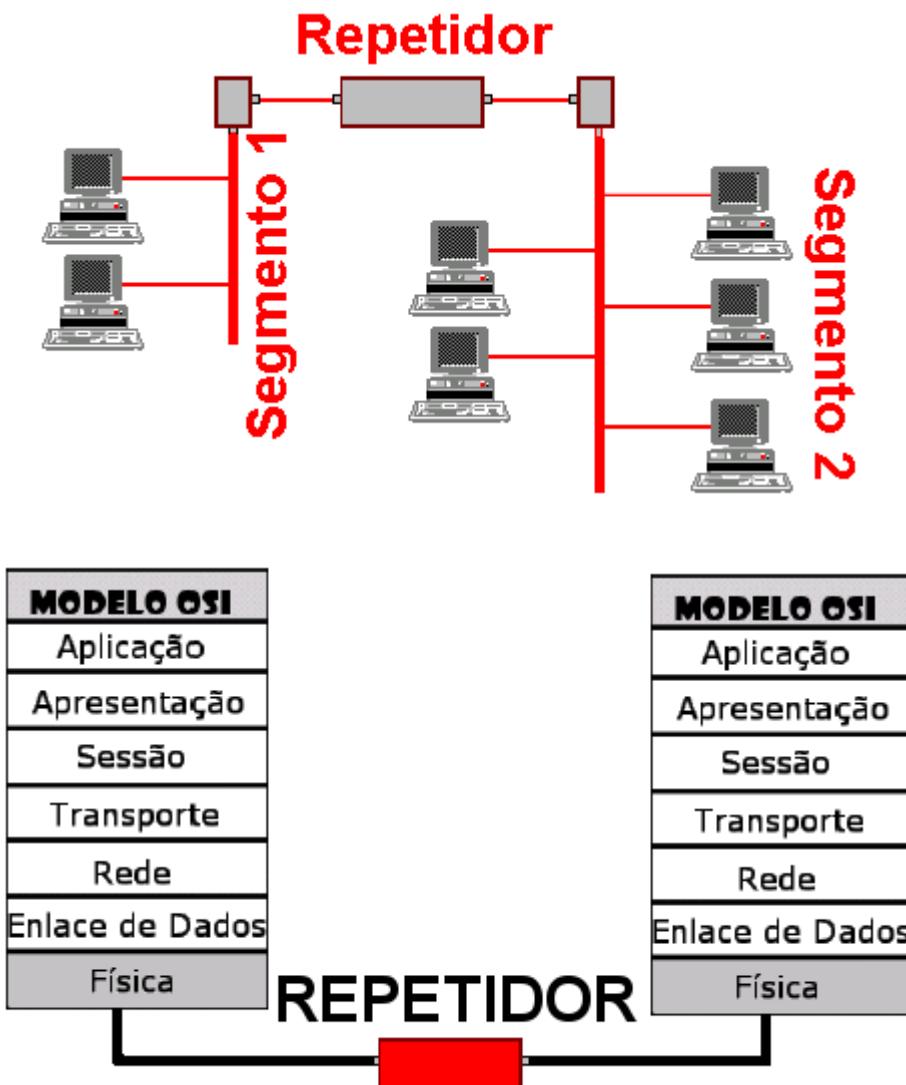


Ativos – São responsáveis pelas comunicações realizadas pelos mais variados dispositivos atuantes na rede como servidores, estações, etc. São componentes ativos os hubs, repetidores, as pontes, os switches, os roteadores, etc. Eles necessitam de alimentação elétrica e realizam “atividades” um pouco mais “complexas” na maioria das vezes.

Assim, esse conjunto formado por componentes passivos e ativos é que possibilita as comunicações realizada pelas redes, sejam estas: LAN's, MAN's, WAN's e PAN's. Logo, este deve adotar uma tecnologia em comum, como a Ethernet, de modo a possibilitar comunicações na rede.

5.7 Repetidores

O Repetidor é um equipamento utilizado para interligação de redes idênticas, pois eles amplificam e regeneram eletricamente os sinais transmitidos no meio físico.



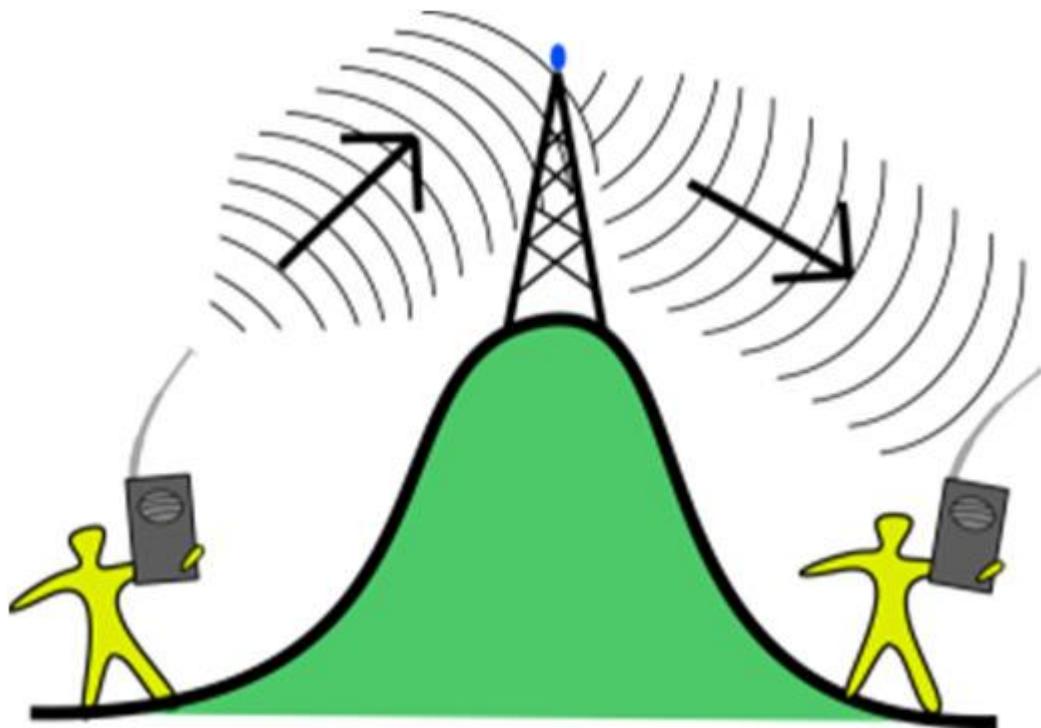
Os repetidores atuam na camada física (Modelo OSI), assim recebem os sinais das transmissões de cada rede que interligam para retransmiti-los nas outras redes.

Lembrando que repetidores não executam nenhum tipo de tratamento sobre as informações retransmitidas por eles. Como recomendação evita-se utilizar esses componentes ativos em LAN's, porque eles degeneram o sinal no domínio digital e provocam problemas de sincronismo entre as interfaces de rede.

5.7.1. Repetidores Wireless

Em redes wireless, os repetidores (também chamados de "expanders", ou expansores) atuam como intermediários entre o ponto de acesso principal e os clientes, assim estes retransmitem os sinais de Informática – Redes de Computadores

comunicação. O conceito é bem simples, eles permitem melhorar a cobertura em pontos cegos da rede, favorecendo o sinal que chega até os clientes, ou para superar obstáculos (posicionar o repetidor em uma posição em que ele tenha uma trajetória com o gerador de sinais principal – muitas vezes um Access Point – e também com o cliente, permitindo assim que o sinal "faça a curva", evitando obstáculos).



Desse modo, usar repetidores permite aumentar o alcance das transmissões, que muitas vezes utilizam as mais variadas tecnologias em ondas de rádio, como redes wireless, wimax e mesmo a conhecida telefonia celular de nosso dia-a-dia.

Uma vez configurados, os repetidores precisam ser apenas alimentados por energia elétrica. Pode-se também supri-los com energia solar, combinando placas solares com baterias e inversores, de modo a conseguir repetidores completamente autônomos.

5.8 Hubs

Hubs são dispositivos ativos que concentram a ligação entre diversos computadores que compõem as LAN's, estes eram muito utilizados no começo das redes de computadores, agora estão em quase desuso. São também conhecidos genericamente como concentradores; os hubs são equipamentos de rede muito fáceis de instalar e gerenciar.



Os Hubs são dispositivos que trabalham na Camada Física (primeira camada) do modelo OSI, pois eles geram novamente o sinal e o retransmitem para todas as suas portas. Hubs são elementos de conexão que atuam como repetidores, assim concentram as conexões físicas nas LAN's. Lembrando que, em redes Ethernet, cada computador da rede é ligado a uma das portas do hub por meio de cabos pares trançados.

Antigamente entre as vantagens na utilização dos hubs, podia-se citar a criação de um ponto de conexão central para os cabos na rede, assim era facilitada a instalação e manutenção dos pontos de rede, o aumento da confiabilidade da rede, pois permitia que defeitos acontecessem num único cabo ou apenas afetasse a máquina conectada ao cabo defeituoso.



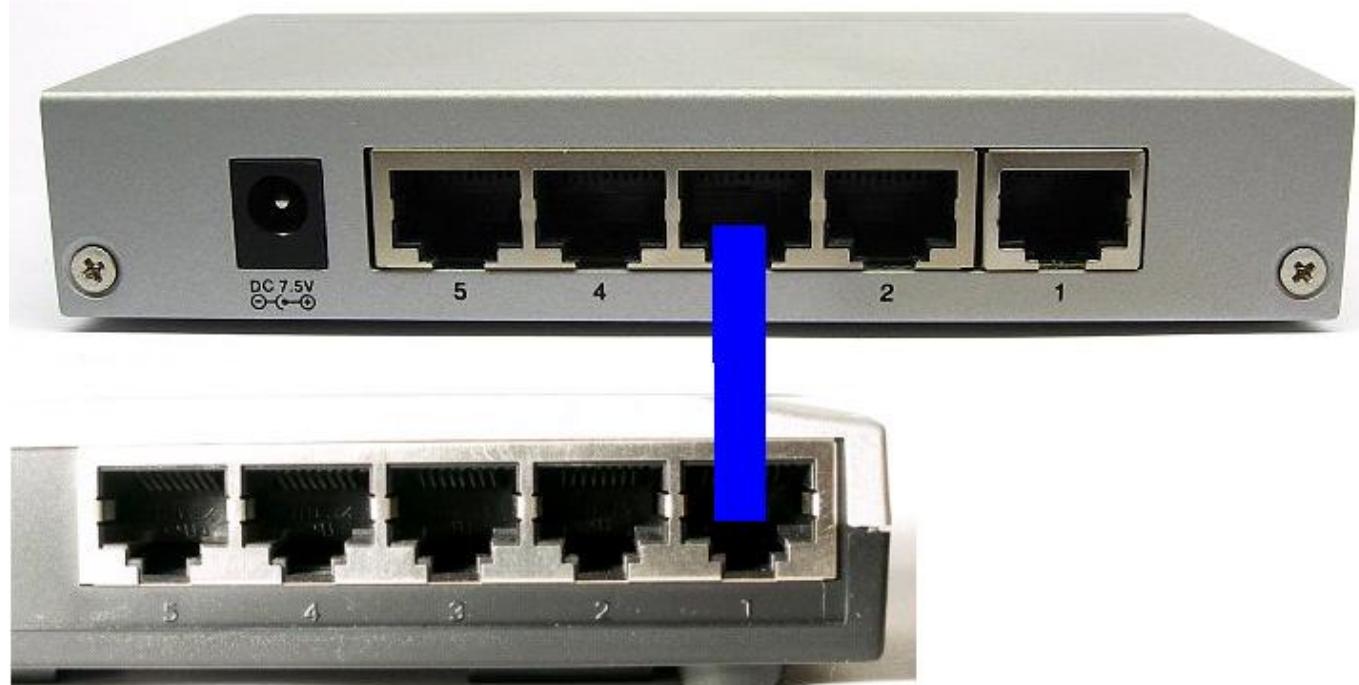
Diferentemente da já estudada topologia em barra onde, se houver uma falha no cabo, pode paralisar toda a rede. Embora a topologia física de uma rede que utiliza HUBs seja em estrela, já a lógica assemelha-se a topologia em barramento, pois as máquinas em rede não são identificadas e todas recebem tráfego toda vez que algum computador transmite.

5.8.1. Interligando Hubs

Grande parte dos modelos de hubs permitem ser interligados com outros hubs de duas maneiras: empilhamento e cascamenteamento.

Cascamenteamento permite que hubs sejam interligados hierarquicamente. Assim, em configurações com mais de dois dispositivos deve-se dividi-los em hubs terminais (denominados HHub – Header Hub) que ficam nos extremos do conjunto, como os hubs intermediários (chamados de IHubs – Intermediary Hubs).

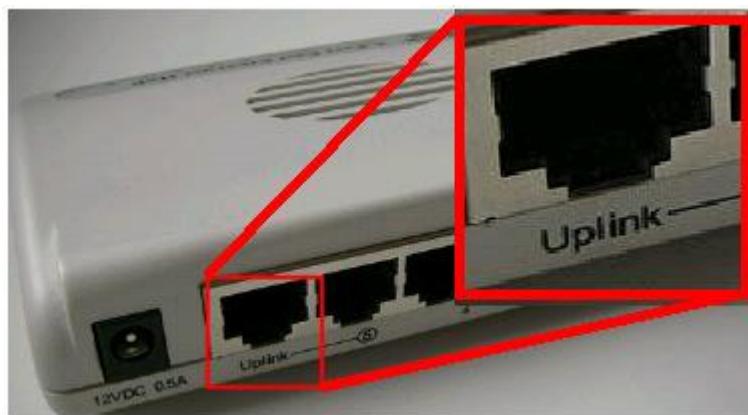
No cascamenteamento a interligação é realizada por meio de uma das portas do HUB com outras portas de outros dispositivos de equipamento, sendo a velocidade de transmissão limitada à velocidade da porta. As regras para o cascamenteamento dependem das especificações dos dispositivos, porque neste tipo de ligação, à medida que vai se "cacasteando", ou seja, conectando mais e mais hubs, o desempenho da rede tende a diminuir.



Normalmente utilizam-se portas específicas para este fim, chamadas Up-Link. Essas portas utilizam cabeamento comum, dispensando a utilização de cabo cross-over. Convém observar que em alguns Informática – Redes de Computadores

modelos é necessária a ativação desta porta especial, logo é necessário ler o manual do fabricante.

Cascadear hubs é barato e prático, porém ocupa portas que poderiam ser usadas para conectar outros dispositivos na LAN. Para obter a quantidade de portas disponíveis para cascadear hubs utiliza-se a expressão: $2n-2$, com n representando o número de hubs usados no cascadeamento.



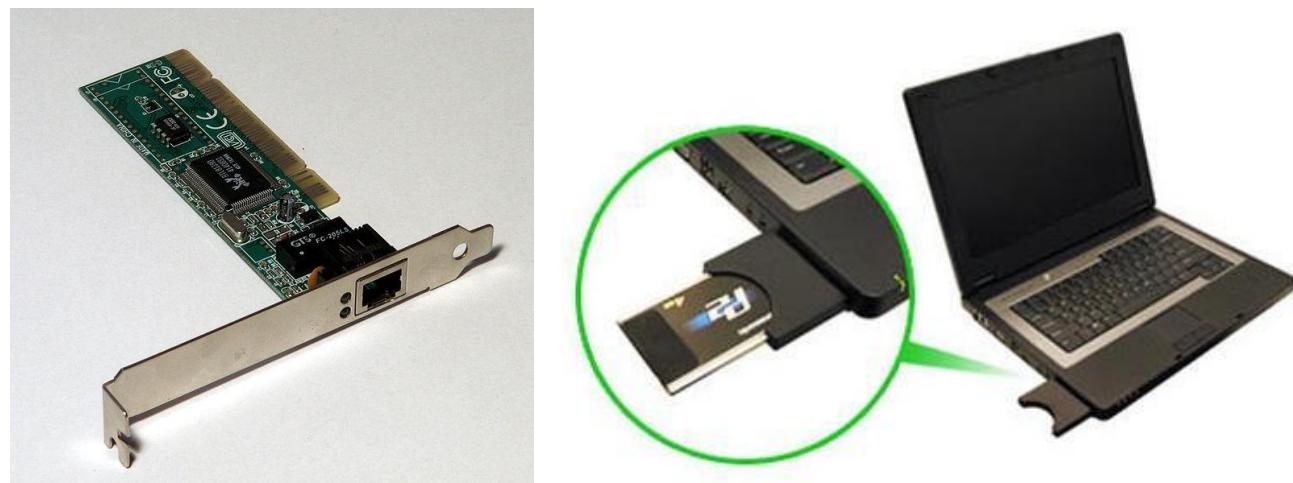
Já no empilhamento, a interligação ocorre através de uma porta específica para empilhamento (conhecida por stack) e cada fabricante possui um tipo de interface própria, a qual possui velocidade de transmissão maior que a velocidade das portas de conexão. Hubs assim empilhados tornam-se um único dispositivo.

LEMBRE-SE – O empilhamento é mais eficiente do que o cascadeamento porque não ocupa as portas, aumentando com isso a quantidade de portas disponíveis para os equipamentos da rede.

Pode-se empilhar vários hubs, contudo deve-se analisar as observações e limitações de cada modelo.

5.9 Placas de redes e o endereço MAC

Placas de rede são tipos de placas de expansão que permitem aos dispositivos executar comunicações em redes. Estas são conhecidas como adaptadores de rede ou Network Interface Card (NIC).



As placas de rede são dispositivos capazes de realizar comunicações entre servidores, estações e demais dispositivos. A grande maioria das placas de rede utiliza ou são compatíveis com a Ethernet.

