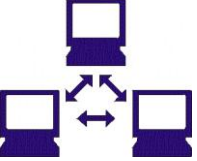
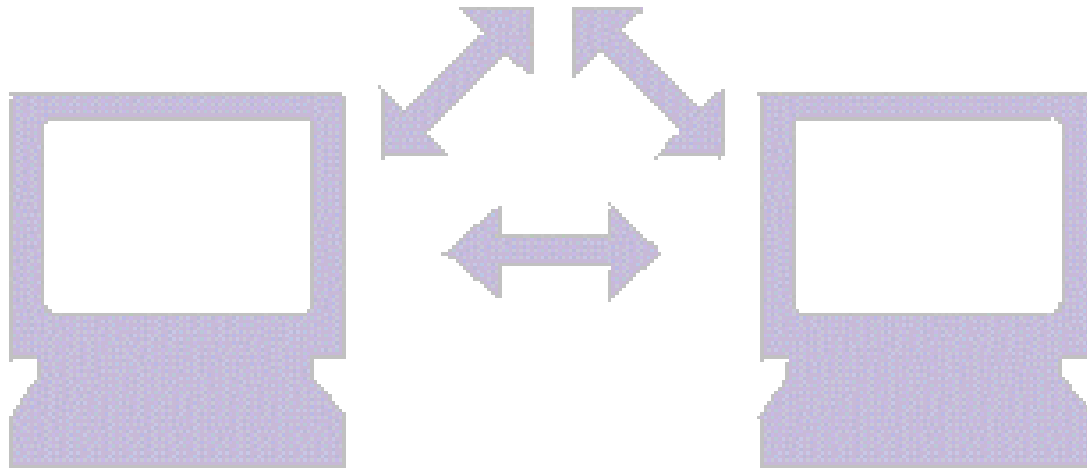


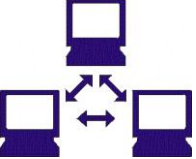
## Redes de Computadores

Instituto Federal da Bahia  
Allan Edgard Silva Freitas



## PROTOS





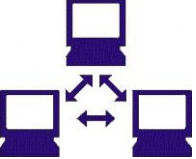
## Protocolos

- Conjunto de regras e convenções sobre a forma que se dará a comunicação entre entidades de sistemas diferentes
- Características:
  - Sintaxe: Formato de dados, codificação
  - Semântica: Mensagem, usa informação de controle para coordenação de erros
  - Timing: Define velocidades e seqüência de envio



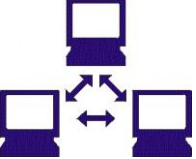
## Protocolos

- Classificações:
  - diretos/indiretos: atua na mesma rede ou em redes distintas
  - monolíticos/estruturados: funcionamento por um ou em camadas
  - simétricos/assimétricos: mesmo protocolo ou protocolos distintos nas duas entidades
  - standard/não standard: padronizados ou proprietários



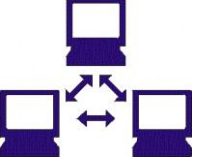
## Protocolos

- Funções:
  - segmentação/reagrupamento
  - encapsulamento
  - controle de conexão
  - ordem de entrega
  - controle de fluxo

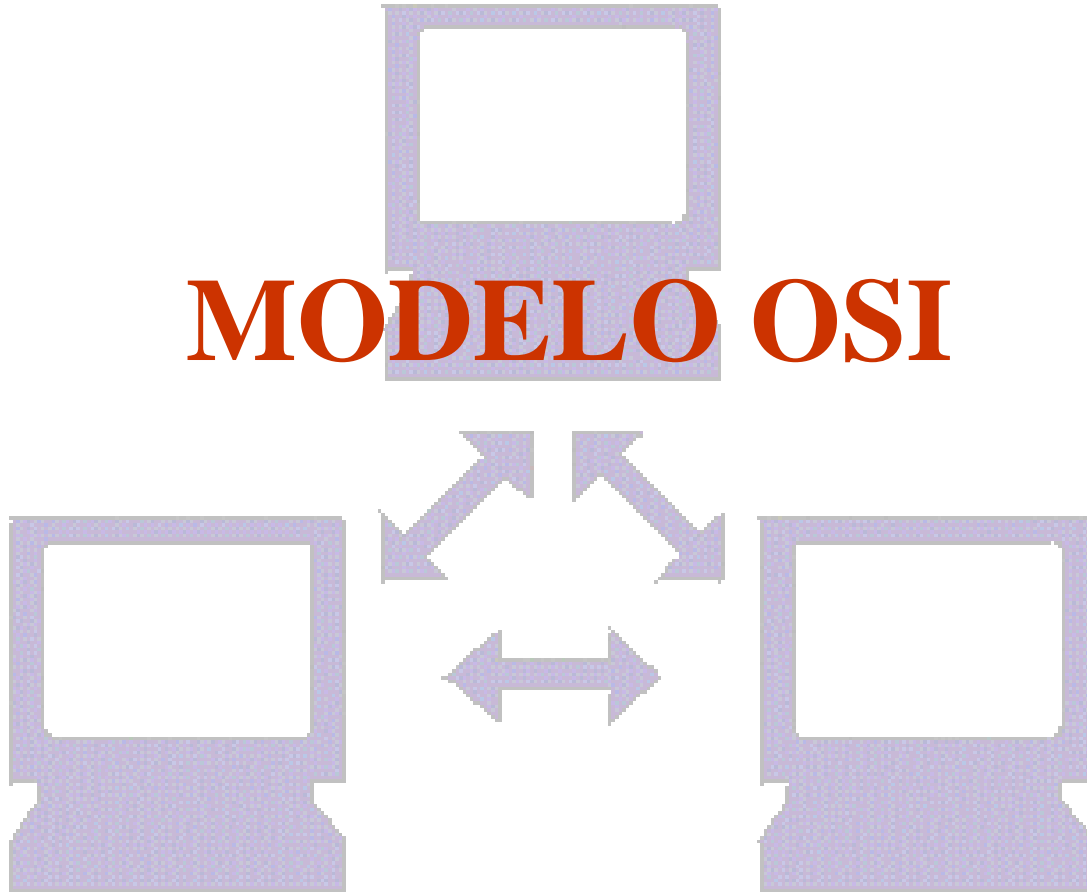


## Protocolos

- Funções:
  - controle de erro
  - endereçamento das entidades e serviços
  - multiplexação
  - serviços de transmissão como QoS, prioridade, segurança, grau de serviço, throughput mínimo, retardo máximo



## MODELO OSI

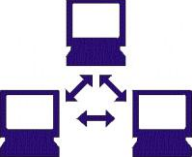




## Modelo OSI

- Proposto pela ISO (1984)
- Em camadas
- Define as funções de cada camada e facilita a criação de novos padrões de protocolo:
  - funções bem definidas em cada camada permitem novos padrões desenvolvidos de forma independente para cada camada
  - mudanças de protocolo em uma camada não afetam software que já existe em outra camada





## Modelo OSI

- Sete camadas dividem as funções de comunicação
- As interfaces entre os módulos são simples
- Princípio do ocultamento da informação:
  - camadas inferiores tratam com uma quantidade grande de detalhes
  - camadas superiores são independentes destes detalhes



## Modelo OSI

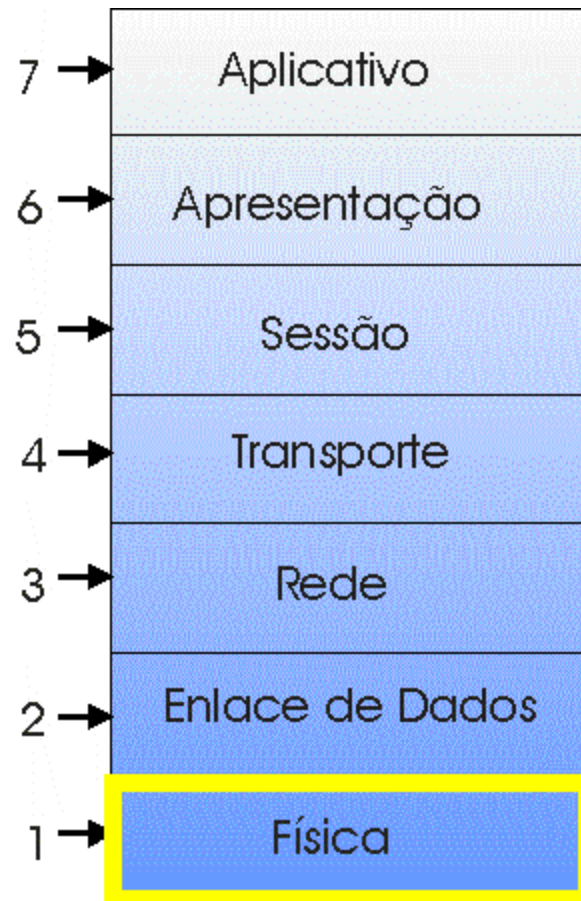
- Cada camada fornece serviços para camada superior e solicita serviços da camada inferior
- Cada camada de uma entidade possui um protocolo que se comunica com o mesmo protocolo na camada correspondente de outra entidade
- Cada camada realiza um subconjunto de funções relacionadas a comunicação entre sistemas



## Modelo OSI

### *Camada Física*

- É a camada responsável por enviar os bits de um computador para o outro por fio ou por outro tipo de conexão.
- Ela lida com os sinais elétricos que representam os estados 0 (desativado) ou 1 (ativado) de um bit que viaja pelo cabeamento da rede





## Modelo OSI

### *Camada de Enlace de Dados*

- É a camada que lida com *pacotes*, grupo de bits transmitidos pela rede. Ela depende da camada Física para enviar os bits
- A camada de Enlace de Dados assegura que os pacotes enviados pela rede serão recebidos e, se necessário, os envia de novo





## Modelo OSI

### *Camada de Rede*

- É a camada que lida com datagramas, que podem ser maiores ou menores que os frames.
- Esta camada lida com o roteamento de datagramas entre os computadores (*host*) da rede, e conhece os endereços desses hosts na rede.

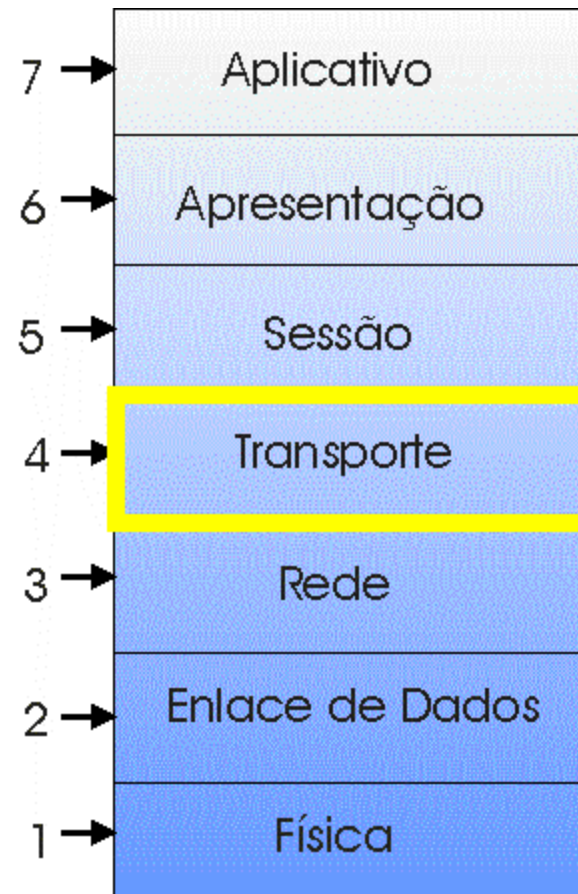




## Modelo OSI

### *Camada de Transporte*

- É a camada que lida com segmentos, que pode ser menor ou maior que os datagramas
- Essa camada assegura (ou não) que as segmentos viajarão entre os hosts sem perda de dados, se haverá estabelecimento de conexão, e, se necessário, organiza o reenvio dos datagramas

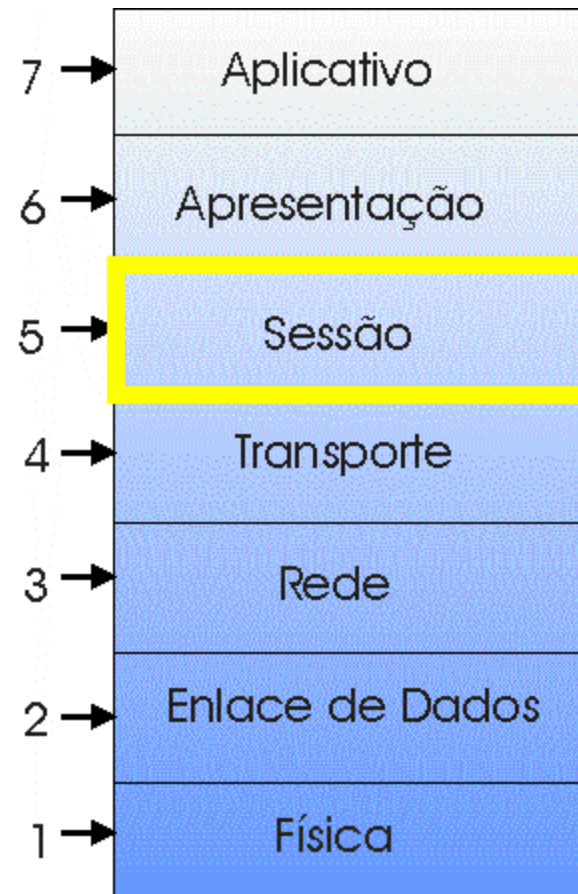




## Modelo OSI

### *Camada de Sessão*

- Essa camada estabelece e mantém uma sessão entre aplicativos que estão sendo executados em computadores diferentes
- Ela trata questões de sincronismo de comunicação

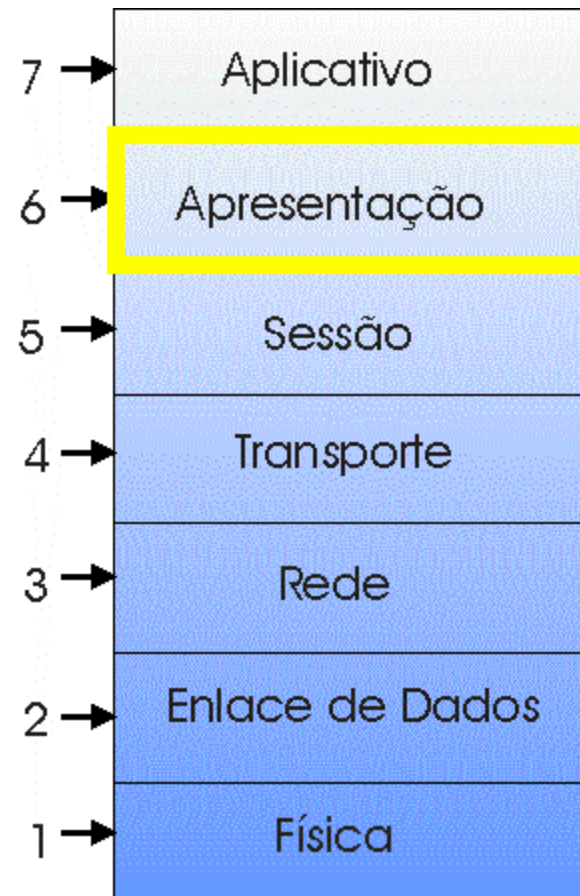




## Modelo OSI

### *Camada de Apresentação*

- Fornece serviços que vários aplicativos diferentes utilizam, tais como criptografia, compressão ou conversão de caracteres (de ASCII para EBCDIC da IBM)



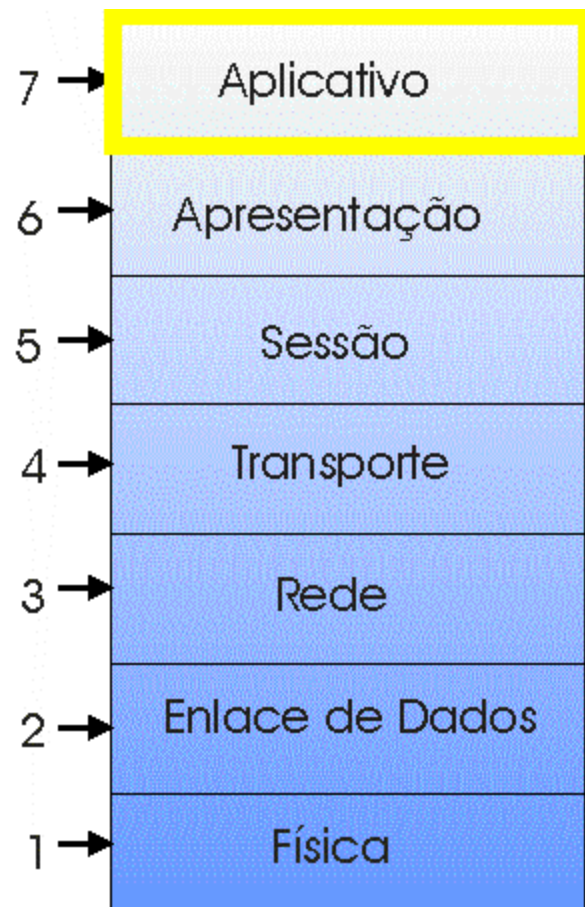


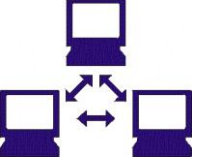


## Modelo OSI

### *Camada de Aplicativo*

- É a camada que lida com as solicitações dos aplicativos que requerem comunicações de rede, como o acesso a um banco de dados ou o envio de um correio eletrônico.
- Esta camada oferece acesso direto aos aplicativos que estão sendo executados em computadores ligados em rede





## Modelo OSI

**HOST A**

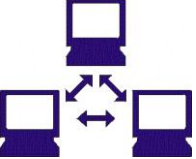


**HOST B**



**Roteador**



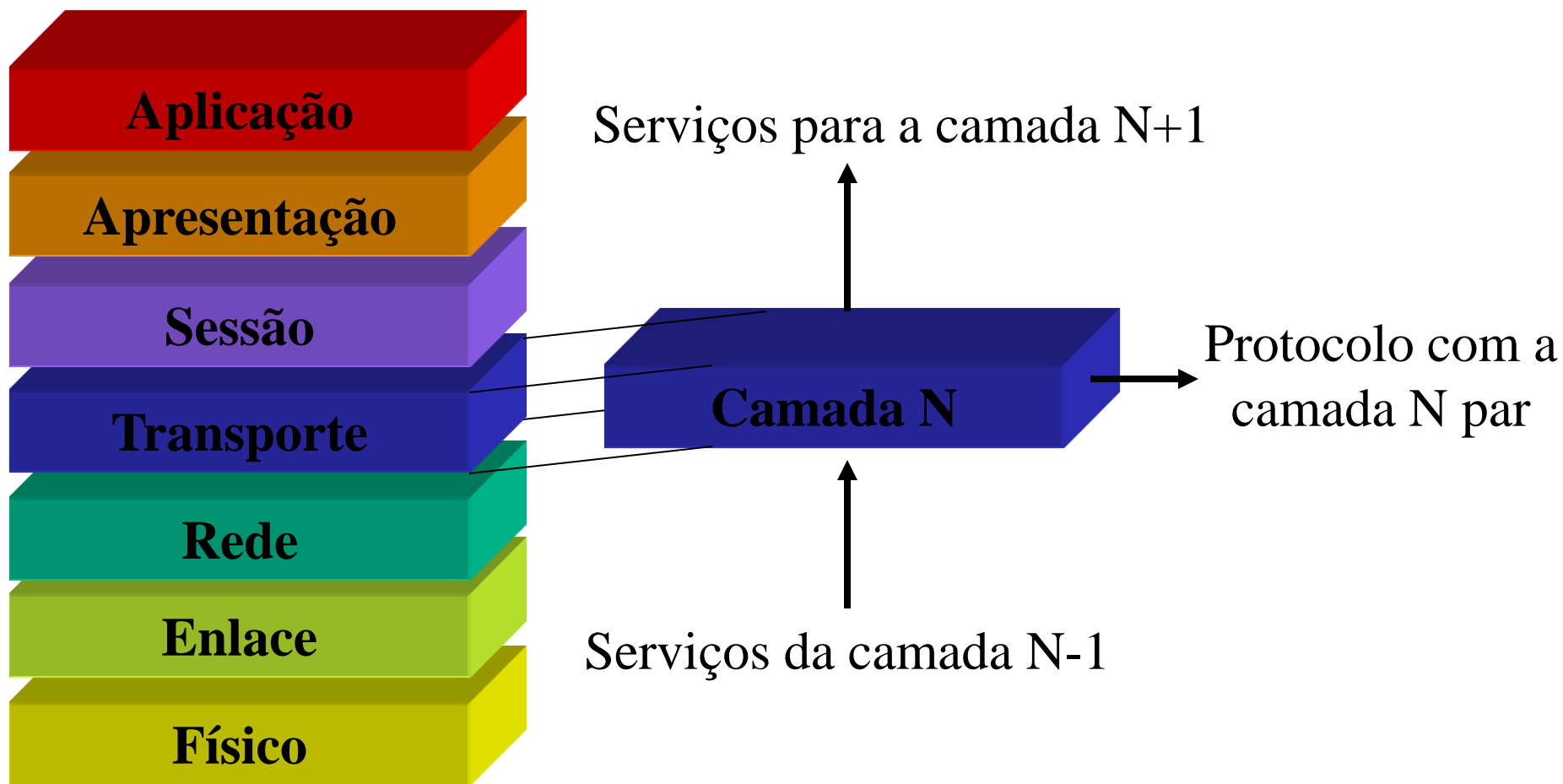


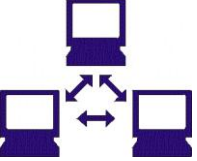
## Modelo OSI

- As camadas rede, enlace e físico podem não estabelecer comunicação fim-a-fim
- A camada de rede estabelece comunicação entre nó de origem e nó de destino, passando por nós roteadores se necessário, estabelecendo na comunicação de um nó a outro comunicações ponto-a-ponto

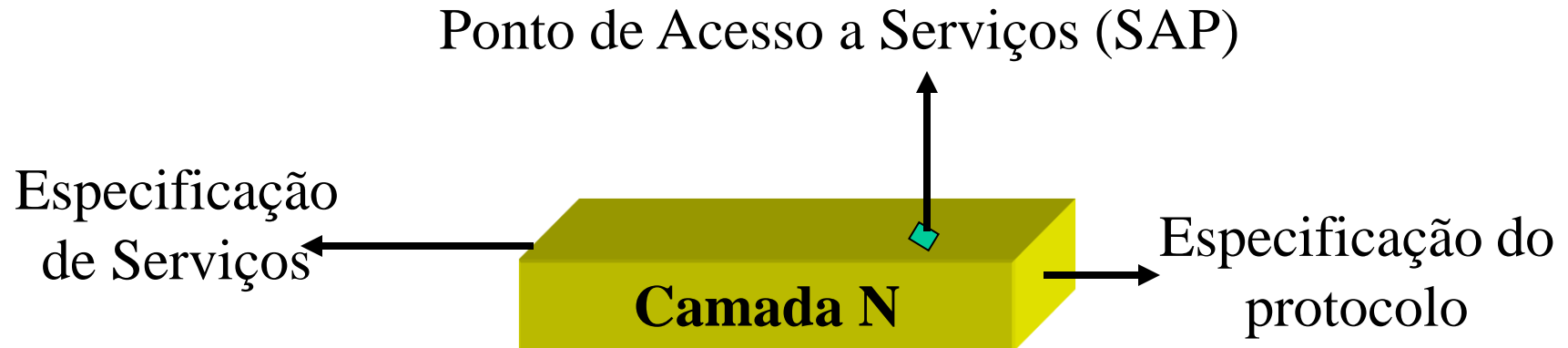


## Modelo OSI





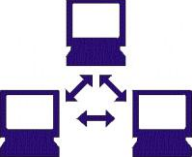
## Modelo OSI





## Modelo OSI

- Especificação de protocolos: 2 entidades de uma mesma camada em sistemas diferentes cooperam e interatuam por um protocolo. Este deve ser especificado de forma precisa: sintática, semântica e timing.
- Definição de serviços: padronização dos serviços a serem ofertados para a camada superior
- Endereçamento: cada camada provê serviços a superior que são acessíveis por meio de um SAP



## Modelo OSI

- Os serviços entre as camadas OSI são expressos em termos de:
  - primitivas: especificam a função a ser executada
  - parâmetros: passam dados ou informações de controle



## Modelo OSI

- Request: Emitida pelo usuário de um serviço para invocá-lo e passar os parâmetros necessários para especificar completamente o serviço
- Indication: A primitiva usada por um provedor de serviço para: indicar que um procedimento foi invocado pelo usuário de camada par e fornecer os parâmetros associados e notificar o usuário do serviço de uma ação iniciada no provedor





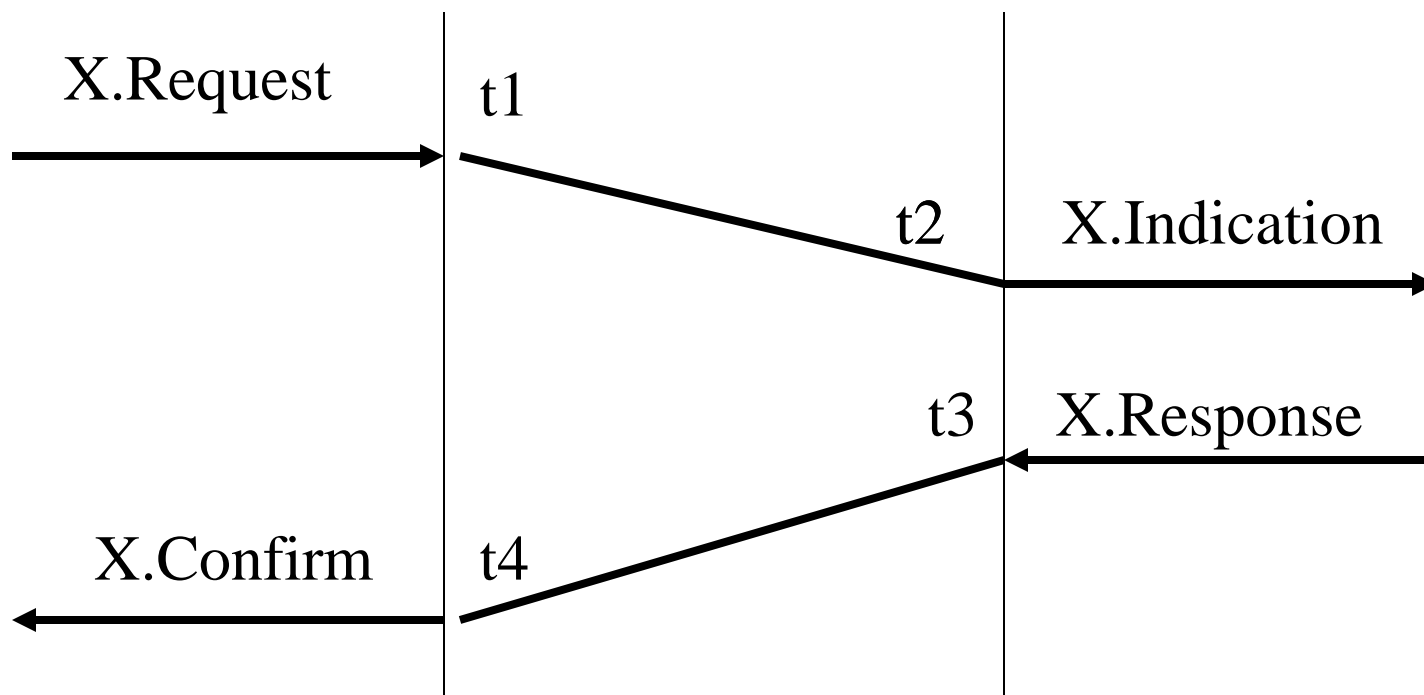
## Modelo OSI

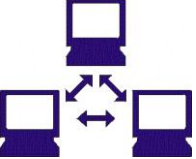
- Response: Primitiva emitida por um usuário do serviço para reconhecer ou completar algum procedimento invocado previamente por meio de um Indication para esse usuário
- Confirm: Primitiva usada pelo provedor de serviço para reconhecer ou completar algum procedimento invocado previamente por meio de um Request pelo usuário do serviço



## Modelo OSI

- Essas primitivas são geradas em todas as camadas





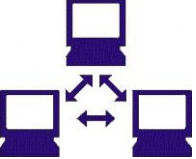
## Camada de Rede

- Serviços da Camada de Rede oferecidos a camada de transporte:
  - serviço orientado a conexão
  - serviço não orientado a conexão
  - serviço confiável
  - serviço não confiável
- Normalmente, serviços orientados a conexão possuem confiabilidade



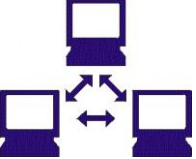
## Camada de Rede

- Serviços da Camada de Rede:
  - conexão (orientado ou não)
  - roteamento
  - controle de congestionamento
- No serviço com conexão estabelece-se circuito virtual
- O circuito virtual determina o roteamento uma única vez para a conexão
- No serviço sem conexão as rotas podem se alterar



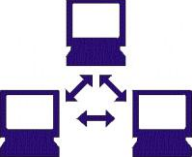
## Camada de Rede

- No serviço sem conexão cada pacote é roteado de forma independente dos demais
- No serviço com conexão se estabelece a rota para todos os pacotes da conexão, podendo-se reservar banda para a conexão



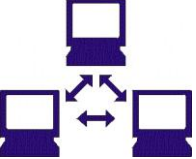
## Roteamento

- Métricas de roteamento:
  - Largura de banda
  - Tipo de carga
  - Distância entre roteadores
  - Congestionamento
  - Número de hops
- Tipos:
  - estático
  - dinâmico



## Roteamento

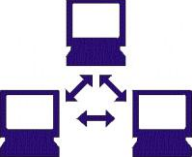
- Tipos de Protocolos de Roteamento:
  - Não Adaptativos
    - Algoritmo de Dijkstra
  - Adaptativos
    - Distância Vetorial (Bellman-Ford)
    - Estado de Enlace (Short Path First)
  - Flooding



## Roteamento

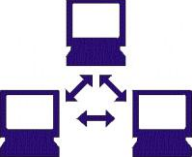
- Tabela de Roteamento:
  - manualmente: inicialização do SO do roteador
  - dinamicamente: tempo de execução





## Flooding

- Roteador envia pacotes para todas as suas interfaces
- Inunda a rede
- O pacote sempre alcança o destino
- Tráfego desnecessário



## Algoritmo de Dijkstra

- Modelagem de Grafo:
  - Arcos são linhas de comunicação (enlaces)
  - Nós são roteadores
  - Rotas são caminhos entre nós de um grafo
  - Cada arco tem um peso indicando o custo do enlace



## Algoritmo de Dijkstra

- Cada nó é rotulado por sua distância ao nó de origem ao longo do menor caminho até então
- inicialmente todos os nós são rotulados com infinito
- cada interação analisa-se a vizinhança do nó ativo e escolhe-se o novo nó ativo
- Inicialmente os rótulos (labels) são provisórios, quando se descobre que o label representa o menor caminho possível ele se torna permanente



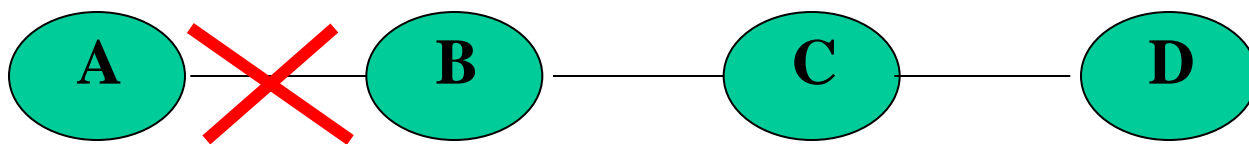
## Distância Vetorial

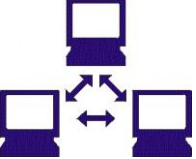
- Cada roteador tem uma tabela de todas as rotas conhecidas
- inicialmente, o roteador tem em sua tabela redes em que se conecta diretamente e rotas estáticas
- cada rota possui uma distância, dada em hops
- cada entrada de rota tem: rede destino, distância e a rota
- cada roteador, periodicamente, envia sua tabela a roteadores vizinhos



## Distância Vetorial

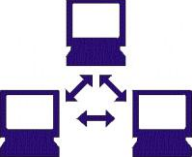
- Roteadores ao receberem tabelas de vizinhos, comparam e atualizam sua própria tabela
- processamento rápido do algoritmo
- convergência lenta
  - ex: D demora para perceber queda do enlace





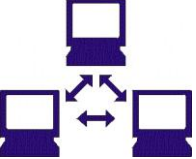
## Estado de Enlace

- Cada roteador deve ter informação completa da topologia
- isto ocorre pelo fato de cada roteador enviar uma mensagem com o estado de seus enlaces por flood para a rede
- cada roteador deve testar continuamente seus enlaces, obtendo o tempo médio de alcance do vizinho
- após obter a topologia o roteador executa Dijkstra



## Hierarquização de Roteamento

- Regiões de roteamento
- informações de rotas internas a região não se propagam fora dela
- rotas padrão



# Controle de Congestionamento

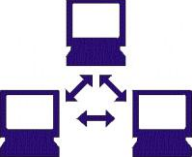
- Loop aberto: controle de trafico de quem envia para a rede, evitando o congestionamento
- Loop fechado: controle de tráfico no roteador, tratando o congestionamento existente
- Caso a rede adote circuito virtual, estabelece-se bandas de uso, assim há uma visão da banda total da rede e evitando-se o congestionamento





## Controle de Congestionamento

- Loop Aberto:
  - Algoritmo do Balde Furado: Limita a informação que pode ser enfileirada para transmissão de dados. Modela um buffer de transmissão finito e taxa limite de transmissão de mensagens provenientes do balde
  - Algoritmo de Balde Furado de Tokens: cria permissões (tokens) de envio de  $N$  bits a cada intervalo de tempo. A mensagem tem de utilizar os tokens, limita o tráfego, mas permite rajadas



## Controle de Congestionamento

- Loop Fechado:
  - Rede com conexão: proíbe o estabelecimento de novos circuitos virtuais e renegocia banda dos existentes
  - Rede sem conexão: descarte do pacote gera pacote regulador informando roteadores do congestionamento, estes aplicam alguma técnica de controle com Loop Aberto
  - Escoamento de carga: último recurso, descarta todos os pacotes ou os de menor prioridade



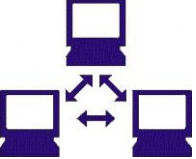
## Camada de Transporte

- 1ª camada com tratamento fim-a-fim
- Fornece serviço com e sem conexão de forma independente de rede
- Faz controle de fluxo fim-a-fim
- Oferece QoS
- Várias conexões de transporte utilizam os serviços de uma comunicação de rede
- Upward Multiplexing: única conexão de transporte usa várias conexões físicas de rede



## Camada de Transporte

- Classe 0: simples, sem mecanismos de detecção e reconhecimento de erros
- Classe 1: recuperação de erros sinalizados pela rede
- Classe 2: multiplexação e controle de fluxo
- Classe 3: recuperação de erros vistos pela rede e multiplexação
- Classe 4: detecção, recuperação, multiplexação e controle de fluxo
- TCP é classe 4



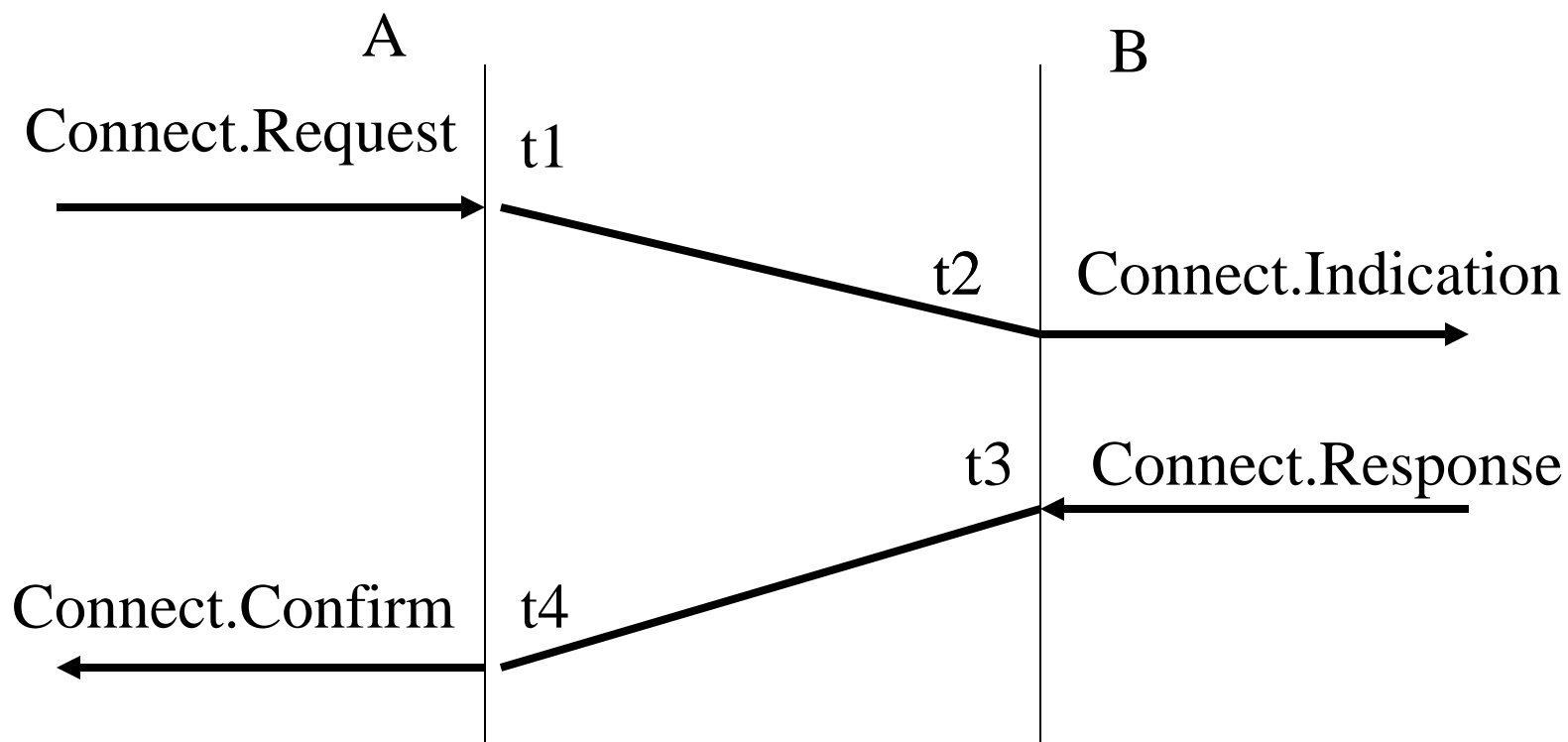
## Camada de Transporte

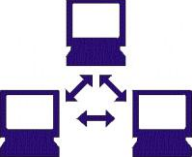
- Classe 0: simples, sem mecanismos de detecção e reconhecimento de erros
- Classe 1: recuperação de erros sinalizados pela rede
- Classe 2: multiplexação e controle de fluxo
- Classe 3: recuperação de erros vistos pela rede e multiplexação
- Classe 4: detecção, recuperação, multiplexação e controle de fluxo
- TCP é classe 4



## Camada de Transporte

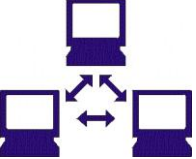
- Three-way handshake
- Se houver time-out mensagem é retransmitida





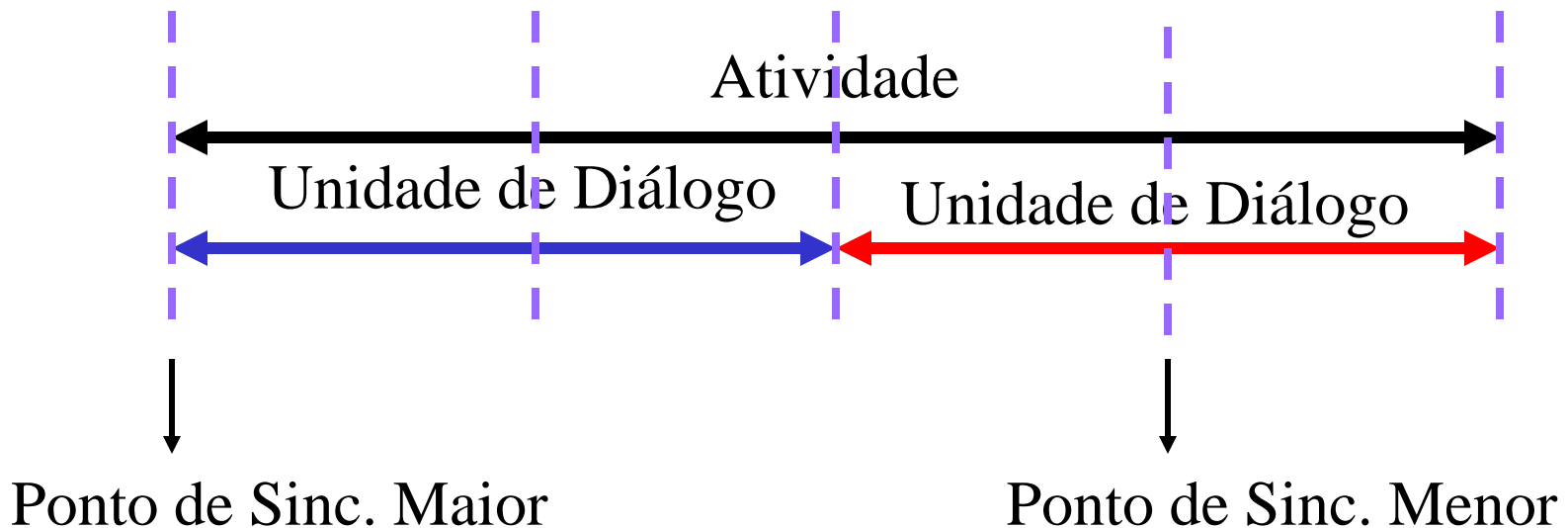
## Camada de Sessão

- Oferecer , a entidades de apresentação cooperantes, meios de organizar e sincronizar seu diálogo, garantindo troca ordenada de dados, via sessão
- define pontos de sincronização em um diálogo
- após erro ou interrupção, comunicação é retomada a partir do ponto de sincronização
- negocia tokens para troca de dados, sincronização e liberação de conexão de sessão



## Camada de Sessão

- Ponto de sincronização maior: estrutura a troca de dados em unidades de diálogo
- Ponto de sincronização menor: estrutura a troca de dados dentro de unidade de diálogo







## Camada de Sessão

- Token de Sessão: Atributo de uma conexão de sessão que é dinamicamente atribuído aos usuários dos serviços da camada de sessão. A posse do token permite o uso exclusivo de um tipo de serviço
  - token de dados
  - token de sincronização maior
  - token de sincronização menor
  - token de liberação ordenada



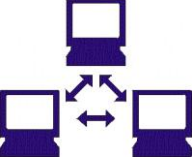
## Camada de Apresentação

- Resolver os problemas de apresentação de informações existentes entre sistemas heterogêneos interconectados em um ambiente OSI
- ASN.1 (Abstraction Syntax Notation.One): define os tipos de dados sem representação física
- BER (Basic Encoding Rules): Define regras de representação física dos tipos de dados, incluindo ordem de bits, uso de ponto flutuante etc.



