



Universidade Federal de Santa Catarina



Departamento de Informática e Estatística

Redes Locais - INE 5344

Prof. Mario Dantas
mario@inf.ufsc.br

Conteúdo Programático

I - Conceitos Básicos de Comunicação e Redes

II - Arquitetura de Redes de Computadores : RM-OSI, IEEE802 e TCP/IP.

Nível físico

Nível de enlace

Nível de rede

Nível de transporte

Nível de aplicação

Conteúdo Programático

III - Redes Locais :

- Token-ring,
- Ethernet,
- FastEthernet,
- GigabitEthernet.

IV - Redes de Alto Desempenho – Protocolos

V - Redes Sem Fio.

Referências Bibliográficas

- Livros Acadêmicos

1. *Tecnologias de Redes de Comunicação e Computadores*, Mario Dantas, Axcel-Books, 2002, ISBN 85-7323-169-6
2. - *Computer Networks*, Andrew Tanenbaum, Third Edition, Editora Prentice-Hall, 1996, ISBN 013-394-248-1
3. - *Redes de Computadores - Das LANs, MANs e WANs as Redes ATM*, Soares-Lemos-Colher, Editora Campus, 1995, ISBN 85-7001-954-8
4. - *Data Communication, Computer Networks and Open Systems*, Fourth Edition, Fred Halsall, Editora Addison Wesley, ISBN 0-901-42293-x

Referências Bibliográficas

- Livros Profissionais

1. - *Planning and Designing High Speed Networks using 100VGAnyLan*, J. F. Costa, Second Edition, Prentice Hall, 1995, ISBN 0-13-459092-x
2. - *Troubleshooting TCP/IP - Analyzing the Protocols of the Internet*, Mark. A. Miller, Prentice Hall, 1992, ISBN 0-13-9536167-x
3. - *Lan Troubleshooting Handbook*, Mark A. Miller, Second Edition, M&T Books, 1993, ISBN 1-55851-301-9.

Motivação

- O excelente custo/benefício dos computadores pessoais nos anos 80, geraram o ambiente ideal para compartilhamento da informação e recursos computacionais (computadores, impressoras, discos).

Motivação

Em adição, mainframes e mini-computadores ocupam seus espaços nas organizações (corporação e departamentos) e precisavam se *falar*.

Motivação

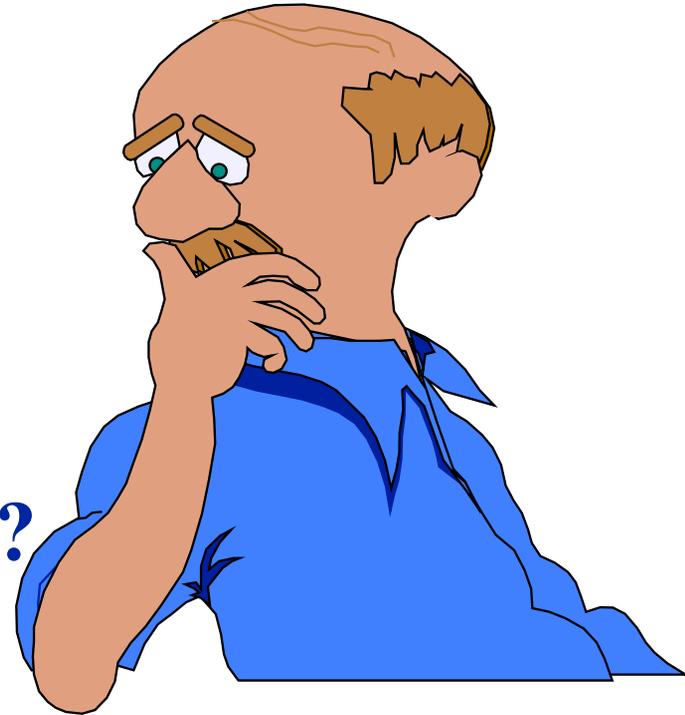
- Aumento da facilidade de acesso aos mais diversos recursos, de software e hardware, nos anos 90 através da *Internet* e a *explosão* da *WEB* consolidaram a direção da utilização das *redes de comunicação*.

Motivação

- Outros fatores modernos e importantes :
 - sistemas de navegação/controlado de carros;
 - palmtop computers;
 - relógios microcomputadores;
 - comunicação voz pela *Internet*;
 - quadros eletrônicos;
 - computadores usáveis.

Qual é a sua visão de rede?

- Interligação de terminais/computadores ?
- Interligação de micros ?
- Interligação de mainframes, PCs, Ws, minicomputadores ?

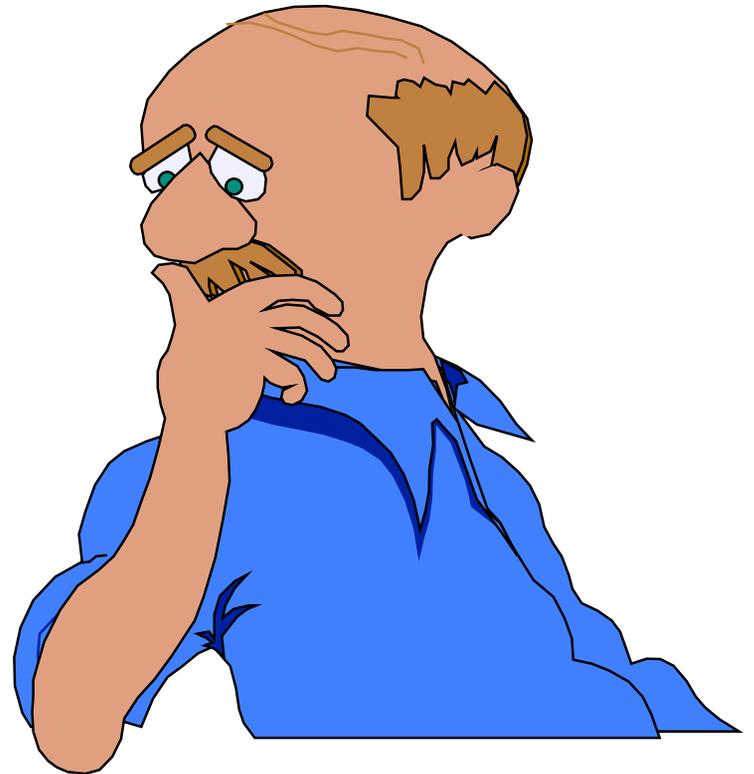


Qual é a sua visão de rede?

- **Interligação de aplicações (Web, Intranet e BDs) ?**
- **Interligação do sistema de telefonia a rede de computadores ?**
- **Interligação das redes de TVs a cabo, rede de telefonia e rede de computadores ?**



Qual é a sua visão ?



I – Conceitos Básicos de Comunicação e Redes

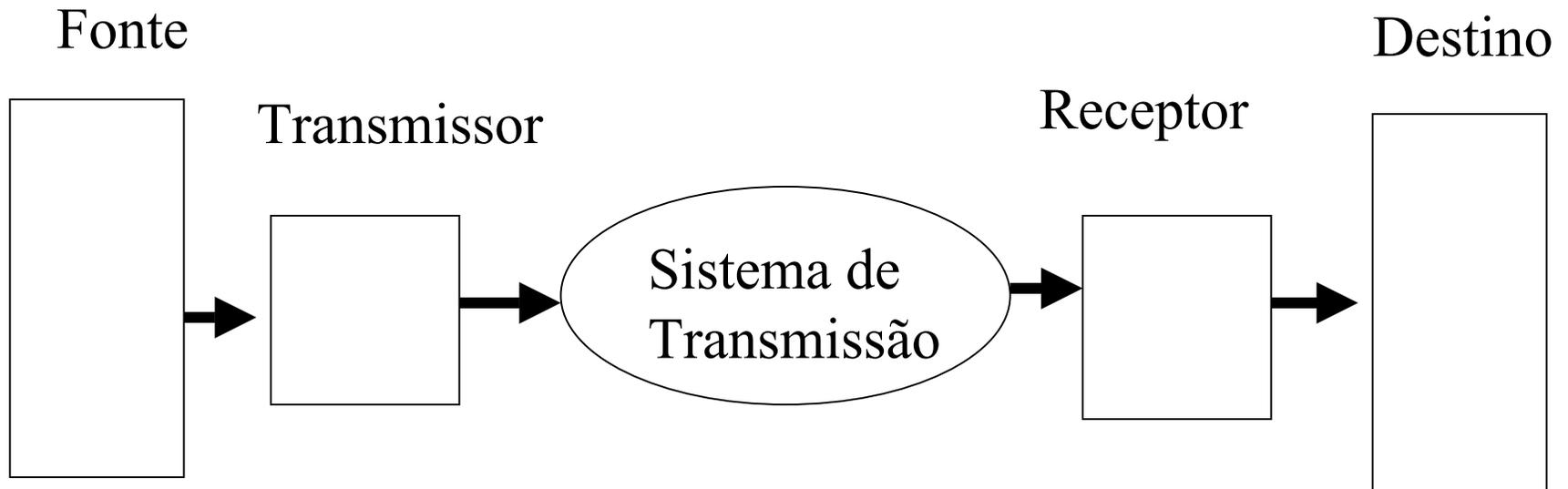
Objetivo

Vamos cobrir nesta unidade do curso, os conceitos básicos e terminologia das redes de comunicação, incluindo-se as redes de computadores.

Desta forma, estaremos aptos a uma discussão mais formal da operação e inter-funcionamento das redes e seus diversos níveis e funções nas próximas unidades.

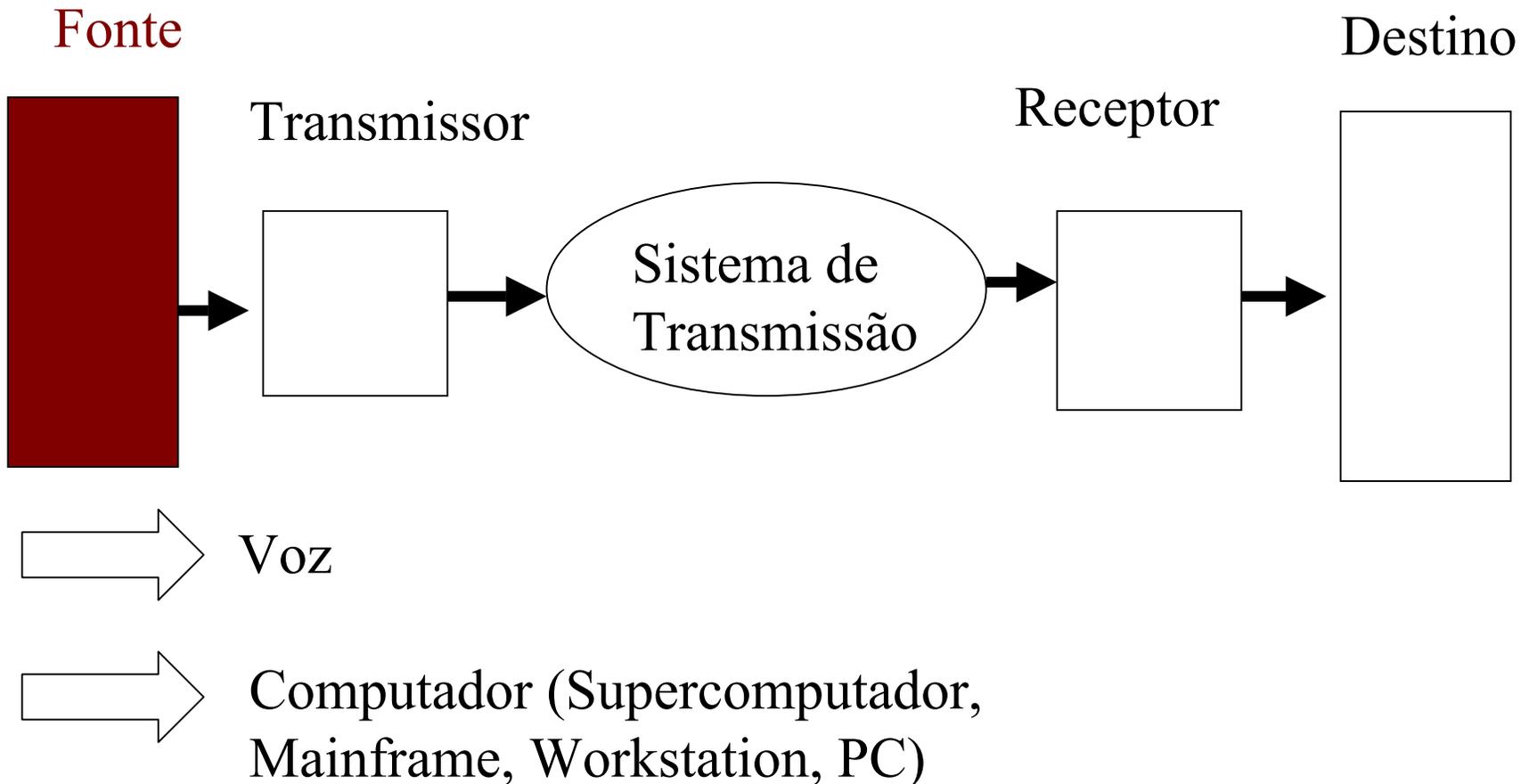
Conceitos de Comunicação

Modelo Genérico de Comunicação



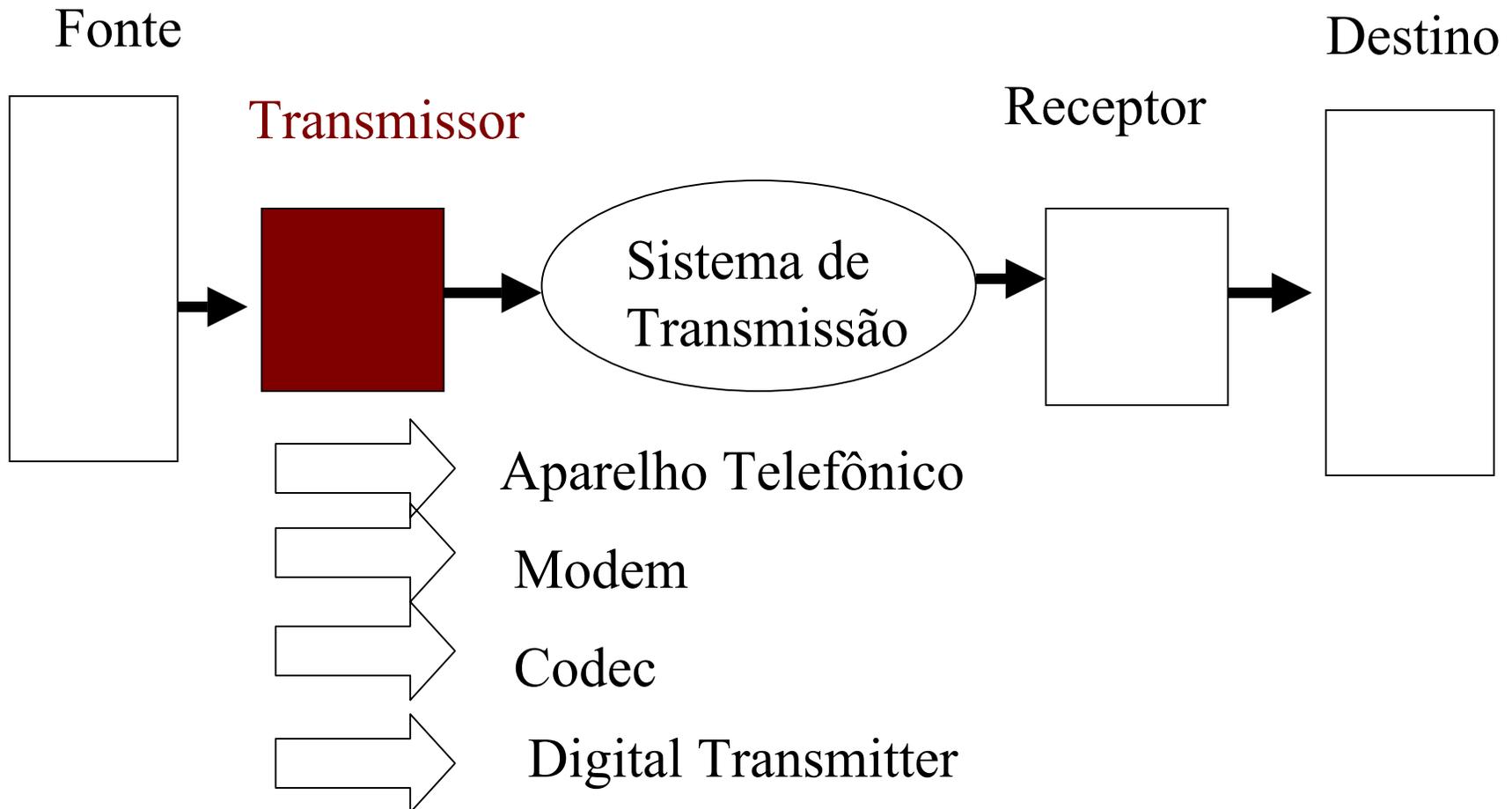
Conceitos de Comunicação

Modelo Genérico de Comunicação



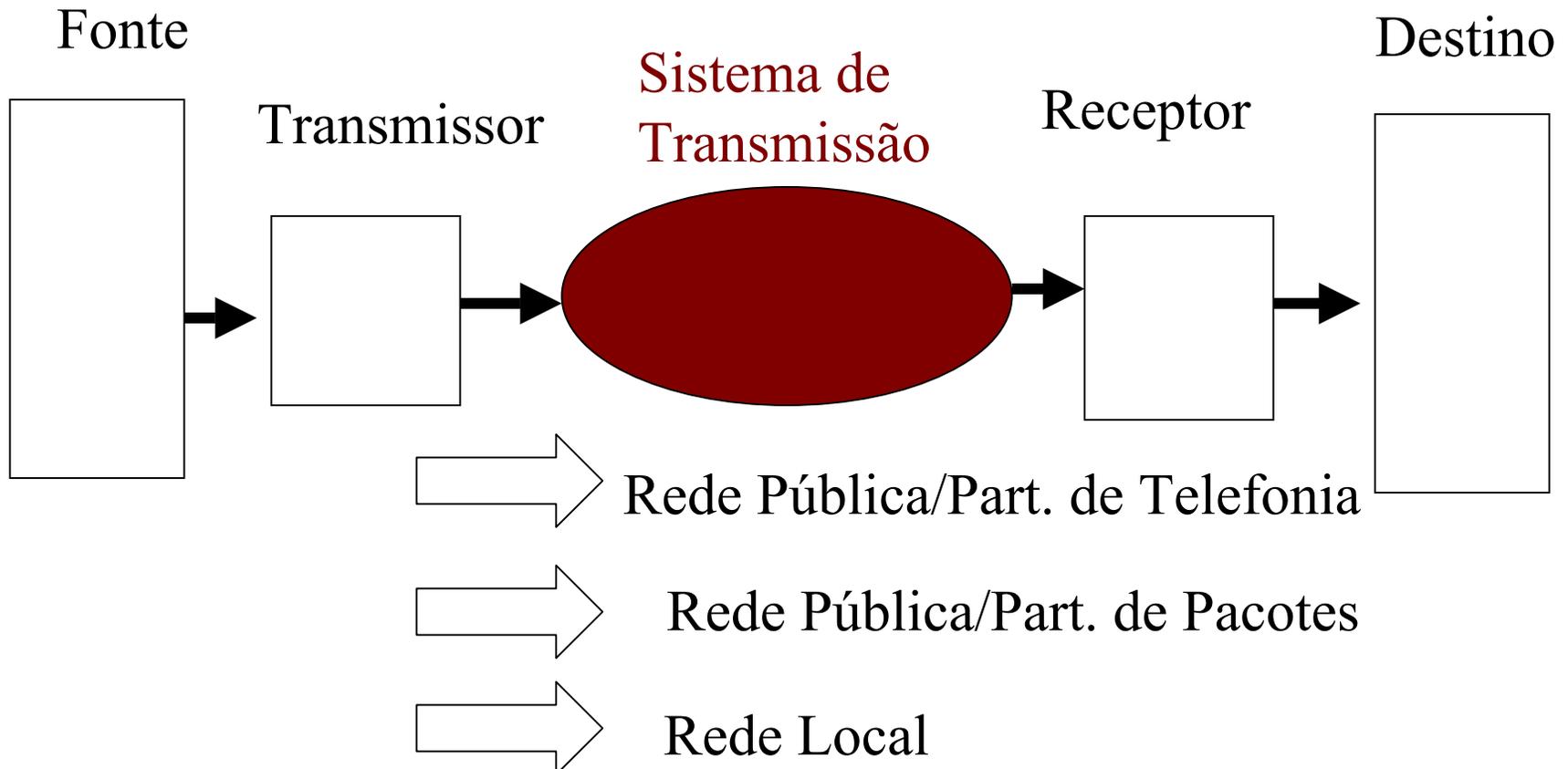
Conceitos de Comunicação

Modelo Genérico de Comunicação



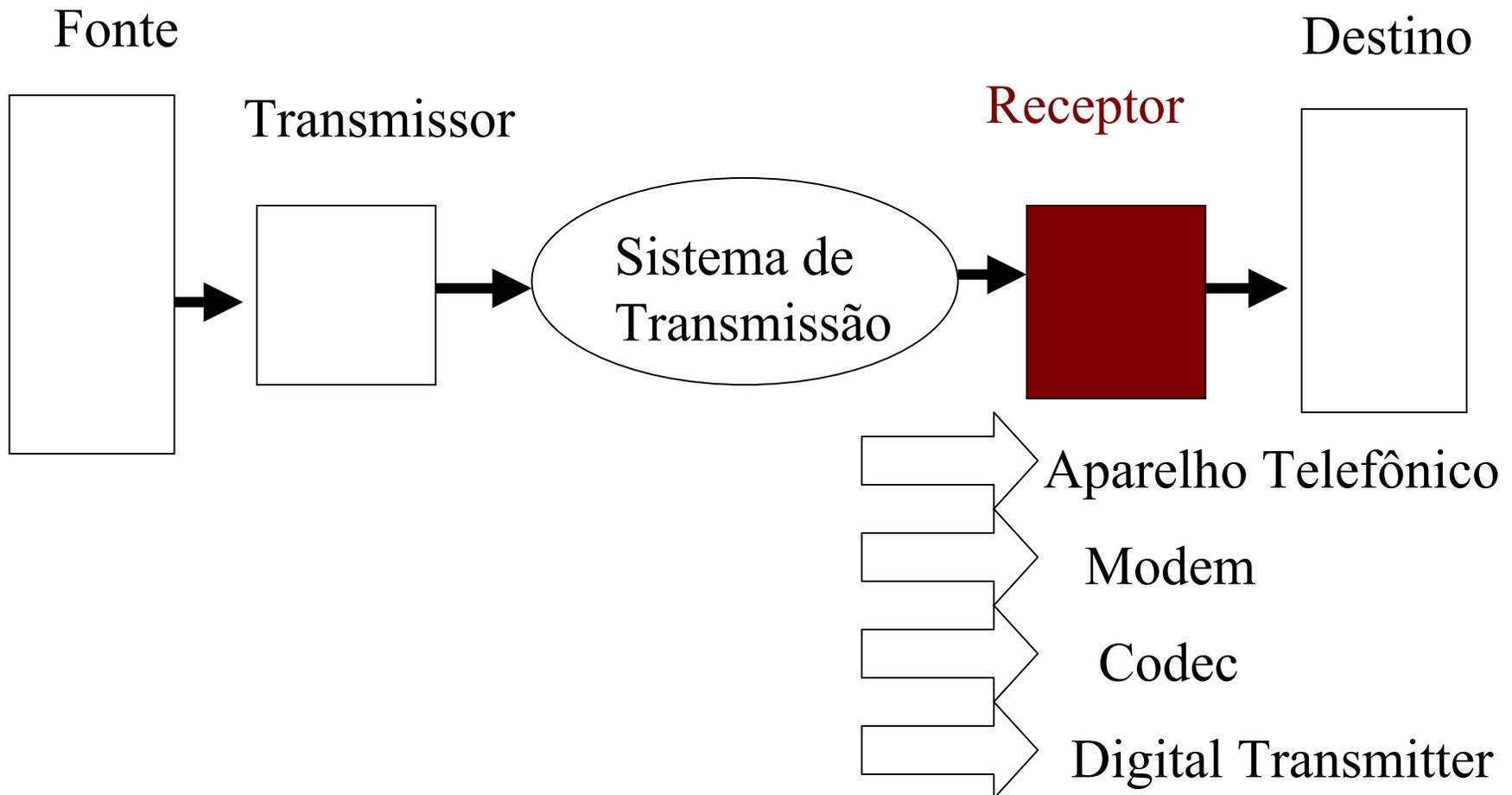
Conceitos de Comunicação

Modelo Genérico de Comunicação



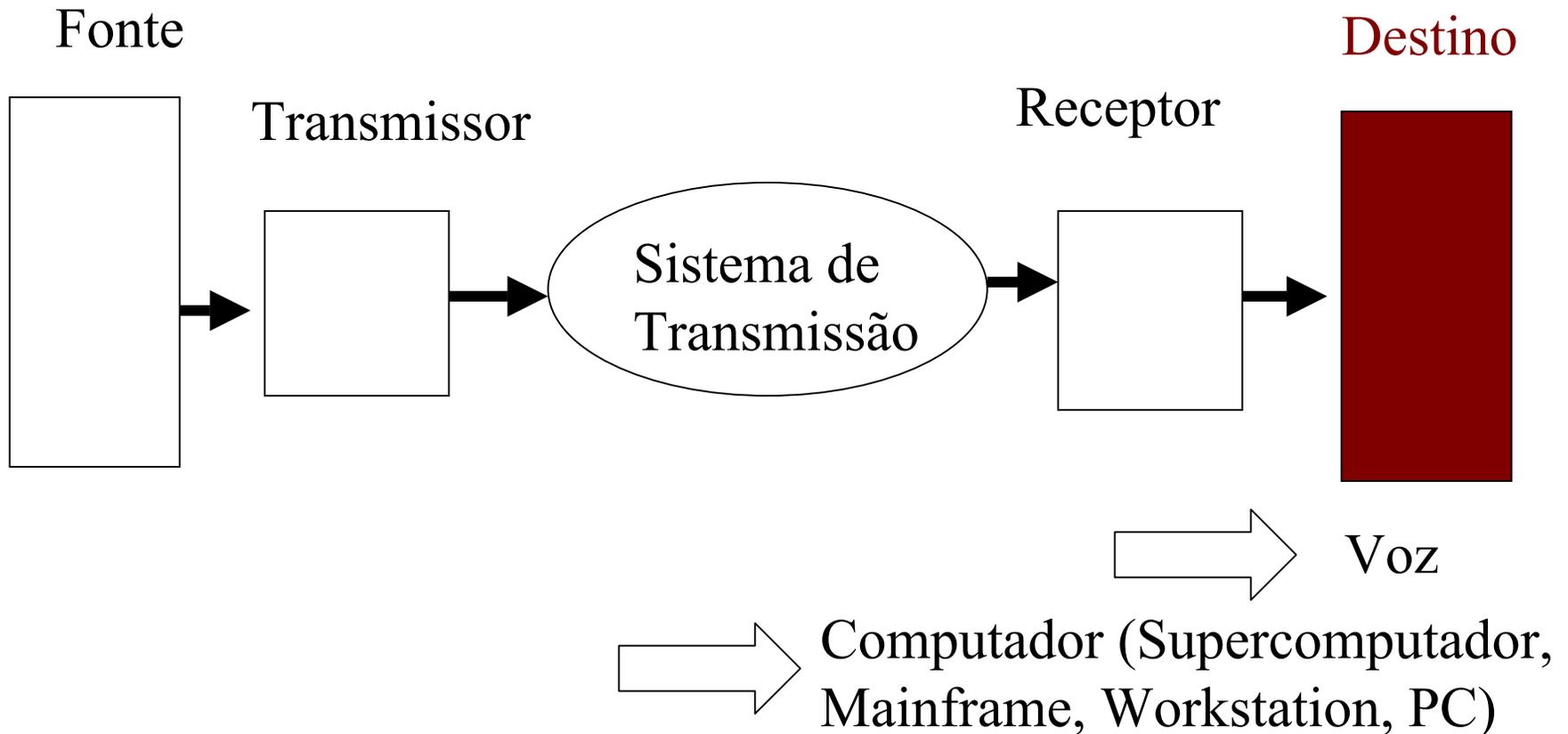
Conceitos de Comunicação

Modelo Genérico de Comunicação



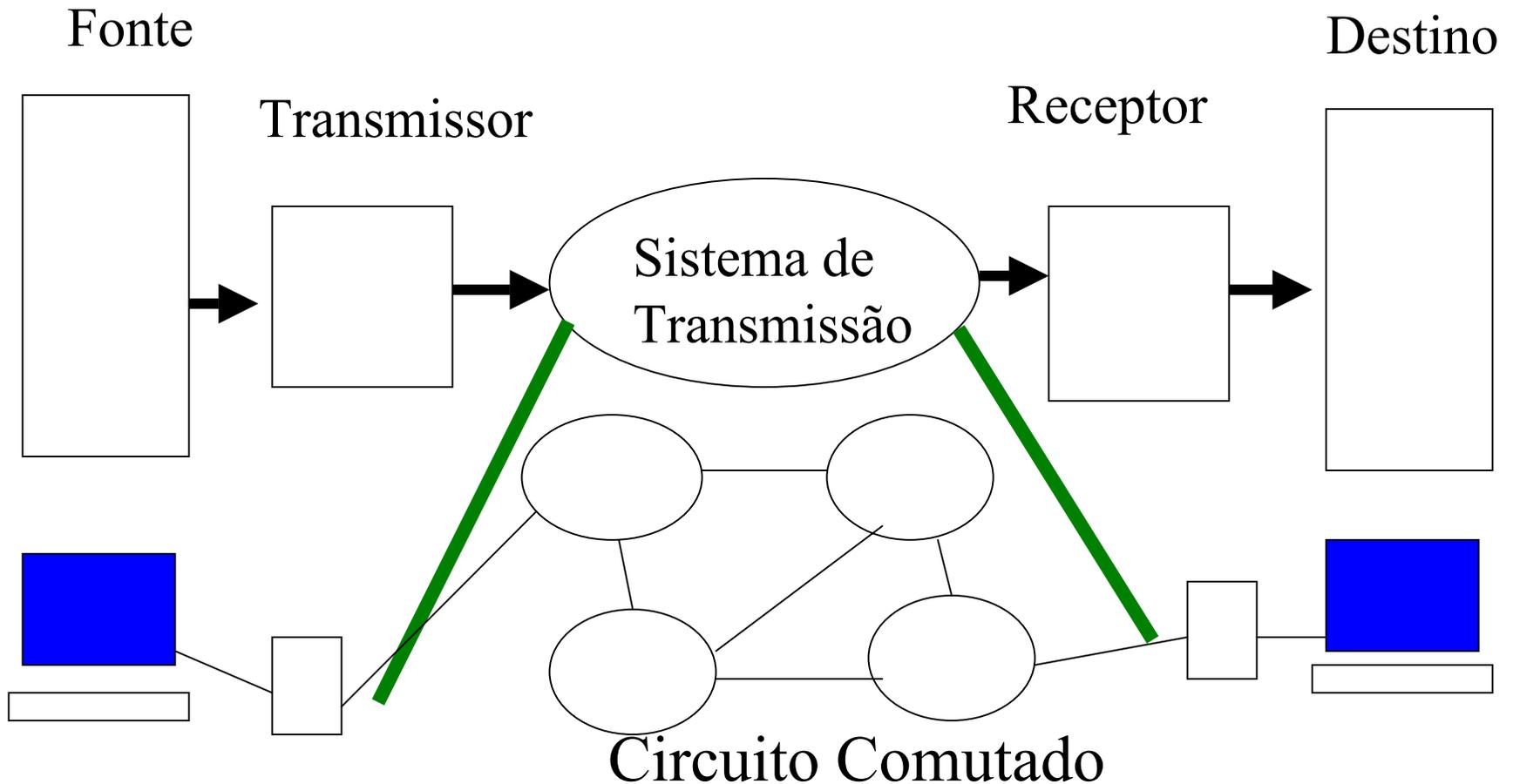
Conceitos de Comunicação

Modelo Genérico de Comunicação



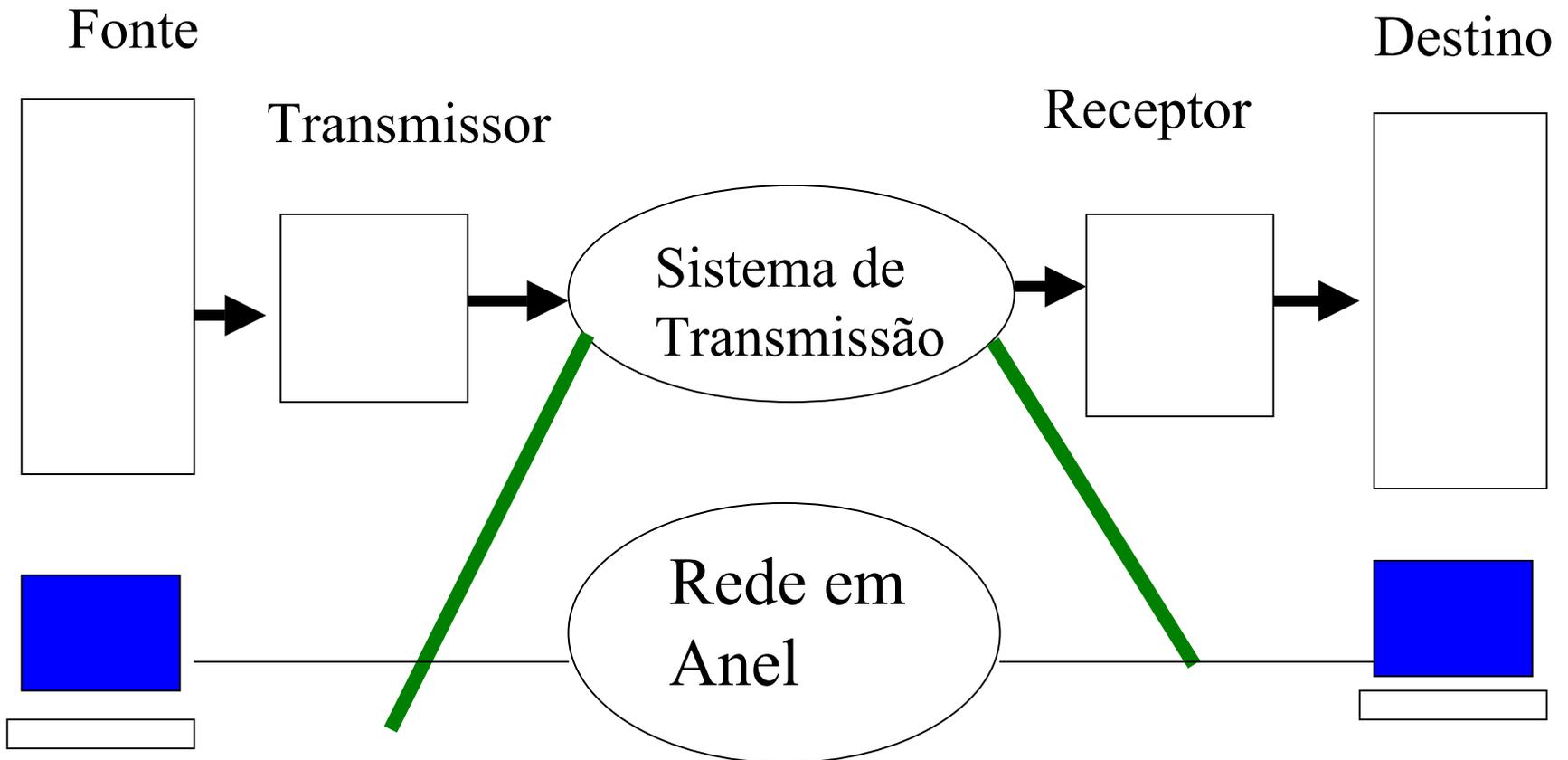
Conceitos de Comunicação

Modelo Genérico de Comunicação



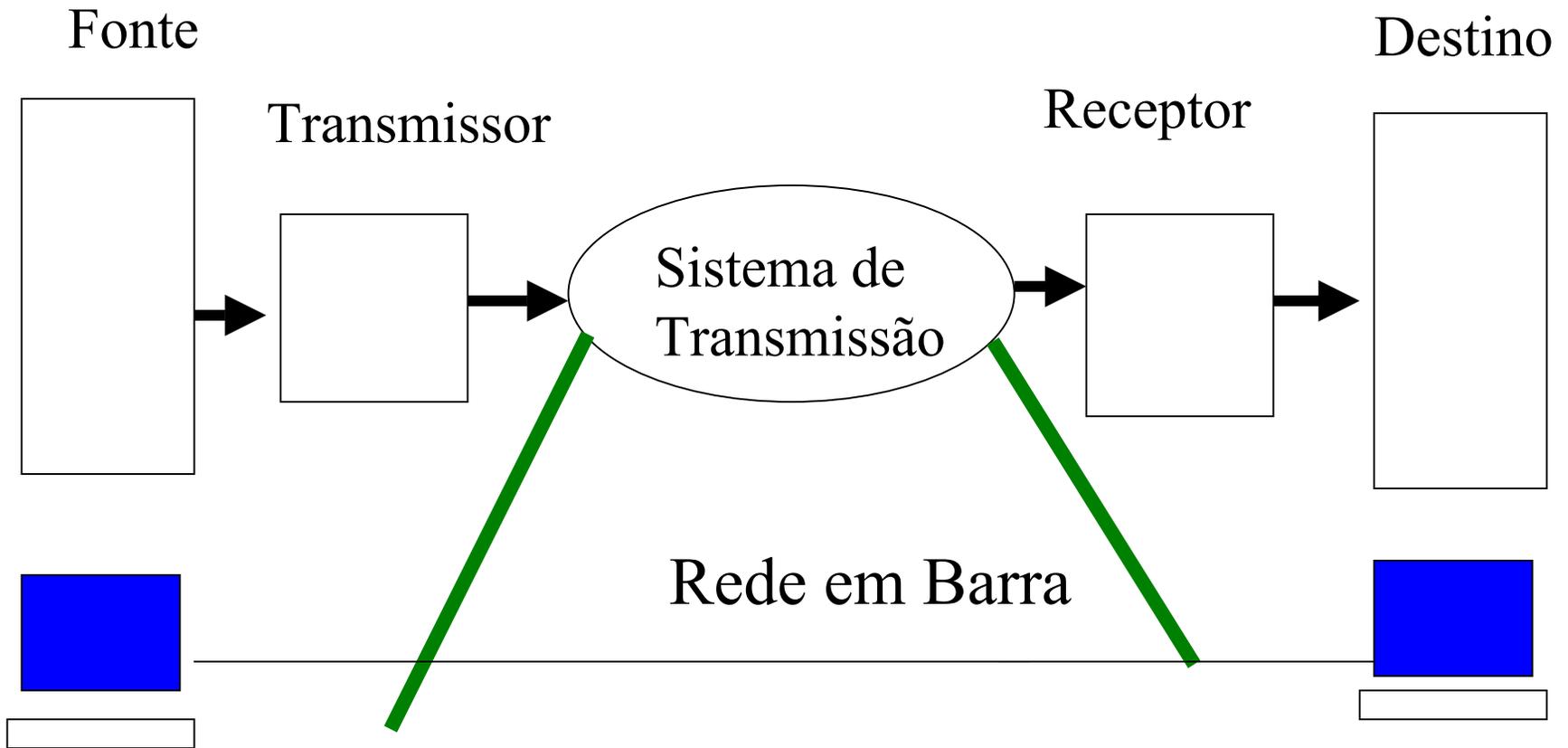
Conceitos de Comunicação

Modelo Genérico de Comunicação



Conceitos de Comunicação

Modelo Genérico de Comunicação



Conceitos de Comunicação

Modelo Genérico de Comunicação



Conceitos de Comunicação e Redes

Informação e Sinal

Os processos envolvidos na transmissão da informação entre dois pontos são :

- Geração da idéia ou imagem na origem.**
- Utilizar um conjunto de símbolos para representação da idéia ou imagem.**
- Codificar os símbolos para uma transmissão no meio físico disponível.**
- Transmitir os símbolos codificados para o destino.**

Conceitos de Comunicação e Redes

- **Decodificação e reprodução dos símbolos.**
- **Re-constituição da idéia, ou imagem, transmitida com o mínimo de degradação.**

***Sinais* são ondas que propagam através de um meio físico, seja este um cabo ou atmosfera.**

Sinais, são geralmente, representados como função do tempo.

Conceitos de Comunicação e Redes

Informação é, geralmente, associada às idéias (ou dados) criadas pelas entidades que desejam transmiti-la para um certo destino.

Desta forma, os *sinais* são a materialização específica da informação para ser transmitida num meio de comunicação qualquer.

Conceitos de Comunicação e Redes

Considere a seguinte tabela :

Meio de Transmissão	Taxa de Transmissão	Largura de Banda
Par Trançado	4 Mbps	3 MHz
Cabo Coaxial	550 Mbps	350 MHz
Fibra Ótica	2 Gbps	2 GHz

Conceitos de Comunicação e Redes

Nos anos vinte, um pesquisador chamado de Nyquist, elaborou um teorema no qual é possível estabelecer um limite teórico na velocidade máxima que podemos transmitir os sinais numa rede de comunicação.

Conceitos de Comunicação e Redes

O teorema de Nyquist diz que capacidade de um canal será (idealmente) ao dobro da largura de banda vezes o logaritmo do número de níveis discretos.

Conceitos de Comunicação e Redes

A relação entre largura de banda, digamos LB , que é medida Hz e a quantidade de bits enviados por segundo (bps), digamos QB , segundo Nyquist, pode ser formulada como :

$$QB = 2 \times LB \times (\log_2 N)$$

Onde N corresponde ao número de valores possíveis níveis de tensões usado no sistema.

Conceitos de Comunicação e Redes

A proposta de Nyquist, como comentamos é um teorema teórico, em outras palavras o mesmo não considera as possíveis interferências que a rede de comunicação é exposta. Em outras palavras, além da consideração dos limites físico do meio o sistema está exposto a interferências externas que podem causar perda de desempenho no ambiente.

Conceitos de Comunicação e Redes

No final dos anos quarenta, Claude Shannon propôs uma extensão ao teorema de Nyquist na qual fosse considerada a parcela do ruído. O Teorema de Shannon é então expresso como :

$$C = LB \times \log_2 (1 + S/R)$$

Conceitos de Comunicação e Redes

Onde C é a capacidade do canal em bits por segundo (bps), S representa a potência média do sinal e R a parcela do ruído. A relação S/R é geralmente expressa em decibéis (dB). A quantidade de decibéis significa dizer que a taxa de sinal-ruído é equivalente a expressão :

$$10 \log_{10} S/R$$

Conceitos de Comunicação e Redes

Dos teoremas de Nyquist e Shannon, respectivamente, podemos concluir que :

- uma melhor codificação nos leva a uma transmissão mais eficiente ;
- mesmo com uma codificação mais eficiente teremos as leis físicas como um fator limitador na transferência dos bits.

Conceitos de Comunicação e Redes

Exemplo : Um caso clássico de cálculo de capacidade de canal, é a consideração do teorema de Shannon aplicado a um canal comum de voz . Suponhamos uma largura de banda de (LB) de 3000 Hz e uma parcela de sinal-ruído (S/R) da ordem de 1023 (ou seja 30 dB).

Conceitos de Comunicação e Redes

Calcule a capacidade do canal para transmissão de dados em bps.

1° Passo – É interessante que seja primeiro calculado a parcela $\log_2(1 + S/R)$, assim :

$$= \log_2(1 + S/R)$$

$$= \log_2(1 + 1023)$$

$$= 10$$

Conceitos de Comunicação e Redes

2º Passo – Com parcela $\log_2(1 + S/R)$ já calculada, a aplicação é direta da formula da capacidade do canal.

$$C = LB \times \log_2(1 + S/R)$$

$$C = 3000 \times 10$$

$$C = 30.000 \text{ bps}$$

Conceitos de Comunicação e Redes

Do cálculo do exemplo anterior, podemos concluir que a taxa máxima de transmissão num canal de voz de 3000 Hz é de 30000 bps. Nossa intenção ao utilizar este exemplo clássico é ajudar a evitar a confusão entre MHz e bps num dado ambiente de rede.

Banda Base e Banda Larga

O termo largura de banda é definido na comunicação de dados como sendo a quantidade máxima de transmissão de diferentes sinais num meio físico (como um cabo coaxial/ótico).

Banda Base e Banda Larga

Qual a diferença entre :

largura de banda e taxa de transmissão ?

A largura de banda é medida em MHz e a taxa de transmissão em MBPS

Banda Base e Banda Larga

A largura de banda de um cabo pode ser dividida em *canais*. As duas formas de utilizar a capacidade de transmissão de um meio físico são :

banda base e banda larga

Banda Base e Banda Larga

Banda base : neste tipo de transmissão toda a largura de banda é usada por um único canal.

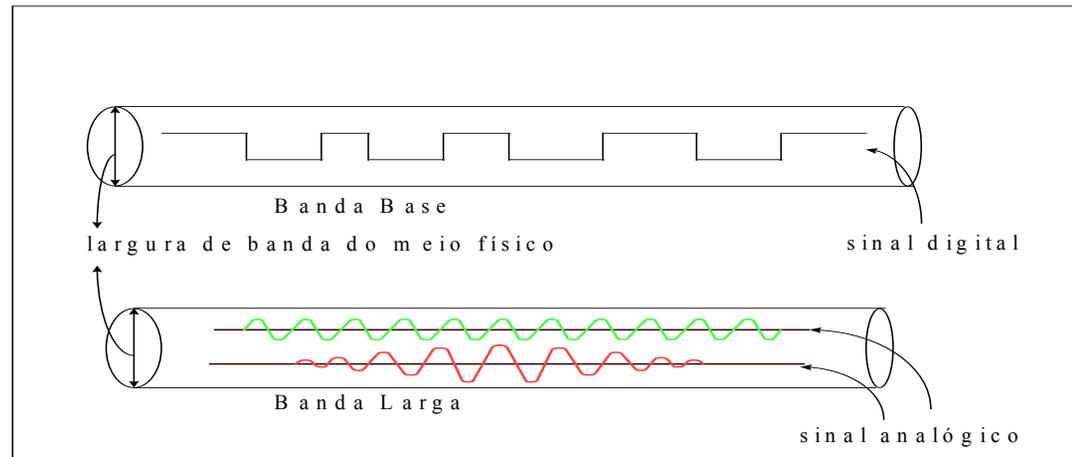
Esta tecnologia é freqüentemente usada para transmissão digital. Por esta razão, a maioria das redes de computadores adotam esta técnica.

Banda Base e Banda Larga

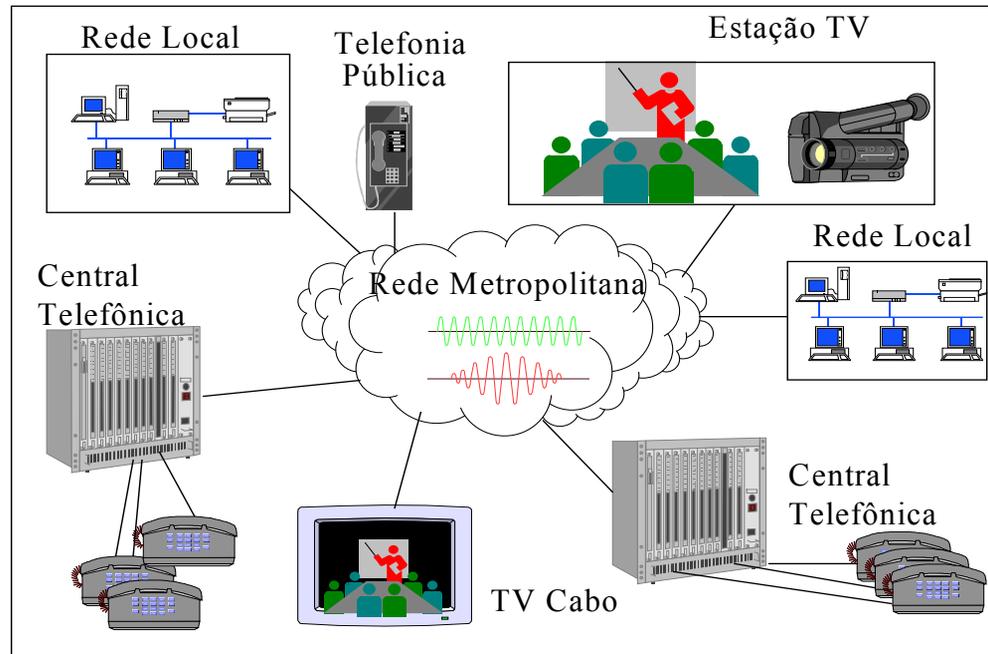
Banda larga : Este modelo de transmissão é caracterizado pela divisão da largura de banda em múltiplos canais.

Podendo cada canal transmitir diferentes sinais analógicos. Por esta razão, redes de banda larga podem transmitir múltiplos sinais simultaneamente.

Banda Base e Banda Larga



Banda Base e Banda Larga



Conceitos de Comunicação e Redes

Tarefas importantes num sistema de comunicação

- Utilização do sistema de comunicação;
- Interfaces;
- Geração do sinal;
- Sincronização;
- Gerência de troca de informação;
- Detecção e correção de erros;
- Controle de fluxo;
- Endereçamento;
- Roteamento;
- Recuperação de informação;
- Formato de mensagens;
- Segurança e gerência da rede.

Conceitos de Comunicação e Redes

Conceitos Básicos

- **LAN** (Local Area Network): uma rede local é um rede com abrangência física de até poucos quilômetros, com uma alta taxa de transferência (centenas de Mbps , ou até milhares), baixa ocorrência de erros e *não ocorre roteamento da informação*.
- **WAN** (Wide Area Network): uma rede geograficamente distribuída engloba uma vasta região (estado, país, continentes), possui uma taxa de transferência (quando comparada com um LAN) na ordem de dezena de Mbps, uma elevada taxa de erros e *existe o roteamento de informação*

Conceitos de Comunicação e Redes

Conceitos Básicos

- **Ethernet** - Rede local em barra, cuja concepção inicial foi idealizada por Robert Metacalf, e implementada em conjunto pelas empresas Xerox, Digital e Intel. Este tipo de rede implementa o acesso com contenção.
- **Token-Ring** - Rede local em anel, idealizada na IBM da Alemanha, visando a interconexão de dispositivos de rede com o acesso ordenado.

Conceitos de Comunicação e Redes

Conceitos Básicos

- **Circuit Switching:** Ambiente de comunicação cujos circuitos são comutados e que podem ser acionados para o uso exclusivo de comunicação entre *nós* da rede de comunicação.
- **Packet Switching:** Técnica que não considera a exclusividade de ligação entre pontos de uma rede de comunicação, mas que se utiliza da mesma para enviar pequenos conjuntos de bits (pacotes) de uma maneira não seqüencial. Ou seja, os pacotes são numerados e enviados na rede com o endereço do destinatário, podendo estes chegar fora de ordem.

Conceitos de Comunicação e Redes

Conceitos Básicos

- **Frame-Relay**: rede de comunicação onde *frames* (quadros) de tamanho variável, trafegam com taxas de velocidade de até 2Mbps, não existindo todo o controle de erro encontrado nas redes de comutação de pacotes.
- **ATM** (Asynchronous Transfer Mode): também conhecida com *cell-relay*, esta técnica de transferência é o amadurecimento das tecnologias de *circuit switching* e *packet switching*. Célula fixas de 53 bytes trafegam pela rede evitando um *overhead* de processamento chegando a centenas de Mbps.

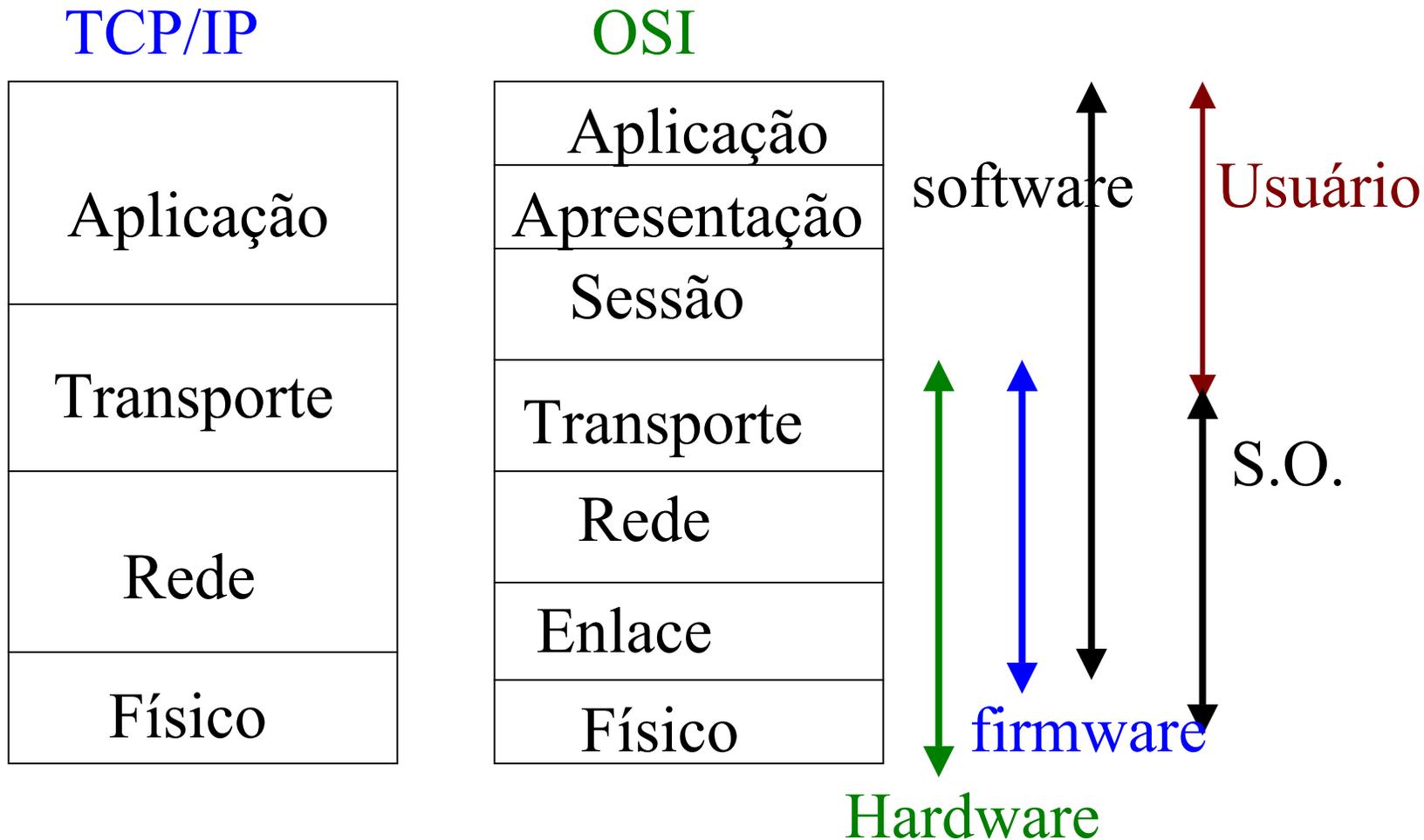
Conceitos de Comunicação e Redes

Conceitos Básicos

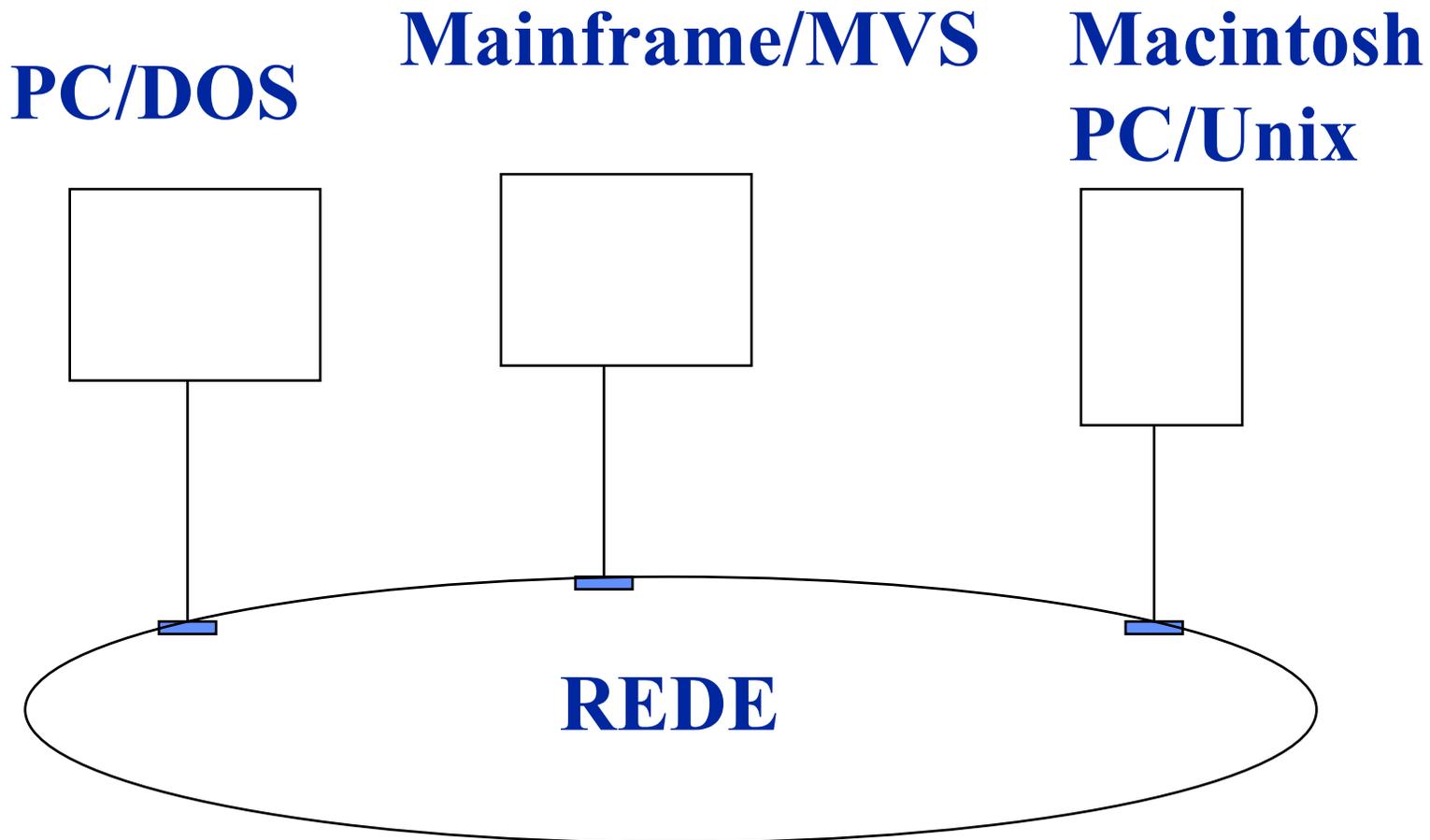
- **Protocolos** : conjunto de regras que definem com a troca de informação entre entidades de uma rede de comunicação deve ser realizada com sucesso, e como os erros deverão ser tratados.
- **Arquitetura de protocolos** : é a estrutura representativa não só dos protocolos disponíveis numa dada arquitetura, mas também das funções e interações de cada protocolo no seu nível de atribuição.

