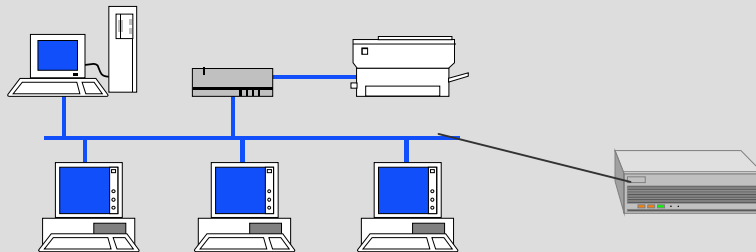


Curso de Administração e Gerência de Redes



Prof. Mario Dantas, PhD

Conteúdo

1. Introdução a Administração e Gerência Redes :
 - conceitos iniciais de A&G
 - estado da arte das redes e sistemas distribuídos
 - arquitetura de redes
 - arquitetura de protocolos
2. Princípio, Organização e Metodologia
3. Tecnologia

Conteúdo

- Recursos Humanos
- Ambientes de Administração e Gerência
- Tendências Futuras

Bibliografia

Network Management – Principle and Practice, **Mani Subramanian**, ISBN 0-201-357442-9, Addison-Wesley, 2000.

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

Bibliografia

A practical guide to effectively managing Cisco network devices, Della Maggiora, Paul L.; Elliott, Christopher E.; Phelps, Kent J.; Pavone, Robert L.; Thompson, James M., Cisco Press, 2000, ISBN 1578701805.

Bibliografia

Managing Computer Networks: A Case-Based Reasoning Approach, **Lundy Lewis**, Artech House, 1995.

TMN: Telecommunications Management Network

Divakara K. Udupa, McGraw-Hill, 1999. ISBN 0-07-065815-3.

Bibliografia

Network Management Systems Essentials **Divakara K. Udupa**, McGraw-Hill, ISBN 0-07-065766-1.

Internetworking with TCP/IP Volume I e II: Design, Implementation, and Internals, Comer, Douglas E., and Stevens, David L., *Prentice-Hall*.

I - Introdução a Administração e Gerência



Administração e Gerência



Na sua opinião como poderíamos definir as seguintes funções em um ambiente computacional:

- Suporte**
- Administração**
- Gerência**

Estrutura Organizacional



Estruturas

- *Decisão* - prove um conjunto de objetivos da organização,
- *Produção* - efetua ações para atingir os objetivos,
- *Informação* - assegura a comunicação entre as partes da organização.

Sistemas Administrativos

Totalidade - o sistema pode ser considerado um todo coerente e indivisível, não aparentando ser um conjunto de elementos simples.

Retroação - esse paradigma pode ser entendido como o uso de informações de entrada, aquelas oriundas da saída do sistema.

Equifinalidade - os mesmos resultados podem ter origens diferentes. Os resultados não são determinados apenas pelas condições iniciais, mas também pelo processo em execução.

Administração e Gerência de Redes

Podemos imaginar os seguintes tópicos como relevantes na A&G das redes :

- Prestação de serviço,**
- Atingir a satisfação de requerimentos de clientes,**
- Compreender a natureza do serviço a ser prestado,**
- Compreensão de métodos adequados a A&G do serviço.**

Alguns pontos comuns de requisições dos clientes, são :

- Alta disponibilidade,
- Integridade do ambiente,
- Segurança,
- Flexibilidade de acesso físico e lógico,
- Alto desempenho,
- Controle e racionalização de custos.

A utilização de *acordos de nível de serviços* tem como objetivo o estabelecimento de :

- distribuição de responsabilidades sobre serviços,
- padrões de uso e modificações no ambiente,
- rotinas de salvaguarda do sistema (backup comuns e aqueles que requerem uma maior complexidade),
- ações a serem todas em casos extremos,
- distribuição de custos e facilidades.

Serviços de Redes

☆ Complexidade da estrutura e funcionamento :

- Em grandes redes temos diferentes topologias e tecnologias,
- Podemos imaginar uma *grande* quantidade de informação,
- Informações sensíveis ou críticas,
- Inúmeros serviços.

🕒 Prestação como commodities

- Sociedade,
- Empresas,
- Residências.

Serviços de Redes

Serviços integrados

- Redes de dados usando banda larga,
- Redes a cabo de TV,
- Redes de serviços integrado (voz, dados, imagem, etc).

Ciclos dos Serviços de Rede

I - Ciclo de vida

- Estratégico**
- Operacional**

II - Escopo de Ações

- Estratégica**
- Tática**
- Execução**

III - Efeitos das Ações

- Longo Prazo**
- Imediato**

Administração e Gerência de Redes

Definição :

A administração e gerência das redes compreendem as *atividades* e *processos* de trabalho das *informações*, obtidas e manipuladas por *pessoas* inseridas em uma *estrutura organizacional*, que utilizam *tecnologias* e *ferramentas*, para assegurar o *serviço de rede* sob determinadas condições.

Administração e Gerência de Redes

Para execução de uma A&G devemos sempre considerar :

- Pessoal
- Ferramentas
- Conhecimento dos processos
- Conhecimento do ambiente

Administração e Gerência de Redes

Repensando uma A&G de Redes

- Avaliação da estrutural atual de A&G,
- Levantamento de solicitações e dificuldades,
- Escolha de uma estrutura de A&G,
- Processos e fontes de informação para a A&G

Administração e Gerência de Redes

Repensando uma A&G de Redes

- Controles :
 - do nível de serviço
 - garantia de qualidade
- Tecnologias e Ferramentas
- Recursos humanos
- Aspectos políticos

Estado da Arte das Redes e Sistemas Distribuídos



**Considerando um ambiente de redes
como definir :**

- LAN**
- MAN**
- WAN**

LANs/WANs e MAC

As características das LANs e WANs devem ser observadas para que tenhamos implementados eficientes MACs. Diferenças de taxas de erro e algoritmos de roteamento dos pacotes.

LANs : as taxas de erros estão compreendidas entre 10^{-8} à 10^{-11} , enquanto que o roteamento usual é o broadcast;

WANs : os erros, geralmente, ocorrem com uma frequência entre 10^{-5} à 10^{-7} e diferentes (e complexos) algoritmos de roteamento são empregados.

LANs/WANs e MAC

Um outra característica interessante que diferencia as duas tecnologias é a abordagem de utilização.

Nas LANs os administradores procuram evitar o intenso uso dos nós aos mesmo tempo, devido a característica de acesso ao meio (***broadcast***).

Por outro lado, nas WANs o ***emprego intensivo*** significa um melhor uso dos enlaces e recursos disponíveis.

LANs/WANs e MAC

Recentemente as LANs vêm sendo classificadas em quatro categorias :

- (1) Baixa e Média Velocidade - entre 10 e 20 Mbps;
- (2) Alta Velocidade - entre 50 e 150 Mbps;
- (3) *Supercomputer LANs* - entre 800 e 1600 Mbps;
- (4) Ultragigabit - redes da ordem de Tbps.

LANs/WANs e MAC

Os protocolos de acesso (usualmente) consideram três dimensões, estas :

- O tempo (síncrono ou assíncrono);
- A topologia (barra, anel, estrela, árvore e multicanal);
- Modo de acesso (aleatório, ordenado ou híbrido).

LANs/WANs e MAC

A topologia *estrela* é caracterizada por um nó central, no qual todos as *estações* estão interconectadas. O nó central pode implementar uma ligação passiva (*hub*), ou ativa (*switched*).

As redes com topologia *estrela* são mais apropriadas para as redes de alta velocidade devido a fácil conexão entre seus pontos finais (ligação ponto-a-ponto) através de fibra ótica.

LANs/WANs e MAC

A topologia *árvore* (*tree*) é uma generalização das configurações em *estrela*. Uma *árvore* consiste de uma estrutura hierárquica, onde as *estações* são as folhas. As *estações* são ligadas a outras *estações* de outro nível por intermédio de enlaces óticos. Todos os níveis são conectados ao nível *maior* da estrutura.

Existe na atualidade um grande interesse no desenvolvimento de redes com topologia em *árvore*. Entre os motivos podemos visualizar a escalabilidade, modularidade e enlace de alta velocidade.

ESTUDO DE CASO

Exemplo A

Um exemplo de rede com MAC *Collision Avoidance Star and Tree Network* é a conhecida *Supernet*.

A arquitetura *Supernet* é uma rede a 100 Mbps, consistindo de um par de árvores com a fibra ótica como meio físico de conexão. O par de árvores é conhecido como *selection tree*.

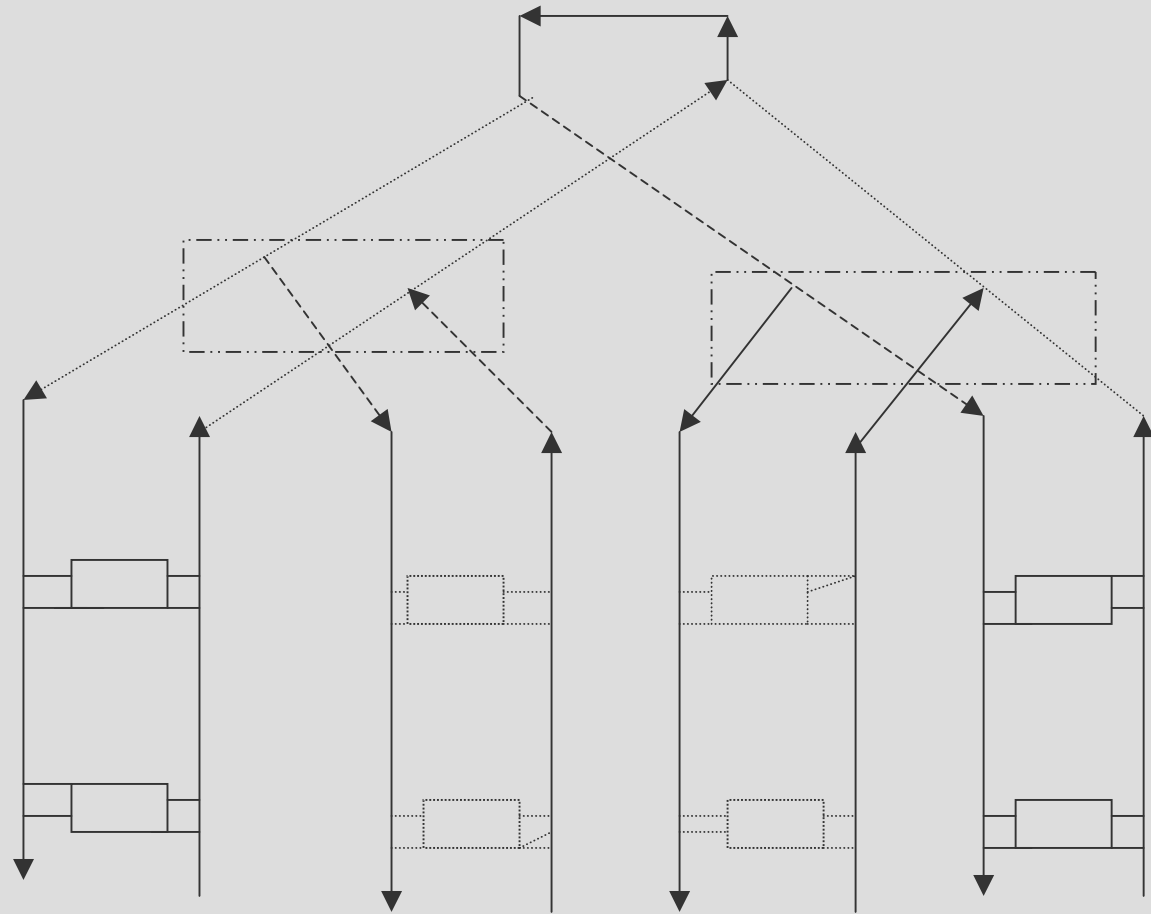
ESTUDO DE CASO

Exemplo A

Na *Supernet* o roteamento é efetuado por um nó concentrador central. Os nós internos da árvore são denominados de *subhubs* e trabalham de forma análoga ao concentrador central.

As estações são interligadas as duas árvores por intermédio de dispositivos inteligentes chamados de *NAC (Network Access Controllers)*.

Supernet Architecture

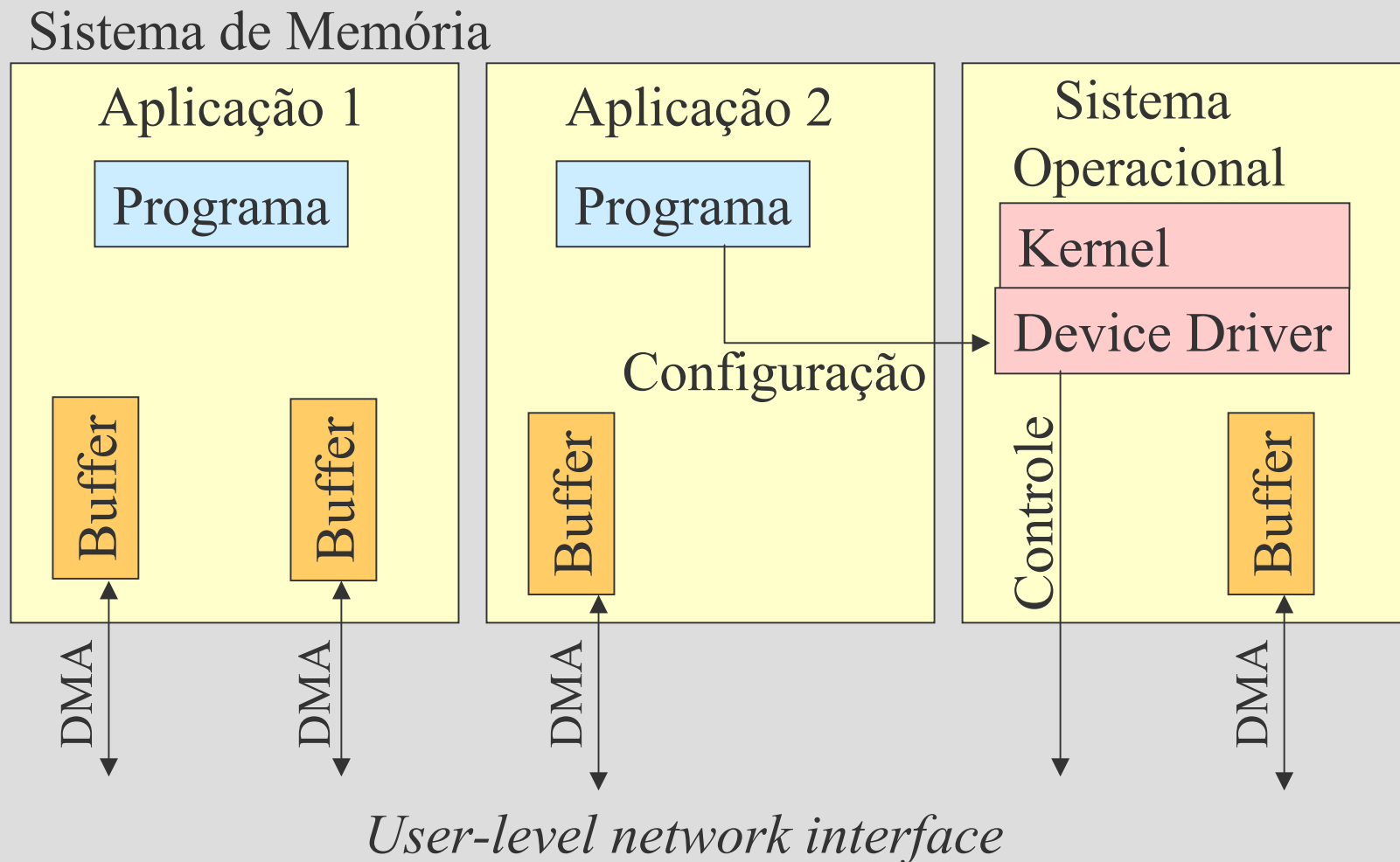


**Considerando um ambiente de redes
como definir :**

- SAN**

- PSTN**

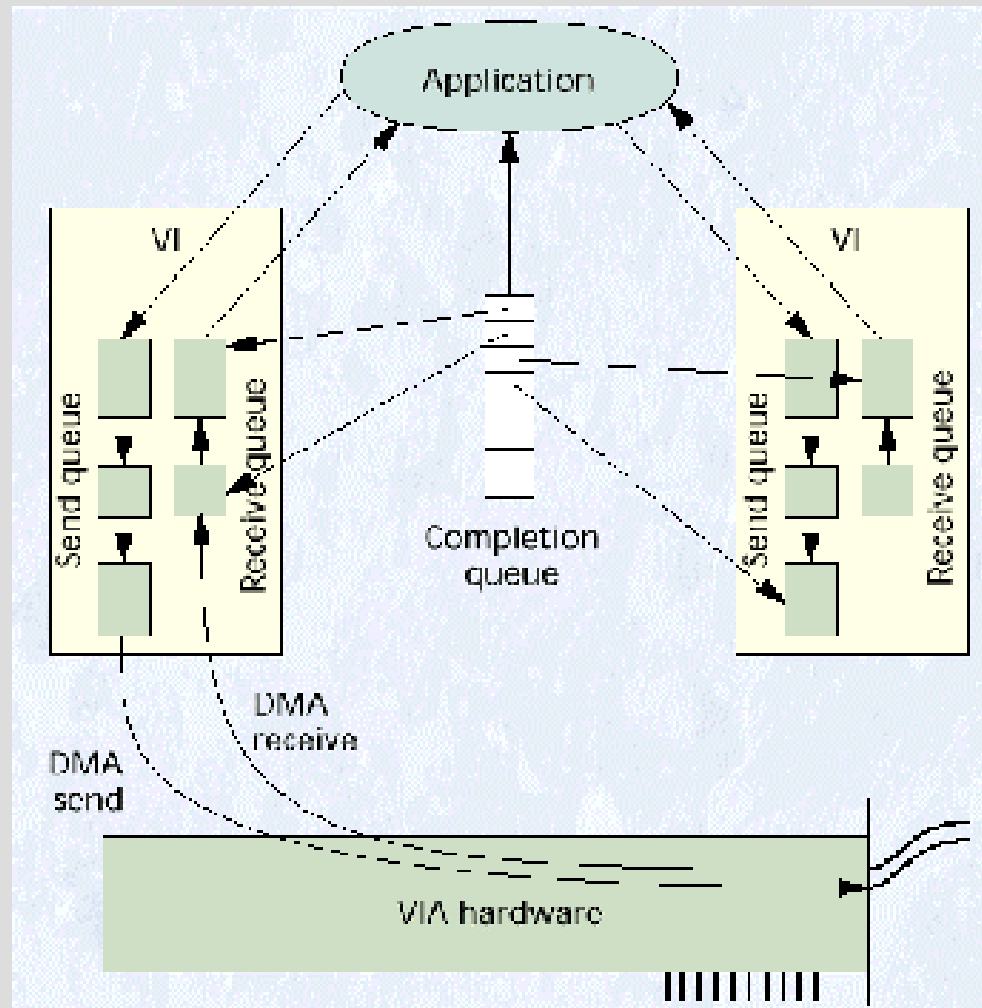
Desempenho no Projeto da Interface



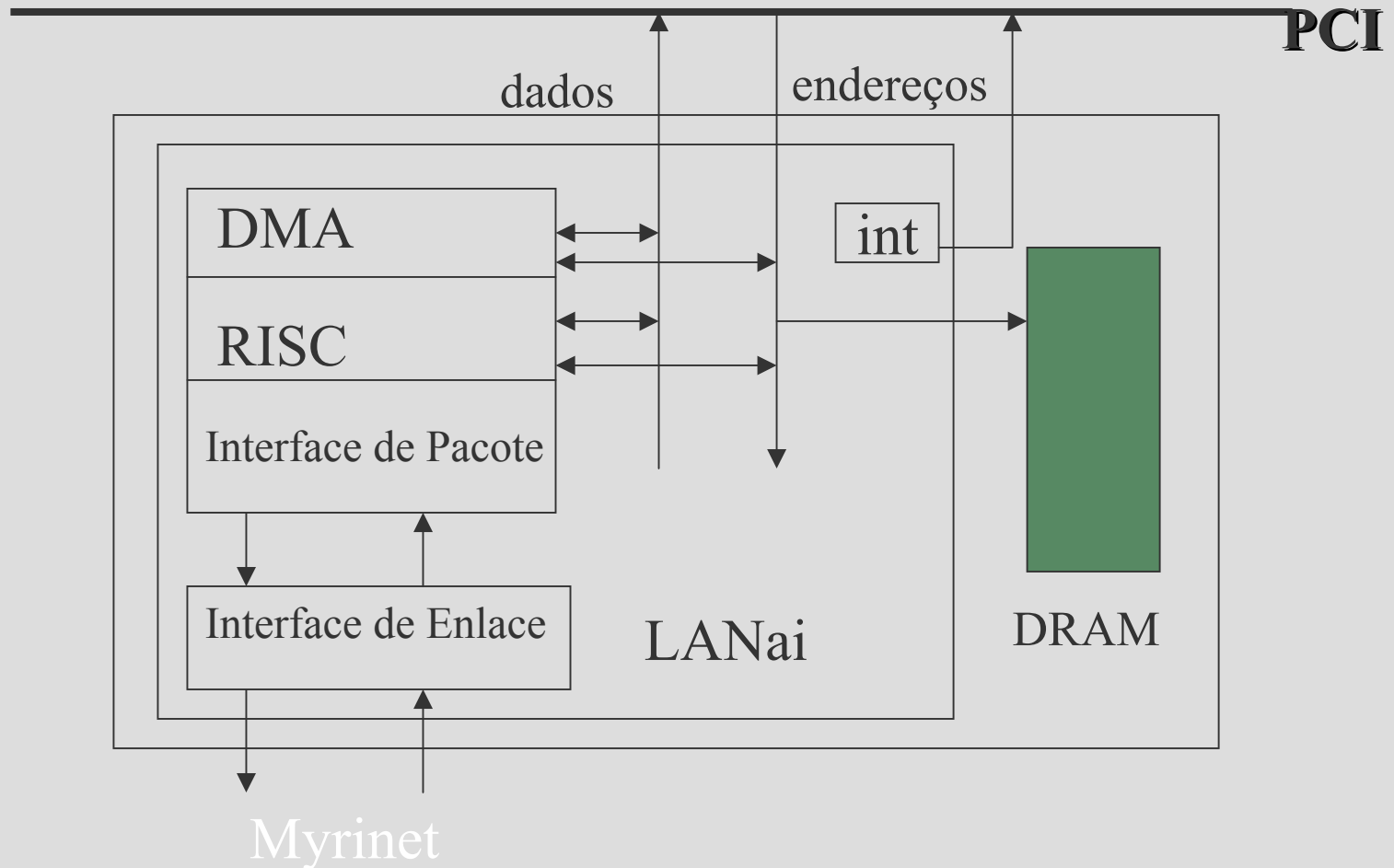
Desempenho no Projeto da Interface

VIA

- Send List
- Receive List



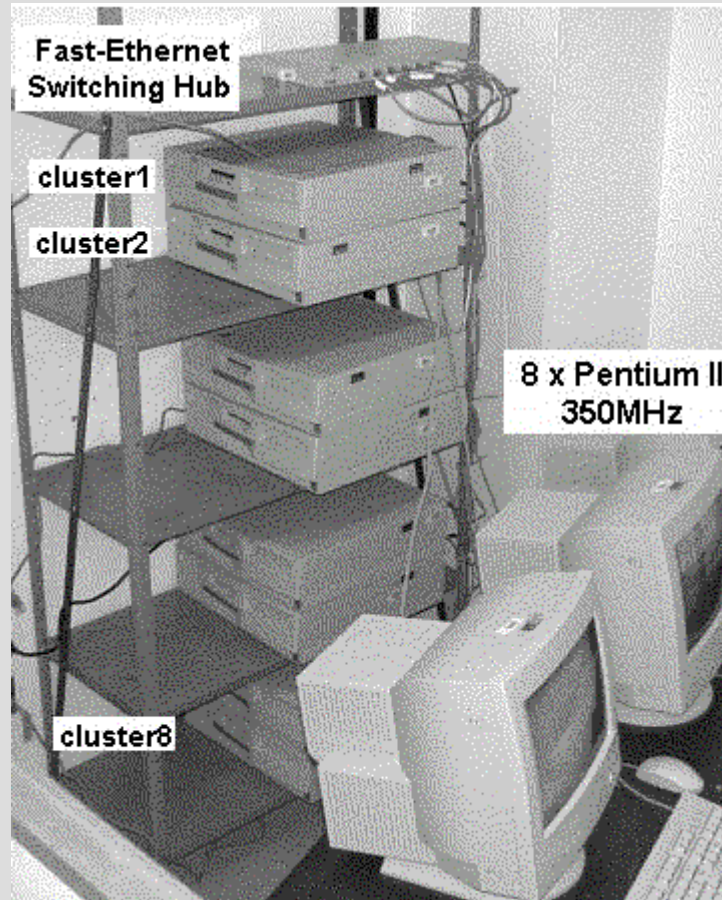
A Interface Host Myrinet



Considerando ambientes distribuídos em redes como definir :

- Cluster**
- Grid**
- Computação Paralela**

Exemplo de Cluster



Das Redes aos GRIDs



O GRID

O paradigma do GRID por ser considerado uma abordagem **nova** nos obriga a adotar uma nova forma de trabalho. Em outras palavras, devemos buscar a ***interoperabilidade distribuída entre diferentes sites***.