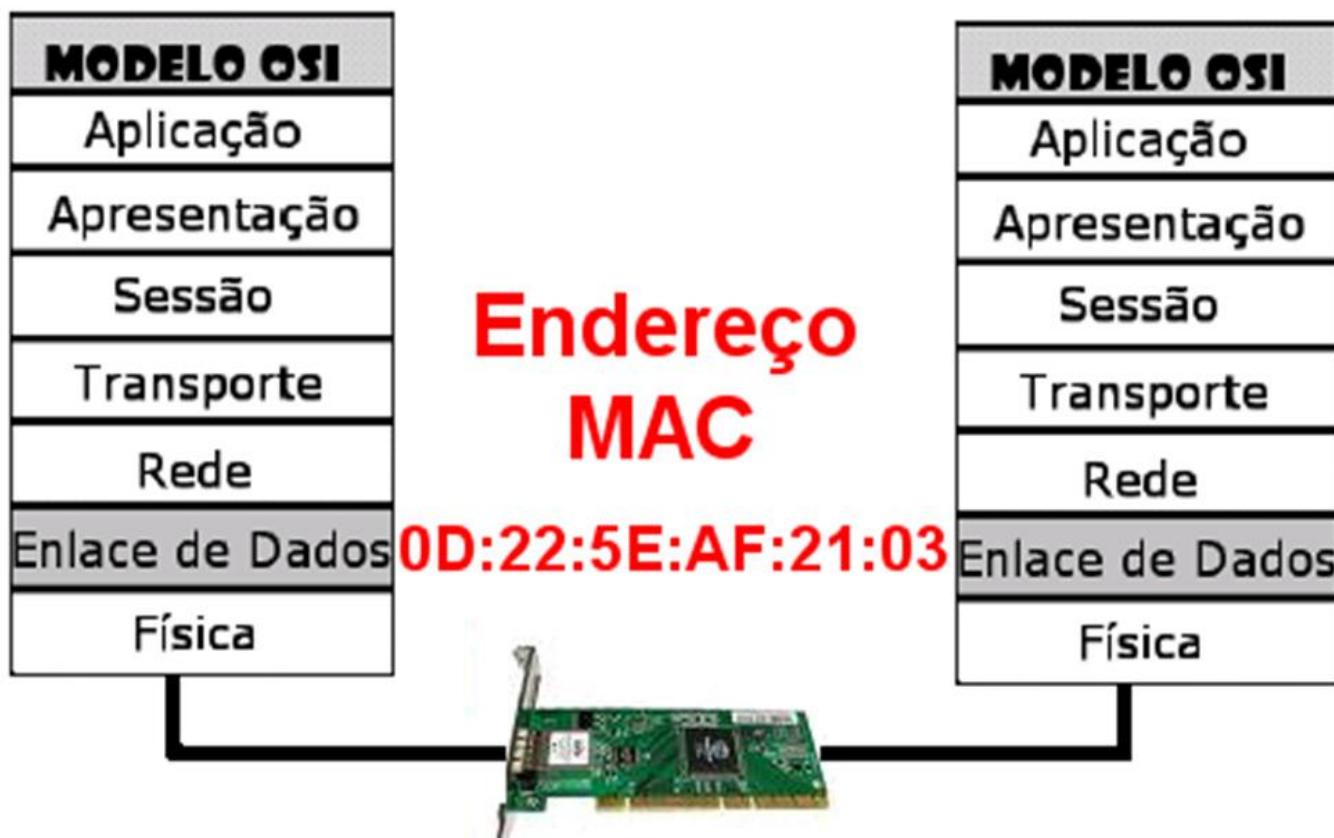
Existe no mercado uma grande variedade de placas de rede com diferentes taxas de transmissão e tecnologias implementadas nestas, sendo muitas placas para redes sem fio, conhecidas por Wireless Network Interface Card (WNIC).

5.9.1. O endereço MAC

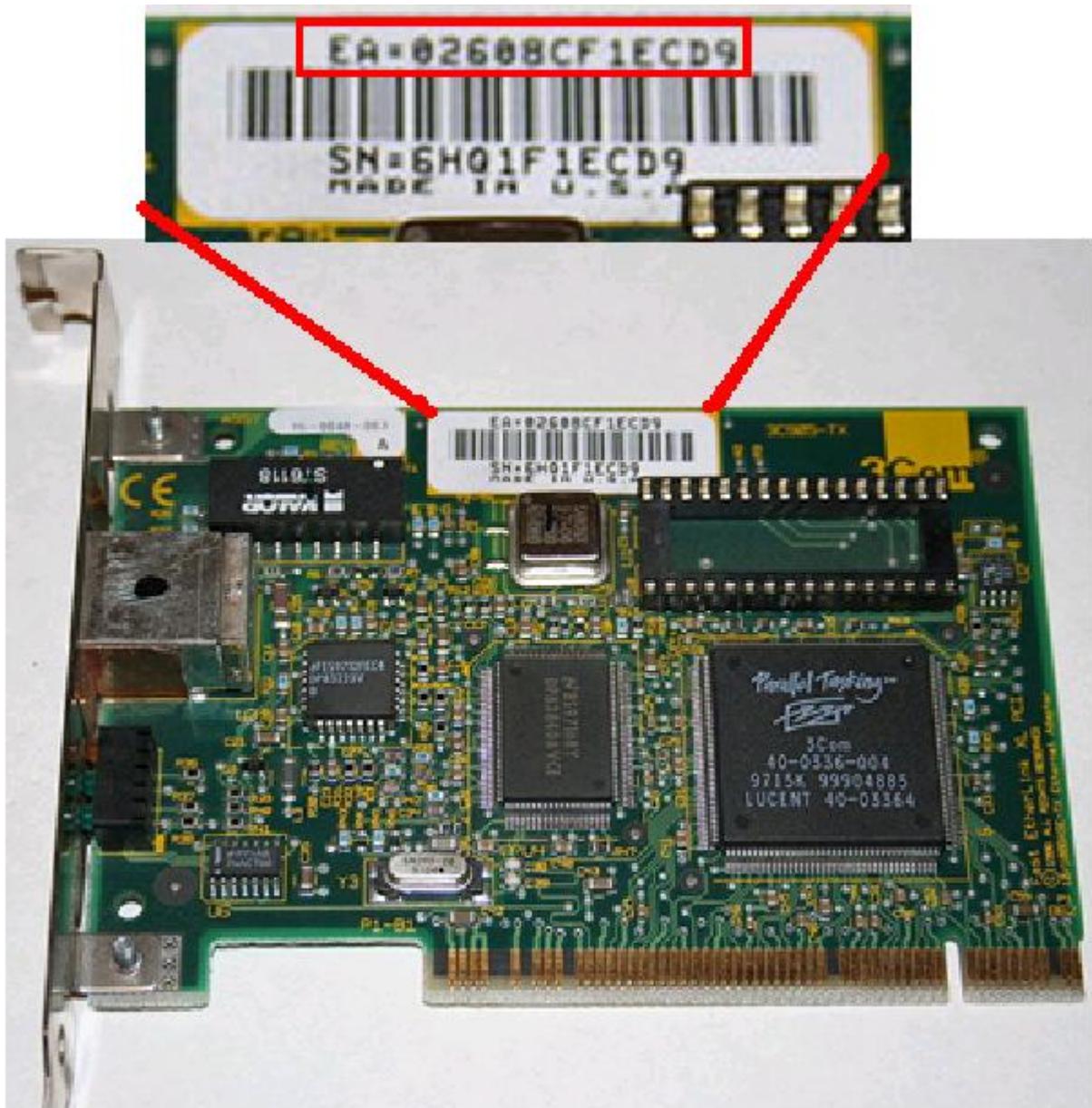
O que diferencia uma placa de rede Ethernet de outra? Estudamos que na topologia em estrela, ao contrário da topologia em barra, todos os dados são transmitidos para todas as estações na barra; uma estação somente recebe as transmissões destinadas a esta estação, ela não precisa receber os dados de outras estações e descarta dados que não são para ela.

Então como isso é feito? A resposta para essas perguntas chama-se endereço Media Access Control (MAC).

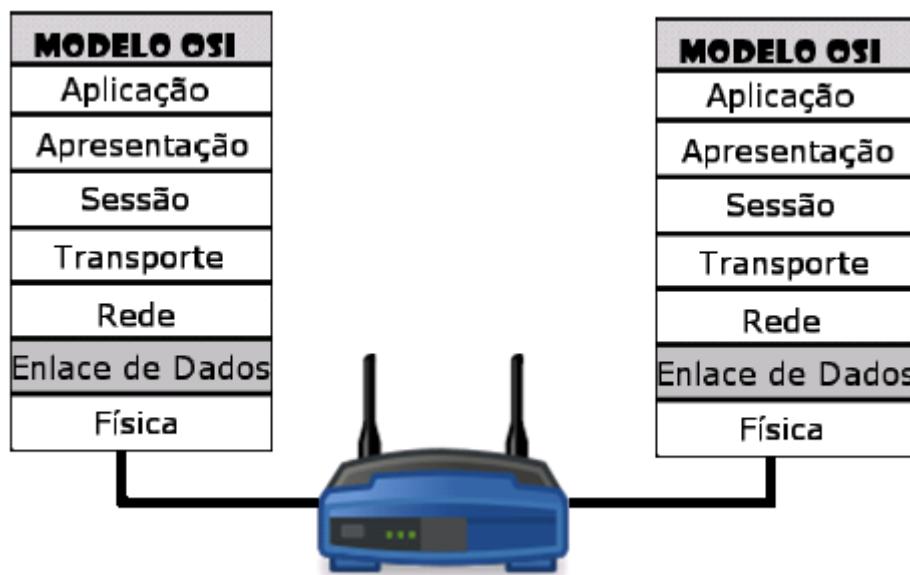
Denomina-se MAC um endereço físico de 48 bits, presentes em toda e qualquer placa de rede, seja placa de expansão, cartão de notebook/laptop, placa sem fio, etc. O MAC é implementado na Camada Enlace de dados ao Modelo OSI. Exemplo de endereço MAC: 0D:22:5E:AF:21:03



No endereço MAC a identificação do fabricante cabe aos três primeiros octetos (no exemplo 0D:22:5E), já os últimos três octetos são implementados pelos fabricantes de placas de rede.



O endereço MAC, assim como a impressão digital, é teoricamente um endereço único, deste modo não deve existir duas ou mais placas de rede com o mesmo endereço MAC. Para visualizar o endereço MAC no LINUX basta digitar ifconfig em algum terminal.



O endereço MAC, assim como a impressão digital, é teoricamente um endereço único, deste modo não deve existir duas ou mais placas de rede com o mesmo endereço MAC. Para visualizar o endereço MAC no LINUX basta digitar ifconfig em algum terminal.

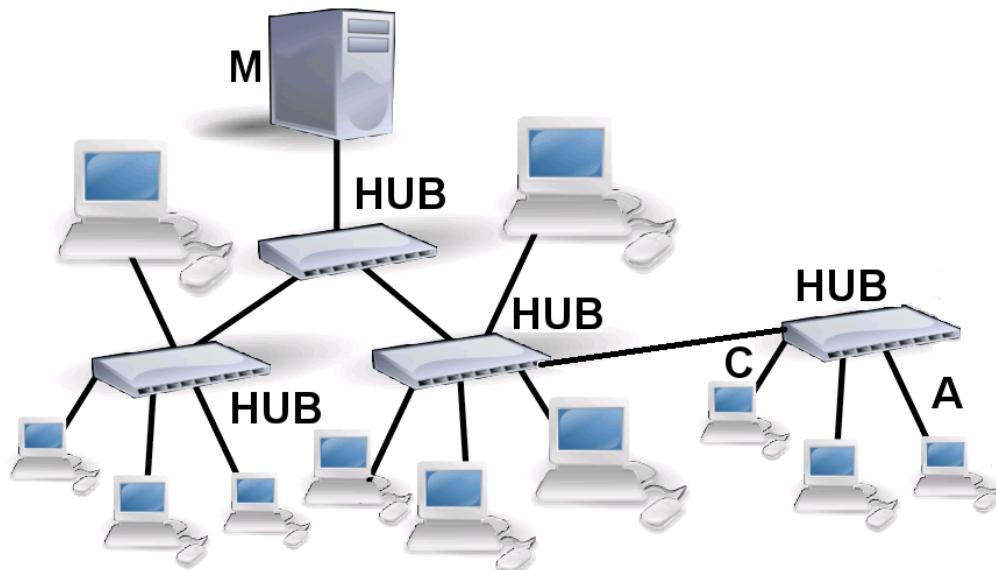
5.10. Pontes

As bridges (pontes) são dispositivos ativos utilizados para permitir interconectar dois segmentos de rede, assim estes dois passam a formar uma mesma rede.

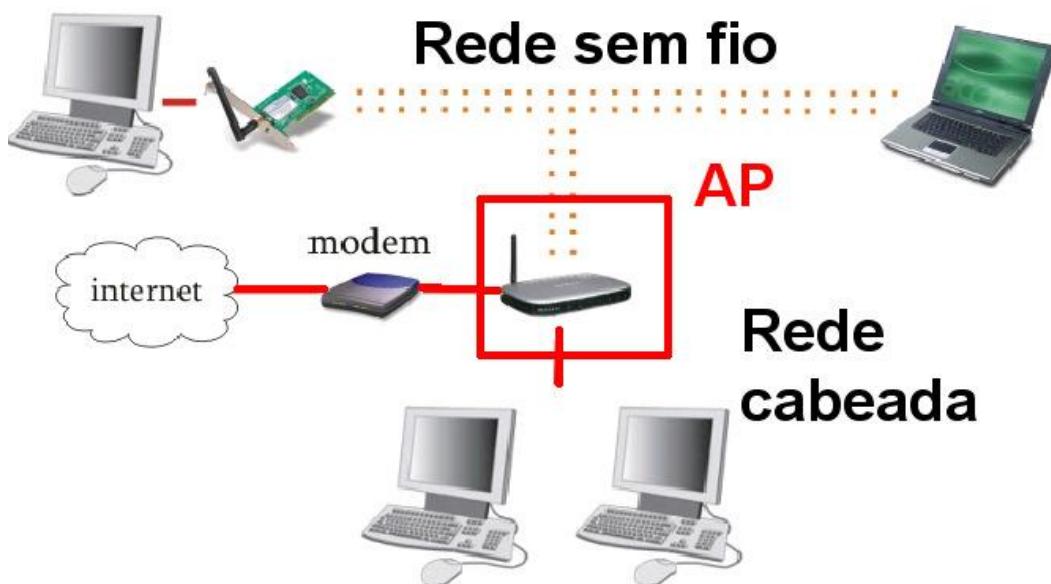
Antigamente existia o cabeamento com cabo coaxial, ou par trançado com hubs, assim o uso de pontes dividia a rede em segmentos menores, reduzindo o volume de colisões e melhorando o desempenho da rede.

Uma ponte trabalha na Camada de Enlace do modelo OSI, pois elas trabalham com os endereços MAC da placa de rede (máquina que transmite) e o MAC da máquina destino, de modo a encaminhar apenas as comunicações necessárias de um segmento a outro.

Atualmente isso é feito por switches, mas quando se usava apenas hubs, as pontes eram muito utilizadas para evitar colisões e melhorar a performance das redes, pois, ao invés de ligar um hub diretamente a outro, o que aumentava as colisões, conectava-se um hub a outro por meio de uma ponte.



Outra utilidade dos bridges é unificar segmentos de rede baseados em mídias diferentes. Antigamente, quando ainda estava acontecendo a transição das redes com cabos coaxiais para as redes de par trançado era muito comum o uso de pontes para interligar uma rede (cabeamento coaxial) na outra (cabo par trançado com hub) e o usuário nem se preocupava com isso.



Atualmente as pontes mais utilizadas são os Access point wireless, pois interligam duas redes diferentes (uma rede cabeada e uma rede sem fio, criando uma só rede).

Segmento 1



HUB

Segmento 2



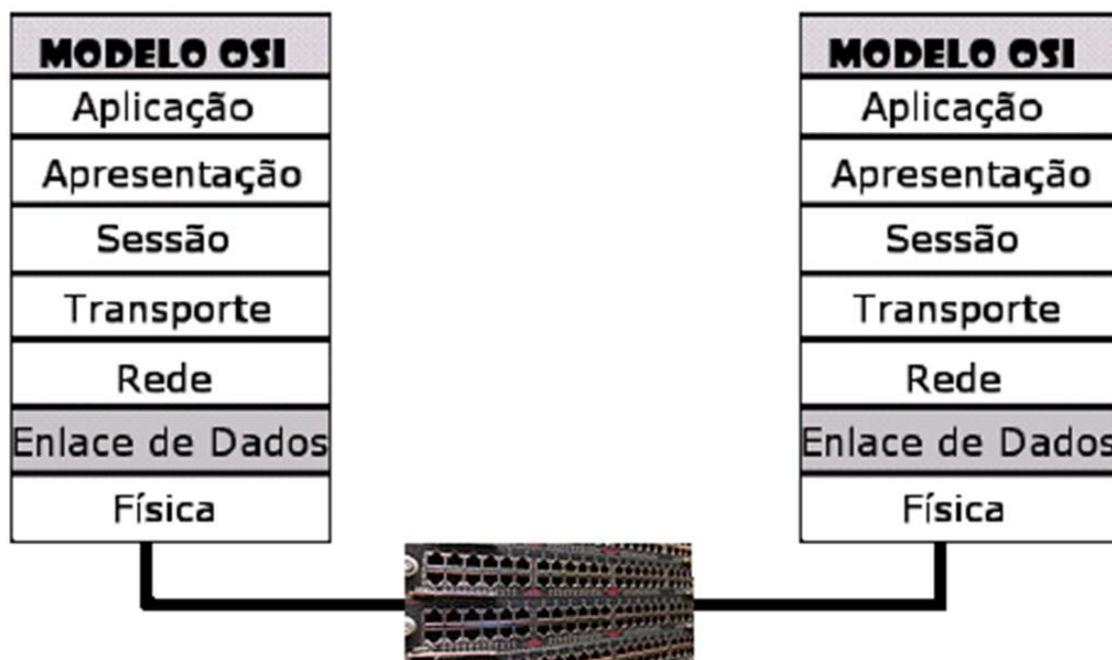
HUB

PONTE

5.11 Switches

5.11.1. Definição e funcionamento

Switch é um dispositivo ativo capaz de filtrar e encaminhar os pacotes entre as máquinas conectadas em suas portas. Este dispositivo também é conhecido por comutador, atuando na Camada de Enlace do Modelo OSI. Lembrando que switches são utilizados na topologia em estrela.



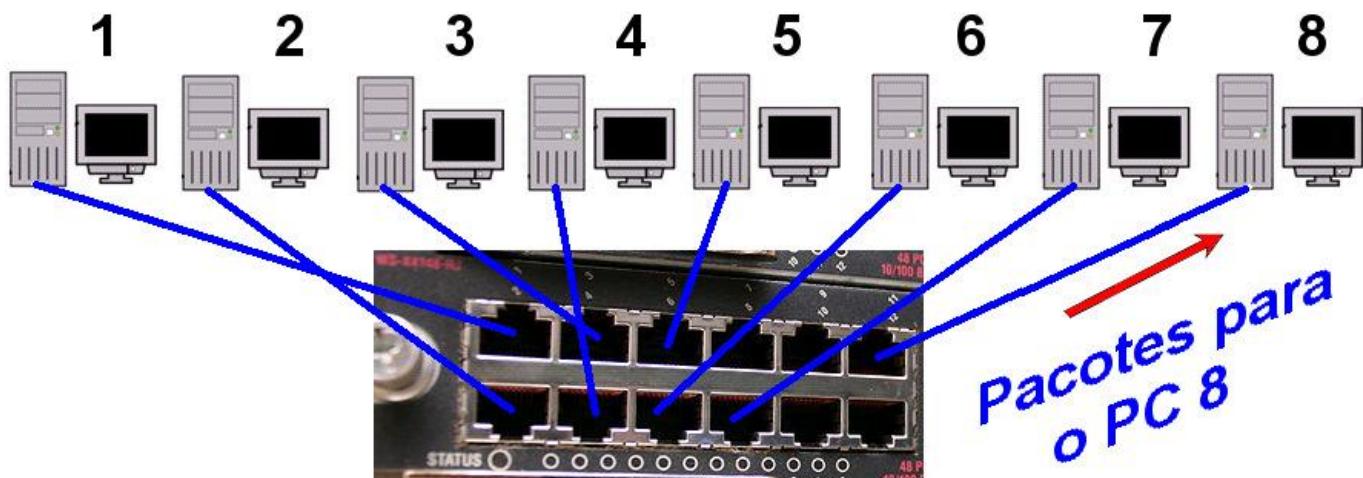
Lembram daqueles desenhos animados onde um personagem liga para alguém, e antes disso atende uma mulher (chamada telefonista) que, sentada de frente a um painel tendo uma mesa com vários pontos de telefones, assim o personagem dizia o número de quem desejava falar e a telefonista conectava

(comutava) os dois telefones e ambos podiam conversar.

Claro que no desenho animado muitas vezes a pobre telefonista era alvo das brincadeiras dos personagens. Os switches operam de modo semelhante a essa telefonista.