Conceitos de Comunicação e Redes

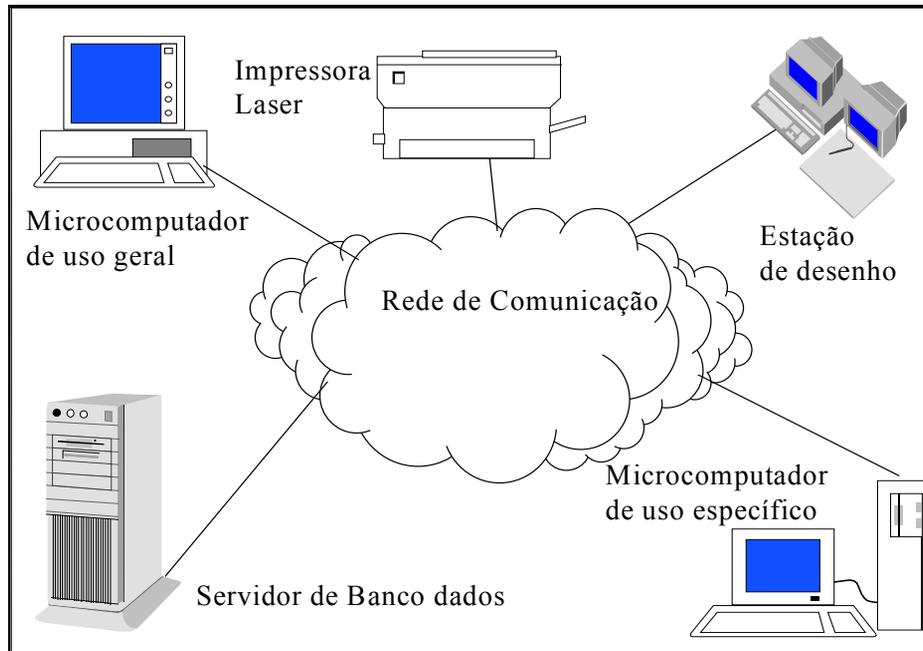
Conceitos Básicos



Conceitos de Comunicação e Redes



Conceitos de Comunicação e Redes



Conceitos de Comunicação e Redes

Num ambiente de rede de computadores os três componentes macros são o hardware, software e as facilidades de telecomunicação. Desta maneira, é fundamental que tenhamos um conhecimento básico da identificação destes componentes e seu interfuncionamento.

Conceitos de Comunicação e Redes

Meio físico -

Em um ambiente de rede o meio físico da rede é definido como o meio utilizado para a comunicação. Em redes de computadores, consideramos também as placas de rede utilizadas para implementar a conexão ao meio físico.

Conceitos de Comunicação e Redes

Os meios físicos são, geralmente, classificados como *guiados* e *não-guiados*.

Exemplos de meios físicos *guiados* são os cabos coaxiais, pares trançados e fibra ótica. Por outro lado, os meios físicos *não-guidos* são representados por transmissões que utilizam a atmosfera terrestre (microondas, rádio e infravermelho) e o espaço (satélites) para a transmissão da informação.

Conceitos de Comunicação e Redes

Placas de rede :

Conhecidas como NIC (*Network Interface Card*) obedecem as características da arquitetura do computador (*host ou nó*) e da rede a qual está conectada.

Estas dependem do tipo de meio físico da rede (exemplo: par trançado e coaxial) e pela taxa de transmissão implementada pela rede no fluxo de dados (Exemplo: 10, 100 ou 1000Mbps).

Conceitos de Comunicação e Redes

O que são *protocolos de comunicação* ?

Conjunto de regras que permitem o enlace com sucesso a comunicação entre dois, ou mais, computadores.

Um dado computador precisar saber como uma mensagem deve ser enviada/recebida pela rede. Só então, tomar a decisão correta para tratar de uma maneira precisa a mensagem a ser enviada ou recebida.

Conceitos de Comunicação e Redes

Parâmetros de Avaliação

A opção por uma dada tecnologia de rede para suporte a um conjunto de aplicações é uma tarefa complexa, devido aos inúmeros parâmetros que são envolvidos na análise.

Exemplos de fatores a serem considerados são :

- custo**
- tempo de resposta**
- taxa de transmissão**
- desempenho**
- facilidade de desenvolvimento**
- modularidade**

Exemplos de fatores a serem considerados são :

- **capacidade de reconfiguração**
- **dispersão geográfica**
- **complexidade lógica**
- **facilidade de uso**
- **disponibilidade**
- **facilidade de manutenção**

Custo -

A composição de custos numa rede é formada pelos computadores, placas de ligação ao meio físico e o próprio meio físico. Redes de alto desempenho requerem interfaces de alto custo quando comparadas redes com menor desempenho.

Retardo (Latency) :

O retardo de envio de uma mensagem entre dois computadores qualquer, numa rede é computado da seguinte forma :

$$\mathbf{R_{total} = R_{trans} + R_{acesso}}$$

Onde: R_{total} - retardo de transferência.

R_{trans} - retardo de transmissão.

R_{acesso} - retardo de acesso

Retardo de acesso –

É o tempo decorrido para que uma mensagem tenha acesso a rede para transmitir.

Retardo de transmissão –

É o tempo decorrido desde o início de transmissão de um computador até a outra ponta (outro computador).

Retardo de transferência –

É o tempo total de uma mensagem para ser enviada de um dado computador a outro (acesso + transmissão).

Desempenho: este parâmetro pode ser avaliado em termos topologia, meio de interconexão, protocolos de comunicação e a velocidade de transmissão. Estes aspectos serão estudados ao longo do presente curso.

Confiabilidade: uma forma de avaliar a confiabilidade de uma rede é considerar aspectos tais como tempo médio entre falhas (MTBF), tolerância a falhas, tempo de reconfiguração após falhas e tempo de reparo (MTTR).

Modularidade: é característica que um determinado sistema de rede possui, quanto a sua expansão e modificação sem que estas alterações causem um impacto na configuração original do projeto.

Topologias

As redes de computadores são caracterizadas pelo (1) *arranjo físico (topologias)* dos equipamentos interligados através dos (2) *meios físicos de transmissão* e (3) um conjunto de regras que organizam a comunicação (*protocolos*) entre computadores.

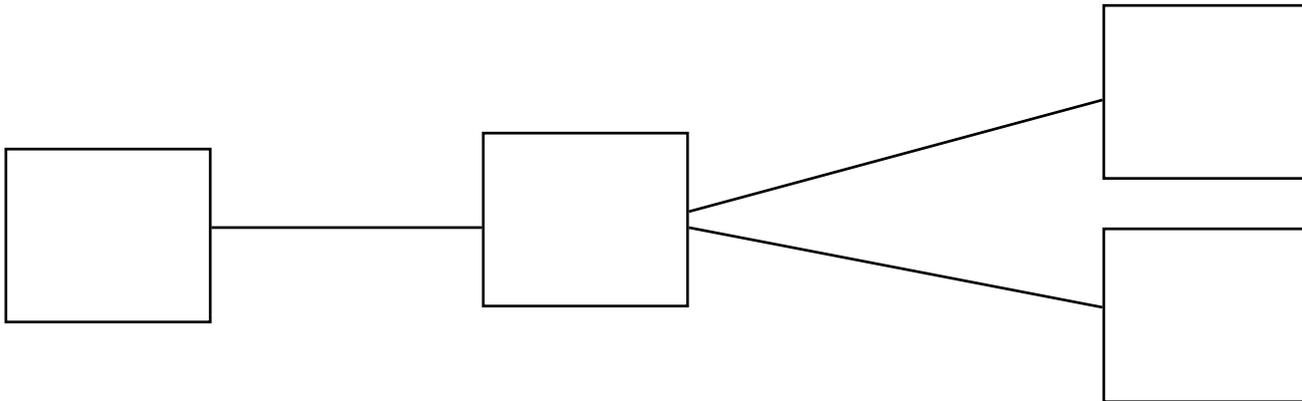
Topologias

“A topologia de uma rede de comunicação refere-se à forma como os enlaces físicos e os nós de comutação estão organizados, determinado os caminhos físicos existentes e utilizáveis entre quaisquer pares de estações conectadas a essa rede.” (Soares, Lemos e Colcher)

Topologias

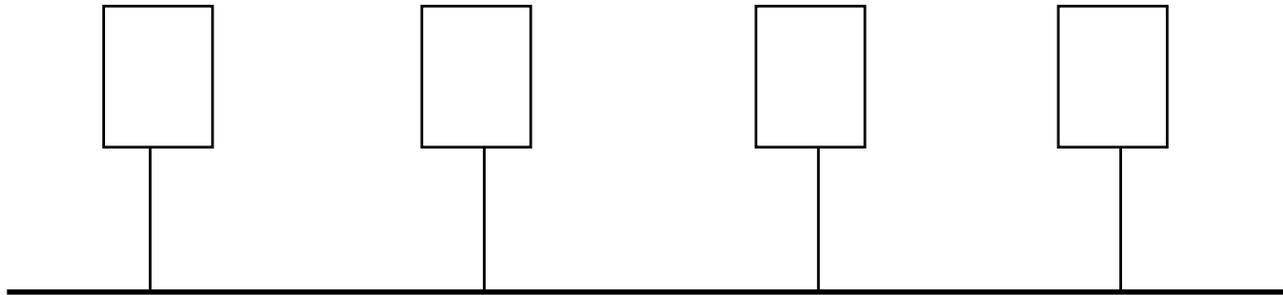
As linhas de comunicação numa rede, podem ser interconectadas das seguintes formas:

- *Ponto-a-ponto* - apenas dois pontos de comunicação existem entre dois equipamentos (um em cada extremidade do enlace ou ligação).



Topologias

- *Multiponto* - neste tipo de ligação, três ou mais dispositivos têm a possibilidade de utilização do mesmo enlace físico.

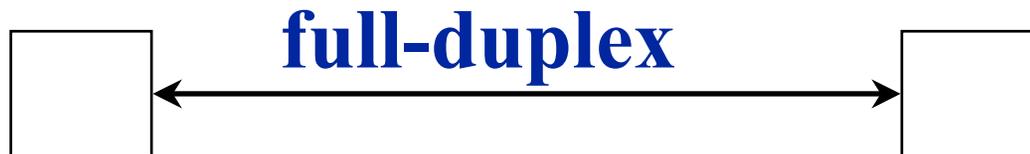
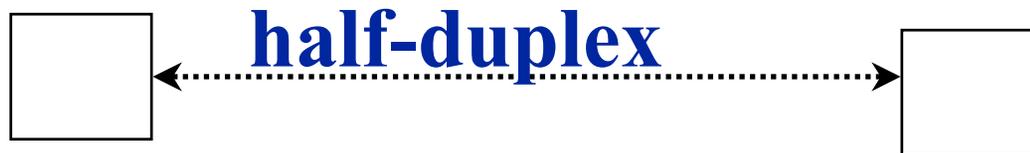


Topologias

O sentido de transmissão de sinal num enlace de comunicação pode ser efetuado de três formas:

- ***Simplex* - a comunicação é efetuada apenas num sentido.**
- ***Half-duplex* - a comunicação é efetuada nos dois sentidos, uma de cada vez.**
- ***Full-duplex* - a comunicação é efetuada nos dois sentidos simultaneamente.**

Topologias



Topologias

Topologias de WANs

As topologias empregadas nas redes geograficamente distribuídas são :

- *topologia totalmente ligada* - os enlaces utilizados são em geral ponto-a-ponto com ligação full-duplex. Desta forma, existe uma comunicação plena entre quaisquer pares de estações.

Topologias

Numa rede com N computadores, $N(N-1)/2$ ligações são necessárias. O custo de tal configuração, em termos de cabos e de hardware para comunicação, cresce com o quadrado do número de computadores. Pelo motivo exposto, esta topologia é economicamente inviável.

Topologias

- **topologia em anel** - neste tipo de configuração diminui-se ao máximo o número de ligações. Uma vez que cada computador é interligado a outro ponto-a-ponto, num único sentido de transmissão (ligação simplex), fechando-se numa forma de anel. Embora o custo desta topologia seja um fator importante quando comparada com a *totalmente ligada*, alguns fatores limitantes inviabilizam tal configuração.

Topologias

Alguns fatores limitantes desta topologia são:

- (1) o número elevado de computadores que uma mensagem tem que passar, até que atinja seu destino; o retardo de recebimento de mensagem é bastante elevado nesta configuração.**
- (2) a inexistência de caminhos alternativos; principalmente quando linhas de baixa velocidade e pouca confiabilidade são empregadas.**

Topologias

- *topologia parcialmente ligada* - esta topologia é uma alternativa híbrida entre as duas anteriores, na qual temos alguns caminhos redundantes. Com estas ligações, a configuração ganha confiabilidade sem aumento de custo. Técnicas de chaveamento de *circuito e mensagem* são utilizadas nesta topologia. Na primeira técnica, temos uma conexão entre dois computadores efetuada durante toda a transmissão.

Topologias

Na segunda técnica, chaveamento de mensagem ou pacote, o caminho é determinado durante o envio da mensagem ou pacote. Não existe um caminho, ou conexão, pré-determinado para o envio.

Topologias

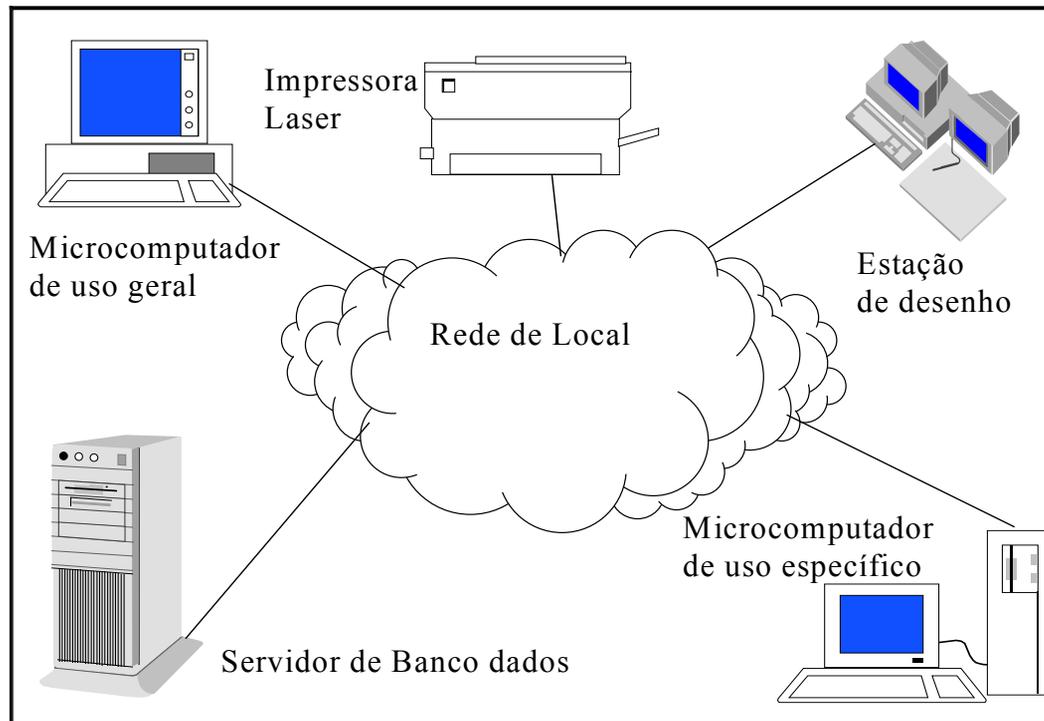
Topologias das LANs

Nesta seção vamos abordar as topologias adotadas nas redes locais. Vamos definir formalmente LAN e MAN, além de conhecer o funcionamento das topologias.

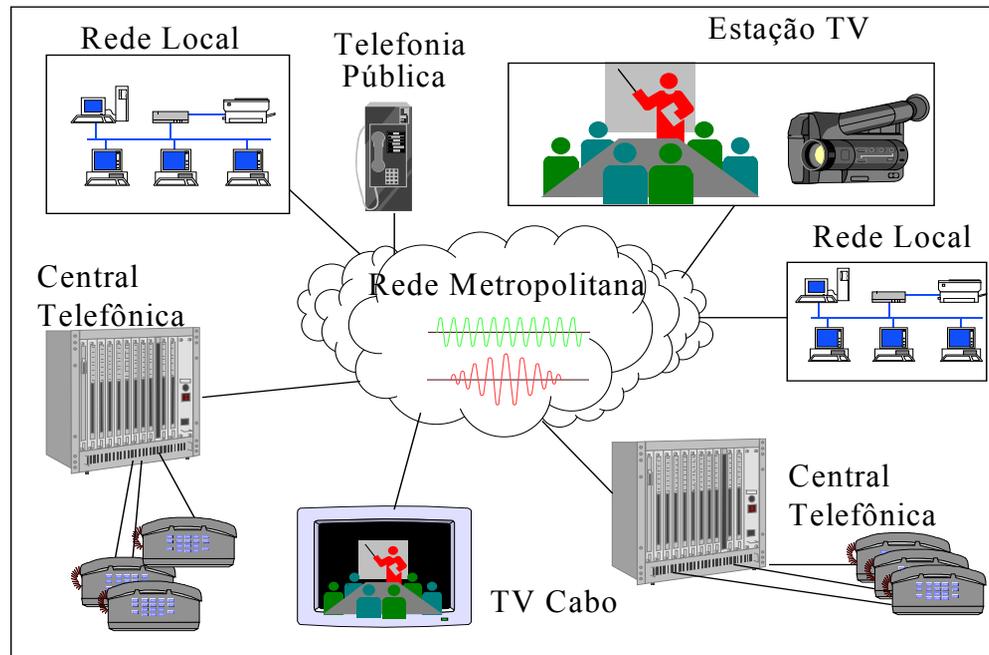
Topologias

Rede Local, ou LAN (Local Área Network), é uma rede com extensão geográfica limitada a poucos metros utilizando-se um software para a comunicação entre computadores denominado de protocolo. As redes locais, usualmente, possuem uma alta taxa de transferência de dados com baixos índices de erro e o proprietário é uma única organização.

Topologias



Redes Metropolitanas, ou MANs (Metropolitan Areas Networks), são definidas como sendo redes maiores que as LANs, geralmente administradas por uma empresa de telecomunicação que fornecem o serviço, abrangendo uma área metropolitana ou compreendendo os limites de uma cidade.



Topologias

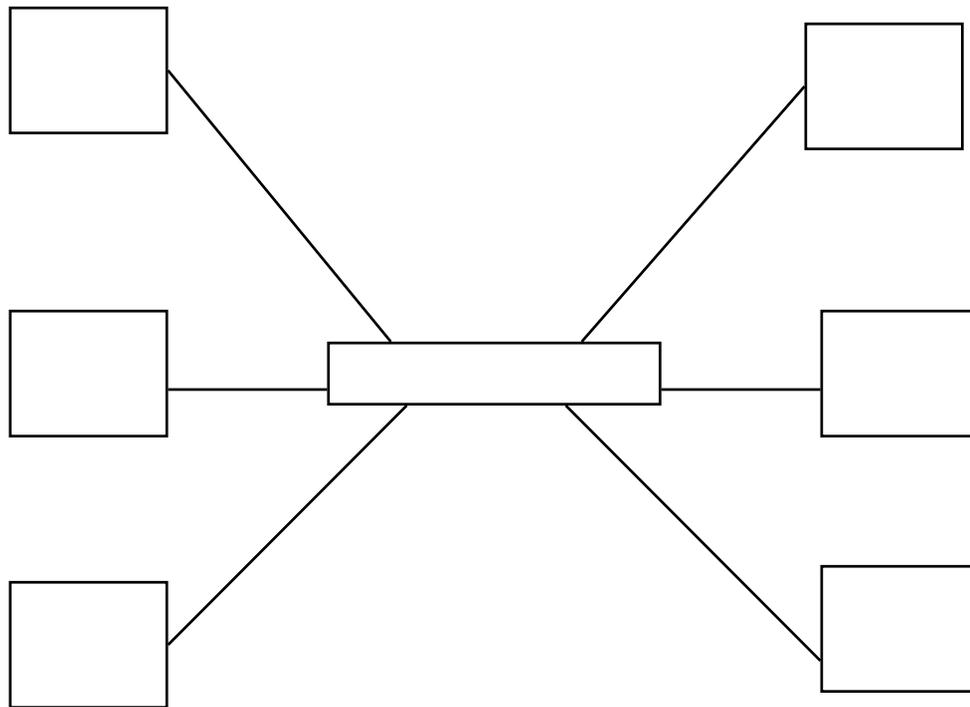
As mais conhecidas implementações topológicas das LANs são as topologias em estrela, a barramento e o anel.

Devido a derivação da tecnologia de redes da área de telecomunicação, a topologia em estrela foi a primeira implementação de rede projetada e implementada.

Topologias

Topologia Estrela - a característica da topologia estrela é a ligação de todos os computadores num equipamento central, ou seja uma ligação ponto-a-ponto. Este equipamento é conhecido como *hub ou concentrador*.

Topologias



Topologia Estrela

Topologias

A configuração em estrela pode implementar a comunicação entre *nós* de duas maneiras distintas, a *broadcast* e a *switched*.

Na forma *broadcast* um *nó* envia uma mensagem para o *concentrador* que espalha para todos os *nós*. Na técnica conhecida como *switched*, a mensagem é direcionada para o destino diretamente.

Topologias

Nas redes com topologia estrela, existem dois tipos de concentradores :

- concentradores ativos que regeneram o sinal recebido. *Multiport repeaters* são dispositivos que efetuam a regeneração de sinal.

- concentradores passivos não atuam no nível do sinal. Os painéis de ligação ponto-a-ponto, são exemplos de concentradores deste tipo.

Topologias

Vantagens da topologia estrela :

- fácil instalação, configuração e reconfiguração.**
- gerência e administração da rede.**
- possibilidade de expansão através da aquisição e interconexão de novos concentradores.**
- a falha de um equipamento (*nó*) não prejudica o funcionamento da rede.**
- possibilidade de adicionar/retirar *nós* com a rede em funcionamento.**

Topologias

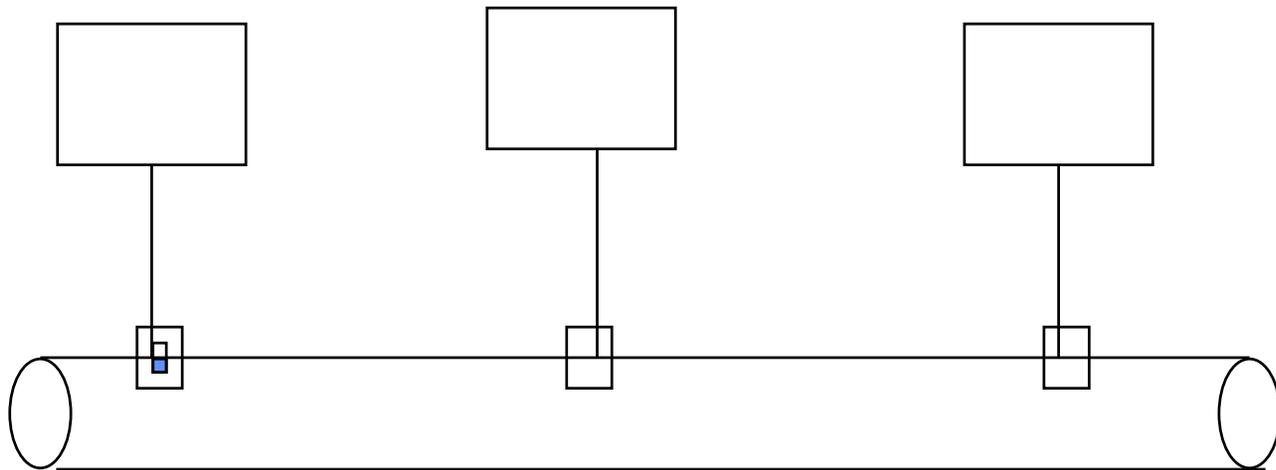
Desvantagens da topologia estrela :

- ponto único de falha (concentrador).**
- como a conexão é ponto-a-ponto, custo mais elevado da estrutura de cabeamento/conexões.**
- no caso de uma rede grande, necessidade de um (ou mais) concentrador(es) para redirecionamento de mensagens.**

Topologias

Topologia em Barra - esta topologia, que na maioria das vezes implementa a configuração multiponto, foi com certeza a mais empregada tecnologia nas redes locais. Exemplos clássicos são a Ethernet e Fast-Ethernet. A natureza da topologia é passiva e repetidores de sinal são usados para a extensão da rede.

Topologias



Topologia de Barra

Topologias

A comunicação entre dois *nós* numa topologia em barra é efetuada da seguinte maneira :

- 1 - Um *nó* remetente envia sua mensagem na barra.**
- 2 - Este sinal é recebido por todos os *nós*.**
- 3 - Somente o *nó* com o endereço destinatário lê a mensagem, os demais ignoram.**
- 4 - Uma mensagem por vez circula no meio, assim todos esperam que o canal fique livre.**

Topologias

Vantagens da topologia em barra :

- instalação simples, relativa pouca manutenção.**
- quantidade de cabeamento é menor quando comparada com outras topologias.**
- extensão da rede é facilmente efetuada através de repetidores.**
- custo baixo devido a grande quantidade de implementações e conseqüente necessidade de componentes.**

Topologias

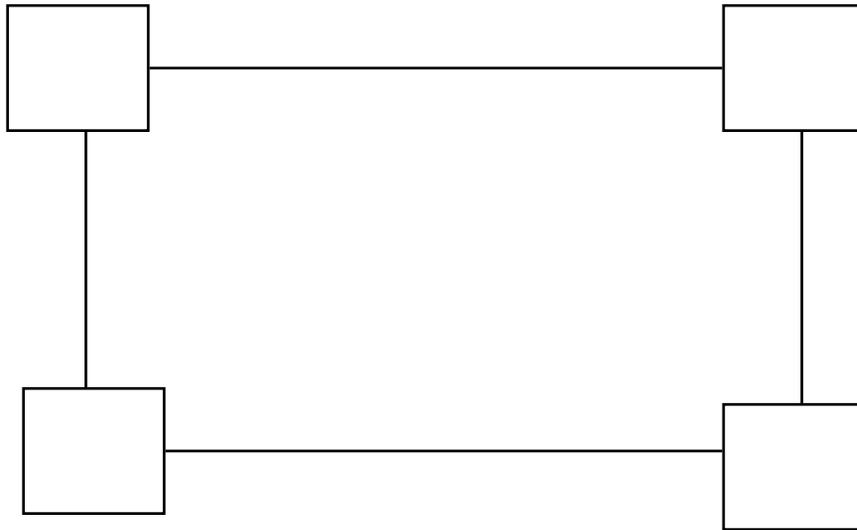
Desvantagens da topologia em barra :

- aumento de *nós* leva a um aumento crescente do número de colisões na rede.**
- aumento de *nós* leva a um aumento crescente de erro de sinal na rede (problema de placas e conexões).**
- gerência física da rede.**

Topologias

Topologia Anel - cada *nó* é conectado a um outro que por sua vez é conectado em outro, formando um anel. O último computador se interliga ao primeiro fechando o círculo do anel.

Topologias



Topologia Anel

Topologias

Vantagens da topologia em anel :

- nenhum computador tem acesso ilimitado a rede.**
- Por causa dos protocolos determinísticos de acesso a rede, com o aumento de *nós* não ocorre uma degradação como na topologia de barra.**

Topologias

Desvantagens da topologia em anel :

- no caso de uma falha num *nó* toda a rede pode ficar comprometida.**
- necessidade de parada da rede para expansão, desconexão de *nós*.**
- dificuldade de gerência.**

Na redes metropolitanas (MANs) são caracterizadas pela utilização de serviços de telecomunicação para que possa conectar os *nós* da rede. Este tipo de rede, é geralmente vista como uma extensão de uma rede local numa cidade ou área metropolitana. Por esta razão a necessidade de serviços públicos de comunicação caracterizam esta rede.

II – Arquitetura de Redes de Computadores

Objetivo

Neste módulo do curso vamos abordar as arquiteturas de Protocolos TCP/IP, ISO/OSI e IEEE visando uma compreensão mais detalhada desses ambientes de rede.

Padronização dos Protocolos

Fica claro que as inúmeras maneiras pelas quais os protocolos podem ser implementados, nos leva a pensar que profundas incompatibilidades podem ocorrer entre estes pacotes de software.

Padronização dos Protocolos

Esta conclusão tem levado organismos internacionais a propor uma série de padrões para os protocolos.

Vamos a seguir conhecer mais sobre o TCP/IP, ISO/OSI e arquitetura IEEE.

Conteúdo

- > Histórico dos Protocolos TCP/IP
- > Endereçamento IP
- > Máscaras
- > Protocolos IP, ICMP, ARP, RARP
- > Camada de Transporte
- > Protocolos de Aplicação (ftp, telnet, DNS)

Conteúdo

- > Internet, WWW e Internet 2
- > Roteamento e algoritmos
- > Diferenças entre IPv4 e IPv6

HISTÓRICO TCP/IP

A importância e o potencial da tecnologia de *internetworking (inter-rede)* foi visualizada pelas agências governamentais americanas de pesquisa.

HISTÓRICO TCP/IP

Assim, nos anos 70s foi inicializado o desenvolvimento de um protocolo que pudesse interoperar diversos computadores com software/hardware

diferentes. Entre os anos 77-79 o protocolo ficou pronto e foi chamado de TCP/IP Internet Protocol Suite.

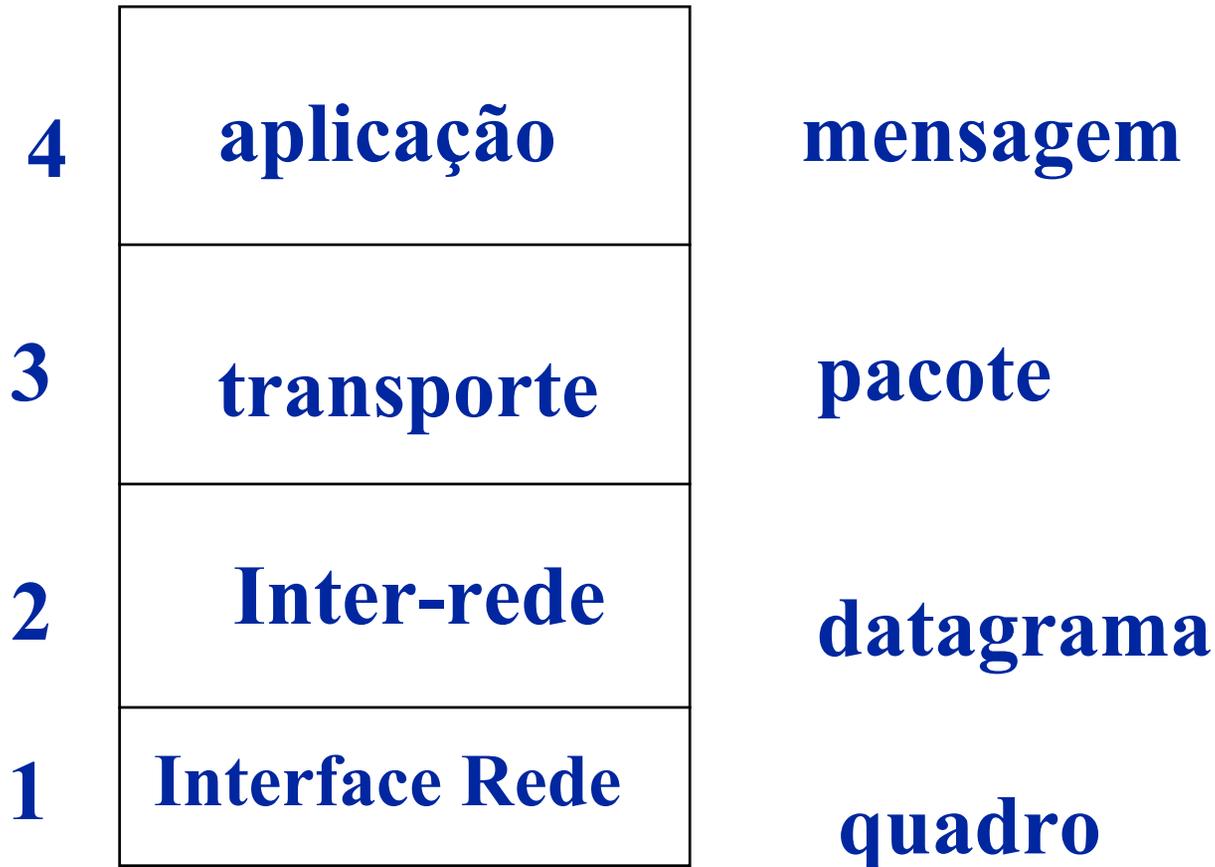
HISTÓRICO TCP/IP

Modelo TCP/IP

aplicação
transporte
internet
sub-rede

Modelo TCP/IP

Unidade de Trabalho



Modelo TCP/IP

Para o perfeito entendimento do protocolo TCP/IP, devemos compreender como este manipula endereços. O TCP/IP conhece três diferentes endereços, estes :

***1 - Hardware* - é o endereço que reside na ROM da NIC. Este endereço é único na rede e se o computador mudar, o endereço o acompanha.**

Modelo TCP/IP

2 - IP - este é um endereço lógico criado na rede Internet (classes A, B ou C), o qual é único por conexão. Este endereço são definidos como :

Classe A - 1 a 126

Classe B - 128 a 191

Classe C - 192 a 223

Classe D - 224 a 239 - reservados para multicast

Classe E - 240 a 247 - reservados para uso futuro

Modelo TCP/IP

3 - Endereço de Porta - este endereço é usado pelos protocolos de transporte (UDP e TCP). Este endereço identifica um processo de um usuário dentro do computador. O endereço tem 16 bits e é usado para identificar um serviço.

Exemplos são :

- tftp(69), bootp(67), time(37), rwho(513)
- rlogin(513), telnet (23), ftp(21), rje(77)

Modelo TCP/IP

aplicação
transporte
internet
rede

Arquitetura TCP/IP

ftp, telnet, nfs, xdr, rpc
tcp, udp
ip, icmp, arp, rarp
protocolos de hardware

Arquitetura TCP/IP

**FTP,rsh,rlogin,ftp,
telnet**

**SNMP, tftp,bootp, rpc,
xdr e nfs**

**Transmission Control
Procotol (TCP)**

**User Datagram Protocol
(UDP)**

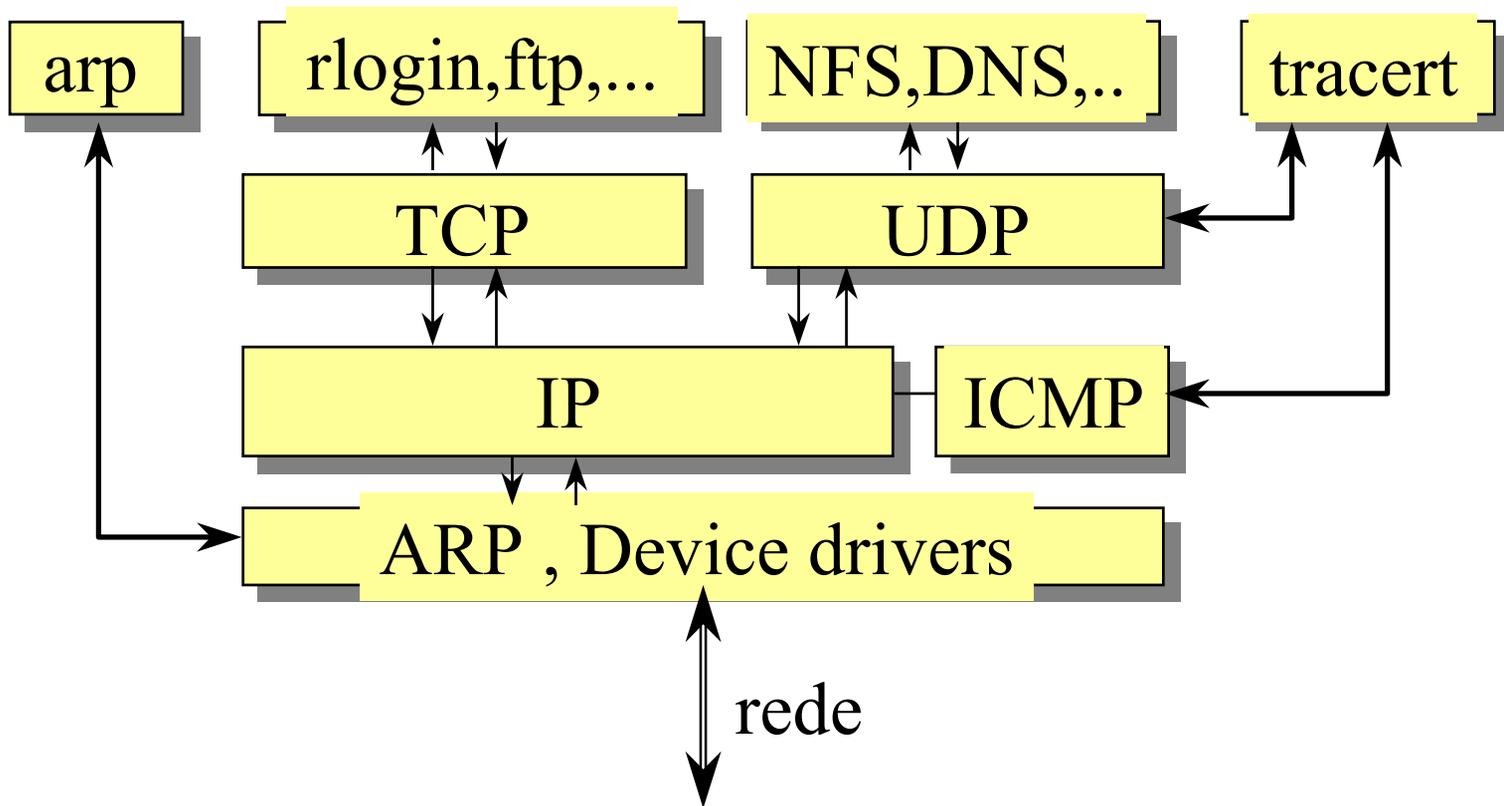
Internet Protocol (IP) + (ICMP)

**Address Resolution
Protocol (ARP)**

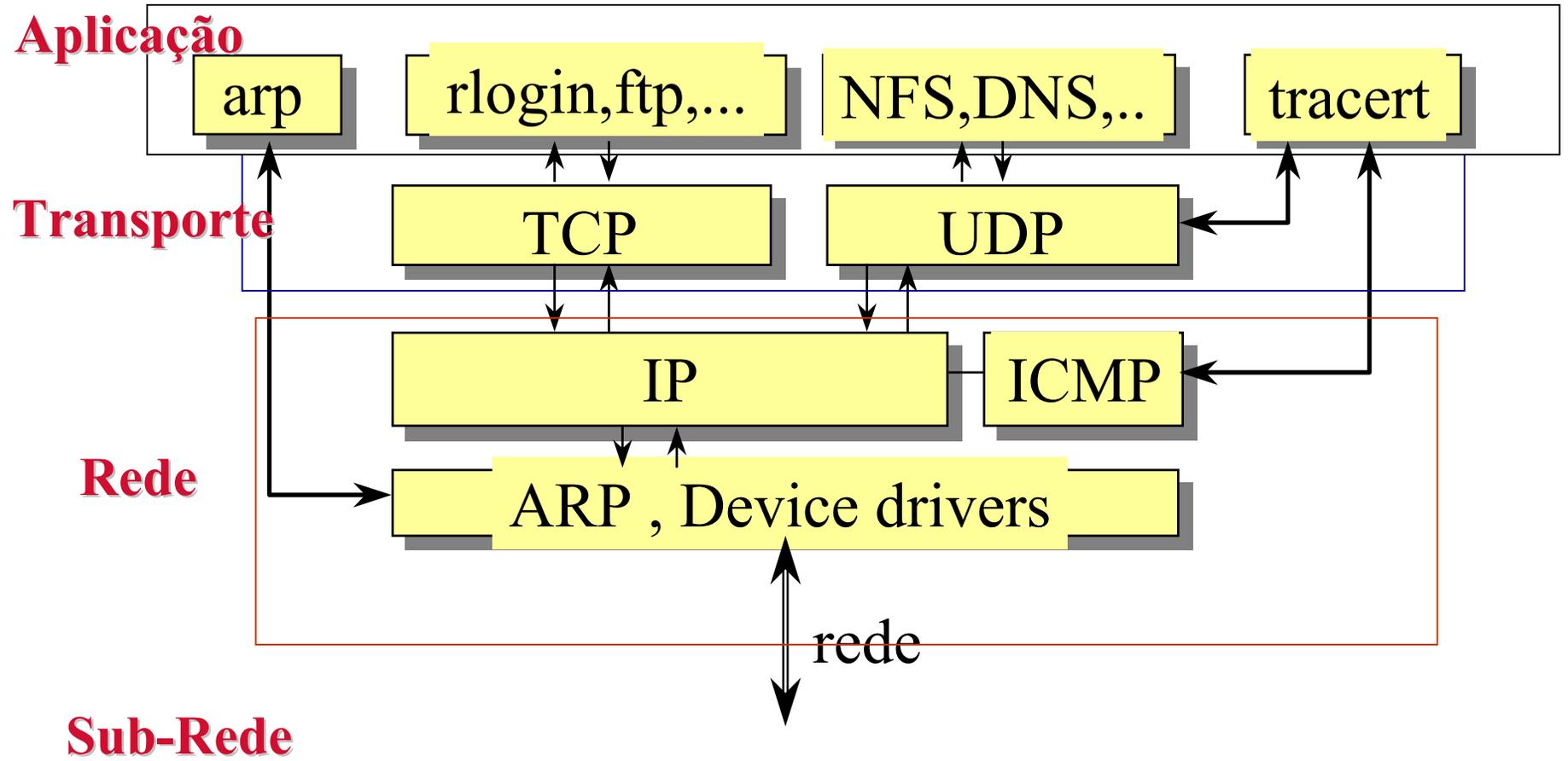
Reverse ARP (RARP)

hardware e protocolos de acesso

Família de Protocolos TCP/IP



Família de Protocolos TCP/IP



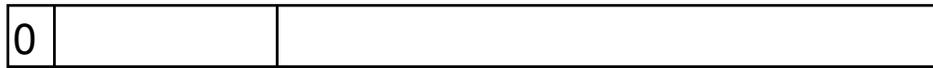
Sub-Rede de Acesso

- Ethernet, Token Ring, Token Bus ;
- FDDI, CDDI;
- X.25, Frame Relay;
- MTU (Maximum Transmission Unit).

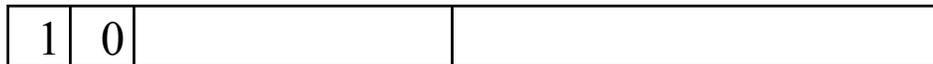
IP (Internet Protocol)

- Endereçamento IP

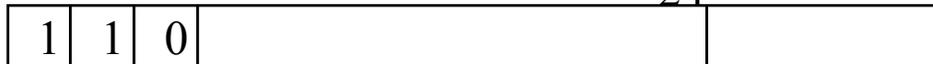
Classe A 8



Classe B 16



Classe C 24



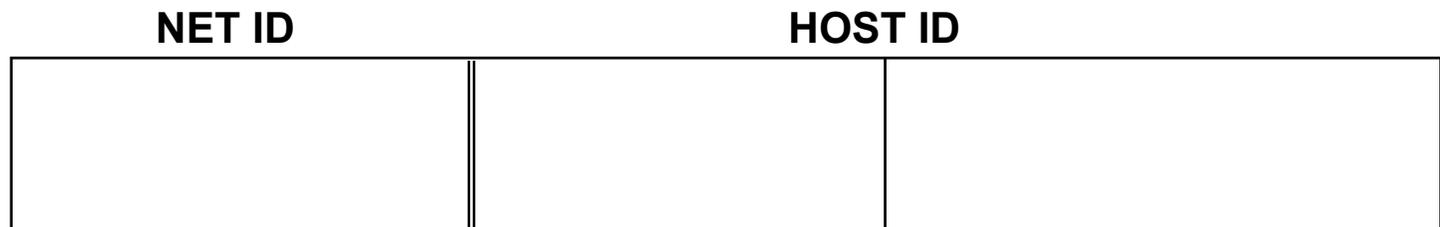
Endereçamento IP

- Classe A [0,126]
 - 0.1.0.0 (16.777.216 endereços de *hosts*)
- Classe B [128,191]
 - 164.41.14.0.0 (65.536 endereços de *hosts*)
- Classe C [192,223]
 - 196.25.15.0 (256 endereços de *hosts*)

Endereços Especiais

- Os campos Net Id e Host Id possuem significados diferentes quando possuem todos seus bits em zero (0) ou em um (1)
- Todos bits em um significa broadcast
 - Net Id: para todas as redes
 - Host Id: para todos os hosts dentro da rede
 - ex.: 192.31.235.255
- Todos bits em zero significa esta rede ou este host
 - ex.: 0.0.0.10
- LoopBack Address
 - 127.0.0.0

MÁSCARAS - Sub-redes(Subnets)



Subnet Id HOST ID (Subnet)

Máscara (Mask): usado para determinar o Net Id e o Host Id do endereço.
Os bits em um (1) representam a parte do Net Id e Subnet Id, enquanto que bits em zero (0) representam o Host Id (Subnet)

ex.: Classe B 143.54.0.0

Sub-rede A: 143.54.10.0

Sub-rede B: 143.54.20.0

Máscara: 255.255.255.0

Indústria X

Administração

Fabrica

Marketing/Vendas



Computadores

Indústria X
(128.7.0.0)

Administração (128.7.254.0)	Fabrica (128.7.253.0)	Marketing/Vendas (128.7.252.0)
--------------------------------	--------------------------	-----------------------------------



Computadores

Indústria X
(128.7.0.0)

Administração (128.7.254.0)	Fabrica (128.7.253.0)	Marketing/Vendas (128.7.252.0)
--------------------------------	--------------------------	-----------------------------------

128.7.254.12
Lúcia



128.7.253.4
Mario



128.7.252.55
John

128.7.254.56
João



128.7.253.1
Lula



128.7.252.65
Carol

128.7.254.64
Maria



128.7.253.2
Libanês



128.7.252.89
Catherin

Computadores

Classe de END.	Máscara Default (Binária)	Máscara Default (Decimal)
A	11111111.00000000.00000000.00000000	255.0.0.0
B	11111111.11111111.00000000.00000000	255.255.0.0
C	11111111.11111111.11111111.00000000	255.255.255.0

Como funcionam as máscaras da Subrede ?

As máscaras são calculadas através da operação do AND lógico sobre endereços envolvidos na rede que desejam se comunicar. Assim, observe o exemplo dos endereços.

Caso 1 - Considere o endereço da funcionária Lúcia, 128.7.254.12. Como a máscara para uma rede da classe B é 255.255.0.0, teríamos a seguinte operação :

```
11111111.11111111.00000000.00000000
10000000.00000111.11111110.00001100
-----
10000000.00000111.00000000.00000000 (128.7.0.0)
```

Como funcionam as máscaras da Subrede ?

Caso 2 - Considere o endereço da funcionário Mario, 128.7.253.4.
Como a máscara para uma rede da classe B é 255.255.0.0, teríamos a seguinte operação :

11111111.11111111.00000000.00000000

10000000.00000111.11111101.00000100

10000000.00000111.00000000.00000000 (128.7.0.0)

Como funcionam as máscaras da Subrede ?

Caso 3 - Considere o endereço da funcionária Catherin, 128.7.252.89.
Como a máscara para uma rede da classe B é 255.255.0.0, teríamos a seguinte operação :

11111111.11111111.00000000.00000000

10000000.00000111.11111100.01011001

10000000.00000111.00000000.00000000 (128.7.0.0)

Como funcionam as máscaras da Subrede ?

Vamos agora considerar os Casos anteriores com uma máscara 255.255.255.0.

Caso 1 - Considere o endereço da funcionária Lúcia, 128.7.254.12.
Como a máscara para uma rede da classe B é 255.255.255.0, teríamos a seguinte operação :

```
11111111.11111111.11111111.00000000
10000000.00000111.11111110.00001100
-----
10000000.00000111.00000000.00000000 (128.7.254.0)
```

Como funcionam as máscaras da Subrede ?

Caso 2 - Considere o endereço da funcionário Mario, 128.7.253.4.
Como a máscara para uma rede da classe B é 255.255.255.0, teríamos a seguinte operação :

11111111.11111111.11111111.00000000

10000000.00000111.11111101.00000100

10000000.00000111.00000000.00000000 (128.7.253.0)

Como funcionam as máscaras da Subrede ?

Caso 3 - Considere o endereço da funcionária Catherin, 128.7.252.89.
Como a máscara para uma rede da classe B é 255.255.255.0, teríamos a seguinte operação :

11111111.11111111.11111111.00000000

10000000.00000111.11111100.01011001

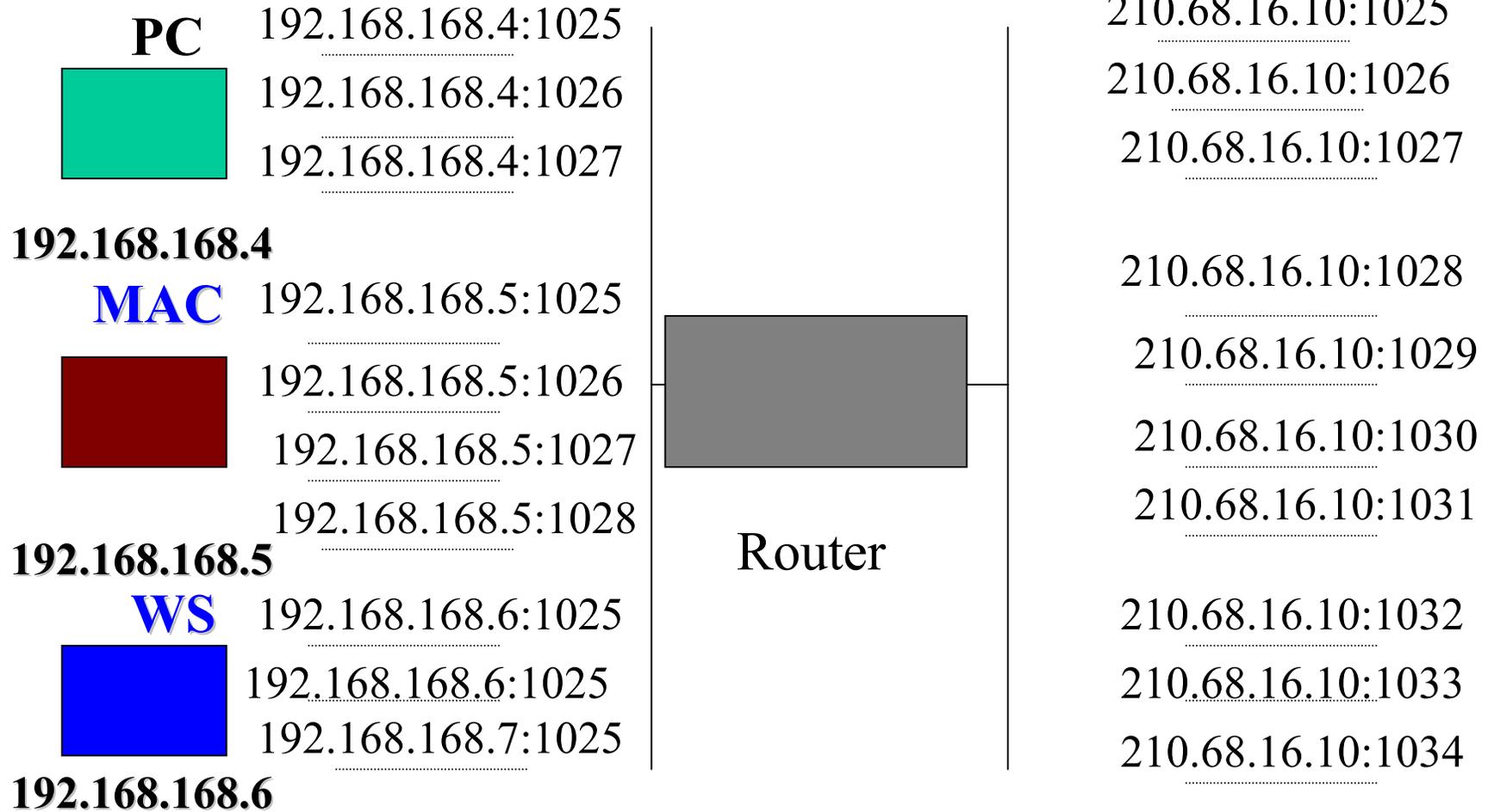
10000000.00000111.00000000.00000000 (128.7.252.0)

Roteamento e Tradução de Endereços

Roteamento - permite que um dispositivo, ou processo, enviar informação entre *hosts* numa rede.

Tradução de Endereços - permite que uma rede *pequena* seja vista pela *Internet* como um simples nó. Desta forma, um único endereço IP (ou um conjunto pequeno de endereços) poderá ser compartilhado pela rede. Este aspecto pode prover dentre outras características uma proteção contra intrusos na rede.