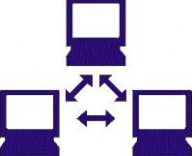
## Camada de Apresentação

- Define sintaxe abstrata (ASN.1) e sintaxe de transferência (BER)
- Transformação dos dados de aplicação para uso especial como compressão e criptografia
- Função:
  - Mapeamento de conexão de apresentação
  - Negociação e renegociação de contexto de apresentação
  - Transformação de sintaxe
  - Repasse dos serviços de sessão para aplicação

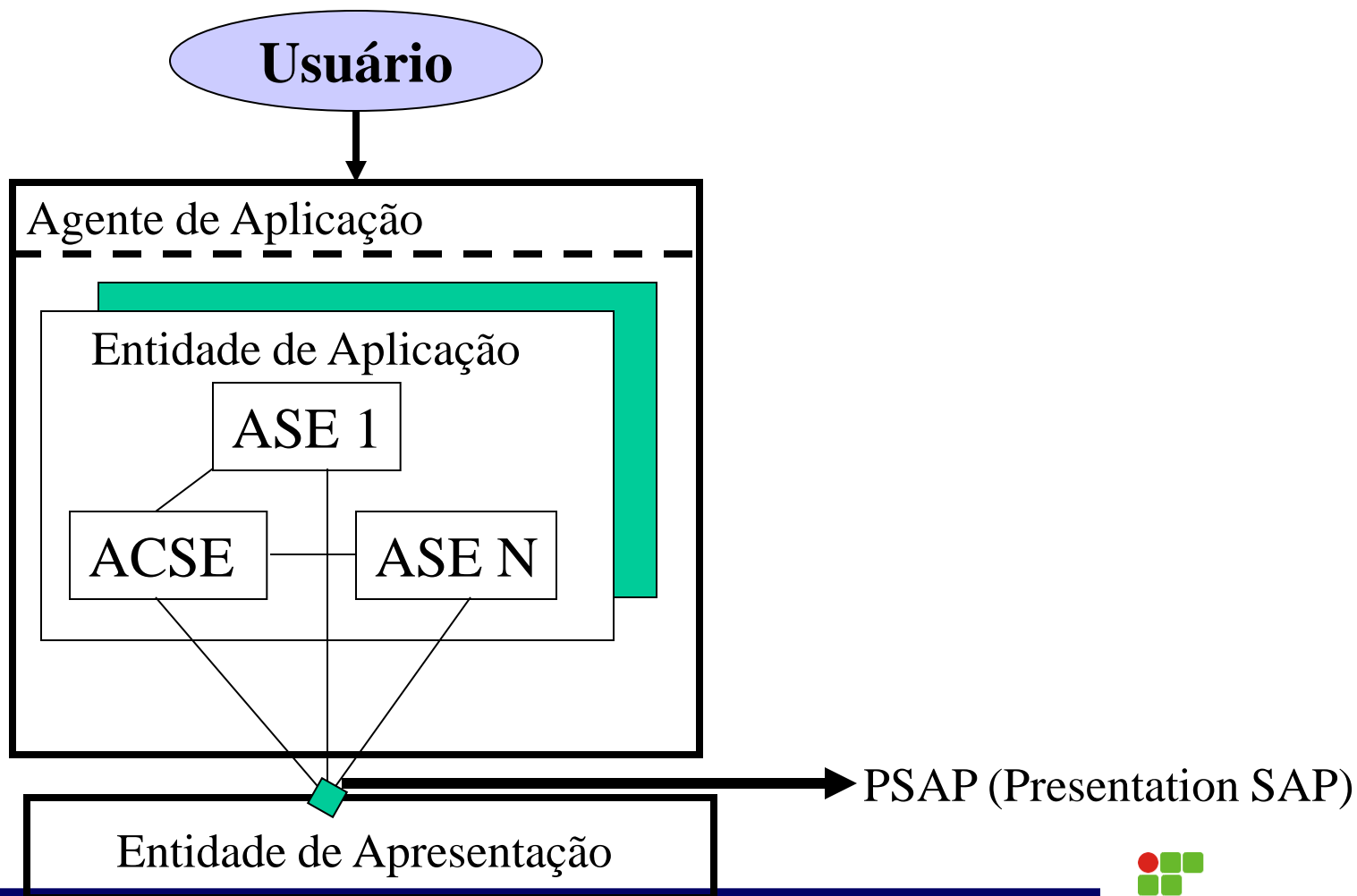


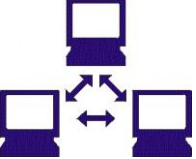
## Camada de Aplicação

- Oferecer aos processos aplicativos meios de acessar o ambiente de comunicação OSI
- Cada processo aplicativo chama uma entidade de aplicação
- Cada entidade de aplicação possui um ACSE que coordena um ou mais ASEs
- Os ASE e ACSE solicitam serviços à camada de apresentação e a mesma, à sessão e assim sucessivamente



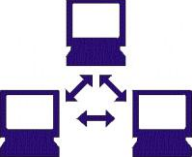
## Camada de Aplicação





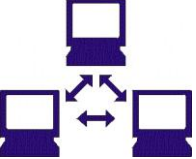
## Camada de Aplicação

- ACSE:
  - Identificar parceiros de comunicação
  - Mapeamento da associação de aplicação
  - Determinar disponibilidade de parceiro de comunicação
  - Determinar QoS aceitável
  - Negociar contexto de apresentação
  - Transferir informações entre processos de aplicação



## Camada de Aplicação

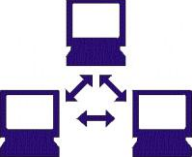
- Elementos de Serviço de Aplicação de Propósito Geral:
  - ACSE (Association Control Service Element)
  - ROSE (Remote Operation Service Element)
  - RSTE (Reliable Transfer Element)
  - TP (Transaction Processing)
  - CCR (Commitment, Concurrency and Recovery)



## Camada de Aplicação

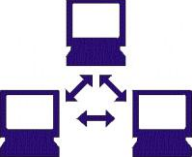
- ROSE fornece comunicação interativa entre parceiros (ex: sistemas distribuídos)
- RSTE fornece transferência confiável de informação, usando serviços de sincronização da camada de sessão
- TP ocupa-se em processos que usam transações
- CCR ocupa-se com concorrência de processos, usando-se commit para transações distribuídas





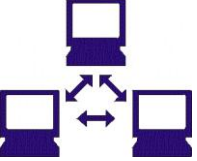
## Camada de Aplicação

- Elementos de Serviço de Aplicação de Propósito Específico:
  - MHS (Message Handling System)
  - FTAM (File Transfer Access Management)
  - VT (Virtual Terminal)
  - JTM (Job Transfer Management)
  - DS (Directory Service)
  - RDA (Remote Database Access)
  - MMS (Manufacturing Message Especification)



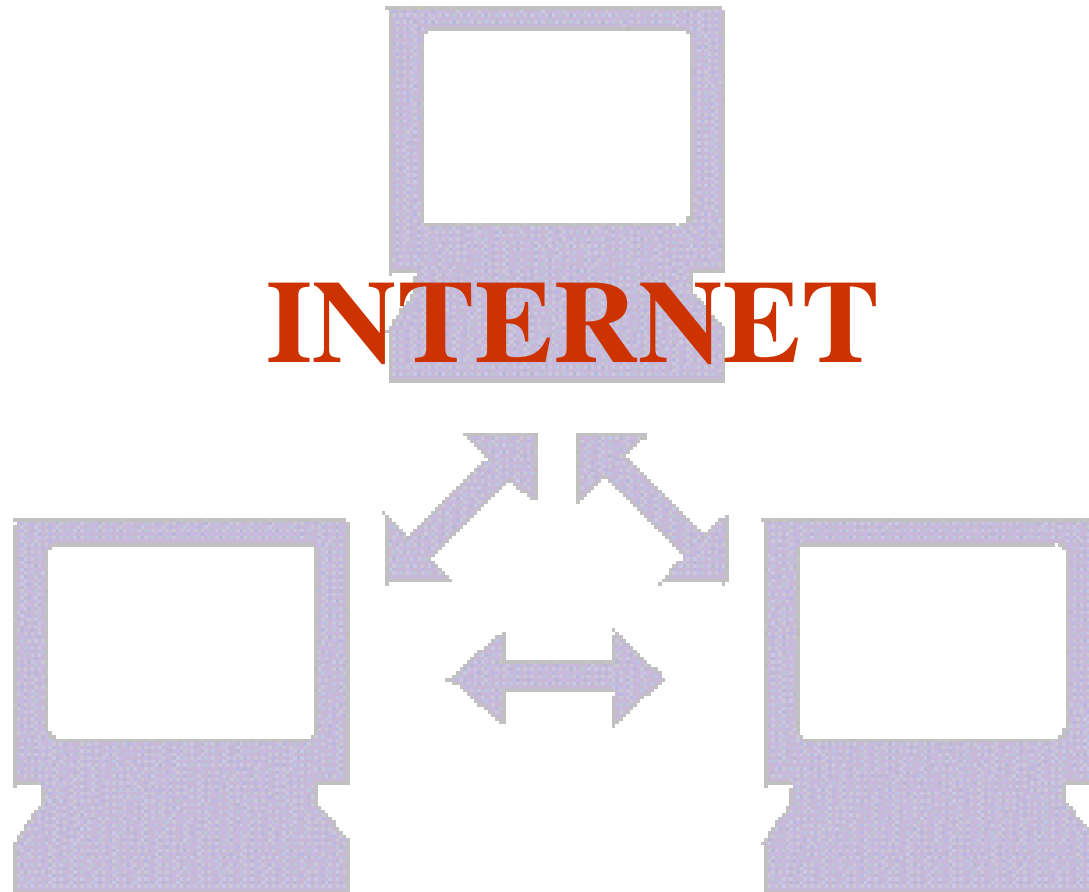
## Camada de Aplicação

- MHS é sistema de mensagens
- FTAM é padronização de FTP
- VT é utilizado em aplicações como telnet
- JTM faz transferência de jobs, por ex., entre mainframes
- DS localiza recursos da rede e é usado por ex por FTAM e MHS
- RDA faz acesso remoto a base de dados
- MMS conecta computadores com elementos como robôs e controladores



# Rede de Computadores

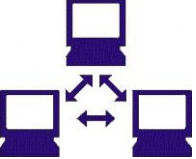
---





## Surgimento da Internet

- Iniciou-se com o DoD:
  - Contexto da Guerra Fria;
  - ARPA (Advanced Research and Projects Agency);
  - ARPANET (1970), interligando 4 Universidades e Centros de Pesquisa:
    - Roteamento e Interdependência de Redes
    - Chaveamento de Pacotes



## Surgimento da Internet

- Evolução da ARPANET:
  - Interligação de Outros Centros de Pesquisa e Universidades;
  - Padronização do TCP/IP no Backbone da ARPANET (1980);
  - Integração do TCP/IP ao UNIX de Berkeley (1983);



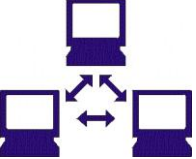
## Surgimento da Internet

- NSF:
  - National Science Foundation;
  - Interligação dos Super-computadores da NSF;
  - NSFNET (1985);
- NSFNET + ARPANET = INTERNET
  - União dos Dois Backbones (1986)
  - Expansão da Internet para a Comunidade Científica Mundial



## Surgimento da Internet

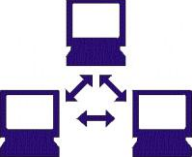
- Evolução da Internet:
  - NSFNET passa a ser mantida com apoio da IBM, da MCI e do MERIT (Responsável por uma Rede Educacional no Michigan), formando a ANS - Advanced Network and Services (1988);
  - Fim da ARPANET (1990);
  - Surge o Backbone militar DRI (1990);
  - Surge a ANSNET (1991/1992);



## Surgimento da Internet

- Evolução da Internet:
  - Backbone Europeu - EBONE (1992);
  - Abertura comercial da Internet (1993).





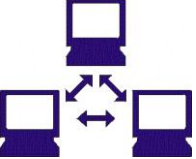
## A Internet no Brasil

- Primeiras Iniciativas:
  - FAPESP, UFRJ e LNCC - Laboratório Nacional de Computação Científica (1988);
  - MCT cria a RNP - Rede Nacional de Pesquisa (1989);
  - Embratel inicia Backbone Comercial (1995).



## A Internet no Brasil

- A Rede Nacional de Pesquisa:
  - PoPs (Points of Presence) em cada estado;
  - Interligação dos PoPs forma o Backbone;
  - Em cada estado são formados a partir dos PoPs Backbones regionais (ex: Rede Bahia, RBTD, Rede Rio, ANSP);
  - Pesquisas e Novas Iniciativas.



## Novas Iniciativas

- Redes Metropolitanas de Alta Velocidade:
  - Tecnologia ATM;
  - IPv4 e IPv6;
  - Vídeo-Conferência.
- 6Bone-BR:
  - Backbone experimental do IPv6;
  - Conectado ao 6Bone;
  - Utiliza túneis de protocolo.



## Novas Iniciativas

- Redes Regionais:
  - Fortalecimento da capilaridade dos Backbones Estaduais;
  - RBTD.
- Internet 2:
  - GigaPoPs
  - Interligação ATM entre os PoPs
  - Link de Alta Velocidade com os EUA.



# O que é a Internet hoje?

- Um emaranhado de redes ligadas entre si;
- Alguma coisa que usa TCP/IP;
- Aquele lugar onde eu vou para bater papo;
- Uma avançada estrutura de comunicações desenvolvida em escala mundial;
- Todas as afirmativas anteriores.



# E qual a filosofia da Internet?

- Compatibilidade:
  - Conectar qualquer coisa. Várias tecnologias.
- Portabilidade:
  - Conectar em qualquer lugar. Abrangência planetária (por enquanto...).
- Disponibilidade:
  - Permitir caminhos alternativos para uma mesma rede. Manter disponível sempre que possível.



## Se é assim, como as coisas funcionam?

- Padrões:
  - Uso de Padrões de Facto;
  - Protocolos Abertos.
- Entidades Chave:
  - IETF, IRTF, Internet Society, IANA, InterNIC;
  - Comitê Gestor e FAPESP (Brasil).
- Discussão dos Padrões:
  - Reference For Comments e Internet Drafts.



## O que há por trás da Internet?

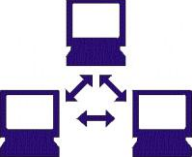
- TCP/IP:
  - Suíte de protocolos e padrões que definem a arquitetura de comunicação da Internet.
- E quais os protocolos principais:
  - IP: Internet Protocol - define Endereçamento
  - TCP: Transmission Control Protocol - define Transporte orientado a conexão
  - UDP: User Datagram Protocol - define Transporte sem conexão





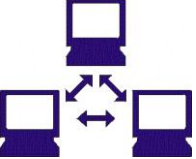
# A Arquitetura da Internet

- Várias redes ligadas entre si;
- Cada nó ligado a Internet é um host;
- Hosts que servem para interligar as redes que formam a Internet são os Gateways ou Roteadores.
- Roteadores transmitem os pacotes de uma rede a outra.



## A Arquitetura da Internet

- Cada rede conectada a Internet tem um endereço;
- Dentro de cada rede, cada host tem seu próprio endereço;
- Temos redes dentro de redes (sub-redes);
- Fator crítico da Internet: endereçamento.



## Endereçamento na Internet

- Endereço IP;
- Classes de endereços;
- Endereços especiais;
- Interfaces;
- Sub-Redes.



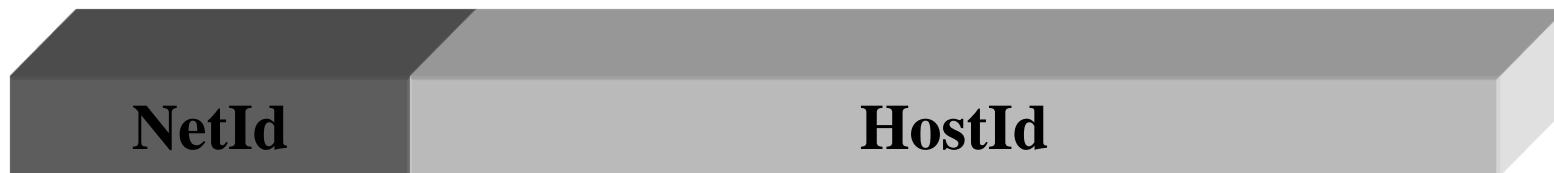
## Endereço IP

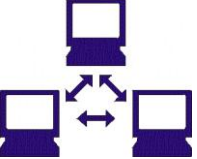
- Proposta:
  - Identifica unicamente uma rede na Internet;
  - Identifica unicamente um host na sua rede;
  - Estrutura hierárquica;
  - Na versão 4 (atual), o protocolo IP possui 32 bits, na versão 6 com 128 bits.



## Classes de Endereços

- Dividimos o endereço IP em:
  - NetId: Identifica a rede dentro de uma classe de endereçamento;
  - HostId: Identifica um host na rede.
- As classes de endereço são pré-definidas.

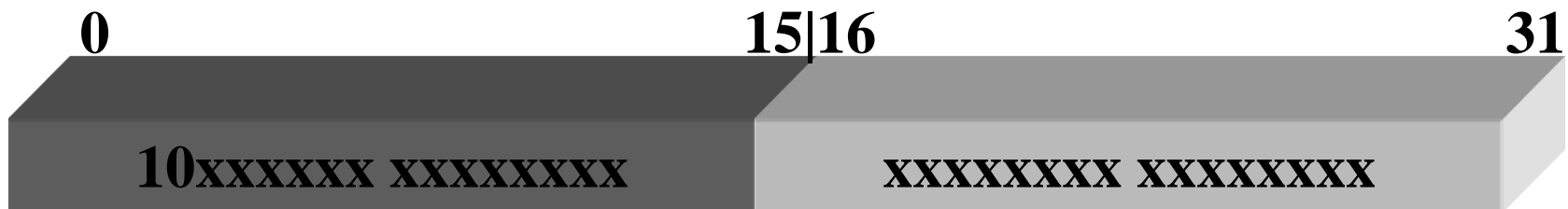




## Classes de Endereços



**CLASSE A**



**CLASSE B**



**CLASSE C**

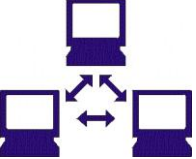


## Classes de Endereços



### CLASSE D

- Multicasting:
  - Formação de um grupo de hosts:
    - Transmissão simultânea para o grupo;
    - Uso do GroupId.
  - Vídeo-Conferência;
  - MBONE.



## Classes de Endereços



### CLASSE E

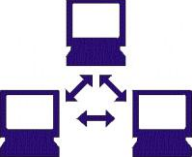
- Reservado para uso futuro





## Classes de Endereços

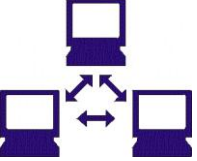
Classe	Redes	Hosts em Cada Rede
A	128	16.777.214
B	16.256	64.534
C	2.097.151.750	254



## Endereços Especiais

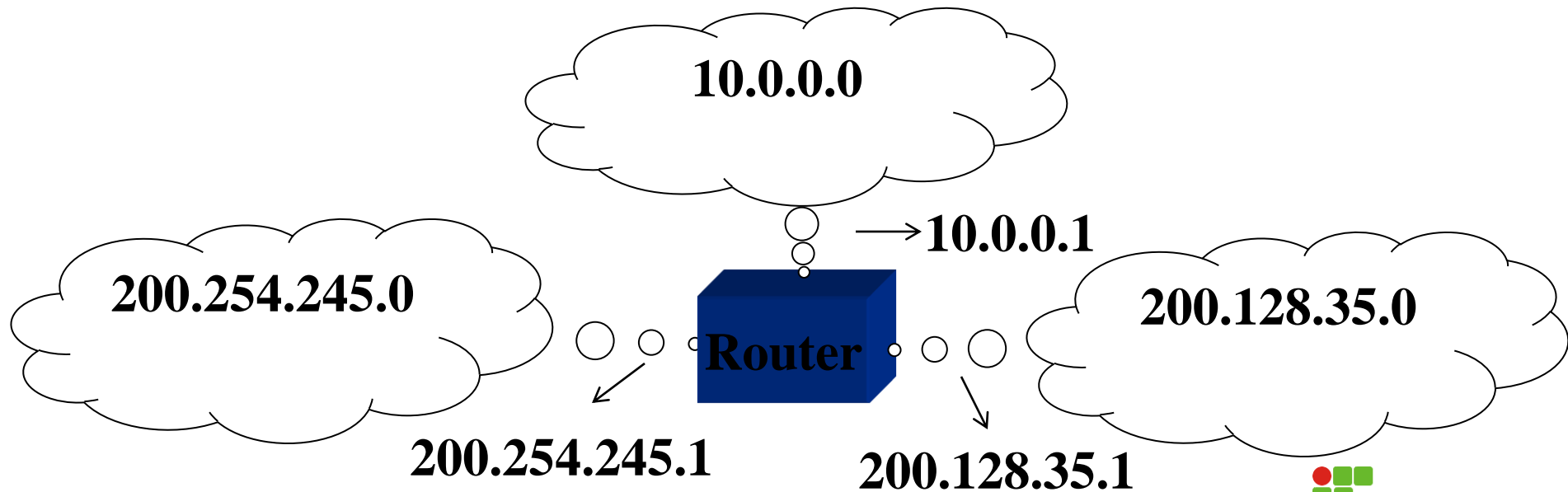
- Endereço da Rede;
- Broadcast Direto;
- Broadcast Limitado;
- Rota Default;
- LoopBack.

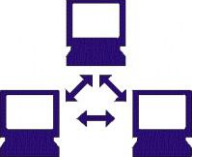
NetId	0 ... 0
NetId	1 ... 1
1 ... 1	1 ... 1
0 ... 0	0 ... 0
127	x ... x



## Interfaces

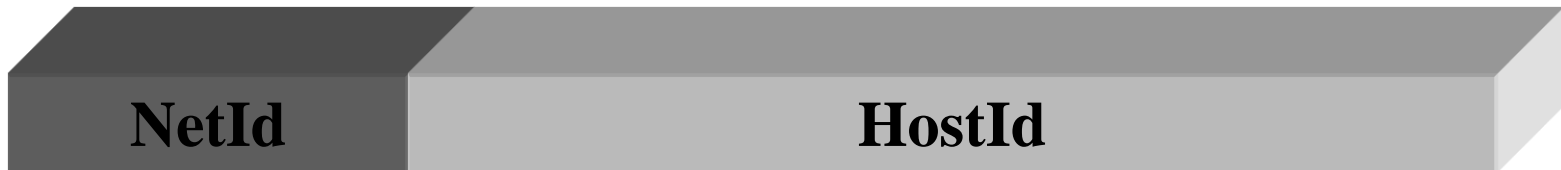
- Endereços IP são atribuídos por interfaces;
- Roteadores possuem diversas interfaces.

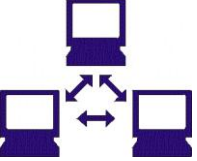




## Sub-Redes

- Subdividir uma rede classe A, B ou C em diversas redes físicas.





## Sub-Redes

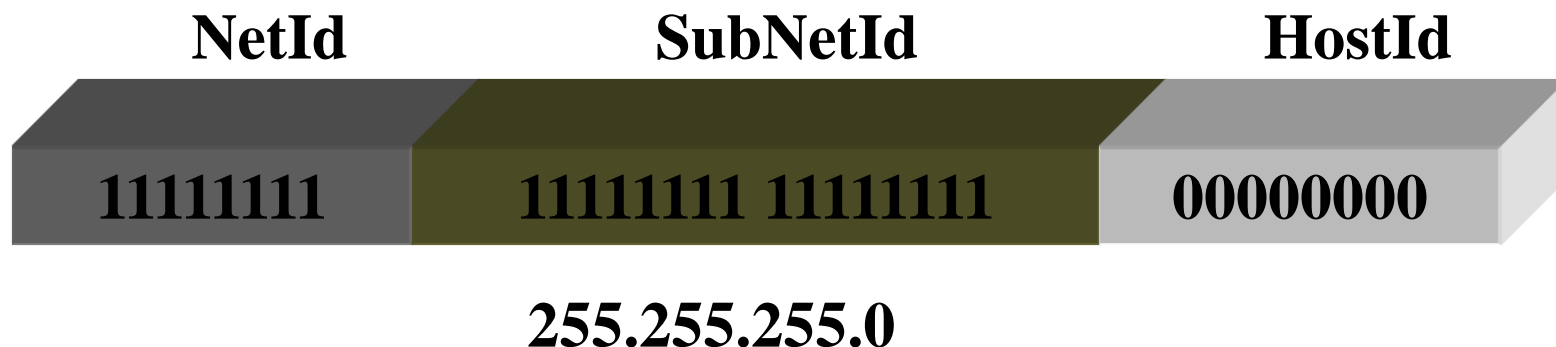
- Dividimos o HostId em:
  - SubNetId: Identifica a rede física;
  - HostId: Identifica um host na rede física.
- Aumenta-se a Hierarquia;
- Permite recursividade do processo.





## Sub-Redes

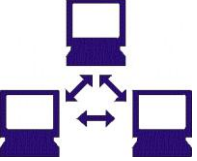
- SubNet Mask:
  - Permite separar o NetId e SubNetId do HostId:
    - Bits em ZERO representam o HostId;
    - Bits em UM representam o NetId+SubNetId.





# CIDR (Classless Inter-Domain Routing)

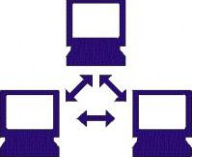
- Ao que se propõe:
  - Usa conceito de sub-rede para criar redes que agrupem blocos contíguos de classes C;
  - Evitar a exaustão de endereços;
  - Usamos uma notação que indica quantos bits do endereço IP formam o bloco CIDR.
    - Ex: 200.128.0.0/16 indica uma rede que possui todas as classes C iniciadas por 200.128.x.x.



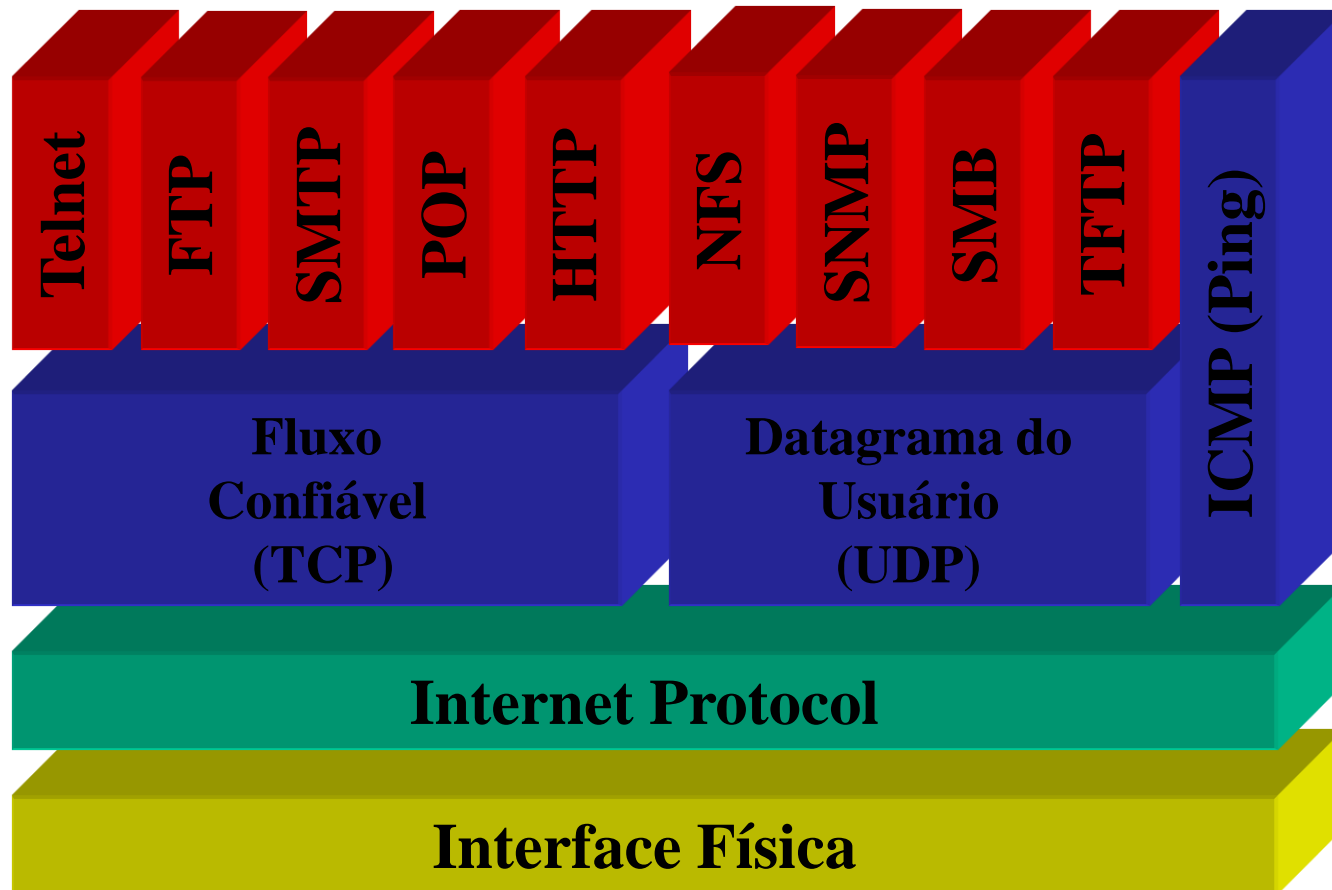
## Protocolos

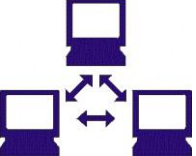
- Conceitos;
- Interação dos protocolos;
- Encapsulamento dos dados.



