ESCOLA
Alcides Maya

Introdução Redes

Sumário

Introdução Redes

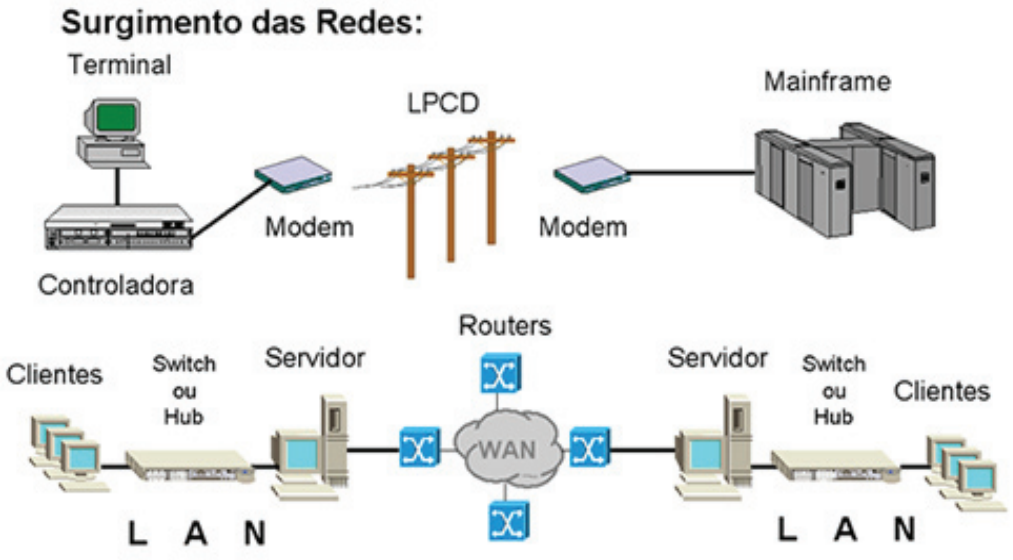
1 INTRODUÇÃO

Comunicação uma das maiores necessidades da sociedade humana. Desenvolvida desde os ancestrais (fumaça, etc.) Telégrafo (1838 por Samuel Morse) inaugura a era da comunicação por sinais elétricos (telefone, rádio, tv).

Outras áreas tiveram grande evolução, por exemplo processamento e armazenamento de informações. Computadores foram, provavelmente, o maior avanço do século.

A Conjunções destas tecnologias (comunicação e processamento de informações), revolucionou o mundo moderno.

2 Definições Básicas sobre Redes



Uma rede pode ser caracterizada por seu:

- Tipo

- Topologia

2.1 Tipos de Redes

LAN (Local Area Network = Rede de Área Local)
MAN (Metropolitan Area Network = Rede de Área Metropolitana)
WAN (Wide Area Network = Rede de Área Distante)

2.1.1 LAN (Local Area Netwok):

- altas taxas de transmissão (até 1Gbps, indo para 10Gbps);

- baixas taxas de erros (1 erro em 10^8 ou 10^{11} bits transmitidos);
- propriedade privada;
- geograficamente limitadas;
- topologias mais utilizadas: estrela, anel e barra.

2.1.2 MAN (Metropolitan Area Network):

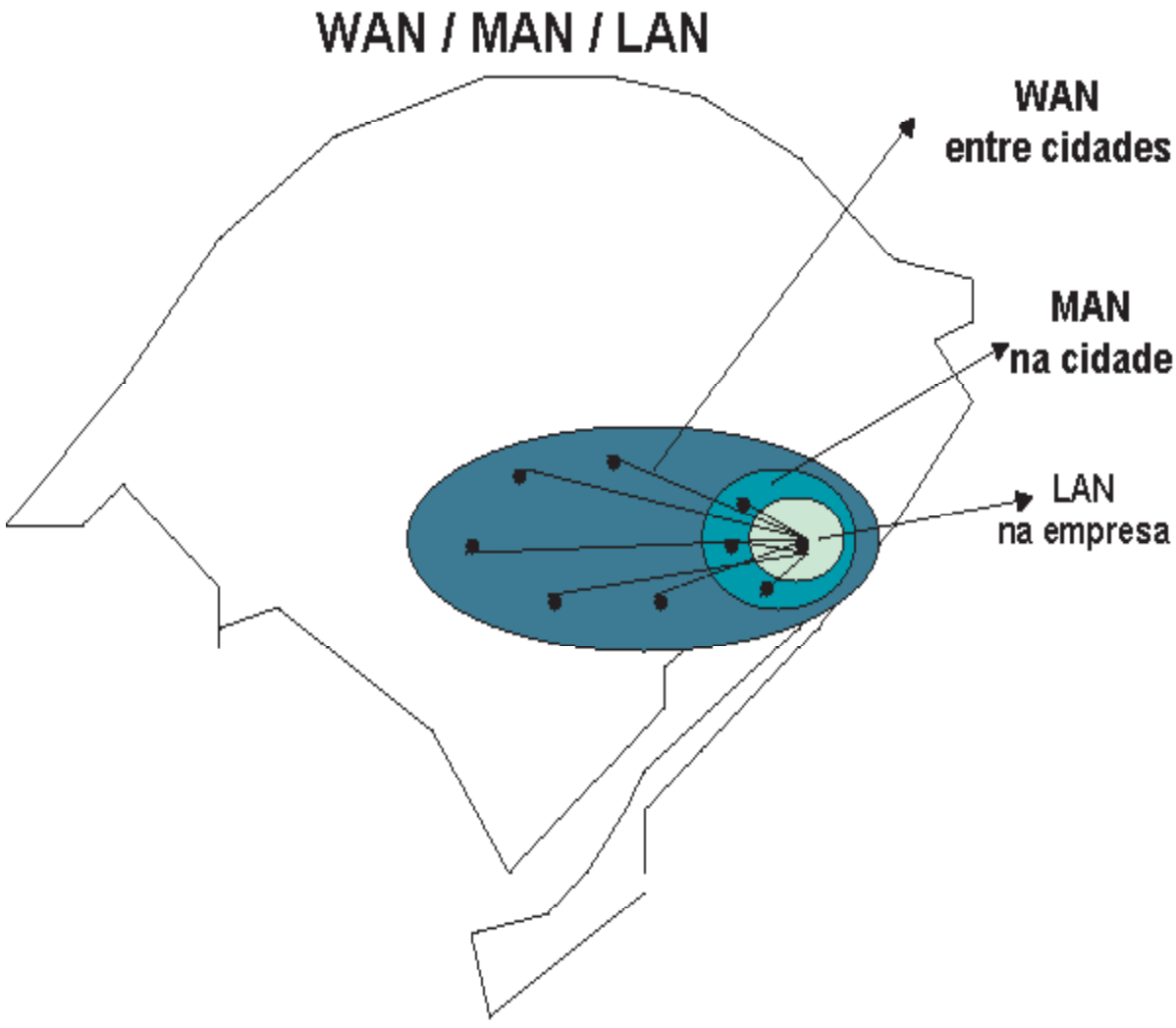
- restrita a uma área metropolitana (cidade e região metropolitana);
- meios de transmissão : Cabos ópticos e coaxiais;
- taxas de transmissão : 10Mbps.

As Redes Metropolitanas (MANs - Metropolitan Area Network) são intermediárias às LANs e WANs, apresentando características semelhantes às redes locais e, em geral, cobrem distâncias maiores que as LANs.

Um bom exemplo de MAN são as redes de TV a cabo.

2.1.3 WAN (Wide Area Network):

- conecta redes locais geograficamente distantes;
- meios de transmissão (satélite, linhas telefônicas, microondas) custo elevado;
- baixas taxas de transmissão (de 64 Kbps a médias de 2 Mbps);
- geralmente são redes públicas.



2.2 Topologias (Conceitos):

- Podemos dizer que, a estrutura de comunicação entre vários processadores é um **"arranjo topológico"** ligado por enlace físico e organizados por regras claras de comunicação, os protocolos. Esses enlaces são as linhas de comunicação.

- A topologia física é muitas vezes confundida com a topologia lógica. Podemos ter topologia lógica em anel mas ligados fisicamente em estrela. Isto é possível principalmente devido aos equipamentos que dispomos hoje no mercado.

2.2.1 Ponto-a-Ponto:

É comunicação entre dois ou mais processadores, não necessariamente conectados diretamente e, que pode usar outros nós como roteadores.

2.2.2 Bus (barramento):

O canal é compartilhado entre todos os processadores, podendo o controle ser centralizado ou distribuído. É a mais comum, possui alto poder de expansão utilizando repetidores.

2.2.3 Ring (anel):

Utiliza em geral ligações ponto-a-ponto que operam em um único sentido de transmissão. O sinal circula o anel até chegar ao destino. É uma topologia confiável, mas com grande limitação quanto a sua expansão pelo aumento de "retardo de transmissão" (intervalo de tempo entre início e chegada do sinal ao nó destino).

2.2.4 Estrela:

Utiliza um nó central (hub ou switch) para chavear e gerenciar a comunicação entre as máquinas. Provoca overhead localizado, já que uma máquina é acionada por vez, simulando um ponto-a-ponto.

3 FORMAS DE COMUNICAÇÃO ATRAVÉS DO MEIO FÍSICO (TIPO) :

- ***simplex*** - o enlace é utilizado apenas em um dos dois possíveis sentidos de transmissão.

- ***half-duplex*** - o enlace é utilizado nos dois possíveis sentidos de transmissão, porém apenas um por vez.

- ***full-duplex*** - o enlace é utilizado simultaneamente nos dois possíveis sentidos de transmissão.

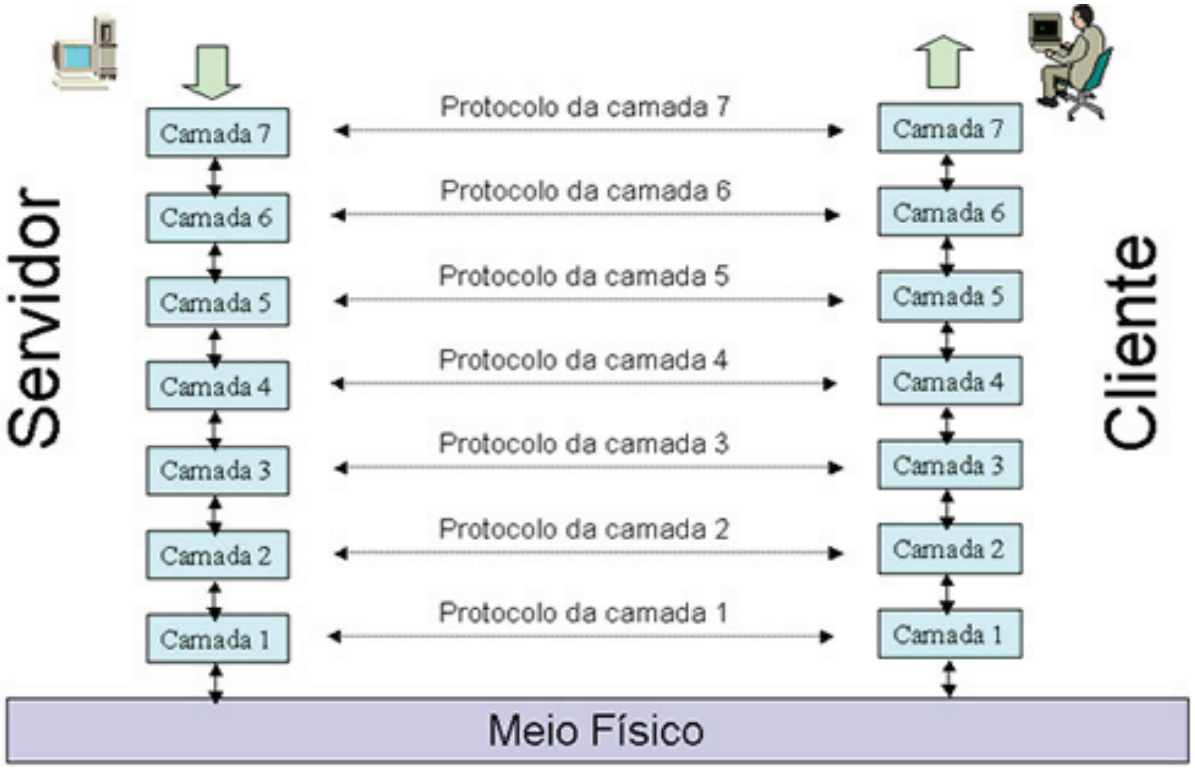
4 MODELO OSI da ISO

O modelo OSI (Open System Interconnection) foi criado em 1977 pela ISO (International Standardization Organization) com o objetivo de criar padrões de conectividade para interligação de sistemas de computadores locais ou remotos. Os aspectos gerais da rede estão divididos em 7 camadas funcionais, facilitando a compreensão de questões fundamentais sobre a rede.

As regras que orientam a conversação entre as camadas são chamadas de "protocolos da camada". Esta conversação é processada entre as respectivas camadas de cada sistema comunicante, porém para que esta comunicação seja efetivada ela tem que "descer" até a camada mais baixa (Física) onde efetivamente as informações são transmitidas.

Os limites entre cada camada adjacente são chamados de interfaces, portanto, a arquitetura de rede é formada de camadas, interfaces e protocolos.

Cada camada oferece um conjunto de serviços à camada superior, usando funções realizadas na própria camada e serviços disponíveis nas camadas inferiores.



4.1 O Modelo de Referência OSI da ISO

4.1.1 Camada 1 - Camada Física

Esta camada compreende as especificações do hardware utilizado na rede (aspectos mecânicos, elétricos e físicos).

4.1.2 Camada 2 - Camada de Enlace

O objetivo desta camada é detectar e opcionalmente corrigir erros que venham a ocorrer na camada física.

4.1.3 Camada 3 - Camada de Rede

Estabelece uma conexão lógica entre dois pontos de uma rede, cuidando do tráfego e roteamentos dos dados na rede.

4.1.4 Camada 4 - Camada de Transporte

As principais funções desta camada são o gerenciamento do estabelecimento e desativação de uma conexão, controle de fluxo, multiplexação das conexões, controle de seqüência de mensagens fim a fim, detecção e recuperação de erros, segmentação e blocagem de mensagens, etc.

4.1.5 Camada 5 - Camada de Sessão

A principal função desta camada é estabelecer e manter conexões entre processos. Reconhece os nós de uma rede local e configura tabelas de endereçamento entre origem e destino, permitindo ao usuário acessar outras máquinas da rede.

4.1.6 Camada 6 - Camada de Apresentação

A função desta camada é a de realizar transformações adequadas nos dados, tais como criptografia, conversão entre caracteres ASCII e EBCDIC, compressão e descompressão de dados.

Os serviços oferecidos por esta camada são: transformação e formatação de dados, seleção de sintaxe, estabelecimento e manutenção de conexões de apresentação. Existe correspondência biunívoca entre os endereços de apresentação e sessão. Não existe nenhum tipo de multiplexação nesta camada de protocolo.

4.1.7 Camada 7 - Camada de Aplicação

Por ser a camada mais alta do modelo OSI, vai fornecer seus serviços funcionando como janela para usuários. Os principais serviços são: correio eletrônico, transferência de arquivos, etc. (X.400, NFS, PC LAN, SNA e outros).

5 MULTIPLEXAÇÃO E MULTIPLEXADORES

Existem duas formas de multiplexação:

– Frequency Division Multiplexing - FDM

– Time Division Multiplexing - TDM

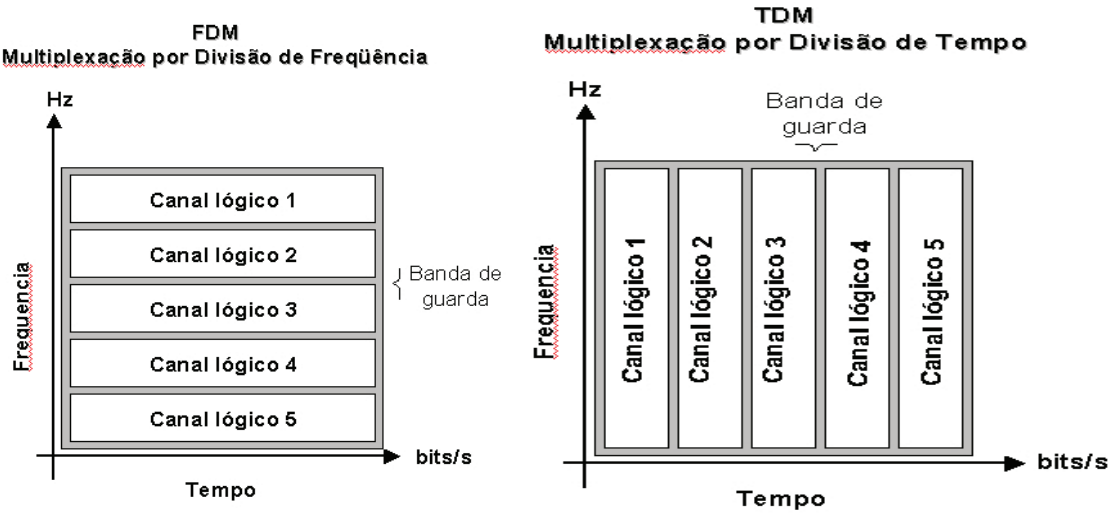
5.1 Multiplexação

É uma técnica que permite a transmissão de mais de um sinal em um mesmo meio físico ou seja é o compartilhamento de um meio de transmissão por vários usuários. Mas qual seria a motivação de se compartilhar um meio de transmissão?

A razão fundamental da implementação da multiplexação se resume na palavra economia. A multiplexação reduz drasticamente o número de meios de transmissão (par trançado, cabo coaxial, fibra óptica) e equipamentos de transmissão de dados e, portanto, os custos de comunicação. Usando uma linha multiplexada vários usuários podem acessar o mesmo meio de comunicação simultaneamente.

Pode-se, portanto, dividir o espaço de Comunicações segundo estes dois enfoques e que caracterizam as duas maneiras de implementar a função de Multiplexação:

- Multiplexação por divisão de freqüência ou **FDM** (Frequency Division Multiplex),
- Multiplexação por divisão de tempo ou **TDM** (Time Division Multiplex).



5.1.1 Características da Técnica de Multiplexação FDM

- é a técnica de multiplexação mais antiga;
- é própria para multiplexação de **sinais analógico**;
- canal lógico multiplexado é caracterizado por uma banda B associada que deve ser menor que a banda do meio;
- é pouco eficiente (exige muita banda de resguardo);
- exige hardware (filtros) próprios para cada canal lógico;
- é caro e de difícil implementação.

5.1.2 Características da Técnica de Multiplexação TDM

- técnica própria para multiplexação de **sinais digitais;**
- os canais lógicos multiplexados são caracterizados por uma taxa medida em bit/s, cuja soma deve ser igual à taxa máxima do meio (canal agregado);
- é eficiente, exige pouco ou nenhum tempo de resguardo;
- pode ser implementado por *software* ou *hardware*;
- é simples e de fácil implementação.

Podemos distinguir dois tipos de canais lógicos:

Canais analógicos, associados a multiplexação analógica FDM, que são caracterizados através de uma determinada largura de banda B, medida em **Hz.**

Ex.: Canal de Voz telefônico B = 4 kHz nominal (útil 3,1 kHz)

Canal de Rádio B = 10 kHz (típico)

Canal de Televisão B = 6 MHz

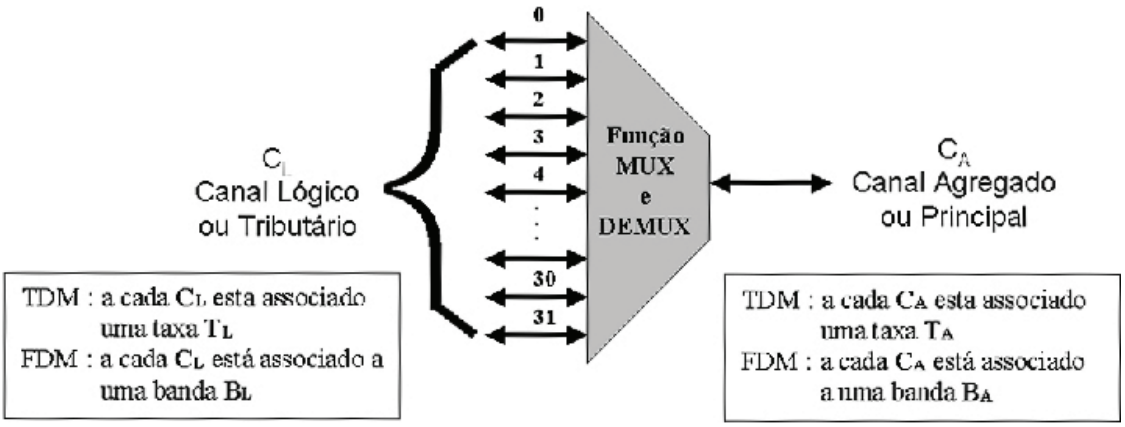
Canais digitais, associados à multiplexação digital TDM, são caracterizados através de uma determinada taxa, medida em bit/s ou bps.