Roteamento e Tradução de Endereços



Exemplo Sub-rede

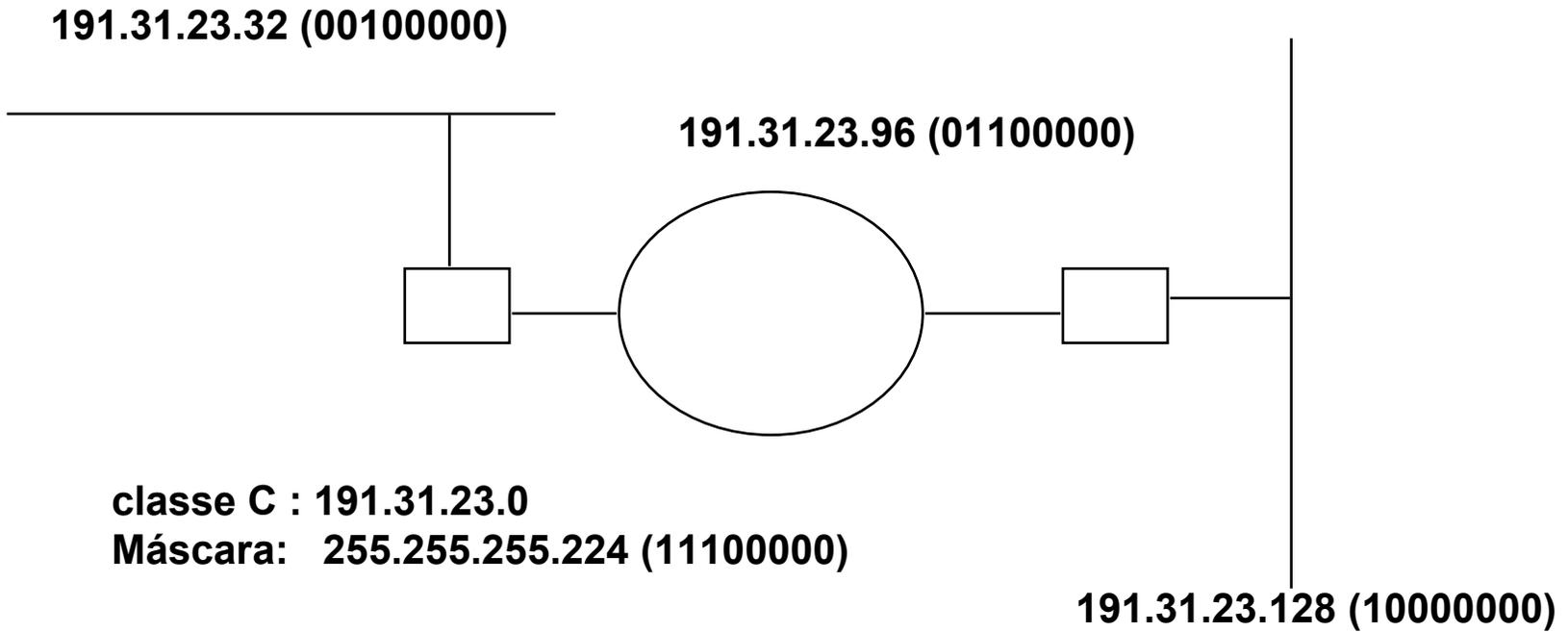


Tabela de Rotas

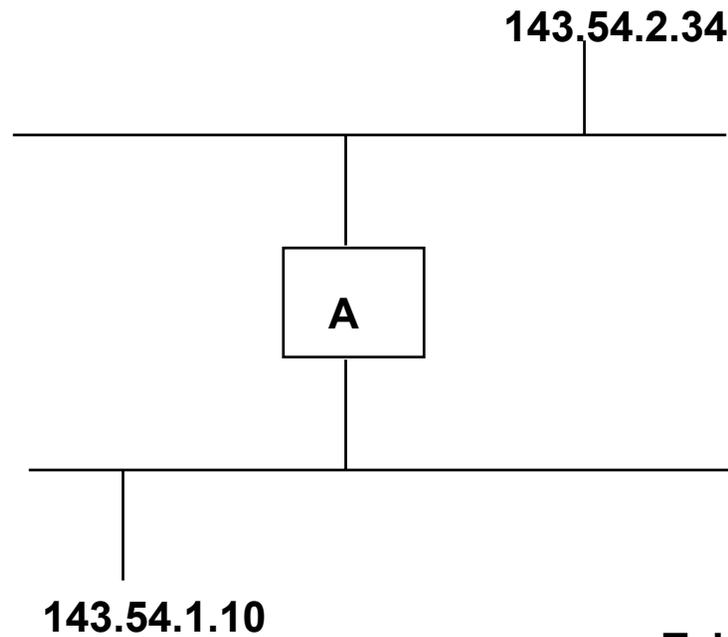


Tabela de rotas de A

rede	gateway
143.54.10.0	143.54.2.34
143.54.100.0	143.54.1.10
200.17.164.0	143.54.1.10

IP

Vers	HLEN	Service Type	Total Legth	
Identification			Flags	Offset
TTL	Protocol		CheckSum	
Source IP				
Destination IP				
Options				PAD
DADOS				

Campos IP

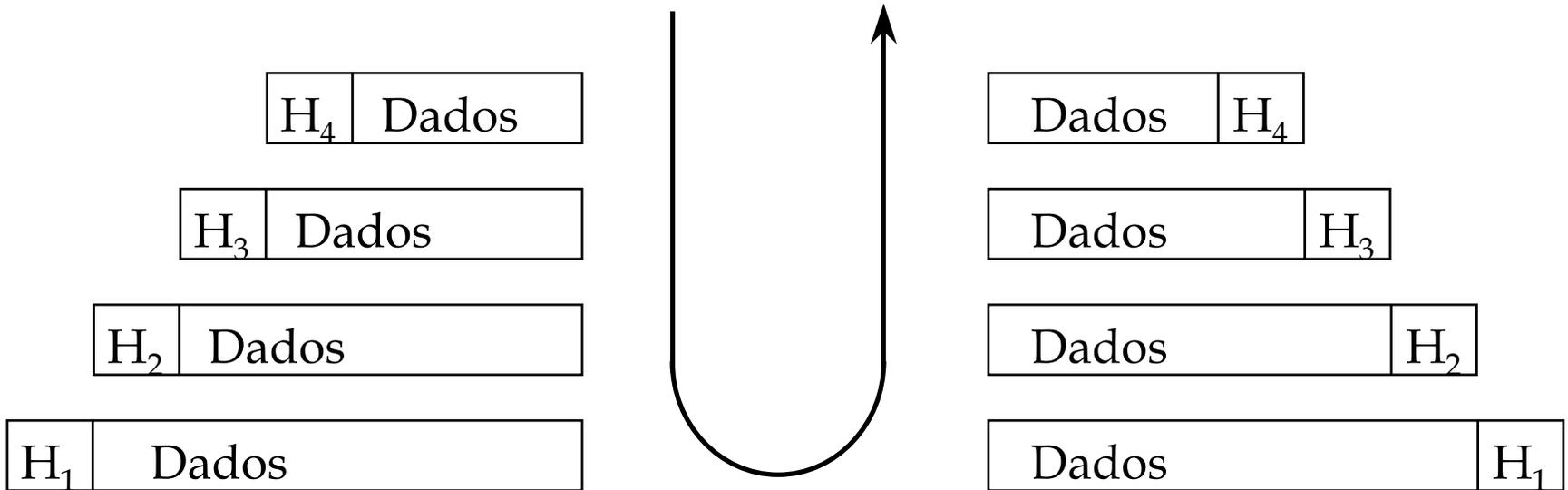
- **Vers:** versão do IP utilizada. Versão atual é a 4
- **Hlen:** tamanho do cabeçalho do datagrama
- **Service Type:** especifica qual a forma de se lidar com o datagrama. Possui 8 bits que indicam os seguintes requisitos:
 - Precedência
 - Mínimo de atraso na transmissão
 - Alto Throughput
 - Alta confiabilidade
- **Total Len:** tamanho total do datagrama

Encapsulamento do Datagrama

- Os datagramas podem ser fragmentados devido ao MTU da sub-rede
- Tamanho máximo de 65531 octetos
- Os campos Identification, Flags e Fragment Offset são usados na fragmentação

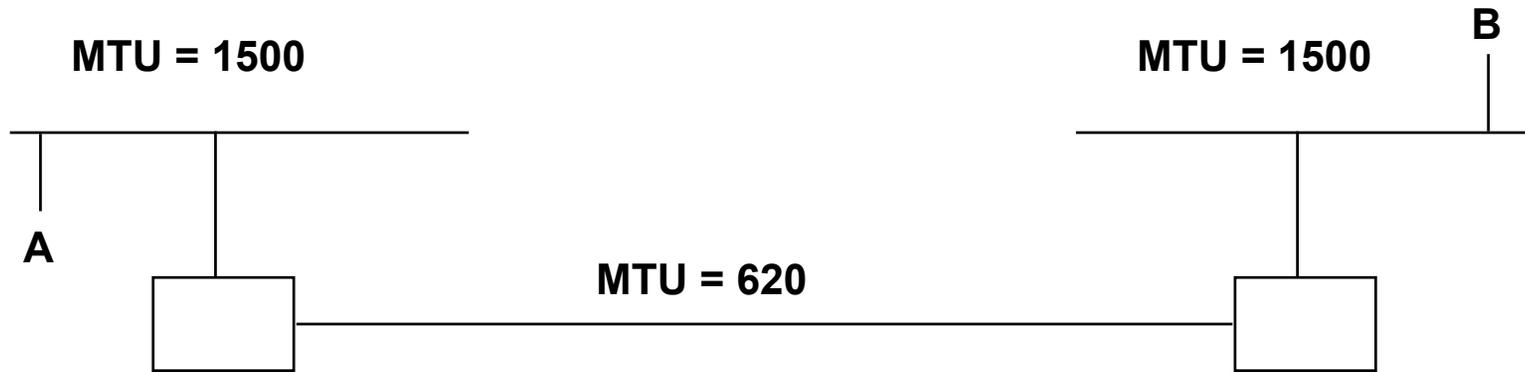
Encapsulamento do Datagrama

- Quebra em pacotes
- Tráfego de sequência de bits



H_x - Cabeçalho (Header) - Controle
Dados - Não tratado pelo nível x

Encapsulamento do Datagrama



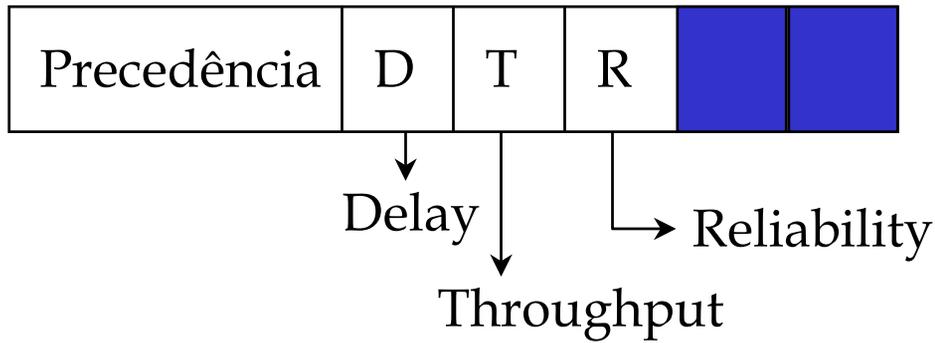
Datagrama de 1400 octetos : A -> B

	Identification	Flags	Offs
Frag1:	xxxx	010	0
Frag2:	xxxx	010	600
Frag3:	xxxx	001	1200

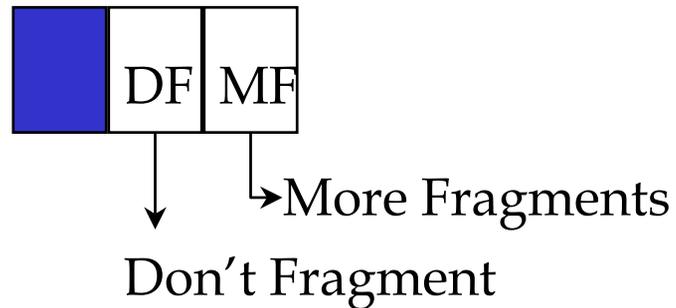
- Fragmentos só são remontados no host destino

Datagrama IP

Tipo de Serviço



Flags



Campos IP

- TTL (Time To Live): número máximo de gateways que um datagrama pode passar. Cada gateway ao repassar um datagrama decrementa de um este valor, caso resulte em zero, o datagrama é descartado
- Protocol: tipo do protocolo encapsulado no datagrama
- CheckSum: garante a integridade dos dados
- Source IP: endereço da máquina emissora do datagrama
- Destination IP: endereço da máquina destino do datagrama

Campo de Opções

- Registro de rota
- Especificação de rota
- Tempo de Processamento de cada gateway
- ...
 - Opção COPY/Fragmentação

Processamento no Roteador

- Se o roteador não tem memória suficiente, o datagrama é descartado
- Verificação do Checksum, versão, tamanhos
 - O Checksum é recalculado, se for diferente do datagrama, este é descartado
- Decremento do TTL
 - se zero, o datagrama é descartado

Processamento no Roteador

- Pode -se considerar o campo Service Type
- Se for necessário e permitido, o datagrama pode ser fragmentado. Cria-se um cabeçalho para cada fragmento, copiando as opções, aplicando o novo TTL e o novo Checksum
- Tratamento do campo opção
- Repasse para a sub-rede destino

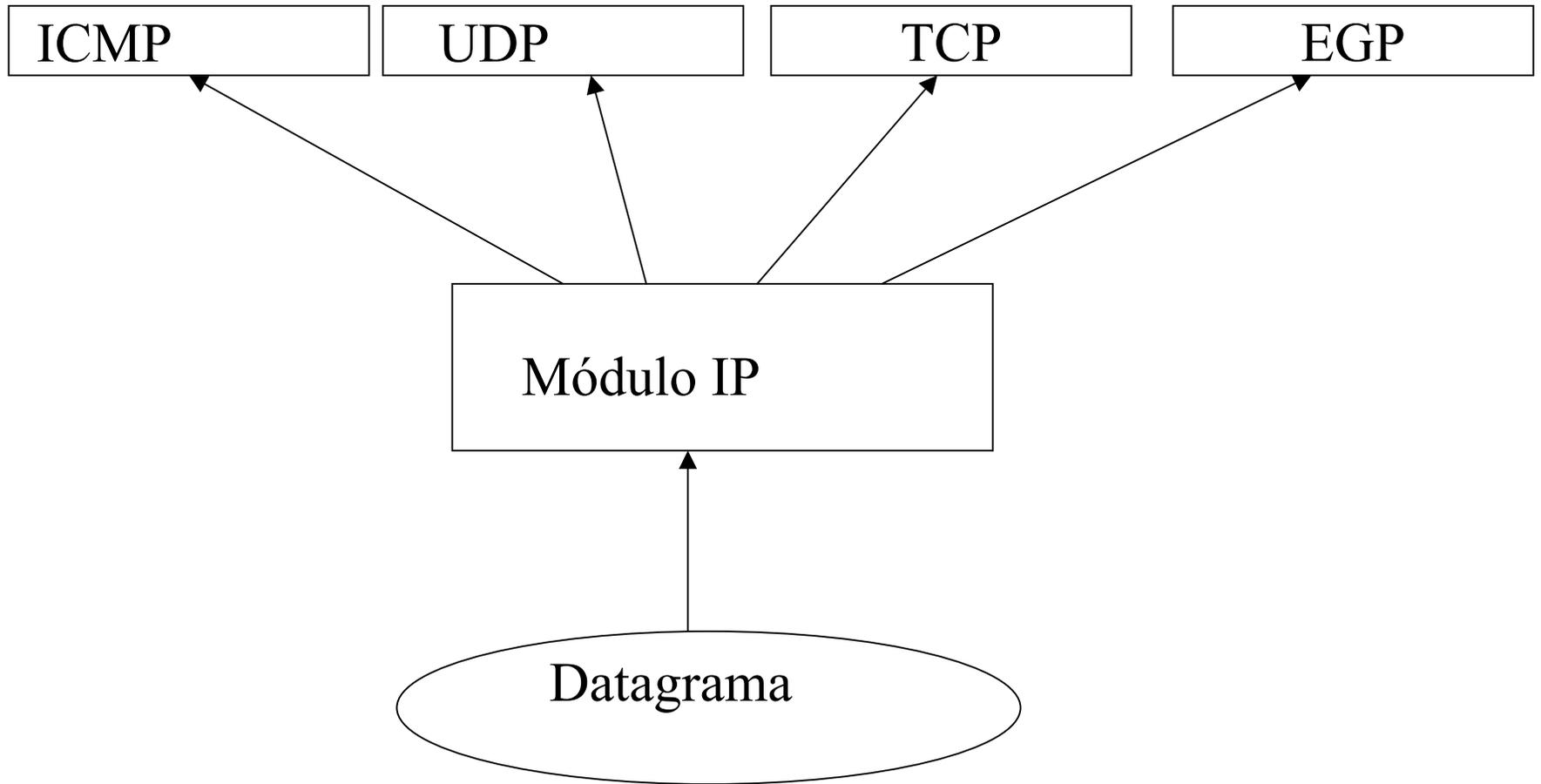
Processamento no Host Destino

- Verificação do Checksum, versão, tamanhos
 - O Checksum é recalculado, se for diferente do datagrama, este é descartado
- Se o datagrama é fragmentado, é disparado um temporizador que evitará o espera indefinida dos outros fragmentos do datagrama original
- Entrega do campo de dados do datagrama para o processo indicado no campo Protocol

Recursos Críticos para o Desempenho IP

- Largura de banda disponível
- Memória disponível para buffers
- Processamento da CPU

Demultiplexação na camada de rede



Protocolo IP - Multiplexação

- Convenção para auto identificação dos datagramas

Protocol	Serviço
0	IP - pseudo
1	ICMP
6	TCP
17	UDP

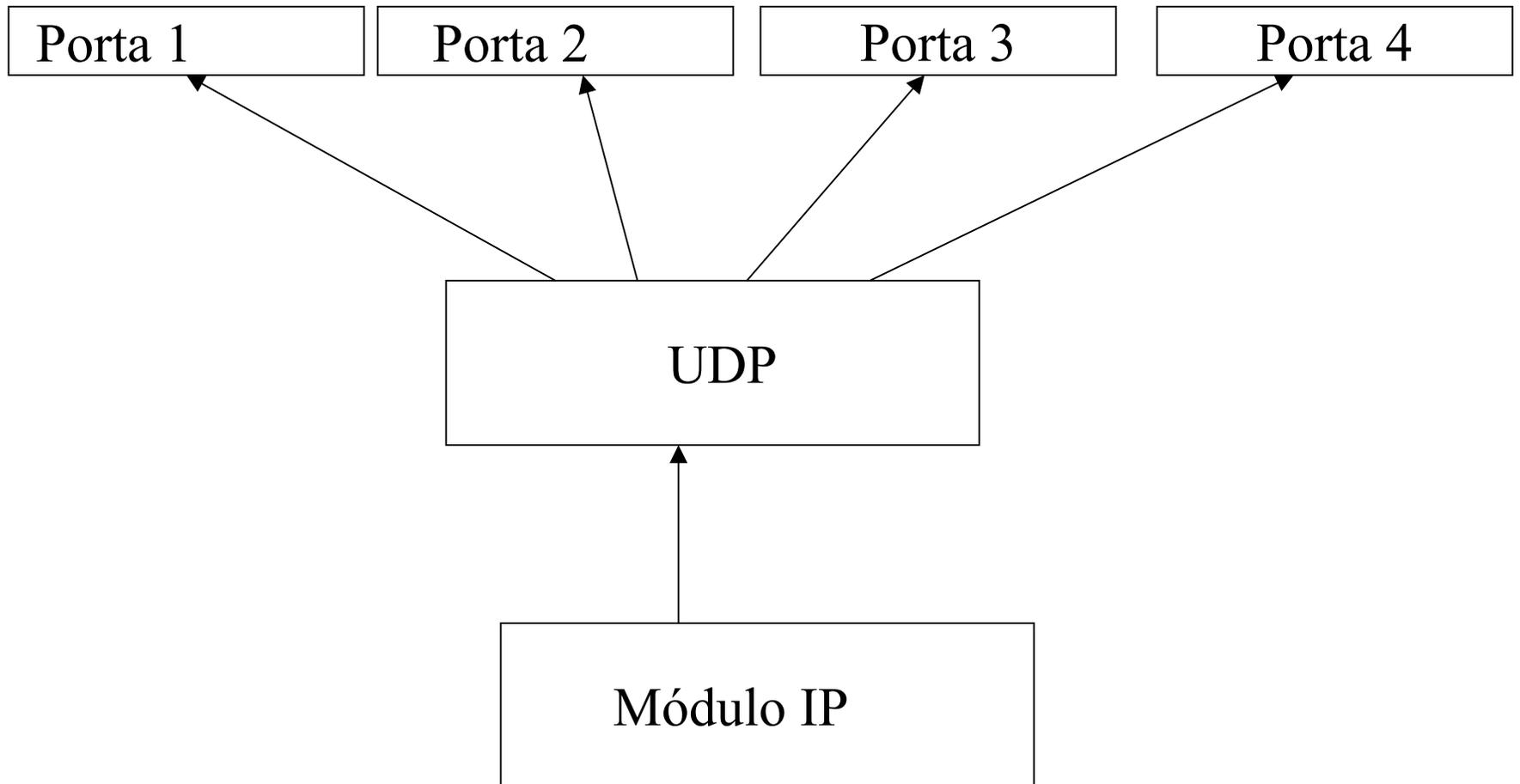
UDP (User Datagram Protocol)

- Protocolo de transporte não orientado à conexão
- Não implementa nenhum mecanismo de recuperação de erros
- São identificados os processos origem e destino através do conceito de porta
- O campo de CheckSum é opcional

UDP

Source Port	Destination Port
Message Length	Checksum
Dados	

Demultiplexação na camada de Transporte



TCP (Transmission Control Protocol)

- Protocolo de transporte orientado à conexão
- Implementa mecanismos de recuperação de erros
- Usa o conceito de porta
- Protocolo orientado a stream

TCP (Transmission Control Protocol)

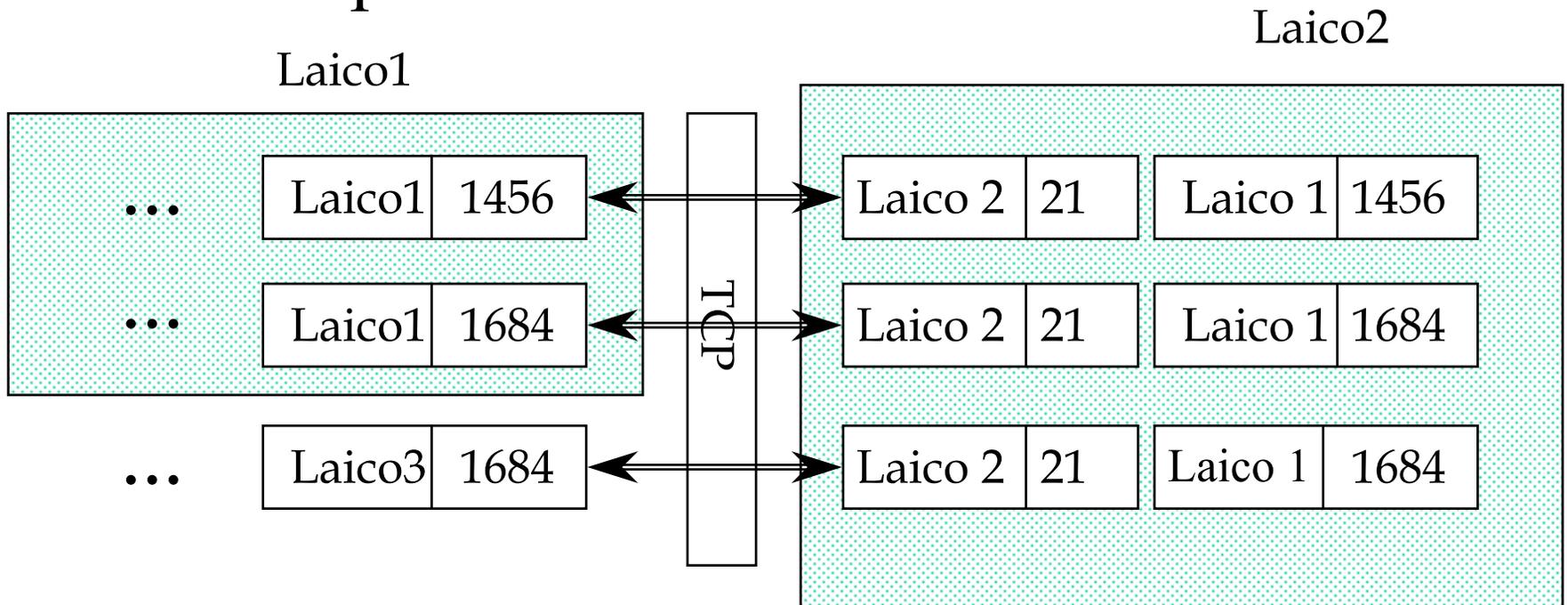
- Usado para aplicações cliente-servidor, serviços críticos,...
- Faz a multiplexação de mensagens para as aplicações
- Conexão (IP,port) <--> (IP,port)
Permite múltiplas sessões do mesmo serviço

Janela Deslizante

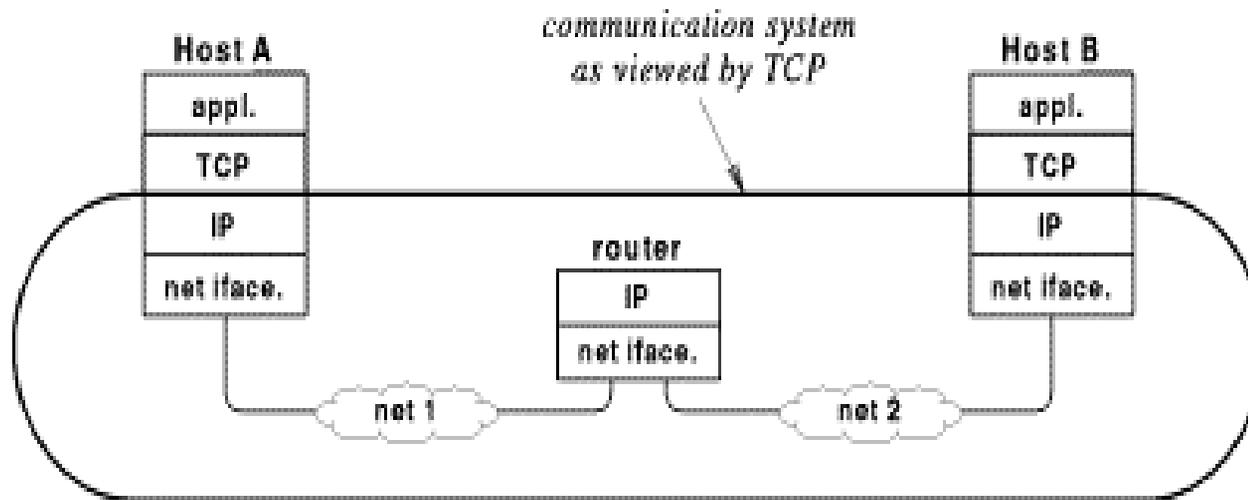
- Cada octeto é numerado
- O tamanho da janela determina o número de octetos que podem ser transmitidos sem reconhecimento
- Através do mecanismo de PIGGYBACK pode-se reconhecer um bloco de octetos via um segmento de dados

TCP - Exemplo

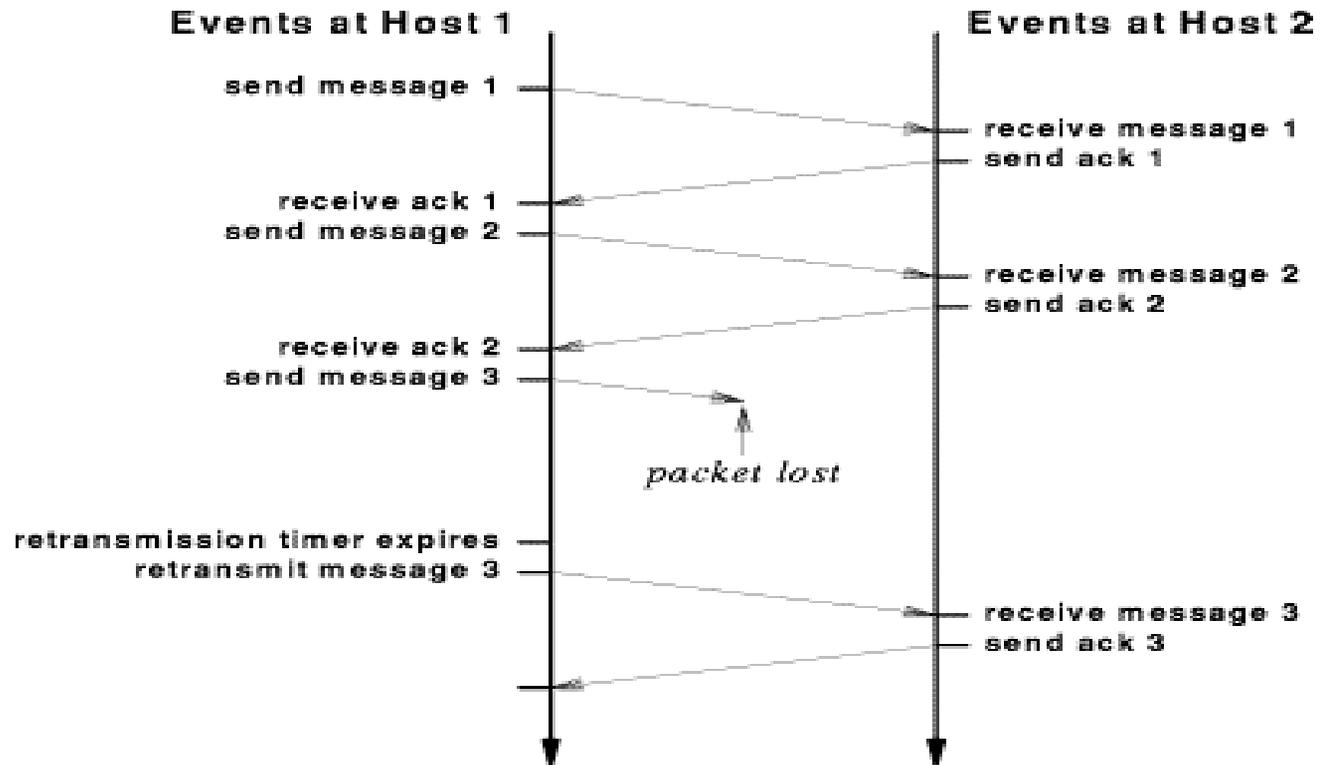
- FTP - port 21



TCP - Visão de comunicação

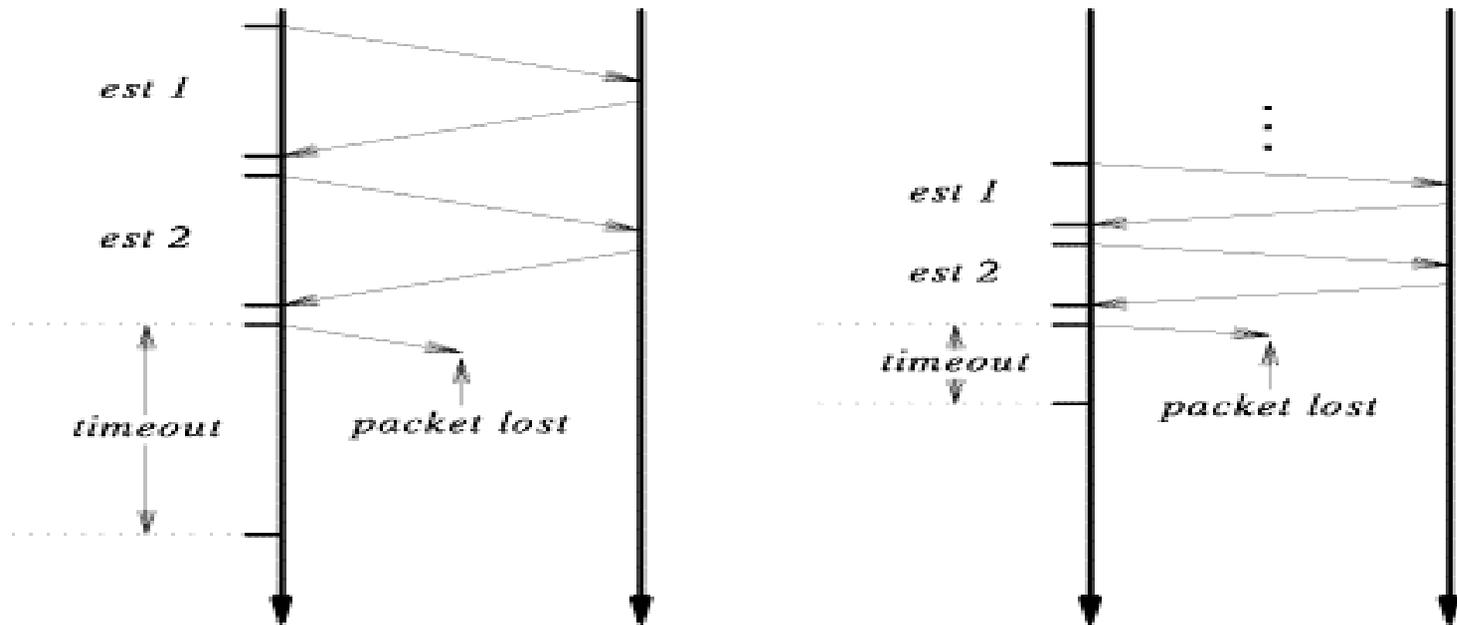


TCP - Confiabilidade

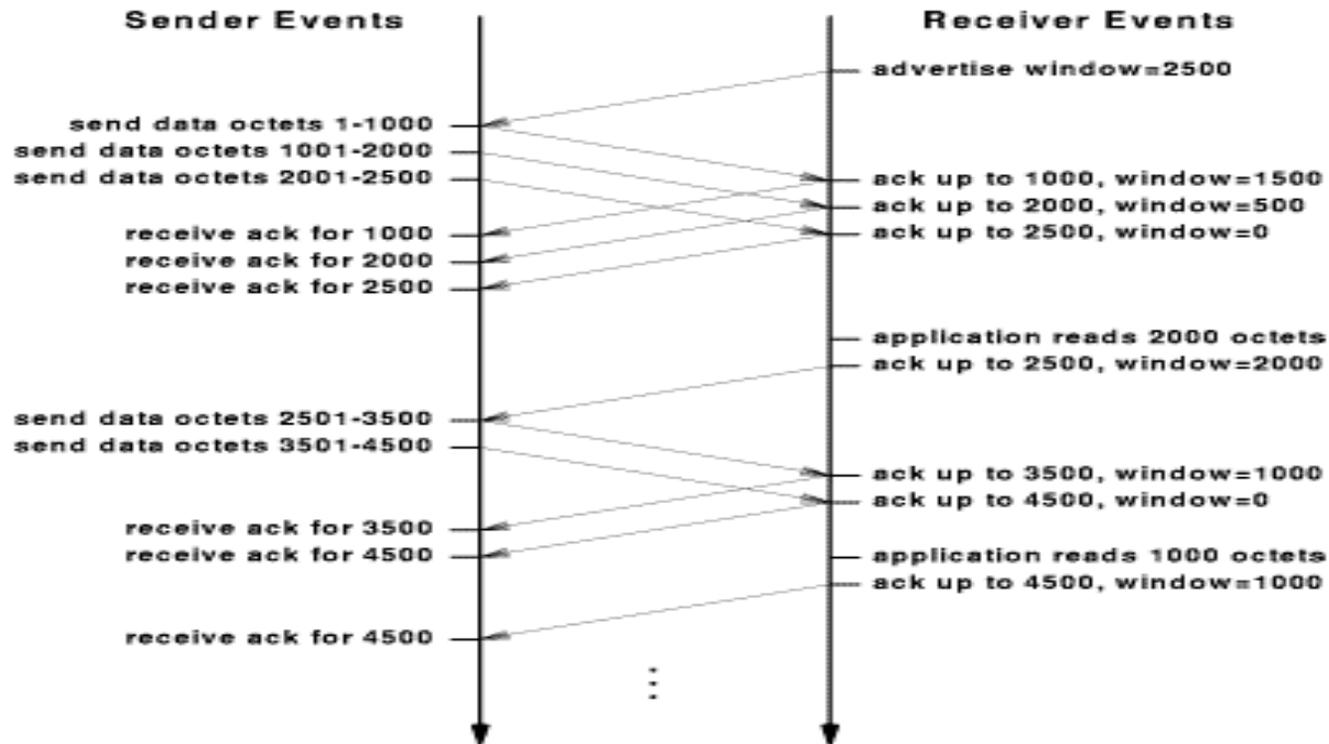


TCP - timeout adaptativo

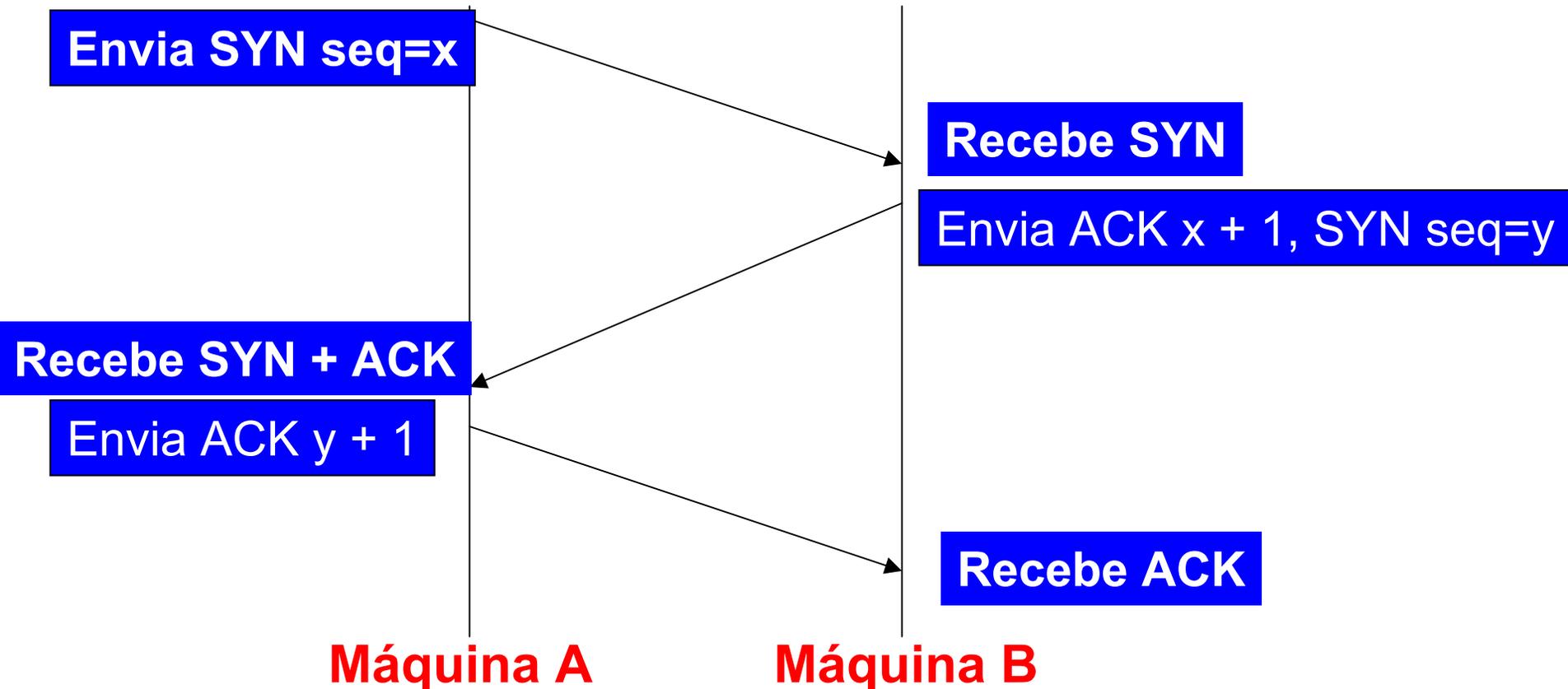
- Verifica o tempo de resposta e ajusta o timeout



TCP - Janela deslizante

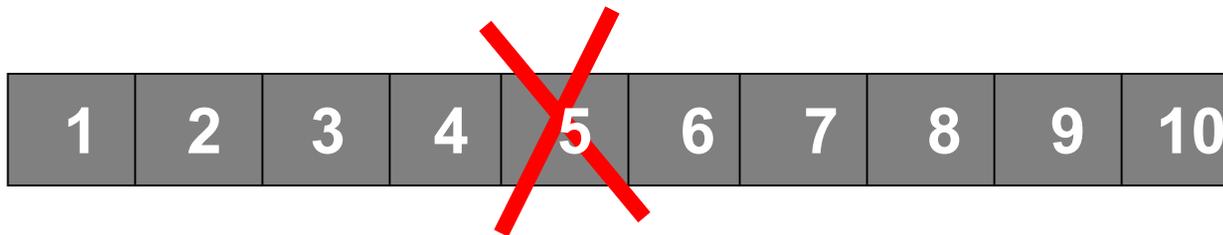


TCP - Estabelecimento de Conexão



TCP - Reconhecimento e retransmissão

Go-back-n x Retransmissão seletiva



Go-back-n

5 6 7 8 9 10

Retransmissão seletiva

5

Diferenças entre IPv4 e IPv6

Introdução

O protocolo IPv6 mantém muitas das funções do IPv4, e que foram responsáveis pelo sucesso da Internet. Alguns exemplos destas características são :

- entrega de datagrama não confiável;
- permite que o remetente escolha o tamanho do datagrama;
- requer que o número de *hops* seja estabelecido no remetente.

- Apesar da similaridade ser verificada em vários pontos nos protocolos IPv4 e IPv6, o novo protocolo adota mudanças significativas.

Exemplo de modificações consideradas no IPv6 são o tamanho de endereçamento e algumas facilidades adicionais (como uma maior flexibilidade para o uso da QoS).

As modificações que foram implementadas no IPv6 podem ser agrupadas em cinco grandes grupos :

- Maior endereço : é uma das características mais marcante da nova versão do IP. O IPv6 quadruplicou o tamanho do IPv4 de 32 bits para 128 bits (*esta expansão foi projetada para atender um futuro ainda não imaginado*) ;

- Formato de cabeçalho flexível : o formato do datagrama IP não é compatível com o antigo datagrama IPv4. A abordagem foi implementar um formato com uma série de cabeçalhos adicionais. Em outras palavras, diferente do IPv4 onde é usado um tamanho fixo para o formato onde os campos têm tamanhos fixos;
- Opções melhoradas : as opções disponíveis no IPv6 são mais poderosas quando comparadas com o IPv4;

- Suporte para reserva de recursos : existe um mecanismo que permite a alocação prévia de recursos da rede. Desta forma, aplicações como vídeo em tempo real que necessitam de uma garantia de largura de banda e baixo retardo podem ser atendidas;
- Previsão para uma extensão do protocolo : esta característica é tida por muitos como a maior melhoria. Em outras palavras, existe uma flexibilidade de expansão do protocolo para novas realidades. De forma oposta ao IPv4, onde existe uma especificação fechada e *completa* do protocolo.

ENDEREÇAMENTO IPv6

O endereço do protocolo IPv6 é composto de 16 octetos. A idéia do tamanho do endereço pode ser mensurada pela afirmação :

Cada pessoa no globo poderá ter suficiente endereço para ter a sua própria Internet, tão grande quanto a Internet atual.

Um endereçamento de 16 octetos representam 2^{128} valores válidos de endereços. Em outras palavras, o tamanho de endereços é da ordem de 3.4×10^{38} .

Se os endereços fosse alocados a uma taxa de um milhão de endereços a cada micro-segundo, teríamos que ter vinte anos para que todos os endereços fossem alocados.

Notação do Endereço IPv6

Devido a dificuldade dos humanos de trabalhar com endereços binários, e grandes, o grupo responsável pelo endereçamento do IPv6 imaginou uma nova notação, *colon hex*.



O que vem a ser isto ?

Colon Hex

é uma representação caracterizada por valores hexadecimais separados por dois pontos. Assim teríamos para o exemplo genérico a seguir:

Decimal

255.255.10.150.128.17.0.0.255.255.255.255.100.140.230.104

Colon Hex

FFFF:A96:8011:0:FFFF:FFFF:648C:E668

Colon Hex

A notação tem claras vantagens, por solicitar menos dígitos e menos separadores. Outras duas vantagens desta abordagem são seguintes técnicas:

- *Compressão de zeros* - em exemplo pode ser o endereço

FF05:0:0:0:0:0:0:B3

Este endereço pode ser representado como :

FF05::B3

Esta técnica somente pode ser usada uma vez num endereço.

Colon Hex

- A abordagem de *colon hex* permite que adotemos a sintaxe de sufixo decimal com ponto. O objetivo é a manutenção da compatibilidade de transição entre o IPv4 e o IPv6.

Exemplo :

0:0:0:0:0:0:0:128.10.2.1

Como seria o uso da técnica de compressão de zeros para este endereço ?



Como seria o uso da técnica de compressão de zeros para este endereço ?



Resposta

:: 128.10.2.1

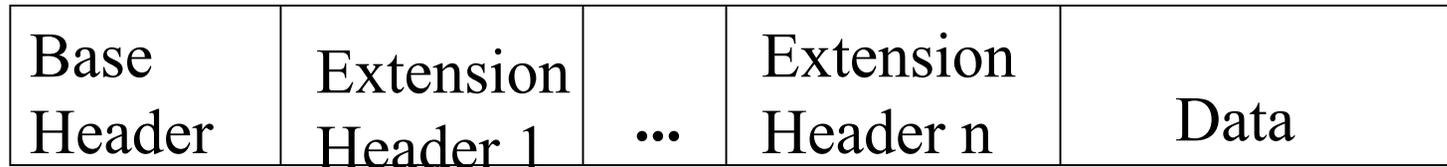
Tipos de Endereços Básicos do IPv6

Os endereços de destino num datagrama no IPv6 tem as seguintes três categorias:

- *Unicast* - o endereço especifica um *host simples* (*computador ou roteador*) que o datagrama deverá ser enviado pelo menor caminho ;
- *Cluster* - o destino é um conjunto de computadores que compartilham um único prefixo de endereço (todos conectados a uma mesma rede física). O datagrama deverá ser encaminhado para o grupo e entregue a um membro do grupo (o mais perto possível).

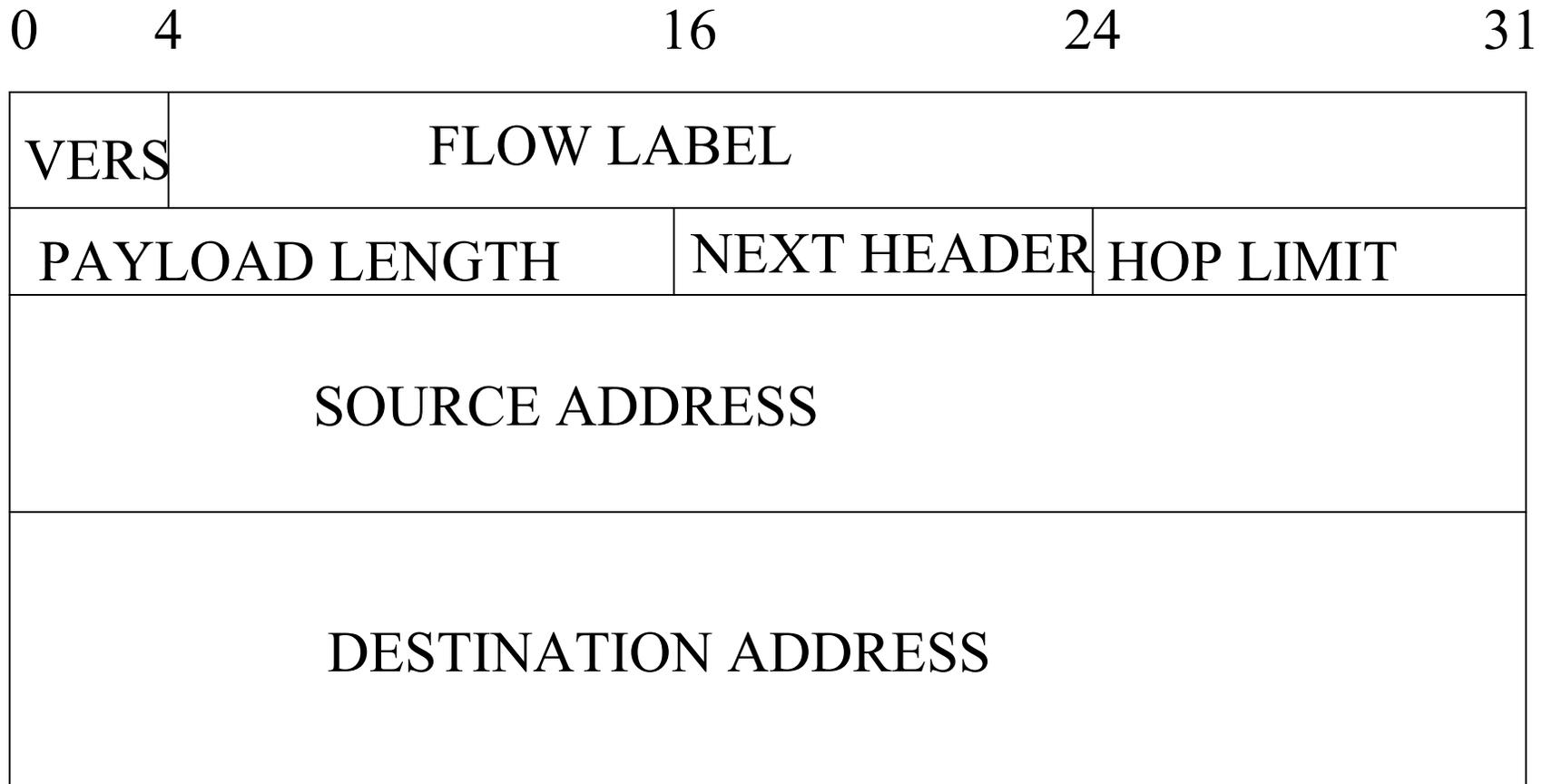
- *Multicast* - o destino é um conjunto de computadores, possivelmente em locais diferentes. Assim o datagrama deverá ser entregue para cada membro do grupo multicast usando facilidade de multicast de hardware, ou broadcast se possível.

Forma Geral do Datagrama IPv6



A figura acima ilustra uma forma geral um datagrama IPv6 genérico. Somente o campo do cabeçalho básico é necessário, os demais são opcionais.

O formato do IPv6 base header é ilustrado abaixo :



FLOW LABEL

Este campo permite que os pacotes que tenham que ter um tratamento diferenciado sejam assim tratados.

O campo tem tamanho de 20 bits, composto do endereço de origem e IP destino, permitindo que os roteadores mantenham o estado durante o fluxo ao invés de estimar a cada novo pacote.

As aplicações são obrigadas a gerar um *flow label* a cada nova requisição. O reuso do *flow label* é permitido quando um fluxo já está terminado ou foi fechado.

FLOW LABEL

A utilização de campo *flow label* prove aos roteadores uma maneira fácil de manter as conexões e manter o fluxo de tráfego numa mesma taxa.

PRIORITY

A utilização do campo *priority* prove aos programas a facilidade de identificar a necessidade de tráfego que os estes necessitam.

O uso efetivo, ou normalização, de como este campo junto com o *flow label* devem plenamente operar ainda estão em discussão.

O campo de 8-bits destinado a *Classe* está no momento a nível de desenvolvimento. Todavia, os 4 bits de prioridade podem nos ajuda a entender o que poderemos ter pela frente.

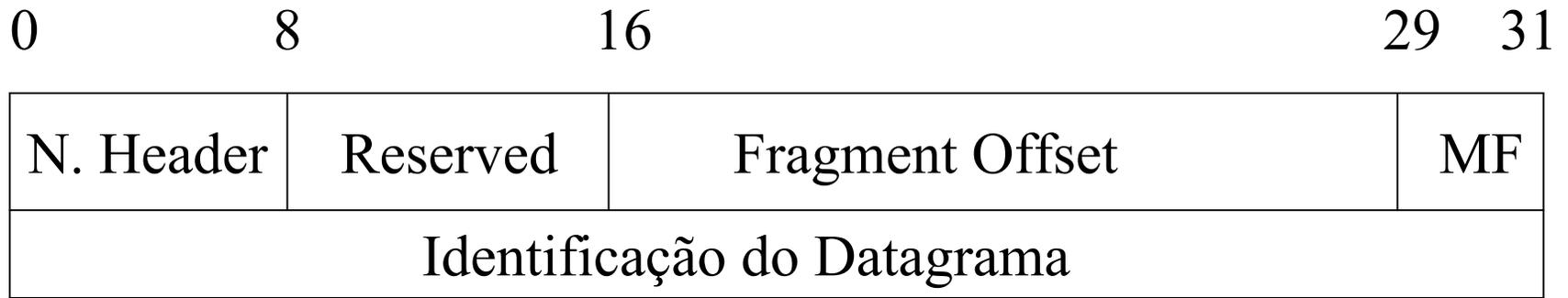
IPv6 Priority Values

Valor	Descrição
0	Tráfego sem características
1	Tráfego Filler (fluxo contínuo de informação onde o tempo particularmente não interessa)
2	Transferência de dados sem supervisão (ex. e-mail)
3	Reservado
4	Transferência grande de dados com supervisão (ex. HTTP, FTP e tráfego NFS).

IPv6 Priority Values

Valor	Descrição
5	Reservado
6	Tráfego Interativo (ex. telnet)
7	Tráfego de Controle da Internet (informação usada por dispositivos que fazem parte da Internet, como roteadores, switches e dispositivos que empregam o SNMP para reportar estados).
8-15	Pacotes em processos que não podem controlar congestionamentos. Pacotes com valor 8 serão descartados antes do de valor 15.

IPv6 fragment extension header é ilustrado



Distribuição de Endereços IPv6

A forma de distribuição dos endereços têm gerado muitas discussões. As discussões ficam baseadas em dois pontos principais :

- Como fazer a gerência de distribuição dos endereços ?
- Como mapear um endereço para um destino ?

Como fazer a gerência de distribuição dos endereços ?

Esta discussão é baseada em qual autoridade deve ser criada para gerenciar a distribuição de endereços.

Na Internet atual temos dois níveis de hierarquia. Em outras palavras, temos um primeiro nível que é responsabilidade da autoridade da Internet. No segundo nível é responsabilidade da organização.

O IPv6 permite múltiplos níveis. Existe uma proposta em tipos de níveis do IPv6 semelhante ao IPv4.

Como fazer a gerência de distribuição dos endereços ?

010	Provider ID	Subscriber ID	Subnet ID	Node ID
-----	----------------	------------------	--------------	---------

010 - tipo de endereço, no caso 010 é um endereço que diz o tipo de provedor auferido;

Provider ID - identificação do provedor

Subscriber ID - identificador do assinante

Subnet ID - informação da rede do assinante

Node ID - informação sobre um nó do assinante.

Como mapear um endereço para um destino ?

Esta pergunta deve ser respondida com o desempenho com meta. De um outra forma, a eficiência computacional deverá ser levada em conta. Independente de autoridades na rede, um datagrama deverá ser analisado e os melhores caminhos deverão ser escolhidos.