Os switches analisam e encaminham os pacotes da máquina origem (analisa o MAC da placa de rede do computador origem) para o destino (analisa o MAC da placa de rede do computador destino). Isso é possível graças ao fato do switch atuar na segunda Camada do OSI (Enlace de dados).

Assim, uma das grandes diferenças entre um hub e um switch deve-se ao fato que os hubs retransmitem todas as transmissões que recebem por qualquer uma de portas para todas as outras portas, daí apenas uma máquina conseguirá transmitir por vez.

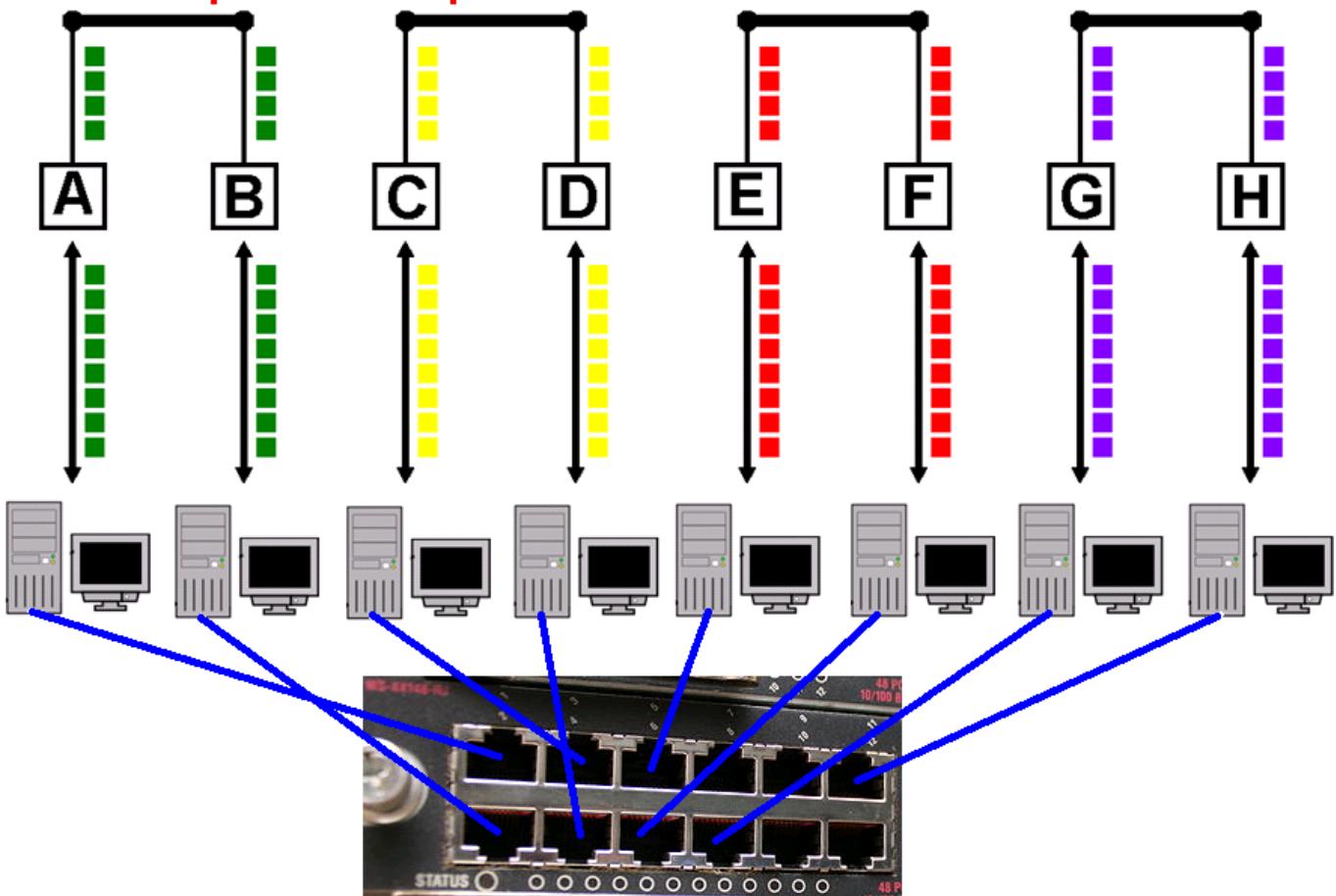


Os switches são capazes de implementar canais de comunicação exclusivos entre o computador, que envia os pacotes dados, e a máquina, destino dessas transmissões, assim inúmeros computadores ficam transmitindo e recebendo dados ao mesmo tempo. Desde modo a performance da rede melhora bastante.

5.11.2. Tipos de Switches

Atualmente quase não mais se utiliza hubs, eles são encontrados apenas em redes antigas, pois está disponível a venda produtos denominados "hub-switches", que são tipos de switches mais baratos. Outra opção é o denominado switch "verdadeiro", que são modelos aptos a gerenciar um número maior de portas que as disponíveis nos "hub-switches" que são mais simples.

O switch fechou canais exclusivos de comunicação entre os computadores que estão comunicando-se mutuamente

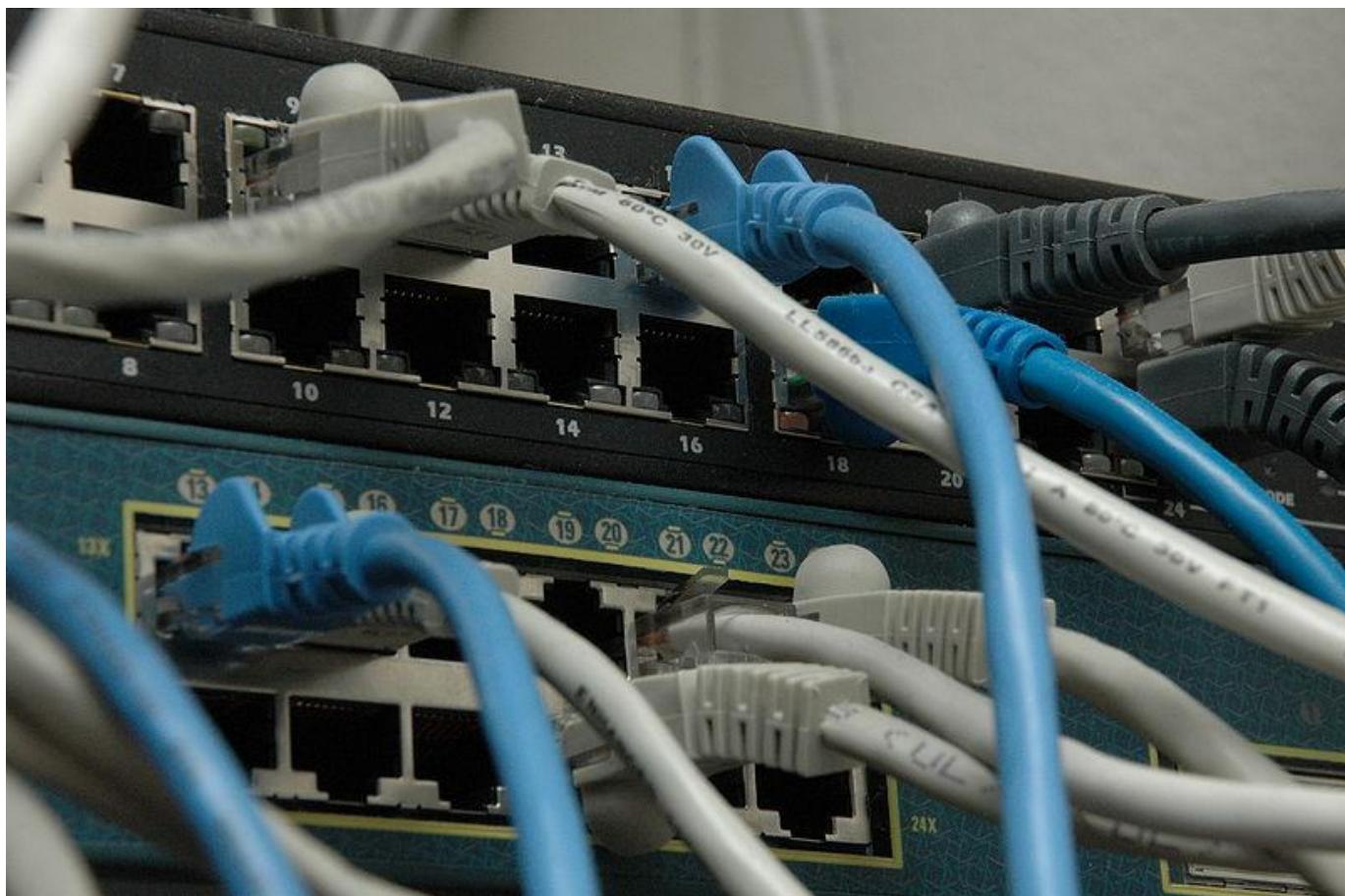


Switches "verdadeiros" e "hubswitches" operam no nível na segunda camada do OSI. Então, quais as diferenças entre ambos?

Eles diferem nas capacidades de gerenciamento e no número de portas disponíveis, assim enquanto os "hub-switches" possuem nenhum ou pouco gerenciamento além de um número reduzido de portas, os switches "verdadeiros" são dotados de interfaces para facilitar o gerenciamento, pois muitas vezes podem ser acessados utilizando navegadores web.

Atualmente é cada vez mais comum as empresas fabricantes desses produtos incorporarem características de produtos diversos num único produto, pois a concorrência no setor de dispositivo de rede é muito acirrada; essas empresas buscam conquistar cada vez mais clientes.

Deste modo, pode-se comprar um dispositivo que possui as características de dois ou mais equipamentos incorporados, esses produtos muitas vezes possuem uma pequena elevação no seu preço, assim é muito vantajoso para os clientes adquiri-los.

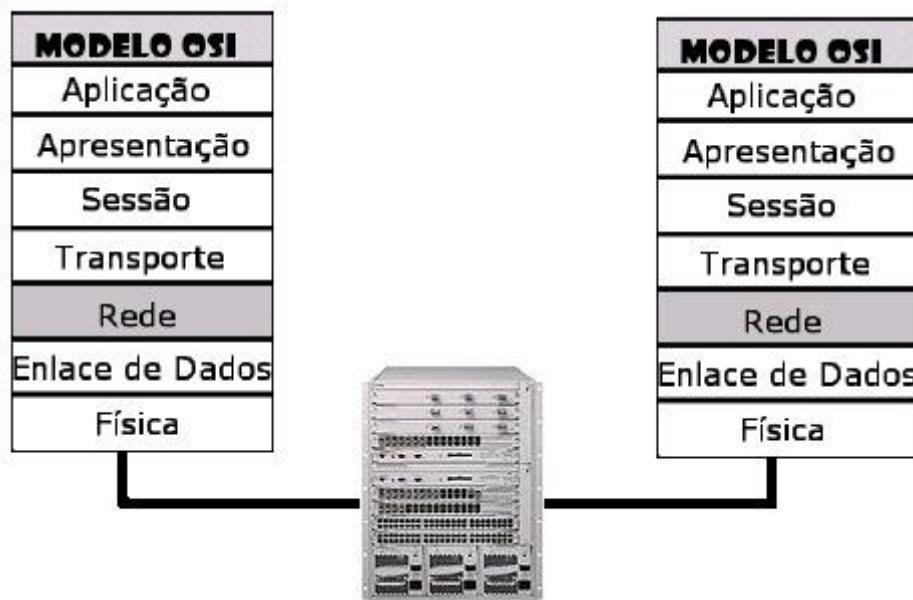


Seguindo essa tendência, pode-se encontrar no mercado dispositivos como os denominados "level 3 switches", um tipo de switch que executa algumas operações realizadas por roteadores.

5.12 Roteadores

Um roteador (router) é um dispositivo de rede ativo utilizado para interligar redes diferentes. São capazes de escolher a “melhor rota” por onde os pacotes serão enviados de uma rede à outra.

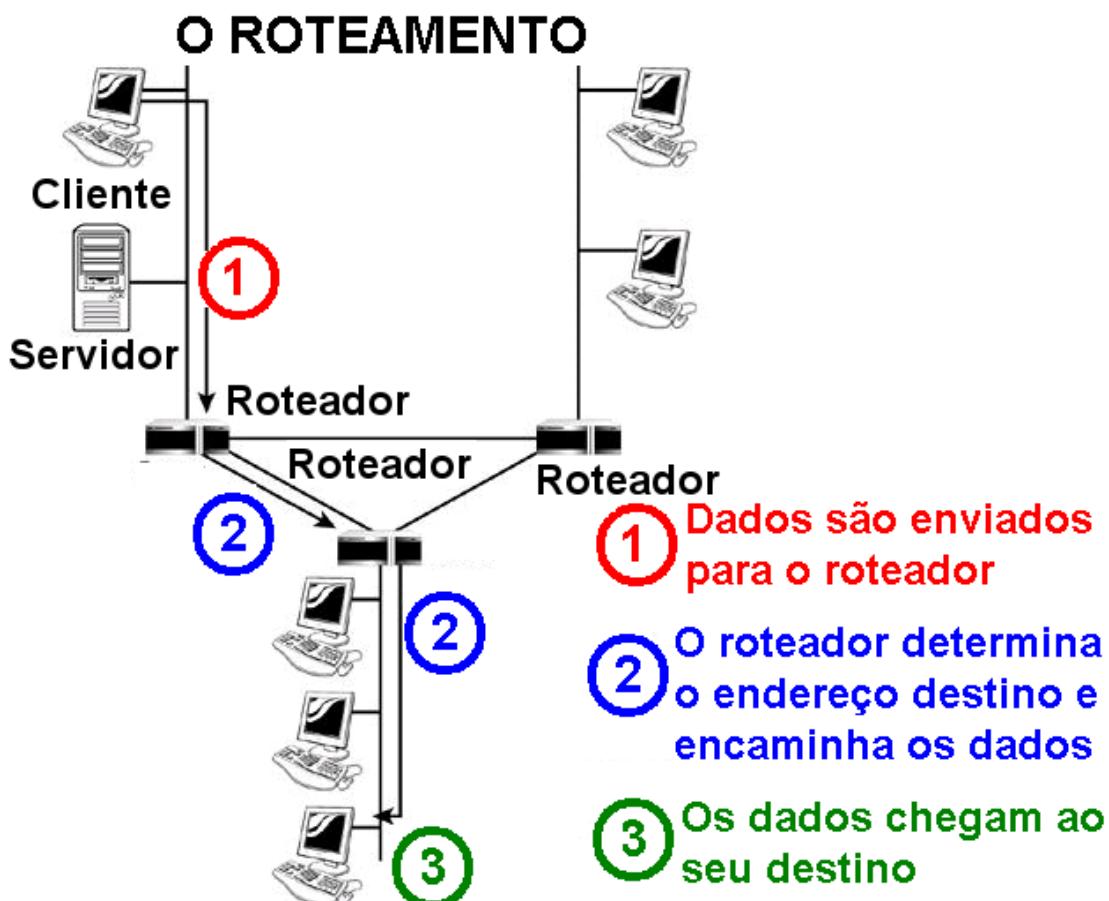
Roteadores interligam redes diferentes e selecionam as melhores rotas (caminho mais rápido e/ou menos congestionado) para as transmissões.



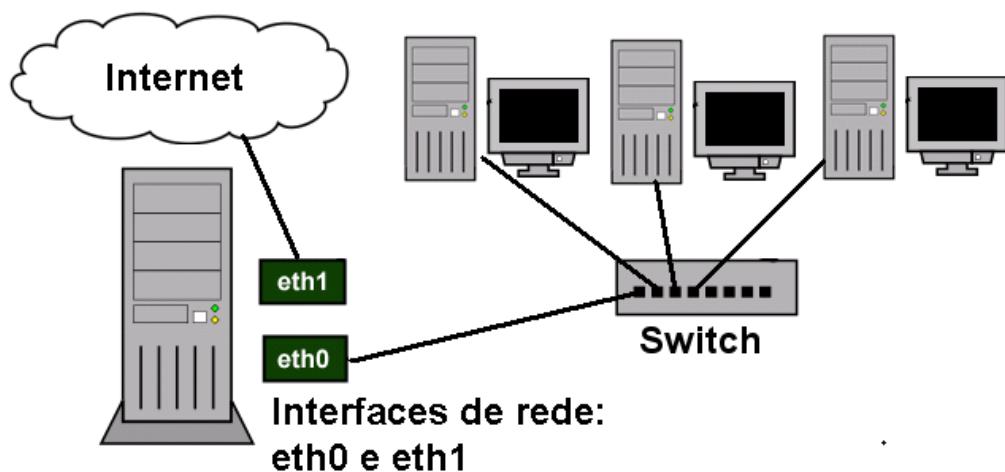
Eles trabalham na Camada de Rede do modelo OSI, assim lidam com o protocolo IP ao invés do MAC.

Os roteadores permitem a interligação de redes diferentes, mesmo em países ou continentes diferentes.

Vocês devem ter percebido que se não fossem os roteadores a Internet como conhecemos hoje, não seria possível.



Roteadores são dispositivos que variam desde PC's comuns que possuem duas ou mais placas de rede com um software que “transforma” esse simples PC num roteador, passando por modems para redes usuários domésticos, até dispositivos com uma supercapacidade de gerenciamento responsáveis por milhares de links com banda larga.



.1: O que Ethernet?

2: O que são componentes de rede ativos e passivos?

3: O que é o repetidor?

4: Em qual camada do modelo OSI o repetidor trabalha? Explique sua resposta.

5: Quando se utiliza repetidores wireless?

6: Defina o que são hubs?

7: Explique o funcionamento do hub.

8: Uma rede composta por vários computadores ligados a um hub possui uma topologia lógica em estrela ou barramento? Explique sua resposta.

9: Diferencie interligação de hubs por cascamenteamento de interligação de hubs por empilhamento.

10: O que é o endereço MAC?

11: O que são pontes? Explique em qual camada do modelo OSI as pontes atuam.

12: O que são switches? Em qual camada do modelo OSI os switches atuam?

13: Como o switch trabalha?

14: O que são roteadores?

6.0. A crimpagem de cabos

Para a montagem (ou crimpagem) de cabos par trançado deve-se ter: alicate de crimpagem, conectores RJ-45 e cabo UTP ou STP (tamanho variável de acordo com a necessidade). O alicate de crimpagem é usado para prender as pontas do cabo aos conectores RJ-45. Estes, por sua vez, são conectados à placa de rede do computador ou ao hub/switch.



6.0.1. Utilizar cabo crossover ou direto?

Quando o objetivo for interligar dois computadores, não existirá necessidade de utilizar dispositivos como hubs ou switches, já que se pode ligar uma máquina à outra diretamente. Neste caso, o cabo do tipo "crossover" (cruzado ou invertido) deve ser utilizado. Por outro lado, quando três ou mais computadores devem ser interligados, um switch deve ser utilizado.



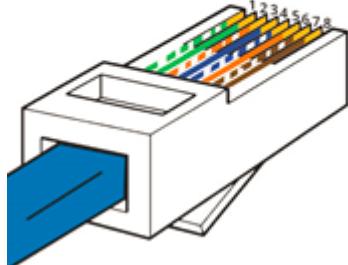
Deve-se criar um cabo para cada computador e conectá-los ao switch. No entanto, o cabo tipo crossover não serve para esse propósito, devendo ser utilizado o cabo do tipo "direto", também conhecido como "patch cable".