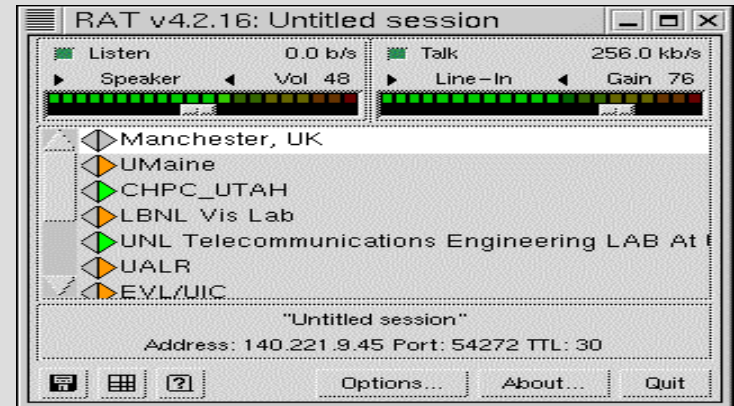
Um exemplo de esforço neste sentido é o projeto CAVE Research Network. Este ambiente permite o compartilhamento colaborativo de espaço virtual.

Estudo de Caso : *Access Grid*

1. Nova geração de video conferência
- 2 Permite a colaboração entre profissionais
3. Objetivo Original – recriar um ambiente informal das conferências

Technologia Access Grid

- Roda na Internet
- Software é aberto
- Relativamente barato



Fatores Positivos Access Grid

- Audio Natural
- Grande display
- Software colaborativo

Uso do Access Grid

- Painel de discussões
- Aulas Distribuídas
- Conferências
- (Amizade com a sogra a distância)

Agente Jota

JOTA Agent

Configure Help












Active Hosts

Get Information

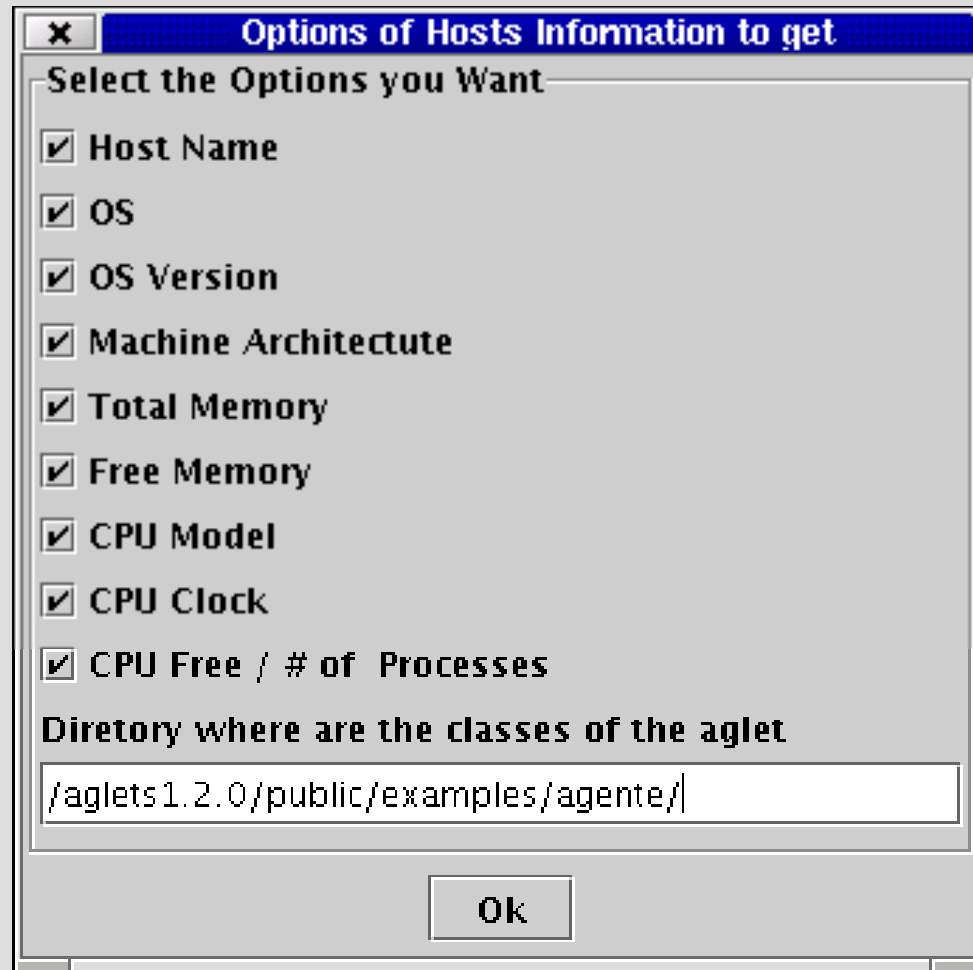
Applications:

- ☒ Gaussian
- ☐ PI Computation
- ☐ Matrix Multiplication

Run

laico5.laico.cic.unb.br  Host: laico5.laico.cic.unb.br OS: Linux Version: 2.2.17-14cl Architecture: i386 Total Mem.: 159.0 MB Free Mem.: 36.0 MB CPU: 348 MHz Model: Pentium II (Deschutes) CPU Free: 97.00% Process: 67 <input type="checkbox"/> Use this Host	laico4.laico.cic.unb.br  Host: laico4.laico.cic.unb.br OS: Linux Version: 2.2.17-14cl Architecture: i386 Total Mem.: 91.0 MB Free Mem.: 2.0 MB CPU: 233 MHz Model: Pentium MMX CPU Free: 78.70% Process: 73 <input type="checkbox"/> Use this Host	laico3.laico.cic.unb.br  Host: laico3.laico.cic.unb.br OS: Linux Version: 2.2.17-14cl Architecture: i386 Total Mem.: 123.0 MB Free Mem.: 2.0 MB CPU: 233 MHz Model: Pentium MMX CPU Free: 93.50% Process: 71 <input type="checkbox"/> Use this Host	laico07.laico.cic.unb.br  Host: laico07.laico.cic.unb.br OS: Linux Version: 2.2.17-14cl Architecture: x86 Total Mem.: 158.0 MB Free Mem.: 46.0 MB CPU: 348 MHz Model: Pentium II (Deschutes) CPU Free: 60.20% Process: 72 <input type="checkbox"/> Use this Host
164.41.14.145   <input type="checkbox"/> Use this Host	164.41.14.146   <input type="checkbox"/> Use this Host	laico2.laico.cic.unb.br  Host: laico2.laico.cic.unb.br OS: Linux Version: 2.2.17-14cl Architecture: i386 Total Mem.: 61.0 MB Free Mem.: 1.0 MB CPU: 233 MHz Model: Pentium MMX CPU Free: 90.90% Process: 84 <input type="checkbox"/> Use this Host	164.41.14.150   <input type="checkbox"/> Use this Host

Agente Jota



Agente Jota

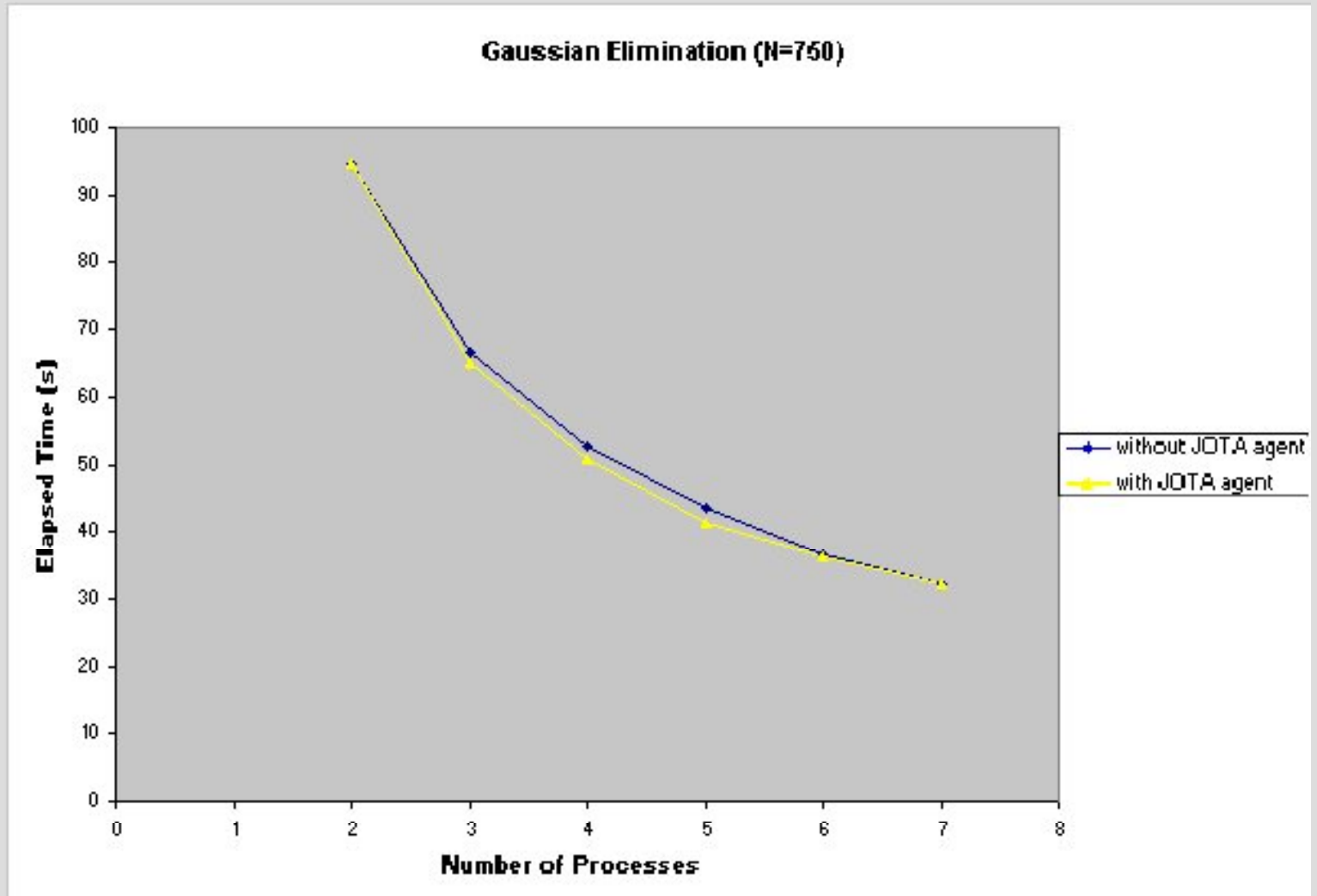
laico5.laico.cic.unb.br



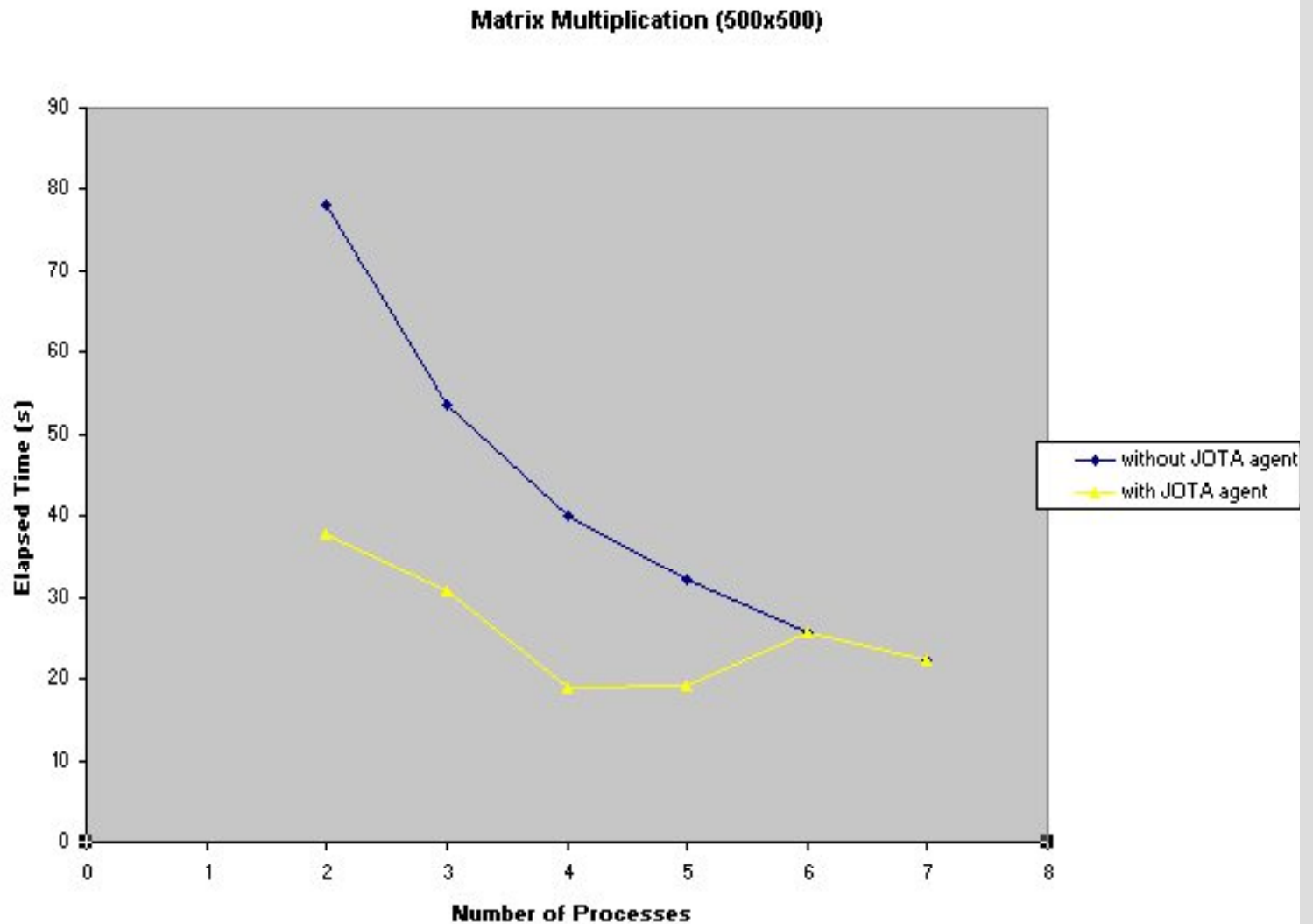
Host: laico5.laico.cic.unb.br
OS: Linux
Version: 2.2.17-14cl
Architecture: i386
Total Mem.: 159.0 MB
Free Mem.: 36.0 MB
CPU: 348 MHz
Model: Pentium II (Deschutes)
CPU Free: 97.00%
Process: 67

☐ Use this Host

Agente Jota

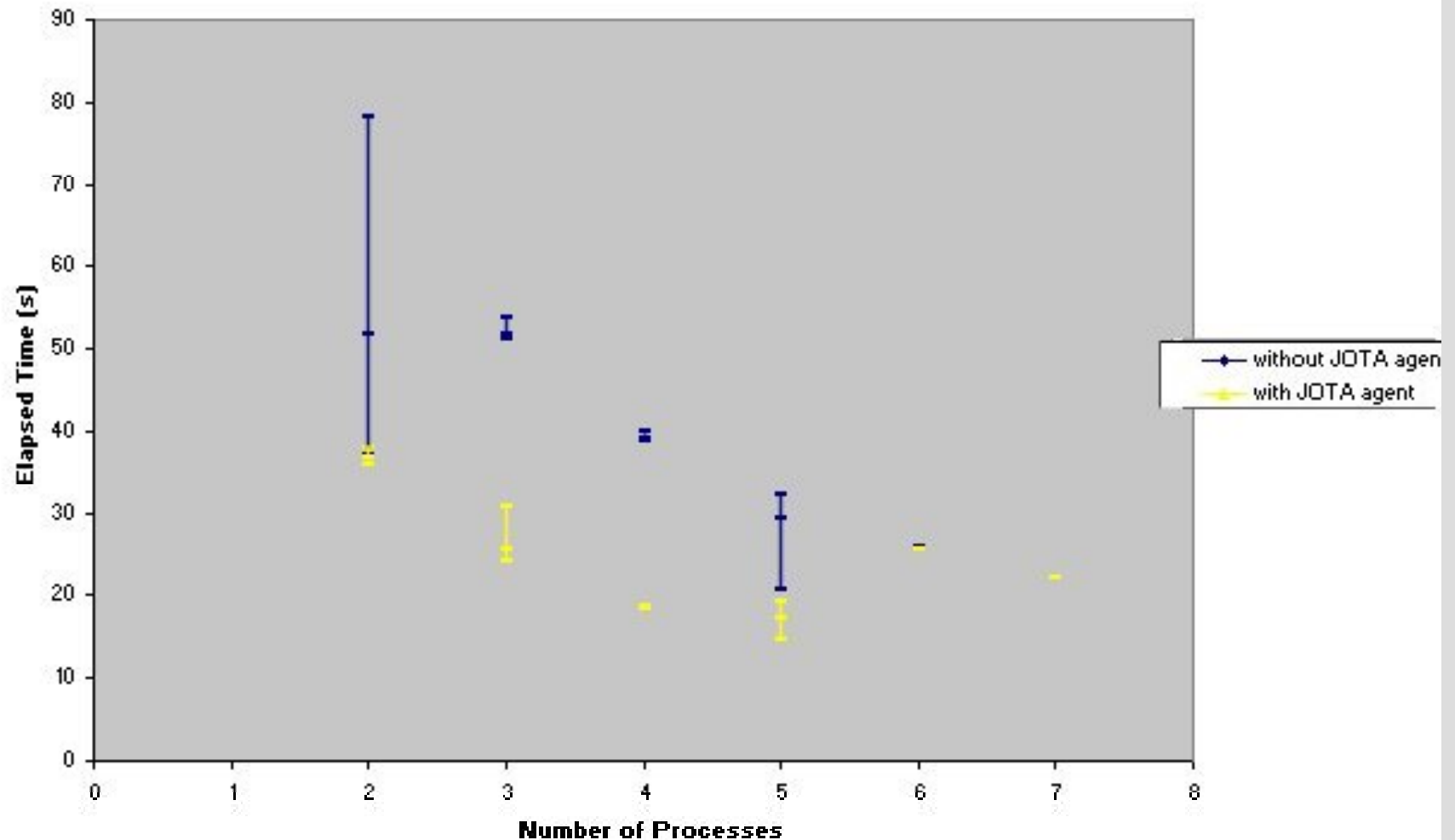


Agente Jota



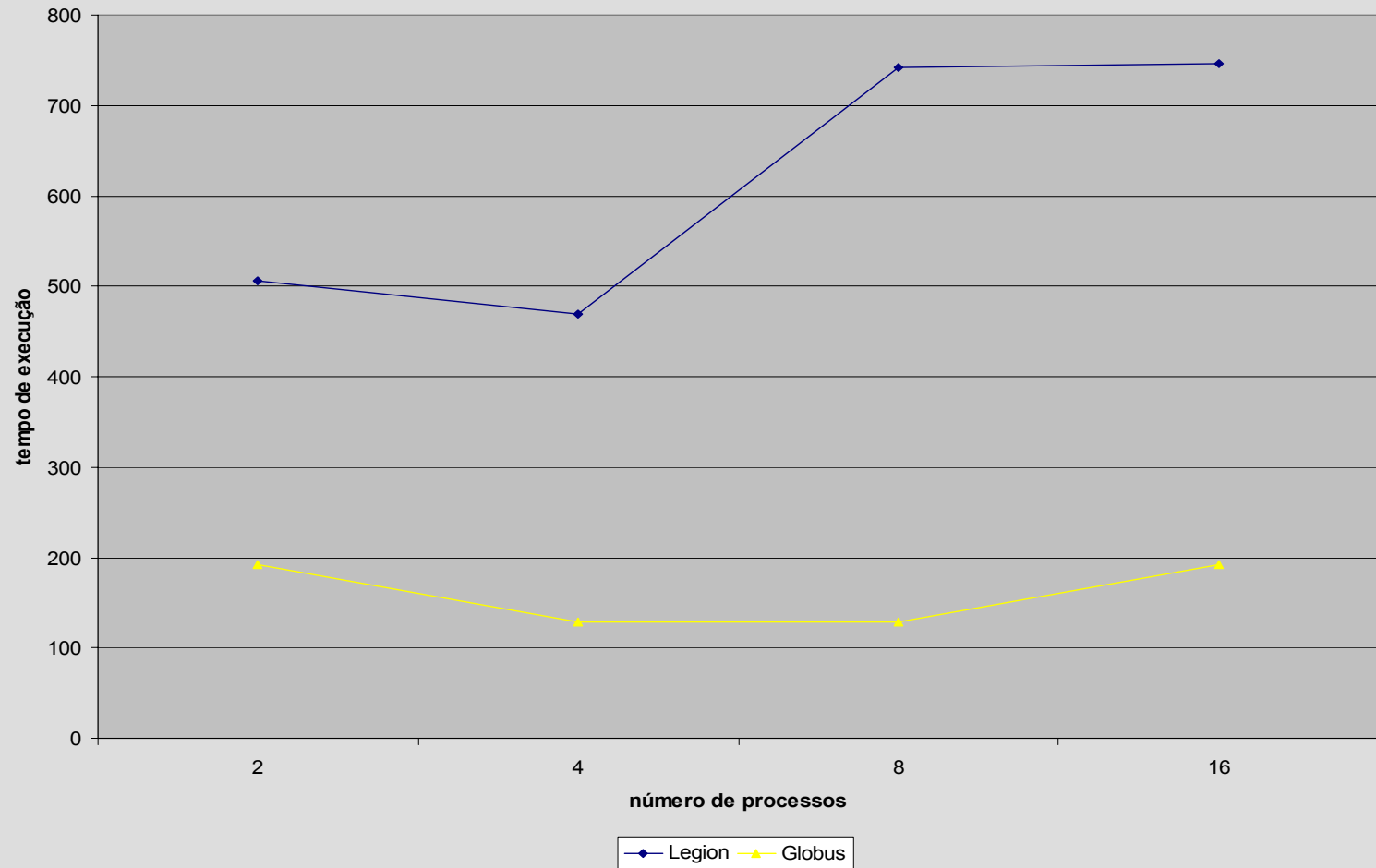
Agente Jota

Matrix Multiplication (500x500)



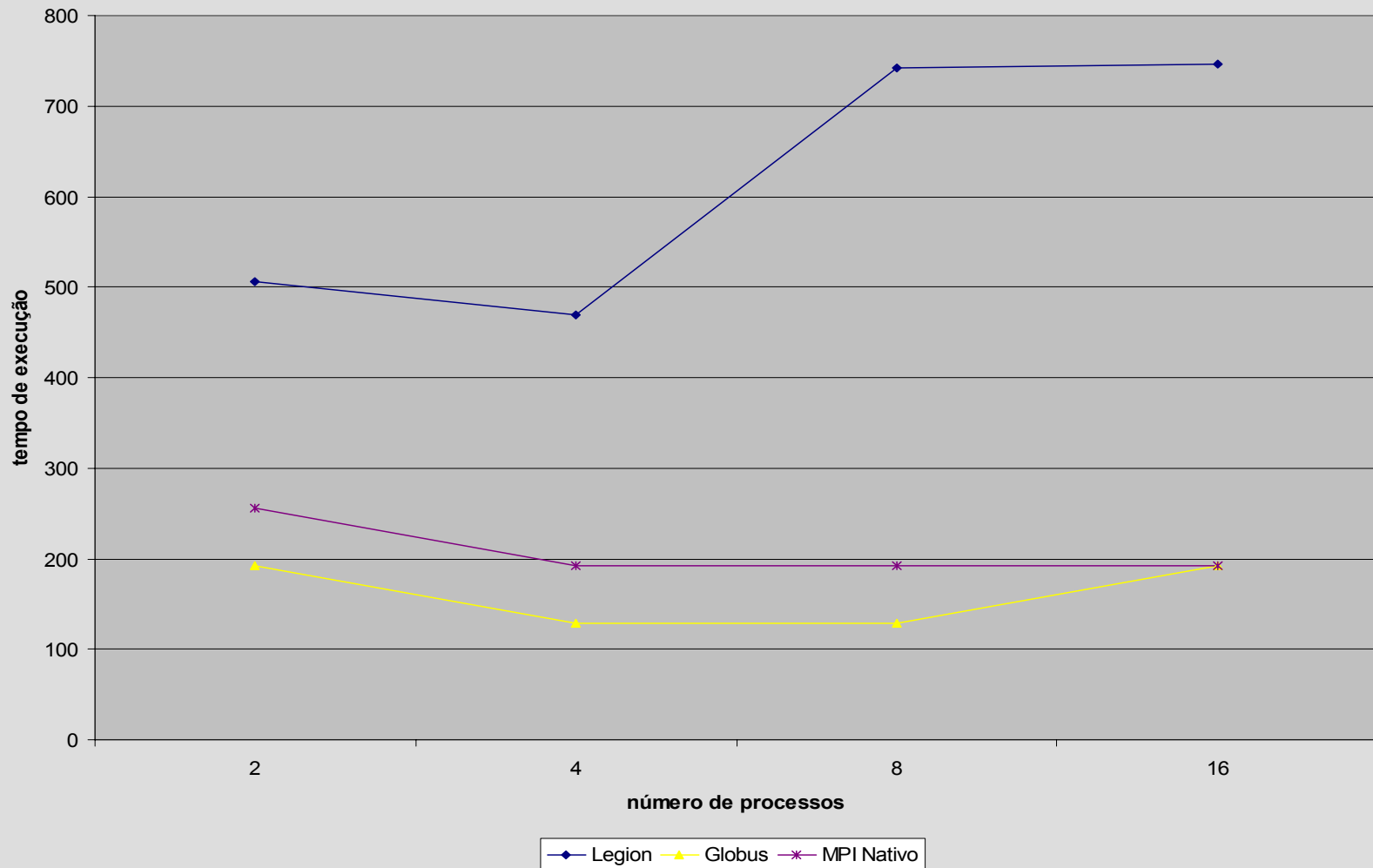
Agente Jota

Multiplicação de Matrizes (500x500)



