


Especialização em Ciência da Computação:
Desenvolvimento de Sistemas Distribuídos
com Orientação a Objetos



Tecnologias de Redes de Computadores

Prof. Mario A.R. Dantas

E-mail: mardantas@computer.org

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, etc).

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*.

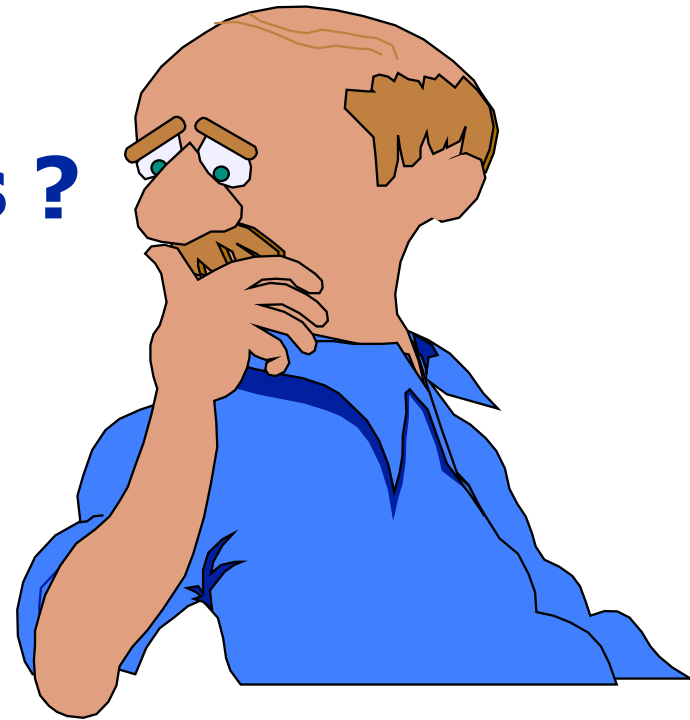
Motivação



- 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 ?**

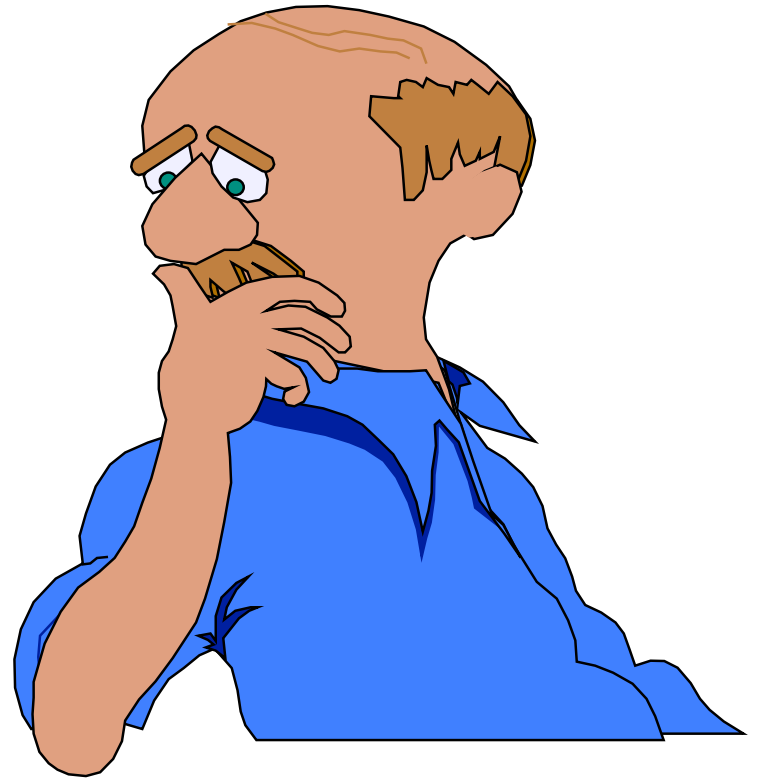


Qual é a sua visão de rede?

- ⌘ **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 ?



Conteúdo



I- Introdução aos princípios de comunicação

II - Arquitetura dos Computadores Modernos

III - Padrões dos Meios Físicos das Redes Locais (LANs), Metropolitanas(MANs) e o padrão IEEE.

Conteúdo



IV-Dispositivos de interconexão de redes.

V - Arquitetura TCP/IP.

**VI - Redes de alta velocidade
(FDDI, ATM, Fast Ethernet, Myrinet).**

Referências Bibliográficas



Livro Texto

- *Tecnologias de Redes de Comunicação e Computadores*, Mario Dantas, Axcel-Books, 2002, ISBN 85-7323-169-6

Outros Livros Acadêmicos

- *Computer Networks*, Andrew Tanenbaum, Third Edition, Editora Prentice-Hall, 1996, ISBN 013-394-248-1
- *Redes de Computadores - Das LANs, MANs e WANs as Redes ATM*, Soares-Lemos-Colher, Editora Campus, 1995, ISBN 85-7001-954-8

Referências Bibliográficas



Livros Profissionais

TCP/IP - Internet, Protocolos e Tecnologias, Fernando Albuquerque, Editora Axcel, 2a. Edição, 1999.

Internetworking com TCP/IP - Tecnologia e Infraestrutura, Geoff Bennett, Editora IBPI-Press, 1998, ISBN 85-7331-857-X

Internetworking com TCP/IP - Protocolos, Serviços, Segurança e Performance, Volume 2, Geoff Bennett, Editora IBPI-Press, 1998, ISBN 85-7331-868-x

Planning and Design- High Speed Networks- Using 100VG-AnyLAN, Second Edition, Janis Furtek Costa, Prentice-Hall, 1995 ISBN 0-13-439092-x

Conteúdo



I- Introdução aos princípios de comunicação

II - Arquitetura dos Computadores Modernos

III - Padrões dos Meios Físicos das Redes Locais (LANs), Metropolitanas(MANs) e o padrão IEEE.

I - Introdução aos **Princípios de Comunicação**

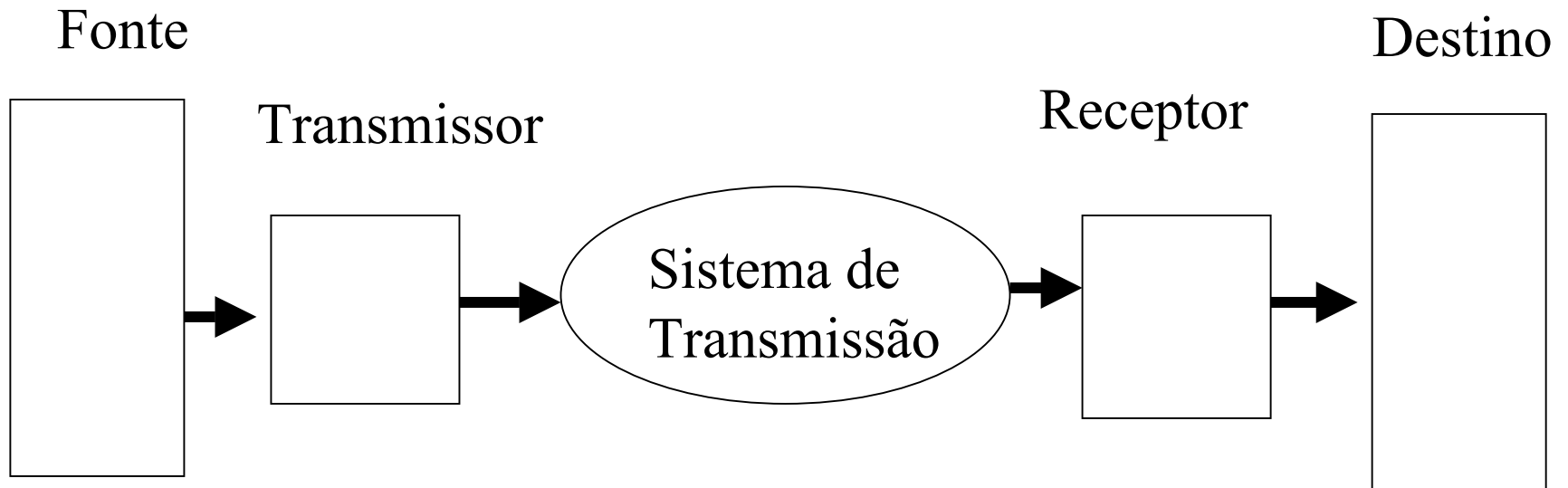
Objetivo :

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.

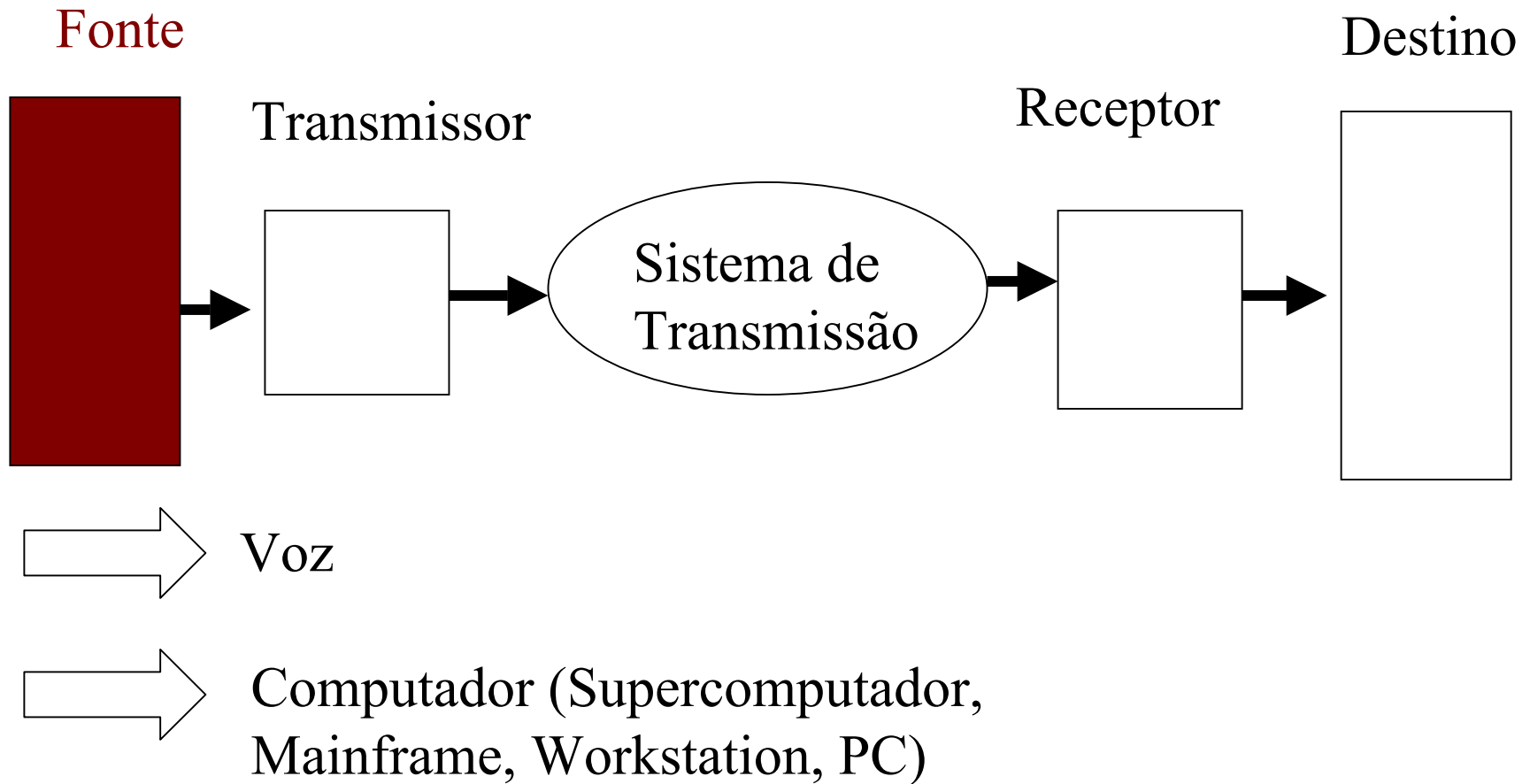
Conceitos de Comunicação

Modelo Genérico de Comunicação



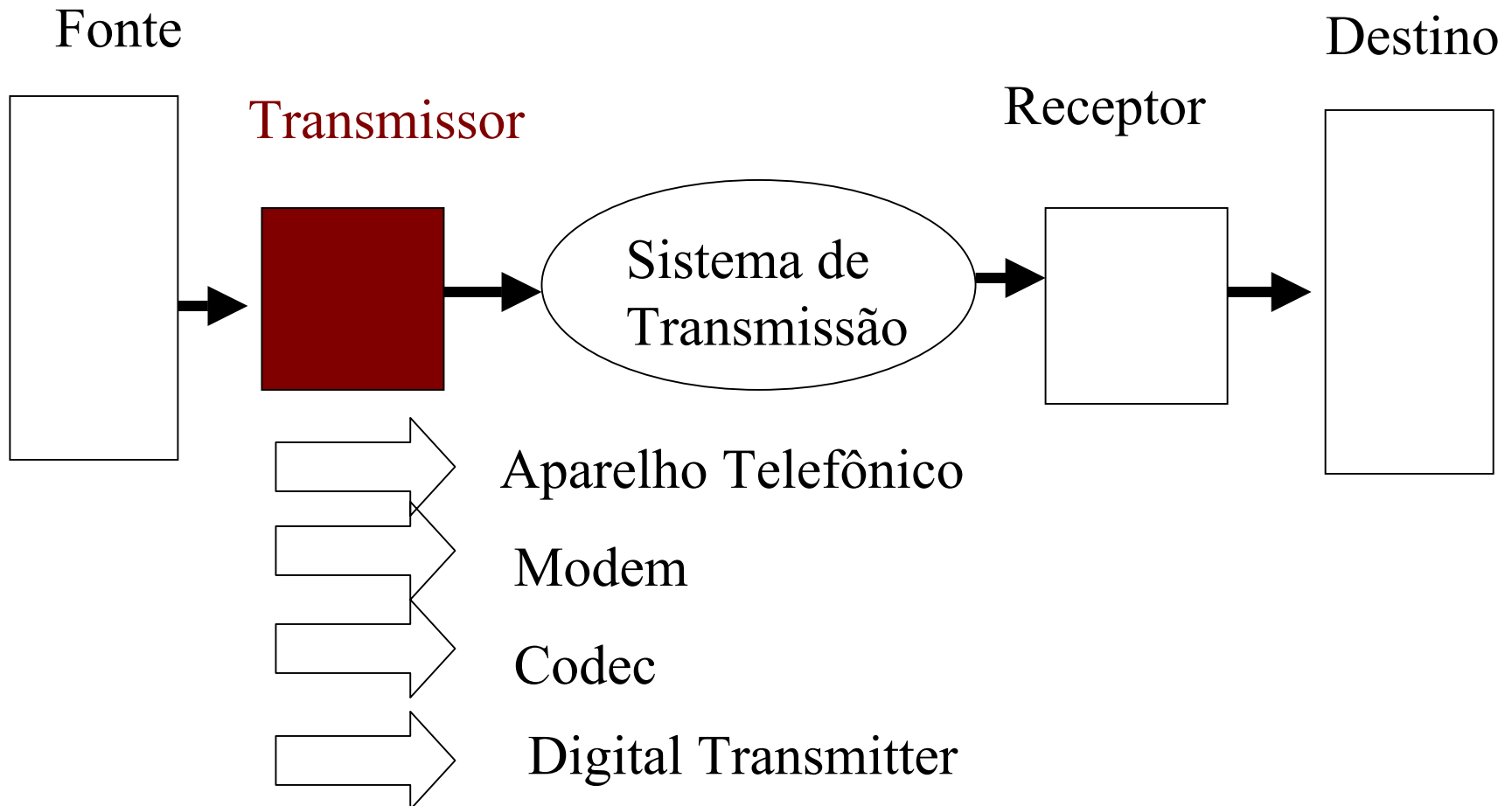
Conceitos de Comunicação

Modelo Genérico de Comunicação



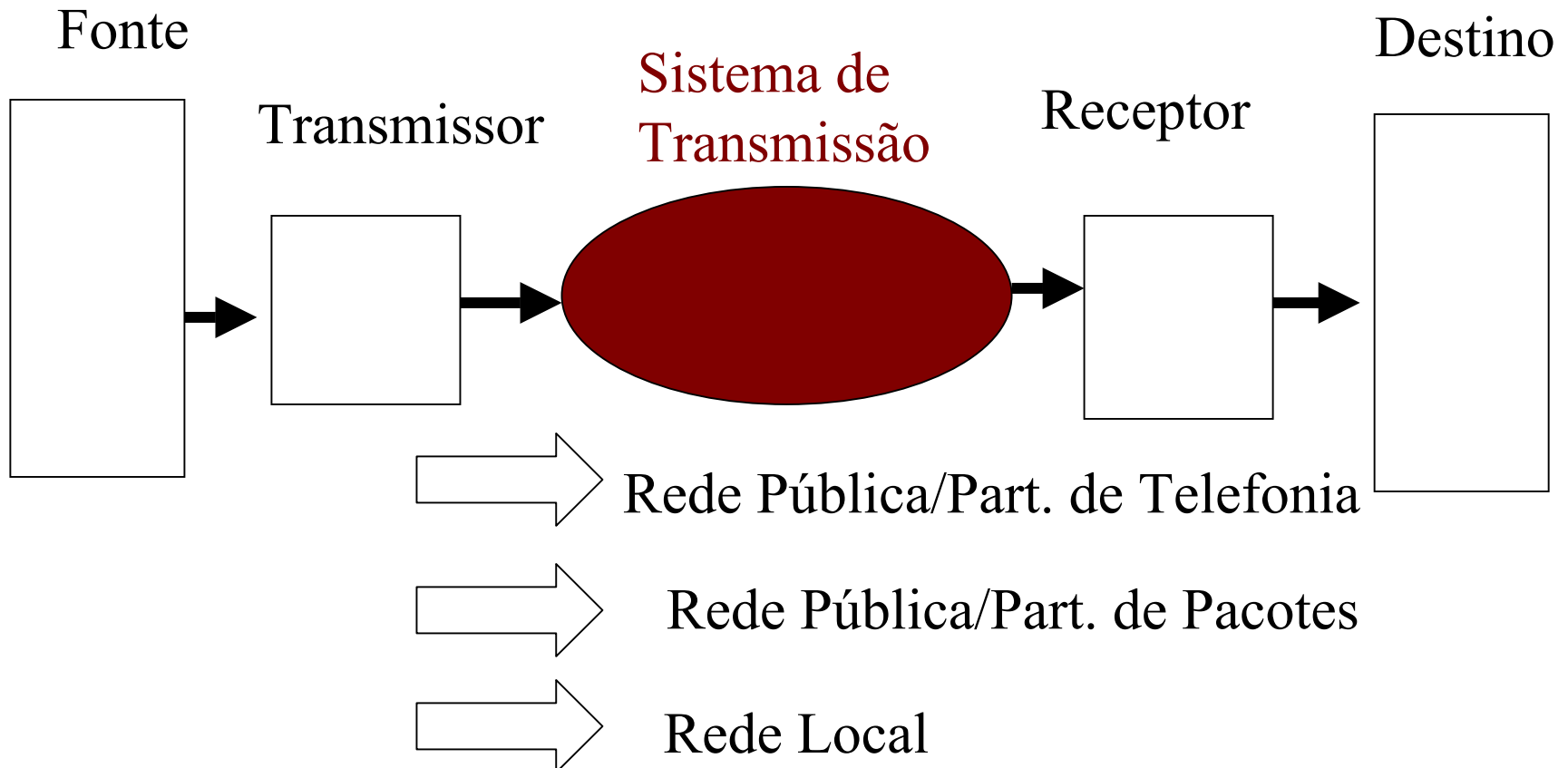
Conceitos de Comunicação

Modelo Genérico de Comunicação



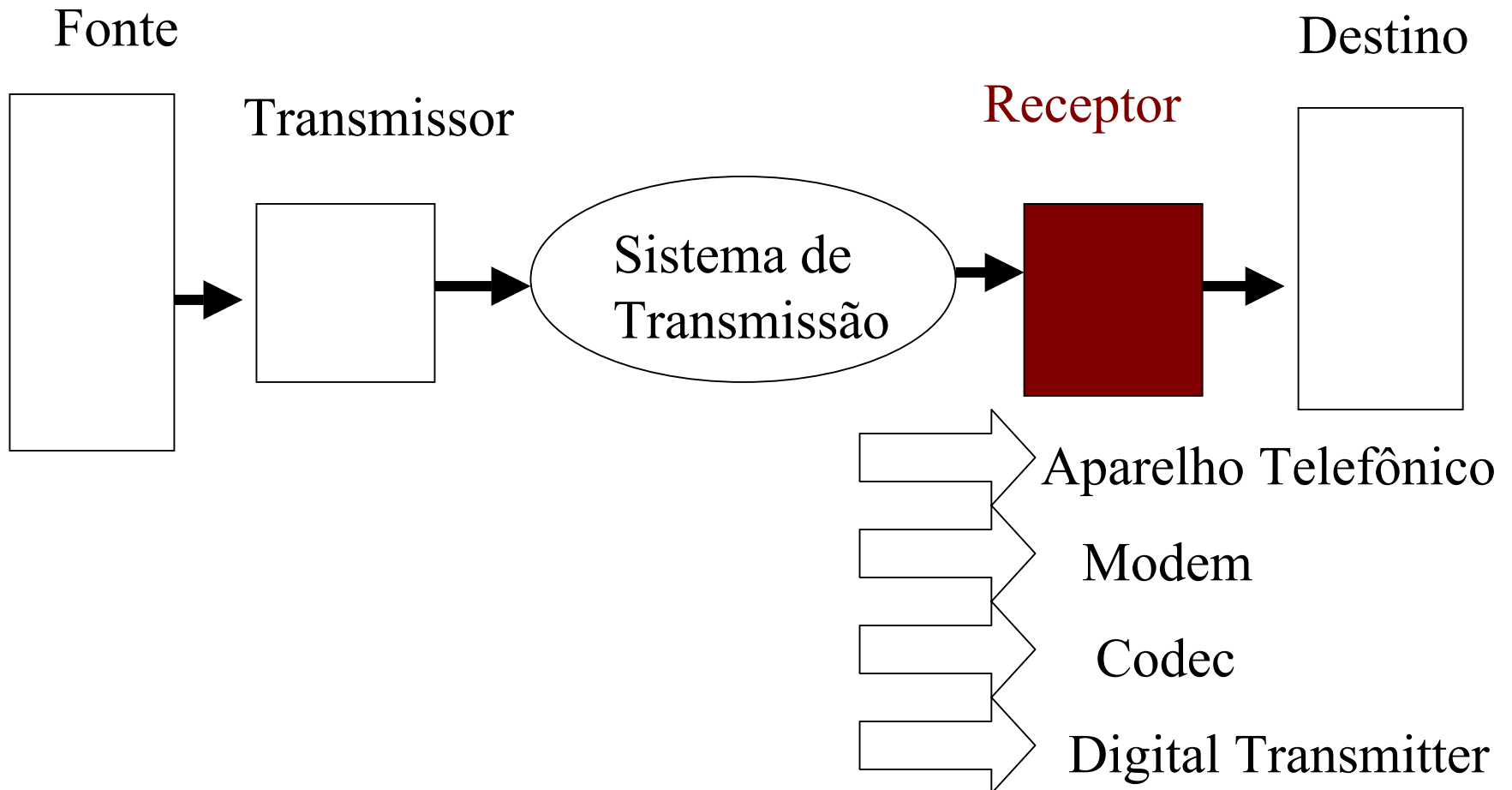
Conceitos de Comunicação

Modelo Genérico de Comunicação



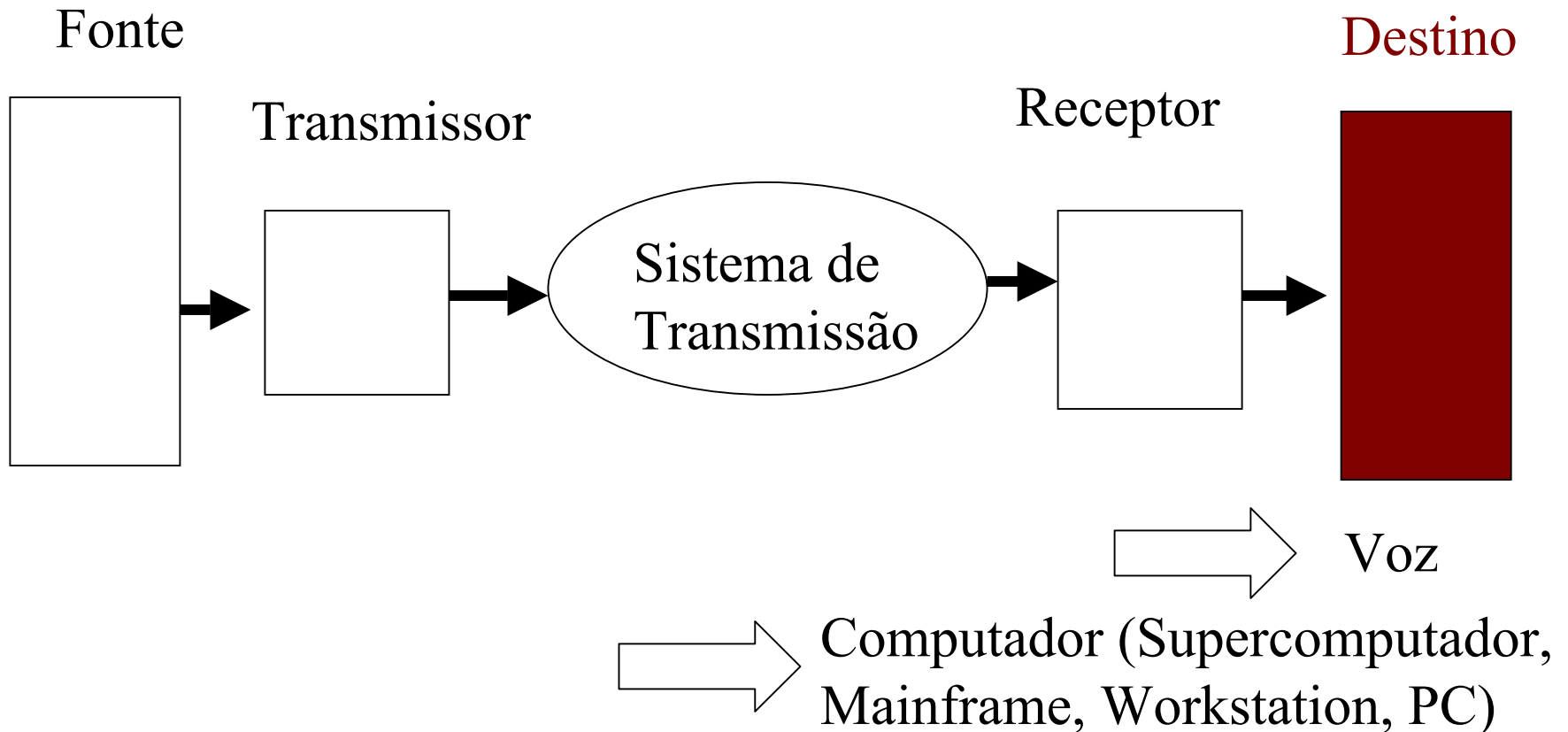
Conceitos de Comunicação

Modelo Genérico de Comunicação



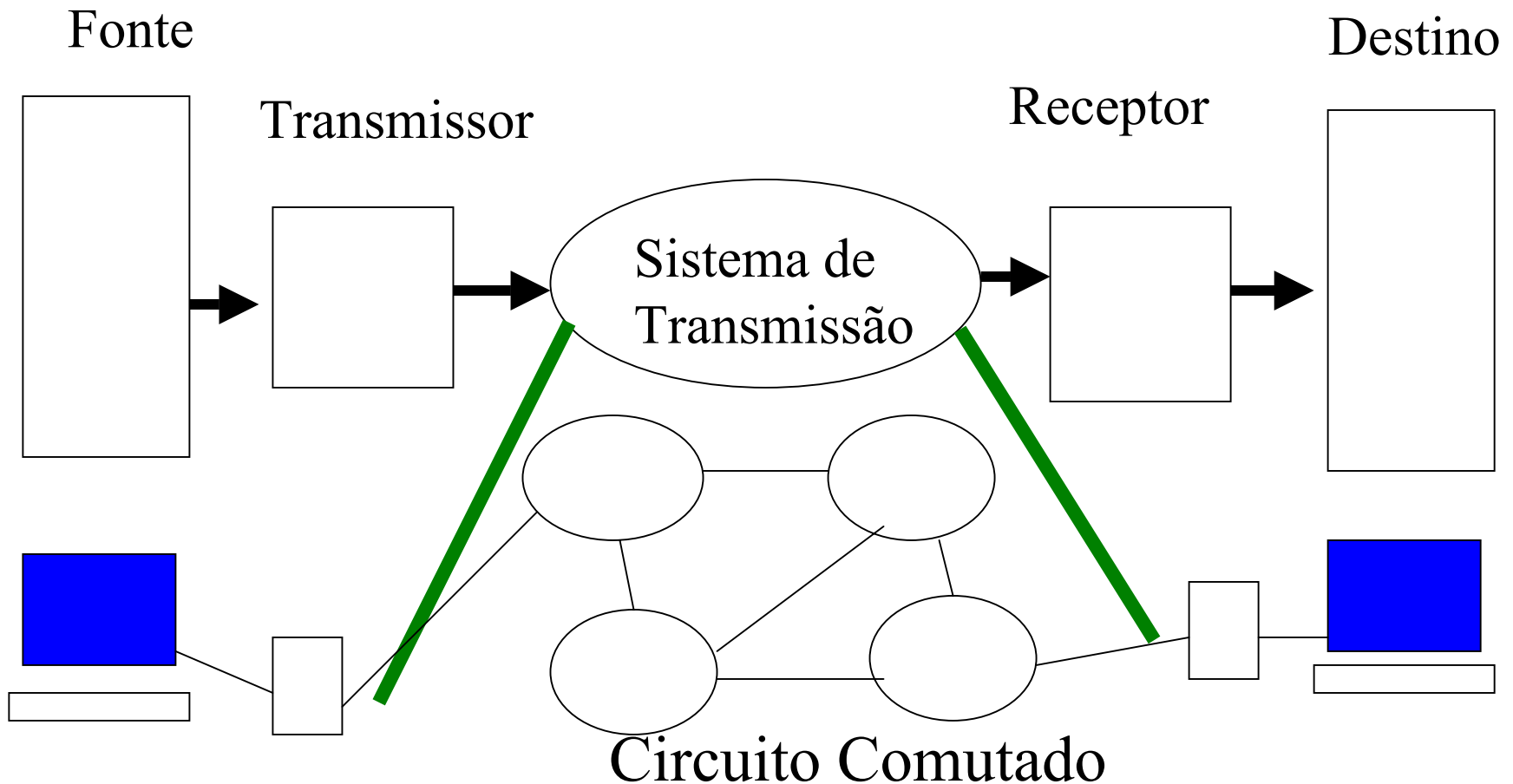
Conceitos de Comunicação

Modelo Genérico de Comunicação



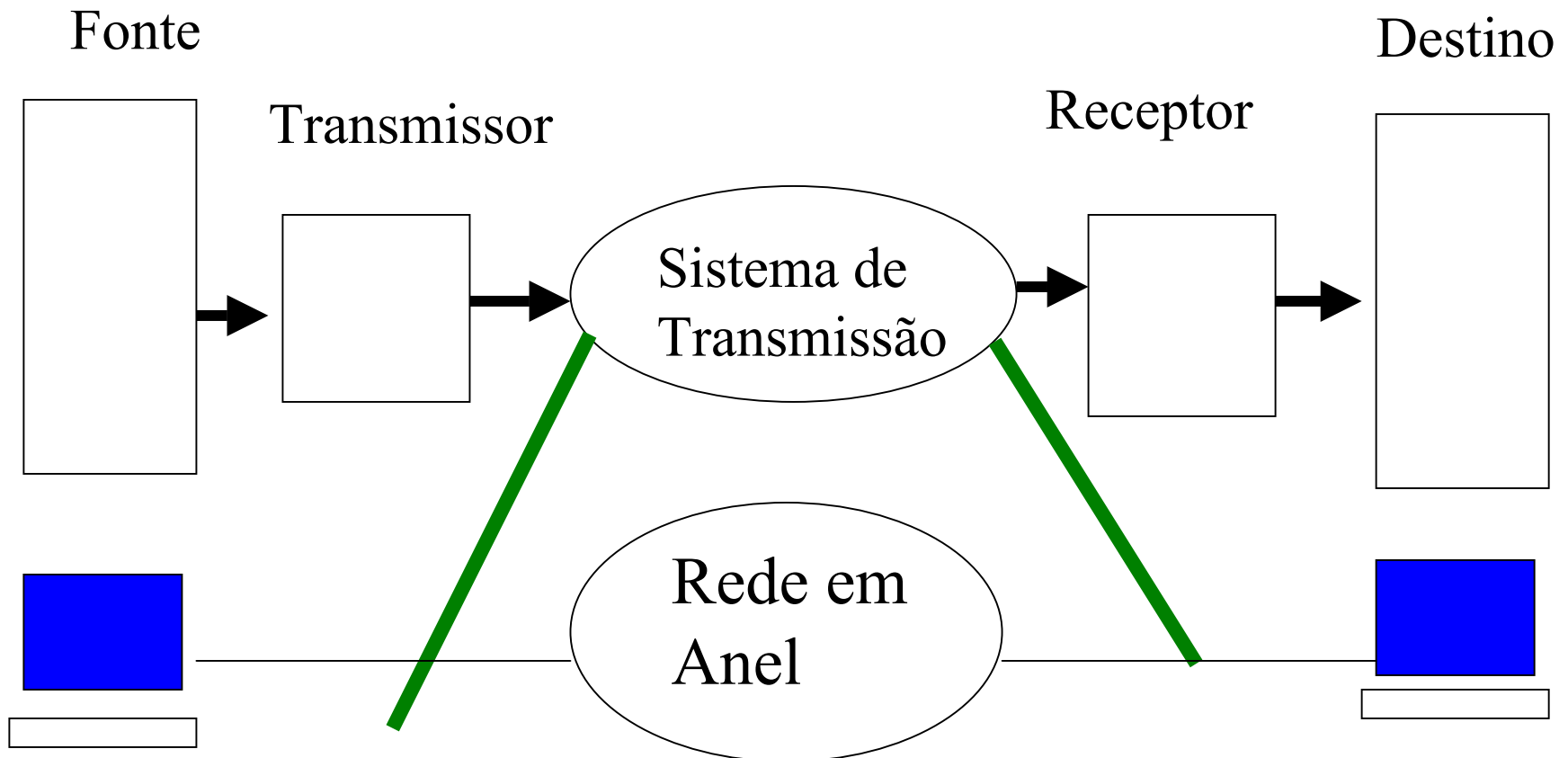
Conceitos de Comunicação

Modelo Genérico de Comunicação



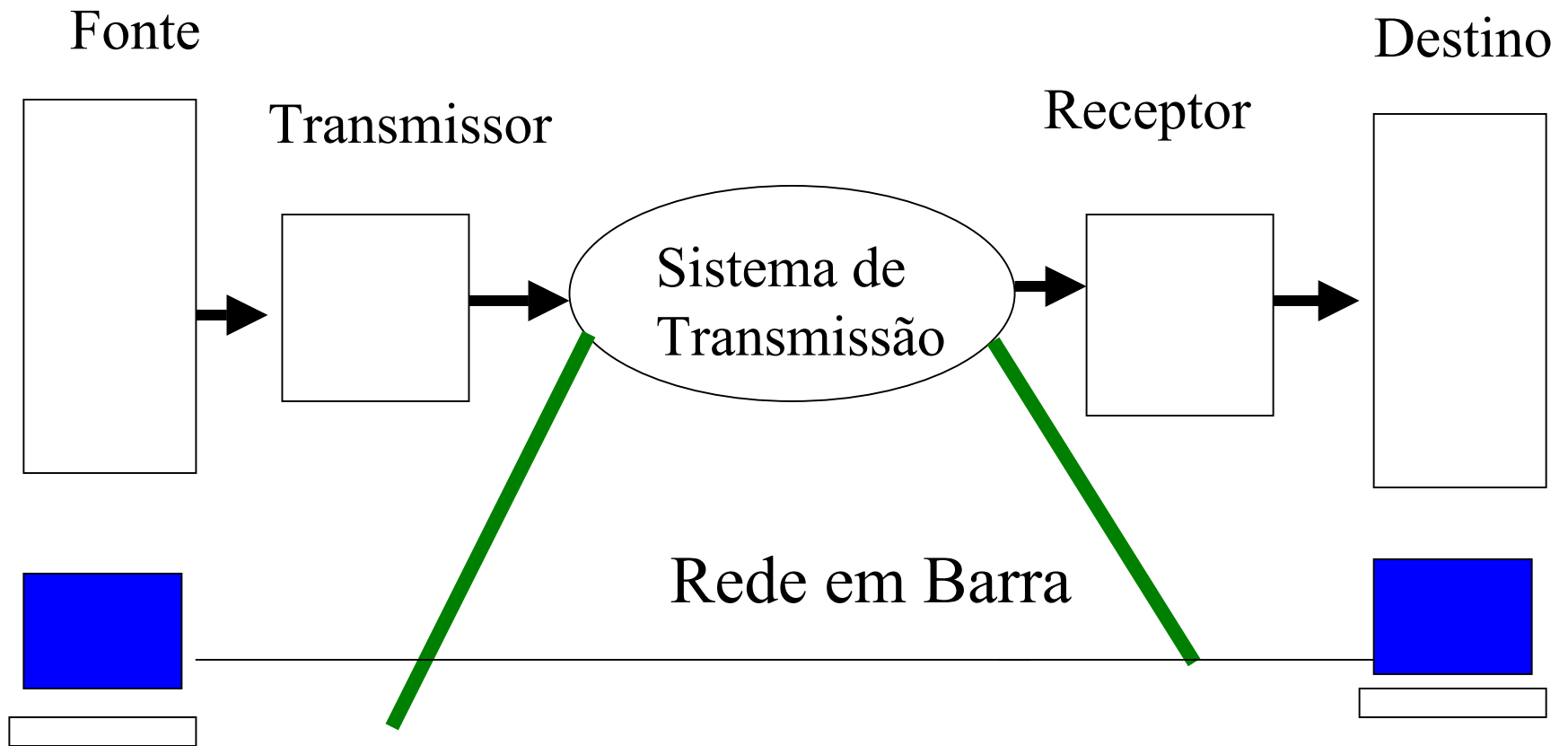
Conceitos de Comunicação

Modelo Genérico de Comunicação



Conceitos de Comunicação

Modelo Genérico de Comunicação



Conceitos de Comunicação

Modelo Genérico de Comunicação



I - Introdução aos **Princípios de Comunicação**

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 p/ destino.**

I - Introdução aos **Princípios de Comunicação**

- 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.

I - Introdução aos Princípios de Comunicação



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

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

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

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

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 sequencial. Ou seja, os pacotes são numerados e enviados na rede com o endereço do destinatário, podendo estes chegar fora de ordem.

Conceitos de Comunicação

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

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.

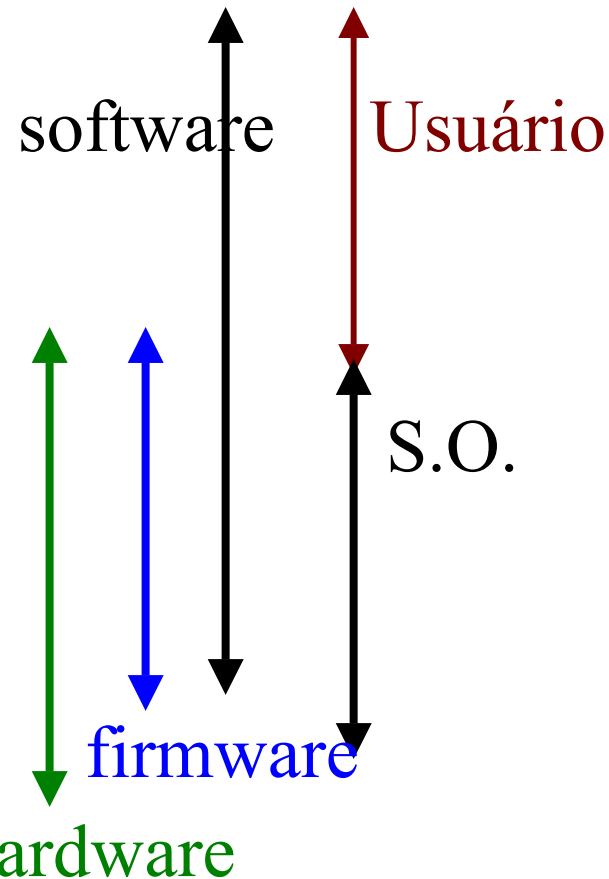
Conceitos de Comunicação

Conceitos Básicos

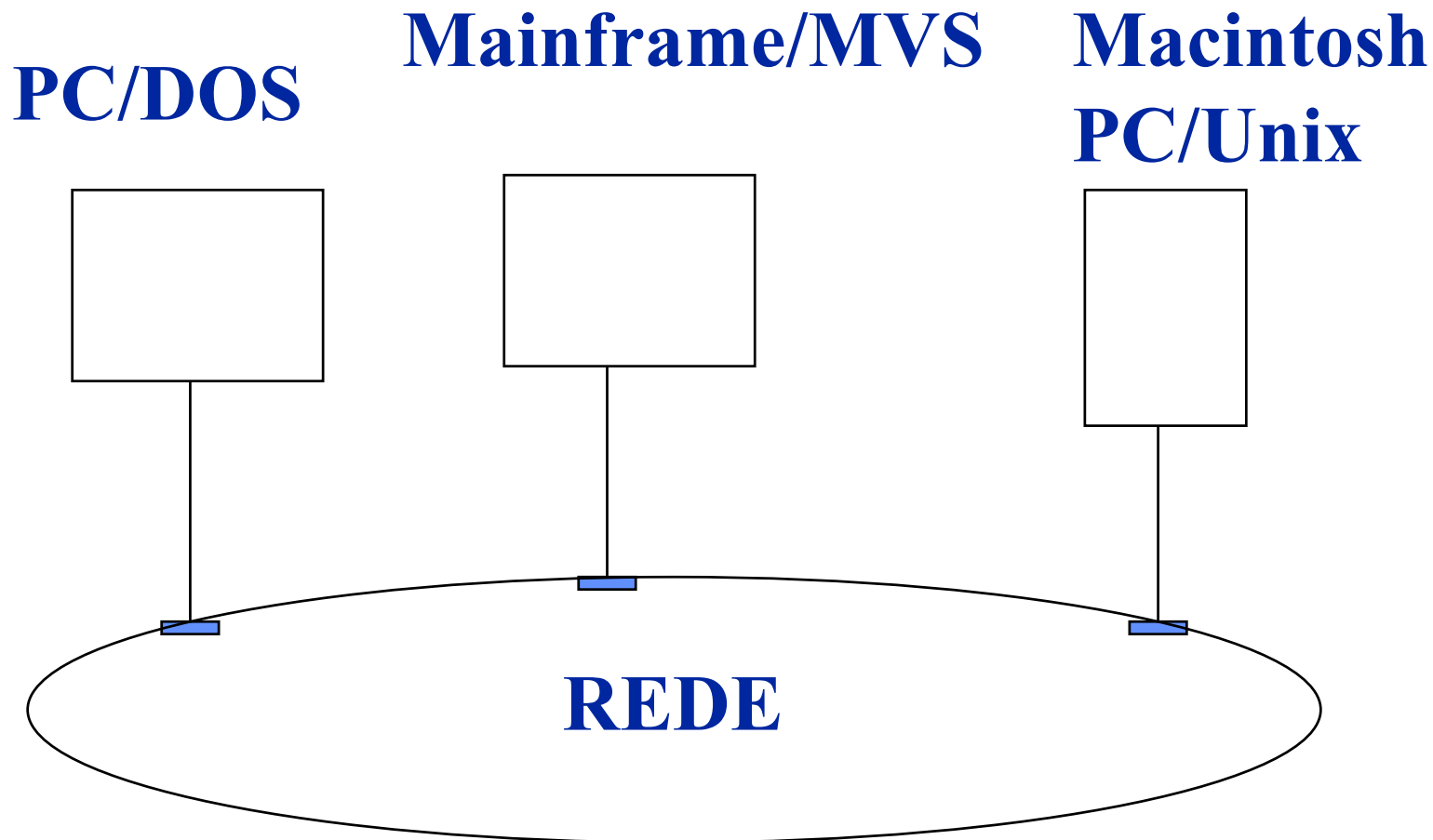
TCP/IP



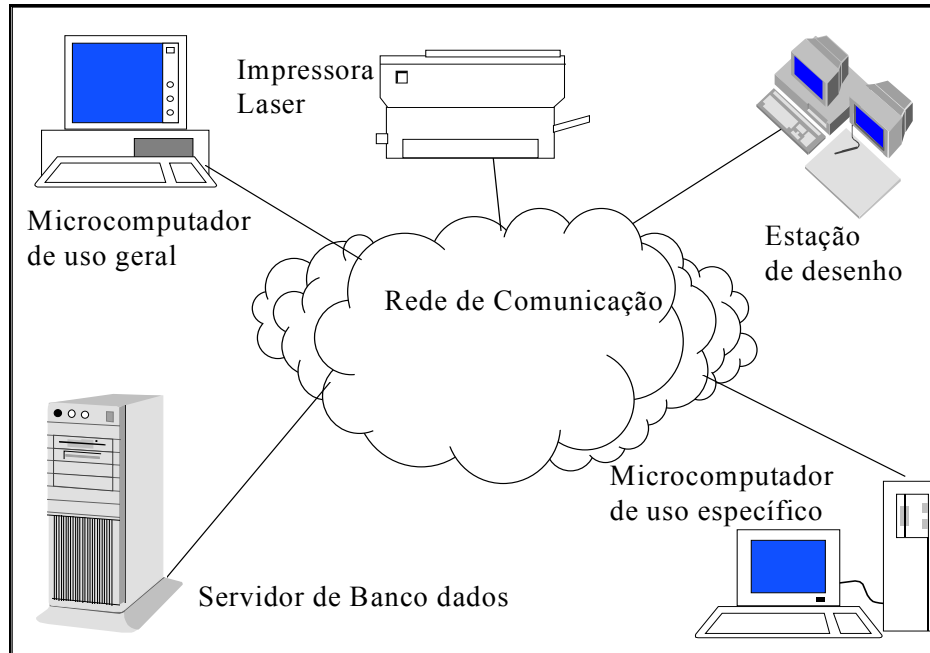
OSI



I - Introdução aos Princípios de Comunicação



I - Introdução aos Princípios de Comunicação



I - Introdução aos **Princípios de Comunicação**

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.

I - Introdução aos **Princípios de Comunicação**

Meio físico - num 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.