TCP - Parâmetros

- MSS - Maximum segment Size
- Padronização de ports
- Controle de Congestionamento

Port	Serviço
15	netstat
21	ftp
23	telnet
25	smtp (mail)

TCP

Source Port		Destination Port	
Sequence Number			
Ack Number			
Hlen	Reserved	Cod Bits	Window
CheckSum		Urgent Pointer	
Opções			
Dados			

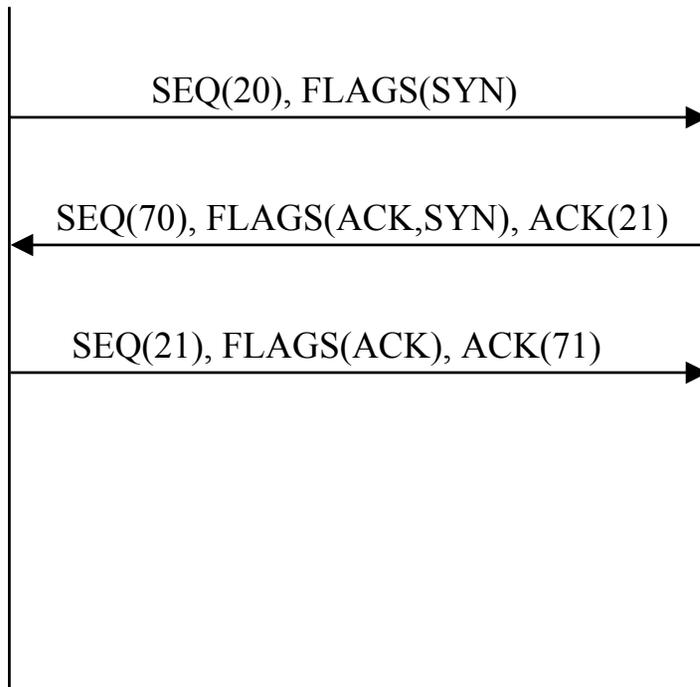
Campos do TCP

- **Portas:** identificam os processos origem e destino
- **Número de sequência:** número do primeiro octeto do campo de dados
- **Número do ACK:** número do octeto que é esperado pelo destino, sendo todos os octetos de número inferior reconhecidos
- **HLEN:** Tamanho em bytes do cabeçalho TCP
- Bytes de código: URG, ACK, PSH, RST, SYN, FIN
- **Window:** Tamanho em octetos da janela que é aceito pelo emissor

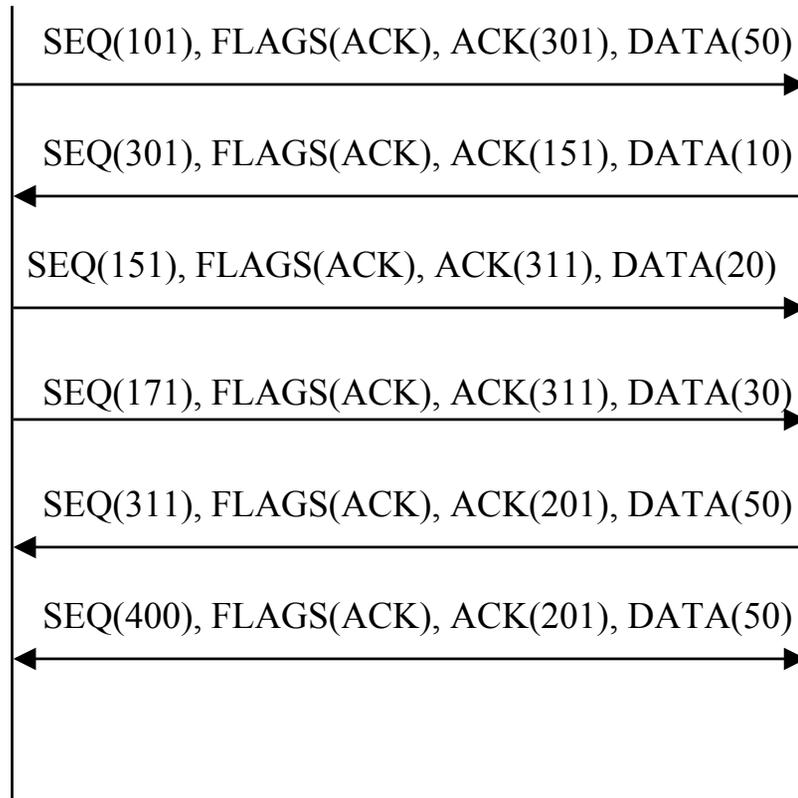
Campos do TCP

- **Checksum:** verificador de erros de transmissão
- **Urgent pointer:** fornece a posição dos dados urgentes dentro do campo de dados
- **Opção:** pode conter negociação de opções tal como o MSS (Maximum Segment Size)

Estabelecimento de Conexão



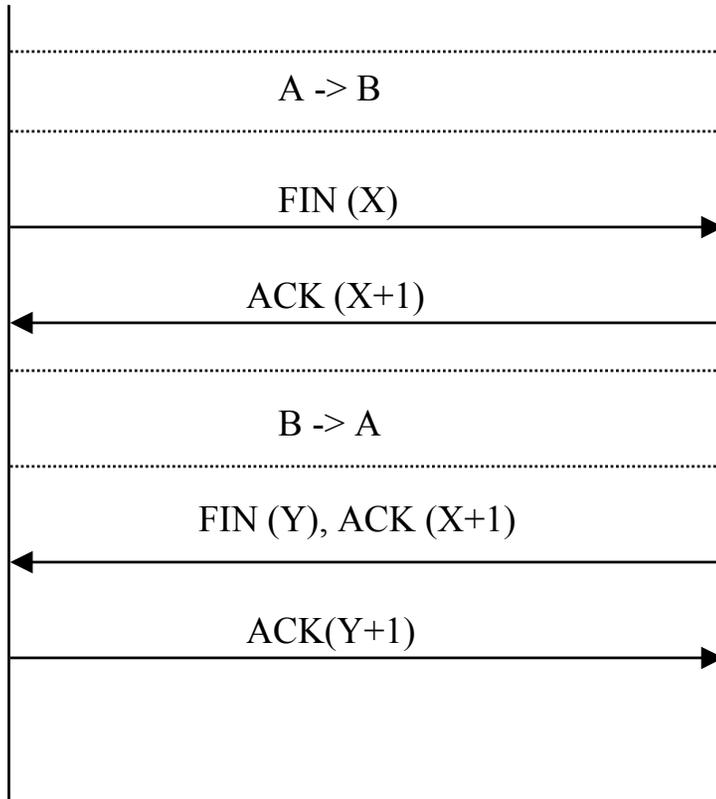
Troca de Dados



Liberação de Conexão

A

B



Porta Padrão

- FTP (21)
- FTP-DATA (20)
- TELNET (23)
- SMTP (25)
- NNTP (119)

ICMP (Internet Control Message Protocol)

- Oferece funções de gerência
- Encapsulado no datagrama IP
- Emitido por um gateway intermediário ou pelo host destino

ICMP

Type	Code ->
Code	Checksum ->
Checksum	Information

Mensagens ICMP

- Echo Request / Echo Reply
- Destination Unreachable
- Source Quench
- Redirect
- Time Exceeded for a Datagram
- Parameter Problem on a Datagram
- Timestamp Request / Timestamp Reply
- Address Mask Request / Address Mask Reply

Destination Unreachable

- Mensagem aplicada nos diversos casos em que o datagrama não pode ser entregue ao destinatário especificado
- Causas (Código): sub-rede inacessível, estação inacessível, protocolo inacessível, fragmentação necessária e campo flag não configurado, falha na rota especificada, repasse proibido por um filtro no gateway intermediário

Time Exceeded

- Retornado por um gateway quando o TTL de um datagrama expira.
- Retornado por um host quando o tempo para remontagem de um datagrama fragmentado expira

Parameter Problem

- Relata a ocorrência de erros de sintaxe ou semântica no cabeçalho de datagrama
- No campo código tem-se o ponteiro para o campo do cabeçalho que gerou o erro contido no campo de dados da mensagem
ICMP

Source Quench

- Serve como regulador de fluxo de recepção. Essa mensagem é gerada por gateways ou hosts quando eles precisam reduzir a taxa de envio de datagramas do emissor. Ao recebê-la, o emissor deve reduzir a taxa de emissão.

Redirect

- Usada pelo gateway para notificar um host sobre uma rota mais adequada ao destinatário do datagrama por ele enviado. É usado pelos hosts para atualizar as suas tabelas de roteamento
- Neste tipo de mensagem não há descarte de datagramas

Echo Request e Echo Response

- São mensagens usadas para testar se a comunicação entre duas entidades é possível. O destinatário é obrigado a responder a mensagem de Eco com a mensagem de Resposta de Eco
- Usado para estimar o throughput e o round trip time
- `ping -s laicox.cic.unb.br`

Timestamp Request e Timestamp Response

- São usadas para medir as características de atraso no transporte de datagramas em uma rede Internet. O emissor registra o momento de transmissão na mensagem. O destinatário, ao receber a mensagem, faz o mesmo.
- No campo de dados é enviado um identificador, número de seqüência, tempo de envio do request, tempo de recebimento do request e tempo envio do response
- Pode-se calcular o tempo de processamento do datagrama no host destino

Address Mask Request e Address Mask Response

- Utilizadas por uma estação na recuperação da máscara de endereços quando é aplicado o sub-endereçamento ao endereço IP. O host emite a mensagem e o gateway responsável responde com a descrição da máscara

ARP (Address Resolution Protocol)

- O nível IP utiliza para o transporte dos datagramas os gateways interligando as sub-redes. Para tal é necessário o conhecimento do endereço físico dos gateways.
- O ARP realiza o mapeamento do endereço lógico IP para o endereço físico da sub-rede
- O ARP é encapsulado direto no protocolo da sub-rede
- O host que pretende mapear um endereço IP para o físico deve enviar um pedido ARP no modo broadcast na rede. O host que receber e verificar que o endereço é o seu, responde com o seu endereço físico

ARP (Address Resolution Protocol)

- Cada host possui um cache dos mapeamentos realizados de forma a utilizar a busca do endereço físico. Contudo tais entradas armazenadas possuem um tempo de vida limitado, permitindo alterações nos endereços.
- Um host ao receber um pedido ARP pode atualizar o sua cache mesmo que o endereço procurado não seja seu

ARP (Address Resolution Protocol)

Hard Type		Proto Type
Hlen	Plen	Operation
Sender HA		
Sender HA		Sender IP
Sender IP		Target HA
Target HA		
Target IP		

RARP (Reverse Address Resolution Protocol)

- Usado por um host para descobrir o seu endereço lógico IP a a partir do seu endereço físico (Diskless)
- O RARP é encapsulado diretamente no protocolo da sub-rede
- Quando o host necessita do seu endereço IP envia um pedido no modo broadcast. O servidor RARP que mantém uma tabela de mapeamento responde.
- Utiliza o mesmo formato de protocolo do ARP
- Pode haver mais de um servidor RARP

Aplicação Internet

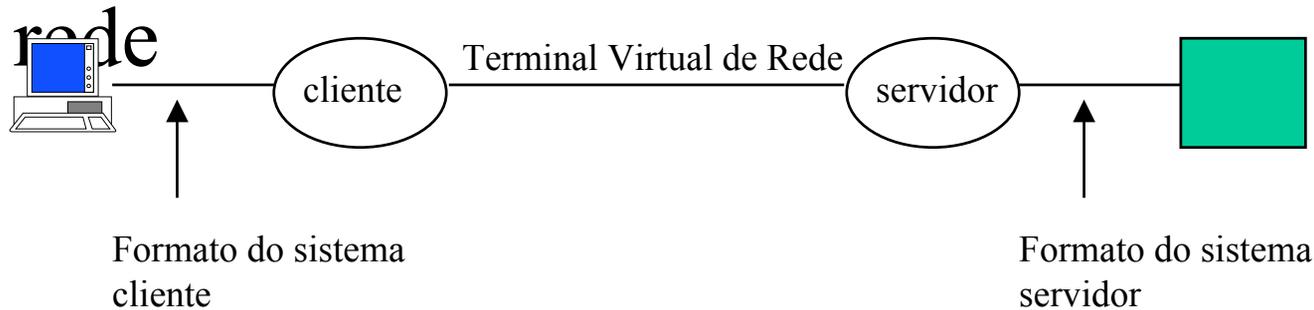
- Modelo Cliente-Servidor
 - Servidor é um processo que espera pedidos de conexão (se TCP), aceita requisições de serviço e retorna uma resposta
 - Cliente é um processo que inicia uma conexão (se TCP), envia requisições e espera resposta.
Geralmente possui uma interface com o usuário
 - A comunicação entre o cliente e o servidor acontece através de um protocolo de aplicação
 - Contra-exemplo: emulador de terminal

Aplicações Internet

- Telnet
- Ftp (File Transfer Protocol)
- SMTP (Simple Mail Transfer Protocol)
- DNS (Domain Name System)
- Gopher
- Http (Hypertext Transfer Protocol)

Telnet

- Implementa o serviço de terminal remoto
- Utiliza o conceito de terminal virtual de



Telnet

- Utiliza TCP/IP
- Terminal Virtual de Rede
 - Usa ASCII com 7 bits para representar dados e 8 bits para representar comandos
 - Interpreta caracteres de controle ASCII, tais como CR e LF
 - Usa o caractere IAC (Interpreter for command - 255) para referenciar um comando, tal como 255 244 para interromper um programa na máquina remota

Telnet

- Possibilita a negociação simétrica de opções com os comandos WILL, DO, DON'T, WON'T
 - Opções disponíveis:
 - Eco
 - Tipo de terminal
 - Uso de EOR (End of Register)
 - Transmissão de dados com 8 bits

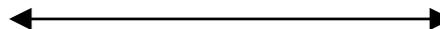
FTP

- Protocolo que permite a transferência de arquivos entre computadores na Internet
- Usa TCP/IP
- **Modelo**

INTERFACE DO
USUÁRIO

|

CLIENTE-FTP
CONTROLE



SERVIDOR-FTP
CONTROLE

⋮

CLIENTE-FTP
DADOS



⋮

SERVIDOR-FTP
DADOS

FTP

- Tipos de dado: ASCII, EBCDIC, Imagem, Local
- Estrutura do arquivo: Não-estruturado, Orientado a registro, Paginado
- Modos de Transferência: Fluxo Contínuo, Blocado, Comprimido
- Re-início de Transferência
- Comandos: controle de acesso, manipulação de diretórios, parâmetros de transferência e de serviços

Controle de Acesso

- user
- pass
- acct
- smnt
- rein
- quit

Manipulação de Diretório

- `cwd` (Change Working Group)
- `cdup` (Change to Parent Directory)
- `mkd` (Make Directory)
- `rmd` (Remove Directory)
- `pwd` (Print Working Directory)
- `list`
- `nlst` (Name List)

Modelo ISO/OSI

Devido ao sucesso na padronização do TCP/IP, em 1983 a ISO (International Standards Organization) propôs um modelo conceitual de referência denominado de OSI (Open Systems Interconnection). O Modelo OSI é constituído de sete camadas (ou níveis) com funções específicas.

Modelo ISO/OSI

É uma padronização de níveis funcionais de protocolos de comunicação.

7	aplicação
6	apresentação
5	sessão
4	transporte
3	rede
2	enlace
1	físico

Modelo ISO/OSI

Vamos a seguir sumarizar as sete camadas do modelo ISO/OSI com algumas de suas funções. Nos próximos slides, após o sumário, descreveremos de forma mais detalhada a função de cada camada do modelo.

Modelo ISO/OSI

<u>Camada</u>	<u>Descrição Sumarizada</u>
Aplicação	<i>prover serviços que suportam direto as aplicações.</i>
Apresentação	<i>traduz formatos.</i>
Sessão	<i>configura sessões.</i>
Transporte	<i>garante a ligação nas conexões.</i>

Modelo ISO/OSI

Camada Descrição Sumarizada

Rede *roteamento de dados.*

Enlace *detecta e corrige erro de dados.*

Físico *especificação elétrica/mecânica.*

Modelo IEEE

A arquitetura do IEEE é conhecida como o Padrão para as redes locais. Suas três camadas são :

3

Logical Link Control - LLC

2

Medium Access Control -MAC

1

Physical Layer - PHY

Modelo IEEE

Logical Link Control (LLC) 802.2

enlace

802.3
MAC

802.4
MAC

802.5
MAC

802.6
MAC

física

802.3
físico

802.4
físico

802.5
físico

802.6
físico

IEEE 802 Standards

802.1 - Higher Layers and Internetworking

802.2 - Logical Link Control (LLC)

802.3 - CSMA/CD

802.4 - Token Bus

802.5 - Token Ring

802.6 - MAN

802.7 - Broadband Tech. 802.8 - Optical Fiber

802.9 - Voice/Data Int. 802.10 - LAN Security

802.11 - Wireless LANs

Comparando o modelo IEEE com OSI

OSI

enlace
física

IEEE

802.2 - Logical link control			
802.1 - Internetworking			
802.3 MAC	802.4 MAC	802.5 MAC	802.6 MAC
802.3 físico	802.4 físico	802.5 físico	802.6 físico

IEEE MAC

Corresponde a porção inferior do nível de enlace definido pelo padrão ISO/OSI.

Suas funções que são relacionadas para o hardware são :

- topologia lógica**
- acesso ao meio físico**
- definição do formato do quadro de transmissão**
- endereçamento de nó**
- checagem da seqüência de quadros**

Modelo SNA

O Systems Network Architecture (SNA) Protocol foi desenvolvido pela IBM após 1974 para atender ao seu modelo em hierarquia de rede.

Os dispositivos da hierarquia eram os *mainframes*, *Communication controllers*, *cluster controllers* e *terminais*.

Modelo SNA

ISO

<u>7</u>	Dia	SNADS	DPM	User Applications	
<u>6 e 5</u>	APPC	CICS	IMS	TSO	DB2
<u>4</u>	APPN	VTAM			
<u>3</u>	NCP				
<u>2</u>	Token Ring		SDLC		X-25
<u>1</u>			v35	RS232-C	

Modelo Netware IPX/SPX

O Netware foi desenvolvido pela Novell no começo dos anos 80s, baseado no protocolo XNS (Xerox Network Protocol).

O protocolo IPX/SPX é orientado ao um servidor central que prove serviços de impressão, acesso a arquivos, troca de mensagens (correio eletrônico) e outros serviços. O IPX (Internetwork Packet eXchange) é o protocolo principal.

Modelo Netware IPX/SPX

O IPX é um protocolo de transporte não-orientado a conexão.

Por outro lado, o SPX (Sequence Packet eXchange) é um protocolo de transporte orientado a conexão. Desta forma, o SPX é utilizado onde a confiabilidade de conexão é necessária.

Modelo Netware IPX/SPX

A arquitetura IPX/SPX, possui outros protocolos tais como o RIP e NLSP que se dedicam ao roteamento.

O protocolo NCP prove dentre outros serviços de transporte, sessão, apresentação e aplicação, tais como: controle de seqüência de pacotes, gerência de sessão, tradução semântica e transferência de arquivos.

III – Redes Locais

Objetivo

Abordar as tecnologias mais freqüentemente empregadas nas redes locais, com especial ênfase nos seus padrões, funcionamento, suas evoluções e limitações.

Em adição, estudaremos alguns conceitos muito importantes hoje considerados em redes de computadores, tais como a qualidade e custo de serviço e ainda as redes virtuais.

Objetivos

1000BASE-X *SC-Connector* *4B5B*

Ethernet vs IEEE 802.3 *IEEE802.12* *PMD*

1000BASE-T *8B6T* *1000BASE-SX*

1000BASE-LX *PAR (Project Authorization Request)*

Repetidor Classe I

1000BASE-CX *Repetidor Classe II*

carrier extension

3.1. Visão geral sobre as LANs

3.2. Padrões das LANs

3.3. Ethernet (CSMA/CD)

3.4. Fast Ethernet

3.5. Gigabit Ethernet

3.6. Redes Token-Passing

3.7. Fiber Distributed Data Interface (FDDI)

3.8. Asynchronous Transfer Mode (ATM)

3.9. Dispositivos de Interconexão

3.1 - Visão geral sobre as LANs

3.1 - Objetivo

Vamos neste módulo abordar alguns aspectos que são importantes para qualquer projeto e implementação de uma *Local Area Network (LAN)*.

Em adição, vamos discutir alguns obstáculos que algumas vezes impedem o perfeito funcionamento de muitas instalações de redes locais.

Introdução

Na sua concepção mais básica, uma LAN pode ser visualizada como :

Uma facilidade de comunicação que prove uma conexão de alta velocidade entre processadores, periféricos, terminais e dispositivos de comunicação de uma forma geral num único prédio ou campus.

No princípio as *LANs* eram vistas como ambientes ideais para o compartilhamento de dispositivos onerosos, tais como impressoras, discos, plotters, scanners, dentre outros equipamentos que podiam ser compartilhados.

Numa segunda fase, as *LANs* são vistas como o *backbone* na descentralização das corporações e a conseqüente necessidade de uma computação distribuída. Nesta etapa, muitas vezes conhecida como a era do *downsizing*, os grandes centros de processamento de dados (CPDs) são reduzidos ou eliminados nas grandes corporações.

LANs x Outras Tecnologias

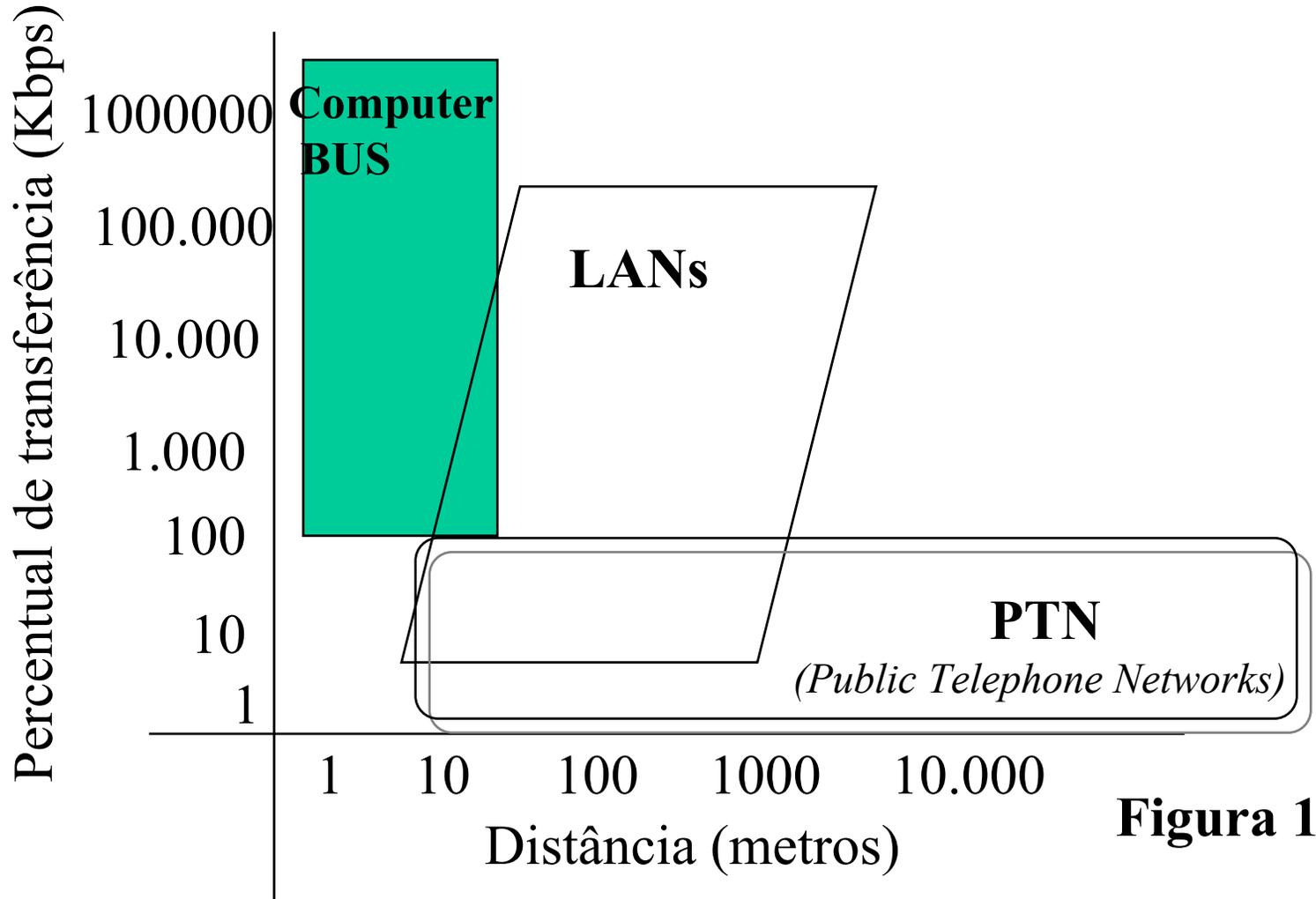


Figura 1

Comentário # 1

A figura 1 ilustra que uma LAN é a tecnologia que representa uma boa resposta para distâncias relativamente pequenas com uma largura de banda considerável (na ordem de Mbps).

É importante, também, sabermos que os barramentos dos computadores (Computer BUS) têm sido empregados como interconexão de computadores. Esta nova abordagem, surgida no final dos anos 90, é conhecida como SAN (System Area Network).

As SANs, diferente das atuais LANs, têm sua largura de banda na casa dos Gbps. A conexão entre *nós* é efetuada ponto-a-ponto. Por outro lado, a maioria das LANs implementam uma ligação multiponto.

Existe um grande número de empresas (o consórcio é formado por cem organizações, dentre as quais IBM, Intel, SGI, 3COM, Cisco, Oracle, Informix, etc) que estão estudando alguns padrões para o efetivo uso das SANs.

O objetivo destas empresas é o estabelecimento de padrões para o uso de uma forma interoperável das interfaces de rede de diferentes fabricantes.

O abordagem VIA (Virtual Interface Architecture) é um esforço neste sentido, utilizando uma SAN Myrinet. Neste ambiente, devido a grande largura de banda a interface de rede é responsável pelo processamento não só dos quadros nos níveis físico e enlace, mas também em camadas superiores.

Comentário # 2

Outro fato interessante que a figura 1 ilustra é a interseção entre uma LAN e uma PTN (Public Telephone Network).

Nas organizações modernas é desejável que os serviços de comunicação da rede (vox, dados, imagem, fax e som) sejam transportados e gerenciados de uma forma única. Desta forma, com um único suporte para o hardware, o software, os diversos tipos de interfaces, a manutenção, a administração e a gerência do ambiente tem seus custos reduzidos.

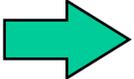
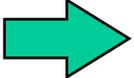
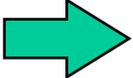
Da observação do comentário #2 tem-se amadurecido um conceito denominado de *communication networks*. A idéia é que os profissionais de LANs e comunicação tenham uma capacidade de entendimento maior das áreas de comunicação e LANs, respectivamente.

Uma LAN ideal

Um projeto de LAN ideal pode ser caracterizado pelo fácil acesso da informação num ambiente semelhante as tomadas elétricas num prédio. Em outras palavras, é interessante que todos tenham acesso a rede em qualquer local da organização.

Em adição, a modularidade deve ser sempre observada. Em outras palavras, qualquer ligação de dispositivos deve ser efetuada sem que nenhuma parada da rede ocorra.

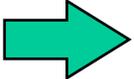
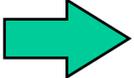
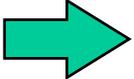
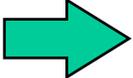
Podemos sumarizar uma LAN ideal como aquela que :

-  A instalação é efetuada de uma só vez;
-  Acesso irrestrito;
-  Independente de aplicação;
-  Modularidade;
-  Fácil manutenção e administração.

O objetivo de uma rede ideal é que :

- a informação possa ser distribuída de uma forma uniforme ao longo do ambiente da corporação;
- os dispositivos interconectados podem ser de fabricantes diferentes permitindo o uso modelos distintos;
- a movimentação de telefones, computadores, impressoras, discos e faxes seja semelhante a uma troca de lâmpada.

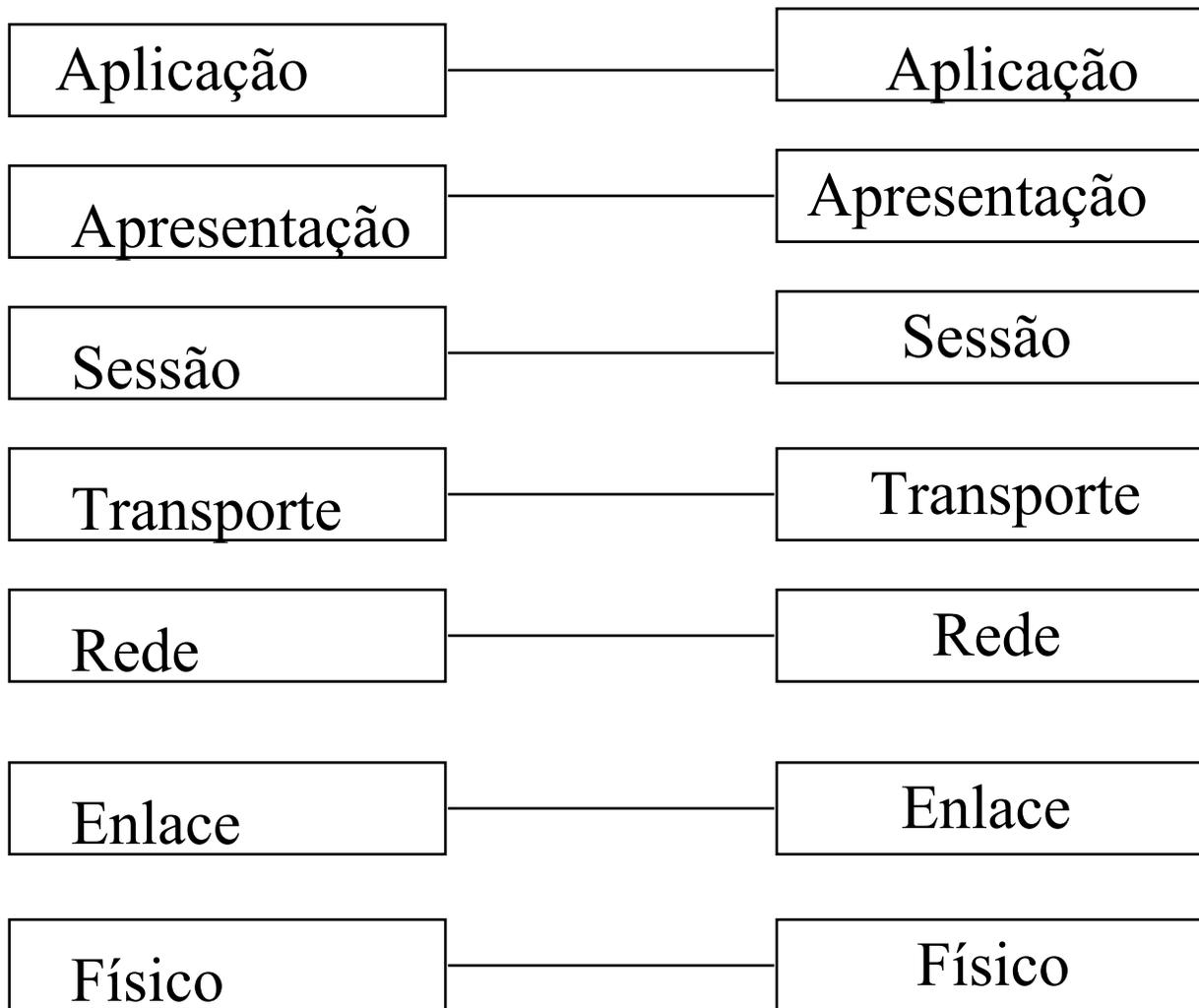
Podemos sumarizar os obstáculos de uma LAN ideal :

-  Falta de planejamento no projeto e instalação;
-  Falta de um único padrão;
-  Solicitações não homogêneas de transmissão (voz, vídeo, alarmes, correio eletrônico, etc);
-  Custo do meio de transmissão;
-  Gerência unificada do ambiente.

O RM-OSI

Uma padronização funcional das redes de comunicação foi estabelecida pelo ISO(International Standards Organization) e esta ficou conhecida como RM-OSI (Reference Model - Open System Interconnection).

O padrão RM-OSI é baseado nos três primeiros níveis propostos pela ITU, pela experiência da arquitetura TCP/IP e por uma melhoria na identificação de funções não estabelecidas previamente.



3.2 - Padrões das LANs

Objetivo

O padrão proposto pela OSI, é genérico no sentido que o mesmo engloba da aplicação a mídia da rede. Neste módulo, nosso objetivo é a abordagem do IEEE (Institute of Electrical and Electronics Engineers) que é conhecido com o órgão normalizador para as redes locais.

Vamos estudar alguns padrões que serão melhor detalhados nos próximos módulos.

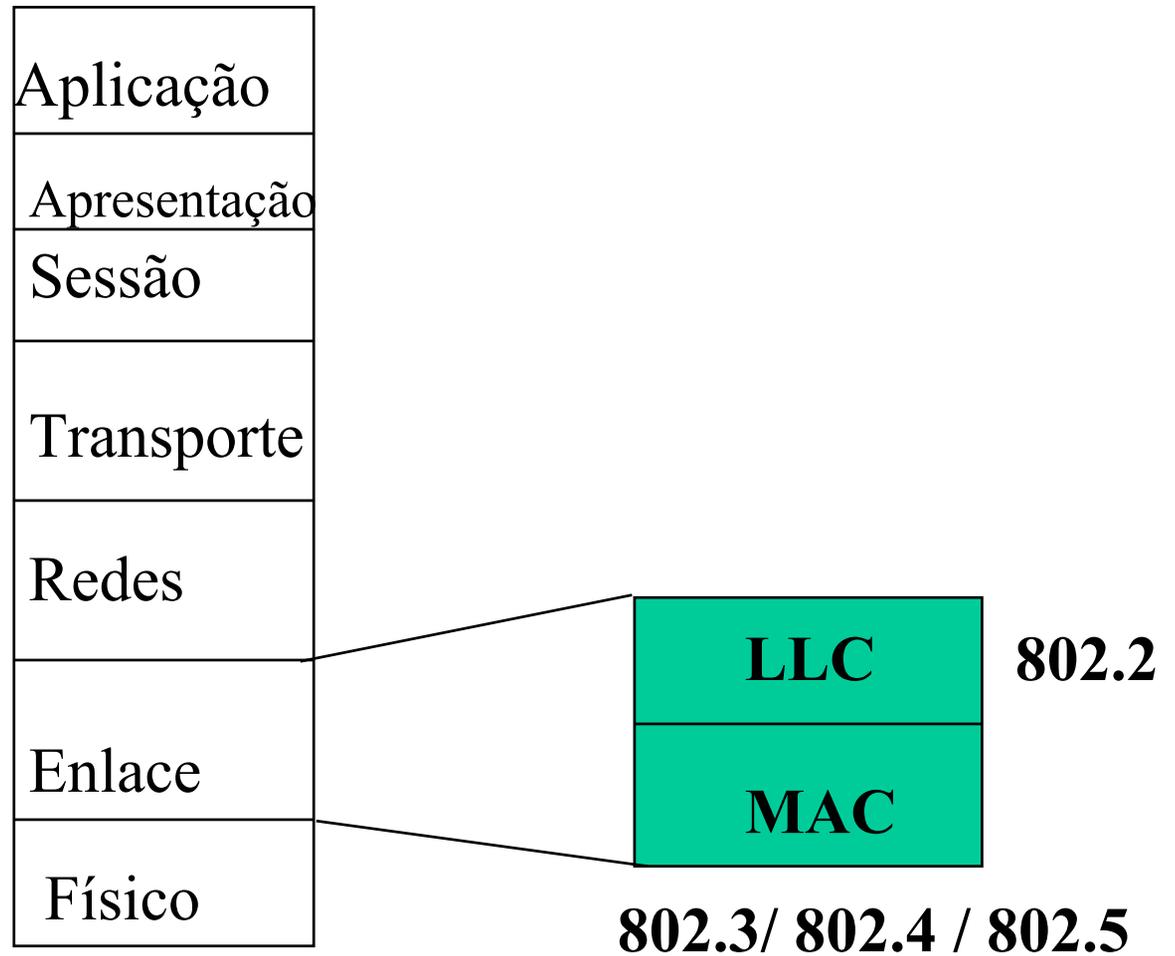
Padrões

Alguns dos padrões mais importantes são :

- 802.1 - Coordenação entre a interface OSI dos níveis 1 e 2 com os cinco níveis superiores;
- 802.2 - Enlace lógico;
- 802.3 - CSMA/CD;
- 802.3u - Fast Ethernet;
- 802.3z - Gigabit Ethernet;

- 802.4 - Token-bus;
- 802.5 - Token- ring;
- 802.9a - IsoENET;
- 802.12 - 100VG-AnyLAN.

Enlace Lógico (802.2)



Enlace Lógico (802.2)

Visando acomodar múltiplos métodos de acesso a uma LAN, o IEEE estabeleceu o padrão 802.2. Este é composto por dois sub-níveis :

- LLC - Controle lógico de enlace - possui dois tipos básicos de serviços. No primeiro serviço, ou tipo 1, é considerada a operação de conexão-não-orientada sem reconhecimento de recebimento.

Neste tipo de serviço, uma *nó* envia uma mensagem para outro(s) *nó(s)* sem que uma conexão lógica tenha sido estabelecida, para controle de seqüência e reconhecimento de recebimento das mensagens.

Enlace Lógico (802.2)

O serviço do tipo 1 é caracterizado pelo de envio de mensagens não essenciais, ou para sistemas em que os níveis mais altos provêem um mecanismo de recuperação e função de seqüência das mensagens enviadas/recebidas

Enlace Lógico (802.2)

O segundo serviço, o do tipo 2, é um serviço mais convencional de comunicação de dados balanceado.

Neste, é estabelecido a conexão lógica entre dois LLCs. Cada LLC pode enviar e receber mensagens e respostas. Cada LLC possui a responsabilidade de assegurar a completa e segura entrega das mensagens que envia.

Media Access Control (MAC)

O IEEE tem estabelecido alguns padrões de acesso ao meio que foram definidos a partir do sucesso de padrões *de facto*.

O IEEE 802.3 (CSMA/CD - Carrier Sense Multiple Access / Collision Detection) define um MAC e o correspondente nível físico para a conexão do cabo coaxial e par trançado de bandabase. Este padrão foi *espelhado* no padrão Ethernet definido pela Xerox, Intel e Digital.

Media Access Control (MAC)

O IEEE 802.5 é o padrão que define o método de acesso no qual para acesso a media compartilhada (ou multiponto), através da passagem de uma permissão (*Token*) numa rede com uma topologia lógica em anel (*Ring*).

A especificação IEEE 802.5 é baseada no padrão *Token Ring* desenvolvido pela IBM. Nesta abordagem quando existe uma permissão livre, um determinado *nó* constrói um quadro que inclui a seguinte informação :

- endereço da estação destinatária;
- seu próprio endereço;
- campo de informação;
- campo de controle de erro.

Media Access Control (MAC)

Como o quadro tem um movimento circular através do anel, todas as estações ao longo do percurso examinam o endereço do *nó destinatário*. Somente a estação destinatária receberá a informação do campo de informação e adicionará um campo de leitura com sucesso.

Quando o quadro é novamente recebido pelo *nó remetente*, este fará a liberação do quadro para que outro *nó* possa ter acesso ao meio. Em caso de erro, o *nó remetente* re-envia o (s) quadro (s) necessário (s).

Nível Físico

Com o desenvolvimento de novas tecnologias de LANs, ficou patente que algumas redes poderiam operar sobre diferentes meios físicos. Um exemplo clássico é uma rede que pode ser implementada empregando três pares de cabos metálicos em um grupo de quatro pares ou um par de fibra ótica para o transporte de 100 Mbps.

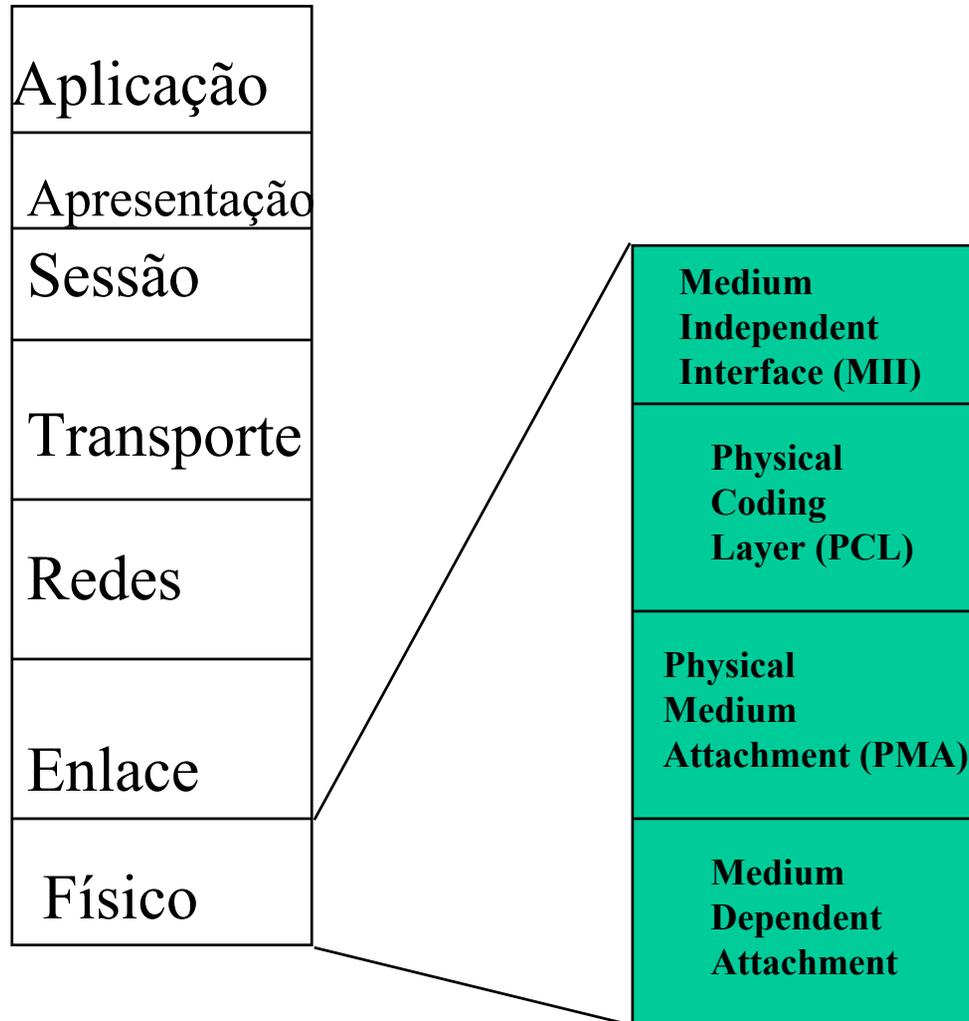
Para o suporte de diferentes meios, foi necessário o uso de diferentes métodos de codificação e percentuais de sinalização. Um exemplo é a facilidade de transmissão utilizando-se de um alto percentual de sinalização numa rede de fibra ótica, em contrapartida a um cabo metálico.

Nível Físico

O IEEE propôs uma subdivisão do nível físico, visando suportar os diferentes tipos de meios físicos empregados para uma mesma especificação de LAN.

A proposta do IEEE é bastante interessante, levando-se em conta a relativa recente utilização de redes de alta velocidade.

Nível Físico



Nível Físico

- **Physical Coding Sublayer (PCS)** - define o método de codificação usado para a transmissão em diferentes tipos de meios físicos.
- **Physical Medium Attachment -(PMA)** faz o mapeamento das mensagens do subnível de codificação física para o meio físico de transmissão.
- **Medium Dependent Attachment** - especifica o conector, com suas características físicas e elétricas , utilizado para fazer a conexão ao meio físico.
- **Medium Independent Interface (MII)** - é possível o estabelecimento de uma nova interface que poderá estabelecer diferentes atributos, todavia estes dever ser compatíveis com os três subníveis apresentados anteriormente.

Acrônimos e Termos

- **BNC** (*Baynoet Neill Concelman*) - Conector do tipo RG58 utilizado em cabos coaxiais no padrão 10BASE2;
- **Crossover** - é a característica que se refere-se ao fato de que alguns cabos de pares trançados entre *nós* Ethernet precisam ter comutados as linhas de transmissão e recepção com o objetivo de que o transmissor esteja conectado ao receptor. Em redes Ethernets, *nós* Ethernet são conectados aos switches e repetidores através de cabos *diretos*. Os switches e repetidores são interconectados entre si através de cabos *crossover*

Acrônimos e Termos

- **Preambulo** - Uma seqüência alternada de 0s e 1s no início de cada quadro a ser transmitido. Um exemplo é a codificação Manchester, quando utilizada o *preambulo* produz uma freqüência de 5 MHz no início de cada quadro. Esta é utilizada pela estação receptora, ou repetidor, como referência para decodificar o dado e o clock de recebimento;
- **Jitter** - Num sinal digital, jitter representa a variação dos sinais por causa do erro no tempo quando na transmissão sobre cabos;

Acrônimos e Termos

- **Jabber** - numa rede de 10 Mbps, o MAU é responsável por interromper uma estação que esteja transmitindo por um tempo excessivo, evitando-se um mau funcionamento da rede. O MAU entra então num estado conhecido por *Jabber*, quando do circuito de saída (DO - Data Out) está ativo num intervalo de tempo entre 20-150 m.s.

Durante o estado de *Jabber*, a transmissão para a rede não é permitida, as colisões são retornadas para o DTE pelo circuito CI (Control In). O MAU permanece neste estado de *Jabber* até que cesse atividade no circuito DO por um período de 0.25 - 0.75s.

Nas redes de 100 Mbps, os repetidores evitam o *Jabbering* dos DTEs terminando suas transmissões quando estas passam de 40.000 bit times.

Acrônimos e Termos

- **QoS** (*Quality of Service*) - é o termo empregado para definir parâmetros específicos necessários para a aplicação do usuário. Os serviço de parâmetros pode ser definido em termos de largura de banda, latência, jitter e atraso;
- **VLAN** - é um domínio lógico de broadcast numa determinada rede física. As redes VLANs são especificadas e diferenciadas através do uso de uma VLAN Tag. O conceito de VLAN é orientado para permitir o pessoal envolvido com o suporte e a administração a configuração das redes, ao mesmo tempo provendo aos usuárrios a conectividade e privacidade que eles esperam tendo múltiplas e separadas redes.;
- **VLAN Tag** - definida nos padrões 802.3ac e 802.1Q é um campo de 4 bytes inserido entre no quadro Ethernet entre os campos SA (Source Address) e o Type/Length . O VLAN Tag é utilizado para diferenciar VLANs lógicas;
- **WINDOW**- é o número total de quadros, pacotes ou células que são recebidas num determinado tempo sem que seja necessário o uso de um mecanismo de *ACK*.

3.3 - Ethernet (CSMA/CD)

Histórico -

A rede local Ethernet (*The Ethernet Local Area Network*) foi criada a cerca de 30 anos por Bob Metcalfe and David Boggs como uma rede local de 3 Mbps. Os dois engenheiros trabalhavam na XEROX PARC (Palo Alto Research Center).

Bob Metcalfe fundou a 3Com e *evangelizou* o uso da Ethernet como um padrão de rede multivendor. Metcalfe, como membro participante, fez a proposta de padronização do Ethernet para o IEEE.

O padrão inicial da Ethernet, conhecido como *DIX* (*Digital, Intel e Xerox*), foi publicado como *Blue Book* em 1980.

A padronização pelo IEEE ocorreu em 1982, como uma rede de 10 Mbps sob os cuidados do Projeto 802. O comite que estabeleceu a norma da nova tecnologia de rede local foi denominado de 802.3 CSMA/CD (Ethernet).

No final de 1982, os padrões DIX e IEEE se juntaram numa única versão.

O padrão IEEE 802.3 foi adotado por inúmeros outras entidades :

- NIST - National Institute of Standards and Technology;
- ECMA - European Computer Manufactures Association;
- ANSI - American National Standards Institute;
- ISO - Internacional Standardatization Organization, onde foi batizado de ISO/IEC 8802-3.

O padrão estabeleceu uma série de especificações para suporte a 10 Mbps em vários tipos de mídias. Inicialmente, para cabos coaxiais grossos (*thick-wire*).

Então com desenvolvimento tecnológico, as especificações evoluíram para os cabos coaxiais finos (*thin-wire*), pares trançados sem blindagem (UTP) e então para as fibras óticas.

Importante ressaltar que o sucesso da Ethernet fez com que até uma especificação de *broadband* de 10 Mbps em mídia de TV a cabo (CATV) fosse produzida.

A norma IEEE 802.3 para o cabeamento UTP provocou um crescimento na utilização do padrão de uma forma nunca antes observada (ou imaginada). Por causa do sucesso das redes UTP, o protocolo CSMA/CD torna-se *dominante* no mercado de LANs com bilhões de adaptadores, repetidores e outros dispositivos necessários para a conexão da rede.

O Ethernet vem evoluindo a medida que a chamada *silicon pressure* torna-se um fator tecnológico de melhoria custo-benefício. Em adição, este fator pressiona todas as tecnologias para que as transmissões tenham velocidades maiores.

A resposta do padrão IEEE 802.3 vem, primeiro, através do *Fast Ethernet* a 100 Mbps. Mais recentemente surge a especificação IEEE 802.3z, o *Gigabit Ethernet* a 1 Gbps.

A Nomenclatura IEEE 802.3

Devido a grande diversidade de opções de cabeamento e técnicas de sinalização o IEEE estabeleceu a seguinte nomenclatura :

x type y

Onde:

- x* - refere-se a velocidade em Mbps ;
- type* - indica o tipo de sinalização ;
- y* - define o comprimento máximo em centenas de metros.

Nomenclatura IEEE 802.3

Exemplos :

10BASE5 - 10 Mbps, Baseband, 500 metros ;

10BASE2 - 10Mbps, Baseband, 200 metros (185metros) ;

10BASET - 10 Mbps, Baseband, twisted-par 100 metros ;

10BROAD36 - 10 Mbps, Broadband, 3.6km ;

Nomenclatura IEEE 802.3

E os exemplos apresentados a seguir, como você interpretaria ?

10BASEFL

10BASEFB

10BASEFP

Nomenclatura IEEE 802.3

O padrão de fibra ótica é um pouco complexo devido a existência de quatro padrões.

FOIRL - Fiber Optic Inter Repeater Link

10BASEFL - Fiber Link

10BASEFB - Fiber Backbone

10BASEFP - Fiber Passive

Nomenclatura IEEE 802.3

E os exemplos apresentados a seguir, como você interpretaria ?

FOIRL - 10Mbps, Baseband, 1km

10BASEFL - 10 Mbps, Baseband, 2 km

10BASEFB - 10 Mbps, Baseband, 2 km

10BASEFP - 10 Mbps, Baseband, 2 km

O Formato do Quadro de Enlace

O dispositivos que transmitem os quadros 802.3 (e também 802.4), efetuam a operação do bit menos significativo para o mais significativo.

Em contraste o *Token-Ring* e *FDDI* que efetuam a transmissão dos quadros de uma maneira inversa, ou seja o mais para o menos significativo. Devido a esta diferença algumas vezes encontramos alguns problemas de interoperabilidade entre tais ambientes.

Assim, dispositivos tais como as *bridges*, *routers* e *switches* devem estar preparados para fazer a conversão necessária.

O Formato do Quadro de Enlace

A forma da especificação 802.3 nos leva a entender que a identificação de *um endereço de um nó, ou um endereço multicast*, dentro do campo de endereço é o primeiro que aparece na mídia. Isto é não é necessário e considerar o endereço mais ou menos significativo do endereço.

O Formato do Quadro de Enlace

Exemplo - Vamos considerar o endereço :

c2-34-56-78-9a-bc

Deste endereço podemos concluir que este não é multicast, pois :

c2 - 1100 0010

O bit menos significativo do primeiro byte (ou seja de *c2*) é 0.

O Formato do Quadro de Enlace

(A) Representação do endereço *c2-34-56-78-9a-bc* armazenado para transmissão iniciando-se no bit menos significativo.

1100 0010	0011 0100	0101 0110	0111 1000	1001 1010	1011 1100
-----------	-----------	-----------	-----------	-----------	-----------

(B) Representação do endereço *c2-34-56-78-9a-bc* armazenado para transmissão iniciando-se no bit mais significativo.

0100 0011	0010 1100	0110 1010	0001 1110	0101 1001	0011 1101
-----------	-----------	-----------	-----------	-----------	-----------

Formato do Quadro de Enlace

Ethernet

Preambulo	Endereço Destinatário	Endereço Origem	Tipo	Dado	FCS
8 bytes	6 bytes	6 bytes	2 bytes	46-1500 bytes	4 bytes

IEEE 802.3

Preambulo	sfd	Endereço Destinatário	Endereço Origem	Tam.	Dado	FCS
7 bytes	1 byte	2/6 bytes	2/6 bytes	2/6 bytes	46-1500 bytes	4 bytes

O Formato do Quadro de Enlace

O campo Tipo (*EtherType Field*) foi criado pela Xerox e por ela administrado até 1997. A partir deste ano o IEEE é responsável pela administração deste campo.

O *EtherType* permite que o equipamento transmissor indique tipo de protocolo este está usando. Só assim o destinatário poderá saber se entende, ou não, o quadro.

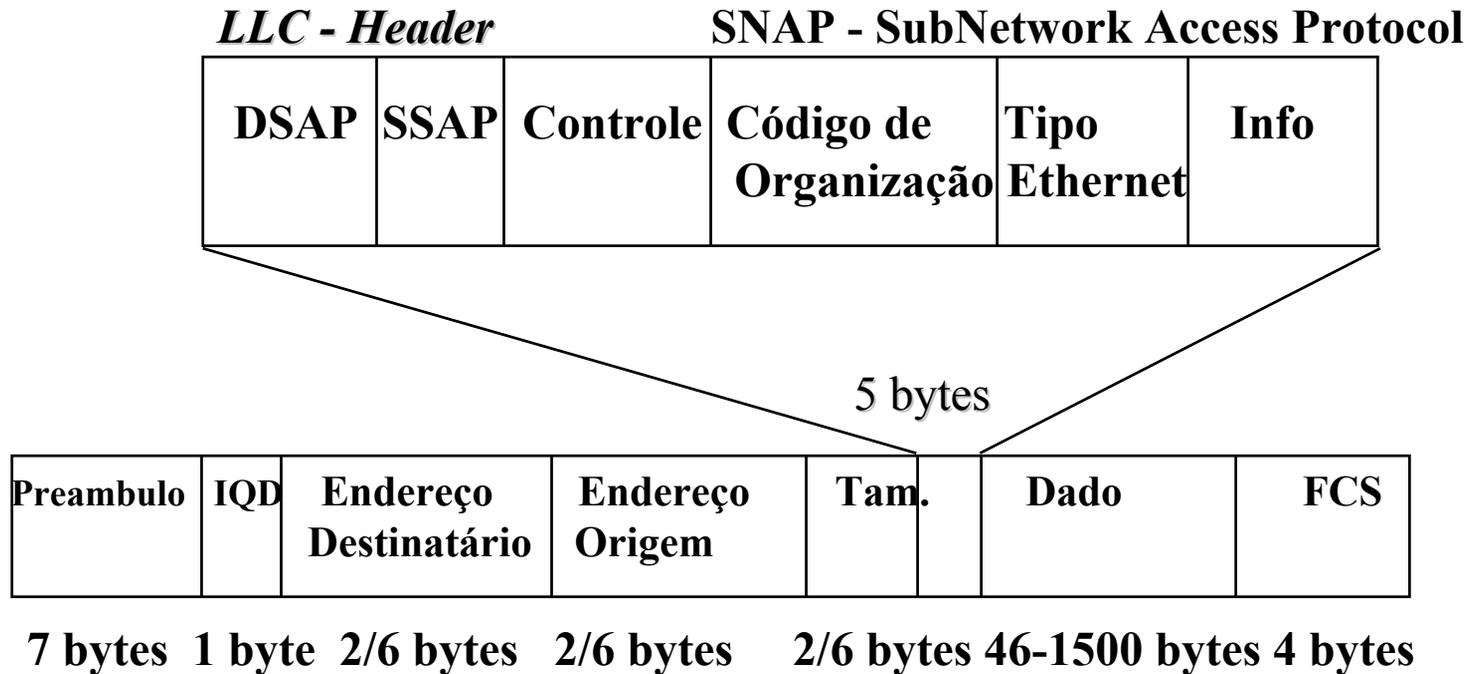
Com 2 bytes de tamanho, um grande conjunto de protocolos podem estabelecidos.

O Formato do Quadro de Enlace

A necessidade de um *header LLC* foi verificada por aqueles que trabalhavam com a especificação Ethernet. Assim, o quadro ganhou campos de informações tais como :

- *DSAP (Destination Service Access Point)*
- *SSAP (Source Service Access Point)*
- *Organizationally Unique identifier*
- *Control* - informação do tipo 1 indica um *datagram*, do tipo 2 *connection-oriented* e do tipo 3 *semireliable*

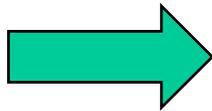
Quadro Ethernet-SNAP



IEEE 802.3

Codificação

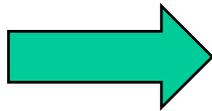
Nenhuma das especificações 802.3 utiliza a codificação binária *simples*, ou seja 0 volts para um bit 0 e 5 volts para um bit 1.



A razão pela qual de tal decisão é uma possível ambigüidade. Um remetente ocioso pode ser interpretado como 0 bit (0 volt).

Codificação

Existe a necessidade de um *host destinatário* saber determinar de forma unívoca o *início, meio e fim* de cada bit.



Utilização da Codificação Manchester e Diferencial Manchester

Codificação

Na codificação *Manchester* cada período de transmissão de um bit é dividido em dois intervalos iguais.

O bit 1 é enviado possuindo no primeiro intervalo uma voltagem alta (+0.85 v) e no segundo uma voltagem baixa (-0.85 v).