Agente Jota

Multiplicação de Matrizes (500x500)

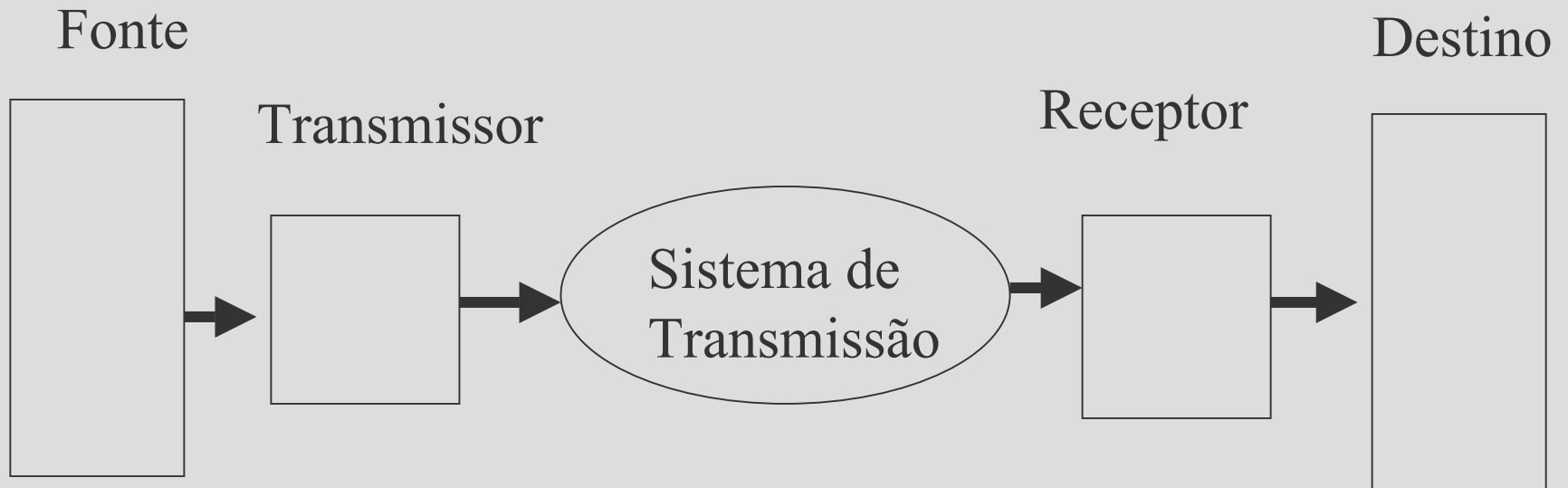


Revisão de Arquitetura de Redes



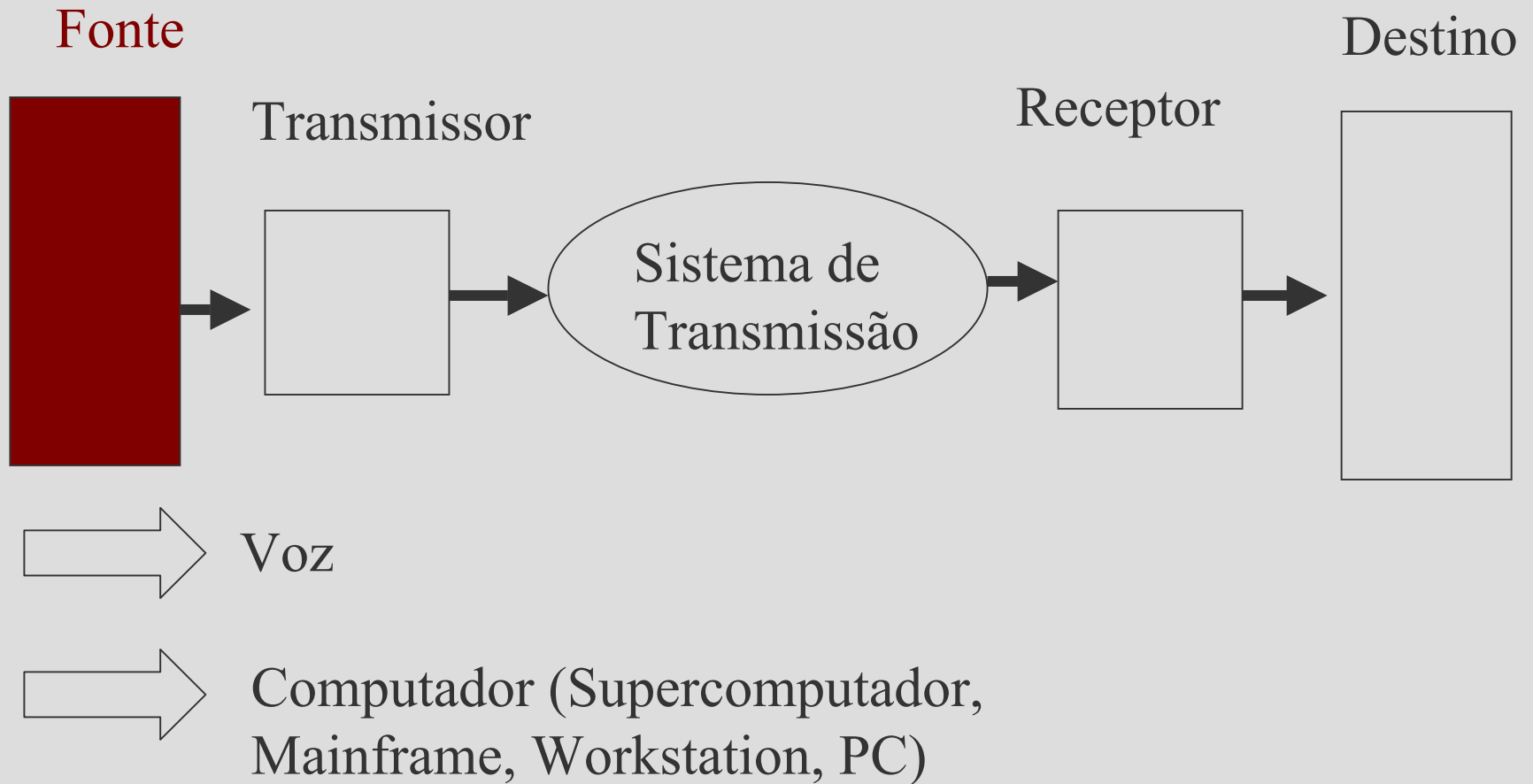
Conceitos de Comunicação

Modelo Genérico de Comunicação



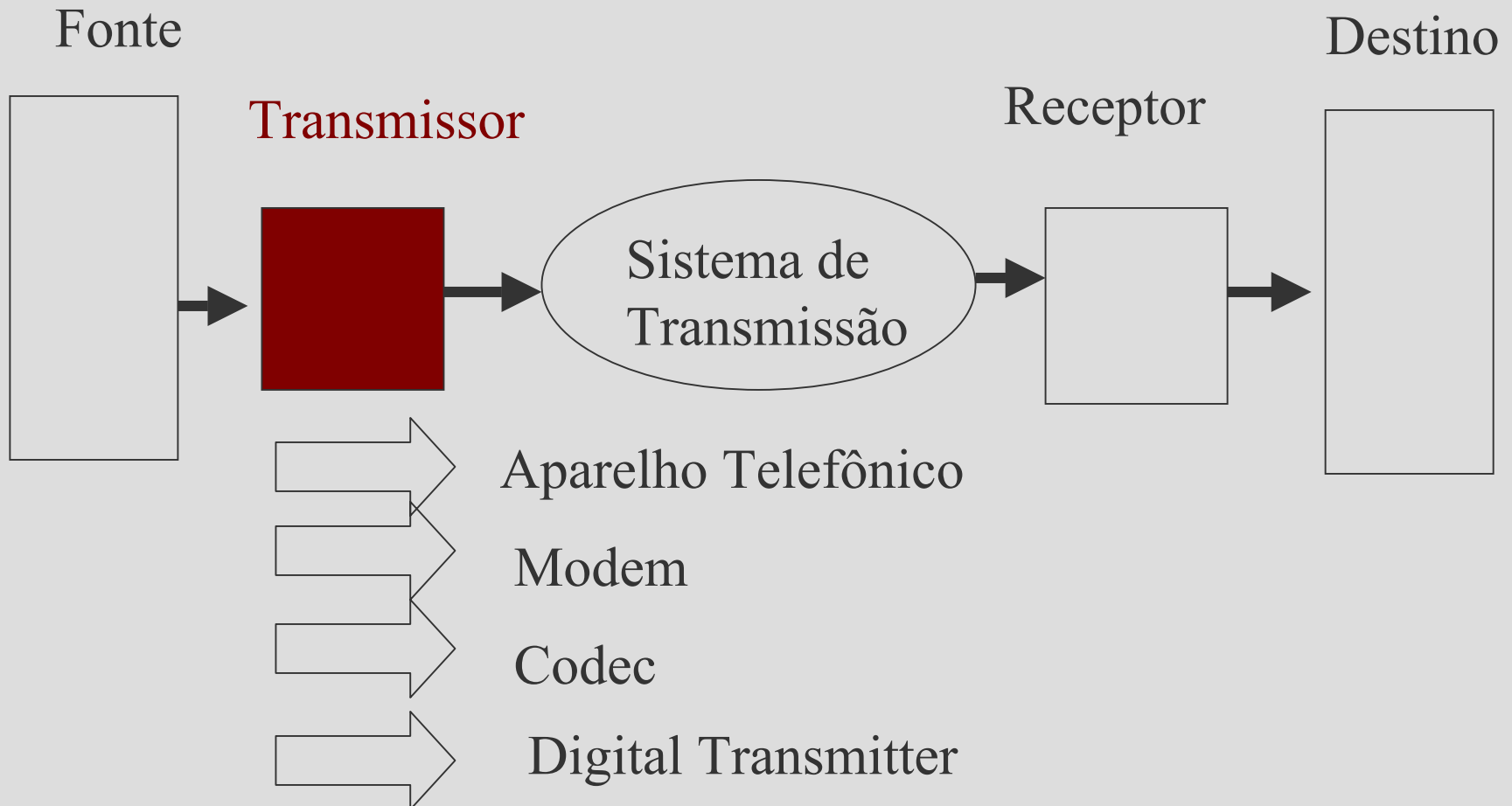
Conceitos de Comunicação

Modelo Genérico de Comunicação



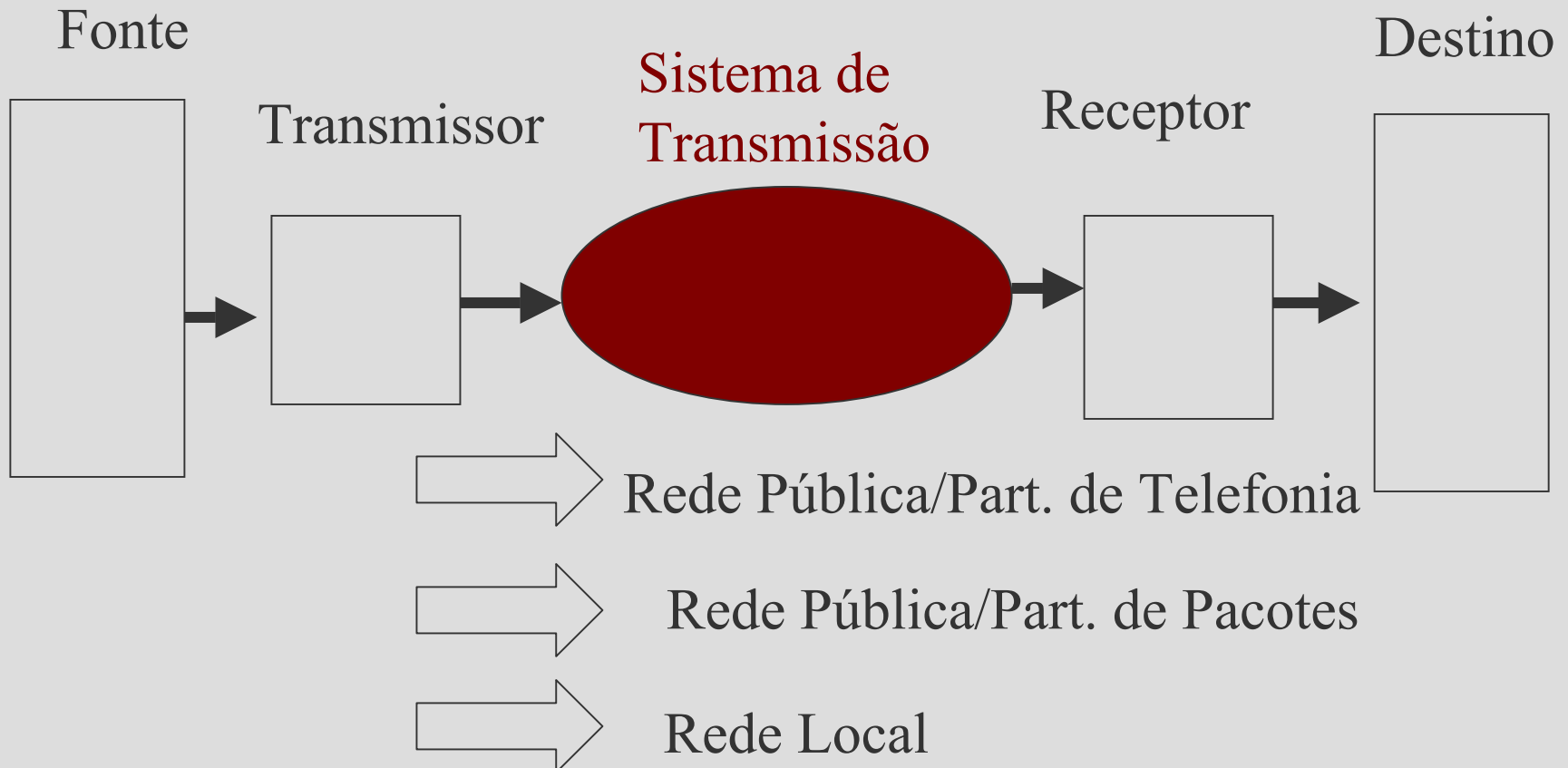
Conceitos de Comunicação

Modelo Genérico de Comunicação



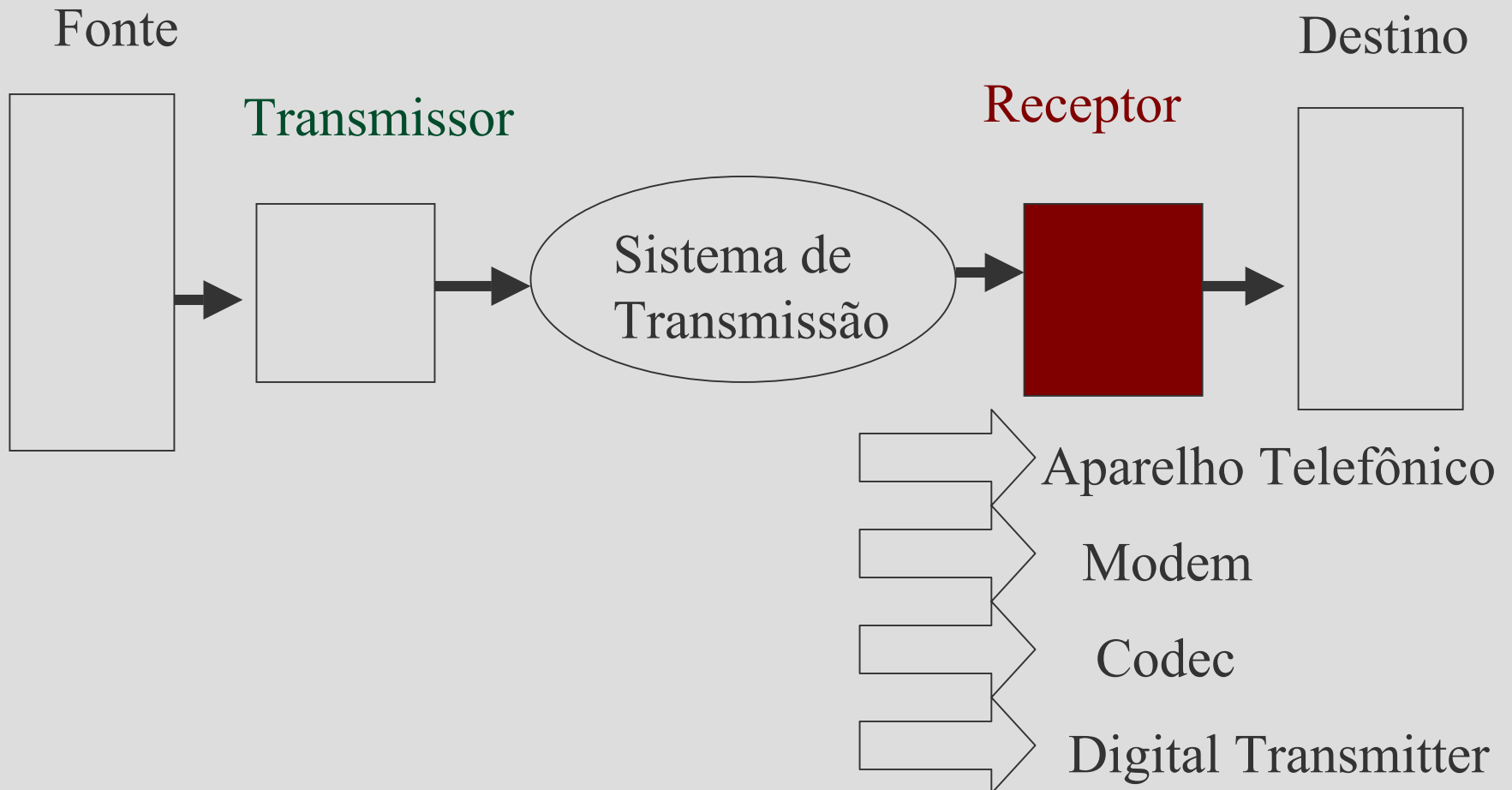
Conceitos de Comunicação

Modelo Genérico de Comunicação



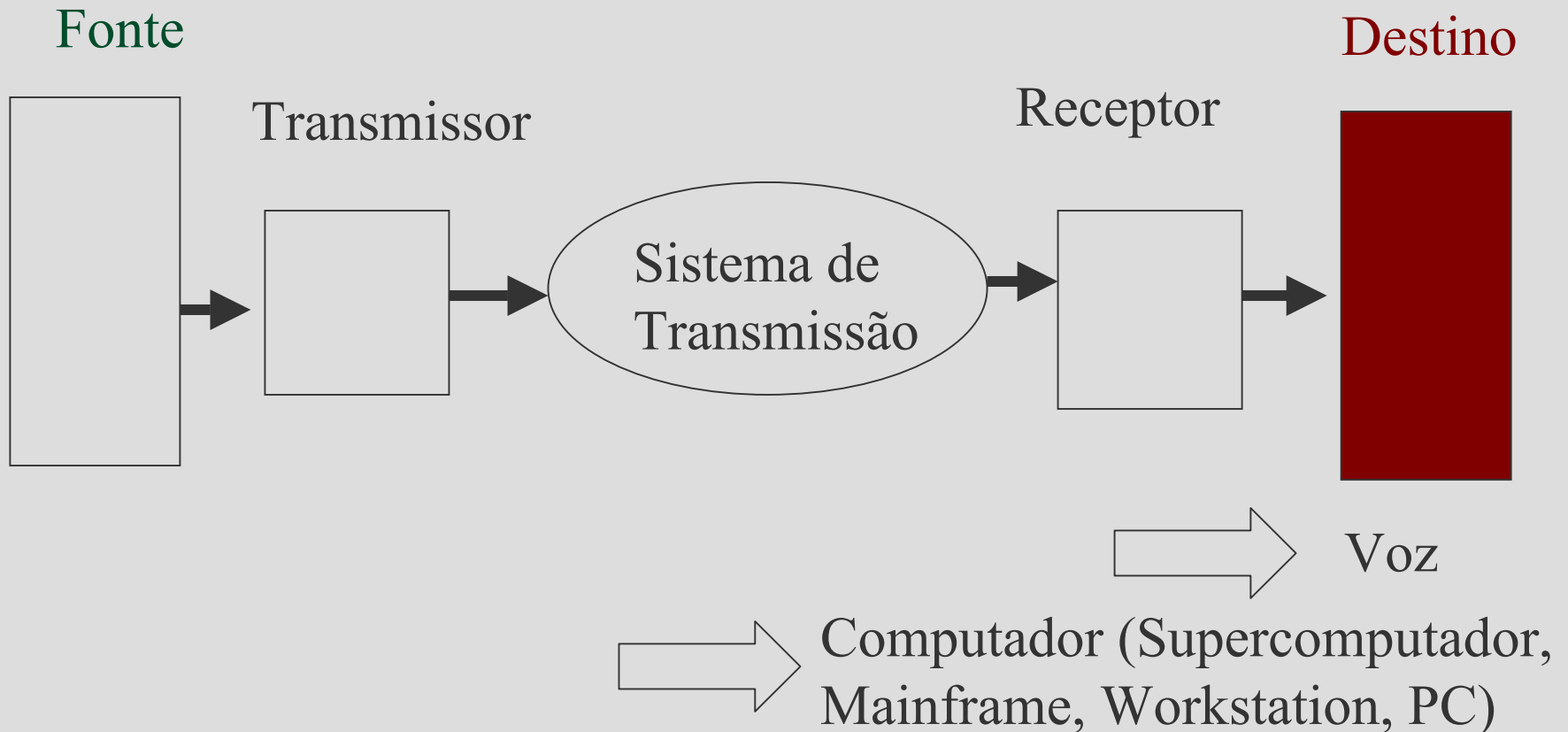
Conceitos de Comunicação

Modelo Genérico de Comunicação



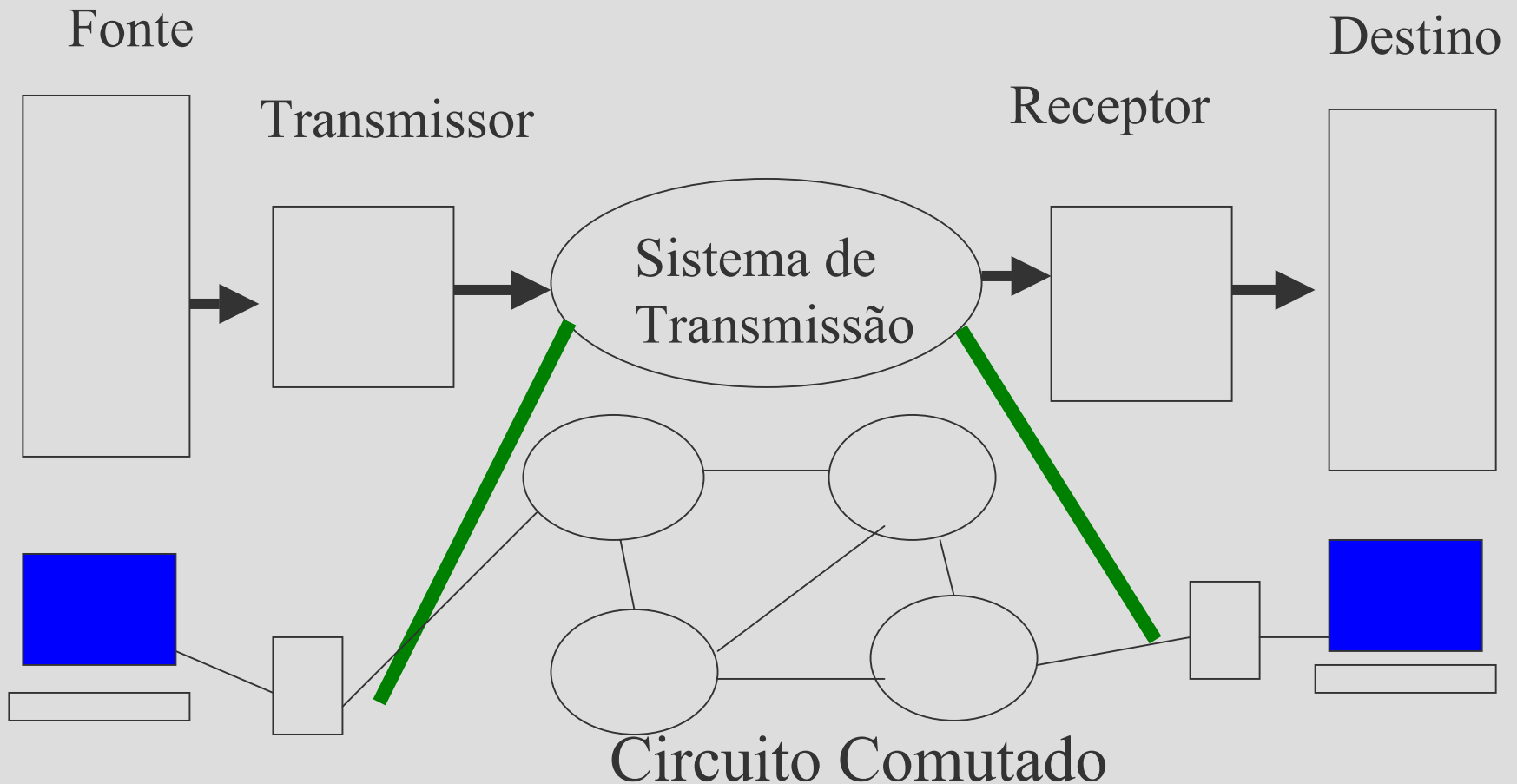
Conceitos de Comunicação

Modelo Genérico de Comunicação



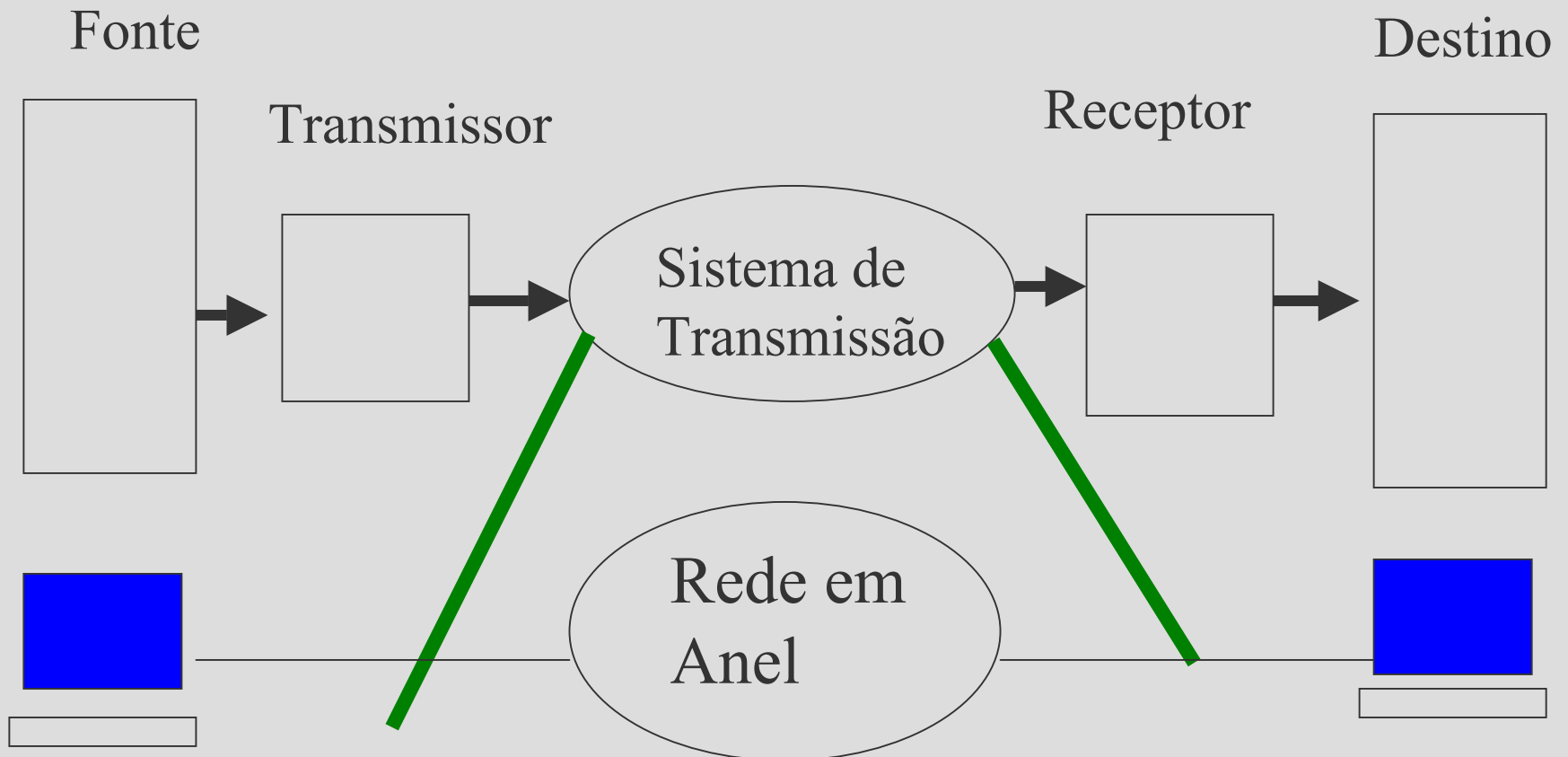
Conceitos de Comunicação

Modelo Genérico de Comunicação



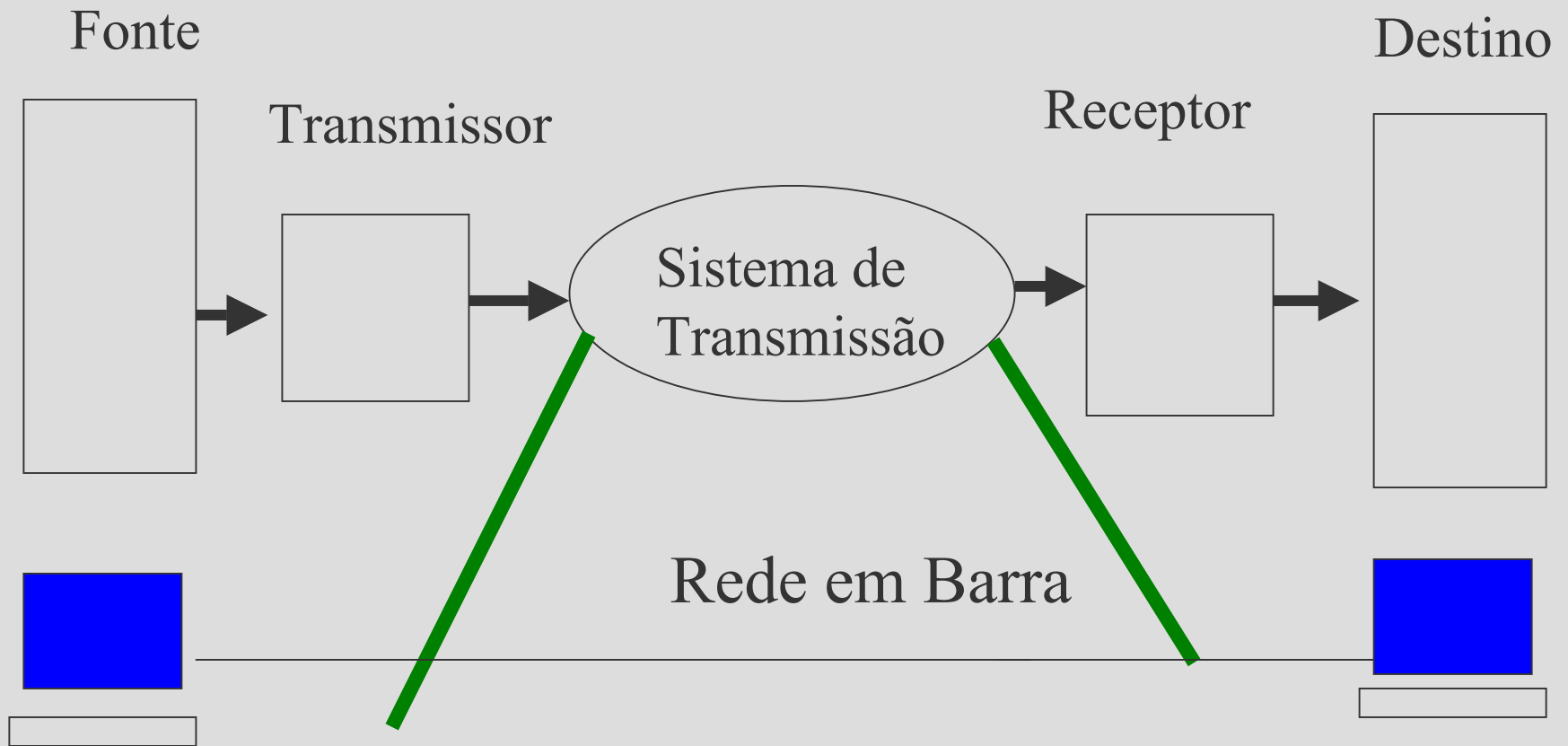
Conceitos de Comunicação

Modelo Genérico de Comunicação



Conceitos de Comunicação

Modelo Genérico de Comunicação



Conceitos de Comunicação

Modelo Genérico de Comunicação



**Considerando um ambiente de rede,
qual seria o conceito correto sobre :**

Informação

Sinal

Informação x Sinal

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

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

Informação \times Sinal

- **Decodificação e reprodução dos símbolos,**
- **Reconstituição da idéia (ou imagem) transmitida com o mínimo de degradação.**

Informação x Sinal

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

Informação x Sinal

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

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

Banda Base e Banda Larga

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

Banda Base e Banda Larga

Qual a diferença entre :

largura de banda e taxa de transmissão ?

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