I - Introdução aos Princípios de Comunicação

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-guiados* são representados por transmissões que utilizam a atmosfera terrestre (microondas, rádio e infravermelho) e o espaço (satélites) para a transmissão da informação.

I - Introdução aos **Princípios de Comunicação**

*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 velocidade implementada pela rede no fluxo de dados (exemplo: 10, 16 ou 100Mbps).*

I - Introdução aos Princípios de Comunicação

O que são *protocolos de comunicação* ?

Conjunto de regras que permitem o estabelecimento 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.

I - Introdução aos **Princípios de Comunicação**

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.

I - Introdução aos **Princípios de Comunicação**

Exemplos de fatores a serem considerados são :

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

I - Introdução aos **Princípios de Comunicação**

Exemplos de fatores a serem considerados são :

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

I - Introdução aos **Princípios de Comunicação**

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.

I - Introdução aos **Princípios de Comunicação**

Latência : a latência, ou retardo, de envio de uma mensagem entre dois computadores qualquer, numa rede é computada da seguinte forma :

$$L_{\text{total}} = L_{\text{trans}} + L_{\text{acesso}}$$

Onde: total - latência de transferência.
trans - latência de transmissão.
acesso - latência de acesso

I - Introdução aos **Princípios de Comunicação**

Latência de Acesso - é o tempo decorrido para que uma mensagem tenha acesso a rede para transmitir.

Latência de Transmissão - é o tempo decorrido desde o início de transmissão de um computador até a outra ponta (outro computador).

I - Introdução aos **Princípios de Comunicação**

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

I - Introdução aos **Princípios de Comunicação**

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.

I - Introdução aos **Princípios de Comunicação**

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).

I - Introdução aos **Princípios de Comunicação**

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.

I - Introdução aos Princípios de Comunicação

Transmissão de Sinais : A comunicação de dados através de um meio físico (cabos/ar) deve ser efetuada de maneira que os dados transmitidos por uma fonte remetente qualquer, sejam entendidos pelo seu destinatário. Esta operação é denominada de *codificação* (ou *modulação*), podendo ser implementada nas formas *digital ou analógica*.

I - Introdução aos **Princípios de Comunicação**

A forma analógica é caracterizada por uma constante troca de estado (Exemplo : relógio analógico).

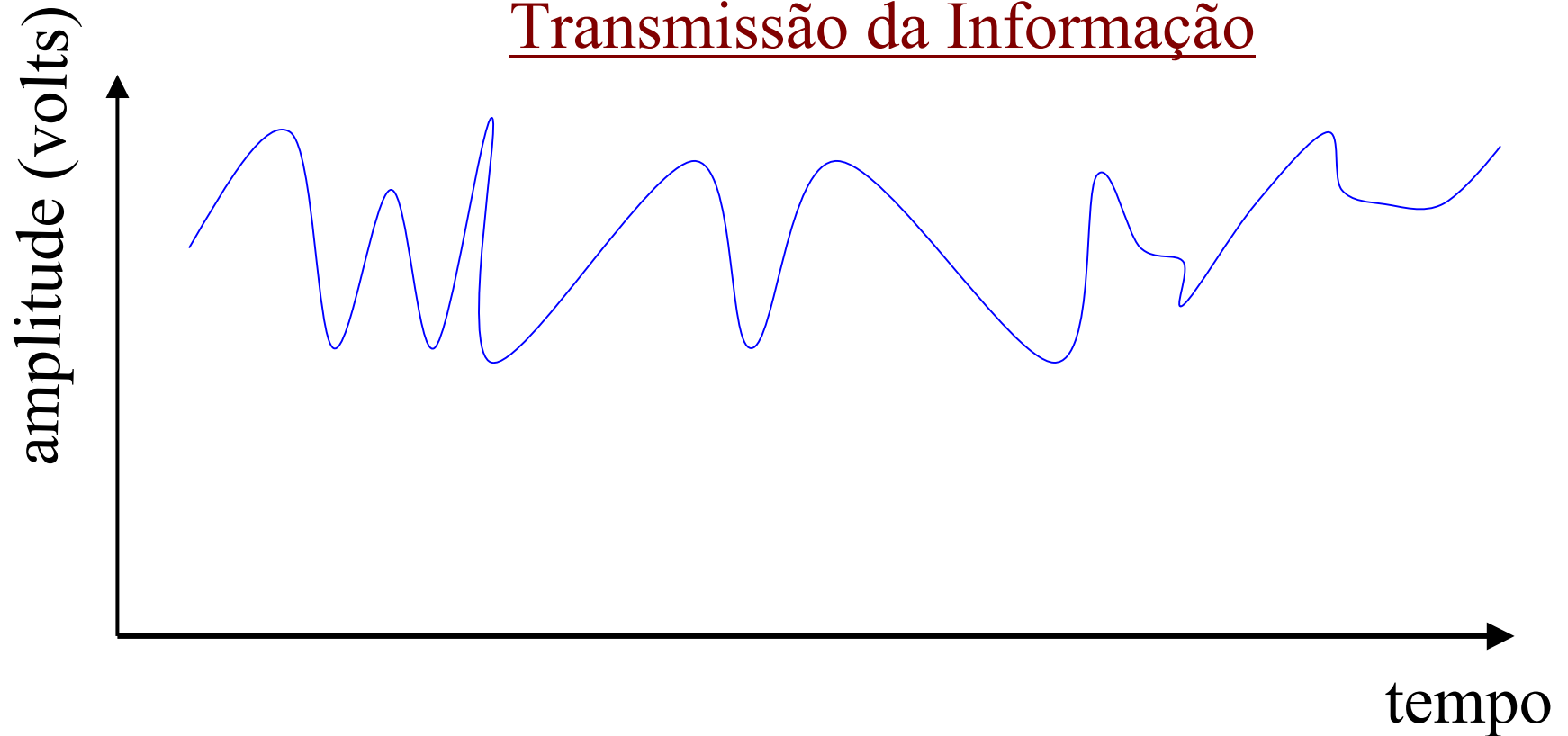
A forma digital consiste de sinais discretos (ou precisos): ligado/desligado, aberto/fechado, 0/1. Não podemos ter estados intermediários, ou seja meio aberto/fechado, meio ligado/desligado, ou entre 0/1.

I - Introdução aos Princípios de Comunicação

Denomina-se banda passante de um sinal o intervalo de frequências que compõem este sinal. A largura de banda deste sinal é o tamanho de sua banda passante, i.e. a diferença entre a maior e a menor frequência que compõe o sinal.

Conceitos de Comunicação

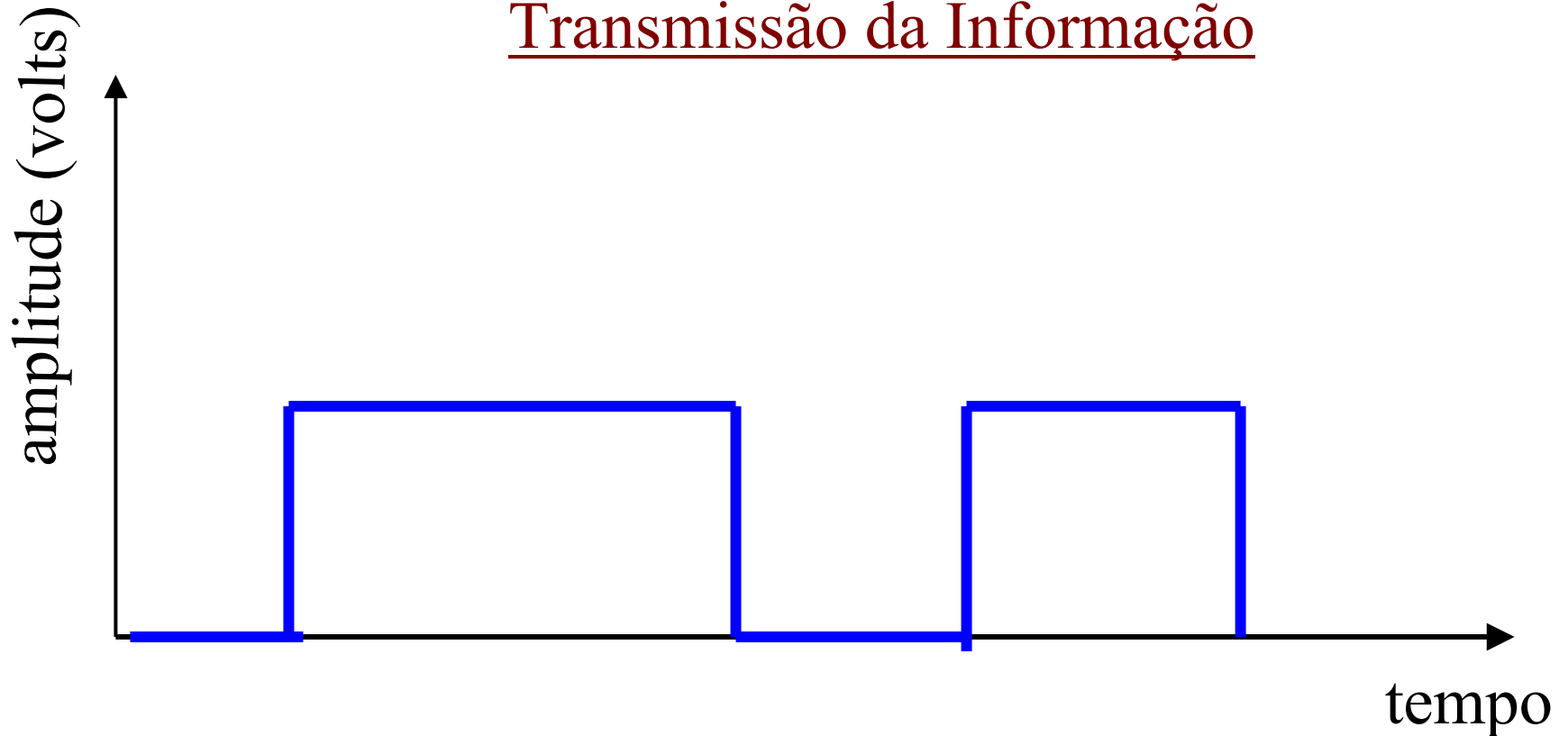
Transmissão da Informação



Sinal Contínuo

Conceitos de Comunicação

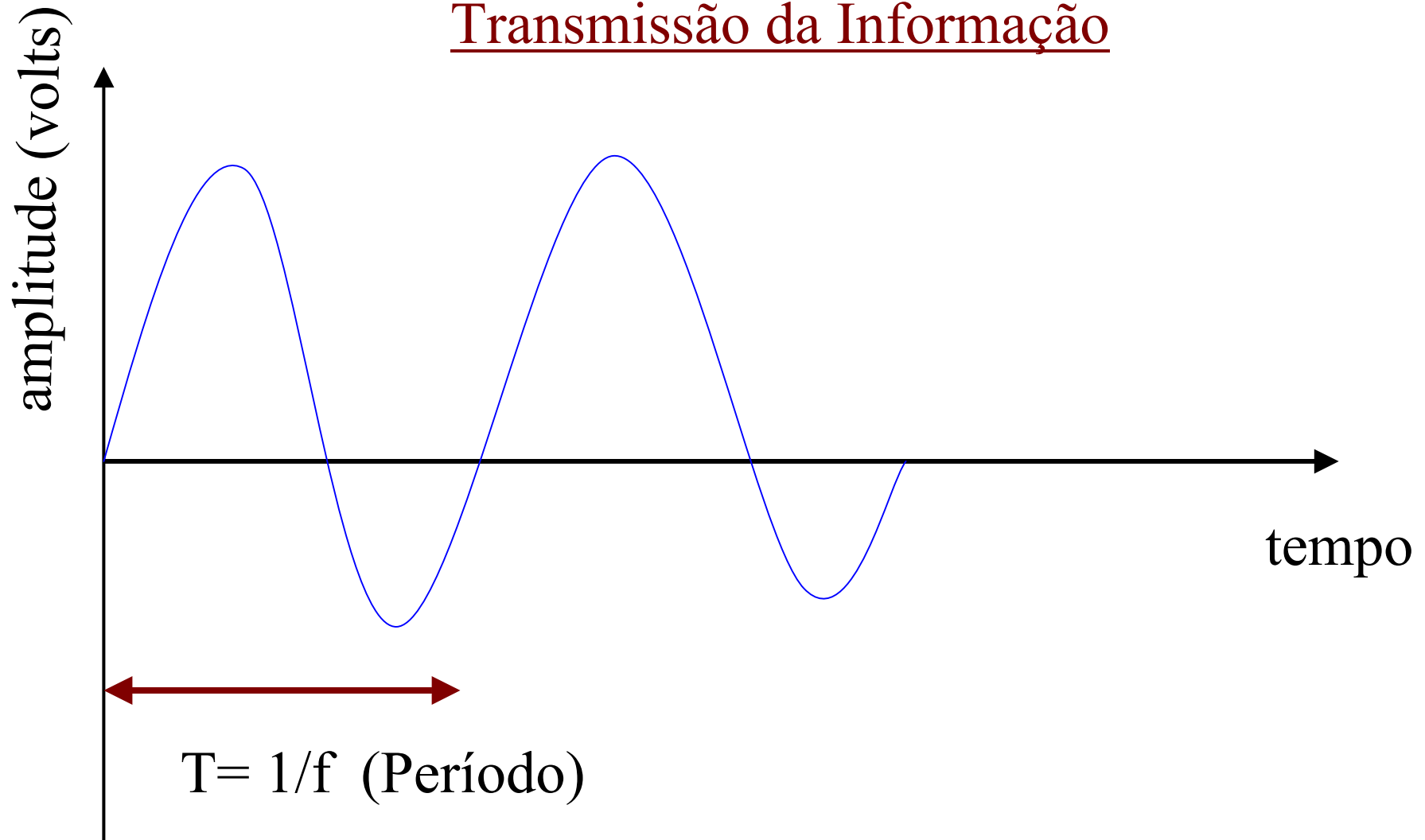
Transmissão da Informação



Sinal Discreto

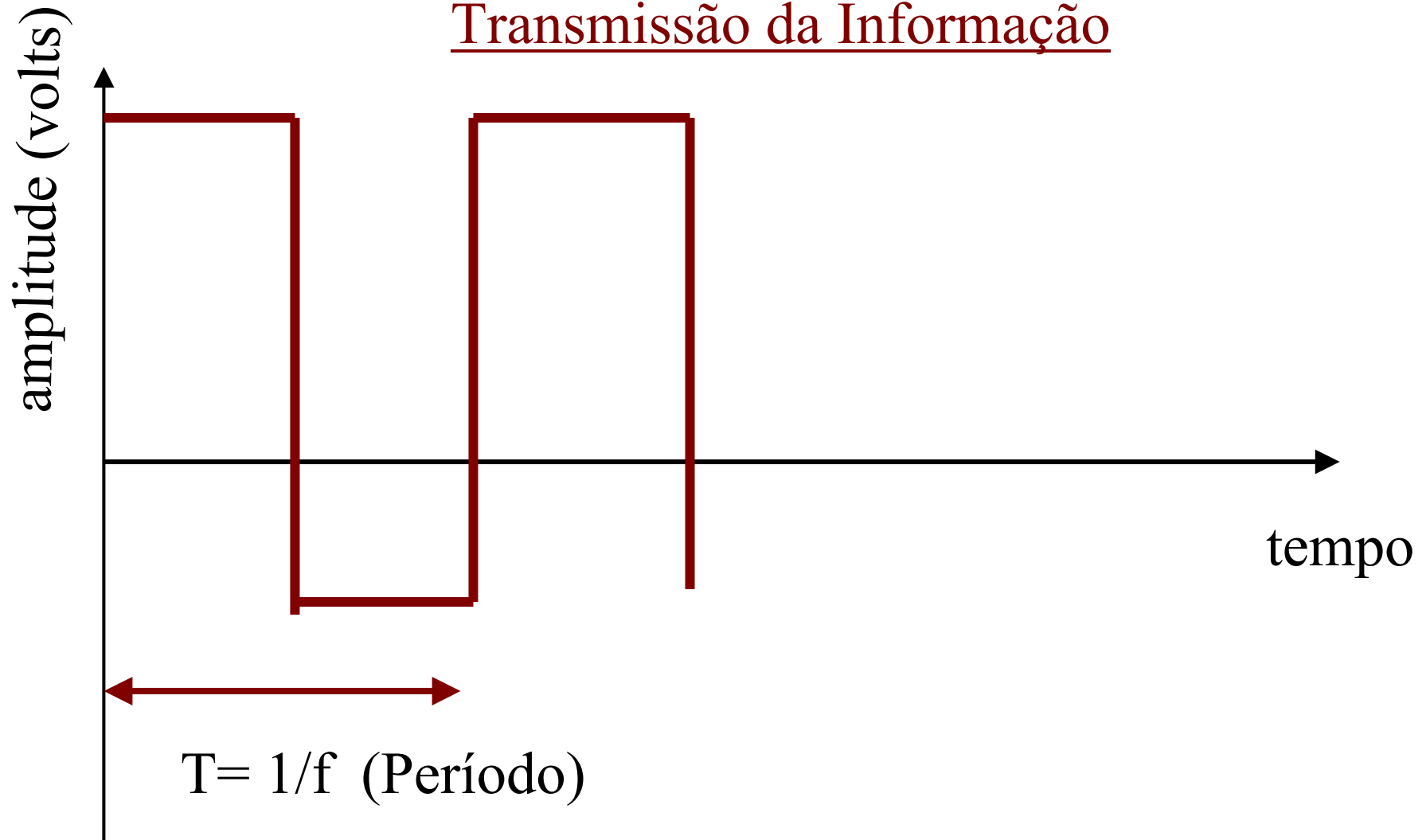
Conceitos de Comunicação

Transmissão da Informação



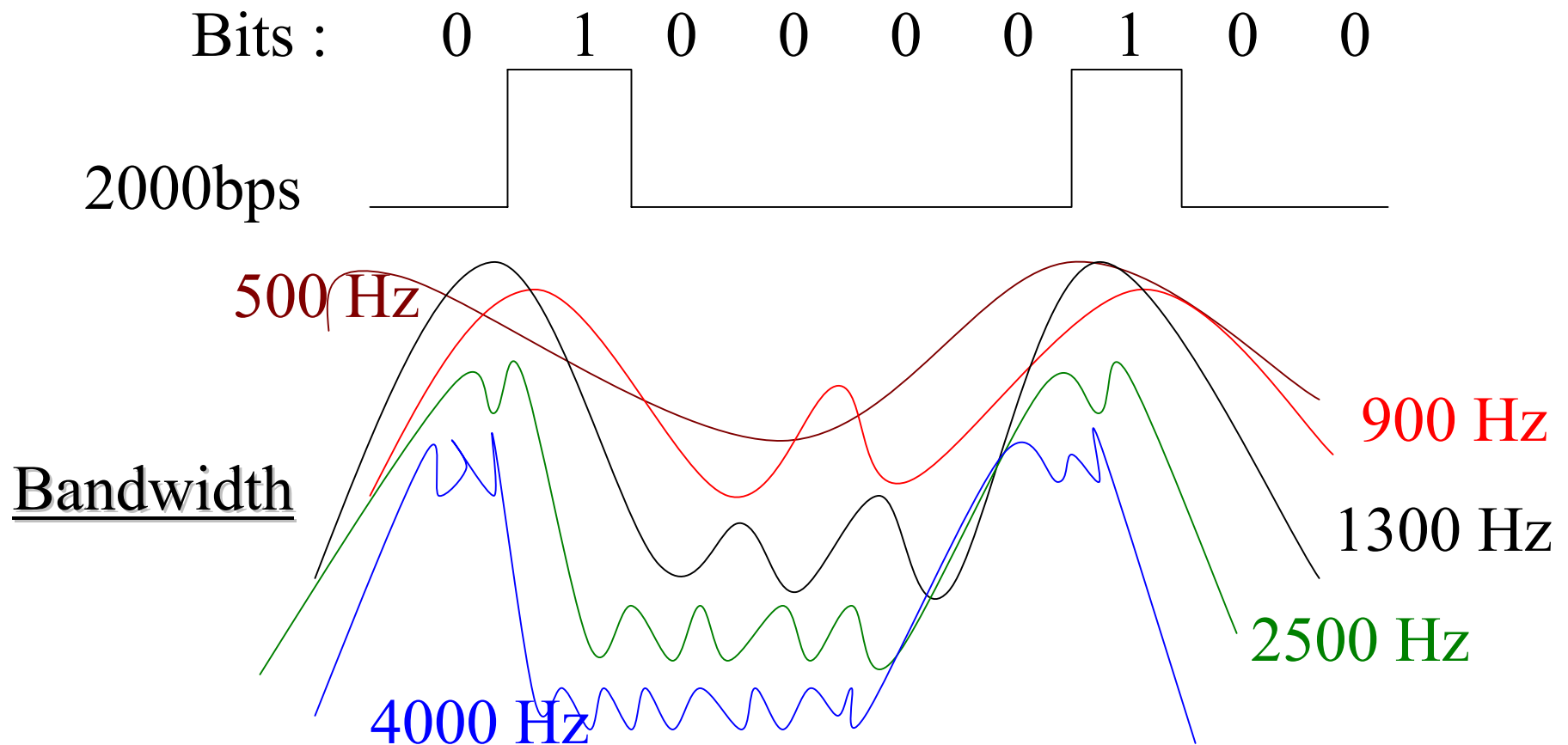
Conceitos de Comunicação

Transmissão da Informação

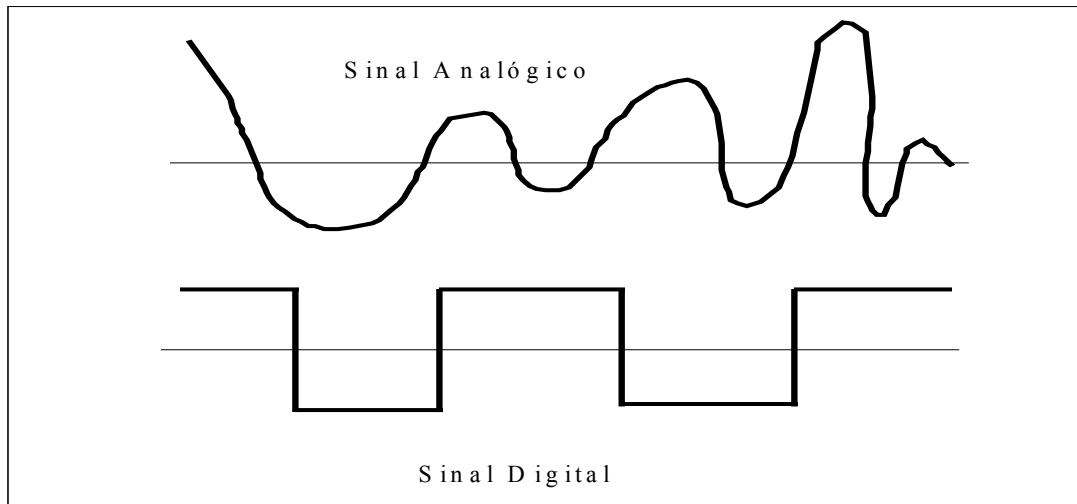


Conceitos de Comunicação

Transmissão da Informação



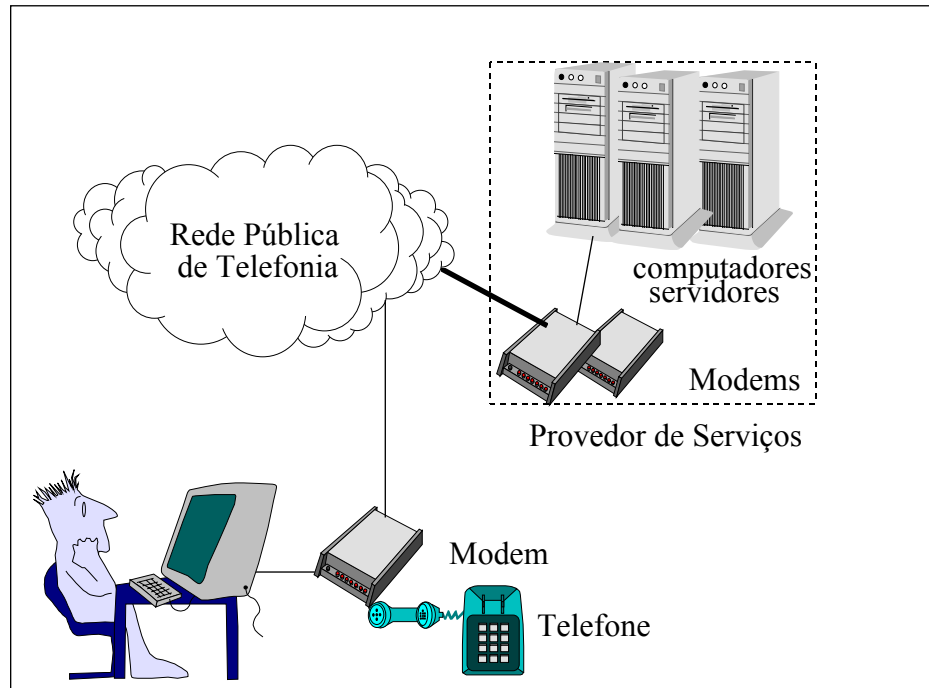
I - Introdução aos Princípios de Comunicação



I - Introdução aos Princípios de Comunicação

O próximo exemplo ilustra o caso clássico de acesso a um provedor de *Internet*. Neste o usuário faz acesso a rede telefônica que o *liga* aos computadores do provedor. *MOD*uladores e *DEM*odulares (*MODEMS*) fazem a comunicação possível através da modulação/demodulação do sinal (ou dados).

I - Introdução aos Princípios de Comunicação



I - Introdução aos Princípios de Comunicação

Transmissão em Banda Base e 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). 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 larga*.

I - Introdução aos **Princípios de Comunicação**



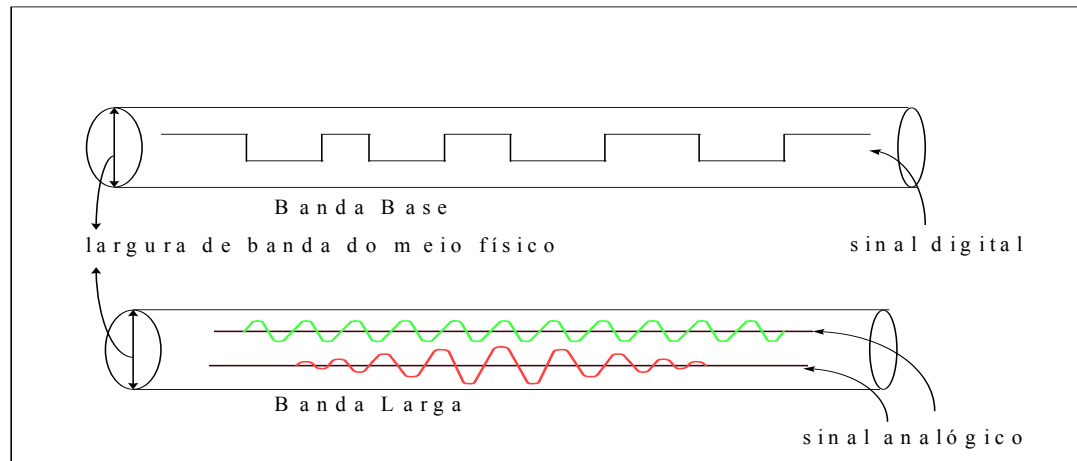
Banda base : neste tipo de transmissão toda a largura de banda é usada por um único canal. Esta tecnologia é frequentemente usada para transmissão digital (embora pode ser empregada em transmissão analógica). Por esta razão, a maioria das redes de computadores adotam esta técnica.

I - Introdução aos **Princípios de Comunicação**

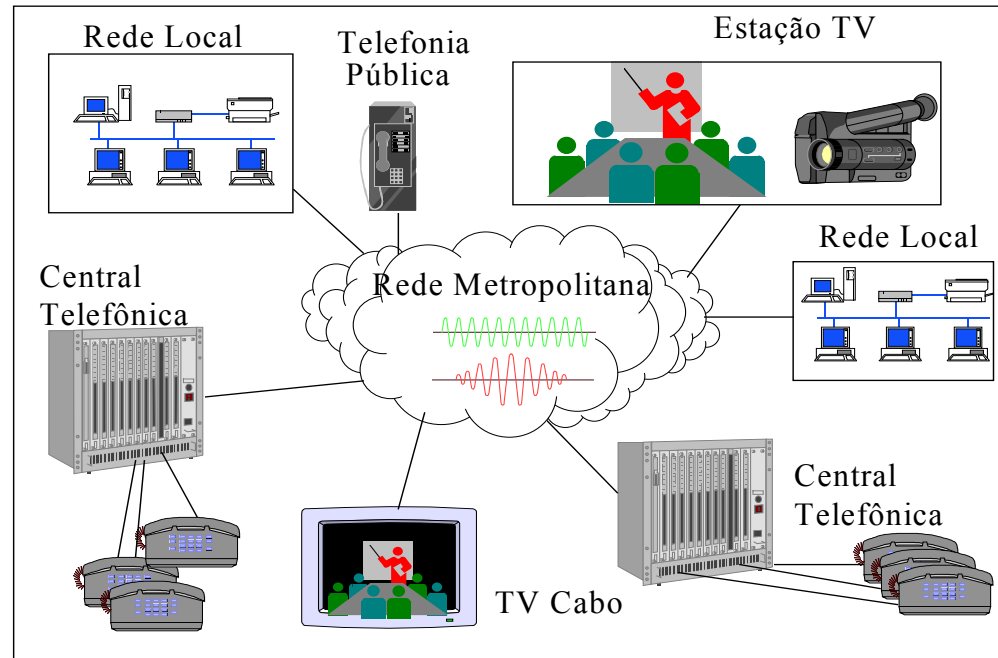


Banda larga : Este modelo de transmissão é caracterizado pela divisão da largura de banda em múltiplos canais. Podendo cada canal transmitir diferentes sinais analógicos. Por esta razão, redes de banda larga podem transmitir múltiplos sinais simultaneamente.

I - Introdução aos Princípios de Comunicação



I - Introdução aos Princípios de Comunicação

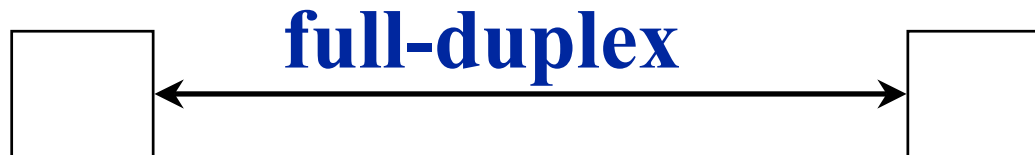


I - Introdução aos **Princípios de Comunicação**

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.

I - Introdução aos Princípios de Comunicação



I - Introdução aos **Princípios de Comunicação**

A necessidade de transmissão dos sinais binários através dos meios físicos das redes, nos obriga a compreender como a transmissão de 0's e 1's ocorre.

Podemos estabelecer, por exemplo, que o bit 1 no transmissor será representado por um determinado nível de voltagem positivo (+V). Por outro lado, o bit 0 pode ser representado por um nível negativo (-V). No receptor, é importante que estes sinais sejam interpretados com +V para 1 e -V para 0.

I - Introdução aos Princípios de Comunicação

Na prática podemos ter os sinais *atenuados (ou reduzidos)* e/ou *distorcidos* no meio de transmissão. Desta forma, o receptor não estará apto a interpretar os sinais de 0's e 1's. Os fenômenos de *atenuação e distorção* são muito influenciados pelos seguintes fatores :

- O tipo de meio de transmissão.
- A velocidade de transmissão dos bits.
- A distância entre dois elementos de comunicação.

I - Introdução aos **Princípios de Comunicação**

Alguns acrônimos importantes que precisamos conhecer são :

- **ITU- T : International Telecommunications Union - Telecommunication Sector.**
- **EIA : Electrical Industries Association.**
- **DCE: Data Communication Equipment**
- **DTE: Data Terminal Equipment**
- **PTT: Post, Telephone and Telecommunications**
- **PSTN: Public Switched Telephone Network**

I - Introdução aos **Princípios de Comunicação**



É importante sabermos algumas características dos meios físicos de transmissão, uma vez que desejamos saber o número máximo de bits que desejamos transmitir por segundo (bps).

I - Introdução aos **Princípios de Comunicação**

Cabo Paralelo

- Mais simples meio de transmissão.
- Equipamentos distantes até 50 metros.
- Velocidade de transmissão menor que 19.2 kbps.
- O sinal (voltagem ou corrente) é aplicado para um fio e ao outro o sinal de terra é aplicado.
- Utilização comum na ligação de DTE/DCE.

I - Introdução aos **Princípios de Comunicação**

PAR TRANÇADO

- Melhor imunidade a ruídos.
- Distância recomendável de até 100 metros.
- Bit rate na casa de centenas de Mbps.
- Qualquer sinal de interferência é *notado* pelo par trançado, reduzindo o efeito no sinal final .
- Cabos ditos UTPs (Unshielded Twisted Pairs) são empregados com frequência em redes telefônicas em aplicações de comunicação de dados.
- STPs (Shielded Twisted Pairs) são empregados onde se deseja reduzir ainda mais os efeitos de sinais de interferência.

I - Introdução aos **Princípios de Comunicação**

Cabo Coaxial

Devido aos fenômenos conhecidos como :

(1) *skin effect*

(2) *radiation effect*

Os cabos coaxiais podem ser usados para minimizar estes dois efeitos.

Skin Effect : a medida que o percentual de bits dos sinais transmitidos aumenta (e por conseguinte a frequência) a corrente fluindo nos fios tendem a fluir apenas nas superfícies dos cabos.

I - Introdução aos **Princípios de Comunicação**

Cabo Coaxial

Assim, teremos uma resistência elétrica dos cabos para sinais de altas frequências, levando para alta atenuação. Em adição, para altas frequências, teremos mais sinais perdidos como resultado dos sinais eletromagnéticos.

- Equipamentos distantes até centenas de metros.
- bit rate na ordem de Mbps.

I - Introdução aos **Princípios de Comunicação**

Fibra Ótica

- Transmissão de sinal de luz numa fibra de vidro.
- Ondas de luz possuem maior largura de banda do que ondas elétricas, permitindo que os cabos óticos transmitam a centenas de Mbps.
- Ondas de luz são imunes a interferências eletromagnéticas e linhas cruzadas.
- Cabos de fibra ótica são eficientes em ambientes que necessitam a transmissão de uma baixa relação de bps em locais onde é alto o ruído devido a eletricidade (exemplo : fábricas)

I - Introdução aos Princípios de Comunicação

Satélite

- Transmissão sem fio.
- Possui vários transponders cada qual cobrindo uma faixa específica de frequência.
- Possui grande largura de banda (500 MHz)
- Os satélites de comunicação são geoestacionários.
- A cobertura de uma área pode ser grande ou localizada. Nesta ultima, os receptores de diâmetros pequenos, chamados de antenas ou pratos (VSATs - Very Small Aperture Terminals) são empregados.

I - Introdução aos **Princípios de Comunicação**

Microondas

- Empregado na impossibilidade de passagem física, ou inviabilidade econômica, de cabos por locais tais como desertos, rios, pântanos, etc.
- Sinal susceptível a distúrbios por impedimentos físicos (por exemplo : um prédio, uma montanha ou condições climáticas).
- Com uma *visada* os sinais podem atingir a 50 Km.

I - Introdução aos Princípios de Comunicação

Atenuação

A medida que o sinal se propagada ao longo de um meio físico sua amplitude diminui. Este fenômeno é chamado de *atenuação de sinal*. Os cabos de transmissão de dados são projetados para permitir que os sinais atenuados sejam detectados e interpretados pelos *circuitos* do receptor. Por outro lado, cabos muito longos recebem amplificadores de sinal visando estabelecer o nível de sinal original. A atenuação de sinal aumenta em função da frequência. Como um sinal compreende uma faixa de frequências, o sinal é distorcido.

I - Introdução aos Princípios de Comunicação

Atenuação

Para resolver o problema, *equalizadores* são empregados para equalizar a atenuação através de uma banda definida de frequências.

A atenuação e ganho são medidas em *decibels (dB)*, o que significa dizer que temos uma medida sem dimensão, ou seja uma medida relativa de magnitude entre os níveis de entrada e saída numa linha de transmissão.

I - Introdução aos **Princípios de Comunicação**

Nota :

Em telecomunicação utilizamos muito escalas em logaritmo para medir relações entre potências de sinais em virtude das grande variações existentes entre os mesmos. Como exemplo, podemos ter um caso de uma variação de 1 para 10.000 o que significa, em logaritmo decimal, a 0 para 4.

I - Introdução aos Princípios de Comunicação

Ruído

Em condições normais, na ausência de sinal numa linha de transmissão de dados (ou canal) não temos idealmente nenhum sinal elétrico. Todavia, existem perturbações aleatórias no meio mesmo na ausência de sinal. Estas perturbações são conhecidas como nível de ruído da linha. A relação sinal-ruído (SR) é normalmente expressa em dB :

$$SR = 10 \text{ LOG } (S/R)$$

I - Introdução aos **Princípios de Comunicação**

Nos anos 60, o Laboratório Bell notou que a falta de um padrão de interface para conexão entre equipamentos de dados e comunicação era um grande problema na indústria de informática. Desta forma, foi proposto um padrão conhecido como RS232 que mais tarde foi melhorado (RS232-C) tornando-se um padrão *de facto*.

I - Introdução aos **Princípios de Comunicação**

Devemos ter uma padronização visando não só a conectividade entre os equipamentos de uma rede, visando a interoperabilidade. Assim, o ITU-T (antigo CCITT) seguindo a experiência do Laboratório da Bell formalizou as recomendações V24 e V28.

I - Introdução aos **Princípios de Comunicação**

Recomendação V.28 -

- **características elétricas dos modems**
- **níveis de tensão para transmissão de dados**
- **estado lógico 1: - limite entre -15 e -25 V**
lógico 0: -limite entre +15 e +25V
- **espera-se um atenuação de 12V ao longo do cabo de transmissão digital.**

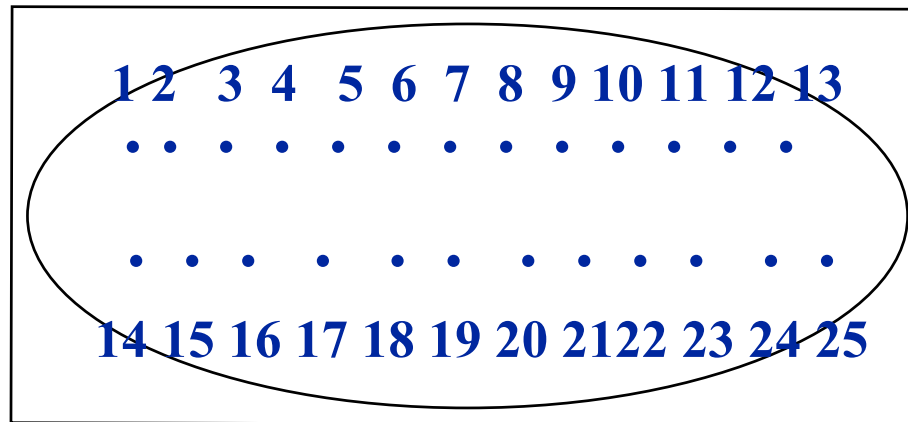
I - Introdução aos **Princípios de Comunicação**

Recomendação V.24 -

- **características funcionais da interface**
- **função de cada pino e direção do sinal (origem/destino)**
- **especificação de mais de 40 circuitos.**

I - Introdução aos **Princípios de Comunicação**

Interface RS232



<u>Pino - RS232 - V.24 - Função</u>			
2	- BA	- 103	- Dados a Transmitir (TX)
3	- BB	- 104	- Dados Recebidos (RX)
6	- CC	- 107	- Modem Pronto (DSR)
20	- CD	- 108	- DTE Pronto (DTR)

I - Introdução aos Princípios de Comunicação

Computador

Modem



I - Introdução aos Princípios de Comunicação

Códigos :

Na transmissão de 0's e 1's, é necessário que tenhamos uma padronização, ou *código*, para que a comunicação entre um ETD e o ECD seja efetuada com sucesso. Existem inúmeros códigos (exemplos são o BCD, Gray, 2 out-of 5, ASCII e EBCDIC dentre outros), estes são implementados com uma certa quantidade de bits. Como o bit pode assumir somente 0 ou 1, temos que o número de elementos de um código é representado por 2^a , onde a é o número de bits empregado pelo código.

I - Introdução aos **Princípios de Comunicação**

Transmissão Serial e Paralela :

Na transmissão de 0's e 1's podemos ter os dados sendo enviados/recebidos de maneira serial ou paralela. Desta forma, na transmissão serial temos os 0's e 1's sendo enviados um após o outro. Por outro lado, na transmissão paralela os 0's e 1's de um byte são enviados simultaneamente em paralelo.

A transmissão paralela é recomendada para casos onde a distância entre remetente e receptor é pequena. Já a transmissão serial é mais adequada para longas distâncias, devido ao baixo custo e maior confiabilidade de transmissão.

I - Introdução aos Princípios de Comunicação

Transmissão Assíncrona e Síncrona :

Numa transmissão assíncrona temos uma sinalização de início (*start*) e fim (*stop*) do caractere transmitido. Para distinguir a sinalização de início e fim, atribui-se ao *stop* um tempo maior que o *start*. Este tipo de técnica ajuda a delimitar com precisão a transmissão de um caractere, embora tenhamos um *overhead* devido a transmissão de sinalização. Como exemplo, vamos supor a transmissão usando o código de 8 bits. Para cada caractere teremos:

$$\text{overhead} = (\text{total bits controle}) / \text{total bits transmitidos}$$

$$\text{overhead} = 3 / (3+8) = 27\%$$

I - Introdução aos Princípios de Comunicação

Transmissão Assíncrona e Síncrona :

Na transmissão síncrona cada bit de um caractere é enviado um após o outro não existindo a sinalização *start/stop* ou *repouso na transmissão*. Existe uma cadeia fixa que efetua o sincronismo para a transmissão dos bits de todo um conjunto de caractere.

SYN	STX	MENSAGEM	ETX	BCC
-----	-----	----------	-----	-----

I - Introdução aos **Princípios de Comunicação**

SYN - Caractere de sincronização

STX - Start of TeXt

MENSAGEM - informação a ser transmitida

ETX - End of TeXt

BCC - Block Check Character

SYN	STX	MENSAGEM	ETX	BCC
------------	------------	-----------------	------------	------------

I - Introdução aos Princípios de Comunicação

Detecção e Correção de Erros:

Na transmissão de 0's e 1's, é necessário que tenhamos uma forma de detectar e corrigir erros que podem ocorrer durante o envio/recebimento de dados. Algumas técnicas conhecidas são:

- *Ecoplexing* : abordagem de detecção, onde se faz uma comparação do caractere digitado no transmissor e ecoado pelo receptor. Caso exista diferença o caractere é reenviado.
- *Paridade* : técnica de detecção, onde acrescenta-se um bit extra ao caractere transmitido, provocando um número *par* (ou *ímpar*) em relação ao número total de bits 1's.

I - Introdução aos **Princípios de Comunicação**

- *Paridade Combinada* : nesta técnica temos uma combinação da paridade vertical e da horizontal de cada bit transmitido, permitindo-nos a detecção e eventual correção de erros. A paridade combinada possibilita a formação de um controle conhecido como BCC.

BCC (Block Check Character) é obtido de todos os bits formados pela paridade horizontal (LRC), sendo implementado nos equipamentos a partir da operação ou exclusivo dos caracteres a serem transmitidos.

I - Introdução aos **Princípios de Comunicação**

- *CRC (Cyclic Redundancy Checking)* : este método de detecção e correção é mais sofisticado, pois emprega um polinômio que nos permite que seja detectado qualquer ocorrência de um grupo de erros e sejam corrigidos.

I - Introdução aos Princípios de Comunicação

Exemplos das técnicas de detecção :

(1) Paridade

PAR

Caractere	Bit de Paridade	Seqüência a Transmitir
1000100	0	10001000
1110000	1	11100001

ÍMPAR

Caractere	Bit de Paridade	Seqüência a Transmitir
1000100	1	10001001
1110000	0	11100000

I - Introdução aos Princípios de Comunicação

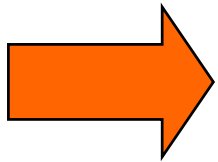
(2a) Paridade Combinada: Considere o envio da palavra *MENSAGEM* empregando o código ASCII.

Bit	M	E	N	S	A	G	E	M	
1	1	1	0	1	1	1	1	1	1
2	0	0	1	1	0	1	0	0	1
3	1	1	1	0	0	1	1	1	0
4	1	0	1	0	0	0	0	1	1
5	0	0	0	1	0	0	0	0	1
6	0	0	0	0	0	0	0	0	0
7	1	1	1	1	1	1	1	1	0
VRC	0	1	0	0	0	0	1	0	

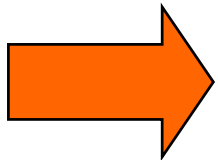
LRC

I - Introdução aos Princípios de Comunicação

- O que significa o envio do dado **MENSAGEM** de um ponto A para um ponto B ?



O ENVIO DO DADO



O ENVIO DOS PARAMETROS DE CONTROLE

- VRC
- LRC
- BCC

I - Introdução aos Princípios de Comunicação

(2b) Paridade Combinada : Vamos considerar que um erro ocorreu no segundo bit da letra *N*. O que acontecerá ?

Bit	M	E	N	S	A	G	E	M	
1	1	1	0	1	1	1	1	1	1
2	0	0	<u>0</u>	1	0	1	0	0	<u>0</u>
3	1	1	1	0	0	1	1	1	0
4	1	0	1	0	0	0	0	1	1
5	0	0	0	1	0	0	0	0	1
6	0	0	0	0	0	0	0	0	0
7	1	1	1	1	1	1	1	1	0
VRC	0	1	<u>1</u>	0	0	0	1	0	

LRC

I - Introdução aos **Princípios de Comunicação**

No exemplo 2b, o VRC do transmissor para a letra N (0) apresentará uma discrepância para o VRC calculado pelo receptor (1). Por outro lado, o mesmo ocorrerá com o LRC que terá valores distintos para o transmissor e receptor.

Como temos um erro único este além de ser detectável poderá ser tratado, uma vez que existe uma interseção entre os erros encontrados pelos VRC e LRC.

I - Introdução aos Princípios de Comunicação

(2c) Paridade Combinada : Agora o erro ocorre nos bits 2 e 7. Qual será a ação da técnica de paridade combinada ?

Bit	M	E	N	S	A	G	E	M	
1	1	1	0	1	1	1	1	1	1
2	0	0	1	<u>0</u>	0	1	0	0	<u>0</u>
3	1	1	1	0	0	1	1	1	0
4	1	0	1	0	0	0	0	1	1
5	0	0	0	1	0	0	0	0	1
6	0	0	0	0	0	0	0	0	0
7	1	1	1	<u>0</u>	1	1	1	1	<u>1</u>
VRC	0	1	0	0	0	0	1	0	

LRC

I - Introdução aos Princípios de Comunicação

No exemplo 2c, o VRC do transmissor para a letra S (0) **não** apresentará discrepância para o VRC calculado pelo receptor (0). Por outro lado, o LRC terá valores distintos para o transmissor e receptor nos bits 2 e 7.