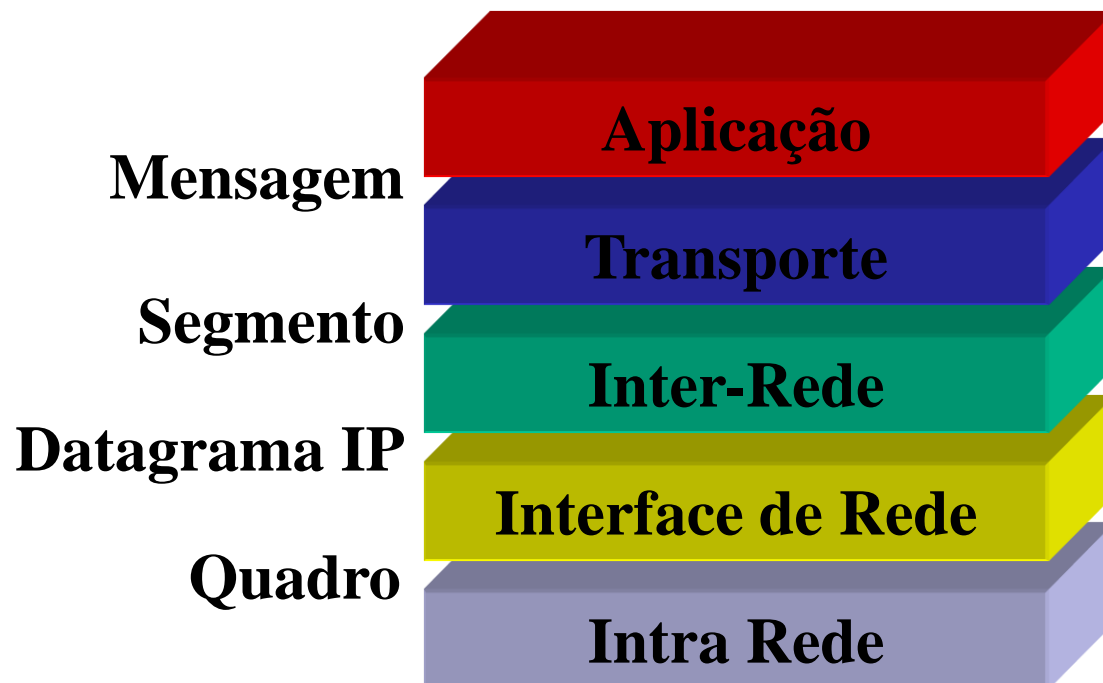


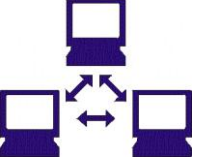
## A Arquitetura TCP/IP





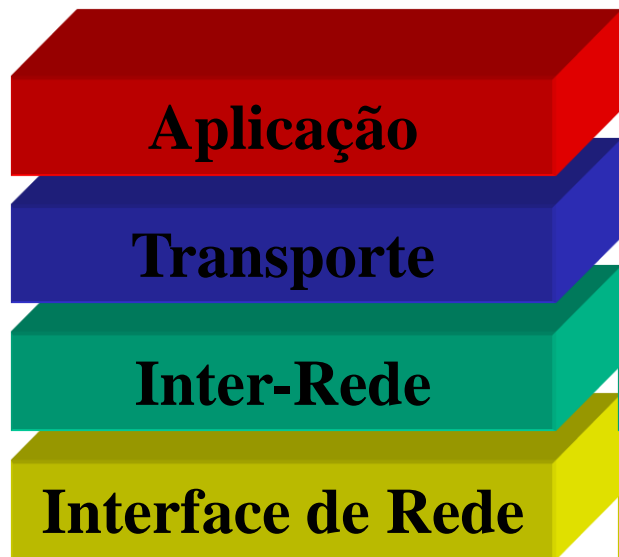
## Níveis Conceituais





## Interação de Camadas

**HOST A**



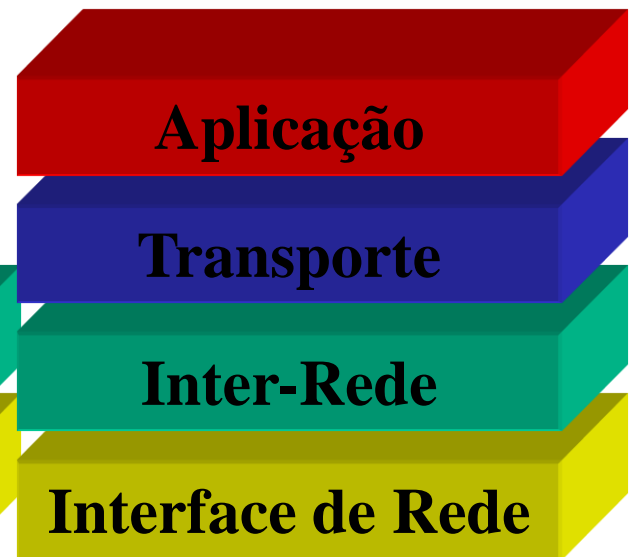
**Rede A**

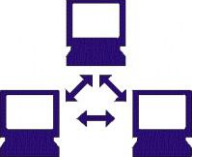
**Roteador**



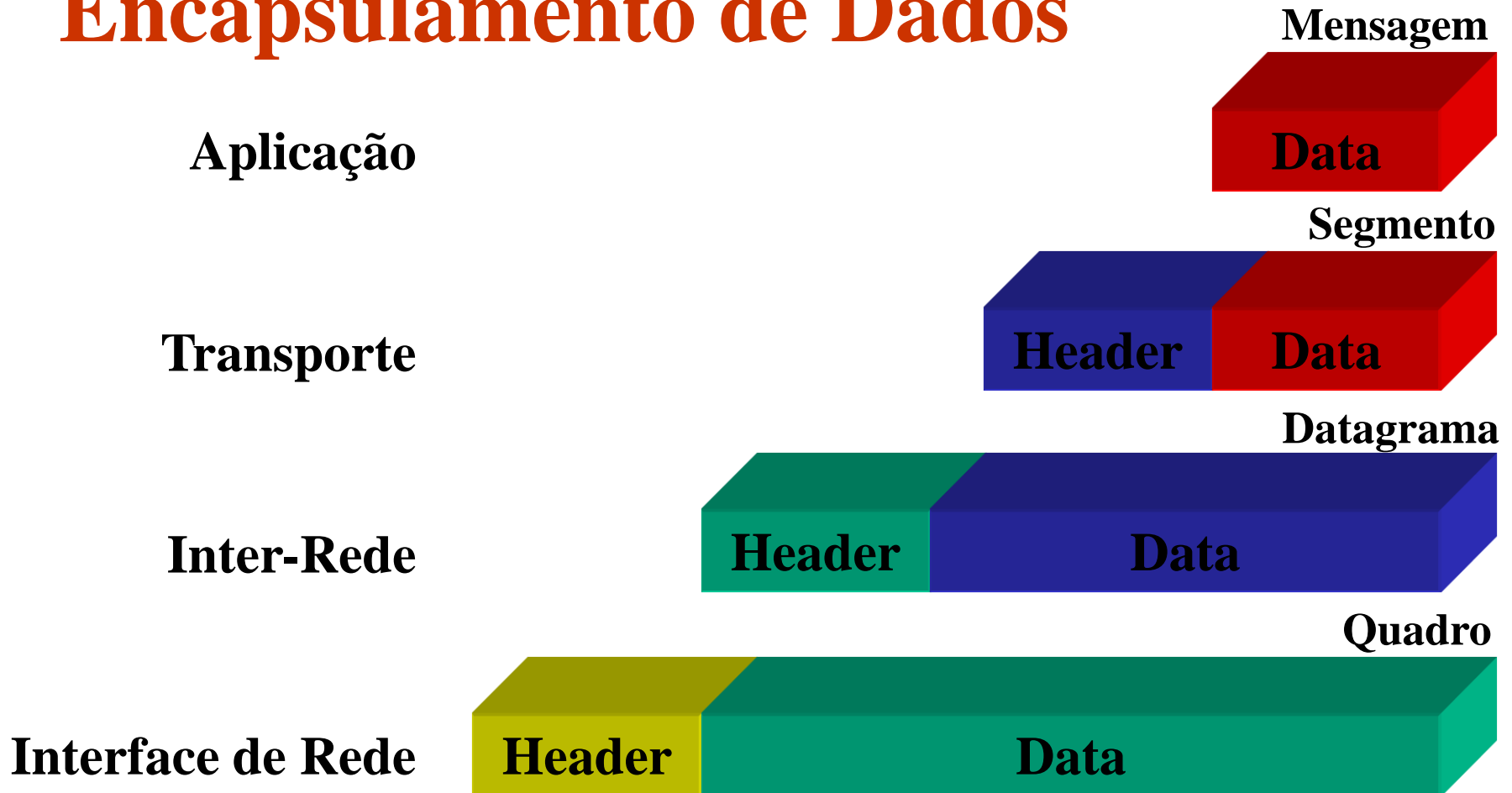
**Rede B**

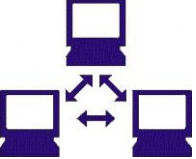
**HOST B**





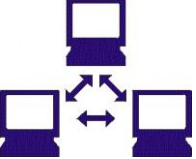
## Encapsulamento de Dados





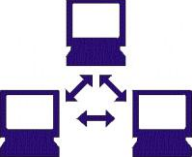
## Interface de Rede

- Características
- Ethernet
- PPP
- ATM
- Mapeamento de Endereços
- ARP
- RARP



## Características

- Tradução de Endereços:
  - Conversão de endereços IP em endereços físicos
- Encapsulamento:
  - Os datagramas IP são transportados em quadros da rede física



## Características

- Transparência:
  - Suporte a diversas tecnologias de rede:
    - Ethernet;
    - Token Ring;
    - FDDI;
    - X-25;
    - Frame Relay;
    - ATM
    - Linhas Seriais.



## Ethernet

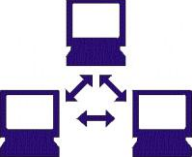
- Endereço Físico:
  - Possui 48 bits;
  - Pacotes de até 1518 bytes (IEEE 802.3);
  - Cada interface tem seu próprio Mac Address.
- Meio compartilhado (Hub):
  - Controle de Colisão;
  - Degradação da performance em 33% (Esqueça QoS).





## Ethernet

- Meio comutado (Switch):
  - Suporte a FULL-DUPLEX:
    - Um par para TX e outro para RX em cada sentido;
    - Dobra velocidade.
  - Back-Plane define capacidade máxima de transmissão entre as portas do Switch;
  - Ainda pode haver colisão entre portas que tentam se comunicar com uma mesma porta simultaneamente.

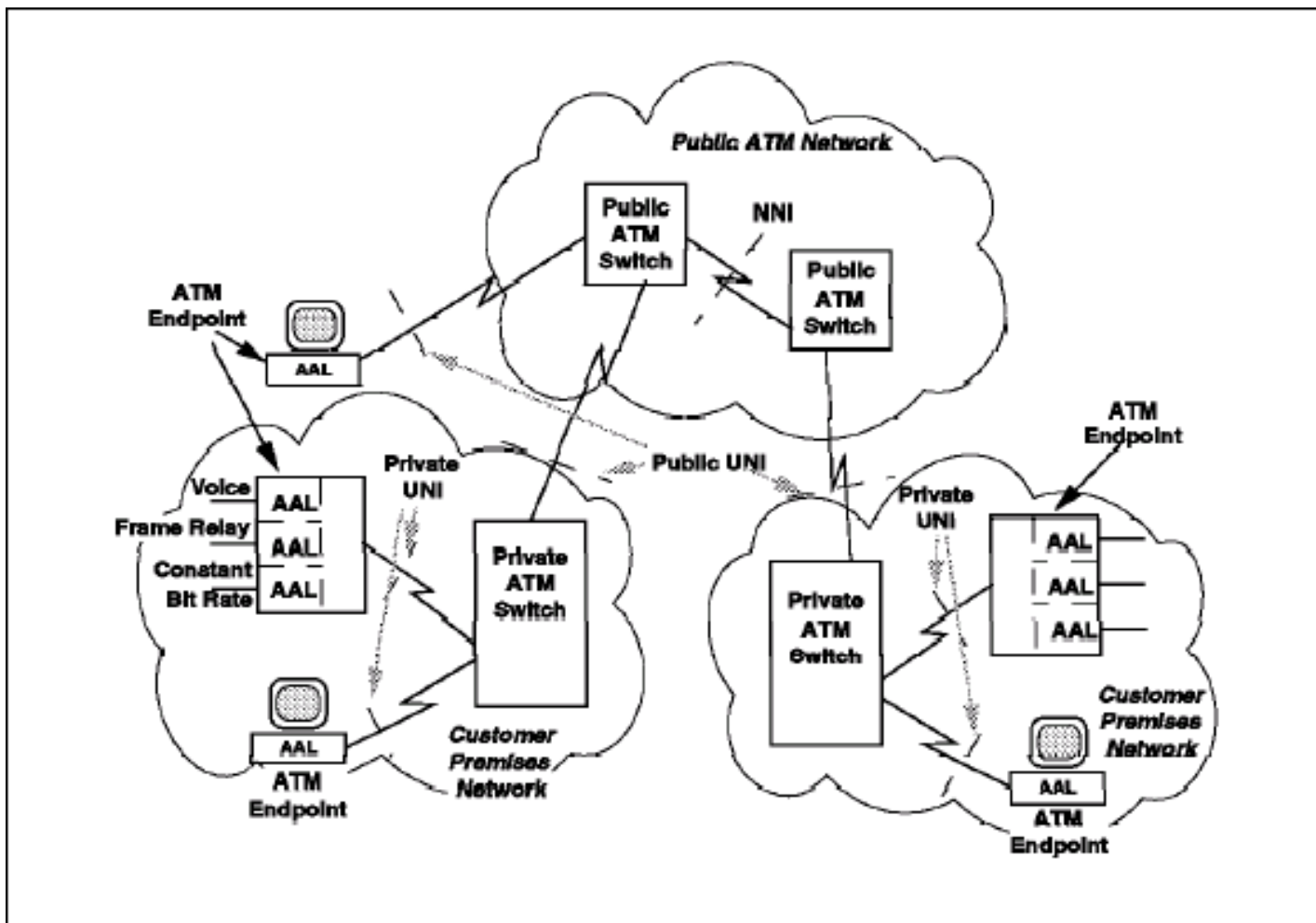


# ATM (Assynchronous Transfer Mode)

- Características:
  - Switching;
  - Suporte a vários tipos de dados;
  - Células de tamanho fixo (53 bytes);
  - Orientado a conexão de ponto a ponto via canais virtuais;
  - Vídeo-conferência;
  - Suporte a Quality of Service (QoS).



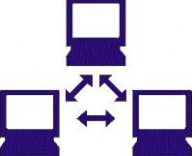
## Rede ATM





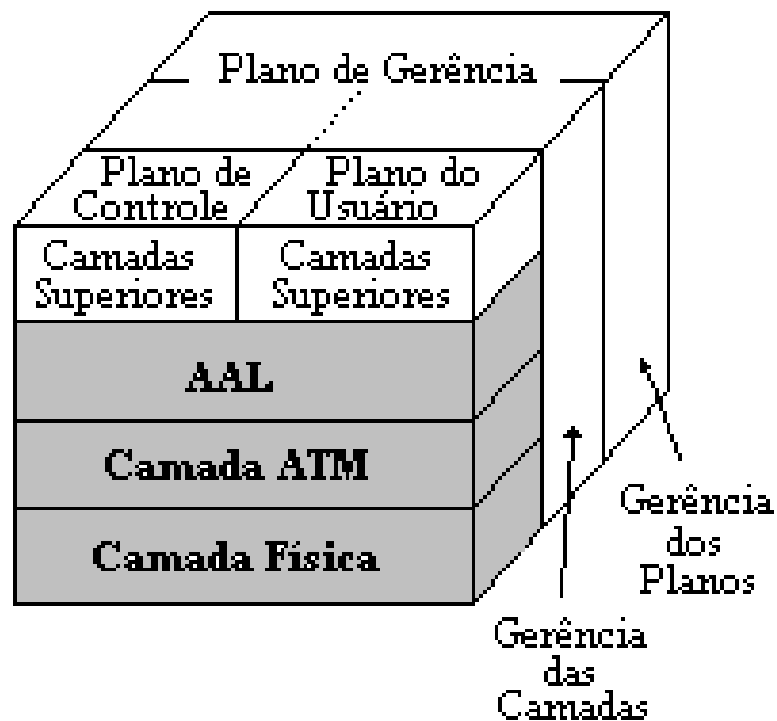
## Rede ATM

- Dispositivos:
  - Private User-Network Interface: Host de uma rede privada conectado ao Switch da rede privada;
  - Public User-Network Interface: Switch de uma rede privada conectado a uma rede pública;
  - Network Node Interface: Conexão entre dois Switches de uma rede.



## Camadas do ATM

### Camadas ATM





## Camadas do ATM

- Camada ATM:
  - Comutação de células;
  - Tratamento do header da célula;
  - Controle genérico de fluxo.
- Camada de Adaptação ATM (AAL):
  - Adapta o ATM aos requisitos da camada superior;
  - Possui tipos definidos para cada serviço.



## AAL (ATM Adaptation Layer)

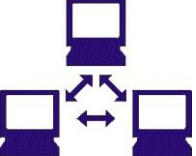
- Adapta diferentes tipos de mídias para transmissão no ATM:
  - AAL0 (Sem tratamento de tipo);
  - AAL1 (Voz e vídeo - Taxa constante - CBR);
  - AAL2 (Voz e Vídeo - Taxa variada - VBR);
  - AAL3 (Dados - Orientado a conexão);
  - AAL4 (Dados - Sem orientação a conexão);
  - AAL5 (Dados - Simplifica AAL3 e AAL4).



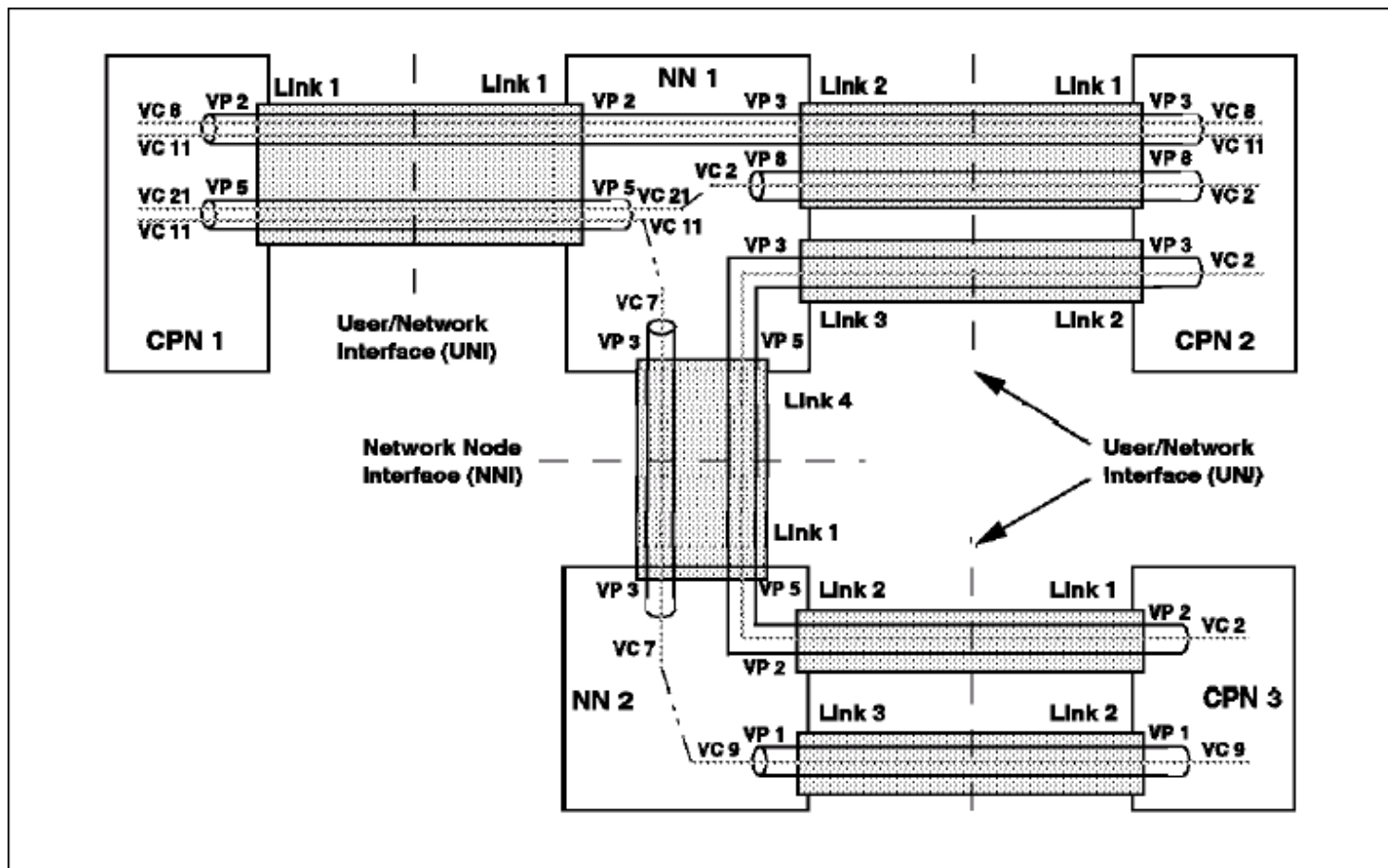
## Camada ATM

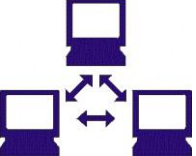
- Endereço ATM de 20 ou 12 Bytes;
- Circuitos virtuais:
  - Links de comunicação entre os Switches;
  - Switches mantêm tables de rotas virtuais para os endereços da rede;
  - Virtual Paths definem a comunicação entre um Host e um Switch ou de um Switch a outro;
  - Virtual Channels são alocados dentro dos VP para cada sessão de comunicação.



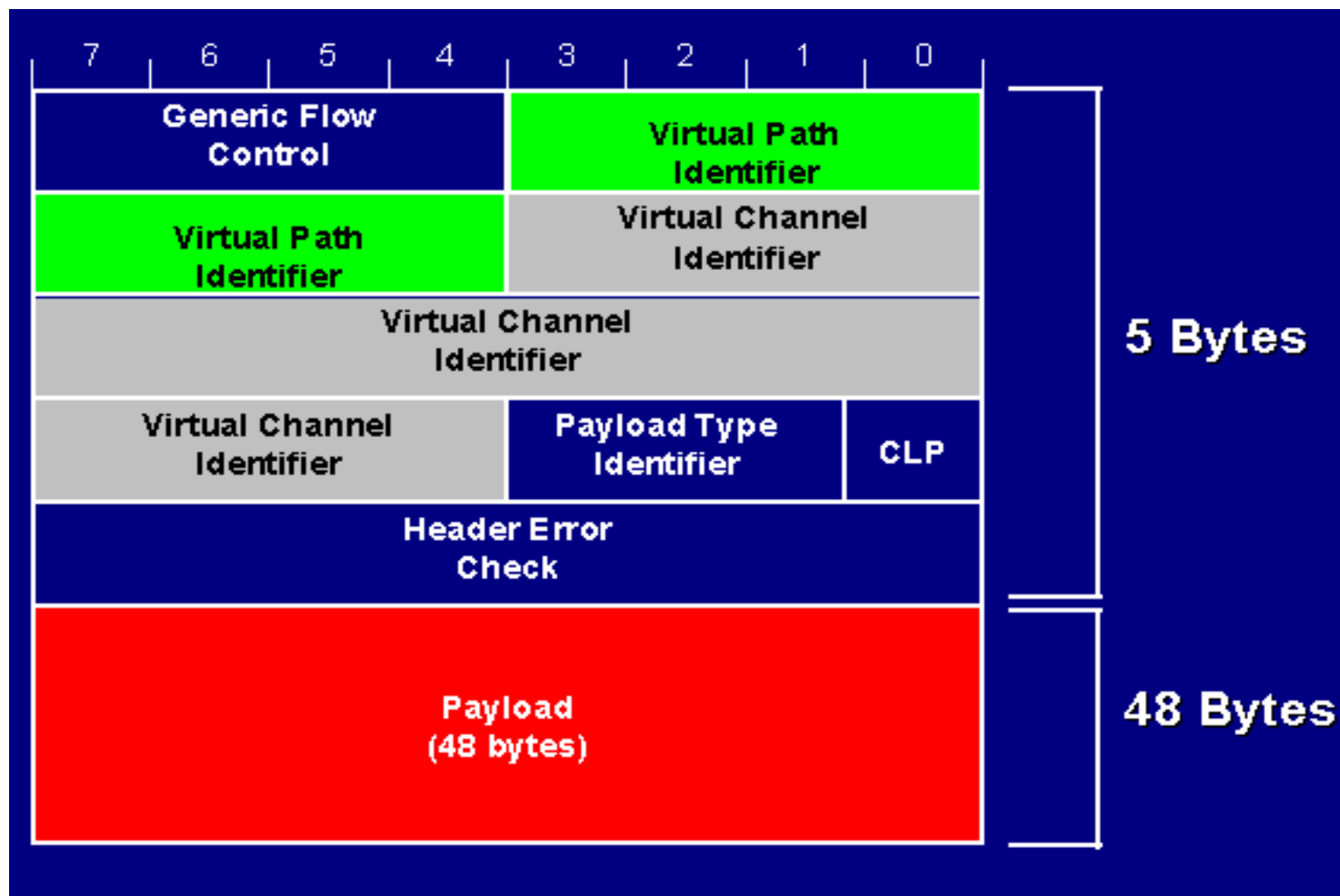


## Comunicação no ATM





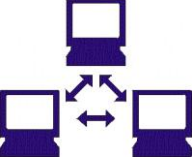
## Célula ATM





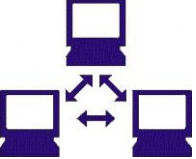
## Célula ATM

- Header (5 Bytes):
  - Virtual Path Identifier: Identifica o path alocado;
  - Virtual Channel Identifier: Identifica o canal alocado;
  - Payload Type Identifier: identifica se a célula passou por congestionamento;
  - Cell Loss Priority: Quando ativo indica que a célula deve ser descartada primeiro num congestionamento;
  - Header Error Check: Check Sum de erro.



## Célula ATM

- Payload (48 Bytes):
  - Dados.
- Células são descartadas no congestionamento;
- Há mecanismos para manutenção da Quality of Service na transmissão das células ATM.



## PPP (Point to Point Protocol)

- Protocolo padrão para transportar datagramas IP sobre conexão serial ponto a ponto.
- Permite utilizar múltiplos protocolos;
- Operação Full-Duplex;
- PPP Síncrono e Assíncrono.



## PPP

- Componentes do PPP:
  - Encapsulamento de datagramas:
    - Uso do HDLC.
  - LCP - Link Control Protocol:
    - Estabelecimento, configuração e teste de conexão a nível de enlace.
  - NCP - Network Control Protocol:
    - Suíte de protocolos para estabelecimento e configuração de protocolos diversos a nível de rede.



## PPP

- Operação:
  - Envio de quadros LCP para configurar e opcionalmente testar o enlace de dados:
    - Inclui mecanismo de negociação de funcionalidades.
  - Envio de quadros NCP para configurar um ou mais protocolos a nível de rede;
  - Envio de datagramas dos diversos protocolos configurados;
  - Liberação do Enlace.



# Mapeamento de Endereços

- Redes físicas tem endereçamento próprio;
- As redes físicas não enxergam o endereçamento IP;
- É necessário um protocolo para:
  - dado um host com um endereço IP, saber seu endereço físico e poder transmitir através da rede física uma mensagem ao mesmo (ARP);
  - realizar o inverso (RARP).





# ARP (Address Resolution Protocol)

- É criada uma tabela com endereços físicos e lógicos em cada host (Cache de Resolução de Endereços);
- Os endereços são obtidos através de envio de mensagens de broadcast para a rede:
  - As mensagens incluem endereços IP e Físico do Host de origem;
  - Os hosts receptores atualizam o seu cache.



## ARP

- Comando arp:
  - Mostra o conteúdo da tabela ARP:

```
C:\> arp -a
```

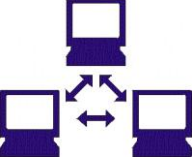
Interface: 10.0.0.4 on Interface 2

Internet Address	Physical Address	Type
10.0.0.3	00-00-21-45-06-b2	dynamic
10.0.0.6	00-10-5a-5c-5d-bf	dynamic
  - Opções:
    - **-a**: mostra todas as entradas;
    - **-d host**: remove uma entrada;
    - **-s host ether\_address**: adiciona uma entrada.



# RARP (Reverse Address Resolution Protocol)

- Utilizado por estações diskless:
  - Obter o endereço IP associado ao endereço físico delas.
- Servidores RARP:
  - Respondem a requisições RARP;
  - Possuem tabela de mapeamentos:
    - /etc/ether
    - /etc/host



## ATM x IP

- Como Suportar IP no ATM?
- ARP não se aplica;
- Duas opções:
  - IP Classical;
  - LAN Emulation.



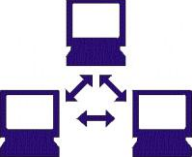
## IP Classical

- Características:
  - Não suporta IP Multicast;
  - Hosts conectados a um mesmo comutador usam conexões ATM Fim-a-Fim com ATMARP e InATMARP (Inverse ATMARP):
    - Servidor de ATMARP.
  - Hosts conectados a comutadores diferentes (diferentes LIS) usam o NHRP (Next Hop Resolution Protocol).



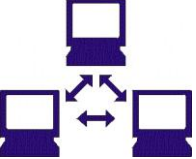
## ATMARP

- Operação:
  - Um Cliente ATMARP solicita resolução de um endereço enviando um endereço IP ao Servidor ATMARP (ARP\_Request);
  - O Servidor consulta a tabela:
    - Se o endereço é encontrado o Endereço ATM é retornado ARP\_REPLAY);
    - Caso Contrário o ARP\_NAK é retornado.



## LANE

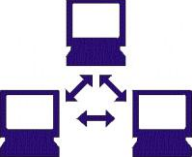
- Características:
  - Aplicações IP rodam na rede ATM sem nenhuma modificação;
  - Simula LANs Ethernet e Token Ring;
  - Combina:
    - Sub-camada ATM-MAC;
    - Resolução de Endereço;
    - Funções Multicast;
    - Interconexão de Redes “herdadas”.



## Nível de Inter-Rede

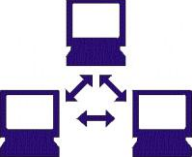
- Características;
- Composição;
- IP;
- ICMP.





## Características

- Datagrama:
  - Unidade básica de transferência de dados;
  - Especifica o formato dos dados na rede.
- Roteamento:
  - Escolha do caminho para o tráfego dos dados.
- Regras:
  - Processamento dos datagramas;
  - Geração de mensagens de erros;
  - Descarte de pacotes.



## Composição

- Internet Protocol (IP):
  - Serviço de entrega de datagramas.
- Internet Control Message Protocol (ICMP):
  - Serviço de informações de controle e erro.
- Internet Group Management Protocol (IGMP):
  - Serviço de entrega multi-ponto (IP Multicast).



## IP (Internet Protocol)

- Serviço de entrega de datagramas;
- Sem conexão;
- Sem reconhecimento;
- Sem garantia de entrega (não confiável):
  - Datagramas podem ser perdidos, duplicados, retardados ou entregues fora da ordem.
- Independência entre datagramas:
  - Trafegam através de caminhos diferentes.



## IP

- Versão atual (IPv4):
  - Unicast, Broadcast e Multicast;
  - 32 bits:
    - Esgotamento de Endereços:
      - Adoção do CIDR (Classless Interdomain Routing);
      - Uso intenso de NAT (Network Address Translator).
- Versão futura (IPv6):
  - Surge o Anycast;
  - 128 bits, QoS etc.



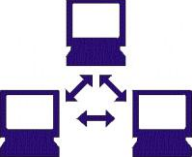
## IP Casting

- Tipos de “Casting”:
  - Unicast: Endereça dados a um host específico;
  - Broadcast: Endereça dados a todos os hosts da sub-rede;
  - Multicast: Endereça dados a todos os hosts que formam um grupo de IP Multicast;
  - Anycast: Endereça dados a qualquer host de um grupo de IP Anycast (IPv6 ou superior)



## IPv4

0	4	8	16	19	24	31
VERS	HLEN	SERVICE TYPE	TOTAL LENGTH			
IDENTIFICATION			FLAGS	FRAGMENT OFFSET		
TIME TO LIVE		PROTOCOL	HEADER CHECKSUM			
SOURCE IP ADDRESS						
DESTINATION IP ADDRESS						
IP OPTIONS (IF ANY)					PADDING	
DATA						



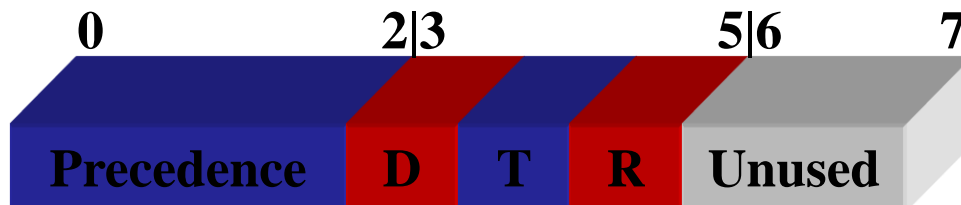
## IPv4

- Campos:
  - Vers:
    - Versão do IP (atual 4).
  - Hlen:
    - Tamanho do cabeçalho;
    - Unidade: 4 octetos.
  - Total Length:
    - Tamanho do datagrama (máximo de 64K octetos);
    - Unidade: 1 octeto.

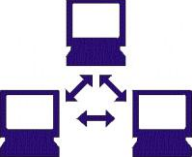


## IPv4

- Campos:
  - Service Type:
    - Define a qualidade do serviço (sem garantia do mesmo);
    - Auxilia no roteamento:
      - **Precedence**: origem do pacote (ex: normal, controle etc.);
      - **D**: Baixo retardo;
      - **T**: Alto throughput;
      - **R**: Alta confiabilidade.

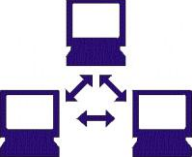






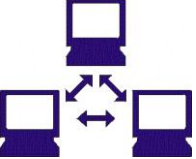
## IPv4

- Campos:
  - Identification:
    - Identificador do datagrama;
    - Único para cada datagrama.
  - Time to Live:
    - Tempo de vida máximo do datagrama;
    - Decrementado a cada roteador intermediário:
      - Descarta o datagrama e acusa erro quando o TTL chega a 0 (ZERO).



## IPv4

- Campos:
  - Protocol:
    - Especifica o protocolo do nível superior (ex: UDP, TCP).
  - Header CheckSum:
    - Controle de erro.
  - Source IP Address e Destination IP Address:
    - Indicam endereço IP de origem e de destino da mensagem, respectivamente.

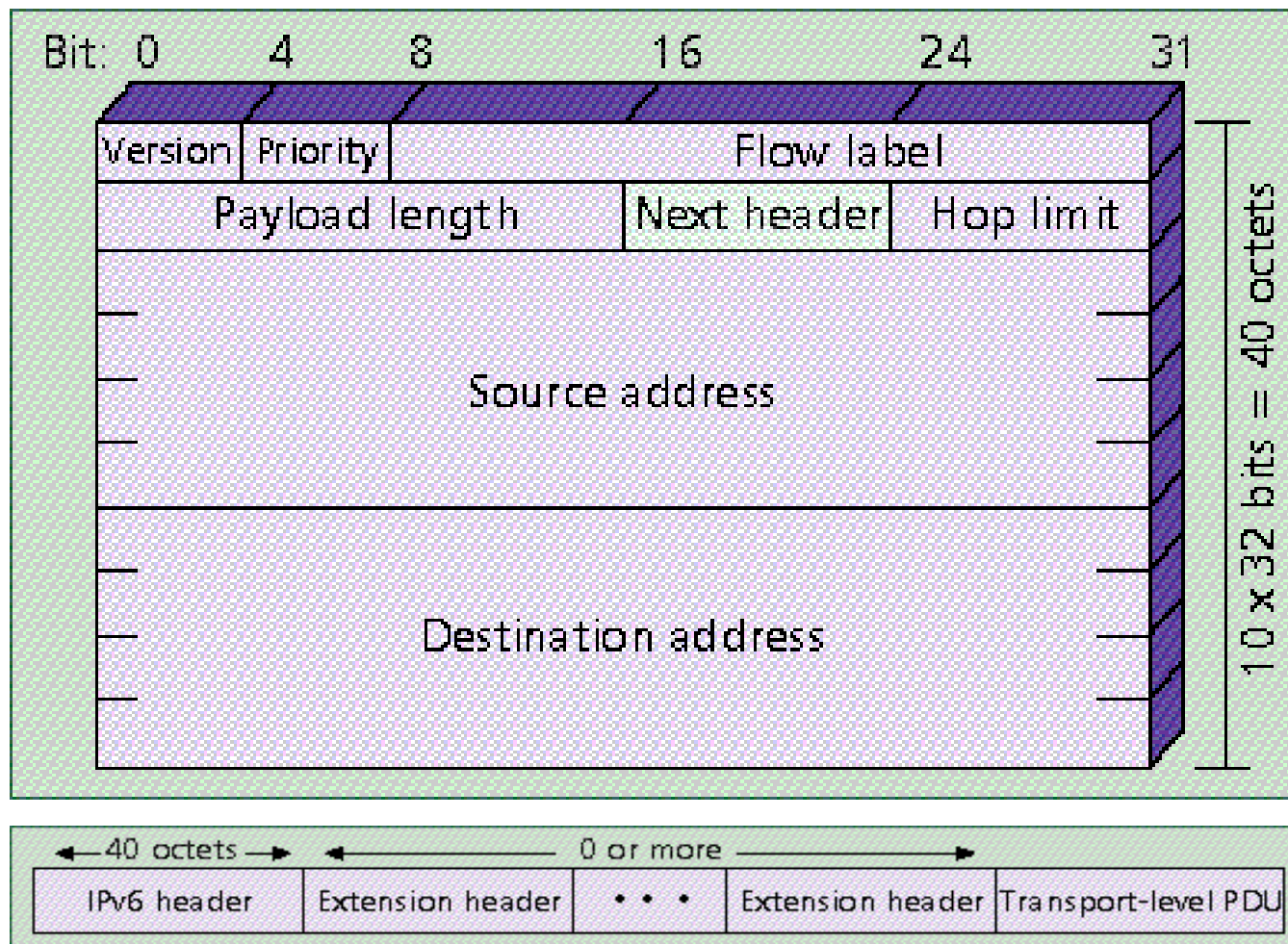


## IPv4

- Campos:
  - IP Options e Padding:
    - Opções relativas a pacotes fragmentados, debugging e testes.
  - Data:
    - Dados a serem transportados.



## IPv6





## IPv6

- Campos:
  - Version:
    - Versão do protocolo (versão 6).
  - Priority e Flow Control:
    - Permitem assinalar pacotes que devem ter tratamento especial;
    - Quality of Service.
  - Payload Length:
    - Tamanho do pacote em octetos (máximo 64K).



## IPv6

- Campos:
  - Next Header:
    - Indica o protocolo superior usado.
  - Hop Limit:
    - Número máximo de hosts por onde o pacote pode trafegar, ao atingir 0 o pacote é descartado.
  - Source Address e Destination Address:
    - Endereços IP de origem e destino da mensagem, respectivamente.



## Atribuindo endereços IP

- Configuração Estática:
  - Máquina a máquina;
  - Lista de endereços por host.
- Configuração Dinâmica:
  - Servidor de configuração:
    - BOOTP;
    - DHCP.
  - Configuração Stateless (IPv6).

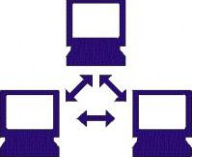


## IP

- Encapsulamento do Datagrama:
  - Idealmente um datagrama preenche um quadro físico;
  - MTU (Maximum Transfer Unit):
    - Ethernet: 1500
    - FDDI: 4470

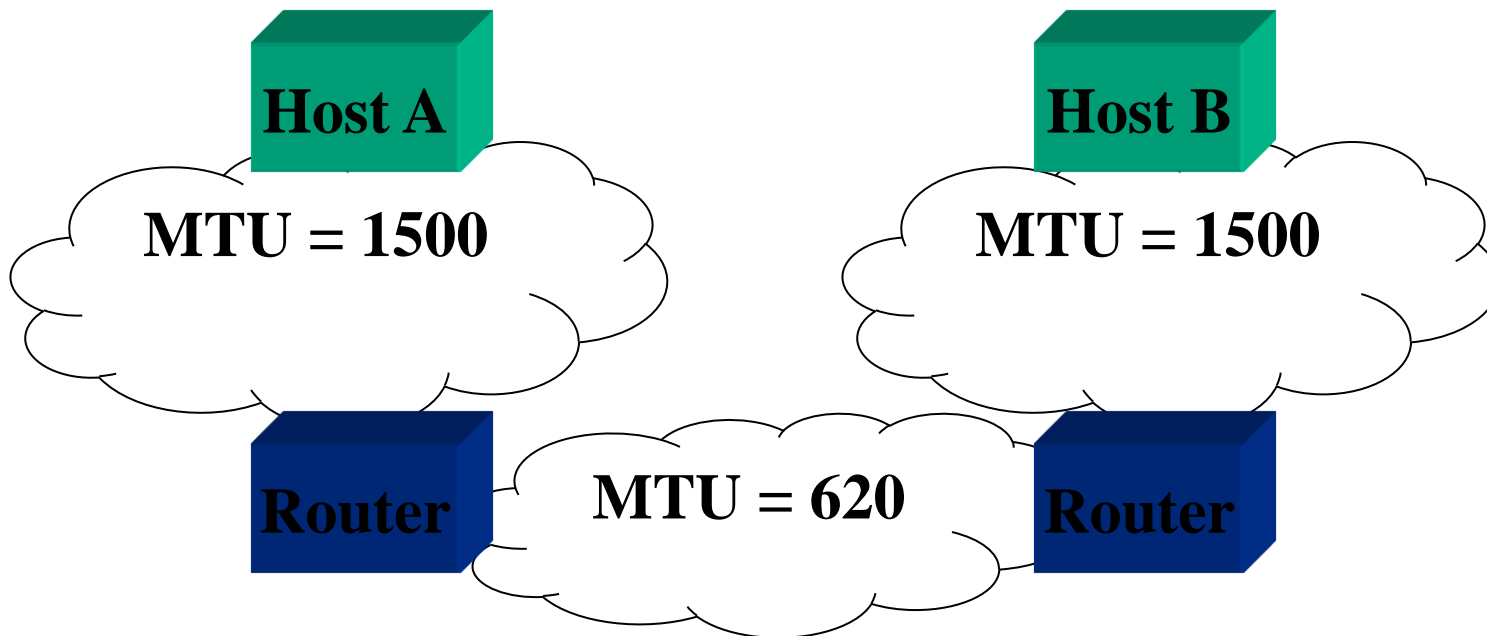






## IP

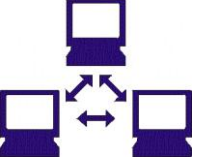
- Qual deve ser o tamanho do datagrama de A para B?





