



# Redes de Computadores

# Comparação entre as Topologias

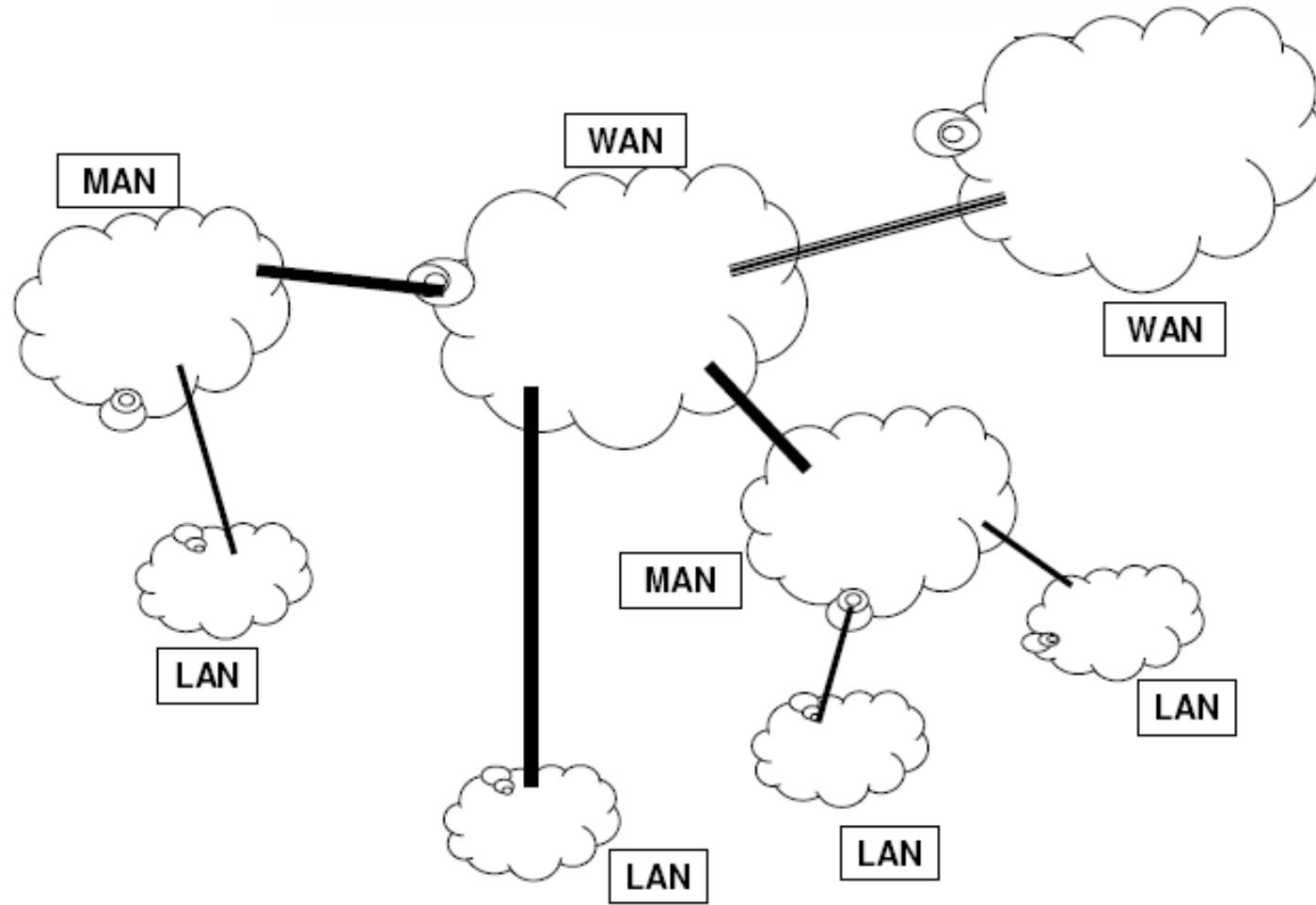
<b><i>Topologia</i></b>	<b><i>Ponto Positivos</i></b>	<b><i>Pontos Negativos</i></b>
Estrela	<ul style="list-style-type: none"><li>- Maior tolerância a falhas</li><li>- Facilidade de instalação</li><li>- Monitoramento centralizado</li></ul>	<ul style="list-style-type: none"><li>- Custo de instalação maior porque requer mais cabos</li></ul>
Anel	<ul style="list-style-type: none"><li>- Facilidade de instalação razoável</li><li>- Requer poucos cabos</li><li>- Desempenho uniforme</li></ul>	<ul style="list-style-type: none"><li>- Se uma estação parar, todas as outras param</li><li>- Dificuldade para a identificação de problemas</li></ul>
Barramento	<ul style="list-style-type: none"><li>- Facilidade de instalação razoável</li><li>- Requer poucos cabos</li><li>- Facilidade de compreensão das ligações</li></ul>	<ul style="list-style-type: none"><li>- Lentidão em períodos de uso intenso</li><li>- Dificuldade para a identificação de problemas</li><li>- Possibilidade de colisão</li></ul>