Como temos um erro duplo este poderá ser detectado, todavia não poderá ser tratado, uma vez que não existe interseção entre os erros encontrados pelos VRC e LRC. A solução será a retransmissão de todo o bloco.

I - Introdução aos Princípios de Comunicação

(2d) Paridade Combinada: Vamos supor o erro apresentado abaixo. Qual será o efeito no receptor ?

Bit	M	E	N	S	A	G	E	M	
1	1	1	0	1	1	1	1	1	1
2	0	0	1	1	0	1	0	0	1
3	1	1	1	0	0	1	1	1	0
4	1	0	<u>0</u>	<u>1</u>	0	0	0	1	1
5	0	0	<u>1</u>	<u>0</u>	0	0	0	0	1
6	0	0	0	0	0	0	0	0	0
7	1	1	1	1	1	1	1	1	0
VRC	0	1	0	0	0	0	1	0	

LRC

I - Introdução aos Princípios de Comunicação

No exemplo 2d, o VRC do transmissor para as letras N (0) e S (0) **não** apresentarão discrepância para o VRC calculado pelo receptor (N(0) e S(0)). De forma idêntica, o cálculo do LRC não apresentará problema (nós que estamos com um).

Como temos um erro quadrado este não poderá ser detectado, nem poderá ser tratado, uma vez que não foram detectados pelo VRC e LRC. A solução será o uso de outra técnica para tratar este tipo de erro.

I - Introdução aos Princípios de Comunicação

(3) CRC - Cyclic Redundancy Checking

- Considere a transmissão da seqüência de bits 10111011.
- Vamos considerar um polinômio gerador $G(x) = x^3 + x^2 + x$.
- O polinômio da entrada é $D(x) = x^7 + x^5 + x^4 + x^3 + x + 1$.
- Multiplicar $D(x)$ por maior índice do gerador x^3 .
- $D'(x) = x^{10} + x^8 + x^7 + x^6 + x^4 + x^3$
- Divide-se $D'(x)$ pelo gerador $G(x)$ e obtém-se resto $R(x)$. No caso em questão, teremos que $R(x)$ será igual a $x^2 + x$ (ou 110). Este valor será enviado junto com $D(x)$, assim teremos a transmissão :

$$\begin{array}{r} \underline{10111011} \quad \underline{110} \\ D(x) \quad R(x) \end{array}$$

I - Introdução aos Princípios de Comunicação

(3) CRC - Cyclic Redundancy Checking

- No receptor, a seqüência 10111011110 será dividida pelo mesmo $G(x)$. Se o resto for igual a zero, nenhum erro ocorreu. Caso contrário, um erro ocorreu e uma retransmissão será requerida.

Observação: Existe uma padronização dos polinômios geradores.

$$\text{CRC-12 - } x^{12} + x^{11} + x^3 + x^2 + 1$$

$$\text{CRC -ITU } x^{16} + x^{12} + x^5 + 1$$

V.41

$$\text{CRC-16 } x^{16} + x^{15} + x^2 + 1$$

I - Introdução aos Princípios de Comunicação

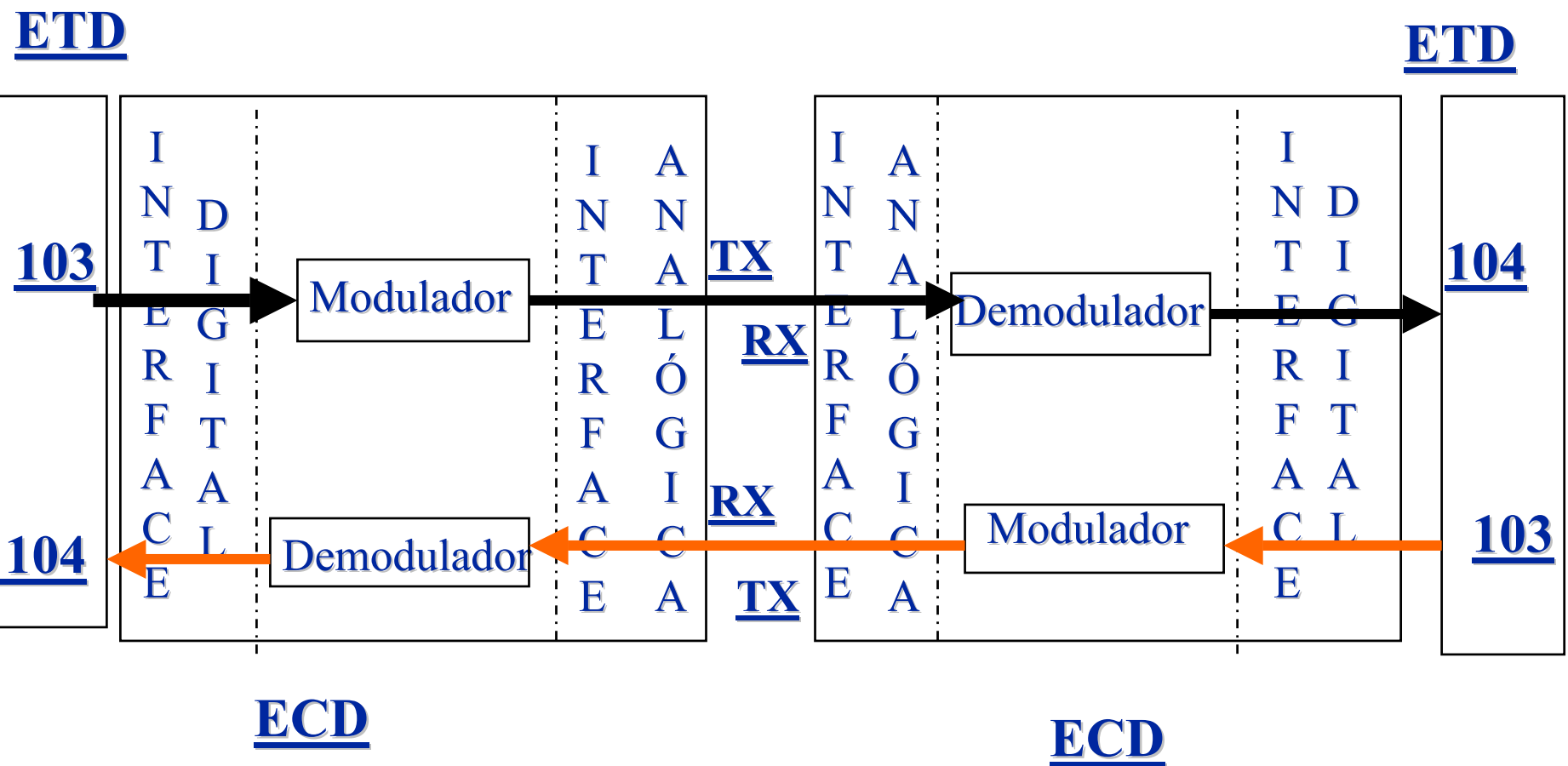
MODEMS

Já estudamos anteriormente que os MODEMS, são dispositivos que nos permitem fazer a Modulação de um sinal no transmissor e a sua correspondente DEModulação no receptor. Os modems são compostos de uma série de circuitos que permitem dentre muitas funções :

- suprimir o *eco* do sinal;
- *equalizar* os sinais recebidos que por algum motivo foram atenuados ou ocorreu um retardo de frequência;
- *embaralhar* (*scrambler*) os dados, evitando uma seqüência longa de bits transmitidos;
- resposta automática;
- uso de facilidades de loops.

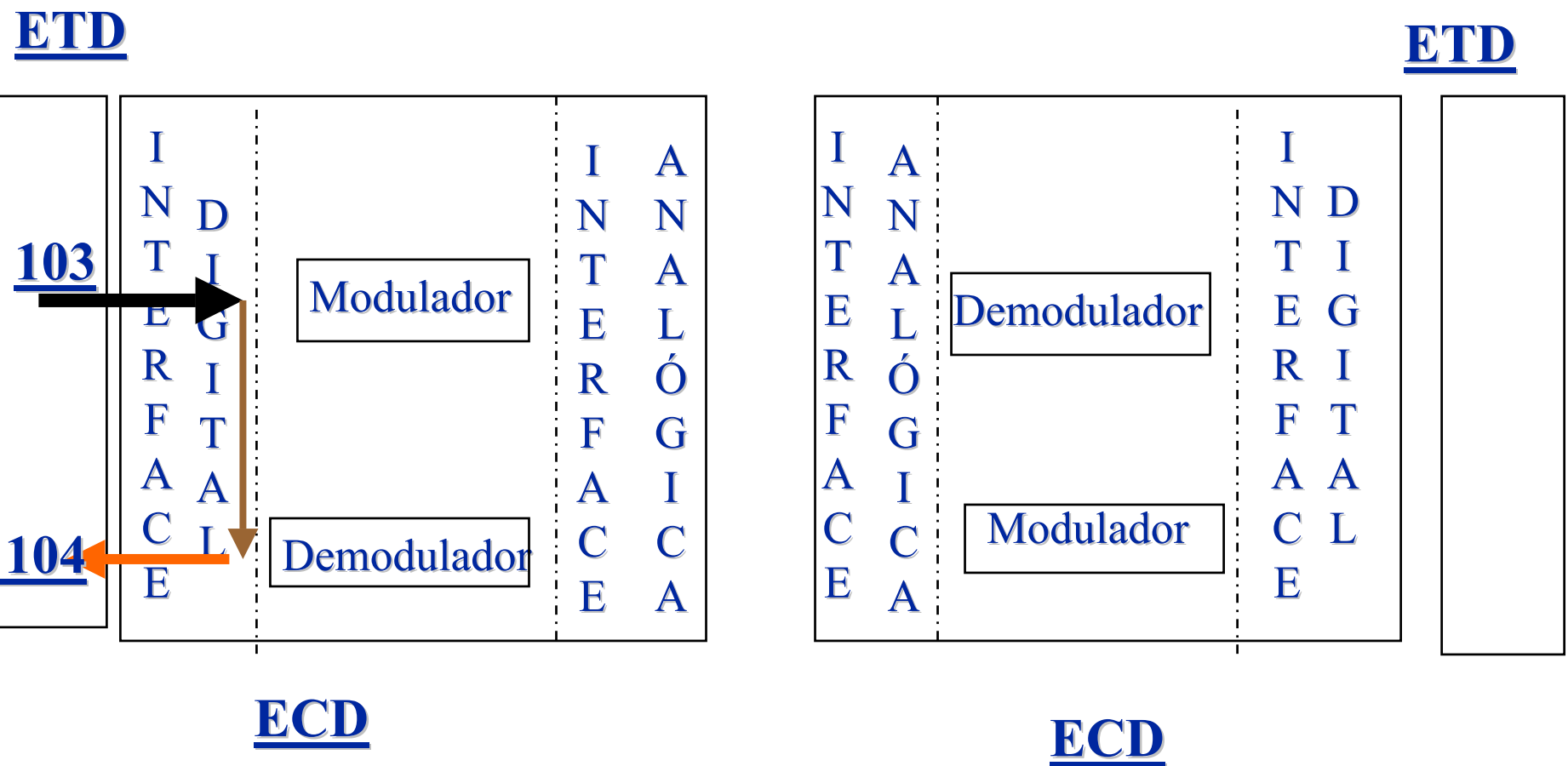
I - Introdução aos Princípios de Comunicação

MODEMS



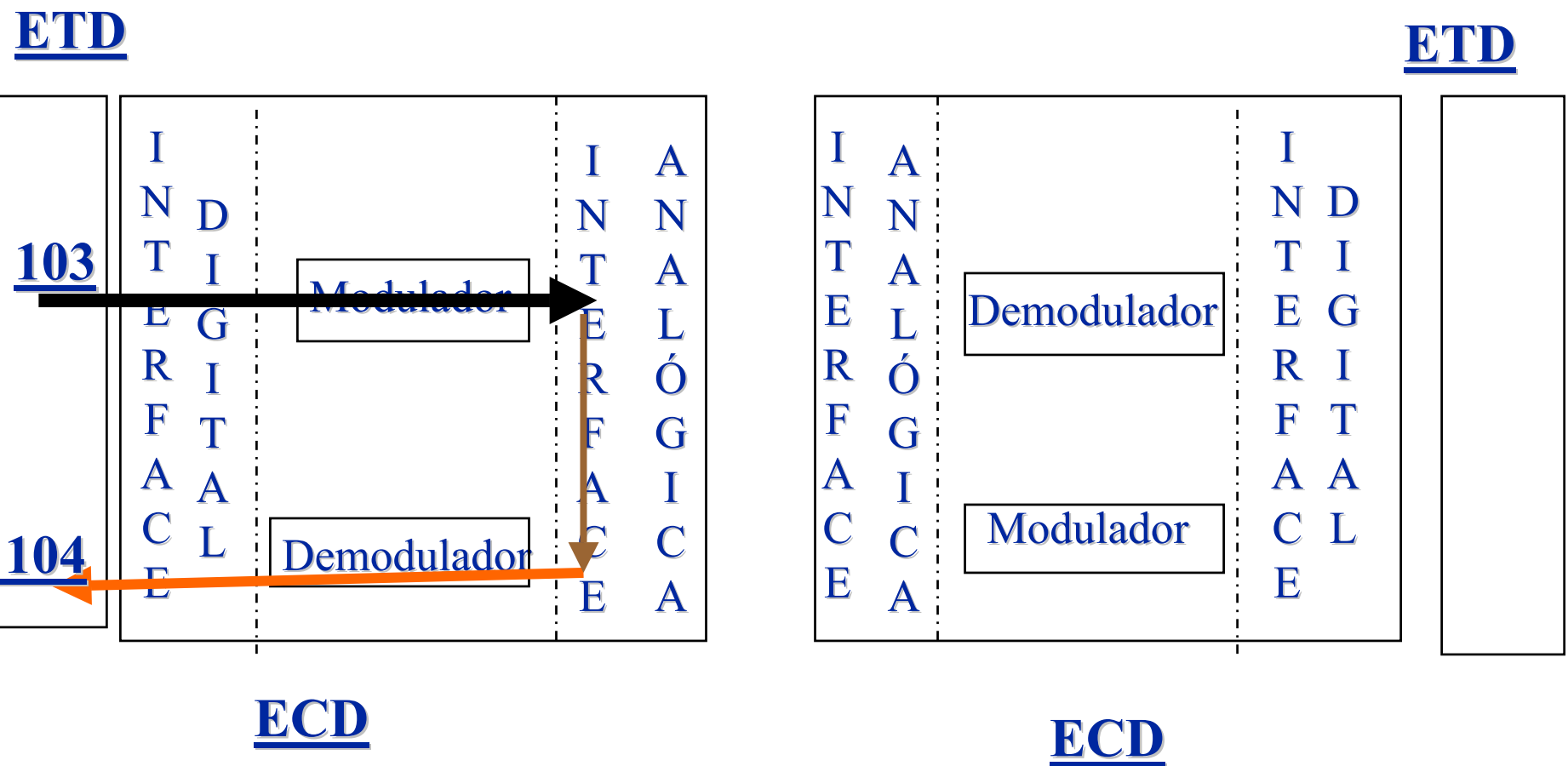
I - Introdução aos Princípios de Comunicação

LOOP DIGITAL LOCAL



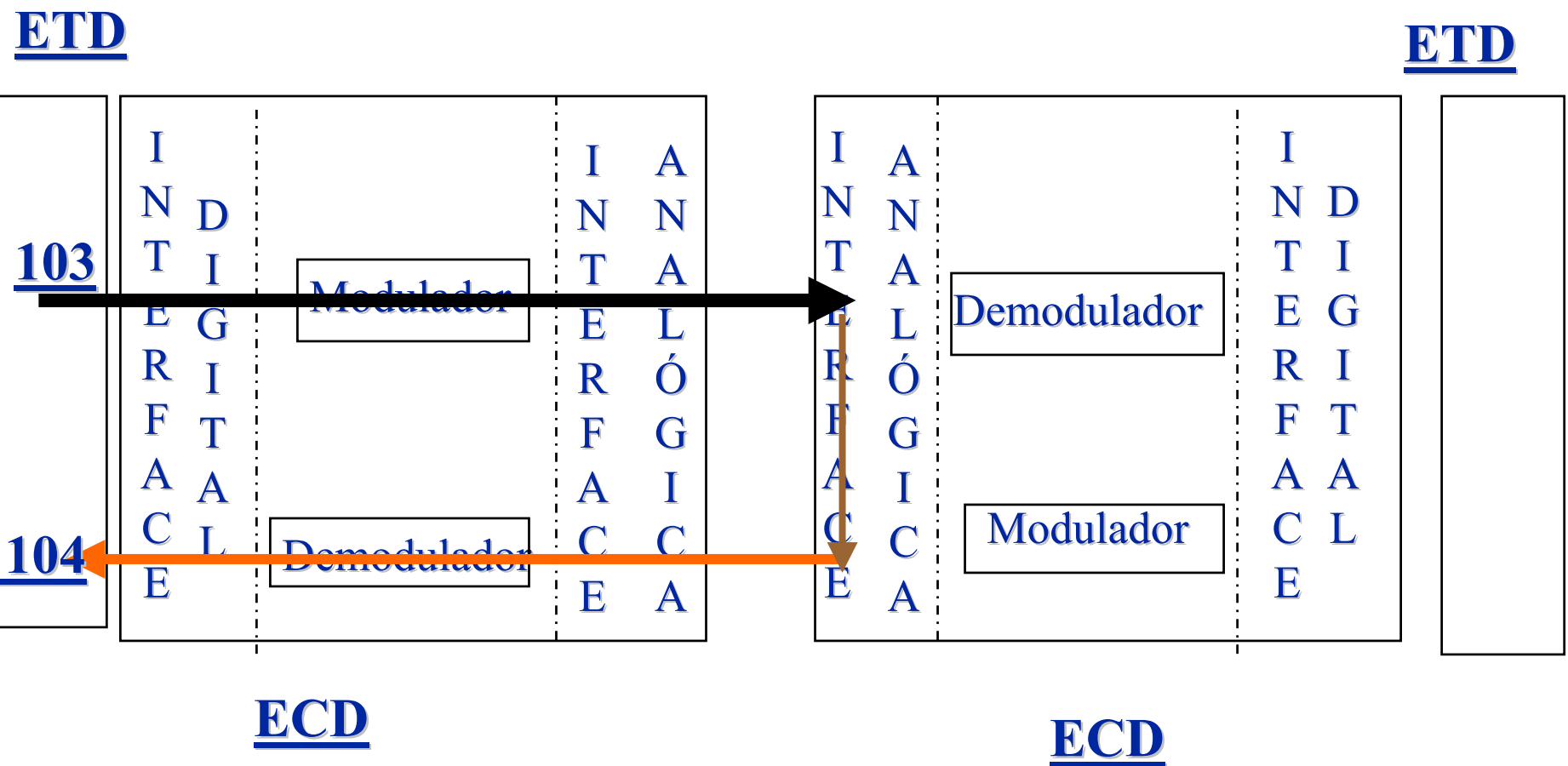
I - Introdução aos Princípios de Comunicação

LOOP ANALÓGICO LOCAL



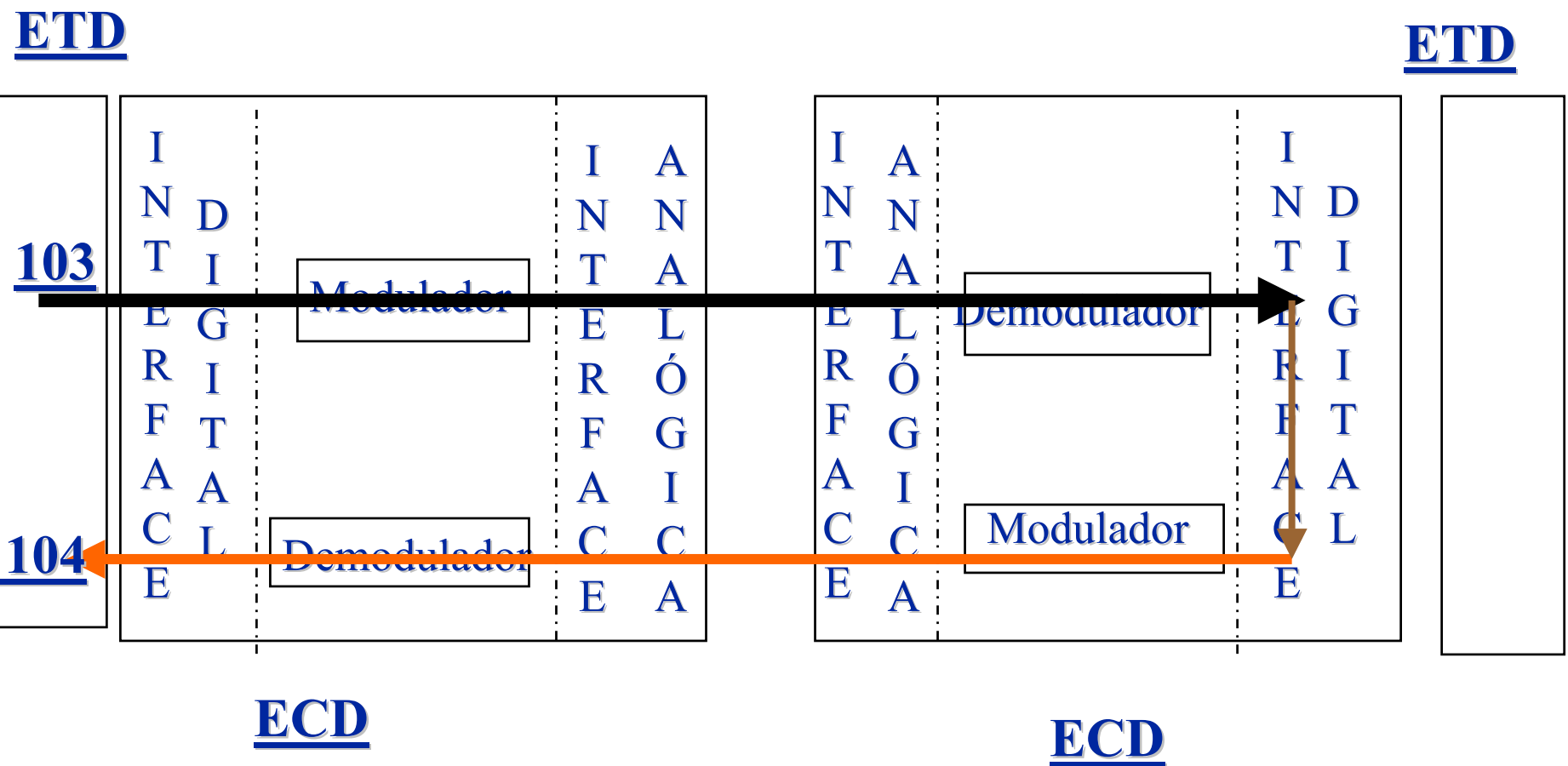
I - Introdução aos Princípios de Comunicação

LOOP ANALÓGICO REMOTO



I - Introdução aos Princípios de Comunicação

LOOP DIGITAL REMOTO



I - Introdução aos Princípios de Comunicação

MODEMS ANALÓGICOS

São equipamentos que realizam a modulação para que os sinais digitais possam ser transmitidos por circuitos de comunicação analógicos.

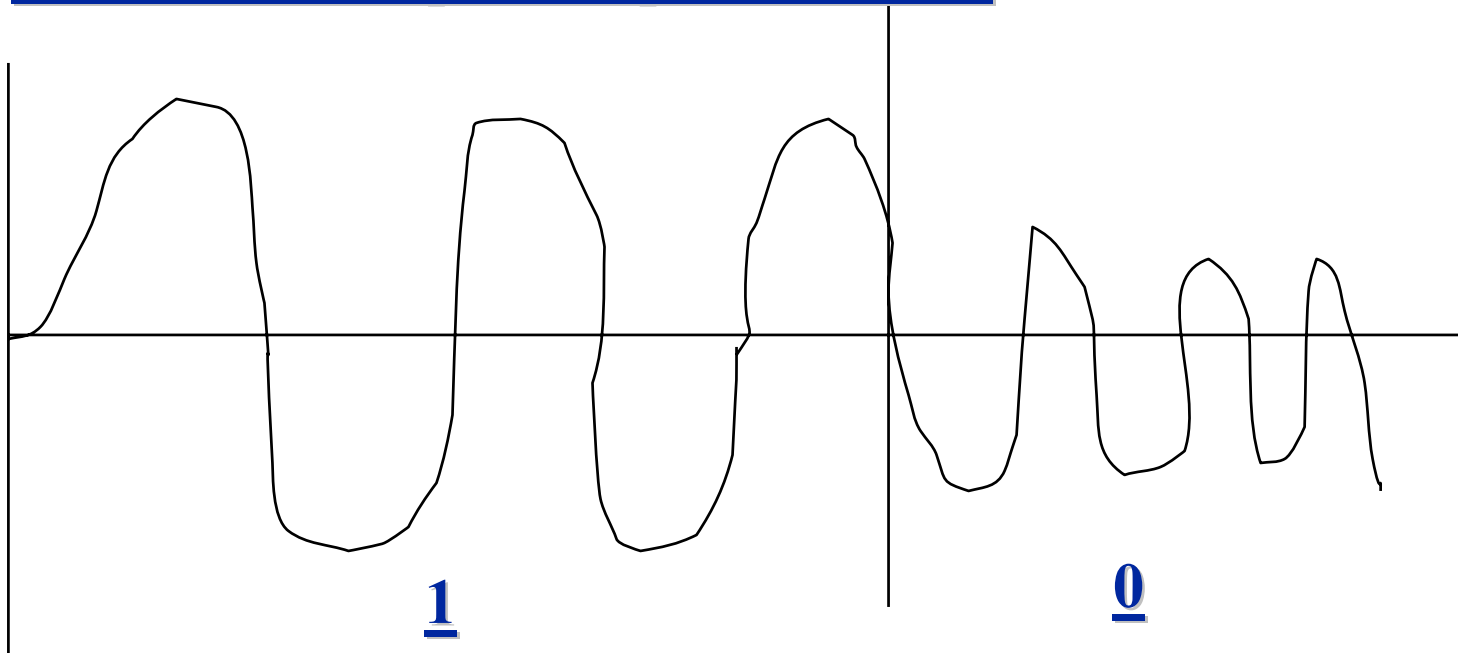
Modulação : É a abordagem na qual uma (ou mais) característica(s) da onda *portadora* é modificada segundo um sinal *modulante* .Um sinal modulante é a informação que se deseja transmitir pela linha de comunicação, no caso da comunicação entre computadores este é o sinal binário. As técnicas de modulação empregam a variação de amplitude, frequência e fase da portadora isoladamente (ou em conjunto). Desta forma, analisando-se a recepção do sinal, as modificações que ocorrem na portadora, pode-se restaurar a informação digital original.

I - Introdução aos Princípios de Comunicação

MODEMS ANALÓGICOS

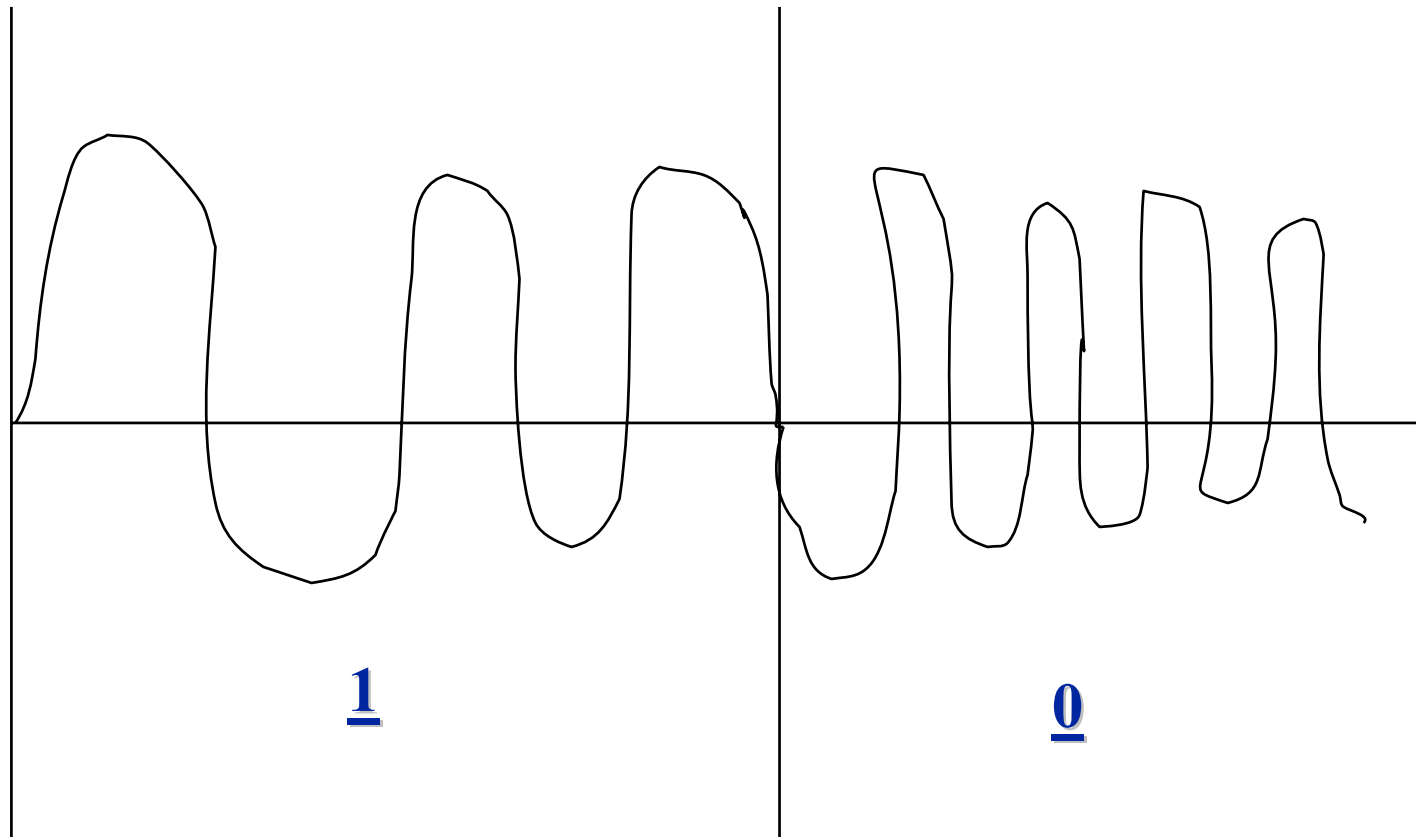
A seguir apresentamos as técnicas básicas de modulação de sinal.

(1) Modulação por Amplitude (AM)



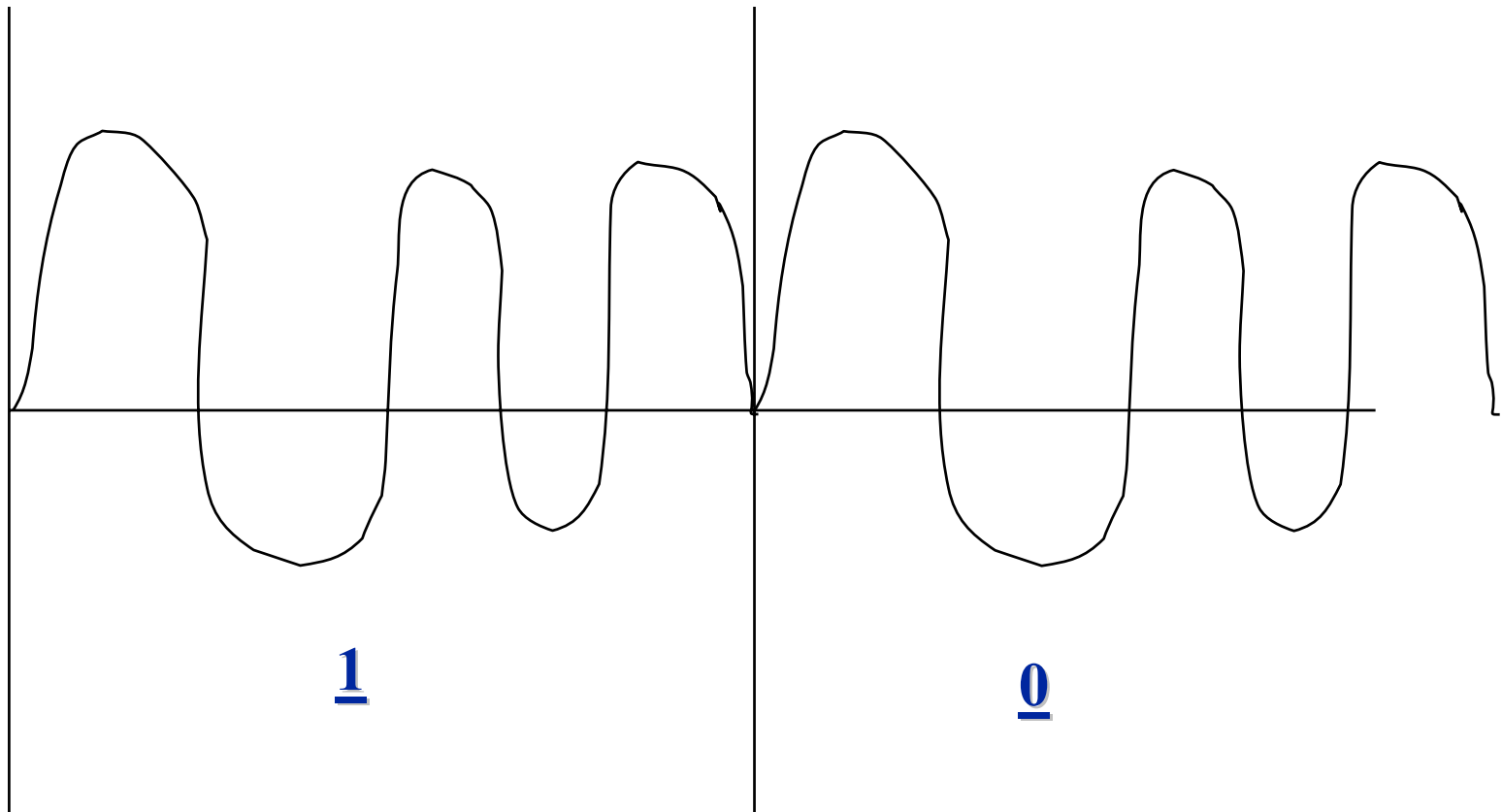
I - Introdução aos Princípios de Comunicação

(2) Modulação por Frequência (FM)



I - Introdução aos Princípios de Comunicação

(3) Modulação por Fase (PM)



I - Introdução aos Princípios de Comunicação

Controle de Fluxo no Enlace

Numa transmissão é importante que a velocidade e quantidade de envio do computador origem possam ser acompanhados no mesmo ritmo pelo computador destino. A nível de enlace é essencial que um mecanismo seja introduzido para que obtenhamos um controle aceitável no fluxo entre computador origem e computador destino. Assim, temos os seguintes exemplos :

- Protocolo de bit alternado - temos o envio de quadros da origem para o destino somente depois que o computador destino envia um reconhecimento de recebimento e processamento de quadro anterior.
- Protocolos com janelas n ($n > 1$) - o controle é efetuado através de quadros especiais e em janelas de transmissão e recepção. Estes protocolos são conhecidos como *sliding windows*, pois permitem o controle de erros e o fluxo de quadros num deslizamento entre origem e destino.

I - Introdução aos **Princípios de Comunicação**

Tipos de Serviços

O nível de enlace pode ter três tipos de serviços que podem ser utilizados pelos nível de rede. Estes :

- **Conexão não-orientada e sem reconhecimento** - é o datagrama não confiável, desta forma este tipo de serviço é mais adequado de utilização em redes onde a taxa de erro é muito pequena.
- **Conexão não-orientada e com reconhecimento** - este tipo de serviço é recomendável para situações onde pequenas mensagens devem ser enviadas com segurança e o custo de estabelecimento e encerramento de uma conexão são altos em relação ao tamanho do quadro que se quer enviar.
- **Conexão orientada** - neste tipo de serviço existe uma garantia que os quadros serão entregues da forma que foram enviados, ou seja (1) será obedecida a numeração dos quadros e (2) não haverá duplicação de quadros na entrega

I - Introdução aos Princípios de Comunicação

Controle de Acesso

A disciplina de acesso ao meio, onde vários computadores estão interligados, é outra função do nível de enlace. Exemplos de técnicas de controle de acesso são:

(1) Master/Slave - nesta configuração uma estação Master (ou primária) envia um quadro de *poll* para saber se as estações Slaves (ou secundárias) querem transmitir. Após o recebimento do quadro de *poll*, a estação secundária pode transmitir se assim o desejar.

(2) CSMA/CD

(3) Token-Bus

(4) Token-Ring

I - Introdução aos **Princípios de Comunicação**

Multiplexação

A camada de enlace, que controla o acesso ao meio, permite vários processos da camada de rede que estejam na mesma estação tenham acesso compartilhado a um meio determinado. Esta técnica é conhecida como multiplexação. A multiplexação é efetuada através do uso dos SAPs (Service Access Points) que permitem que solicitações diferentes da camada de rede possam ser atendidas de maneira diferente, todavia utilizando o acesso ao meio já existente.

I - Introdução aos **Princípios de Comunicação**

Devido as características de alto desempenho, baixo retardo e relativa pequena taxa de erro dos sistemas de comunicação das redes locais, os protocolos empregados nas camadas inferiores do modelo OSI foram projetados de maneira a aproveitar tais características. Nesta parte do curso vamos estudar os *protocolos de acesso ao meio*.

I - Introdução aos **Princípios de Comunicação**

Os protocolos de acesso ao meio são desenvolvidos na maioria das vezes para uma determinada topologia de rede. Devido a certas características de algumas implementações, estas podem ser adotadas em topologias diferentes daquelas para o qual o protocolo foi originalmente projetado. Desta forma, é importante que conheçamos as estratégias de controle de acesso ao meio de diferentes protocolos para diferentes topologias.

I - Introdução aos Princípios de Comunicação

No estudo dos protocolos de acesso ao meio, geralmente, adota-se alguns parâmetros para que possamos quantificar a solução adotada pela técnica de acesso ao meio. Dentre alguns pontos importantes devemos nos preocupar com :

- **Capacidade** : é o maior *throughput* que o método pode tirar do meio com relação a banda passante disponível. Para esta avaliação, ou seja para a avaliação de capacidade, são considerados a taxa de transmissão, comprimento da rede, número de *hosts*, tamanho do quadro e cabeçalho, o retardo em cada *host*.

I - Introdução aos Princípios de Comunicação

- **Eqüidade no acesso** : todos os *host* de mesma classe de prioridade devem ter igual acesso ao meio. É importante que não esqueçamos que a igualdade de classe não significa vamos ignorar o item prioridade.
- **Prioridade** : é desejável que algumas redes disponham de recursos de prioridade. Um exemplo clássico são redes de controle em tempo real.
- **Estabilidade** : em ambientes onde o *workload* é grande, deseja-se alocar um determinado intervalo de tempo diferenciado para cada *host*.
- **Retardo de transferência** : como estudamos anteriormente, este representa o tempo de acesso ao meio acrescido do tempo de transmissão. Em alguns protocolos este tempo é limitado.

I - Introdução aos **Princípios de Comunicação**

As abordagens mais empregadas no desenvolvimento dos métodos de acesso ao meio são de maneira macro subdividas em :

(1) métodos baseados em contenção; e

(2) aqueles de acesso ordenado sem a utilização de técnicas de contenção.

I - Introdução aos Princípios de Comunicação

(I) Acesso Baseado em Contenção

Uma rede que utiliza esta abordagem, não disciplina o acesso ao meio. O que equivale a dizer que mais de um *host* pode ter acesso a rede, fato este que poderá provocar uma colisão com uma (provável) perda de mensagens. Neste tipo de acesso, projeta-se uma estratégia de controle de contenção na qual dos *hosts* espera-se a habilidade de detecção de colisão e uma posterior retransmissão da(s) mensagem(ns).

I - Introdução aos **Princípios de Comunicação**

(II) Acesso Baseado em Contenção

Ainda com relação ao acesso baseado em contenção, espera-se que o tráfego da rede consuma apenas uma parte do *throughput*, o número de colisões seja pequeno e por conseguinte o número de retransmissões também deva ser pequeno.

Com estas condições de contorno de ambiente, podemos dizer que um protocolo baseado nesta técnica pode ser bastante eficiente.

Dentre alguns protocolos vamos estudar :

- Aloha
- CSMA/CA
- CSMA
- ReC-Ring
- CSMA/CD

I - Introdução aos Princípios de Comunicação

Aloha

Método de contenção desenvolvido pela Universidade do Havaí, nos anos 70, visando uma interligação entre um *Mainframe* e seus terminais. O *Mainframe* estava localizado no *Main-Campus* e os terminais espalhados nas diversas ilhas.

O sistema de comunicação era uma rede de radiodifusão via satélite. A rede Aloha era composta de dois canais de frequência de rádio. Um primeiro canal pelo qual a difusão de mensagens era efetuada no sentido *Mainframe*-terminais. O segundo canal com alocação definida para a difusão no sentido terminais-*Mainframe*.

I - Introdução aos Princípios de Comunicação

Aloha - Características do método :

- O primeiro canal somente pode ser usado para *ouvir* pelos terminais.
- O segundo canal é utilizado por qualquer terminal para a transmissão de quadros, independente se o mesmo estiver sendo usado ou não.
- A detecção de colisão é efetuada através de um *timer* na transmissão da mensagem. Caso o quadro de confirmação não chegue ao final do *timer* ter finalizado, uma retransmissão é necessária.
- O intervalo dos *timers* é aleatório, visando diminuir a probabilidade de colisões.
- O *Mainframe* percebe a colisão pela análise do CRC.

I - Introdução aos Princípios de Comunicação

Slotted-Aloha - Características do método :

- Restringe o tempo que o terminal pode começar a transmitir, visando reduzir o tempo gastopor informações inúteis presentes no canal, oriundas de quadros colididos.
- Principal objetivo é que quadros em colisão se sobreponham o máximo. Desta forma, se os quadros colidirem deste o início o tempo total de transmissão superposta será menor que aquele onde a colisão acontece em um tempo qualquer de transmissão.
- Os quadros colididos superpostos (informação inútil), será menor o que implicará num melhor *throughput* no uso do canal.

I - Introdução aos **Princípios de Comunicação**

CSMA (Carrier Sense Multiple Access)- Características do método:

- Sincronização dos quadros em colisão fazendo com que se superponham desde o início, mas não pela divisão de tempo.
- Existe um esforço para evitar colisão.
- Algumas variações detecta-se quadros colididos em tempo de transmissão abordando a mesma.
- É objetivo desta abordagem que os quadros colidam o menor tempo possível melhorando a eficiência do uso do canal.

I - Introdução aos Princípios de Comunicação

CSMA (Carrier Sense Multiple Access)- Características do método:

- *Host **ouve*** o meio para saber se o mesmo está livre para transmitir seus quadros.
- No caso onde o meio está livre, o *host* começa sua transmissão.
- No caso onde o meio está ocupado, o *host* espera por um tempo e volta mais uma vez a tentar a transmissão. Os vários métodos de CSMA, são implementados diferentemente quando a política da *espera de transmissão*.
- Um colisão só ocorre quando dois *hosts* tentam transmitir no mesmo instante.

I - Introdução aos Princípios de Comunicação

np - CSMA/ p-CSMA- Características dos métodos:

- Na abordagem *np (non-persistent)-CSMA*, o *host* ao **ouvir** o meio e notar uma transmissão, este fica esperando por um espaço de tempo aleatório antes de tentar novamente o acesso.
- O método *p (persistent)-CSMA* é caracterizado pela continua operação de **ouvir** o meio até que este fique livre para transmissão. Uma vez que o meio está livre, este faz sua transmissão com um probabilidade p , ou seja ele espera um intervalo p antes de transmitir para evitar colisão. No caso da implementação *CSMA 1-Persistent*, após o meio ficar livre a transmissão é imediatamente inicializada.

I - Introdução aos Princípios de Comunicação

CSMA/CD (Carrier Sense Multiple Access/Collision Detection)-

Características do método:

- Detecção de colisão é realizada durante a transmissão.
- Na transmissão, o *host* fica ouvindo o meio o tempo todo. Caso uma colisão ocorra a transmissão é abortada.
- Após a detecção da colisão o *host* espera por um tempo para tentar uma nova transmissão.
- Considerando-se que a propagação no meio é finita, quadros têm um tamanho mínimo para que todos os *hosts* possam detectar um colisão.

I - Introdução aos Princípios de Comunicação

CSMA/CD (Carrier Sense Multiple Access/Collision Detection)-

Características do método:

Neste método, as relações apresentadas a seguir, devem ser observadas para que os *hosts* possam fazer uma detecção de colisão.

$M \geq 2 C_{tp}$ - Redes em banda base.

$M \geq 4 C_{tp}$ - Redes em banda larga.

Onde :

M - tamanho do quadro.

C - taxa de transmissão.

t_p - tempo de propagação.

I - Introdução aos **Princípios de Comunicação**

CSMA/CD (Carrier Sense Multiple Access/Collision Detection)-

Características do método:

A eficiência do método CSMA/CD é verificada pela relação :

$$E = 1 / (1 + (3.4 \times t_p \times C/M))$$

Onde podemos concluir :

- quanto maior a distância : maior o tempo de propagação, menor a eficiência e maior o tamanho mínimo do quadro para a detecção de colisão.
- quanto maior a taxa de transmissão : maior o tamanho mínimo do quadro e menor a eficiência. A eficiência é maior para quadros maiores.

I - Introdução aos Princípios de Comunicação

ReC-Ring (Resolvable Contention Ring) -

Características do método :

- Um *host* começa a transmitir quando sabe que o anel está livre.
- Um quadro transmitido é enviado num único sentido e dá um volta completa pelo anel que o remetente o remove.
- Um *host* espera que um trem de quadros acabe de passar pelo anel até que comece a transmitir.
- Todos os *host* sabem sua posição no anel em relação a um nó de referência.
- A colisão ocorre quando um *host* estiver transmitido e chega um quadro de um *host* anterior ao primeiro.

I - Introdução aos Princípios de Comunicação

ReC-Ring (Resolvable Contention Ring) -

Características do método :

- Detectada uma colisão, o *host* suspende sua transmissão e efetua uma comparação no índice do *host* que enviou o quadro e o seu. Se seu índice for maior com relação ao nó de referência, então o *host* espera pelo trem de quadros. Caso contrário, o *host* retransmite imediatamente, descartando o quadro recebido.

I - Introdução aos Princípios de Comunicação

(II) Acesso Ordenado sem Contenção

Uma rede que utiliza esta abordagem, *disciplina* o acesso ao meio. O que equivale a dizer que apenas um *host* pode ter acesso a rede, fato este que evita uma possível colisão com uma perda de mensagens. Cada método de acesso ordenado é, geralmente, projetado para uma determinada topologia. Todavia, este fato não é limita o uso de determinadas abordagens entre topologias diferentes para as quais o método não foi originalmente projetado. Os métodos de acesso ordenado mais conhecidos são o *polling*, *slot*, *inserção de retardo*, *por passagem de permissão* e *por reserva*.