O bit 0, por outro lado, é enviado possuindo no primeiro intervalo uma voltagem baixa (-0.85 v) e no segundo uma voltagem alta (+0.85 v).

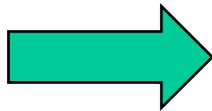
Codificação

O esquema da codificação *Manchester* garante cada bit tem uma transição no meio, facilitando inclusive a sincronização entre remetente e destinatário.



A desvantagem da codificação Manchester é que esta requer duas vezes mais largura de banda que outros métodos de codificação, porque os pulsos são a metade da largura usada.

Codificação



A codificação Manchester por sua simplicidade é empregada em todos os sistemas de banda base (baseband) do 802.3.

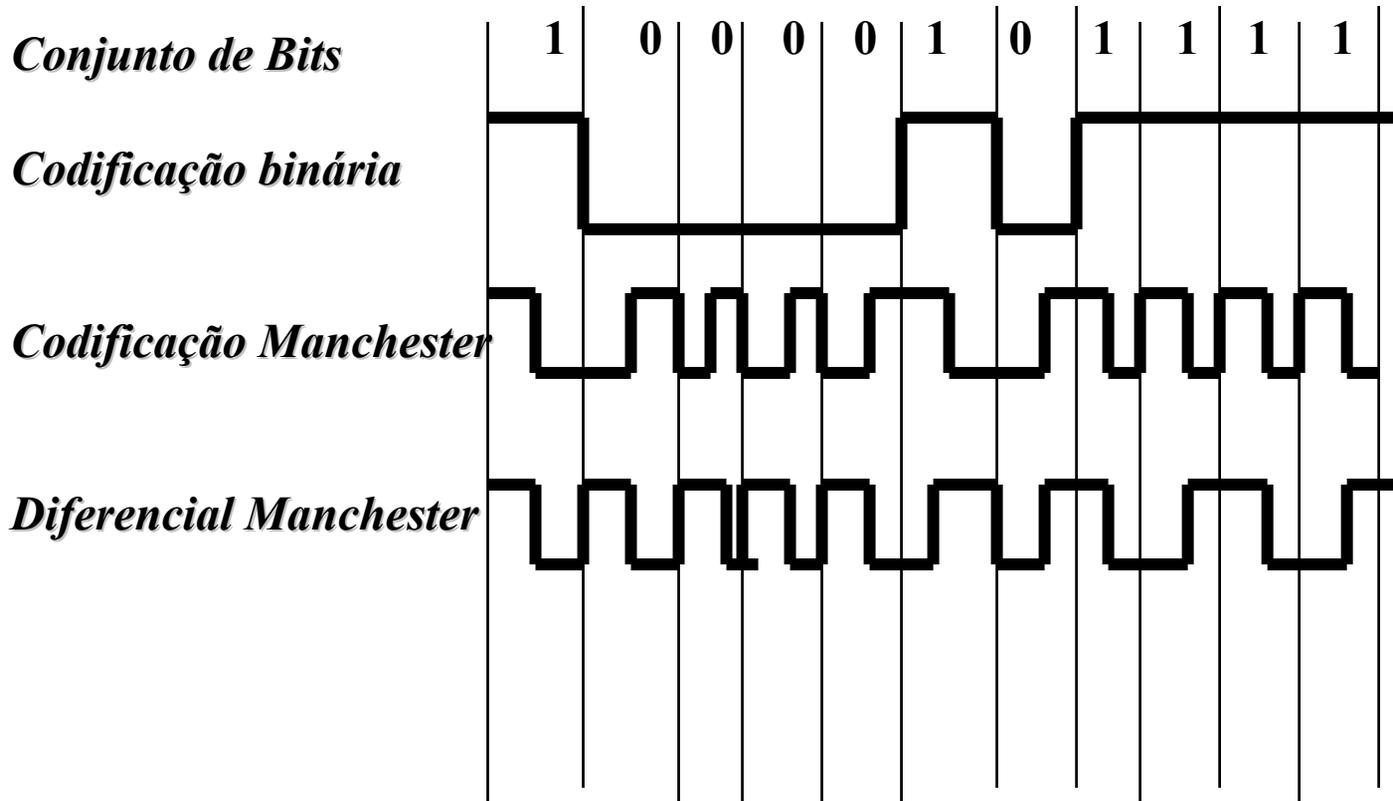
Codificação

Na codificação *Diferencial Manchester* cada período de transmissão de um bit é dividido em dois intervalos iguais, tal como a codificação *Manchester*.

O bit 1 é enviado possuindo no primeiro intervalo uma ausência de voltagem.

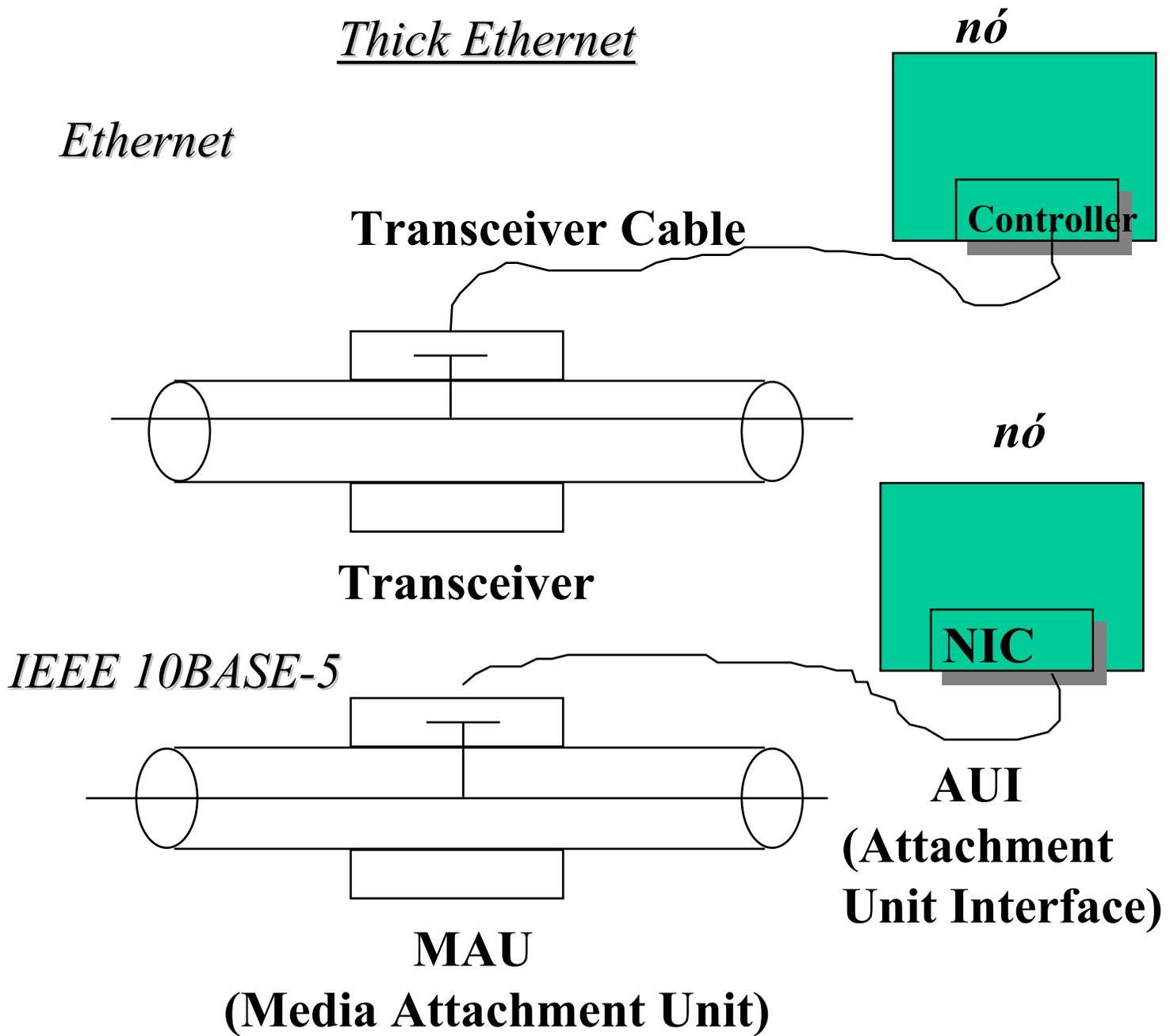
O bit 0, por outro lado, é enviado possuindo no primeiro intervalo uma voltagem.

Codificação



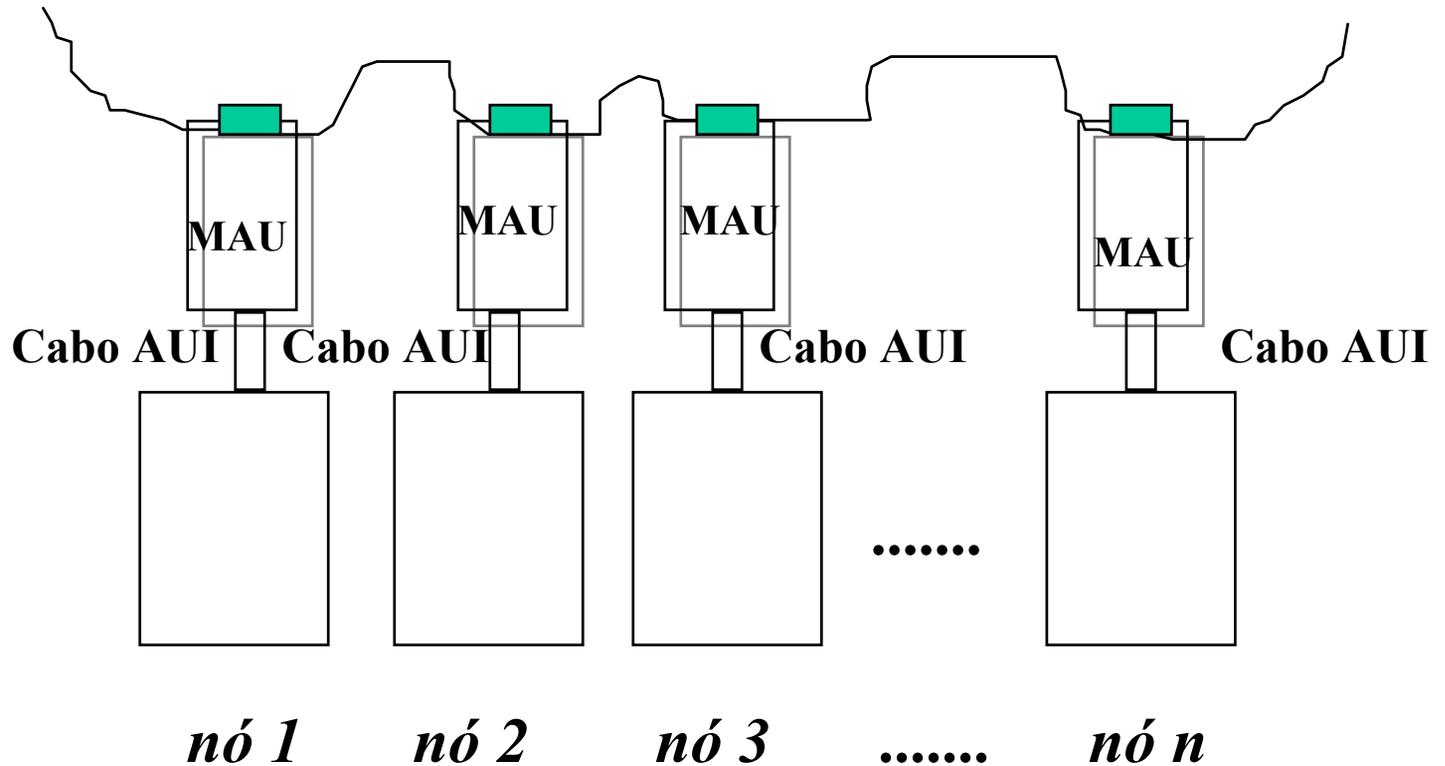
Cabos Coaxiais e Pares Trançados

Vamos a seguir conhecer as especificações do padrão IEEE 802.3 referente aos cabos coaxiais e pares trançados. A idéia é que possamos ter uma visão global destas especificações.



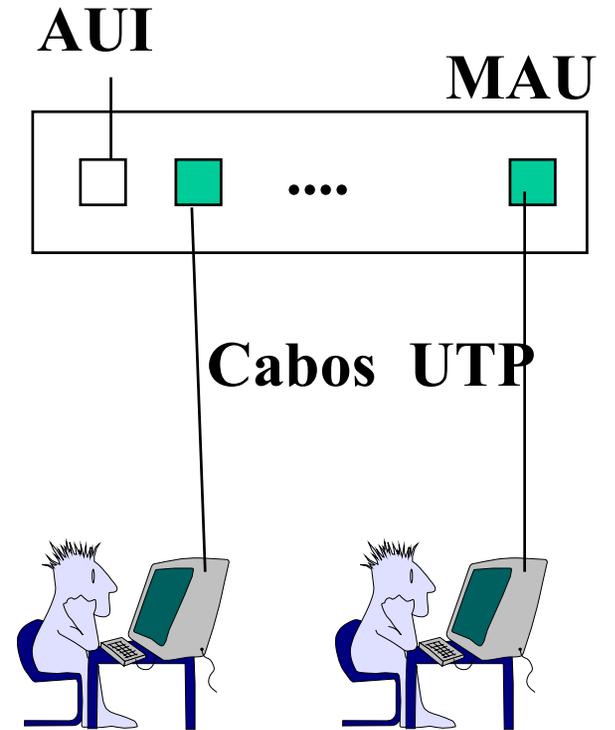
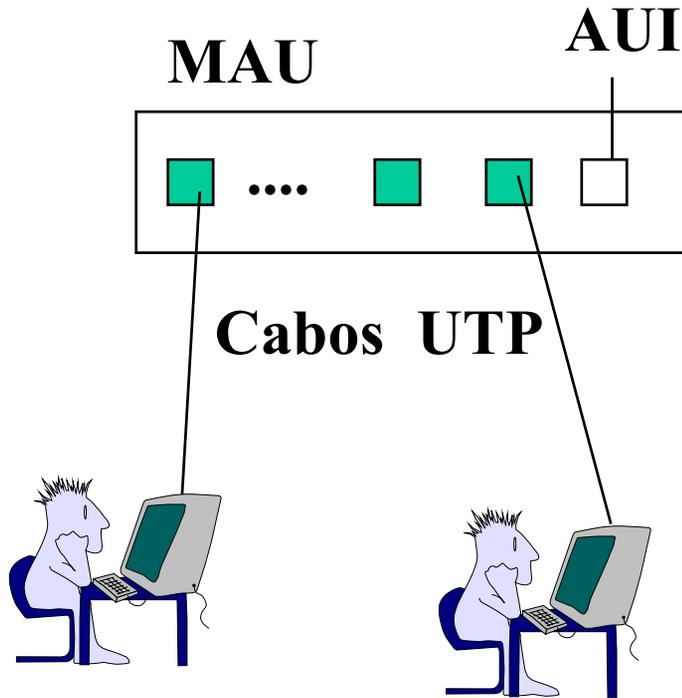
IEEE 10BASE2

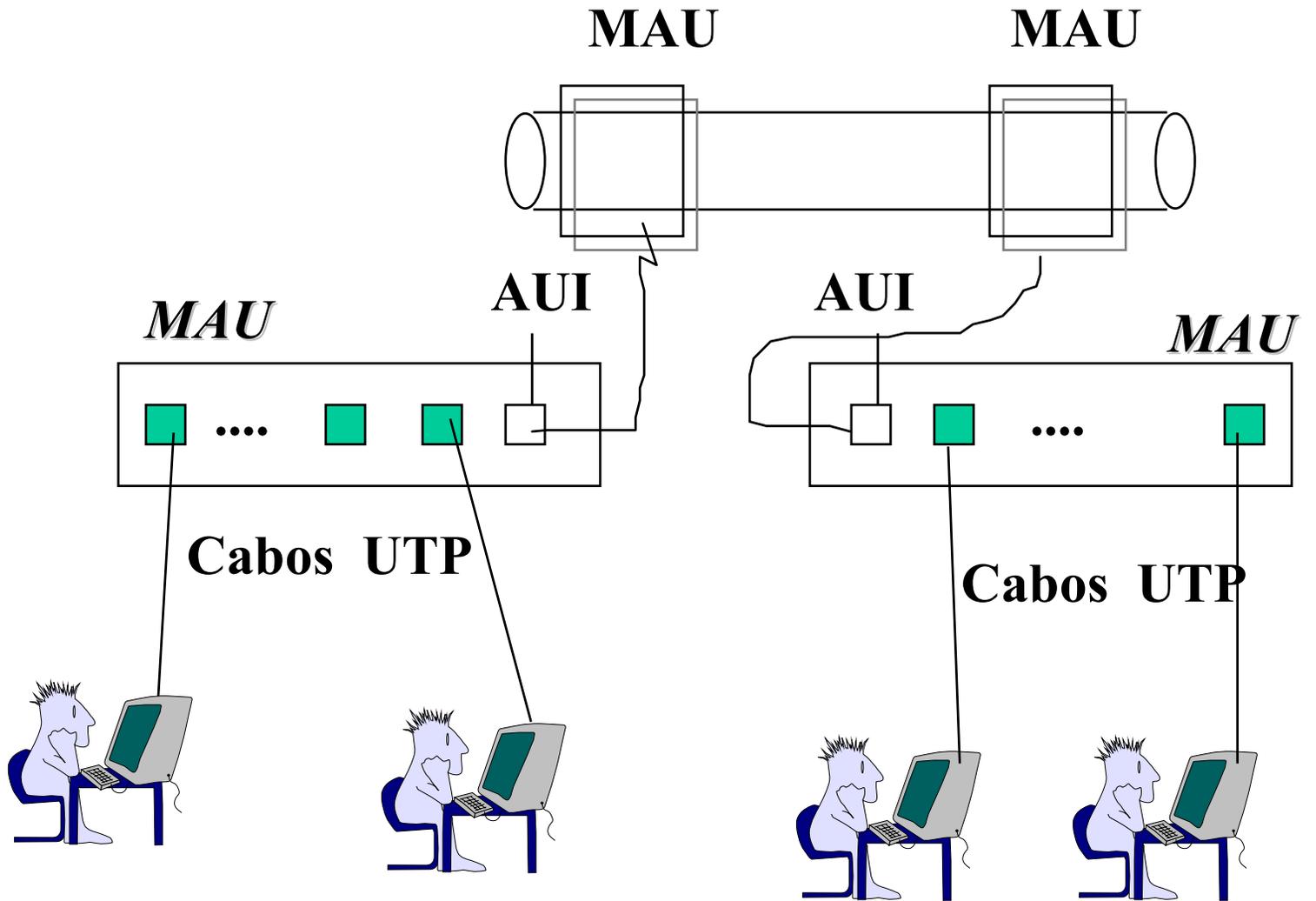
**Cabo Coaxial
Máximo de
185 metros**



O padrão 10BASE2 também é conhecido comercialmente como *Thinnet* ou *Cheapernet*.

IEEE 10BASET





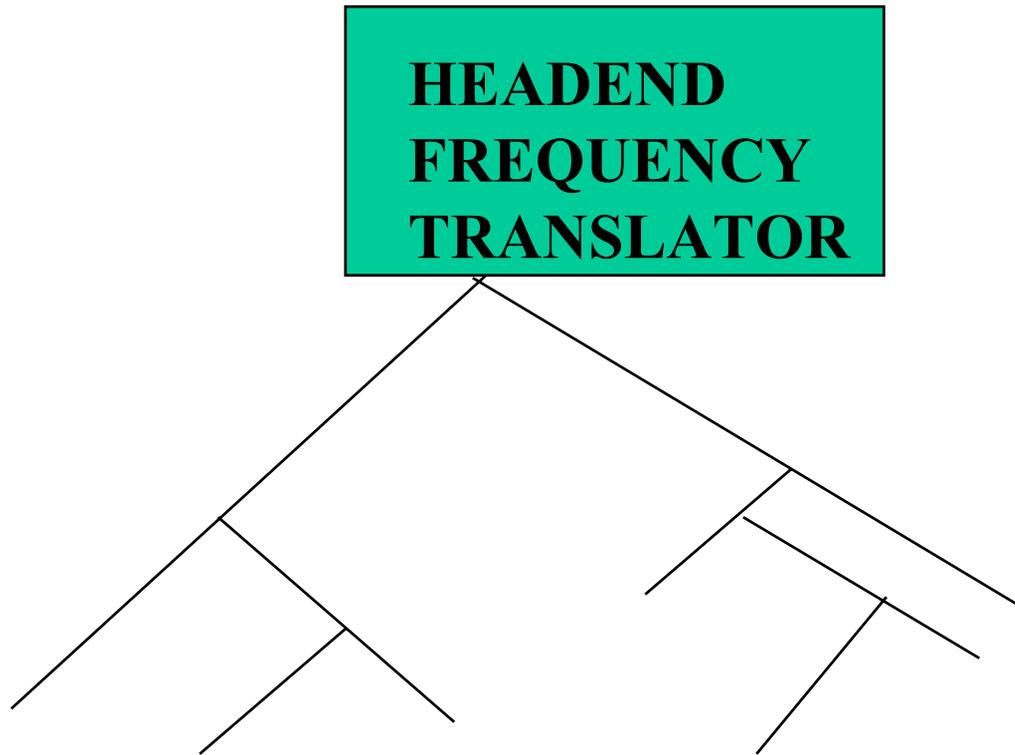
MAU - Medium Access Unit

MAU - Media Attachment Unit

IEEE 10BROAD36

Padrão IEEE 802.3 projetado para operar sobre um ambiente CATV (Community Antenna Television), ou TV a cabo.

Numa distância de até 3.6 Km é efetuada uma sinalização de 10 Mbps em Broadband. Este tipo de abordagem possui, ainda, no momento um pequeno mercado.



Uma rede de banda larga como uma árvore estruturada, com o requerimento de um tradutor de frequência no *headend*.

Regra 5-4-3

A versão original do Ethernet, baseada em cabo coaxial, fazia com que tivéssemos uma fácil configuração de rede como uma árvore estruturada.

O princípio básico do CSMA/CD é que um sinal transmitido dentro da rede deve alcançar todos os pontos num determinado intervalo de tempo. Em outras palavras, cada elemento que compõe a LAN (repetidores e pontes) que impõem um certo atraso na comunicação devem propagar o sinal transmitido sem que o retardo cause prejuízo ao método de CSMA/CD.

Regra 5-4-3

Desta forma, algumas regras foram criadas para que empiricamente os projetistas de rede tomassem os devidos cuidados para que a rede não perdesse performance, a medida que novas extensões ocorressem. Vamos então comentar uma regra denominada de 5-4-3.

A regra 5-4-3 estabelece que :

A transmissão entre dois nós numa rede Ethernet não pode percorrer mais do que 5 segmentos conectados por 4 repetidores com o máximo de 3 segmentos povoados.

Primeira parte da Regra - 5 segmentos

A existência de no máximo 5 segmentos entre quaisquer dois nós é baseada no fato do limite de 500 metros de cabo por segmento e o máximo de 2500 metros, resultando numa janela de colisão em um sentido de 23 us.

Importante lembrar que o máximo de uma LAN Ethernet é de 2500 metros composta da seguinte forma :

- 1500 metros de cabo com característica multiponto;
- 1000 metros de cabo adicionais para uma ligação ponto-a-ponto de dois segmentos.

Segunda parte da Regra - 4 repetidores

A existência de no máximo 4 repetidores vem estabelecer o *máximo delay* pelo qual os quadros Ethernet podem ser submetidos sem que ocorra um erro na análise da colisão.

Terceira parte da Regra - 3 Segmentos Povoados

A consideração de 3 segmentos povoados, ou seja segmentos com um ou mais dispositivos conectados, vem ratificar a atenção para o tempo de transmissão dos quadros em redes com cabeamento de cobre. Neste tipo de rede o retardo é bastante elevado, assim a regra 5-4-3 não se aplica as instalações onde cabos de fibra ótica são empregados.

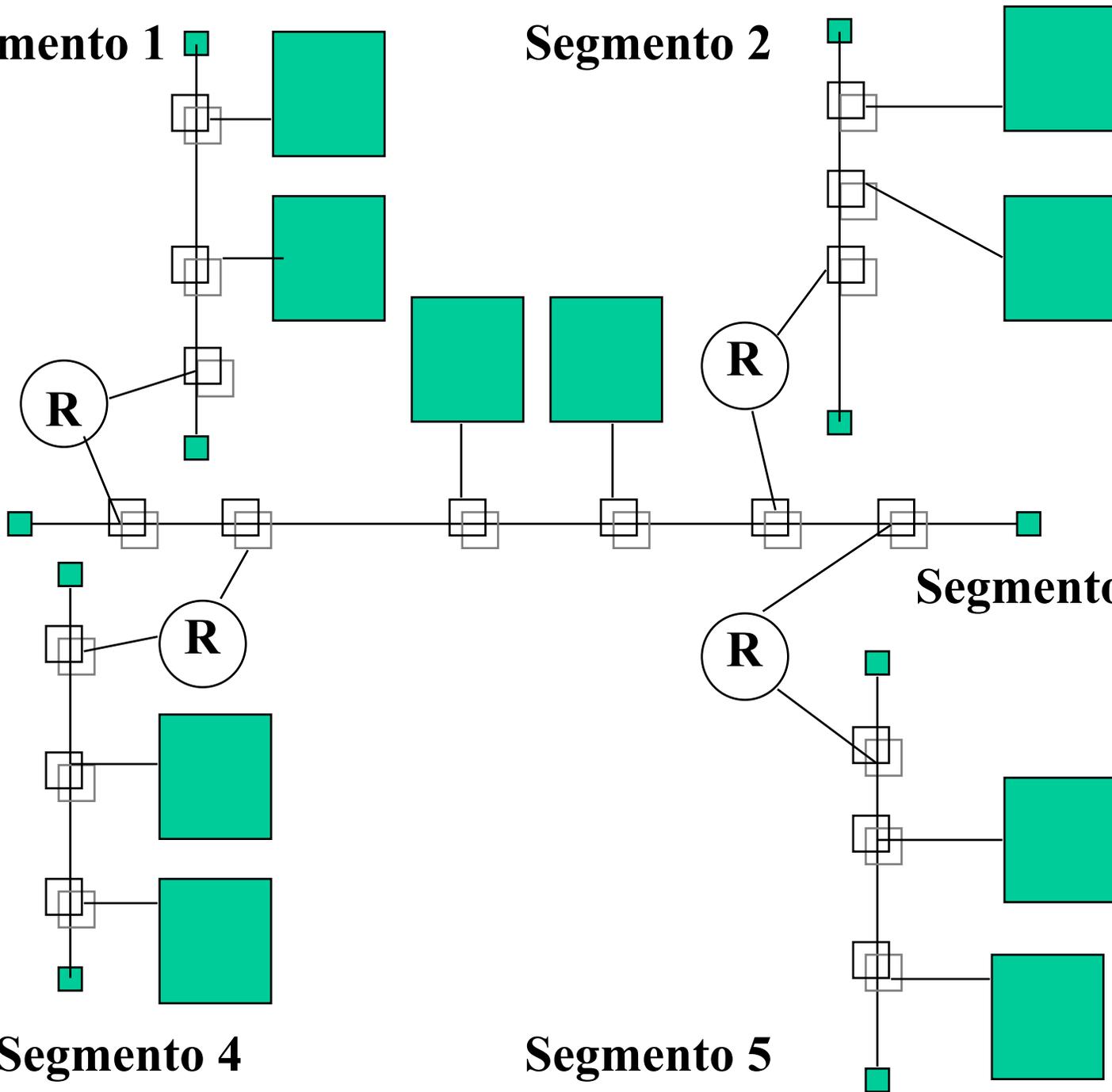
Segmento 1

Segmento 2

Segmento 3

Segmento 4

Segmento 5



3.7 - Fibra Ótica

O cabeamento de fibra ótica como mídia de comunicação oferece várias vantagens importantes quando comparado com o cabeamento baseado em cobre.

Os benefícios maiores são as suas características de enorme largura de banda e a baixa atenuação. Em adição, a mídia ótica não é afetada, e também não emite, ruído elétricos com altas frequências.

Fibra Ótica

A fibra possui algumas desvantagens :

- Geralmente seu custo é maior que os cabos de cobre. Existe uma tendência de queda , devido a (1) melhoria no processo de fabricação, e (2) que uma quantidade maior de fibra vem sendo empregada para aplicações de longa distância.

(Existem alguns tipos de fibra que são relativamente baratos, como por exemplo a POF (Plastic Optical Fiber), todavia estas fibras não atendem a alta demanda de transferência de dados e cabos longos para as implementações de LANs. Por esta razão o IEEE não tem nenhuma especificação de padrão para estes modelos fibras.)

Fibra Ótica

A fibra possui algumas desvantagens :

- Os conectores são mais onerosos e o processo de efetuar as conexões é mais complexo de ser efetuado. Neste processo, é necessário um pessoal especializado (e muitas vezes caro) para efetuar a instalação.

Fibra Ótica

A fibra possui algumas desvantagens :

- Devido ao uso do padrão IEEE 802.3 em 10 Mbps, uma enorme capacidade de largura de banda da fibra não é utilizada. Esta pequena utilização é devido a sinalização em banda base. Por esta razão, a fibra somente é empregada nas versões de Ethernet quando longas distâncias, necessidade de imunidade a ruído e segurança são importantes e o custo é um fator secundário.

Fibra Ótica

Nas especificações dos equipamentos MAU de fibra são comuns as determinações de duas fibras para que seja provido um caminho de sinalização para o envio e outro para o recebimento de mensagens.

Em todas as especificações é empregado uma fibra *multimodo de 62.5/125 um*. Onde 62.5 refere-se ao núcleo do cabo e 125 ao revestimento.

Fibra Ótica

Fibra Multimodo : todas as fibras consistem de grande número de subestruturas incluindo o núcleo, o qual carrega a maior parte da luz. O revestimento, faz com que a luz curve e se confine ao núcleo. Este é revestido de um nível de substrato, geralmente o vidro, que não carrega a luz e coberto por outros níveis que são responsáveis pela proteção do núcleo.

Numa fibra multimodo, o núcleo é relativamente maior do que a onda de luz que este carrega. Desta forma, a luz pode propagar-se pela fibra em diferentes caminhos, ou modos, daí o nome da fibra. Para se ter um exemplo, os núcleos na fibra multimodo variam de 50 a 1.000um, enquanto que a onda de luz tem 1 um.

Fiber Optic Inter-Repeater Link (FOIRL)

O *FOIRL* foi o primeiro padrão de fibra a ser definido. Semelhante ao padrão 10BASET requer o uso de repetidores para agir como centro principal para um grupo de *nós*.

Quando foi desenvolvido, o padrão FOIRL, foi restrito para a ligação apenas de repetidores distantes até 1km. Esta restrição foi estabelecida apenas no padrão, uma vez que não existia nenhum impedimento técnico para a ligação entre um DTE e um repetidor.

Fiber Optic Inter-Repeater Link (FOIRL)

Como o *FOIRL* utiliza diferentes caminhos para a sinalização de transmissão e recepção, o MAU em cada extremidade da fibra verifica as conexões para garantir a continuidade do enlace.

O padrão *FOIRL* especifica que um *signal inativo* é representado por uma transmissão de 1 MHz entre MAUs, na ausência do tráfego de pacotes de dados.

Fiber Optic Inter-Repeater Link (FOIRL)

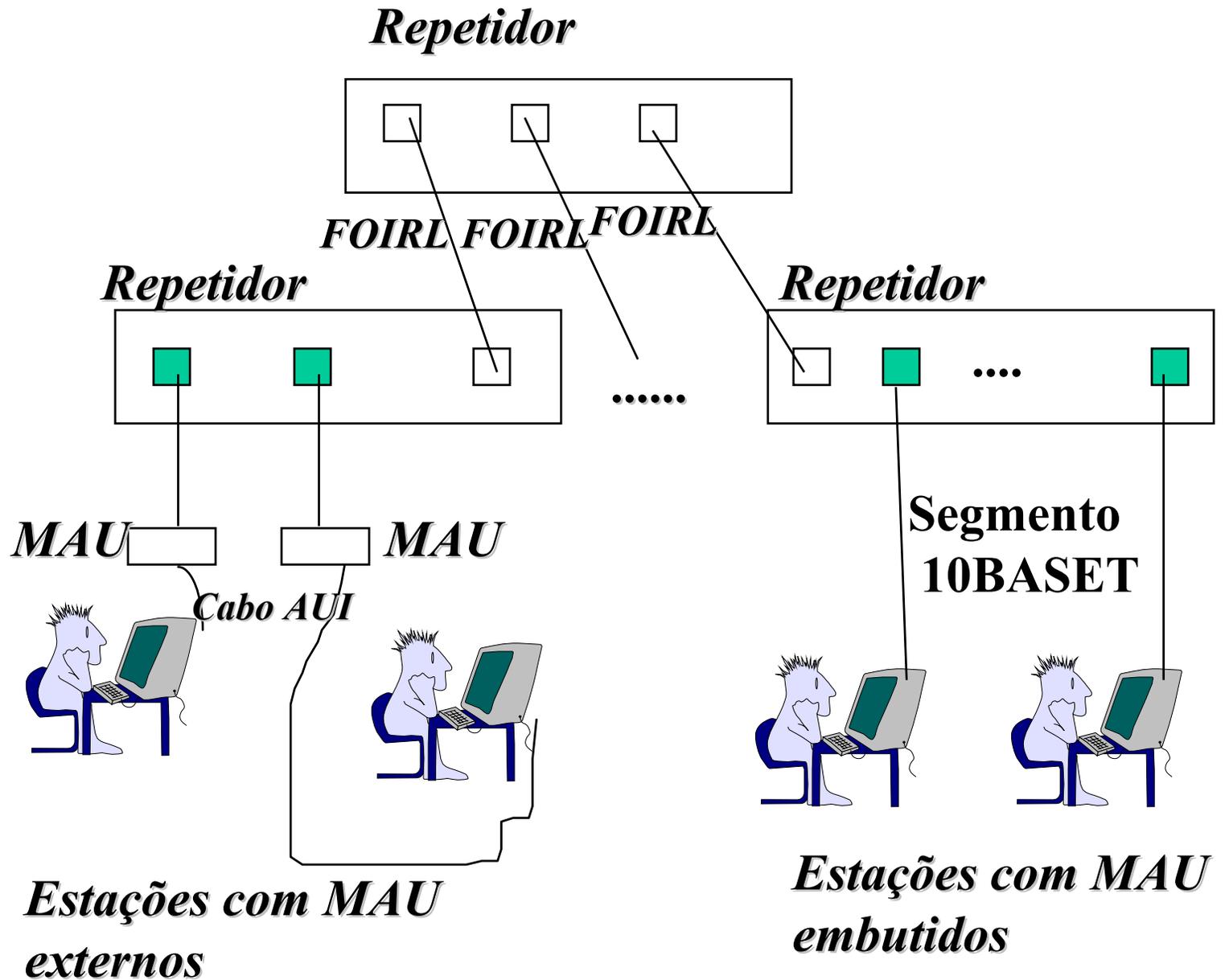
No caso da não detecção da atividade de 1 MHz, definida como *low-light condition*, o MAU entra em estado de *Link-Fail* (falha de enlace) e evita que um DTE ou repetidor transmita para a rede.

Semelhante aos repetidores 10BASET, o teste de pulso de enlace, ou seja o *FOIRL* sinal de não atividade, é passado somente entre MAUs. Isto significa que o mesmo não é passado entre o concentrador e o DTE.

O *FOIRL* emprega um conector denominado de *F-SMA* (plug-and-socket), utilizado entre o cabo de fibra e MAU.

10BASE-FL

O padrão *10BASE-FL* (*10BASE-Fiber Link*) foi projetado para substituir a especificação original *FOIRL*, permitindo a ligação não somente entre os repetidores mas também enlaces entre repetidor e DTE. A especificação *10BASE-FL* é compatível com o *FOIRL* em muitas funções, incluindo a sinalização de 1MHz de detecção de inatividade e o assincronismo entre pacotes e sinais de controle entre repetidores.



10BASE-FL

As melhorias do *10BASE-FL* sobre o *FOIRL* podem ser vistas pelos pontos :

- Extensão da distância entre os pontos para 2 Km;
- O conector BFOC (Bayonet Fiber Optical Connector), também conhecido como conector STa, é especificado para o cabo de fibra e para o MAU;

10BASE-FL

- A especificação da sinalização para o número de aumentos/quedas é relaxada, fato que permite a redução de exigência do drive de alimentação de potência elétrica;
- Outro fator interessante foi que a especificação adotou a mesma abordagem do padrão *10BASET* para o estado dos *nós* para o MAU. O que significa dizer que implementadores precisam apenas entender apenas um conjunto adicional de requisições para os MAUs

10BASE-FB

O padrão *10BASE-FB* (*10BASE-Fiber Backbone*) foi projetado como uma interface melhor de interconexão entre os enlaces de repetidores. O MAU *10BASE-FB* é essencialmente definido dentro do equipamento, ou seja não considera o AUI.

Uma sinalização de 2.5 MHz é usada para indicar que o caminho de transmissão está livre. Em adição, a transmissão entre de dados entre repetidores é sincronizada utilizando este sinal de 2.5 MHz.

10BASE-FB

Um exemplo da melhoria de performance do tempo de resposta de MAU com o padrão *10BASE-FB* pode ser observado pelo fato :

No caso do FOIRL a função de recebimento de pacotes do repetidor fica bloqueada por um relógio local durante o tempo de inatividade. Quando um preambulo é recebido, esta função do repetidor necessita de gastar alguns segundos para poder fazer uma reserva para processar a chegada dos pacotes.

10BASE-FB

As melhorias do *10BASE-FB* podem ser notadas por :

- Extensão da distância entre os pontos para 2 Km;
- O conector BFOC (Bayonet Fiber Optical Connector), também conhecido como conector STa, é especificado para o cabo de fibra e para o MAU;

10BASE-FB

- A existência de uma estratégia de sinalização que permite a detecção de uma falha remota, permitindo o MAU de uma ponta do enlace a indicação de *Jabber*, *Low Light* ou *perda de sincronismo* com o MAU da outra ponta.

10BASE-FB

O padrão *10BASE-FB* foi essencialmente projetado para servir como uma tecnologia de backbone, todavia não o suporte de muitas empresas de comercialização de produtos de rede. A razão foi a pequena base instalada e a adequação do padrão *FOIRL* para a base existente.

10BASE-FP

O padrão *10BASE-FP (Fiber Passive)* foi projetado para uma abordagem de topologia de estrela. A mídia da rede é composta pelo equipamento concentrador da estrela, que não possui elementos ativos, e o cabeamento ótico.

Cada sinal ótico que entra numa determinada porta é ecoado para todas as portas, inclusive aquela pela qual o sinal chegou. Desta forma, se múltiplos sinais chegarem simultaneamente no concentrador uma colisão irá ocorrer.

Para garantir uma detecção de colisão confiável, um MAU de fibra ótica passivo possui inúmeras diferenças de outros tipos de MAU do padrão 802.3.

10BASE-FP

Pela maior complexidade exigida pelos MAUs do tipo *10BASE-FP*, seu uso não é largamente suportado pelos vendedores da área de rede.

O uso do padrão *10BASE-FP* é localizado à aqueles casos onde, por exemplo, o sinal elétrico/potência não estão disponíveis.

IV - Fast Ethernet

4.1 - Introdução

As inúmeras vantagens da implementação 10BASE-T induziram pesquisadores e técnicos a proposição de desenvolvimento de um novo padrão de produtos a 100 Mbps.

O desenvolvimento da nova especificação foi caracterizado pelo surgimento de dois grupos de trabalhos, estes são apresentados a seguir :

- Grupo I - aqueles que acreditavam que o Ethernet MAC deveria ser mantido, modificando-se o mínimo para atingir 100 Mbps;
- Grupo II - os participantes desta segunda corrente acreditavam que o protocolo CSMA/CD deveria ser substituído.

4.2 - Grupo I

Os principais paradigmas desta corrente de desenvolvimento foram baseados nos seguintes aspectos :

- fazer trocas mínimas nas operações do protocolo MAC ;
- adicionar funções ao nível físico e repetidores;
- suportar várias categorias de cabos UTP (com ênfase inicial na Categoria 5) e fibra ;

A proposta do Grupo I foi baseada nos seguintes fatos :

- O *bom nome* da tecnologia *Ethernet* ;
- A grande base instalada de hardware e software;
- O grande número de profissionais que conheciam a tecnologia Ethernet;

Este grupo ficou conhecido como 802.3 u Task Force e desenvolveu o padrão 100 Mbps baseado em *melhorias* em cima do especificação original Ethernet.

A *disputa* para o desenvolvimento da padrão *Fast Ethernet* foi cercado por inúmeras brigas técnicas, políticas e de marketing.

O Grupo I foi apoiado por um grande número de empresas fabricantes de dispositivos de rede, auto denominados de *FEA (Fast Ethernet Alliance)*.

4.3 - Grupo II

O Grupo II acreditava que o protocolo de MAC da Ethernet, o CSMA/CD, poderia ser substituído por um protocolo de acesso ao meio mais eficiente. Em adição seria, semelhante ao Grupo I, necessário uma nova definição de funções na camada física e repetidores. Esta nova definição é essencial para o suporte de uma grande variedade de topologias que empregam os cabos UTP e fibra ótica.

Este grupo formou o 802.12 Task Force e desenvolveu um novo protocolo de acesso ao meio. O novo MAC desenvolvido foi batizado de *Demand Priority Access Method (DPAM)*.

4.4 - Final Score

Ao final, foi aprovado pelo IEEE as duas propostas de especificações de 100Mbps. Estes padrões foram normalizados como IEEE 802.3 u e IEEE 802.12.

A especificação 802.3u, chamada de 100BASE-T ou *Fast Ethernet*, devido ao marketing original do poderoso nome 802.3 foi abraçada pela maioria dos fabricantes de produtos de rede. Embora, seja reconhecido o valor das alterações efetuadas pela especificação 802.12 (também conhecida como 100VG-AnyLAN).

4.5 - FAST ETHERNET

O *Fast Ethernet* é o termo empregado para referência a uma série de três especificações físicas de LANs de 100Mbps, descritas no IEEE 802.3 uS (um addendum do padrão 802.3).

As três especificações do *Fast Ethernet* são :

- 100BASE-T4
- 100BASE-TX
- 100BASE-FX

As três especificações mantêm o uso do protocolo de controle de acesso CSMA/CD e função dupla de velocidade de 10/100 Mbps na rede. Isto significa que o investimento nas NICs 10 Mbps são preservadas e que o futuro *upgrade* para 100 Mbps pode ser efetuado sem traumas ou gastos adicionais na rede.

O custo de um ambiente de 100 Mbps foi *estabelecido* que seria em torno de 2 vezes o custo de uma configuração de 10 Mbps. A idéia do grupo que desenvolveu a tecnologia era :

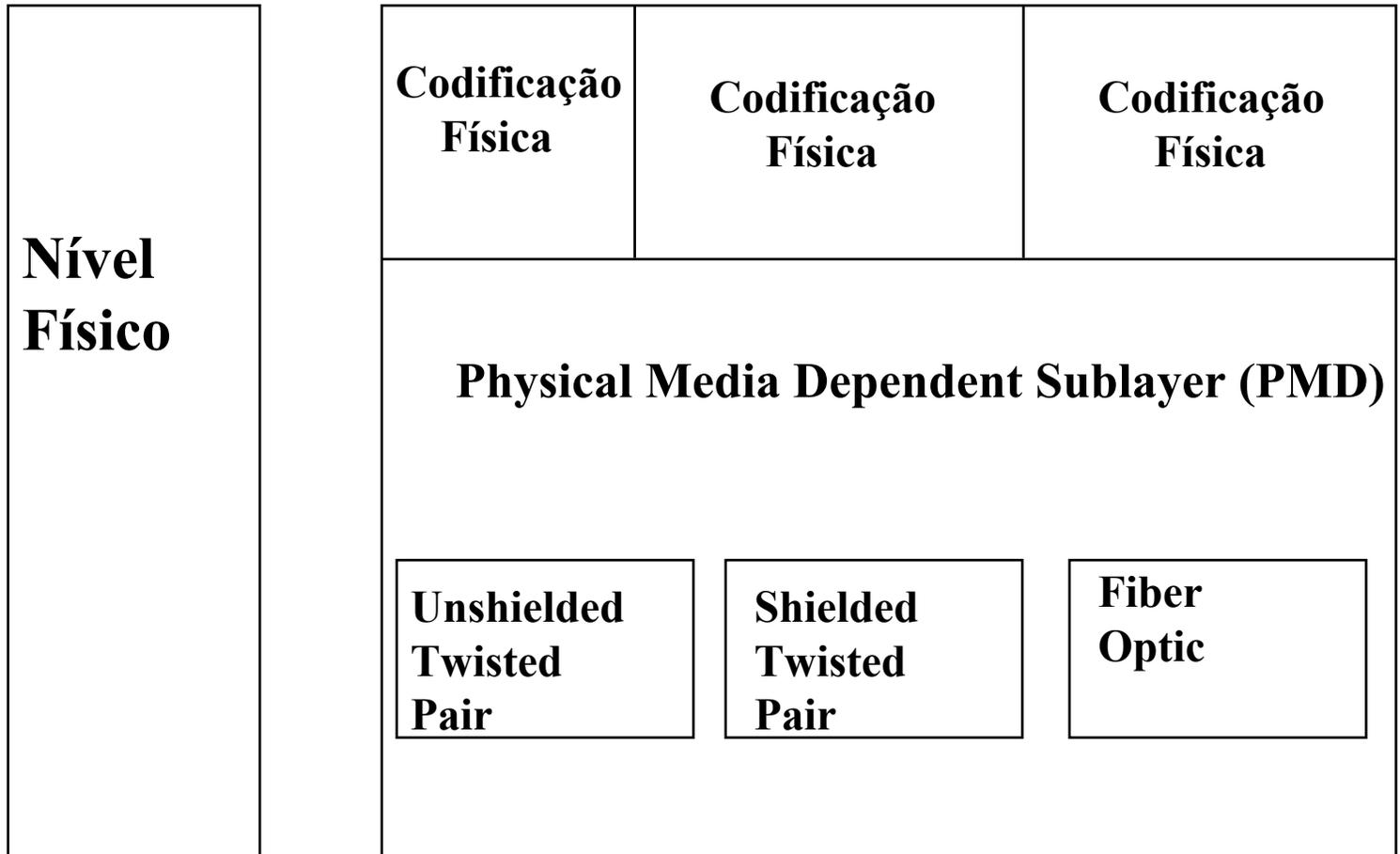
“10 vezes o aumento de performance pelo preço de 2”

4.6 - Subdivisão do Nível Físico

Da mesma forma que o nível de enlace foi subdividido na especificação IEEE 802.3 uS, o nível físico também o foi.

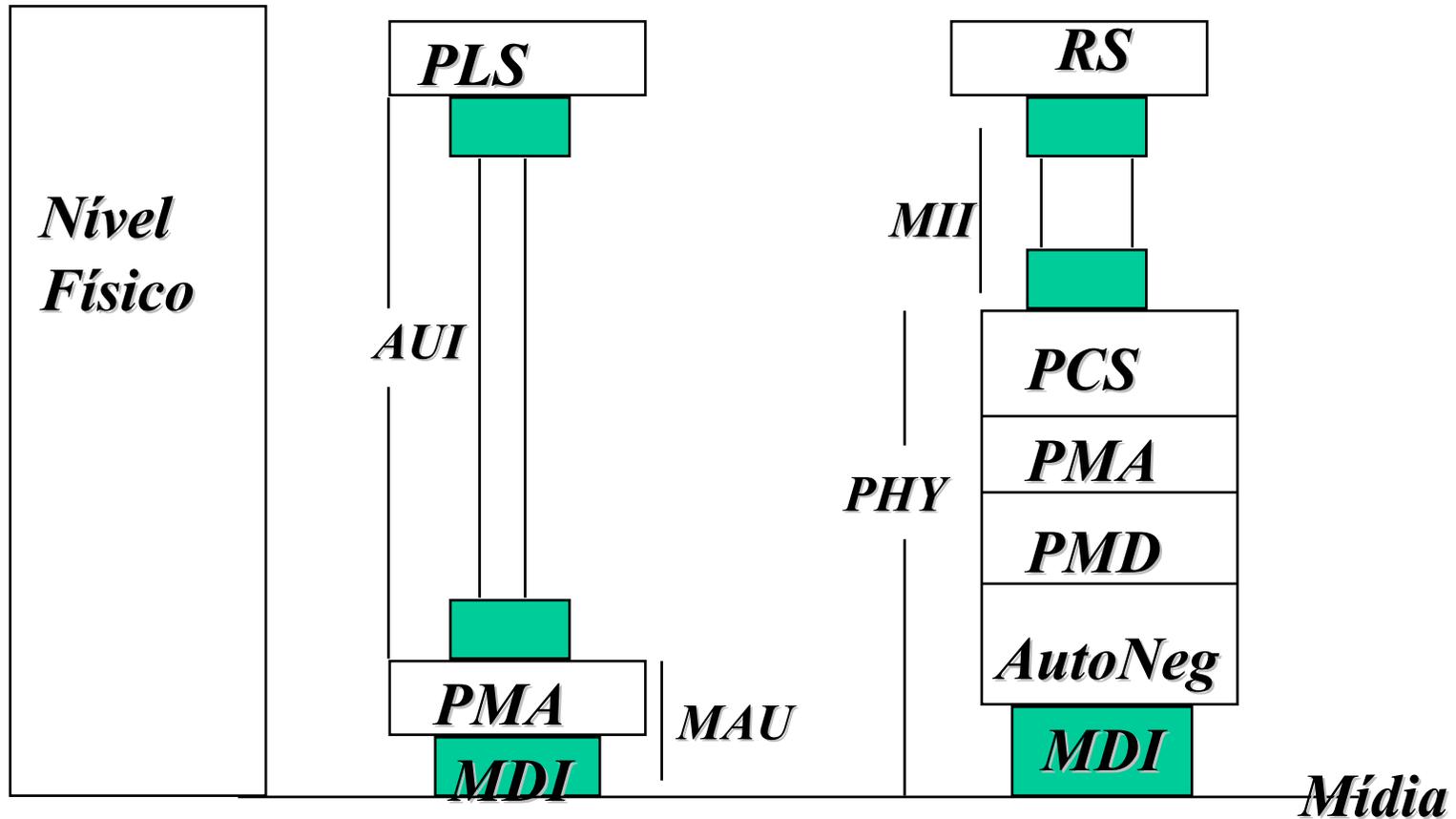
A idéia da subdivisão do meio físico foi baseada nos três diferentes tipos diferentes de mídias : par trançado (UTP), par trançado blindado (STP) e o cabo de fibra ótica.

Fast Ethernet
Subdivisão do Meio Físico



10 Mbps

100 Mbps



Nível Físico 10 Mbps

PLS (Physical Layer Signaling) - especifica o esquema de sinalização empregado. No caso de 10 Mbps o *PLS* é implementado empregando a função Manchester de codificação/decodificação;

AUI (Attachment Unit Interface) - é a interface de conexão de um *nó* ou *repetidor* para um MAU;

PMA (Physical Medium Attachment) - é a porção do MAU que contém a circuitaria responsável pela interface dos circuitos do AUI para uma específica mídia.

MDI (Medium Device Interface)

Nível Físico 100 Mbps

RS (Reconciliation Sublayer) - mapeia o funcionamento do MAC para sinais elétricos da interface MII;

MII (Medium Independent Interface) - é a interface lógica de sinalização equivalente a 10 Mbps AUI. A MII faz a conexão dos níveis RS e PCS, permitindo que múltiplos tipos de mídias sejam interconectados ao subnível MAC;

PCS (Physical Coding Sublayer) - faz a função de codificação para os dispositivos ligados a uma rede 100Base-T;

Nível Físico 100 Mbps

PMA (Physical Medium Attachment) - é a porção do MAU que contém a circuitaria responsável pela interface dos circuitos do AUI para uma específica mídia;

PMD (Physical Medium Dependent) - é a porção do *PHY*, ou nível físico, responsável por fazer a interface com a mídia física;

AutoNeg - um algoritmo que permite que dispositivos com diferentes tipos de velocidade (10, 100 e 1000 Mbps) possam efetuar seus enlace através de uma negociação (exemplo : full ou half-duplex).

Diferenças entre 10 e 100 Mbps

- *MII vs AUI*

É importante observar que a função exercida pela interface *MII* é a mesma que a da *AUI* - fazer a decomposição a nível de MAC para diferentes níveis físicos.

A interface *AUI* não é recomendada para altas velocidades de dados devido as altas frequências envolvidas.

A interface *MII* ao invés de utilizar uma abordagem de *bit-serial* como o *AUI*, a interface utiliza 4-bits (*nibble*) em cada direção de transmissão e recepção. Esta opção permite que possamos ter uma frequência de 25 MHz ao invés de 100 MHz, caso uma interface de um bit foi usada.

Diferenças entre 10 e 100 Mbps

Algumas outras características interessantes da *MII* são :

- permitir a gerência e controle de erro dedicado entre o MAC e o PHY;
- um outro fator importante observado na implementação da *MII* foi o número de pinos de sinal, uma vez que a interface deveria atender também ao padrão 10 Mbps. A interface emprega um conector de 40 pinos para acomodar 18 pinos de sinal (dados transmitidos e recebidos, sinal de clock, controle de erro e detecção de colisão);
- uma outra diferença refere-se a distâncias, a *AUI* permite um comprimento de até 50 metros e a *MII* de 0.5 metros

Diferenças entre 10 e 100 Mbps

- Reconciliation Sublayer (RS)

A função do *RS* é a manutenção das características do padrão Ethernet original. Assim, o *Reconciliation Sublayer* converte informações originais do MAC de bit-serial para uma informação definida pela *MII*

Diferenças entre 10 e 100 Mbps

- Operação em Velocidade Dual (10 e 100 Mbps)

Durante o desenvolvimento do 100 Mbps, a base instalada de dispositivos de rede de 10 Mbps já era cerca de dezenas de milhões. Assim, foi desenvolvido um protocolo denominado de *Auto-Negotiation*.

A negociação de velocidade ocorre sem a intervenção do usuário e permite também a determinação de transmissão em half e full-duplex.

Diferenças entre 10 e 100 Mbps

O funcionamento da função *Auto-Negotiation* ocorre da seguinte forma :

- O dispositivo transmite um conjunto de pulso especiais (*special pulse train* ou *Fast Link Pulse Burst*) depois de ser ligado;
- O dispositivo deverá reconhecer um pulso semelhante do *dispositivo parceiro de enlace* com o qual está se conectando;
- Se o dispositivo reconhece que o *dispositivo parceiro de enlace* é compatível com sua forma operacional, o chamado modo ótimo é selecionado e os dispositivos mudam para o estado operacional.

Diferenças entre 10 e 100 Mbps

- Categoria de Cabos e Número de Pares Trançados

Na Ethernet 10 Mbps é possível a utilização híbrida de cabos coaxiais e trançados na instalação o mesmo instante. Ou seja é possível termos um *thick-wire* no qual são conectados dispositivos (exemplo: *hubs*) onde existem conexões em UTP.

No caso do padrão 100 Mbps não é permitido a *mistura* de cabeamento, assim todas as ligações são efetuadas ponto-a-ponto usando UTP, STP ou fibra ótica como um enlace permitido.

Diferenças entre 10 e 100 Mbps

- Categoria de Cabos e Número de Pares Trançados

O padrão 100 Mbps inicialmente suportava três tipos de cabos de pares trançados, duas versões para a UTP categoria dos tipos 3 e 5 e uma versão para STP.

A especificação 100BASE-TX define operação em dois pares da categoria 5 ou STP. Por outro lado, a 100BASE-T4 estabelece a operação sobre 4 pares da categoria 3. Já a operação em fibra, 100BASE-FX, estabelece um par de 50/100 um

Diferenças entre 10 e 100 Mbps

- Categoria de Cabos e Número de Pares Trançados

Uma outra especificação, a 100BASE-T2, mais recentemente desenvolvida, define operação em dois pares da categoria 3.

Diferenças entre 10 e 100 Mbps

- Topologia

O diâmetro de abrangência de uma rede 100BASE-T é reduzida quando comparada com uma rede 10BASE-T. As razões para esta diferenças são :

- redução do *bit-time*;
- o efeito direto da redução do *bit-time* no parâmetro *round-trip delay*;

Visando diminuir os efeitos das restrições topologias, dois tipos de repetidores foram definidos. Estes são conhecidos como Classe I e Classe II.

100BASE-T4

A especificação *100BASE-T4* representa uma rede 100 Mbps, CSMA/CD, que opera sobre quatro pares da Categoria 3, 4 e 5 de cabos de pares trançados sem blindagem (UTP), ou com blindagem (STP).