# Área de Abrangência

# Área de Abrangência

- **LAN** (Local Area Network): Pequeno número de computadores em áreas restritas (pequenas distâncias entre eles) *Redes Locais*
- **MAN** (Metropolitan Area Network): Médio número de computadores em áreas de grande porte (cidades) *Redes Metropolitanas*
- **WAN** (Wide Area Network): Grande número de computadores em áreas envolvendo várias cidades e/ou países *Redes de Amplo Alcance*

# Área de Abrangência



# **Redes Cliente Servidor**

# **Redes Ponto a Ponto**

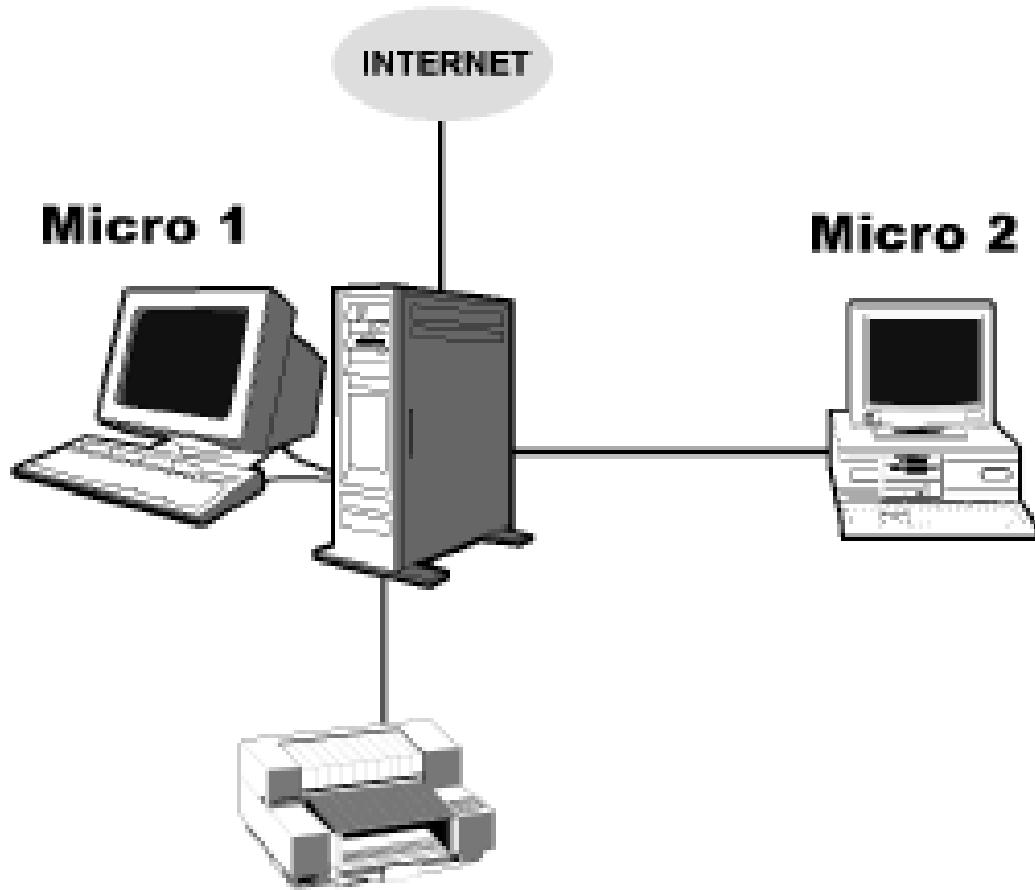
# O que são Servidores?

- São computadores ou equipamentos que disponibilizam seus recursos para outros computadores
- Exemplos:
  - ***Servidor de arquivos:*** seus discos rígidos podem ser acessados por outros computadores
  - ***Servidor de impressão:*** suas impressoras e/ou plotters podem ser usados por outros computadores
  - ***Servidor de “backup”:*** suas unidades de fita magnética, discos ópticos ou outros dispositivos de armazenamento podem ser usados por outros computadores