I - Introdução aos Princípios de Comunicação

Polling - Características do método :

- Esta técnica é caracterizada por um *host* central periodicamente enviando quadros aos *host secundários* se estes têm algo para transmissão.
- Cada *host* de forma ordenada faz sua transmissão, quando for o caso, após o questionamento do *host principal (ou master)*.
- Na falta de quadros a transmitir, um *host secundário* responde ao mestre com um quadro status que está vivo, todavia não tem nada para ser transmitido.

I - Introdução aos Princípios de Comunicação

Polling - Características do método :

- Para melhorar a eficiência do *host central* algumas variações do método *polling* implementam uma tática de começar o questionamento pelo *host* mais distante. Após ser questionado passa o quadro de questionamento para o mais próximo a ele e assim por diante até que um *host* tenha algo para transmitir. Neste ponto, o *host central* volta a tomar conta do ambiente.
- Caminhos específicos para controle e informações de controle enviadas junto com quadros de informação são algumas variações de implementações de *polling* que melhoram a performance desta técnica.

I - Introdução aos Princípios de Comunicação

Slot - Características do método :

- Abordagem desenvolvida nos anos 70 para redes de topologia em anel (exemplos de redes que usam slot são Fasnets e ATM Ring).
- A ideia é dividir o espaço de comunicação em um número inteiro de pequenos segmentos, conhecidos como *slots*, dentro dos quais uma mensagem pode ser armazenada.
- Uma ilustração desta técnica é um movimento circular de caminhões, onde uns caminhões estão com carga e outros vazios. Um *host* que deseja transmitir deve esperar por um caminhão vazio (*slot vazio*) e então carregá-lo com carga (mensagem).
- Muitos *slots* correm em vazio quando não existem mensagens a transmitir.

I - Introdução aos **Princípios de Comunicação**

Inserção de retardo - Características do método :

- Na inserção de retardo a técnica empregada é, como o nome diz, a inserção de um determinado tempo entre as transmissões e recepções.
- O retardo é efetuado através da NIC, que dispõe de circuitos para recepção e transmissão. O retardo existe, pois ocorre um chaveamento de seleção entre a recepção e transmissão. O que significa dizer que se a NIC estiver recebendo um quadro, ocorrerá um retardo na transmissão de um quadro, pois é necessário que seja efetuado um chaveamento para o circuito de transmissão.

I - Introdução aos Princípios de Comunicação

Passagem de Permissão - Características do método :

- Neste tipo de protocolo de acesso existe um esquema de controle de uma permissão (*token*), que é um padrão pré-definido, é passada seqüencialmente de um estação para outra. Somente o *host* que dispõe do *token* pode efetuar a transmissão. Não é necessário que a ordem física seja a ordem lógica de transmissão. A abordagem de passagem de permissão é muito empregada em redes em anel e de topologia de barra. Algumas implementações não consideram um padrão como o *token*, mas a presença e a ausência de quadros a transmitir fazendo avançar um ponteiro, interno a cada *host*, que fará a sinalização do próximo *host* que poderá transmitir.

I - Introdução aos Princípios de Comunicação

Passagem de Permissão - Características do método :

- Os principais exemplos de protocolos de acesso que empregam este método são o *token-bus* e *token-ring*. Alguns outros protocolos menos conhecidos, tais como *expressnet* e *fast-ring*, também usam a passagem de permissão.

Concessionária de Telecomunicações



Como um estudo de caso de uma concessionária de telecomunicações, escolhemos a empresa EMBRATEL devido ao grande número de serviços oferecidos e ainda por sua abrangência nacional e internacional.

Concessionária de Telecomunicações



HISTÓRICO

Objetivos: a EMBRATEL- Empresa BRAsileira de TELecomunicações - foi fundada em 1965 com a missão da (1) integração do Brasil através das telecomunicações e (2) a interligação do Brasil com o mundo.

Etapas :

- Em 1969 é inaugurada a Estação Terrena de Tanguá, no Rio de Janeiro. Na sua ligação internacional a empresa registra alguns fatos marcantes, tais como a transmissão direto de Roma a benção do Papa Paulo VI, o homem chegando a Lua e o Brasil Tri-campeão(70).
- Criação do serviço DDD- Discagem Direta à Distância-e transmissão nacional a cores pela TV em 1972 (evento Festa da Uva - RGS).

Concessionária de Telecomunicações



HISTÓRICO

- Criação do serviço DDI - Discagem Direta Internacional- em 1975 e neste período entram em operação as conexões de três cabos submarinos, estes BRACAN e ATLANTIS para a Europa e o BRUS para a América do Norte.
- Em 1985 com o satélite Brasilsat é alcançada a cobertura de todo o território nacional. Desta forma, serviços de transmissão de TV, telefone, telex e comunicação de dados tornam-se nacionalmente acessíveis.
- Lançamento de cabos submarinos em fibras óticas para as comunicações para suportar diversas aplicações reduzindo sensivelmente o custo de telecomunicação estão entre as metas atuais da Embratel. Dentre os esforços neste sentido destacam-se :

Concessionária de Telecomunicações



HISTÓRICO

- **América I** : ligação entre o Brasil e os EUA, este interligando as três Américas e que tem a participação de 24 países, dentre os quais o Japão e os EUA.
- **Unisur** : interligação dos países do cone sul - Brasil, Argentina, Uruguai Chile e Paraguai e com extensão destes países para a rede mundial de fibras.
- **Linha Fortaleza-Florianópolis** : ligação de fibra ótica terminada em 1996, numa rota de 5.100 quilômetros, duplicando a capacidade instalada de transmissão entre todas as capitais no trecho compreendido entre na linha. Esta linha quando terminada, interligará Brasília as capitais e principais cidades brasileiras.

Concessionária de Telecomunicações



HISTÓRICO

A Rede Nacional de Fibras Óticas da Embratel, será o *backbone* para a transmissão de voz, imagem, textos e dados entre o Brasil, a América do Sul e o mundo.

Concessionária de Telecomunicações



A EMPRESA

- Atua em 4.000 cidades brasileiras;
- Interage com mais de 200 países;
- Número de empregados na ordem de 11.000;
- Conjunto de 30 serviços de telecomunicações;
- Maior lucro (1996) - R\$ 406 milhões;
- Receita líquida de R\$ 1.894 bilhão;
- Investimentos na casa dos R\$850 milhões
(88 % de recursos próprios)
- Impostos pagos na ordem de R\$ 513 milhões para os Governos Federal, Estadual e Municipal.

Concessionária de Telecomunicações

A REDE

A Rede da Embratel que prove mais de 30 serviços diferentes de telecomunicações, utiliza o seguinte conjunto de ambientes :

- **Rede Básica Terrestre** - com mais de 23.000 quilômetros de troncos de microondas;
- **Sistema Brasileiro de Telecomunicações por Satélites** - suporte dos satélites da série BRASILSAT e atendimento através de mais de 70 estações terrenas;
- **Satélites dos Consórcios INTELSAT** - organização internacional de telecomunicações por satélites, do qual a Embratel é participante, que cobre todo o planeta com inúmeros satélites para tal finalidade. Em adição, o sistema **INMARSAT** opera sistemas de satélites para comunicações móveis com cobertura global, alta velocidade, com aplicações comerciais e para situações de emergência.

Concessionária de Telecomunicações



A REDE

- **Redes de Serviços** : estas incluem a Rede Nacional de Telefonia, a Rede de Comunicação de Dados, a Rede Nacional de Rádio e Televisão e a Rede Nacional de Estações Costeiras.

Concessionária de Telecomunicações

A Rede Básica Terrestre

Esta rede tem uma expansão contínua, com elevado índice de digitalização em seus troncos de microondas, sendo completada pelos sistemas ópticos de longa distância. Com referência a rede óptica, já foi iniciada entre os trechos Rio de Janeiro-São Paulo, Rio de Janeiro- Belo Horizonte, São Paulo-Belo Horizonte e Fortaleza-Florianópolis.

A rede óptica de longa distância continua em implantação e dentre seus objetivos estão a garantia dos níveis de confiabilidade e disponibilidade do sistema.

Concessionária de Telecomunicações



A Rede de Telefonia

Esta rede continua em crescente implantação e expansão das centrais de comutação (CPA-T) com mais de 38.000 novos juntores. Esta rede tem um grau de 77 % de digitalização.

Fazem parte desta rede os serviços denominados de *Telefonia Avançada*, muito utilizada por empresas que adotam os serviços 0800 e 0900.

Concessionária de Telecomunicações



A Rede de Comunicação de Dados e Telemáticos

Com capacidade de atendimento de serviços digital, esta rede continua em expansão, pode atender atualmente até 300 circuitos com tecnologia E1 de 2 Mbit/sec.

Concessionária de Telecomunicações



Produtos e Serviços - DADOS

- TRANSDATA : aluguel de circuitos especializados de comunicação de dados nacional. A transdata oferece ligações dedicadas e especializadas.
- RENPAC : Serviço públicos especializados de comunicação de dados por comutação de pacotes, admitindo um largo conjunto de diferentes equipamentos, protocolos e velocidades.

FASTNET: Serviço público de comunicação de dados, com abrangência nacional e internacional, baseado no protocolo FRAME-RELAY. Entre as características do serviço FASTNET, a Embratel destaca a rapidez, qualidade e disponibilidade do serviço.

Concessionária de Telecomunicações

Produtos e Serviços - DADOS

- MULTISAT : serviço de transmissão bidirecional de sinais digitais, via satélite, ponto-multiponto de âmbito internacional.
- STM 400 : serviço de tratamento de mensagens nacional/internacional. Este serviço prove com segurança, rapidez e sigilo absoluto a troca de mensagens e arquivos em qualquer ponto do país e do exterior. Entre suas facilidades, destaca-se a possibilidade de envio de mensagens para mais de 100 destinatários, simultaneamente. Com vários acordos internacionais comerciais, a EMBRATEL prove neste serviço a troca de mensagem com outros serviços de troca de mensagem no exterior.

Concessionária de Telecomunicações



Produtos e Serviços - DADOS

- DIGISAT : serviço internacional de aluguel de circuitos digitais via satélite em alta velocidade. Permite a interligação de um, ou mais, ponto(s) no Brasil com um, ou mais, ponto(s) no exterior para o intercâmbio de dados de computadores, voz digitalizada, áudio, videoconferência, teleprocessamento, fax, distribuição eletrônica de documentos e transferência de arquivos.
- MEGADATA : é o serviço de telecomunicações caracterizado pelo aluguel de circuitos digitais dedicados de alta velocidade, interestadual entre localidades que disponham da plataforma digital da EMBRATEL.

Concessionária de Telecomunicações

Produtos e Serviços - DADOS

- TOPNET: é um serviço cujo objetivo é prestar uma solução completa de rede para o cliente, disponibilizando um conjunto de facilidades como acessos, bandas e interfaces com outros serviços.
- DATASAT: aluguel de circuitos de comunicação de dados via Satélite, podendo distribuir dados emitidos de um ponto central para diversos pontos receptores. Este serviço ainda disponibiliza a comunicação de dados ponto-a-ponto e multiponto, previamente identificados pelo gerador e receptor da mensagem.

Concessionária de Telecomunicações



Produtos e Serviços - DADOS

- DATAFAX : serviço público nacional/internacional de fax com a facilidade de multiendereçoamento.
- SERVIÇOS INTERNET - o serviço de conexão à rede Internet é oferecido pela EMBRATEL, posto que esta dispõe do maior *backbone* na América Latina, considerando-se sua abrangência e capacidade de transmissão. Dentre as facilidades oferecidas pelo serviço de acesso a Internet, a EMBRATEL disponibiliza: IPDIRETO, INFOSERV, UUCP, INTRANET e EXTRANET.

Concessionária de Telecomunicações

Produtos e Serviços - DADOS

- MULTI REDE DIGITAL: rede sobre a qual podem ser alocadas redes privadas virtuais para formação de redes corporativas de empresas, integrando-se a comunicação de voz, texto, dados, fax e imagem.

Concessionária de Telecomunicações

Produtos e Serviços - SOM-IMAGEM

- Televisão Internacional - serviço destinado à transmissão de sinais de televisão em âmbito internacional, transportando as imagens geradas por emissoras comerciais ou outras geradoras para a realização de eventos em geral.
- TV DIGITAL : serviço destinado à transmissão de sinais digitais de TV, em circuito fechado para a formação de redes.
- RADIOSAT : serviço especial de retransmissão de sinais de áudio via satélite, disponível nas modalidades AM, FM e FM estéreo.

Concessionária de Telecomunicações

Produtos e Serviços -VOZ

A interligação das concessionárias estaduais entre si, formando uma rede nacional e ainda com o exterior com a rede mundial de telefonia. O sistema atinge a 3.000 localidades brasileiras e 150 países. A EMBRATEL fornece ainda serviços de telefonia privada, abrangendo circuitos de voz nacionais e internacionais. Dentre os serviços :

- VIPNET - serviço internacional de rede privada virtual de voz. Através do estabelecimento de uma rede virtual, o usuário dispõe do tráfego de voz, dados e fax com as vantagens de uma rede privada implementada utilizando-se as facilidades da rede pública.

Concessionária de Telecomunicações

Produtos e Serviços -VOZ

- TELEFONIA NACIONAL - DDD, 0800 e 0900
- TELEFONIA INTERNACIONAL - DDI, BRASIL DIRETO, CALL HOME DIRECT E TELECARD.
- DIGIDIAL : serviço nacional e internacional que permite originar e receber chamadas a 64 kbit/sec ou múltiplos, através da Rede Pública Comutada, com garantia de conectividade digital, desde a origem até o destino.

Concessionária de Telecomunicações

Produtos e Serviços - Comunicação Móvel

O Brasil tem dimensões continentais e uma faixa costeira de 7.408 km. Desta forma, a existência de um serviço que possa fornecer serviço não só de voz, mas também de texto e dados para unidades móveis - tais como navios, caminhões, carros, trens - é uma necessidade óbvia. O serviço MOVSAT, ou serviço móvel de comunicação via satélite, é a facilidade de comunicação móvel oferecida pela EMBRATEL.

Serviços Internacionais de Satélites



As redes de comunicação são muitas vezes limitadas por problemas físicos e de largura de banda. Recentemente, um conjunto grande de provedores de facilidades via satélites vêm ganhando espaço tanto no mercado como no “*espaço*” propriamente dito. Dentre das muitas empresas que prestam serviços via satélites, temos : IRIDIUM, ELLIPSO, TELEDESIC, GLOBOSTAR, SKYBRIDGE, ICO e ORBCOMM.

Vamos a seguir estudar os serviços oferecidos por estas empresas e as facilidades que cada uma pode prover para seu usuário.

Serviços Internacionais de Satélites



O uso de satélites geo-estacionários (*geosynchronous*) tem sido por muitos anos a solução para as aplicações que dependiam de um *link* via satélite. Todavia, por estarem cerca de 36.000 km de distância da terra, acima do equador, estes determinam um retardo de meio segundo para a comunicação. Para o uso de voz, este retardo não é tão sensível quando comparamos com a transmissão de dados. É ainda interessante lembrarmos que para aqueles satélites ainda mais distantes o custo do envio e equipamentos de retransmissão aumentam o custo do empreendimento.

Serviços Internacionais de Satélites



Pelos motivos expostos, os chamados LEO birds e MEO birds têm ganho a atenção de várias corporações. O motivo de atenção pode ser explicado pelo baixo retardo (*latency*) dos mesmos para a comunicação. No primeiro caso, temos os LEO (Low Earth Orbit) os quais estão distantes entre 600 a 1600 km da terra. Por outro lado, os MEO (Medium Earth Orbit) têm sua orbita entre 4.000 à 10.000 km.

Serviços Internacionais de Satélites



A utilização de frequências na casa dos GHz os sinais deste satélites podem ser capturados por antenas pequenas em dispositivos móveis, incluindo-se aqueles existentes são facilmente carregados à mão. Pode-se prover uma cobertura global com menores custos de lançamento e dispositivos necessários para repetição e emissão de sinal. A desvantagem dos LEO/MEO é a maior quantidade de satélites necessários para cobrir o globo.

Serviços Internacionais de Satélites

PROVEDORES

IRIDIUM

- sistema com 66 satélites;
- início dos testes em Setembro de 1998 por 20.000 usuários;
- os *birds* têm orbitas de 780 Km, com peso de 700 kg e com 48 spot beams;
- uso de banda baixa entre 1616 até 1626.5 MHz;
- os serviços fornecidos são pager e voz;
- a interligação dos *birds* (satélites) é efetuada na banda de 23.18 à 23.38 GHz entre quatro birds agrupados;
- *downlinks* na faixa de 19.4 até 19.6 GHz e *uplinks* de 29.1 até 29.3 GHz.

Serviços Internacionais de Satélites

PROVEDORES

IRIDIUM

- serviços não destinados a transmissão grande de dados;
- serviços de comunicação global de usuário de telefones móveis;
- serviços de voz, dados e fax digitais

Serviços Internacionais de Satélites

PROVEDORES

ELLIPSO

- início de operação em 2001;
- utilização de duas constelações de satélites tipo MEO;
- Ellipso Borealis é uma das constelações apontando para o hemisfério norte numa órbita distante da terra de 7.606 km;
- Ellipso Concordia serve as regiões tropicais e hemisfério sul numa órbita distante da terra de 8.050 km;
- o objetivo principal deste provedor é fornecer serviços com baixo custo apoiado no design do seu sistema de satélites.

Serviços Internacionais de Satélites

PROVEDORES

TELEDESIC

- início de operação em 2003;
- utilização de satélites do tipo LEO;
- uso de 288 *birds* em doze órbitas com o objetivo de prover serviços de telecomunicação semelhantes aos serviços das fibras ópticas;
- projeto ambicioso de donos ambiciosos (Bill Gates, Craig McCaw e Principe Bim Talal), com investimentos de US\$ 9 bilhões.

Serviços Internacionais de Satélites

PROVEDORES

GLOBOSTAR

- início de operação em 1998;
- utilização de 8 (+12 ?) satélites do tipo LEO;
- projeto da Qualcomm e TESAM (France Telecom e Alcatel);
- para 1999 é planejado o envio de 32 *birds*;
- uso de telefonia publica via satélites (teste já efetuados em Setembro/98);

Serviços Internacionais de Satélites

PROVEDORES

SKYBRIDGE

- início de operação no final de 2001;
- utilização de 80 satélites do tipo LEO;
- projeto e serviços semelhantes a TELEDÉSIC;
- custo do projeto na ordem de US\$4.2 bilhões;

Serviços Internacionais de Satélites

PROVEDORES

ICO

- início de operação no final de 1998;
- utilização de 10 satélites do tipo MEO;
- projeto e serviços criados por uma comunidade internacional de países com metade dos países em desenvolvimento (Brasil, China, MIAMI, Índia, Turquia, URSS) ;
- serviço orientado para comunicação telefônica;

Serviços Internacionais de Satélites

PROVEDORES

ORBCOMM

- início de operação no final de 1998;
- utilização de 28 satélites do tipo LEO;
- serviço orientado para monitoração (carros, tubulações, serviços elétricos e equipamentos pesados);

II - Arquitetura dos computadores modernos



Objetivo: Os aspectos da evolução tecnológica na área da arquitetura dos computadores, podem prover uma melhor visão aos profissionais envolvidos em projetos de redes e suporte a aplicações distribuídas. Em adição, este conhecimento auxilia no desenvolvimento de um censo crítico mais técnico do assunto.

II - Arquitetura dos computadores modernos



Os primeiros Computadores Eletrônicos:

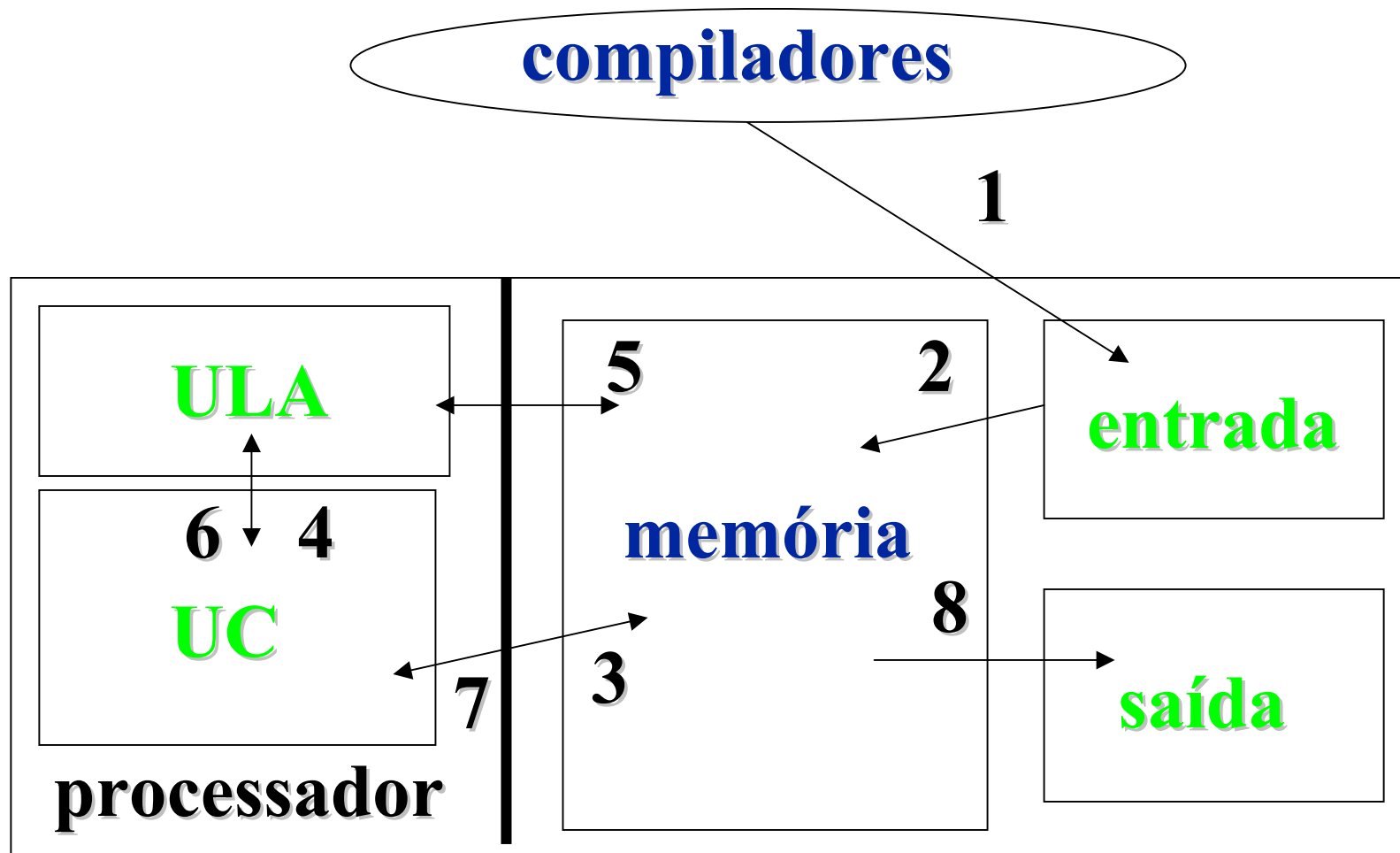
- **J. Presper Eckert e John Mauchly construíram o primeiro computador eletrônico na Moore School na Universidade da Pennsylvania durante a II Guerra Mundial. A máquina chamada de ENIAC - Electronic Numerical Integrator and Calculator- foi somente conhecida do público em 1946. Esta máquina foi usada pelo US Army para cálculo das tabelas de tiro.**

II - Arquitetura dos computadores modernos

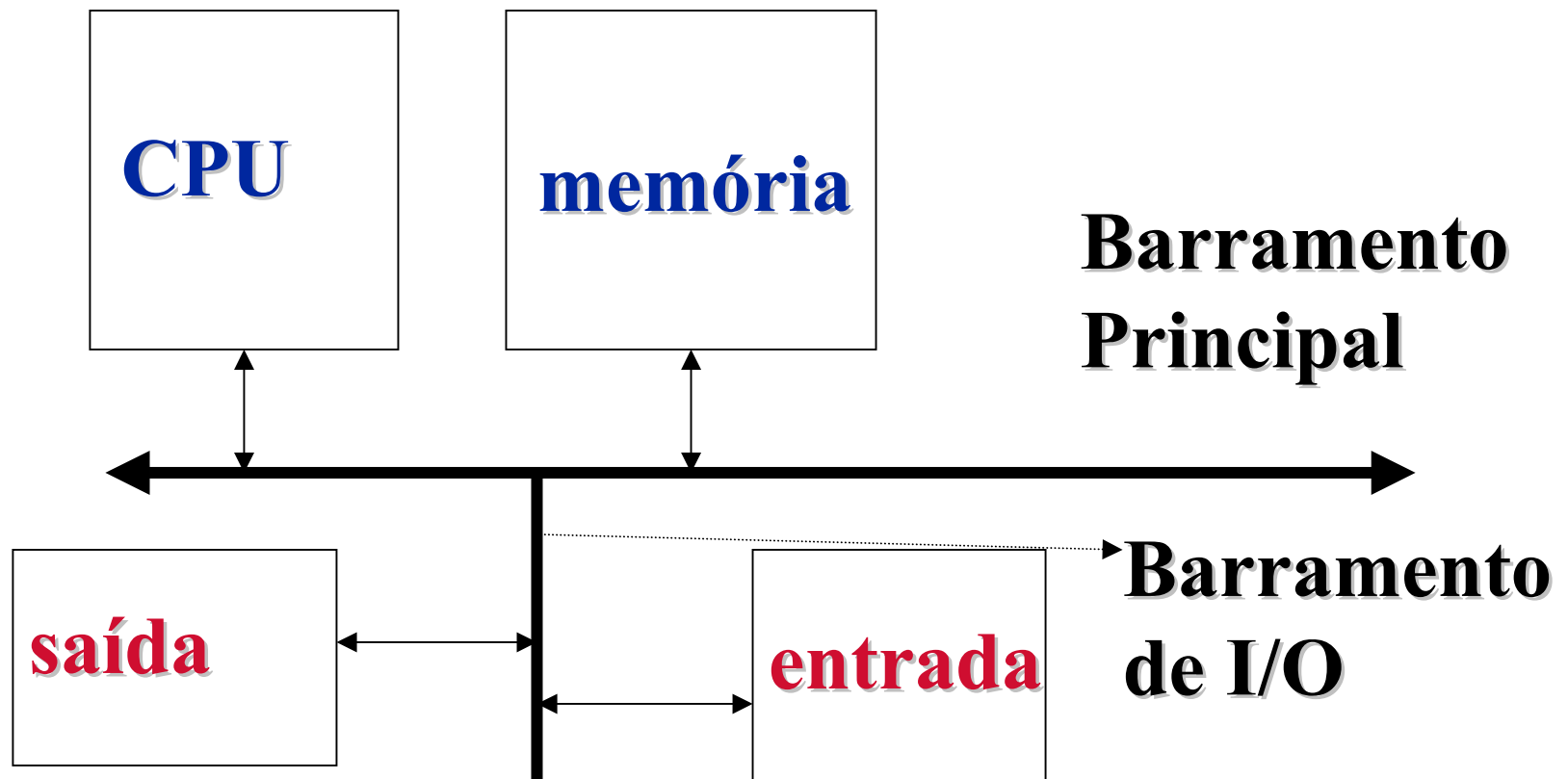


Os primeiros Computadores Eletrônicos:
Em 1944, von Neumann foi convidado a participar do projeto. Nesta época o grupo discutia como armazenar os programas para ser processados. Von Neumann escreveu um artigo sobre o trabalho chamando o computador de EDVA - Electronic Discrete Variable Automatic Computer. Deste fato, surgiu o termo famoso *a arquitetura de von Neumann.*

II - Arquitetura dos computadores modernos



II - Arquitetura dos computadores modernos



II - Arquitetura dos computadores modernos



Os primeiros Computadores Eletrônicos:

- **Em 1946, Maurice Wilkes da Universidade de Cambridge visitou a Moore School para assistir aulas sobre o desenvolvimento de computadores eletrônicos. Voltando para Cambridge decidiu criar um projeto semelhante, e criou o EDSAC (Electroni Delay Storage Automic Calculator).**

II - Arquitetura dos computadores modernos



Os primeiros Computadores Eletrônicos:

O EDSAC foi o primeiro computador eletrônico operacional quanto ao armazenamento de programas.

- Konrad Zuse na Alemanha no final dos anos 30 e princípios dos anos 40 desenvolveu um computador programável.**
- Outra iniciativa foi o Colossus desenvolvido pelos ingleses durante a II Guerra.**

II - Arquitetura dos computadores modernos



Eckert and Muchly formaram um empresa em 1947 para a construção do primeiro computador comercial, o Binac. Depois de problemas financeiros, estes venderam a Remington-Rand que colocou no mercado o UNIVAC I (Universal Automatic Computer). O número de 48 sistemas foram construídos e o custo do primeiro em 1958 foi de US\$ 1.000.000 .

II - Arquitetura dos computadores modernos



A IBM estava no mercado de escritórios, mas não antes de 1950 decidiu investir na construção do seu primeiro computador, IBM/701 (1952). Só em 1964, num comunicado surpreendente para a época anunciou o lançamento do System/360. Um máquina que podia variar em sua configuração e preço.

II - Arquitetura dos computadores modernos



A Digital por volta de 1965 começa a comercializar o PDP-8, que foi o primeiro *minicomputador* do mercado. Este computador foi uma boa notícia para o mercado de usuários, uma vez que esta máquina podia ser comprada por US\$ 20.000. Somente em 1971 a Intel apresentou o primeiro microprocessador do mercado, o Intel 4004.

II - Arquitetura dos computadores modernos



Em 1963 Seymour Cray anunciou o primeiro *supercomputador*, o *CDC 6600*. Em 1976, Cray já na sua empresa anuncia a máquina mais rápida e cara do mundo, o *Cray-I*. Em 1996, a SGI (Silicon Graphics) compra a Cray Research o que indica a não existência de mais nenhuma empresa no mercado dedicada a construção de *supercomputadores*.

II - Arquitetura dos computadores modernos



Em 1977, a computação pessoal é alcançada através do *Apple II* de Steven Jobs e Steve Wozniak. Devido ao baixo custo, grande volume de armazenamento para a época e a alta confiabilidade estabeleceu-se a indústria dos computadores pessoais. Somente quatro anos depois, 1981, a IBM lança o IBM-PC com o processador Intel e o DOS da Microsoft.

II - Arquitetura dos computadores modernos



Devido a arquitetura aberta do IBM-PC, logo este microcomputador tornou-se padrão no mercado. A Apple ficou com um segundo lugar muito abaixo dos computadores IBM-PC compatíveis. Hoje em dia é verificado que o CD mais vendido no mundo é o CD do Sistema Operacional da Microsoft.

II - Arquitetura dos computadores modernos

(Fonte: Hennessy e Patterson)

Geração	Período	Tecnologia	Produto
I	1950-59	Tubos a vácuo	Computador
II	1960-68	Transistors	Computador baixo custo
III	1969-77	C. Integrados	Minis
IV	1978-	LSI e VLSI	PC e WS

II - Arquitetura dos computadores modernos

(Fonte: Museu do Computador - Boston)

Ano	Nome	Memória (k)	Preço (US\$)
51	Univac I	48	1.000.000
64	IBM /360	64	1.000.000
65	PDP-8	4	16.000
76	Cray I	32768	4.000.000
81	IBM PC	256	3.000
91	HP9000	16384	7.400
96	Intel Pro	16384	4.400

II - Arquitetura dos computadores modernos



É reconhecido na literatura e verificado no mercado, o fato de que novos projetos de computadores, com arquiteturas proprietárias, tornam-se a cada dia mais inviáveis economicamente. Mas de onde vem a inovação e o desempenho dos novos computadores ?

II - Arquitetura dos computadores modernos



Cientistas da computação têm trabalho no aumento do desempenho das taxas dos *clocks* dos processadores. Desta maneira, arquiteturas de processadores *CISCs* e *RISCs* têm inovado os projetos dos computadores modernos empregando técnicas :

- (1) inovativas quanto ao maior uso de software e
- (2) semelhantes à aquelas utilizadas em supercomputadores e mainframes.

II - Arquitetura dos computadores modernos



O que vem ser um computador com arquitetura CISCs ?

É um computador que emprega um processador com uma arquitetura conhecida como Complex Instruction Set Computer, ou seja um processador que utiliza complexas instruções de baixo nível de hardware (assembler) para o funcionamento do ambiente.

II - Arquitetura dos computadores modernos



O que vem ser um computador com arquitetura CISCs ?

Neste paradigma de projeto a inteligência do software é desconsiderada, ou seja quase tudo é efetuado a nível de assembler. *Supercomputadores e Mainframes* empregam este tipo de arquitetura.

II - Arquitetura dos computadores modernos



O que vem ser um computador com arquitetura CISCs ?

Um exemplo muito interessante de se notar é a empresa de microprocessadores *Intel*. Esta empresa usa esta tecnologia em seus processadores. Os processadores *Pentium* e o *P6* (este ainda começando a ser lançado no mercado) são exemplos de CPUs que empregam esta tecnologia CISC. Então por que RISC ?

II - Arquitetura dos computadores modernos



O que vem ser um computador com arquitetura CISCs ?

O processador *P7* da Intel lançado após o *P6* pode ilustrar uma possível resposta. Este processador emprega uma técnica mista, onde algumas instruções baseada na tecnologia *CISC* são incorporadas ao conjunto de instruções do processador.

II - Arquitetura dos computadores modernos

O que vem ser um computador com arquitetura CISCs ?

Item	286	386	486	Pentium	P6	P7
• Projeto	1978	1982	1986	1989	1990	1993
• MIPS	1	5	20	100	250	500
• Venda	1983	1986	1990	1994	1996	2000
• Instalação (milhões)	9,7	44,2	75	4.5	-	-

II - Arquitetura dos computadores modernos



O que vem ser um computador com arquitetura RISC ?

Nos anos 80 alguns projetos de processores, algumas vezes conhecidos como *orientados a linguagem*, foram estabelecidos por várias empresas. Esta abordagem foi denominada de *RISC (Reduce Instruction Set Computer)*.

II - Arquitetura dos computadores modernos



O que vem ser um computador com arquitetura RISC ?

O estágio de evolução das linguagens de programação e o baixo custo de memória podiam significar menos instruções de baixo nível (assembler). Exemplo de processadores RISCs são MIPS, Sun SPARC, HP PA-RISC, IBM PowerPC, DEC Alpha.

II - Arquitetura dos computadores modernos



O que vem ser um computador com arquitetura RISC ?

Como Patterson e Hennessy comentam, desde 1982 quase todos os novos *instruction sets* seguem a tecnologia *RISCs*.

II - Arquitetura dos computadores modernos



Conjunto de Instruções	Número Unidades
• 80x86	50.000.000
• MIPS	5.500.000
• PowerPC	3.300.000
• SPARC	700.000
• HP PA-RISC	300.000
• DEC Alpha	200.000

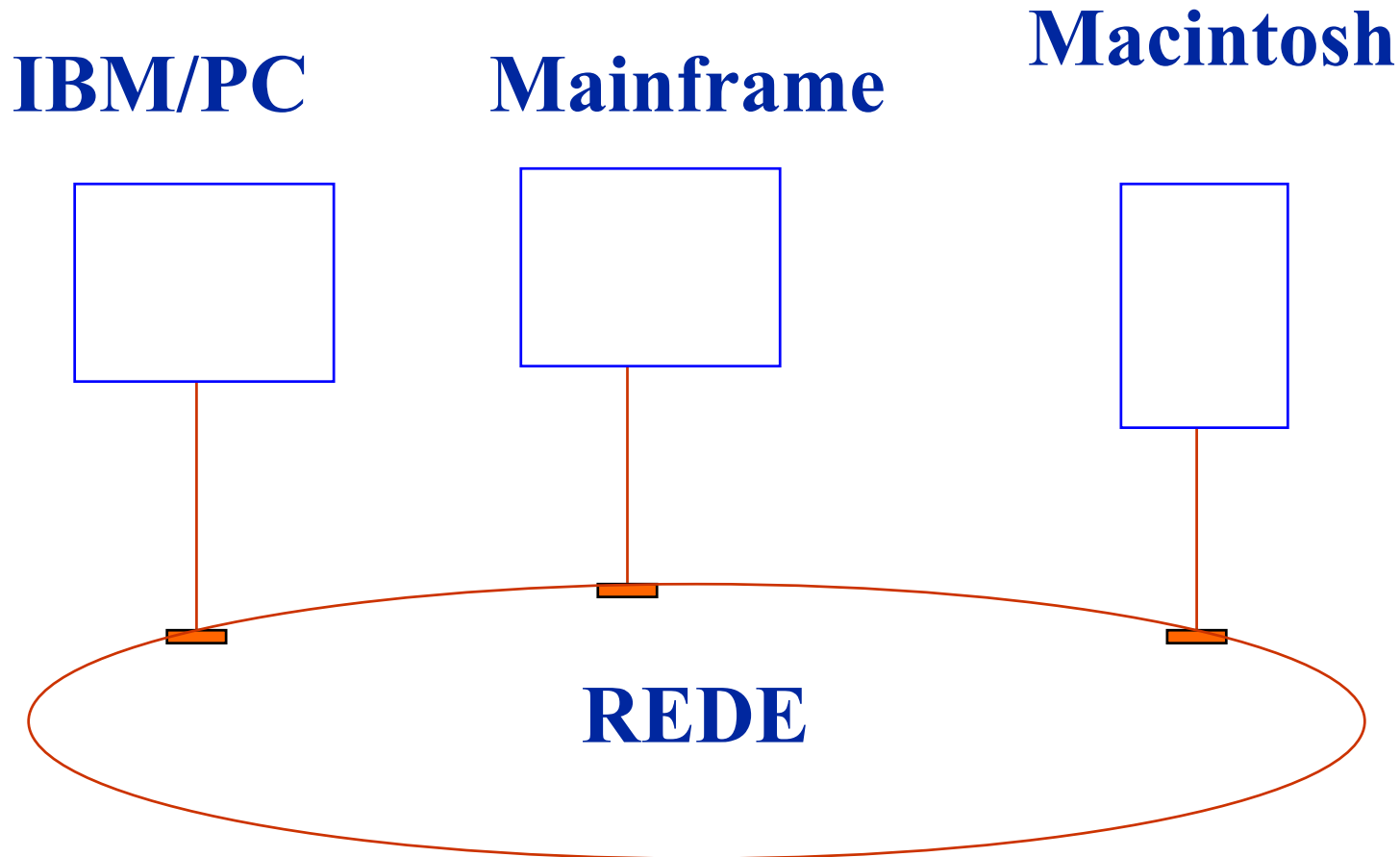
II - Arquitetura dos computadores modernos



Como poderíamos definir os seguintes sistemas computacionais?

- **Supercomputador**
- **Mainframe (grande porte)**
- **Minicomputador**
- **Workstation**
- **Microcomputador**

II - Arquitetura dos computadores modernos



II - Arquitetura dos computadores modernos



Rede de Interconexão (Interconnection Networks) são redes de altíssima velocidade projetadas para interconectar processadores e memórias numa arquitetura paralela. A ordem de grandeza da largura de banda é de *Gbytes/sec* e o retardo na casa dos *n segundos*.

II - Arquitetura dos computadores modernos

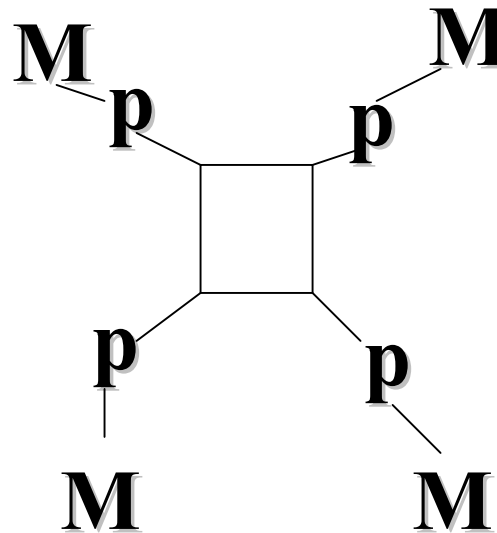
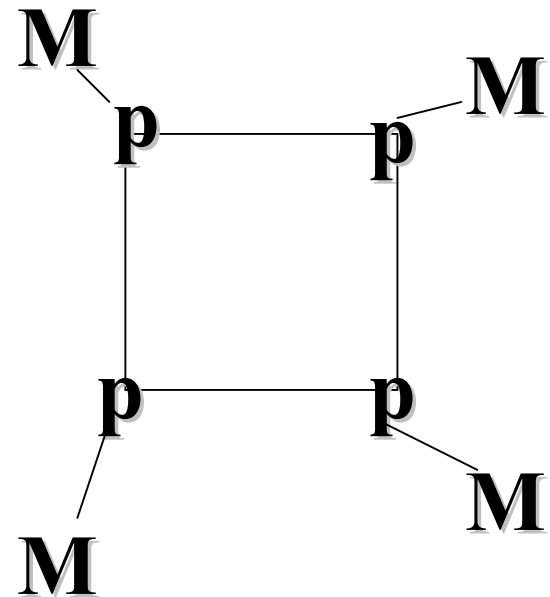


Redes de Interconexão podem ser configuradas de uma forma estática ou dinâmica. Topologias adotadas geralmente usadas são:

- *linear array, ring, star, tree, nearest-neighbor mesh, systolic array, completely connected, 3-cube, 4-cube*

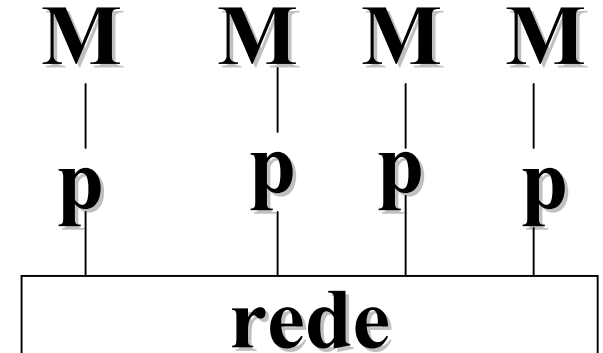
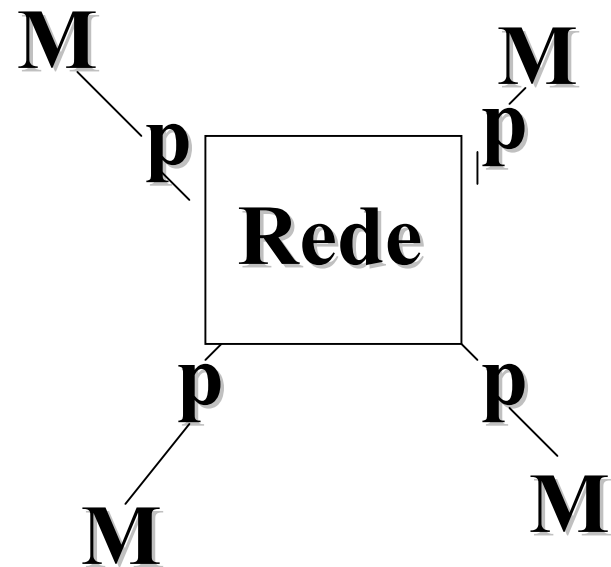
II - Arquitetura dos computadores modernos

⌘ Redes de Interconexão



II - Arquitetura dos computadores modernos

⌘ Redes de Interconexão



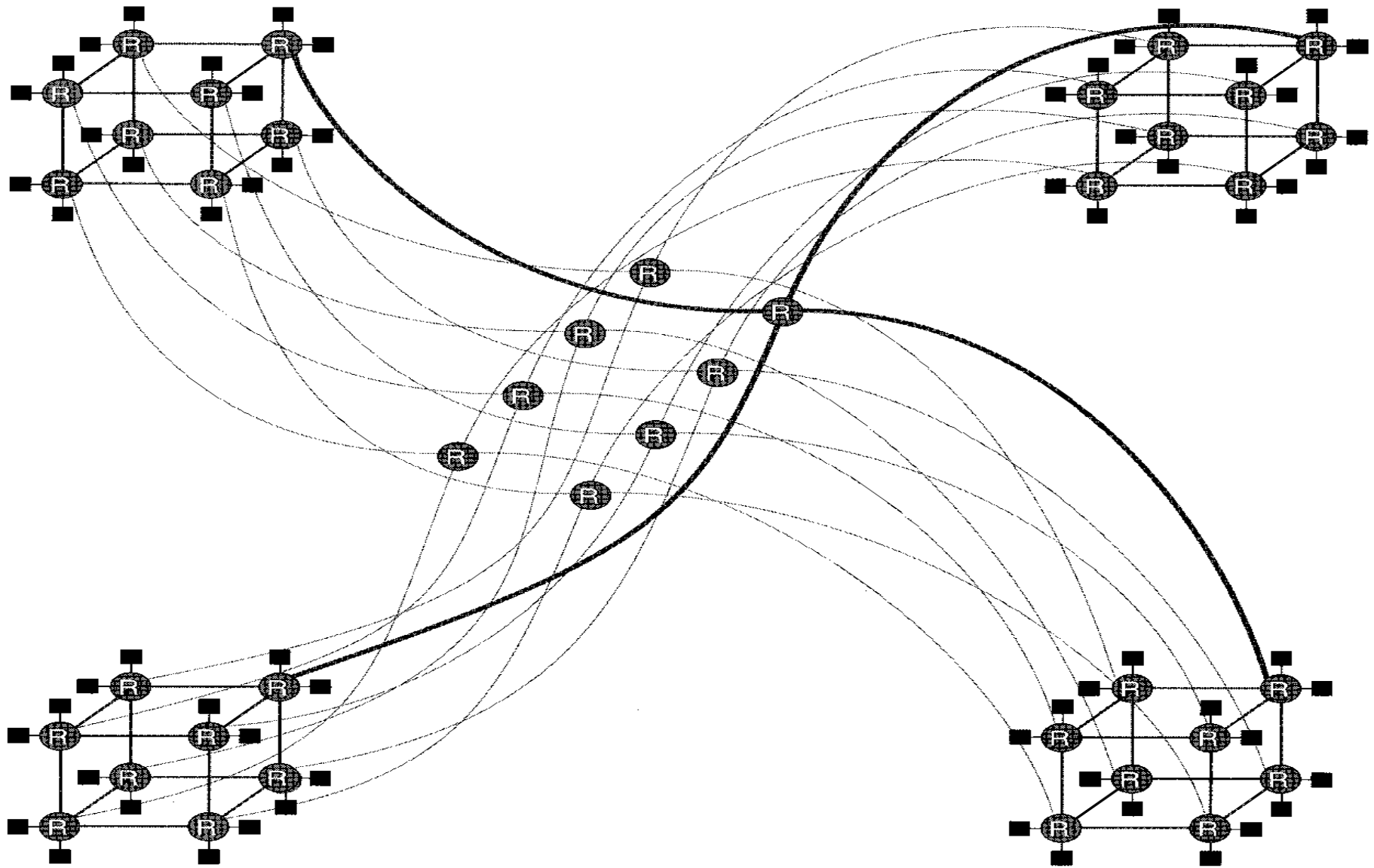


Figure 2-20 128-processor Cray Origin2000 System Topology
Using the Cray Meta Router

Conteúdo



I- Introdução aos princípios de comunicação

II - Arquitetura dos Computadores Modernos

III - Padrões dos Meios Físicos das Redes Locais (LANs), Metropolitanas(MANs) e o padrão IEEE.