Em resumo, para ligar computador a computador, usa-se cabo crossover. Para ligar computador a hub, usa-se cabo direto. A diferença entre eles é que o cabo crossover tem a disposição de seus fios diferentes nas pontas, uma em relação à outra, enquanto que o cabo direto tem a disposição dos fios iguais em cada extremidade.

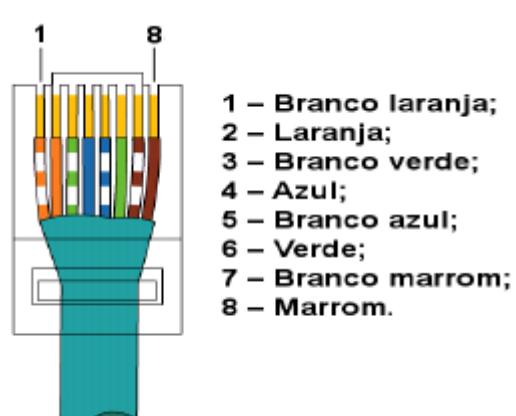
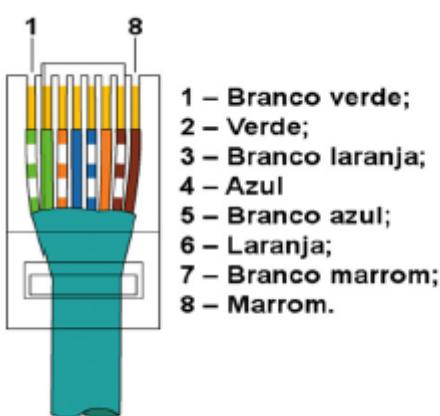
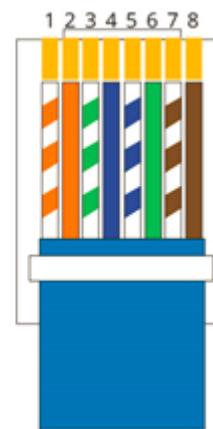
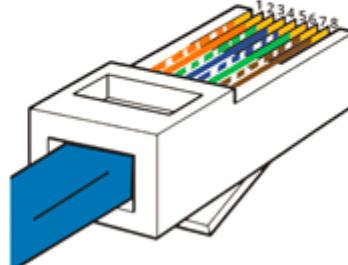
6.0.2. Padrões T568A e T568B

A norma EIA/TIA-568-B prevê duas montagens para os cabos, denominadas T568A e T568B. A montagem T568A usa a sequência branco e verde, verde, branco e laranja, azul, branco e azul, laranja, branco e castanho, castanho. Já a montagem T568B, usa a sequência branco e laranja, laranja, branco e verde, azul, branco e azul, verde, branco e castanho, castanho.

**RJ45 Pinout
T-568A**



**RJ45 Pinout
T-568B**



As duas montagens são totalmente equivalentes em termos de desempenho, cabendo ao montador escolher uma delas como padrão para sua instalação. É boa prática que todos os cabos dentro de uma instalação sigam o mesmo padrão de montagem.

Um cabo cujas duas pontas usam a mesma montagem é denominado Direto (cabo), já um cabo em

que cada ponta é usada uma das montagens é denominado Crossover.

Existem cabos com diferentes representações destes códigos de cores.

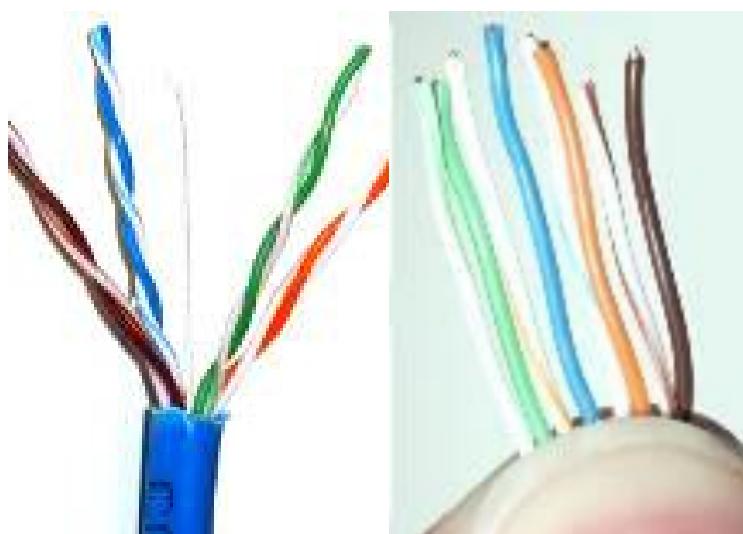
- O fio com a cor branca pode ser a cor mais clara (verde-claro, azul-claro, laranja-claro, castanho-claro);
- Fio branco com uma lista de cor;
- Fio completamente branco. Neste caso é necessário ter atenção aos cabos que estão entrelaçados;
- Fio dourado representando o fio "branco e castanho".

Passo-a-passo para a montagem do Cabo Par-Trançado CAT5e:

1. Corta-se o cabo de conexão horizontal (para ligar da tomada para o computador) no comprimento desejado (geralmente o cabo deve ter 1,5m).

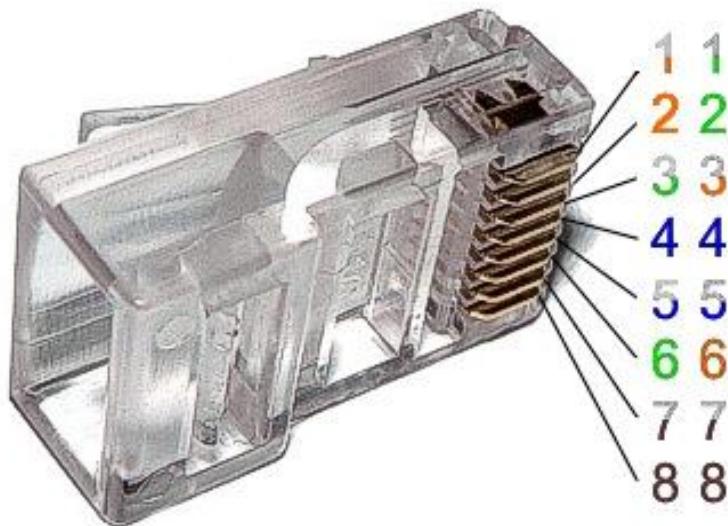


2. Em cada ponta, com a lâmina do alicate crimpador retira-se a capa de isolamento azul com um comprimento aproximado de 2 cm.



3. Prepare os oito pequenos fios para serem inseridos dentro do conector RJ45, obedecendo a sequência de cores desejada (T568A ou T568B).

4. Após ajustar os fios na posição, corta-se as pontas dos mesmos com um alicate ou com a lâmina do próprio crimpador para que todos fiquem no mesmo alinhamento e sem rebarbas, para que não ofereçam dificuldades na inserção no conector RJ45.



5. Segure firmemente as pontas dos fios e os insira cuidadosamente dentro do conector, observando que os fios fiquem bem posicionados.

6. Examine o cabo percebendo que as cabeças dos fios entraram totalmente no conector RJ45. Caso algum fio ainda não esteja alinhado refaça o item 4 para realinhar.

7. Insira o conector já com os fios colocados dentro do alicate crimpador e pressione até o final.
8. Após a crimpagem dos dois lados, use um testador de cabos para certificar se que os 8 fios estão funcionando bem.

6.1. Wireless

6.1.1. O que é uma rede wireless?

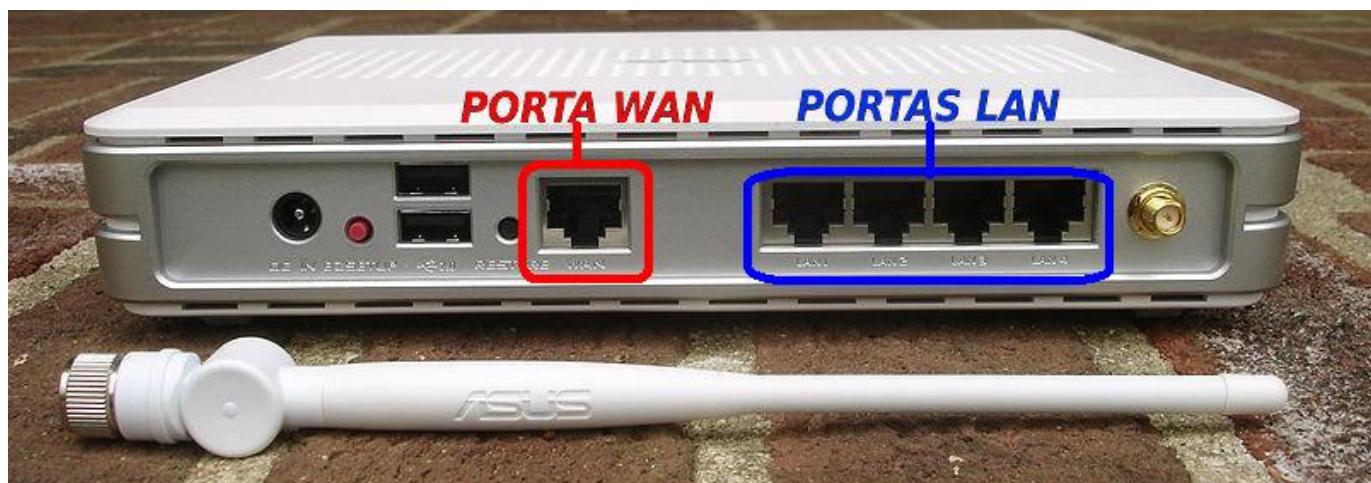
Uma rede sem fio se refere a uma rede de computadores sem a necessidade do uso de cabos – sejam eles telefônicos, coaxiais ou ópticos – por meio de equipamentos que usam radiofrequência (comunicação via ondas de rádio) ou comunicação via infravermelho, como em dispositivos compatíveis com IrDA.



O uso da tecnologia vai desde transceptores de rádio, como walkie-talkies até satélites artificiais no espaço. Seu uso mais comum é em redes de computadores, servindo como meio de acesso à Internet através de locais remotos como um escritório, um bar, um aeroporto, um parque, ou até mesmo em casa, etc.

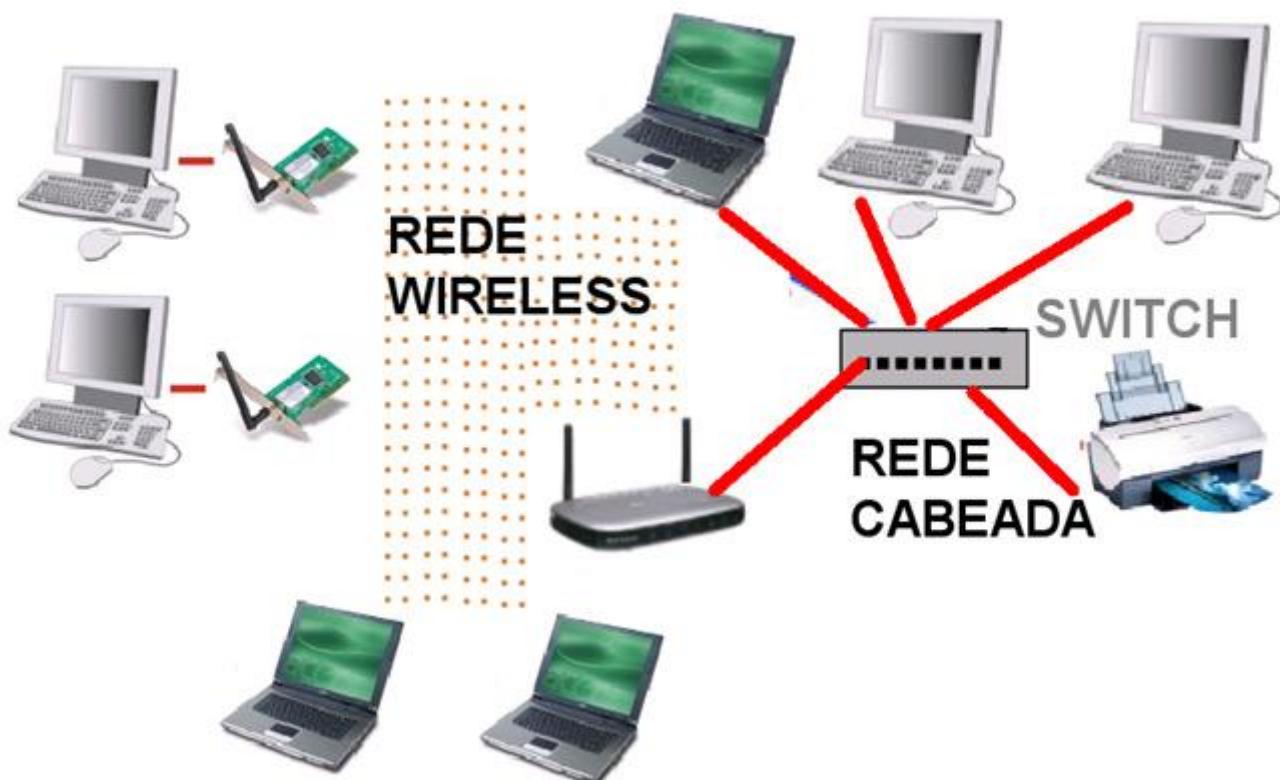
Numa rede wireless, o switch é substituído pelo ponto de acesso (access-point em inglês, comumente

abreviado como "AP" ou "WAP", de "wireless access point"), que tem a mesma função central que o switch desempenha nas redes com fios: retransmitir os pacotes de dados, de forma que todos os micros da rede os recebam.



A topologia é semelhante à das redes de par trançado, com o switch central substituído pelo ponto de acesso. A diferença é que são usados transmissores e antenas em vez de cabos.

Os pontos de acesso possuem uma saída para serem conectados em um switch tradicional, permitindo que você "junte" os micros da rede cabeada com os que estão acessando através da rede wireless, formando uma única rede, o que é justamente a configuração mais comum.



Pode-se configurar um switch para atender a rede cabeada, usando um cabo também para interligar o ponto de acesso à rede. O ponto de acesso serve apenas como a "última malha", levando o sinal da rede até os micros com placas wireless. Eles podem acessar os recursos da rede normalmente, acessar arquivos compartilhados, imprimir, acessar a Internet, etc.

Nesse caso, o ponto de acesso atua como um bridge, transformando os dois segmentos em uma única rede e permitindo que eles se comuniquem de forma transparente aos usuários.

6.1.2. Tipos de redes Wireless

Basicamente, existem dois tipos de redes móveis sem fio: as redes infra-estruturadas e as redes ad hoc.



Redes infra-estruturadas – São aquelas em que o Host Móvel (HM) está em contato direto com uma Estação de Suporte à Mobilidade (ESM), o nosso já conhecido Ponto de Acesso (AP), na rede fixa. A comunicação precisa passar pelo Access Point, mesmo que os equipamentos móveis estejam a uma distância em que poderiam, eventualmente, comunicar-se diretamente. Neste caso, os nós móveis, mesmo próximos uns dos outros, estão impossibilitados de realizar qualquer tipo de comunicação direta.



Redes Ad Hoc – Outro tipo importante de rede móvel é a rede ad hoc, onde os dispositivos são capazes de trocar informações diretamente entre si. Ao contrário do que ocorre em redes convencionais, não há pontos de acesso, ou seja, não existem estações de suporte à mobilidade (sem infra-estrutura de conexão) e os nós dependem uns dos outros para manter a rede conectada. Por esse motivo, redes ad hoc são indicadas principalmente em situações onde não se pode, ou não faz sentido, instalar uma rede fixa.

Lembrando que as estações de uma rede ad hoc podem se mover arbitrariamente. Deste modo, a topologia da rede muda frequentemente e de forma imprevisível. Assim, a conectividade entre os nós móveis muda constantemente, requerendo uma permanente adaptação e reconfiguração de rotas.

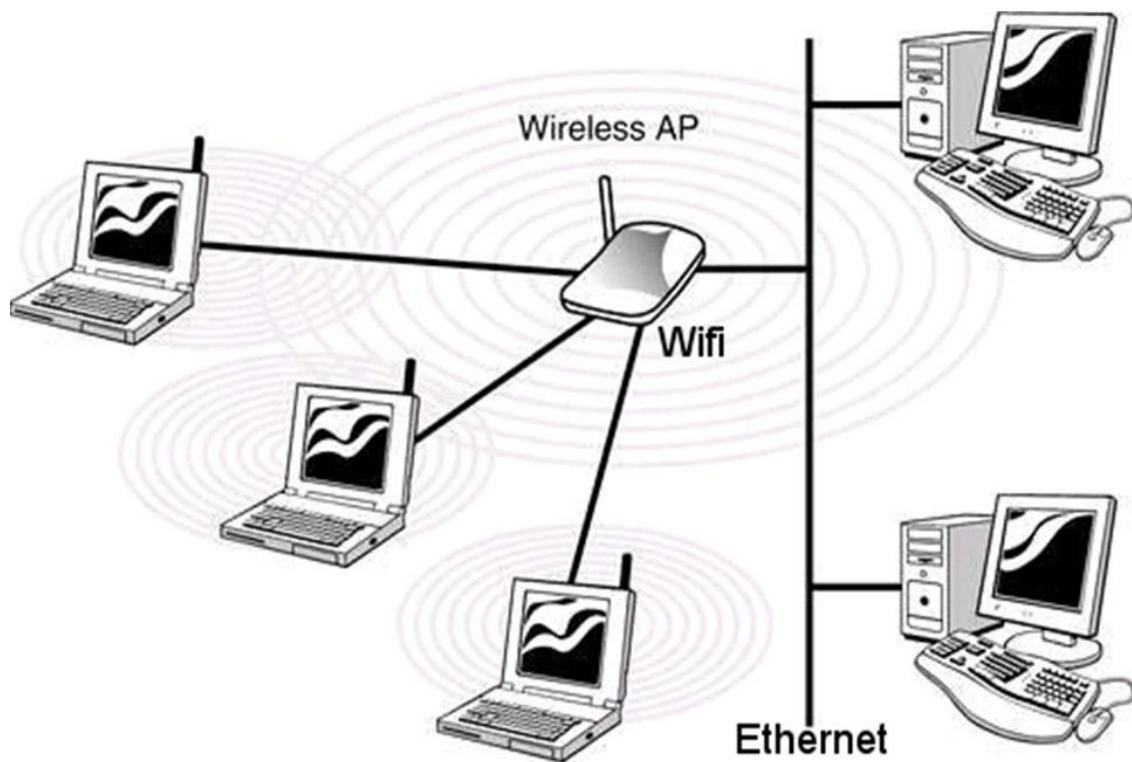
6.2 A Tecnologia Wi-Fi

A tecnologia Wi-Fi (ou simplesmente WiFi) permite a interconexão de computadores através de redes sem fio (wireless). A implementação desse tipo de rede está se tornando cada vez mais comum, não só nos ambientes domésticos e empresariais, mas também em locais públicos (bares, lanchonetes, shoppings, livrarias, aeroportos, etc) e em instituições acadêmicas.



Wi-Fi é um conjunto de especificações para redes locais sem fio - Wireless Local Area Network (WLAN), baseada no padrão IEEE 802.11.