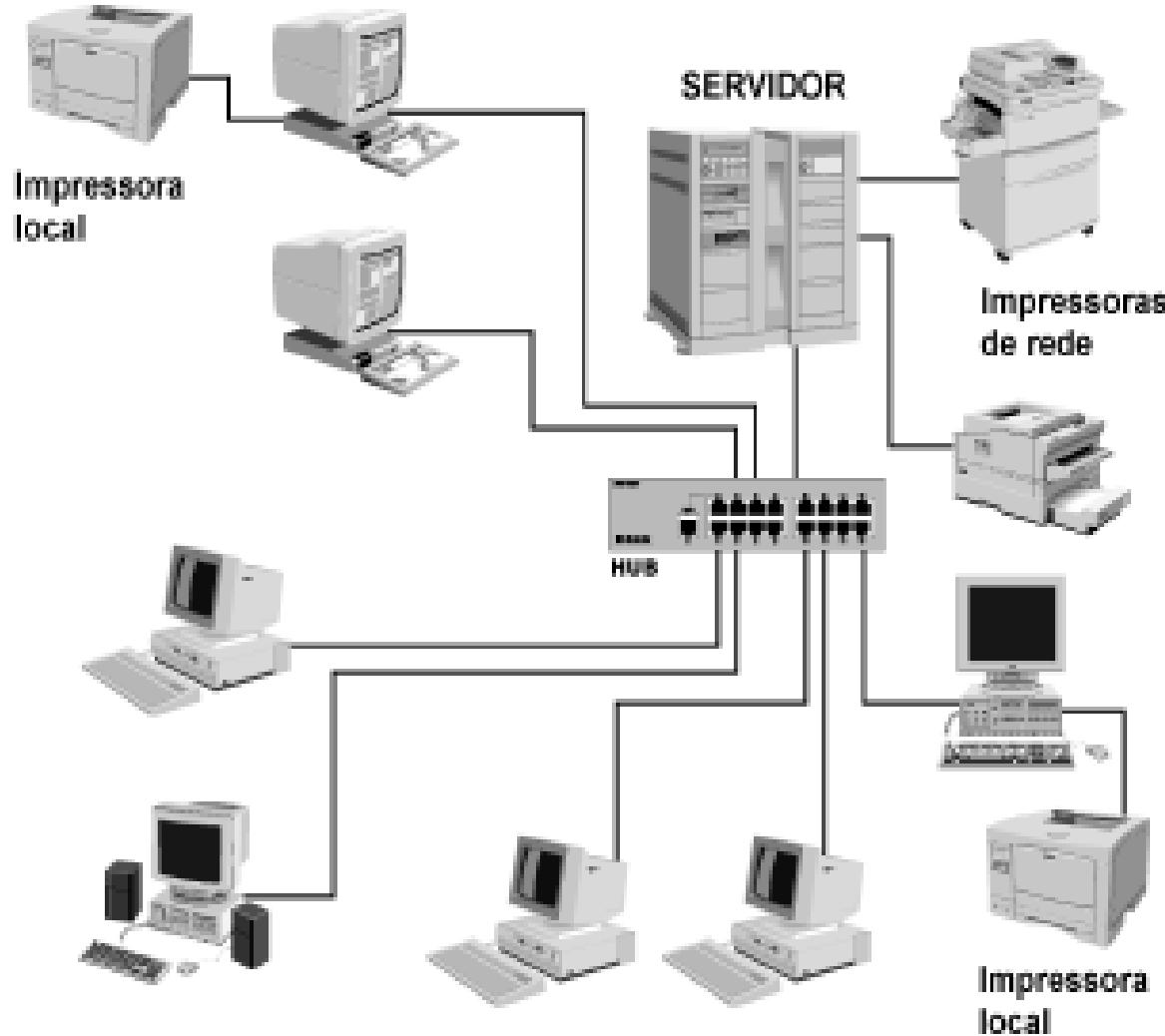
# O que são computadores Clientes?

- São os computadores que usam os recursos dos servidores
- Também podem ser chamados em alguns casos de “estações de trabalho”
- Tipos de operação
  - Somente como cliente
  - Cliente e Servidor simultâneos (servidor não dedicado) comum em redes pequenas

# Servidor Não-Dedicado



# Servidor Dedicado



# Redes Ponto a Ponto

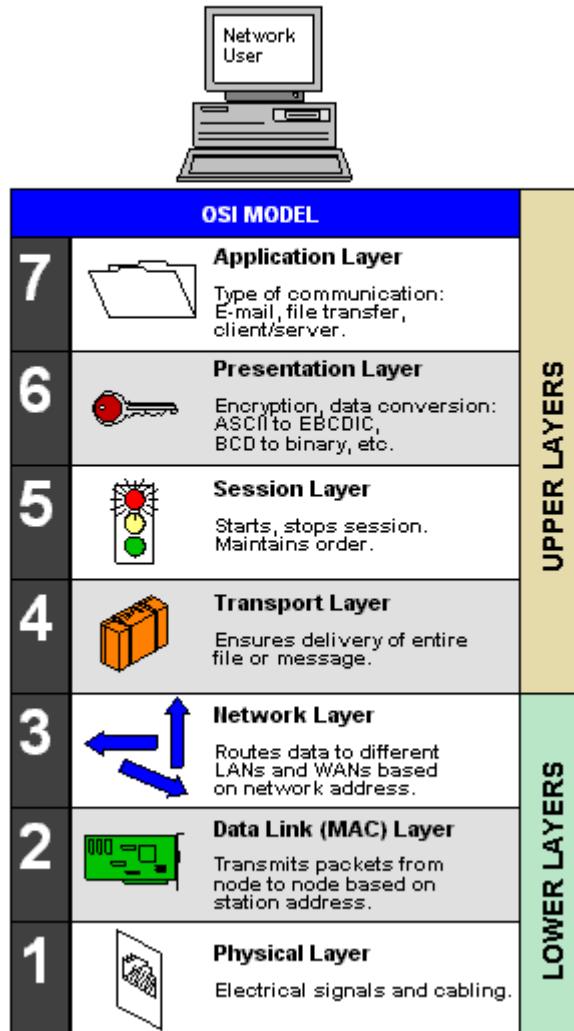
- Usam servidores com sistemas operacionais não dedicados  
*(Exemplos: Windows XP e Windows Vista)*
  - Segurança limitada
  - Instalação e manutenção simples
  - Normalmente não requer um profissional especializado
  - Baixo custo
  - Indicada para o ambiente doméstico e/ou pequenas empresas