III - Os padrões das LANS e MANS



As redes de computadores são classificadas como:

- **LAN (Local Área Network) - redes locais.**
- **MAN (Metropolitan Área Network) - redes metropolitanas.**
- **WAN (Wide Área Network) - redes globais ou geograficamente distribuídas.**

III - Os padrões das LANS e MANS



*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 velocidade implementada pela rede no fluxo de dados (exemplo: 10, 16 ou 100Mbps).*

III - Os padrões das LANS e MANS

O que são *protocolos de comunicação* ?

Conjunto de regras que permitem o estabelecimento 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.

III - Os padrões das LANS e MANS



Topologia - é o termo empregado para descrever a maneira pela qual os equipamentos estão interligados. O termo *topologia física* refere-se a interligação física, enquanto que *topologia lógica* descreve como a rede funciona (exemplo Token-Ring).

III - Os padrões das LANS e MANS

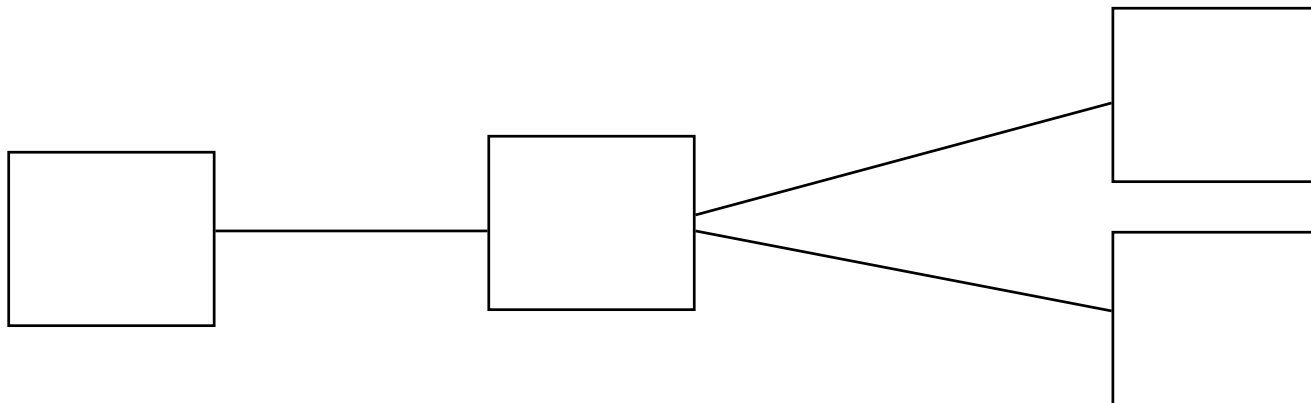


“A topologia de uma rede de comunicação refere-se à forma como os enlaces físicos e os nós de comutação estão organizados, determinado os caminhos físicos existentes e utilizáveis entre quaisquer pares de estações conectadas a essa rede.” (Soares, Lemos e Colcher)

III - Os padrões das LANS e MANS

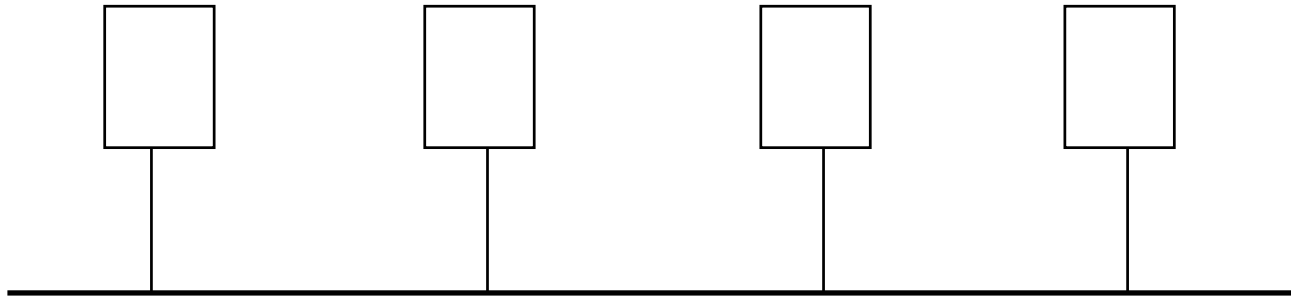
As linhas de comunicação numa rede, podem ser interconectadas das seguintes formas:

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



III - Os padrões das LANS e MANS

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



III - Os padrões das LANS **e MANS**



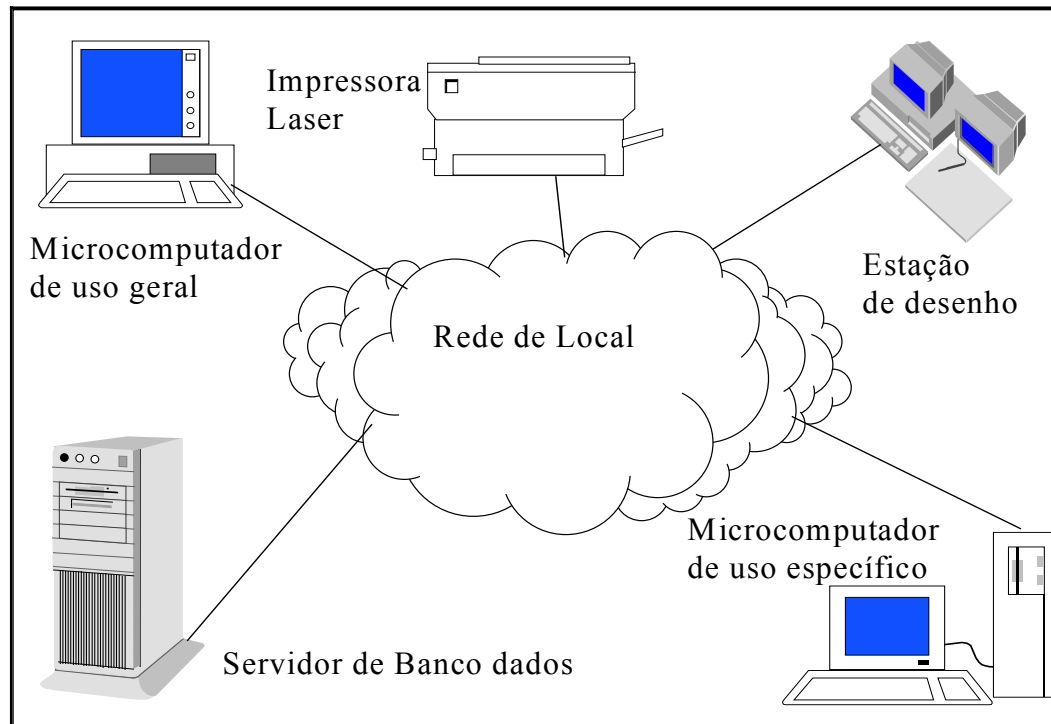
Vamos abordar as topologias adotadas nas redes locais. Vamos definir formalmente LAN e MAN, além de conhecer o funcionamento das topologias.

III - Os padrões das LANS e MANS



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.

III - Os padrões das LANS e MANS

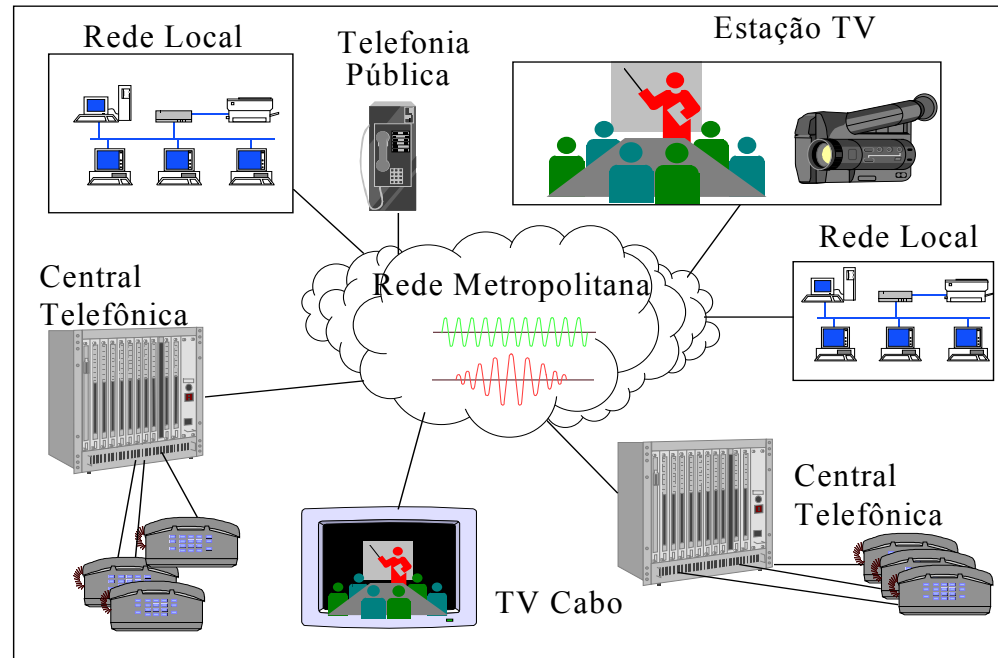


III - Os padrões das LANS e MANS



Redes Metropolitanas, ou MANs (Metropolitan Áreas 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.

III - Os padrões das LANS e MANS



III - Os padrões das LANS **e MANS**



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

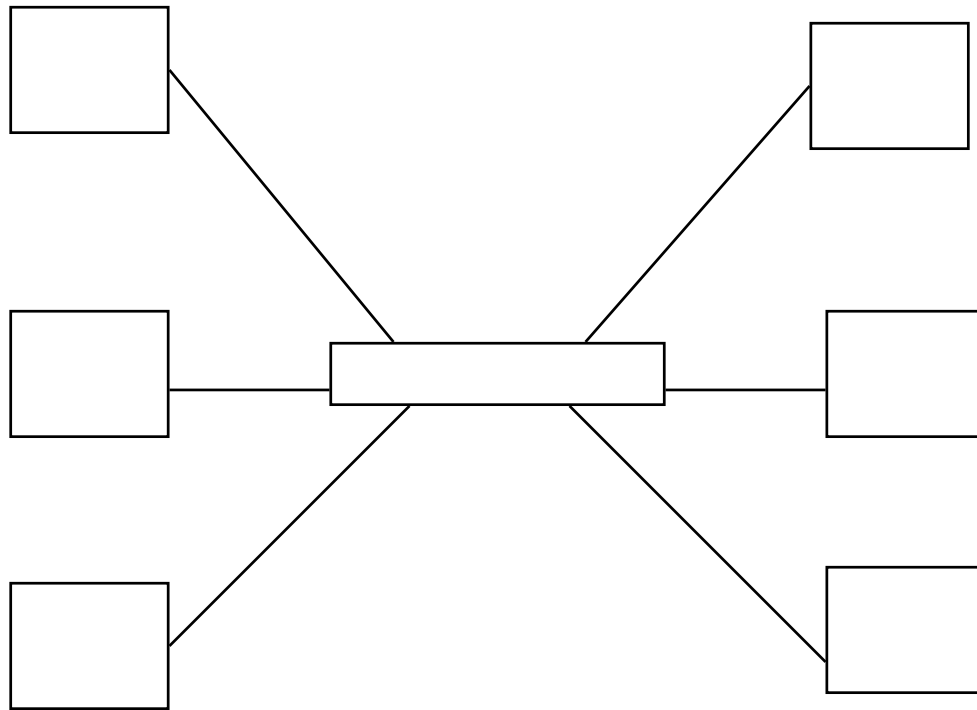
Devido a derivação da tecnologia de redes da área de telecomunicação, a topologia em estrela foi a primeira implementação de rede projetada e implementada.

III - Os padrões das LANS **e MANS**



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*.

III - Os padrões das LANS e MANS



Topologia Estrela

III - Os padrões das LANS e MANS



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.

III - Os padrões das LANS e MANS



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.**

III - Os padrões das LANS e MANS



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.**

III - Os padrões das LANS e MANS



Desvantagens da topologia estrela :

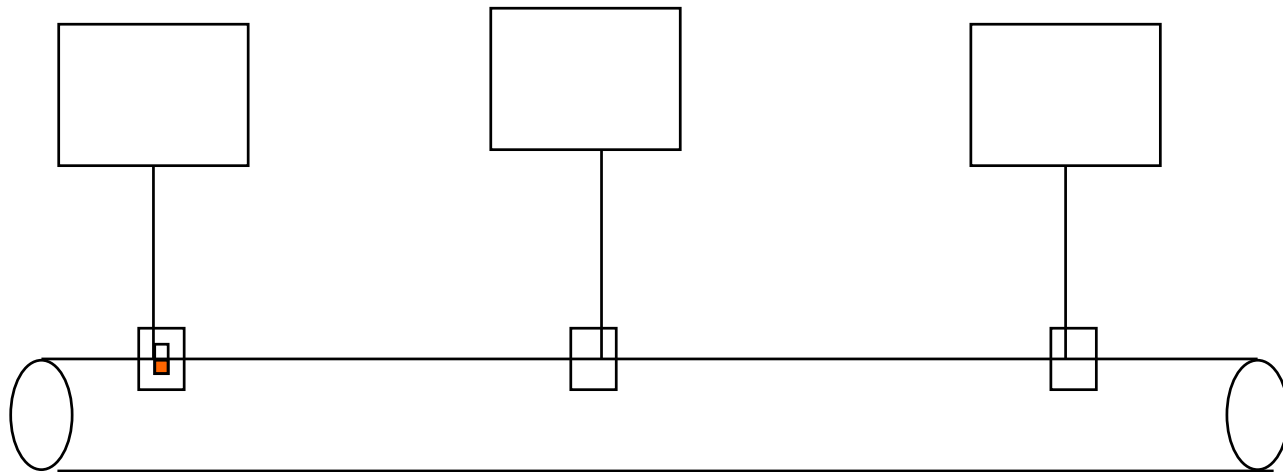
- ponto único de falha (concentrador).**
- como a conexão é ponto-a-ponto, custo mais elevado da estrutura de cabeamento/conexões.**
- no caso de uma rede grande, necessidade de um (ou mais) concentrador(es) para redirecionamento de mensagens.**

III - Os padrões das LANS e MANS



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.

III - Os padrões das LANS e MANS



Topologia de Barra

III - Os padrões das LANS e MANS



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.

III - Os padrões das LANS e MANS



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.**

III - Os padrões das LANS e MANS



Desvantagens da topologia em barra :

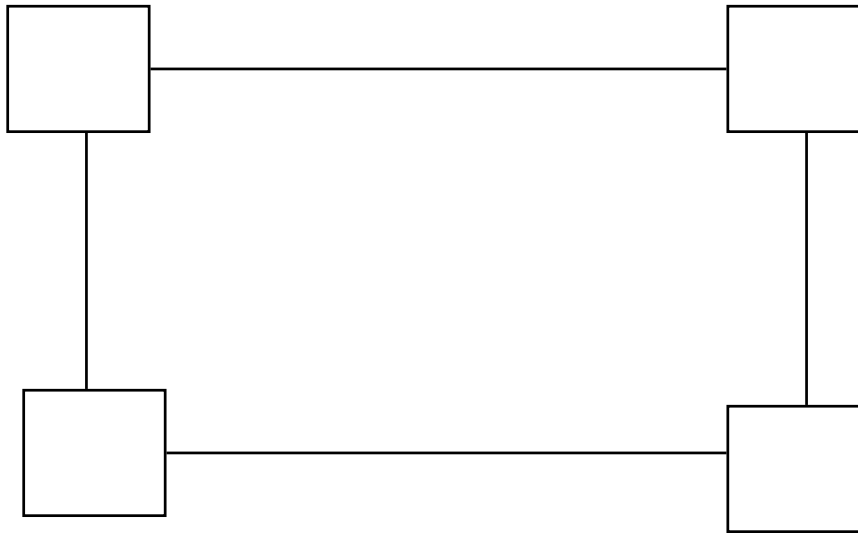
- aumento de *nós* leva a um aumento crescente do número de colisões na rede.**
- aumento de *nós* leva a um aumento crescente de erro de sinal na rede (problema de placas e conexões).**
- gerência física da rede.**

III - Os padrões das LANS **e MANS**



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.

III - Os padrões das LANS e MANS



Topologia Anel

III - Os padrões das LANS e MANS



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.**

III - Os padrões das LANS e MANS



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.**

III - Os padrões das LANS e MANS



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.

III - Os padrões das LANS e MANS

Os meios físicos de transmissão mais empregados nas redes são os cabos de par trançado, coaxial e fibra ótica. O ar pode ser usado como meio físico de transmissão nas redes de computadores, através do uso de sinais de infravermelho, micro-ondas e radio. Todavia, estes dispositivos de transmissão (geralmente) implicam em custos elevados.

III - Os padrões das LANS e MANS

Par trançado -a transmissão das propriedades elétricas neste tipo de cabo tende a ser mais constante, quando comparados com cabos paralelos.

Outras propriedades :

- largura de banda de Mbps para distâncias curtas
- bastante susceptível a ruídos
- fácil de manuseio, ou seja instalação fácil.
- menor custo por comprimento.

III - Os padrões das LANS e MANS

Cabo coaxial - condutor cilíndrico interno coberto por tubo metálico e separado por material dielétrico. Outras características são :

- condutor interno (geralmente) utiliza cobre.
- tubo metálico tem função de condutor de retorno e blindagem eletrostática.
- taxa de transmissão de dezenas de Mbps.
- custo > par trançado < facilidade de instalação.

III - Os padrões das LANS e MANS

Fibra ótica - filamento de sílica , onde a atenuação independe da frequência (até 16Gbps). Imune a interferência eletromagnética, utilização de conversores óticos-eletrônicos para *codificação e decodificação* de sinal. Custo por comprimento mais elevado quando comparado com cabos coaxiais e pares trançados. Os dois tipos de fibra mais usados são o *monomodo e multimodo*.

III - Os padrões das LANS e MANS

Monomodo : um único caminho para o sinal luminoso é utilizado na transmissão. O sinal usa codificação de laser. Estas fibras têm maior largura de banda e podem ser empregadas para longas distâncias.

Multimodo : vários caminhos para luz são usados, o uso de LEDs(Light-emitting diodes) são empregados para gerar a *luz*, logo esta fibra é mais barata.

III - Os padrões das LANS e MANS

Padrões do Nível Físico (IEEE 802.3)

- **10Base2 (coaxial flexível)**
- **10Base5 (coaxial grosso)**
- **10BaseF (fibra)**
- **10BaseT (par trançado)**

III - Os padrões das LANS e MANS



Protocolos - são um conjunto de regras que determinam como ocorrerá o processo de comunicação. Assim, inúmeros protocolos existem para a comunicação entre computador-meio físico, computador-rede de comunicação, computador-computador e computador-impressora.

Exemplos de protocolos são CSMA/CD, X25, TCP/IP, UDP/IP, NFS, NetBios, etc.

III - Os padrões das LANS e MANS



Pilha de protocolos: protocolos são organizados em pilhas de funções, ou seja cada nível na pilha de um certo protocolo é caracterizado por um protocolo que executa um serviço para o protocolo acima. Cada nível de protocolo se comunica com o outro nível acima ou abaixo através de entidades denominadas de interface. Todavia, na comunicação ponto-a-ponto cada nível só vê seu nível correspondente no outro computador.

III - Os padrões das LANS **e MANS**



Protocolos proprietários são aqueles implementados por fabricantes na comunicação de sua redes fechadas. Exemplos de protocolos proprietários são o SNA da IBM, DNA da Dec, Netware da Novell.

III - Os padrões das LANS **e MANS**



Protocolos abertos são caracterizados por suas definições estabelecidas por órgãos normativos (exemplo IEEE, CCITT e ISO) e são projetados independentes de fabricantes

Clássicos exemplos são os protocolos da IEEE, tal como o IEEE 802.x, a ISO/OSI 8802.x e o TCP/IP.

III - Os padrões das LANS e MANS

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. Esta conclusão tem levado organismos internacionais a propor uma série de padrões para os protocolos. Vamos a seguir conhecer mais sobre o ISO/OSI, TCP/IP e arquitetura IEEE.

III - Os padrões das LANS e MANS

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.

III - Os padrões das LANS e MANS

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

MODELO ISO/OSI

É uma padronização de níveis funcionais de protocolos de comunicação.

III - Os padrões das LANS **e MANS**



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.

III - Os padrões das LANS e MANS



<u>Camada</u>	<u>Descrição de algumas funções</u>
aplicação	prover serviços que suportam direto as aplicações.
apresentação	traduz formatos.
sessão	configura sessões.
transporte	garante a ligação nas conexões.
rede	roteamento de dados.
enlace	detecta e corrige erro de dados.
físico	especificação elétrica/mecânica.

III - Os padrões das LANS e MANS

TCP/IP

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

III - Os padrões das LANS e MANS

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.

III - Os padrões das LANS e MANS

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

III - Os padrões das LANS e MANS

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)**

III - Os padrões das LANS e MANS

Modelo TCP/IP

aplicação
transporte
internet
rede

ftp, telnet, nfs, xdr, rpc

tcp, udp

ip, icmp, arp, rarp

protocolos de hardware

III - Os padrões das LANS e MANS

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	

III - Os padrões das LANS e MANS



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

III - Os padrões das LANS e MANS

Comparando o modelo IEEE com OSI

OSI

IEEE

enlace	802.2 - Logical link control			
	802.1 - Internetworking			
	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

III - Os padrões das LANS e MANS



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 sequencia de quadros

III - Os padrões das LANS e MANS



4	aplicação	mensagem
3	transporte	pacote
2	Inter-rede	datagrama
1	Interface Rede	quadro

III - Os padrões das LANS e MANS

Modelo IEEE

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

<u>3</u>	Logical Link Control - LLC
<u>2</u>	Medium Access Control -MAC
<u>1</u>	Physical Layer - PHY

III - Os padrões das LANS e MANS

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

III - Os padrões das LANS e MANS

Modelo SNA

O Systems Network Architecture (SNA) Protocol foi desenvolvido pela IBM após 1974 para atender ao seu modelo hierarquico de rede. Os dispositivos da hierarquia eram os *mainframes*, *communication controllers*, *cluster controllers* e *terminais*.

III - Os padrões das LANS e MANS

ISO

Modelo SNA

<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		

III - Os padrões das LANS e MANS

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 (Inter-network Packet eXchange) é o protocolo principal.

III - Os padrões das LANS e MANS

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.

III - Os padrões das LANS e MANS

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 sequência de pacotes, gerência de sessão, tradução semântica e transferência de arquivos.

Conteúdo



IV-Dispositivos de interconexão de redes.

V - Arquitetura TCP/IP.

**VI - Redes de alta velocidade
(FDDI, ATM, Fast Ethernet, Myrinet).**

IV - Dispositivos de interconexão das redes



Visando a expansão das redes, existem vários dispositivos cujas funções possibilitam efetuar de maneira transparente para usuários e aplicações uma extensão do alcance da rede. Desta forma, vamos abranger este tópico conhecendo os hubs, repetidores, pontes (bridges), roteadores e gateways.

IV - Dispositivos de interconexão das redes

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.

IV - Dispositivos de interconexão das redes

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.

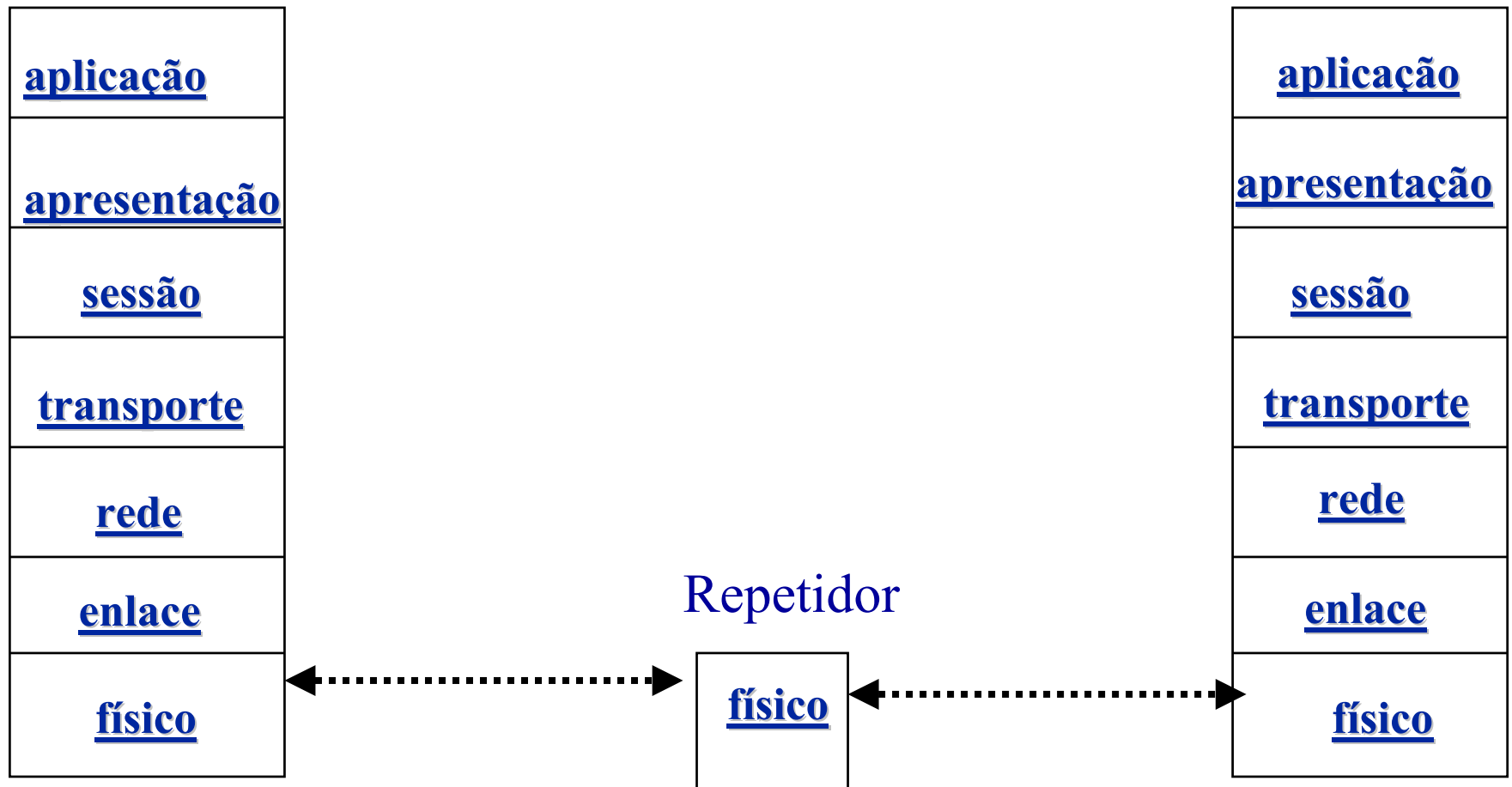
IV - Dispositivos de interconexão das redes

Ligação Inter-Redes

Repetidores -

São utilizados 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.

IV - Dispositivos de interconexão das redes



IV - Dispositivos de interconexão das redes

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;

IV- Dispositivos de Interconexão de Redes

Bridges Convencionais

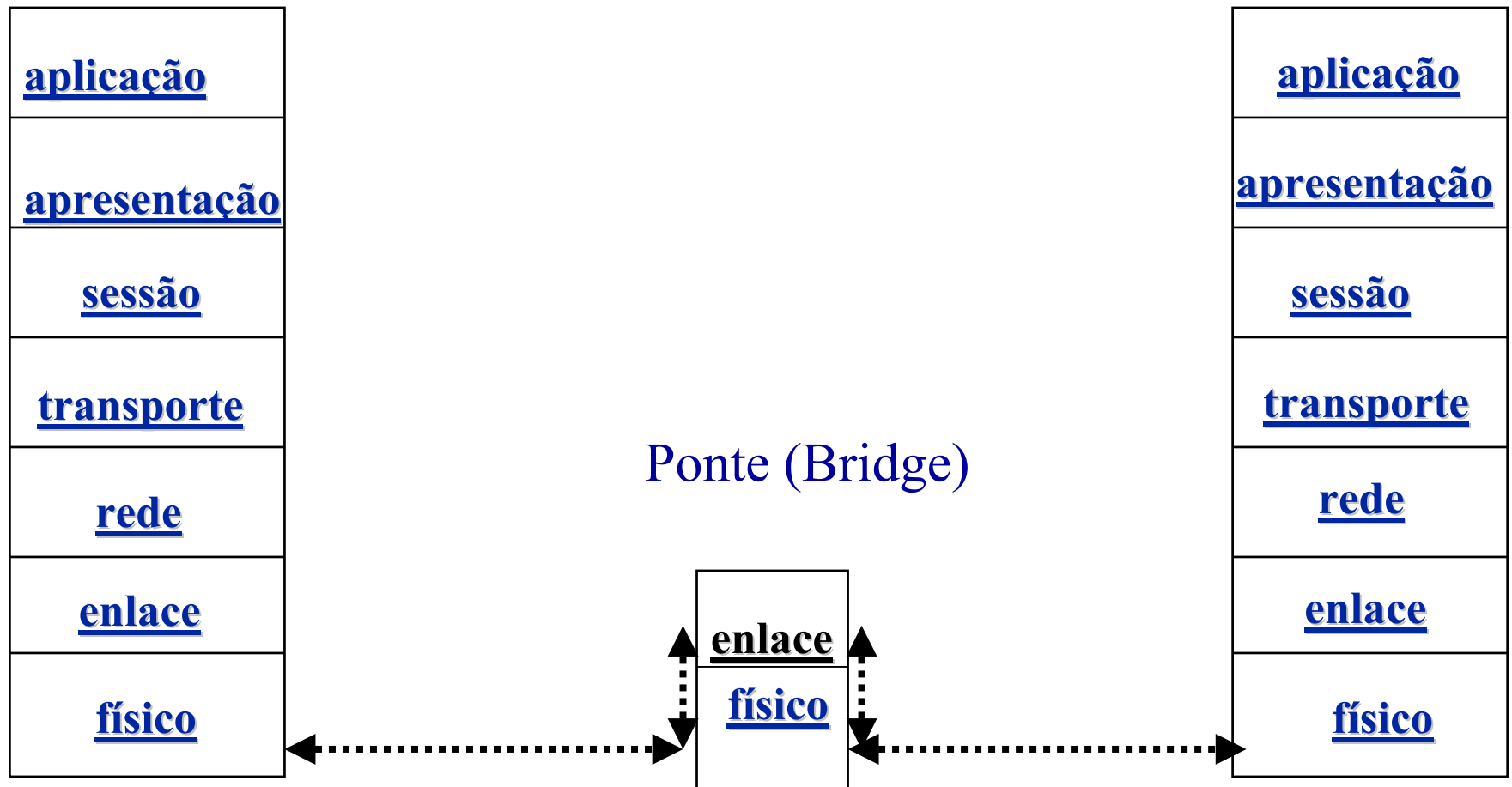
As *bridges convencionais* conectam segmentos de uma mesma tecnologia de rede. As *bridges* são usadas para *aumentar* a capacidade da rede, pois diferente dos *repetidores* estas selecionam/filtram os sinais entre os segmentos. Quando uma mensagem é por exemplo de um segmento A, este não é propagado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

IV- Dispositivos de Interconexão de Redes

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 .

IV - Dispositivos de interconexão das redes



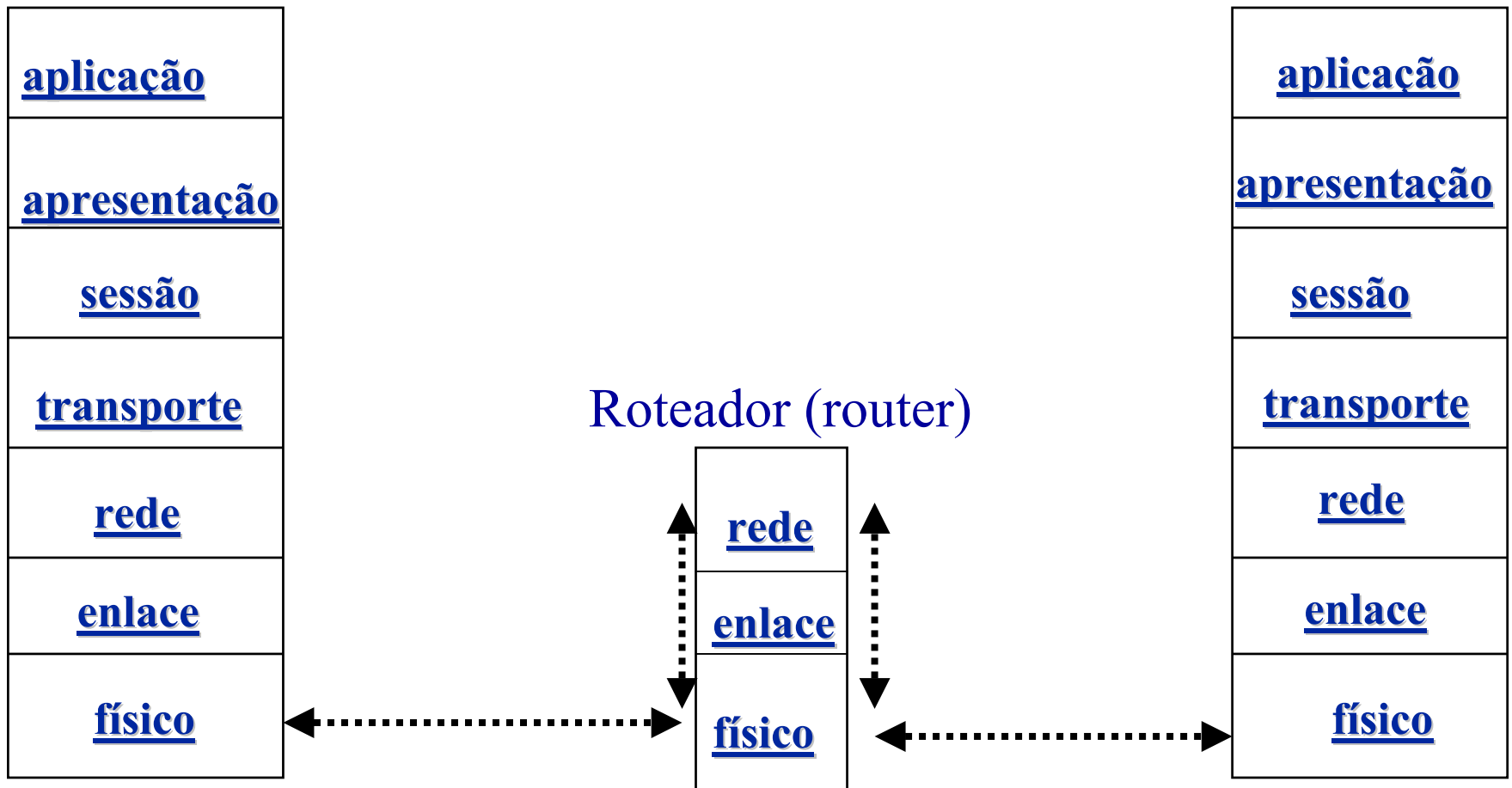
IV - Dispositivos de interconexão das redes

Ligação Inter-Redes

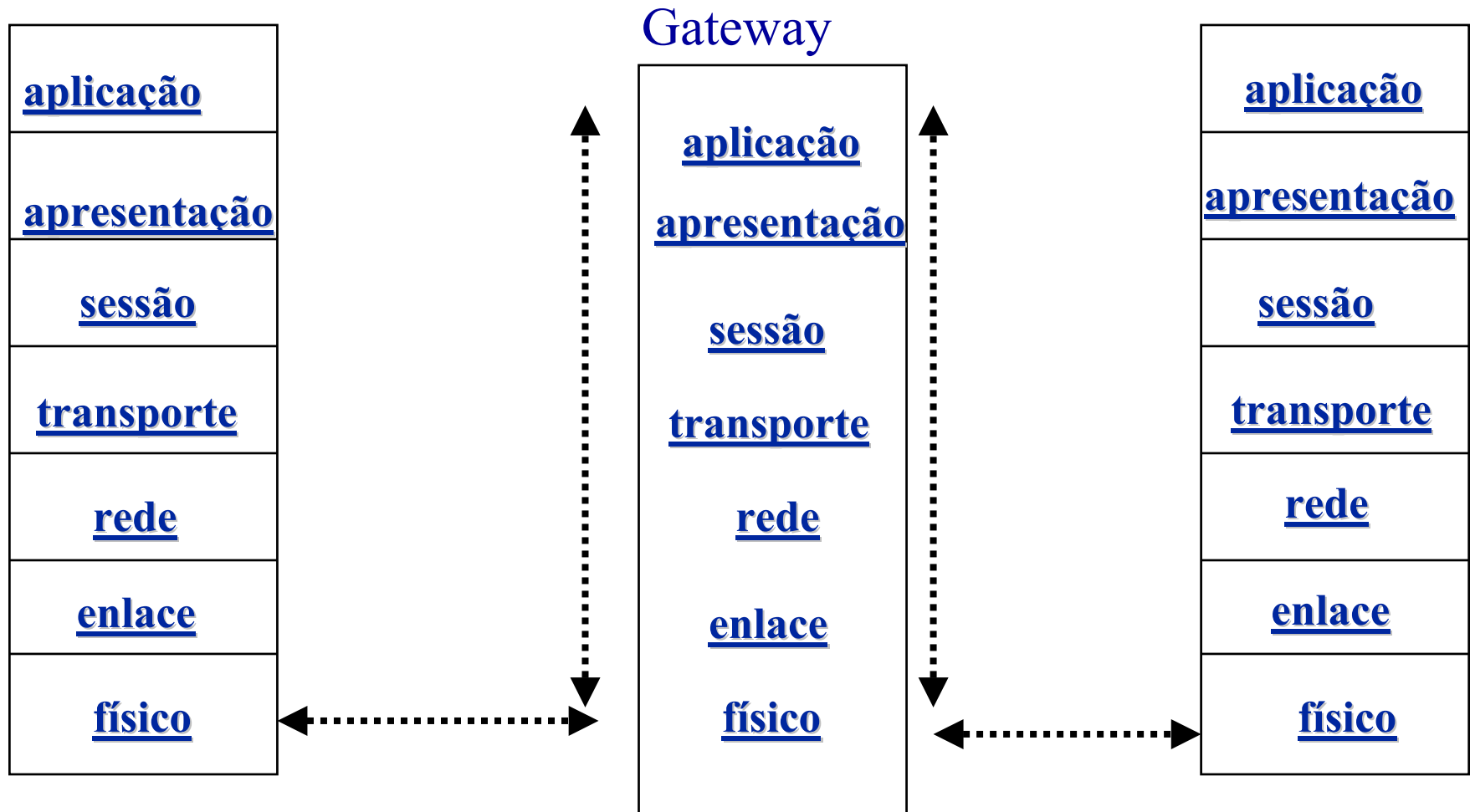
Roteadores (Routers)-

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.

IV - Dispositivos de interconexão das redes

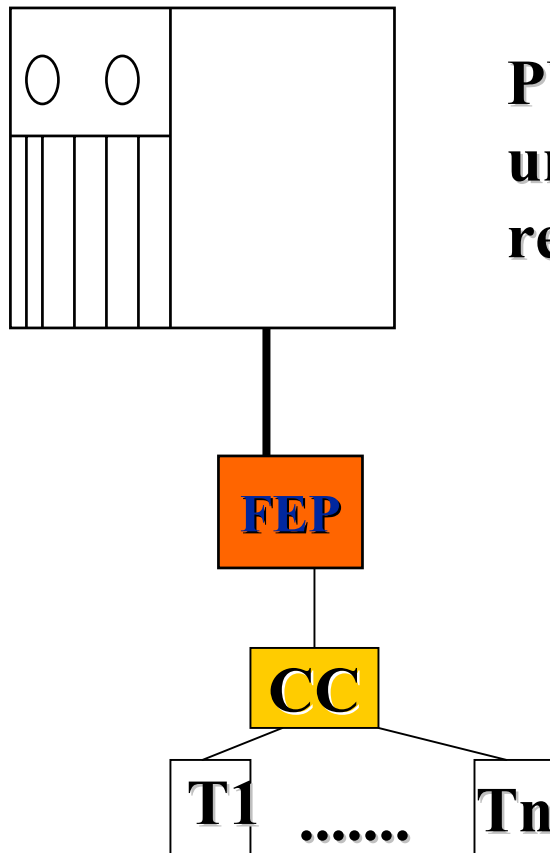


IV - Dispositivos de interconexão das redes



IV - Dispositivos de interconexão das redes

Exemplo - SNA/IBM



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

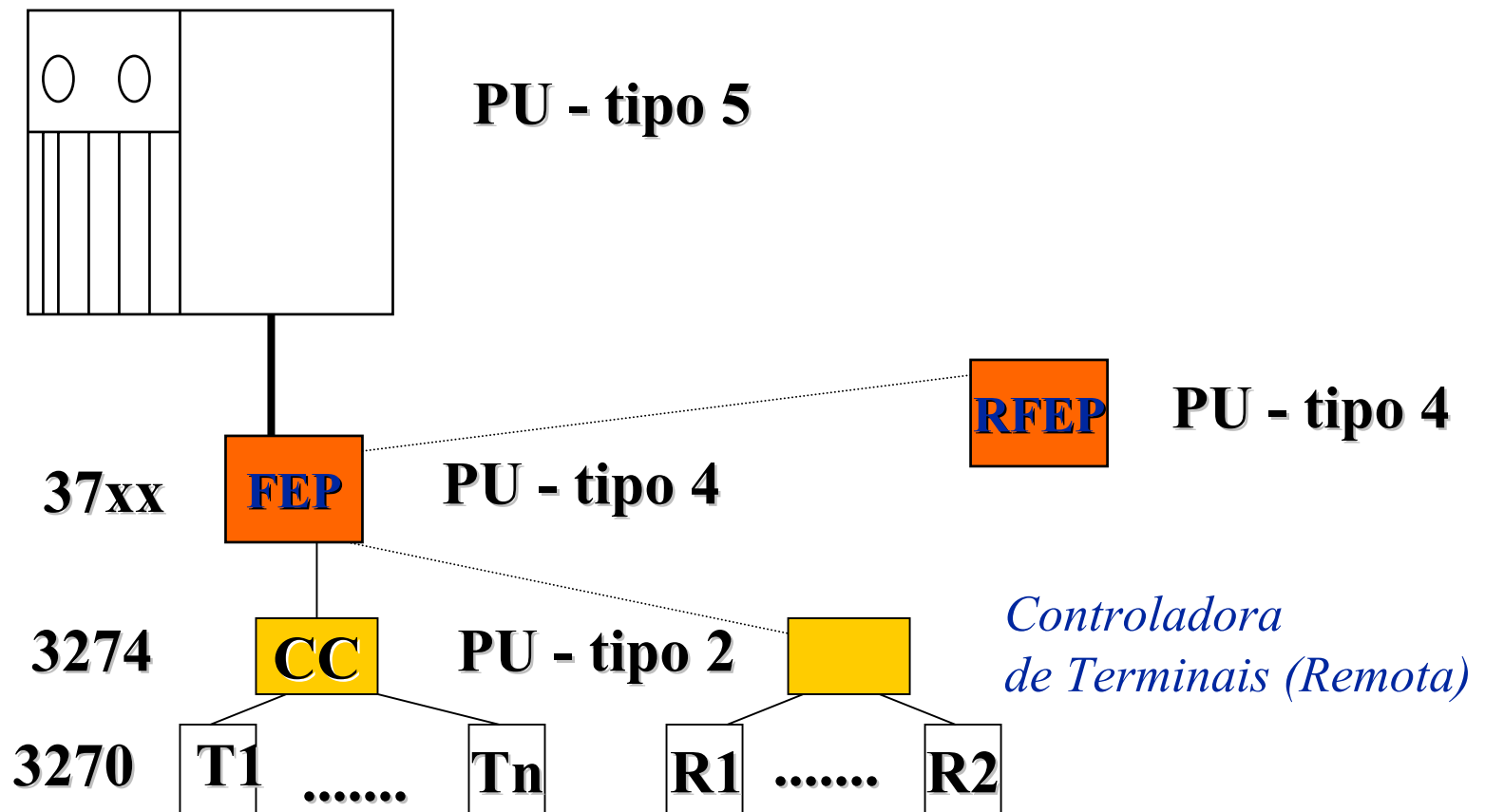
Controladora de Comunicação

Controladora de Terminais

Terminais

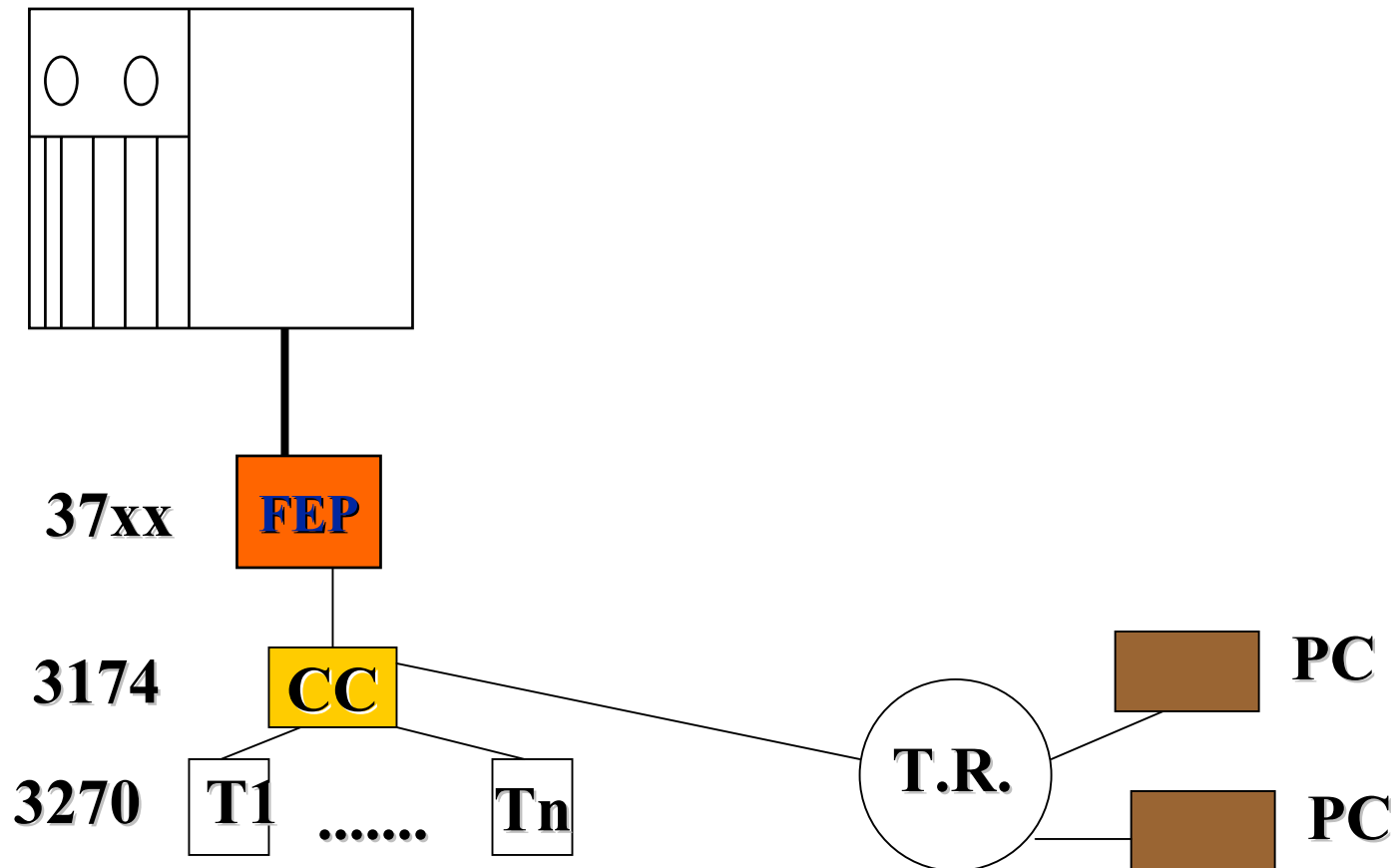
IV - Dispositivos de interconexão das redes