Banda Base e Banda Larga

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

Banda Base e Banda Larga

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

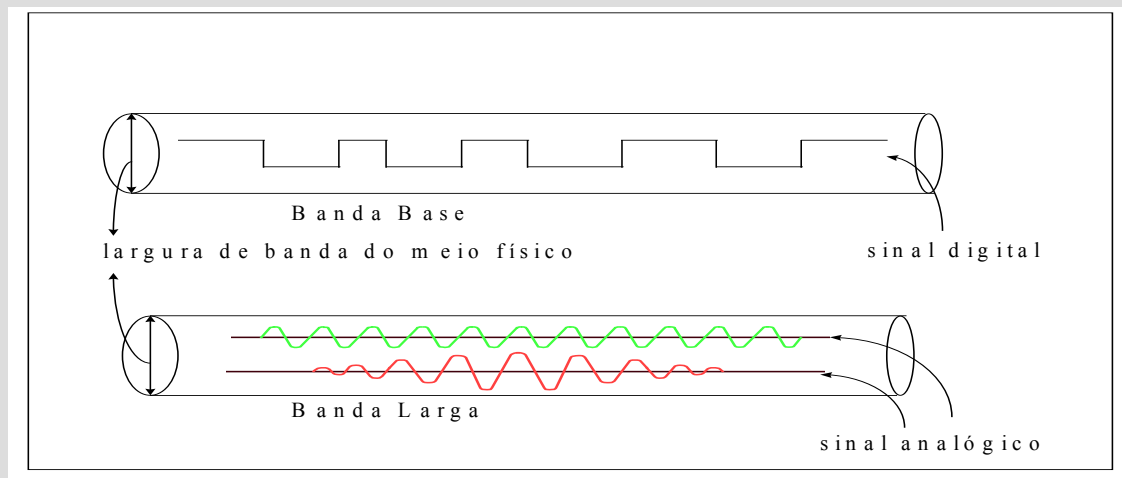
Esta tecnologia é freqüentemente usada para transmissão digital. Por esta razão, a maioria das redes de computadores adotam esta técnica.

Banda Base e Banda Larga

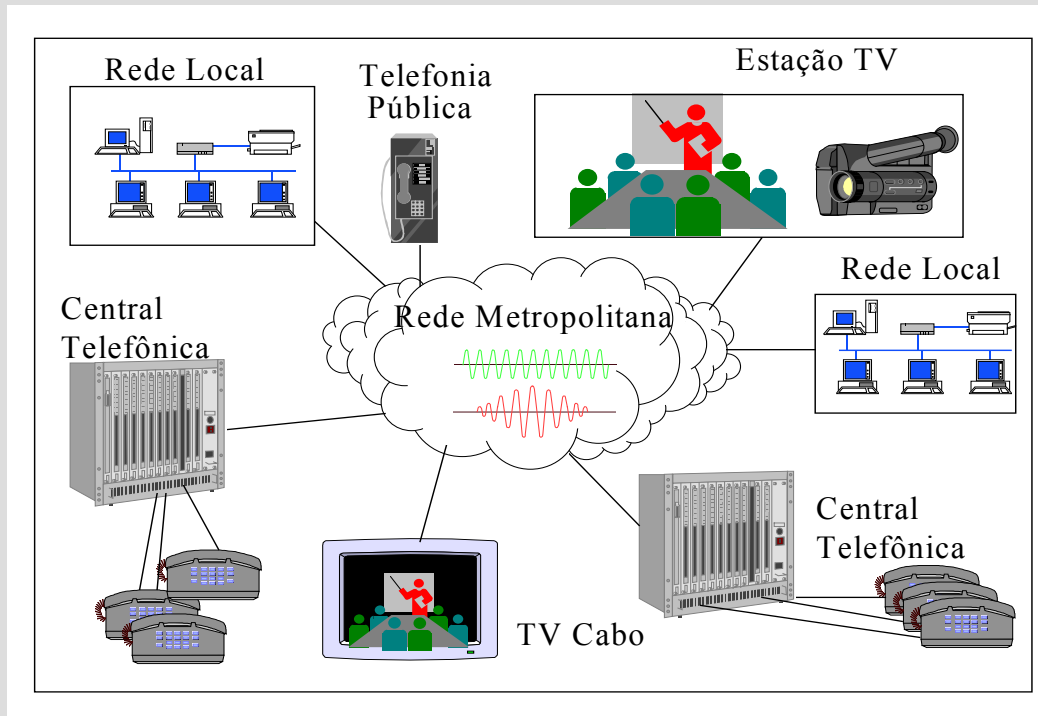
Banda larga : Este modelo de transmissão é caracterizado pela divisão da largura de banda em múltiplos canais.

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

Banda Base e Banda Larga



Banda Base e Banda Larga



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.

Dispositivos de Interconexão das Redes

Antes trabalhar com qualquer protocolo a nível de rede, é interessante um trabalho inicial para compreenderemos 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.

Dispositivos de Interconexão das 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.

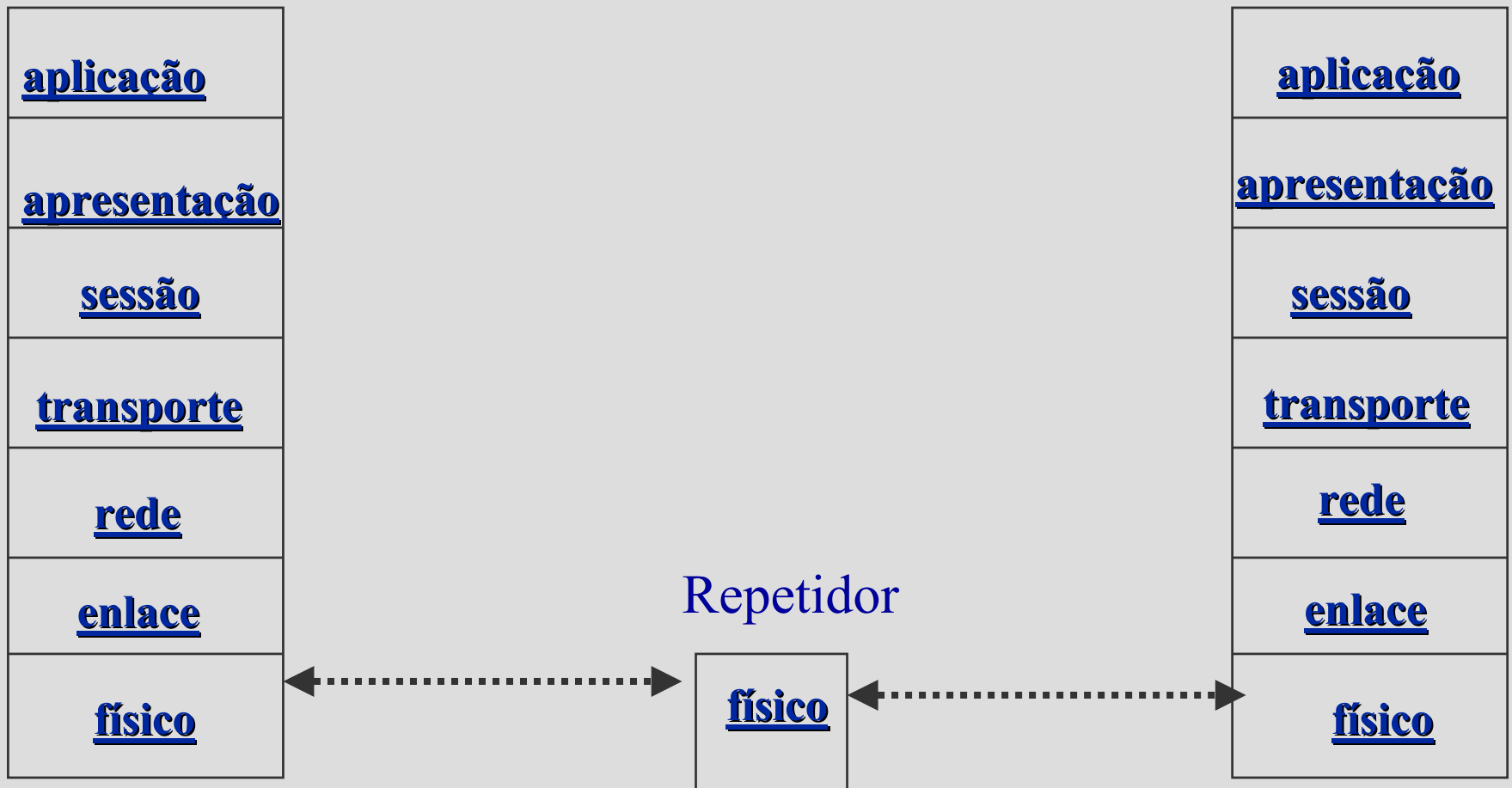
Inteligentes: além de *regenerar* os sinais, estes dispositivos podem fazer *gerência* e *seleção* de conexões.

Dispositivos de Interconexão das 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.

Dispositivos de Interconexão das Redes



Dispositivos de Interconexão das 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;

Dispositivos de Interconexão das Redes

Pontes (Bridges) -

- 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;

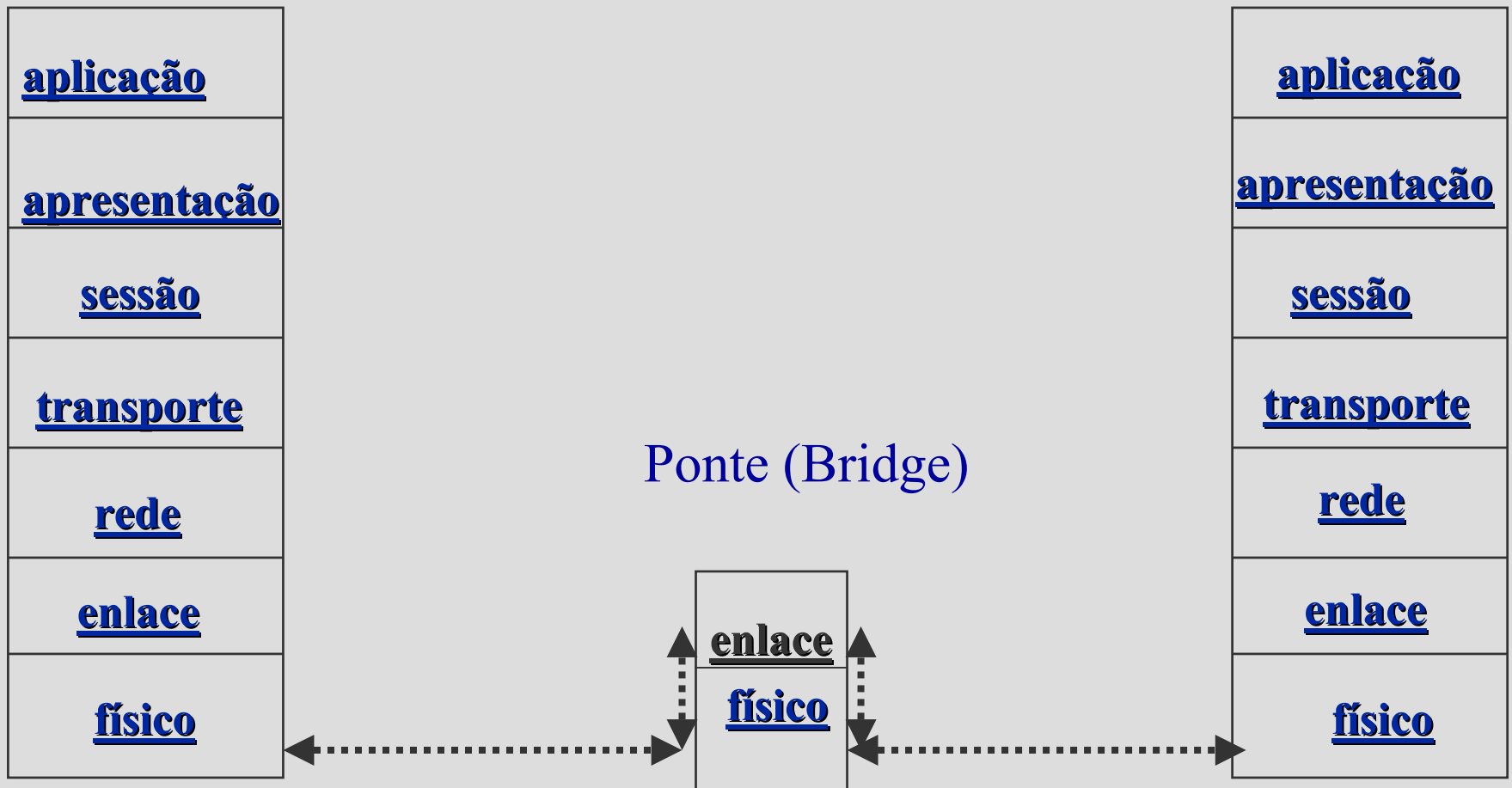
Dispositivos de Interconexão das Redes

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 taxas de implementação das redes interligadas .

Dispositivos de Interconexão das Redes



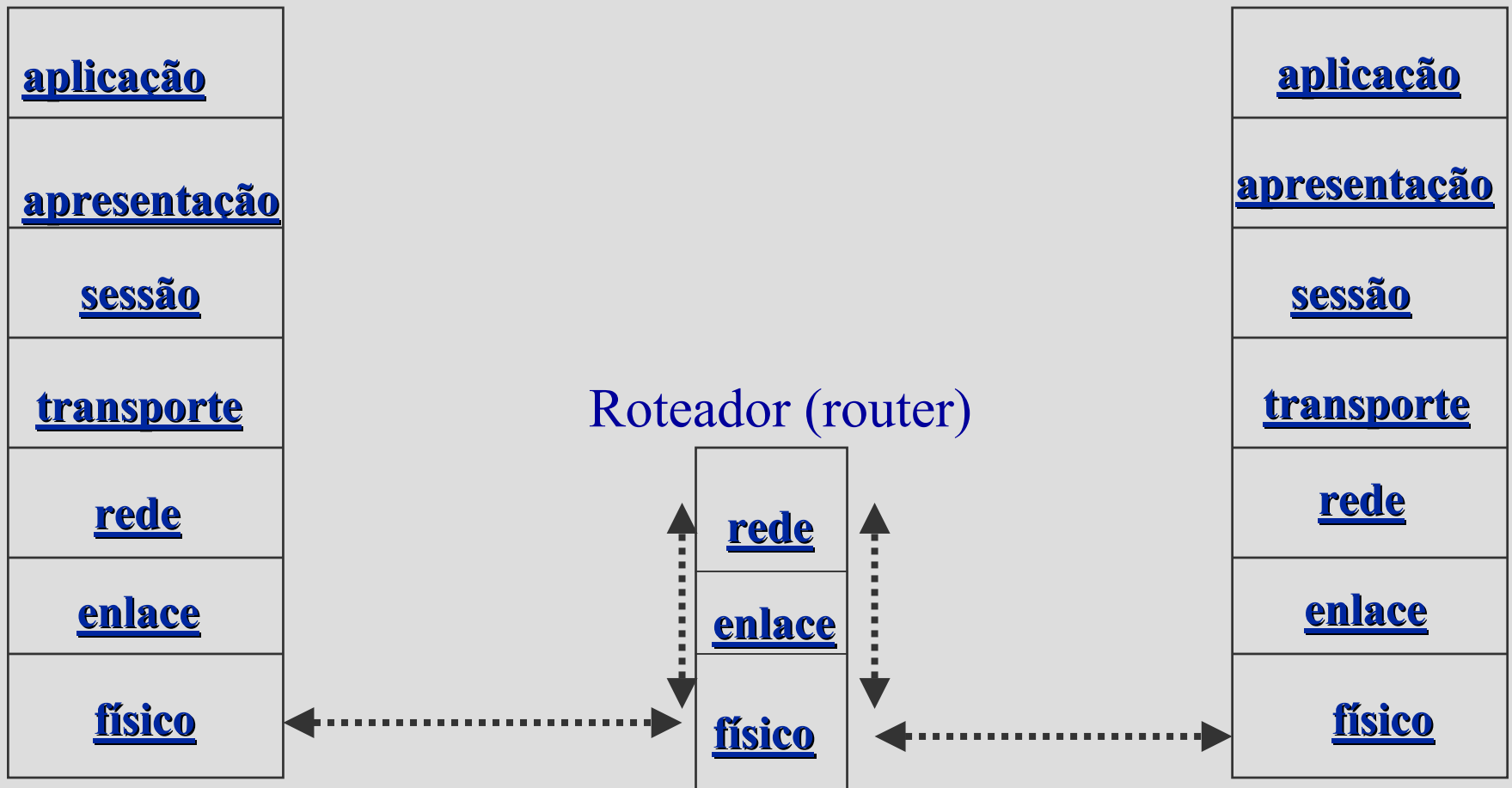
Dispositivos de Interconexão das Redes

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.