O nome Wi-Fi é tido como uma abreviatura do termo inglês "Wireless Fidelity", embora a Wi-Fi Alliance, entidade responsável principalmente pelo licenciamento de produtos baseados na tecnologia, nunca tenha afirmado tal conclusão. É comum encontrar o nome Wi-Fi escrito como WiFi, Wi-fi ou até mesmo wifi. Todas essas denominações se referem à mesma tecnologia.



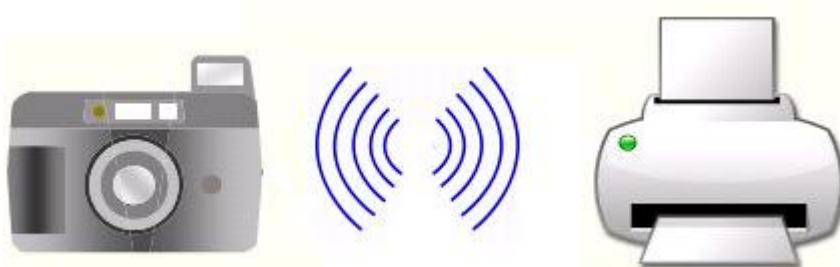
Com a tecnologia Wi-Fi, é possível implementar redes que conectam computadores e outros dispositivos compatíveis (telefones celulares, consoles de videogame, impressoras, etc) que estejam próximos geograficamente.

A flexibilidade do Wi-Fi é tão grande, que se tornou viável a implementação de redes que fazem uso dessa tecnologia nos mais variados lugares, principalmente pelo fato das vantagens citadas no parágrafo anterior resultarem em diminuição de custos.

Assim sendo, é comum encontrar redes Wi-Fi disponíveis em hotéis, aeroportos, rodoviárias, bares, restaurantes, shoppings, escolas, universidades, escritórios, hospitais, etc, que oferecem acesso à internet, muitas vezes de maneira gratuita. Para utilizar essas redes, basta ao usuário ter algum laptop, smartphone ou qualquer dispositivo compatível com Wi-Fi. Para obter uma padronização das tecnologias sem fio algumas empresas uniram-se para criar um grupo para lidar com essa questão e, assim, nasceu em 1999 a Wireless Ethernet Compatibility Alliance (WECA), que passou a se chamar Wi-Fi Alliance, em 2003. Assim como acontece com outros consórcios de padronização de tecnologias, o número de empresas que se associam à Wi-Fi Alliance aumenta constantemente.

A WICA passou a trabalhar com as especificações que são compatíveis com a tecnologia Ethernet. Assim, o que muda de um padrão para o outro são suas características de conexão: um tipo funciona com cabos, o outro, por radiofrequência. A vantagem disso é que não é necessária a criação de nenhum protocolo específico para a comunicação de redes sem fio baseada nessa tecnologia. Além disso, é possível ter redes que utilizam ambos os padrões. Adaptadores, Access Point e Roteadores Wi-Fi.

Para que um determinado produto receba um selo com essa marca, é necessário que ele seja avaliado e certificado pela Wi-Fi Alliance. Essa é uma forma de garantir ao usuário que todos os produtos com o selo Wi-Fi Certified seguem normas de funcionalidade que garantem a interoperabilidade entre si.



Todavia, isso não significa que dispositivos que não ostentam o selo não funcionam com dispositivos que o tenham (mas, é preferível optar por produtos certificados para diminuir o risco de problemas) considerando que toda a base do Wi-Fi está no padrão 802.11.

Todavia, isso não significa que dispositivos que não ostentam o selo não funcionam com dispositivos que o tenham (mas, é preferível optar por produtos certificados para diminuir o risco de problemas) considerando que toda a base do Wi-Fi está no padrão 802.11.

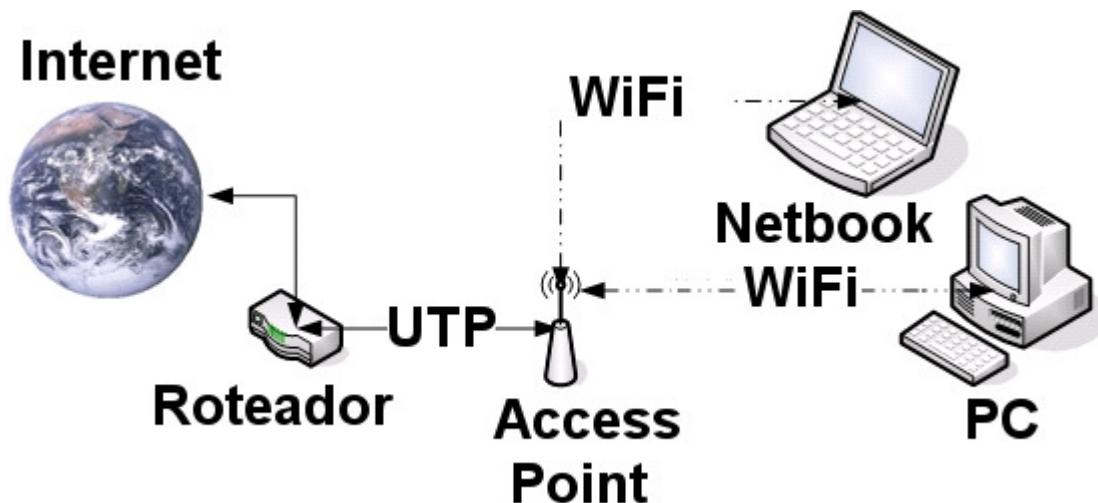


O padrão 802.11 estabelece normas para a criação e para o uso de redes sem fio. A transmissão dessa rede é feita por sinais de radiofrequência, que se propagam pelo ar e podem cobrir áreas na casa em centenas de metros.

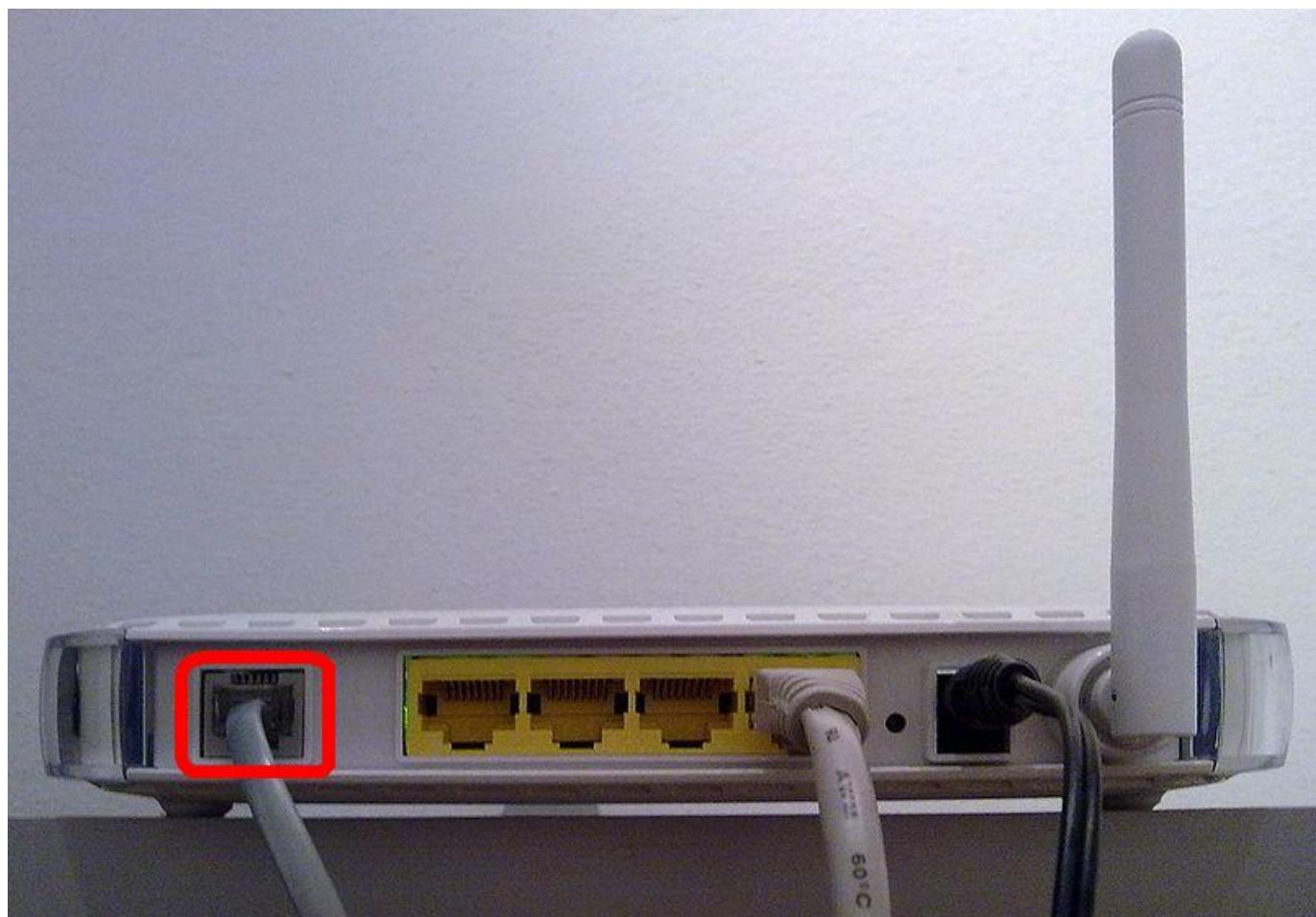
Como existem inúmeros serviços que podem utilizar sinais de rádio, é necessário que cada um opere de acordo com as exigências estabelecidas pelo governo de cada país. Essa é uma maneira de evitar problemas, especialmente interferências.



As redes Wi-Fi são tão práticas que o seu uso não precisa ser feito apenas por PCs. Há até smartphones e consoles de videogames capazes de acessar tais redes. Se você comprar um notebook atual, certamente ele virá com um módulo Wi-Fi.



Assim, você poderá acessar as redes sem fio da sua empresa, da sua escola, de sua casa ou de qualquer outro lugar de acesso público. Mas, e se você precisar que um computador desktop sem dispositivo Wi-Fi acesse uma determinada rede wireless? Para isso, basta instalar nele uma placa Wi-Fi ou um adaptador USB Wi-Fi.



Por sua vez, os adaptadores USB Wi-Fi utilizam, como o próprio nome indica, qualquer porta USB presente no computador. A vantagem desse tipo de dispositivo está no fato de não ser necessário abrir o

computador para instalá-lo e de poder removê-lo facilmente de uma máquina para acoplá-lo em outra. No entanto, como adaptadores USB geralmente são pequenos, sua antena é de tamanho reduzido, o que pode fazer com que o alcance seja menor que o de uma placa Wi-Fi PCI ou PCI Express. Mas, isso não é regra, e tal condição pode depender do fabricante e do modelo do dispositivo.

Nos ambientes domésticos e nos escritórios de porte pequeno, por exemplo, é comum encontrar dois tipos de aparelhos: os que são chamados simplesmente de access point e os roteadores wireless. Ambos são dispositivos parecidos, mas o access point apenas propaga dados de uma rede wireless, sendo muitas vezes usado como uma extensão de uma rede baseada em fios.

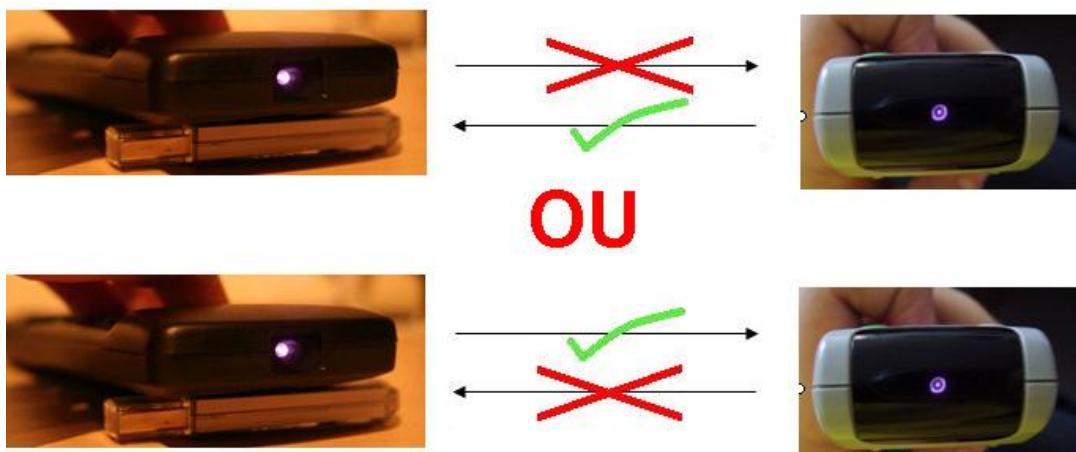
O roteador wireless, por sua vez, é capaz de direcionar o tráfego da internet, isto é, de distribuir os dados da rede mundial de computadores entre todas as estações. Para que isso seja feito, geralmente liga-se o dispositivo de recepção da internet (por exemplo, um modem ADSL) no roteador, e este faz a função de distribuir o acesso às estações. Se, no entanto, o usuário possui um modem que também faz roteamento, precisa apenas de um access point, pois o próprio modem se encarregará do compartilhamento do acesso à internet.

Antes de comprar o seu equipamento wireless, seja para montar uma rede, seja para fazer com que um dispositivo acesse uma, é importante conhecer as características de cada aparelho para fazer a aquisição certa. Via de regra, deve-se optar pelos equipamentos que possuem tecnologias mais recentes, mas também deve-se considerar a relação custo-benefício e os recursos oferecidos por cada dispositivo.

6.3. O infravermelho

Na década de 90, Hewlett Packard e outras empresas formaram o Infrared Data Association (IrDA) com o intuito de criar um padrão para transmissão sem fio, utilizando o espectro de infravermelho.

Atualmente, graças aos esforços, este grupo cresceu e conta com vários membros no mundo inteiro.



Para transmitir informações, os sistemas de comunicação em infravermelho utilizam frequências muito altas, localizadas um pouco abaixo do espectro de luz visível.

Comunicam-se utilizando Light Emitting Diode (LED's) – Diodo Emissor de Luz e suas transmissões podem ser full-duplex (enviar e receber dados ao mesmo tempo) ou half-duplex (enviar e receber dados, porém um por vez).



Os dispositivos que utilizam o IrDA podem ter um transmissor e um receptor separadamente ou um transceptor (combinação de transmissor e receptor em um único dispositivo). O padrão IrDA é dividido em dois tipos: IrDA Data e o IrDA Control.

- IrDA Data: utilizados em dispositivos que interagem para a troca de dados. A taxa de transferência varia conforme uma classificação: Serial Infrared (SIR) com 115,2 kbps, MIR (Medium Infrared) com 1,152 Mbps, Fast Infrared (FIR) com 4 Mbps, Very Fast Infrared (VFIR) com 16 Mbps e o Ultra Fast Infrared (UFIR) com 100 Mbps.
- IrDA Control: seu propósito é transmitir pequenos pacotes de controle entre dispositivos. Lidam, principalmente, com periféricos de interface com o usuário: teclados, mouses, joysticks, microfones e etc. Sua taxa de transmissão é de até 75 kbps.

A transmissão em infravermelho não interfere em sistemas que trabalham com espelhamento de espectro, possibilitando o uso das duas em conjunto. E para usar esta tecnologia não é necessária autorização do governo.

Por atingir alguns poucos metros e não penetrar em objetos opacos (atravessar uma parede, por exemplo), geralmente, aplica-se esta tecnologia em Redes Pessoais (PAN's). Também, torna-se oportuno comentar que... a tecnologia em questão sofre muita interferência da luz solar, pois uma considerável parcela

da luz do sol está no intervalo infravermelho.

6.4 Tecnologia Bluetooth

O Bluetooth é uma tecnologia que permite uma comunicação simples, rápida, segura e barata entre computadores, smartphones, telefones celulares, mouses, teclados, fones de ouvido, impressoras e outros dispositivos, utilizando ondas de rádio no lugar de cabos. Assim, é possível fazer com que dois ou mais dispositivos comecem a trocar informações com uma simples aproximação entre eles.



Bluetooth é um padrão global de comunicação sem fio e de baixo consumo de energia que permite a transmissão de dados entre dispositivos compatíveis com a tecnologia. Para isso, uma combinação de hardware e software é utilizada para permitir que essa comunicação ocorra entre os mais diferentes tipos de aparelhos. A transmissão de dados é feita através de radiofrequência, permitindo que um dispositivo detecte o outro independente de suas posições, desde que estejam dentro do limite de proximidade.

Para que seja possível atender aos mais variados tipos de dispositivos, o alcance máximo do Bluetooth foi dividido em três classes:

- Classe 1: potência máxima de 100 mW, alcance de até 100 metros;

- Classe 2: potência máxima de 2,5 mW, alcance de até 10 metros;
- Classe 3: potência máxima de 1 mW, alcance de até 1 metro.

Isso significa que um aparelho com Bluetooth classe 3 só conseguirá se comunicar com outro se a distância entre ambos for inferior a 1 metro, por exemplo. Neste caso, a distância pode parecer inutilizável, mas é suficiente para conectar um fone de ouvido a um telefone celular pendurado na cintura de uma pessoa.

É importante frisar, no entanto, que dispositivos de classes diferentes podem se comunicar sem qualquer problema, bastando respeitar o limite daquele que possui um alcance menor.

O Bluetooth é uma tecnologia criada para funcionar no mundo todo, razão pela qual se fez necessária a adoção de uma frequência de rádio aberta, que seja padrão em qualquer lugar do planeta.

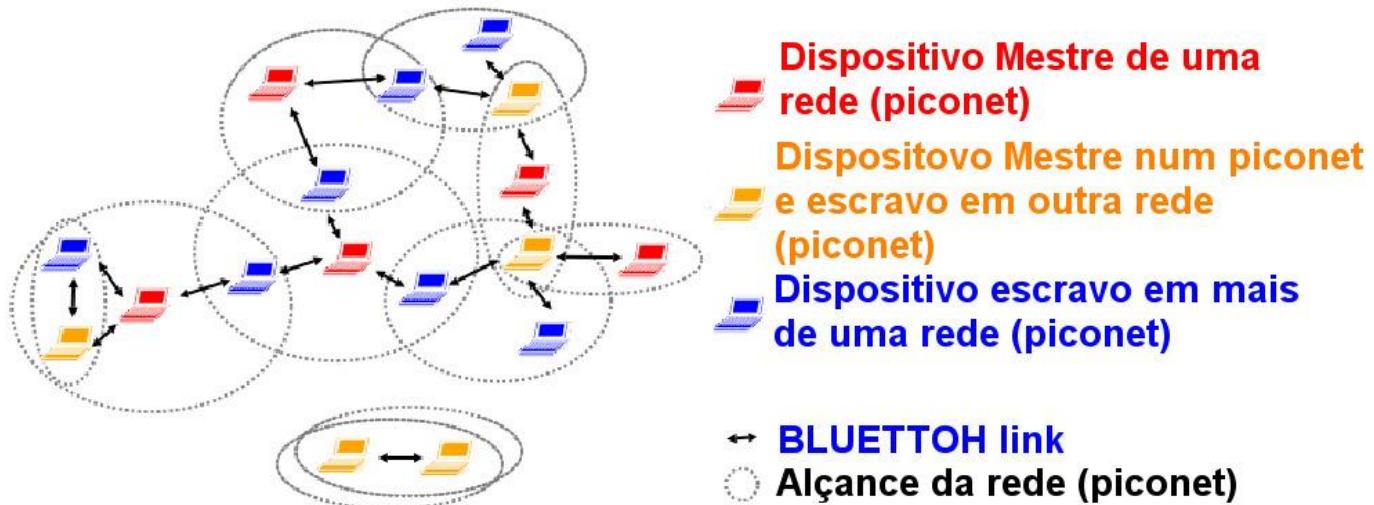


Um dispositivo comunicando-se por Bluetooth pode tanto receber quanto transmitir dados (modo full-duplex), a transmissão é alternada entre slots para transmitir e slots para receber, um esquema denominado FH/TDD (Frequency Hopping/Time-Division Duplex).