Exemplo - SNA/IBM



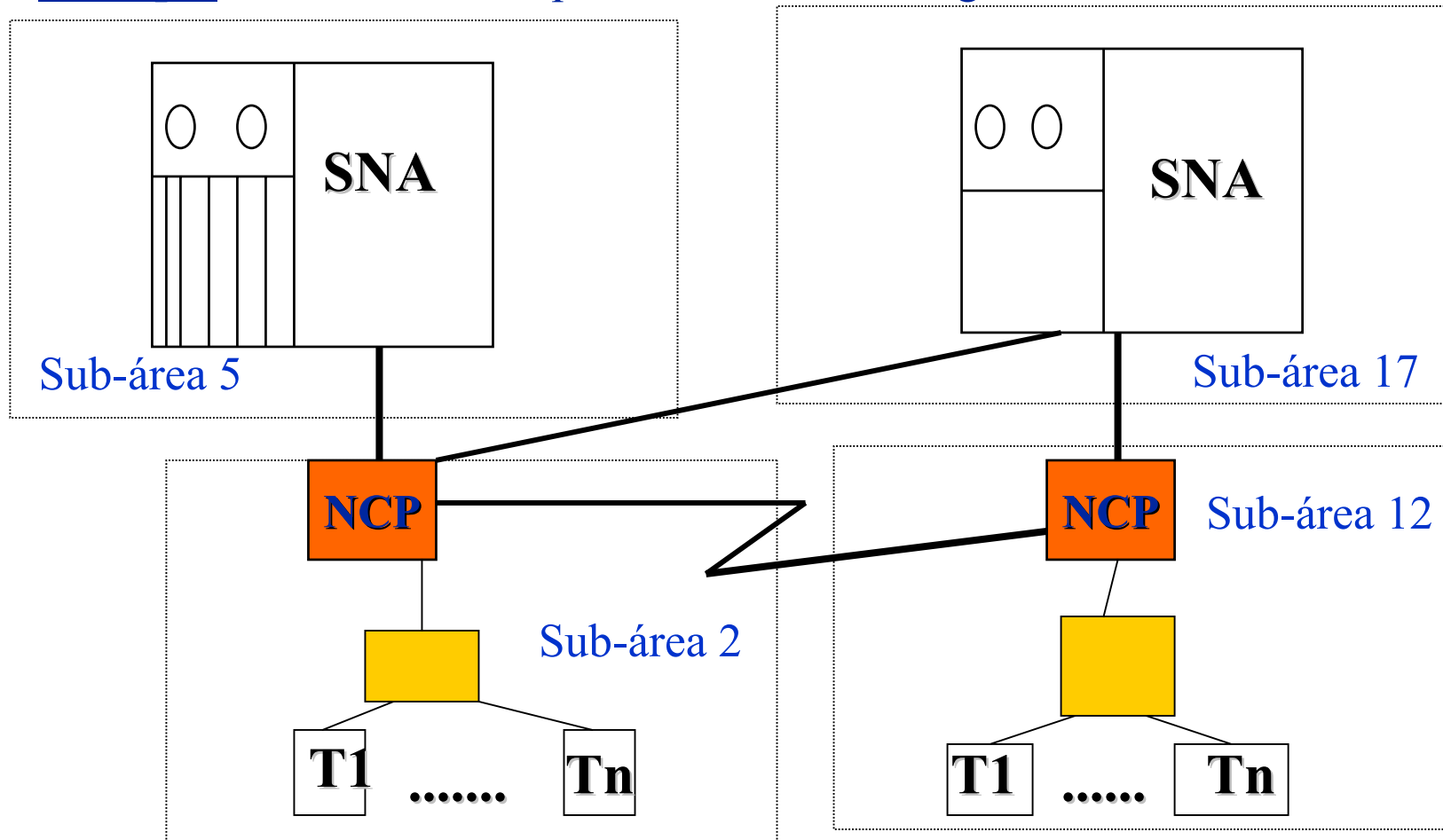
IV - Dispositivos de interconexão das redes

Exemplo - SNA/IBM



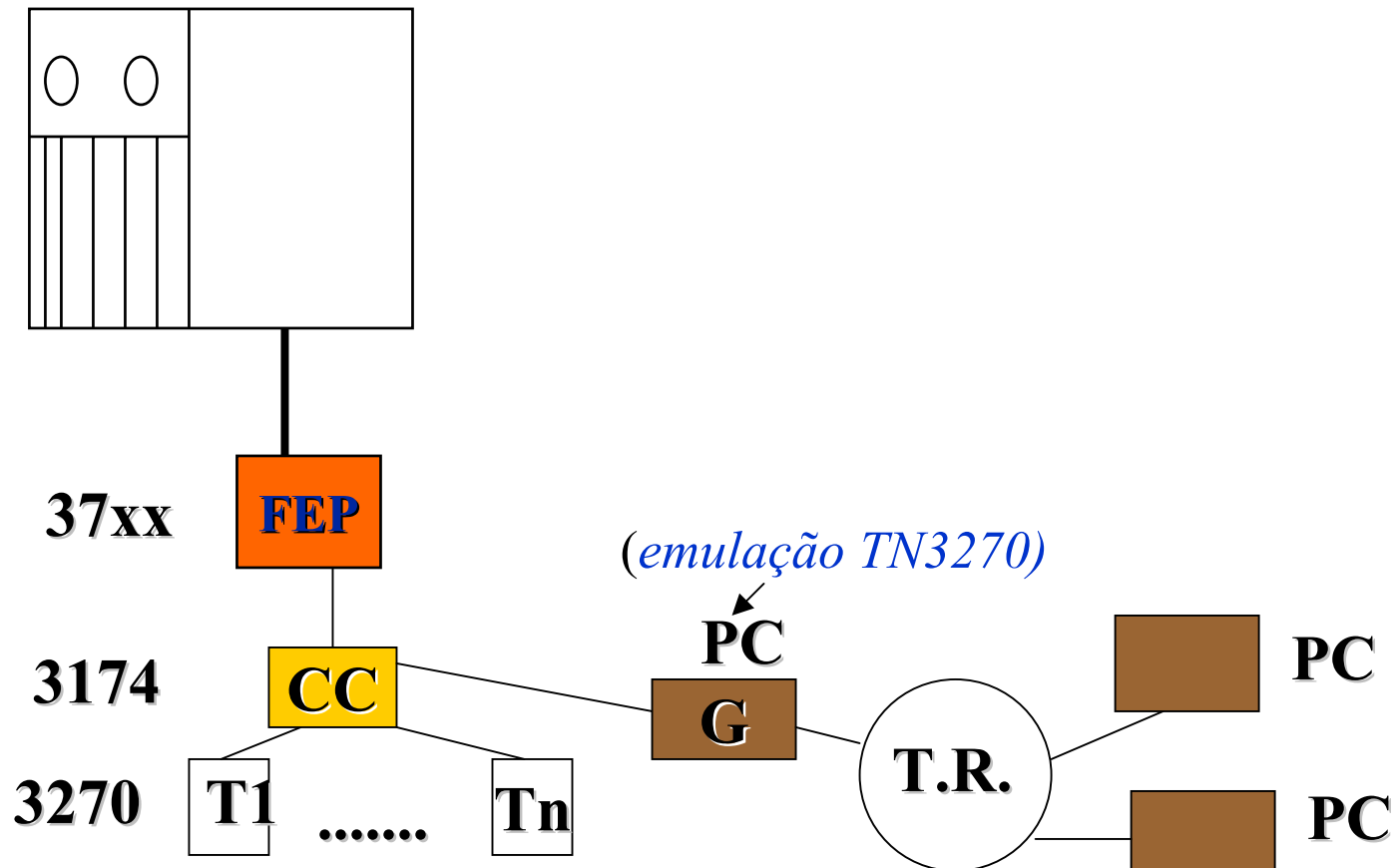
IV - Dispositivos de interconexão das redes

Exemplo - SNA/IBM e os possíveis Acessos Lógicos



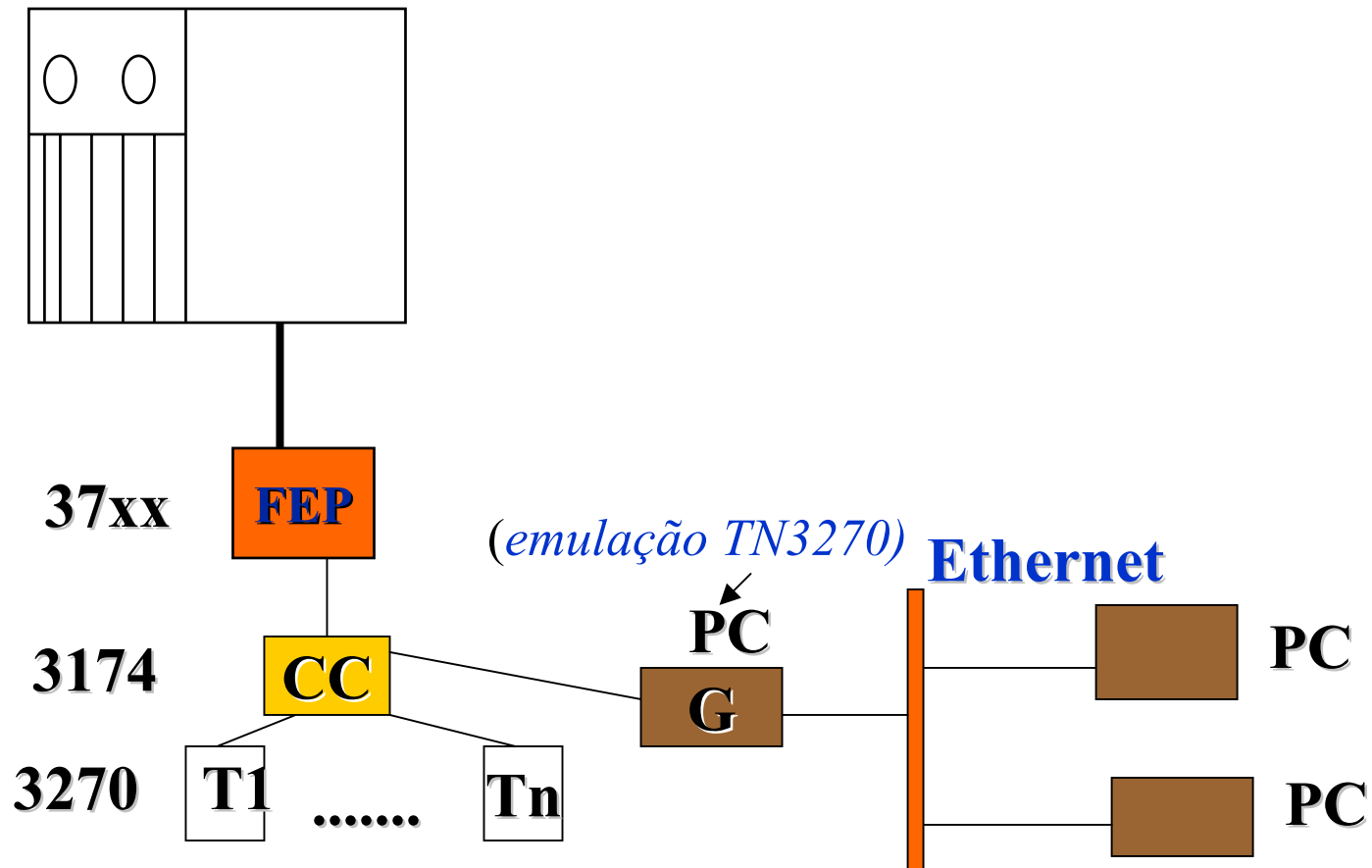
IV - Dispositivos de interconexão das redes

Exemplo - SNA/IBM



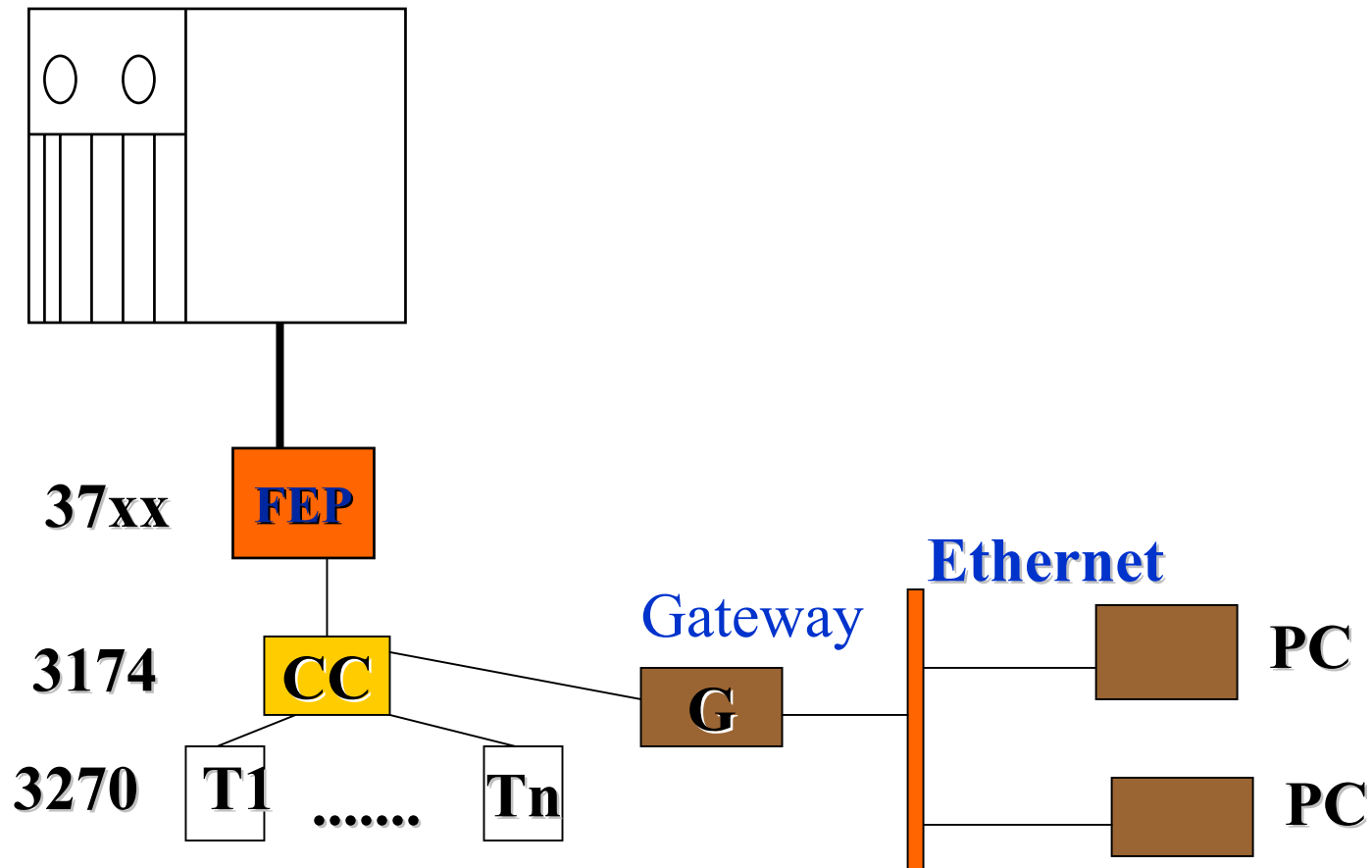
IV - Dispositivos de interconexão das redes

Exemplo - SNA/IBM e um Ambiente TCP/IP



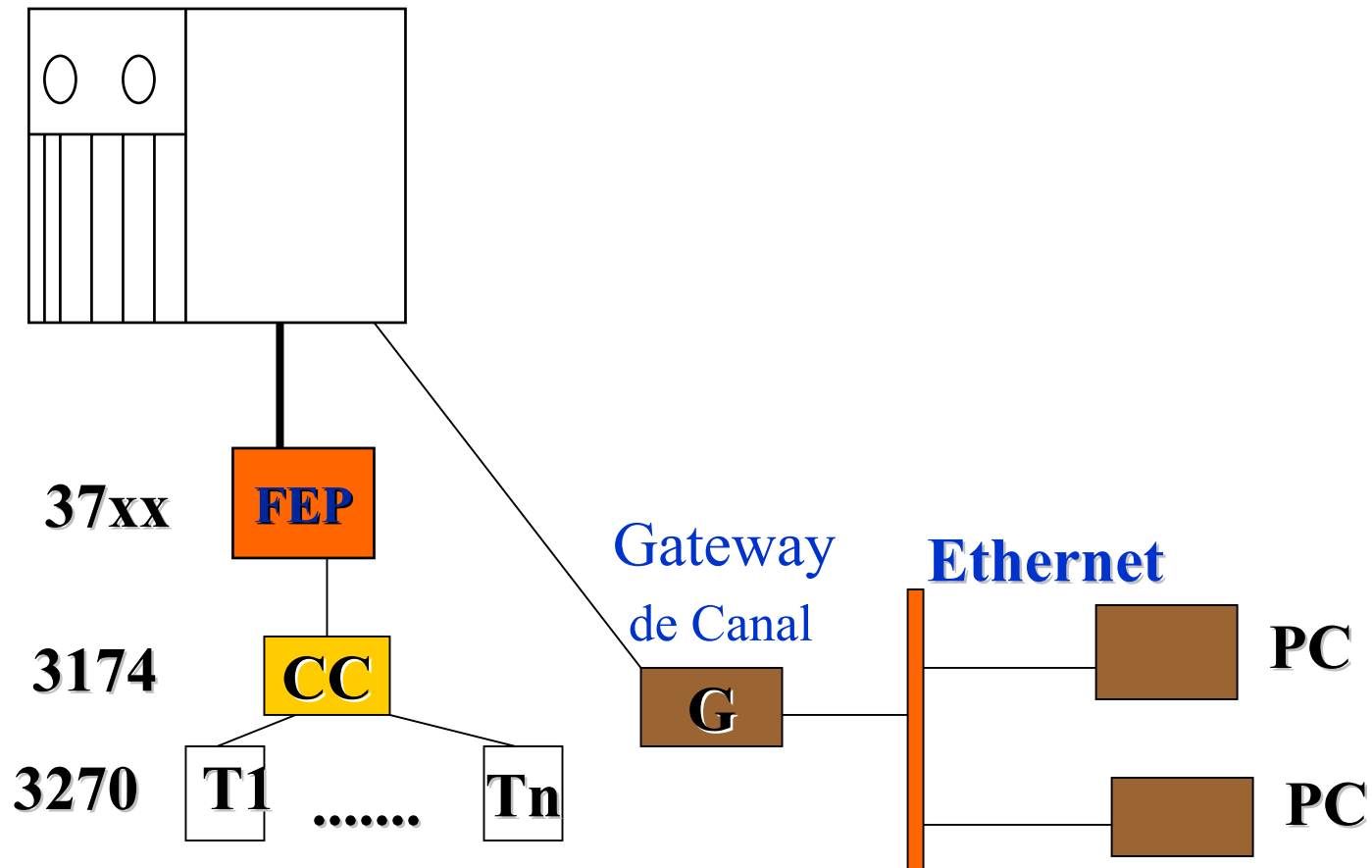
IV - Dispositivos de interconexão das redes

Exemplo - SNA/IBM e um Ambiente TCP/IP



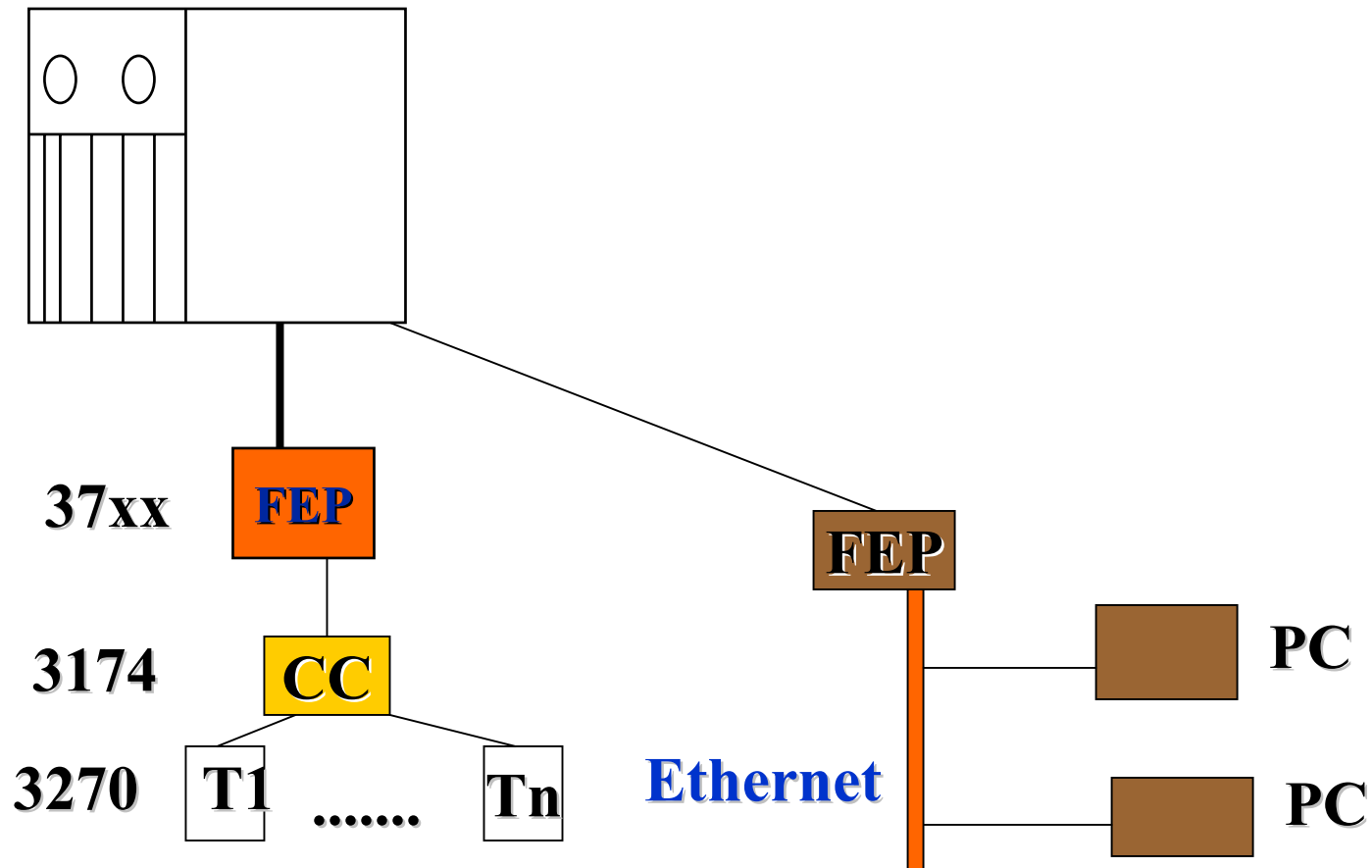
IV - Dispositivos de interconexão das redes

Exemplo - SNA/IBM e um Ambiente TCP/IP



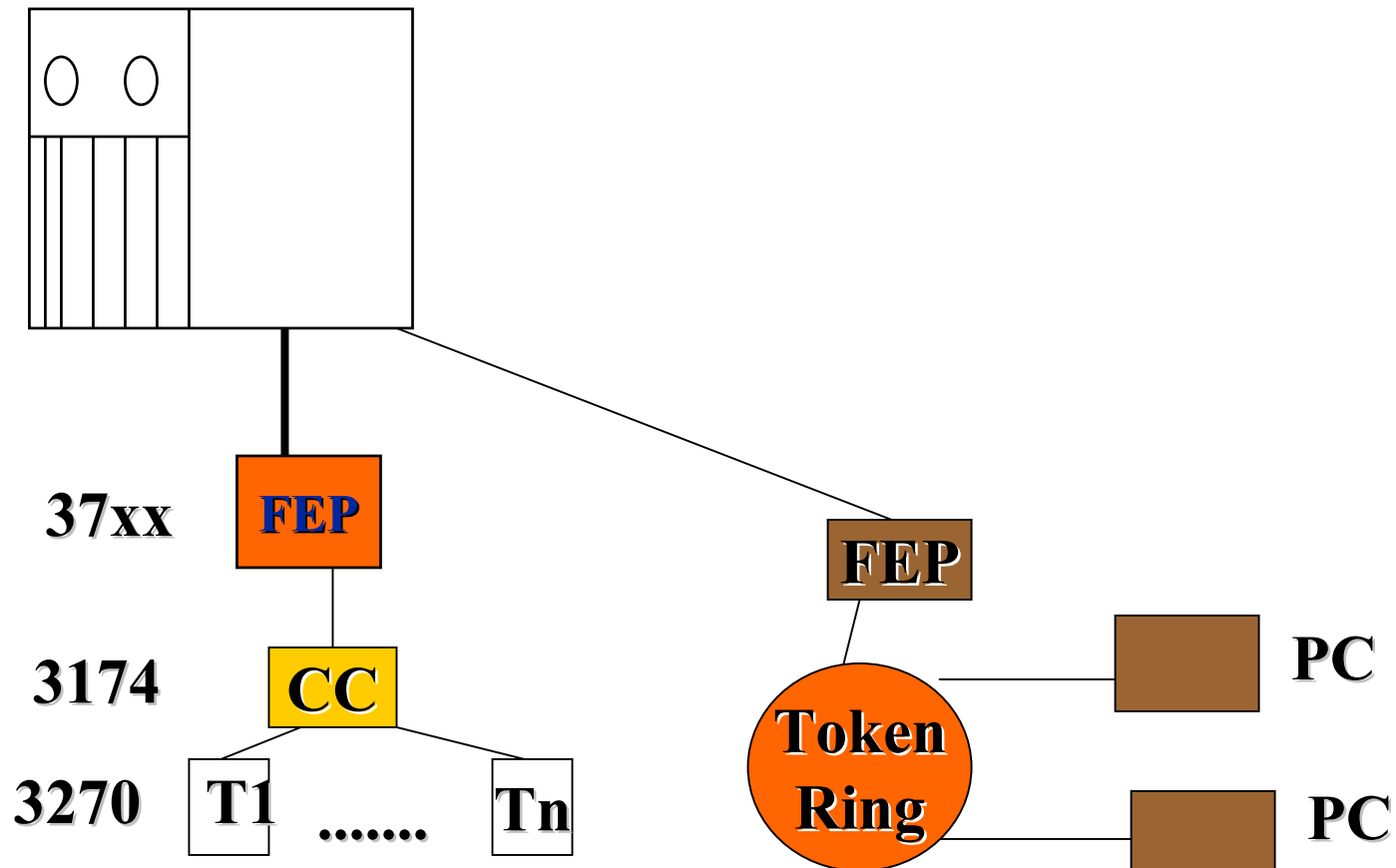
IV - Dispositivos de interconexão das redes

Exemplo - SNA/IBM e um Ambiente TCP/IP



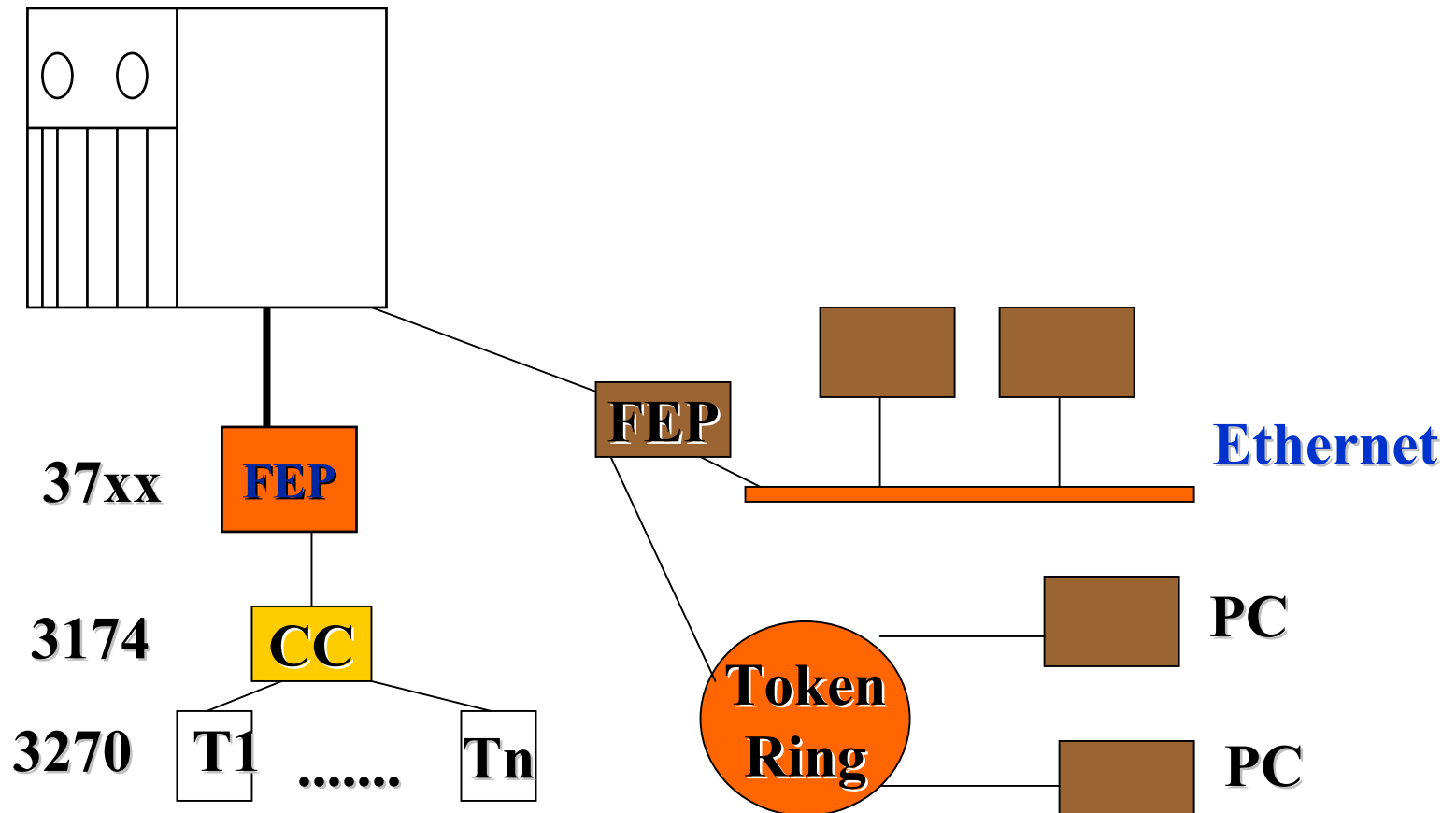
IV - Dispositivos de interconexão das redes

Exemplo - SNA/IBM e um Ambiente TCP/IP



IV - Dispositivos de interconexão das redes

Exemplo - SNA/IBM e um Ambiente TCP/IP



Conteúdo



IV-Dispositivos de interconexão de redes.

V - Arquitetura TCP/IP.

**VI - Redes de alta velocidade
(FDDI, ATM, Fast Ethernet, Myrinet).**

V - Arquitetura TCP/IP



Neste módulo do curso vamos abordar a arquitetura TCP/IP visando uma compreensão mais detalhada deste ambiente.

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

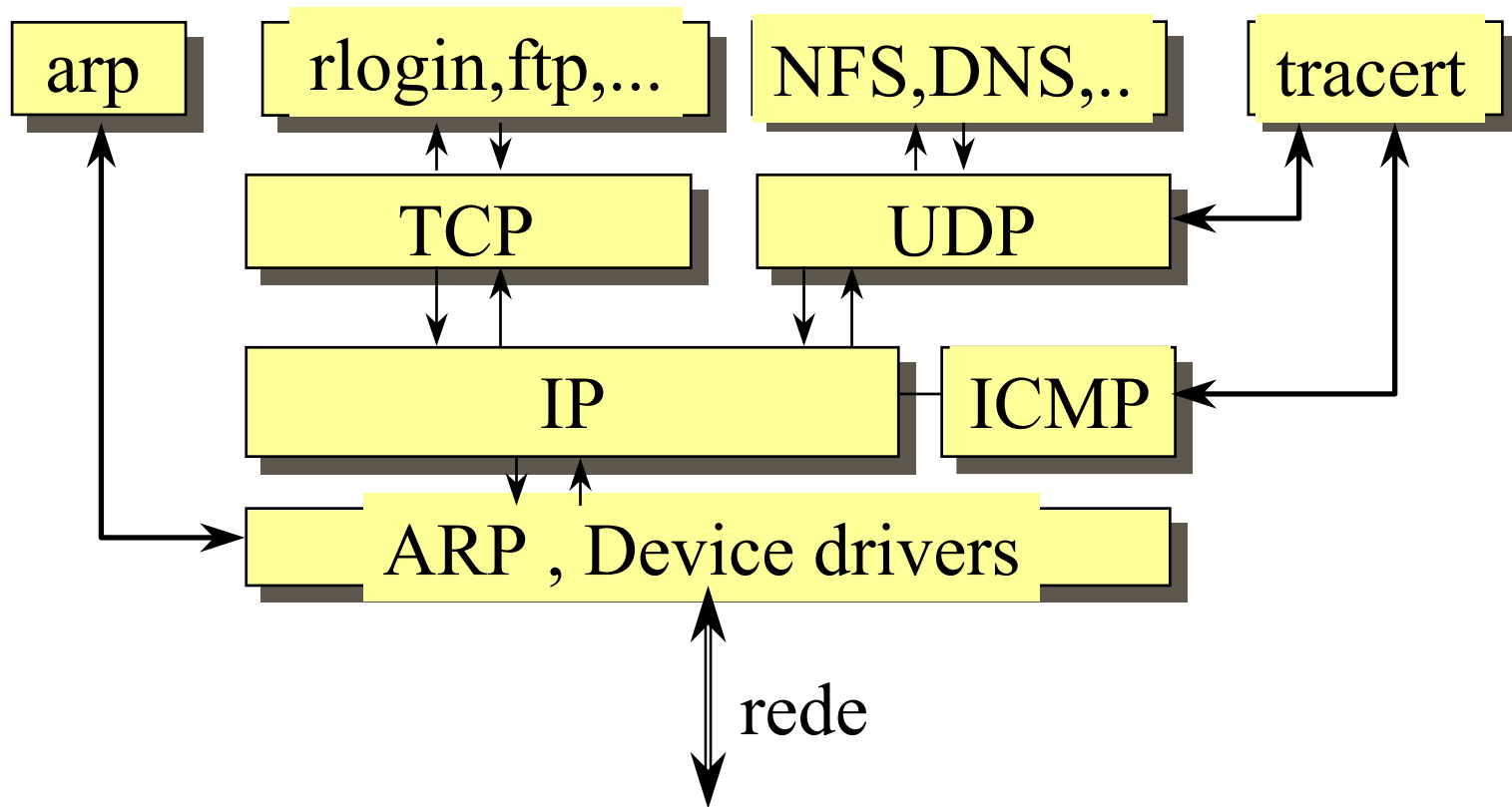
HISTÓRICO TCP/IP



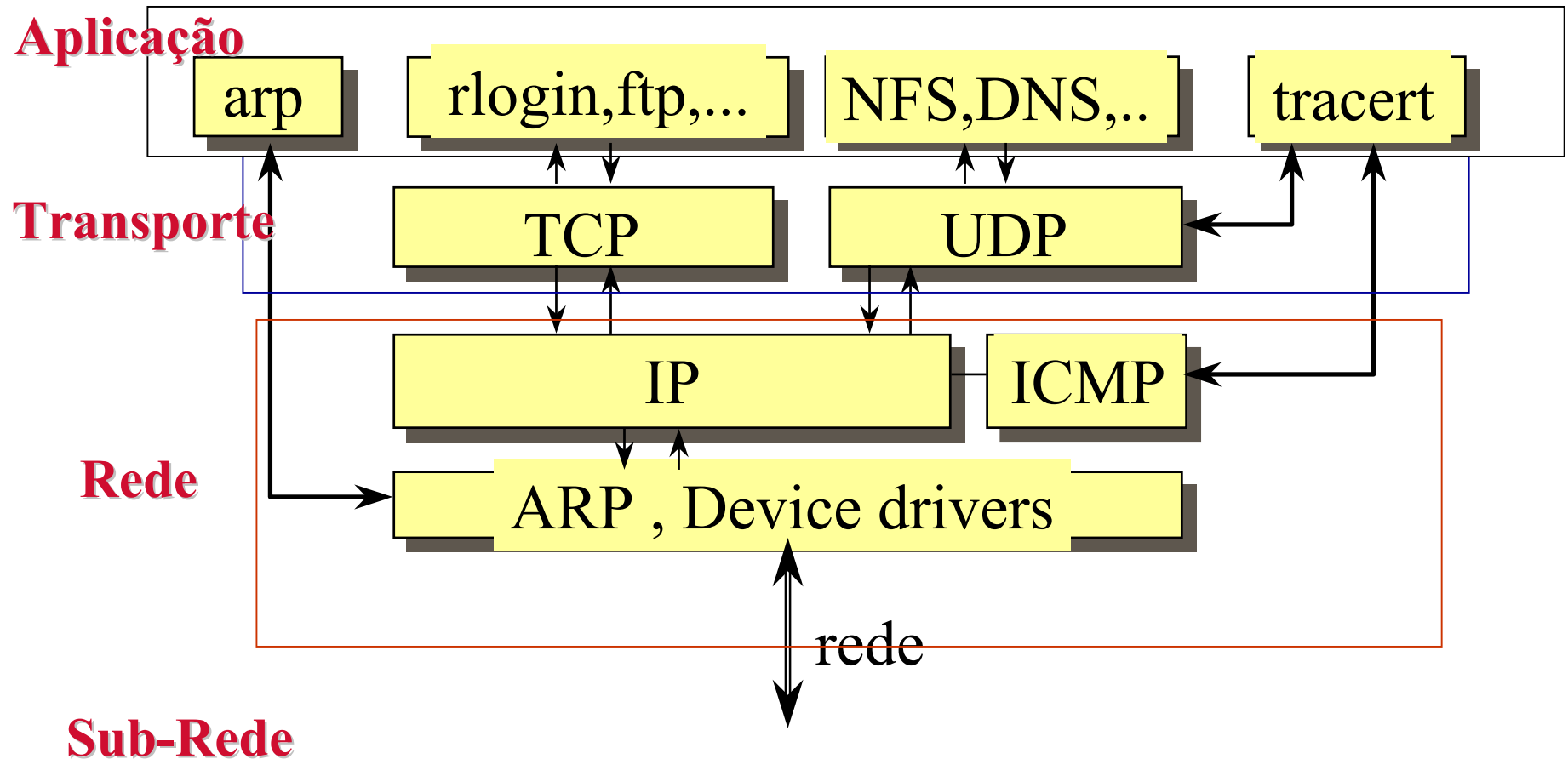
Modelo TCP/IP

aplicação
transporte
internet
sub-rede

Família de Protocolos TCP/IP



Família de Protocolos TCP/IP



Sub-Rede de Acesso

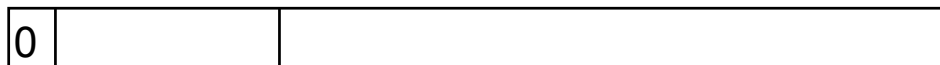


- ⌘ Ethernet, Token Ring, Token Bus ;
- ⌘ FDDI, CDDI;
- ⌘ X.25, Frame Relay;
- ⌘ MTU (Maximum Transmission Unit).

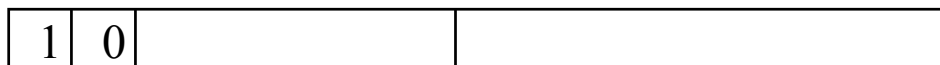
IP (Internet Protocol)

⌘ Endereçamento IP

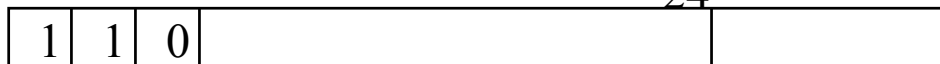
Classe A 8



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*)

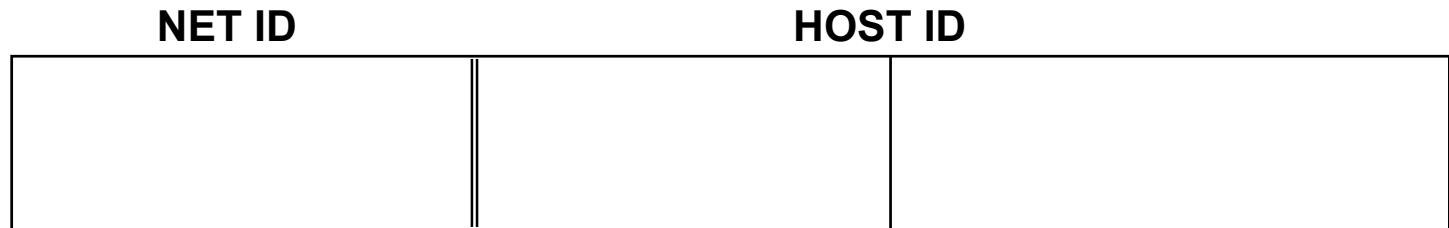
⌘ Classe C [192,223]

☑ 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

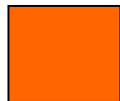
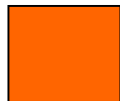
Máscara: 255.255.255.0

Indústria X

Administração

Fabrica

Marketing/Vendas



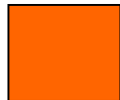
Computadores

Indústria X (128.7.0.0)

Administração
(128.7.254.0)

Fabrica
(128.7.253.0)

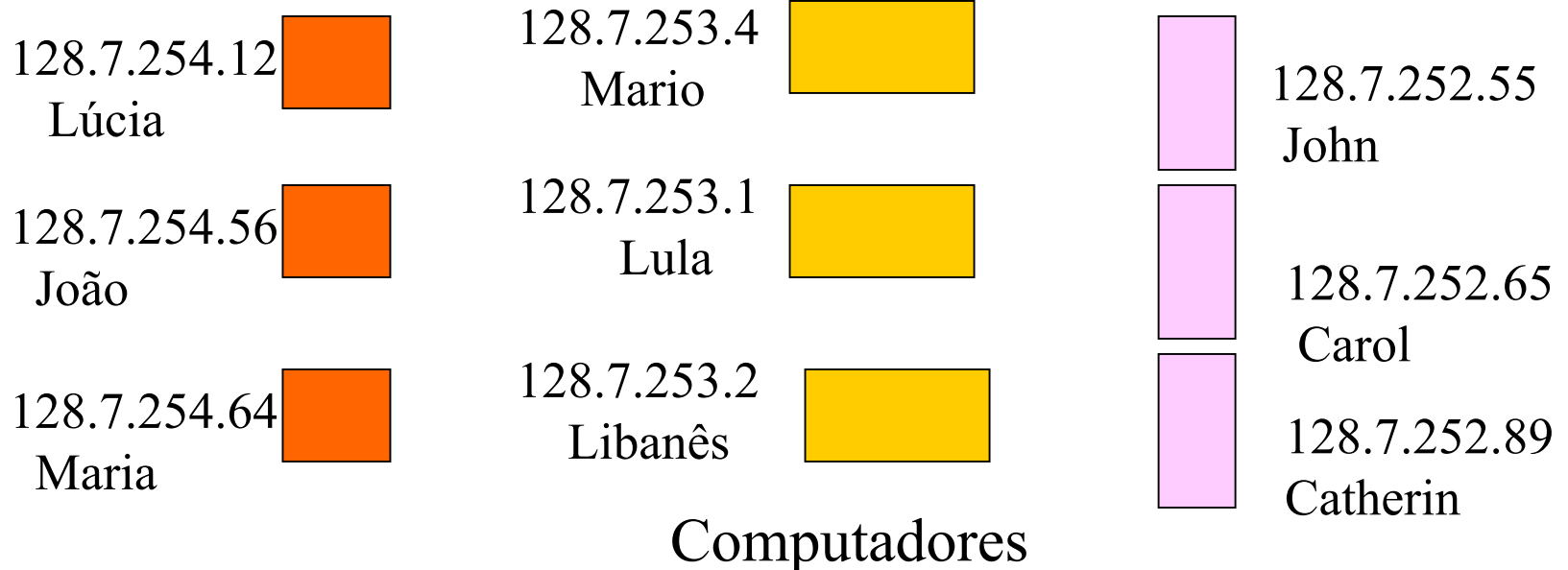
Marketing/Vendas
(128.7.252.0)



Computadores

Indústria X (128.7.0.0)

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



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)

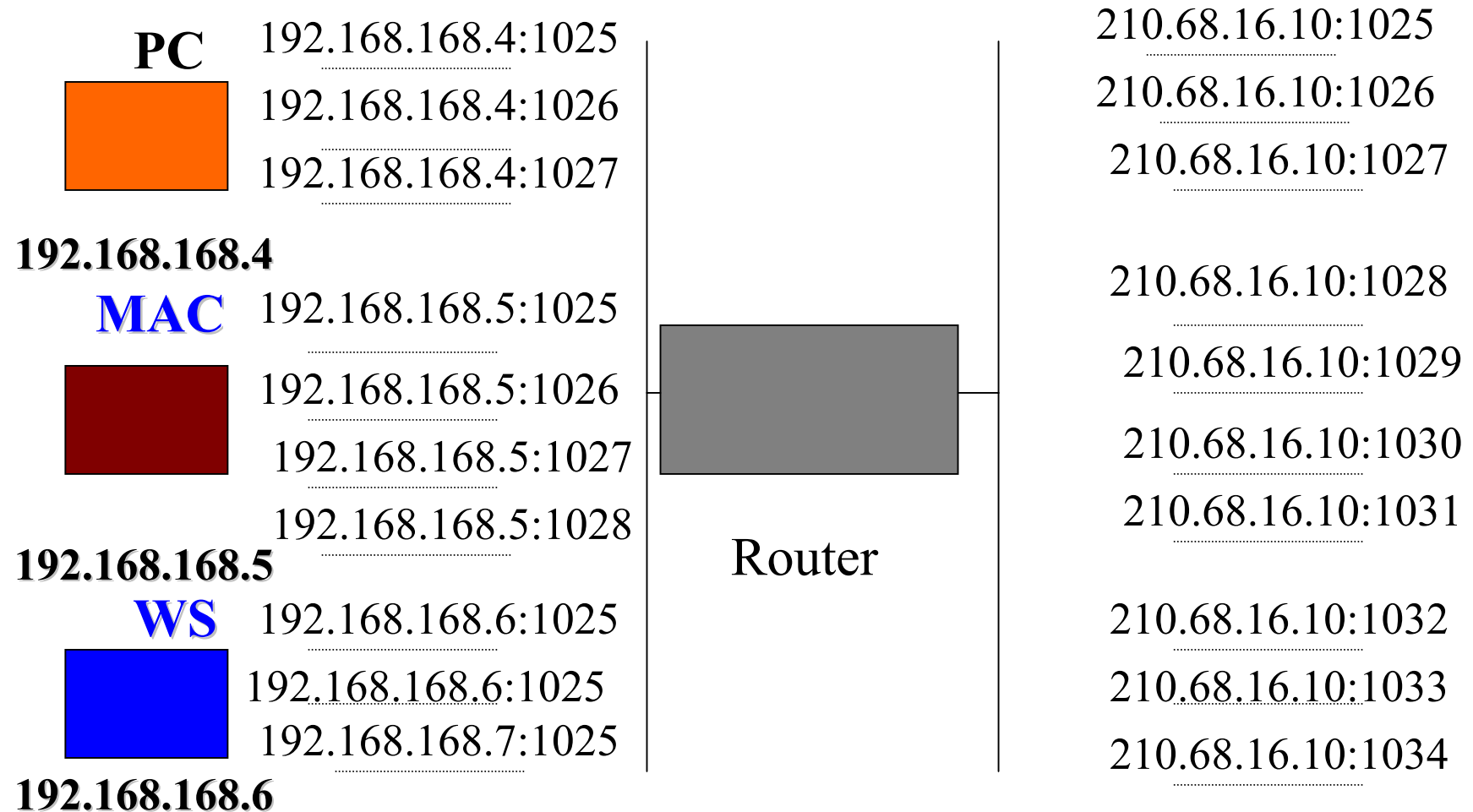
Roteamento e Tradução de Endereços



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

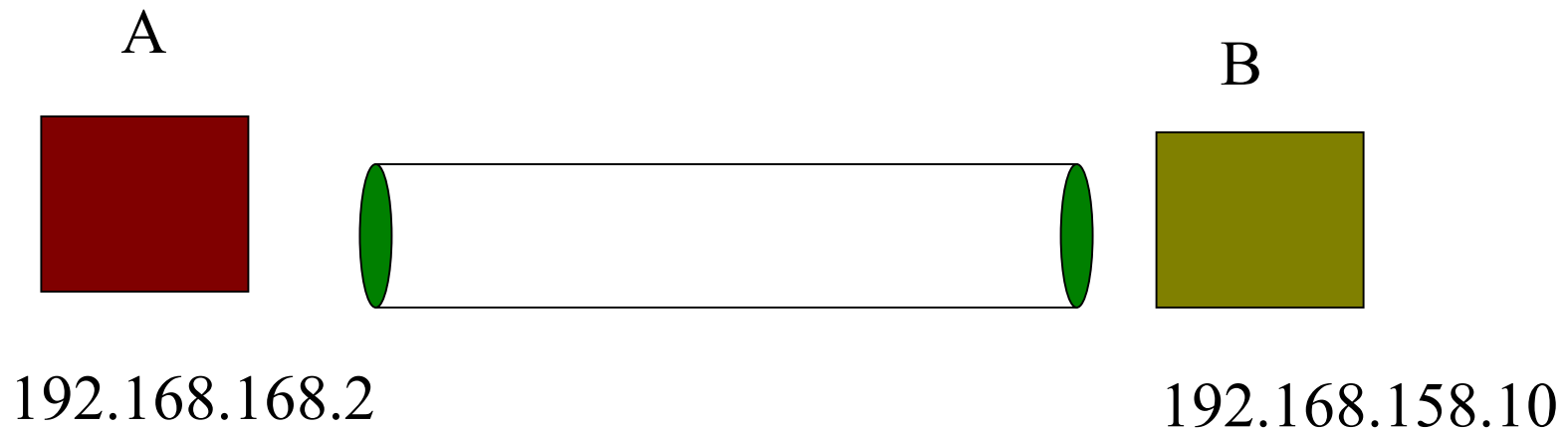
Tradução de Endereços - permite que uma rede *pequena* seja vista pela *Internet* como um simples nó. Desta forma, um único endereço IP (ou um conjunto pequeno de endereços) poderá ser compatilhado pela rede. Este aspecto pode prover dentre outras características uma proteção contra intrusos na rede.