Dispositivos de Interconexão das Redes



Dispositivos de Interconexão das Redes

Gateways –

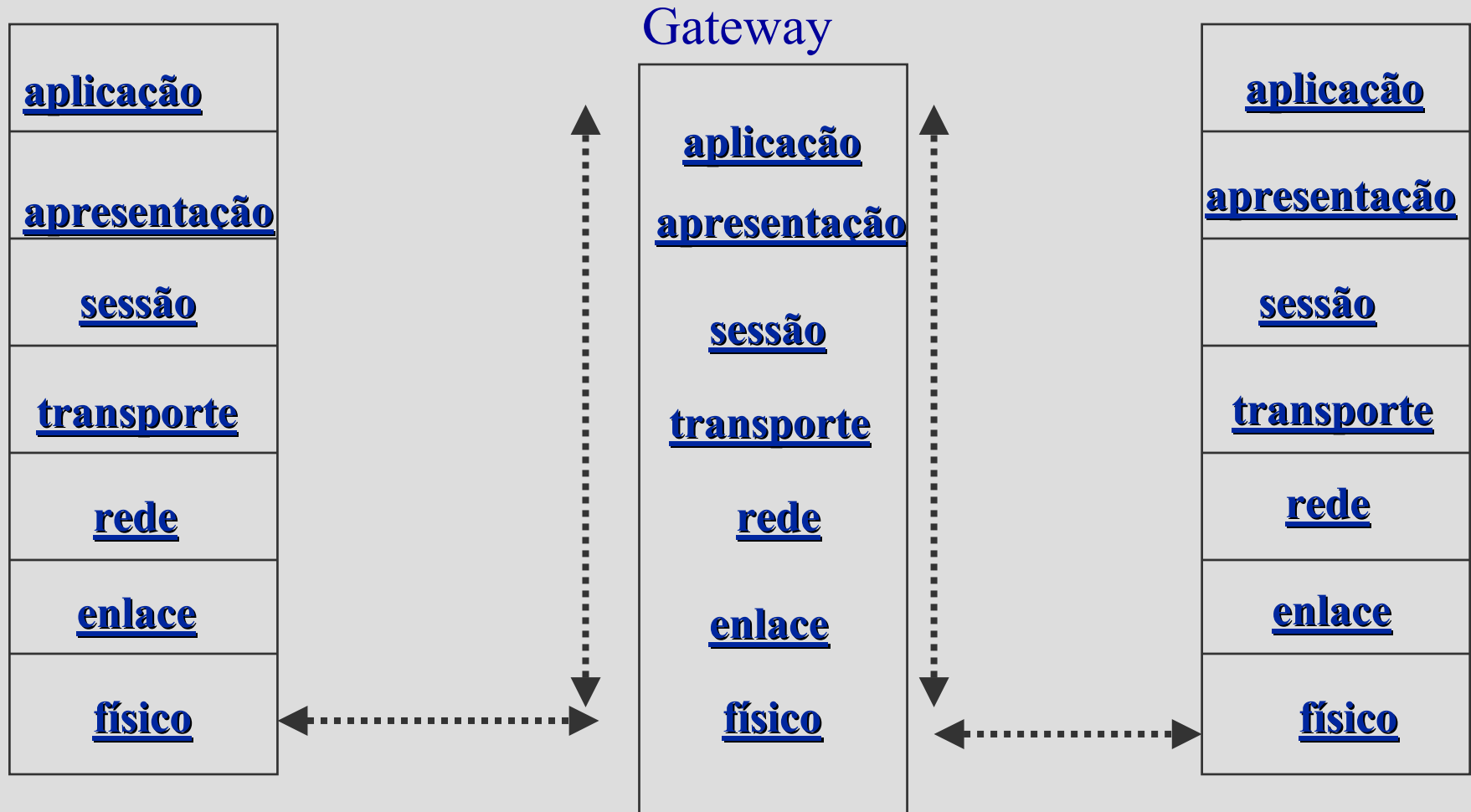
Os gateways são um tipo especial de roteador empregado para fazer o roteamento de pacotes em redes com arquiteturas distintas. A idéia é que duas aplicações em dois ambientes distintos possam se comunicar, apesar das diferenças entre seus respectivos *hosts*.

Dispositivos de Interconexão das Redes

Gateways –

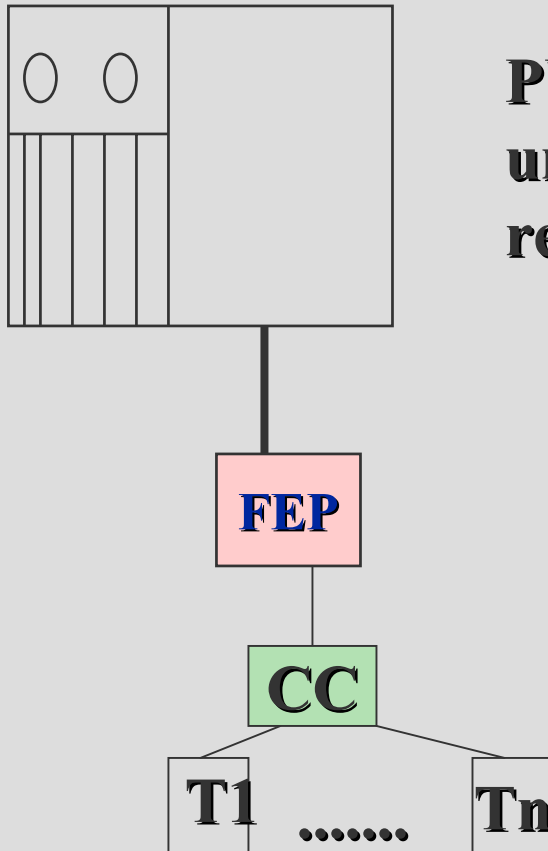
Uma situação que ilustra como exemplo o uso de *gateways* é eficaz, é aquela na qual um *host* de uma rede TCP/IP deseja fazer um conexão e se interoperar com um ambiente IBM/SNA. Nenhuma das camadas dos dois protocolos têm alguma similaridade, então o roteamento ocorre não só entre as diferentes arquiteturas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

Dispositivos de Interconexão das Redes



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.