## IP

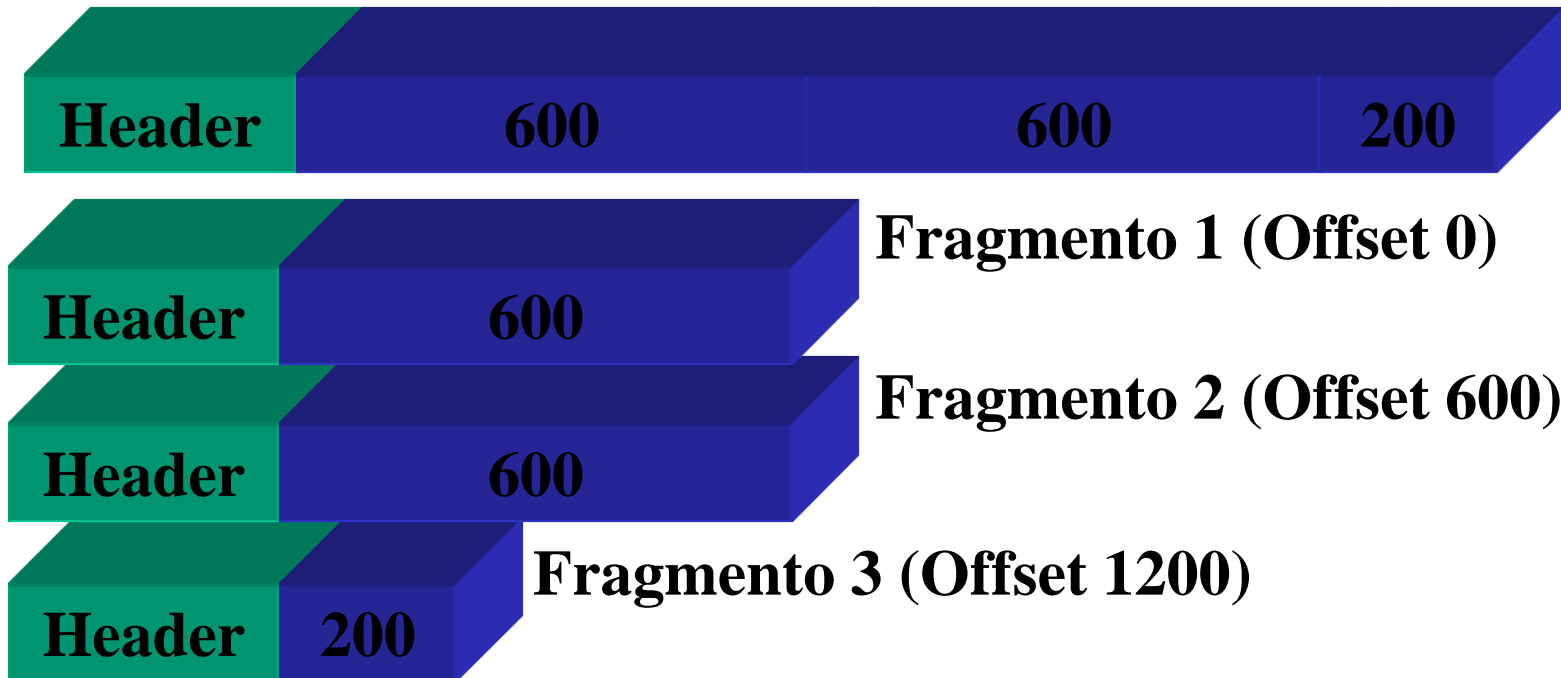
- Fragmentação:
  - Mecanismo de divisão do datagrama original em pequenos fragmentos;
  - Ocorre sempre que o datagrama atravessar uma rede com MTU menor que o tamanho do datagrama.



## IP

- Fragmentação:

### Datagrama





## IP

- Controle da Fragmentação:
  - Identification:
    - Copiado do datagrama original.
  - Fragment Offset:
    - Posição do fragmento no datagrama original;
    - Unidade: 8 octetos.



## IP

- Controle de Fragmentação:
  - Total Length:
    - Tamanho do fragmento.
  - Flags:
    - **don't fragment:** habilita fragmentação com 0 (ZERO);
    - **more fragments:** indica o fim do datagrama original com 0 (ZERO).



## IP

- Processamento de Datagramas no Roteador:
  - Recebe datagrama:
    - Se memória insuficiente, descarta o datagrama.
  - Calcula o checksum:
    - Se diferente do dado no datagrama, descarta.
  - Decrementa o TTL:
    - Se zero, descarta o datagrama e gera erro.
  - Aplica algoritmo de roteamento:
    - Pode ser necessário usar fragmentação;
    - Trata os campos Service Type e IP Options.



## IP

- Processamento de Datagramas no Destino:
  - Recebe datagrama:
    - Se memória insuficiente, descarta o datagrama.
  - Calcula o checksum:
    - Se diferente do dado no datagrama, descarta.
  - Se fragmento de datagrama:
    - Inicializa temporizador;
    - Remonta o datagrama original.
  - Entrega o datagrama ao protocolo indicado no campo protocol.



# ICMP (Internet Control Message Protocol)

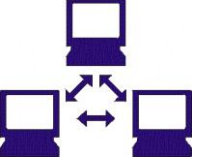
- Objetivos:
  - Permitir gateways e hosts trocarem mensagens de erro e de controle;
  - Realizar a comunicação entre IPs em gateways e hosts.





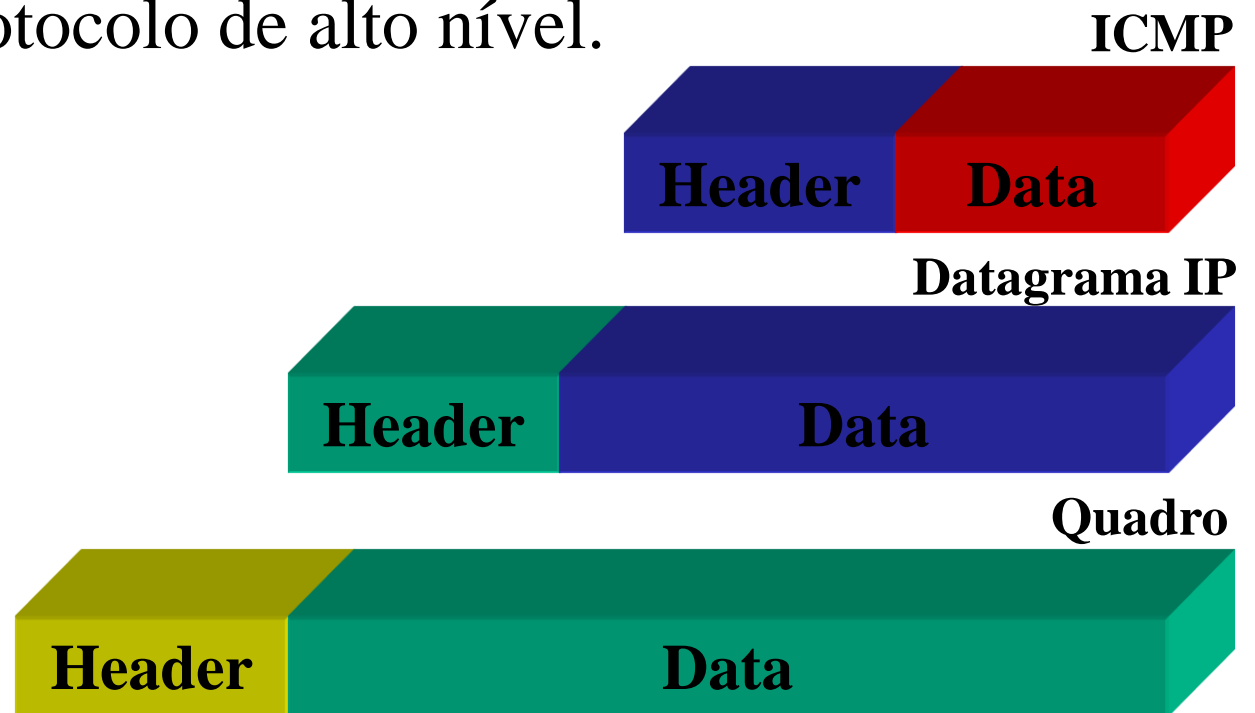
## ICMP

- Funções:
  - Controle de fluxo;
  - Notificação de erros;
  - Redirecionamento de rotas;
  - Requisição de Informações.



## ICMP

- Encapsulamento:
  - Não é protocolo de alto nível.





## ICMP

<b>Código</b>	<b>ICMP Message Type</b>
<b>0</b>	<b>Echo Reply</b>
<b>3</b>	<b>Destination Unreachable</b>
<b>4</b>	<b>Source Quench</b>
<b>5</b>	<b>Redirect</b>
<b>8</b>	<b>Echo request</b>
<b>11</b>	<b>Time exceeded for a Datagram</b>
<b>12</b>	<b>Parameter problem on a Datagram</b>
<b>13/14</b>	<b>Timestamp Request/Reply</b>
<b>17/18</b>	<b>Address Mark Request/Reply</b>



## ICMP

- Echo Request/Echo Reply:
  - Testa a comunicação entre dois sistemas.

```
genio:~$ ping www.cefet.br
```

```
PING kardec.cefetba.br (200.254.245.1): 56 data bytes
```

```
64 bytes from 200.254.245.1: icmp_seq= 0 ttl= 128 time= 0.7 ms
```

```
64 bytes from 200.254.245.1: icmp_seq= 1 ttl= 128 time= 0.4 ms
```

```
64 bytes from 200.254.245.1: icmp_seq= 2 ttl= 128 time= 0.4 ms
```

```
64 bytes from 200.254.245.1: icmp_seq= 3 ttl= 128 time= 0.4 ms
```

```
--- kardec.cefetba.br ping statistics ---
```

```
4 packets transmitted, 4 packets received, 0% packet loss
```

```
round-trip min/avg/max = 0.4/0.4/0.7 ms
```



## ICMP

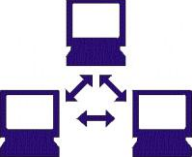
- Destination Unreachable:
  - Não é possível entregar datagrama ao destino.

Código	Tipo
0	Network Unreachable
1	Host Unreachable
2	Protocol Unreachable
3	Port Unreachable
6/7	Destination Host-Network Unknown



## ICMP

- Source Quench:
  - Controle de congestionamento na recepção.
- Redirect:
  - Notificar rota mais adequada para o destino.
- Time Exceeded:
  - Gateway detecta que o TTL do datagrama expirou;
  - Ocorreu Timeout na espera por fragmentos do datagrama.



## Nível de Transporte

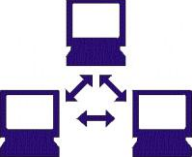
- Características;
- Portas;
- Protocolos;
- UDP;
- TCP.



## Características

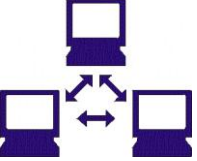
- Comunicação fim-a-fim entre aplicações;
- Controle de fluxo;
- Serviço Confiável:
  - Controle de erro;
  - Controle de sequência.
- Divisão de mensagens em segmentos;
- Mecanismos de identificação de processos.



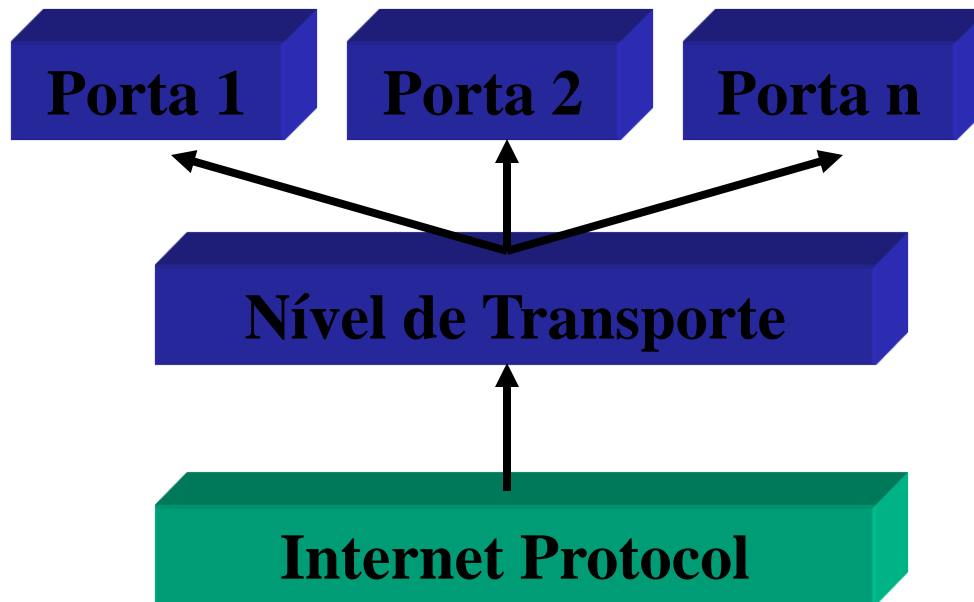


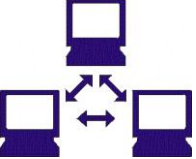
## Portas

- Identificam os processos origem e destino;
- Viabilizam a comunicação fim-a-fim;
- Sistema operacional oferece interface para especificar e acessar as portas;
- Permite envio e recepção de datagramas de forma independente;
- Utilizam buffers de transmissão e recepção.



## Portas





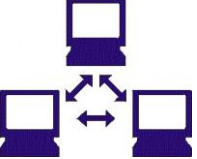
## Protocolos

- UDP (User Datagram Protocol):
  - Serviço sem conexão;
  - Baixo overhead;
  - Não confiável;
  - Detecção de erro;
  - Sem controle de sequência.
- TCP: (Transport Control Protocol):
  - Serviço orientado a conexão;
  - Confiável;
  - Detecção de erro.



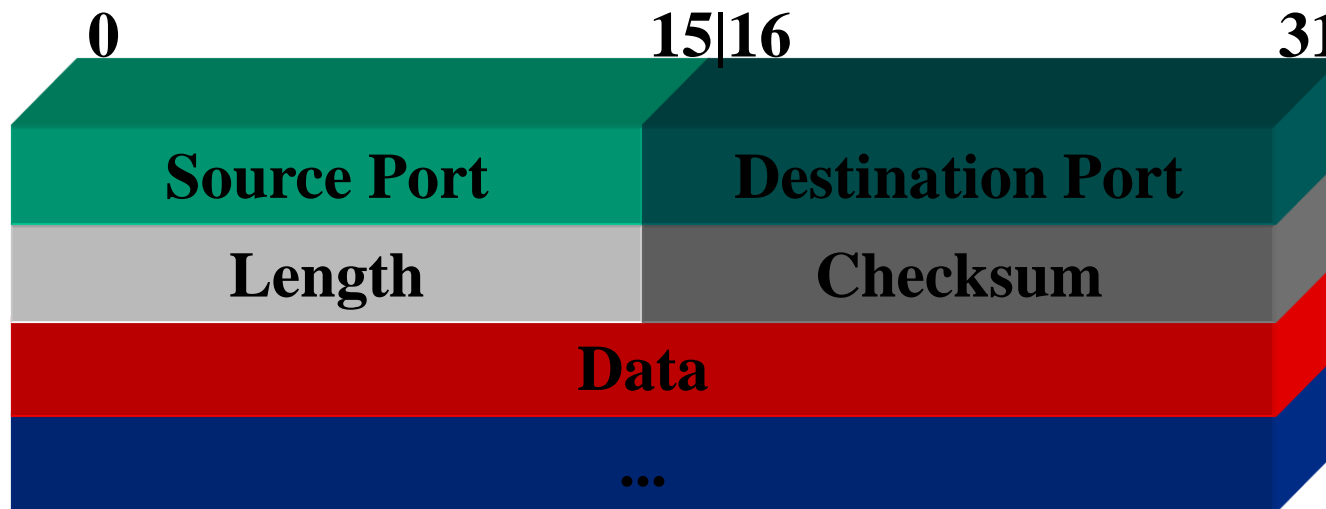
# UDP (User Datagram Protocol)

- Por que UDP?
  - Para aplicações que implementam mecanismo de entrega confiável;
  - Pequena quantidade de dados a transmitir;
  - Aplicações tipo query/response;
  - Serviços em que pequenas porções de informações podem ser perdidas.



## UDP

- Formato do Datagrama:





## UDP

- Campos:
  - Source Port e Destination Port:
    - Portas usadas pelo processo;
    - Source Port é opcional.
  - Length:
    - tamanho do datagrama (em octetos).
  - Checksum:
    - Verificação de erro no datagrama (opcional).
  - Data:
    - Dados do usuário.



## TCP (Transport Control Protocol)

- Características:
  - Baseado em fluxo de dados (Stream):
    - Seqüência de bytes não estruturada.
  - Conexão com circuito virtual:
    - Estabelecimento/Encerramento de conexões;
    - Transferência de dados;
    - Full-Duplex.
  - Buffers:
    - Controle automático de envio;
    - Mecanismo push.



## TCP

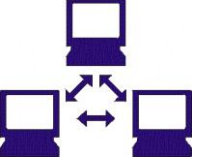
- Segmentos:
  - TCP manipula o stream de dados como uma seqüência de octetos divididos em segmentos;
  - Cada segmento é encapsulado em um datagrama IP.
- Número de seqüência:
  - Octetos no stream de dados são numerados em seqüência.



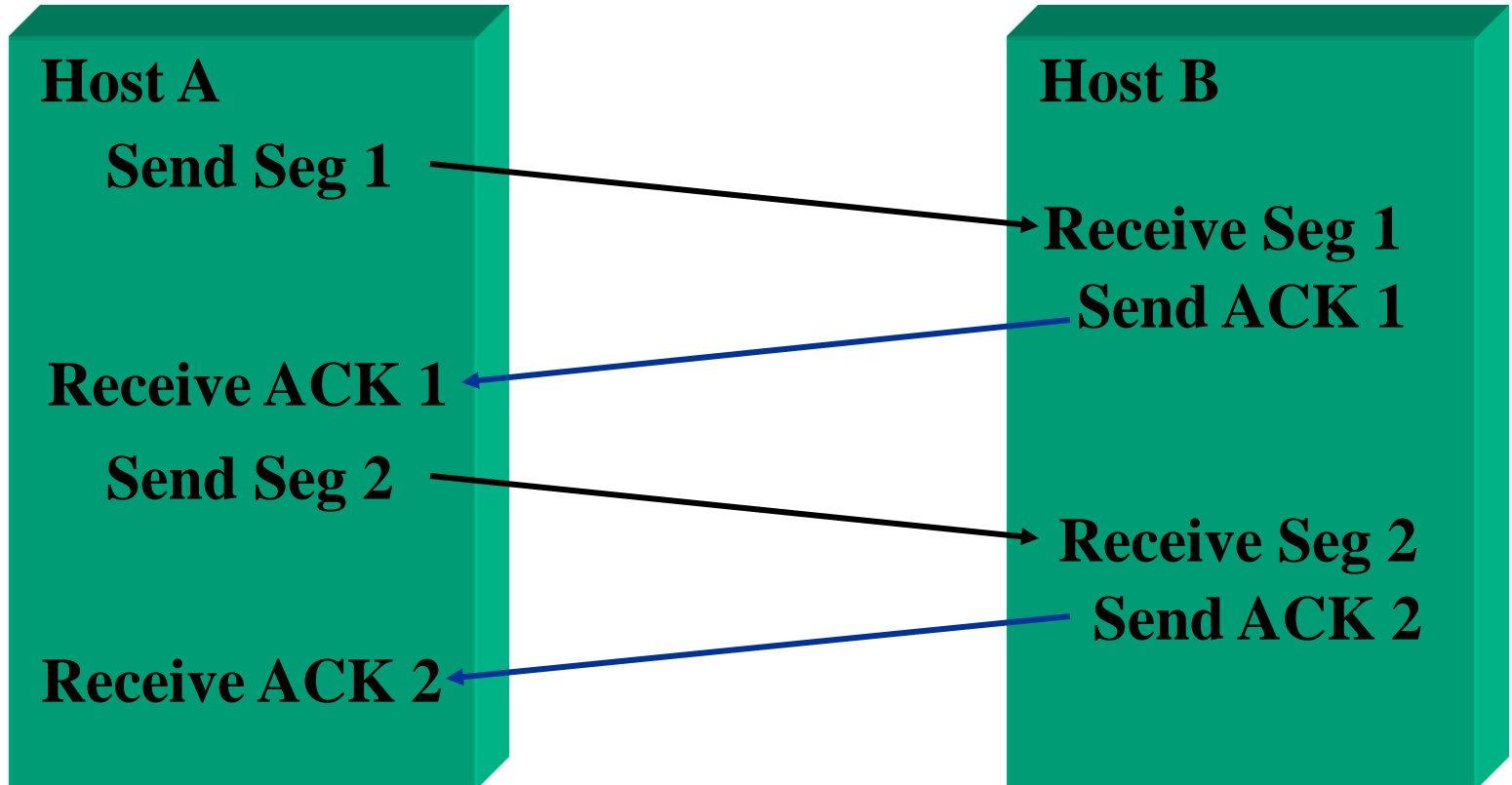


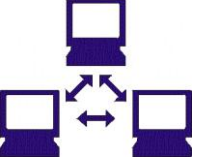
## TCP

- Confiabilidade:
  - Reconhecimento positivo com retransmissão;
  - Utiliza Piggybacking no reconhecimento:
    - Reconhecimento imediato com leve mudança na velocidade do fluxo de modo imperceptível ao usuário, de modo a manter comportamento constante.
  - Retransmissão baseada em Timeout.

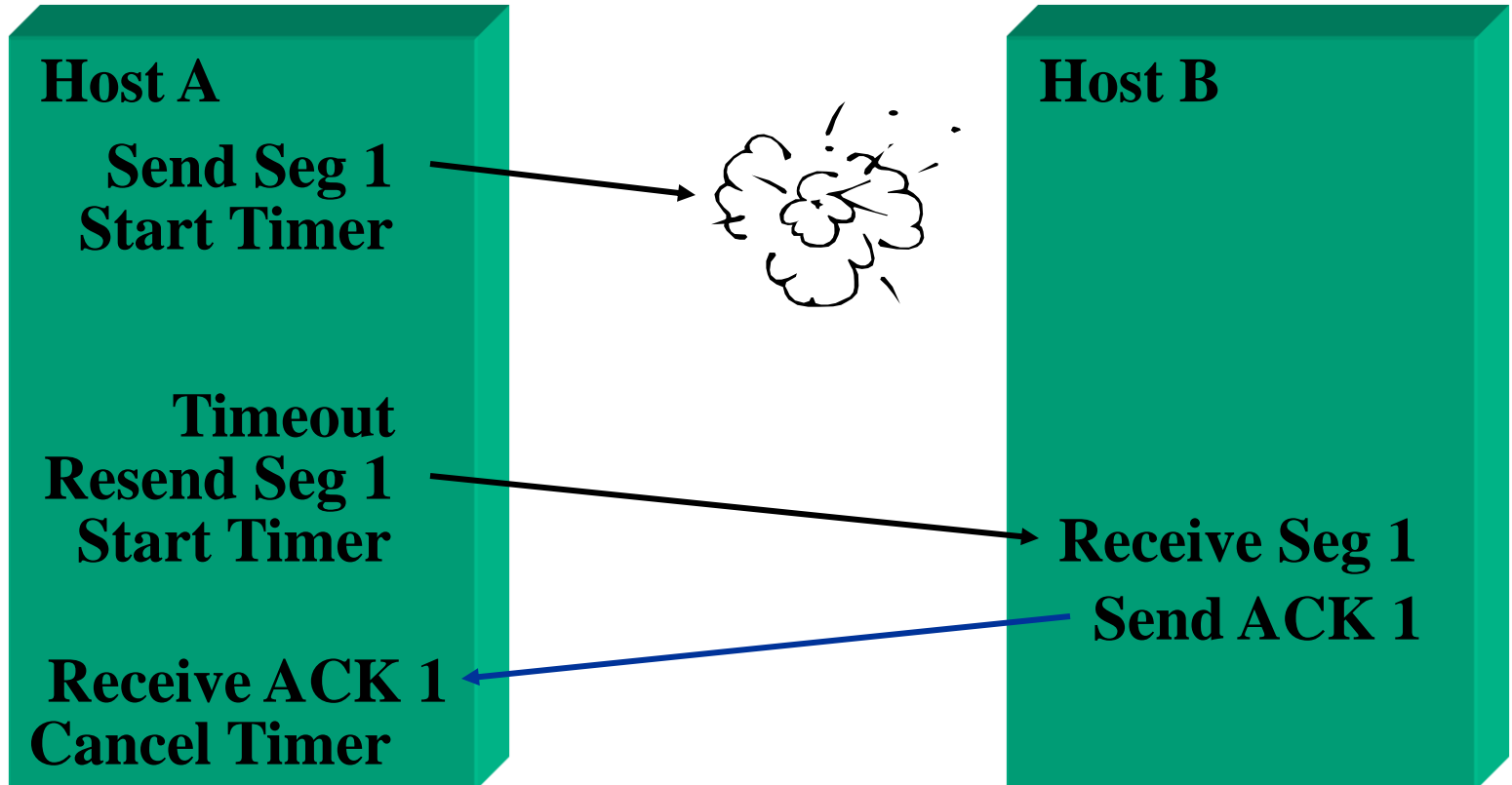


## TCP





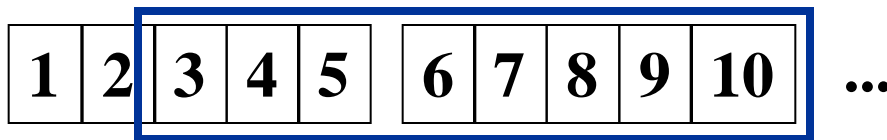
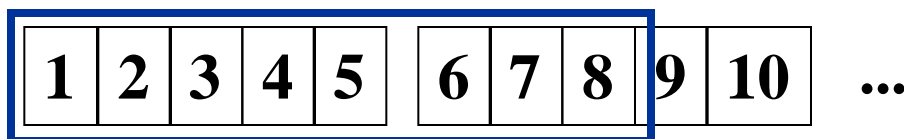
## TCP

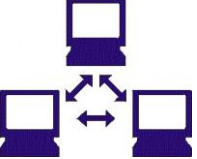




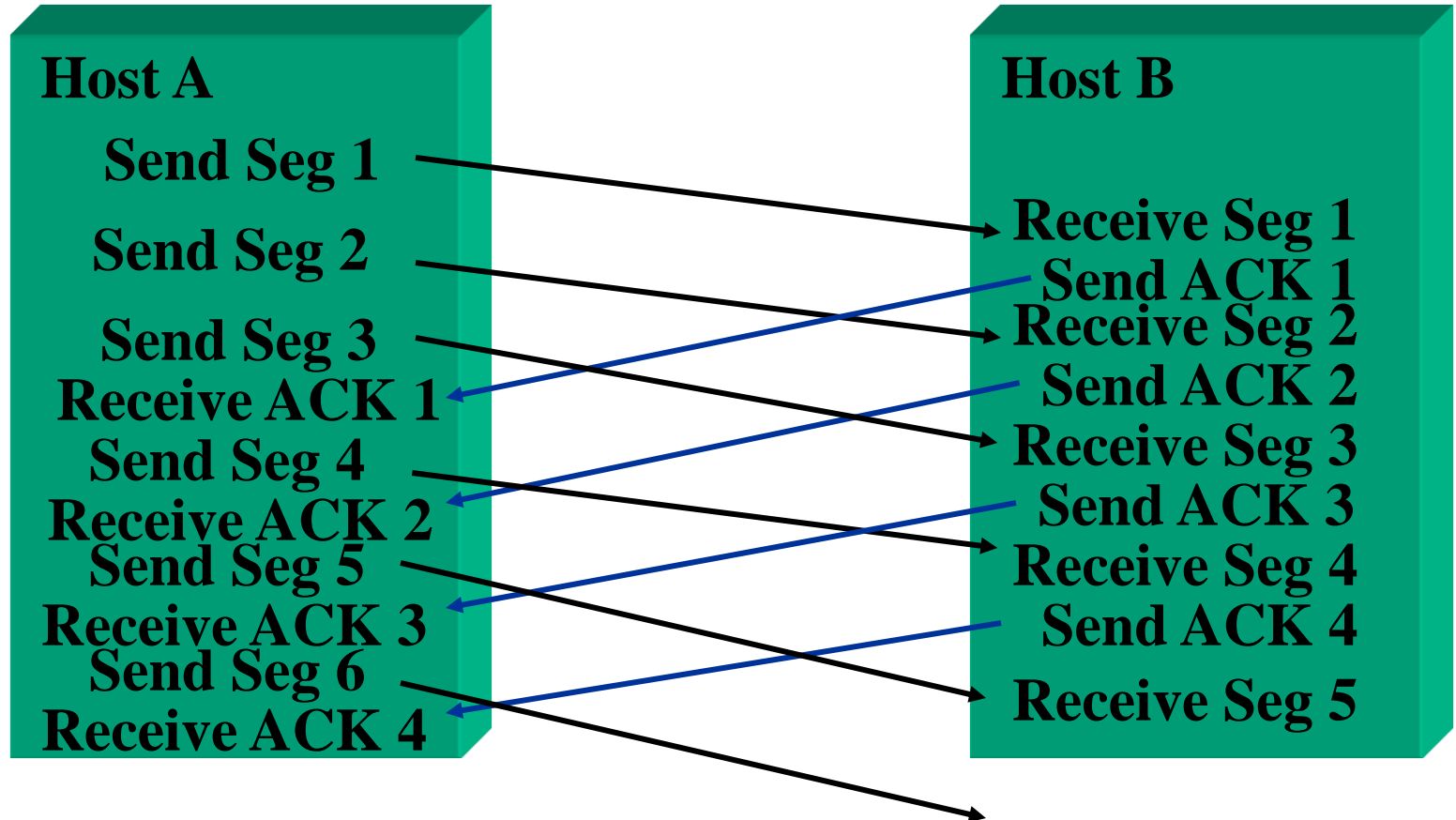
## TCP

- Sliding Window (Janela Flutuante):
  - Permite o transmissor enviar múltiplos segmentos antes de receber o reconhecimento;
  - Eficiência de transmissão e controle de fluxo.





## TCP





## TCP

Source Port		Destination Port	
Sequence number			
Acknowledgement Number			
Offset	Reserved	Flags	Windows
Checksum		Urgent Pointer	
Options			Padding
Início dos dados			



## TCP

- Campos:
  - Source Port e Destination Port:
    - Identificam os processos origem e destino da conexão.
  - Sequence Number:
    - Posição do segmento dentro do fluxo de dados.
  - Acknowledgment Number:
    - Número do próximo octeto que o destino espera receber.
  - Offset:
    - Indica o início da área de dados do segmento.



## TCP

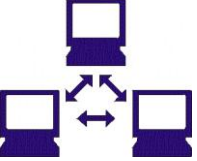
- Campos:
  - Flags:
    - URG: Campo Urgent Pointer válido;
    - ACK: Campo Ack Number válido;
    - PSH: Segmento requer um push;
    - RST: Reseta a conexão;
    - SYN: Sincronizar números de sequência;
    - FIN: Origem finalizou stream de bytes.





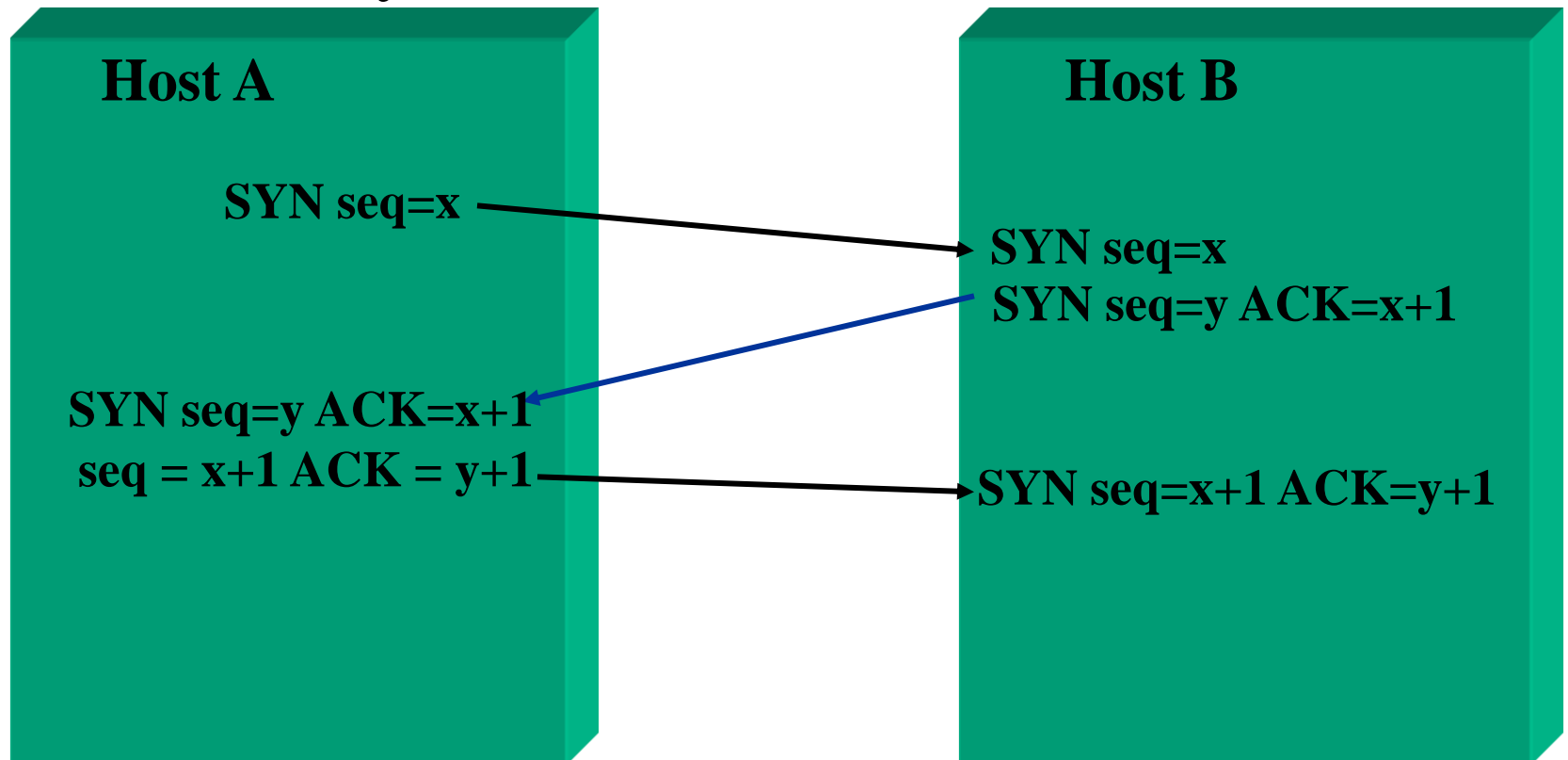
## TCP

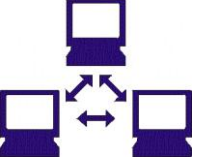
- Campos:
  - Window:
    - Especifica o tamanho da janela.
  - Checksum:
    - Verificação de erro no segmento.
  - Urgent Pointer:
    - Posição dos dados urgentes no segmento.,
  - Options:
    - Tamanho de Segmento Máximo (MSS).