Roteamento e Tradução de Endereços



Técnicas de Compartilhamento de Links

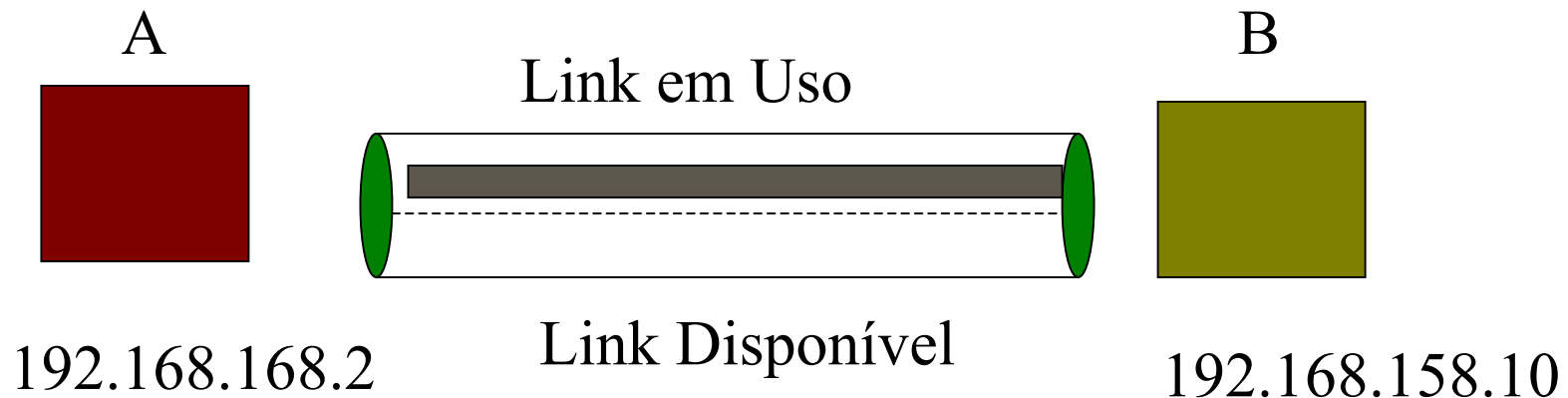
PPP (Point-to-Point Protocol) - este protocolo provê um mecanismo padrão para que dispositivos numa rede TCP/IP possam se comunicar através de uma linha de comunicação simples (ou única).



Técnicas de Compartilhamento de Links

Multilink PPP - A RFC 1717 define o *multilink* para o protocolo PPP visando que o mesmo possa permitir vários *links* simultâneos num único canal de comunicação. As ligações podem ser adicionadas, ou cortadas, visando a utilização com eficiência do canal.

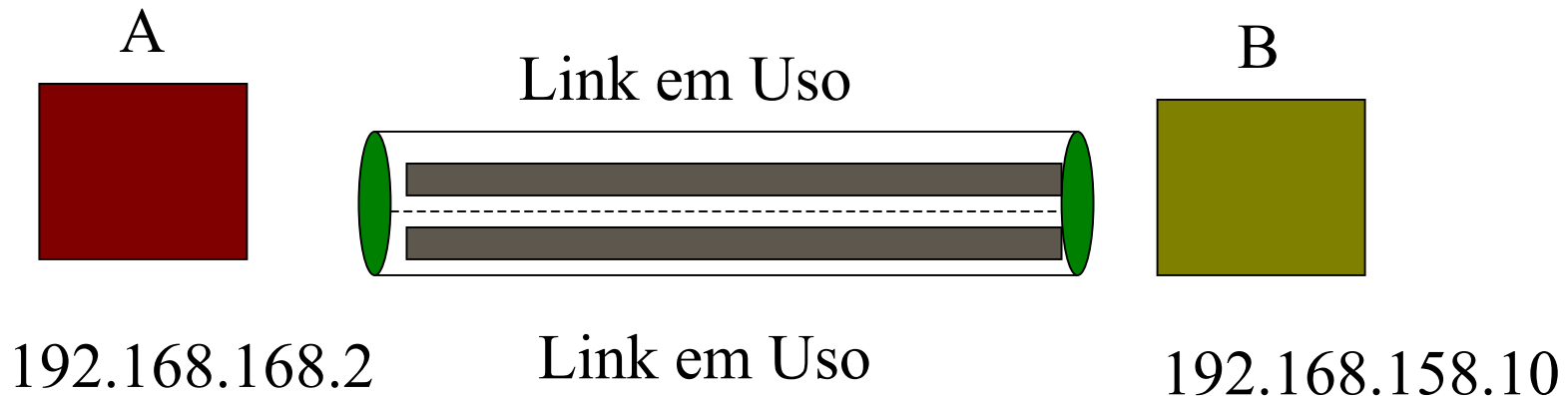
Exemplo - Tráfego Leve



Técnicas de Compartilhamento de Links

Multilink PPP - A RFC 1717 define o *multilink* para o protocolo PPP visando que o mesmo possa permitir vários *links* simultâneos num único canal de comunicação. As ligações podem ser adicionadas, ou cortadas, visando a utilização com eficiência do canal.

Exemplo - Tráfego Pesado



Técnicas de Compartilhamento de Links



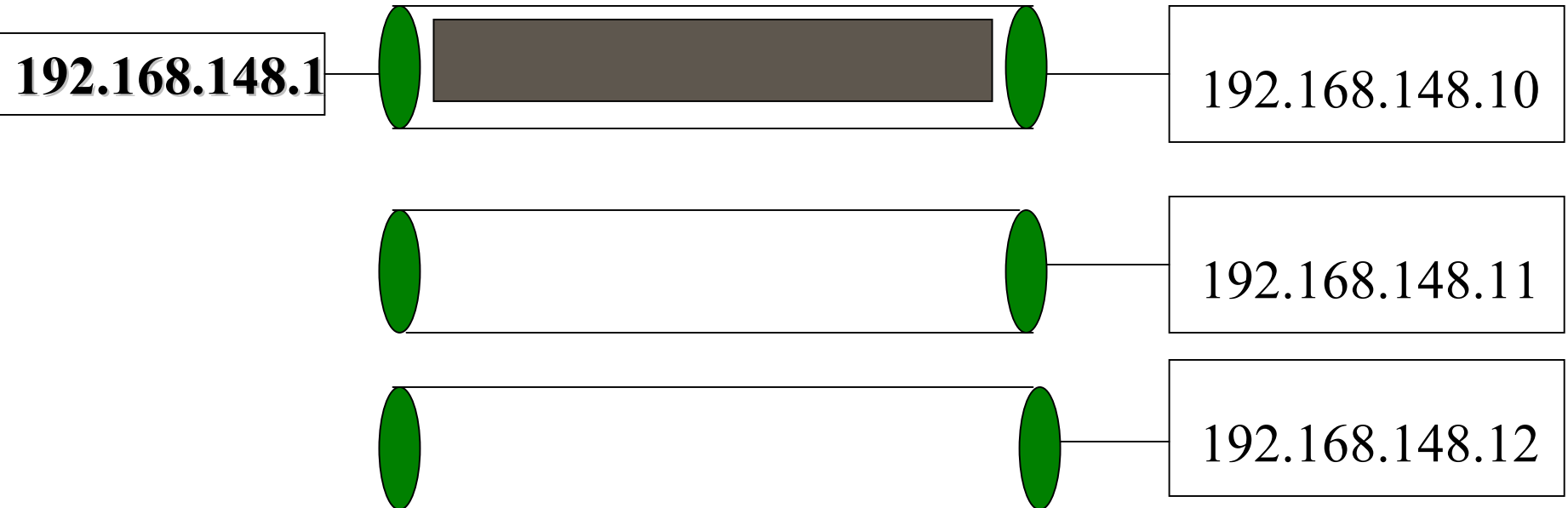
COLT (Connection Optimized Link Technology) - esta técnica foi criada pela empresa RAMP Networks para seus roteadores (*routers analógicos*).

Embora RAMP empregue o PPP para seus protocolos seriais, eles não se utilizam do *Multilink PPP*. Ao contrário da criação de um *grande canal*, o COLT distribui o tráfego por múltiplos diferentes canais. Como exemplo empregando diferentes canais dos modems:

- temos no primeiro o *download* de *mail* ;
- no segundo existe uma conexão HTTP;
- no terceiro uma conexão FTP;

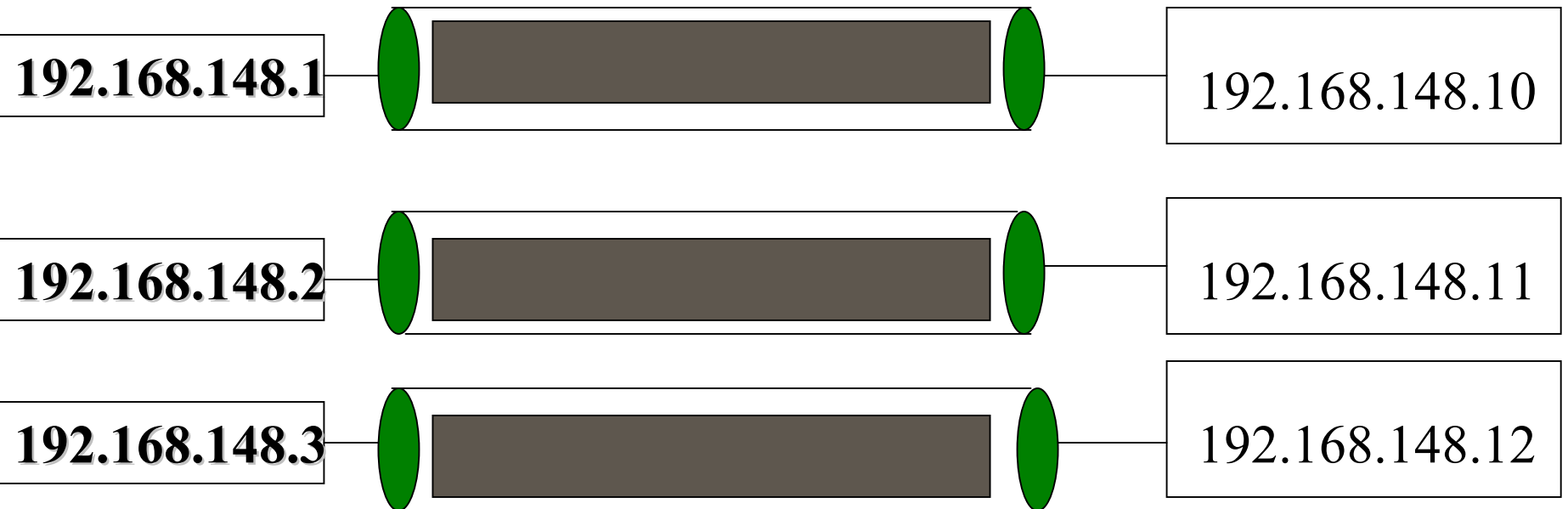
Técnicas de Compartilhamento de Links

COLT - Exemplo de Tráfego Leve



Técnicas de Compartilhamento de Links

COLT - Exemplo de Tráfego Pesado



Técnicas de Compartilhamento de Links

Software vs Appliances

Software - roteamento e tradução de endereços podem executar com muita facilidade num PC, ou Workstation. Com auxílio de pequenos pacotes de software comprados (exemplo - *iNet for Windows 95*, da Artisoft), ou freeware/shareware (exemplo - *IPMasq* para Unix).

Até mesmo o Multilink PPP pode já estar implementado no Sistema Operacional.

Técnicas de Compartilhamento de Links

Software vs Appliances

Appliance (dispositivo de uso específico) - a utilização destes dispositivos têm provado que :

Vantagens:

- *mais baratos;*
- *mais fácil de gerenciar;*
- *menos susceptível a erros;*

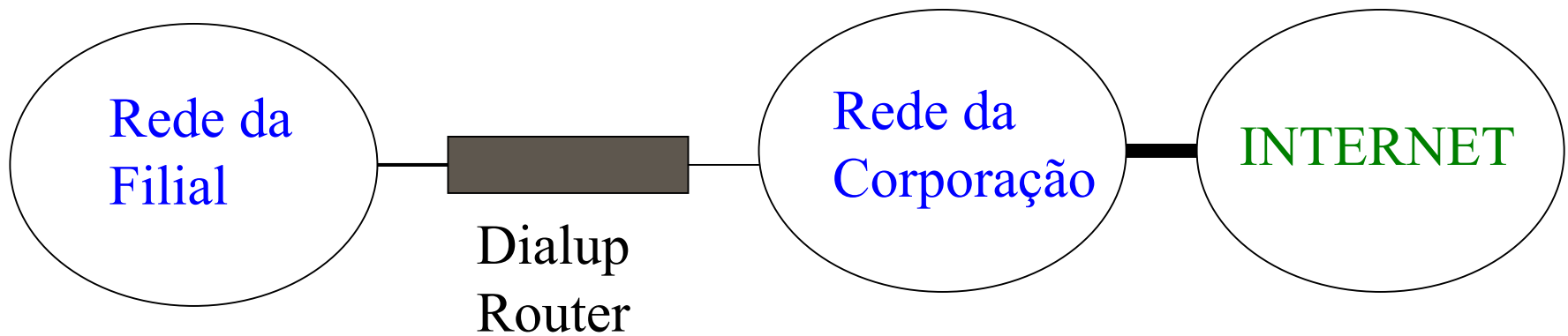
Desvantagem:

- *falta de flexibilidade.*

Técnicas de Compartilhamento de Links

Roteadores Pequenos em Corporações

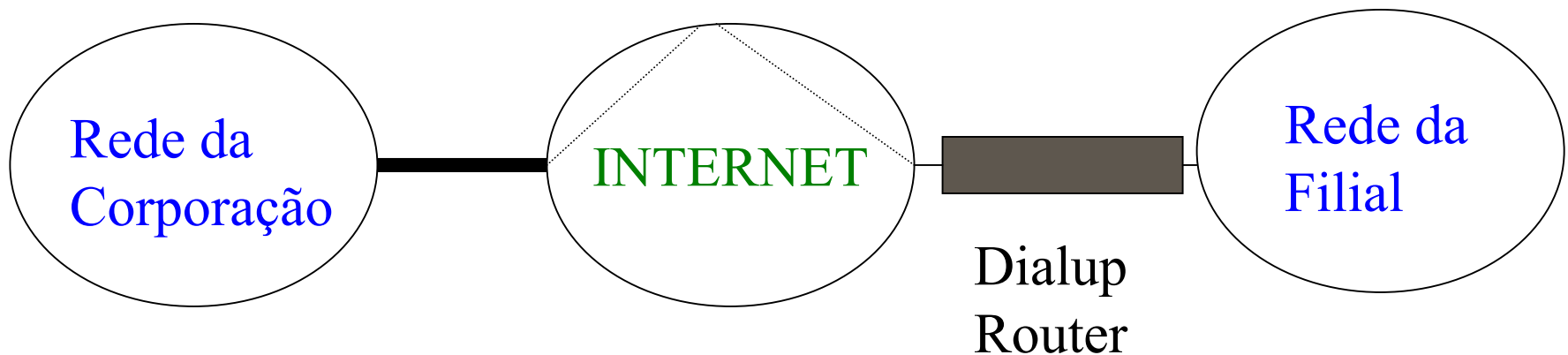
Situação A



Técnicas de Compartilhamento de Links

Roteadores Pequenos em Corporações

Situação B



Exemplo Sub-rede

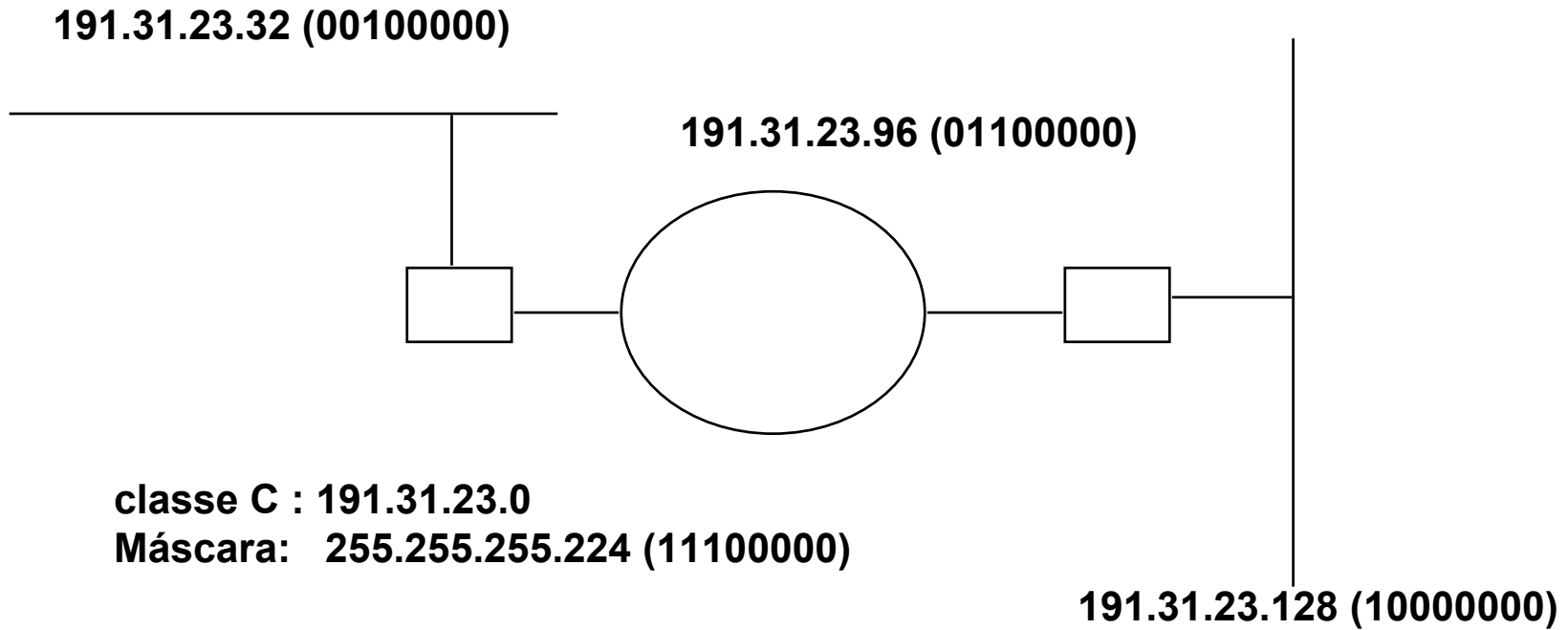


Tabela de Rotas

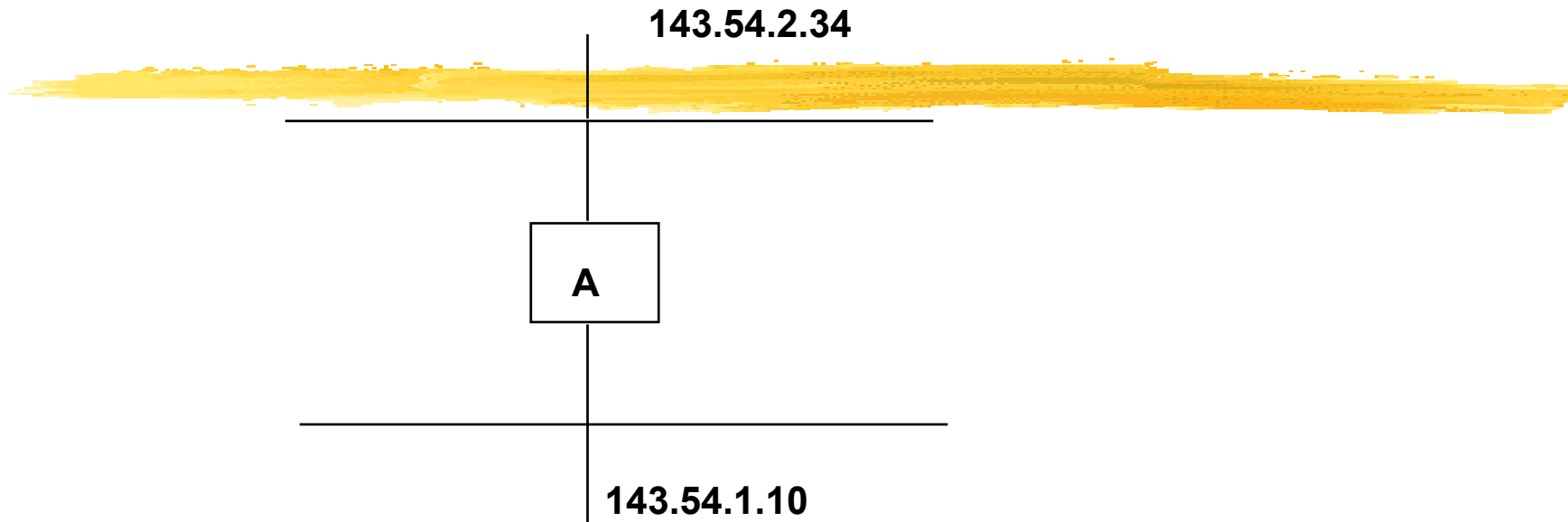


Tabela de rotas de A

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

Protocolos IP, ICMP, ARP e RARP

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 (ou 6 ?)
- ⌘ **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

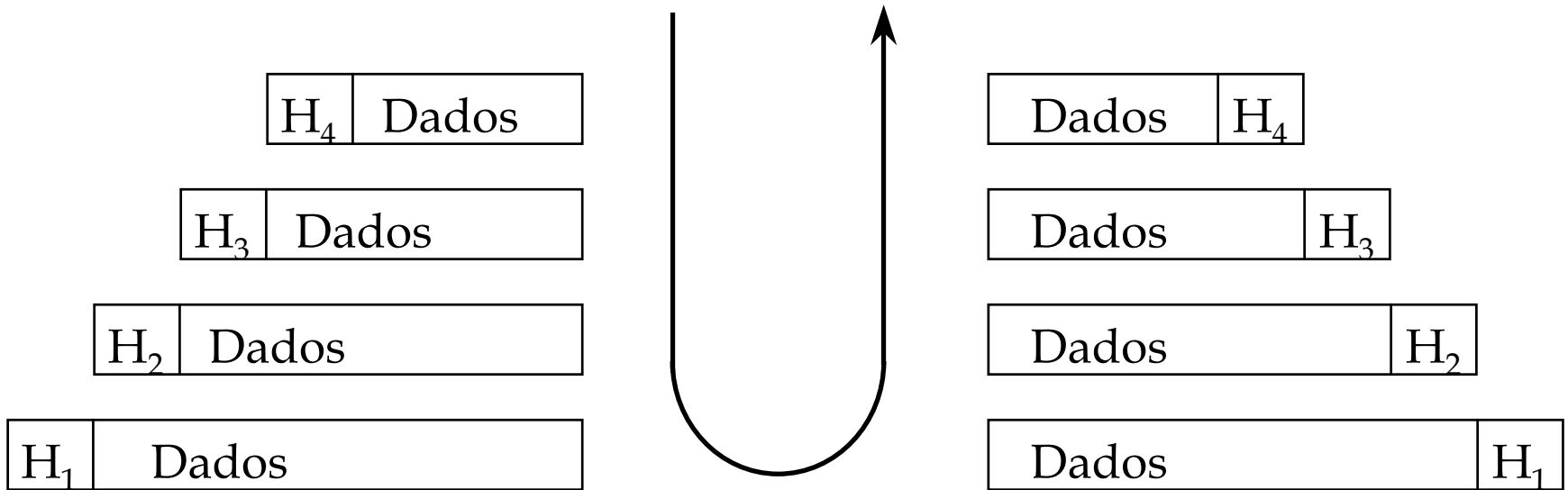
Encapsulamento do Datagrama



- ⌘ 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

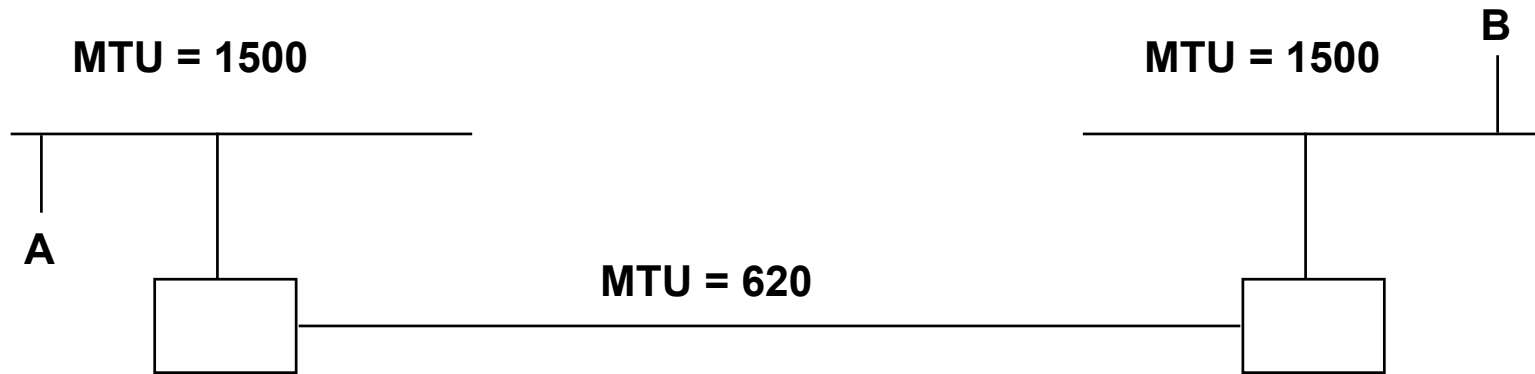
Encapsulamento do Datagrama

- ⌘ Quebra em pacotes
- ⌘ Tráfego de sequência de bits



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

Encapsulamento do Datagrama



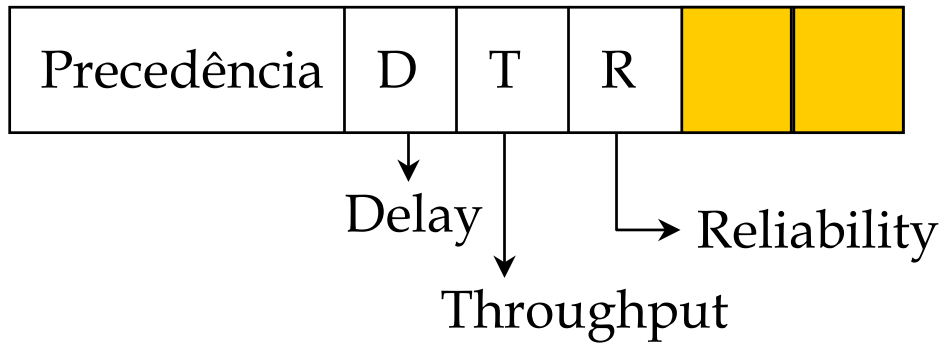
Datagrama de 1400 octetos : A -> B

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

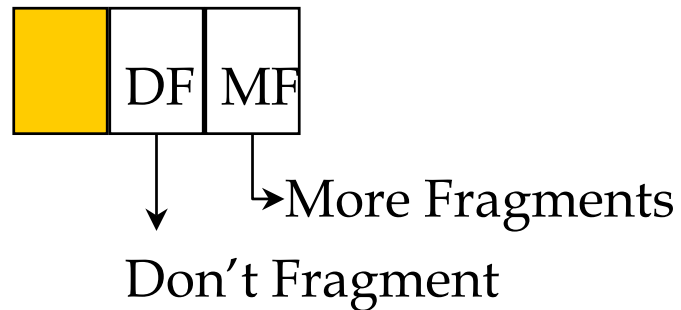
- Fragmentos só são remontados no host destino

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

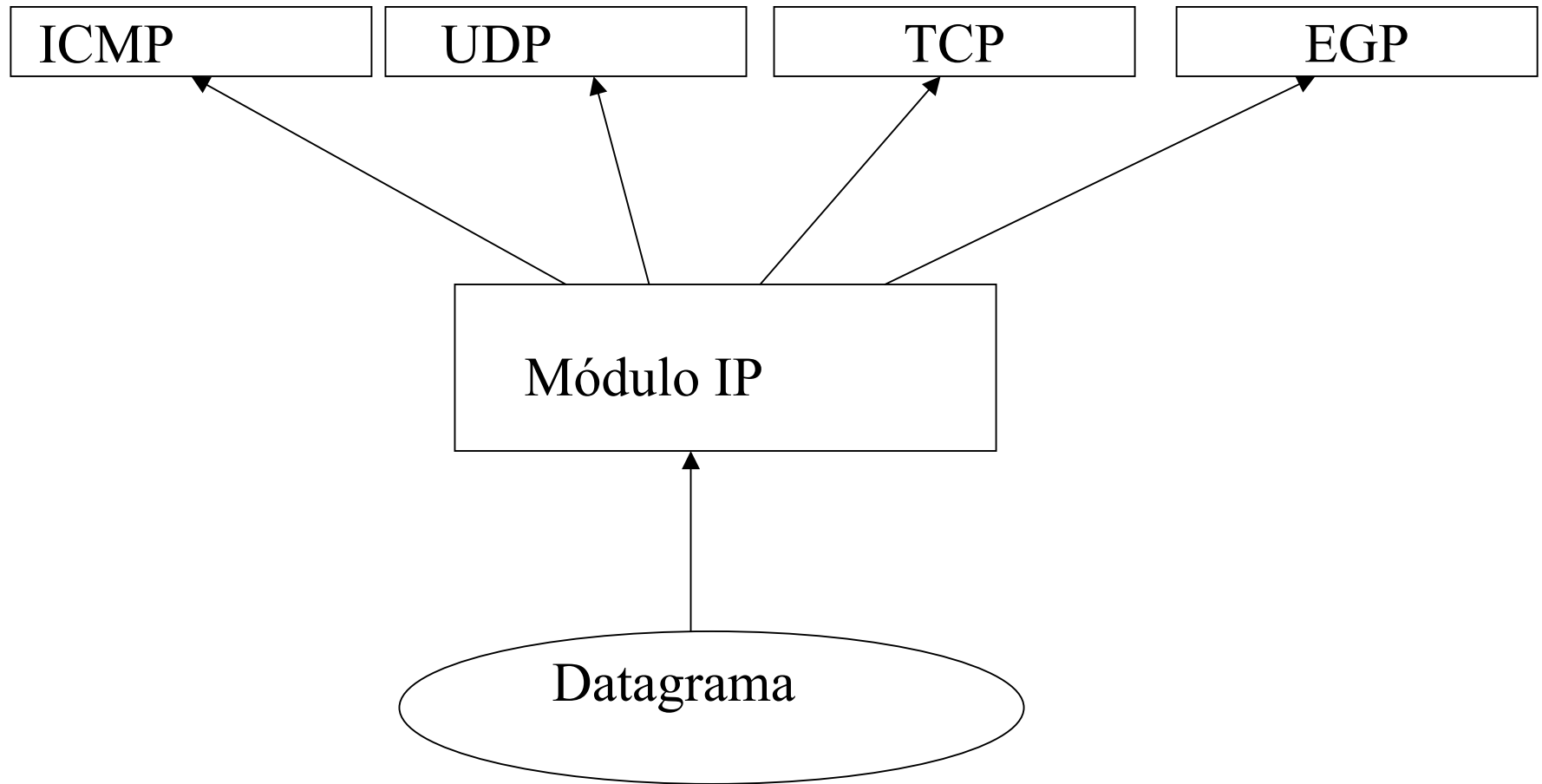
- ⌘ Verificação do Checksum, versão, tamanhos
 - ☒ O Checksum é recalculado, se for diferente do datagrama, este é descartado
- ⌘ Se o datagrama é fragmentado, é disparado um temporizador que evitará o espera indefinida dos outros fragmentos do datagrama original
- ⌘ Entrega do campo de dados do datagrama 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

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

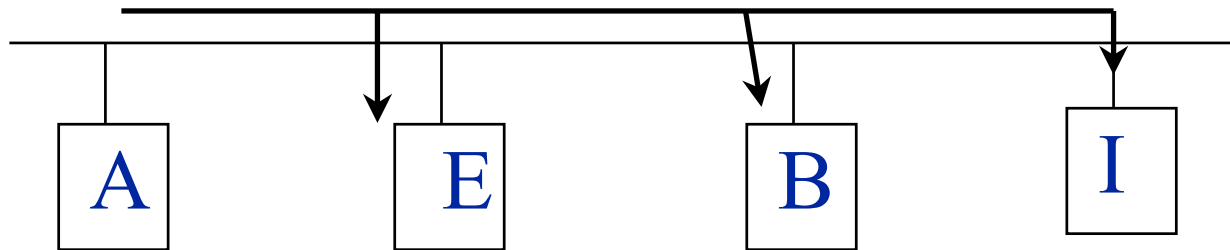
ARP (Address Resolution Protocol)



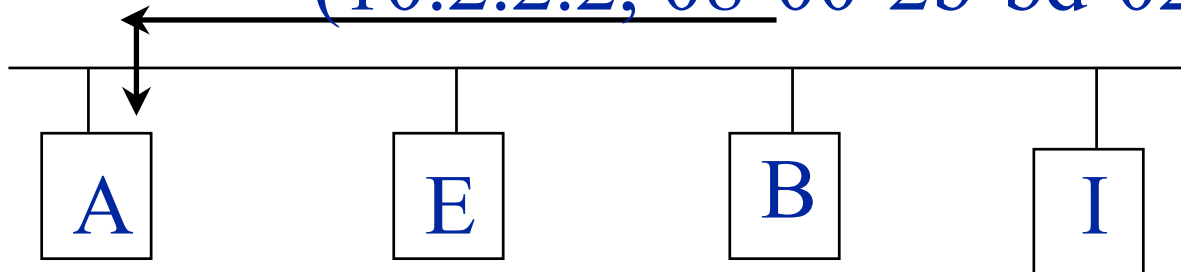
Hard Type		Proto Type
Hlen	Plen	Operation
Sender HA		
Sender HA		Sender IP
Sender IP		Target HA
Target HA		
Target IP		

ARP (Address Resolution Protocol)

(10.2.2.2, Fb)



(10.2.2.2, 08-00-2b-bd-02-01)

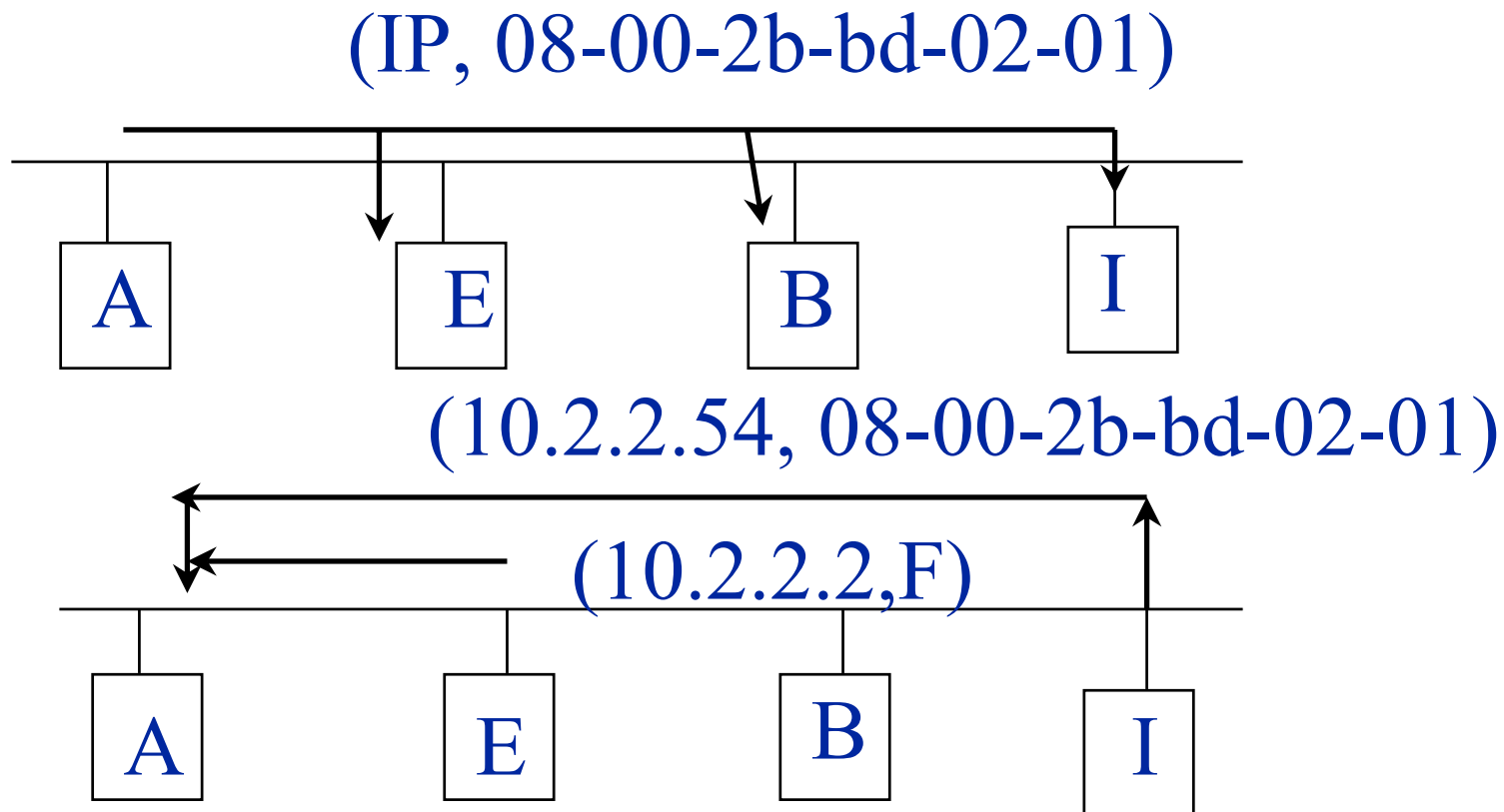


RARP (Reverse Address Resolution Protocol)



- ⌘ Usado por um host para descobrir o seu endereço lógico IP 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

RARP (Reverse Address Resolution Protocol)




Camada de Transporte

UDP (User Datagram Protocol)

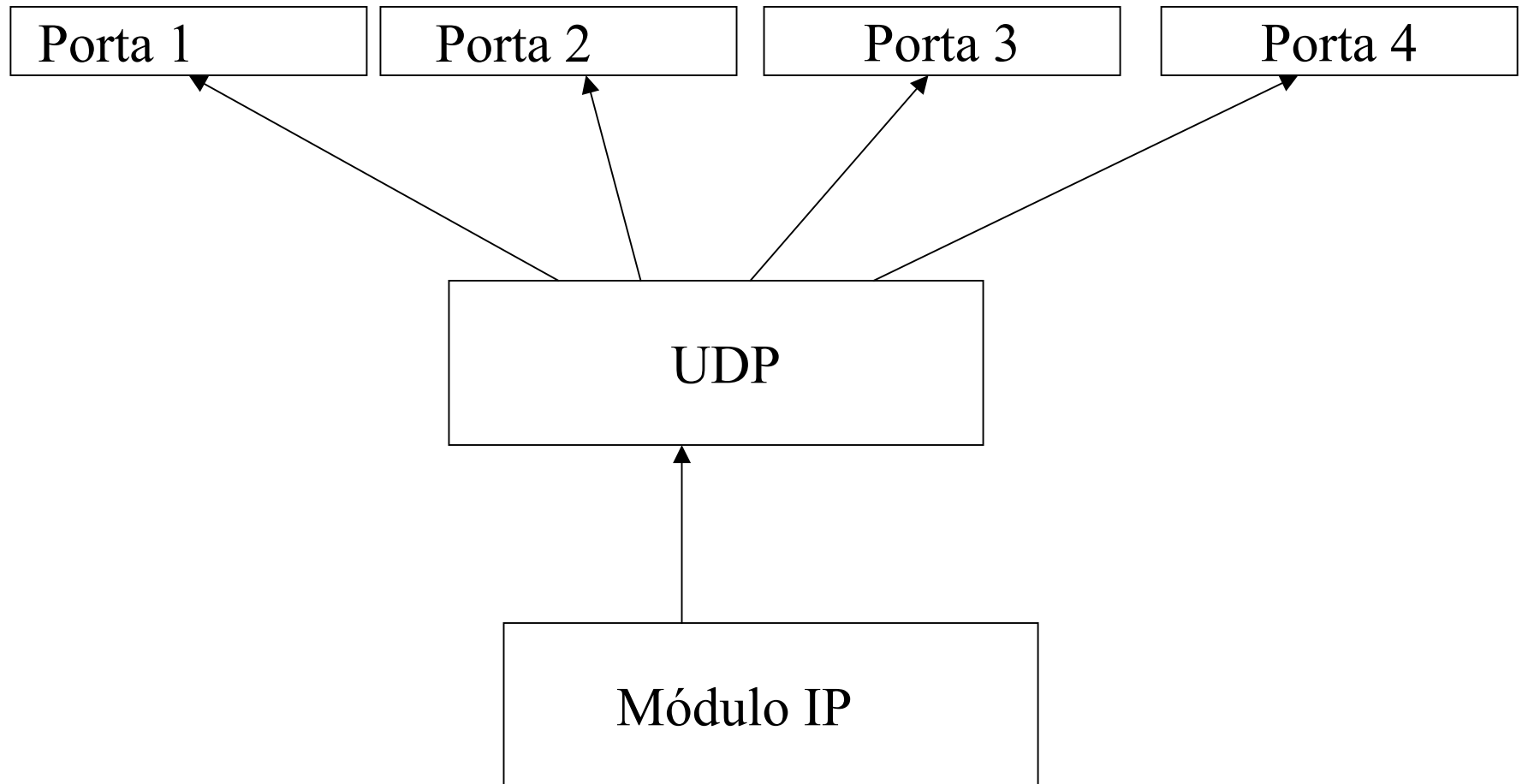
- ⌘ Protocolo de transporte não orientado à conexão
- ⌘ Não implementa nenhum mecanismo de recuperação de erros
- ⌘ São identificados os processos origem e destino através do conceito de porta
- ⌘ O campo de CheckSum é opcional