O padrão *100BASE-T4* é similar ao *10BASE-T*, ou seja é uma rede baseada no concentrador (ou Hub). A diferença de paradigma está baseada na melhor detecção de colisão através da redução permitida da área da rede.

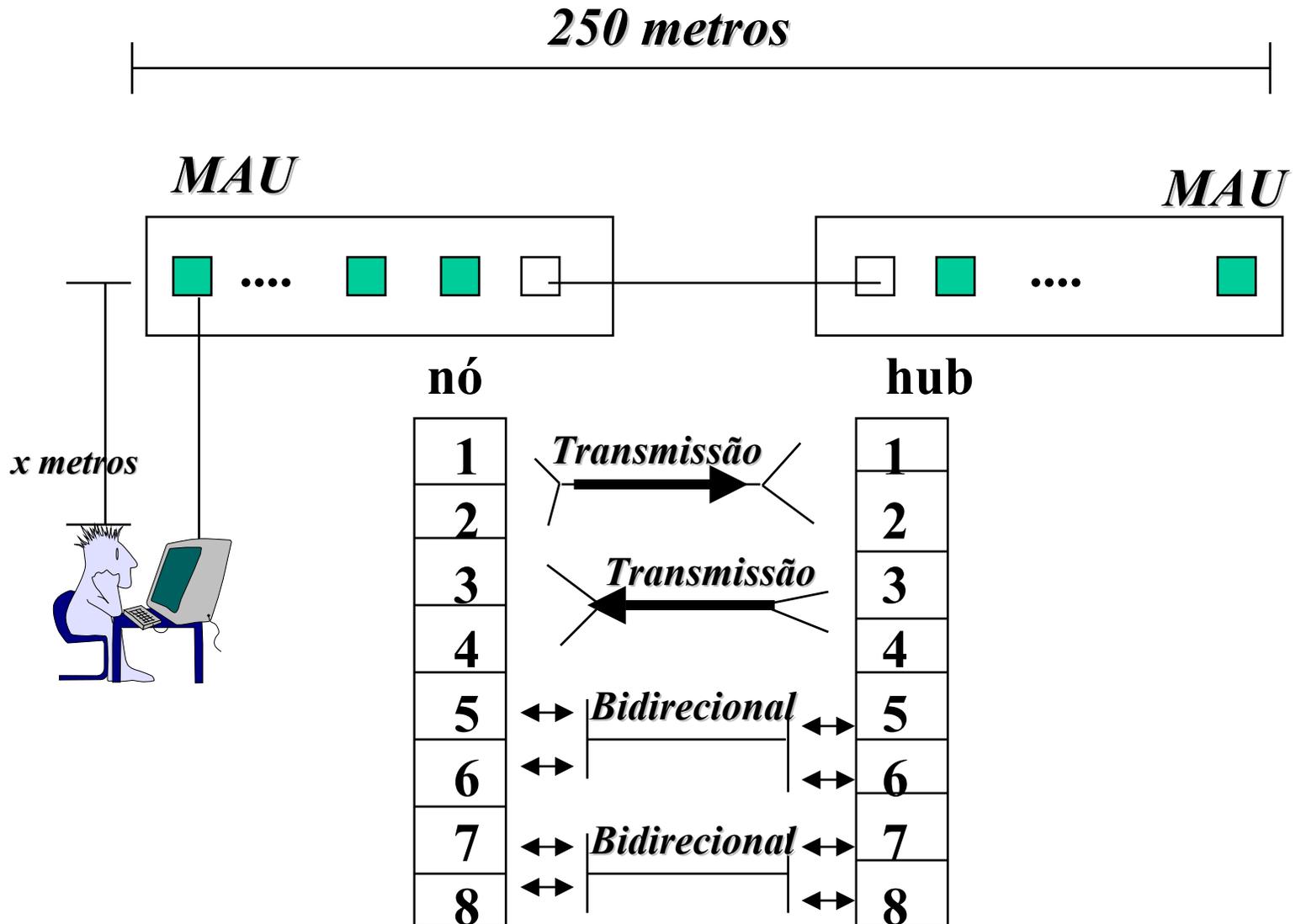
Uma rede *100BASE-T4* permite uma distância de no máximo de 250 metros e a distância entre um *nó* e um *Hub* é de 100 metros.

100BASE-T4

Para obtenção de velocidade de 100Mbps requer três alterações no nível físico :

- três pares de cabos são usados para a transmissão (o quarto é empregado para detecção de colisão), isto prove uma melhoria três vezes quando comparado com o 10BASET;

IEEE 100BASE-T4



100BASE-T4

Observações:

- (1) A figura anterior ilustra as dimensões permitidas no padrão. Importante observar que a distância máxima de 250 metros deve levar em conta a distância do *Hub* ao *nó*. Ou seja, os 250 metros da figura já considera os x metros do *nó* mais distante.
- (2) As conexões usadas para o 100BASE-T4 são RJ-45, que simplificam as conexões de cabos a *Hubs* e *nós*.

100BASE-T4

Observações:

(3) A figura, assim como numa configuração 10BaseT, ilustra que dois pares são empregados para a detecção da colisão. Isto é os pares de transmissão no sentido *Nó-Hub e Hub-Nó*, assim que detectam recepção na porta oposta (ou seja, no *Hub* a porta de recepção do *Nó* e no *Nó* a porta do *Hub*) e estes estão transmitindo é evidenciada a situação de colisão.

100BASE-T4

- a codificação 8B6T é utilizada. Nesta codificação, 8 bits de entrada são transformados em um código único de 6 símbolos ternários. Esta codificação substitui a Manchester aumentando o *throughput* para 256 vezes quando comparado com o 10BASE-T.



Por que 256 vezes ?



Podemos fazer a transmissão de 2^8

Codificação 8B6T

Exemplo - Considere a transmissão do seguinte conjunto de bits :

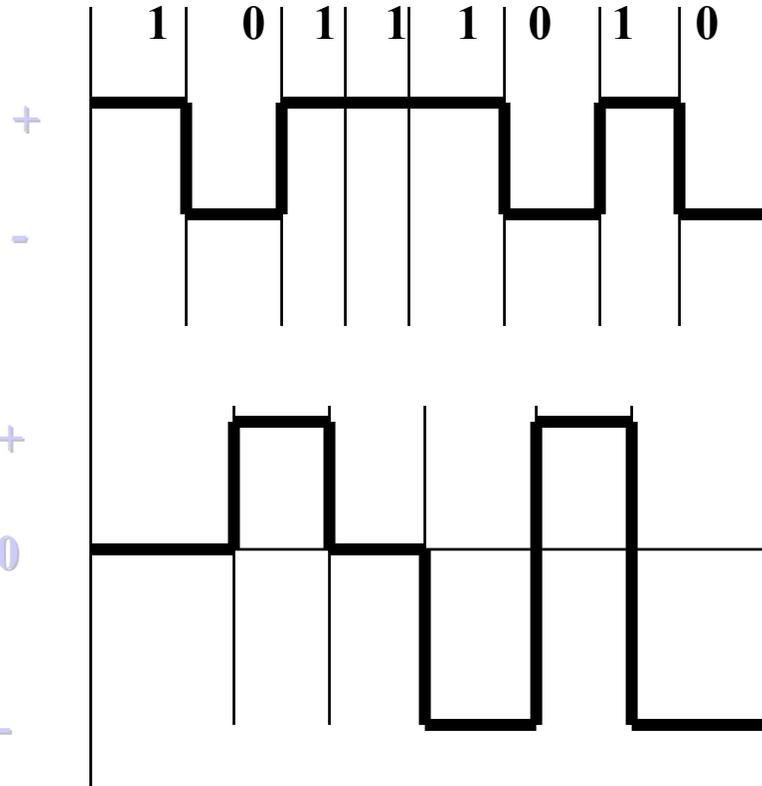
1 0 1 1 1 0 1 0 .



Como você imagina que esta transmissão será efetuada empregado a codificação 8B6T ?

Codificação 8B6T

Conjunto de 8 Bits



*Codificação
6 Ternaria*

Codificação 8B6T

Considerando o exemplo da transmissão do conjunto de bits 1 0 1 1 1 0 10 (BA, em hexadecimal), teríamos :

0 + 0 - + -

100BASE-T4

- a última alteração foi a modificação do relógio de sinalização de velocidade de 20 MHz para 25MHz. Esta mudança representou um aumento de 1.25 vezes em relação ao padrão 10BASE-T.



Por que 25 MHz ?



$$***100 \times (6/8) / 3 = 25 \text{ MHz}***$$

100BASE-T4

Quando as três alterações são efetuadas, o padrão 100BASE-T4 tem uma performance 10 vezes superior ao 10BASE-T, ou seja 100 Mbps.

100BASE-TX

A especificação *100BASE-TX* representa um segundo tipo de rede 100 Mbps, CSMA/CD, que opera sobre dois pares da Categoria 5 de cabos de pares trançados sem blindagem (UTP). Um par de fios é usado para detecção de colisão e recepção de dados.

O uso de dois pares de fios requer troca do relógio de velocidade e método de codificação. O *100BASE-TX* usa 125 MHz de frequência e uma codificação conhecida como 4B5B.

100BASE-TX

Na codificação 4B5B, a cada 4 bits estes são mapeados num código de 5 bits. Porque este método requer apenas 16 símbolos para representação dos dados, os demais símbolos são empregados para controle.

O uso da alta frequência no 100BASE-TX este só pode ser implementado em cabos da categoria 5. Por outro lado, cabos das categorias 3 e 4 podem ser utilizados na especificação 100BASE-T4 por causa dos 25 MHz de velocidade do clock de transmissão.

100BASE-TX

Semelhante ao 100BASE-T4, o padrão 100BASE-TX restringe o limite da rede para até 250 metros e a maior distância entre um *hub* e um *nó* é de 100 metros.

100BASE-FX

A especificação *100BASE-FX* representa o terceiro tipo de rede 100 Mbps, CSMA/CD, que opera sobre uma fibra (padrão 62.5/125 micron) multimodo.

A fibra possui um caminho para a transmissão e outro para a recepção, o cruzamento do sinal é efetuado pelo adaptador da rede.

A transmissão é efetuada usando uma onda de luz de 1350 nm e o segmento máximo permitido é de 412 metros.

A codificação adotada no *100BASE-FX* é idêntica a segunda versão do Fast Ethernet (100BASE-TX).

100BASE-FX

O padrão aceita três conectores :

- O conector SC foi projetado para facilitar o uso e pode ser empurrado levemente para que seja colocado no seu lugar ;
- O conector MIC (Media Interface Connector) representa o conector padrão usado em redes locais FDDI. Este foi projetado para facilitar a interconexão, assegurando que o cabo está devidamente conectado ;
- O conector ST que é caracterizado por uma chave interna. A conexão é efetuada alinhando-se o conector a chave interna, que posteriormente é fechada.

Repetidores Fast Ethernet

O padrão *Fast Ethernet* prove a opção de dois tipos de repetidores, denominados de Classe I e Classe II.

O repetidor de Classe I opera da seguinte forma :

- (a) Primeiro traduzindo o sinal na porta de chegada para um determinado formato digital ;
- (b) Depois re-traduzindo o sinal digital para um sinal apropriado para a transmissão na porta de saída.

Repetidores Fast Ethernet

A operação de tradução e re-tradução consome, como era de se esperar, um tempo considerável neste tipo de repetidor.

Por outro lado, um repetidor *Fast Ethernet* da Classe I é a opção correta para ser utilizado onde diferentes segmentos de *Fast Ethernet* existem (exemplo : *100BASE-T4* e *100BASE-TX*).

Num dado ambiente de *Fast Ethernet*, quando o tamanho máximo de cabo é utilizado, somente um repetidor da Classe I pode ser usado. A razão para esta restrição é o enorme tempo gasto nas traduções/re-traduções, operações estas que podem prejudicar o domínio de colisões.

Repetidores Fast Ethernet

O repetidor da Classe II é utilizado naqueles ambientes onde somente segmentos com idênticos métodos de sinalização são empregados.

Assim, um repetidor da Classe II pode ser encontrado exclusivamente com segmentos de um tipo de *Fast Ethernet*, ou seja *100BASE-TX*, ou *100BASE-T4* ou *100BASE-FX*.

Como o tempo de propagação no repetidor da Classe II é pequeno, até dois repetidores podem ser usados em conjunto numa rede quando considerando o tamanho máximo.

Switched Ethernet

Solução de rede Ethernet conhecida como *Switched Ethernet* começou a aparecer no mercado no ano de 1993, na época que foi iniciado o desenvolvimento do *Fast Ethernet*.

As duas tecnologias começaram a interagir culminando num grande quantidade de troca de funções complementares entre as duas tecnologias.

Fast Ethernet (802.3 u), *Full Duplex Ethernet (802.3 x)* e *VLAN Tagging* foram iniciados e implementados como uma iniciativa da indústria para a migração de redes Ethernets de alto desempenho de uma base de mídia compartilhada para uma tecnologia de switching.

Switched Ethernet

- Switches de Nível 2

Um dispositivo denominado de *switch de nível 2* são na verdade *pontes (bridges)*. A razão para a denominação de *switch de nível 2* vem dos dois seguintes aspectos :

(1) Este dispositivo efetua a maioria de suas funções a nível de hardware. Por outro lado, uma *bridge* e um dispositivo orientado (ou baseado) por software - este software faz a filtragem, aprende a configuração e repassa quadros dentre outras funções.

Os *switches* utilizam *ASIC (Application Specific Integrated Circuit)*, que são chips que efetuem determinadas funções.

Switched Ethernet

(2) Uma razão de mercado da migração do *bridging* para o *switching* foram as sérias limitações apresentadas pelas *bridges* (exemplos : *tempestades de broadcast, instabilidade topológicas*).

Switched Ethernet

Um switch, semelhante a uma bridge, permite que múltiplas portas estejam ativas simultaneamente. Um switch possui ainda outras características que podem ser implementadas em hardware, tais como :

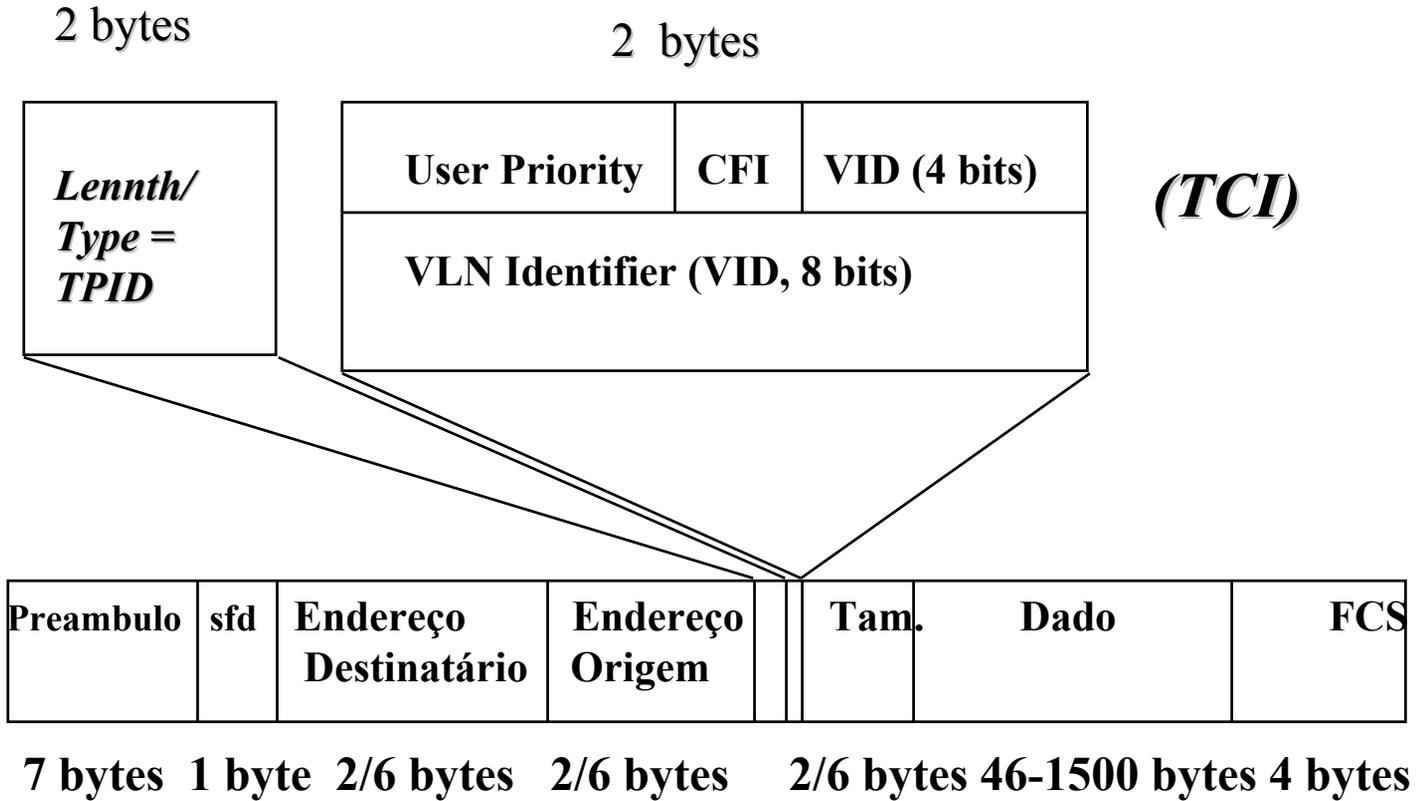
- operação de portas nos modos de half e full-duplex;
- *sensibilidade* para detecção de 10 e 100 Mbps por porta;
- *aprendizagem de performance*;
- classificação do tráfego ;
- sofisticado sistema de gerenciamento.

Switched Ethernet

Um switch pode ainda ter *feature* para *VLAN Tagging*.

VLAN Tagging, definido nos padrões IEEE 802.3ac e 802.1Q, é um campo de 4 bytes inserido no quadro Ethernet original entre os campos do endereço do remetente e o campo tipo/tamanho. Este campo permite a identificação de diferentes redes lógicas VLANs.

Formato do Quadro VLAN Tag (802.3 ac)



IEEE 802.3 ac

Formato do Quadro VLAN Tag (802.3 ac)

Observações :

- Como o *tag* é inserido dentro do quadro, este é considerado um *tag* intruso e não um simples encapsulamento;
- A inserção do campo de *tag* significa que o CRC deverá ser recomputado todas as vezes que este for inserido ou retirado;
- O tamanho do quadro ficará 4 bytes maior quando o *tag* estiver presente.

Formato do Quadro VLAN Tag (802.3 ac)

Observações :

- O padrão 802.3 foi alterado para aceitar o *tag*. Assim, os quadros Ethernet passando a ser caracterizados entre 64 até 1522 bytes. Os quadros que têm o campo VLAN EtherType *setado* é esperado que o quadro tenha um tamanho máximo de 1522 bytes, caso contrário o quadro deve ter 1518 bytes.

Formato do Quadro VLAN Tag (802.3 ac)

Os dois campos de 16 bits do *VLAN Tag* são:

(1) *VLAN Tag Protocol Identifier (TPID)* - é globalmente atribuído e reservado o campo EtherType com o valor 0x81-00.

(2) *Tag Control Information* - é composto dos três campos :

- *prioridade do usuário* - campo de 3 bits que pode ser composto de até 8 níveis de prioridade e existe em todos os quadros *VLAN Tag*. As prioridades estão especificadas na recomendação 802.1p. Os fabricantes usamna prática poucos valores de prioridade. O valor 0 é o maior e o 7 o maior. Este campo permite que tenhamos o conceito de *classe de serviço* suportados em redes Ethernets.

Formato do Quadro VLAN Tag (802.3 ac)

- *Canonical Formt Indicator (CFI)* - este é um campo de um bit que seu uso real foi projeto para o encapsulamento de um quadro *Token-Ring*. Embora não exista menção deste fato no documento 802.3 e os fabricantes implementam o valor 0 para este campo.
- *VLAN IDentifier (VID)* - este campo de 12 bits é o campo de associação VLAN, conforme a tabela a seguir alguns valores são reservados. Todos os demais valores são utilizáveis e localmente adminstrados.

Formato do Quadro VLAN Tag (802.3 ac)

<i>VID</i>	<i>Significado/Uso</i>
0x0-00	Null VLAN ID. Indica que o <i>tag</i> não contém informação VID, apenas informação de prioridade. Assim, este é conhecido como <i>Priority Tagged Frame</i>. Um ponte <i>VLAN</i> somente enviará este quadro depois de classificar um TCI apropriado na porta de saída ou retirar a <i>VLAN Tag</i> retransmitindo o quadro sem informação de <i>tag</i>.
0x0-01	Valor padrão de porta <i>VLAN</i>, usado para classificação por uma <i>bridge</i>. O valor por ser trocado por gerenciamento baseado por <i>porta</i>.
0x-F-FF	Reservado

VLAN

O conceito de *VLAN (Virtual LAN)* é uma facilidade de operação numa rede *switched*. Esta facilidade permite que o administrador da rede configure a mesma como sendo uma única entidade interligada. Todavia, é assegurado aos usuários a conectividade e privacidade que é esperada como se houvessem múltiplas redes separadas.

VLANs foram definidas inicialmente na especificação 802.1Q, de uma forma genérica como sendo utilizável para todas as LANs do padrão 802.

O padrão 802.1 é responsável pelos problemas de interconexão e *bridging* entre as LANs.

VLAN

O IEEE 802.1 define as condições necessárias para transporte de informação e o uso da informação VLAN (VLAN Tag) no tamanho de um quadro.

Assim, o pessoal envolvido com do padrão IEEE 802.3 estabeleceu um grupo de trabalho para trabalhar com as *VLANs*, este o IEEE 802.3ac. Em outras palavras, o 802.3ac é uma recomendação do grupo 802.3 muito próxima do 802.1Q, todavia específica para o padrão Ethernet.

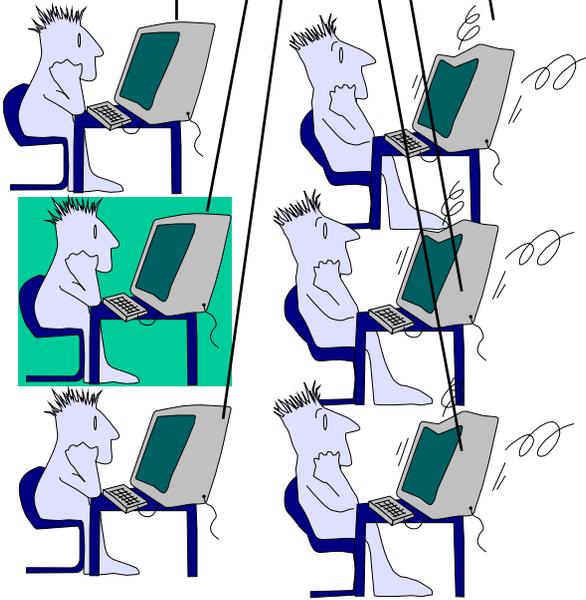
VLAN

o tag é retirado
na entrada



100BASE-TX/FX

switch



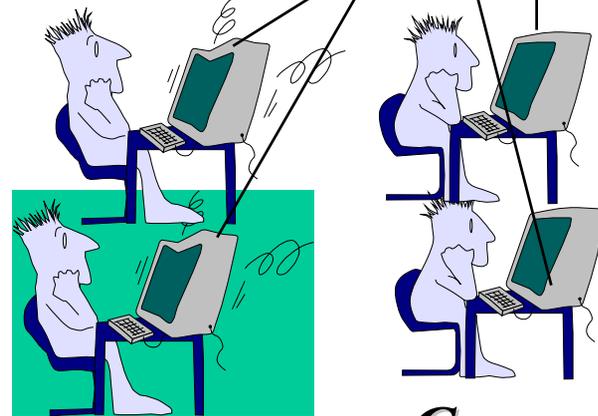
Grupo I

Grupo II

pacote recebe um tag
na saída



switch



Grupo I

Grupo II

VLAN

Na figura anterior, os dois *switches* representam duas redes. Considerando-se um deles, temos dois grupos distintos de pessoas trabalhando juntas de uma forma lógica, ou virtual. Embora todos estejam ligados no mesmo *switch* foram criados dois grupos (Grupo I e II).

Uma definição mais precisa para uma *VLAN* seria um domínio lógico de *broadcast*. Ou seja, temos um domínio onde todos os participantes de um mesmo grupo estão *se vendo*. Os demais, embora ligados no mesmo *switch* não pertencem a *VLAN*.

Administração VLAN

O exemplo apresentado sobre a *VLAN* é uma associação simples de uma *VLAN*. Um *switch* pode aplicar associações alternadas para a *VLAN* baseada na inspeção do quadro Ethernet nos campos de *MAC*, *Subnet* e *Protocolos*. Este tipo de associação é conhecida como *VLAN Binding*.

Embora a *VLAN* baseada em portas pareça consistente para muitos produtos de fabricantes de rede, os produtos *VLAN* baseados em *MAC*, *Subnet* e *Protocolos* vêm ganhando uma grande aceitação (exemplo : o advento de *switches do nível 3*).

V- Gigabit Ethernet

O *Gigabit Ethernet* representa a última versão do Ethernet (Março - 1996) padronizado pelo IEEE. Esta versão da Ethernet é originada do *PAR (Project Authorization Request)*.

O *Gigabit Ethernet* opera a 1 Gbps. O *PAR* resultou numa especificação denominada de *IEEE 802.3z* cobrindo a transmissão em fibra ótica e cabos de cobre para pequenas distâncias (Julho - 1997).

Nesta época um outro Comitê (*802.3ab*) foi formado para gerar a especificação para o *Gigabit Ethernet* para rodar em cabos de pares trançados.

Por que *Gigabit Ethernet* ?

O sucesso da tecnologia 100BASE-T indicaram que um *backbone* com maior largura de banda era necessário para a conexão de dispositivos de 100 Mbps.

Intranets, extranets e ligações convencionais a Internet impulsionaram o desenvolvimento de redes de Gbps.

Backbones até então eram implementados usando as tecnologias de *FDDI* (100 Mbps) e *ATM* (622 Mbps, OC-12, até 2.4 Gbps, OC-48).

A desvantagem dos *backbones FDDI* e *ATM* ficam patentes na necessidade de troca de formato dos quadros.

Por que *Gigabit Ethernet* ?

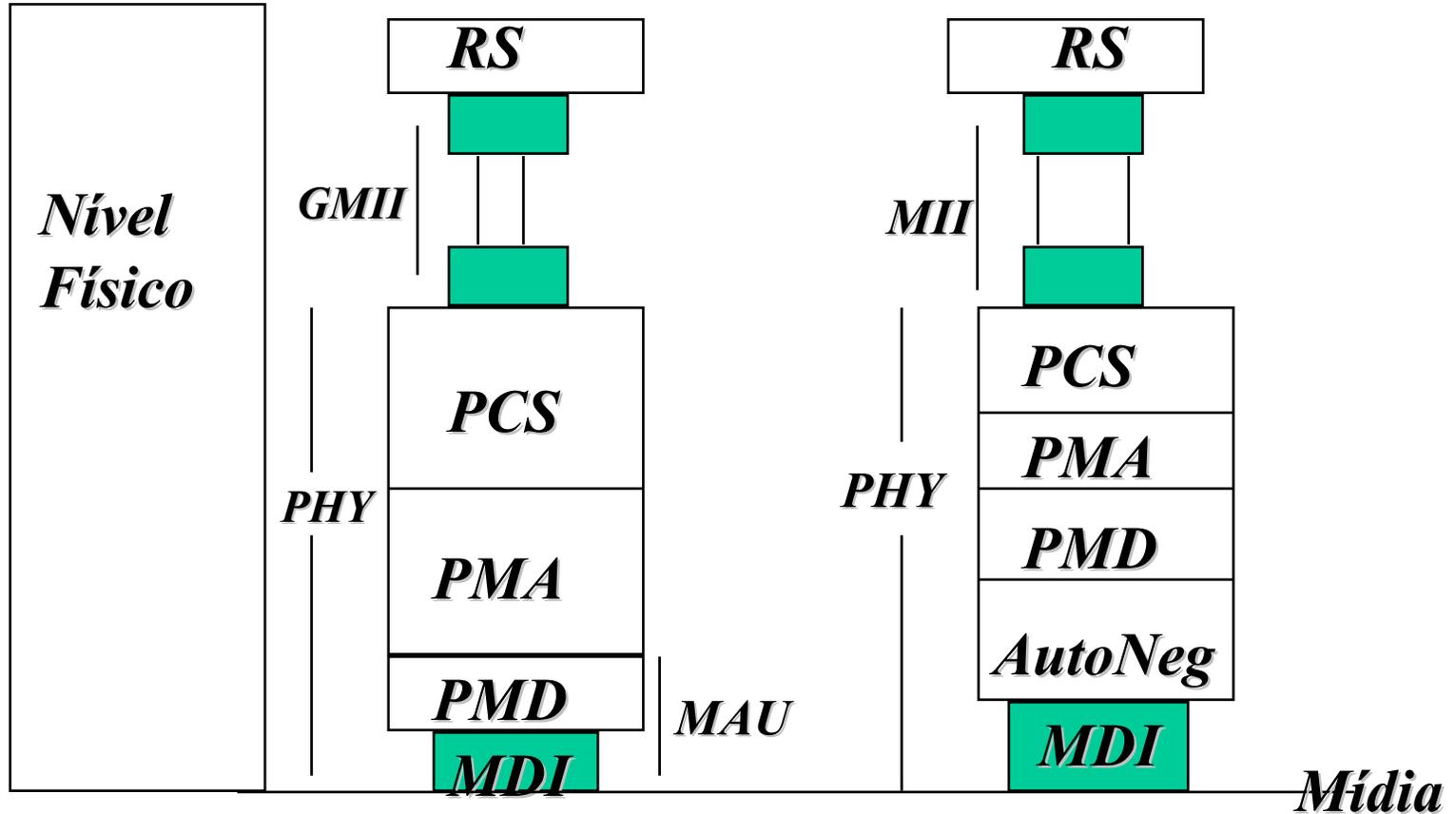
Observação

Em redes onde o *switching* e o *routing* em alta velocidade existem, o preço de segmentação, montagem, encapsulamento/desencapsulamento e conversão do quadro são muito elevados.

Isto significa dizer custos em termos de eficiência de implementação e velocidade de operação para a porção de software, silicon e capacidade dos sistemas para efetuar tais operações na mesma velocidade da linha de transmissão.

1000 Mbps

100 Mbps



Nível Físico 100 Mbps

RS (Reconciliation Sublayer) - mapeia o funcionamento do MAC para sinais elétricos da interface MII;

MII (Medium Independent Interface) - é a interface lógica de sinalização equivalente a 10 Mbps AUI. A MII faz a conexão dos níveis RS e PCS, permitindo que múltiplos tipos de mídias sejam interconectados ao subnível MAC;

PCS (Physical Coding Sublayer) - faz a função de codificação para os dispositivos ligados a uma rede 100Base-T;

Nível Físico 100 Mbps

PMA (Physical Medium Attachment) - é a porção do MAU que contém a circuitaria responsável pela interface dos circuitos do AUI para uma específica mídia;

PMD (Physical Medium Dependent) - é a porção do *PHY*, ou nível físico, responsável por fazer a interface com a mídia física;

AutoNeg - um algoritmo que permite que dispositivos com diferentes tipos de velocidade (10, 100 e 1000 Mbps) possam efetuar seus enlaces através de uma negociação (exemplo : full ou half-duplex).

Diferenças entre *Fast Ethernet* e *Gigabit Ethernet*

- *GMII* e *MII* - Ocorreu uma manutenção quanto ao aspecto de sinalização, todavia o tamanho dos caminhos de dados de transmissão e recepção foram aumentados para 8 bits (no *MII* estes eram de 4 bits).

Como aumento do tamanho de caminhos foi possível uma elevação razoável da frequência dos clocks e caminhos de transmissão. Apesar desta alterações a frequência foi aumentada para 125 MHz.

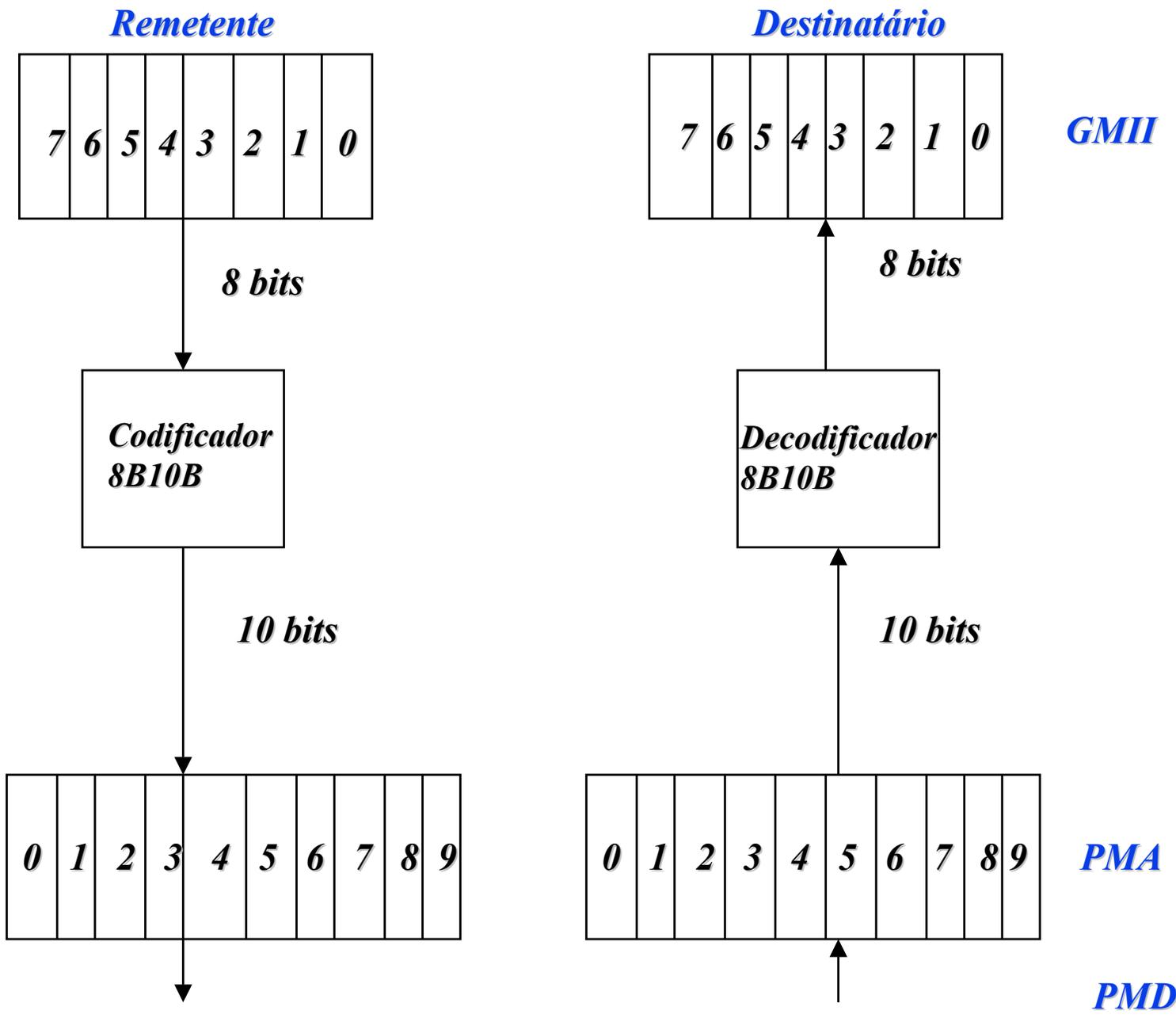
Diferenças entre *Fast Ethernet* e *Gigabit Ethernet*

- *Auto-Negotiation* - na especificação Gbps a função de auto negociação é definida como uma função na camada *PCS*. O esquema de operação é semelhante ao 100Base-T, ou seja o *nó* estabelece a capacidade do link remoto e determina um modo ótimo de operação compartilhado pelos dois dispositivos.

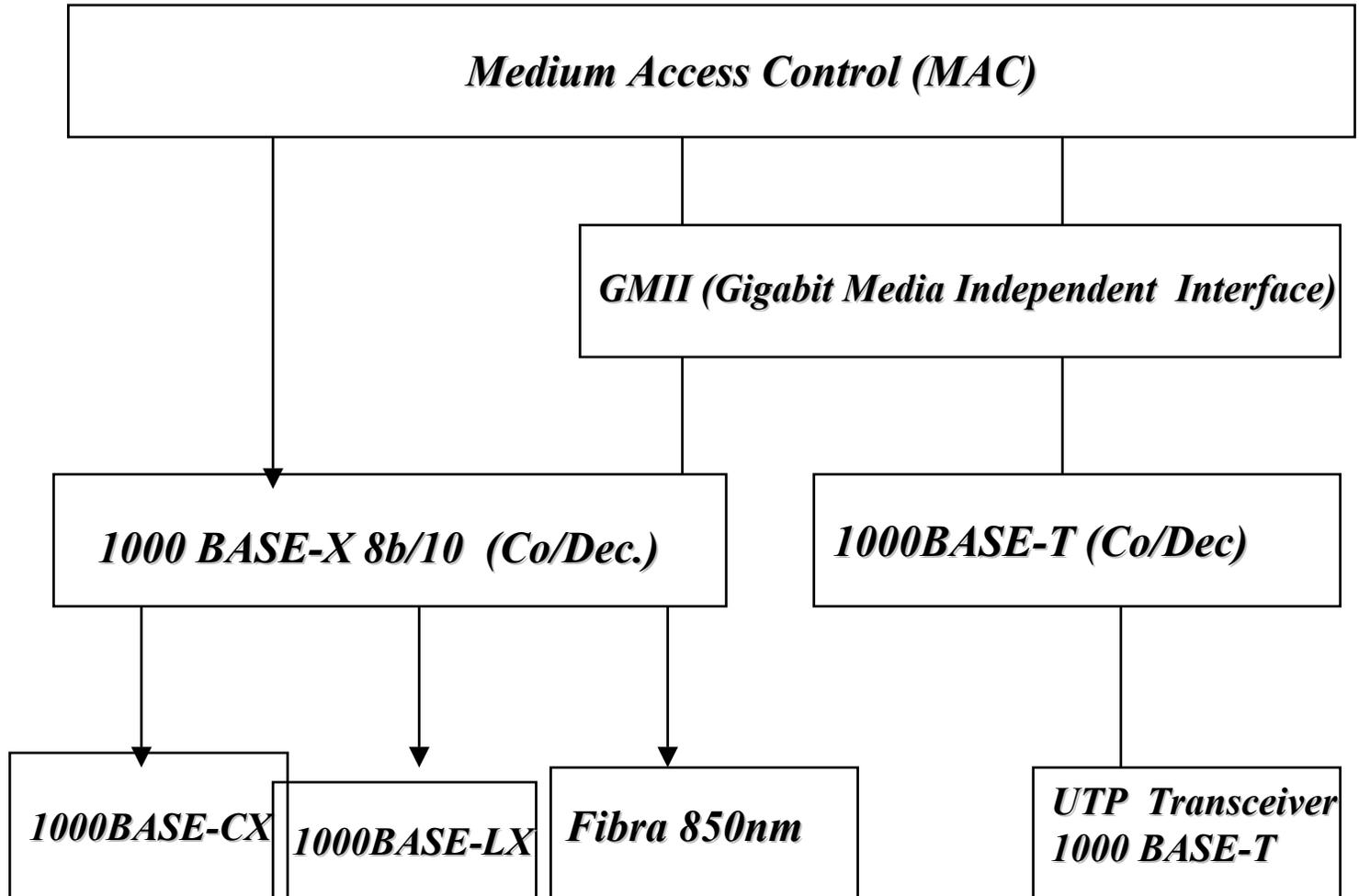
Diferenças entre *Fast Ethernet* e *Gigabit Ethernet*

- *Adoção da Codificação do Fiber Channel* - Visando a adoção de um padrão de sinalização de Gbps reconhecida-mente eficiente, o comite do *Gigabit Ethernet* resolveu adotar o sistema utilizado pelo padrão ANSI X3, *Fiber Channel*.

A sinalização usada pelo *Fiber Channel* é a de *8B10B*, a qual codifica a cada oito bits de dados em 10 bits de código. Ainda são incorporados bits adicionais para conferência de erro.



PMD - Gigabit Ethernet



Diferenças entre *Fast Ethernet* e *Gigabit Ethernet*

Fiber Channel - é uma arquitetura de transferência de dados desenvolvida por um Consórcio de fabricantes de computadores e de dispositivos de armazenamento de massa que foi padronizado pela ANSI.

Este padrão foi projetado para dispositivos de armazenagem de massa que necessitam de uma largura grande de banda. O padrão suporta velocidade de transferência em full-duplex a 100 Mbps.

Diferenças entre *Fast Ethernet* e *Gigabit Ethernet*

- *Modificação de Operação do CSMA/CD* - o retardo de transferência de um quadro (*round-trip-delay*) afeta de maneira direta o tamanho da rede. Este fato pode ser explicado pelo fato que o *MAC* precisa estar pronto para detectar uma colisão durante um certo período de tempo (*slot time*).

Para os padrões 10 e 100 Mbps o *slot time* era de 512 *bit times*. Caso este *slot time* fosse mantido para a rede Gbps, a topologia de rede em termos de tamanho seria reduzida de uma maneira não razoável para uma rede local.

Diferenças entre *Fast Ethernet* e *Gigabit Ethernet*

A modificação de operação do CSMA/CD foi efetuada alterando-se o *slot time* para 512 bytes. Num modo de operação de *full-duplex*, desde que nenhum conceito de colisão está presente a operação do protocolo MAC fica inalterado. Exceto pelo aumento de velocidade.

Diferenças entre *Fast Ethernet* e *Gigabit Ethernet*

- *Prioridade da Fibra sobre outros tipos de mídias* - diferente do *Fast Ethernet* que visa a interconexão de dispositivos no já existente cabeamento de UTP, o comite compreendeu que a tecnologia *Gigabit Ethernet* deveria ser focada como uma solução *backbone*, ou seja utilizando a fibra ótica como o meio de transmissão adequado. Assim, a prioridade da especificação foi orientada para a tecnologia de fibra ótica

Diferenças entre *Fast Ethernet* e *Gigabit Ethernet*

- *Utilização de Repeater Único* - a especificação de *Gigabit Ethernet* considerou que era aceitável o uso de um único tipo de repetidor. Mesmo considerando-se as modificações efetuadas no MAC para a extensão dos limites da rede e sua operação em *Full-Duplex*. O comitê não achou razoável o uso de diferentes repetidores.

Diferenças entre *Fast Ethernet* e *Gigabit Ethernet*

- *Topologia* - um aumento na velocidade do protocolo *CSMA/CD* leva a uma redução no tamanho da rede, desde que nenhum parâmetro do MAC seja re-escalado.

No aumento de 10 para 100 Mbps, o tamanho da rede foi reduzido de 2 km para 200 m. Desta forma, surgiu a necessidade de alteração no MAC para que tivéssemos a rede de Gbps numa abrangência superior a 20 m. Com a alteração do MAC a rede Gbps foi mantida com uma distância de até 200 m.

Switch de Nível 3

Concorrentemente com o desenvolvimento do padrão *Gigabit Ethernet*, os fabricantes de rede começam a disponibilizar os dispositivos que aplicavam a nível de hardware o esquema de *switching a nível de rede*.

Gigabit Ethernet

Meios Físicos

O *Gigabit Ethernet* suporta a transmissão sobre os seguintes meios :

- três tipos de cabos de fibras óticas - 9, 50 e 62.5 micron;
- cabos coaxiais duplos trançados de curta distância de cobre;
- cabos UTP das categorias 4 e 5.

A transmissão do *Gigabit Ethernet* sobre cada um dos meios físicos mencionados é normalizado pela especificação 1000BASE-X

Gigabit Ethernet

Meios Físicos

<i>Padrão 1000BASE-X</i>	<i>Suporte de Meio Físico</i>
<i>1000BASE-SX</i>	850 nm transmissão de laser em fibra multimodo
<i>1000BASE-LX</i>	1300 nm transmissão de laser em fibra multimodo, ou single mode
<i>1000BASE-CX</i>	Cabo trançado com par de cobre duplo com proteção
<i>1000BASE-T</i>	Cabos de cobre trançados UTP das categorias 4 e 5.

Gigabit Ethernet

Meios Físicos

<i>Meio Físico</i>	<i>Distância (m)</i>
Fibra simples de 9 micron, com laser de 1300 nm (LX)	3.000
Fibra multimodo de 62.5 micron, com laser de 850 nm (SX)	300
Fibra multimodo de 62.5 micron, com laser de 1300 nm (LX)	550

Gigabit Ethernet

Meios Físicos

<i>Meio Físico</i>	<i>Distância (m)</i>
Fibra multimodo de 50 micron, com laser de 850 nm (SX)	550
Fibra multimodo de 50 micron, com laser de 1300 nm (LX)	550
Cabo de cobre STP (CX)	25
Categoria 5 UTP (T)	100

Gigabit Ethernet

MAC

O protocolo de acesso ao meio (*MAC*) usado pela Ethernet convencional é o CSMA/CD. Este protocolo estabelece que todos os quadros, independentes do seu tamanho, devem obedecer a uma *percepção* de propagação *round-trip time*.

O tamanho da rede máxima no padrão Ethernet é de 2.5 km. Assim, para manter a scalabilidade o *FAST ETHERNET* reduziu o tamanho máximo dos cabos entre *nós* para até 250 metros e o tamanho máximo entre um *hub* e uma *workstation* para 100 metros.

Gigabit Ethernet

MAC

No padrão *Gigabit Ethernet* decidiu-se alterar o tamanho do quadro. Caso o tamanho do quadro não fosse alterado, o tamanho máximo de transmissão seria de aproximadamente 25 metros entre dois *nós* via uma mídia de cobre.

É evidente que a distância de 25 metros não é um comprimento desejável, ou flexível, para que uma LAN possa ser utilizada.

Gigabit Ethernet

MAC

No *Gigabit Ethernet* foi estendido o tamanho de todos os quadros menores que 512 bytes.

A técnica utilizada foi o *empacotamento* de uma extensão no quadro com símbolos especiais que não ocorrem dentro do quadro.

A técnica de estender o quadro é conhecida com *carrier extension*. Por outro lado, um método denominado de *packet bursting* auxilia na compensação do efeito do *carrier extension* não permitindo que ocorra uma degradação na performance da rede.

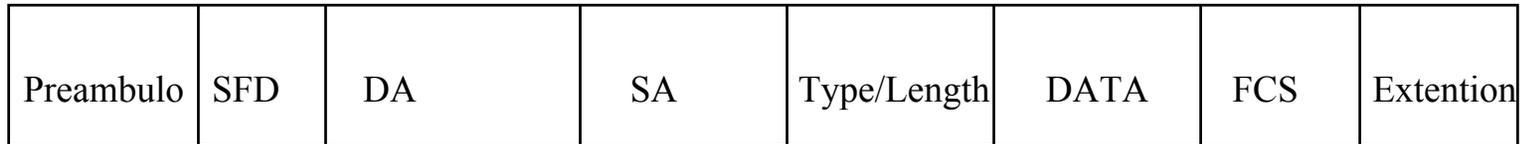
Gigabit Ethernet

Carrier Extension

Os quadros *Gigabit Ethernet* que não excedem 64 bytes em tamanho, 72 bytes quando consideramos os campos *preambulo e start of frame delimitate (sfd)*, são estendidos para 512 bytes com a adição de símbolos especiais.

Gigabit Ethernet

Carrier Extension



— *64 bytes de tamanho mínimo* —

— *512 bytes de tamanho mínimo* —

— *Cobertura do FCS* —

— *Duração do Evento de Transmissão* —

Gigabit Ethernet

Carrier Extension

Importante observar que :

- a extensão de símbolos *non-data* estendem o quadro para fins de detecção de colisão ;
- como a extensão é efetuada após o campo de FCS, apenas o quadro original sem a extensão será computado;
- como a extensão é removida pelo destinatário, os protocolos de mais alto nível na pilha são inócuos para a extensão.

Gigabit Ethernet

Carrier Extension

Exemplo - Imagine que você está em frente a um terminal e que você recebe a seguinte mensagem de uma aplicação :

- *Entre 1 para Continuar, S para Sair.*

Sua resposta com *um caractere* irá acarretar na necessidade de 45 caracteres adicionados ao campo de Dados no quadro Ethernet.

Assumindo que a transmissão é numa LAN *Gigabit Ethernet*, 448 *carrier extension bytes* serão adicionados para formar os 512 bytes necessários para o quadro.

Gigabit Ethernet *Carrier Extension*

Logo, um dado de um byte resulta em 511 bytes de overhead. Este efeito não é desejado uma vez que não é eficiente e que atinge um nível de performance somente um pouco superior ao de uma rede *Fast Ethernet*.

Do problema causado pelo *carrier extension*, a tecnologia *Gigabit Ethernet* emprega um método denominado de *packet bursting*.

Gigabit Ethernet

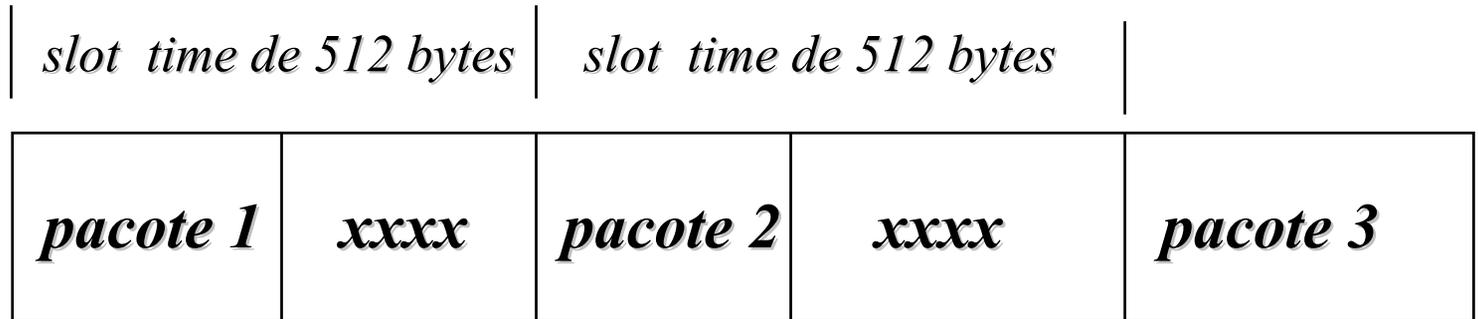
Packet Bursting

Com o método de *packet bursting*, o *nó* que possui dois ou mais pacotes a serem transmitidos, enviam o primeiro pacote usando a técnica *carrier extension* se este é menor que 512 bytes em tamanho.

No caso da transmissão ser efetuada com sucesso, ou seja sem que haja uma colisão, todos os demais pacotes são enviados subsequentemente até que expire um *burst time*, cuja duração é de 1500 bytes. Neste momento, qualquer pacote sendo transmitido é transmitido até completar.

Gigabit Ethernet

Packet Bursting



xxxx - carrier extension

Gigabit Ethernet

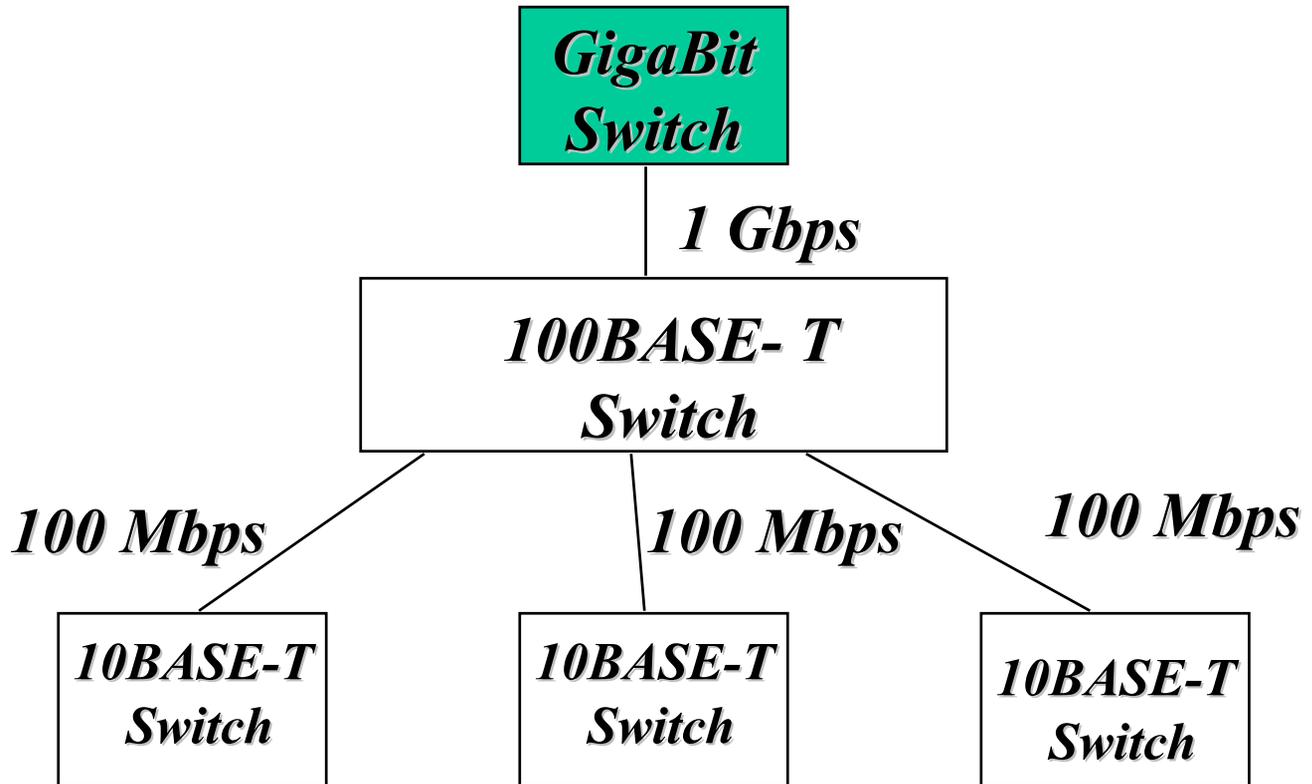
Utilização

A grande largura de banda que o *Gigabit Ethernet* prove faz com que esta tecnologia de LAN seja aproveitada como o uso de *backbone* para a interconexão de LANs Ethernet convencionais e *Fast Ethernets*.

Nesta tendência natural para uso como *backbone*, fabricantes já dispõem de *switches* com várias portas 1 Gbps e *switches* com 100/1000 bps. Estes últimos *switches* representam dispositivos com uma porta, ou mais, de 1 Gbits e as demais de 100 Mbps.

Gigabit Ethernet

Utilização



Gigabit Ethernet

Utilização

Muitas *NICs* de *Fast Ethernet* pode ser auto-sensíveis para operações de 10 e 100 Mbps é possui contruir LANs inter-estruturadas permitindo-se que o uso de 10, 100 e 1000 Mbps.

Trabalhando com Gigabit Ethernet

Nossos próximos passos serão em direção ao efetivo uso da tecnologia de rede de *Gigabit Ethernet* na prática. Assim, vamos abordar aspectos tais como : atender ao desafio de largura de banda, migração para a nova técnica, gerência, upgrades de *switches*, compartilhamento com os ambientes de *FDDI*, upgrade do desktop, qualidade de serviço, RSVP (*Reservation Protocol*), nível 3 *switching*, IP e Tag switching.

Desafio de atender a largura de banda

A maior tendência de evolução das redes está diretamente relacionada ao uso da *Internet*. Desta forma, as tecnologias de redes, semelhante a *Internet*, devem ser capazes de atender de uma *aceitável* solicitações de aplicações tão distintas como *e-mail*, *e-business*, *on-line shopping*, *aplicações multimídia e outras*.

Muito importante de se frisar que o uso de diferentes aplicações faz com que as redes tenham que ser capazes de suportar o crescimento geométrico no tráfego e os diferentes tipos de requerimentos de largura de banda.

Desafio de atender a largura de banda

Outro ponto interessante sobre a necessidade da largura de banda é a obsolescência da *Regra 80/20*. Esta estabelecia empiricamente que 80 % de todo o tráfego de um rede era local. Os restantes 20 % eram de acesso remoto.

Assim numa rede corporativa, qualquer rede local deve estar projetada para acesso muitas vezes superiores ao do acesso local de rede. Um exemplo são as *extranets*.