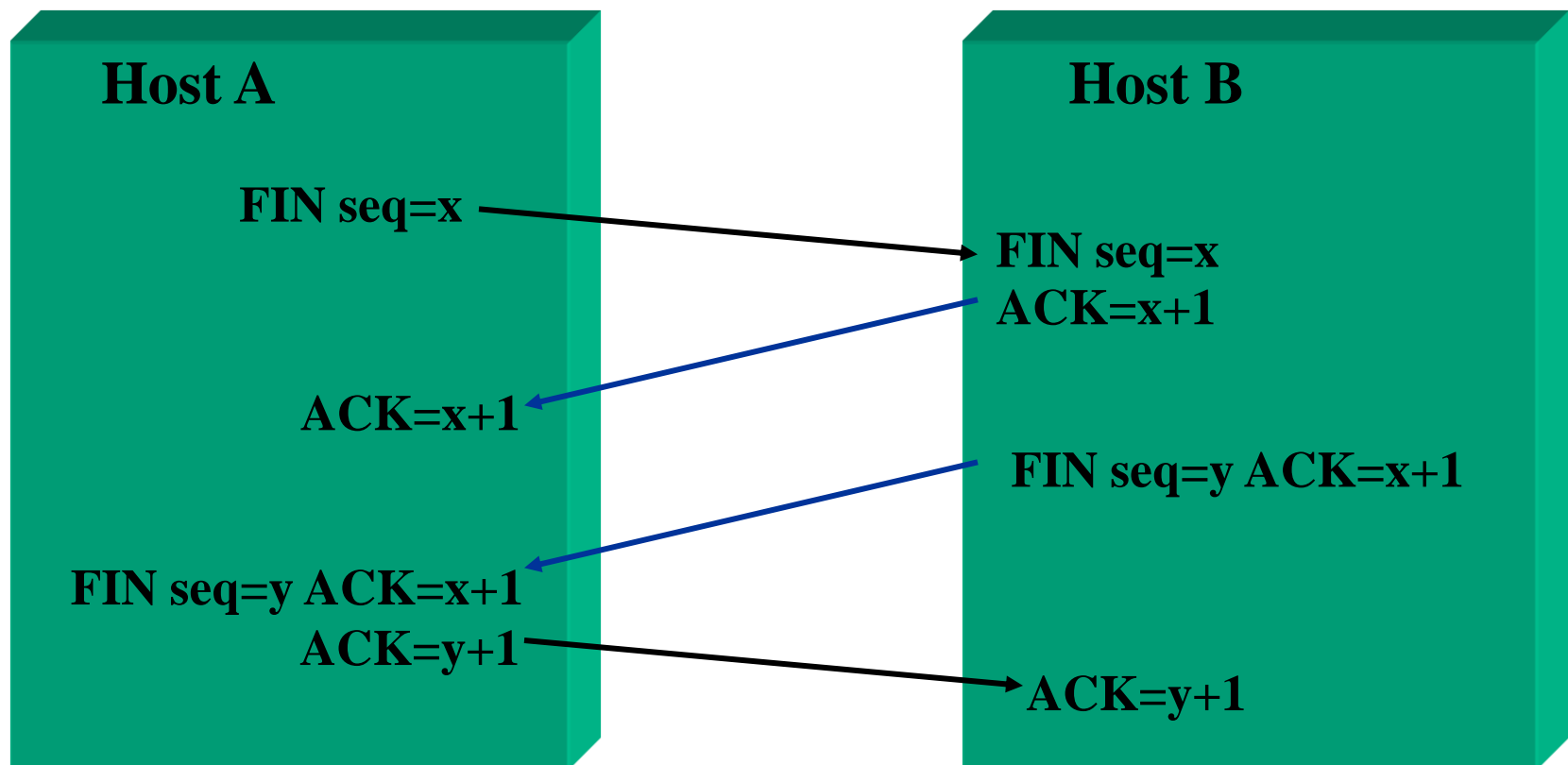
## TCP

- Three-way Handshake:





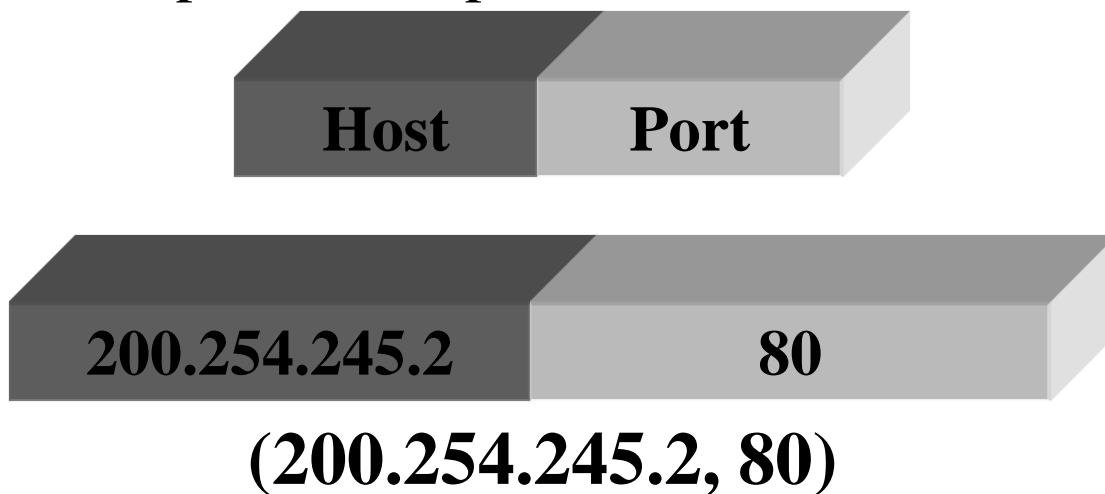
## TCP





## TCP:

- Portas, Conexões e Endpoints:
  - TCP utiliza o conceito de conexão para identificar os dois pontos envolvidos na comunicação;
  - A conexão é identificada por um par de Endpoints;
  - Um Endpoint é um par de inteiros na forma:



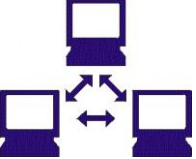


## TCP:

- Portas, Conexões e Endpoints:
  - Endpoints permitem que uma determinada porta possa ser compartilhada por múltiplas conexões:

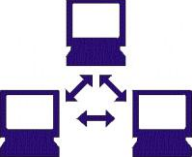
(200.254.245.21, 1184)    (200.254.245.2, 80)

(200.128.35.2, 1112)    (200.254.245.2, 80)



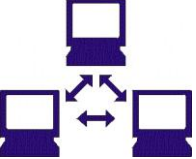
## Nível de Aplicação

- Características;
- Modelo Cliente-Servidor;
- Portas Definidas;
- Multiplexação e Desmultiplexação.



## Características

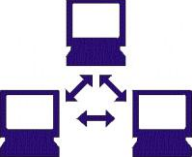
- Interage com o protocolo de transporte para enviar e receber dados;
- Aplicação define o protocolo de transporte desejado;
- Baseado no modelo Cliente/Servidor.



## Modelo Cliente/Servidor

- Servidor:
  - Processo que oferece um serviço;
  - Aceita uma requisição através da rede, executa o serviço e retorna o resultado.
- Cliente:
  - Processo que requisita o serviço;
  - Normalmente interage com o usuário.





## Modelo Cliente/Servidor

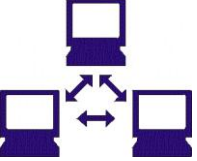
- Um servidor, espera por requisições em uma porta bem conhecida (Well-Known Port), reservada para o serviço oferecido;
- Um cliente aloca uma porta arbitrária e não reservada.



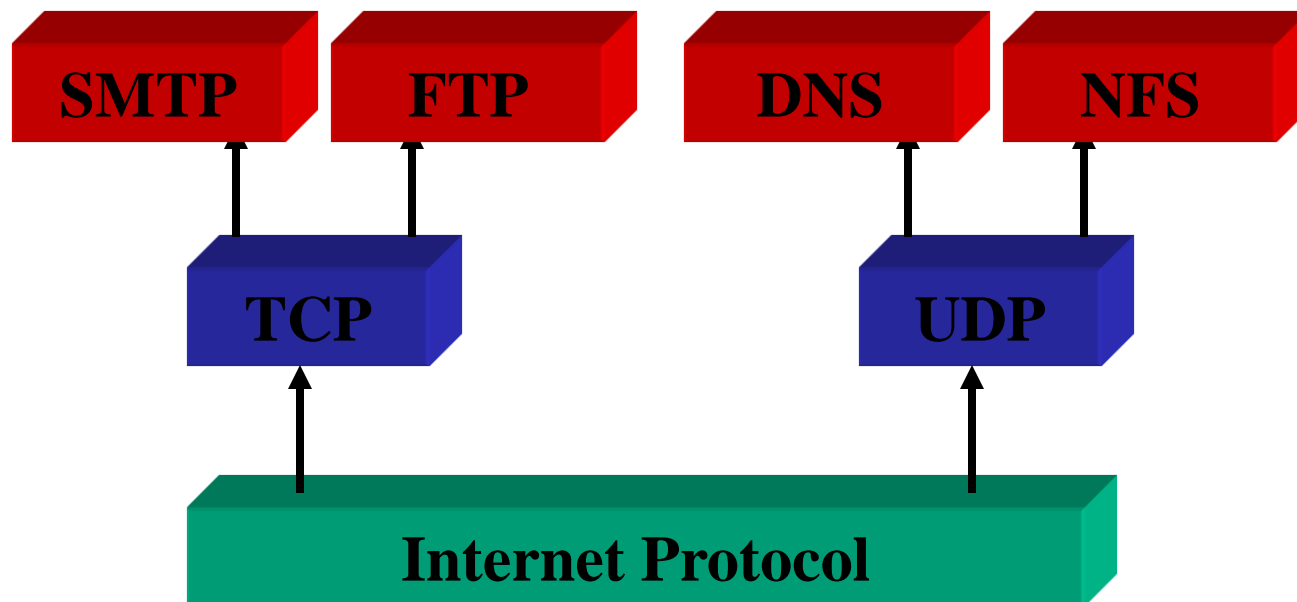
## Portas Definidas (Well-Known Ports)

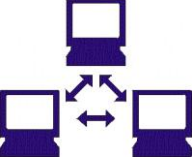
- Definidas no host:
  - /etc/services

Portas	Nome	Descrição
20	FTP-DATA	File Transfer Protocol (DATA)
21	FTP	File Transfer Protocol
22	SSH	Secure Shell Login
23	TELNET	Terminal Connection
25	SMTP	Simple Mail Transfer Protocol
53	DOMAIN	Domain name Server
80	WWW	Hiper Text Transfer Protocol



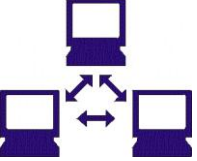
## Multiplexação e Desmultiplexação





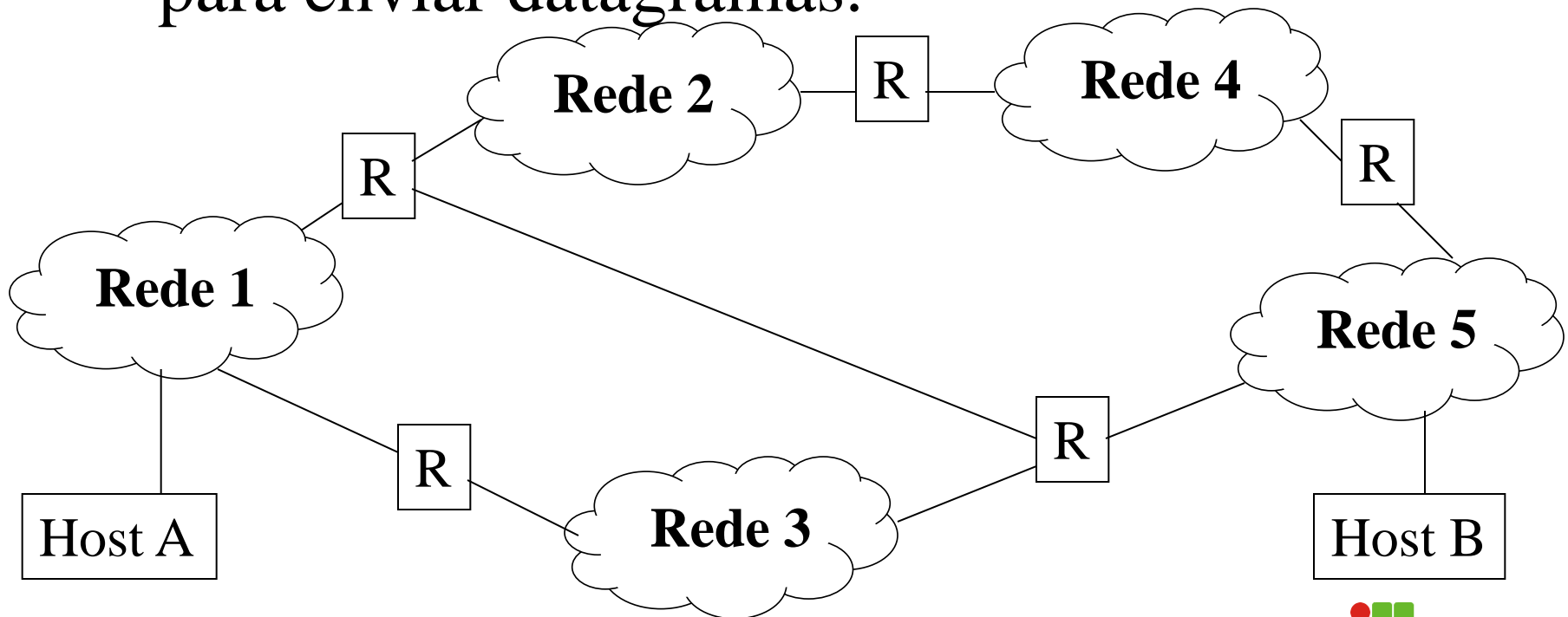
## Roteamento

- O que é?
- Roteador;
- Métricas de roteamento;
- Processo de roteamento.



## O que é?

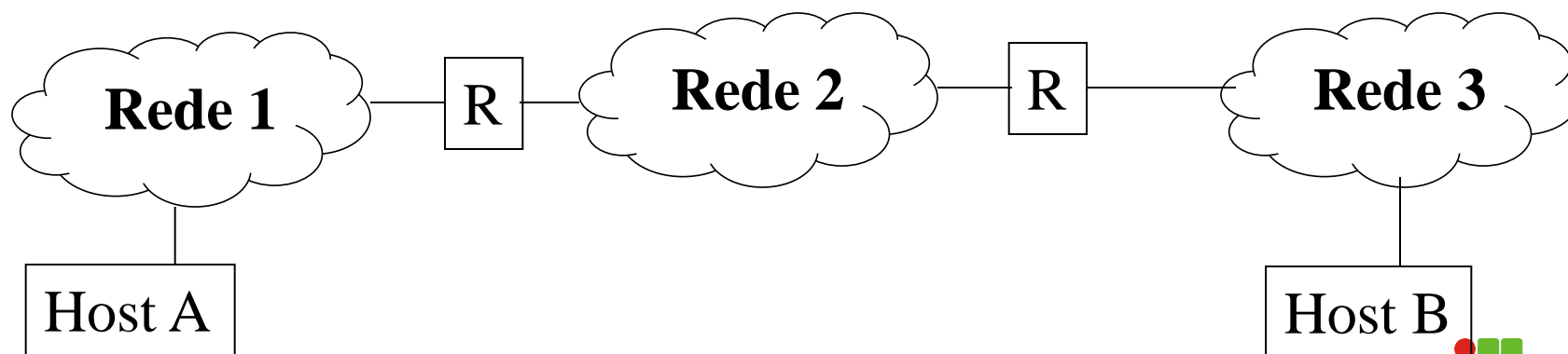
- Processo de escolha de um caminho (rota) para enviar datagramas.

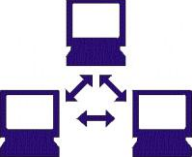




## Roteador

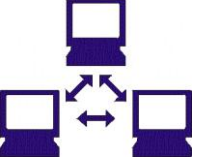
- Sistema que implementa algoritmo de roteamento;
- Os datagramas passam pelos roteadores para alcançar o destino final;
- Pode ser host multi-homed:
  - Ligado a diversas redes.





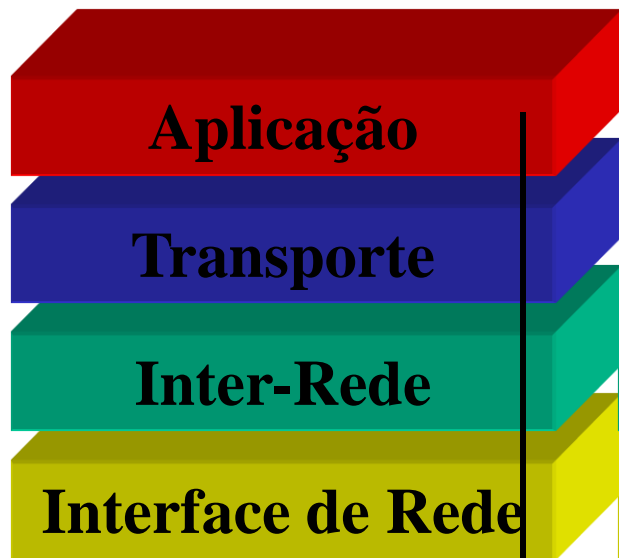
## Métrica de Roteamento

- Conjunto de indicadores que permitem a função de roteamento ser otimizada:
  - Comprimento do caminho;
  - Retardo;
  - Confiabilidade;
  - Taxa de transmissão;
  - Carga.



## Processo de Roteamento

**HOST A**



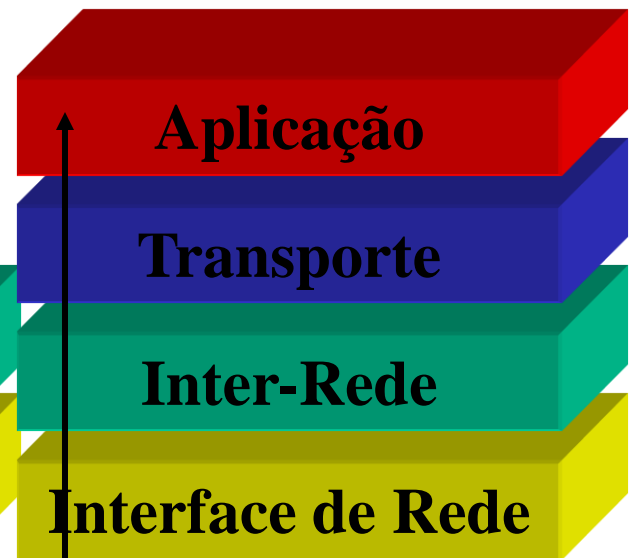
**Rede A**

**Roteador**

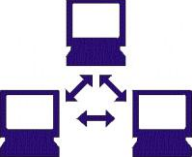


**Rede B**

**HOST B**







## Tabela de Roteamento

- Funções;
- Exemplo;
- Rota Default;
- Representação de rotas;
- Algoritmo de roteamento;
- Inicialização e manutenção.



## Funções

- Armazenar informações sobre os possíveis destinos e como enviar datagramas aos mesmos;
- Consultar como decidir enviar o datagrama;
- As entradas da tabela fornecem informações sobre roteamento para as redes físicas.

S	N	R
---	---	---

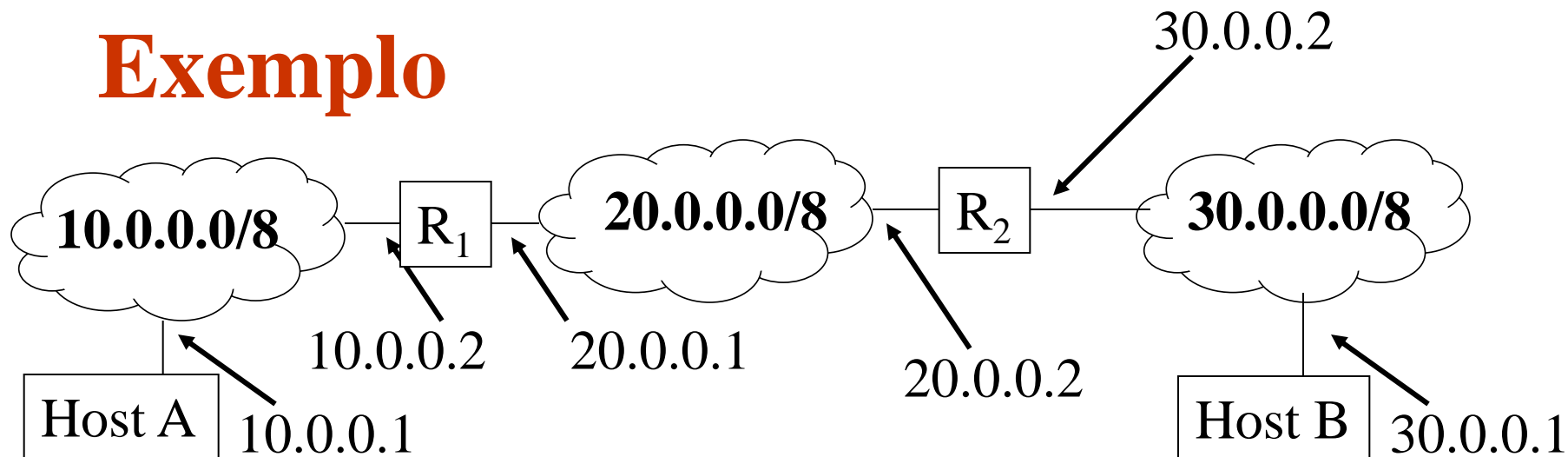
S: Máscara de rede;

N: Endereço IP da rede destino;

R: Endereço IP do roteador (next hop)



## Exemplo

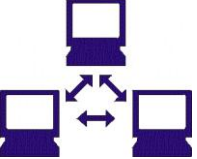


Roteador R<sub>1</sub>:

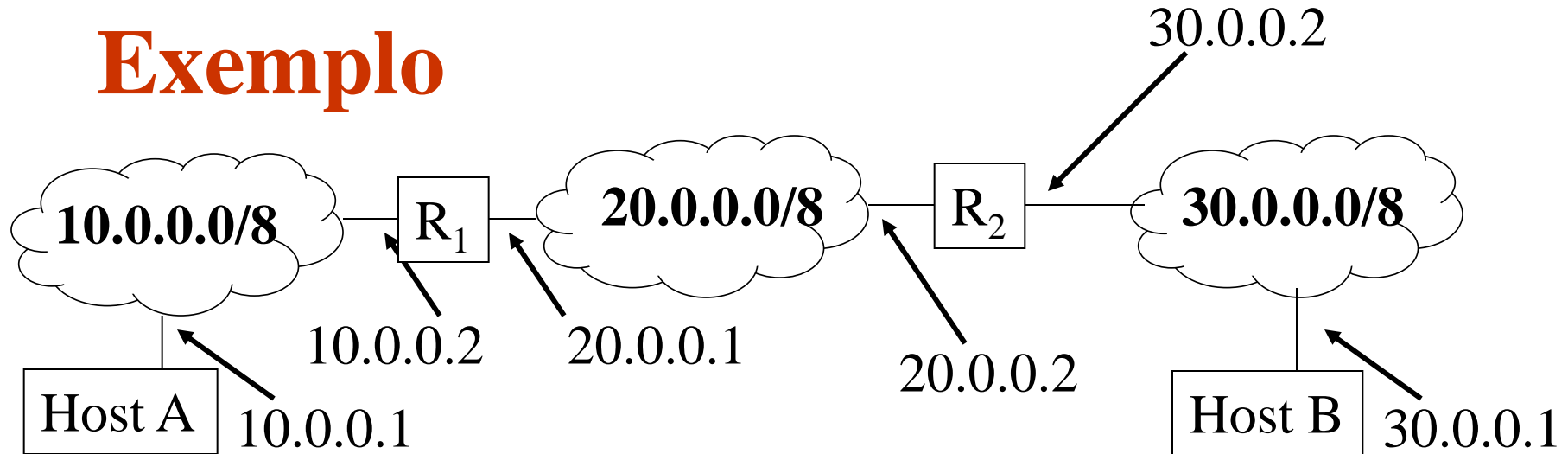
Netmask	Network	Route
255.0.0.0	10.0.0.0	Direct
255.0.0.0	20.0.0.0	Direct
255.0.0.0	30.0.0.0	20.0.0.2

Roteador R<sub>2</sub>:

Netmask	Network	Route
255.0.0.0	10.0.0.0	20.0.0.1
255.0.0.0	20.0.0.0	Direct
255.0.0.0	30.0.0.0	Direct



## Exemplo



Host A:

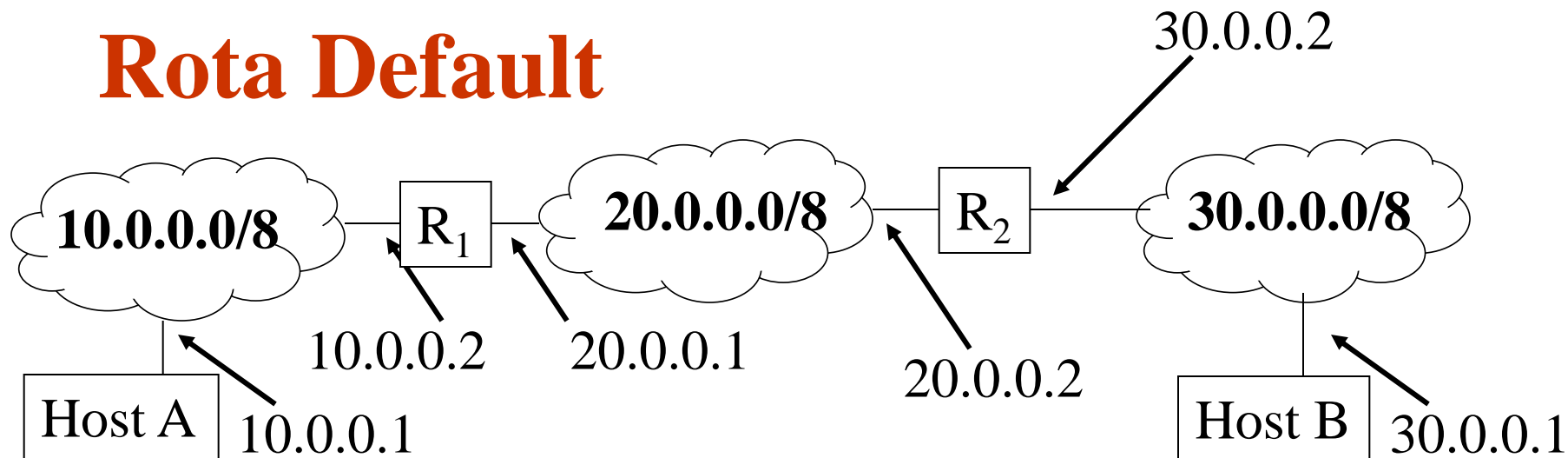
Netmask	Network	Route
255.0.0.0	10.0.0.0	Direct
255.0.0.0	20.0.0.0	10.0.0.2
255.0.0.0	30.0.0.0	10.0.0.2

Host B

Netmask	Network	Route
255.0.0.0	10.0.0.0	30.0.0.2
255.0.0.0	20.0.0.0	30.0.0.2
255.0.0.0	30.0.0.0	Direct



## Rota Default



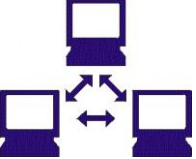
- Aplicada se não há rota na tabela associada ao host de destino.

Host A:

Netmask	Network	Route
255.0.0.0	10.0.0.0	Direct
0.0.0.0	0.0.0.0	10.0.0.2

Host B

Netmask	Network	Route
255.0.0.0	30.0.0.0	Direct
0.0.0.0	0.0.0.0	30.0.0.2



## Representação de rotas

- Rede diretamente conectada:
  - S: Máscara da rede ou sub-rede;
  - N: Endereço da rede ou sub-rede.
- Host Individual:
  - S: 255.255.255.255;
  - N: Endereço do Host.
- Rota Default:
  - S: 0.0.0.0;
  - N: 0.0.0.0.



## Algoritmo de Roteamento

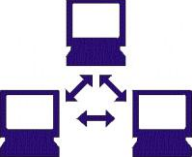
- Extrair endereço IP destino (D) do datagrama;
- Para cada entrada na tabela de roteamento:
  - Seja X o resultado de  $(D \text{ and } S)$ ;
  - Se  $X=N$ :
    - Rotear o datagrama para o next-hop R.
  - Se nenhuma entrada válida:
    - Declarar erro de roteamento.



## Inicialização e manutenção

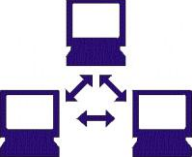
- Tabelas de roteamento são inicializadas a partir dos arquivos de configuração;
- Alterações nas tabelas implicam em respectivas mudanças nas rotas seguidas pelos datagramas;
- Roteadores propagam informações de roteamento para assegurar a consistência das tabelas;
- Protocolos são usados para propagar e manter as tabelas de roteamento.





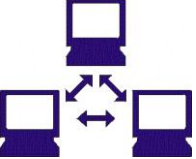
## Protocolos de Roteamento

- Objetivo;
- Classificação;
- Características.



## Objetivo

- Construir tabelas de roteamento completas e consistentes nos diversos roteadores;
- Classificação:
  - Número de caminhos;
  - Propagação de rotas.



## Classificação

- Número de caminhos:
  - Caminho único:
    - Apenas uma entrada na tabela para determinada rede;
  - Múltiplos caminhos:
    - Diversas entradas na tabela para uma determinada rede.



## Classificação

- Propagação de rotas:
  - Vetor-distância:
    - periodicamente envia uma cópia de sua tabela de roteamento para seus roteadores vizinhos;
    - Menor processamento, lenta convergência
  - Estado de Enlace:
    - Periodicamente propaga informações sobre o estado de seus enlaces para todos os outros roteadores;
    - Maior processamento, rápida convergência.



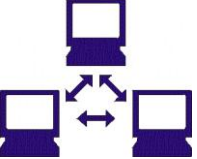
## Classificação

- Interior/Exterior:
  - Interior Router Protocol:
    - Projetado para a propagação de rotas dentro de um mesmo Autonomous System.
  - Exterior Protocol Router:
    - Projetado para a propagação de rotas entre Autonomous Systems..

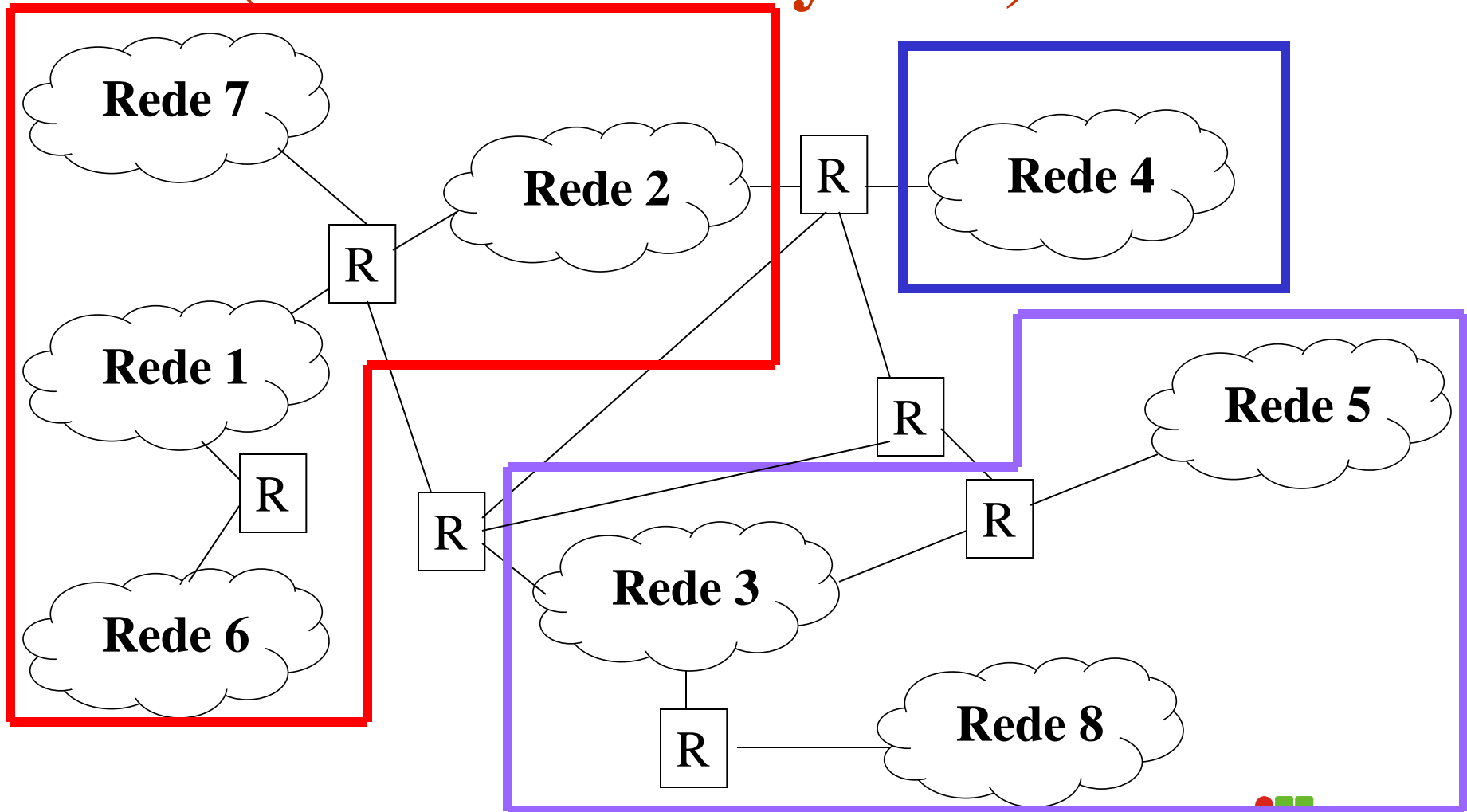


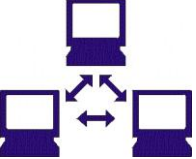
## AS (Autonomous System)

- Agrupamento de redes conectadas entre si;
- Cada AS possui um conjunto próprio de blocos de endereços;
- Os AS se comunicam entre si para propagarem mensagens para os blocos de endereço externos.



## AS (Autonomous System)

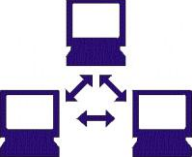




# RIP (Router Information Protocol)

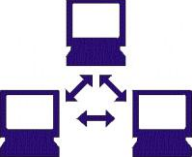
- Características;
- Classificação dos Sistemas;
- Tabela de Rotas;
- Propagação de Rotas;
- Atualização de Rotas;
- routed.





## Características

- Ver RFC1058 (1988);
- Popularizado em 1982 pela implementação *routed* do BSD/Unix;
- Classificação:
  - Caminho único;
  - Vetor-distância.



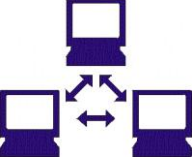
## Classificação dos sistemas

- Ativos:
  - Propagam rotas para outros sistemas;
  - Escutam e atualizam suas rotas baseados nas propagações dos outros sistemas ativos;
  - Roteadores atuam em modo ativo.
- Passivos:
  - Escutam e atualizam suas rotas baseados nas propagações dos sistemas ativos;
  - Hosts atuam em modo passivo.



## Tabela de Rotas

- Destination (D):
  - Endereço da rede/host destino.
- Next Hop (H):
  - Endereço IP do próximo roteador até o destino.
- Interface (I):
  - Interface local do host a ser utilizada para a rota.
- Metric (M):
  - Distância em hops até o destino.
- Timers:
  - Temporizadores que auxiliam as funções do RIP.



## Propagação de Rotas

- Mensagem de broadcast a cada 30 seg.;
- Mensagem contém pares (D, M):
  - D: Endereço IP da rede destino;
  - M: Distância da rede.
- Distância medida por número de roteadores intermediários (hop count):
  - 1: Diretamente conectado;
  - n: Número de roteadores Intermediários.

**Menor Hop Count não indica melhor rota**



## Atualização de rotas

- Se K recebe mensagem de J através da interface I:
  - Para cada par (D, M) fornecido por J, K atualiza sua tabela se:
    - J conhece um caminho mais curto para D;
    - K roteia D através de J e M fornecido por J mudou;
    - K não sabe rotear para D.
    - Cada atualização será da forma:

<b>D</b>	<b>J</b>	<b>M+1</b>	<b>0</b>
----------	----------	------------	----------



## Atualização de rotas

Sistema 10.0.0.10

Destination	Distance	Route
10.0.0.0	1	Direct
20.0.0.0	8	10.0.0.2
30.0.0.0	5	10.0.0.2
40.0.0.0	6	10.0.0.1
50.0.0.0	2	10.0.0.2



Sistema 10.0.0.10

Destination	Distance	Route
10.0.0.0	1	Direct
20.0.0.0	8	10.0.0.2
30.0.0.0	5	10.0.0.2
40.0.0.0	6	10.0.0.1
45.0.0.0	5	10.0.0.1
50.0.0.0	2	10.0.0.2

Sistema 10.0.0.1

Destination	Distance
10.0.0.0	1
20.0.0.0	8
30.0.0.0	5
40.0.0.0	6
45.0.0.0	4
50.0.0.0	2



## routed

- Propagação e atualização de tabelas de roteamento via RIP
  - routed [-q];
  - -q: inibe propagação de rotas.
- Inicialização via arquivo /etc/gateway:

```
net/host dest_address gateway addr_gateway metric n active/passive
```

```
net 150.101.1.0 gateway 200.19.17.4 metric 2 active
```



# OSPF (Open Shortest Path First)

- Protocolo tipo IRP projetado para realizar roteamento dentro de um AS;
- Especificado na RFC 1583 (OSPF-2);
- Propagação das rotas baseado em estado de enlace;
- Determinação de rotas baseado no algoritmo SPF (Dijkstra);
- Motivação:
  - Suprir deficiências do RIP em adequar-se a grandes redes heterogêneas.





## OSPF

- Características:
  - Sumarização de rotas:
    - melhora o desempenho e escalabilidade da rede.
  - Balanceamento de carga:
    - Se rotas de custos iguais existem, roteadores poderão utilizá-las de forma balanceada.
  - Tratamento de tipo de serviço:
    - Roteamento baseado em tipo de serviço solicitado por protocolos de nível superior.
  - Múltiplos caminhos



## BGP (Border Gateway Protocol)

- Protocolo tipo ERP projetado para realizar roteamento entre Autonomous Systems;
- Vetor-distância com características de Estado de Enlace;
- Motivação:
  - Suprir deficiências do EGP (Exterior Gateway Protocol):
    - Propaga apenas informações de alcançabilidade;
      - Não interpreta métricas.
    - Estrutura em árvore;
    - Não detecta laços de roteamento.



## Linux e TCP/IP

- Distribuições:
  - Slackware;
  - Debian;
  - RedHat;
  - Caldera;
  - etc.
- Configuração pode variar de acordo com a distribuição.
- Será dado enfoque ao Slackware.



## Linux e TCP/IP

- Configurando a rede:
  - utilitário netconfig;
    - Altera arquivo `/etc/rc.inet1`.
  - comando ifconfig:
    - `ifconfig eth0 <ip_address> broadcast <broadcast> netmask <netmask>`.
  - Ou via DHCP;
  - Servidor de DHCP no Linux: `dhcpd`.



## Linux e TCP/IP

- Configurando a rede:
  - comando route:
    - define e exibe rotas;
    - **Rota para redes locais:**
      - route add -net <network> netmask <netmask> [gw <gateway>] eth0.
    - **Rota default:**
      - route add -net default gw <gateway> netmask 0.0.0.0 metric 1.



## Linux e TCP/IP

- Verificando a rede:
  - ifconfig: exibe as interfaces configuradas;
  - netstat: exibe status das conexões;
    - netstat -rn;
    - netstat -atu.
  - route: exibe a tabela de rotas;
  - ping e traceroute: permitem investigar conexão a outros hosts para resolver problemas.



## Linux e TCP/IP

- Arquivos de configuração:
  - /etc/rc.d: Arquivos a serem executados na inicialização:
    - rc.inet1;
    - rc.inet2;
    - rc.local;
    - inittab;
    - rc.S e rc.M.
  - inetd: Inicializa uma série de serviços:
    - inetd.conf.



## Linux e TCP/IP

- O kernel do sistema:
  - opções avançadas de networking:
    - IP Masquerade;
    - IP Forwarding;
    - IPv6;
    - etc.
  - Pode-se ter o mínimo necessário rodando no sistema.