Ex.: Canal digital de voz Taxa: 64 kbit/s

Canal E1 (MUX 1o nível) Taxa: 2,048 Mbit/s

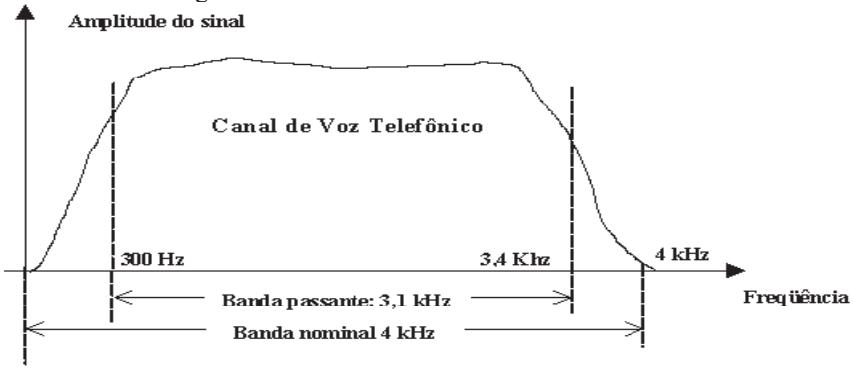
Canal E3 (MUX 3o nível) Taxa: 34 Mbit/s

O multiplexador abaixo realiza tanto as funções de multiplexação como demultiplexação, é duplex, portanto, obedece às relações indicadas.



5.2 Multiplexação FDM

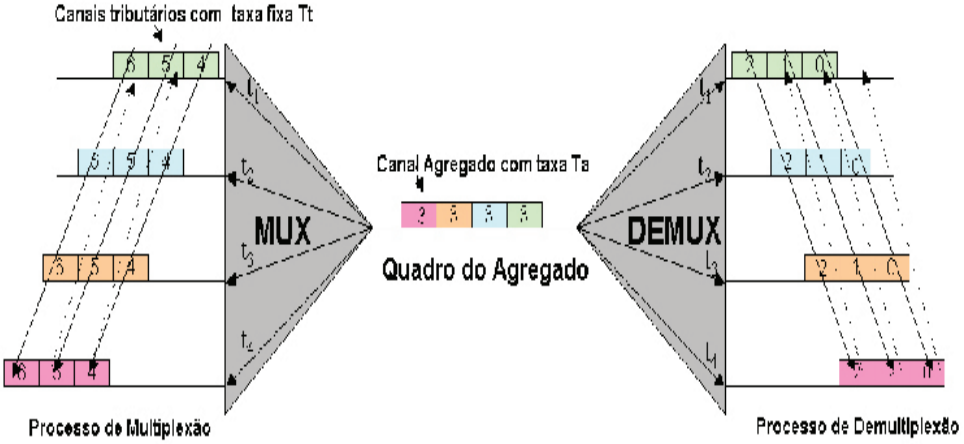
Próprio para sistemas analógicos, foi o primeiro sistema de multiplexação utilizado no sistema telefônico analogico. Neste sistema a base é o chamado canal de voz telefônico mostradas abaixo.



O canal de voz possui uma largura de banda nominal de 4 kHz, porém, desta banda somente 3,1 kHz são aproveitáveis. No primeiro nível de multiplexação FDM, 12 canais de voz são multiplexados, formando o chamado canal de Gupo. Cinco canais de grupo, por sua vez, são multiplexados em um canal de Supergrupo, que contém 60 canais de voz. No terceiro nível, cinco canais de supergrupo são multiplexados em um canal de Grupomestre, que carrega 300 canais de voz.

5.3 Multiplexação TDM

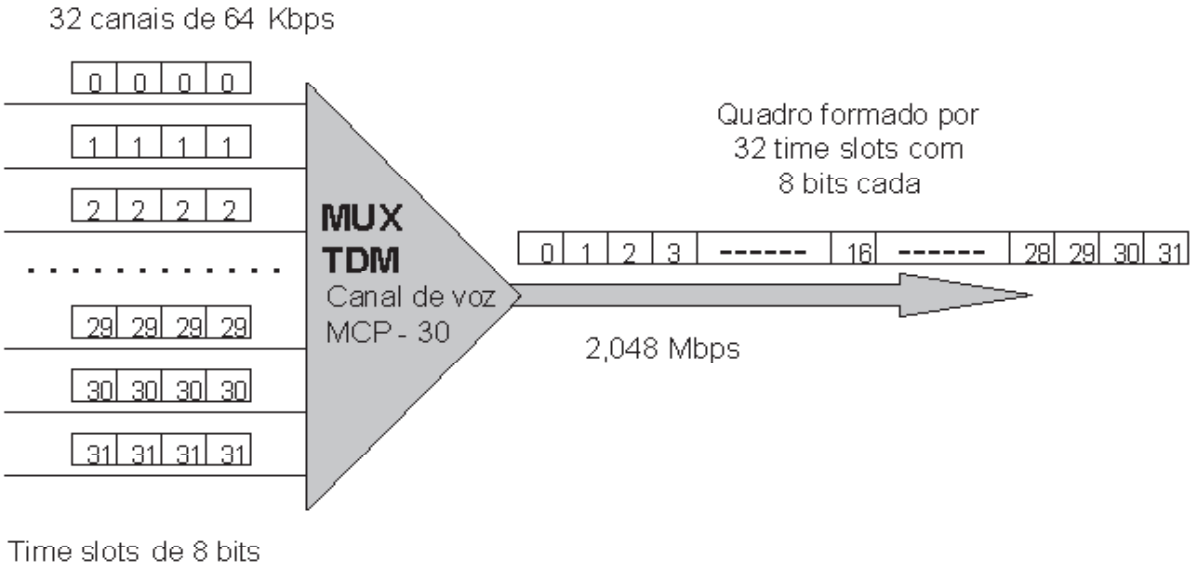
Na multiplexação por divisão de tempo, são amostrados ciclicamente os diversos canais tributários e em cada amostragem é recolhida uma fatia de sinal (fatia de tempo/time slot), que é utilizado na montagem de um quadro agregado, que corresponde às amostragens de todos tributários durante um ciclo de amostragem.



Características da Multiplexação TDM

- Sistema é totalmente síncrono e as taxas, tanto dos canais tributários como do canal agregado, são constantes e fixas.
- Num sistema TDM, a soma das taxas dos tributários deve ser igual à taxa do canal agregado.
- Sistemas TDM são implementados em hardware, através de equipamento específicos.
- TDM é largamente utilizado no suporte telefônico onde a base são os canais digitais de voz de taxa fixa.

5.3.1 Multiplex TDM de Canais de Voz Digitais(Sistema MCP-30/Telebrás)



Características:

- Cada canal é amostrado 8.000 vezes/s, gerando cada vez uma fatia de tempo constituída de 8 bits. (8000/s x 8 bit = 64 kbit/s)

- Canal de Voz digital: Fatias de Tempo de 8 bits (octeto) repetidos de 125 em 125 μs.

$$Taxa \quad \frac{8}{125.10^{\square 6}} \quad 64kbit/s$$

- 32 fatias de tempo (Slot times) são agregadas em um quadro constituído de 32 x 8 bits = 256 bits com duração de 125μs (1/8000).

- A comutação de fatias de tempo dentro do quadro caracterizam a comutação entre os canais digitais segundo um matriz de comutação do tipo 32 x 32.

6 MEIOS DE COMUNICAÇÃO, CABEAMENTO ESTRUTURADO

O sistema de cabeamento (cabling) é o meio físico de transmissão de dados, o qual interliga os nós da rede.

O sistema de cabeamento consiste num aparato físico que conecta os terminais de cada uma das placas de rede do grupo que irá constituir a rede, de modo a formar um único sistema.

Existem várias maneiras de se interligar computadores por cabo.

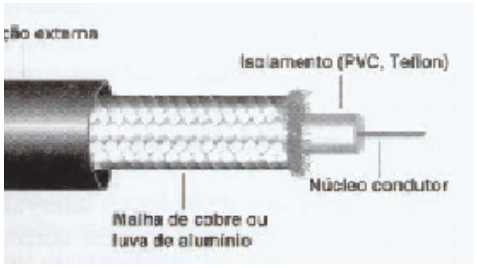
A forma de implementação difere enormemente por:

- Topologia;
- Ambiente a ser interligado;
- Padrão de rede escolhido;
- Custos.

As principais e mais comuns opções de meio físico por cabeamento são:

- Cabo Coaxial;
- Cabo de Par Trançado;
- Fibra Óptica.

Meios de Comunicação, Cabeamento Estruturado



6.1 Cabo Coaxial

Características:

- Custo baixo;
- Relativamente simples de manipular;
- Amplamente utilizado nos sistemas IBM de grande porte;
- Menor sensibilidade à interferência eletromagnética;
- Tipos de cabeamento possíveis: 10Base5 e 10Base2.

ou RG-59/U	75 ohms	3/16"	Utiliza um rabicho RG-62 na extremidade com BNC
Cabo espesso Ethernet	50 ohms	1/2"	Transceptor/MAU no cabo espesso com uma derivaçãdo de par trançado até o cordão da rede
Cabo derivado de Ethernet espesso (não é coaxial, é um cabo de par blindado)	-	3/8"	DIX/AUI

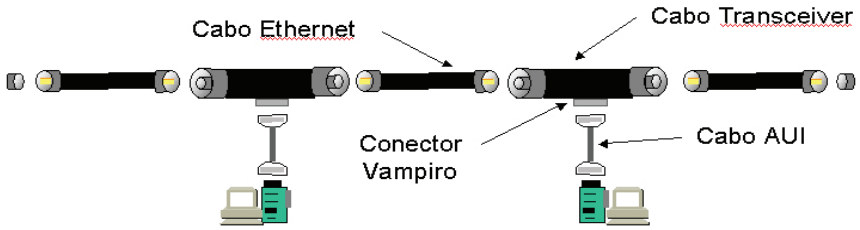
6.1.1 Cabo Coaxial 10Base5

Características:

- Diâmetro do cabo é de 0.4", com 50 ohms de impedância;
- A rede é também chamada de "Thicknet";
- Taxa de transferência: 10 Mbps;
- Tamanho máximo por segmento: 500 metros;
- Os nós se conectam ao meio (cabo grosso) através de um "transceiver" chamado de MAU (Medium Attachment Unit);
- Nas duas extremidades do cabo, devem existir terminadores.

Cabo Coaxial 10Base5

- A conexão dos cabos aos transceivers é feita por meio de conectores tipo "N". Entre o transceiver e a NIC usa-se um conector DB-15 (15 pinos), conhecidos como conectores AUI (Attachment Unit Interface).

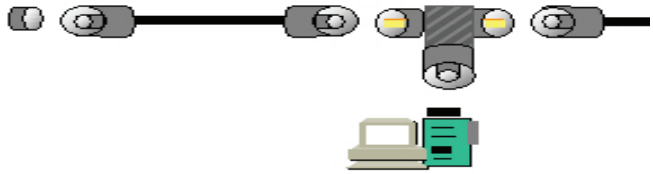


6.1.2 Cabo Coaxial 10Base2

Características:

- Diâmetro do cabo é de 0.18", com 50 ohms de impedância;
- A rede é também chamada de "Thinnet", por usar cabo fino;
- Taxa de transferência: 10 Mbps;
- Tamanho máximo por segmento: 185 metros;
- Os nós se conectam ao meio através de conectores BNC;
- Nas duas extremidades do cabo, devem existir terminadores;

- Não exige transceivers, sua função está embutida nas NICs.



6.2 Comparação entre coaxial fino e grosso:

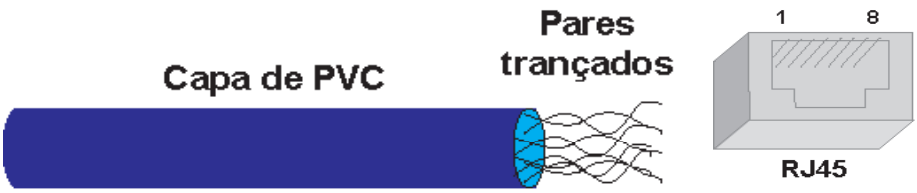
PARÂMETROS	Coaxial Fino	Coaxial Grosso
Banda Passante	10 Mbps	10 Mbps
Comprimento do Barramento	185 m	500 m
Comprimento Máximo do cabo AUI	Não utiliza	50 m
Nós por Barramento	30	100
Distância mínima entre nós	0,50 m	2,50 m
Diâmetro externo	4,90 mm	10,30 mm
Impedância	50 Ω	50 Ω
Blindagem	Simples/dupla	dupla
Conector típico	BNC	TAP coaxial

6.3 Cabo Par Trançado - UTP

6.3.1 Características:

- Custo muito baixo. Simples de manipular;
- Amplamente utilizado nos sistemas de telefonia;
- Alta sensibilidade à interferência eletromagnética;
- Alta atenuação.

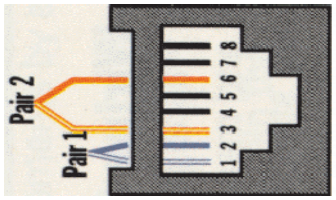
6.3.2 Cabo de Pares Trançados

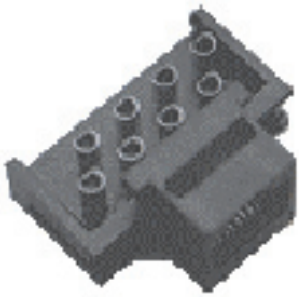


1 - Output Transmit Data + Tx
2 - Output Transmit Data - Tx
3 - Input Receive Data + Rx
6 - Input Receive Data - Rx
4, 5, 7, 8 - não utilizados

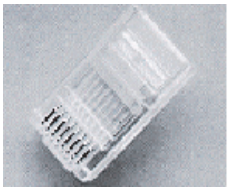
Classificação de par trançado

Categoria	*Velocidade*	*Mídia do Cabo*	*Conector*	*Uso*
Categoria 1	Não adequada a LANs			
Categoria 2	Não adequada a LANs			
Categoria 3	Até 10 Mbps	UTP 4 pares 100 ohms	568A ou 568B de 8 fios	10Base-T
Categoria 4	Até 16 Mbps	STP 2 pares 150 ohms	STP-A	10Base-T ou Token Ring
Categoria 5	Até 100 Mbps	UTP 4 pares 100 ohms	568A ou 568B de 8 fios	10Base-T, 100Base-T, FDDI, ATM, Token Ring

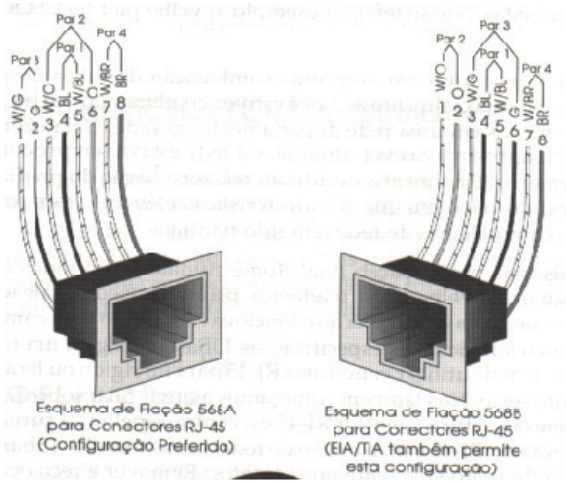




CONECTOR RJ-45
FÊMEA



CONECTOR RJ-45
MACHO



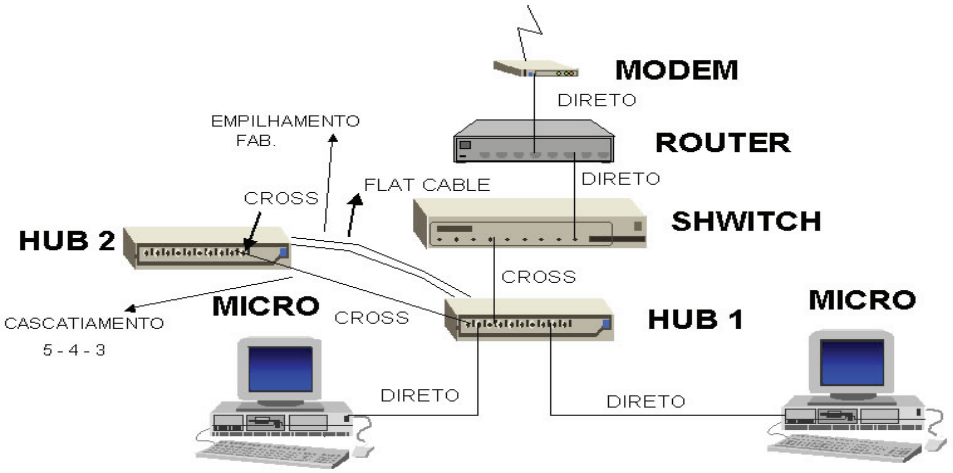
A construção de cabos “par trançados” deve seguir a seguinte ordem dos fios (vistos de cima, da esquerda para direita, com o conector mais afastado do observador).

Sequência Padrão 268A	*Sequêmcia do Padrão 568B*
1 - Branco - Verde	*1 - Branco - Laranja*
2 - Verde	*2- Laranja*
3 - Branco - Laranja	*3 - Branco - Verde*
4 - Azul	*4 - Azul*
5 - Branco - Azul	*5 - Branco - Azul*
6 - Laranja	*6 - Verde*
7 - Branco - Marrom	*7 - Branco - Marrom*
8 - Marrom	*8 - Marrom*

Entre uma máquina e um HUB, deve ser usado um cabo direto.

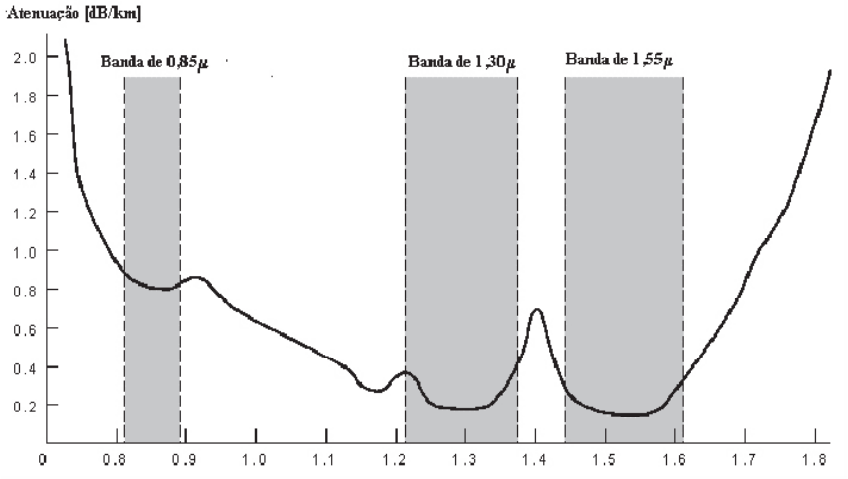
Para construir um cabo direto, as duas pontas devem ser iguais, do Padrão 568A, como descrito acima.

Entre dois HUBs ou um HUB e um SWITCH, ou ainda entre dois micros, deve ser usado um cabo cross-over. Para construir um cabo com os pares trocados, (tipo cross-over) uma ponta deve seguir a sequência do Padrão 568A, enquanto a outra ponta deve seguir o padrão 568B.



6.4 Fibra Óptica

A fibra óptica típica tem três janelas de propagação como mostra o gráfico abaixo.



Para facilitar a manipulação de parâmetros desta zona do espectro de freqüência, adota-se em comunicações ópticas preferencialmente o comprimento de onda λ, que está relacionado com a freqüência pela seguinte expressão:

$\lambda = c / f$ (c: velocidade da luz no vácuo; 3 x 108 m/s)

Nota : Banda de luz visível; 0,4 a 0,7 microns [1micron = μm = 10-6 metros]

As três bandas assinaladas na figura, e que são utilizadas em comunicação de dados, possuem cada uma, uma largura de banda de 26 a 30 THz:

Banda de 0,85μm (ou λ=850ηm)

Nesta banda é utilizada a tecnologia de LED ou Laser e fotodetectores baseados na tecnologia de arsenito de gálio (GaAs). Atenuação de aproximadamente 17% por Km.

Banda de 1,30 μm (ou λ=1300 ηm)

Tecnologia de LED ou Laser baseada em InGaAsP, mais cara porém a atenuação é de aproximadamente 4% por Km.