# Redes Cliente Servidor

- Usam servidores com sistemas operacionais dedicados  
*(Exemplos: Windows 2000 Server e Windows 2003 Server)*
  - Alto nível de segurança e Custo mais Elevado
  - Instalação e manutenção mais complexas
  - Normalmente requerem um profissional ou uma equipe de profissionais especializados
  - Indicada normalmente para empresas de médio e grande porte

# Modelos de Referência

From Computer Desktop Encyclopedia  
© 2004 The Computer Language Co. Inc.



# Bibliografia da disciplina

- **Bibliografia Obrigatória**

- Redes de computadores - TANENBAUN, Andrew S.

- **Bibliografia Indicada**

- Guia Internet de Conectividade – Cyclades Brasil
- Redes de Computadores – Curso Completo – Gabriel Torres
- Redes de Computadores e a Internet – Kurose e Ross

# Padrões

Para evitar soluções proprietárias nas redes, foram apresentadas sugestões de arquiteturas abertas.

Duas destas arquiteturas são de particular importância e estão contidas nos Modelos de Referência:

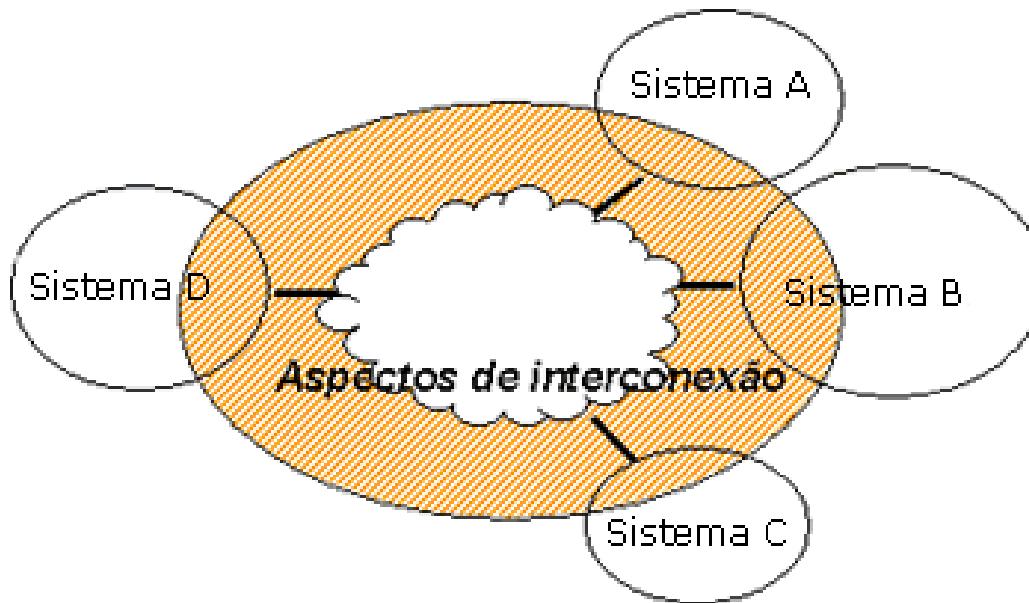
**OSI** (1978, revisado em 1983)

**TCP/IP** (1974, com alterações em 1985).

# Modelo OSI

- OSI significa Open Systems Interconnection (Sistema aberto de Interconexão);
- Desenvolvido pela International Organization for Standardization (ISO);
- Criar padrões de conectividade para interligação de sistemas de computadores, tratando apenas da interligação de sistemas e não dos aspectos internos dos sistemas;
- O Modelo de referência OSI apresenta sete camadas.