Topologia de Gigabit Ethernet

<i>Topologia</i>	<i>Objetivo</i>	<i>Modos</i>	<i>Mídia</i>	<i>Aplicação</i>
<i>Switched</i>	<i>Alto throughput Longas distâncias</i>	<i>Full Duplex Half Duplex</i>	<i>Fibra : Multi e Simples, Cobre</i>	<i>Campus e Prédios Backbones, Gabinetes de Cabos</i>
<i>Shared</i>	<i>Custos reduzidos Pequenas distâncias</i>	<i>Half Duplex</i>	<i>Fibra Multi e Cobre</i>	<i>Servers farms Desktops</i>

Comparação de Gigabit, 100Base-T e 10Base-T

<i>Facilidade</i>	<i>10Base-T</i>	<i>100Base-T</i>	<i>1000Base-T</i>
<i>Velocidade</i>	<i>10 Mbps</i>	<i>100 Mbps</i>	<i>1000 Mbps</i>
<i>Cat. 5 UTP</i>	<i>100 m</i>	<i>100 m</i>	<i>100 m</i>
<i>STP</i>	<i>500 m</i>	<i>100 m</i>	<i>25 m</i>
<i>Fibra Multimodo</i>	<i>2 km</i>	<i>412 m (hd) 2 km (fd)</i>	<i>220 m (hd)</i>
<i>Fibra Monomodo</i>	<i>25 km</i>	<i>20 km</i>	<i>5 km</i>

Migração para a Tecnologia Gigabit Ethernet

A tecnologia *Gigabit Ethernet* funciona com o mesmo formato de quadro do padrão IEEE 802.3, assim como funções de gerência. Em adição, já vimos que o *Gigabit* pode operar sobre a infraestrutura de cabeamento existente para 10 e 100 Mbps. O cabeamento suportado pelo *Gigabit* também é aquele empregado em redes *FDDI e ATM*.

Na migração para o *Gigabit* existe uma facilidade da organização migrar preservando as aplicações de software existentes, sistemas operacionais, aplicações de gerência de rede e protocolos de rede (exemplo : TCP/IP).

Gerência em Gigabit Ethernet

Os elementos gerenciados, tais como *objetos, atributos e ações* foram especificados no padrão 1000 Mbps de maneira idêntica a das especificações 10 e 100 Mbps.

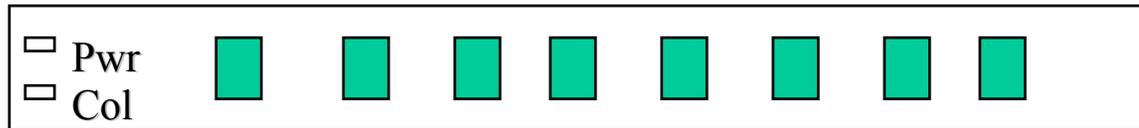
A gerência da rede pode ser efetuada da mesma forma que anteriormente efetuada, todavia os usuários terão uma maior largura de banda.

O custo de gerenciamento é muito menor num ambiente *Gigabit Ethernet*, quando comparado com outras redes como por exemplo ATM. Num ambiente não Ethernet diferentes especificações são utilizadas.

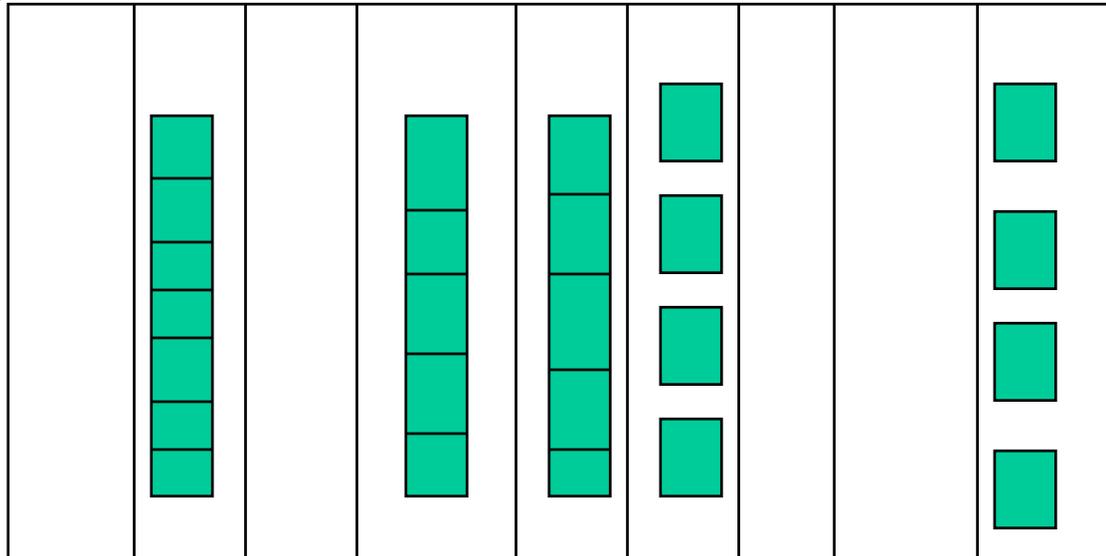
Upgrade de Switches

Os repetidores podem ser classificados em três categorias :

(a) Não-Modular

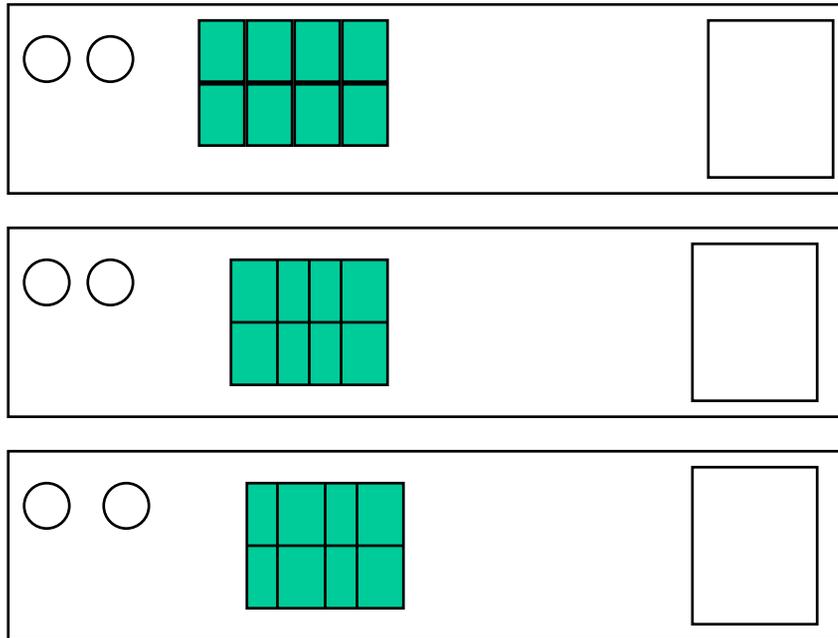


(b) Modular



Upgrade de Switches

(c) Stackable Repeater



Upgrade de Switches

Uma direção natural de *upgrade* é o uso de um *switch* de *Gigabit* como backbone naqueles ambientes onde *switches* de 100 Mbps eram empregados com links da LAN.

Classe de Serviço (CoS) e Qualidade de Serviço (QoS)

Na terminologia de redes com grande largura de banda, dois conceitos de gerenciamento da largura de banda são geralmente confundidos. Estes :



Class of Service (CoS) ?



Quality of Service ?

Classe de Serviço (CoS) e Qualidade de Serviço (QoS)



Class of Service (CoS) ?



- *Class of Service (CoS) - Classe de Serviço* determina os limites de serviços, de uma forma discreta, que uma determinada rede deve oferecer aos pacotes através da classificação do tráfego.

Classe de Serviço (CoS) e Qualidade de Serviço (QoS)



Quality of Service ?



- *Quality of Service (QoS) - Qualidade de Serviço* permite a negociação de um determinado serviço, de forma dinâmica, através da reserva de largura de banda.

Classe de Serviço (CoS) e Qualidade de Serviço (QoS)



- *Class of Service (CoS) - Classe de Serviço* determina os limites de serviços, de uma forma discreta, que uma determinada rede deve oferecer aos pacotes através da classificação do tráfego.



- *Quality of Service (QoS) - Qualidade de Serviço* permite a negociação de um determinado serviço, de forma dinâmica, através da reserva de largura de banda.

Classe de Serviço (CoS) e Qualidade de Serviço (QoS)

Várias organizações trabalham os padrões *CoS* e *QoS*.

O modelo *CoS* inclui o *Differentiated Services (DiffServ)* do IETF, as extensões do 802.1D conhecida como 802.1p/Q e o *user-network interface (LUNI 2.0)* do ATM Forum.

Por outro lado, os modelos de *QoS* incluem *Integrated Services (IntServ)* do IETF e ATM Forum's *QoS*.

Classe de Serviço (CoS)

No paradigma de *Classe de Serviço (CoS)* a sinalização reside em cada pacote dos dados. Assim, esta informação diz ao dispositivo que vai tratar o pacote qual classe o pacote pertence.

Num ambiente de *CoS*, o tráfego pode ser classificado como por exemplo *best-effort* ou *multimídia*. Outra possível classificação seria *possível para descarte* ou *alto grau de segurança*.

Qualidade de Serviço (QoS)

Uma prioridade bem definida dos tipos de tráfegos numa rede é um fator importante para aqueles pontos onde ocorrem os congestionamentos. Nestes locais, decisões sobre o retardo de envio, ou descarte de pacotes devem ser priorizados por *switches e routers*.

Exemplos de aplicações que necessitam de uma prioridade diferencial são *o processamento de transações, aplicações de tempo real, video, etc.*

Qualidade de Serviço (QoS)

A *Qualidade de Serviço (QoS)* implica não só na prioridade do tráfego, mas também :

- numa garantia de largura de banda ;
- características de latência e o jitter da rede ;

As LANs já utilizam a prioridade a algum tempo através do parâmetro *Type of Service (ToS)* do IP.

Por outro lado nas WANs, os routers empregam uma política de prioridade na fila de saída para aqueles pacotes que devem seguir em frente.

Qualidade de Serviço (QoS)

A *Qualidade de Serviço (QoS)* nas LANs pode ser implementada através de protocolos como o *ReSerVation Protocol (RSVP)*.

O *RSVP* é um protocolo fim-a-fim que permite que um *nó* requisição uma certa reserva de garantia de largura de banda na rede.

O *RSVP* opera no nível 3 para fluxo de dados baseados em *IP*. O protocolo permite que *switches do nível 3 e routers* mantenham filas com prioridades múltiplas.

Reservation Protocol (RSVP)

O protocolo *RSVP* foi projetado para permitir que numa ligação qualquer, o remetente, o destinatário e os roteadores pudessem se comunicar a fim de estabelecer o estado da rota para suportar serviços que exijam *QoS*.

Um *nó* emprega o protocolo *RSVP* para solicitar um serviço específico de qualidade (*QoS*) à rede segundo uma necessidade de uma dada aplicação. Assim, esta solicitação vai desde o *nó* de origem passando pelos roteadores até chegar ao *nó* destinatário.

Reservation Protocol (RSVP)

Nos roteadores dois mecanismos de controle são utilizados :

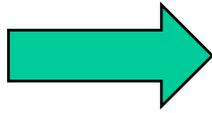


- Admissão



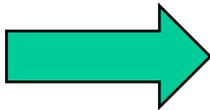
- Policiamento

Reservation Protocol (RSVP)



- Admissão - determina se o roteador possui recursos suficiente para atender a solicitação do serviço *QoS* ;

Reservation Protocol (RSVP)



- Policiamento - determina se o usuário possui permissão administrativa para solicitar o serviço.

Reservation Protocol (RSVP)

No caso positivo das políticas de admissão e policiamento, os parâmetros necessários ao atendimento do *QoS* são configurados no quadro do *RSVP*.

Reservation Protocol (RSVP)

O protocolo *RSVP* identifica uma sessão de comunicação através do endereço do destinatário, tipo de protocolo de transporte e o número da porta do destino.

As operações do *RSVP* somente se aplicam aos pacotes de uma sessão. Outras características do protocolo são :

- permite o uso de multicast ;
- fácil de implementação em *nós, switches e roteadores* ;
- não é um protocolo de roteamento.

Nível 3 de Switching

Nos últimos anos a tecnologia de *switching* tem ajudado a melhorar a performance das LANs através da substituição das LANs com mídias compartilhadas e largura de banda fixas.

Usuário se beneficiam das *LANs Switched* efetuando suas ligações ponto-a-ponto, evitando o compartilhamento das redes a cabo.

Para melhorar a performance das *LANs Switched*, criando ambiente de redes lógicos o nível 3 era uma função que deveria ser implementada nos *switches*, semelhante aquela função dos roteadores.

Nível 3 de Switching

Multilayer switching é uma evolução prática das tecnologias de LAN *switching* e o *routing*. Esta técnica de baixo custo em comparação com o *routing*, remove os problemas de *escalabilidade* e *throughput* que limitam o crescimento de uma LAN.

O *Multilayer switching* permite que tenhamos um LAN, ou um conjunto de LANs, conhecida pelo *Switch*. Desta forma, não somente *segmentos de LANs* podem existir num *switch*, mas *diferentes LANs*

Nível 3 de Switching

Multilayer switching possui inúmeras abordagens para a implementação da solução de *switching*. Estas técnicas diferem umas das outras da forma pela qual a comutação de pacotes será efetuada. Entre as mais conhecidas técnicas de comutação temos :

- *IP Switching* ;
- *Tag Switching* ;
- *ARIS*.

IP Switching

O *IP Switching* foi desenvolvido pela Ipsilon em 1996, permitindo que o reencaminhamento em alta-velocidade de pacotes em redes ATM. A solução *IP Switching* foi rotulada como mais simples e eficaz do que o protocolo *MPOA (MultiProtocol Over ATM)*.

IP Switching

Um *switch IP* mapeia as funções de re-encaminhamento de um roteador na matrix do hardware de um *switch*. A técnica pode ser usada por qualquer aplicação que empregue o *IP*, não sendo restrita a nenhum tipo de protocolo de roteamento em particular.

O conceito de *fluxo* é o utilizado pelo *IP Switching*. Nesta abordagem, o re-encaminhamento é determinado pelos primeiros pacotes no *fluxo*.

IP Switching

Um exemplo da operação do *IP Switching* é o envio de uma seqüência de pacotes de uma determinada porta de origem endereços para uma porta de destino com os mesmos requisitos de *QoS*.

Os primeiros pacotes determinam a classificação do fluxo. Esta classificação é armazenada e utilizada para os próximos pacotes do fluxo. Com esta ação é evitada a consulta a tabela de roteamento.

Tag Switching

O *Tag Switching* foi uma abordagem desenvolvida pela CISCO em Setembro de 1996. Esta técnica recai numa categoria de roteamento conhecida como *label-swapping*.

O conceito de *label-swapping* no qual pacotes Ethernet, ou células ATM, carrega uma etiqueta de tamanho fixo que diz para os *nós switches* como processar a informação.

Aggregate Route-Based IP Switching (ARIS)

Este protocolo em coordenação com outros protocolos da camada de rede (exemplo OSPF), estabelece enlaces comutados numa rede de Roteadores Comutados Integrados (*Integrated Switch Routers - ISR*) .

O protocolo ARIS propõe uma pequena modificação na abordagem de comutação de *labels*. O diferencial da proposta é que o *label* usado para rotear, ou comutar, pacotes entre nós é carregado na porção de endereço do destinatário. Para *unicast*, o endereço MAC do ponto egresso da rede é identificado pelos ARIS.

Aggregate Route-Based IP Switching (ARIS)

O protocolo ARIS difere do *Tag Switching* no uso do algoritmo baseado em rotas, ao contrário do algoritmo comutado por fluxo empregado no *Tag Switching*.

VI- Redes Token-Passing

Devido a contenção existente nas redes CSMA, o que pode algumas vezes gerar situações indesejáveis, redes *Token-Passing* foram idealizadas para prover aos *nós* um acesso determinístico.



Mas como é efetuado esse acesso ordenado ?

A maneira de acessar a rede de forma ordenada é caracterizada pelo uso de um *token* (uma permissão).

Em outras palavras aquele *nó* que dispõe da permissão pode fazer sua transmissão. O *token* é passado de *nó a nó* até que o *nó* que está pendente da mensagem receba o pacote.



Qual a próxima estação a ter acesso ao token ?

A maneira de acessar a rede de forma ordenada é caracterizada pelo uso de um *token* (uma permissão).

Em outras palavras aquele *nó* que dispõe da permissão pode fazer sua transmissão. O *token* é passado de *nó a nó* até que o *nó* que está pendente da mensagem receba o pacote.



Qual a próxima estação a ter acesso ao token ?

Depois da mensagem ter sido transmitida, o *token* é passado para a próxima estação. A abordagem das redes *Token-Passing* baseiam-se no *polling* distribuído.



O que significa o distributed polling ?

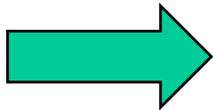
Duas topologias existem nas redes *token-passing*, estas a *token-ring* e *token-bus*.



Quais as diferenças que você imagina existir entre uma abordagem token-ring e outra token-bus ?



• *Uma rede em anel (**token-ring**) apresenta a necessidade de um módulo ativo em série no enlace de transmissão.*



• *Na configuração em anel, diferente da barra, a distorção do sinal é menor.*



Por que ?



Por que ?

Uma rede **token-ring** é implementada ponto-a-ponto. Por outro lado, na configuração de barra, *múltiplas conexões (transceivers)* implicam na distorção da qualidade de sinal e controle do mesmo.



• No anel não existe limitação inerente de distância, porque cada ponto de acesso das estações representam um elemento regenerador do sinal digital.



• Numa configuração em barra, existe a alocação do canal inteiro para um elemento ativo.



*Por que o uso inteiro da largura de banda ?
Como é efetuada a alocação no anel ?*



*Por que o uso inteiro da largura de banda?
Como é efetuada a alocação no anel ?*

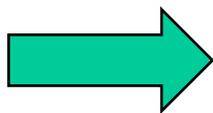


Uma configuração com topologia em barra deve estar naturalmente empregando uma mídia de acesso multiponto de banda base.



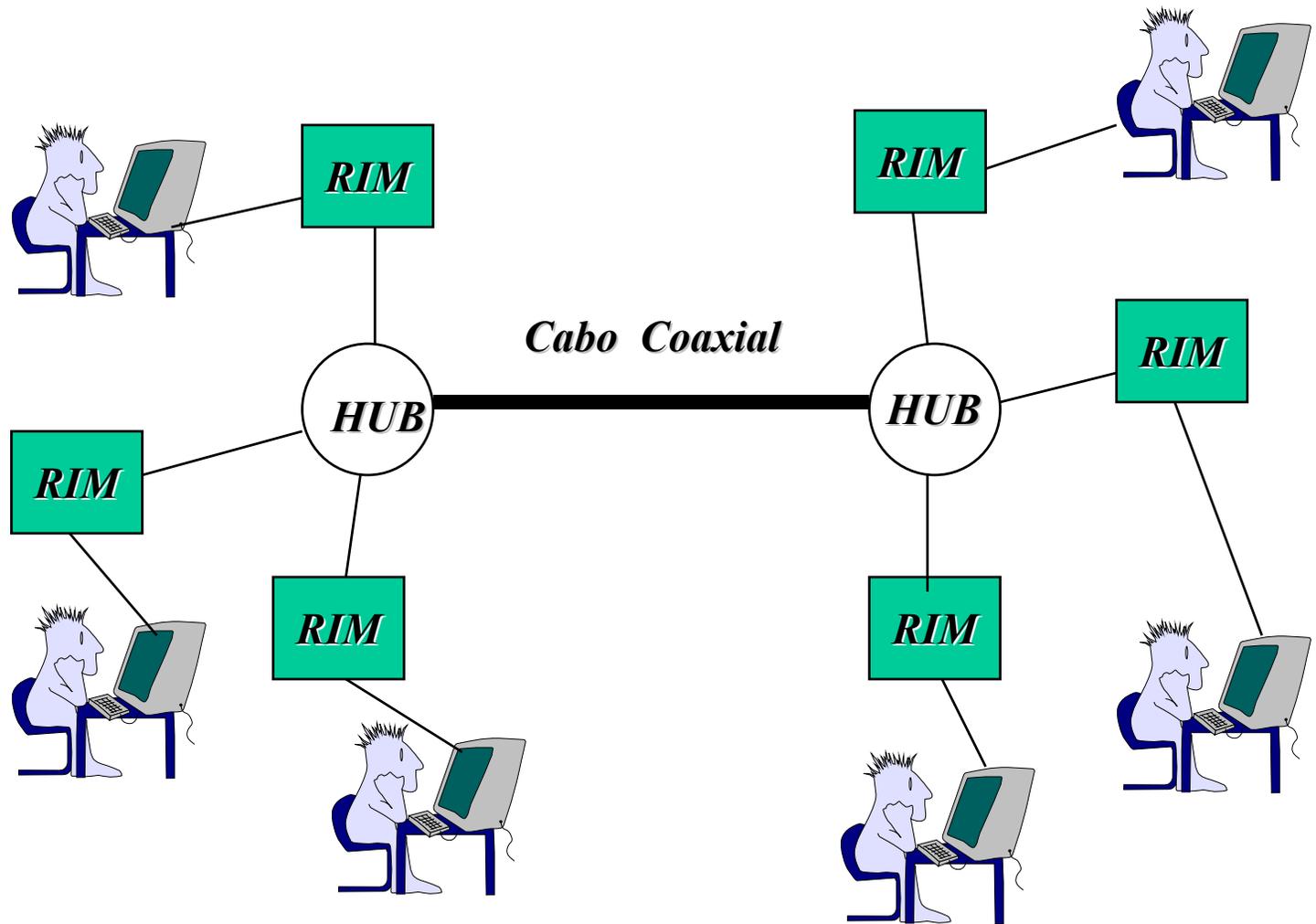
Uma rede **token-ring** é possível criarmos subcanais empregando a técnica de multiplexação por divisão tempo.

Duas implementações de *Token* são *bastantes conhecidas* :

 *ARCnet (Attached Resource Computer network)* : primeira rede americana implementada na filosofia token-passing, desenvolvida pela Datapoint Corp. .

Os protocolos e a rede eram a princípio proprietários, tornando aberto em 1982. Uma configuração *ARCnet* é funcionalmente uma *token-passing bus*, embora sua topologia seja híbrida *barra/estrela*..

Topologia Física - Rede ARCnet



RIM - Resource Interface Module

As características gerais de uma rede *ARCnet* são :

- Transmissão em Baseband 2.5 Mbps;
- Estações podem estar distantes até quase 8 km;
- Hub podem ter distâncias entre si de até 2 000 pés;
- Numa configuração *máxima* nós temos até 10 *hubs*;
- Existência de 5 formatos básicos de pacotes de mensagem:

As quatro primeiras mensagens são utilizadas para informação de controle e a quinta é responsável por carregar informação entre nós.

Tipo de Mensagem

<i>1</i>	<i>Alert</i>	<i>EOT</i>	<i>DID</i>	<i>DID</i>					<i>Token</i>
<i>2</i>	<i>Alert</i>	<i>ENQ</i>	<i>DID</i>	<i>DID</i>					<i>Free-buffer enquiry</i>
<i>3</i>	<i>Alert</i>	<i>ACK</i>	<i>ACK - Buffer Disponível</i>						
<i>4</i>	<i>Alert</i>	<i>NACK</i>							
<i>5</i>	<i>Alert</i>	<i>SOH</i>	<i>SID</i>	<i>DID</i>	<i>DID</i>	<i>COUNT</i>	<i>DATA</i>	<i>CRC</i>	<i>CRC</i>

Dados



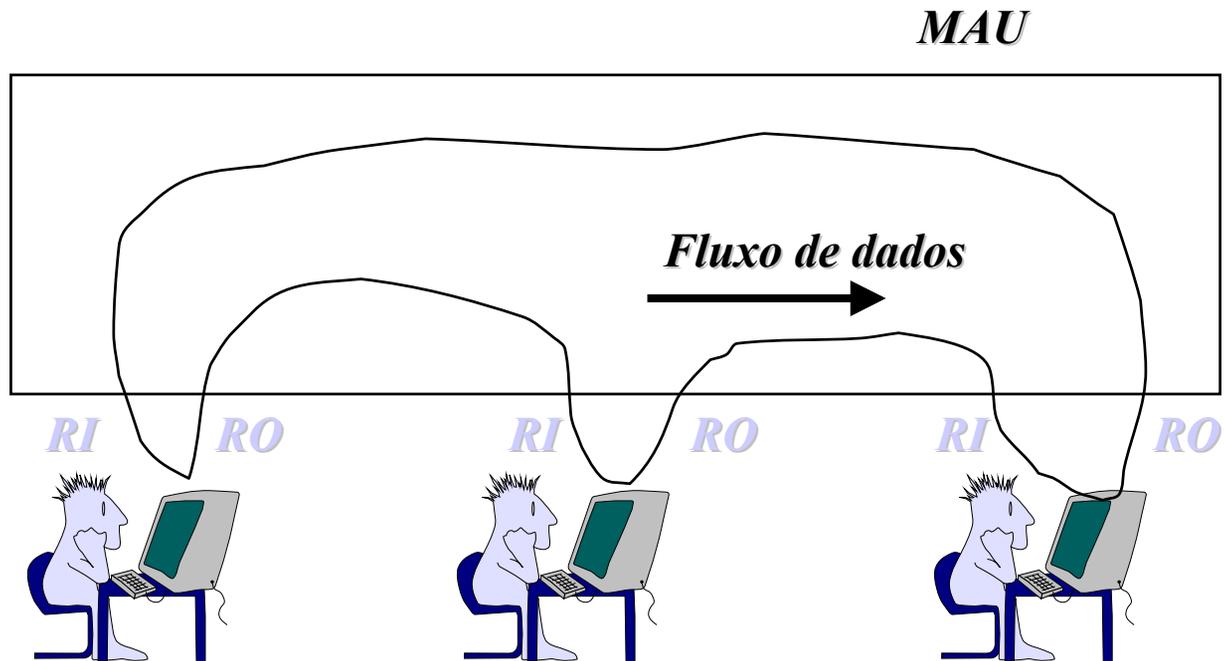
Token-Ring - nos meados dos anos 80 a IBM lançou sua *token-passing* que possui uma característica híbrida entre um abordagem física em estrela e funcionamento em forma de anel. Esta rede foi batizada de *Token-Ring*.

A rede *Token-Ring*, semelhante ao caso da *Ethernet*, foi padronizada pelo IEEE como o padrão 802.5. Em comparação com o padrão 802.3, os dispositivos do 802.5 são mais caros devido ao maior grau de sofisticação de controle da rede.

As características gerais de uma rede *Token-Ring* são :

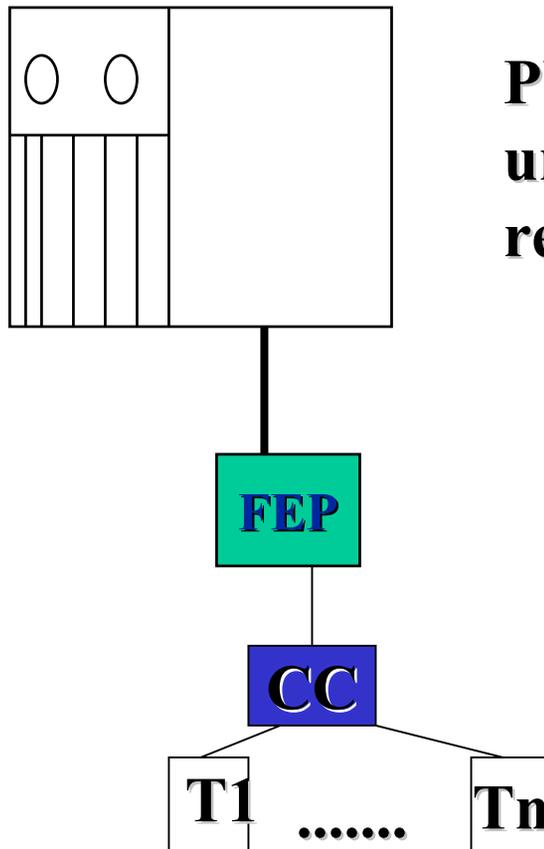
- Transmissão em 4 e 16 Mbps;
- A rede de 4 Mbps pode suportar 72 dispositivos (9 MAUs com 8 portas) e os cabos podem ser UTP e STP;
- A rede de 16 Mbps pode suportar 250 dispositivos e somente cabos STP podem ser usados;
- O monitor ativo da rede é aquele que possui o maior endereço de rede;

Topologia Física - Rede Token-Ring



Topologia Física - Rede SNA

Exemplo - SNA/IBM



PU (Physical Unit) : Componente de uma rede SNA que gerencia os recursos de um nó, só existe um por nó.