Banda de 1,55 μm (ou λ=1550 ηm)

Também utiliza tecnologia de LED ou Laser baseada em InGaAsP, com outras dopagens. A atenuação também é de aproximadamente 4% por Km.

As comunicações ópticas estão associadas ao desenvolvimento do laser (1960) e da própria fibra (1970).

Comparando-se a comunicação óptica com as outras técnicas de transmissão, tomando-se como base a banda passante de cada uma, temos:

Pares de fios	⇒	B= ~10^6 Hz
Cabo Coaxial	⇒	B= ~ 10^8 Hz
Radio e TV (espaço)	⇒	B= ~ 5 x 10^8 Hz
Micro Ondas (espaço)	⇒	B= 10^{11} Hz
Luz de Laser (fibra)	⇒	B= 10^{16} Hz

O aumento da capacidade de micro ondas para laser em fibra óptica é de ~100.000 x, representando um aumento fantástico.

6.4.1 Fundamentos físicos da transmissão óptica

As fibras ópticas são feitas tanto em vidro (Sílica - SiO_2) como em plástico. As fibras de plástico são mais baratas, mas com atenuação bem maior. As dimensões físicas do diâmetro variam de 5 a 100 m (1 micron = 10^{-6} m).

O mecanismo de propagação da luz pela fibra está baseado num fenômeno físico chamado refração de um raio luminoso ao passar entre dois meios com índices de refração distintos.

Índice de refração **η=c / v** c = velocidade da luz no vácuo

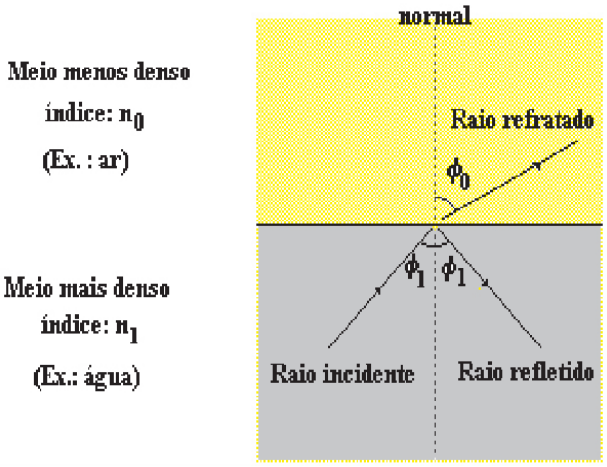
v = velocidade da luz no meio

O índice de refração depende da freqüência pois **λ=c/f**, onde:

λ = comprimento de onda

f = freqüência da onda.

O fenômeno da refração de um raio luminoso



Existe uma relação entre os índices dos meios e os ângulos dos raios luminosos incidentes e refratados em relação a uma reta normal à superfície de separação conhecida como Lei de Snell.

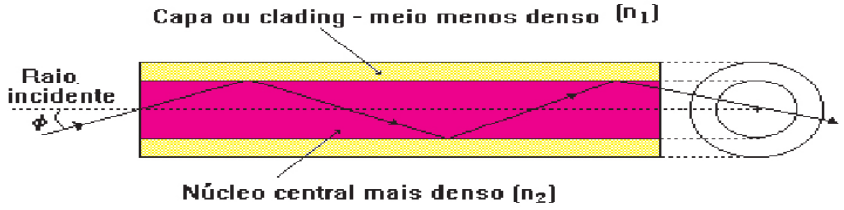
n0 senΦ 0 = n1 sen Φ 1

A física mostra que existe um ângulo Φ c, chamado ângulo crítico, tal que, qualquer ângulo de incidência Φ 1 com Φ 1≤ Φ c , não haverá raio refratado, ou seja , o raio será totalmente refletido de volta no limite entre os dois meios. Pode se mostrar que este ângulo crítico Φ c pode ser dado por:

Φ c = ângulo crítico

Dois meios quaisquer com n1< n2 (n1 menos denso)

A fibra óptica é constituída de um núcleo de vidro mais denso, circundado por uma cobertura (clading) menos densa. Abaixo temos o mecanismo de propagação de um raio luminoso numa fibra óptica.

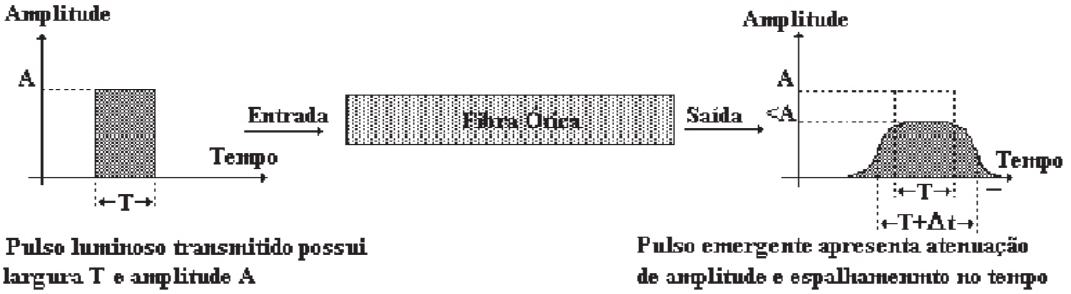


O ângulo crítico corresponde a uma determinada freqüência de radiação e é chamado de modo de transmissão da fibra para uma determinada radiação.

A cada comprimento de onda λ corresponde uma determinada abertura numérica.

A transmissão de uma onda luminosa por uma fibra óptica é limitado quanto ao comprimento da fibra, devido principalmente a dispersão no tempo e a atenuação na amplitude do sinal luminoso. Abaixo, mostramos as conseqüências destes dois fenômenos sobre um pulso luminoso.

Atenuação de amplitude e dispersão temporal em fibra óptica



A atenuação é causada principalmente por impurezas no material (transparência) e é de difícil controle na fabricação.

Fibra de 1a. geração $\lambda = 0{,}8\mu m$ atenuação 5 dB/Km

Fibra de 2a. geração $\lambda = 1{,}3\ \mu m$ atenuação 0,7 - 1 dB/Km

Fibra de 3a. geração $\lambda = 1{,}55\mu m$ atenuação < 0,5 dB/Km

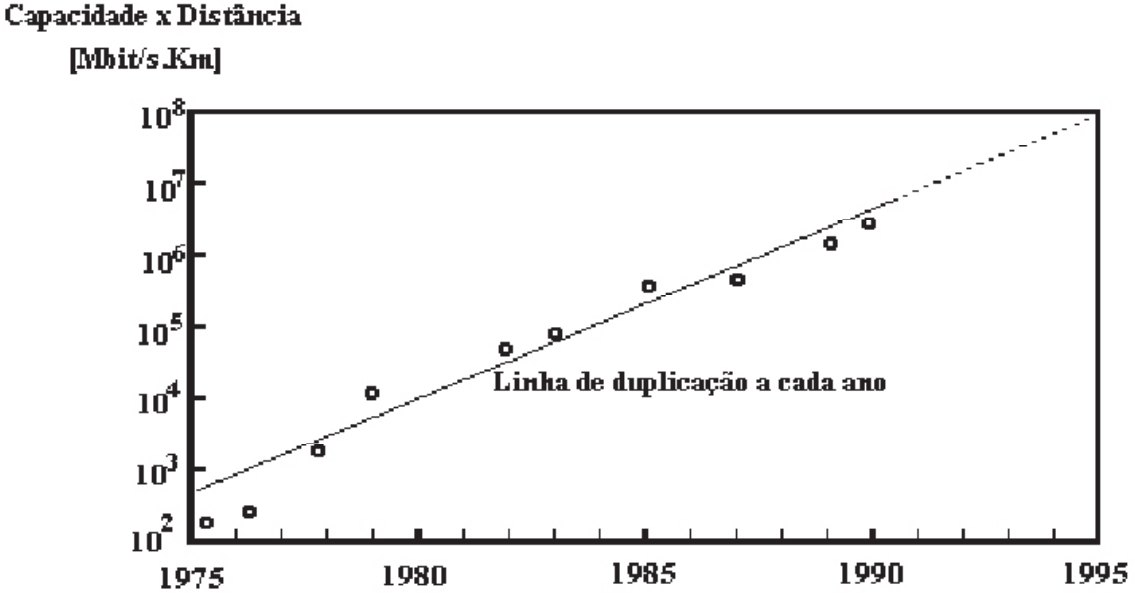
Fibra de 4a. geração $\lambda = 1{,}55\mu m$ atenuação < 0,1 dB/Km

A dispersão de tempo é causada principalmente devido a incidência da luz em vários ângulos na entrada , fazendo com que os caminhos percorridos variem e os tempos de chegada no outro lado também (dispersão modal). Um outro fator que causa dispersão é que a luz na entrada possui diversos comprimentos de onda (luz policromática) o que causa tempos de propagação diferentes e portanto dispersão. Também impurezas dentro da fibra óptica são causadores de dispersão.

A **atenuação de amplitude** do pulso luminoso ao passar por uma fibra óptica é principalmente devido as perdas causadas por impurezas dentro do núcleo central. As modernas técnicas de purificação tem conseguido fibras com atenuação menor que 0,1 dB/Km e a cada ano o comprimento do segmento entre repetidores praticamente dobra. As fibras de vidro são classificadas em três tipos segundo critérios de construção física e a correspondente performance associada. Definiu-se um fator de qualidade para as fibras ópticas denominado, Capacidade de Transmissão da fibra, o qual é praticamente constante para cada tipo de fibra. A Capacidade de Transmissão C_T de uma fibra é por definição, o produto da banda passante (ou também taxa máxima) pela distância. C_T é aproximadamente constante para um determinado tipo de fibra.

CT = Banda Passante x Distância

A capacidade de transmissão das fibras de vidro tem praticamente dobrado a cada ano como pode ser observado abaixo:



6.4.2 Tipos de Fibra óptica:

De acordo com a tecnologia de construção do núcleo central da fibra podemos distinguir entre três tipos de fibra óptica:

a - fibra óptica do tipo multimodo com índice degrau;

b - fibra óptica do tipo multimodo com índice gradual;

c - fibra óptica monomodo.

A fibra multimodo com índice degrau foram as primeiras fibras a surgir. São de fabricação simples e atualmente são largamente empregadas em aplicações de curta distância, como por exemplo em redes locais e automação industrial.

A fibra multimodo com índice gradual apresenta um índice de refração no núcleo variável, consegue-se desta forma uma menor dispersão temporal.

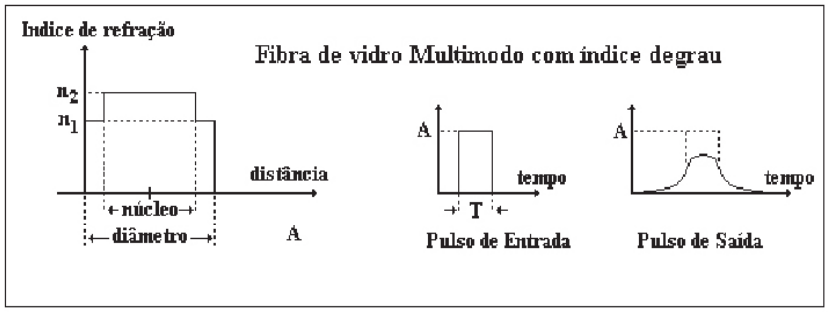
Performances de Fibras Ópticas

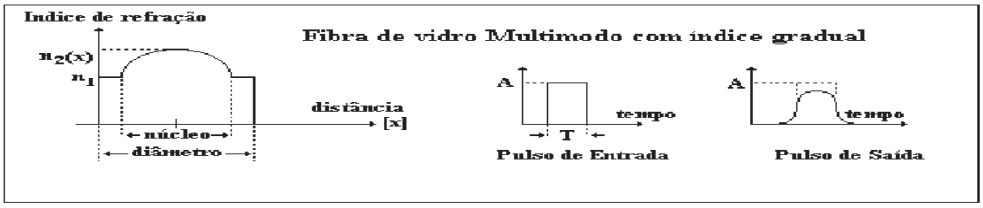
Tipo de Fibra	Capacidade de Transmissão C_T [Hz.Km]	Diâmetro [m]
Multimodo degrau	15 - 25 MHz.Km	100 a 200
Multimodo índice gradual	~ 400 MHz.Km	50 a 100
Monomodo	~ 1000 GHz.Km	2 a 10

Na fibra monomodo consegue-se um modo único de propagação através do estreitamento do diâmetro do núcleo da fibra, minimizando-se desta forma a dispersão temporal.

As fibras monomodo são atualmente as fibras que apresentam o melhor desempenho e por isso são utilizadas em troncos de fibra óptica de longa distância.

Detalhes construtivos dos diversos tipos de fibras e performance quanto a dispersão temporal considerando segmentos de mesmo comprimento.





6.5 Redes Wireless

O que são Redes Wireless?

A palavra wireless provém do inglês: wire (fio, cabo); less (sem); ou seja: sem fios.

Wireless então caracteriza qualquer tipo de conexão para transmissão de informação sem a utilização de fios ou cabos.

Uma rede sem fio é um conjunto de sistemas conectados por tecnologia de rádio através do ar.

Pela extrema facilidade de instalação e uso, as redes sem fio estão crescendo cada vez mais.

Dentro deste modelo de comunicação, enquadram-se várias tecnologias, como Wi-Fi, InfraRed (infravermelho), bluetooth e Wi-Max.

Seu controle remoto de televisão ou aparelho de som, seu telefone celular e uma infinidade de aparelhos trabalham com conexões wireless.

Podemos dizer, como exemplo lúdico, que durante uma conversa entre duas pessoas, temos uma conexão wireless, partindo do principio de que sua voz não utiliza cabos para chegar até o receptor da mensagem.

Nesta categoria de redes, há vários tipos de redes que são: Redes Locais sem Fio ou **WLAN** (Wireless Local Area Network), Redes Metropolitanas sem Fio ou **WMAN** (Wireless Metropolitan Area Network), Redes de Longa Distância sem Fio ou **WWAN** (Wireless Wide Area Network), redes **WLL** (Wireless Local Loop) e o novo conceito de Redes Pessoais Sem Fio ou **WPAN** (Wireless Personal Area Network).

As aplicações de rede estão divididas em dois tipos: aplicações indoor e aplicações outdoor.

Basicamente, se a rede necessita de comunicação entre dois ambientes, a comunicação é realizada por uma aplicação outdoor (dois prédios de uma mesma empresa, por exemplo).

A comunicação dentro de cada um dos prédios é caracterizada como indoor.

A comunicação entre os dois prédios é realizada por uma aplicação outdoor.

Como funcionam?

Através da utilização portadoras de rádio ou infravermelho, as WLANs estabelecem a comunicação de dados entre os pontos da rede.

Os dados são modulados na portadora de rádio e transmitidos através de ondas eletromagnéticas.

Múltiplas portadoras de rádio podem coexistir num mesmo meio, sem que uma interfira na outra.

Para extrair os dados, o receptor sintoniza numa freqüência específica e rejeita as outras portadoras de freqüências diferentes.

Num ambiente típico, o dispositivo transceptor (transmissor / receptor) ou ponto de acesso (Access Point) é conectado a

uma rede local Ethernet convencional (com fio).

Os pontos de acesso não apenas fornecem a comunicação com a rede convencional, como também intermediam o tráfego com os pontos de acesso vizinhos, num esquema de micro células com roaming semelhante a um sistema de telefonia celular.

6.5.1 Componentes de uma Rede Wireless

BSS (Basic Service Set) - Corresponde a uma célula de comunicação da rede sem fio.

STA (Wireless LAN Stations) - São os diversos clientes da rede.

AP (Access Point) - É o nó que coordena a comunicação entre as STAs dentro da BSS.

Funciona como uma ponte de comunicação entre a rede sem fio e a rede convencional.

DS (Distribution System) - Corresponde ao backbone da WLAN, realizando a comunicação entre os APs.

ESS (Extended Service Set) - Conjunto de células BSS cujos APs estão conectados a uma mesma rede convencional.

Nestas condições uma STA pode se movimentar de uma célula BSS para outra permanecendo conectada à rede.

Este processo é denominado de Roaming.

As Redes **WLAN** podem ser configuradas como:

Ad-hoc mode – Independent Basic Service Set (IBSS).

A comunicação entre as estações de trabalho é estabelecida diretamente, sem a necessidade de um AP e de uma rede física para conectar as estações.

Infrastructure mode – Infrastructure Basic Service Set.

A rede possui pontos de acessos (AP) fixos que conectam a rede sem fio à rede convencional e estabelecem a comunicação entre os diversos clientes.

Tecnologias empregadas

Há várias tecnologias envolvidas nas redes locais sem fio e cada uma tem suas particularidades, suas limitações e suas vantagens.

A seguir, são apresentadas algumas das mais empregadas.

Sistemas Narrowband: Os Sistemas Narrowband (banda estreita) operam numa freqüência de rádio específica, mantendo o sinal de de rádio o mais estreito possível o suficiente para passar as informações.

O crosstalk indesejável entre os vários canais de comunicação pode ser evitado coordenando cuidadosamente os diferentes usuários nos diferentes canais de freqüência.

Spread Spectrum: É uma técnica de rádio freqüência desenvolvida pelo exército e utilizado em sistemas de comunicação de missão crítica, garantindo segurança e rentabilidade.

O Spread Spectrum é o mais utilizado atualmente.

Utiliza a técnica de espalhamento espectral com sinais de rádio freqüência de banda larga, foi desenvolvida para dar segurança, integridade e confiabilidade deixando de lado a eficiência no uso da largura de banda.

Em outras palavras, maior largura de banda é consumida que no caso de transmissão narrowaband, mas deixar de lado este aspecto produz um sinal que é, com efeito, muito mais ruidoso e assim mais fácil de detectar, proporcionando aos receptores conhecer os parâmetros do sinal spread-spectrum via broadcast.

Se um receptor não é sintonizado na freqüência correta, um sinal spread-spectrum inspeciona o ruído de fundo.

Existem duas alternativas principais:

- Direct Sequence Spread Spectrum (**DSSS**) e

Direct Sequence Spread Spectrum (DSSS): Gera um bit-code (também chamado de chip ou chipping code) redundante para cada bit transmitido.

Quanto maior o chip maior será a probabilidade de recuperação da informação original.

Contudo, uma maior banda é requerida.

Mesmo que um ou mais bits no chip sejam danificados durante a transmissão, técnicas estatísticas embutidas no rádio são capazes de recuperar os dados originais sem a necessidade de retransmissão.

- Frequency Hopping Spread Spectrum (**FHSS**).

A maioria dos fabricantes de produtos para Wireless LAN tem adotado a tecnologia DSSS depois de considerar os benefícios versus os custos e benefício que se obtém com ela.

Tal é o caso dos produtos Wireless da D-Link.

Frequency-Hopping Spread-Spectrum (FHSS): Utiliza um sinal portador que troca de freqüência no padrão que é conhecido pelo transmissor e receptor.

Devidamente sincronizada, a rede efetua esta troca para manter um único canal analógico de operação.

Outras Tecnologias

A comunicação wireless está presente há um bom tempo no nosso cotidiano.

Falemos da conexão sem fio mais comum – os controles remotos para televisores, som, DVD, entre outros, utilizam conexão por raios infravermelhos (InfraRed).

Essa conexão atua em um alcance máximo de 5m aproximadamente, e com ângulo de 45 graus a partir da fonte.

Apesar de oferecer conexão, o InfraRed trazia a inconveniência de sempre necessitar do alinhamento dos dispositivos, o que criava uma certa dificuldade para locomoção, além de ter a mesma velocidade de uma porta serial.

Foi então desenvolvida a tecnologia conhecida como bluetooth.

Essa tecnologia atua em um raio de 10m, com uma velocidade maior que o InfraRed, utilizando a Rádio Freqüência.

Com bluetooth, o sinal se propaga em todas as direções, não necessita alinhamento e torna a locomoção mais fácil.

Os padrões de velocidade são:

- Assíncrono, a uma taxa máxima de 723,2 kbit/s (unidirecional).
- Bidirecional Síncrono, com taxa de 64 kbit/s, que suporta tráfego de voz entre os dois dispositivos.

Com o sucesso do Wi-Fi, a Intel começou a apoiar uma outra nova tecnologia denominada Wi-Max.

Esta conexão wireless de alta velocidade permite um alcance de até cerca de 48 Km.

Uma outra solução é a Mobile-Fi, uma tecnologia que permite banda larga sem fio em veículos em movimento.

A NTT DoCoMo e alguns startups trabalham atualmente na definição de um protocolo, o que deve acontecer até 2006.

A Nextel também está conduzindo testes com o Mobile-Fi.