6.4.1. Redes Bluetooth

Quando dois ou mais dispositivos se comunicam através de uma conexão Bluetooth, eles formam uma rede denominada piconet. Nessa comunicação, o dispositivo que iniciou a conexão assume o papel de master (mestre), enquanto que os demais dispositivos se tornam slave (escravos). Cabe ao master a tarefa de regular a transmissão de dados entre a rede e o sincronismo entre os dispositivos.

Cada piconet pode suportar até 8 dispositivos (um master e 7 slaves), no entanto, é possível fazer com que esse número seja maior através da sobreposição de piconets.



Em poucas palavras, isso significa fazer com que uma piconet se comunique com outra dentro de um limite de alcance, esquema esse denominado scatternet. Note que um dispositivo slave pode fazer parte de mais de uma piconet ao mesmo tempo, no entanto, um master só pode ocupar essa posição em uma única piconet. Para que cada dispositivo saiba quais outros fazem parte de sua piconet, é necessário fazer uso de um esquema de identificação. Assim, ocorre a troca de sinais entre os dispositivos que estabelecem a conexão e demais informações de sincronismo.

Como o Bluetooth é uma tecnologia que também oferece como vantagem economia de energia, um terceiro sinal denominado Scan é utilizado para fazer com que os dispositivos que estiverem ociosos entrem em stand-by, isto é, operem em um modo de descanso, poupando eletricidade. Todavia, dispositivos neste estado são obrigados a "acordar" periodicamente para checar se há outros aparelhos tentando estabelecer conexão.

Com a popularização das redes Wi-Fi, o mercado ficou com dúvidas em relação ao futuro do Bluetooth, mas o aumento expressivo de aparelhos compatíveis com a tecnologia fez com que todos os temores se dissolvessem. E faz sentido: o objetivo do Bluetooth é permitir a intercomunicação de dispositivos próximos utilizando o menor consumo de energia possível (mesmo porque muitos desses dispositivos são alimentados por baterias) e um custo de implementação baixo. O Wi-Fi, por sua vez, mostra-se mais como um concorrente das tradicionais redes de computadores com fio (padrão Ethernet, em sua maioria).



1: Por que foram criadas especificações para o cabeamento de redes de computadores? E por que é

importante compreender essas especificações?

2: O que é o cabo coaxial?

3: Quais as vantagens em utilizar o cabo par trançado ao invés do cabo coaxial?

4: Explique o que diferencia o cabo par trançado UTP do STP.

5: O que se utiliza para montar cabos de rede?

6: O que diferencia um cabo crossover de um cabo direto?

7: Por que a etapa mais complicada ao instalar cabos de rede é a passagem dos cabos? E qual o outro problema de uma rede cabeada ao se utilizar notebooks, PDA's e laptops?

8: O que é uma rede wireless?

9: Qual a função do Access Point numa rede sem fio?

10: O AP é uma ponte? Por quê?

11: Quais os dois tipos de redes sem fio? Diferencie uma da outra.

12: O que é o Wi-Fi?

13: O que é o IrDA?

14: Diferencie transmissões full-duplex de half-duplex

15: Diferencie o AP de um roteador Wi-Fi.

16: O que é o Bluetooth?

17: Quais as três classes do Bluetooth?

18: O que é o piconet e como ele está relacionado com o funcionamento do Bluetooth?

PRATICANDO!!!

1: Dimensione uma rede Wireless composta por laptops que estão se conectando a um Access Point.

2: Implemente a atividade um com a criação de uma rede composta por PC's e cabeada, interligue a rede cabeada com a rede sem fio da atividade 1.

3: Crie uma pequena rede com dispositivos Wi-Fi, com ou sem Access Point.

7.0 Projeto de Redes de Computadores

As redes de computadores atuais caracterizam-se tanto pela especificidade e variedade das alternativas tecnológicas disponíveis quanto pelos sistemas de comunicação e requisitos necessários em termos de confiabilidade e capacidade dos meios de transmissão.

A implantação de um tipo particular de topologia de rede para dar suporte a um dado conjunto de aplicações não é uma tarefa tão simples. Cada arquitetura possui características que afetam sua adequação à uma aplicação em particular.

Independente do tamanho e do grau de complexidade, o objetivo básico de uma rede de computadores é garantir que todos os recursos de informações sejam compartilhados rapidamente, com segurança e de forma confiável. Para tanto, a rede deve possuir meios de transmissão eficientes, regras básicas (protocolos) e mecanismos capazes de garantir o transporte das informações entre os seus elementos constituintes.

Ainda é comum a prática de se improvisar sistemas de cabeamento para a interligação dessas redes, sem existir um planejamento e estudos prévios.

O cabeamento é normalmente instalado ao acaso, sem a observação de técnicas específicas. Nesses casos, um novo ponto de rede deve ser instalado cada vez que se deseja utilizar uma nova aplicação ou quando ocorrem mudanças de layout dentro da edificação.

Uma rede estruturada elimina a dispersão dos cabos destinados ao transporte dos sinais de dados na área de instalação, não permitindo a mistura com os demais cabos de eletricidade e controle, por exemplo, identificando os cabos e facilitando a manutenção. Dessa forma, garante a flexibilidade e facilidade de manutenção. Com esta solução, é possível eliminar os cabos desnecessários, já que é feito um remanejamento na estrutura da rede.

Para facilitar a sua implementação, o projeto de uma rede de computadores pode ser dividido basicamente em duas etapas: o projeto físico e o projeto lógico. O projeto físico refere-se à topologia física da rede propriamente dita, composta pelos meios de

comunicação (que podem ser pares metálicos, fibras ópticas, rádio enlaces, etc), pelos dispositivos de rede (placas de rede, switches, hubs, roteadores, etc), pelos próprios computadores e demais elementos constituintes do hardware.

Já o projeto lógico, diz respeito à topologia lógica das partes físicas, ou seja, o conjunto de regras

que permitem o funcionamento de todo o conjunto do hardware de rede. Assim, o projeto lógico trata do conjunto dos recursos que os usuários veem quando estão utilizando a rede, tais como espaço em disco rígido, impressoras e aplicativos, aos quais um computador tem acesso quando está conectado na rede.

7.1. O projeto lógico

7.1.1. Compreendendo os endereços IP

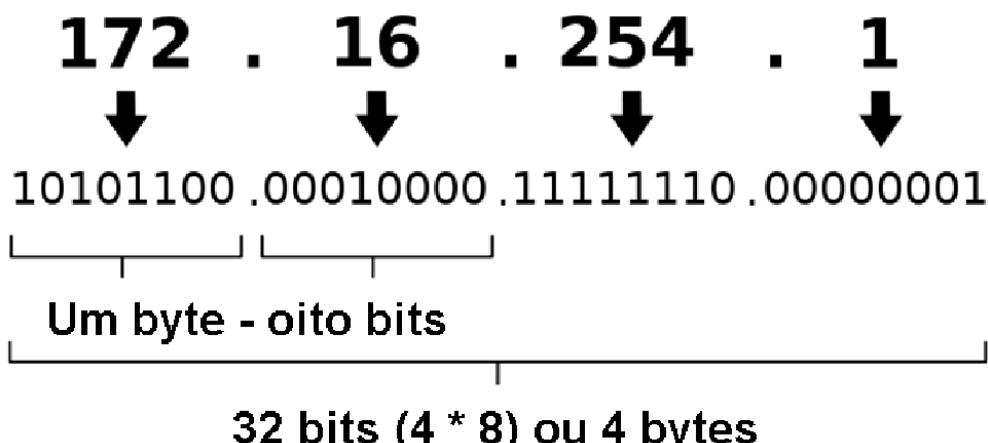
Como comunicar e/ou localizar uma máquina na Internet? Todo hospedeiro tem um endereço exclusivo. O endereço IP na versão 4 (ipv4), que é atualmente o mais utilizado, é um número de 32 bits. Você está acostumado a ver endereços de Internet, como: www.e-jovem-ce.com.br/ e www.linux.org; porém, na verdade, este nome está referenciado a um endereço IP que permite acesso a determinada máquina, sem a necessidade de decorar números.

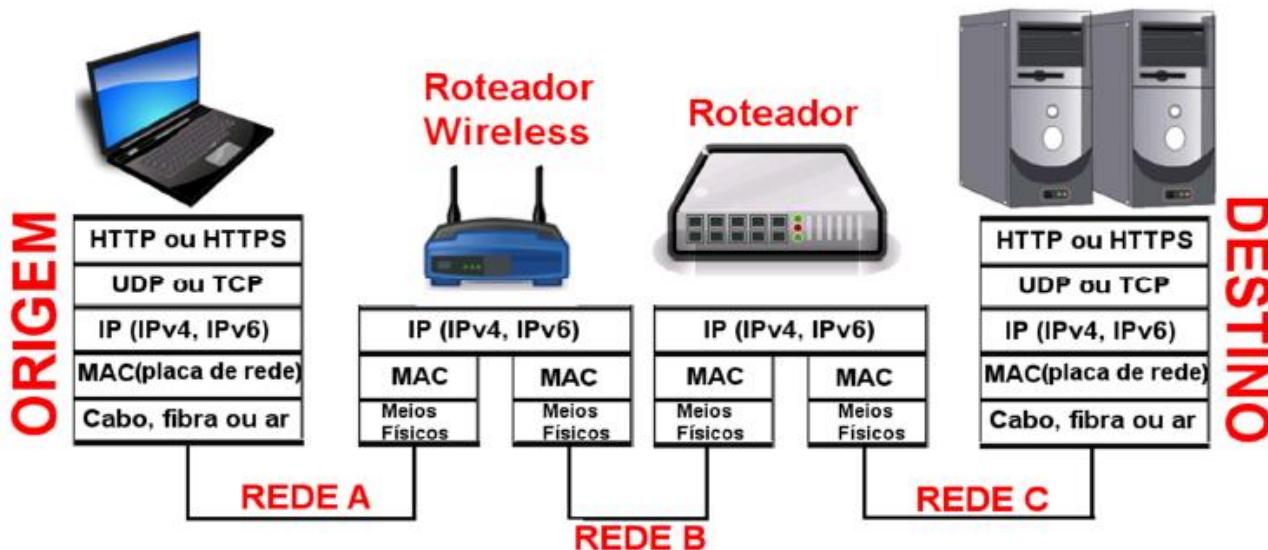
Um endereço IP é normalmente representado por quatro números decimais, um para cada porção de 8 bits, separados por pontos. Logo, o endereço IP é um número formado por 4 octetos, cada octeto com 8 bits.

Por exemplo, uma única máquina pode ter um endereço de IP geralmente expresso de 3 formas:

1. 149.76.12.4 = notação decimal de quatro partes, é a mais utilizada e mais legível;
2. 0x954C0C04 = notação hexadecimal;
3. 10010101.01001100.00001100.00000100 = notação binária. Note a quantidade de 32 bits, divididos em 4 octetos (conjuntos de 8 bits) e a correspondência entre cada octeto com o valor decimal equivalente.

Endereço IP (versão 4) em notações decimal e binária

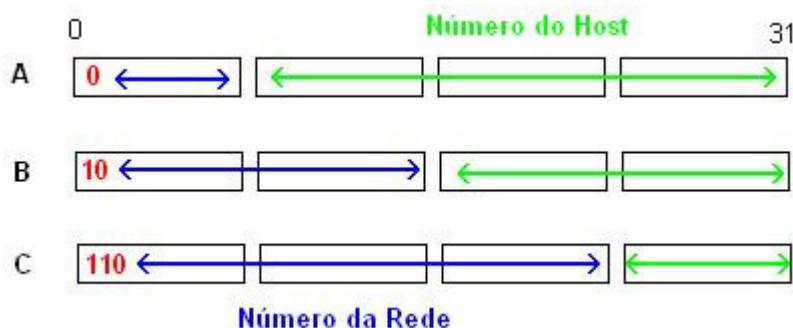




7.1.2. Número IP: identificando rede e máquina.

Simplesmente por razões de tornar o controle da atribuição de números IP mais organizada, os criadores do TCP/IP resolveram dividir o número IP em duas partes:

1. Número de rede: está contido em um ou mais octetos do número IP. Esse número indica em que rede o hospedeiro está conectado. Cada rede deve ter endereço único.

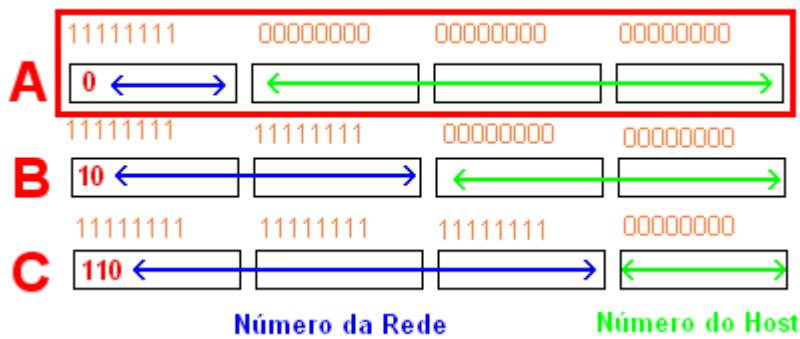


2. Número de máquina: é o número de identificação da máquina na rede. É através dele que localizamos um determinado host na rede, esse número também deve ser único na rede. Por exemplo, poderíamos ter um número IP com 13.121.111.1, onde 13 é o número que identifica a rede e 121.111.1 identifica um host desta rede.

7.1.3. Classes de endereços IPv4

Ao iniciar a distribuição dos números IP para empresas, os criadores do TCP/IP perceberam que era vantajoso definir blocos de endereços contíguos, no sentido de facilitar a administração. Verificaram também que as empresas tinham portes diferentes, e com isto surgiram as classes, que definem tipos de

redes de tamanhos diferentes.



Quando alguma empresa necessitava de números IP, era fornecido um bloco contíguo de endereços IP de uma classe adequada a sua necessidade, baseada na quantidade de hosts a serem identificados com números IP.

Foram definidos 5 tipos de classes: A, B, C, D e E. Para se identificar uma classe, procurou-se definir algo que seria melhor implementado em nível de hardware. Por isto, cada classe foi definida baseando-se no primeiro dos quatro bytes do número IP.

Assim, para identificar se um número IP pertence à classe A basta saber o valor do bit do primeiro byte. Caso seja 0, pode-se concluir imediatamente que se refere à classe A, caso contrário deve-se testar o segundo bit. Se o segundo bit for 0 pode-se concluir imediatamente que se refere à classe B, caso contrário deve-se verificar o terceiro bit, e assim por diante. Note então que para se identificar uma classe, basta saber qual a posição do bit 0 no primeiro byte.

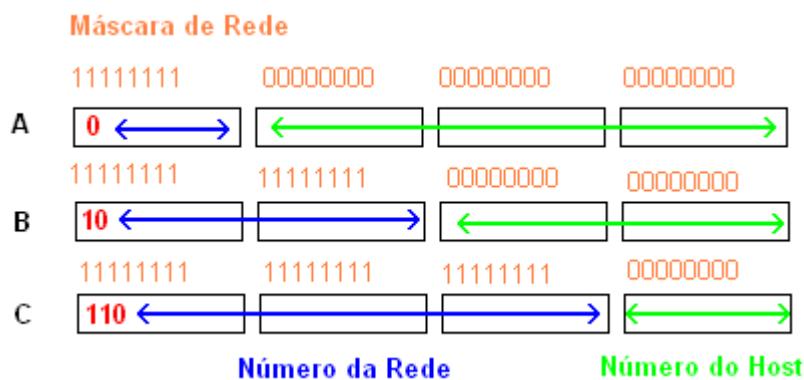
Classe	Bits iniciais	Início	Fim	Máscara de Subrede padrão	Notação CIDR
A	0	1.0.0.1	126.255.255.254	255.0.0.0	/8
B	10	128.0.0.1	191.255.255.254	255.255.0.0	/16
C	110	192.0.0.1	223.255.255.254	255.255.255.0	/24

7.1.4. Máscara de rede

Os 32 bits das Máscaras de Sub-rede são divididos em duas partes: um primeiro bloco de 1s, seguido por um bloco de 0s. Os 1s indicam a parte do endereço IP que pertence à rede e os 0s indicam a parte que pertence ao host.

Normalmente, as máscaras de sub-rede são representadas com quatro números de 0 a 255 separados por três pontos. A máscara 255.255.255.0 (ou 11111111.11111111.11111111.00000000), por exemplo, em

uma rede da classe C, indica que o terceiro byte do endereço IP é o número de sub-rede e o quarto é o número do host.



Normalmente, as máscaras de sub-rede são representadas com quatro números de 0 a 255 separados por três pontos. A máscara 255.255.255.0 (ou 11111111.11111111.11111111.00000000), por exemplo, em uma rede da classe C, indica que o terceiro byte do endereço IP é o número de sub-rede e o quarto é o número do host.

Classe	Bits iniciais	Início	Fim	Máscara de Subrede padrão	Notação CIDR
A	0	1.0.0.1	126.255.255.254	255.0.0.0	/8
B	10	128.0.0.1	191.255.255.254	255.255.0.0	/16
C	110	192.0.0.1	223.255.255.254	255.255.255.0	/24

7.1.5. Endereços IP para redes privadas

Todo computador da Internet recebe um endereço IP único. Caso você queira ter uma rede local própria, precisará de alguns endereços únicos. Neste caso você não precisa usar os números válidos na Internet, porque há um bloco de endereços que foi reservado apenas para as redes privadas. Os endereços de rede apresentados abaixo podem ser utilizados em sua rede local. Vejamos:

1. 10.0.0.0 a 10.255.255.255 - permite endereçar uma rede classe A;
2. 172.16.0.0 - 172.31.255.255 - permite endereçar 16 redes classe B;
3. 192.168.0.0 - 192.168.255.255 - permite endereçar 256 redes classe C.

7.2. Serviços utilizáveis na rede

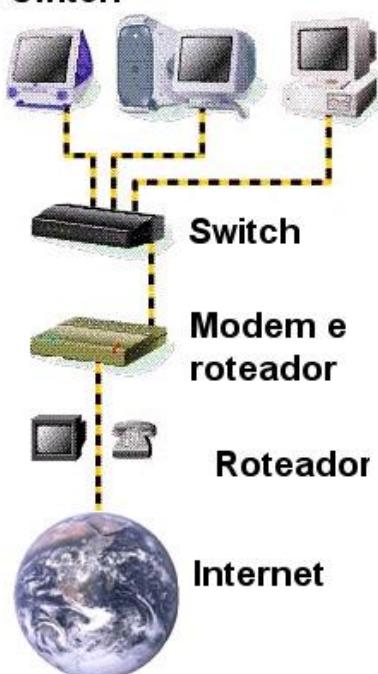
7.2.1. Compartilhamento de internet (modems + roteadores sem fio)

Cada vez mais, a Internet via banda larga está disponível a um número maior de pessoas, assim está se Informática – Redes de Computadores

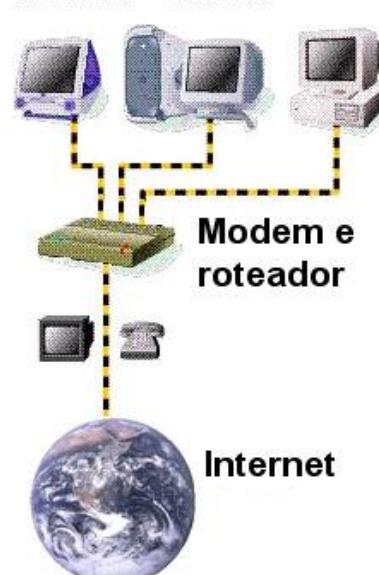
tornando cada vez mais comum a existência de redes de pequeno porte nas casas e escritórios. Estas duas realidades somadas levam à necessidade de compartilhar a conexão à Internet entre os diversos computadores da maneira mais barata e eficaz possível.