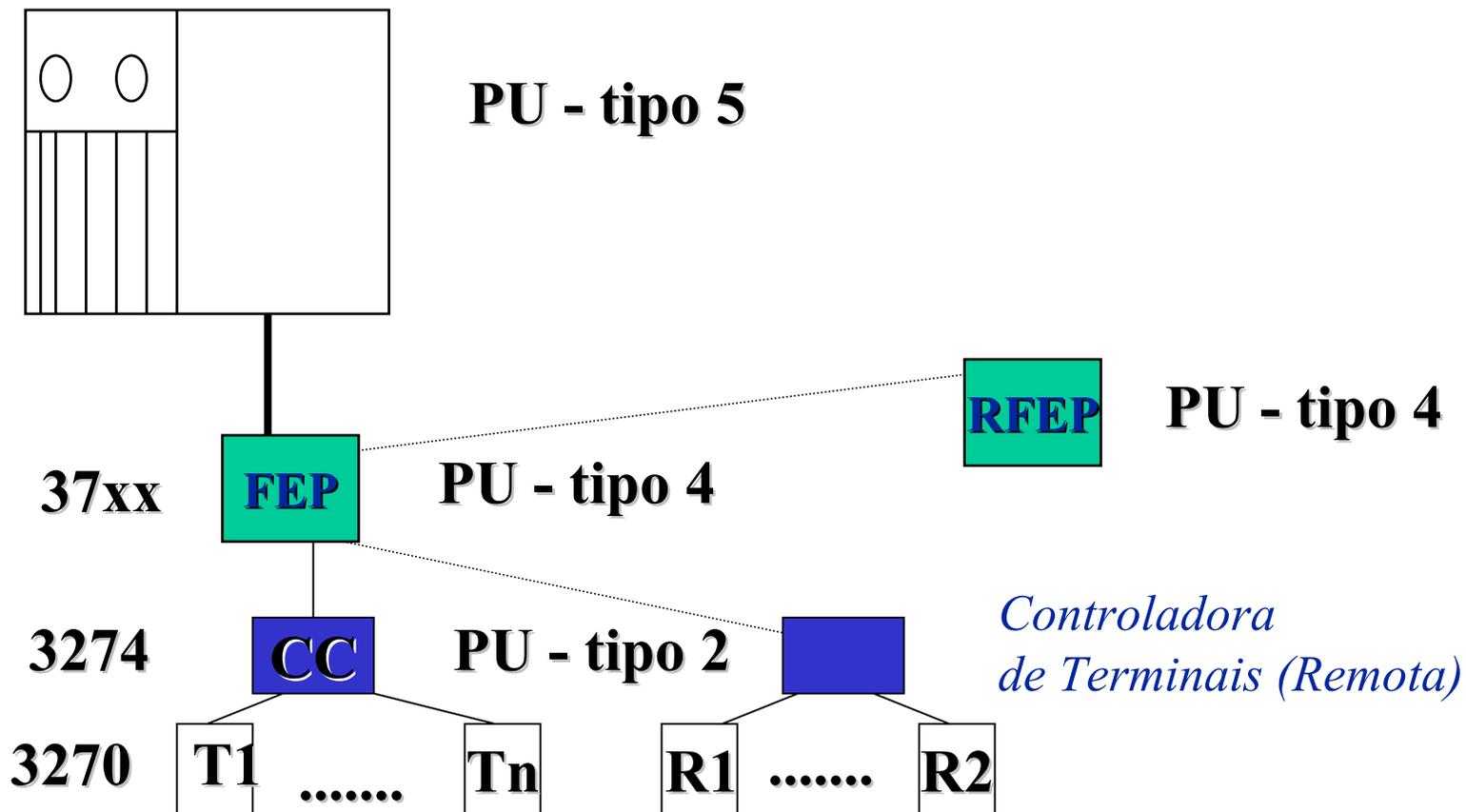
Controladora de Comunicação

Controladora de Terminais

Terminais

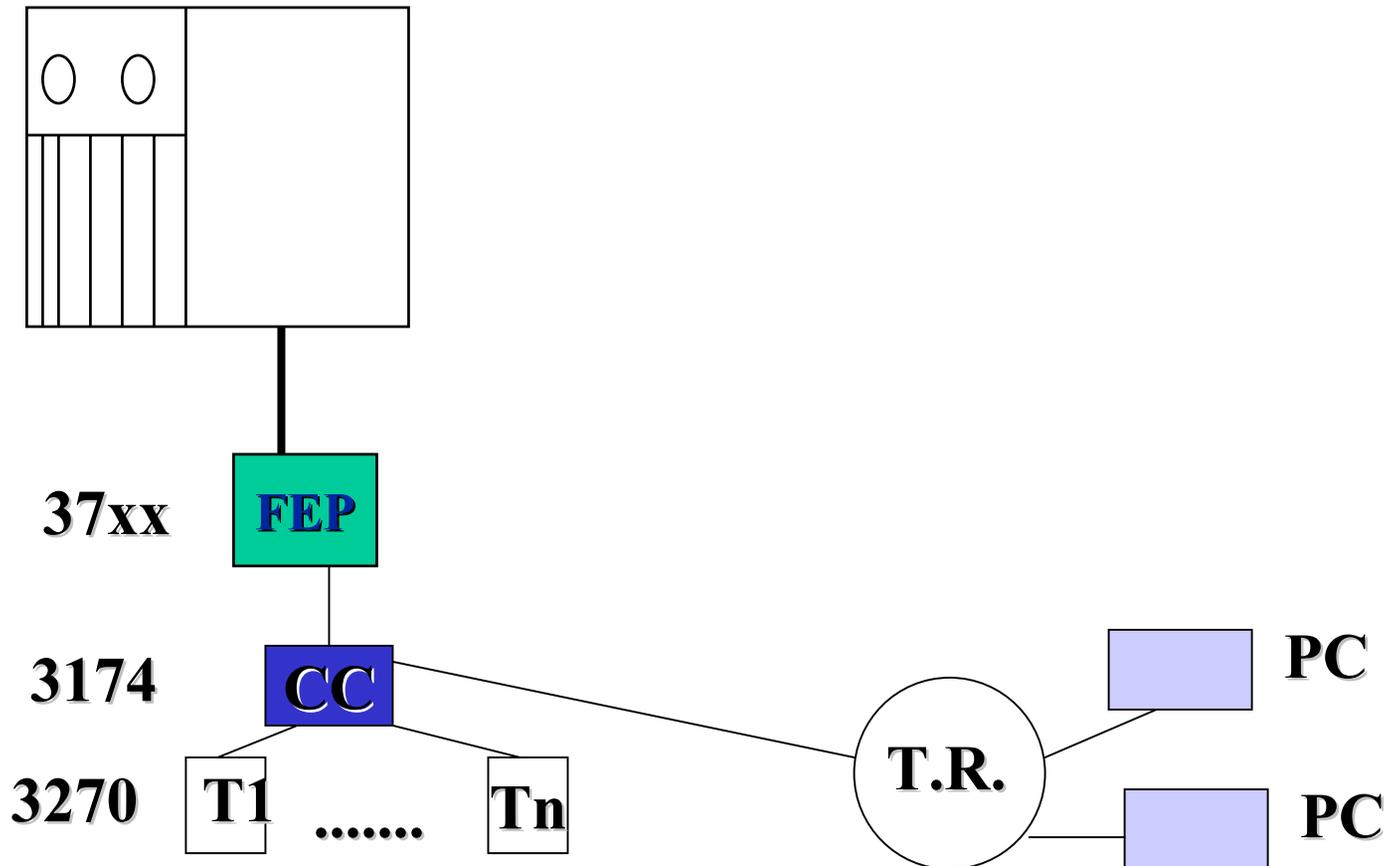
Topologia Física - Rede SNA

Exemplo - SNA/IBM



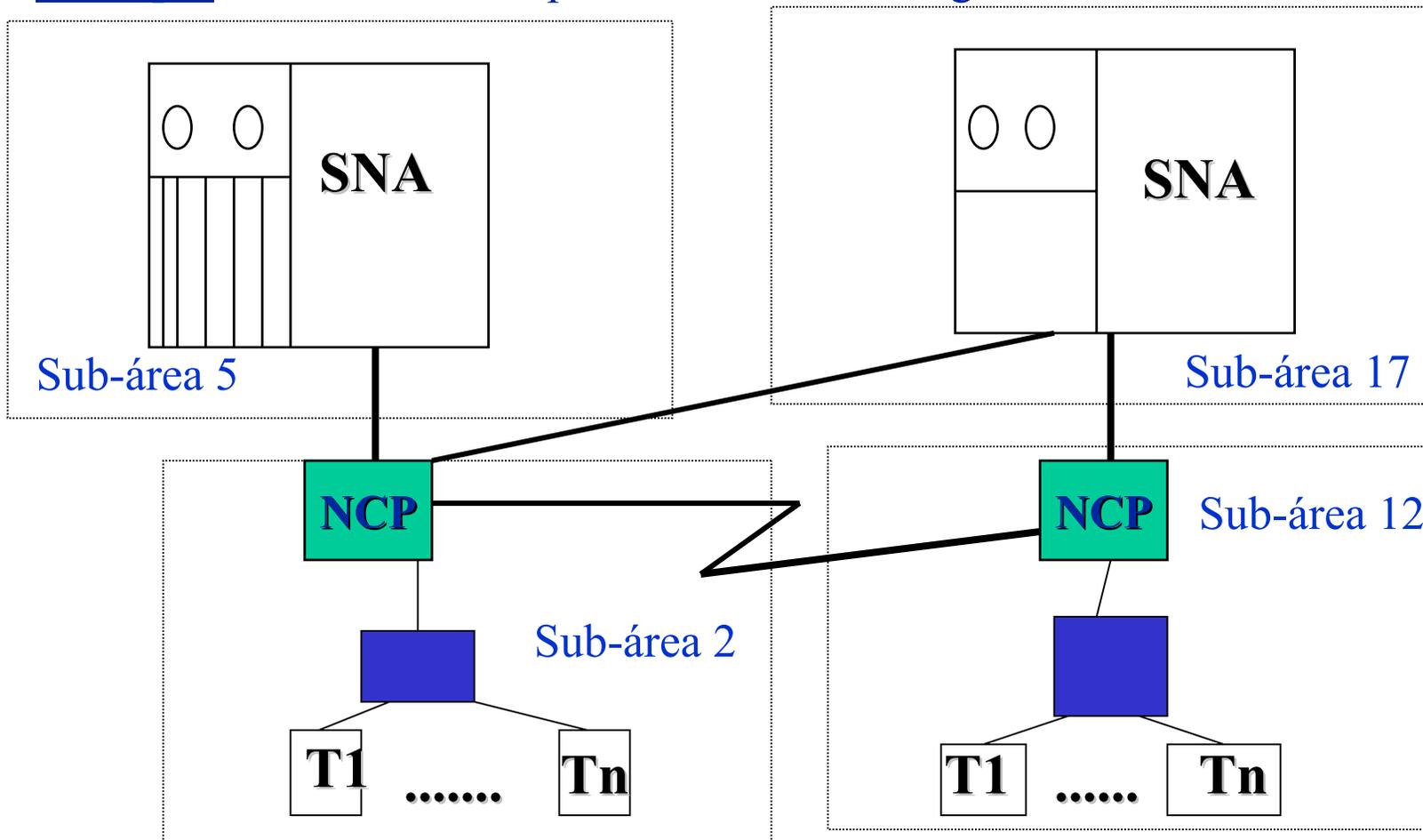
Topologia Física - Rede SNA

Exemplo - SNA/IBM



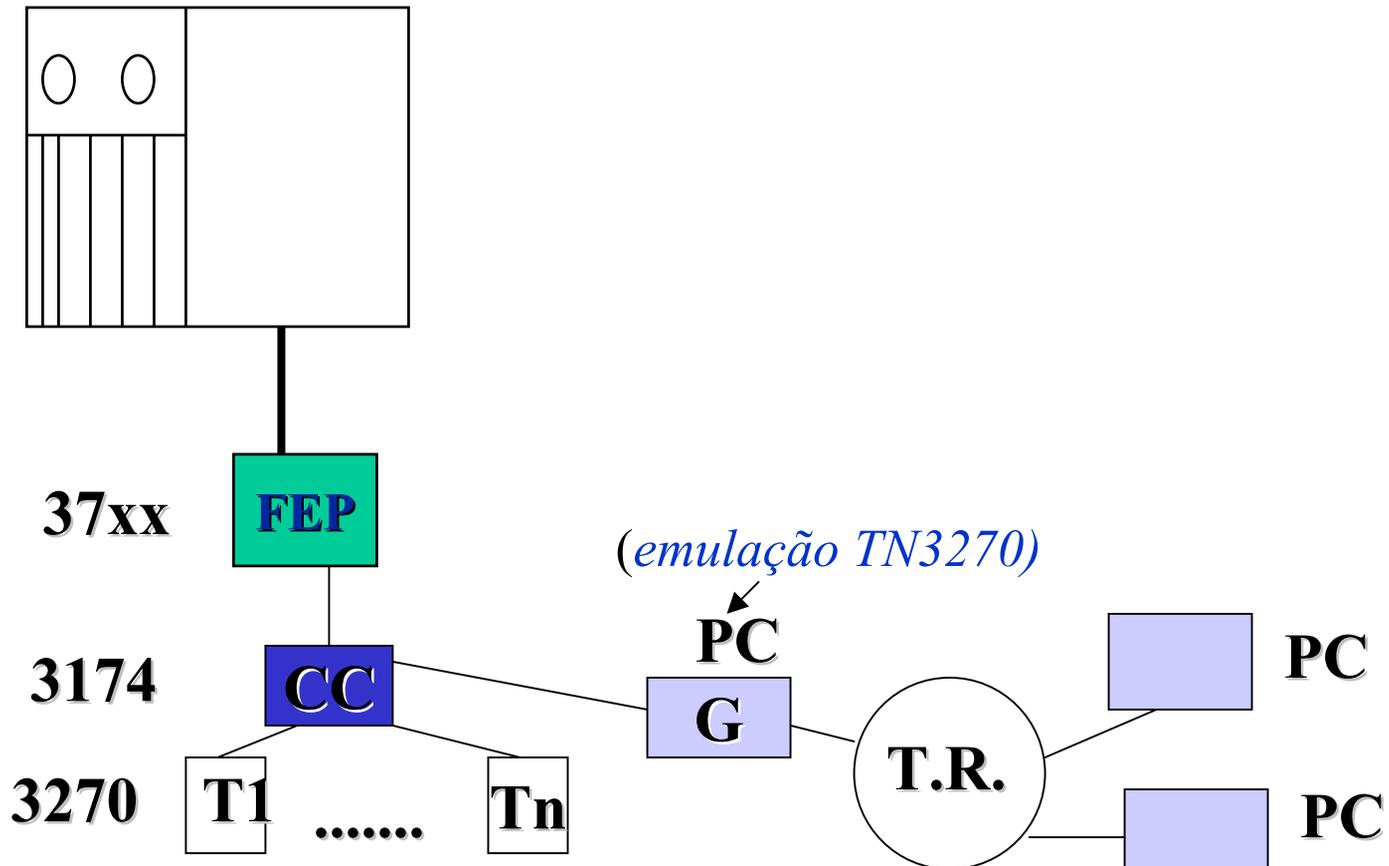
Topologia Física - Rede SNA

Exemplo - SNA/IBM e os possíveis Acessos Lógicos



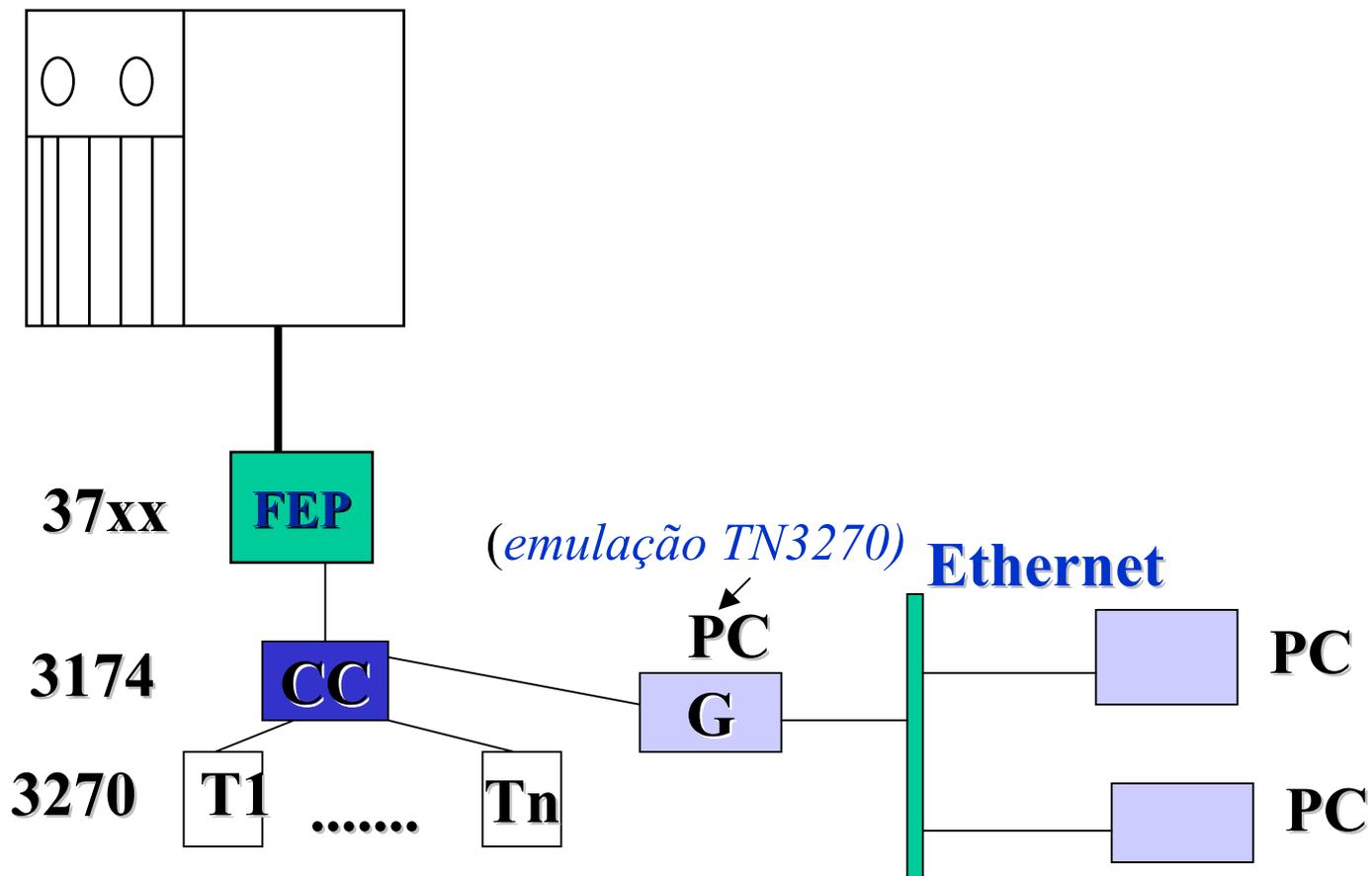
Topologia Física - Rede SNA

Exemplo - SNA/IBM



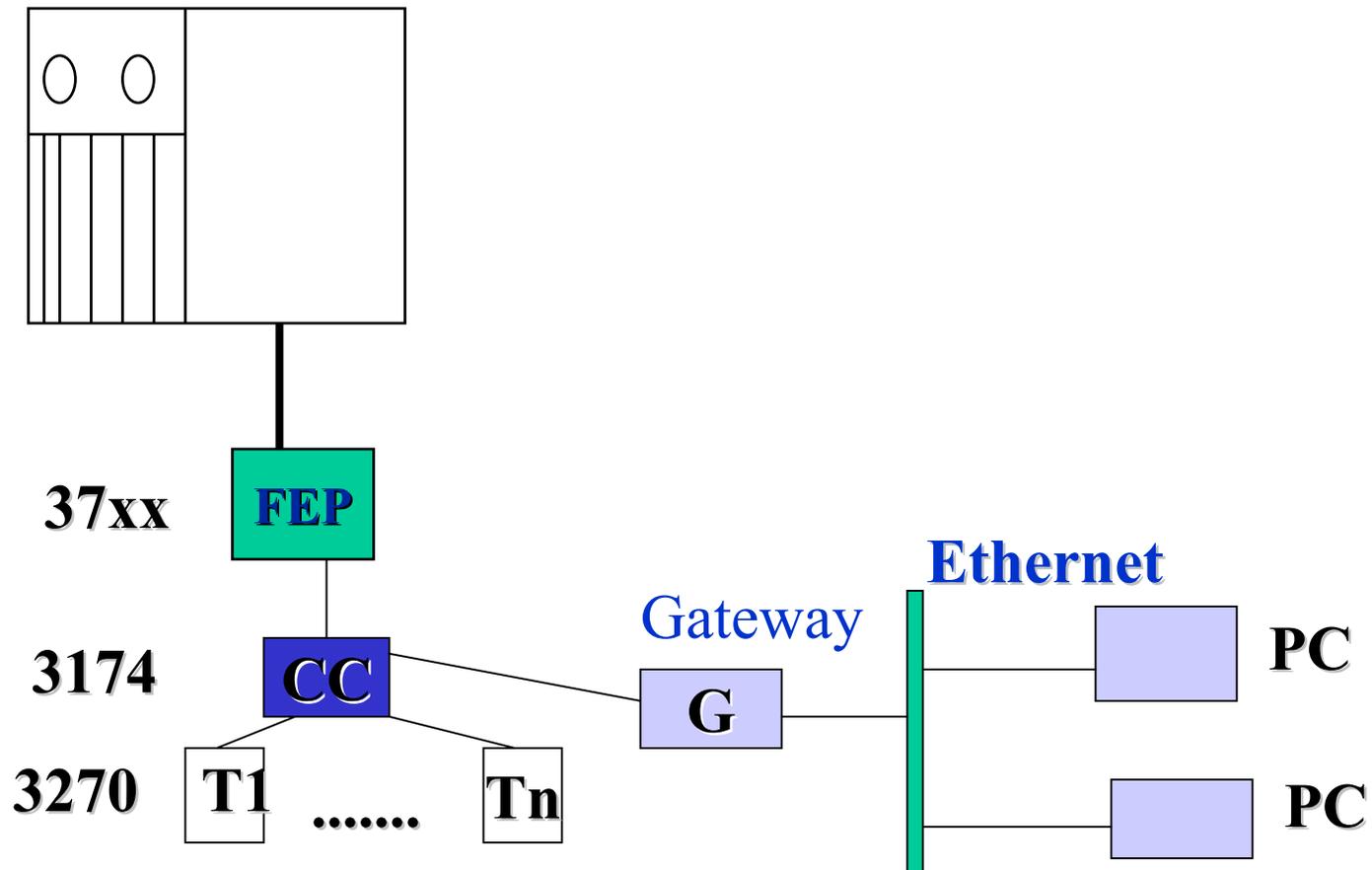
Topologia Física - Rede SNA

Exemplo - SNA/IBM e um Ambiente TCP/IP



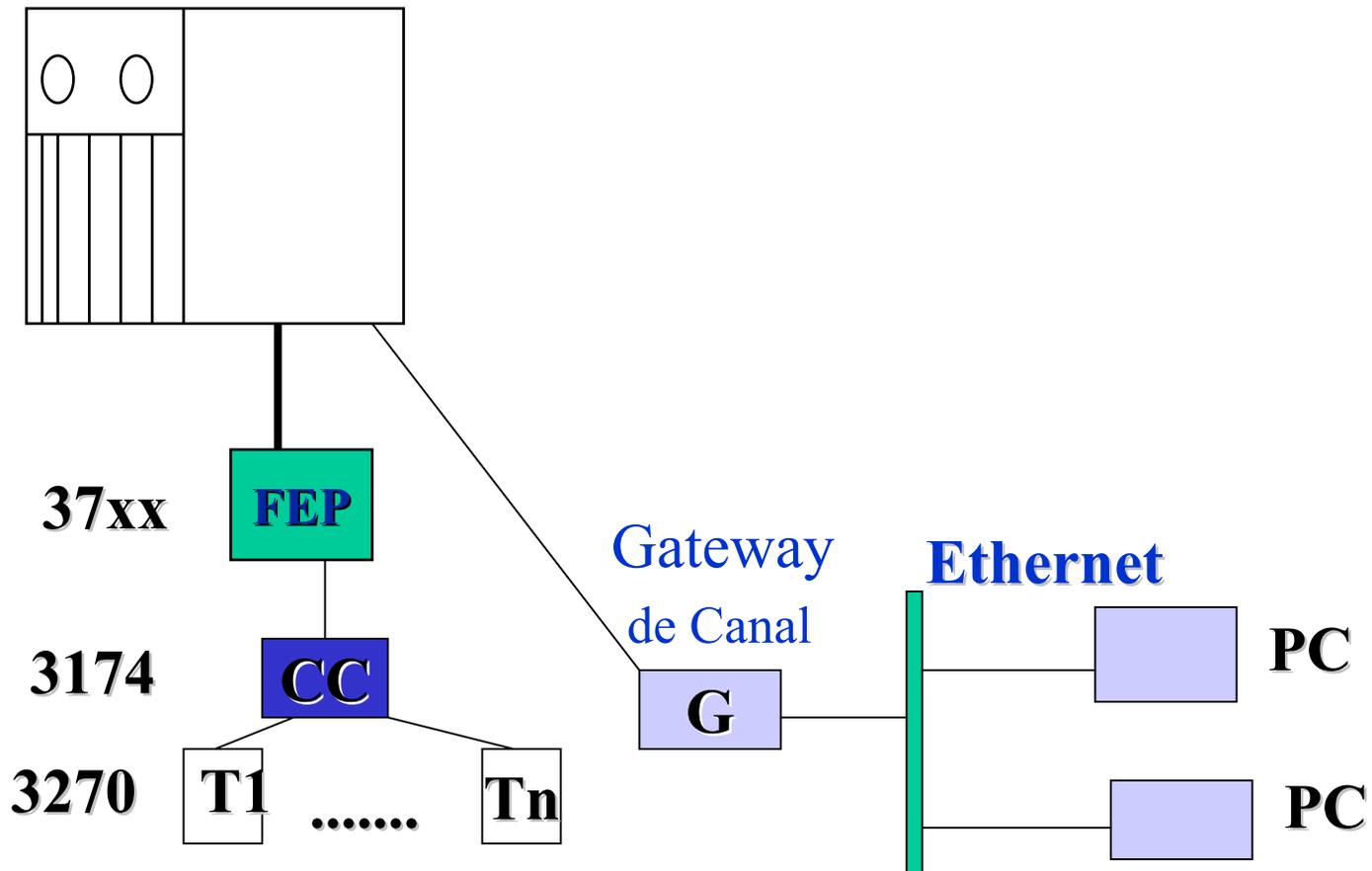
Topologia Física - Rede SNA

Exemplo - SNA/IBM e um Ambiente TCP/IP



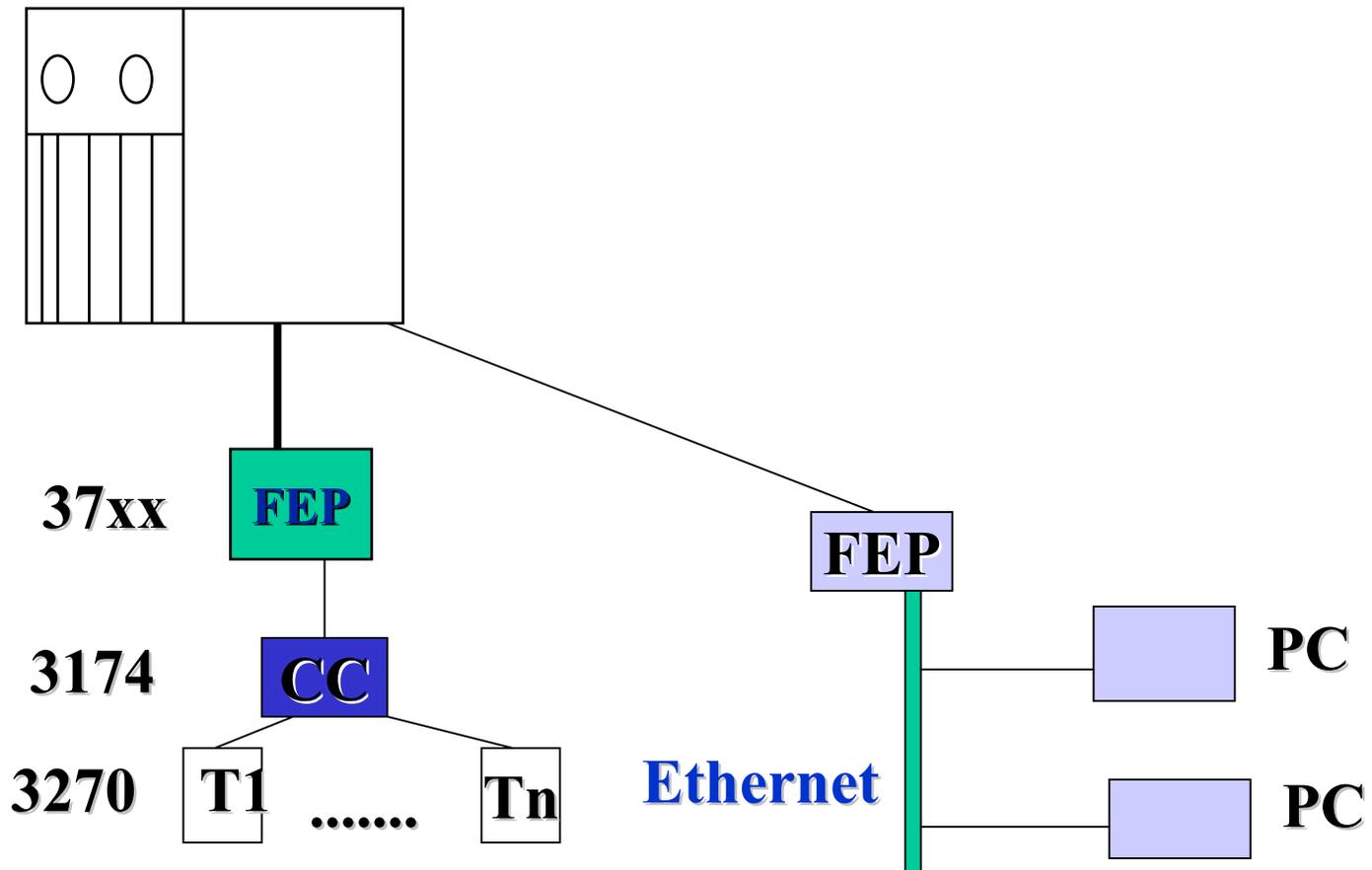
Topologia Física - Rede SNA

Exemplo - SNA/IBM e um Ambiente TCP/IP



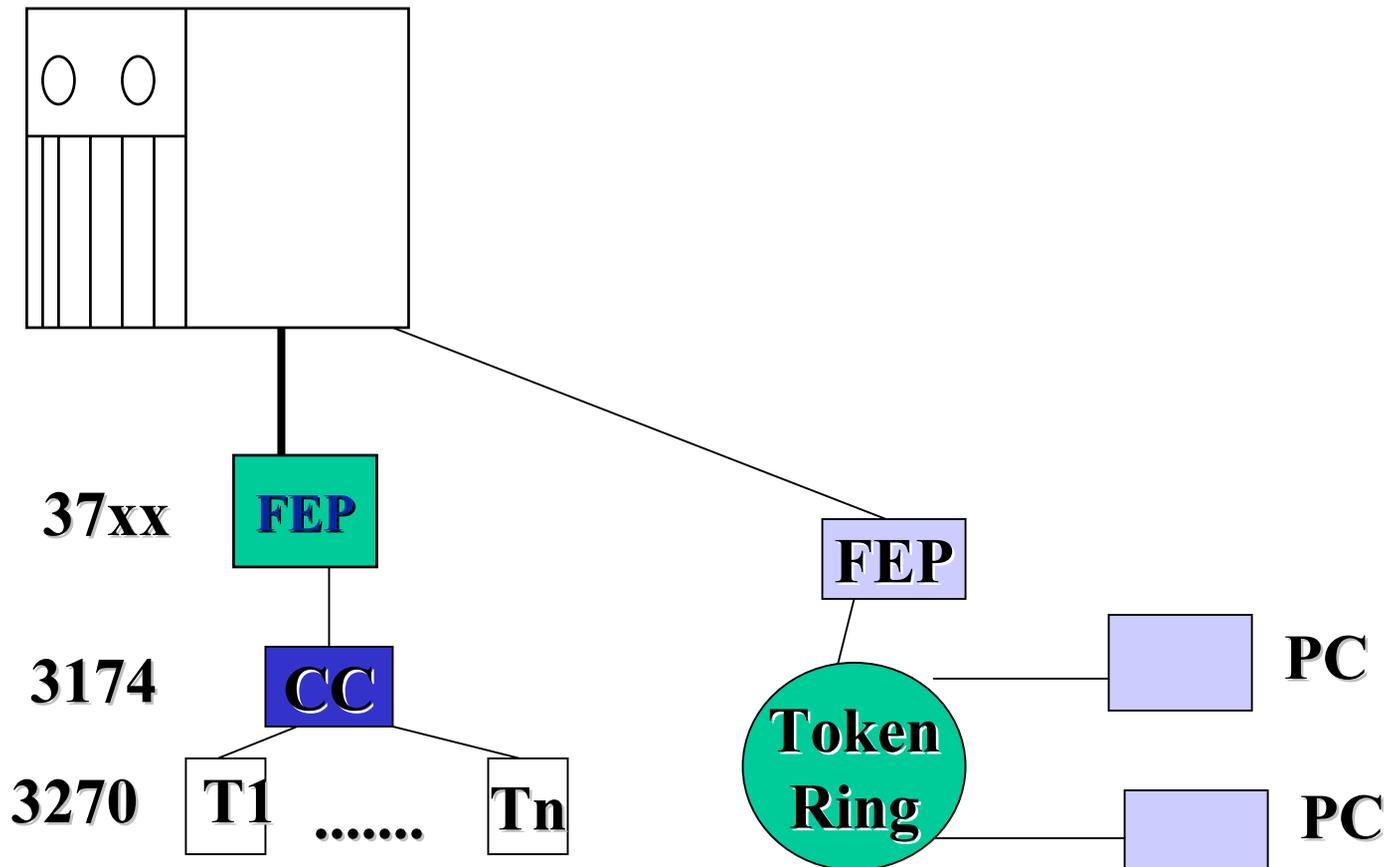
Topologia Física - Rede SNA

Exemplo - SNA/IBM e um Ambiente TCP/IP



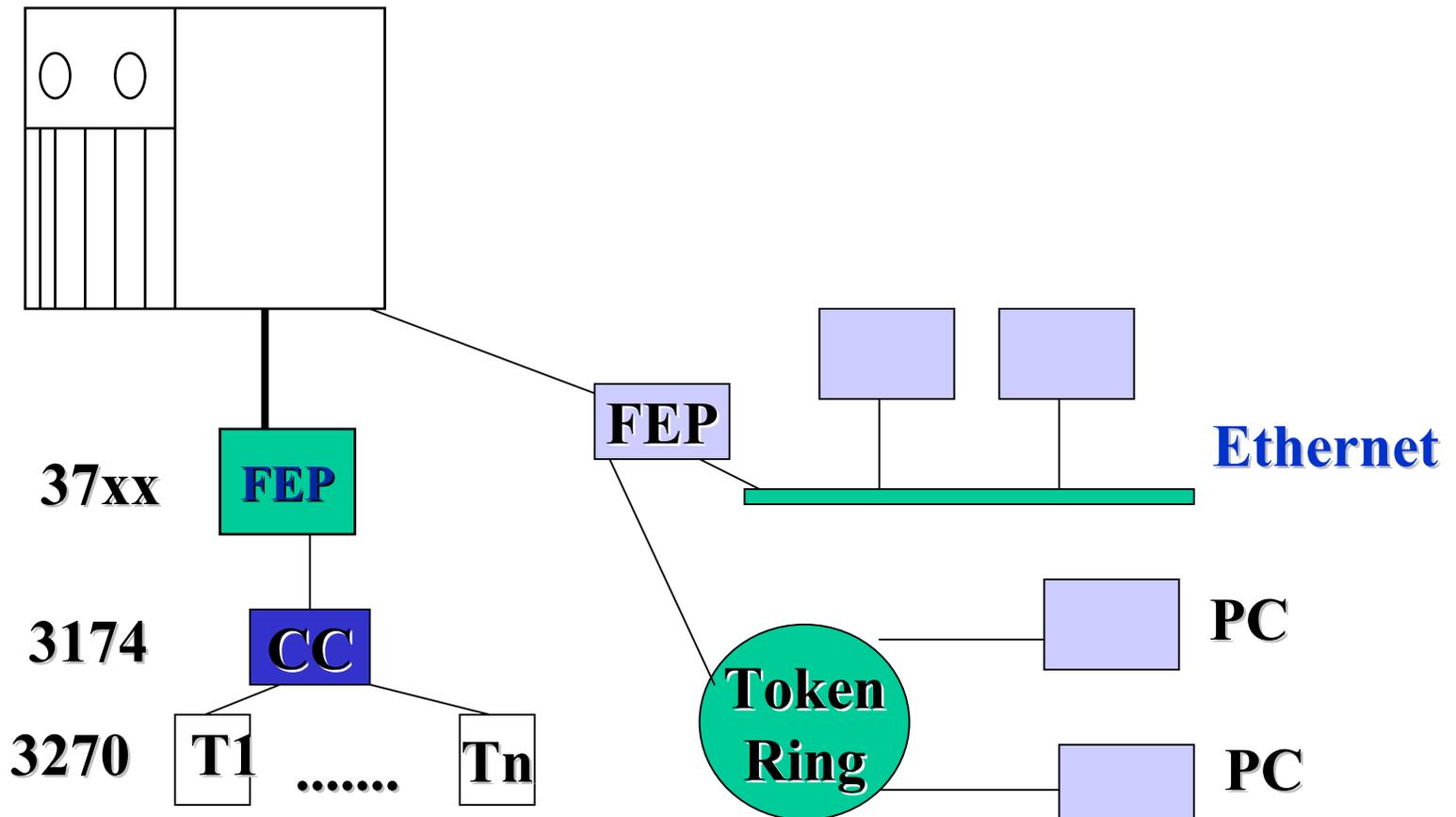
Topologia Física - Rede SNA

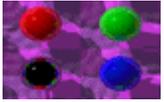
Exemplo - SNA/IBM e um Ambiente TCP/IP



Topologia Física - Rede SNA

Exemplo - SNA/IBM e um Ambiente TCP/IP





VII - Fiber Distributed Data Interface (FDDI)

O FDDI representa uma tecnologia de rede local que prove 100 Mbps sobre cabos de fibra ótica.

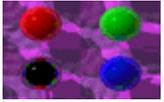
O padrão FDDI foi desenvolvido pela ANSI, Task Group X3T9.5.



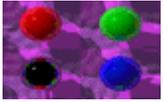
Por que a ANSI desenvolveu o padrão ?



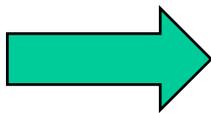
Pois o projeto do FDDI foi desenvolvido para conectar dispositivos de armazenamento e microprocessadores lossely coupled.



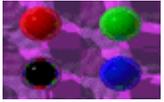
Embora o FDDI tenha sido desenvolvido como um padrão para I/O, ou seja não existiu um comite IEEE 802, esta foi a primeira LAN que nos anos 80 implementava um suporte de rede de 100 Mbps.



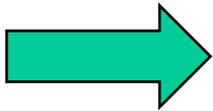
Como você imagina a topologia de uma LAN FDDI ?



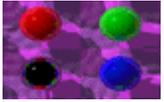
O FDDI usa dois anes como *backbone* de transmissão. Um primeiro, o primário. E um segundo, o secundário.



Como você imagina o funcionamento geral de uma LAN FDDI ?



O anel primário é empregado como meio para circular a informação. No caso de defeito, o anel secundário entra em ação. Este mecanismo é conhecido como self-healing. A topologia é conhecida como *counter-rotating ring*.

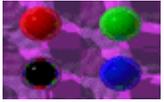


Como você imagina o acesso a uma LAN FDDI ?



Similar a uma rede *token ring*, a LAN FDDI usa um *token* para prover acesso a rede. A rede possui três tipos de *stations*. Sendo um SAS e dois tipo DAS.

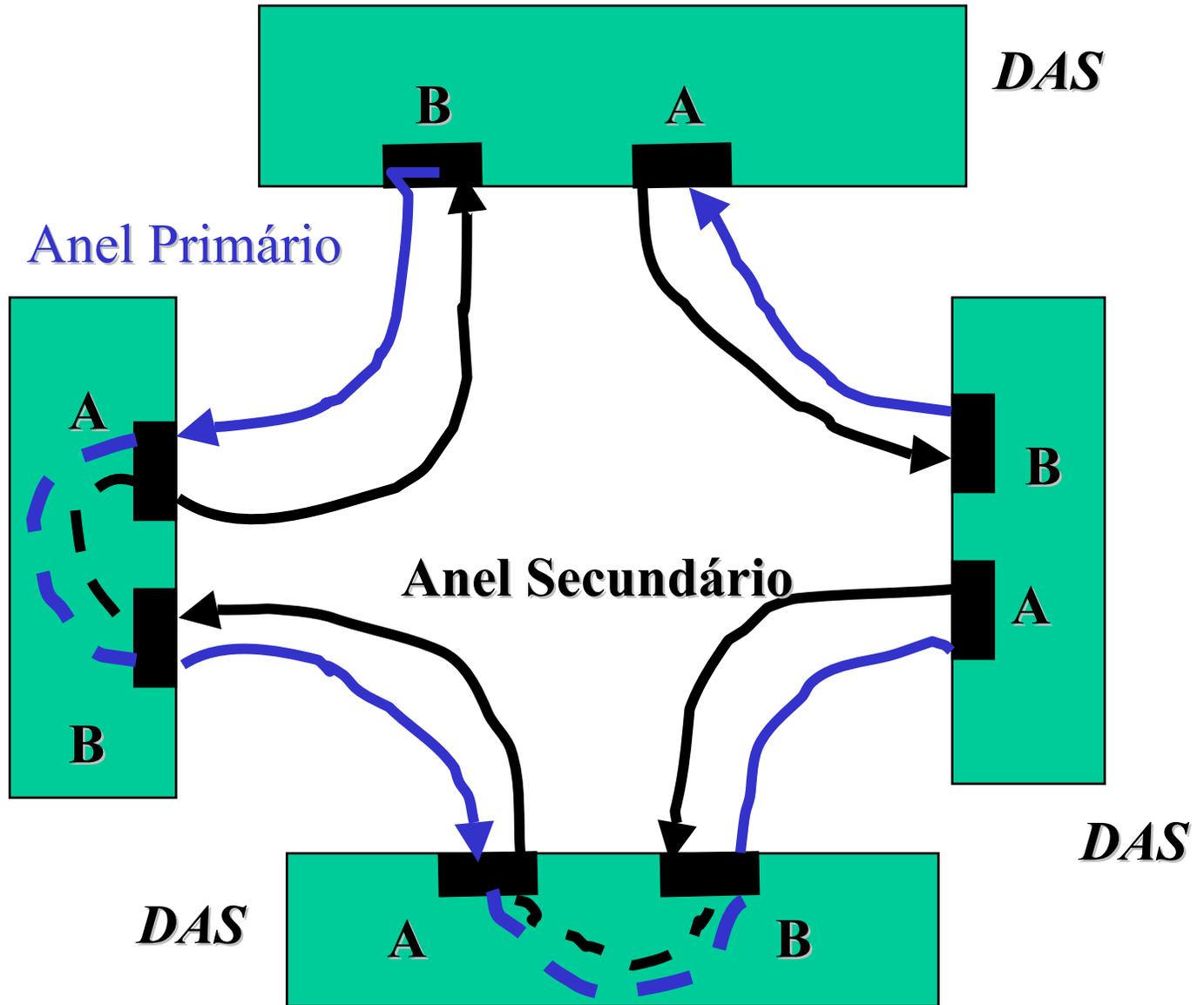
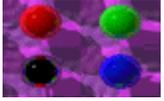
- SAS - Single Attached Station;
- DASs - Dual Attached Station.



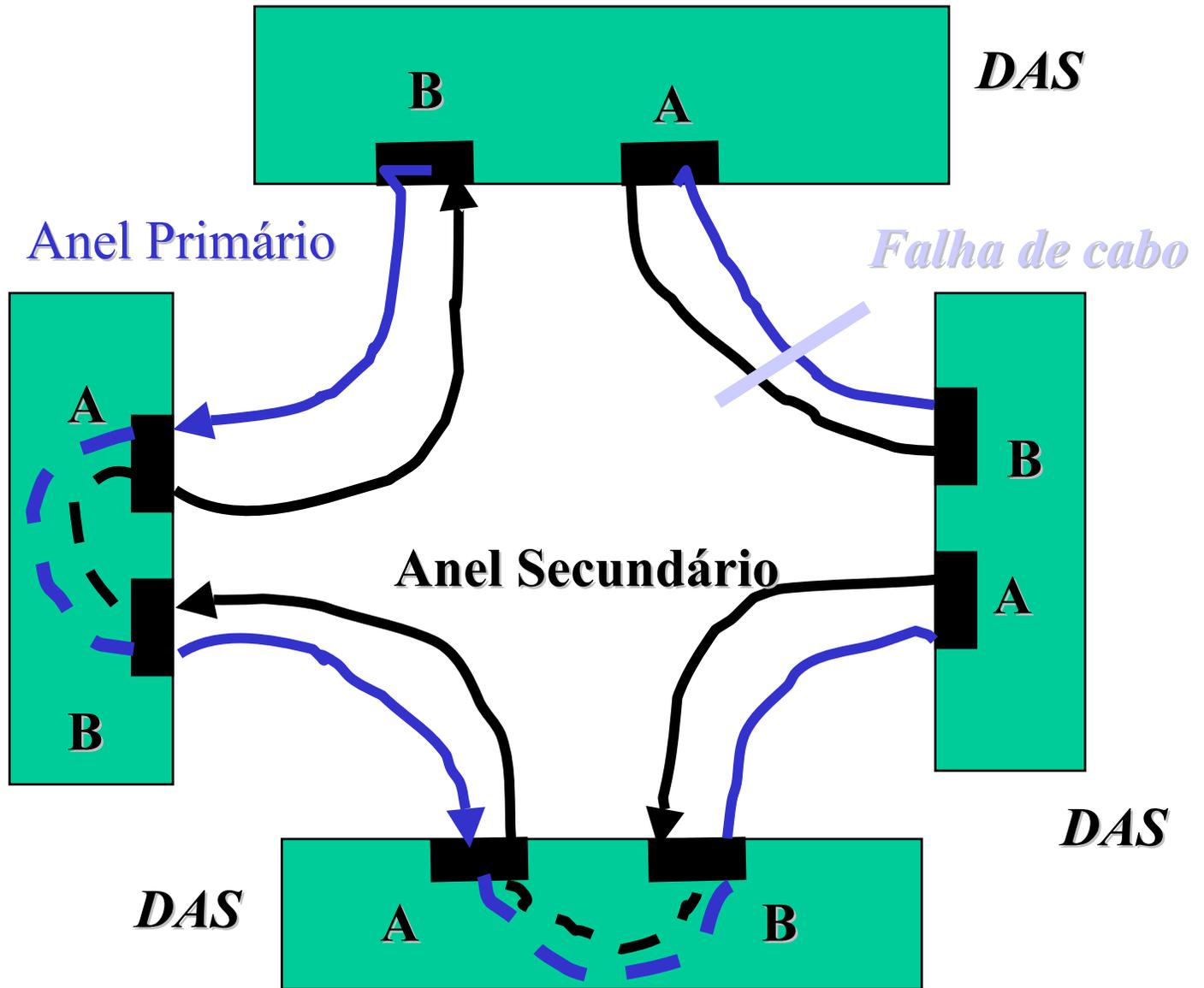
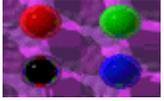
Computadores e dispositivos de rede, tais como pontes e roteadores, obtêm acesso a rede através de sua interface SAS. Esta é interconectada a uma interface DAS.

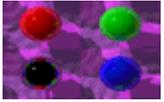
Cada DAS possui duas conexões óticas conhecidas como portas **A** e **B**. A porta **A** contém uma entrada de anel primário e uma saída secundária. Por outro lado, uma porta **B** contém uma saída de anel primário e uma entrada de anel secundária..

Primeiro exemplo de DAS



Primeiro exemplo de DAS



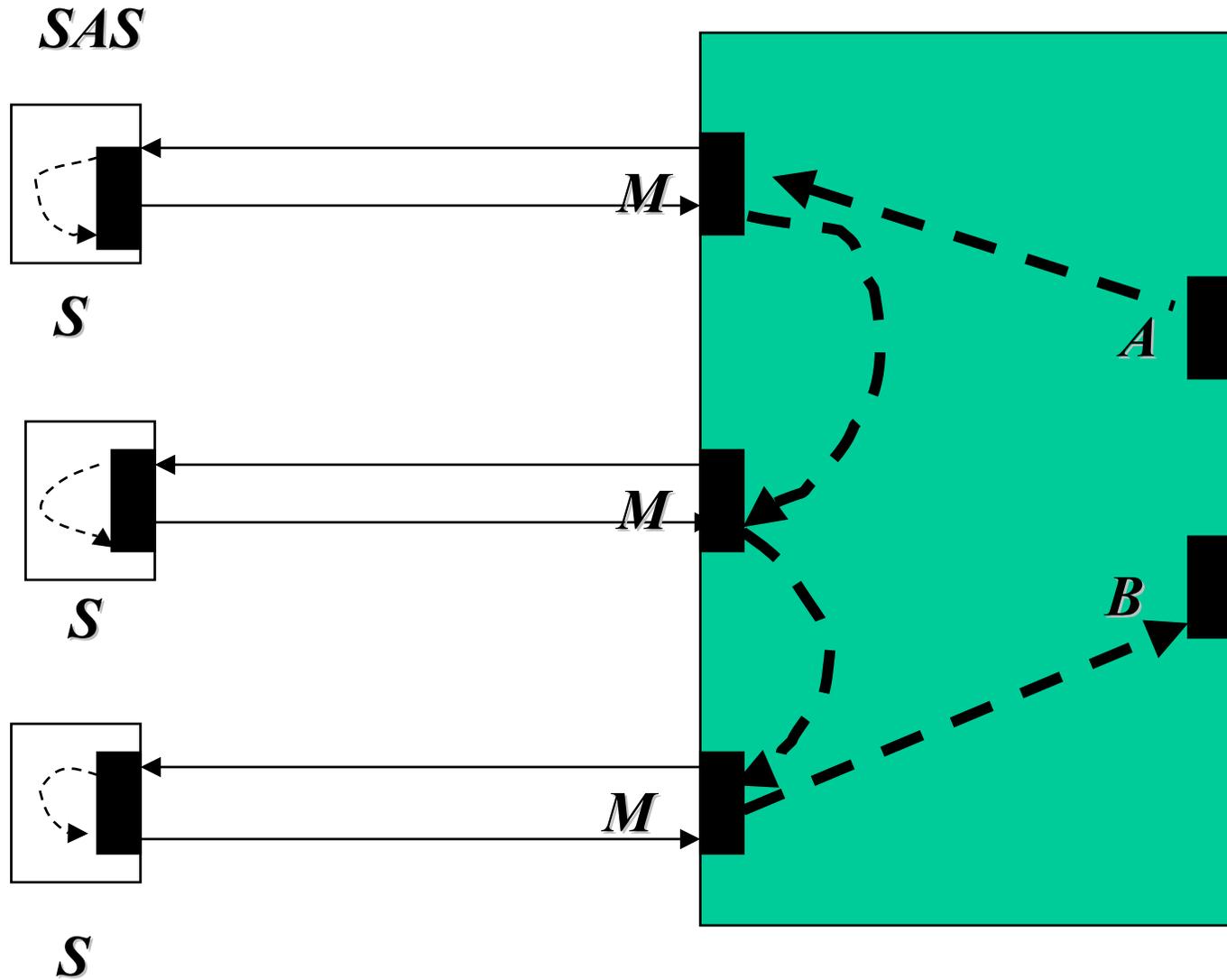
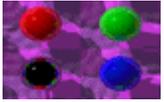


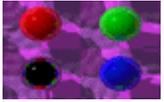
O segundo tipo de DAS cuja função é a de concentrador, contém um conjunto de interfaces (denominadas de **M**) em adição as interfaces **A** e **B**.

As interfaces **M**, ou master ports, são usadas para prover conectividade com **SAS.**, ou outras **DAS**. Com esta extensão é aumentada a capacidade de acesso ao anel primário.

Segundo exemplo de DAS

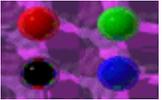
DAS





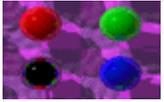
Características Gerais do FDDI

- Os conectores dos dispositivos SAS e DAS são diferentes para facilitar a conexão correta de cabos entre portas **M** e **S** ;
- A conexão entre portas SASs e DASs parecem obedecer uma topologia estrela, em oposição ao anel de DASs;
- A conexão entre portas SASs e DASs é efetuada através de um cabo contendo duas fibras, uma transmissão e outra para recepção;
- A característica de *self-healing* é somente obedecida na topologia em anel, ou seja entre DASs



Características Gerais do FDDI

- Nos anos 90 o uso comum das redes FDDI foram como *backbones* para a conexão de LANs de baixa velocidade, estas conectadas através de pontes ou roteadores;
- Outro ambiente de uso do FDDI foi como interface em dispositivos comutados (*switches*) para prover acesso de 100 Mbps para servidores;
- O elevado custo da fibra levou ao desenvolvimento do CDDI (Copper Distributed Data Interface), todavia o sucesso do Ethernet 100BASE-T fez com que a competitividade do CDDI não fosse viável.

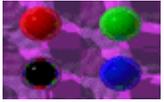


VIII- Asynchronous Transfer Mode (ATM)

8.1 - Introdução

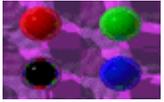
ATM é uma tecnologia de *switching* baseada *células* de tamanho fixo (*53 bytes*) para transporte da informação.

A filosofia da rede é a transferência da informação numa simples LAN, ou através do globo. Outra meta do ATM é a de ser uma ponte entre diferentes antigos legados de redes e a manutenção da oferta de uma qualidade de serviço.



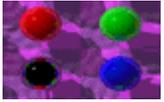
O desenvolvimento da tecnologia ATM é observado em quatro diferentes segmentos numa rede de computadores:

- Desktop (placas e conexões) ;
- LAN;
- Backbone ;
- WAN;

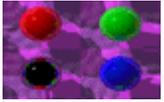


8.2 - Características do ATM

- O ATM não transfere as células de maneira assíncrona, como o nome sugere;
- As células são transmitidas de uma forma contínua e síncrona, sem interrupção entre as células;
- Quando não existe transmissão por parte do usuário, a célula ATM é preenchida com uma seqüência de bits para indicar que a célula está *vazia, ou livre*;



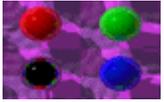
- A natureza assíncrona do ATM vem do tempo indeterminado quando a próxima unidade de informação lógica de conexão será iniciada;
- O tempo não utilizado por uma conexão lógica é cedido para outra conexão, ou usado por células livres;
- O significado do tempo não utilizado pode ser traduzido como *células para uma determinada conexão podem chegar de maneira assíncrona*;
- O roteamento de cada célula é efetuado através do endereço dentro da própria célula.



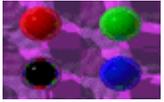
8.3 - Características das Células

A utilização de células pequenas e de tamanho fixo nas redes ATM resulta num conjunto de vantagens :

- Implementação em hardware de alto desempenho para os *switches* ATM. Estes são mais simples e mais efficientes;
- Em 622 Mbps, as células ATM podem ser comutadas em apenas $0.68\mu\text{s}$;



- O desempenho do ATM é uma importante consideração a ser observada por causa do fluxo orientado das células e a comutação rápida em hardware que permite que tenhamos um tamanho fixo para a célula; .
- Com o tamanho da célula fixo é possível fazer uma alocação de memória sem desperdício, uma vez que o incremento de memória será conhecido previamente;
- Não só o armazenamento das células é eficiente na memória, mas também a busca;
- Outro fator importante de células de tamanho pequeno e fixo, é o transporte eficiente de informação constante com baixa velocidade como a voz.

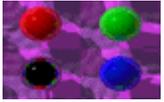


8.4 - Capacidade do ATM

O ATM, diferente de outros protocolos, pode transportar *voz, video, dados, imagem e gráficos* separadamente, ou simultaneamente empregando o mesmo enlace.

A característica de transporte de múltiplos tipo de informação no ATM deve-se ao fato do tamanho fixo das pequenas células do ATM e da qualidade de serviço (*QoS*).

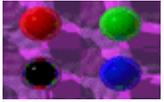
A figura a seguir nos mostra uma célula ATM e nos ajuda a entender a habilidade de transferência eficiente de informação multimídia.



8.5 - Campos da Célula

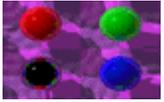
Os primeiros cinco bytes contém informação de controle, o cabeçalho e endereçamento. Os demais quarenta e oito bytes, chamados de *payload*, contém os dados.

O header to ATM é pequeno para maximizar a eficiência da rede ATM. Por outro lado, deveríamos ter o *payload* o maior possível para melhorar ainda mais o desempenho da rede. Todavia, as redes ATM foram projetadas para o transporte não exclusivo de grandes quantidades de informação. Informação como *voz* e o *tráfego de vídeo* são *payloads* endereçados pelo ATM.



O Forum ATM (<http://www.atmforum.org>) quando das discussões da concepção do padrão, não apenas se preocupou com a eficiência, mas também com o efeito do *retardo de empacotamento*.

O *retardo de empacotamento* é o tempo gasto para o preenchimento de uma célula ATM com uma amostra de voz digitalizada de 64 kbps. O tamanho de 53 bytes da célula ATM foi um compromisso entre a eficiência de *payload* e o *retardo de empacotamento*.



Célula ATM Genérica



GPC - Generic Flow Control (só para UNI)

VPI - Virtual Path Identifier

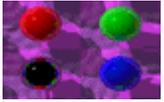
VCI - Virtual Channel Identifier

PTI - Payload Type

CLP - Cell Loss Priority

HEC - Header Error Control

PDU - Protocol Data Unit

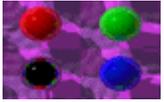


Apresentamos a seguir os campos de uma célula ATM :

- GPC (Generic Flow Control) - estes 4 bits são usados para o controle local de fluxo para múltiplos usuários no lado do usuário de uma switch compartilhando o acesso sob uma linha padrão adotando-se uma ***UNI padronizada***. Este campo geralmente não é usado e é setado para 0.

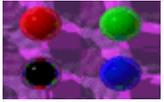
No caso de uma rede privada para uma interface de rede ***P-NNI (Private Network Network Interface)*** estes bits são usados para informação de endereço.

- VPI (*Virtual Path Identifier*)- os 8 bits do provêm 255 possíveis caminhos para as células UNI e 4095 para P-NNI.



- VCI (*Virtual Channel Identifier*) - cria a possibilidade de uso de mais 16 bits, ou seja 65536, possíveis conexões dentro de cada *path de endereço*. Alguns endereços são usados para funções reservadas como sinalização.
- PTI (*Payload Type Identifier*) - este campo para a distinção entre células de usuários das células chamadas de OA&M (Operation, Administration and Maintenance), que são comandos e estatísticas na rede.

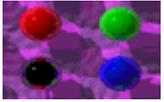
No caso de um *engarafamento (congestion)* na rede o PTI é alterado a medida que ele vai passando entre os *switches*. Assim, a rede pode diminuir o *engarafamento* descartando células que estão em excesso para a garantia de uma determinada velocidade.



- CLP (*Cell Loss Priority*) - este bit é um indicador de dois estados de prioridade informando a rede qual célula deve ser descartada no caso de *engarafamento* da rede.

O campo CLP é setado para 0 inicialmente nas células. Quando as mesmas trafegam pela rede e um determinado *switch* observa que existe um congestionamento, a célula terá seu CLP modificado para 1 pelo *switch*. Esta mudança sinaliza que não existe condição de ser atendido os parâmetros negociados durante o início da conexão.

As células com bit igual a um serão descartadas primeiramente. Caso o problema continue, aquelas com valor 0 começarão a ser descartadas.

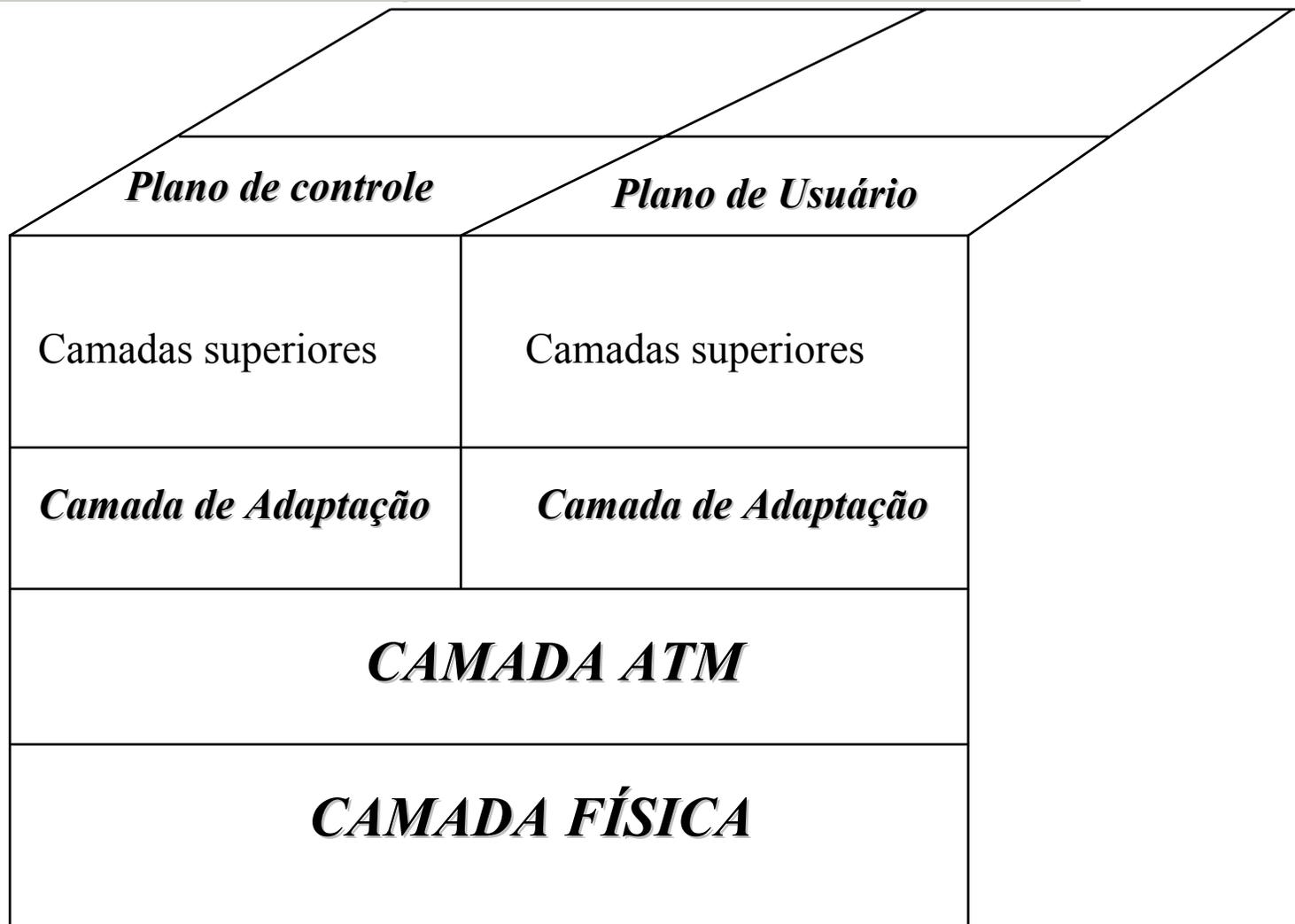
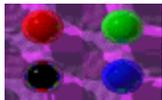


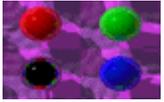
- HEC (Header Error Control) - possui a capacidade de corrigir erros simples de cabeçalho e detectar erros múltiplos para assegurar o endereçamento correto.

No caso de header com múltiplos erros, estes serão descartados pelo *nó*, ou *switch*, que detectar o erro.

O HEC não faz verificação de erros no *payload*, uma vez que os mesmos devem ser tratados pelos protocolos de transporte.

8.6 - Modelo de Referência de Protocolo (PRM)

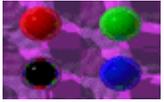




As três camadas do ATM têm as seguintes funções :

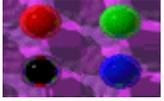
(1) *Física* : conversão dos sinais para um formato elétrico, ou ótico, compatível para o carregamento/descarregamento de células para um quadro de transmissão adequado. Alguns dos meios físicos suportados são :

155 Mbps	Sonet/STS-3c, fibra ótica
	Cat 5 UTP
622 Mbps	Sonet/STS-12c, fibra ótica
25 Mbps	Cat 3,4 e 5



(2) *ATM* : prove a comutação e o roteamento dos pacotes ATM, para seus respectivos VPIs e VCIs. Este nível é responsável por gerar os headers das células ATM e extraí-los quando as células chegam.

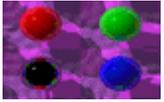
De uma forma geral, a camada ATM é responsável por prover um conjunto comum de serviços para suporte aos protocolos de alto-nível, tais serviços podem ser traduzidos nos dados, voz, imagem e aplicações de vídeo.



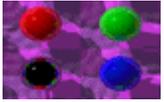
(3) *AAL* : esta camada garante a transferência de dados de uma determinada fonte para a aplicação destino sob uma rede ATM. A AAL empacota os dados da aplicação em células antes do seu efetivo transporte e os extraí no nó destinatário.

O AAL é composto de diversos tipos, devido aos diferentes tipos de tráfego existente. Existem cinco AAL, estes :

- AAL 1- usado para aplicação de tempo real e aplicações de bit constante - tais como voz e vídeo;



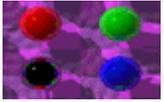
- AAL 2 - usado para aplicação de tempo real e aplicações de bit variável, como por exemplo vídeo de MPEG;
- AAL 3/4 - estas camadas foram projetadas para prover suporte para aplicações que não necessitam de tempo real, originalmente idealizada como suporte ao tráfego de LANs;
- AAL 5 - esta camada foi projetada para substituir a AAL 3/4 para propósitos de suporte as LANs, uma vez que possui baixo overhead por célula e um protocolo de encapsulamento simples.



8.7 - ATM x Gigabit Ethernet

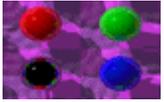
Qualquer comparação entre o ATM e o Gigabit Ethernet deve ser levado em conta o contexto, isto é desktop/LAN/WAN.

- Desktop - a maioria das placas de rede no computadores, sejam estes pessoais ou workstations empregam a tecnologia 100Base-T;
- WAN - por outro lado, as redes WANs estão ficando a cada dia mais orientadas a ATM. Nos USA, muitas redes frame relay estão empregando *switches ATM*;



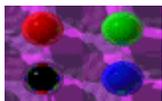
8.7 - ATM x Gigabit Ethernet

- LAN (ou em redes corporativas) podem empregar indistintamente ATM e Gigabit Ethernet. A escolha de uma, ou outra tecnologia, é uma função de parâmetros tais como custo e serviços solicitados pela aplicação, tamanho da rede, topologia e necessidade de redundância.



Comparação global entre Gigabit Ethernet e ATM

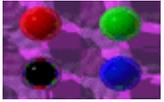
<i>Rede</i>	<i>Desktop</i>	<i>Protocolos de LAN</i>	<i>Escalabilidade</i>	<i>WAN</i>	<i>QoS/ Multimídia</i>
<i>Ethernet</i>	<i>Sim</i>	<i>Sim</i>	<i>Sim</i>	<i>Emergente</i>	<i>Emergente</i>
<i>ATM</i>	<i>Sim, com MPOA e LANE</i>	<i>Sim, com MPOA e LANE</i>	<i>Sim, com MPOA e LANE</i>	<i>Yes</i>	<i>Yes</i>



Facilidades do Gigabit Ethernet e ATM

<i>Facilidades</i>	<i>Ethernet</i>	<i>ATM</i>
<i>P/P/L</i>	<i>Baixo custo</i>	<i>Custo Moderado</i>
<i>QoS</i>	<i>RSVP, IEEE802.1Q/p</i>	<i>Garantida com a gerência de tráfego</i>
<i>Aplicações Usuários</i>	<i>Dados de Alta velocidade voz/video sobre IP</i>	<i>Dados, voz e video</i>
<i>Disponibilidade</i>	<i>Final de 1997</i>	<i>Comço de 1996</i>
<i>Aplicações de Rede</i>	<i>Backbones, servidores Campus backbones</i>	<i>WAN, Backbones e Servidores Campus Backbones.</i>

P/P/L - Preço/Performance/Largura de Banda

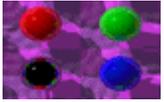


Os protocolos que executam sobre o ATM devem ser adaptados para executar em cima da camada de adaptação.

Três clássicas soluções são :

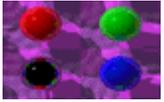
- IP sobre ATM - é uma abordagem antiga com uma base instalada considerável. É um protocolo de nível 3, que mapeia endereços IP para endereços ATM. Assim, é permitido que dispositivos ATM enviar pacotes IP nas redes ATM.

As desvantagens da abordagem são (1) o IP só aceita o protocolo IP , (2) IP sobre ATM não possui suporte para tráfego multicast e (3) a falta de um protocolo de alocação dinâmica de endereços IP/ATM causa problema de escala.

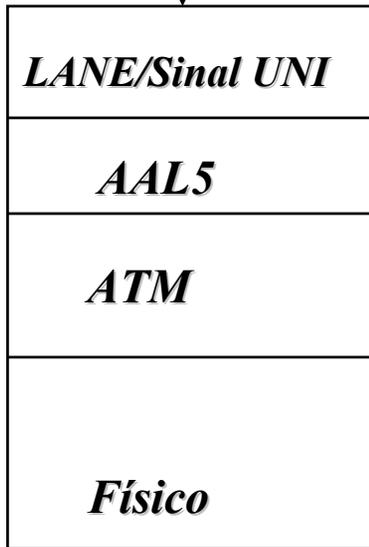


- O protocolo LANE (*LAN Emulation*) foi desenvolvido para *esconder* dos usuários Ethernet a rede ATM. Assim, o LANE trabalha como uma ponte em cima do AAL5.

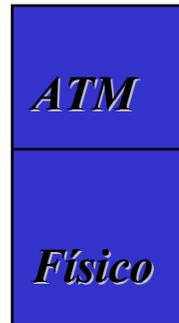
O protocolo encapsula todos os pacotes no MAC Ethernet e então é enviado para a rede ATM.



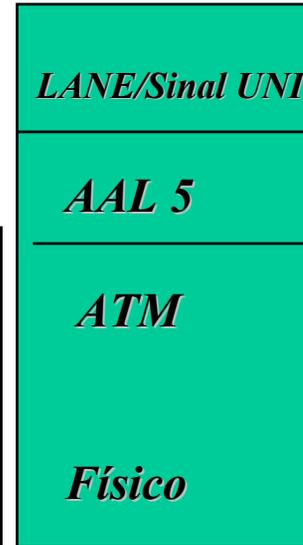
ATM LANE HOST



ATM Switch

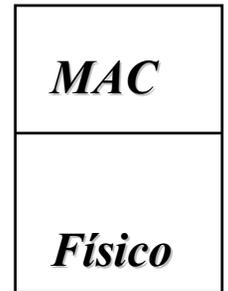


Switch Nível 2



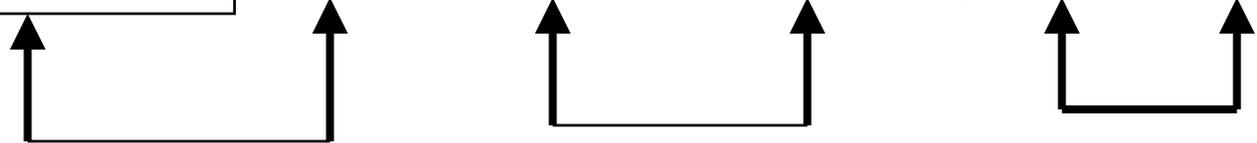
Drive de rede

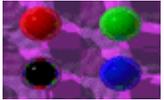
Ethernet Host



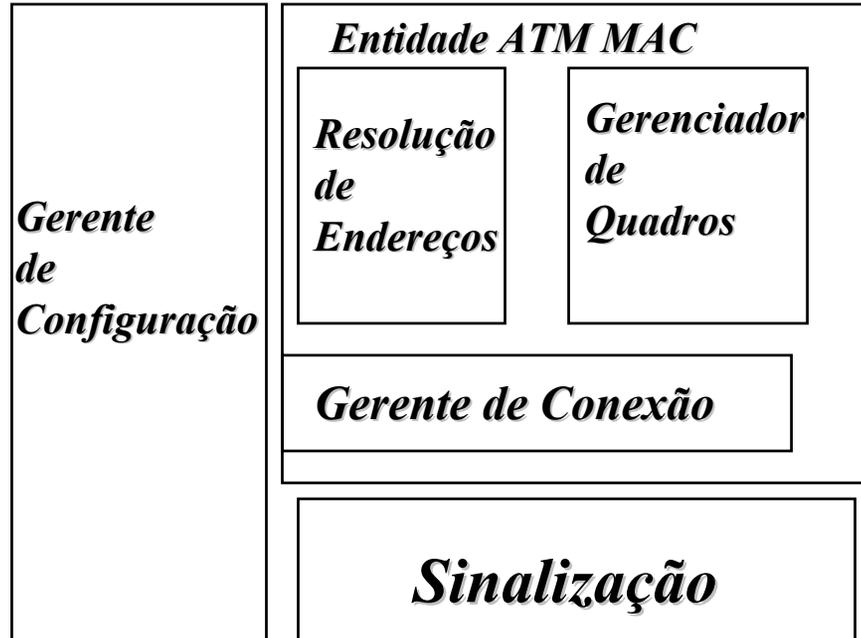
Célula ATM

Quadro Ethernet





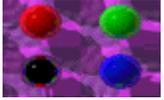
Subcamada ATM-MAC



AAL 1/AAL 2/AAL 3-4/AAL5

Camada ATM

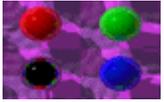
Camada Física



- ***MPOA (MultiProtocol Over ATM)*** foi um protocolo desenvolvido pelo ATM Forum objetivando prover protocolo de roteamento para múltiplos protocolos.

A idéia do MPOA é prover de forma limpa um ambiente de *inter-rede* nas redes ATMs considerados antigos legados, como por exemplo o Ethernet.

O MPOA prove os serviços do IP sobre ATM e LANE, fazendo a ponte e roteamento de pacotes.



IX - Dispositivos de Interconexão

Visando a expansão das redes, existem vários dispositivos cujas funções possibilitam efetuar de maneira transparente para os usuários e as aplicações uma extensão do alcance da rede.

Desta forma, neste tópico vamos trabalhar com os hubs, repetidores, pontes (bridges), roteadores e gateways.

Ligação Inter-Redes

Antes trabalhar com qualquer protocolo a nível de rede, é interessante um trabalho inicial para compreendermos como as redes podem ser interligadas em diferentes situações. A ligação denominada de *inter-rede* é um tópico essencial para que possamos trabalhar com os princípios e eventuais problemas da camada de rede de qualquer protocolo.

Ligação Inter-Redes

HUBS

- Passivo: nestes equipamentos só existem sinais do segmento de rede. NÃO existe regeneração de sinal.
- Ativo: existe nestes dispositivos *a regeneração* de sinal, o que significa que a rede pode abranger distâncias maiores em termos de cabeamento.
- Inteligentes: além de *regenerar* os sinais, estes dispositivos podem fazer *gerência e seleção* de conexões.

Ligação Inter-Redes

Repetidores -

São empregados para a interligação de redes de idênticas arquiteturas.

A função de um repetidor é receber os pacotes de um segmento, ou rede, e repetir este pacote para o outro segmento de rede.

Não é efetuado nenhum tratamento sobre o pacote.



Repetidor



Ligação Inter-Redes

Pontes (Bridges) -

As pontes são dispositivos que interligam segmentos de redes. O objetivo do uso de uma ponte, ao invés de um repetidor pode ser entendido pelos seguintes pontos :

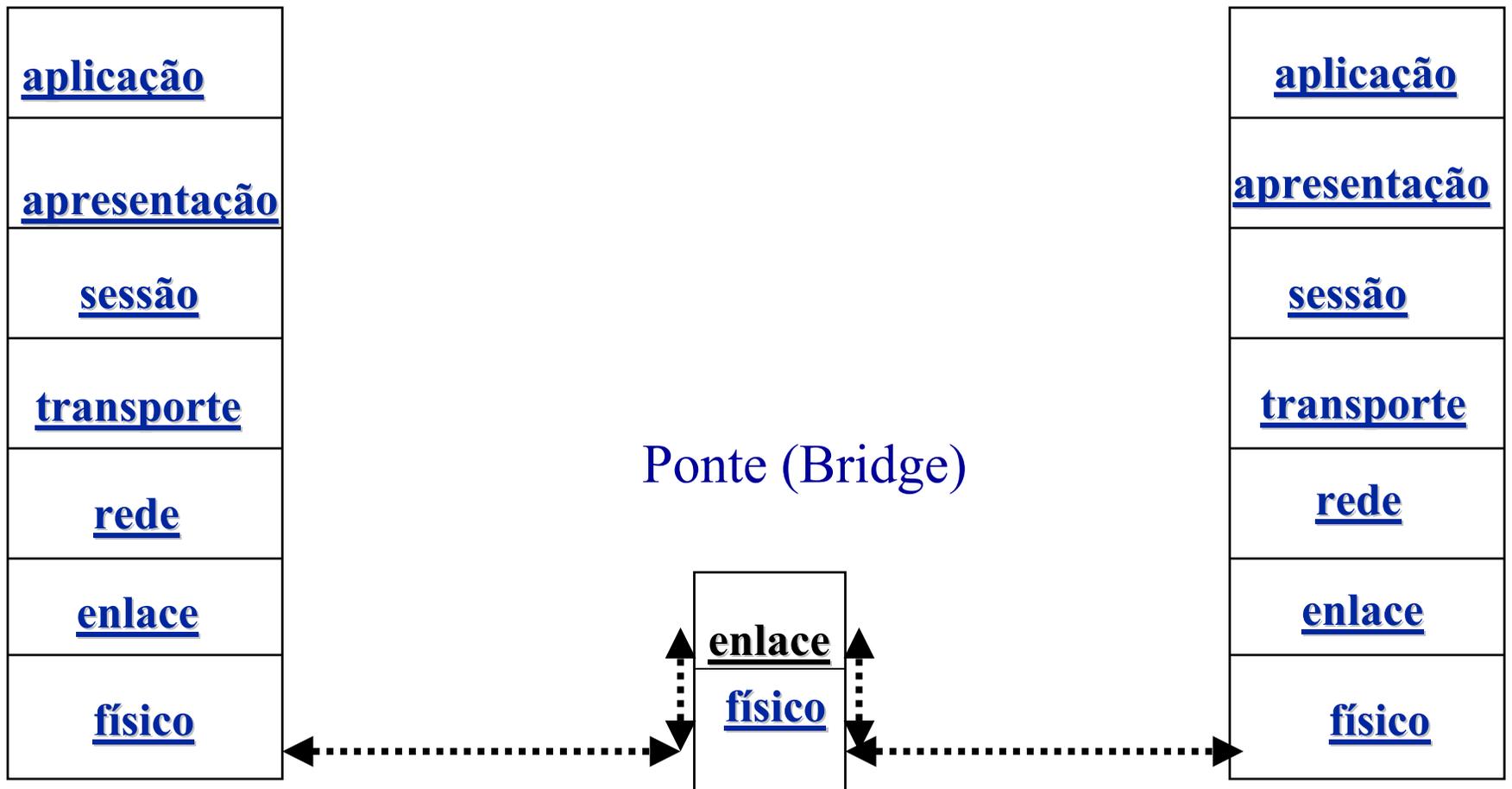
- deseja-se a transmissão de pacotes entre dois segmentos de rede;
- deseja-se um filtro na transmissão entre os dois segmentos;
- deseja-se uma facilidade de armazenamento para a transmissão entre os segmentos;
- deseja-se melhorar o desempenho de uma rede que começa a crescer;
- deseja-se que numa eventual falha de um dos segmentos o outro não seja afetado;

Bridges Convencionais

As *bridges convencionais* conectam segmentos de uma mesma tecnologia de rede. As *bridges* são usadas para *aumentar* a capacidade da rede, pois diferente dos *repetidores* estas selecionam/filtram os sinais entre os segmentos. Quando uma mensagem é por exemplo de um segmento A, este não é propagado num segmento B.

Bridges de Tradução

As *bridges de tradução* têm a função de resolver as diferenças de formatos dos quadros das diferentes LANs na camada de MAC. Uma outra função destes equipamentos é, por exemplo, tratar das diferenças entre as diversas velocidades de implementação das redes interligadas .



Ligação Inter-Redes

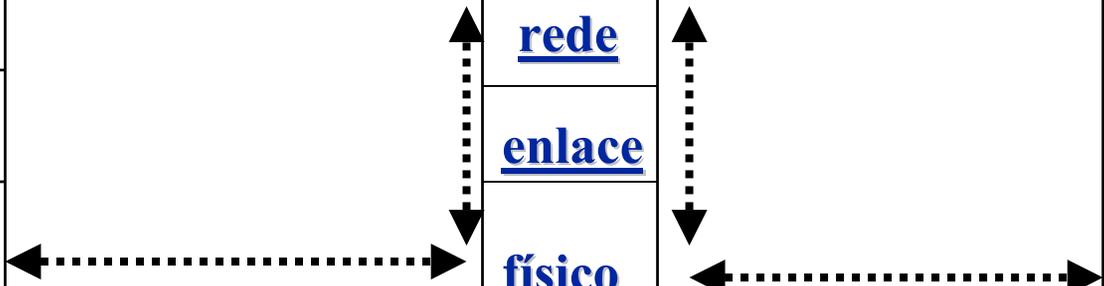
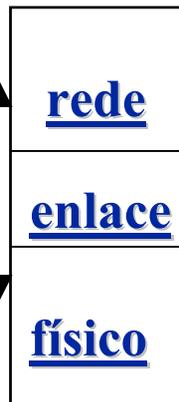
Roteadores (Routers)-

Os roteadores são os dispositivos que permitem a interligação de redes distintas formando-se um verdadeiro ambiente de inter-rede.

De uma maneira mais específica, os roteadores são responsáveis pelo recebimento dos pacotes do nível inferior, tratar o cabeçalho de inter-rede destes pacotes, descobrindo qual o roteamento necessário, construir um novo pacote com um novo cabeçalho de inter-rede e quando necessário enviar o novo pacote para o novo destino.



Roteador (router)



Ligação Inter-Redes

Como uma determinada *rede* pode ser composta por um conjunto de redes internas independentes, denomina-se este ambiente como um *sistema autônomo*.

Os protocolos utilizados dentro de um sistema autônomo, que efetuam as funções de roteamento, são chamados de **IGP** (Interior Gateway Protocol).

Por outro lado, aqueles protocolos empregados para interligar sistemas autônomos distintos, são conhecidos por **EGP** (Exterior Gateway Protocol).

Ligação Inter-Redes

Gateways -

Os gateways são um tipo especial de roteador empregado para fazer o roteamento de pacotes em redes com arquiteturas distintas. A idéia é que duas aplicações em dois ambientes distintos possam se comunicar, apesar das diferenças entres seus respectivos *hosts*.

Ligação Inter-Redes

Uma situação que ilustra como exemplo o uso de *gateways* é eficaz, é aquela na qual um *host* de uma rede TCP/IP deseja fazer um conexão e se interoperar com um ambiente IBM/SNA. Nenhuma das camadas dos dois protocolos têm alguma similaridade, então o roteamento ocorre não só entre as diferentes arquiteturas mas também entre as diferentes camadas.