Uma outra tecnologia nova que desponta é a UltraWideband, que permite a transmissão de arquivos enormes sobre distâncias curtas – mesmo através de paredes.

Existe no momento uma disputa pela definição deste protocolo entre Texas Instruments e Intel de um lado, e Motorola do outro.

6.5.2 Segurança

Vejamos as principais dicas para se ter uma rede Wireless Segura.

Uma rede sem fio é um conjunto de sistemas conectados por tecnologia de rádio através do ar, com um transmissor irradiando os dados transmitidos através da rede em todas as direções, como impedir que qualquer um possa se conectar a ela e roubar seus dados?

Um ponto de acesso instalado próximo à janela da sala provavelmente permitirá que um vizinho a dois quarteirões da sua casa consiga captar o sinal da sua rede, uma preocupação agravada pela popularidade que as redes sem fio vêm ganhando.

Para garantir a segurança, existem vários sistemas que podem ser implementados, apesar de nem sempre eles virem ativados por default nos pontos de acesso.

O que realmente precisamos saber para que a rede sem fio implementada esteja com o nível correto de segurança?

Em primeiro lugar é preciso conhecer os padrões disponíveis, o que eles podem oferecer e então, de acordo com sua aplicação, política de segurança e objetivo, implementar o nível correto e desejado.

Ser o último disponível não garante, dependendo de sua configuração, que a segurança será eficiente.

É preciso entender, avaliar bem as alternativas e então decidir-se de acordo com sua experiência e as características disponíveis nos produtos que vai utilizar, objetivando também o melhor custo.

A segurança wireless é um trabalho em andamento, com padrões em evolução.

Com tempo e acesso suficientes, um hacker persistente provavelmente conseguirá invadir seu sistema wireless.

Ainda assim, você pode tomar algumas atitudes para dificultar ao máximo possível o trabalho do intruso, nas variantes de conotação maléfica da palavra.

Temos, assim, práticas típicas concernentes a redes sem fio, sejam estas comerciais ou não, conhecidas como wardriving e warchalking.

O padrão IEEE 802.11 fornece o serviço de segurança dos dados através de dois métodos: autenticação e criptografia.

Este padrão 802.11 define duas formas de autenticação: **Open System** e **Shared Key.**

Independente da forma escolhida, qualquer autenticação deve ser realizada entre pares de estações, jamais havendo comunicação multicast.

Em sistemas BSS as estações devem se autenticar e realizar a troca de informações através do Access Point (AP).

As formas de autenticação previstas definem:

Autenticação Open System - é o sistema de autenticação padrão.

Neste sistema, qualquer estação será aceita na rede, bastando requisitar uma autorização.

É o sistema de autenticação nulo.

Autenticação Shared key – neste sistema de autenticação, ambas as estações (requisitante e autenticadora) devem compartilhar uma chave secreta.

A forma de obtenção desta chave não é especificada no padrão, ficando a cargo dos fabricantes a criação deste mecanismo.

A troca de informações durante o funcionamento normal da rede é realizada através da utilização do protocolo WEP.

O AP responde para estação com uma

mensagem de 128 bytes denominada

Challenge Text **("CT").**

Autenticação do cliente feita com **"Shared Keys"**.

A autenticação do tipo Open System foi desenvolvida focando redes que não precisam de segurança para autenticidade de dispositivos.

Nenhuma informação sigilosa deve trafegar nestas redes já que não existe qualquer proteção.

Também se aconselha que estas redes permaneçam separadas da rede interna por um Firewall (a semelhança de uma zona desmilitarizada – DMZ).

A autenticação Shared Key utiliza mecanismos de criptografia para realizar a autenticação dos dispositivos.

Um segredo é utilizado como semente para o algoritmo de criptografia do WEP na cifragem dos quadros.

A forma de obter esta autenticação é a seguinte:

1. Estação que deseja autenticar-se na rede envia uma requisição de autenticação para o AP.
2. O AP responde a esta requisição com um texto desafio contendo 128 bytes de informações pseudorandômicas.
3. A estação requisitante deve então provar que conhece o segredo compartilhado, utilizando-o para cifrar os 128 bytes enviados pelo AP e devolvendo estes dados ao AP.
4. O AP conhece o segredo, então compara o texto originalmente enviado com a resposta da estação.

Se a cifragem da estação foi realizada com o segredo correto, então esta estação pode acessar a rede.

Dentro do utilitário de configuração você poderá habilitar os recursos de segurança.

Na maioria dos casos todos os recursos abaixo vêm desativados por default a fim de que a rede funcione imediatamente, mesmo antes de qualquer coisa ser configurada.

Para os fabricantes, quanto mais simples for a instalação da rede, melhor, pois haverá um número menor de usuários insatisfeitos por não conseguir fazer a coisa funcionar.

Mas, você não é qualquer um.

Vamos então às configurações:

SSID

A primeira linha de defesa é o SSID (Service Set ID), um código alfanumérico que identifica os computadores e pontos

de acesso que fazem parte da rede.

Cada fabricante utiliza um valor default para esta opção, mas você deve alterá-la para um valor alfanumérico qualquer que seja difícil de adivinhar.

Geralmente estará disponível no utilitário de configuração do ponto de acesso a opção “broadcast SSID”.

Ao ativar esta opção o ponto de acesso envia periodicamente o código SSID da rede, permitindo que todos os clientes próximos possam conectar-se na rede sem saber previamente o código.

Ativar esta opção significa abrir mão desta camada de segurança, em troca de tornar a rede mais “plug-and-play”.

Você não precisará mais configurar manualmente o código SSID em todos os micros.

Esta é uma opção desejável em redes de acesso público, como muitas redes implantadas em escolas, aeroportos, etc., mas caso a sua preocupação maior seja a segurança, o melhor é desativar a opção.

Desta forma, apenas quem souber o valor ESSID poderá acessar a rede.

WEP

O Wired Equivalency Privacy (WEP) é o método criptográfico usado nas redes wireless 802.11.

O WEP opera na camada de enlace de dados (data-link layer) e fornece criptografia entre o cliente e o Access Point.

O WEP é baseado no método criptográfico RC4 da RSA, que usa um vetor de inicialização (IV) de 24 bits e uma chave secreta compartilhada (secret shared key) de 40 ou 104 bits.

O IV é concatenado com a secret shared key para formar uma chave de 64 ou 128 bits que é usada para criptografar os dados.

Além disso, o WEP utiliza CRC-32 para calcular o checksum da mensagem, que é incluso no pacote, para garantir a integridade dos dados.

O receptor então recalcula o checksum para garantir que a mensagem não foi alterada.

Apenas o SSID, oferece uma proteção muito fraca.

Mesmo que a opção broadcast SSID esteja desativada, já existem sniffers que podem descobrir rapidamente o SSID da rede monitorando o tráfego de dados.

Eis que surge o WEP, abreviação de Wired-Equivalent Privacy, que como o nome sugere traz como promessa um nível de segurança equivalente à das redes cabeadas.

Na prática o WEP também tem suas falhas, mas não deixa de ser uma camada de proteção essencial, muito mais difícil de penetrar que o SSID sozinho.

O WEP se encarrega de encriptar os dados transmitidos através da rede.

Existem dois padrões WEP, de 64 e de 128 bits.

O padrão de 64 bits é suportado por qualquer ponto de acesso ou interface que siga o padrão WI-FI, o que engloba todos os produtos comercializados atualmente.

O padrão de 128 bits por sua vez não é suportado por todos os produtos.

Para habilitá-lo será preciso que todos os componentes usados na sua rede suportem o padrão, caso contrário os nós que suportarem apenas o padrão de 64 bits ficarão fora da rede.

Na verdade, o WEP é composto de duas chaves distintas, de 40 e 24 bits no padrão de 64 bits e de 104 e 24 bits no padrão de 128.

Por isso, a complexidade encriptação usada nos dois padrões não é a mesma que seria em padrões de 64 e 128 de verdade.

Além do detalhe do número de bits nas chaves de encriptação, o WEP possui outras vulnerabilidades.

Alguns programas já largamente disponíveis são capazes de quebrar as chaves de encriptação caso seja possível monitorar o tráfego da rede durante algumas horas e a tendência é que estas ferramentas se tornem ainda mais sofisticadas com o tempo.

Como disse, o WEP não é perfeito, mas já garante um nível básico de proteção.

Esta é uma chave que foi amplamente utilizada, e ainda é, mas que possui falhas conhecidas e facilmente exploradas por softwares como AirSnort ou WEPCrack.

Em resumo o problema consiste na forma com que se trata a chave e como ela é “empacotada” ao ser agregada ao pacote de dados.

O WEP vem desativado na grande maioria dos pontos de acesso, mas pode ser facilmente ativado através do utilitário de configuração.

O mais complicado é que você precisará definir manualmente uma chave de encriptação (um valor alfanumérico ou hexadecimal, dependendo do utilitário) que deverá ser a mesma em todos os pontos de acesso e estações da rede.

Nas estações a chave, assim como o endereço ESSID e outras configurações de rede podem ser definidos através de outro utilitário, fornecido pelo fabricante da placa.

WPA, um WEP melhorado

Também chamado de WEP2, ou TKIP (Temporal Key Integrity Protocol), essa primeira versão do WPA (Wi-Fi Protected Access) surgiu de um esforço conjunto de membros da Wi-Fi Aliança e de membros do IEEE, empenhados em aumentar o nível de segurança das redes sem fio ainda no ano de 2003, combatendo algumas das vulnerabilidades do WEP.

A partir desse esforço, pretende-se colocar no mercado brevemente produtos que utilizam WPA, que apesar de não ser um padrão IEEE 802.11 ainda, é baseado neste padrão e tem algumas características que fazem dele uma ótima opção para quem precisa de segurança rapidamente: Pode-se utilizar WPA numa rede híbrida que tenha WEP instalado.

Migrar para WPA requer somente atualização de software.

WPA é desenhado para ser compatível com o próximo padrão IEEE 802.11i.

Vantagens do WPA sobre o WEP

Com a substituição do WEP pelo WPA, temos como vantagem melhorar a criptografia dos dados ao utilizar um protocolo de chave temporária (TKIP) que possibilita a criação de chaves por pacotes, além de possuir função detectora de erros chamada Michael, um vetor de inicialização de 48 bits, ao invés de 24 como no WEP e um mecanismo de distribuição de chaves.

Além disso, uma outra vantagem é a melhoria no processo de autenticação de usuários.

Essa autenticação se utiliza do 802.11x e do EAP (Extensible Authentication Protocol), que através de um servidor de autenticação central faz a autenticação de cada usuário antes deste ter acesso a rede.

RADIUS

Este é um padrão de encriptação proprietário que utiliza chaves de encriptação de 128 bits reais, o que o torna muito mais seguro que o WEP. Infelizmente este padrão é suportado apenas por alguns produtos.

Se estiver interessado nesta camada extra de proteção, você precisará pesquisar quais modelos suportam o padrão e selecionar suas placas e pontos de acesso dentro desse círculo restrito.

Os componentes geralmente serão um pouco mais caro, já que você estará pagando também pela camada extra de encriptação.

Permissões de acesso

Além da encriptação você pode considerar implantar também um sistema de segurança baseado em permissões de acesso.

O Windows 95/98/ME permite colocar senhas nos compartilhamentos, enquanto o Windows NT, 2000 Server, já permitem uma segurança mais refinada, baseada em permissões de acesso por endereço IP, por usuário, por grupo, etc.

Usando estes recursos, mesmo que alguém consiga penetrar na sua rede, ainda terá que quebrar a segurança do sistema operacional para conseguir chegar aos seus arquivos.

Isso vale não apenas para redes sem fio, mas também para redes cabeadas, onde qualquer um que tenha acesso a um dos cabos ou a um PC conectado à rede é um invasor em potencial.
Alguns pontos de acesso oferecem a possibilidade de estabelecer uma lista com as placas que têm permissão para utilizar a rede e rejeitar qualquer tentativa de conexão de placas não autorizadas.

O controle é feito através dos endereços MAC das placas, que precisam ser incluídos um a um na lista de permissões, através do utilitário do ponto de acesso.

Muitos oferecem ainda a possibilidade de estabelecer senhas de acesso.

Somando o uso de todos os recursos acima, a rede sem fio pode tornar-se até mais segura do que uma rede cabeada, embora implantar tantas camadas de proteção torne a implantação da rede muito mais trabalhosa.

ACL (Access Control List)

Esta é uma prática herdada das redes cabeadas e dos administradores de redes que gostam de manter controle sobre que equipamentos acessam sua rede.

O controle consiste em uma lista de endereços MAC (físico) dos adaptadores de rede que se deseja permitir a entrada na rede wireless.

Seu uso é bem simples e apesar de técnicas de MAC Spoofing serem hoje bastante conhecidas é algo que agrega boa segurança e pode ser usado em conjunto com qualquer outro padrão, como WEP, WPA etc.

A lista pode ficar no ponto de acesso ou em um PC ou equipamento de rede cabeada, e a cada novo cliente que tenta se conectar seu endereço MAC é validado e comparado aos valores da lista.

Caso ele exista nesta lista, o acesso é liberado.

Para que o invasor possa se conectar e se fazer passar por um cliente válido ele precisa descobrir o MAC utilizado.

Como disse, descobrir isso pode ser relativamente fácil para um hacker experiente que utilize um analisador de protocolo (Ethereal, por exemplo) e um software de mudança de MAC (MACShift por exemplo).

De novo, para aplicações onde é possível agregar mais esta camada, vale a pena pensar e investir em sua implementação, já que o custo é praticamente zero.

O endereço MAC, em geral, está impresso em uma etiqueta fixada a uma placa de rede ou na parte de baixo de um notebook.

Para descobrir o endereço MAC do seu computador no Windows XP, abra uma caixa de comando (*Iniciar / Todos os Programas / Acessórios / Prompt de Comando*), digite **getmac** e pressione a tecla *Enter*.

Faça isso para cada computador na rede e entre com a informação na lista do seu roteador.

Mantendo a sua rede sem fio segura

Na verdade essa lista de sugestões se aplica para todos os casos, sejam redes sem ou com fios.

1. Habilite o WEP.

Como já vimos o WEP é frágil, mas ao mesmo tempo é uma barreira a mais no sistema de segurança.

2. Altere o SSID default dos produtos de rede.

SSID é um identificador de grupos de redes.

Para se juntar a uma rede, o novo dispositivo terá que conhecer previamente o número do SSID, que é configurado no ponto de acesso, para se juntar ao resto dos dispositivos.

Mantendo esse valor default fica mais fácil para o invasor entrar na rede.

3. Não coloque o SSID como nome da empresa, de divisões ou departamentos.

4. Não coloque o SSI como nome de ruas ou logradouros.

5. Se o ponto de acesso suporta broadcast SSID, desabilite essa opção.

6. Troque a senha default dos pontos de acessos e dos roteadores.

Essas senhas são de conhecimento de todos os hackers.

7. Tente colocar o ponto de acesso no centro da empresa.

Diminui a área de abrangência do sinal para fora da empresa.

8. Como administrador você deve repetir esse teste periodicamente na sua empresa a procura de pontos de acessos novos que você não tenha sido informado.

9. Aponte o equipamento notebook com o Netstumbler para fora da empresa para procurar se tem alguém lendo os sinais que transitam na sua rede.

10. Muitos pontos de acessos permitem que você controle o acesso a ele baseado no endereço MAC dos dispositivos clientes.

Crie uma tabela de endereços MAC que possam acessar aquele ponto de acesso.

E mantenha essa tabela atualizada.

11. Utilize um nível extra de autenticação, como o RADIUS, por exemplo, antes de permitir uma associação de um dispositivo novo ao seu ponto de acesso.

Muitas implementações já trazer esse nível de autenticação dentro do protocolo IEEE 802.11b.

12. Pense em criar uma subrede específica para os dispositivos móveis, e disponibilizar um servidor DHCP só para essa sub-rede.

13. Não compre pontos de acesso ou dispositivos móveis que só utilizem WEP com chave de tamanho 40 bits.

14. Somente compre pontos de acessos com memória flash. Há um grande número de pesquisas na área de segurança nesse momento e você vai querer fazer um upgrade de software no futuro.

6.5.3 Protocolos

Porquê a Necessidade de Padrões para uma LAN Sem Fios?

Antes da adesão do protocolo 802.11, fabricantes de redes de dados sem fios faziam equipamentos que eram baseados em tecnologia proprietária.

Sabendo que iam ficar presos ao comprar do mesmo fabricante, os clientes potenciais de redes sem fios viraram para tecnologias mais viradas a protocolos.

Em resultado disto, desenvolvimento de redes sem fios não existia em larga escala, e era considerado um luxo só estando ao alcance de grandes companhias com grandes orçamentos.

O único caminho para redes LAN sem fios (WLAN - Wireless Local Area Network) ser geralmente aceite era se o hardware envolvido era de baixo custo e compatível com os restantes equipamentos.

Reconhecendo que o único caminho para isto acontecer era se existisse um protocolo de redes de dados sem fios.

O grupo 802 do Instituto de Engenheiros da Eletrônica e Eletricidade (IEEE -Institute of Electrical and Electronics Engineers, uma associação sem fins lucrativos que reúne aproximadamente 380.000 membros, em 150 países.

Composto de engenheiros das áreas de telecomunicações, computação, eletrônica e ciências aeroespaciais, entre outras, o IEEE definiu algo em torno de 900 padrões tecnológicos ativos e utilizados pela indústria, e conta com mais 700 em desenvolvimento), tomou o seu décimo primeiro desafio.

Porque uma grande parte dos membros do grupo 802.11 era constituído de empregados dos fabricantes de tecnologias sem fios, existiam muitos empurrões para incluir certas funções na especificação final.

Isto, no entanto atrasou o progresso da finalização do protocolo 802.11, mas também forneceu um protocolo rico em atributos ficando aberto para futuras expansões.

No dia 26 de Junho em 1997, o IEEE anunciou a retificação do protocolo 802.11 para WLAN.

Desde dessa altura, custo associado a desenvolvimento de uma rede baseada no protocolo 802.11 tem descido.

Desde o primeiro protocolo 802.11 ser aprovado em 1997, ainda houve várias tentativas em melhorar o protocolo.

Na introdução dos protocolos, primeiro veio o 802.11, sendo seguido pelo 802.11b.

A seguir veio 802.11a, que fornece até cinco vezes a capacidade de largura de banda do 802.11b.

Agora com a grande procura de serviços de multimídia, vem o desenvolvimento do 802.11e.

A seguir será explicado cada protocolo falando entre outros.

Cada grupo, que segue tem como objetivo acelerar o protocolo 802.11, tornando-o globalmente acessível, não sendo necessário reinventar a camada física (MAC - Media Access Control) do 802.11.

6.5.3.1 802.11b

A camada física do 802.11b utiliza espalhamento espectral por seqüência direta (DSSS – Direct Sequence Spread Spectrum) que usa transmissão aberta (broadcast) de rádio e opera na freqüência de 2,4000 a 2,4835 GHz no total de 14 canais com uma capacidade de transferência de 11 Mbps, em ambientes abertos (~ 450 metros) ou fechados (~ 50 metros).

Esta taxa pode ser reduzida a 5,5 Mbps ou até menos, dependendo das condições do ambiente no qual as ondas estão se propagando (paredes, interferências, etc).

Dentro do conceito de WLAN (Wireless Local Area Network) temos o conhecido Wi-Fi.

O Wi-Fi nada mais é do que um nome comercial para um padrão de rede wireless chamado de 802.11b, utilizado em aplicações indoor.

Hoje em dia existem vários dispositivos a competir para o espaço aéreo no espectro de 2,4 GHz.

Infelizmente a maior parte que causam interferências são comuns em cada lar, como por exemplo, o microondas e os telefones sem fios.

Uma das mais recentes aquisições do 802.11b é do novo protocolo Bluetooth, desenhado para transmissões de curtas distâncias.

Os dispositivos Bluetooth utilizam espalhamento espectral por salto na freqüência (FHSS – Frequency Hopping Spread Spectrum) para comunicar entre eles.

A topologia das redes 802.11b é semelhante a das redes de par trançado, com um Hub central.

A diferença no caso é que simplesmente não existem os fios e que o equipamento central é chamado Access Point cuja função não defere muito da hub: retransmitir os pacotes de dados, de forma que todos os micros da rede os recebam, existem tanto placas PC-Card, que podem ser utilizadas em notebooks e em alguns handhelds, e para placas de micros de mesa.

Exemplo de uma rede 802.11b

6.5.3.2 802.11g

Este é o irmão mais novo do 802.11b e que traz, de uma forma simples e direta, uma única diferença: Sua velocidade alcança 54 Mbits/s contra os 11 Mbits/s do 802.11b.

Não vamos entrar na matemática da largura efetiva de banda dessas tecnologias, mas em resumo temos uma velocidade três ou quatro vezes maior num mesmo raio de alcance.