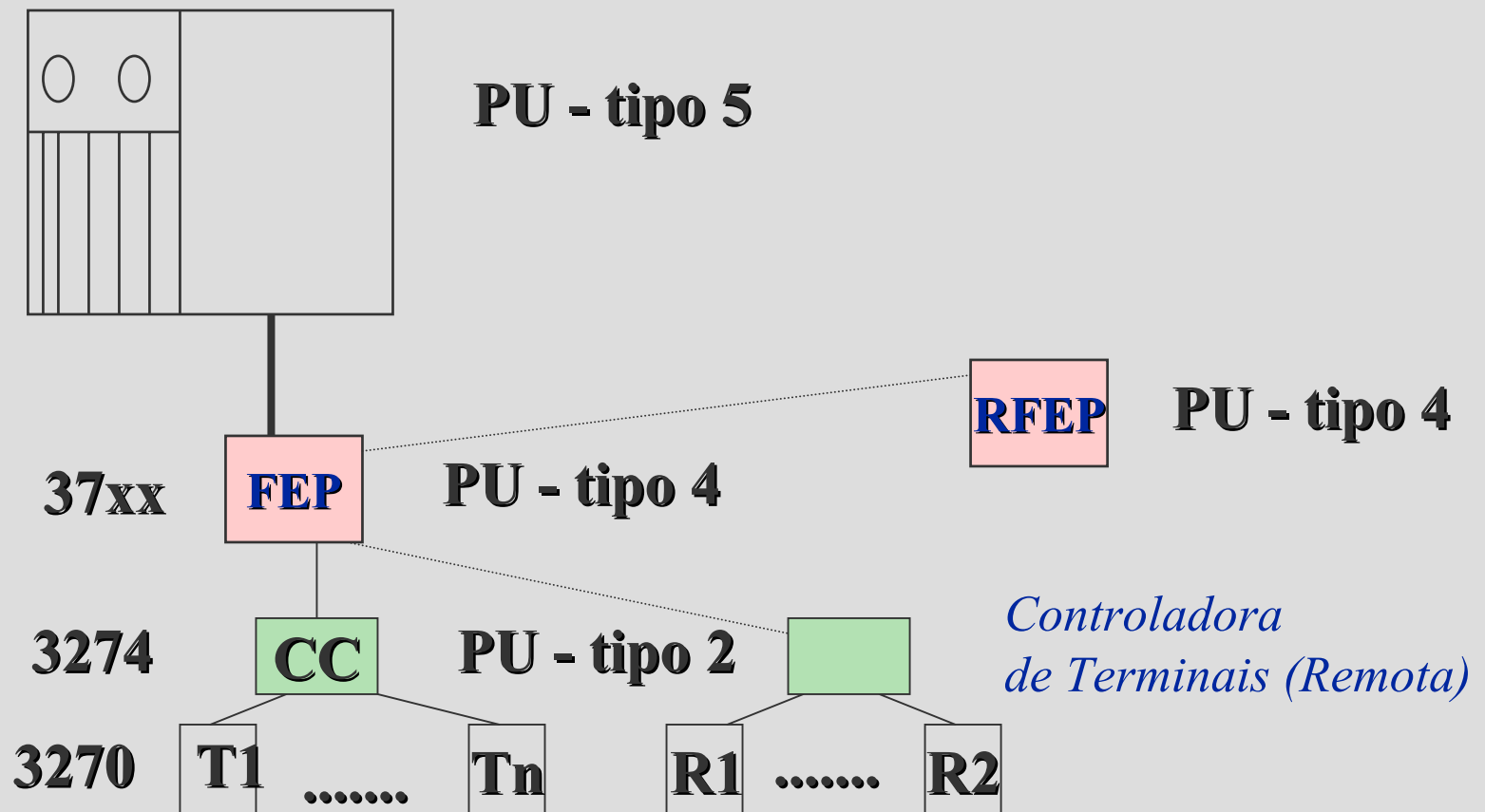
*Controladora
de Comunicação*

*Controladora
de Terminais*

Terminais

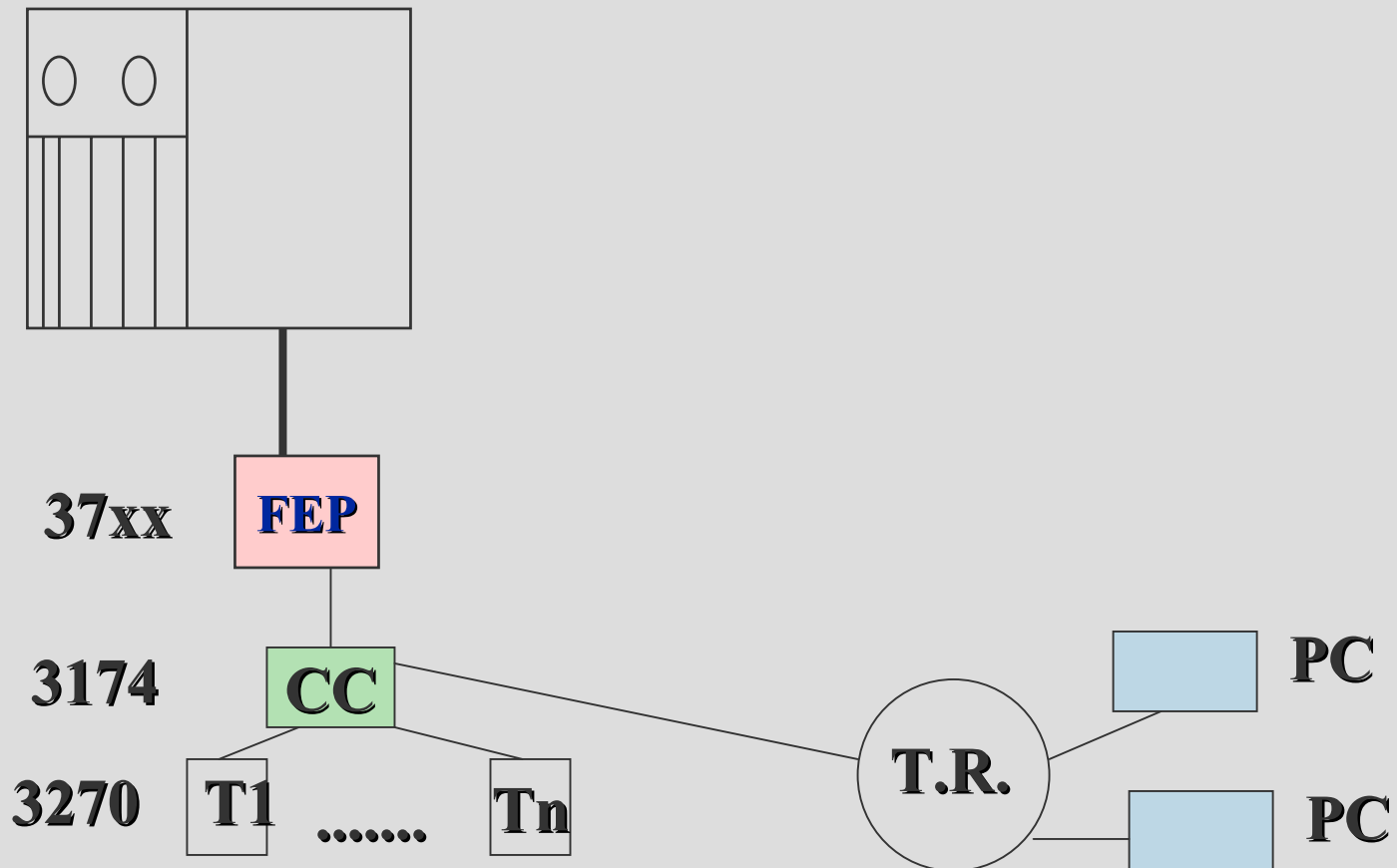
Dispositivos de Interconexão das Redes

Exemplo - SNA/IBM



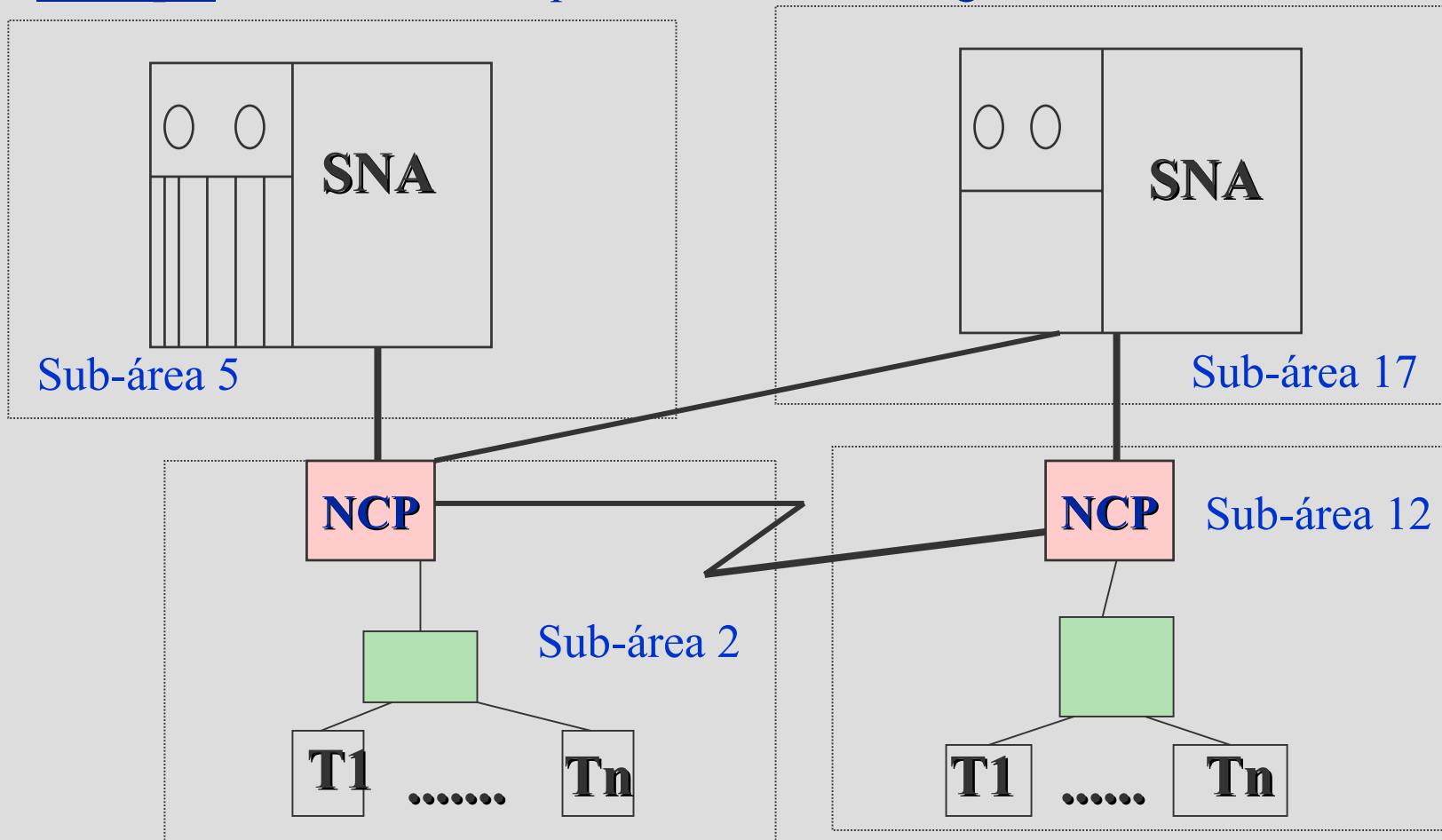
Dispositivos de Interconexão das Redes

Exemplo - SNA/IBM



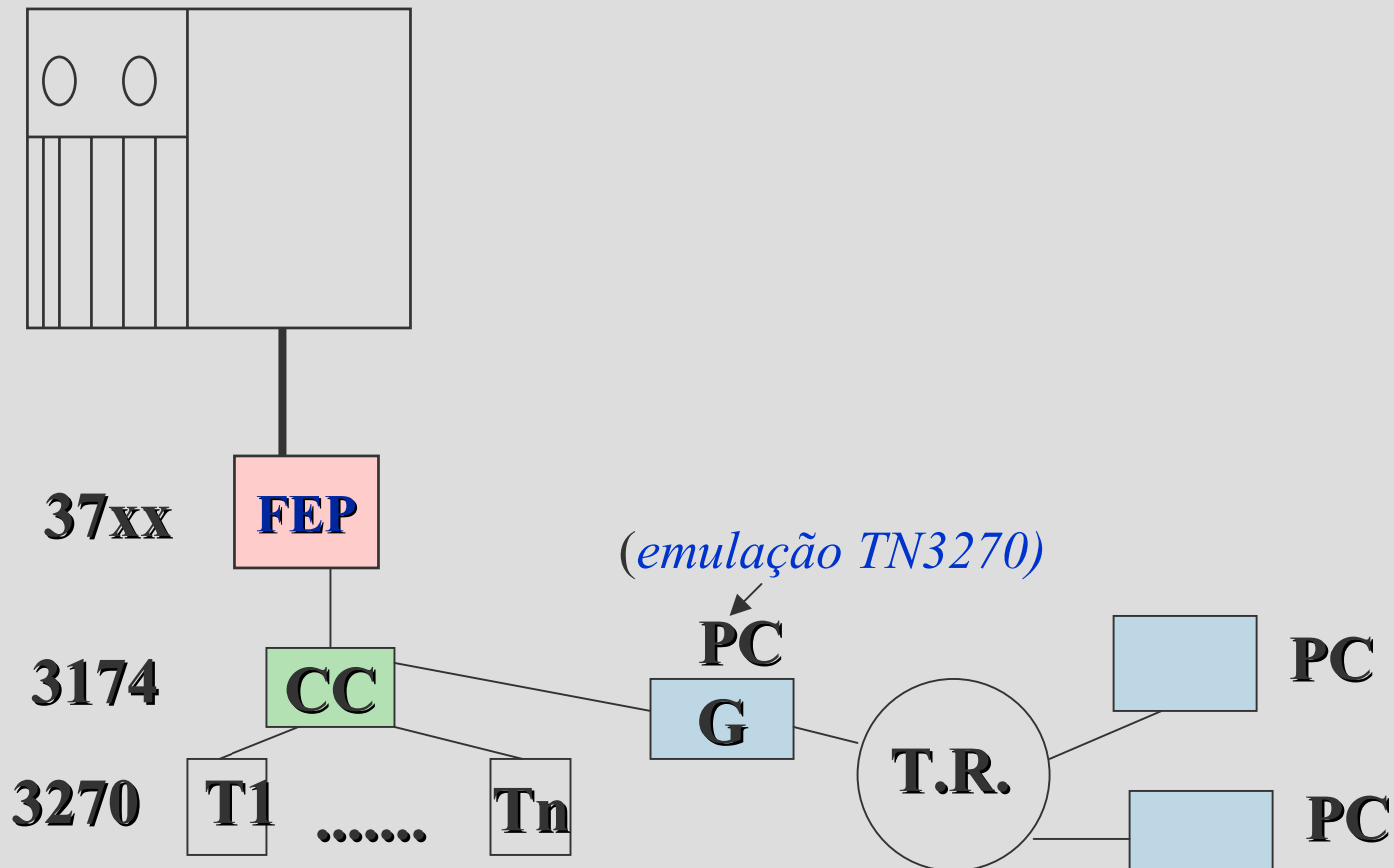
Dispositivos de Interconexão das Redes

Exemplo - SNA/IBM e os possíveis Acessos Lógicos



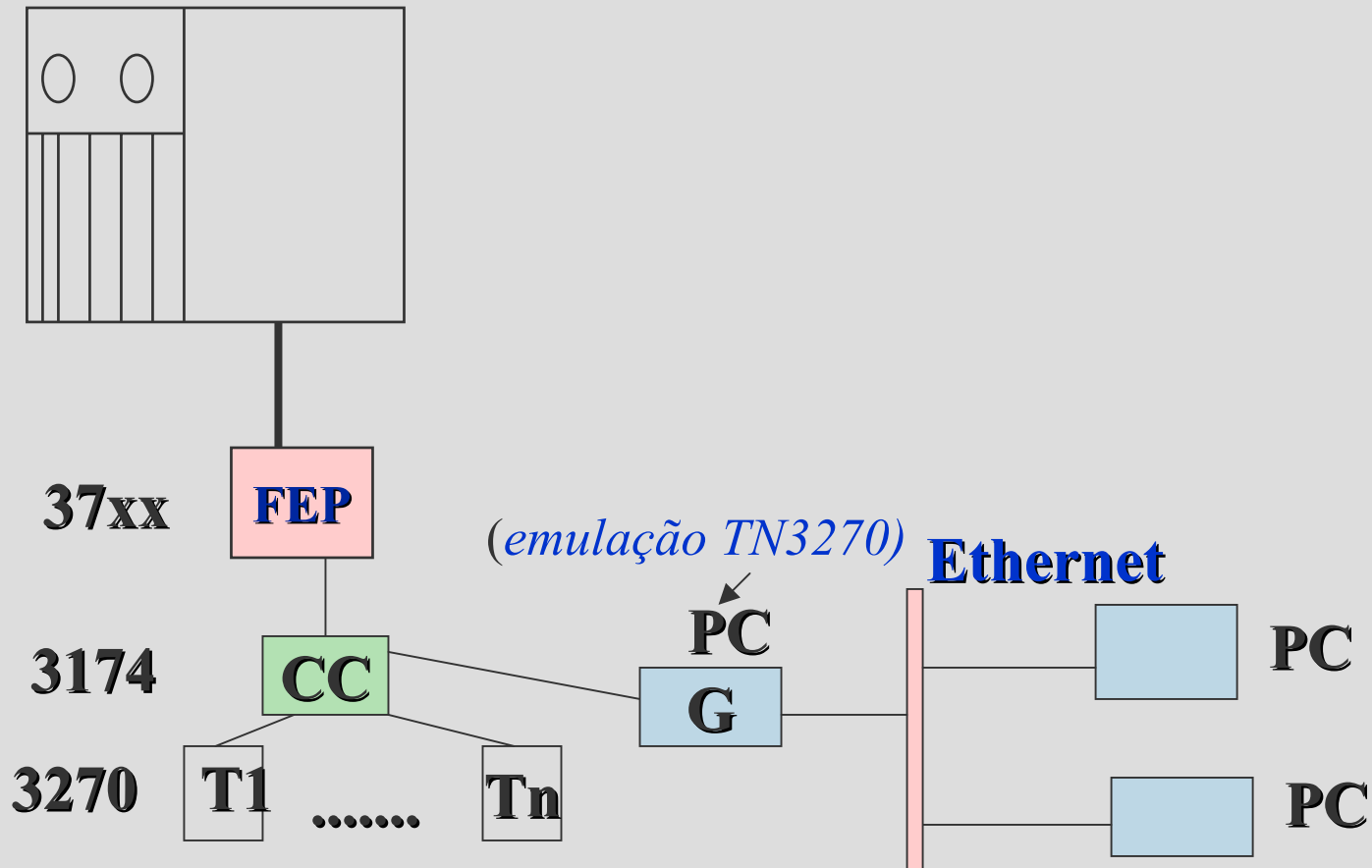
Dispositivos de Interconexão das Redes

Exemplo - SNA/IBM



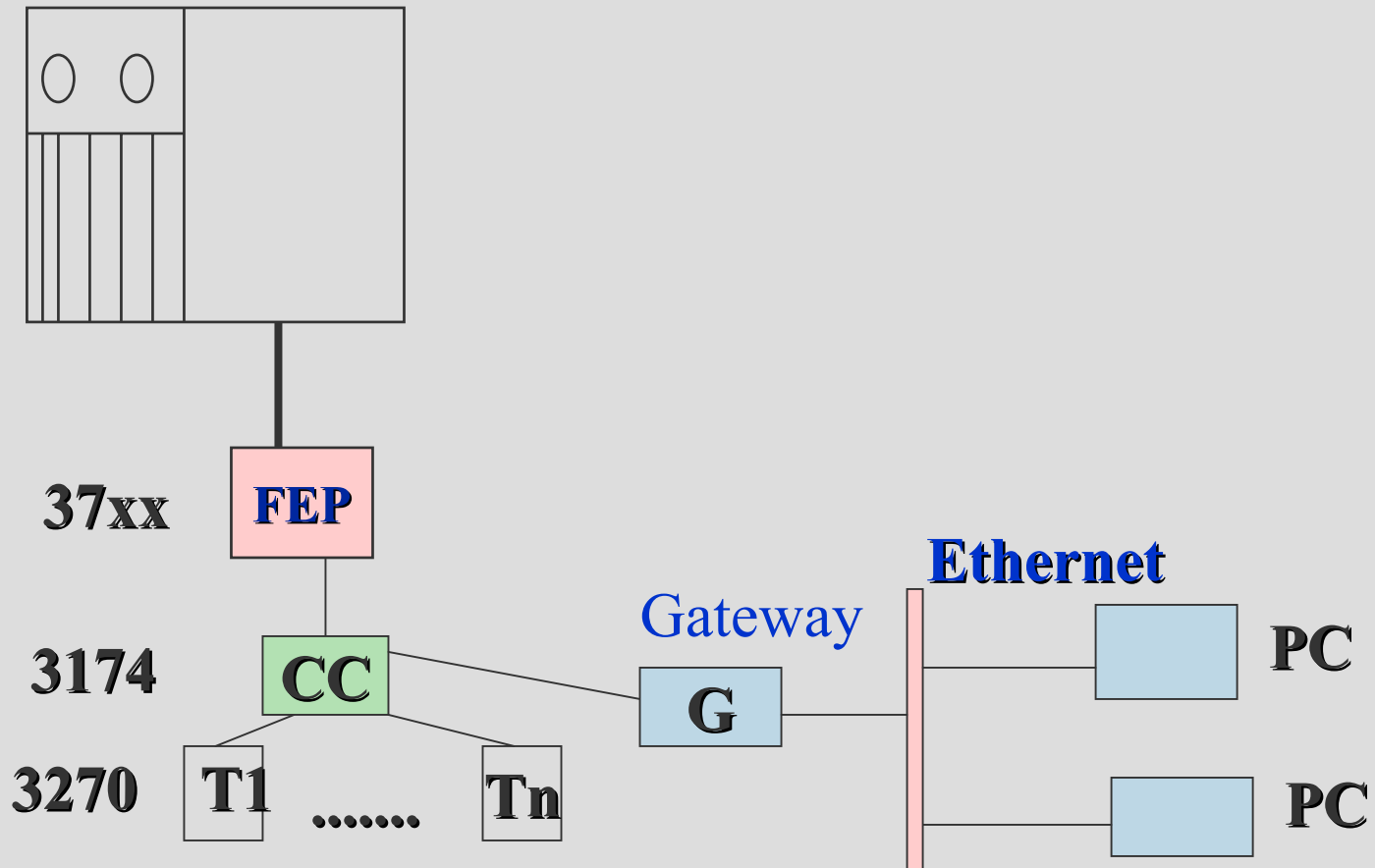
Dispositivos de Interconexão das Redes

Exemplo - SNA/IBM e um Ambiente TCP/IP



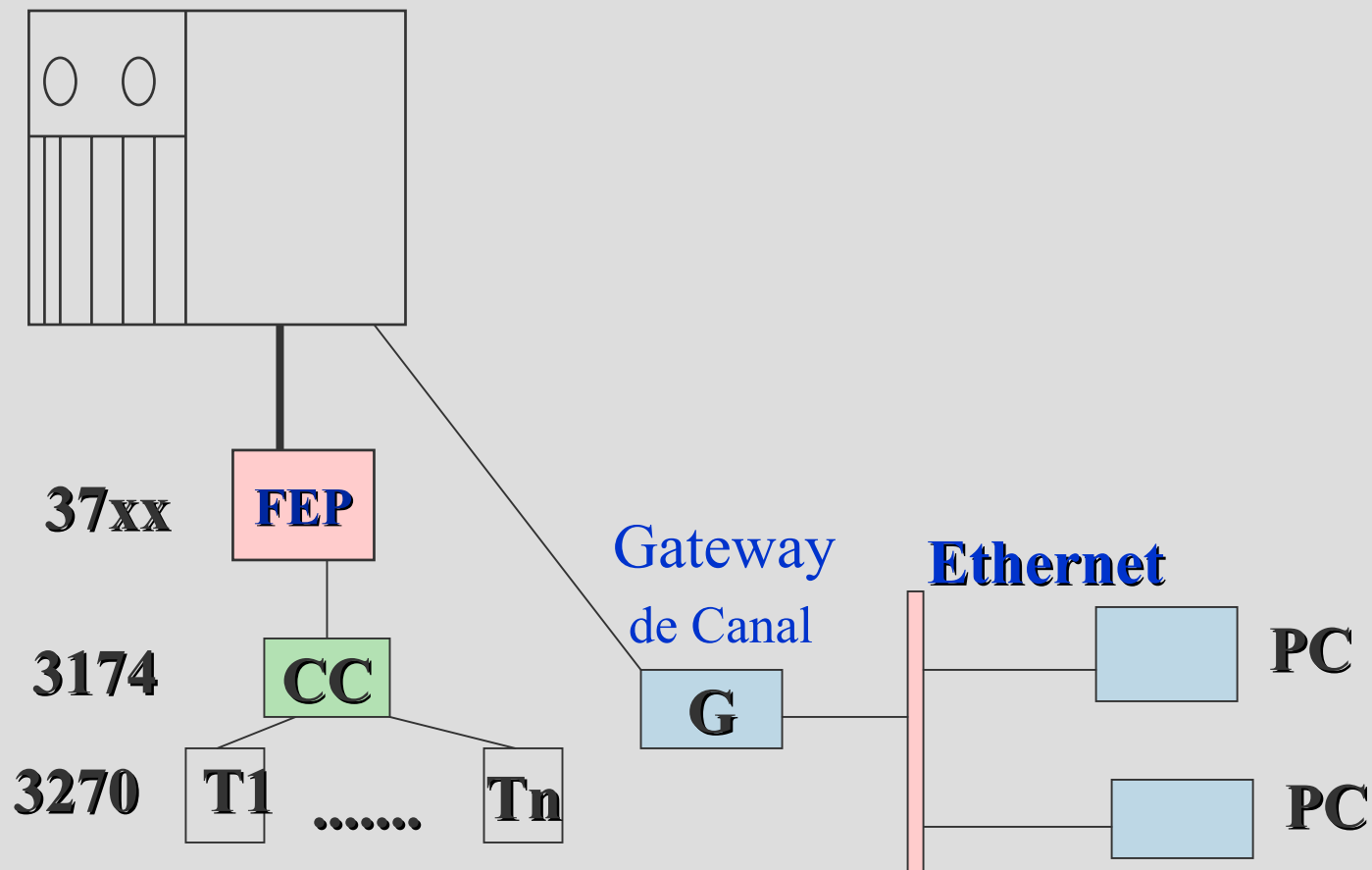
Dispositivos de Interconexão das Redes

Exemplo - SNA/IBM e um Ambiente TCP/IP



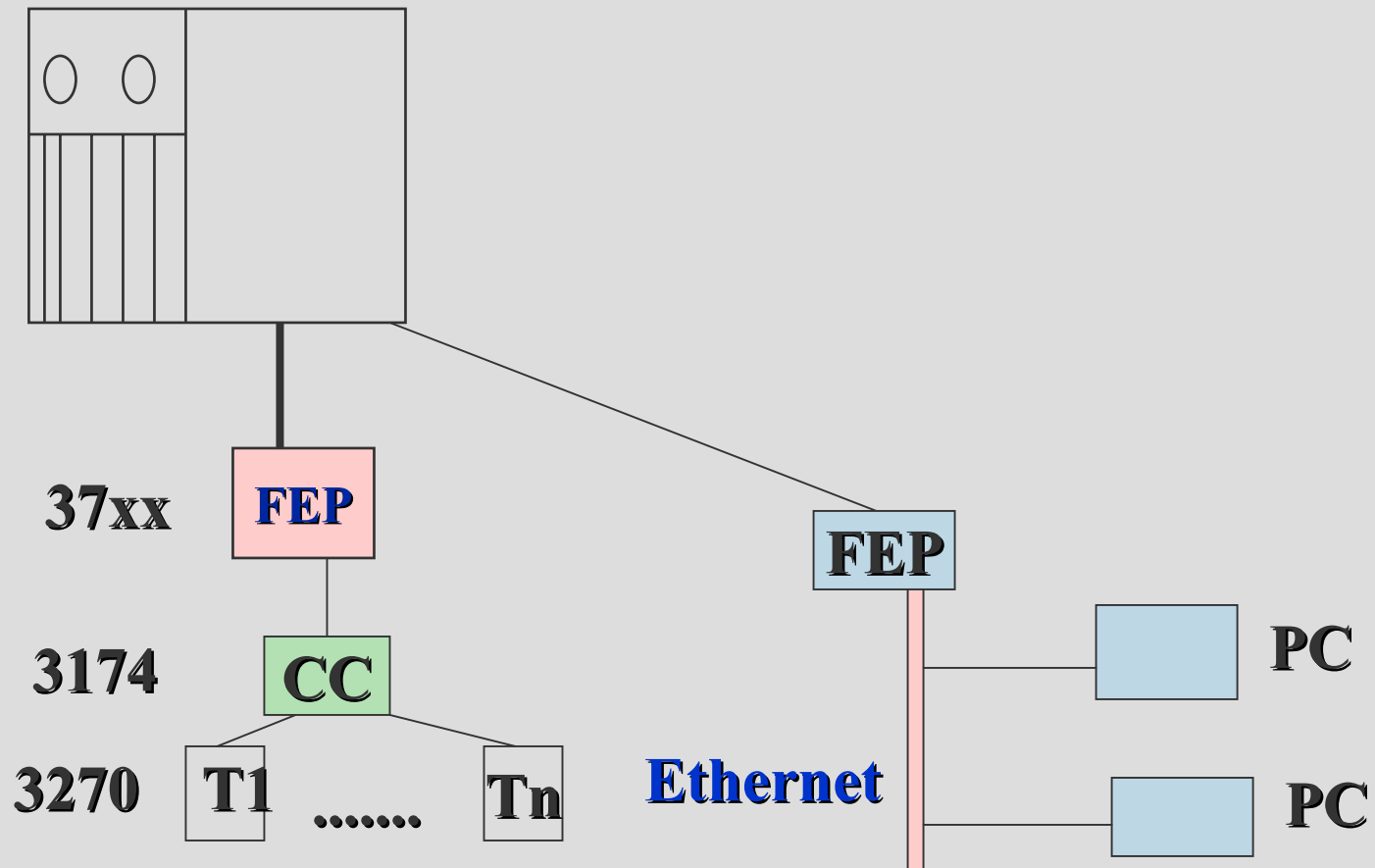
Dispositivos de Interconexão das Redes

Exemplo - SNA/IBM e um Ambiente TCP/IP



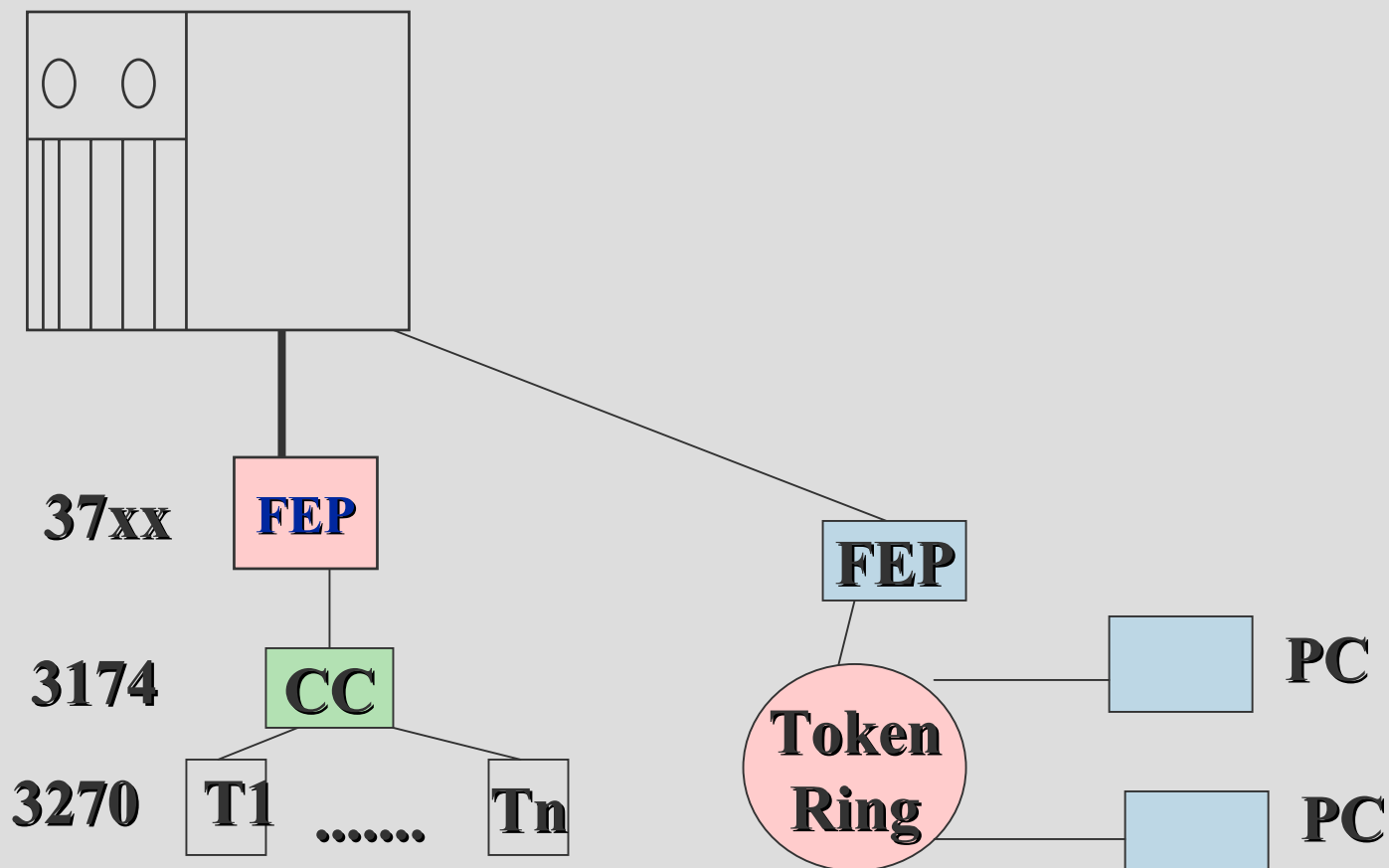
Dispositivos de Interconexão das Redes

Exemplo - SNA/IBM e um Ambiente TCP/IP



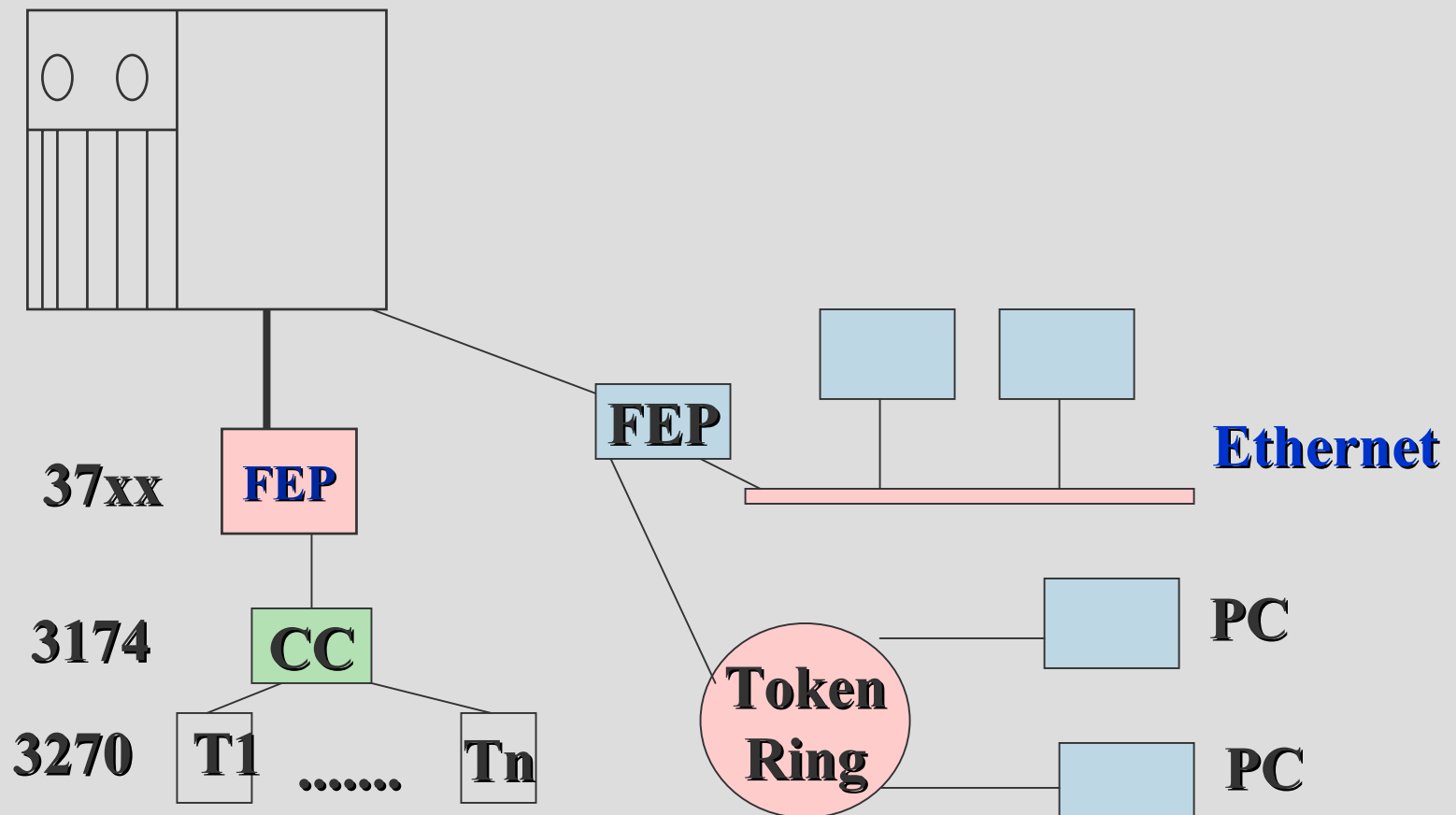
Dispositivos de Interconexão das Redes

Exemplo - SNA/IBM e um Ambiente TCP/IP



Dispositivos de Interconexão das Redes

Exemplo - SNA/IBM e um Ambiente TCP/IP



Revisão de Arquitetura de Protocolos



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

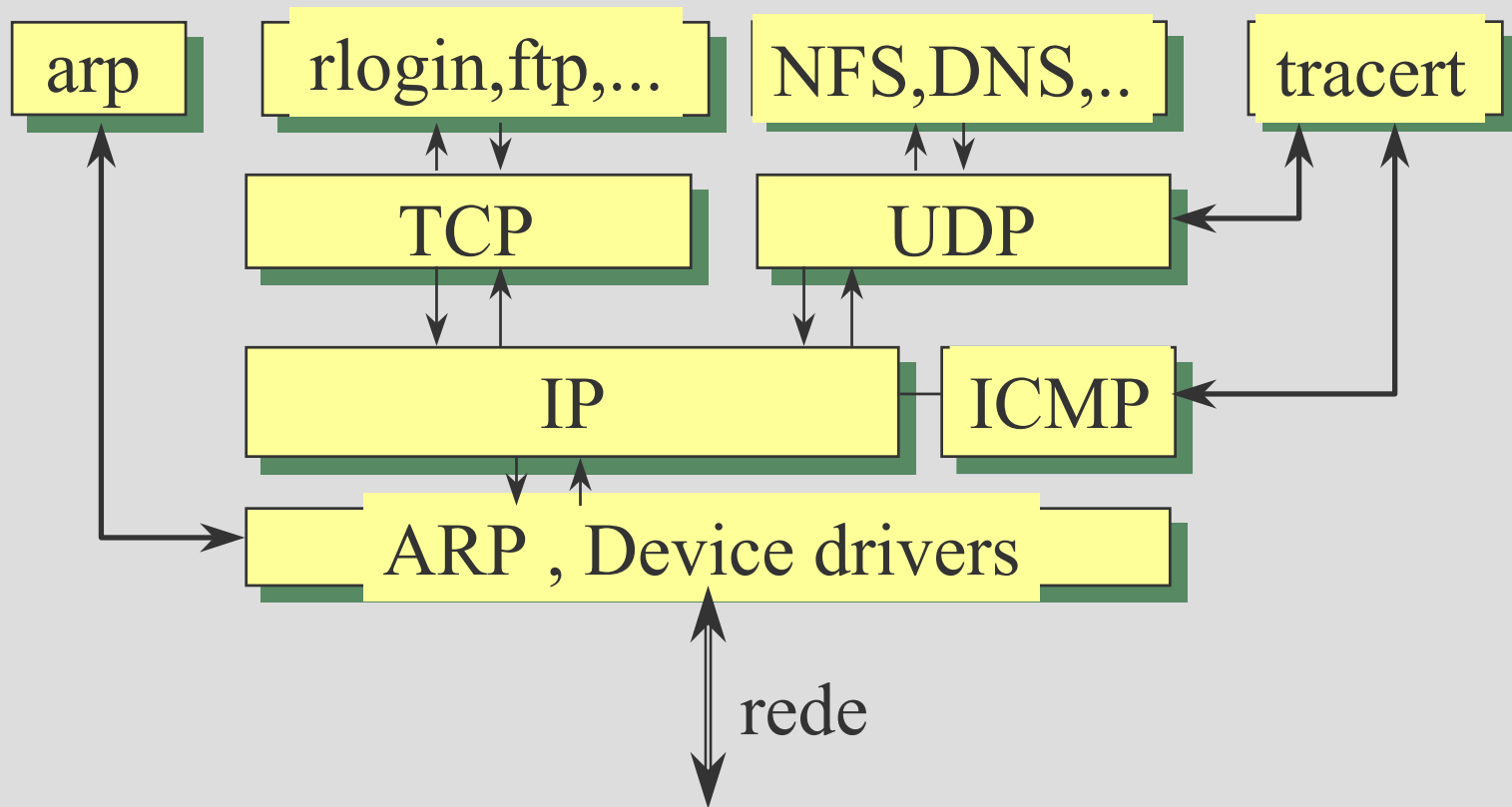
- > Internet, WWW e Internet 2
- > Roteamento e algoritmos
- > Diferenças entre IPv4 e IPv6