Ao planejar a sua rede local de modo a escapar de todas as complicações, deve-se encontrar os equipamentos e um provedor que suporte uma das configurações a seguir:

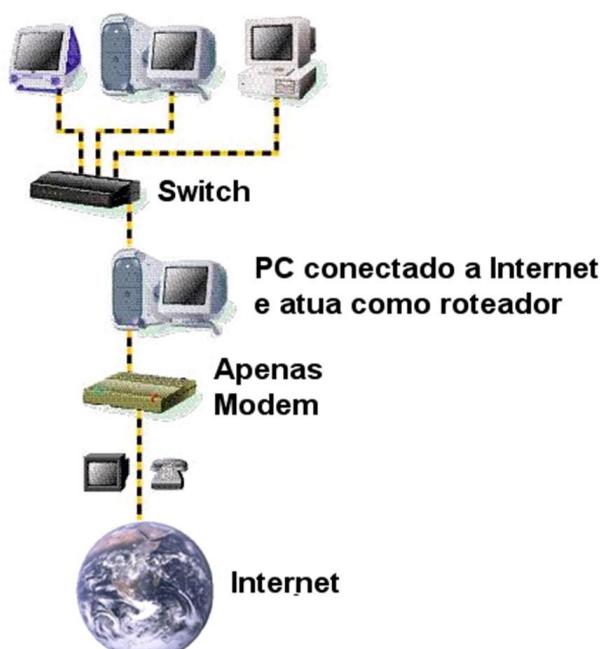
Caso 1 - Modem conectado ao switch



Caso 2 - Uso de um Modem- Switch



Caso 3 - PC conectado e atuando como roteador



No caso 1, o modem (que é um roteador, também, compartilha o acesso à internet com vários computadores) está conectado a um switch, onde estão conectados também os demais PC's da LAN.

Configurar os computadores neste tipo de configuração é trivial, mas nem sempre se pode recorrer a este método: alguns modems podem ter perda de performance se conectados diretamente a um hub, outros exigem a conexão direta a um computador por razões diversas.

Infelizmente alguns provedores bloqueiam este tipo de compartilhamento mesmo quando o modem o suporta, pois assim a pessoa paga apenas uma conexão à Internet que é acessada por vários clientes.



No caso 2, o modem também é um switch, assim este possui entradas para conexões simultâneas dos cabos de rede de diversos micros. Neste caso, conectar toda a sua rede local à Internet passa a ser uma tarefa extremamente simples.

Essas são as configurações recomendáveis, mas se o seu projeto não possui os equipamentos que permitem compartilhar sua conexão simplesmente conectando cabos de rede extras, resta o recurso de habilitar este recurso no micro que possui a conexão.

No caso 3 temos a instalação de uma segunda placa de rede no computador com acesso à Internet, seguida da configuração deste computador como roteador, assim este passar a rotear as comunicações entre a rede local e a Internet.

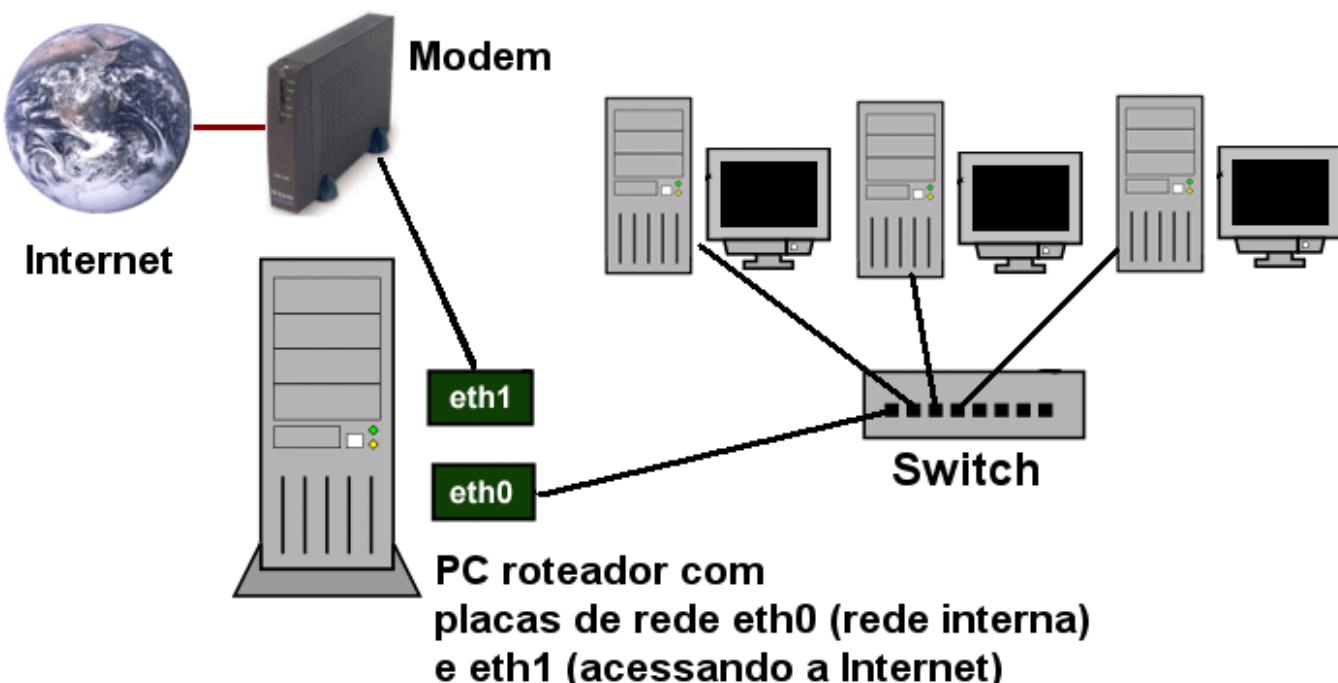
Não importa qual o método que você escolha para seu projeto. Será necessário configurar sua rede local normalmente. A seguir, algumas dicas de configuração para a rede local:

- Use endereços IP estáticos, na faixa 192.168.1.X, onde X é um número entre 1 e 254, para todos os micros. O micro que tem a conexão à Internet também vai receber um endereço desta faixa na sua segunda placa de rede (a eth1).
- Use a máscara de rede 255.255.255.0.
- Configure o endereço dos servidores DNS do seu provedor em todos os micros da rede.
- Informe a todos os micros da rede local que o seu gateway padrão ou sua rota default é o endereço IP da placa eth1 do micro que tem a conexão.

Siga os passos acima usando as ferramentas providas pelo seu sistema operacional, seguindo as instruções providas na documentação do mesmo. De modo geral, esta operação é trivial e pode ser feita facilmente.

7.2.1.1. Configurando o micro com acesso à Internet

Este é o ponto crucial de sua conexão. O micro com duas placas de rede é que faz o encaminhamento do tráfego entre a sua rede local e a Internet, realizando uma operação de troca de endereçamento que pode se chamar NAT ou Masquerading, dependendo do contexto.



A forma de configurar esta operação varia de acordo com a distribuição de Linux adotada, mas o prérequisito é que as duas placas de rede já estejam adequadamente configuradas e em operação. Assim, antes de prosseguir configure o micro de tal forma que você consiga acessar normalmente a Internet nele (seguindo sempre as instruções do seu provedor), e que você possa também acessar (ou no mínimo obter retorno através do comando ping) os micros da rede local. Naturalmente o acesso à Internet ocorrerá através da primeira placa de rede (chamada de eth0), enquanto o acesso à rede local ocorrerá através da segunda placa (a eth1).

7.2.2. Configuração de compartilhamento de internet por dispositivos diferentes.

O compartilhamento de internet consiste no recebimento de link de conexão com a internet e repasse das propriedades deste para a rede interna. O mesmo pode ser feito por intermédio de um computador, como servidor de internet(gateway para a internet), ou através de modens e roteadores em conjunto ou integrados.

A arquitetura mínima para acesso à internet exige a utilização de um modem que trabalha como agente mediador da conexão entre o provedor de acesso à internet e, minimamente, um computador.

Nesta estrutura o modem pode trabalhar em modo bridge e em modo router de acordo com o método de autenticação realizado no processo de conexão, como é explicado à seguir:

MODO BRIDGE

Neste modo o roteador serve como ponte de conexão com o servidor de acesso do provedor de internet, de forma que há necessidade de uso de um discador para que a autenticação de usuário e senha seja realizada na máquina em que se deseja realizar conexão. Este modo passa as configurações de acesso direto para máquina sendo criada uma conexão ponto a ponto entre servidor de internet (OI, GVT, Telefônica, ...) e o computador do cliente através do modem que passa a existir nas configurações do computador como uma interface de rede virtual.

Nos modens adsl normalmente este tipo de configuração é a padrão o que denota o uso de discadores da OI, Telefônica, entre outras.

MODO ROUTER

No modo router o roteador recebe as informações de autenticação, como usuário e senha, no momento de sua configuração, pois este processo passa a ser realizado diretamente pelo modem, que repassa a conexão de internet através de um servidor de DHCP interno que deve ser habilitado e configurado junto as

configurações de acesso a internet.

Observe que neste tipo de conexão o modem faz interface com a internet, porém ele tem acesso direto ao servidor do provedor, enquanto que o computador da rede interna se conecta a ele para que possa acessar os dados dos sites da internet e navegar tranquilamente, lembrando que neste caso a configuração de rede é automática.

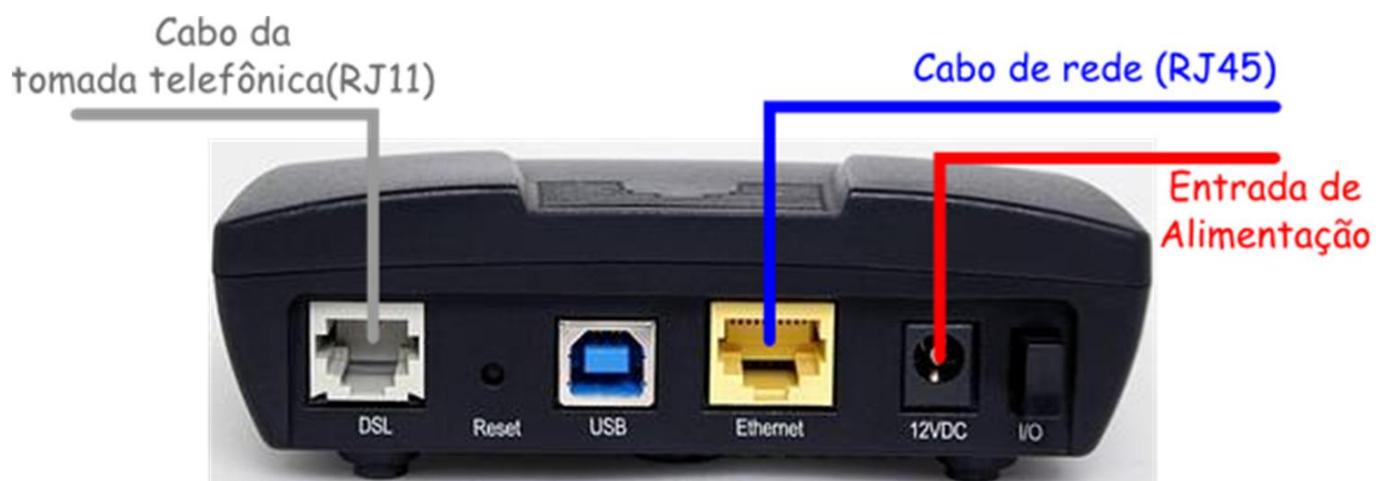
Entre estes dois métodos existem discussões sobre vantagens e desvantagens que são principalmente expostas pela seguinte questão, as portas de acesso às aplicações são configuradas junto ao modem quando o mesmo está em modo router, ou seja, a segurança de rede fica a cargo de quem o configura, melhor opção quando se necessita de segurança para a rede interna.

Quando as redes têm acesso externo realizado direto pelo modo bridge o sistema operacional é responsável pela segurança dele através de utilização de firewall, porém em alguns casos por padrão o sistema vem com várias portas abertas, o que o torna mais vulnerável, porém para alguns usuários a abertura destas portas diretamente com o servidor melhora na performance de downloads e acessos.

Logo deve-se pesar as demandas para decidir que tipo de configuração atenderá melhor as suas demandas.

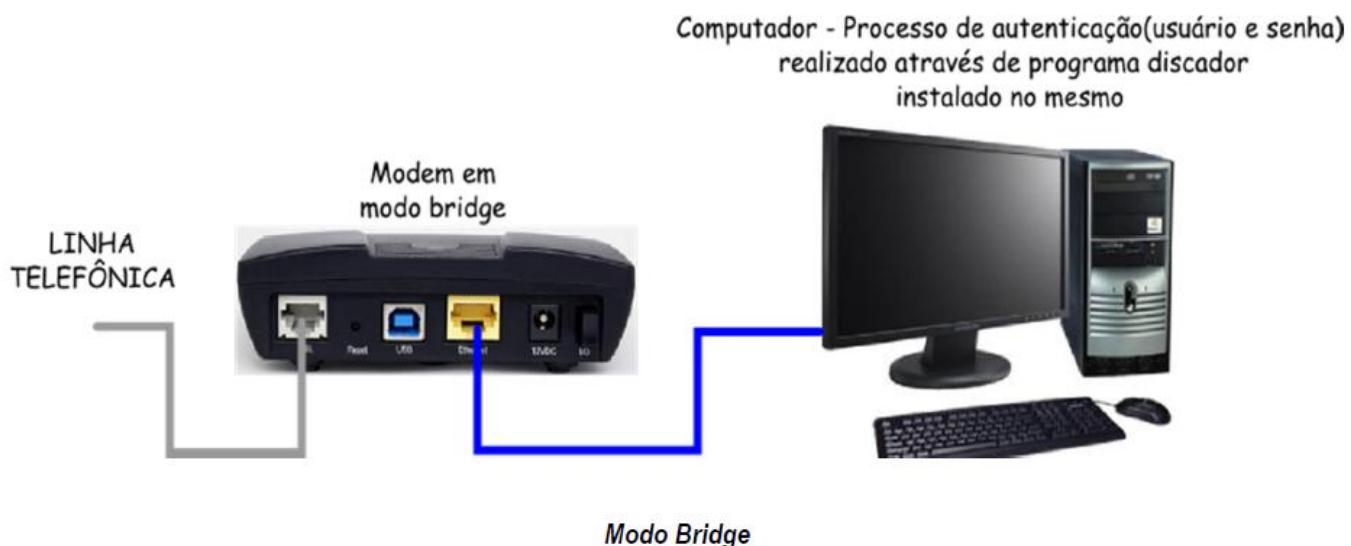
REDE MODEM/ROUTER

Como citado anteriormente, o Modem é o equipamento que faz a interface entre a rede de internet e o seu computador ou rede de interna de computadores. A seguir na imagem identificamos os conectores deste tipo de aparelho.



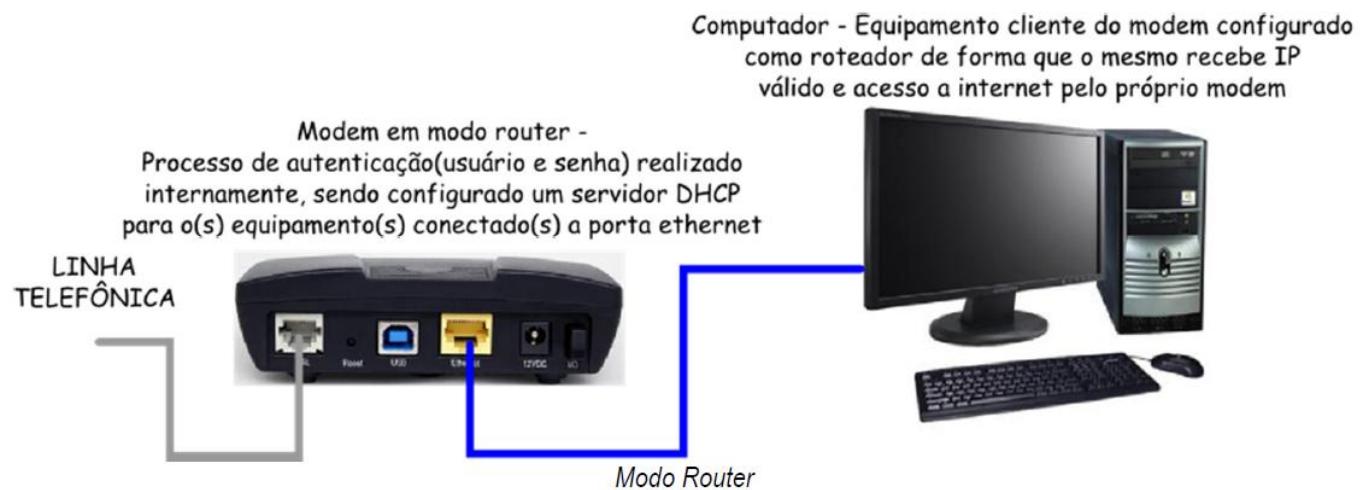
Neste tipo de modem, recebemos o sinal ADSL da rede telefônica e o transmitimos através da rede lógica (saída ethernet), que pode ser ligada diretamente a um computador ou a um switch/roteador, dependendo da configuração do modem.

Dentre as configurações router e bridge podemos demonstrar através de imagens as ligações do sistema de acordo com as necessidades de uso. Observe a seguir a topologia dos tipos de configurações e suas descrições.



Observe que no modo bridge o sistema operacional recebe as configurações de acesso a rede através de um software discador responsável pela autenticação do equipamento junto ao provedor de acesso a internet, passando o modem a ser visto com uma interface de rede para conexão ponto a ponto. Logo as configurações como ip, gateway e DNS são fornecidas ao sistema junto as configurações do discador. Em alguns casos o sistema discador é disponibilizado pelas operadoras e contém as configurações necessárias para o funcionamento correto da conexão, em outros casos há necessidade de pesquisar os dados para tal configuração, este ocorre quando se utiliza um software de terceiro ou nativo do sistema operacional para realizar a autenticação e conexão.

No modo router o modem passa a ser configurado para utilização de um discador interno, ou seja, o sistema operacional, não é mais encarregado desta função, logo o modem passará a gerenciar a conexão com o servidor do provedor de internet sempre que for ligado. Ainda no modem deve-se configurar uma ferramenta de compartilhamento da conexão que o mesmo estabelece com a internet, esta ferramenta é um servidor de DHCP que provê as configurações de IP, máscara de rede, gateway e DNS a ser utilizado durante uma conexão para acesso a rede e a internet.