A freqüência e número de canais são exatamente iguais aos do 802.11b, ou seja, 2.4GHz com 11 canais (3 non overlaping).

Não há muito que falar em termos de 802.11g senão que sua tecnologia mantém total compatibilidade com dispositivos 802.11b e que tudo o que é suportado hoje em segurança também pode ser aplicado a este padrão.

Exemplificando, se temos um ponto de acesso 802.11g e temos dois laptops conectados a ele, sendo um 802.11b e outro 802.11g, a velocidade da rede será 11 Mbits/s obrigatoriamente.

O ponto de acesso irá utilizar a menor velocidade como regra para manter a compatibilidade entre todos os dispositivos conectados.

No mais, o 802.11g traz com suporte nativo o padrão WPA de segurança, que também hoje já se encontra implementado em alguns produtos 802.11b, porém não sendo regra.

O alcance e aplicações também são basicamente os mesmos do 802.11b e ele é claramente uma tecnologia que, aos poucos, irá substituir as implementações do 802.11b, já que mantém a compatibilidade e oferece maior velocidade.

Esta migração já começou e não deve parar tão cedo.

Hoje, o custo ainda é mais alto que o do 802.11b, porém esta curva deve se aproximar assim que o mercado começar a usá-lo em aplicações também industriais e robustas.

5.5.3.3 802.11a

Por causa da grande procura de mais largura de banda, e o número crescente de tecnologias a trabalhar na banda 2,4GHz, foi criado o 802.11a para WLAN a ser utilizado nos Estados Unidos.

Este padrão utiliza a freqüência de 5GHz, onde a interferência não é problema.

Graças à freqüência mais alta, o padrão também é quase cinco vezes mais rápido, atingindo respeitáveis 54 Mbit/seg. Note que esta é a velocidade de transmissão nominal que inclui todos os sinais de modulação, cabeçalhos de pacotes, correção de erros, etc., a velocidade real das redes 802.11a é de 24 a 27 Mbit/seg, pouco mais de 4 vezes mais rápido que no 802.11b.

Outra vantagem é que o 802.11a permite um total de 8 canais simultâneos, contra apenas 3 canais no 802.11b.

Isso permite que mais pontos de acesso sejam utilizados no mesmo ambiente, sem que haja perda de desempenho.

O grande problema é que o padrão também é mais caro, por isso a primeira leva de produtos vai ser destinada ao mercado

corporativo, onde existe mais dinheiro e mais necessidade de redes mais rápidas.

Além disso, por utilizarem uma frequência mais alta, os transmissores 8021.11a também possuem um alcance mais curto, teoricamente metade do alcance dos transmissores 802.11b, o que torna necessário usar mais pontos de acesso para cobrir a mesma área, o que contribui para aumentar ainda mais os custos.

6.5.3.4 802.11e

O 802.11e do IEEE fornece melhoramentos ao protocolo 802.11, sendo também compatível com o 802.11b e o 802.11a.

Os melhoramentos inclui capacidade multimídia feito possível com a adesão da funcionalidade de qualidade de serviços (QoS – Quality of Service), como também melhoramentos em aspectos de segurança.

O que significa isto aos ISP's?

Isto significa a habilidade de oferecer vídeo e áudio à ordem (on demand), serviços de acesso de alta velocidade a Internet e Voz sobre IP (VoIP – Voice over Internet Protocol).

O que significa isto ao cliente final? Isto permite multimídia de alta-fidelidade na forma de vídeo no formato MPEG2, e som com a qualidade de CD, e a redefinição do tradicional uso do telefone utilizando VoIP.

QoS é a chave da funcionalidade do 802.11e.

Ele fornece a funcionalidade necessária para acomodar aplicações sensíveis a tempo com vídeo e áudio.

Grupos do IEEE que estão desenvolvendo outros protocolos:

Grupo 802.11d – Está concentrado no desenvolvimento de equipamentos para definir 802.11 WLAN para funcionar em mercados não suportados pelo protocolo corrente (O corrente protocolo 802.11 só define operações WLAN em alguns países).

Grupo 802.11f – Está a desenvolver Inter-Access Point Protocol (Protocolo de acesso entre pontos), por causa da corrente limitação de proibir roaming entre pontos de acesso de diferentes fabricantes.

Este protocolo permitiria dispositivos sem fios passar por vários pontos de acesso feitos por diferentes fabricantes.

Grupo 802.11g – Estão a trabalhar em conseguir maiores taxas de transmissão na banda de rádio 2,4GHz.

Grupo 802.11h – Está em desenvolvimento do espectro e gestão de extensões de potência para o 802.11a do IEEE para ser utilizado na Europa.

Ponto de Acesso (Access Point)

Um número limite de estações que podem ser conectadas a cada ponto de acesso depende do equipamento utilizado, mas, assim como nas redes Ethernet, a velocidade da rede cai conforme aumenta o número de estações, já que apenas uma pode transmitir de cada vez.

A maior arma do 802.11b contra as redes cabeadas é a versatilidade.

O simples fato de poder interligar os PCs sem precisar passar cabos pelas paredes já é o suficiente para convencer algumas pessoas, mas existem mais alguns recursos interessantes que podem ser explorados. Sem dúvidas, a possibilidade mais interessante é a mobilidade para os portáteis.

Tanto os notebooks quanto handhelds e as futuras webpads podem ser movidos livremente dentro da área coberta pelos pontos de acesso sem que seja perdido o acesso à rede.

Esta possibilidade lhe dará alguma mobilidade dentro de casa para levar o notebook para onde quiser, sem perder o acesso à Web, mas é ainda mais interessante para empresas e escolas.

No caso das empresas a rede permitiria que os funcionários pudessem se deslocar pela empresa sem perder a conectividade com a rede e bastaria entrar pela porta para que o notebook automaticamente se conectasse à rede e sincronizasse os dados necessários.

No caso das escolas a principal utilidade seria fornecer acesso à Web aos alunos.

Esta já é uma realidade em algumas universidades e pode tornar-se algo muito comum dentro dos próximos anos.

A velocidade das redes 802.11b é de 11 Mbps, comparável à das redes Ethernet de 10 Mbps, mas muito atrás da velocidade das redes de 100 Mbps.

Estes 11 Mbps não são adequados para redes com um tráfego muito pesado, mas são mais do que suficientes para compartilhar o acesso à web, trocar pequenos arquivos, jogar games multiplayer, etc.

Note que os 11 Mbps são a taxa bruta de transmissão de dados, que incluem modulação, códigos de correção de erro, retransmissões de pacotes, etc., como em outras arquiteturas de rede.

A velocidade real de conexão fica em torno de 6 Mbps, o suficiente para transmitir arquivos a 750 KB/s, uma velocidade real semelhante à das redes Ethernet de 10 Mbps.

Mas, existe a possibilidade de combinar o melhor das duas tecnologias, conectando um ponto de acesso 802.11b a uma rede Ethernet já existente.

No ponto de acesso da figura abaixo você pode notar que existem portas RJ-45 da tecnologia Ethernet que trabalham a 100Mbps, veja figura:

7 ATIVOS DE REDES

1- Elementos de redes de computadores

Para que uma rede de computadores possa funcionar é necessário que existam, além do cabeamento propriamente dito, equipamentos de comunicação cuja função é controlar a comunicação entre as estações de trabalho e periféricos ou mesmo entre os próprios equipamentos de comunicação.

Vários equipamentos são usados com finalidades diferentes em uma rede de computadores.

Dentre esses equipamentos destacam-se:

7.1 Hubs

A melhor tradução para hub em português é concentrador.

Os hubs foram introduzidos como melhorias para as topologias de redes de computadores.

Trata-se de um dispositivo de hardware que funciona na camada física do Modelo OSI, que atua como um ponto de conexão central de fiação, normalmente na configuração física em estrela.

7.1.1 Tipos de Hubs

Existem três tipos principais de hub: passivo, ativo e inteligente.

Um hub passivo não requer energia para funcionar, atuando meramente como um ponto de conexão físico.

Os hubs ativos, por outro lado, requerem energia e são utilizados para reabilitar e fortalecer os sinais que passam por eles.

Já os hubs inteligentes podem fornecer serviços como comutação de pacotes e roteamento de tráfego.

7.1.1.1 Hub Passivo

Um hub passivo é um dispositivo adequado para redes onde a distribuição física das estações é tal que a degradação do sinal, quando emitido entre quaisquer estações adjacentes está dentro do limite aceitável, ou seja, apenas conecta segmentos de mídia entre si sem a regeneração de sinal.

Esse tipo de concentrador, que funciona como um centro de fiação, diminui o problema causado pelo aumento da distância entre estações consecutivas.

7.1.2.2 Hub Ativo

Um hub ativo é semelhante ao hub passivo, mas possui repetidores embutidos nas portas onde são conectados os cabos que ligam o hub às estações.

Esse tipo de hub restaura a amplitude, a forma e o sincronismo do sinal quando ele passa por suas duas portas.

A principal desvantagem é que alguns hubs ativos amplificam os ruídos juntamente com o sinal.

A distância máxima permitida entre um hub ativo e uma estação é geralmente o dobro da que é permitida quando um hub passivo é utilizado.

7.1.2.3 Hub Inteligente

Os hubs inteligentes, além da regeneração de sinal e gerenciamento de rede, também executam atividades tais como a seleção do caminho dos sinais, podendo escolher rotas diferentes para o envio desse sinal.

Esta possibilidade de comutação significa que a rede pode ser estruturada de forma que todos os segmentos da mídia de transmissão estejam permanentemente conectados, mas cada segmento seja utilizado apenas quando um sinal for direcionado para um determinado equipamento nesse segmento.

7.1.2 Interligação de hubs – Regra 5-4-3

Os hubs podem ser utilizados em diversas implementações de redes.

Dentro das limitações impostas por cada fabricante, é possível interligar equipamentos distintos e de marcas distintas, obedecendo-se à regra 5-4-3 para hubs.

Esta regra limita em distância o número de segmentos ponto a ponto de uma rede em 5 (100 metros por segmento e um máximo de 500 metros), o número de repetidores existentes (no máximo 4), sendo um repetidor para cada par de segmentos e apenas 3 segmentos podem conter hosts.

Por exemplo, uma aplicação é mostrada a seguir, onde as seguintes limitações se aplicam para um sinal no sentido da estação origem para a estação destino: No máximo 5 segmentos (a conexão entre o hub e a estação conta como um segmento), com até 4 repetidores/hubs e o limite de 3 segmentos populosos.

Segmentos populosos contêm mais de dois nós. Segmentos não populosos contêm somente um nodo em cada ponta.

Redes em estrela são consideradas como segmentos não populosos.

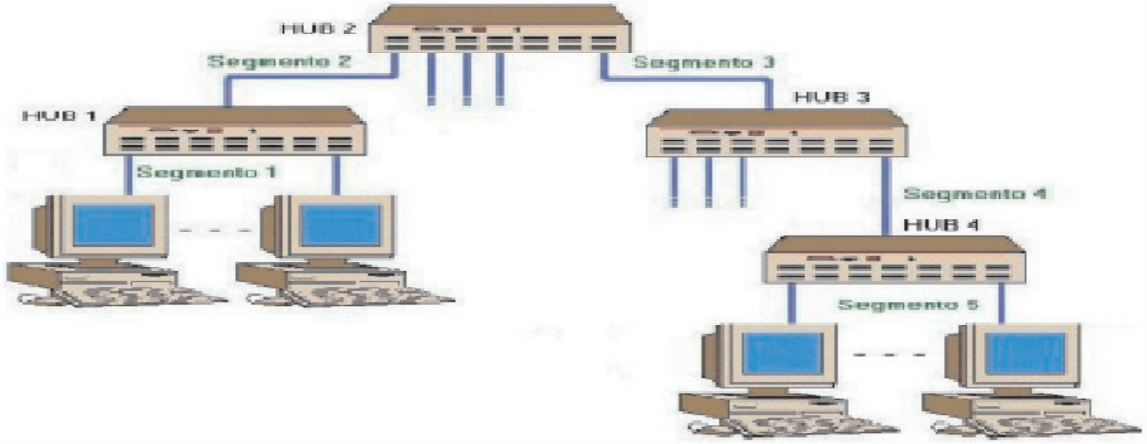


Figura 1 – Regra 5-4-3

7.1.3 Cascateamento e Empilhamento

A maioria dos modelos de hubs possibilita a interligação dos equipamentos sob duas formas básicas: o empilhamento e o cascateamento.

7.1.3.1 Cascateamento

Os hubs podem ser interligados em uma configuração hierárquica caracterizando o que se chama de cascateamento.

Em interligações com mais de dois hubs, especificam-se os hubs terminais que ficam nas pontas do conjunto como HHub (Header Hub) e os hubs intermediários como IHubs (Intermediary Hubs).

Os hubs terminais utilizam uma de suas portas para se conectar ao hub vizinho, já que fazem o papel de terminadores do conjunto.

Os hubs intermediários utilizam duas de suas portas para se comunicar com os vizinhos, funcionando como uma ponte para os demais hubs do segmento.

O número de portas utilizadas para o cascateamento pode ser obtido pela seguinte expressão: P= 2 n-2, onde P é o número de portas e n é o número de hubs usados no cascateamento.

No cascateamento, a interligação se dá através de uma porta de um equipamento com a outra porta de outro equipamento, sendo a largura de banda limitada à velocidade da porta (10/100/1000Mbps).

As regras para o cascateamento dependem das especificações dos dispositivos porque neste tipo de ligação, à medida que vai se "cacasteando", a performance da rede vai caindo.

Alguns fabricantes limitam em cinco metros o comprimento máximo do cabo UTP que conecta os hubs com velocidades até 100Mbps.

Normalmente utilizam-se portas frontais que podem ser específicas para este fim, chamadas de portas Up-Link.

Essas portas utilizam cabeamento comum, dispensando a utilização de cabo cross-over.

Convém observar que em alguns modelos é necessária a ativação desta porta especial, o que obriga ao instalador conhecer

o manual de operação do equipamento.

7.1.3.2 Empilhamento

Existem hubs empilháveis (stackable), que são ligados por um barramento de alta velocidade e que funcionam como se fosse um único equipamento.

Nesse caso, o empilhamento pode ser feito apenas entre equipamentos de um mesmo fabricante e não ocorre a incidência da regra 5-4-3 na pilha de hubs.

No empilhamento, a interligação ocorre através de uma porta específica para empilhamento (stack) e cada fabricante possui um tipo de interface própria a qual possui velocidade transmissão maior que a velocidade das portas de conexão.

O empilhamento é mais eficiente do que o cascateamento porque não ocupa as portas frontais para conexão, aumentando com isso a quantidade de portas disponíveis para os equipamentos da rede.

Pode-se empilhar até quatro equipamentos, sempre considerando as observações e limitações de cada fabricante.

7.2 - Switches

Trata-se de uma evolução do hub, com funções de pontes e roteadores e hardware especial que lhe confere baixo custo e alta eficiência.

A tecnologia dos switches agrega avanços tecnológicos capazes aumentar o throughput da rede.

Ele consegue chavear com velocidade, disponibilizando uma banda maior para quem envia ou recebe um pacote de dados.

Um switch permite a troca de mensagens entre várias estações ao mesmo tempo e não apenas compartilhar um meio para isso, como acontece com os hubs.

Desta forma estações podem obter para si taxas efetivas de transmissão bem maiores do que as observadas em uma rede utilizando hubs.

O switch tornou-se necessário devido às demandas por maiores taxas de transmissão e melhor utilização dos meios físicos.

Além deste fato, podem-se definir níveis de prioridade nas portas.

7.3 – Bridges (pontes)

A bridge (ponte) é outro dispositivo usado para conectar segmentos de rede que operam no nível 2 do modelo OSI (Enlace de dados) e são muito utilizadas para isolar (diminuir) o tráfego entre segmentos de redes.

As pontes lêem o endereço MAC de destino de cada pacote de dados que chega e, depois, examinam as tabelas de bridging para determinar o que fazer com o pacote.

Por funcionar basicamente como um repetidor, uma ponte pode receber transmissões de qualquer segmento.

Entretanto, ela é mais rigorosa do que um repetidor na hora de retransmitir esses sinais.

Se o endereço de destino do pacote estiver no mesmo segmento em que o pacote foi recebido, a ponte não encaminhará o pacote, mas, se o destino do pacote estiver em um segmento diferente, a ponte o passará adiante.

Encaminhando apenas os pacotes endereçados a outros segmentos de rede, uma ponte consegue reduzir consideravelmente o congestionamento na rede.

Entretanto, pontes encaminham todas as transmissões de difusão (broadcast) que recebem e, portanto são incapazes de reduzir este tipo de tráfego.

As pontes podem conectar segmentos que utilizem tipos diferentes de meio.

Um exemplo é uma ponte de conversão, que faz a tradução de diferentes métodos de acesso de meio, permitindo que sejam conectados vários tipos de rede.

Outro tipo especial, a ponte transparente ou de aprendizado, “aprende” com o tempo para onde deve direcionar os pacotes que recebe de forma contínua, montando tabelas de bridging e incluindo novas entradas quando necessário.

Uma das desvantagens que podem surgir da utilização de pontes é a de levar mais tempo do que os repetidores para atravessar os dados, pois examinam o endereço MAC de cada pacote.

Elas também são mais caras e difíceis de operar.

As pontes são totalmente transparentes para os outros dispositivos de rede e, por isso diversas redes locais interligadas por uma ponte formam uma única rede lógica.

Também não há limite no número de pontes como ocorre no caso de repetidores.

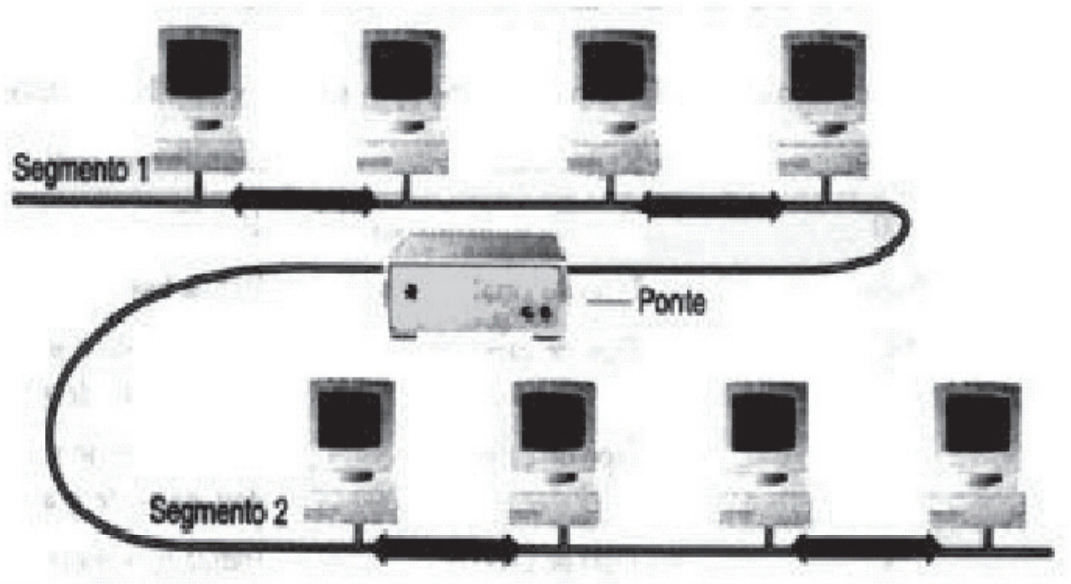


Figura 2 - Exemplo do emprego de bridge

7.3.1 Bridges X Switches

Existem certas características que são comuns tanto nas pontes quanto nos switches na camada de enlace de dados.

Uma ponte não examina informação da camada 3 (e superiores).

Segmentam domínios de banda, mas não domínios de difusão.

Um switch se comporta essencialmente como uma ponte, porém, tira vantagem de uma eletrônica mais rápida que possibilita uma latência menor, ou seja, é mais rápido, oferece uma densidade maior de portas e um "custo" mais baixo por porta.

Uma ponte trabalha no modo "armazenar e encaminhar".

A ponte recebe a estrutura completa, determina a porta de saída, prepara a estrutura, calcula um CRC e transmite-a, caso o meio esteja livre.

Já o switch trabalha no modo "processamento de penetração".

No switch, o endereço de destino é rapidamente examinado, a porta de saída é escolhida e imediatamente os bits são transmitidos.

1.4 – Repetidores e Amplificares

São dispositivos da camada física do modelo OSI que recebem, amplificam e retransmitem sinais, sendo utilizados na conexão de dois ou mais segmentos de uma LAN, reconstituindo e retransmitindo os sinais elétricos do meio físico.