HISTÓRICO TCP/IP

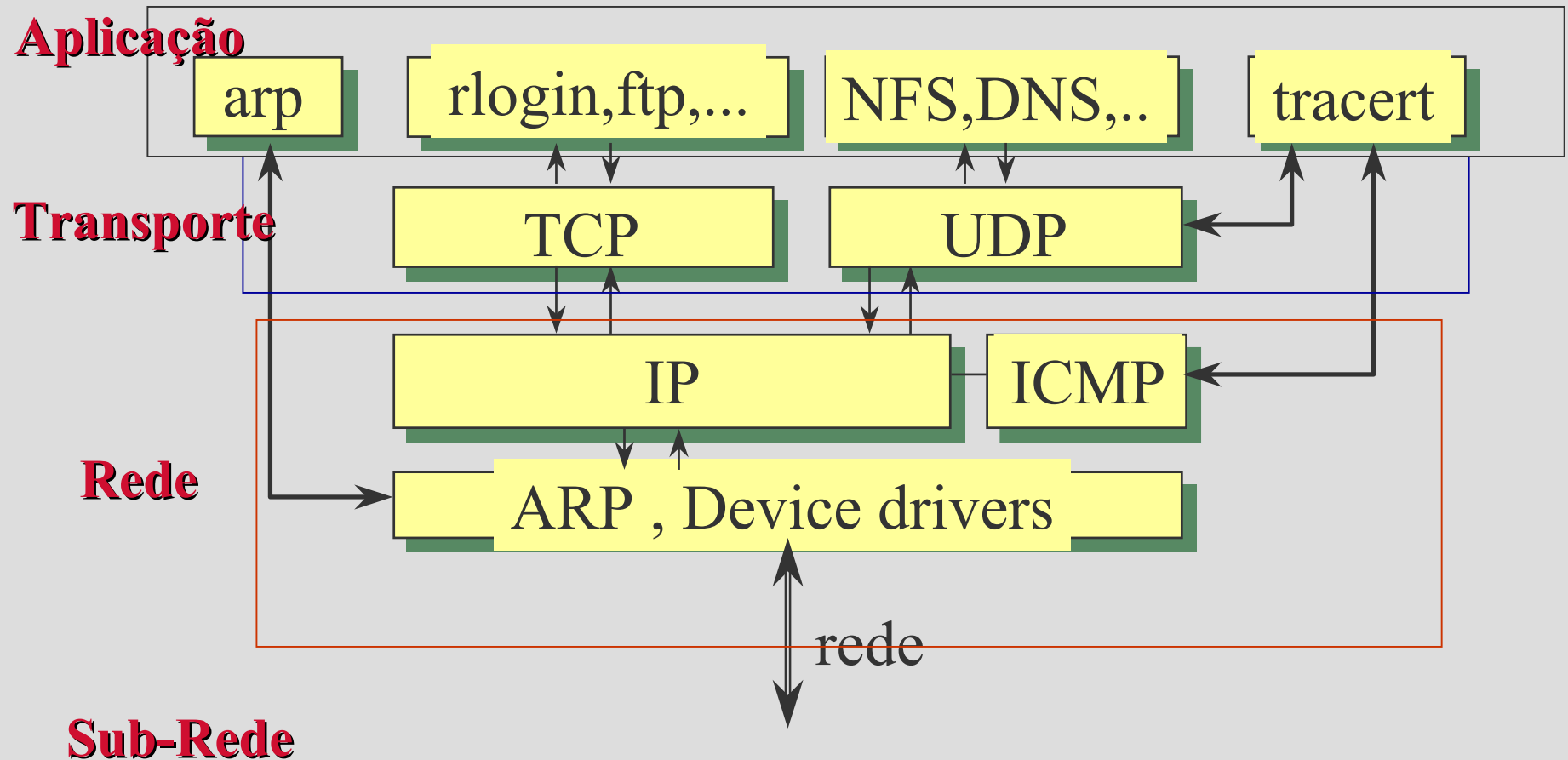
Modelo TCP/IP

aplicação
transporte
internet
sub-rede

Família de Protocolos TCP/IP



Família de Protocolos TCP/IP

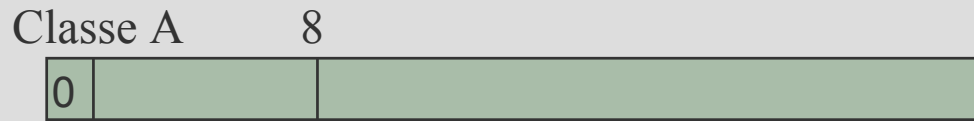


Sub-Rede de Acesso

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

IP (Internet Protocol)

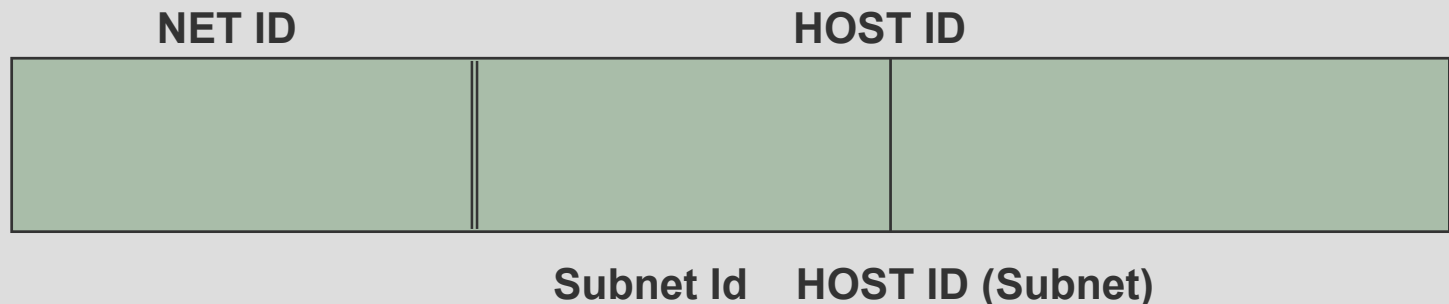
■ Endereçamento IP



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*)

MÁSCARAS - Sub-redes(Subnets)



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 164.41.0.0

Sub-rede A: 164.41.10.0

Sub-rede B: 164.41.20.0

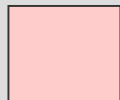
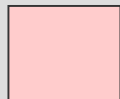
Máscara: 255.255.255.0

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)

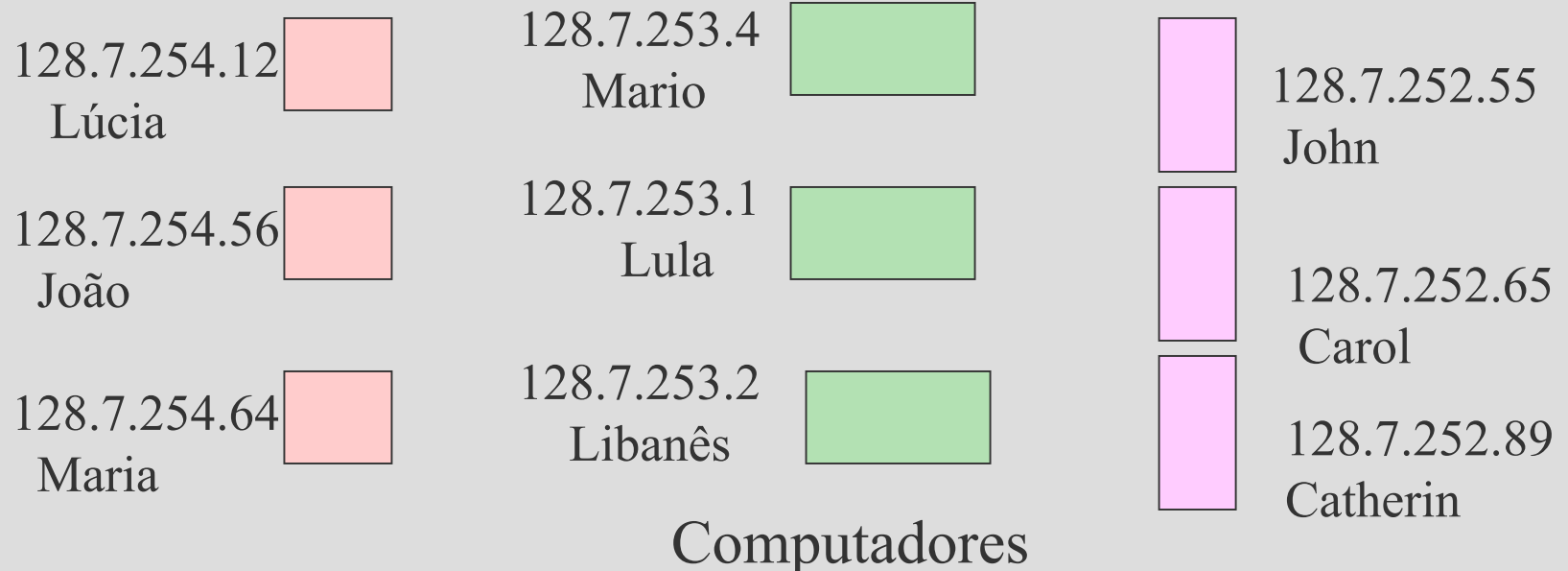


Computadores

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)

Como funcionam as máscaras da Subrede ?

Vamos agora considerar os Casos anteriores com uma máscara 255.255.255.0.

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

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

Como funcionam as máscaras da Subrede ?

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

11111111.11111111.11111111.00000000

10000000.00000111.11111101.00000100

10000000.00000111.00000000.00000000 (128.7.253.0)

Como funcionam as máscaras da Subrede ?

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

11111111.11111111.11111111.00000000

10000000.00000111.11111100.01011001

10000000.00000111.00000000.00000000 (128.7.252.0)

Tabela de Rotas

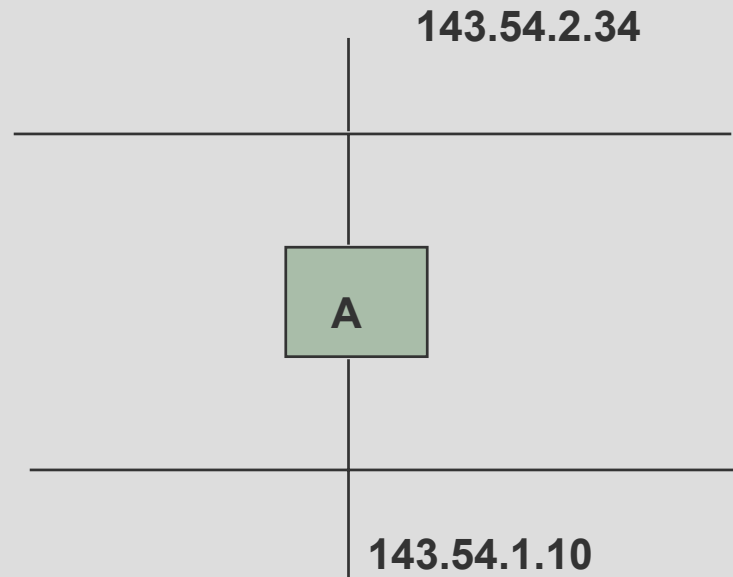


Tabela de rotas de A

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

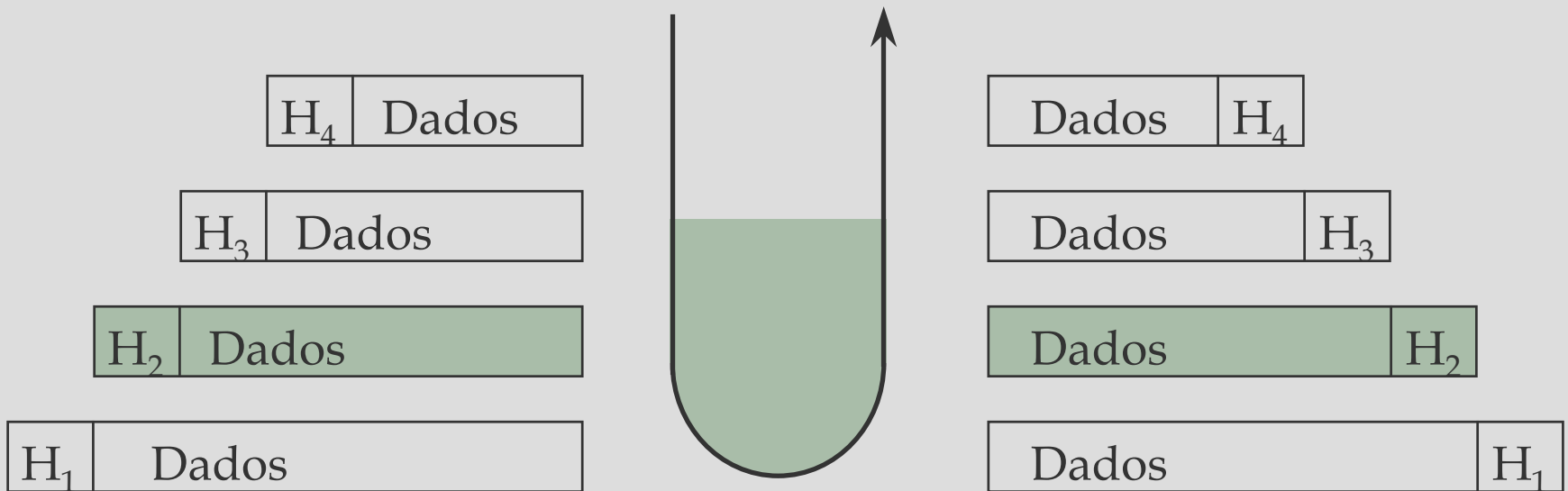
- **Vers:** versão do IP utilizada. Versão atual é a 4 (ou 6 ?)
- **Hlen:** tamanho do cabeçalho do datagrama
- **Service Type:** especifica qual a forma de se lidar com o datagrama. Possui 8 bits que indicam os seguintes requisitos:
 - Precedência
 - Mínimo de atraso na transmissão
 - Alto Throughput
 - 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

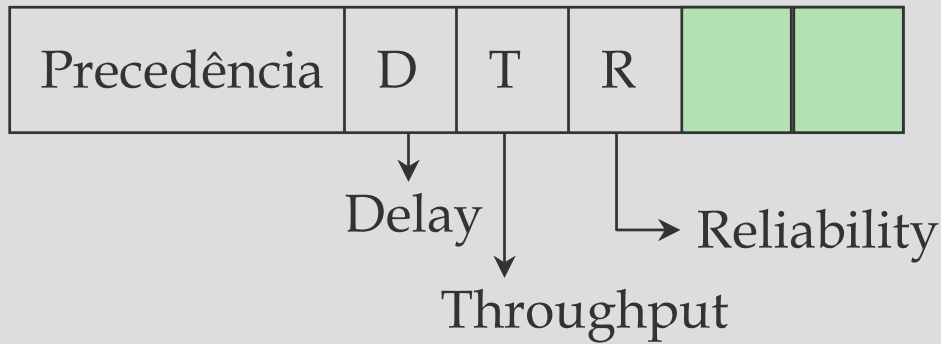
- Quebra em pacotes
- Tráfego de sequência de bits



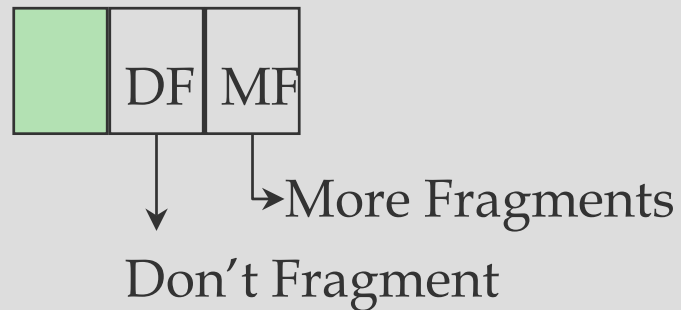
H_x - Cabeçalho (Header) - Controle
Dados - Não tratado pelo nível x

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

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

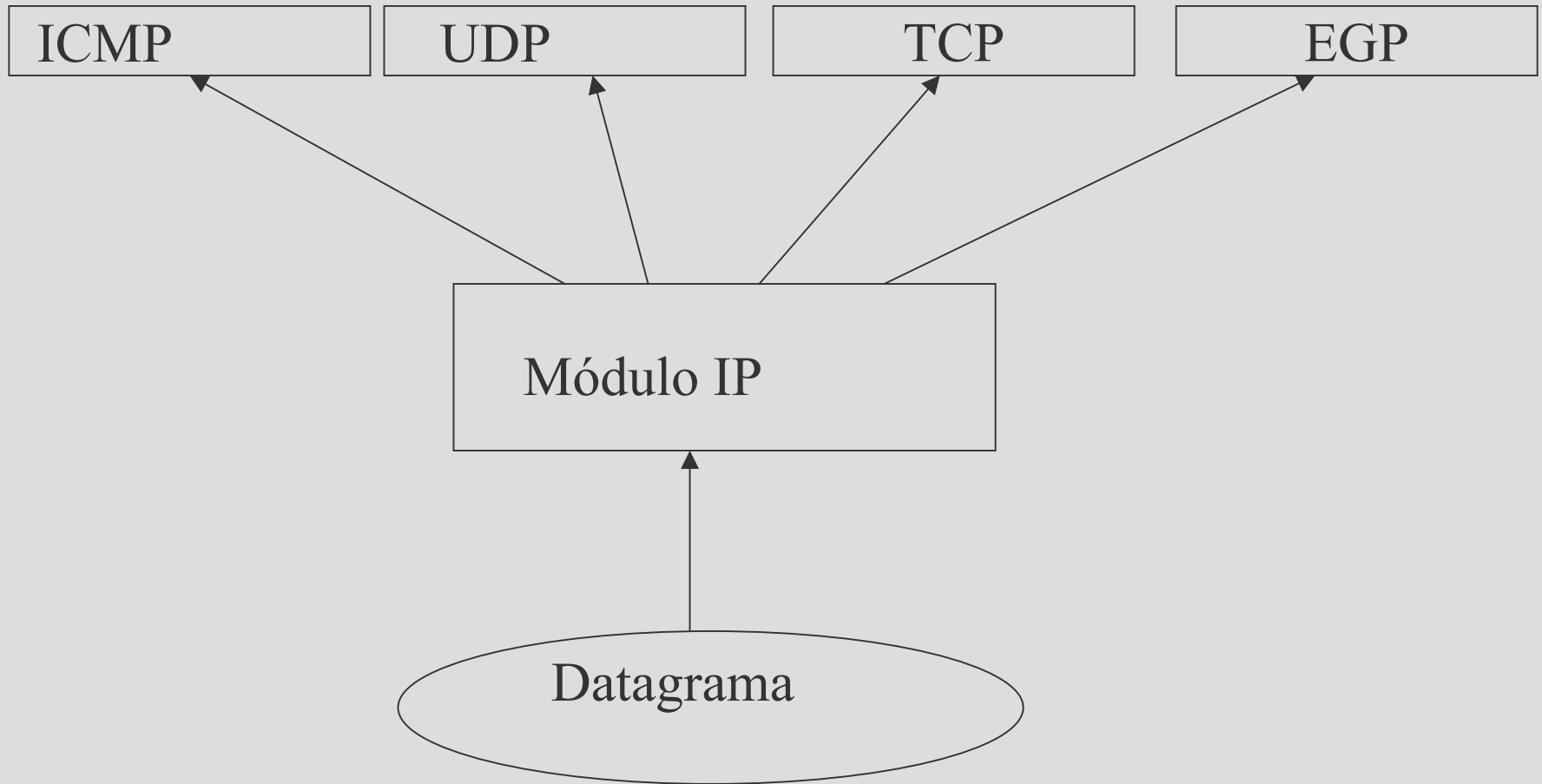
Processamento no Host Destino

- 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

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)

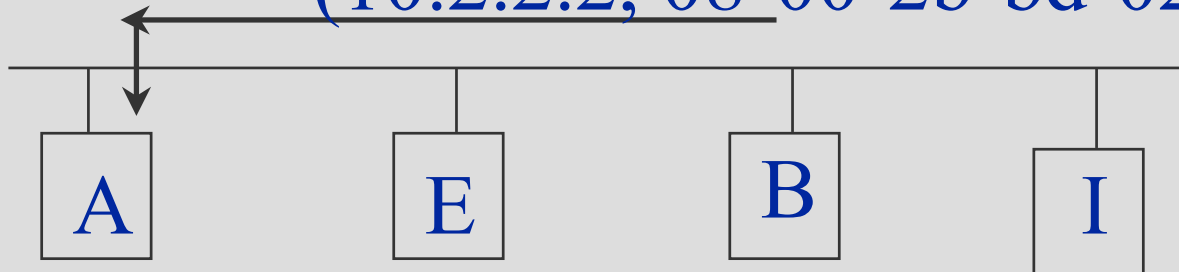
Hard Type		Proto Type
Hlen	Plen	Operation
Sender HA		
Sender HA		Sender IP
Sender IP		Target HA
Target HA		
Target IP		

ARP (Address Resolution Protocol)

(10.2.2.2, Fb)



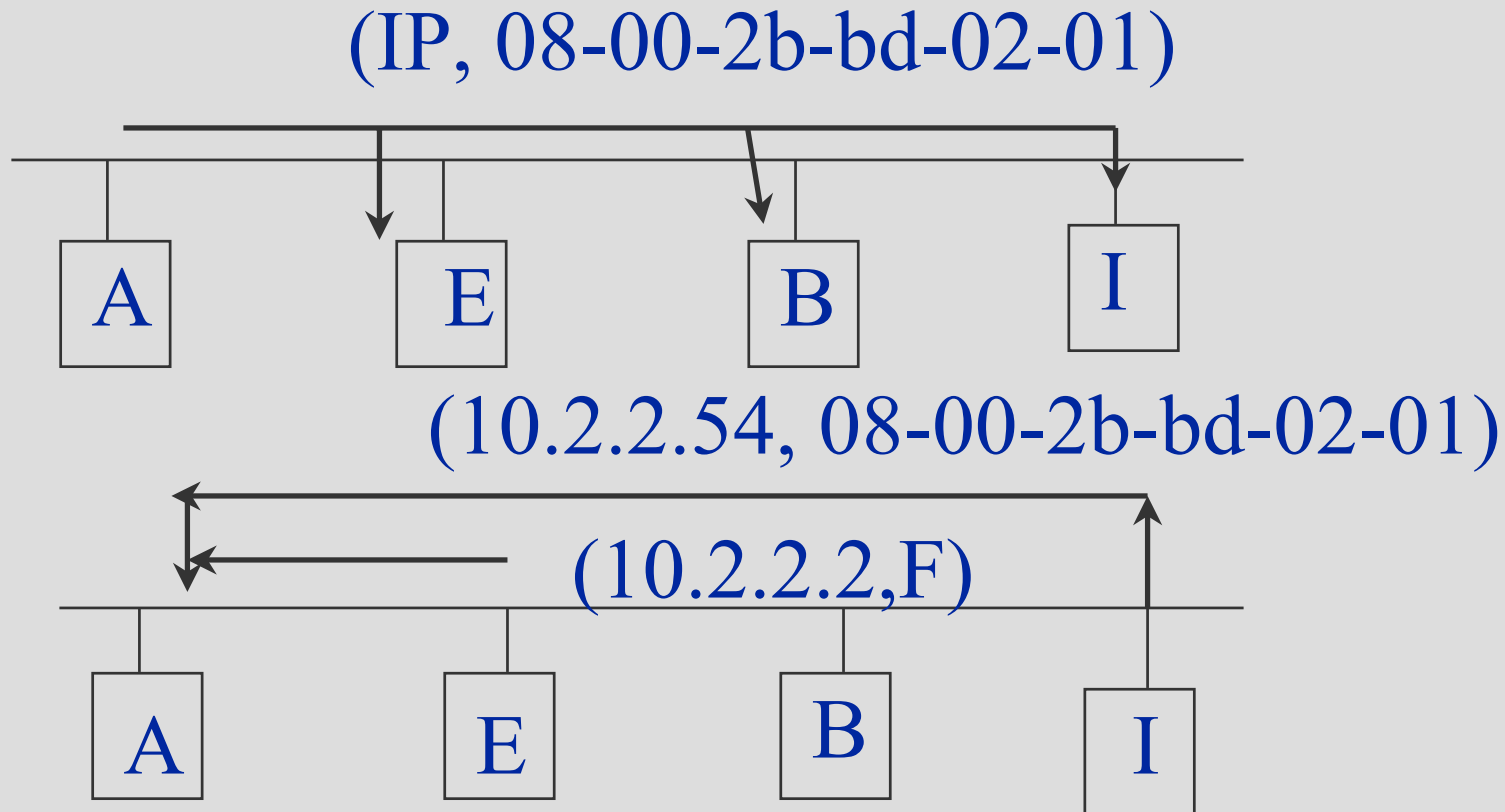
(10.2.2.2, 08-00-2b-bd-02-01)



RARP (Reverse Address Resolution Protocol)