Este processo é chamada de roteamento de modem e comumente é utilizada a nomenclatura de modem roteado para o modem que contém as configurações deste modo.

Observe que apesar do exemplo mostrar apenas um computador ligado ao modem roteado, pela configuração utilizada pode-se ligar mais de um computador simultaneamente a rede criada pelo modem roteado através de um equipamento de rede que permita a conexão entre mais de um aparelho, a exemplo de um switch, haja vista que o modem roteado disponibiliza as configurações de rede para um número de computadores limitado total de ip's que este pode disponibilizar, este total é configurado junto o servidor de DHCP do mesmo.

No fim deste tutorial existem uma lista de links com dicas de como configurar os mais variados tipos de modems utilizados pelas operadoras e disponíveis no mercado.

REDE MODEM + ROTEADOR

Neste tipo de rede o elemento adicionado ao modem é o roteador que trabalha em conjunto com modem no gerenciamento da rede interna. A seguir falamos mais das funcionalidades do roteador.

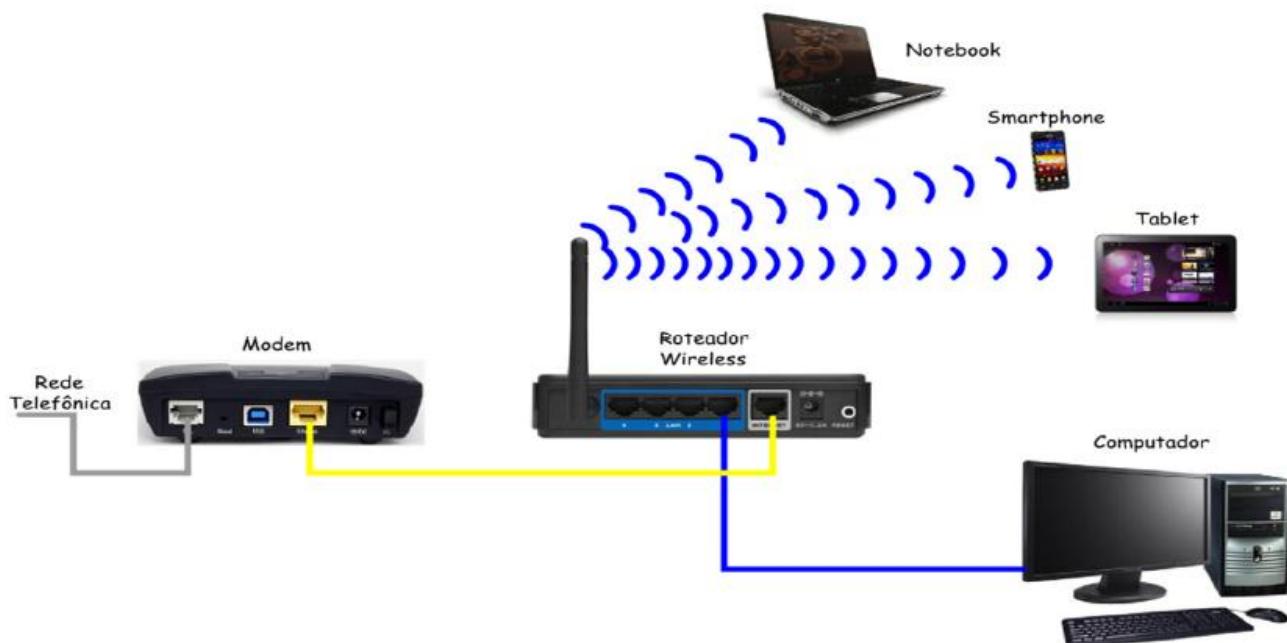
Aparelho utilizado para roteamento de pacotes entre redes disponibilizando acesso entre equipamentos da rede interna e/ou rede externa. Na imagem abaixo podemos identificar os conectores de um roteador.



Dentre os tipos de conexão identificados na imagem acima temos a antena de rede wireless, que não é um item padrão dos roteadores, haja vista que o modelo apresentado se trata de um roteador wireless, ou seja, que provê conexão a rede interna e ou externa através de rede sem fio.

Este equipamento pode ser encontrado sem antena para rede sem fio, trabalhando apenas como reteador de pacotes entre redes cabeadas.

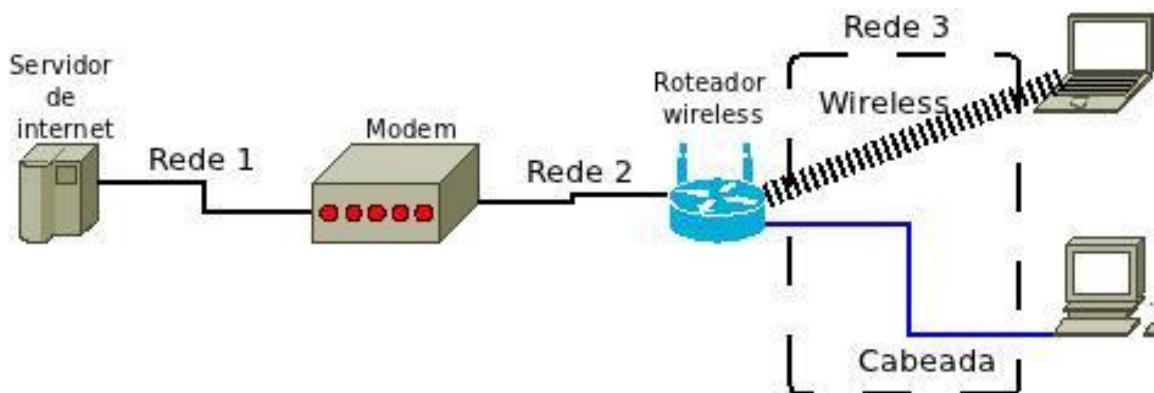
Dentre suas funcionalidades básicas temos a configuração de servidor de DHCP, discagem PPPoE em modens, reaplicadores de rede, firewall, QoS, entre outras. A seguir serão demonstradas algumas das arquiteturas utilizadas de acordo com os processos de configuração destes equipamentos junto aos modens e computadores.



Na estrutura mostrada acima podemos ter dois tipos de configuração:

a) Processo de autenticação no modem (modem roteado)

Neste tipo de configuração o modem fica roteado como descrito na sessão anterior, o que vai fazer com que existam três redes como o descrito a baixo.



Observe que a rede 1 é estabelecida entre o servidor do provedor de internet e o modem que fica na residência ou estabelecimento do cliente. Esta rede é rede ponto a ponto que necessita de autenticação realizada pelo discador configurado no modem.

A rede 2 é estabelecida entre o modem e o roteador wireless, haja vista que com a configuração do modem ativa o mesmo passa a distribuir ips válidos pelo servidor de DHCP, logo o roteador passa a receber configurações deste.

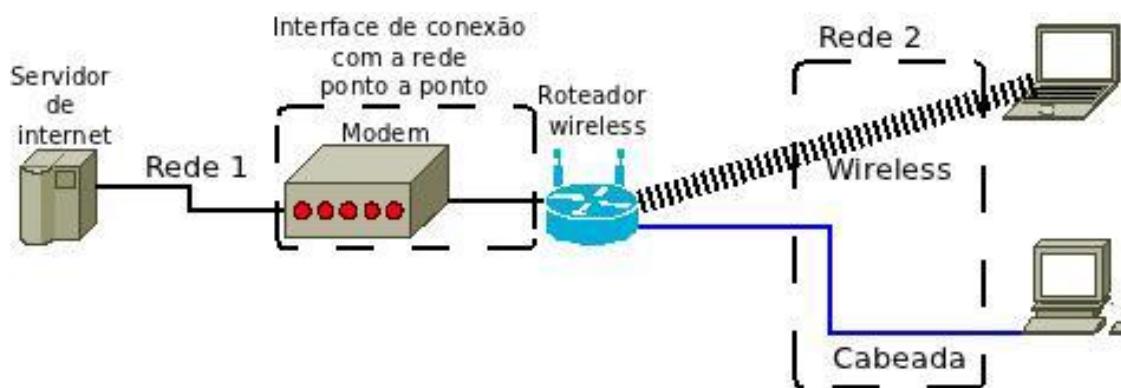
Por fim a rede 3 fica depois do roteador, podendo receber dois tipos de configuração. A primeira trata da utilização dos dados do modem diretamente, ou seja, o roteador se comporta como um switch, apenas distribuindo acesso ao modem, que por sua vez faz a distribuição das configurações válidas.

A segunda forma se refere ao uso do roteador como cliente da rede 2, ou seja, o mesmo recebe configurações diretamente do modem para que possa se conectar ao mesmo e em seguida é utilizado como provedor de configurações básicas para a rede 3 através de um servidor de DHCP interno a este.

Observe que em todos os casos a topologia utilizada é a mesma, sendo diferenciada apenas pela configuração dos equipamentos. Outro ponto a ser observado é que independente da configuração os equipamentos depois do roteador wireless recebem acesso a internet, sendo transparente para eles a diferença entre as configurações aqui citadas.

b) Processo de autenticação no roteador

Ainda utilizando a mesma estrutura do modelo anterior podemos configurar o roteador para realizar a discagem do modem e utilizá-lo como periférico de conexão para rede ponto a ponto entre o servidor de internet e o roteador utilizado na rede interna como mostra a figura a seguir.



Observe que nesta nova estrutura existem apenas duas redes, uma entre servidor e roteador, pois o modem serve como interface de conexão para o roteador, e outra entre o roteador e os computadores da rede interna.

Neste caso o roteador recebe configurações de rede para discagem PPPoE de maneira que o modem funcione como interface entre a internet e o roteador. Neste tipo de configuração o roteador tem as funcionalidades de gerenciamento de rede responsáveis por questões que vão desde o acesso através da distribuição de configurações via DHCP a segurança da rede instalada e configurada através de regras de roteamento e firewall.

REDE MODEM + SERVIDOR

Uma outra forma de configurar o compartilhamento de internet é utilizando um computador como servidor intermediário de internet em conjunto com o modem, a estrutura do mesmo é exposta na imagem seguir.

Observe que nesta imagem temos como agente intermediário um servidor que tem conexão direta com o modem e com a rede interna através de duas interfaces de rede denominadas como eth0, para a conexão com o modem e eth1, para conexão com a rede interna.



Nesta estrutura podemos ter o modem configurado como router e como bridge ficando a cargo do servidor trabalhar as demais funcionalidades de roteamento entre as redes conectadas as interfaces eth0 e eth1. A seguir serão descritos os procedimentos de configuração de um servidor linux para compartilhamento de redes tanto com modem em modo bridge como em modo router.

7.3 O projeto físico

Projetar uma rede de computadores obedece a algumas premissas básicas, seja esta rede uma pequena LAN ou uma MAN, estas são aplicadas tanto em redes cabeada, como wireless, de modo que para ter uma rede confiável e que atenda as necessidades de seus usuários torna-se importante fazer um bom projeto da rede.

Deve-se realizar um levantamento da infra-estrutura necessária (dispositivos de conectividade, cabos, acessórios e outros) para uma nova rede, ou mesmo, analisar os requisitos para a implantação de uma nova rede estruturada, instalação de equipamentos de rádio frequência, redes wireless, etc, de forma a maximizar sua cobertura e eficiência, bem como reduzir os custos de investimento.

É recomendado analisar as condições técnicas do local da instalação, que inclui verificar a existência ou não de obstáculos que possam dificultar o lançamento do cabeamento ou o posicionamento de antenas, facilidades de pontos de energia, aterramento, ventilação, segurança, etc.

7.3.1 Montagem da infra-estrutura física

A seguir, temos os materiais necessários para a montagem do cabeamento da rede.



1. Alicate de crimpagem - esta é a ferramenta mais importante no processo, pois ele crimpa os contatos do conector, fazendo com que eles entrem em contato com os fios do cabo de rede. Se seu alicate não for bom, as conexões serão ruins.



2. Testador (opcional) - Apesar de não ser necessário, ter um bom testador de cabos pode evitar e resolver os problemas de configuração e instalação. A maioria dos testadores tem duas caixas que passam sinais uma para a outra, acendendo LEDs do outro lado. Eles também podem mostrar o resultado do teste. Por que testar os cabos? Cabos ligeiramente danificados podem causar intermitência do sinal, perda de pacotes e corrupção de dados.



4. Cabo de rede - ele pode ser encontrado em lojas de computadores, material elétrico e home centers. Você pode conseguir um cabo categoria 5, 5e ou 6, dependendo do que precisa. Para comprimentos menores que 15m use um cabo trançado, para mais de 15m use um cabo sólido.



5. Descapadores de cabos específicos para cabos de rede, um alicate de corte ou mesmo uma tesoura.

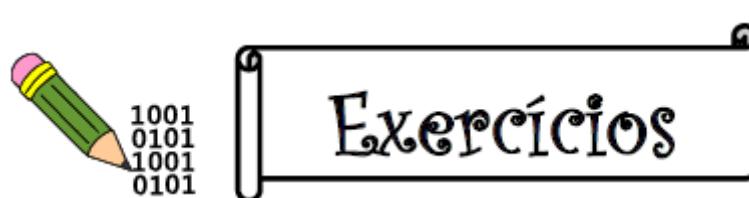
7.3.2 Tomadas na parede

Uma boa opção ao cabear é usar tomadas para cabos de rede, ao invés de simplesmente deixar os cabos soltos. Elas dão um acabamento mais profissional e tornam o cabeamento mais flexível, já que você pode ligar cabos de diferentes tamanhos às tomadas e substituí-los conforme necessário (ao mudar os micros de lugar, por exemplo). Existem vários tipos de tomadas de parede, tanto de instalação interna quanto externa.

O cabo de rede é instalado diretamente dentro da tomada. Em vez de ser crimpado, o cabo é instalado em um conector próprio (o tipo mais comum é o conector 110) que contém lâminas de contato. A instalação é feita usando uma chave especial, chamada em inglês de punch down tool.

A ferramenta pressiona o cabo contra as lâminas, de forma a criar o contato e ao mesmo tempo corta o excesso de cabo. Alguns conectores utilizam uma tampa que quando fechada empurra os cabos, tornando desnecessário o uso da ferramenta (sistema chamado de tool-less ou auto-crimp). Eles são raros, justamente por serem mais caros.

O próprio conector inclui o esquema de cores dos cabos, junto com um decalque ou etiqueta que indica se o padrão usado corresponde ao EIA 568A ou ao EIA 568B.



1: Diferencie projeto lógico de uma rede do projeto físico.

2: Por que é vantajoso projetar uma rede com cabeamento estruturado?

3: Por que se utiliza endereços IP em computadores em rede?

4: “O endereço IP é uma sequência de números composta de 32 bits”. Explique essa frase.

5: Quais as três formas utilizadas para expressar endereços IP?

6: O que são o número de rede e número de host num endereço IP?

7: Explique as classes de endereços IP?

8: Defina máscara de sub-rede.

9: Por que utilizar servidores DNS é tão importante? E como funciona o DNS?

10: O que são domínios?

11: Defina memória cache? E qual sua importância?

12: Explique qual a principal função de um servidor DHCP numa rede.

13: Em quais situações recomenda-se utilizar servidores DHCP?

14: O que é um modem-roteador?

15: Cite duas configurações possíveis que permitam compartilhar uma única conexão com a Internet com uma rede local.

16: Cite 3 comandos de redes Linux e explique cada um deles?

17: Qual a importância de se utilizar um testador de cabos no processo de crimpagem de cabos de rede?

18: Por que recomenda-se utilizar tomadas para os cabos de rede?

Referências

Apostila Projeto MEDIOTEC – SEDUC - Técnico em Informática _Modulo I _Parte2.pdf

Vasconcelos, L. (2009). Hardware na Prática - 3^a Edição. Rio de Janeiro: Laércio Vasconcelos Computação.

Morimoto, C. E. (2002). Manual de Hardware Completo 3^a Edição.

Martins, L. (2007). Curso Profissional de Hardware. São Paulo: Digerati Books.

Hino Nacional

Ouviram do Ipiranga as margens plácidas
De um povo heróico o brado retumbante,
E o sol da liberdade, em raios fúlgidos,
Brilhou no céu da pátria nesse instante.

Se o penhor dessa igualdade
Conseguimos conquistar com braço forte,
Em teu seio, ó liberdade,
Desafia o nosso peito a própria morte!

Ó Pátria amada,
Idolatrada,
Salve! Salve!

Brasil, um sonho intenso, um raio vívido
De amor e de esperança à terra desce,
Se em teu formoso céu, risonho e límpido,
A imagem do Cruzeiro resplandece.

Gigante pela própria natureza,
És belo, és forte, impávido colosso,
E o teu futuro espelha essa grandeza.

Terra adorada,
Entre outras mil,
És tu, Brasil,
Ó Pátria amada!
Dos filhos deste solo és mãe gentil,
Pátria amada, Brasil!

Deitado eternamente em berço esplêndido,
Ao som do mar e à luz do céu profundo,
Fulguras, ó Brasil, florão da América,
Iluminado ao sol do Novo Mundo!

Do que a terra, mais garrida,
Teus risonhos, lindos campos têm mais flores;
"Nossos bosques têm mais vida",
"Nossa vida" no teu seio "mais amores."

Ó Pátria amada,
Idolatrada,
Salve! Salve!

Brasil, de amor eterno seja símbolo
O lábaro que ostentas estrelado,
E diga o verde-louro dessa flâmula
- "Paz no futuro e glória no passado."

Mas, se ergues da justiça a clava forte,
Verás que um filho teu não foge à luta,
Nem teme, quem te adora, a própria morte.

Terra adorada,
Entre outras mil,
És tu, Brasil,
Ó Pátria amada!
Dos filhos deste solo és mãe gentil,
Pátria amada, Brasil!

Hino do Estado do Ceará

Poesia de Thomaz Lopes
Música de Alberto Nepomuceno
Terra do sol, do amor, terra da luz!
Soa o clarim que tua glória conta!
Terra, o teu nome a fama aos céus remonta
Em clarão que seduz!
Nome que brilha esplêndido luzeiro!
Nos fulvos braços de ouro do cruzeiro!

Mudem-se em flor as pedras dos caminhos!
Chuvas de prata rolem das estrelas...
E despertando, deslumbrada, ao vê-las
Ressoa a voz dos ninhos...
Há de florar nas rosas e nos cravos
Rubros o sangue ardente dos escravos.
Seja teu verbo a voz do coração,
Verbo de paz e amor do Sul ao Norte!
Ruja teu peito em luta contra a morte,
Acordando a amplidão.
Peito que deu alívio a quem sofria
E foi o sol iluminando o dia!

Tua jangada afoita enfune o pano!
Vento feliz conduza a vela ousada!
Que importa que no seu barco seja um nada
Na vastidão do oceano,
Se à proa vão heróis e marinheiros
E vão no peito corações guerreiros?

Se, nós te amamos, em aventuras e mágoas!
Porque esse chão que embebe a água dos rios
Há de florar em meses, nos estios
E bosques, pelas águas!
Selvas e rios, serras e florestas
Brotam no solo em rumorosas festas!
Abra-se ao vento o teu pendão natal
Sobre as revoltas águas dos teus mares!
E desfraldado diga aos céus e aos mares
A vitória imortal!
Que foi de sangue, em guerras leais e francas,
E foi na paz da cor das hóstias brancas!



GOVERNO DO ESTADO DO CEARÁ

Secretaria da Educação