Os repetidores e amplificadores são usados em redes de computadores que utilizam esquemas de sinalização digitais para reforçar o sinal que trafega pela rede.

Nessas redes, a potência do sinal diminui (ou é atenuada) com o aumento da distância entre os pontos de rede.

Assim, eles amplificam o sinal recebido de um segmento de rede e repetem esse mesmo sinal no outro segmento.

Alguns modelos disponíveis possuem recursos de "auto-particionamento", ou seja, em ocorrendo uma falha dos segmentos da rede, o dispositivo irá efetivamente isolar o acesso à conexão defeituosa, permitindo que a transmissão de dados aos segmentos remanescentes não seja afetada.

A limitação do número de repetidores está de acordo com o protocolo utilizado (no protocolo Ethernet o número máximo é de quatro).

7.4 Repetidores

Um repetidor exerce a função de regenerador de sinal entre dois segmentos de redes locais.

Eles são necessários para fornecer corrente para controlar cabos longos.

Um repetidor permite interconectar dois segmentos de rede de mesma tecnologia e, eventualmente, podem ligar redes com meios de transmissão diferentes, por exemplo, cabo coaxial com fibra óptica ou com pares trançados.

Como resultado é possível aumentar a extensão de uma rede local, de forma que o conjunto de segmentos interconectados se comporte como um único segmento.

Os repetidores permitem que sejam realizadas transmissões confiáveis em distâncias maiores do normalmente seriam possíveis com o tipo de meio utilizado.

Quando um repetidor recebe uma transmissão atenuada, ele limpa e reforça o sinal e o transfere para o próximo segmento.

Os repetidores operam ao nível dos cabos e sinais elétricos, amplificam e re-sincronizam os sinais.

Assim, todo o tráfego em um segmento da rede é repassado para o outro.

Os segmentos de rede conectados por repetidores são chamados IRLs (Inter-Repeater Links).

Esses segmentos devem obedecer às restrições de tamanho máximo para cada tipo de meio físico.

Muitas vezes o nome hub é atribuído indevidamente aos repetidores.

Em geral, as arquiteturas de rede especificam o número máximo de repetidores permitido em uma única rede.

Por norma, podemos ter, no máximo, quatro repetidores entre duas estações de uma rede.

A razão para isso é um fenômeno chamado retardo de propagação.

Nos casos onde existem vários repetidores na mesma rede, o curto período de tempo que cada repetidor leva para limpar e amplificar o sinal, multiplicado pelo número de repetidores e ou amplificadores, pode resultar em um retardo perceptível nas transmissões.

Ao utilizar repetidores é necessário considerar que eles não possuem recursos de endereçamento ou conversão, não podendo, ser usados com o objetivo de reduzir o congestionamento da rede.

1.4.2 – Amplificadores

Os amplificadores, embora semelhantes aos repetidores em finalidade, são usados para permitir que sejam realizadas transmissões em maiores distâncias em redes que usam sinalização analógica (conhecida com transmissão de banda larga).

Os sinais analógicos podem transferir voz e dados simultaneamente.

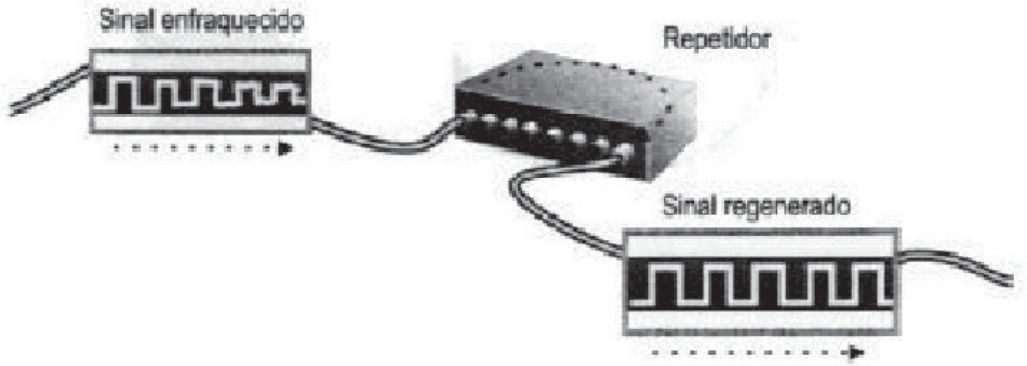


Figura 3 - Exemplo do emprego de repetidor

7.5 Roteadores

Os roteadores são também chamados de gateways de rede ou gateways conversores de meio.

Não examinam todo o frame existente na rede como acontece com as pontes.

Um roteador é um dispositivo de conectividade que atua na camada de rede do Modelo OSI e pode conectar dois ou mais segmentos de rede (ou sub redes).

Como são nós de rede, eles percebem apenas os frames a eles endereçados.

Abrem cada frame e lêem as informações de endereço nível 3 (no caso do TCP/IP, o endereço IP) , extraindo as informações sobre a rede para qual deve ser endereçado, enviando-o para uma de suas interfaces de rede.

Um roteador funciona de maneira semelhante a uma ponte, mas, em vez de usar o endereço MAC da máquina para filtrar o tráfego, ele usa as informações de endereçamento de rede encontradas na área da camada de rede do pacote de dados.

Após obter essas informações de endereçamento, o roteador utiliza uma tabela de roteamento com endereços da rede para determinar para onde encaminhar o pacote.

Ele faz isso comparando o endereço da rede do pacote com as entradas na tabela de roteamento.

Se for encontrada uma correspondência, o pacote e enviado para a rota determinada.

No entanto, se o roteador não encontrar uma correspondência, o pacote de dados geralmente é abandonado.

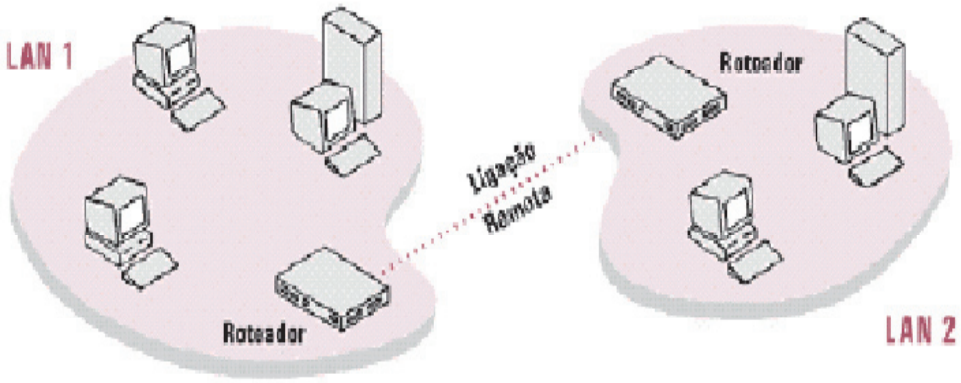


Figura 4 - Emprego de roteadores em redes locais

7.5.1 Roteadores X Switches

A distinção entre switches e roteadores atualmente é um tanto difícil.

Muitos switches admitem módulos de roteamento, assim como a maioria dos roteadores também controla protocolos de pontes e comutação.

Alguns fabricantes chamam seus produtos de Switch de camada 3, switch de roteamento, roteadores de comutação ou switch de várias camadas.

Alguns roteadores podem encaminhar pacotes com extrema rapidez, então os fabricantes acrescentam a palavra “switch” para lembrar que o roteador é (quase) tão rápido quanto um switch de camada 3.

7.6 Brouters

O termo brouter é uma combinação das palavras bridge (ponte) e router (roteador).

Como o nome sugere, um brouter combina funções de uma ponte e de um roteador.

Quando um brouter recebe um pacote de dados, ele verifica se o mesmo foi enviado com protocolo roteável ou não roteável.

No caso de se tratar de um pacote de protocolo roteável, o brouter executa uma função de roteamento enviando o pacote ao seu destino fora do segmento local, se necessário.

Por outro lado, se o pacote contiver um protocolo não roteável, o brouter executa uma função de bridging, usando o endereço MAC para encontrar o destinatário correto no segmento local.

Os brouters precisam manter tabelas de bridging e de roteamento para realizar essas funções, conseqüentemente eles atuam nas camadas de rede e de enlace de dados do Modelo OSI.

7.7 Gateways

Um gateway permite a comunicação entre dois ou mais segmentos de uma rede, executando basicamente a mesma função do roteador e ainda outras duas: a conversão de protocolos entre redes ou simplesmente o encaminhamento de pacotes específicos de uma rede para outra.

Um gateway representa geralmente um computador dedicado executando um software que realiza serviços de conversão e que permite a realização de comunicações entre sistemas diferentes na rede.

Atuam principalmente na camada de aplicação do modelo OSI, embora realizem freqüentemente funções na camada de sessão e, ocasionalmente, na camada de rede.

Entretanto, para a maioria das aplicações, um gateway atua em ou acima da camada de transporte.

Os Gateways, também são chamados de conversores de protocolos e adequados para conexões de WAN.

Diferente da ponte que apenas canaliza a mensagem usando um protocolo dentro do formato de dados de outro protocolo, um gateway pode receber uma mensagem com um tipo de protocolo e converter os dados para outro formato de protocolo.

Por exemplo, um cliente utilizando IPX/SPX que destina uma mensagem a um cliente executando algum outro protocolo (por exemplo, TCP/IP), em um segmento de rede remoto.

Após determinar que o destino do pacote de mensagem é uma estação TCP/IP, o gateway converte os dados da mensagem para este protocolo.

Convém notar que a dificuldade na conversão de protocolos torna os gateways bastante complexos e de difícil implementação, o que pode aumentar em muito o custo da interligação de redes remotas.

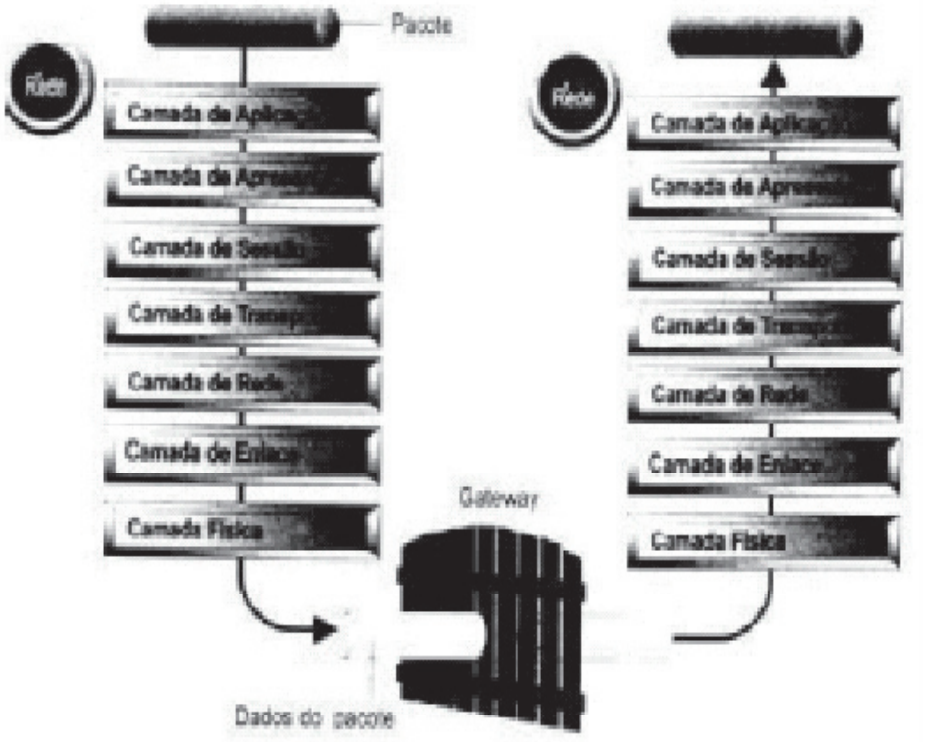


Figura 5 - Emprego de gateway

7.8 Transceivers

Os termos Transceiver, Network Interface Card (NIC) e Adaptador de Mídia descrevem interfaces de rede.

Tecnicamente, uma interface de rede inclui todas as conexões físicas e lógicas entre um computador, ou outro dispositivo, e a mídia de transmissão.

Um transceiver tem a função de retirar da rede os sinais endereçados ao dispositivo em que está ligado.

É alimentado eletricamente por tal dispositivo.

Quando é usada mídia física (par trançado ou fibra óptica), os transceptores são geralmente acoplados aos conectores de gênero oposto daqueles diretamente acoplados à mídia (sendo macho ou fêmea).

Quando não for usada mídia física, os transceptores são apenas dispositivos de transmissão e recepção porque não é necessário nenhum tipo de conector mecânico.

Uma rede pode conter várias rotas com de cabos e repetidores, mas dois transceivers não podem estar a mais de 2,5 km de distância um do outro e nenhum caminho entre dois transceivers pode atravessar mais de quatro repetidores.

7.8.1 Baluns e Adaptadores

A norma ANSI/EIA/TIA-568-A esclarece que o cabeamento da área de trabalho pode variar bastante em função das necessidades das aplicações de redes.

Normalmente utiliza-se um cabo com conectores idênticos em ambas as extremidades.

Entretanto existem aplicações de rede que exigem um adaptador específico, o qual deverá estar sempre na parte externa da tomada (também conhecida como jack) da área de serviço, de maneira a não comprometer a flexibilidade futura daquele ponto.

São compreendidos três tipos de adaptadores: os adaptadores para conectividade (ex: Telco/RJ-45, acopladores e divisores), os adaptadores passivos (Baluns) e os adaptadores ativos.

Historicamente os baluns surgiram como dispositivos utilizados para permitir que aplicações de dados IBM, que rodavam normalmente sobre sistemas com cabos coaxiais, pudessem ser transmitidas sobre o meio físico UTP.

O nome balun origina-se das diferenças entre os modos de transmissão utilizados em sistemas coaxiais (Não Balanceado) e em sistemas UTP (Balanceado) - BALUN = BALanced + Unbalanced.

Existe uma enorme gama de Baluns que suportam uma variedade de aplicações específicas.

Muitas vezes a presença de um conector BNC de um lado do cabo e um RJ-45 do outro pode levar ao entendimento que este Balun serve para todas as aplicações que contenham esta combinação de interfaces de conexão.

Esta visão está errada, pois muitas vezes os Baluns possuem requisitos elétricos específicos para uma certa aplicação, com limitações específicas de distâncias que às vezes não são apropriadas para as demais aplicações aparentemente possíveis.

Normalmente em cada link são utilizados números pares de Baluns, sendo instalada uma peça externamente à tomada na área de trabalho e uma peça no armário de telecomunicações ou na sala de equipamentos.

Figura 7 - Exemplos de Baluns e Adaptadores

7.8.2 Conversores de Mídia

A finalidade do conversor de mídia é receber os sinais de um tipo de conector e convertê-lo para serem usados em outro tipo de conector.

Quando uma placa de interface de rede utiliza um conector diferente do que já está conectado à mídia de transmissão, usa-se um adaptador de mídia de transmissão.

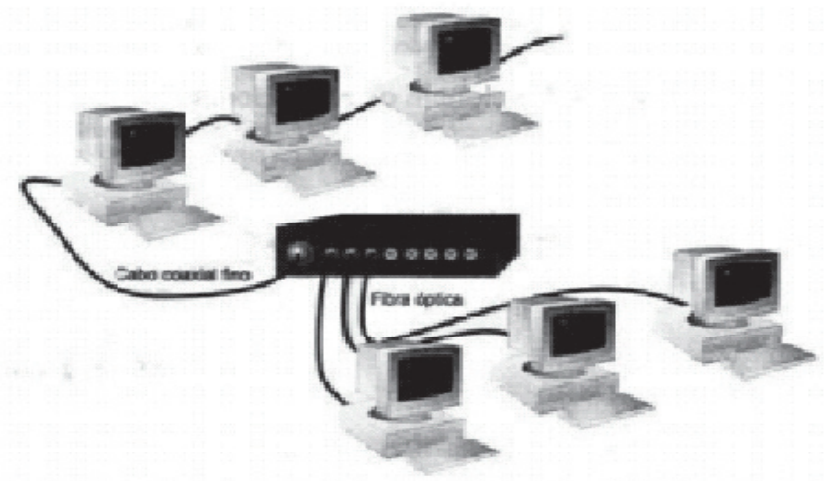


Figura 8 - Emprego de conversor de mídia

7.9 Modems

O Modem é um dispositivo conversor de sinais que faz a comunicação entre computadores através de uma linha telefônica. Seu nome é a contração das palavras MOdulador e DEModulador.

O Modem executa uma transformação, por modulação (modem analógico) ou por codificação (modem digital), dos sinais emitidos pelo computador, gerando sinais analógicos adequados à transmissão sobre uma linha telefônica.

No destino, um equipamento igual a este demodula (modem analógico) ou decodifica (modem digital) a informação, entregando o sinal digital restaurado ao equipamento terminal a ele associado.

Os padrões de modems definem questões de compatibilidade tais como velocidade de transmissão e controle de erros.

Estes padrões são definidos pelo ITU - International Telegraph Union.

Figura 9 - Aplicação do modem na interligação de redes

7.10 Multiplexadores

São dispositivos usados para permitir que uma única linha de comunicação seja comutada (compartilhada) por mais de um computador. Isso pode ocorrer porque algumas linhas podem ficar inativas por longos períodos de tempos, com nenhum ou pouquíssimo fluxo de dados entre o terminal e o computador.

Se os períodos ativos das várias linhas nunca coincidirem, uma única linha pode ser comutada para atender a vários terminais.

Se não for possível assegurar que somente um terminal esteja ativo num dado instante de tempo, é preciso proporcionar uma linha saindo do comutador com uma capacidade maior do que qualquer outra linha de entrada.

Se a capacidade da linha de saída excede a soma das capacidades de todas as linhas de entrada, o comutador executa a função de multiplexador.

A multiplexação pode ser efetivada dividindo-se a banda de freqüência do canal de maior velocidade em várias bandas mais estreitas e alocando cada uma delas para cada um dos terminais.

Essa forma de multiplexação é conhecida como FDM

– Frequency Division Multiplexing.

Uma forma mais sofisticada consiste em amostrar cada linha oriunda de um terminal, seqüencialmente, enviando o sinal recebido por um canal de alta velocidade.

Essa forma é conhecida como TDM - Time Division Multiplexing. No caso anterior, a velocidade de transmissão oriunda de cada terminal não pode exceder a capacidade do canal que lhe foi alocado.

Ocasionalmente, pode-se usar uma mídia de transmissão que proporciona maior capacidade do que um único sinal pode ocupar.

Para usar eficientemente toda a banda passante da mídia de transmissão, deve-se instalar multiplexadores.

Um multiplexador combina dois ou mais sinais separados num único segmento de mídia de transmissão.

7.11 Estabilizadores e No-breaks

7.11.1 Estabilizadores

O estabilizador é utilizado com a finalidade de possibilitar uma tensão de saída sempre estável, protegendo os equipamentos de variações de tensão da rede elétrica.

O estabilizador “regula” a tensão de entrada de maneira a evitar mudanças bruscas nos níveis elétricos (para mais ou para menos).

Os estabilizadores possuem um transformador com múltiplas saídas, sendo que cada saída apresenta um nível de tensão diferente.

Um circuito eletrônico interno chamado de comparador de tensão seleciona um ponto de saída diferente enquanto a tensão de entrada varia, mantendo a tensão de alimentação constante.

7.11.2 No-Breaks

O No-Break ou UPS (Uninterruptible Power Supply) tem a finalidade de proteger e manter os equipamentos eletrônicos alimentados quando ocorrerem falhas na rede de distribuição elétrica.

Assim, os usuários de redes de computadores podem salvar e fechar os arquivos e programas em utilização (o tempo de autonomia mais comum é de algo entre 10 e 15 minutos).

Alguns tipos permitem que o uso por algumas horas ininterruptas sem energia elétrica.

O No-Break possui uma ou varias baterias, que são utilizadas quando um circuito eletrônico identifica a interrupção de energia e começa a alimentar automaticamente o equipamento.

Esse circuito eletrônico executa duas funções através de uma Chave de Transferência interna ao No-Break: ligar as cargas na corrente elétrica quando essa corrente estiver em condições satisfatórias e conectar o conjunto de baterias as cargas quando o fornecimento de energia elétrica for interrompido ou no caso de alguma anormalidade.

No No-Break também existem um Inversor e um Retificador.

O Inversor é um circuito interno que transforma a tensão das baterias em tensão alternada.

Já o Retificador transforma a tensão alternada da rede elétrica em tensão continua, com finalidade de alimentar o inversor.

Também existe um sistema de proteção contra "pane" chamado de By Pass, que alimenta as cargas diretamente com energia elétrica.