## Linux e TCP/IP

- O kernel do sistema:
  - compilando-se o kernel:
    - `cd /usr/src/linux;`
    - `make menuconfig;`
    - `make dep;`
    - `make clean;`
    - `make bzImage` ou `make zlilo;`
    - `make modules;`
    - `make install` e `make modules_install`.



## Linux e TCP/IP

- Gerenciamento remoto:
  - Telnet:
    - via inetd;
    - inseguro.
  - Secure Shell Login:
    - via inetd ou /etc/rc.d/rc.inet2;
    - criptografia com chaves públicas e privada.



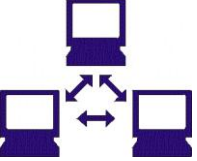
# FTP (File Transfer Protocol)

- Protocolo de transferência de arquivos;
- No Linux:
  - É integrado ao sistema;
  - Suporte aos home directories dos usuários;
  - Servidor wu-ftp e cliente ftp;
  - Usuário ftp no Linux permite acesso anônimo ao ftp;
  - Senha sem criptografia;
  - Ativo no Linux via inetd.



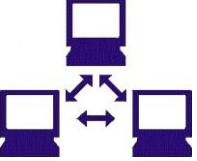
# NFS (Network File System)

- Sistema de Arquivos para Acesso Remoto no Ambiente UNIX;
- É montado como um dispositivo qualquer do sistema;
- Apresenta problemas de segurança.



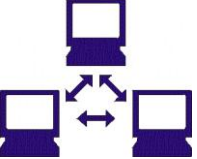
## DNS

- Endereços IP não são amigáveis;
- Uso de nomes para identificar hosts;
- Estabelecimento de uma hierarquia;
- Base de dados distribuída.

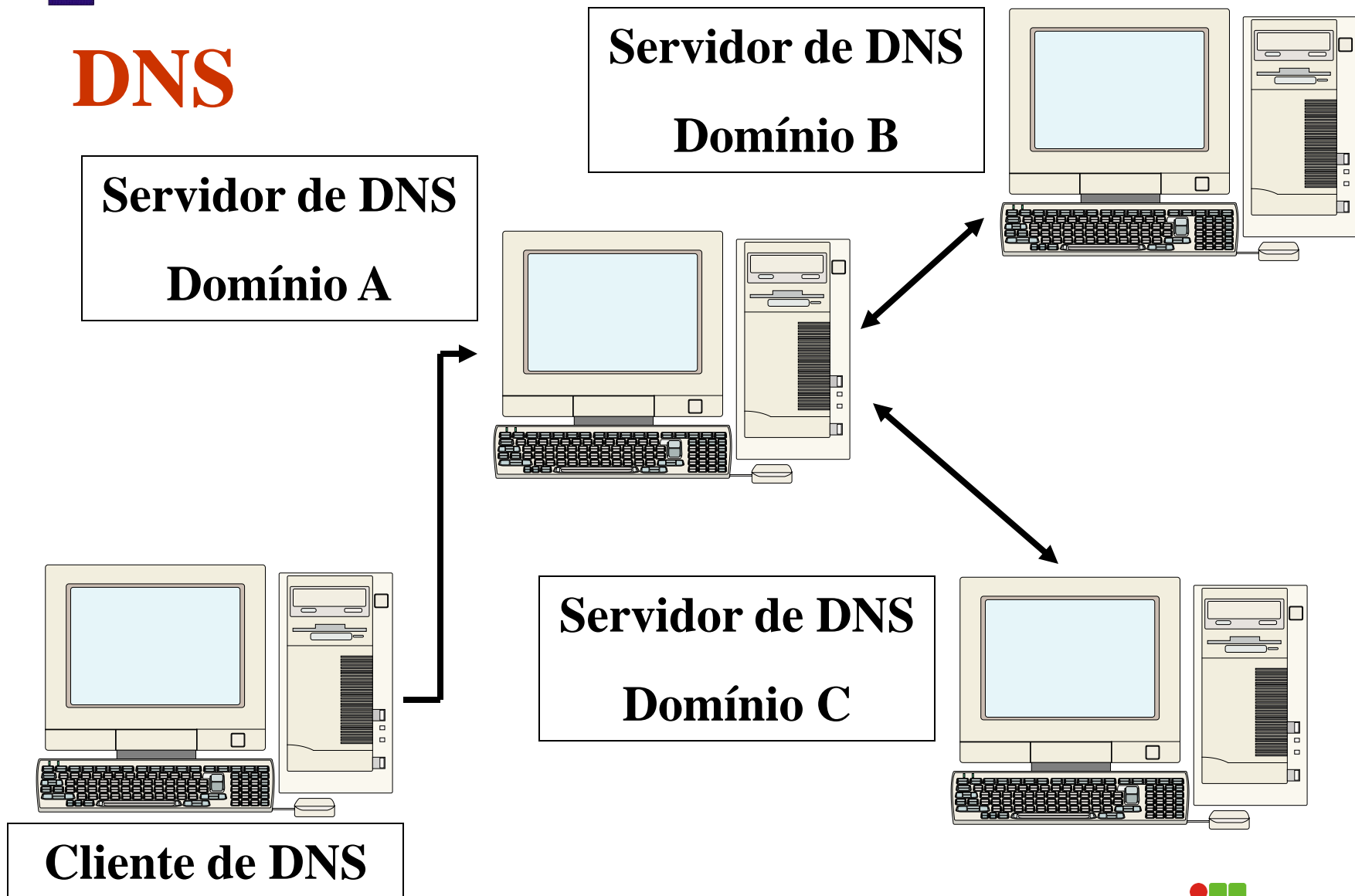


## DNS

- Mapeamento:
  - direto: nome para endereço IP;
  - reverso: endereço IP para nome.
- Comunicação cliente/servidor;
- Uso de TCP e UDP na porta 53.



## DNS





## DNS

- Estrutura:
  - Hierarquia de nomes e domínios:
    - Cada domínio representa um grupo de máquinas;
    - Não é necessário haver correspondência entre um domínio direto e uma rede;
    - Existe um domínio reverso para cada rede.
  - Administração descentralizada:
    - Servidores principais;
    - Servidores secundários;
    - Recursivamente.





## DNS

- Estrutura:
  - Criação de níveis:
  - Primeiro nível - Root domain ( . ):
    - ROOT-SERVERS
    - Delega autoridade para segundo nível.
  - Segundo nível - Top Level Domains:
    - Domínios dos países: .BR, .UK, .PT.
    - Classes de domínios dos EUA: .EDU, .GOV, .MIL, .COM.



## DNS

- Estrutura:
  - Terceiro nível - Top Level Domains:
    - Classes de domínios: .GOV.IT, .COM.BR, CO.UK;
    - Organizações nos EUA: LINUX.ORG, IBM.COM.
  - Quarto nível:
    - Nomes de Hosts: WWW.AOL.COM;
    - Nomes de ortganizações: IBM.COM.BR.
  - Quinto Nível:
    - Segue assim por diante...



## DNS x Linux

- Named:
  - Configura por `/etc/named.conf`
    - options:
      - directory.
    - type master;
    - type slave;
    - type hint;
    - file;
    - masters.



## DNS x Linux

- Named:
  - zonas de configuração;
  - arquivo cache:
    - localização de ROOT-SERVERS;
    - cache.
  - named.local;
  - arquivos de zona direta e reversa;
  - zonas secundárias;
  - diretório /var/named.



## DNS x Linux

- Arquivos de zona:
  - IN SOA (Start of Authority);
  - IN NS (Name Server);
  - IN MX (Mail eXchanger);
  - IN A (Address);
  - IN CNAME (Canonical NAME);
  - IN PTR (reverse PoinTeR).



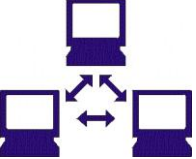
## DNS x Linux

- Opções no IN SOA:
  - Serial: indica a versão do mapa de DNS;
  - Refresh: intervalo de tempo a partir do qual um servidor secundário deve checar o serial do primário;
  - Retry: caso não haja sucesso o servidor secundário espera o tempo de retry e tenta novamente.



## DNS x Linux

- Opções no IN SOA:
  - Expire: Caso o primário não consiga ser contactado no tempo do campo Expire, todos os mapas do secundário são descartados.



## DNS x Linux

```
/*  
sample of a named.conf  
*/  
  
options {  
    directory “/var/named.conf”  
};  
  
zone “.” in {  
    type hint;  
    file “root.cache”;  
}
```





## DNS x Linux

```
Zone “lab.cefetba.br” in {  
    type “master”;  
    file “teste.zone”;  
};
```

```
zone “cefetba.br” in {  
    type “slave”;  
    file “cefetba.zone”;  
    masters {200.254.245.2};  
};
```

```
zone “245.254.200.in-addr.arpa” in {  
    type master;  
    file “reverso.200.254.245”;  
};
```



## DNS x Linux

**; labs.cefetba.br**

**;**

**@ IN SOA host.labs.cefetba.br root.host.labs.cefetba.br (**

**199907270001 ; serial**

**3600 ; refresh**

**900 ; retry**

**3600000 ; expire**

**3600 ; minimum**

**IN NS host.labs.cefetba.br;**

**hosta IN A 10.0.20.1**

**hostb IN A 10.0.20.2**

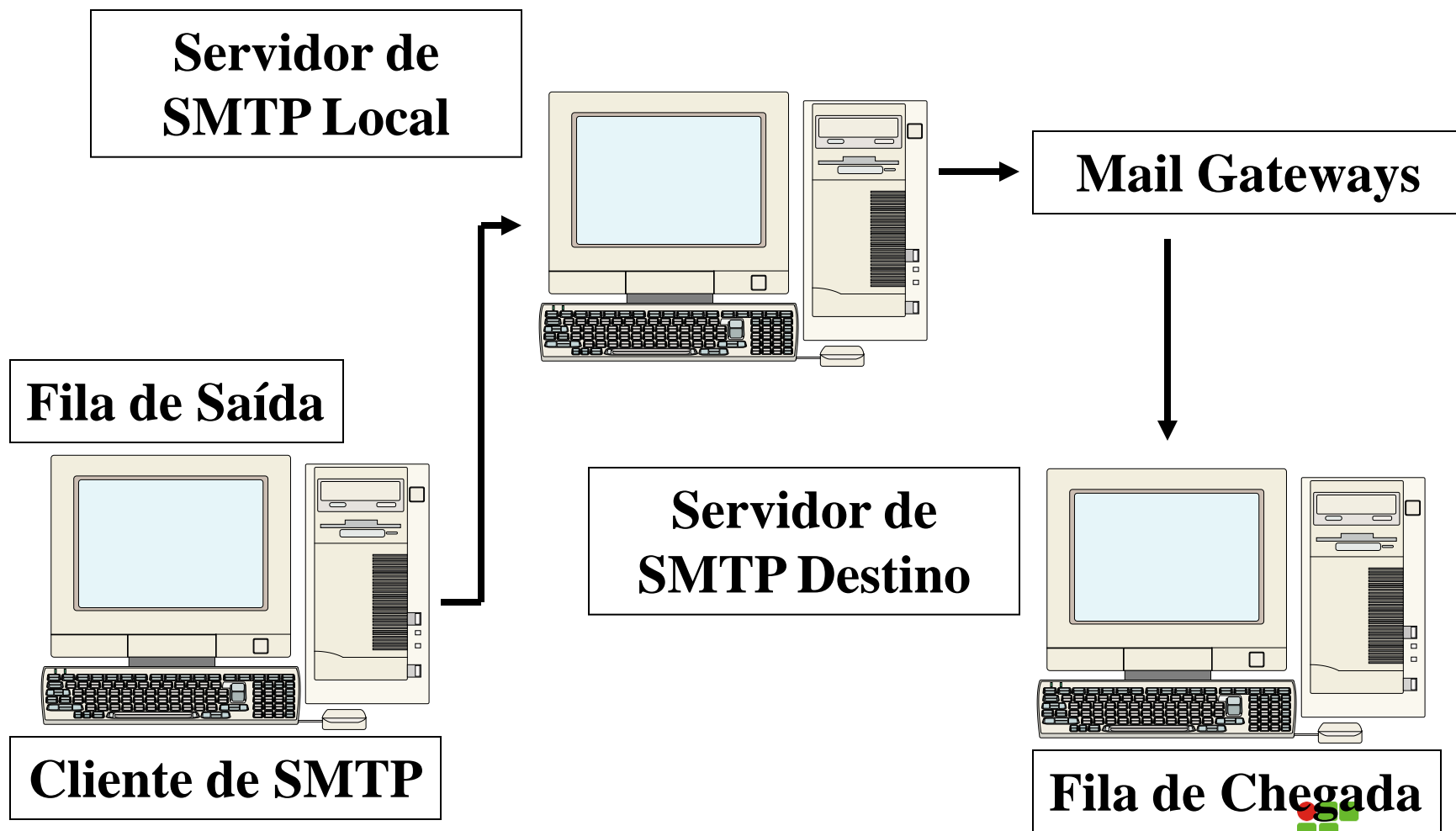
**host IN A 10.0.20.3**

**www IN CNAME hosta**

**};**



## SMTP - Simple Mail Transfer Protocol





## SMTP

- Protocolo de transferência de mensagens:
  - Endereços eletrônicos:
    - user@dominio;
    - aliases.
  - Spool de saída:
    - Usuário não precisa esperar até o delivery da mensagem.
  - Spool de entrada:
    - Usuário não precisa estar on-line para receber mensagens.



## SMTP

- Protocolo de transferência de mensagens:
  - Mail forwarding:
    - Mensagens de um usuário são redirecionadas para outro correio eletrônico.
  - Mail gateways:
    - Máquinas intermediárias no processo de entrega de mail;
    - Aumentam a interoperabilidade.
  - Conexão TCP na porta 25.



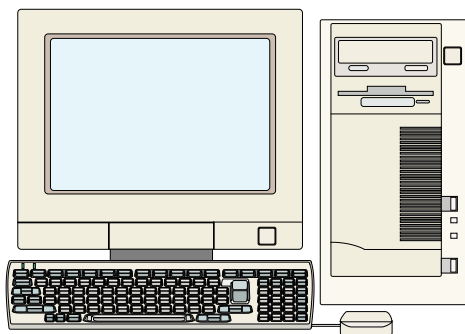
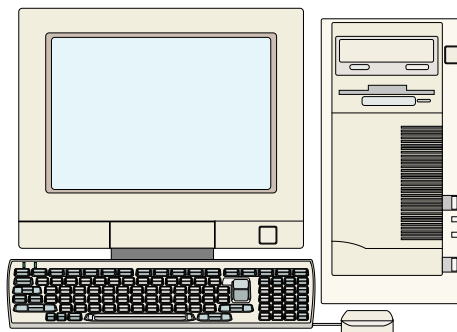
## SMTP x Linux

- Sendmail:
  - Servidor SMTP padrão da Internet:
  - Configuração:
    - **/etc/sendmail.cf**: configuração geral:
      - **DM**: realizar mascaramento de domínios;
      - **Cw**: autoridade sobre domínios.
    - **/etc/sendmail.cw**: autoridade sobre domínios;
    - **comando newaliases**: criar aliases.
  - Proteção contra “SPAM”:
    - Aceitar conexões apenas de redes conhecidas;
    - Não realizar relay.

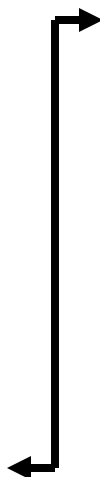


## POP - Post Office Protocol

**Servidor de  
POP3**



**Cliente de POP3**





## POP3

- Características:
  - permite que o usuário retire suas mensagens da fila de chegada;
  - As mensagens são transferidas para a máquina do usuário:
    - Opcionalmente podem ser mantidas no servidor.
  - Não há criptografia de senhas ou mensagens.
    - Usa-se PGP para criptografia de mensagens.
  - Usa porta 110 do TCP.





## WWW

- Hiper Transfer Protocol (HTTP):
  - Maior volume de tráfego da Internet;
  - Transferência de páginas de Hipertexto (HTML):
    - Texto;
    - Imagens;
    - Som e vídeo;
    - Objetos e aplicações.
  - Execução remota de aplicações:
  - Scripts CGI, IDC< ASP, Java Servlets;
  - Retorno em HTML.



## WWW

- Hiper Transfer Protocol (HTTP):
  - Etapas da conexão:
    - Abrir conexão:
      - O cliente contacta o servidor.
    - Solicitação de dados:
      - Cliente envia mensagens ao servidor:
        - » Request headers definem o método de processamento do pedido e informam as capacidades do cliente;
        - » Dados extra, se necessário.



## WWW

- Hiper Transfer Protocol (HTTP):
  - Etapas da conexão:
    - Resposta do servidor:
      - Response headers indicando o status do pedido e o tipo de dados;
      - Dados solicitados.
  - Possibilidade de várias conexões simultâneas de um cliente a um mesmo servidor.
    - Transferência simultânea de texto e imagens.



## WWW x Linux

- Apache - Servidor WWW:
  - `/var/lib/apache/conf/httpd.conf`: configuração auto-explicativa;
  - `/var/lib/apache/sbin/apachectl [start|stop|restart]`.
- Lynx - Cliente WWW via Texto;
- Netscape - Cliente gráfico de WWW.



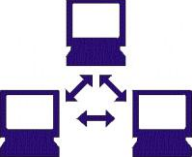
## WWW x Linux

- CGI (Common Gateway Interface):
  - C, Perl, Shell Scripts;
  - Deve se ter cuidado com segurança;
  - Os CGIs são executados no servidor como usuário nobody do grupo nogroup.
- Configurações Extras:
  - Página do usuários:
    - public\_html.
  - Domínios virtuais.



## NT x Linux

- Conectividade de sistema de arquivos:
  - NFS no NT:
    - Omni NFS Client.
  - Samba no Linux:
    - /etc/smb.conf;
    - /etc/sbin/nmbd;
    - /etc/sbin/smbd.
  - Smbfs no Linux:
    - smbclient '\\server\share' <password> -U <user>
    - smbmount '\\server\share' <password> -c mount /mnt -U <user>



## NT x Linux

- Backups:
  - Montagem remota de filesystem;
  - tar, cpio e dd no Linux;
  - Microsoft Backup no NT.



## NT x Linux

- Interoperabilidade:
  - DNS Server a partir da versão 4.0 do NT;
  - Exchange Mail Server;
  - Port do Sendmail para o NT;
  - Impressão no NT via Linux com Samba;
  - Uso de LPD e LPR para interoperabilidade de impressão;
    - Impressoras devem ser post-scripts.





## NT x Linux

- Interoperabilidade:
  - WWW e FTP no NT via IIS (Internet Information Service);
  - Gerenciador de DHCP no NT;
  - Gerenciador de WINS no NT.



## NT x Linux

- Gerenciamento de usuários:
  - No Linux:
    - adduser;
    - rmuser;
    - /etc/passwd;
    - /etc/shadow.
  - No NT:
    - Gerenciador de Usuários para Domínios;
    - Informações de Usuários ficam gravadas na SAM (Registro do NT)



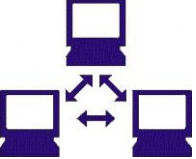
## NT x Linux

- Domínios NT:
  - Linux:
    - Samba não suporta controle de PDC e BDC;
    - Deve-se usar o PAM para o usuário Linux ter sua senha validada pelo NT.
  - Windows:
    - Samba pode atuar como meio de autenticação.



## NT x Linux

- Segurança:
  - Linux:
    - ext2 suporta segurança a nível de owner, group do owner e todos;
    - senhas do sistema são criptografadas no passwd ou no shadow (shadow incrementa segurança).
  - Windows:
    - NTFS suporta segurança a nível de owner, grupos locais e globais e todos, sendo mais flexível;
    - Senhas são criptografadas na SAM.



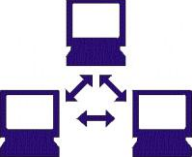
## Gerência de Redes

- Conceitos Básicos;
- Principais MIBs;
- Plataformas de Gerência;
- Aplicações de Gerência;
- Gerência Web-based.



## Gerência de Rede

- Objetivos
  - “Controlar, administrar e monitorar eficientemente os recursos de hardware e software presentes na rede”;
  - As funções de gerência são incluídas nos elementos da rede;
  - As informações coletadas visam evitar, detectar ou intervir em problemas.



## Gerência de Redes

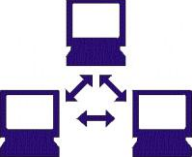
- Quadro atual:
  - Complexidade:
    - Explosão das redes;
    - Equipamentos dos mais diversos tipos.
  - Heterogeneidade:
    - Diversos fornecedores.
  - Qualificação:
    - Falta de pessoal qualificado



## Gerência de Redes

- Atuação da gerência nos elementos gerenciados:
  - Medir e comparar desempenho;
  - Verificar e alterar configuração;
  - Detectar e atuar em falhas;
  - Verificar e atuar na segurança;
  - Contabilizar dados estatísticos (ex: tráfego).





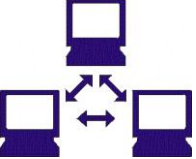
## Gerência de Redes

- Como gerenciar:
  - Obter dados da rede;
  - Tratar os dados;
  - Realizar diagnóstico;
  - Encaminhar soluções.



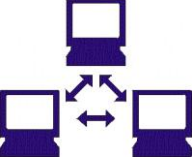
## Gerência na mão...

- Uso do ping;
- Uso do traceroute;
- Gerência reativa:
  - Atuar após detectado o problema;
  - O problema pode ser detectado ao acaso;
  - O problema pode não ser detectado.
- Retirar o cabo da porta.



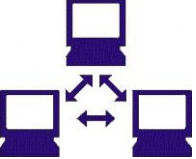
## Arquitetura de Gerência

- Componentes:
  - Nodos gerenciados ou Agentes;
  - Estações Gerenciadoras da rede ou Gerentes;
  - Protocolo de Gerência;
  - Informação de Gerência.



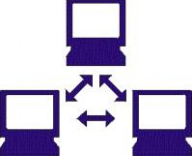
## Agentes

- Características:
  - Mantém a informação de Gerência;
  - São formados por software inserido nos elementos a serem gerenciados:
    - Hubs, switches, roteadores;
    - Servidores, estações de trabalho;
    - etc.

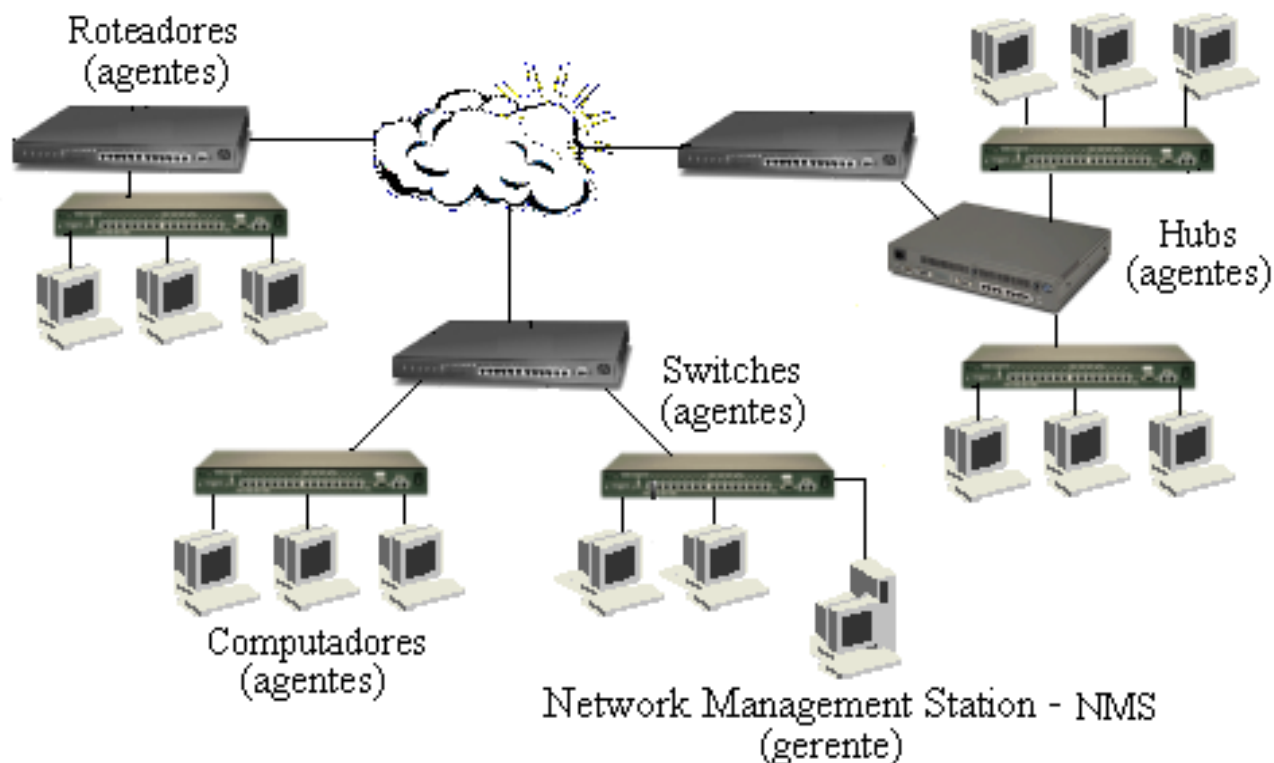


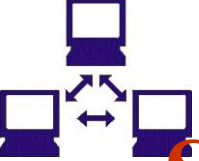
## Gerentes

- Características:
  - São formados por software que recebe e manipula os dados a serem gerenciados;
  - Os dados são obtidos dos agentes através do protocolo de gerência.



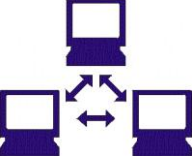
## Uma Rede Gerenciada



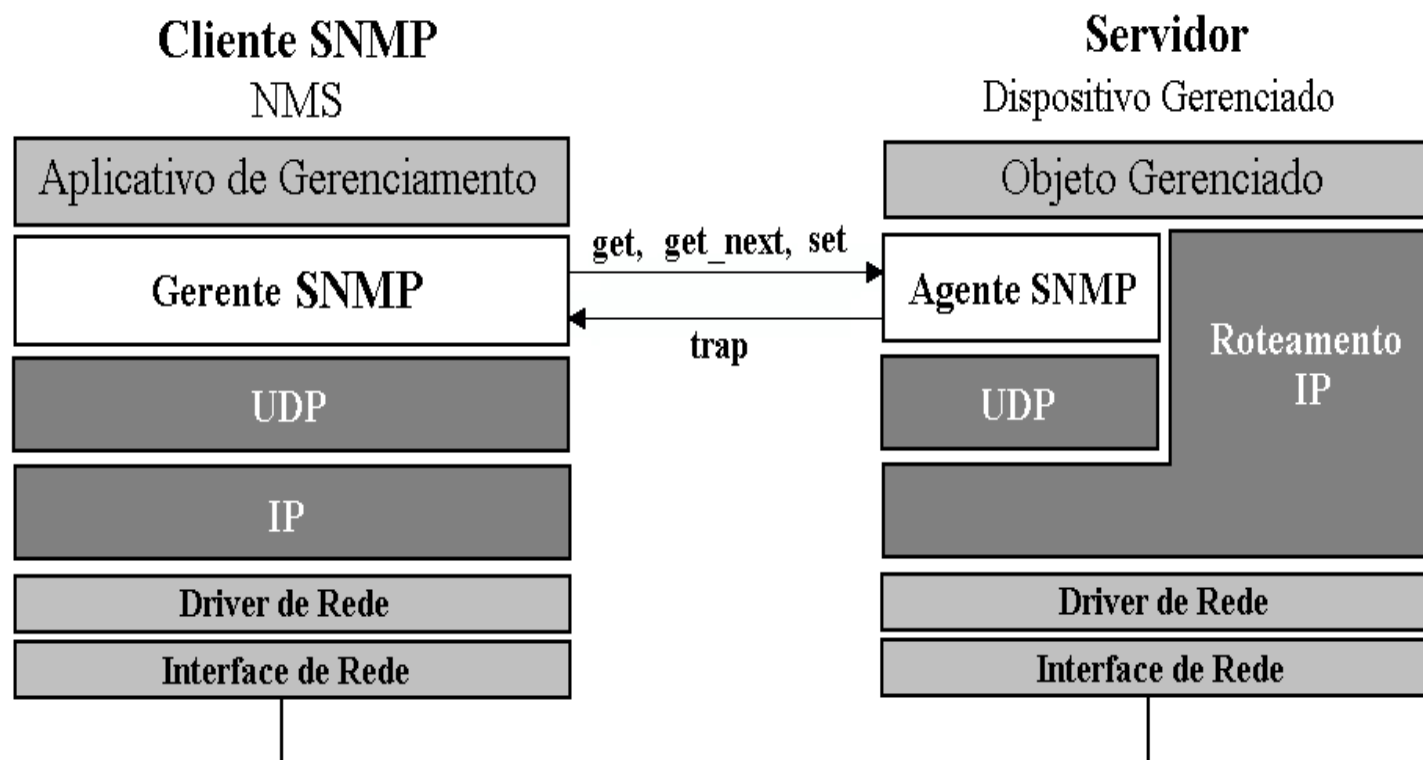


# SNMP (Simple Network Management Protocol)

- Protocolo de facto;
- Largamente usado;
- Usa as primitivas básicas :
  - get - adquirir uma variável específica;
  - get\_next - operação de encaminhamento;
  - set - alterar valores das variáveis;
  - trap - informar eventos extraordinários.



## O Modelo SNMP

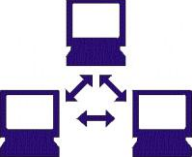






## Segurança

- Uma comunidade determina a relação entre agentes e um ou mais gerentes;
- O nome da comunidade é o mecanismo de autenticação empregado pelo SNMP:
  - A comunidade é uma senha
- Inseguro.



# Informação de Gerência

- Estrutura da Informação de Gerenciamento:
  - Structure of Management Information - SMI.
- Base de Dados das Informações de Gerência:
  - Management Information Base - MIB.

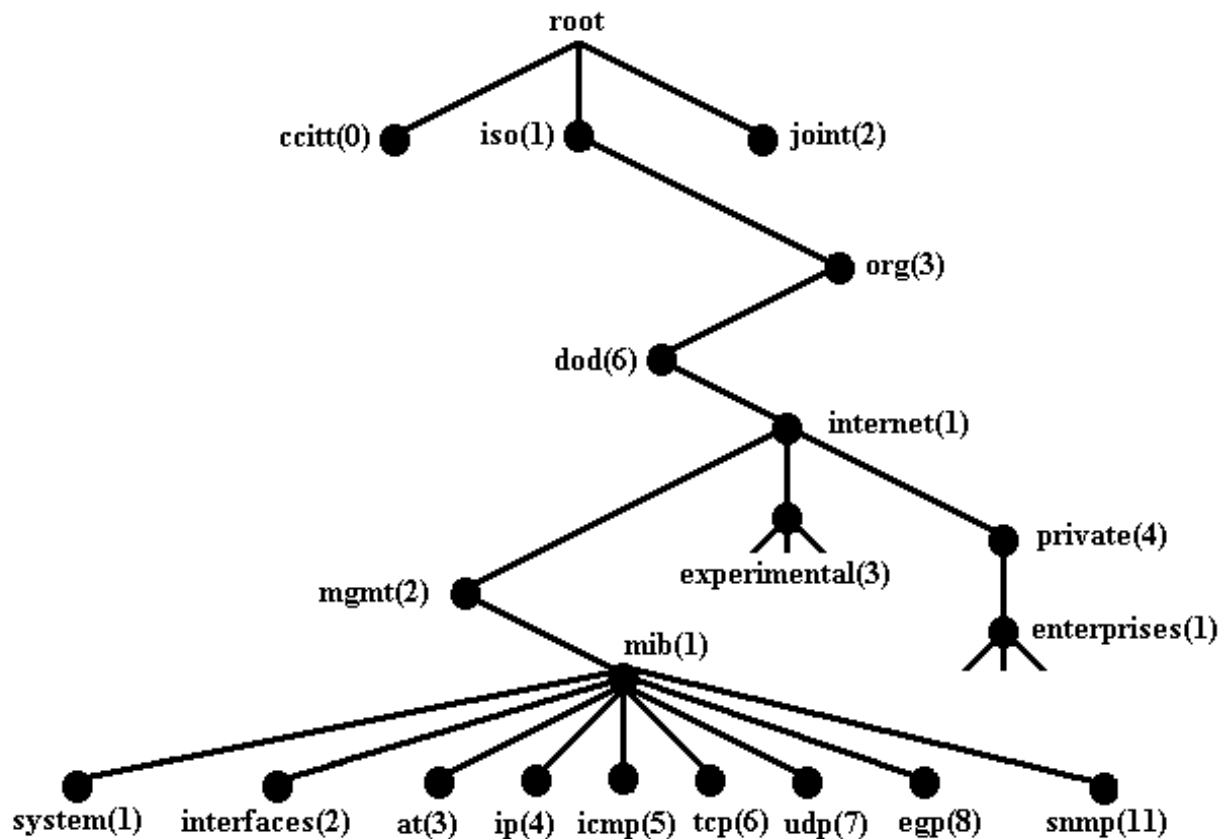


# Representação dos Dados

- Estrutura em árvore foi criada para identificar os objetos gerenciáveis;
- Cada órgão de padronização internacional tem um espaço alocado dentro desta estrutura;
- Cada nó da árvore possui um rótulo composto de uma descrição textual e um número inteiro.



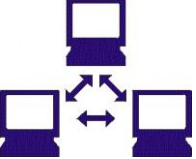
## Árvore de Identificadores





## Variáveis e Instâncias

- Cada nó da árvore agrupa um conjunto de variáveis relacionadas;
- As variáveis descrevem a informação mantida nos agentes;
- O valor da variável representa uma instância desta variável;
- Tipos:
  - simples (escalares);
  - tabelas.



# Identificação e Recuperação de Instâncias

- O Identificador é formado pela concatenação do nome do objeto com um sufixo;
- Depende do tipo de objeto, sendo definido pelas seguintes regras:
  - “0” se não é uma coluna em uma tabela;
  - caso contrário é positivo .



## Exemplos de Instâncias

- A identidade de uma instância de `sysDescr`:  
`sysDescr.0` ou `1.3.6.1.2.1.1.1.0`  
(`iso.org.dod.internet.mgmt.mib-2.system.sysDescr.0`)
- Instâncias de colunas *ifTable* são identificadas pelo valor da coluna *ifEntry*. A instância *ifDescr* associada à primeira interface é:

`ifDescr.1` ou `1.3.6.1.2.1.2.2.1.2.1`

(`iso.org.dod... ..mib-2.interfaces.ifTable.ifEntry.ifDescr.1`)



## Linhas de Tabelas

- Uma linha é identificada por combinação de colunas;
- Uma conexão TCP é identificada por vários objetos:
  - tcpConnLocalAddress (89.1.1.42)
  - tcpConnLocalPort (21)
  - tcpConnRemAddress (10.0.0.51)
  - tcpConnRemPort (2059)
- Seu identificador seria:

tcpConnState.89.1.1.42.21.10.0.0.51.2059

ou ainda

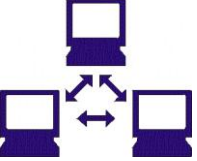
1.3.6.1.2.1.6.13.1.1.89.1.1.42.21.10.0.0.51.2059



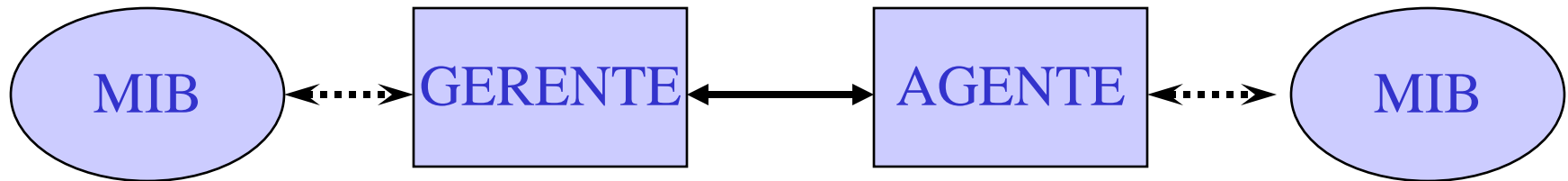


## O comando Get Next

- Permite obter a próxima instância de um objeto:
  - get-next (após ter obtido ifIndex) ↴ ifDescr.1.
- O get\_next pode ser usado para examinar se um objeto é suportado por um agente:
  - get-next (ipRouteDest) ? ipRouteDest.0.0.0.0;
  - getnext(ipRouteDest.0.0.0.0)?ipRouteDest.192.33.4.0;
  - get-next (ipRouteDest.192.33.4.0) ? ipRouteifIndex.0.0.0.0.



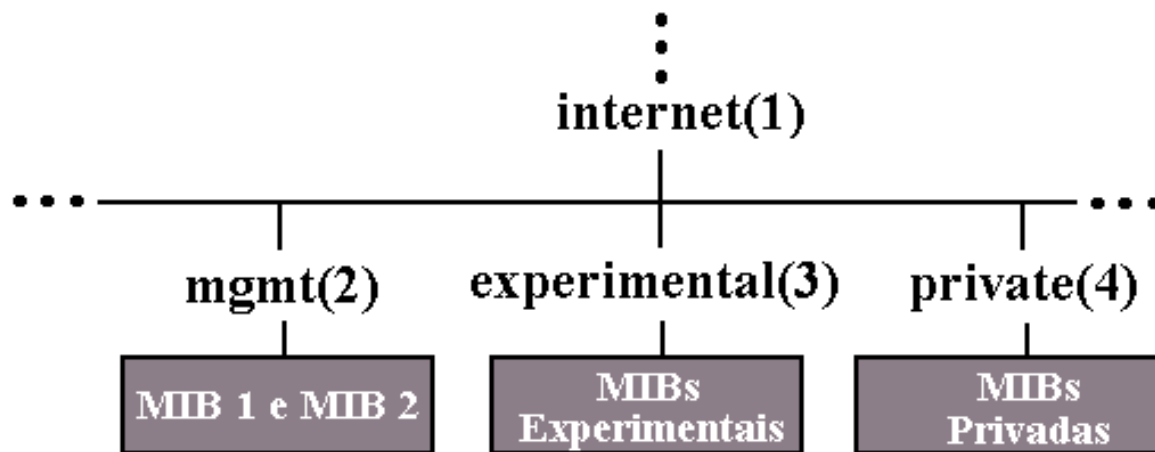
## MIB - Base de Informação de Gerência

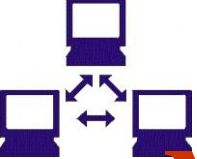




## Sub-árvore Internet

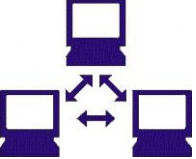
- Três nodos têm sido definidos





# Mecanismos de Extensibilidade das MIBs

- Padronização de novos objetos : MIB I  $\rightarrow$  MIB II;
- Adição de objetos largamente utilizados que não são padrão, através da sub-árvore experimental;
- Adição de objetos proprietários através da sub-árvore private;
- Navegar na MIB:
  - snmpwalk.