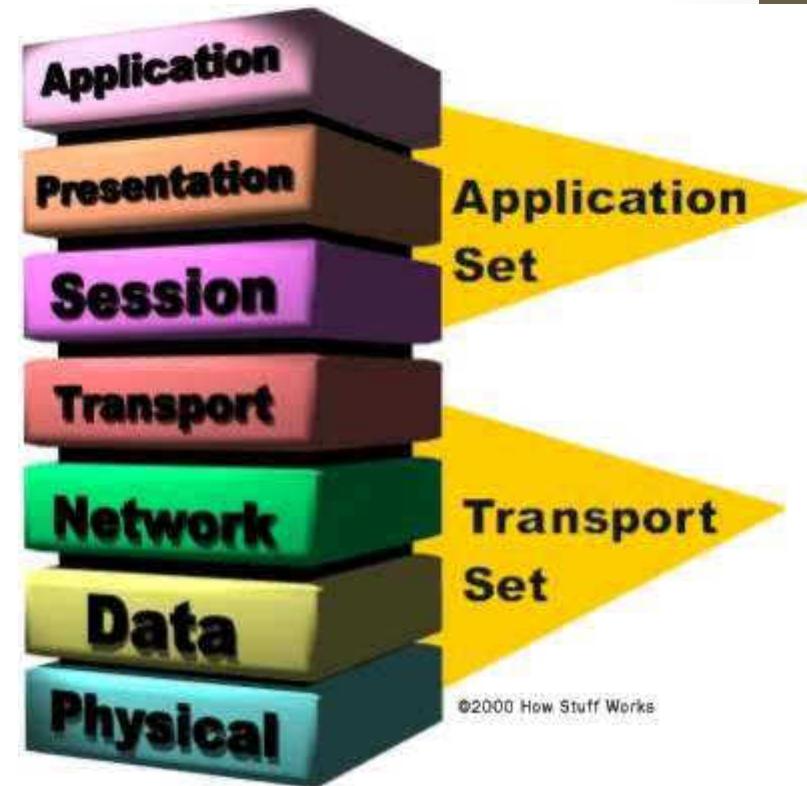
# Modelo OSI



- Se o Sistema A fosse de um fabricante diferente dos Sistemas B, C ou D não haveria a possibilidade de Interligação porque não existia padronização.
- Com o modelo a partir de 1978, os fabricantes começaram a criar seus sistemas seguindo este padrão.

# Modelo OSI

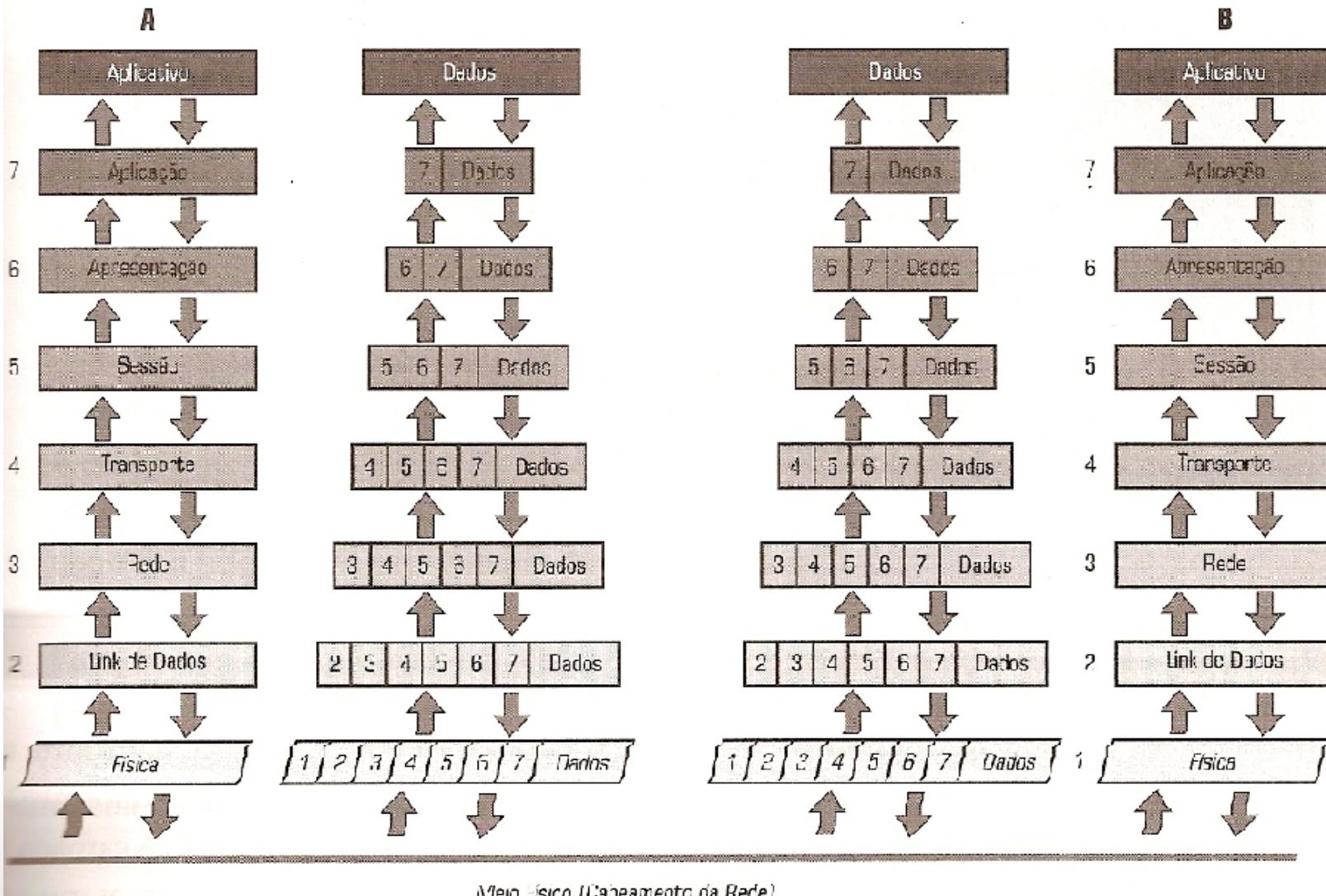
- É um modelo de 7 camadas, onde cada camada só se comunica com uma camada imediatamente superior ou inferior
- Foi dividido em 3 Blocos:
  - camadas de Aplicação (Aplicação / Apresentação / Sessão );
  - camadas de rede (Física / Enlace / Rede);
  - camada de transporte que tem a função de fazer a comunicação entre esses dois blocos