7.11.2.1 Tipos de No-Breaks

Existem dois tipos básicos de No-Breaks: On-line e Off-line.

A diferença está na forma como a energia chega ao computador:

7.11.2.1.1 No-Break On-line

Possui forma de transmissão de energia elétrica alternada que entra no inversor, que transforma em energia elétrica continua para ser armazenada pela bateria e esta envia a sua carga para outro inversor que converte a energia elétrica para alternada novamente e será esta que irá alimentar o equipamento.

Assim, a bateria nunca ficará sem carga.

Quando houver falta de energia, a energia elétrica irá direto da bateria para o computador automaticamente.

Existem ainda dois tipos de no-breaks on-line: on-line em paralelo e on-line em série:

 No-Break on-line em paralelo - a bateria e a energia elétrica da entrada do no-break são ligadas simultaneamente à saída do equipamento.

Como a bateria está sempre ligada na saída do no-break, não há retardo em seu acionamento, entretanto, como a energia elétrica também está presente na saída, quaisquer problemas na rede elétrica (como variações de tensão e ruídos) são repassados para a saída do no-break.

 No-Break on line em série – nesse tipo, o equipamento é alimentado continuamente apenas pela bateria.

Quando falta energia elétrica, não há qualquer tipo de retardo.

A tensão elétrica presente na entrada do no-break é usada apenas para carregar a bateria, assim a saída do no-break fica totalmente isolada da entrada.

Com isso, qualquer problema na rede elétrica (variações, ruídos, etc) não afeta o equipamento conectado na saída.

7.11.2.1.2 No-Break Off-line

Os no-breaks off-line são os mais baratos e apresentam um retardo em seu acionamento.

A tensão elétrica é transmitida diretamente para as cargas, sem o condicionamento de energia.

Quando ocorre a falta tensão elétrica a chave de transferência é ligada e assim as baterias fornecem a energia através do inversor.

Quando a energia elétrica falha, o no-break demora um tempo (tipicamente 16 ms) para detectar que a falha e acionar a bateria. Embora esse retardo seja pequeno, pode afetar o funcionamento de equipamentos mais sensíveis.

Um tipo de no-break off-line muito comum é o line interactive.

Esse tipo de no-break oferece um retardo menor (tipicamente de 6ms) e traz um estabilizador de tensão embutido.

7.11.3 Filtros de Linha

O papel desse tipo de equipamento é filtrar ruídos da rede elétrica, especialmente os gerados por motores, tais como de condicionadores de ar, aquecedores, etc.

O componente eletrônico do filtro responsável pela filtragem chama-se varistor, e está presente tanto nas fontes de alimentação dos equipamentos eletrônicos, quanto dentro dos estabilizadores de tensão.

Isso significa que os filtros de linha aplicam-se basicamente para aumentar o número de tomadas disponíveis para ligar os equipamentos ao estabilizador.

7.12 Resumo

Relação entre os níveis do modelo OSI e os equipamentos apresentados:

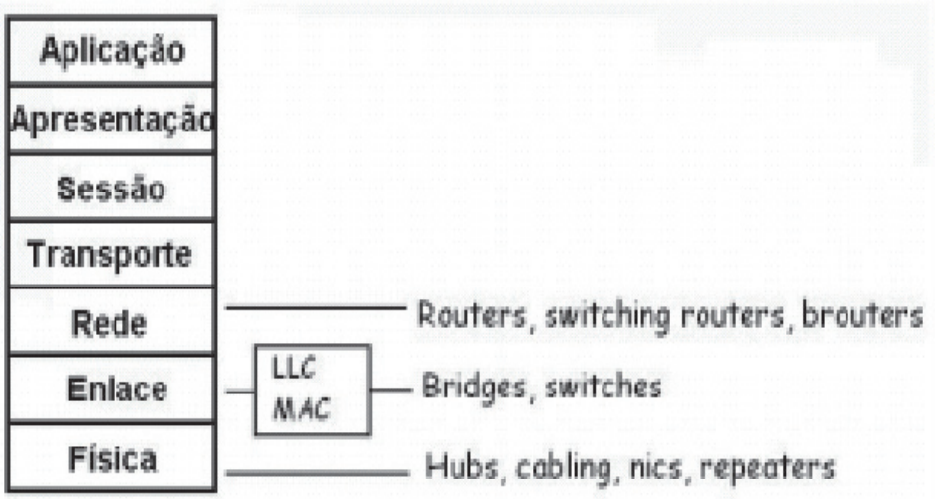


Figura 10 - Elementos de redes x Modelo OSI

8 PROTOCOLOS TCP/IP

8.1 Arquitetura Internet

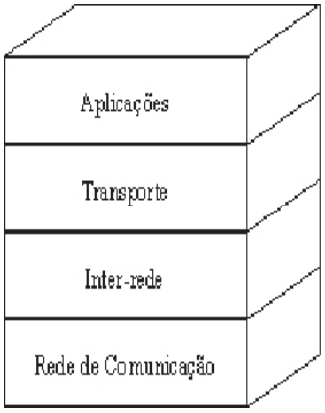
A arquitetura internet se baseia praticamente em um **serviço de rede não orientado à conexão** (datagrama não confiável), o **Internet Protocol (IP)** e em um **serviço de transporte orientado à conexão**, oferecido pelo **Transmission Control Protocol (TCP)**.

Juntos, estes protocolos se completam, oferecendo um serviço confiável de uma forma simples e eficiente.

A arquitetura internet se baseia em um modelo com quatro camadas (figura a seguir), onde cada uma executa um conjunto bem definido de funções de comunicação.

No modelo em camadas da internet, não existe uma estruturação formal para cada camada, conforme ocorre no modelo OSI.

Ela procura definir um protocolo próprio para cada camada, assim como a interface de comunicação entre duas camadas adjacentes.



Modelo em Camadas da Internet

Camada de Rede de Comunicação

Na camada de rede de comunicação da internet, não existe um padrão para a sub-rede de acesso, possibilitando a conexão de qualquer tipo de rede, desde que haja uma interface que compatibilize a tecnologia da rede com o protocolo IP.

Desta forma, um número muito grande de tecnologias pode ser utilizado na sub-rede de acesso, como Ethernet, Token Ring, FDDI, X.25, Frame Relay, ATM, etc.

Para que todas estas tecnologias possam ser "vistas" pela rede internet, existe a necessidade de uma conversão de endereçamentos do formato utilizado pela sub-rede e o formato IP.

Esta conversão é realizada pelos gateways, que tornam a interconexão das redes transparente para o usuário (fig. abaixo).

Além das conversões de protocolos, os gateways são responsáveis pela função de roteamento das informações entre as sub-redes.

Interconexão de Sub-Redes à Rede Internet

Camada de Inter-Rede

A camada de Inter-Rede, também chamada de Internet, é equivalente à camada de rede do modelo OSI.

Nela são especificados vários protocolos, dentre os quais se destaca o IP (Internet Protocol).

O IP é um protocolo não orientado a conexão, cuja função é transferir blocos de dados denominados datagramas da origem até o destino, podendo passar inclusive por várias sub-redes (a origem e o destino são hosts identificados por endereços IP).

A operação no modo datagrama é uma comunicação não confiável, não sendo usado nenhum reconhecimento fim a fim ou entre nós intermediários, nem qualquer tipo de controle de fluxo.

Nenhum mecanismo de controle de erro de dados é utilizado, apenas um controle de verificação do cabeçalho, para garantir que os gateways encaminhem as mensagens corretamente.

Algumas das principais características do protocolo IP são as

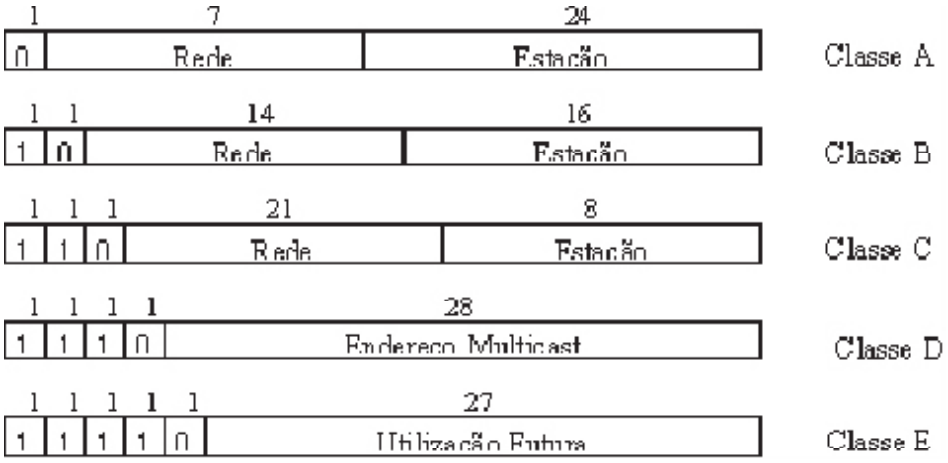
seguintes:

- Serviço de datagrama não confiável;
- Endereçamento hierárquico;
- Facilidade de fragmentação e remontagem de pacotes;
- Campo especial indicando qual o protocolo de transporte a ser utilizado no nível superior;
- Identificação da importância do datagrama e do nível de confiabilidade exigido;
- Descarte e controle de tempo de vida dos pacotes inter-redes

no gateway.

8.2 Endereçamento IP

O roteamento dos datagramas através das sub-redes são feitos baseados no seu endereço IP, números de 32 bits normalmente escritos como quatro octetos (em decimal), por exemplo 9.179.12.66. Devido ao fato de existirem redes dos mais variados tamanhos compondo a inter-rede, utiliza-se o conceito de classes de endereçamento:



Formato dos Endereços IP

Os endereços IP indicam o número da rede e o número do host, sendo que a classe A suporta até 127 redes com 16 milhões de hosts cada uma, a classe B 16384 redes com até 64 mil hosts cada uma, a classe C 2 milhões de redes com até 256 hosts cada uma e a classe D, onde um datagrama é dirigido a um grupo de hosts.

Os endereços a partir de 1111 estão reservados para uso futuro.

A Internet utiliza a classe C para endereçamento de suas redes e máquinas.

Quando um novo provedor de acesso se conecta à ela, ele recebe 256 endereços para serem utilizados pelos seus hosts (ou “usuários”).

Como um provedor pode ter mais de 256 clientes, ele utiliza um esquema de alocação dinâmica de IP, ou seja, quando o usuário se conecta ao provedor de acesso, ele recebe um endereço IP, podendo desta forma haver até 256 usuários conectados simultaneamente a um provedor de acesso.

8.2.1 Formato do Datagrama IP

O protocolo IP recebe da camada de transporte mensagens

divididas em datagramas de 64 kbytes cada um, sendo que cada um destes é transmitido através da Internet, sendo ainda possivelmente fragmentados em unidades menores à medida em que passam por sub-redes.

Ao chegarem ao seu destino, são remontados novamente pela camada de transporte, de forma a reconstituir a mensagem original.

8.2.1.1 Fragmentação e Remontagem de Datagramas

Como os datagramas IP atravessam redes das mais diversas tecnologias, os tamanhos dos quadros nem sempre devem ser os mesmos.

Portanto deve haver uma certa flexibilidade em termos de tamanho de pacote a ser transmitido, de forma a este pacote se adaptar à sub-rede que vai atravessar.

Esta flexibilidade se dá através da facilidade de fragmentação e remontagem de datagramas.

Quando for necessário transmitir um datagrama maior do que o suportável pela rede, deve-se particionar o pacote em fragmentos. Estes fragmentos são transportados como se fossem datagramas independentes. Para poder recompor o datagrama original no destino, são utilizados alguns campos do cabeçalho do datagrama. Quando o destino recebe o primeiro fragmento, inicia-se uma temporização para se aguardar o conjunto completo dos fragmentos que compõem o datagrama. Caso um dos fragmentos não chegue durante este intervalo, o datagrama é descartado, acarretando em uma perda de eficiência.

8.3 Camada de Transporte

A camada de transporte tem o objetivo de prover uma comunicação confiável entre dois processos, estando eles

ocorrendo dentro da mesma rede ou não.

Ela deve garantir que os dados sejam entregues livres de erros, em seqüência e sem perdas ou duplicação.

A Arquitetura Internet especifica dois tipos de protocolos na camada de transporte:

- o UDP (User Datagram Protocol) e o

- TCP (Transmission Control Protocol).

O UDP é um protocolo não orientado à conexão que pode ser considerado como uma extensão do protocolo IP, e não oferece nenhuma garantia em relação à entrega dos dados ao destino.

Já o protocolo TCP oferece aos seus usuários um serviço de transferência confiável de dados, através da implementação

de mecanismos de recuperação de dados perdidos, danificados ou recebidos fora de seqüência, minimizando o atraso na sua transmissão.

A cada fragmento transmitido é incorporado um número de seqüência, de forma a não se perder a ordem dos segmentos a serem juntados para formar o datagrama.

Existe um mecanismo de reconhecimento para executar essa função que funciona da seguinte forma: o reconhecimento transmitido pelo receptor ao receber o segmento X é o número do próximo segmento que o receptor espera receber (X+1), indicando que já recebeu todos os segmentos anteriores a este.

Através da análise dos números de segmento, o receptor pode ordenar os segmentos que chegaram fora de ordem e eliminar os segmentos duplicados.

Com base no checksum que é adicionado a cada segmento transmitido, os erros de transmissão são tratados e os segmentos danificados são descartados.

Existe ainda um controle de fluxo baseado no envio da capacidade de recebimento do receptor, contado a partir do último byte recebido, ao transmissor.

Desta forma o transmissor consegue controlar a quantidade de dados que são enviados ao receptor para não haver descarte de segmentos nem necessidade de retransmissão, que ocasionam a queda do desempenho da rede.

Para permitir que vários usuários (processos de aplicação)

possam utilizar simultaneamente os serviços do protocolo TCP,

foi criado o conceito de porta.

Para não haver problemas de identificação de usuários, o identificador da porta é associado ao endereço IP onde a entidade TCP está sendo realizada, definindo assim um socket.

A associação de portas a processos de aplicação (usuários) é tratada de forma independente por cada entidade TCP.

No entanto, processos servidores que são muito utilizados, como FTP, Telnet, etc, são associados a portas fixas, divulgadas aos usuários.

Uma conexão é identificada pelo par de sockets ligados em suas extremidades.

Um socket local pode participar de várias conexões diferentes com sockets remotos.

Uma conexão pode ser utilizada para transportar dados em

ambas as direções simultaneamente, ou seja, as conexões TCP

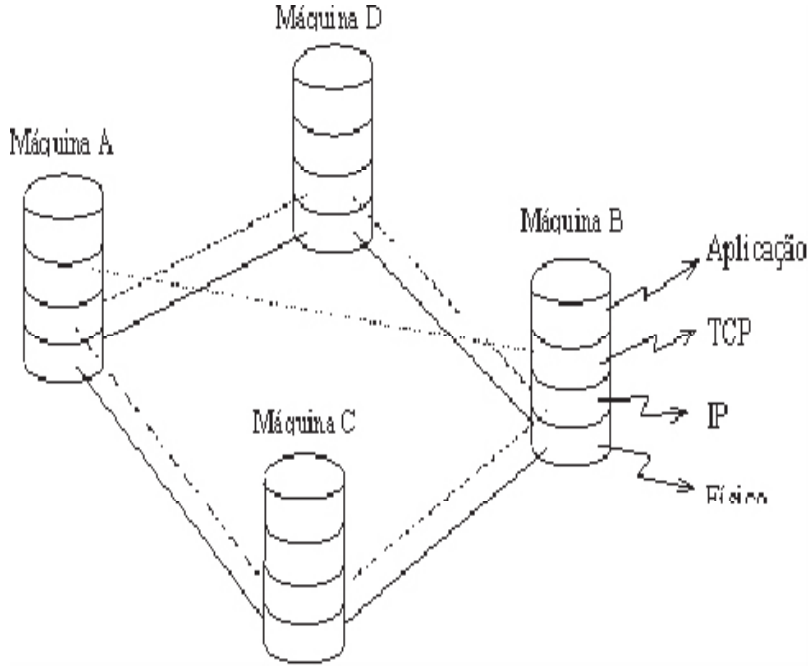
são full-duplex.

É importante observar aqui que quando se fala que o TCP é

orientado à conexão, não se fala em conexão a nível físico,

mas sim a nível lógico.

Este conceito pode ser compreendido através da figura abaixo.



Serviços orientados e não orientados à conexão

No caso da figura anterior, a máquina A quer se comunicar com

a máquina B através de uma rede em anel utilizando TCP/IP.

A única conexão física que existe entre A e B é através do anel,

passando pelas máquinas C e D.

A nível de IP, a comunicação não é orientada à conexão, portanto é muito simples enxergar que os dados possuem apenas dois caminhos para ir de A até B: através de C ou através de D.

A nível de TCP, porém, a comunicação entre os computadores A e B ocorre como se houvesse uma conexão direta entre eles.

Isso implica que, se a nível de IP os dados podem chegar fora de ordem, o TCP tem que garantir a ordenação destes dados, de forma que eles sempre chegem na ordem correta, como aconteceria se houvesse uma conexão física direta entre A e B.

8.3.1 O Protocolo TCP – RFC793

Entidades TCP trocam dados na forma de segmentos, que consiste num cabeçalho de 20 bytes (fixo) mais uma parte opcional, seguido de zero ou mais bytes de dados.

O software TCP decide qual deve ser o tamanho dos segmentos, limitado de duas formas:

- Tamanho máximo do segmento, de 65.535 bytes, menos os cabeçalhos TCP e IP.
- Tamanho da MTU (Maximum Transfer Unit) da rede.

Se o segmento passar por uma rede com MTU menor, deve ser fragmentado, recebendo um novo cabeçalho TCP e IP (40 bytes a mais).

Originalmente, a ARPANET assumia que o nível de subnet oferecia um serviço totalmente confiável de transmissão

de dados.

Dessa forma, o primeiro protocolo de nível de transporte era bastante simples, e ficou conhecido como NCP (Network Control Protocol), sendo satisfatório para o ambiente inicial da ARPANET.

À medida que o tempo foi passando, a ARPANET cresceu e começou a incluir na sua estrutura muitas redes locais, algumas subredes baseadas em rádio, e também muitos canais via satélite, fazendo com que a confiabilidade entre a máquina fonte e máquina destino fosse diminuída.

Isso forçou a criação de um novo protocolo de nível de transporte, que ficou conhecido como TCP (Transfer Control Protocol), e foi especificamente desenvolvido para tolerar uma subrede não confiável.

TCP é um protocolo de nível de transporte orientado à conexão, portanto, oferece uma comunicação confiável entre máquina fonte e destino, além de controle de fluxo e recuperação de erros, permitindo uma transmissão de dados full-duplex.

O processo de usuário pode enviar mensagens de qualquer tamanho, e o TCP divide essa mensagem em blocos iguais ou menores que 64 Kbytes, enviando cada peça separadamente.

O nível de rede não oferece garantias que os pedaços vão ser entregues na mesma seqüência que foram transmitidos, portanto, o TCP deve prever uma forma de remontar os pedaços em ordem.

Caso uma mensagem seja perdida, o TCP deve prever mecanismos de time-out para retransmitir o pedaço perdido.

8.3.1.1 Three Way Handshake (RFC 793)

1) **A --> B SYN** my sequence number is **X**

2) **A <-- B ACK** your sequence number is **X**

3) **A <-- B SYN** my sequence number is **Y**

4) **A --> B ACK** your sequence number is **Y**

Como os passos 2 e 3 podem ser feitos juntos, o reconhecimento é feito em três etapas.

Ele é necessário pois cada entidade pode ter um número de seqüência diferente, e os dois devem saber qual o número do outro.

8.3.1.2 Timeout no TCP

É adaptativo, ou seja, o host tenta estabelecer a conexão (SYN no IP e porta destino).

Se não obtiver resposta (SYN ACK) em 3s, tenta 2a vez, aumentando timeout para 6s.

Se não vier, dobra timeout (12s), tentando 3a vez.

Se não vier resposta, tenta novamente.

Se não vier resposta, dá erro dizendo que conexão falhou.

Durante a conexão é similar, se adaptando ao tempo que a resposta está demorando para chegar.

UDP - User Datagram Protocol – RFC 768

O UDP é um protocolo de nível de transporte orientado à transmissão de mensagens sem o estabelecimento de uma conexão entre máquina fonte e destino, fornecendo uma comunicação menos confiável que o TCP.

Ele envia as mensagens (sem conexão) e não oferece nenhuma garantia de entrega ou seqüência.

O formato do cabeçalho do UDP é mostrado na figura a seguir.

Source Port (16 bits)	Destination Port (16 bits)
Length (16 bits)	Checksum (16 bits)

O campo length dá o tamanho do cabeçalho mais o campo de dados.