## Principais MIBs

- MIB I;
- MIB II;
- MIBs para gerência de LANs;
- MIBs para gerência de WANs;
- MIB RMON;
- MIB ATM.



## MIB I

- MIB I, primeira MIB da Internet, inclui o número mínimo de objetos gerenciados;
- Os objetos desta MIB constituem-se nos dados dos nodos que são tidos como gerais e essenciais ao gerenciamento.

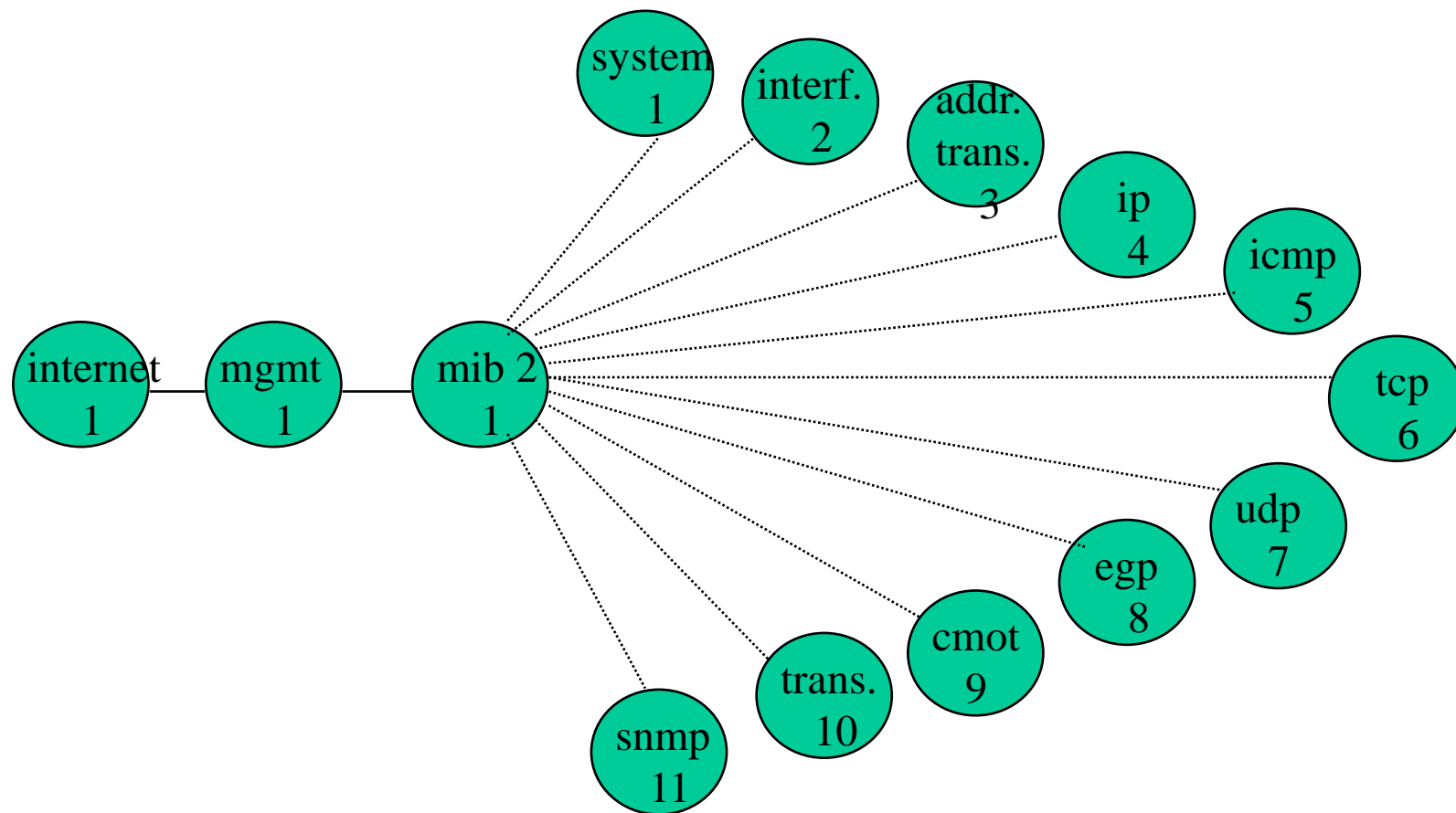


## MIB II

- A MIB II, uma extensão da MIB I, apresenta novos objetos padronizados:
  - Inclusão da tabela udp;
  - Definição de novos grupos: transmission e snmp;
  - Expansão da tabela egp.
- Mib II 50% maior que MIB I;



## MIB II: Estrutura







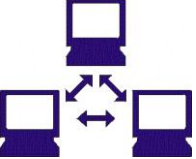
## MIB II: System Group

- Informações sobre a configuração dos sistemas:
  - Descrição do dispositivo (sysDescr);
  - Nome do dispositivo (sysName);
  - Identificação do software agente (sysObjectID);
  - Há quanto tempo o agente está no ar (sysUpTime) ;
  - Localização física do dispositivo (sysLocation).



## MIB II: Interfaces Group

- Informações sobre as interfaces:
  - Quantidade de interfaces (ifNumber);
  - Descrição da interface (ifDescr);
  - Tipo da interface (ifType);
  - Velocidade de transmissão (ifSpeed);
  - Endereço físico do meio (ifPhysAddress);
  - Contador de bytes na entrada/saída;
  - Contador de erros.



## MIB II: IP Group

- Informações sobre o subsistema IP:
  - Endereço associado ao agente (ipAddrTable);
  - Manutenção das rotas, nas tabelas de roteamento (ipRouteTable);
  - Mapeamento entre endereços IP e endereços específicos do meio (ipNettoMediaTable).



## MIB II: ICMP Group

- Dois contadores para cada tipo de mensagem:
  - Número de vezes que a mensagem foi gerada e recebida.
- Total de mensagens recebidas, enviadas, recebidas com erro e não enviadas devido a erros.



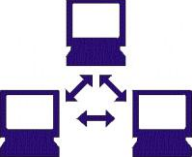
## MIB II: TCP Group

- Informações sobre:
  - Identificador do algoritmo de retransmissão (tcpRtoAlgorithm);
  - Número máximo de conexões simultâneas permitidas (tcpMaxConn);
  - Número de segmentos recebidos (tcpInSegs);
  - Número de segmentos enviados (tcpOutSegs).



## MIB II: UDP Group

- Informações sobre:
  - Datagramas destinados a portas desconhecidas (udpNoPorts);
  - Endereço IP local (udpLocalAddress);
  - Porta UDP local (udpLocalPort).



# MIB II: Transmission e SNMP Groups

- Define MIBs específicas do meio de transmissão (Transmission Group);
- Informações específicas do protocolo de gerência SNMP (SNMP Group).



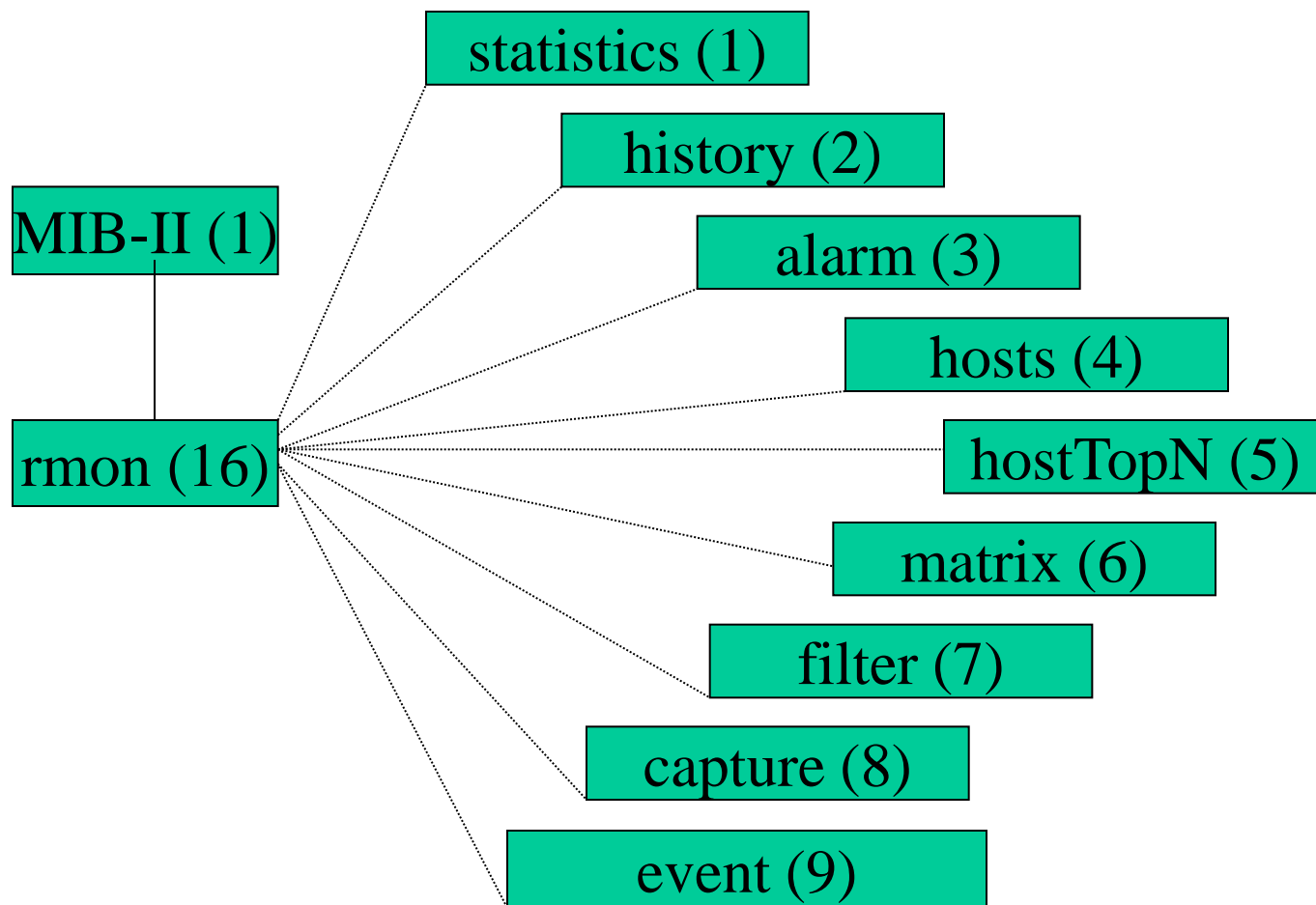
# MIB RMON (Remote MONitoring)

- Monitoração de redes locais;
- Benefícios:
  - Análise e monitoramento poderosos;
  - Histórico sobre tendências em segmentos locais;
  - Funções tradicionais de decodificação de protocolo;
  - Monitoramento centralizado de redes remotas;
  - Interoperabilidade de fornecedores;
  - Criação de eventos quando limiares são atingidos.





## MIB RMON1: Estrutura





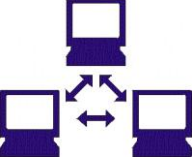
## MIB RMON1: Grupos

- Estatísticas relativas a cada uma das interfaces (Statistics Group);
- Controle de estatísticas periódicas (History Group);
- Geração de eventos, quando limiares pré-estabelecidos são atingidos (Alarm Group);
- Estatísticas sobre cada host descoberto na rede (Host Group).



## MIB RMON1: Grupos

- Descrição dos hosts que iniciam uma lista ordenada por uma de suas características (HostTopN Group);
- Estatísticas sobre “conversas” entre dois endereços hosts (Matrix Group);
- Captura de pacotes através de um filtro (Filter Group).



## MIB RMON1: Grupos

- Captura de pacotes que passaram por um canal (Packet Capture Group);
- Controle da geração e notificação de eventos (Event Group).

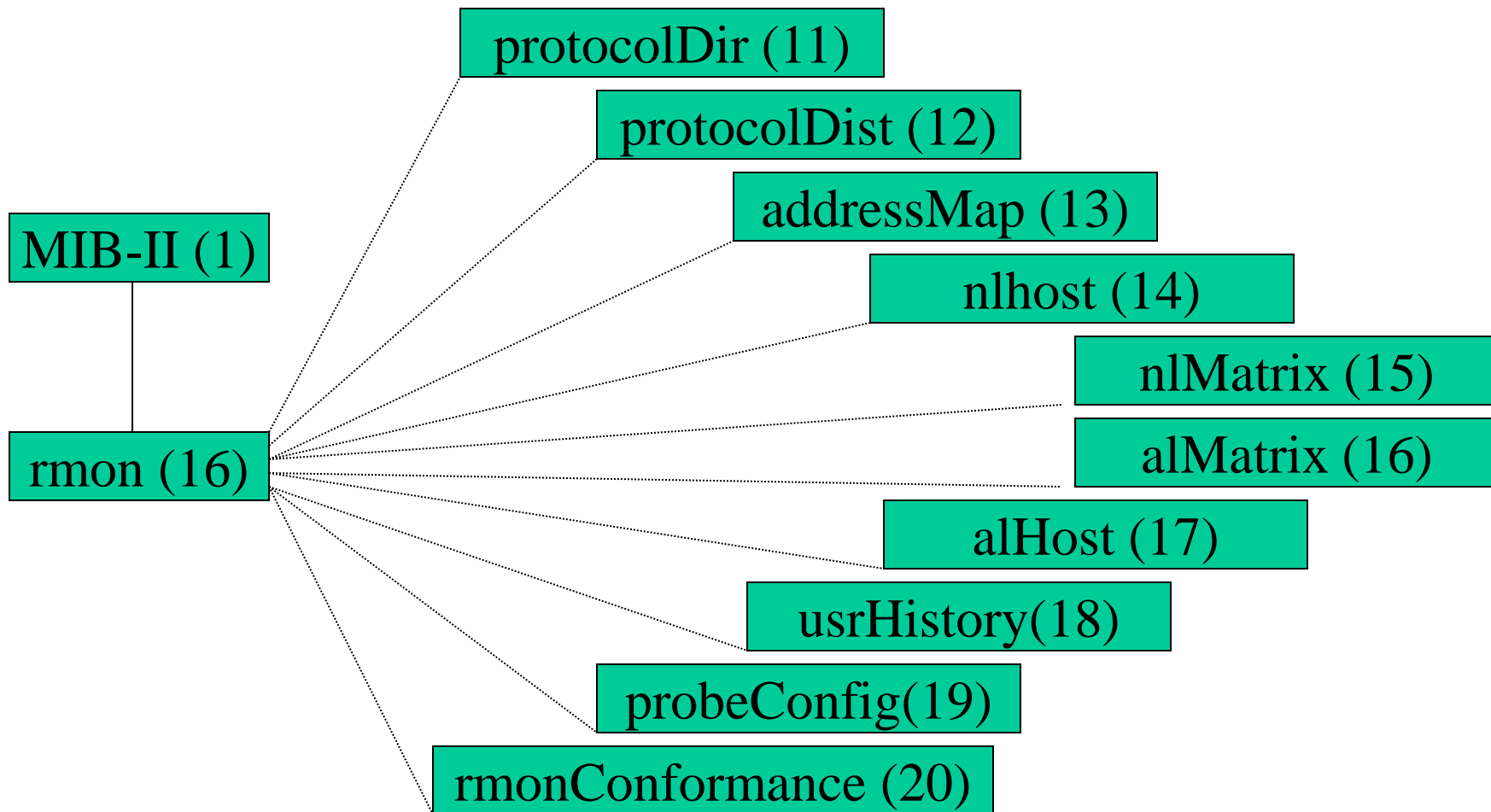


## MIB RMON2: Novidades

- Monitoramento de tráfego ampliado;
- Maior confiança no fornecedor;
- Correlação com a camada física;
- História completa.



## MIB RMON2: Estrutura





## MIB RMON2: Grupos

- Lista de protocolos que podem ser monitorados (Protocol Directory Group);
- Coleção das quantidades de pacotes dos diferentes protocolos detectados no segmento de rede (Protocol Distribution Group);
- Lista de endereços MAC relativos aos endereços de rede descobertos (Address Mapping Group).



## MIB RMON2

- Quantidade de tráfego de/para cada endereço de rede (Network Layer Host Group);
- Quantidade de tráfego entre pares de endereços de rede (Network Layer Matrix Group);
- Quantidade de tráfego, por protocolo, de/para cada endereço de rede (Application Layer Host Group).



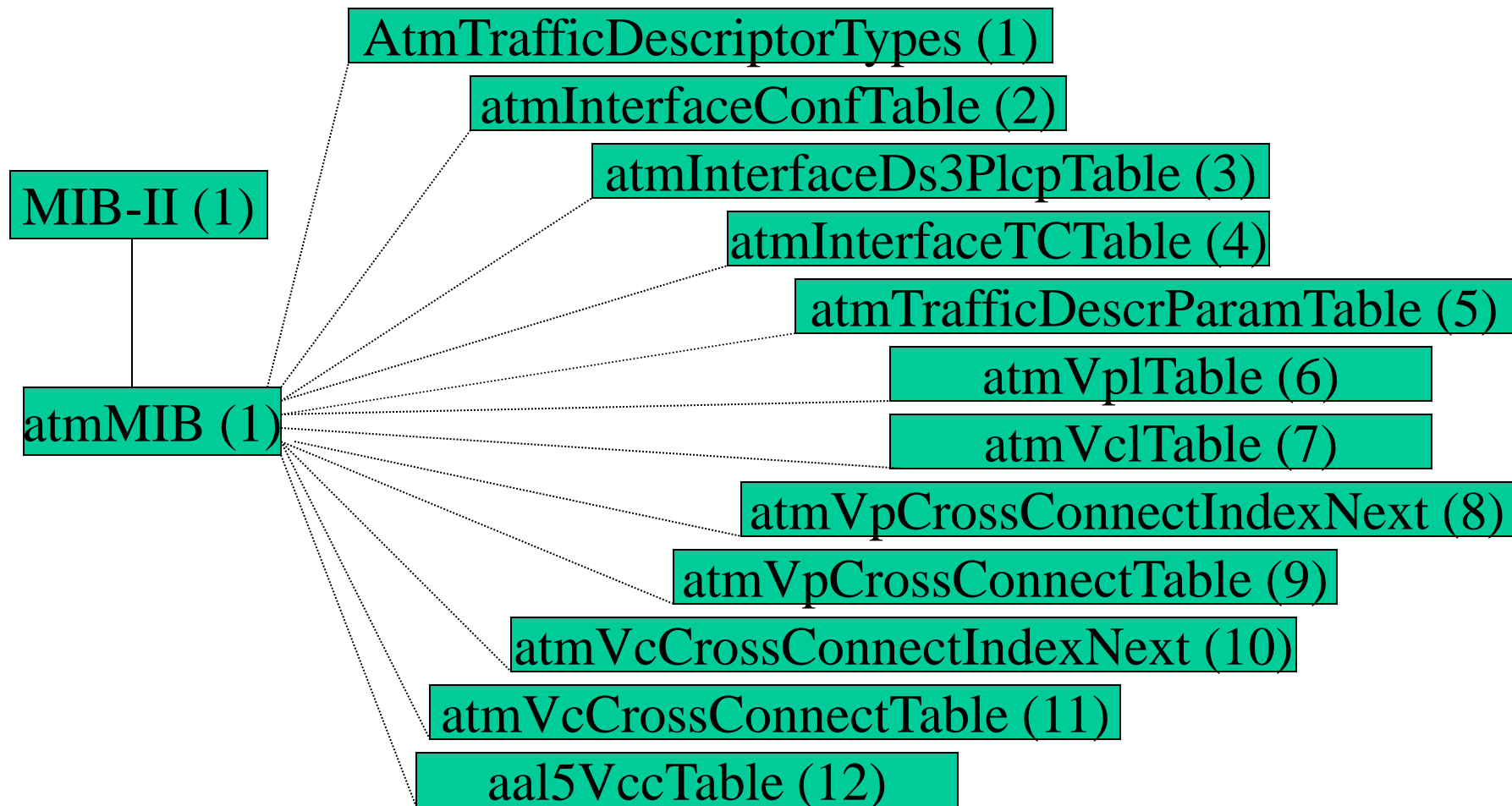


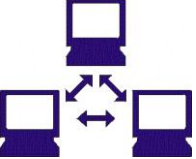
## MIB RMON2: Grupos

- Quantidade de tráfego, por protocolo, enviado entre pares de endereços de rede (Application Layer Matrix Group);
- História especificada pelo usuário (User History Group);
- Controle da configuração de parâmetros operacionais do monitor (Probe Configuration Group).



## MIB ATM (Asynchronous Transfer Mode)

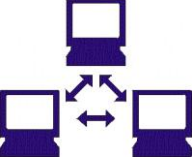




## Plataforma de Gerência

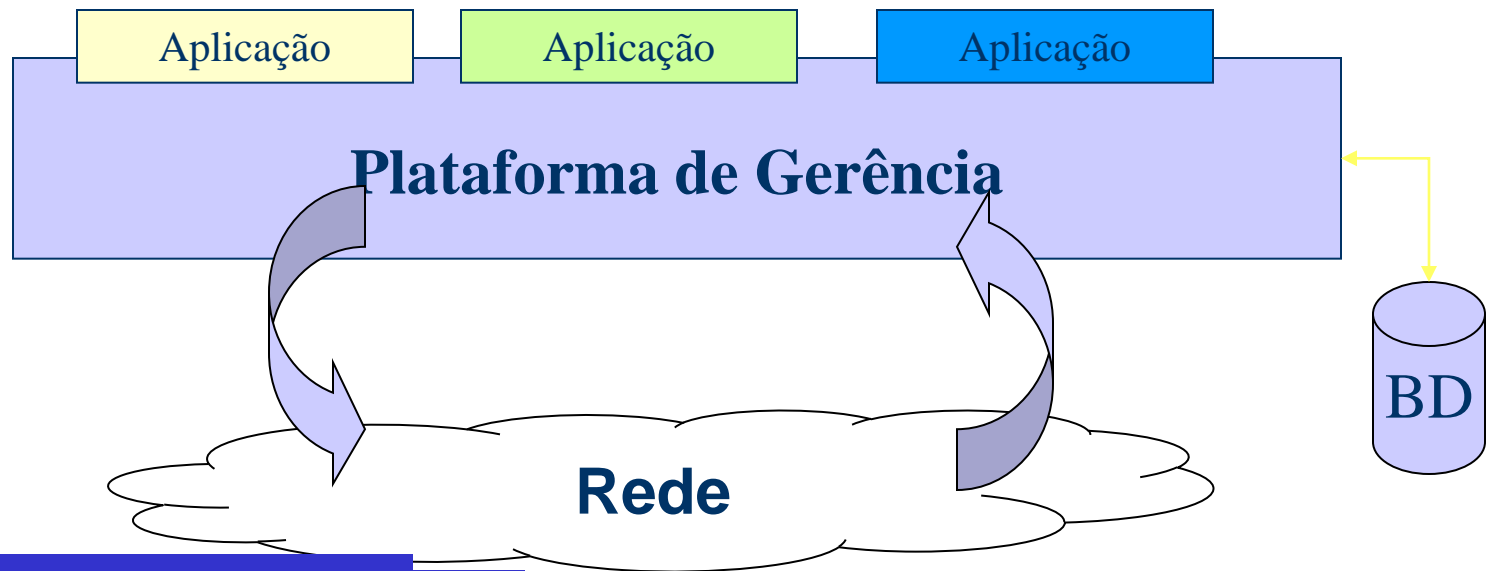
- Software no qual se baseia o gerenciamento das redes e sistemas:
  - “Sistema Operacional” da Gerência de Redes;
  - Funções básicas de gerência + Ambiente para o desenvolvimento de aplicações.





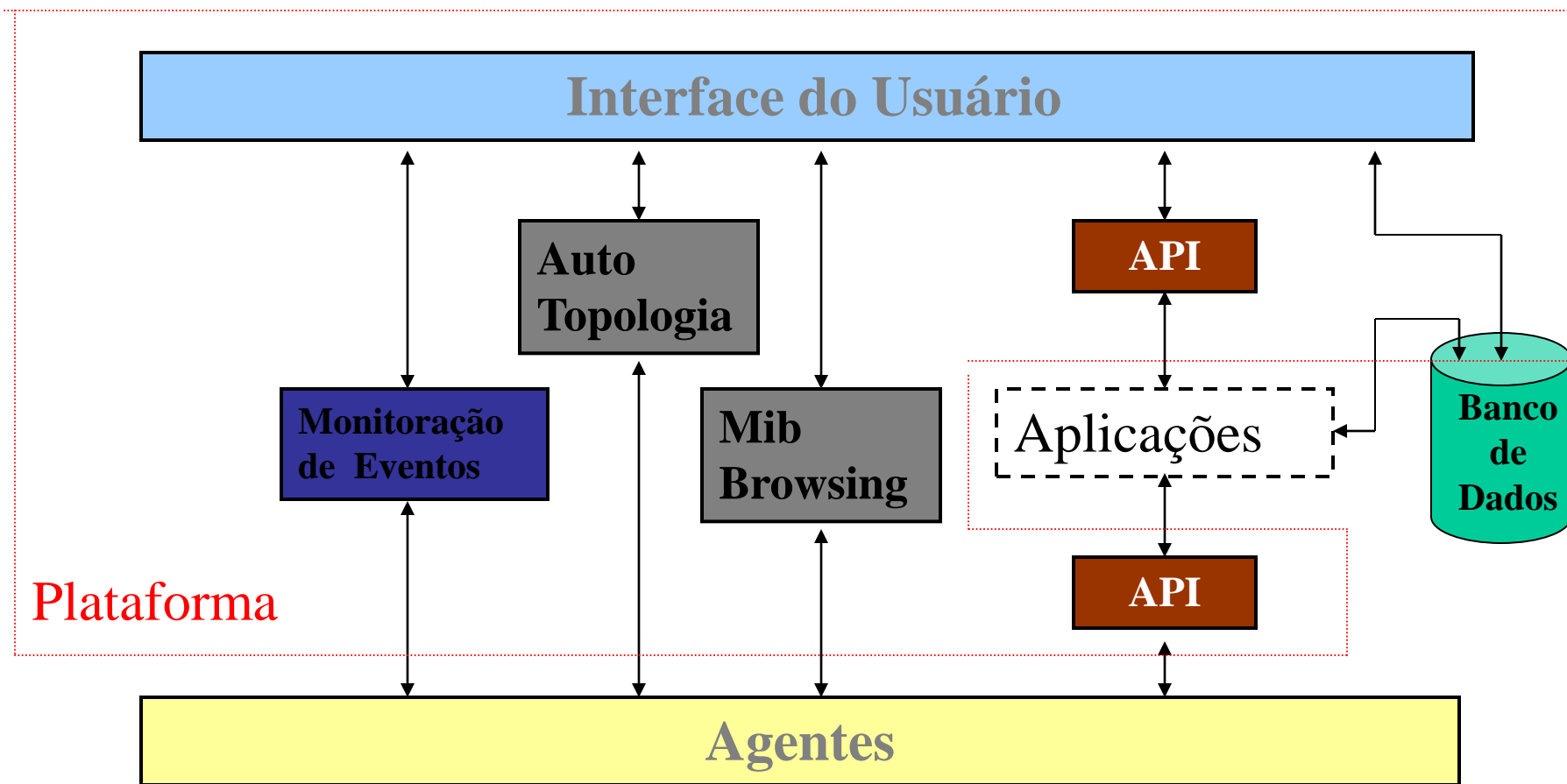
## Plataformas de Gerência

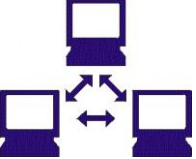
- Sobre a plataforma estão as diversas aplicações utilizadas pelos gerentes;
- A plataforma deve provê serviços básicos para as aplicações que se conectam a ela.





## Componentes de uma Plataforma





## Plataformas de Gerência

- OpenView da HP;
- SunNetManager da Sun Microsystems;
- NetView da IBM;
- Spectrum da Cabletron Corp.;
- Ca-Unicenter da Computer Associates.



## Aplicações de Gerência

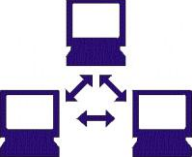
- Atendem as necessidades específicas de gerência nas suas cinco áreas:
  - **Configuração;**
  - **Faltas;**
  - **Desempenho;**
  - **Segurança;**
  - **Contabilidade.**
- Comunicam-se via protocolo de gerência;
- Normalmente ficam nas estações gerentes da rede.



# Gerência de Configuração

- Objetivos
  - Garantir a identificação apropriada da configuração da rede (hardware + software);
  - Controle e registro de mudanças.
- O gerenciamento de configuração facilita a implementação de mudanças no sistema.





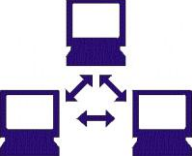
# Gerência de Configuração

- Atividades:
  - Parametrização/configuração de dispositivos;
  - Autotopologia;
  - Gerenciamento de bens;
  - Gerenciamento de configuração de software.

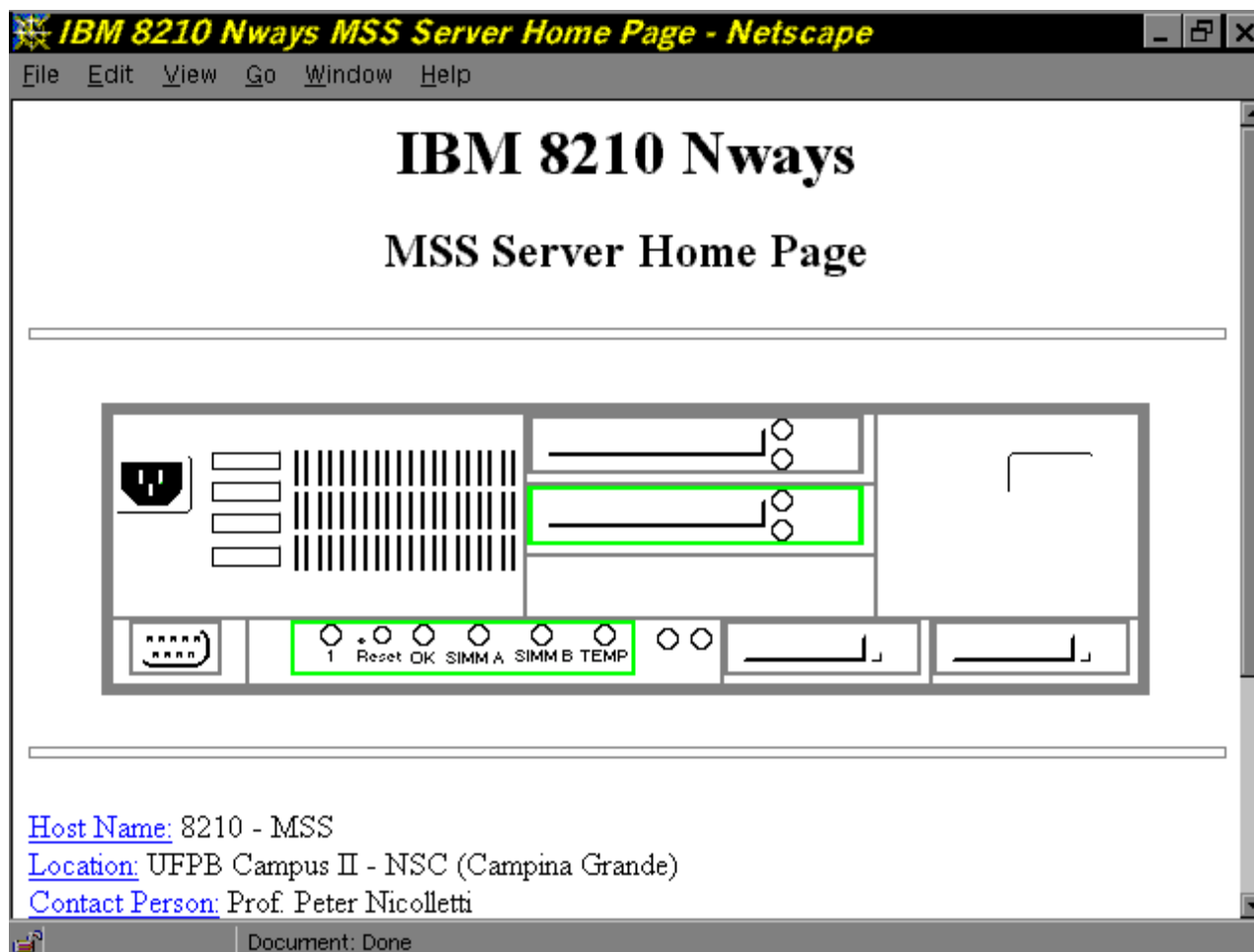


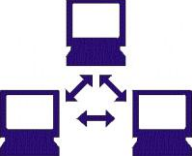
# Parametrização de Dispositivos

- Não há padronização (MIBs desenvolvidas por cada fornecedor);
- Cada fornecedor desenvolve o sistema de configuração de seus próprios dispositivos;
- Dispositivos são normalmente configurados via Telnet.

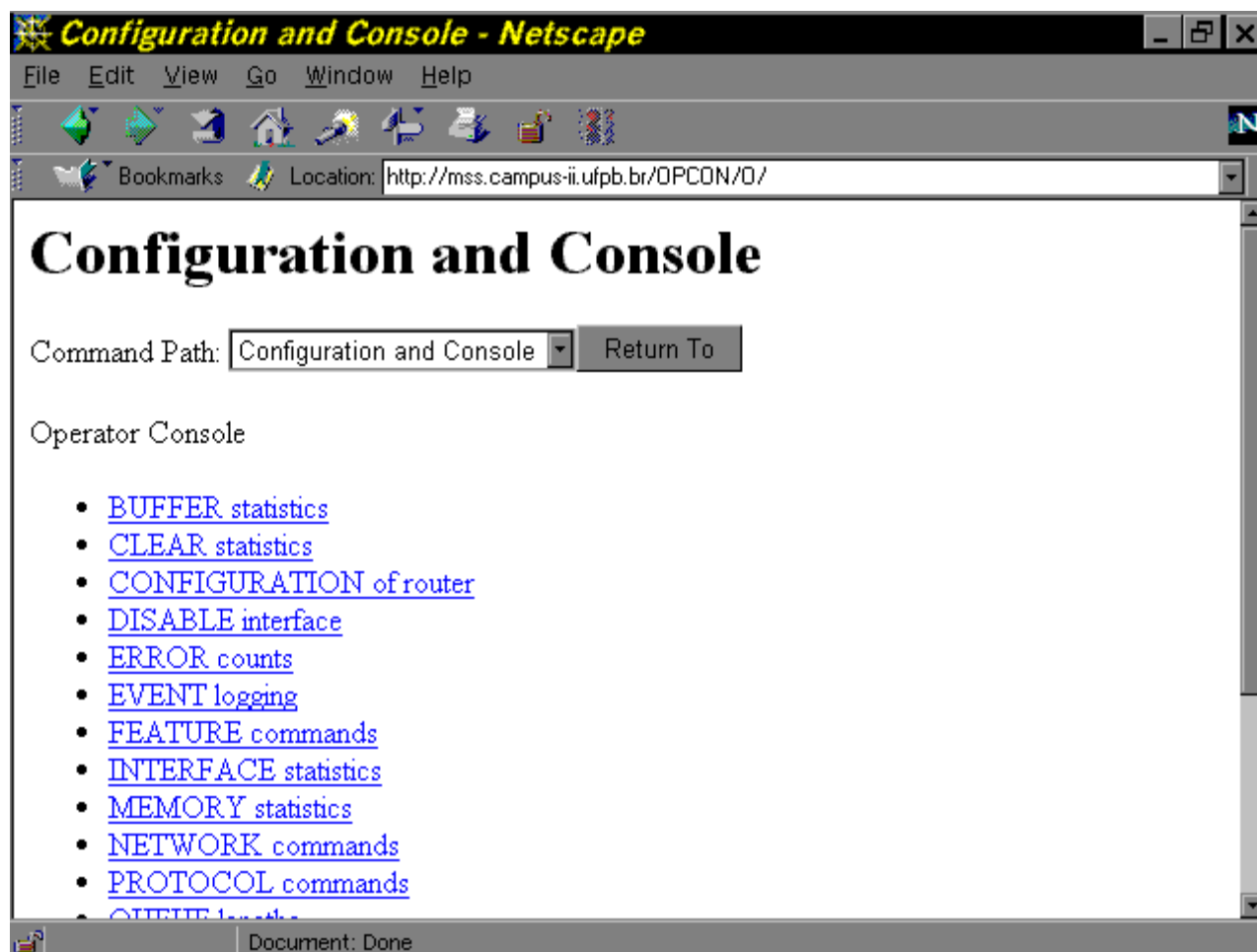


## Exemplo





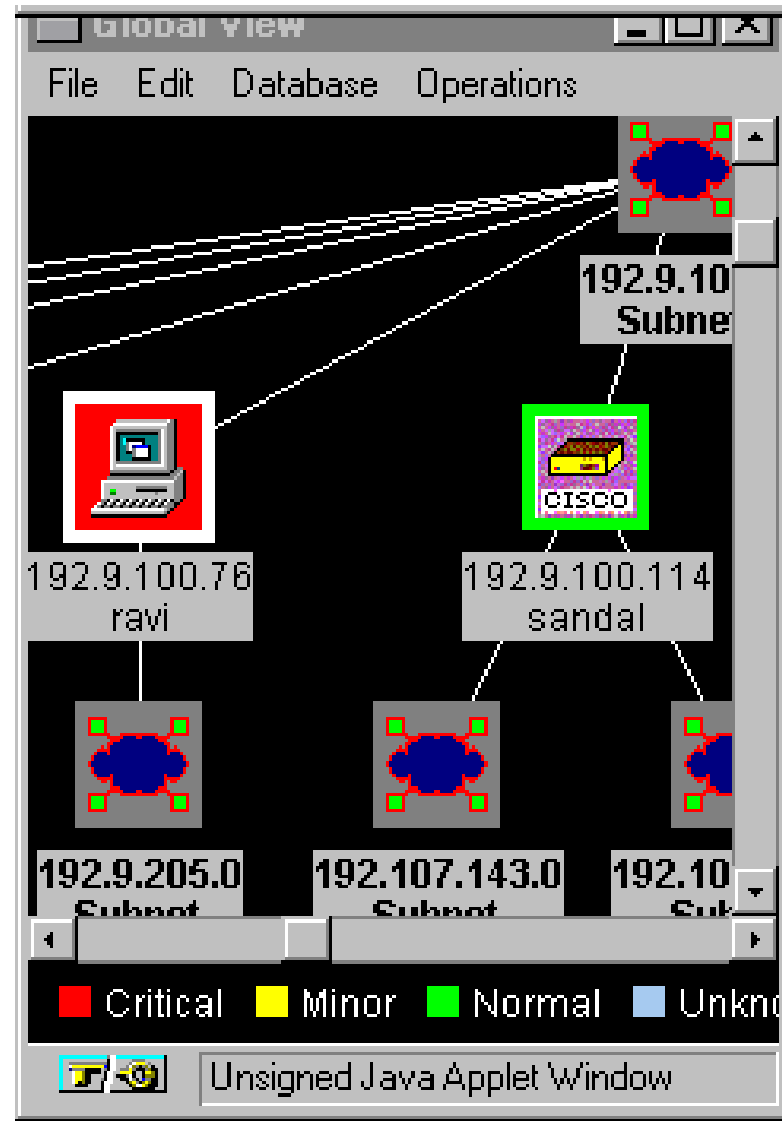
## Exemplo

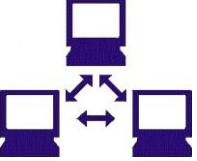




## Autotopologia

- Objetivo:
  - A aplicação deve “aprender” automaticamente a configuração da rede como um todo e mostrá-la numa forma gráfica adequada.