# Por que usamos camadas?

- Um modelo de referência em camadas permite a discussão da arquitetura (análise de cada camada).
- Modularização facilita a manutenção e a atualização do sistema
- As mudanças na implementação de uma camada são transparentes para o resto do sistema

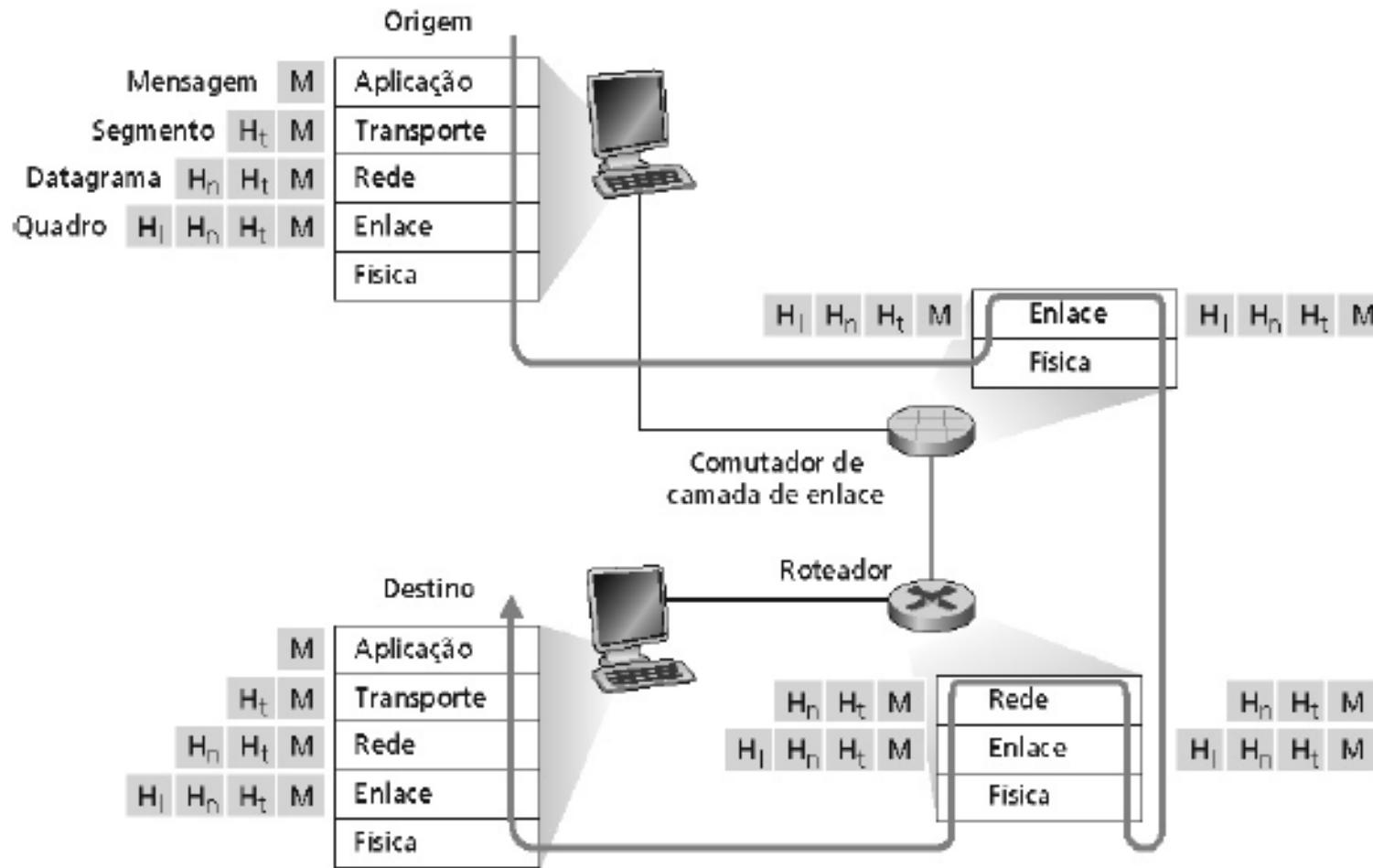
# Funcionamento



# Encapsulamento de dados

- Quando uma aplicação envia seus dados através de um sistema baseado em camadas, cada uma dessas “partes” acrescenta informações importantes para a manipulação daquele pacote pelo respectivo protocolo da camada
- **Os dados acrescentados por uma camada são importantes somente para ela, e não influenciam os dados de outras camadas**
- No final, os dados são enviados como uma seqüência única de bits pela rede

# Encapsulamento de Dados



# Função das Camadas

## Camada 7 – Aplicação

- Responsável em permitir o acesso das aplicações à rede provendo serviços de rede ao usuário de forma transparente
- Definição dos protocolos da aplicação propriamente ditos
- Ex: FTP, SMTP, SNMP, etc.