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

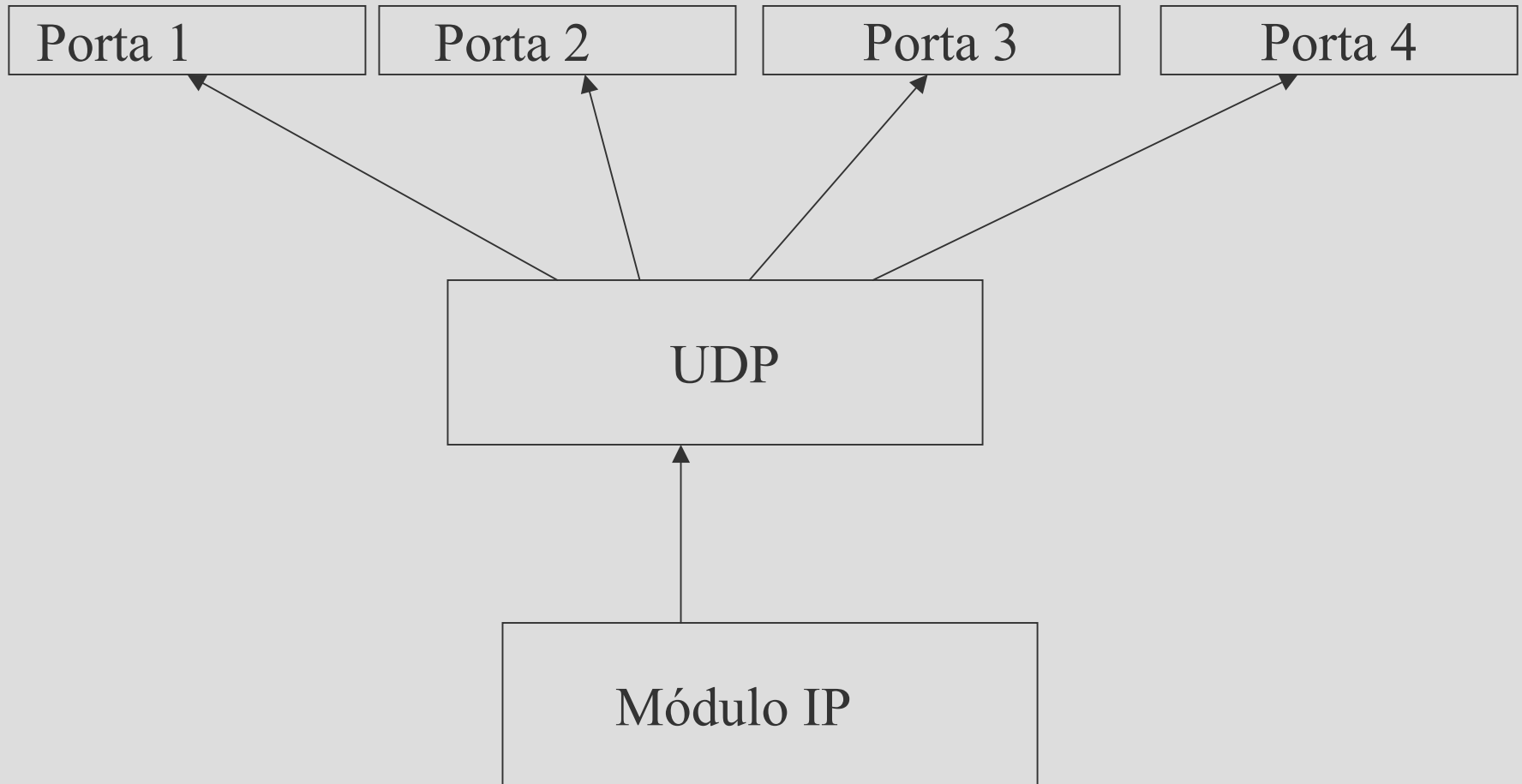
UDP (User Datagram Protocol)

- 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)

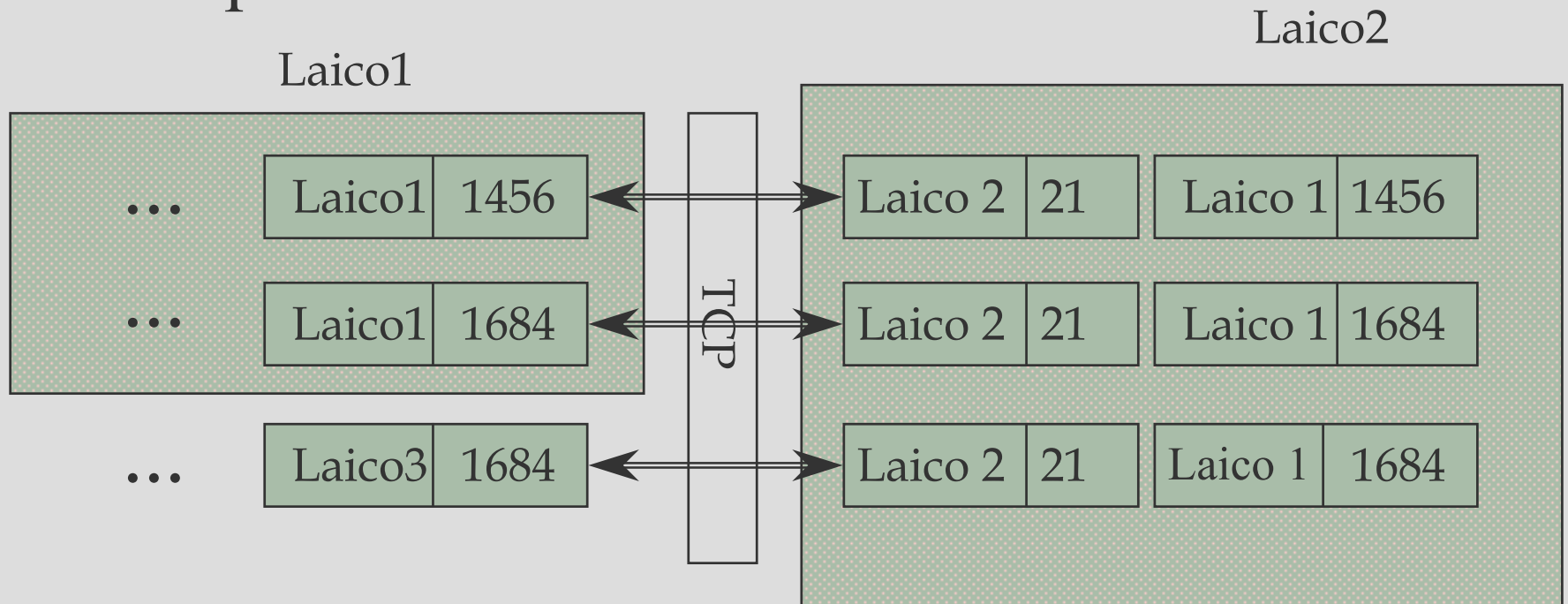
- Usado para aplicações cliente-servidor, serviços críticos,...
- Faz a multiplexação de mensagens para as aplicações
- Conexão (IP,port) <--> (IP,port)
Permite multiplas sessões do mesmo serviço

Janela Deslizante

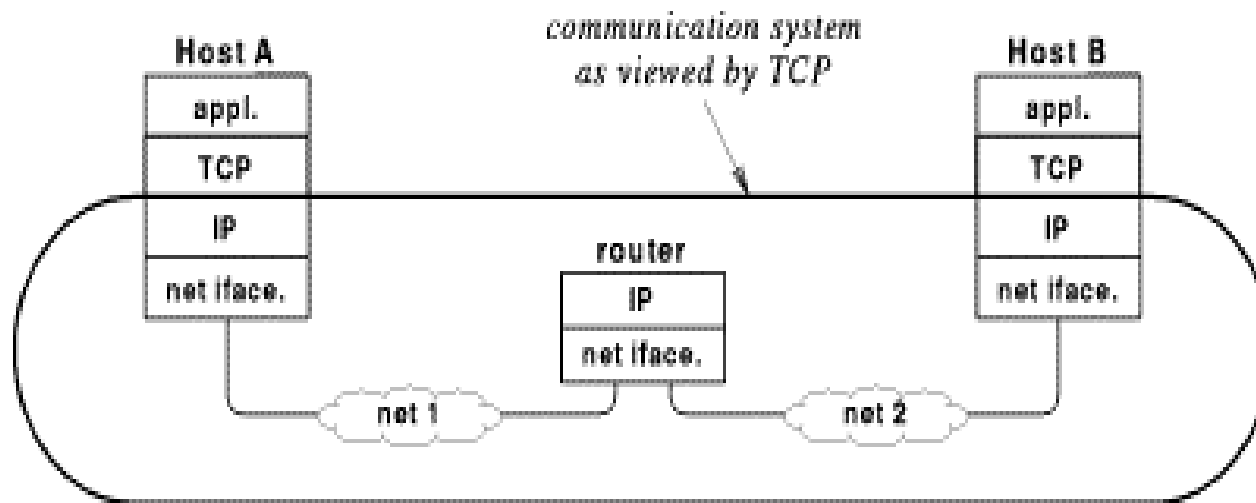
- Cada octeto é numerado
- O tamanho da janela determina o número de octetos que podem ser transmitidos sem reconhecimento
- Através do mecanismo de PIGGYBACK pode-se reconhecer um bloco de octetos via um segmento de dados

TCP - Exemplo

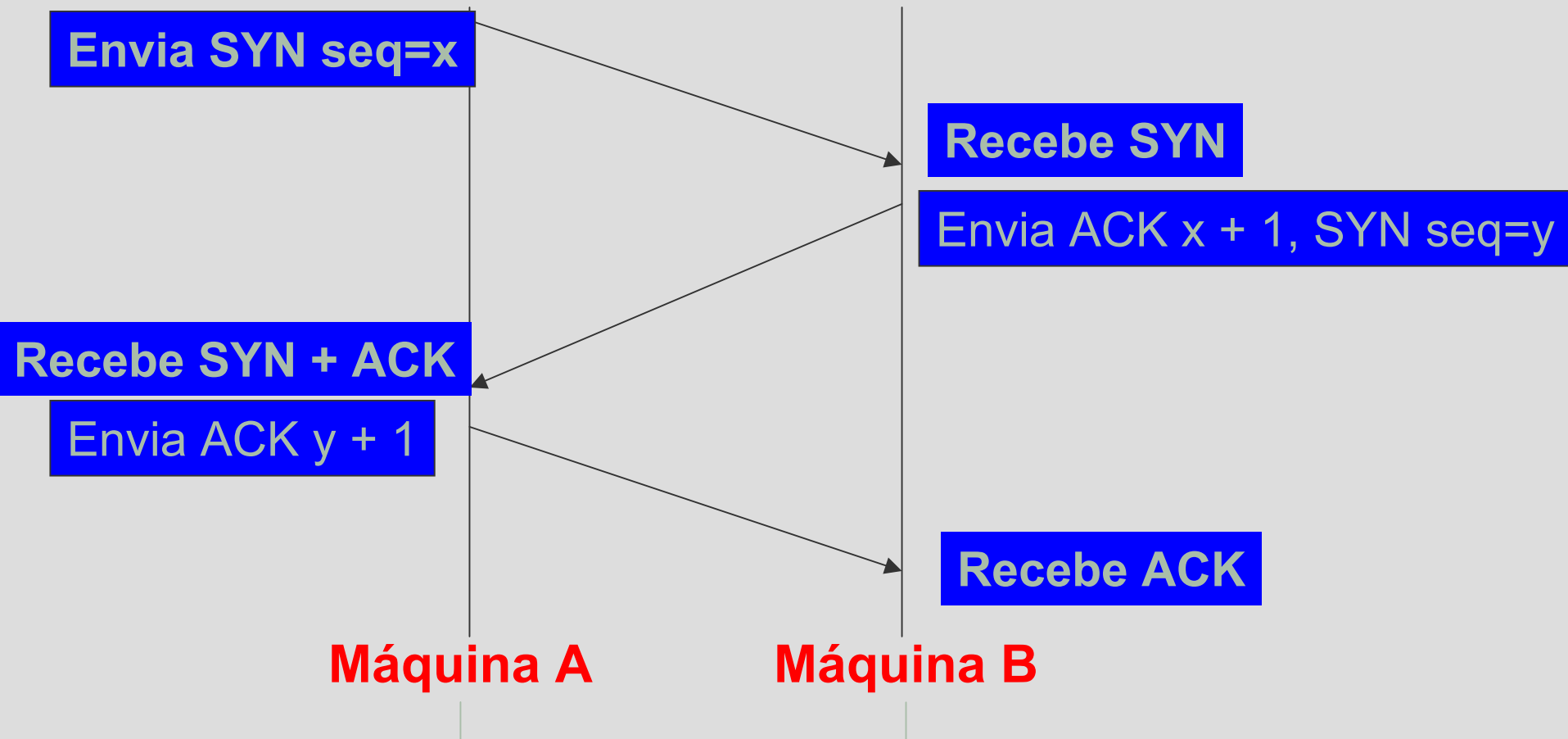
- FTP - port 21



TCP - Visão de comunicação

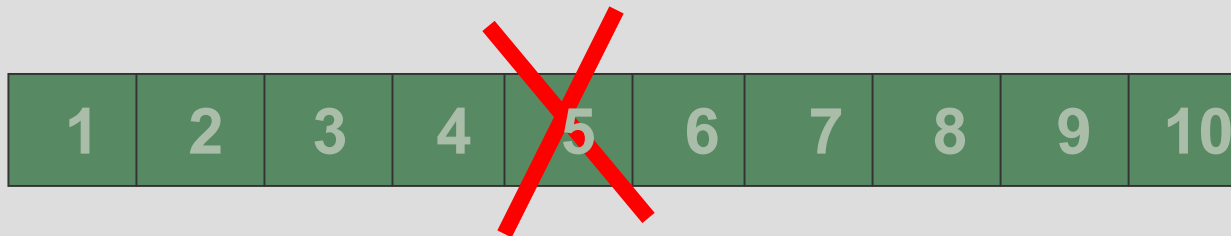


TCP - Estabelecimento de Conexão



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)

TCP

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

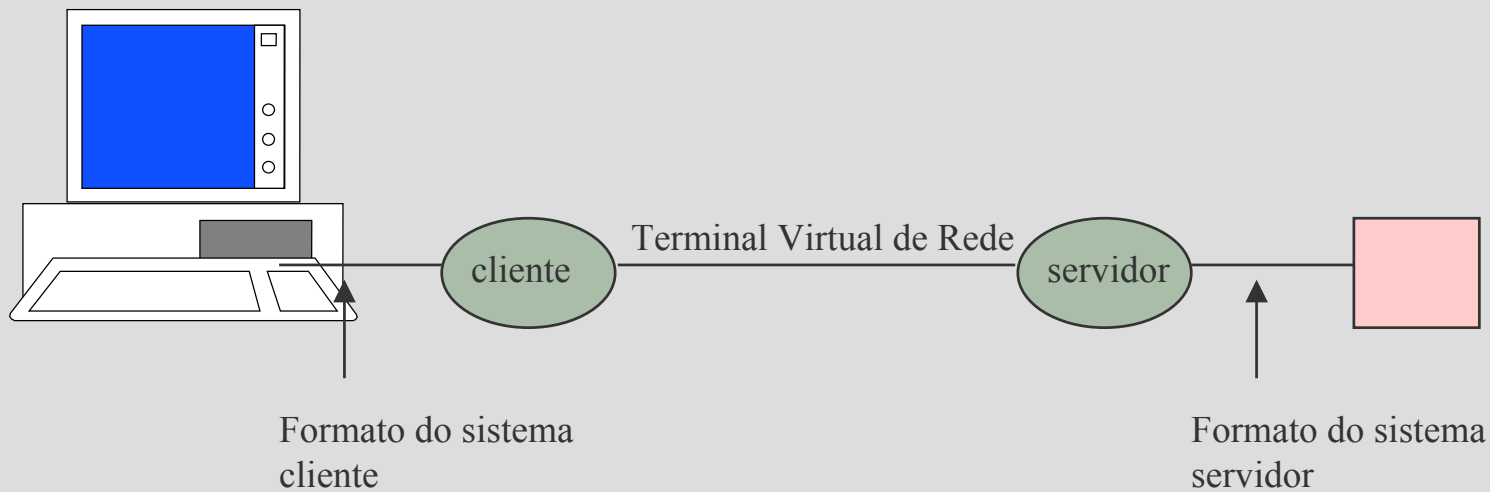
Campos do TCP

- **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

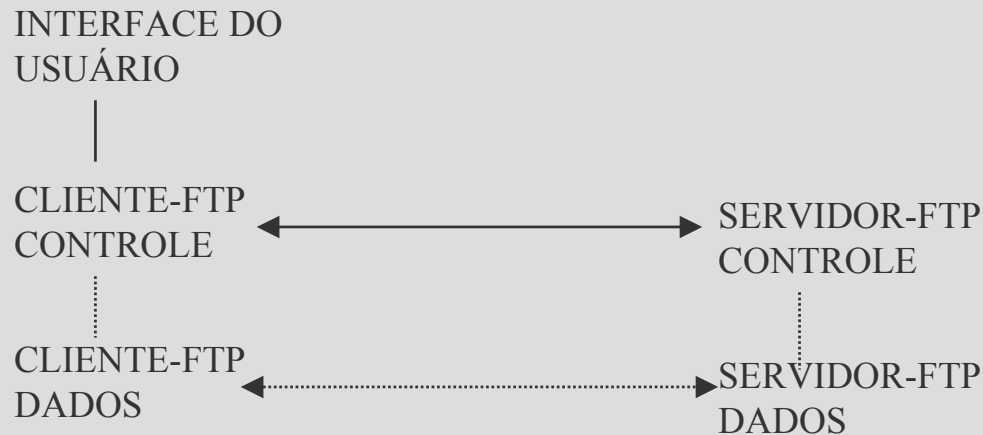
- **Checksum:** verificador de erros de transmissão
- **Urgent pointer:** fornece a posição dos dados urgentes dentro do campo de dados
- **Opção:** pode conter negociação de opções tal como o MSS (Maximum Segment Size)

Telnet



FTP

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



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>

Diferenças entre IPv4 e IPv6

Introdução

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

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

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

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

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

- Maior endereço : é uma das características mais marcante da nova versão do IP. O IPv6 quadruplicou o tamanho do IPv4 de 32 bits para 128 bits (*esta expansão foi projetada para atender um futuro ainda não imaginado*) ;
- Formato de cabeçalho flexível : o formato do datagrama IP não é compatível com o antigo datagrama IPv4. A abordagem foi implementar um formato com uma série de cabeçalhos adicionais. Em outras palavras, diferente do IPv4 onde é usado um tamanho fixo para o formato onde os campos têm tamanhos fixos.

- Opções melhoradas : as opções disponíveis no IPv6 são mais poderosas quando comparadas com o IPv4;
- Suporte para reserva de recursos : existe um mecanismo que permite a alocação prévia de recursos da rede. Desta forma, aplicações como vídeo em tempo real que necessitam de uma garantia de largura de banda e baixo retardo podem ser atendidas;
- Previsão para uma extensão do protocolo : esta característica é tida por muitos como a maior melhoria. Em outras palavras, existe uma flexibilidade de expansão do protocolo para novas realidades. De forma oposta ao IPv4, onde existe uma especificação fechada e *completa* do protocolo.

ENDEREÇAMENTO IPv6

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

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

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

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

Notação do Endereço IPv6

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



O que vem a ser isto ?

Colon Hex

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

Decimal

255.255.10.150.128.17.0.0.255.255.255.255.100.140.230.104

Colon Hex

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

Colon Hex

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

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

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

Este endereço pode ser representado como :

FF05::B3

Esta técnica somente pode ser usada uma vez num endereço.

Colon Hex

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

Exemplo :

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



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

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).

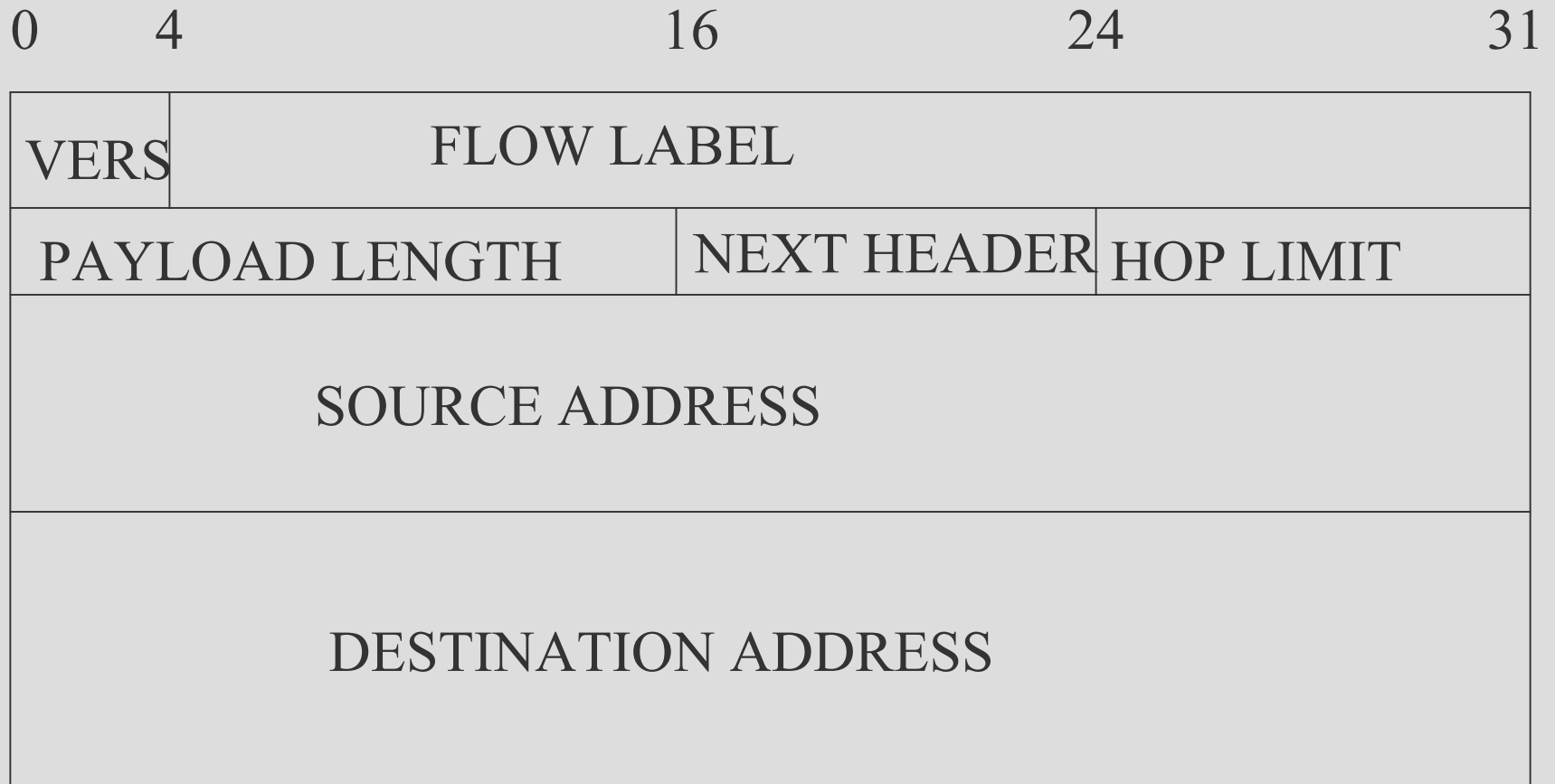
- *Multicast* - o destino é um conjunto de computadores, possivelmente em locais diferentes. Assim o datagrama deverá ser entregue para cada membro do grupo multicast usando facilidade de multicast de hardware, ou broadcast se possível.

Forma Geral do Datagrama IPv6

Base Header	Extension Header 1	...	Extension Header n	Data
----------------	-----------------------	-----	-----------------------	------

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 :



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.

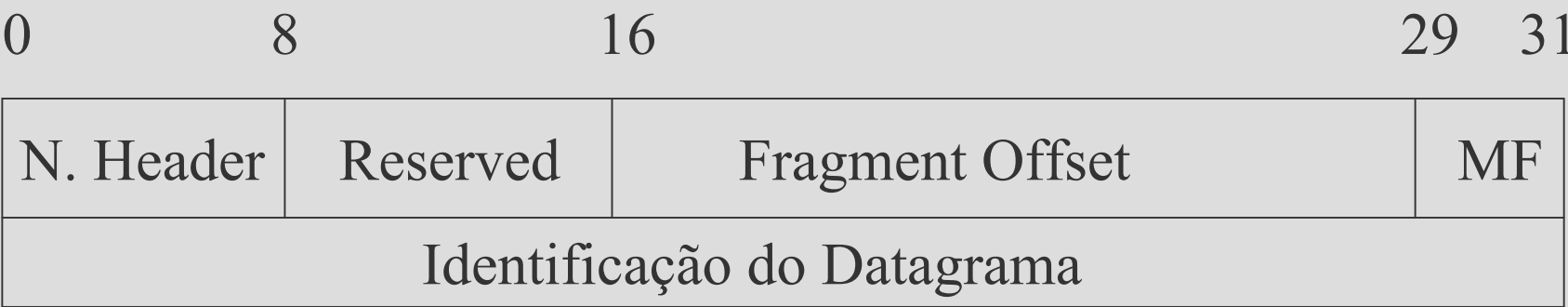
IPv6 Priority Values

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 :



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.