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 multiplas sessões do mesmo serviço

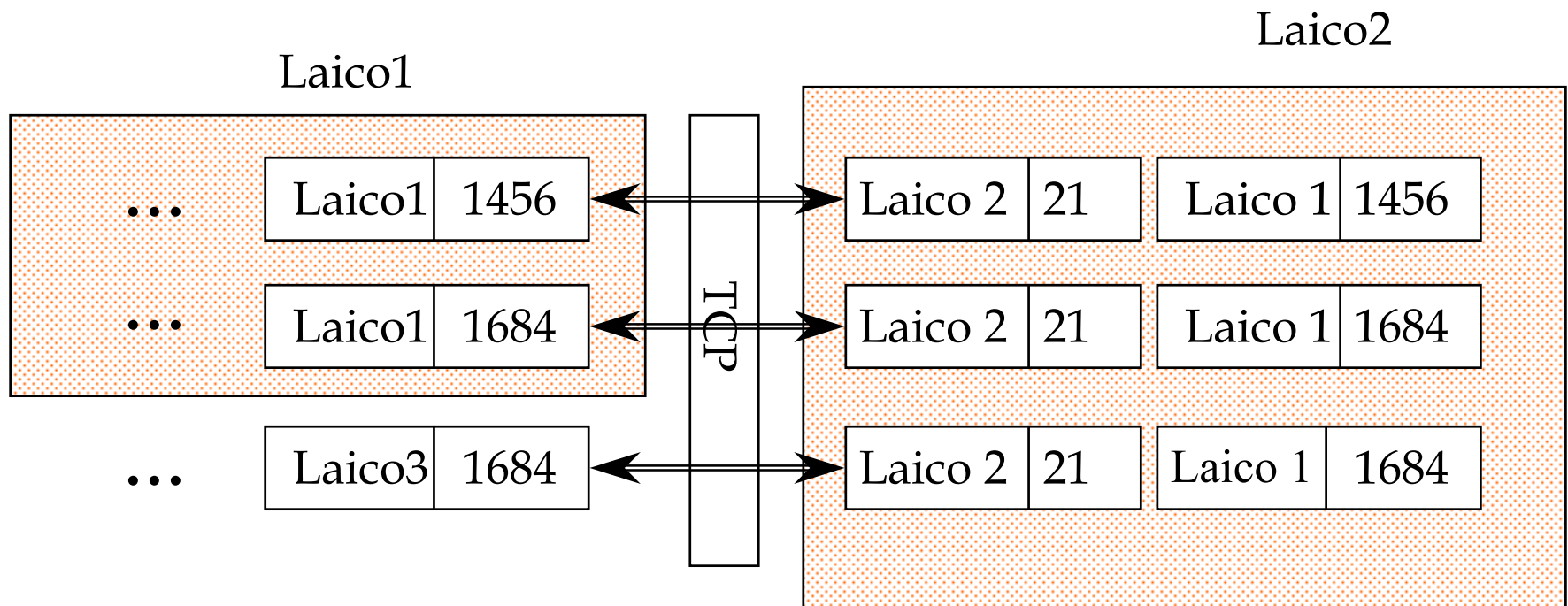
Janela Deslizante



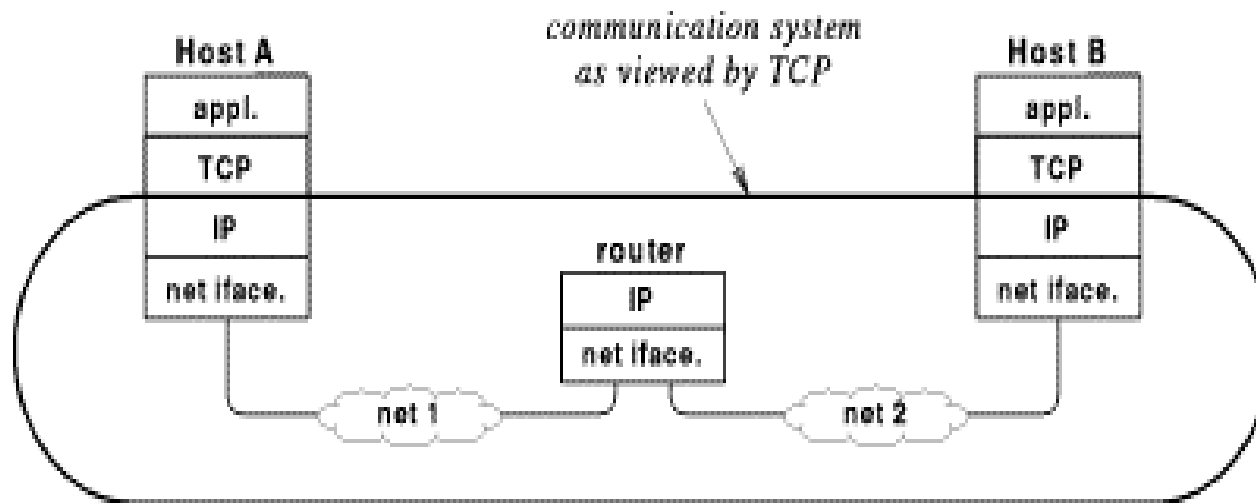
- ⌘ Cada octeto é numerado
- ⌘ O tamanho da janela determina o número de octetos que podem ser transmitidos sem reconhecimento
- ⌘ Através do mecanismo de PIGGYBACK pode-se reconhecer um bloco de octetos via um segmento de dados

TCP - Exemplo

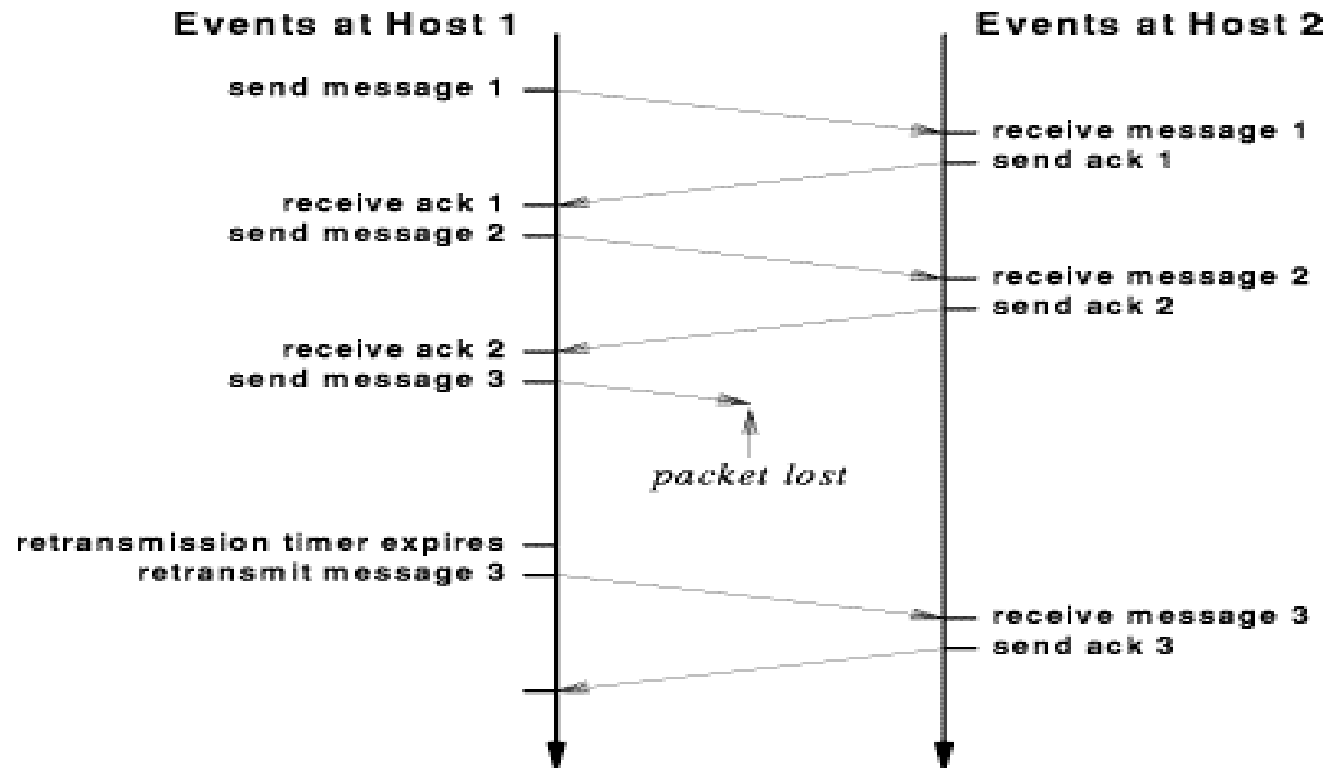
⌘ FTP - port 21



TCP - Visão de comunicação

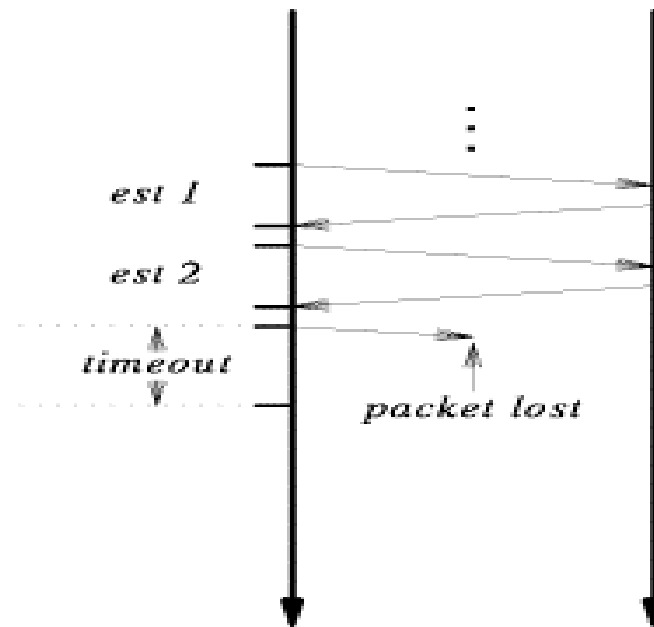
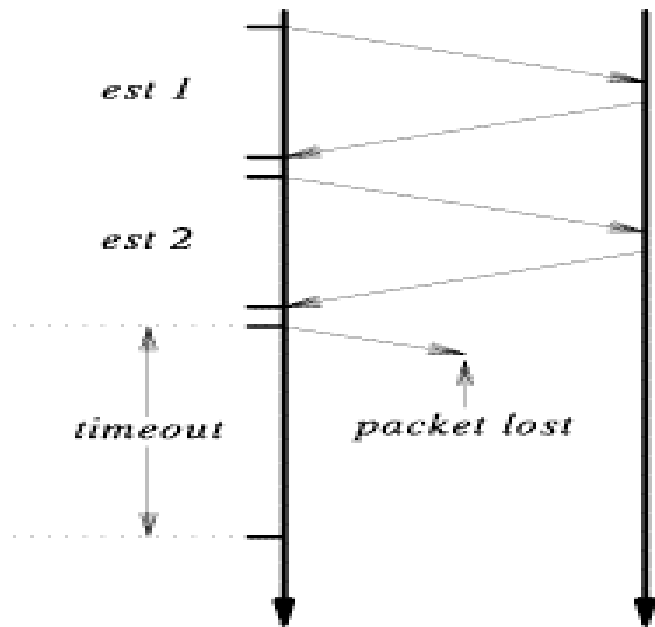


TCP - Confiabilidade

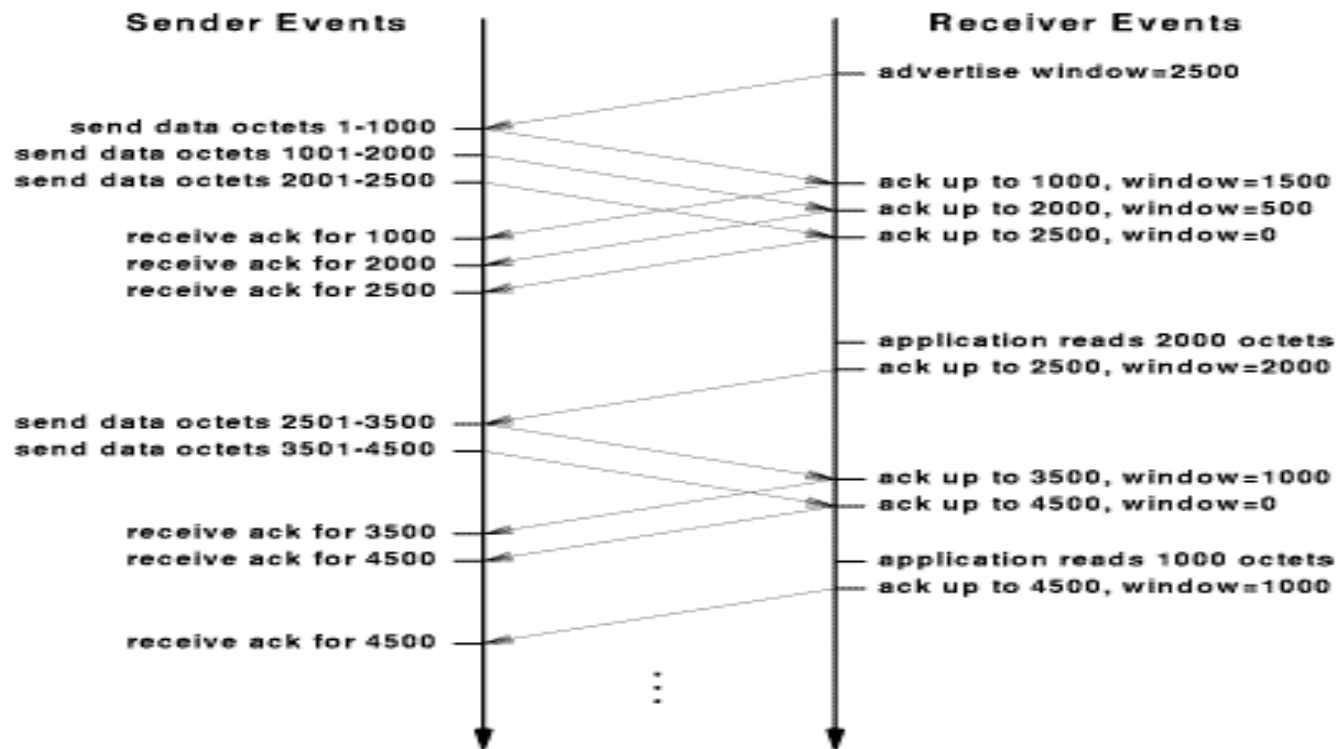


TCP - Timeout Adaptativo

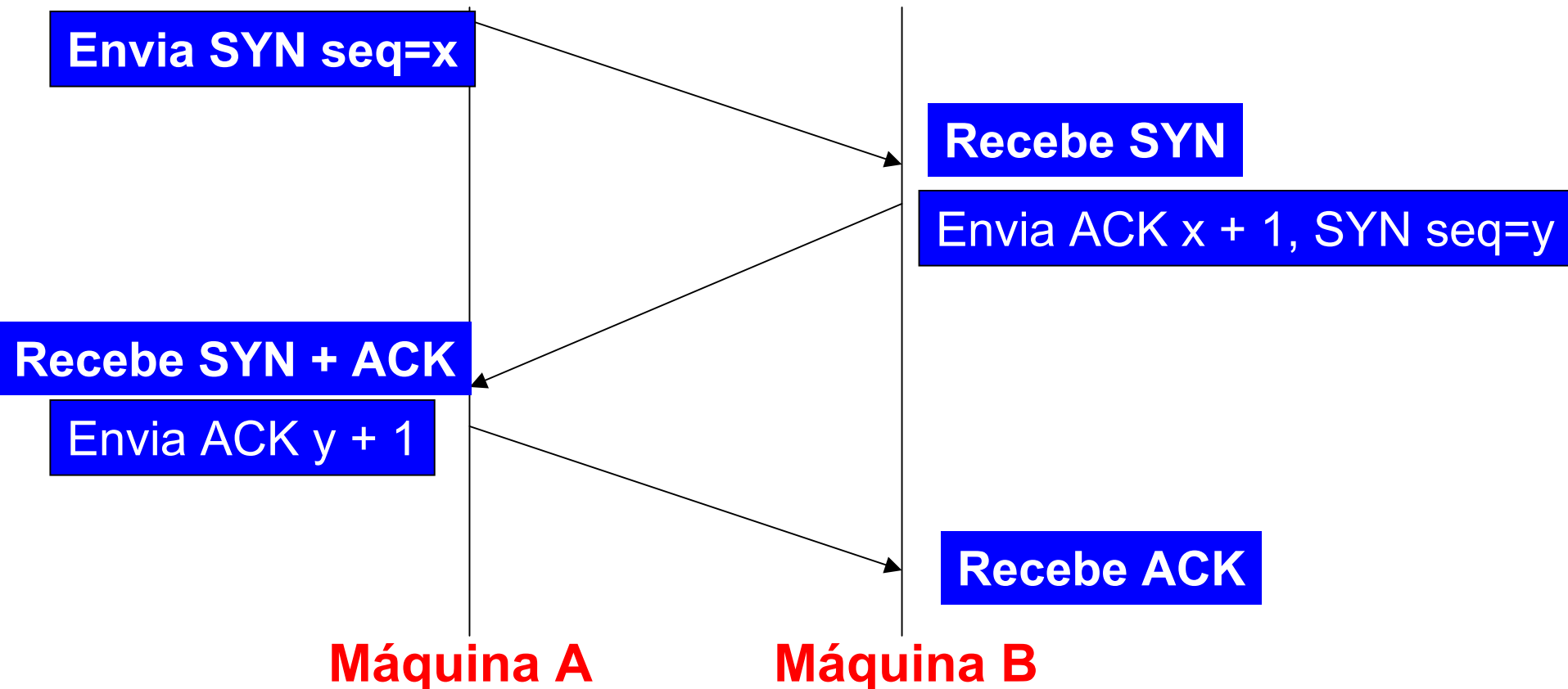
⌘ Verifica o tempo de resposta e ajusta o timeout



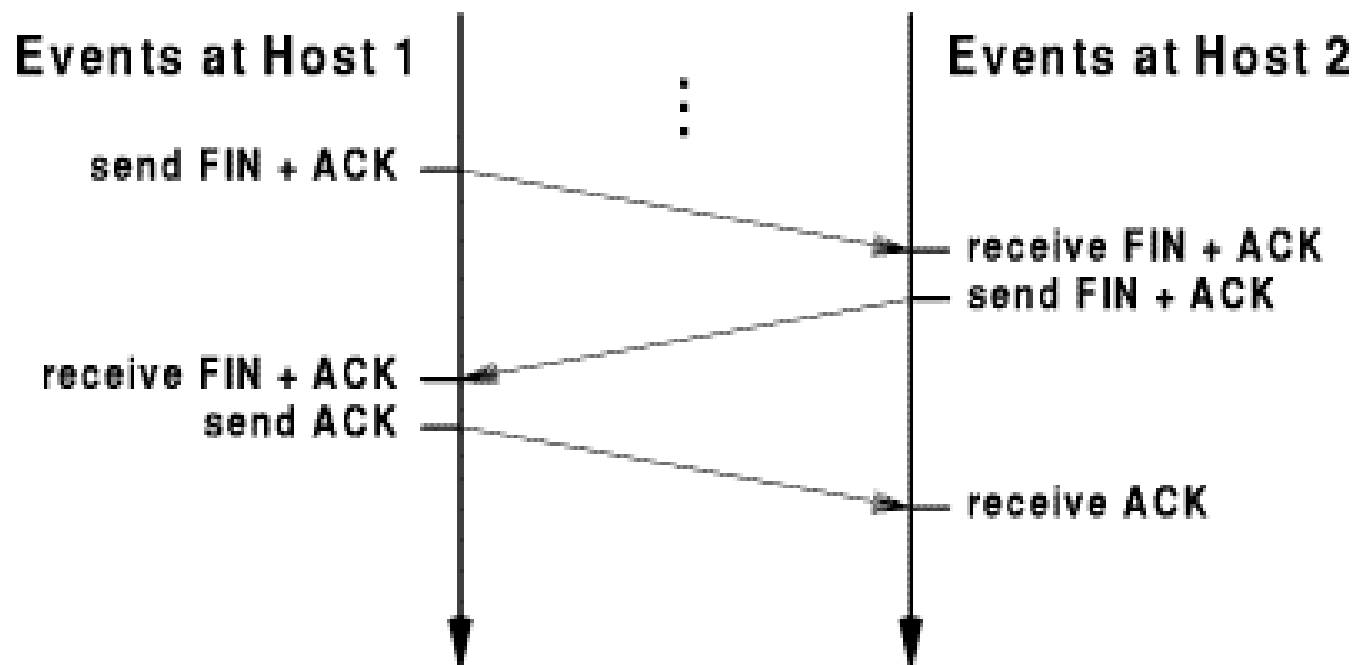
TCP - Janela deslizante



TCP - Estabelecimento de Conexão

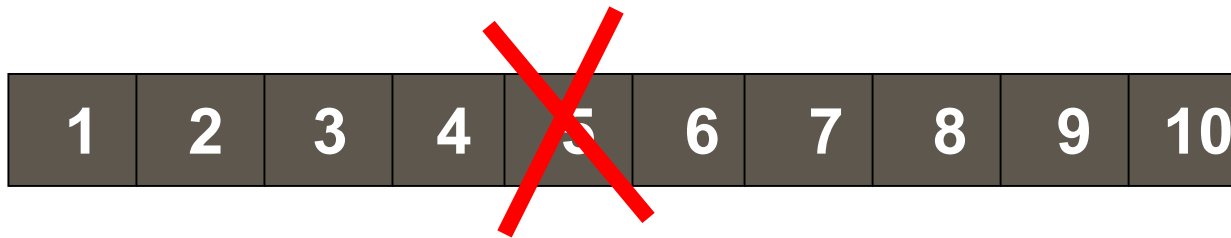


TCP - Estabelecimento de conexão



TCP - Reconhecimento e retransmissão

Go-back-n x Retransmissão seletiva



Go-back-n



Retransmissão seletiva

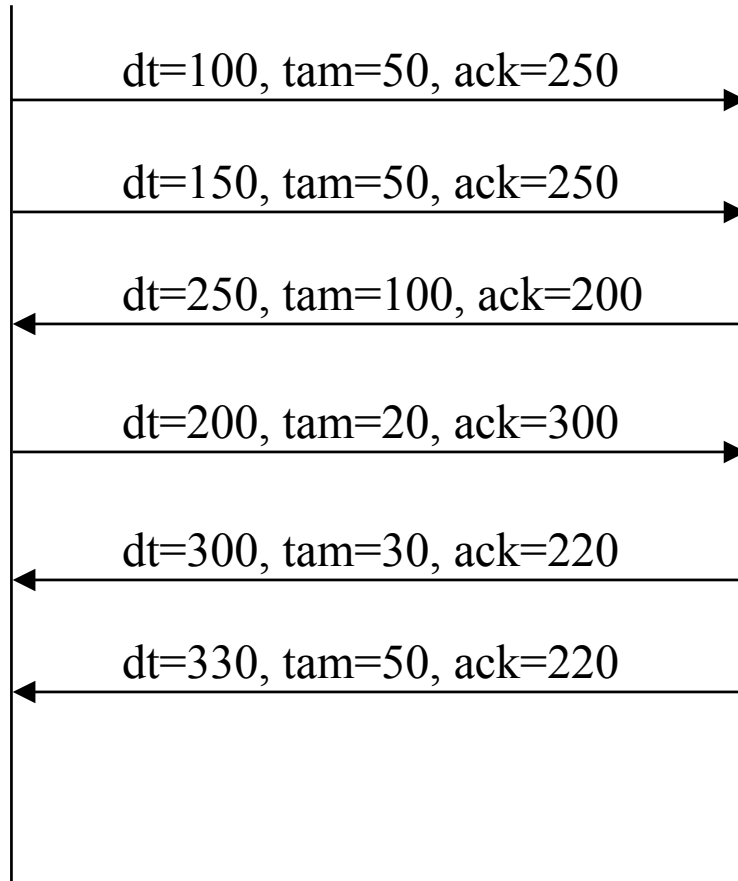
5

TCP - Parâmetros

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

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

Janela Deslizante



TCP



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

Campos do TCP



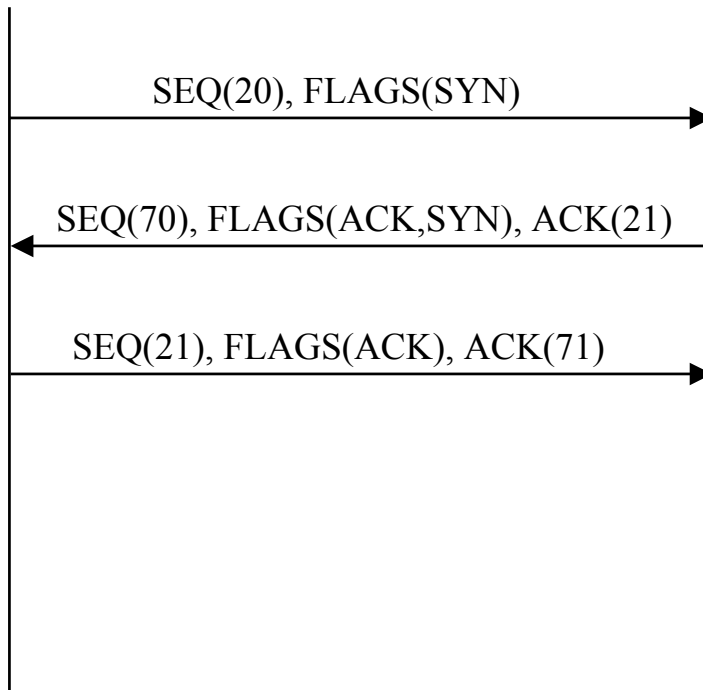
- ⌘ **Portas:** identificam os processos origem e destino
- ⌘ **Número de sequência:** número do primeiro octeto do campo de dados
- ⌘ **Número do ACK:** número do octeto que é esperado pelo destino, sendo todos os octetos de número inferior reconhecidos
- ⌘ **HLEN:** Tamanho em bytes do cabeçalho TCP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

Campos do TCP

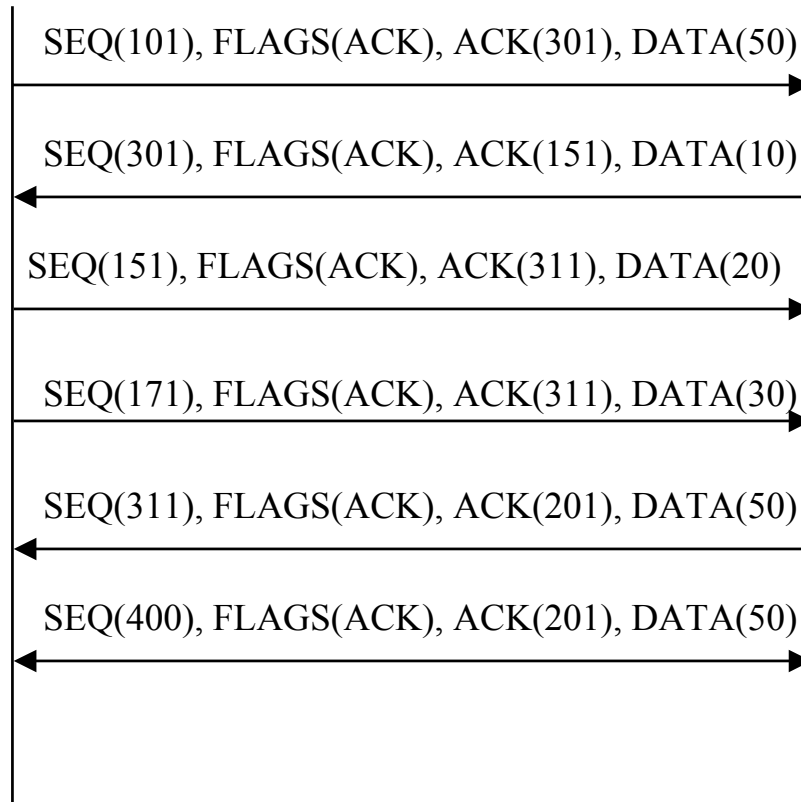


- ⌘ **Checksum:** verificador de erros de transmissão
- ⌘ **Urgent pointer:** fornece a posição dos dados urgentes dentro do campo de dados
- ⌘ **Opção:** pode conter negociação de opções tal como o MSS (Maximum Segment Size)

Estabelecimento de Conexão



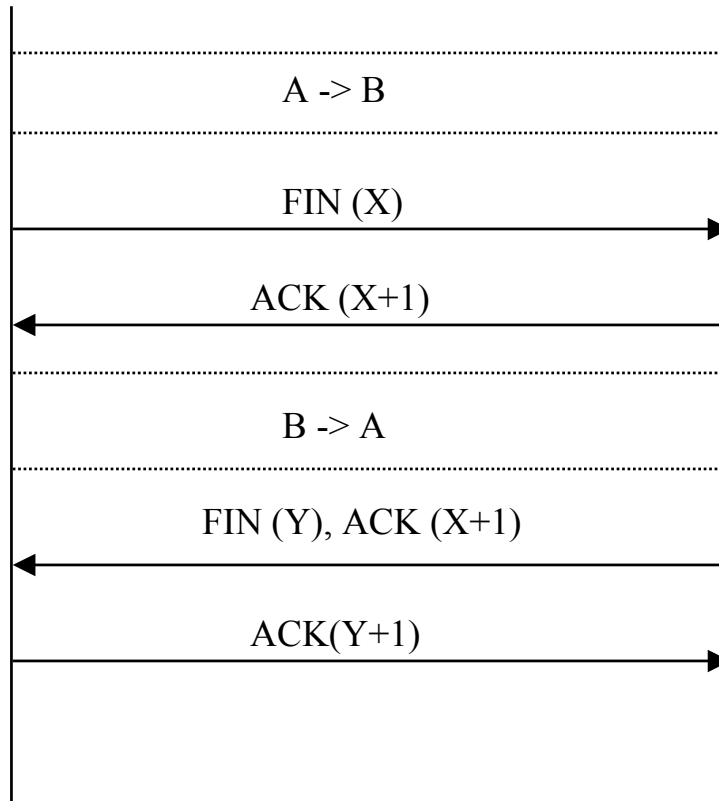
Troca de Dados



Liberação de Conexão

A

B



Porta Padrão



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

Protocolos de Aplicação

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



- ⌘ 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

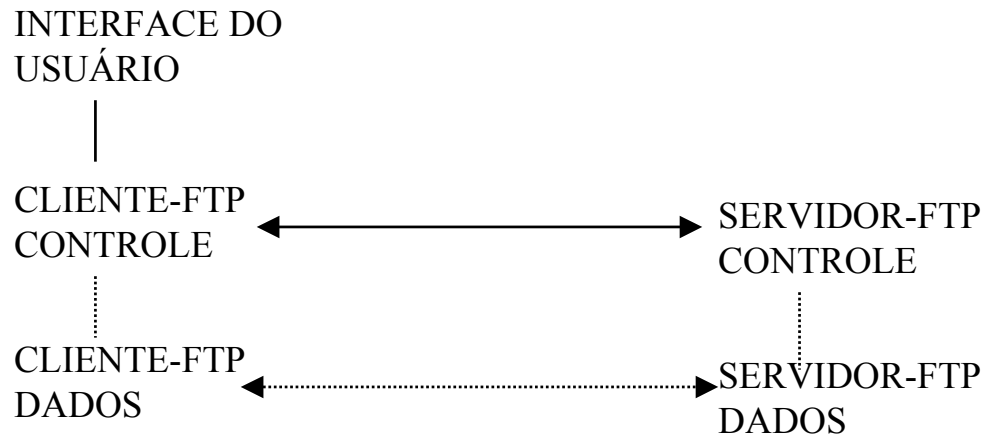
Telnet



- ⌘ 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



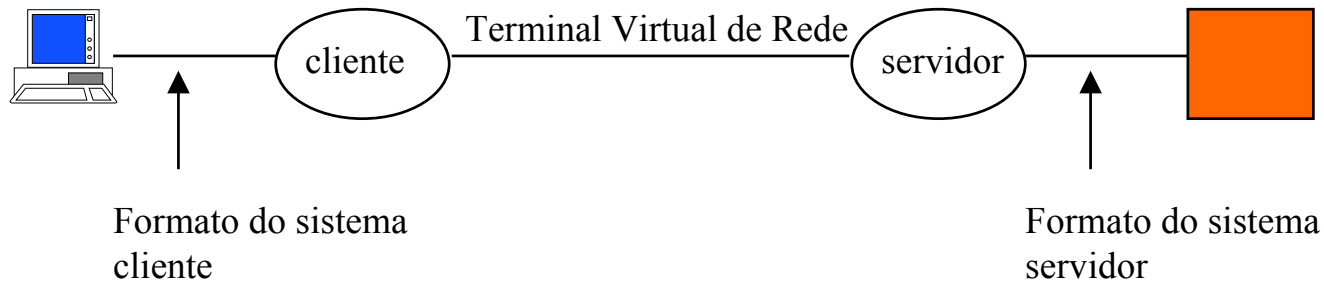
FTP



- ⌘ 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

Telnet

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



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)


Internet, WWW e Internet2

Introdução

Muito se tem se falado e se confundido na área de computação com os conceitos de *Internet, WWW e Internet 2*.


A Internet (Inter-network) surgiu do projeto ARPNET (*Advanced Research Projects Agency Network*) com suporte da ARPA (*Advanced Research Project Agency*).

O objetivo era propiciar uma rede global, com um protocolo padronizado, para troca de informação entre diferentes *hosts* a rede conectados.



O Internet conheceu seus primeiros passos nos anos 70 e nos anos 80 a rede cresceu além das fronteiras dos USA. A partir deste instante é caracterizada a rede *Internet* como conhecemos hoje em dia.

A WWW (*World Wide Web*) é uma concepção de Tim Barners-Lee do CERN (Laboratório Europeu de Pesquisa de Física Nuclear, sediado na Suíça). O objetivo da WWW é procura e recuperação da informação de uma maneira *transparente na Internet*.



A Internet2 é um esforço de estabelecimento de um ambiente para que a Internet possa suportar aplicações que requeiram uma melhor qualidade de serviço. Em outras palavras, disponibilizar para as aplicações facilidades tais como :

- uso de multimídia em tempo real;
- maior largura de banda e baixa latência;
- protocolos que permitam maior negociação de recursos e melhor desempenho de conexões.

Referências -



- <http://www.isoc.org/history/brief.html>
- <http://www.starts.com/internet/history>
- <http://let.leidenuniv.nl/history/ivh/internet.htm>
- <http://www.nsf.gov/od/lpa/news/media/fs325.htm>
- <http://www.rnp.br/rnp2/rnp2-i2-historico.html>
- <http://www.nsf.gov/od/lpa/news/media/fs325.htm>
- <http://www.isoc.org/internet/history/brief.htm>
- <http://www.isoc.org/isoc>
- <http://webopedia.internet.com/TERM/H/HTTP.html>
- <http://www.w3.org/consortium>

Referências -



- <http://www.internet2.edu/html/mission.html>;
- <http://www.rnp.br/rnp2/rnp2-i2-aplicacoes.html>
- <http://www.stars.com/internet/about.htm>
- <http://www.rnp.br/rnp2-i2-gigapop.html>
- <http://www.rnp.br/rnp2/rnp2-i2-qbone.html>



Protocolos de Roteamento

Os protocolos roteamento são as rotinas de elaboração de mapas, ou tabelas, pelas quais os roteadores descobrem o formato da rede.

Um ponto fundamental é sabermos como é efetuada a distribuição de informação de roteamento numa rede ocorre. Desta forma, a seguir vamos estudar alguns protocolos de roteamento que adotam diferentes abordagens para roteamento.



Protocolos de Roteamento

De uma maneira macro, os protocolos de roteamento são classificados como não-adaptativos e adaptativos. Onde, os protocolos não-adaptativos não consideram em suas decisões medidas ou estimativas de tráfego e a topologia da rede. Por este motivo são protocolos ditos estáticos. Em contraste, os protocolos adaptativos baseiam suas decisões como um reflexo da carga da rede e de uma possível troca da topologia da rede.



Ligação Inter-Redes

Alguns dos protocolos de roteamento mais conhecidos são :

- ***Shortest Path*** : o conceito empregado neste tipo de algoritmo é a construção de um grafo da subnet. Cada ponto do grafo representa um roteador e cada linha meio de comunicação.

Para achar uma rota entre dois roteadores quaisquer, o algoritmo acha a rota com menor distância (*shortest path*).

Diversas métricas são empregadas neste tipo de protocolo, tais como o número de *hops* e distância.

Vale lembrar que protocolos baseados nesta abordagem são estáticos.



Ligação Inter-Redes

- ***Flooding*** : este tipo de protocolo estático é baseado na técnica de que cada pacote que chega será enviado para todas as interfaces do roteador, exceto aquela pela qual o pacote chegou. A conclusão mais óbvia, é que este tipo de abordagem provoca uma ***inundação*** de pacotes. Existem procedimentos chamados de *represadores*, que ajudam a melhorar o desempenho deste tipos de algoritmos.

Dentre estas técnicas temos :

- (1) Contadores de hops - faz o decremento a cada *hop*.
- (2) Reconhecimento de pacotes *flooding* - estes não serão reenviados.
- (3) Flooding seletivo - só é feito um broadcast numa determinada direção.



Ligação Inter-Redes

Os protocolos baseados em *flooding* embora pareçam não práticos, estes são utilizados onde uma solução robusta é necessária. Exemplos práticos são (1) o caso de redes militares onde todos roteadores devem ser notificados para uma dada aplicação e (2) em banco de dados distribuídos, onde muitas vezes todas as bases devem ser atualizadas.



Ligação Inter-Redes

- ***Flow-Based*** (Baseado em fluxo) - neste método estático a carga de ligação entre dois pontos quaisquer e a topologia são levados em consideração. As métricas (carga e topologia) são conhecidas previamente para a consideração do roteamento nos protocolos baseados nesta abordagem.



Ligação Inter-Redes

- ***Distance Vector*** (Vetor de distância) - a maioria das redes modernas empregam algoritmos de roteamento dinâmico. O algoritmo conhecido por *distance vector* é um dos dois mais utilizados. A concepção deste protocolo é manter sua tabela (ou vetor) com as melhores distâncias para cada destino através de uma específica linha. O vetor é mantido atualizado através do processo dinâmico de troca de informação com seus roteadores vizinhos. Algumas informações do vetor são (por exemplo) o número de hops, o tempo de retardo em milissegundos e o número total de pacotes enfileirados ao longo do *path* (caminho).



Ligação Inter-Redes

- ***Link State*** - este protocolo com abordagem dinâmica é um dos dois mais populares algoritmos empregado em redes modernas. O link state, substituiu o protocolo vetor distance na rede ARPANET. Dentre as razões, a métrica de distância não leva em consideração a larga de banda das linhas e o conceito de vetor demora muito na convergência. São cinco os pontos, nos quais este protocolo se baseia:
 - Descobrir seus vizinhos e descobrir seus endereços de rede;
 - Calcular o retardo ou custo para cada de seus vizinhos;
 - Construir um pacote contanto tudo o que ele aprendeu;
 - Propagar o pacote sabidinho para todos os roteadores;
 - Computar o menor caminho para todos os outros roteadores.



Ligação Inter-Redes

- ***Hierarchical Routing*** - não é possível que com o crescimento exponencial de uma rede que os protocolos até então apresentados possam atender plenamente a função de roteamento com sucesso. No roteamento conhecido por *hierarchical*, temos o roteamento em áreas chamadas de *regiões*. Cada roteador somente conhece sua região. Para grandes redes são necessárias algumas subdivisões para que os roteadores possam trabalhar com eficiência, tais como cluster de regiões, zonas de clusters, grupos de zonas e assim por diante.



Ligação Inter-Redes

- **Broadcast** - Numa abordagem do tipo broadcast enviam-se pacotes para todos simultaneamente. Aplicações como previsão do tempo e bolsa de valores são típicos exemplos onde temos que possuir uma rede que possa absorver informações desta maneira. Vários protocolos podem implementar o broadcasting, exemplos de algoritmos são :

- (1) Um algoritmo de broadcast simples;
- (2) Um algoritmo de flooding;
- (3) Um algoritmo de multidestinos.



Ligação Inter-Redes


- ***Multicast*** - a idéia de enviar pacotes para um grupo seletivo é chamado de *multicasting* e os protocolos que implementam este tipo de roteamento são denominados de *algoritmos multicast*. Nesta abordagem é necessário que a figura de gerência de grupo exista. Ou seja, a necessidade de criação/destruição de grupos junto com a requisição de processos que requerem sua junção/disjunção a um determinado grupo são exemplos de tarefas a serem efetuadas pelo protocolo de multicast.

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 $3.4 \times (10^{38})$.

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 ?

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 :


0 4 16 24 31

VERS	FLOW LABEL		
PAYLOAD LENGTH		NEXT HEADER	HOP LIMIT
SOURCE ADDRESS			
DESTINATION ADDRESS			

Interessante de se notar que o IPv6 Base Header possui menos informação que um header do datagrama IPv4. A causa para tal fato foi a remoção dos campos de opções e alguns campos fixos para o extension headers. Assim vale os comentários :

- O TTL foi substituído pelo HOP LIMIT;
- O Service Type foi trocado pelo FLOW LABEL
- O campo do protocolo foi trocado pelo campo NEXT HEADER;
- O campo HEADER LENGTH foi eliminado e o campo PAYLOAD LENGTH é agora usado.

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.

O formato de um IPv6 fragment extension header é ilustrado abaixo :

0 8 16 29 31

N. Header	Reserved	Fragment Offset	MF
Identificação do Datagrama			

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.

Conteúdo



IV-Dispositivos de interconexão de redes.

V - Arquitetura TCP/IP.

VI - Redes de alta velocidade

(FDDI, ATM, Fast Ethernet, Myrinet).

VI - Redes de Alta Velocidade



FDDI (Fiber Distributed Data Interface) é uma rede em anel duplo, que emprega cabos de fibra-ótica para implementar uma rede rápida e segura. A rede FDDI implementa o protocolo token-passing e vários quadros podem ser transmitidos simultaneamente.

O FDDI-I era implementado a 100Mbps e o FDDI- III já possui velocidade da ordem de Gbps.

Asynchronous Transfer Mode (ATM)

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;

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 sequência 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.

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 eficientes;
- 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.

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.

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 Fórum 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 *engarrafamento* da rede.

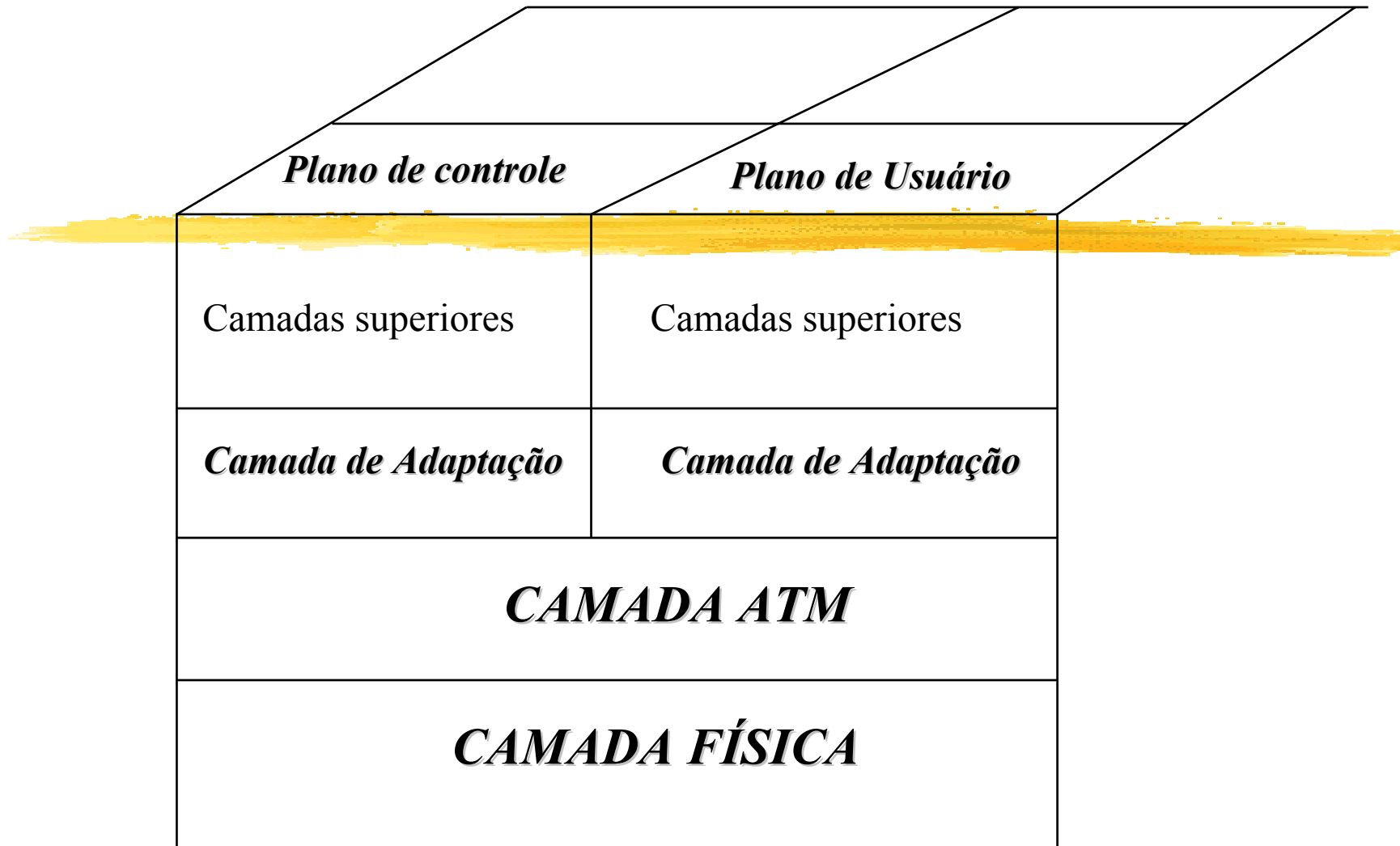
O campo CLP é setado para 0 inicialmente nas células. Quando as mesmas trafegam pela rede e um determinado *switch* observa que existe um congestionamento, a célula terá seu CLP modificado para 1 pelo *switch*. Esta mudança sinaliza que não existe condição de ser atendido os parâmetros negociados durante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



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.

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.

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*;

ATM x Gigabit Ethernet

A thick, horizontal yellow brushstroke with a textured, painterly appearance, spanning most of the width of the slide.

- 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.