# Função das Camadas

## Camada 6 – Apresentação

- Também chamada de camada de Tradução
- Trabalha com aspectos sintáticos e semânticos da informação, é responsável pela formatação de dados.
- Por ex.: compactação / codificação dos dados de modo que a aplicação os receba em um formato reconhecível / EBCDIC para ASCII, por exemplo / Criptografia de dados



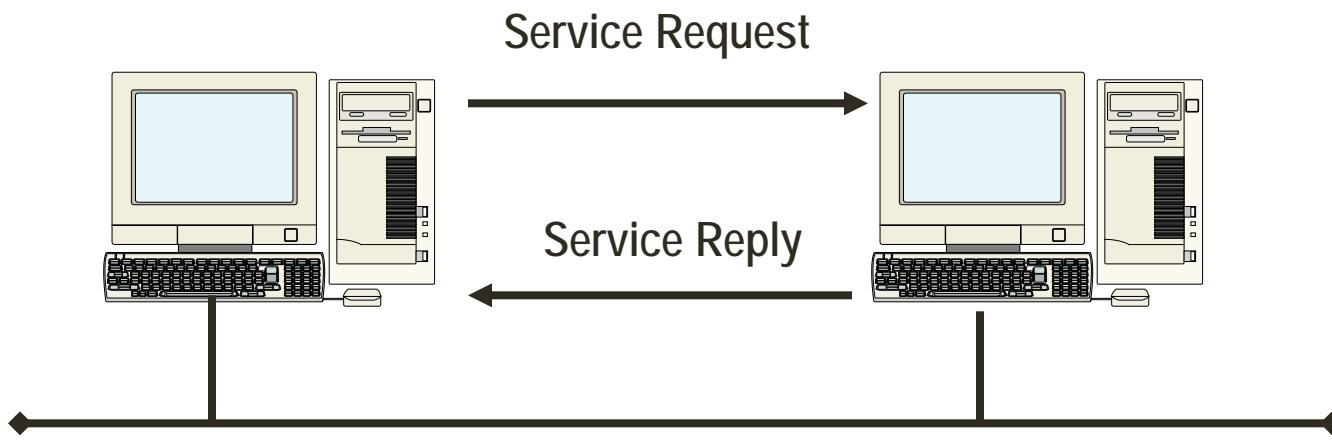
# Função das Camadas

## Camada 5 – Sessão

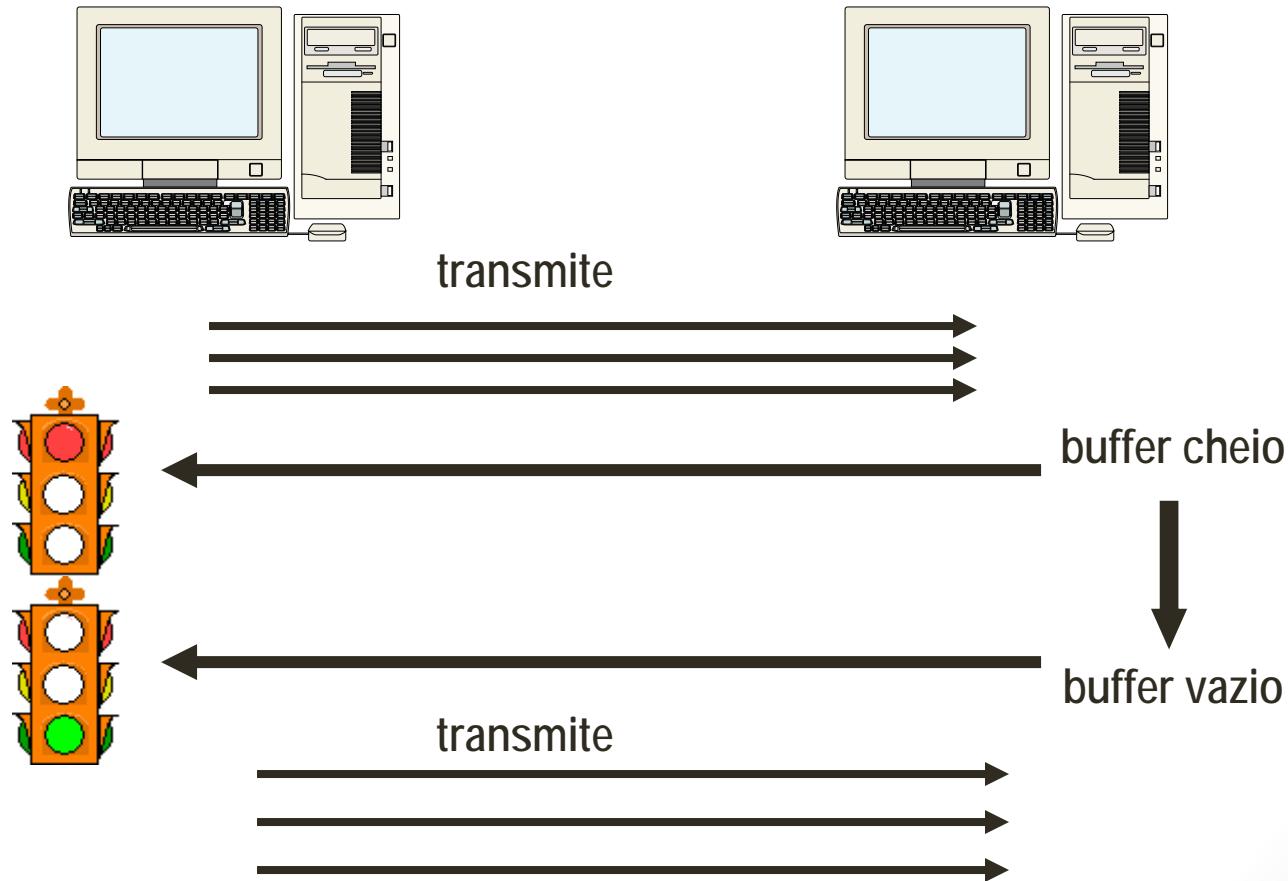
- Permite que usuários de diferentes máquinas estabeleçam sessões (comunicação) entre eles
- Na sessão são definidos como será feita a transmissão de dados (controle de fluxo), além de colocar marcações nos dados que estão sendo transmitidos
- O nível de sessão **estabelece, gerencia e termina as sessões entre entidades** da camada de apresentação.
- Ex: Autenticação / Tipo de Comunicação (Half-duplex ou Full Duplex)