## Autotopologia

- Aspectos:
  - Descobrimento de dispositivos;
  - Descobrimento de topologia;
  - Geração de mapas.



## Autotopologia

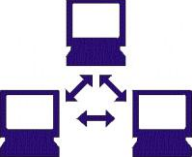
- O que descobrir? Qual o ponto de partida?
  - Endereços dentro de uma faixa de endereços;
  - Nodos “interessantes” podem ser escolhidos de acordo com critérios pré-definidos.



## Algoritmos Utilizados

- SNMP broadcast:
  - Induzirá todos os dispositivos da rede a responderem com suas identidades (endereços);
  - Quantidade de respostas produzidas pode gerar colisões;
  - Pressupõe que todos os dispositivos implementam um agente SNMP.





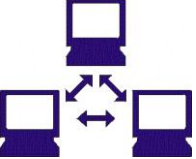
## Algoritmos Utilizados

- Envio de pacotes ICMP ECHO:
  - Envio seqüencial de uma requisição ICMP ECHO para cada possível endereço dentro de um espaço de endereços;
  - Consumo de tempo e recursos para grandes redes pode ser proibitivo.



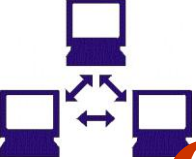
## Algoritmos Utilizados

- Uso de dispositivos RMON:
  - Descobrimento de dispositivos a partir do endereço-fonte dos pacotes que eles enviam;
  - Recuperação de uma lista de endereços descobertos/mantidos em sua base de dados;
  - Aquisição de dispositivos RMON dedicados pode ser um inconveniente.



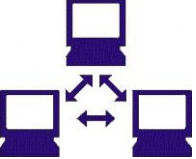
## Gerenciamento de Bens

- Objetivo:
  - Geração de inventários para um efetivo gerenciamento de bens.
- Dispositivos = bens possuídos:
  - “As coisas não podem ser gerenciadas e os custos controlados, se não há uma indicação de que eles existem”.



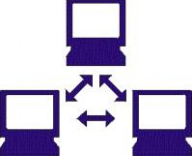
# Gerência de Configuração de Software

- Implementar controle de versões para o software instalado no sistema:
  - software “da casa” + servidores;
  - software de controle de dispositivos.
- Prover coordenação para a atualização de múltiplos produtos em uma ou mais localidades conforme necessário.



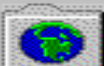

## Gerência de Falhas

- Objetivos
  - Detectar, diagnosticar e corrigir um comportamento anormal da rede
- O que é uma falta?
  - Causa do mau funcionamento de algum componente da rede (hardware ou software)












## Exemplo

**Enterprise Sites**

 [Universal](#)     [MyDomain](#)













---

**Devices in critical state within Universal:**

 <a href="#">nms-thunder-pc</a>	 <a href="#">bs301alpha1</a>	 <a href="#">192.168.4.82</a>	 <a href="#">192.168.4.53</a>
 <a href="#">192.168.4.52</a>	 <a href="#">192.168.4.51</a>	 <a href="#">134.177.234.168</a>	 <a href="#">000081446688</a>
 <a href="#">0000813A064002</a>			

---

**Devices in warning state within Universal:**

 <a href="#">nms_rain-pc</a>	 <a href="#">3959787</a>	 <a href="#">1941369</a>	 <a href="#">192.168.4.60</a>
 <a href="#">192.168.4.201</a>	 <a href="#">1905491</a>	 <a href="#">1506016</a>	 <a href="#">134.177.234.54</a>
 <a href="#">134.177.234.165</a>	 <a href="#">134.177.234.160</a>	 <a href="#">0000812eb9e8</a>	 <a href="#">000081263060</a>

---


**Devices in caution state within Universal:**

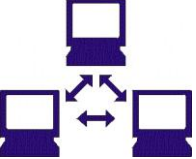


## Manipulação de Alarmes

### Active Alarm List

#### Payroll Department

Log Number	<a href="#">1001</a> 				
Time Reported	Aug 15 1996 9:33PM	Priority	5 (High)	Status	Active
Reported by	PayCalc	Problem	Unacceptable Network Response		
Log Number	0450				
Time Reported	Aug 15 1996 8:33PM	Priority	1 (Low)	Status	Warning
Reported by	PayCalc	Problem	Poor Data Base Response		
Log Number	0350				
Time Reported	Aug 15 1996 7:45PM	Priority	1 (Low)	Status	Warning
Reported by	PayCalc	Problem	Poor Network Response		



# Repasse de Alarmes

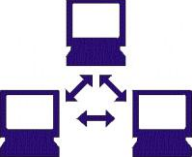
- Todos os alarmes gerados são enviados para um manipulador de alarmes;
- O manipulador de alarmes possibilita o repasse de alarmes para outras estações/aplicações;
- Útil quando os dispositivos geradores de alarmes só conseguem enviar tais mensagens para um número limitado de gerentes/aplicações.





## Filtragem de Alarmes

- Alarmes podem ser filtrados de diferentes formas (através do endereço IP origem e tipos de mensagens, por exemplo);
- Quando uma condição de filtragem é satisfeita, várias ações podem ser tomadas:
  - registro de ocorrência do alarme num arquivo de log;
  - repasse da mensagem para outro host;
  - execução de um programa local para processar o alarme.



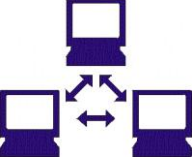
# Correlação de Eventos

- Método utilizado para automatizar a identificação de faltas;
- Interpretação de múltiplos eventos como uma unidade;
- Reduz a quantidade de informação apresentada aos usuários (gerentes da rede).



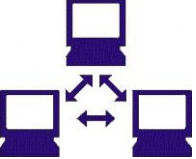
# Gerência de Desempenho

- Objetivos:
  - Coletar dados sobre o estado operacional da rede;
  - Controlar e analisar o tempo de resposta;
  - Avaliar a qualidade dos serviços oferecidos;
  - Identificar possíveis gargalos na rede;
  - Manter dados sobre o desempenho da rede em estados passados (history data).



## Gerência de Desempenho

- Aspectos:
  - Monitoração da rede;
  - Planejamento de capacidade.



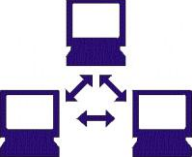
## Monitoração da Rede

- Processo através do qual se obtém informação sobre o estado da rede;
- Quem faz?



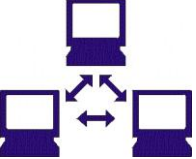
# Monitoração da Rede: Quem Faz?

- Frequentemente, é feita pelo gerente;
- O agente também pode, automaticamente, monitorar condições de exceção:
  - Elimina a necessidade de pollings constantes realizados pelo gerente;
  - Se uma exceção ocorreu o agente envia um alarme para o gerente.



## Monitoração da Rede

- Tipos:
  - Monitoração temporal (time-driven monitoring);
  - Monitoração causal (event-driven monitoring).



# Planejamento de Capacidade

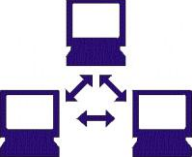
- Objetivos:
  - Conhecer utilização efetiva da rede;
  - Determinar futuros requisitos de recursos.





# Planejamento de Capacidade

- Analisar o impacto causado pela adição de novos usuários e/ou aplicações;
  - Identificar a carga adicional imposta.
- Avaliar quedas de desempenho;
- Identificar picos de utilização dos recursos da rede.



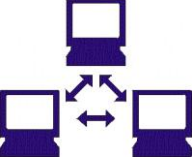
# Planejamento de Capacidade

- Benefícios:
  - Aumentar a disponibilidade da rede;
  - Reduzir custos;
  - Melhorar a infra-estrutura da rede para suportar necessidade atuais e futuras;
  - Aumentar satisfação do usuário;
  - Pró-ativamente gerenciar a rede no sentido de obter um desempenho ótimo.



# Gerência de Segurança

- Questões:
  - A mensagem foi corrompida ou alterada?
  - Quem requisitou a realização da operação?
  - Quais objetos são acessados nesta operação?
  - Quais são os direitos que o requisitante tem sobre os objetos manipulados durante a operação?



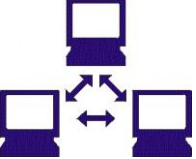
# Gerenciamento de Segurança

- Objetivos:
  - Controlar o acesso aos recursos da rede através do uso de técnicas de autenticação e políticas de autorização;
  - Prover identificação, autenticidade, integridade, privacidade, auditoria e replay protection.



# Identificação e Autenticação

- Identificação
  - Consiste em prover algum tipo de mecanismo para possibilitar a identificação do usuário:
    - o método userID/senha utilizado nos programas de login;
- Autenticação:
  - Garantia de que o usuário identificado é realmente o usuário identificado - autenticação da origem.



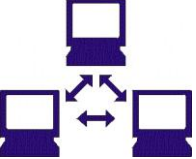
# Autorização e Integridade

- Autorização:
  - Identificação do conjunto de direitos de acesso pertinentes ao usuário;
- Integridade:
  - Garantia da incorruptibilidade dos dados enviados.



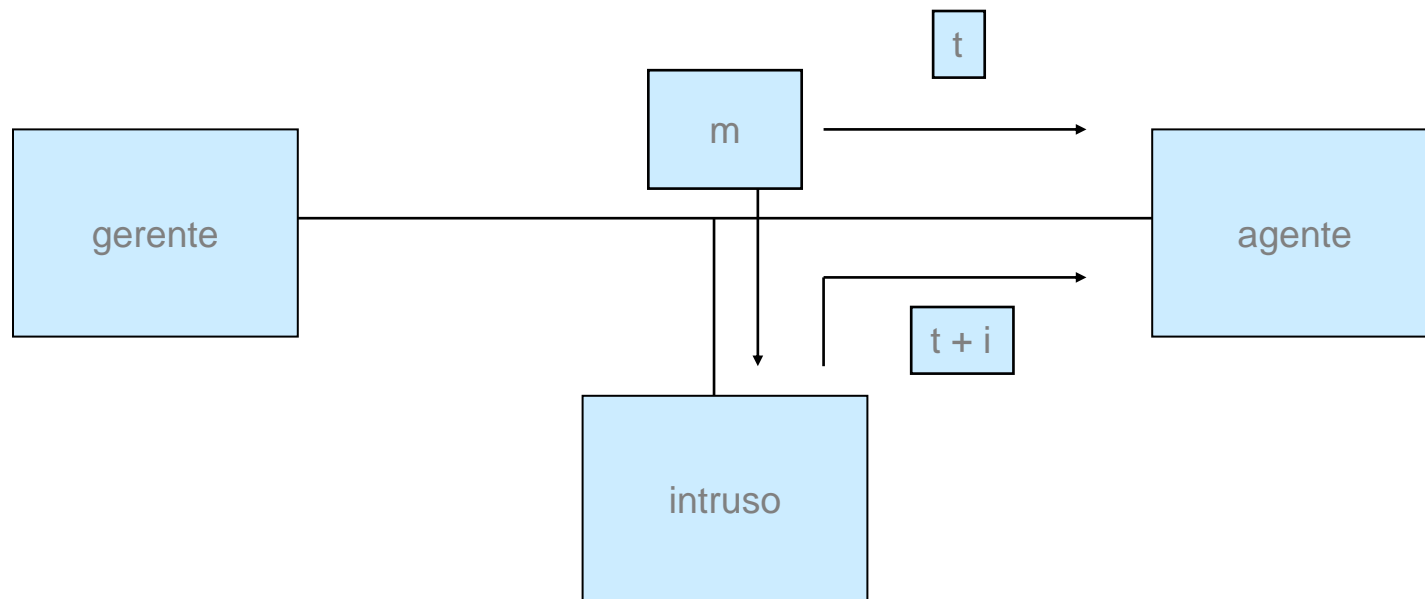
# Privacidade e Auditoria

- Privacidade:
  - Garantia de que os dados enviados não serão acessíveis a pessoas não-autorizadas.
- Auditoria:
  - Prover informação para detecção de violações de segurança do sistema;
  - Eventos relevantes podem ser configurados.

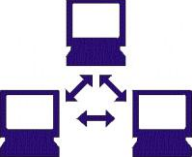


## Replay Protection

- Cenário de problema (e agora???)







# Replay Protection

- Solução => replay protection:
  - gerar timestamps para limitar o tempo de validade das mensagens enviadas na rede;
  - evitar que uma mensagem possa ser processada qualquer tempo depois do seu envio original.



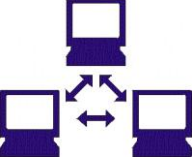
# Funcionalidades de Soluções Disponíveis

- Geração de logs de segurança. Esta informação é configurável;
- Blacklistings:
  - Negação automática de acesso quando consecutivas tentativas de login falham.



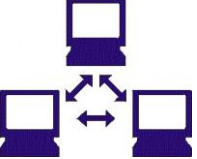
# Gerência de Contabilidade

- Objetivo:
  - Coletar e processar dados relacionados ao consumo de recursos da rede:
    - blocos de discos utilizados;
    - número de páginas impressas;
    - utilização de CPU;
    - tráfego da rede em dado instante.



# Funcionalidade de Soluções Disponíveis

- Ajuste dinâmico de taxas de uso;
- Análise de tendência:
  - Determinar crescimento de taxas de utilização e projetar atualizações do sistema mais eficientemente.



## Solução de gerenciamento atual...





# Qualidade das Aplicações

- Desenvolvedores de aplicações são reféns dos:
  - Fabricantes de dispositivos de rede;
  - Desenvolvedores de Plataforma de Gerência.
- Os esforços deveriam ser direcionados para prover mais “inteligência” aos produtos.



# Escalabilidade e Mobilidade

- Todo o processamento da gerência é feito na NMS, logo por imposições de HW e SW há limites quanto ao n° de objetos gerenciados;
- O Gerente pode ‘atuar na rede’ fora da NMS? Nem pensar:
  - Mobilidade não existe no paradigma tradicional de gerência.



## Segurança

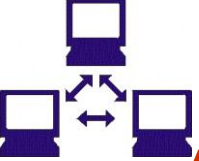
- O SNMP v.1 e v.2 não oferece segurança:
  - Há apenas uma senha, o community name, que valida os usuários para funções de gerência.
- Ao invés do comando Set do SNMP, usa-se Telnet (Backdoor) para configurar os dispositivos.





## Custos

- Plataformas de gerência são caríssimas;
- O Hardware necessário para suportá-las também é caro;
- Há ainda custos com treinamento e software de terceiros;
- Resultado:
  - Empresas de pequeno ou médio capital ficam de fora das soluções de gerência:
    - Utilizam a técnica da porta aberta e comandos como Ping e Traceroute para ajudá-los nesta tarefa



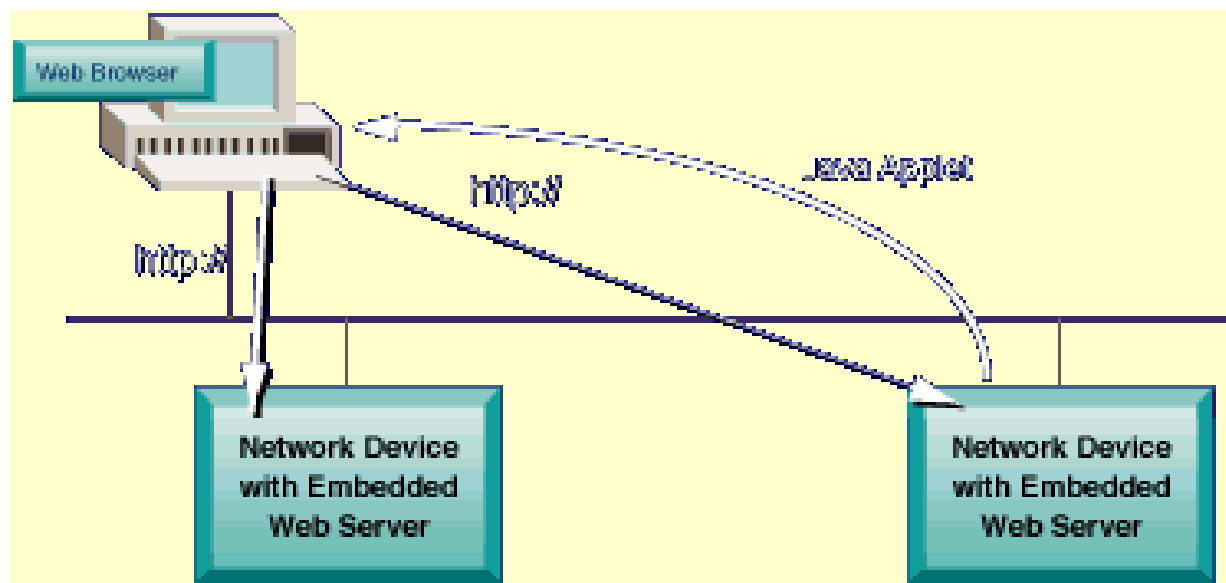
# Arquiteturas de Gerência baseadas em WEB

- Modelo 2 Camadas
  - Modelo 3 Camadas
- Já no mercado*
- WBEM
  - JMAPI
- Padrões emergentes*



## Modelo 2 Camadas

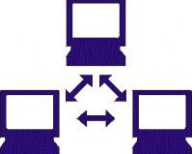
- Servidor Web embutido em cada dispositivo
  - Cada dispositivo conta com sua própria URL



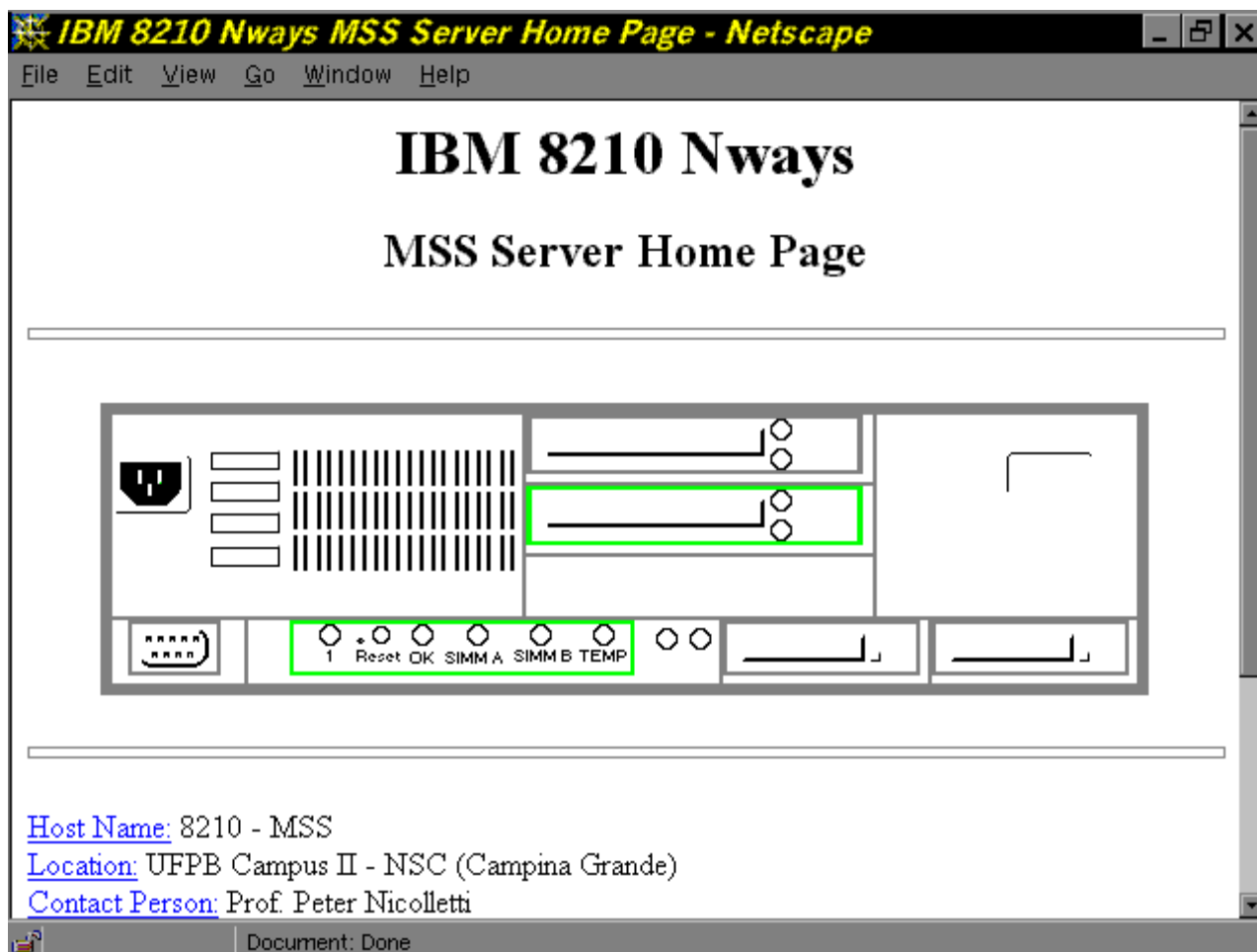


## Modelo 2 Camadas

- Dispositivos com Dual Stack ( SNMP e HTTP) já são comuns no mercado:
  - Configuração e monitoração mais amigáveis;
  - Aplicações embutidas passam a ser um diferencial  $\Rightarrow$  +qualidade ; + escala  $\Rightarrow$  - custos.
- Não provê uma visão geral e integrada (big picture) do ambiente gerenciado:
  - Como única solução de gerência é indicado apenas para pequenas redes.



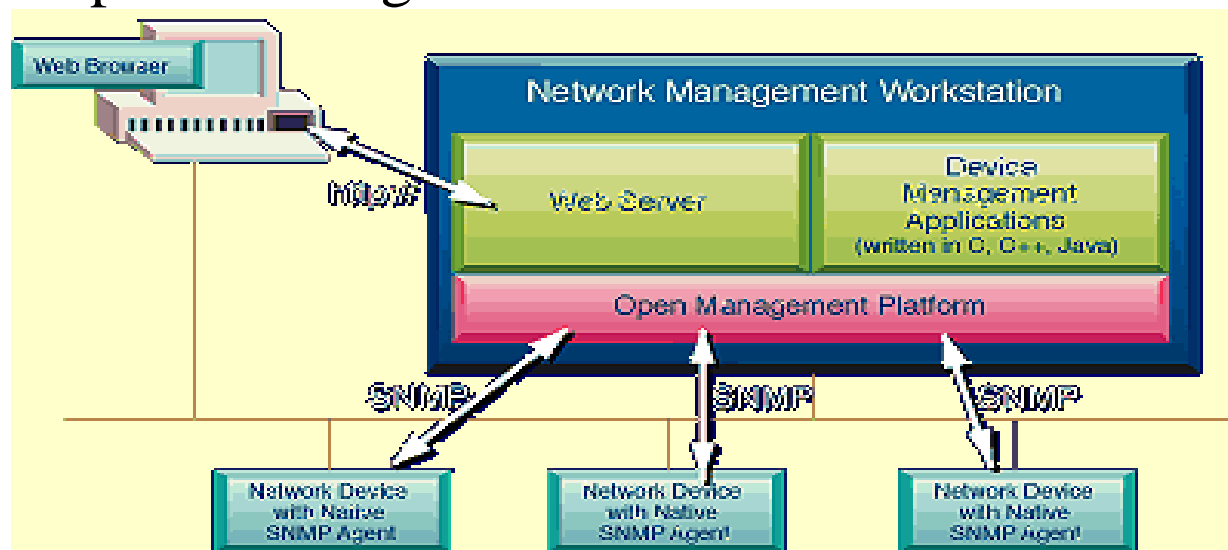
## Exemplo





## Modelo 3 Camadas

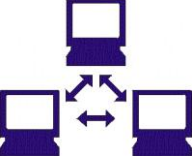
- Estação intermediária (Proxy) que se comunica com os dispositivos de rede em SNMP e com o Browser em HTTP
  - Geralmente adiciona-se um Servidor WEB a um produto de gerência



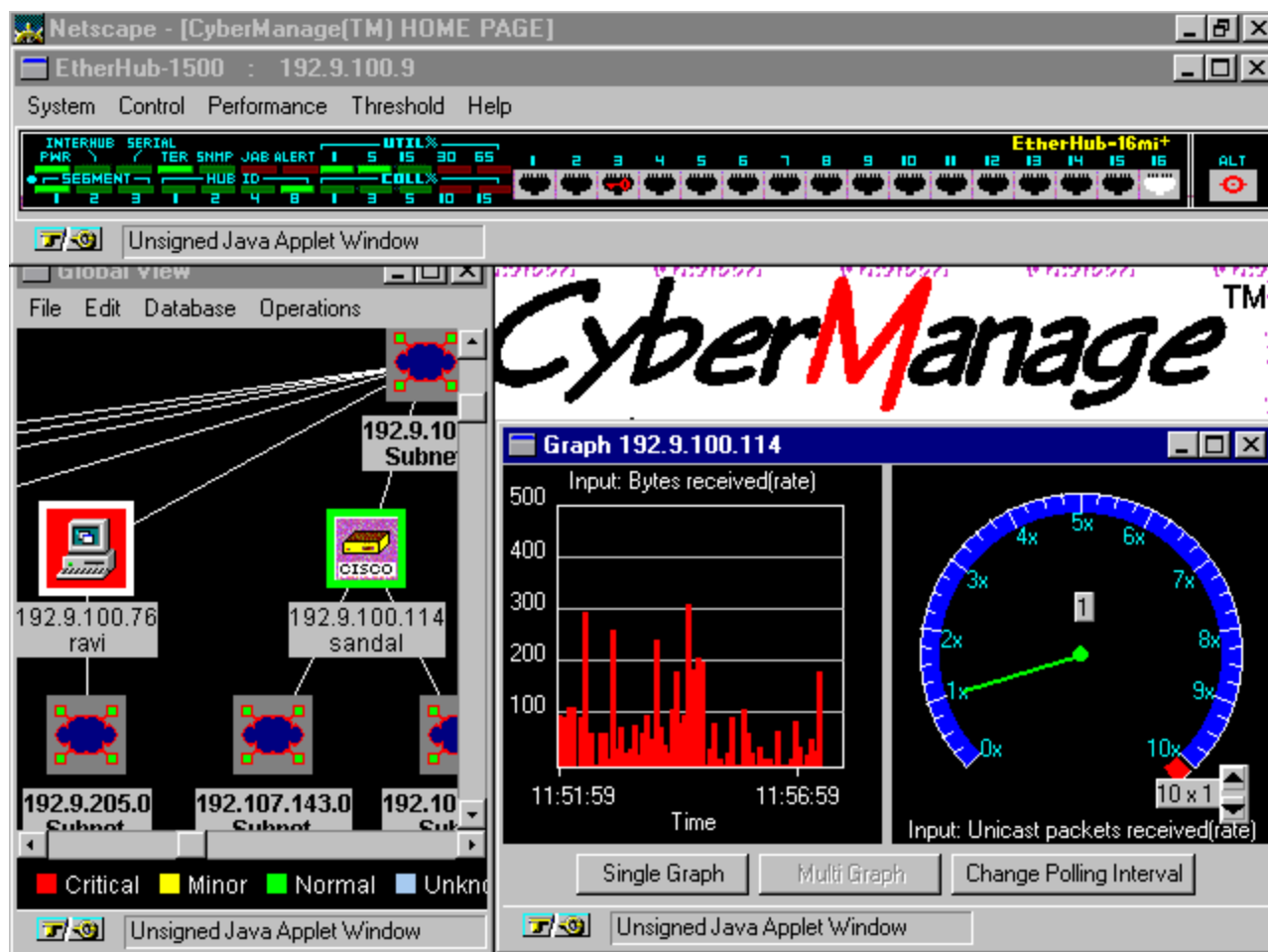


## Modelo 3 Camadas

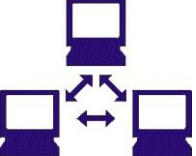
- Browser resolve os problemas de mobilidade e de usabilidade;
- Provê Big Picture do ambiente gerenciado;
- Preserva toda a base instalada em SNMP:
  - Até que novos padrões se firmem, parece ser a solução mais adequada.



## Exemplo







## Exemplo

### Statistics of: Internet Access

Updated on: Fri, Jul 17 1998 20:00

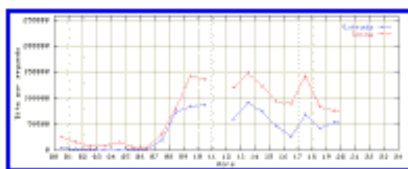
Update Status

Hardware: Cisco 7206: Serial line 2, port 0

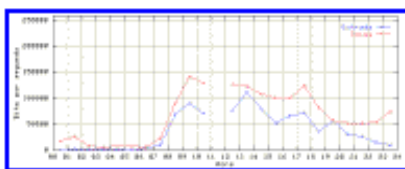
Operational Status: ●

Alarms: None

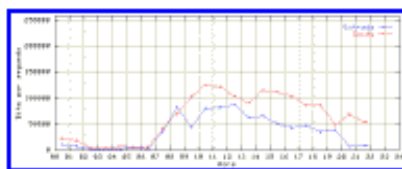
#### Input/Output Bandwidth



Fri Jul 17 1998

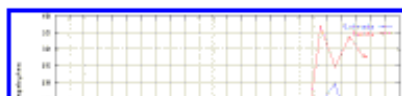
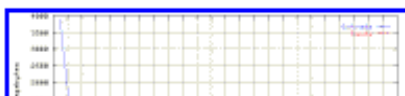
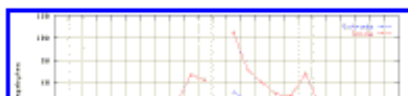


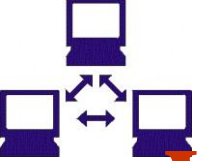
Thu Jul 16 1998



Wed Jul 15 1998

#### Input/Output Errors





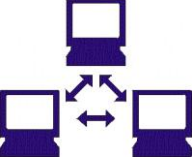
# WBEM - Web-Based Enterprise Management

- Consórcio de fabricantes (Microsoft, Cisco, 3Com, Intel e BMC Software);
- Criar padrões de gerência baseada em Web para toda a empresa:
  - rede;
  - aplicações;
  - sistemas.



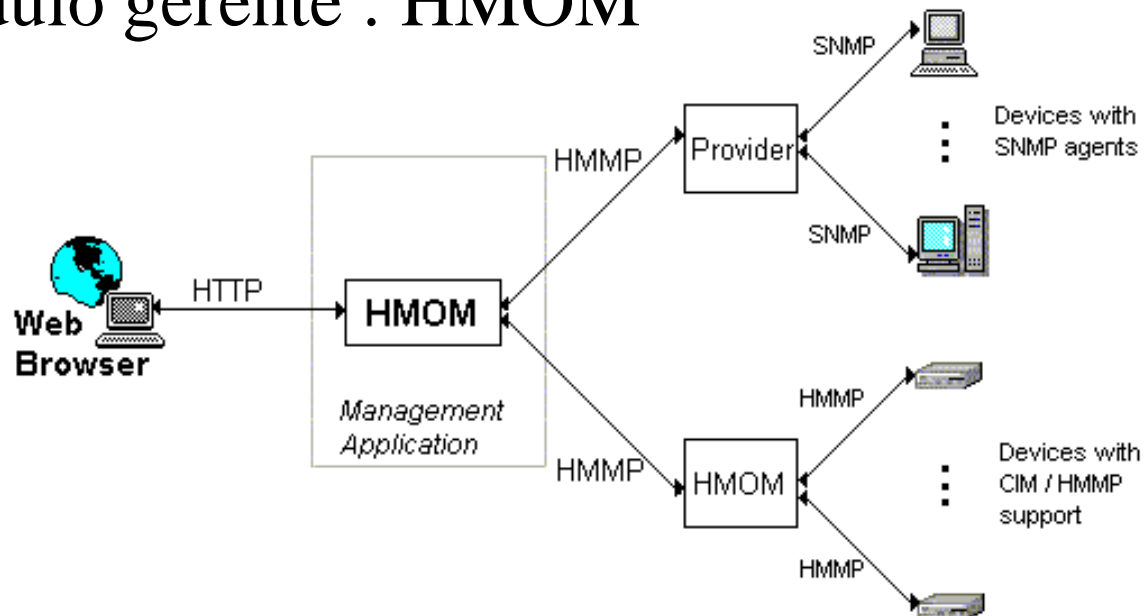
# Arquitetura WBEM

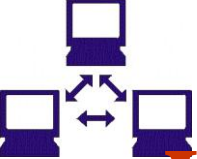
- É composta de:
  - CIM (Common Information Model) - modelo de dados OO já aprovado pelo DMTF;
  - HMMP (HyperMedia Management Protocol) - protocolo criado para atuar sobre os objetos no CIM (em fase de padronização pelo DMTF);
  - HMOM (HyperMedia Object Manager) - módulo gerente responsável por consolidar dados de gerência vindos de diferentes fontes.



## Arquitetura WBEM

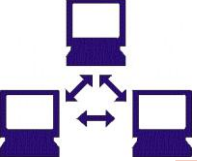
- Interface : Browser
- Comunicação : Protocolo HMMP
- Modelo de Dados : CIM
- Módulo gerente : HMOM





## WBEM

- É uma iniciativa ambiciosa;
- Redesenha todo o panorama de gerência de redes, desde o modelo de dados até o protocolo usado:
  - Lentidão na sua real padronização.



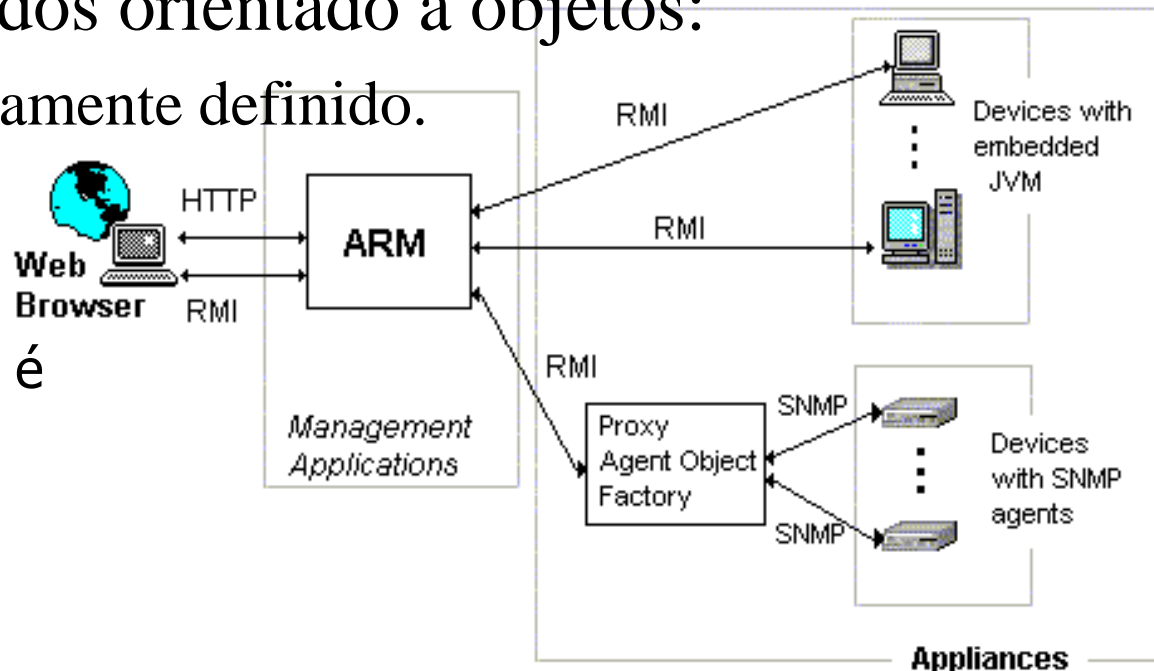
# JMAPI - Java Management Application Programming Interface

- É um conjunto de objetos, métodos e classes Java para o desenvolvimento de soluções de gerência num ambiente heterogêneo;
- Objetivos
  - Melhorar a integração de aplicações de gerência de redes e sistemas;
  - Fornecer soluções independentes de ambiente operacional.

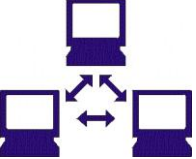


## JMAPI - Arquitetura

- Interface via browser Web;
- Comunicação via RMI;
- Modelo de dados orientado a objetos:
  - Não completamente definido.



Hierarquia de ARMs não é prevista na arquitetura (menos escalabilidade).



## JMAPI

- Consistência de estilo, interfaces e até funcionalidades entre as aplicações;
- Preserva a base instalada em SNMP.





## WBEM x JMAPI

- Os especialistas na área dividem-se;
- Algumas empresas apoiam as duas iniciativas (Cisco e 3com);
- Uma coisa parece ser consenso, há espaço para um mix de tecnologias e o mercado irá decidir o padrão para gerência de facto.



## E o SNMP?

- O SNMP possui um legado muito grande e ainda é uma boa alternativa para buscar dados de gerência;
- Além disso, ainda falta muito para as outras alternativas alcançarem o seu sucesso e por isso todas as abordagens WBM fornecem suporte a ele.