O campo de checksum também é para o cabeçalho mais dados.

Exemplos de usos do UDP

- Protocolo TFTP (Trivial FTP) - /* link para servidor de TFTP */

-Transmissão de voz e vídeo pela rede

-Transmissão em multicast (normalmente é não confiável, apesar de existirem protocolos multicast confiáveis).

-Mensagens SNMP.

Vamos ver então o que aprendemos até então:

O TCP/IP, na verdade, é formado por um grande conjunto de diferentes protocolos e serviços de rede.

O nome TCP/IP deriva dos dois protocolos mais comumente utilizados:

IP: É um protocolo de endereçamento, um protocolo de rede.

Podemos afirmar que as principais funções do protocolo IP são endereçamento e roteamento, ou de uma maneira mais simples, fornecer uma maneira para identificar unicamente cada máquina da rede (endereço IP) e uma maneira de encontrar um caminho entre a origem e o destino (Roteamento).

TCP: O TCP é um protocolo de transporte e executa importantes funções para garantir que os dados sejam entregues de uma maneira confiável, ou seja, sem que os dados sejam corrompidos.

Vamos imaginar uma situação prática, onde você deseja enviar um arquivo com cerca de 10 MB de um computador de origem para um computador de destino.

Uma das primeiras coisas que tem que ser feitas é encontrar uma rota, um caminho entre a origem e o destino.

Este é o papel do protocolo IP, mais especificamente da função de roteamento.

Uma vez encontrado o caminho, o próximo passo é dividir o arquivo de 10 MB em pacotes de tamanhos menores, os quais possam ser enviados pelos equipamentos de rede.

Além da divisão em pacotes menores, o TCP tem que garantir que os pacotes sejam entregues sem erros e sem alterações.

Pode também acontecer de os pacotes chegarem fora de ordem.

O TCP tem que ser capaz de identificar a ordem correta e entregar os pacotes para o programa de destino, na ordem correta.

Por exemplo, pode acontecer de o pacote número 10 chegar antes do pacote número 9.

Neste caso o TCP tem que aguardar a chegada do pacote número 9 e entregá-los na ordem correta.

Pode também acontecer de serem perdidos pacotes durante o transporte.

Neste caso, o TCP tem que informar à origem de que determinado pacote não foi recebido no tempo esperado e solicitar que este seja retransmitido.

Todas estas funções – garantir a integridade, a seqüência correta e solicitar retransmissão – são exercidas pelo protocolo TCP – Transmission Control Protocol.

Além do TCP existe também o UDP, o qual não faz todas estas verificações e é utilizado por determinados serviços.

A seguir apresento uma descrição dos protocolos TCP e UDP e um estudo comparativo.

8.3.2 TCP – Uma Visão Geral

O Transmission Control Protocol (TCP) é, sem dúvidas, um dos mais importantes protocolos da família TCP/IP.

É um padrão definido na RFC 793, “Transmission Control Protocol (TCP)”, que fornece um serviço de entrega de pacotes confiável e orientado por conexão.

Ser orientado por conexão, significa que todos os aplicativos baseados em TCP como protocolo de transporte, antes de iniciar a troca de dados, precisam estabelecer uma conexão.

Na conexão são fornecidas, normalmente, informações de logon, as quais identificam o usuário que está tentando estabelecer uma conexão.

Um exemplo típico são os aplicativos de FTP (Cute – FTP, ES-FTP e assim por diante).

Para que você acesse um servidor de FTP, você deve fornecer um nome de usuário e senha.

Estes dados são utilizados para identificar e autenticar o usuário.

Após a identificação e autenticação, será estabelecida uma sessão entre o cliente de FTP e o servidor de FTP.

Algumas características do TCP:

· Garante a entrega de datagramas IP: Esta talvez seja a principal função do TCP, ou seja, garantir que os pacotes sejam entregues sem alterações, sem terem sido corrompidos e na ordem certa.

O TCP tem uma série de mecanismos para garantir esta entrega.

· Executa a segmentação e reagrupamento de grandes blocos de dados enviados pelos programas e Garante a seqüencialização adequada e entrega ordenada de dados segmentados: Esta característica refere-se a função de dividir

grandes arquivos em pacotes menores e transmitir cada pacote separadamente.

Os pacotes podem ser enviados por caminhos diferentes e chegar fora de ordem.

O TCP tem mecanismos para garantir que, no destino, os pacotes sejam ordenados corretamente, antes de serem entregues ao programa de destino.

Verifica a integridade dos dados transmitidos usando cálculos de soma de verificação: O TCP faz verificações para garantir que os dados não foram alterados ou corrompidos durante o transporte entre a origem e o destino.

· Envia mensagens positivas dependendo do recebimento bem-sucedido dos dados.

Ao usar confirmações seletivas, também são enviadas confirmações negativas para os dados que não foram recebidos: No destino, o TCP recebe os pacotes, verifica se estão OK e, em caso afirmativo, envia uma mensagem para a origem, confirmando cada pacote que foi recebido corretamente.

Caso um pacote não tenha sido recebido ou tenha sido recebido com problemas, o TCP envia uma mensagem ao computador de origem, solicitando uma retransmissão do pacote.

Com esse mecanismo, apenas pacotes com problemas terão que ser enviados, o que reduz o tráfego na rede e agiliza o envio dos pacotes.

· Oferece um método preferencial de transporte de programas que devem usar transmissão confiável de dados baseada em sessões, como bancos de dados cliente/servidor e programas de correio eletrônico: Ou seja, o TCP é muito mais confiável do que o UDP (conforme mostrarei mais adiante) e é indicado para programas e serviços que dependam de uma entrega confiável de dados.

Como o TCP funciona

O TCP baseia-se na comunicação ponto a ponto entre dois hosts de rede.

O TCP recebe os dados de programas e processa esses dados como um fluxo de bytes.

Os bytes são agrupados em segmentos que o TCP numera e seqüência para entrega.

Estes segmentos são mais conhecidos como “Pacotes”.

Antes que dois hosts TCP possam trocar dados, devem primeiro estabelecer uma sessão entre si.

Uma sessão TCP é inicializada através de um processo conhecido como um Tree-Way Handshake (algo como Um Aperto de Mão Triplo).

Esse processo sincroniza os números de seqüência e oferece informações de controle necessárias para estabelecer uma conexão virtual entre os dois hosts.

De uma maneira simplificada, o processo de Tree-Way Handshake, pode ser descrito através dos seguintes passos:

· O computador de origem solicita o estabelecimento de uma sessão com o computador de destino: Por exemplo, você utiliza um programa de FTP (origem) para estabelecer uma sessão com um servidor de FTP (destino).

· O computador de destino recebe a requisição, verifica as credenciais enviadas (tais como as informações de logon) e envia de volta para o cliente, informações que serão utilizadas pelo cliente, para estabelecer efetivamente a sessão.

As informações enviadas nesta etapa são importantes, pois é através destas informações que o servidor irá identificar o cliente e liberar ou não o acesso.

· O computador de origem recebe as informações de confirmação enviadas pelo servidor e envia estas confirmações de volta ao servidor.

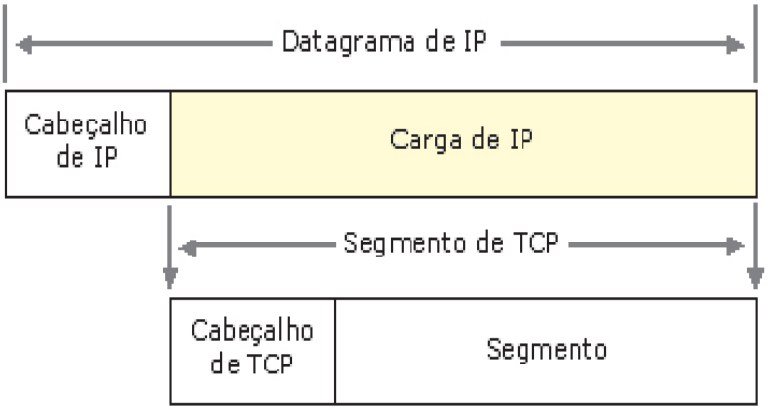
O servidor recebe as informações, verifica que elas estão corretas e estabelece a sessão.

A partir deste momento, origem e destino estão autenticados e aptos a trocar informações usando o protocolo TCP.

Se por algum motivo, as informações enviadas pela origem não estiverem corretas, a sessão não será estabelecida e uma mensagem de erro será enviada de volta ao computador de origem.

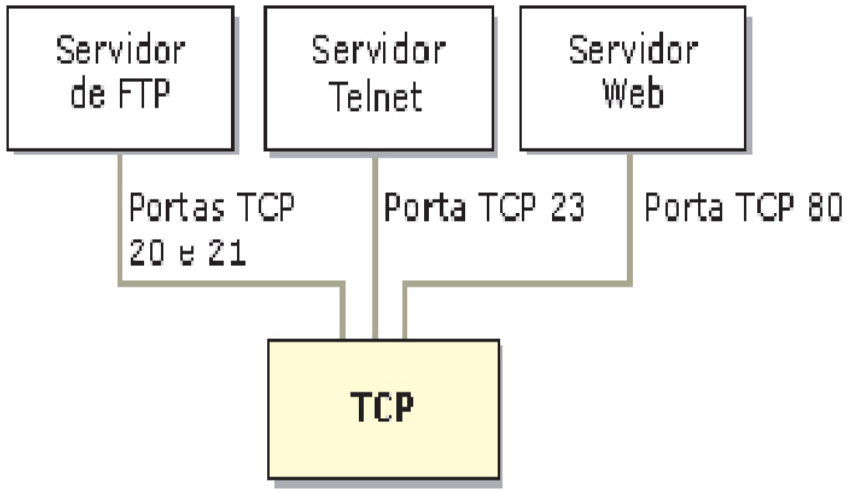
Depois de concluído o Tree-Way Handshake inicial, os segmentos são enviados e confirmados de forma seqüencial entre os hosts remetente e destinatário.

Um processo de handshake semelhante é usado pelo TCP antes de fechar a conexão para verificar se os dois hosts acabaram de enviar e receber todos os dados.
Os segmentos TCP são encapsulados e enviados em datagramas IP, conforme apresentado na figura a seguir:



7.3.3.2.1 O conceito de Portas TCP

Os programas TCP usam números de porta reservados ou conhecidos, conforme apresentado na seguinte ilustração:



Mas o que você pode estar se perguntando é: O que é uma Porta TCP?

Bem, sem entrar em detalhes técnicos do TCP/IP, vamos explicar, através de um exemplo prático, o conceito de porta.

Vamos imaginar um usuário, utilizando um computador com conexão à Internet.

Este usuário, pode, ao mesmo tempo, acessar um ou mais sites da Internet, usar o Outlook Express para ler suas mensagens de email, estar conectado a um servidor de FTP, usando um programa como o WS-FTP, para fazer download de um ou mais arquivos, estar jogando DOOM através da Internet.

Todas as informações que este usuário recebe estão chegando através de pacotes que chegam até a placa de Modem ou até o Modem ADSL, no caso de uma conexão rápida.

A pergunta que naturalmente surge é:

Como o sistema sabe para qual dos programas se destina cada um dos pacotes que estão chegando no computador?

Por exemplo, chega um determinado pacote.

É para uma das janelas do Navegador, é para o cliente de FTP, é um comando do DOOM, é referente a uma mensagem de E-mail ou quem é o destinatário deste pacote?

A resposta para esta questão é o mecanismo de portas utilizado pelo TCP/IP.

Cada programa trabalha com um protocolo/serviço específico, ao qual está associado um número de porta.

Por exemplo, o serviço de FTP, normalmente opera na porta 21 (na verdade usa duas portas, uma para controle e outra para o envio de dados).

Todo pacote que for enviado do servidor FTP para o cliente, terá, além dos dados que estão sendo enviados, uma série de dados de controle, tais como o número do pacote, código de validação dos dados e também o número da porta.

Quando o pacote chega no seu computador, o sistema lê no pacote o número da porta e sabe para quem encaminhar o pacote.

Por exemplo, se você está utilizando um cliente de FTP para fazer um download, os pacotes que chegarem, com informação de Porta = 21, serão encaminhados para o cliente de FTP, o qual irá ler o pacote e dar o destino apropriado.

Outro exemplo, o protocolo HTTP, utilizado para o transporte de informações de um servidor Web até o seu navegador, opera, por padrão, na porta 80.

Os pacotes que chegarem, destinados à porta 80, serão encaminhados para o navegador.

Se houver mais de uma janela do navegador aberta, cada uma acessando diferentes páginas, o sistema inclui informações, além da porta, capazes de identificar cada janela individualmente.

Com isso, quando chega um pacote para a porta 80, o sistema identifica para qual das janelas do navegador se destina o referido pacote.

Em resumo: O uso do conceito de portas, permite que vários programas estejam em funcionamento, ao mesmo tempo, no mesmo computador, trocando informações com um ou mais serviços/servidores.

O lado do servidor de cada programa que usa portas TCP escuta as mensagens que chegam no seu número de porta conhecido.

Todos os números de porta de servidor TCP menores que 1.024 (e alguns números mais altos) são reservados e registrados pela Internet Assigned Numbers Authority (IANA, autoridade de números atribuídos da Internet).

Por exemplo, o serviço HTTP (servidor Web), instalado em um servidor, fica sempre "escutando" os pacotes que chegam ao servidor.

Os pacotes destinados a porta 80, serão encaminhados pelo sistema operacional para processamento do servidor Web.

A tabela a seguir é uma lista parcial de algumas portas de servidor TCP conhecidas usadas por programas baseados em TCP padrão.

Nº da porta TCP	Descrição
20	Servidor FTP (File Transfer Protocol, protocolo de transferência de arquivo) (canal de dados).
21	Servidor FTP (canal de controle)
23	Servidor Telnet
53	Transferências de zona DNS (Domain Name System, sistema de nomes de domínios).
80	Servidor da Web (HTTP, Hypertext Transfer Protocol, protocolo de transferência de hipertexto).
139	Serviço de sessão NetBIOS

Para obter uma lista atualizada e completa de todas as portas TCP conhecidas e registradas atualmente, consulte o seguinte endereço: www.iana.org/assignments/port-numbers.

UDP – Uma Visão Geral

O User Datagram Protocol (UDP) é um padrão TCP/IP e está definido pela RFC 768, "User Datagram Protocol (UDP)".

O UDP é usado por alguns programas em vez de TCP para o transporte rápido de dados entre hosts TCP/IP.

Porém o UDP não fornece garantia de entrega e nem verificação de dados.

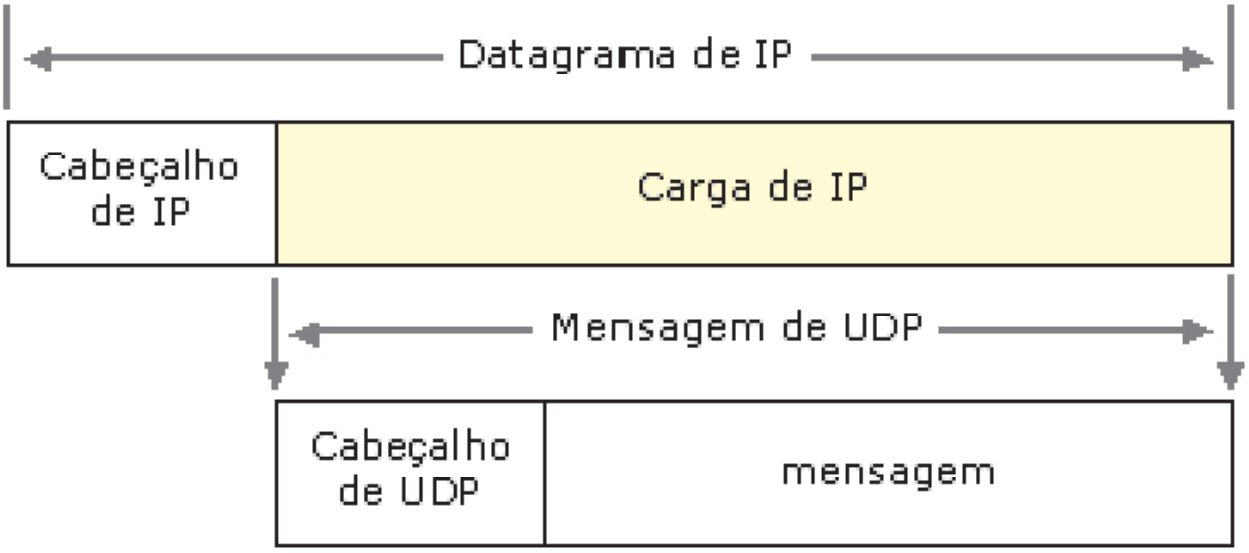
De uma maneira simples, dizemos que o protocolo UDP manda os dados para o destino; se vai chegar ou se vai chegar corretamente, sem erros, só Deus sabe.

Pode parecer estranho esta característica do UPD, porém você verá que em determinadas situações, o fato de o UDP ser muito mais rápido (por não fazer verificações e por não estabelecer sessões), o uso do UDP é recomendado.

O protocolo UDP fornece um serviço de pacotes sem conexão que oferece entrega com base no melhor esforço, ou seja, UDP não garante a entrega ou verifica a seqüência para qualquer pacote.

Um host de origem que precise de comunicação confiável deve usar TCP ou um programa que ofereça seus próprios serviços de seqüencialização e confirmação.

As mensagens UDP são encapsuladas e enviadas em datagramas IP, conforme apresentado na seguinte ilustração:



Portas UDP

O conceito de porta UDP é idêntico ao conceito de portas TCP, embora tecnicamente, existam diferenças na maneira como as portas são utilizadas em cada protocolo.

A idéia é a mesma, por exemplo, se um usuário estiver utilizando vários programas baseados em UDP, ao mesmo tempo, no seu computador, é através do uso de portas, que o sistema operacional sabe a qual programa se destina cada pacote UDP que chega.

O lado do servidor de cada programa que usa UDP escuta as mensagens que chegam no seu número de porta conhecido.

Todos os números de porta de servidor UDP menores que 1.024 (e alguns números mais altos) são reservados e registrados pela Internet Assigned Numbers Authority (IANA, autoridade de números atribuídos da Internet).

Cada porta de servidor UDP é identificada por um número de porta reservado ou conhecido.

A tabela a seguir mostra uma lista parcial de algumas portas de servidor UDP conhecidas usadas por programas baseados em UDP padrão.

Nº porta UDP	Descrição
53	Consultas de nomes DNS (Domain Name System, sistema de nomes de domínios).
69	Trivial File Transfer Protocol (TFTP)
137	Serviço de nomes NetBIOS
138	Serviço de datagrama NetBIOS
161	Simple Network Management Protocol (SNMP)
520	Routing Information Protocol (RIP, protocolo de informações de roteamento).

Para obter uma lista atualizada e completa de todas as portas TCP conhecidas e registradas atualmente, consulte o seguinte endereço: www.iana.org/assignments/port-numbers.

Comparando UDP e TCP:

Geralmente, as diferenças na maneira como UDP e TCP entregam os dados assemelham-se às diferenças entre um telefonema e um cartão postal.

O TCP funciona como um telefonema, verificando se o destino está disponível e pronto para a comunicação.

O UDP funciona como um cartão postal — as mensagens são pequenas e a entrega é provável, mas nem sempre garantida.

UDP é geralmente usado por programas que transmitem pequenas quantidades de dados ao mesmo tempo ou têm necessidades em tempo real.

Nessas situações, a baixa sobrecarga do UDP (pois este não faz as verificações que são feitas pela TCP) e as capacidades de broadcast do UDP (por exemplo, um datagrama, vários destinatários) são mais adequadas do que o TCP.

O UDP contrasta diretamente com os serviços e recursos oferecidos por TCP.

A tabela a seguir compara as diferenças em como a comunicação TCP/IP é tratada dependendo do uso de UDP ou TCP para o transporte de dados.

UDP	TCP
Serviço sem conexão; nenhuma sessão é estabelecida entre os hosts.	Serviço orientado por conexão; uma sessão é estabelecida entre os hosts.
UDP não garante ou confirma a entrega ou seqüência os dados.	TCP garante a entrega através do uso de confirmações e entrega seqüenciada dos dados.
Os programas que usam UDP são responsáveis por oferecer a confiabilidade necessária ao transporte de dados.	Os programas que usam TCP têm garantia de transporte confiável de dados.
UDP é rápido, necessita de baixa sobrecarga e pode oferecer suporte à comunicação ponto a ponto e ponto a vários pontos.	TCP é mais lento, necessita de maior sobrecarga e pode oferecer suporte apenas à comunicação ponto a ponto.

Tanto UDP quanto TCP usam portas para ntificar as comunicações para cada programa TCP/IP, conforme descrito anteriormente.