# Camada de Sessão



# Controle de Fluxo



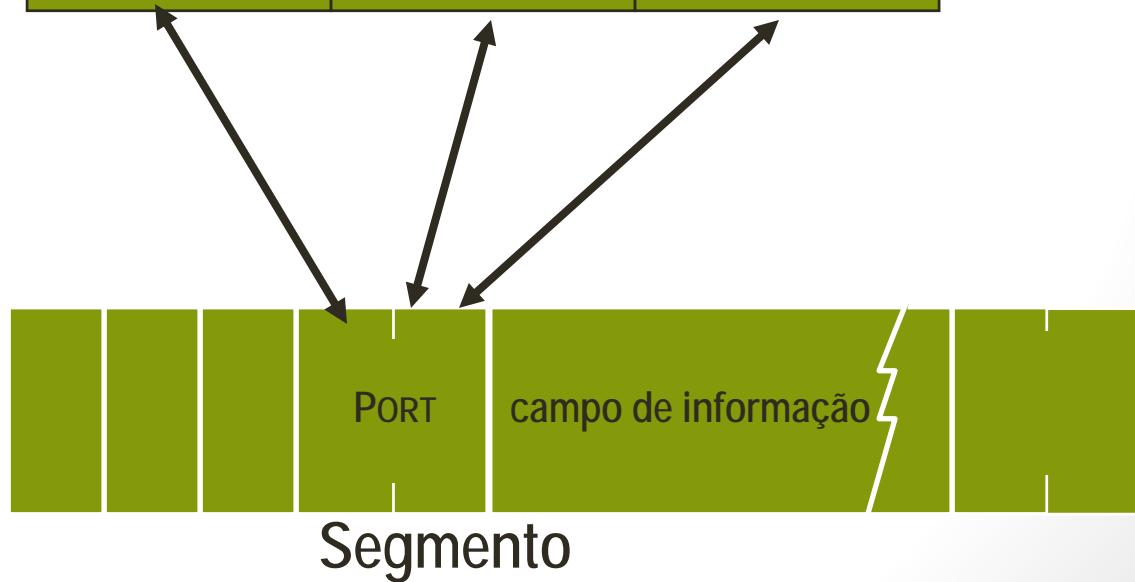
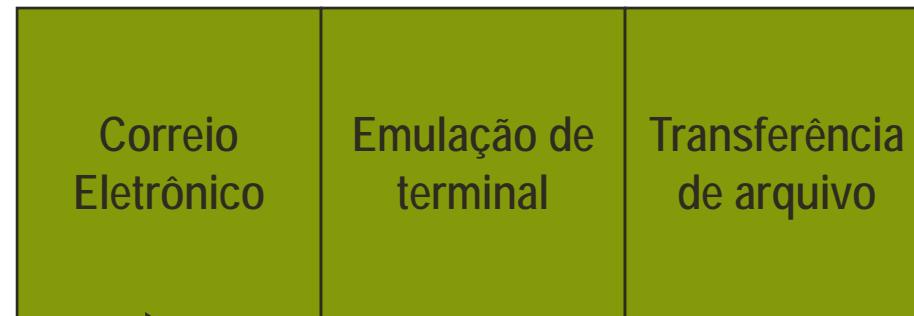
# Função das Camadas

## Camada 4 – Transporte

- Possuem a visão “fim a fim” de um processo de comunicação (programa).
- Devem garantir que os dados transmitidos pelo programa de um computador cheguem ao seu destino com integridade, usando para isso mecanismos como controle de tráfego e correção de erros.
- Estabelecer e terminar conexões.
- Ex. Protocolo TCP e UDP



# Camada de Transporte



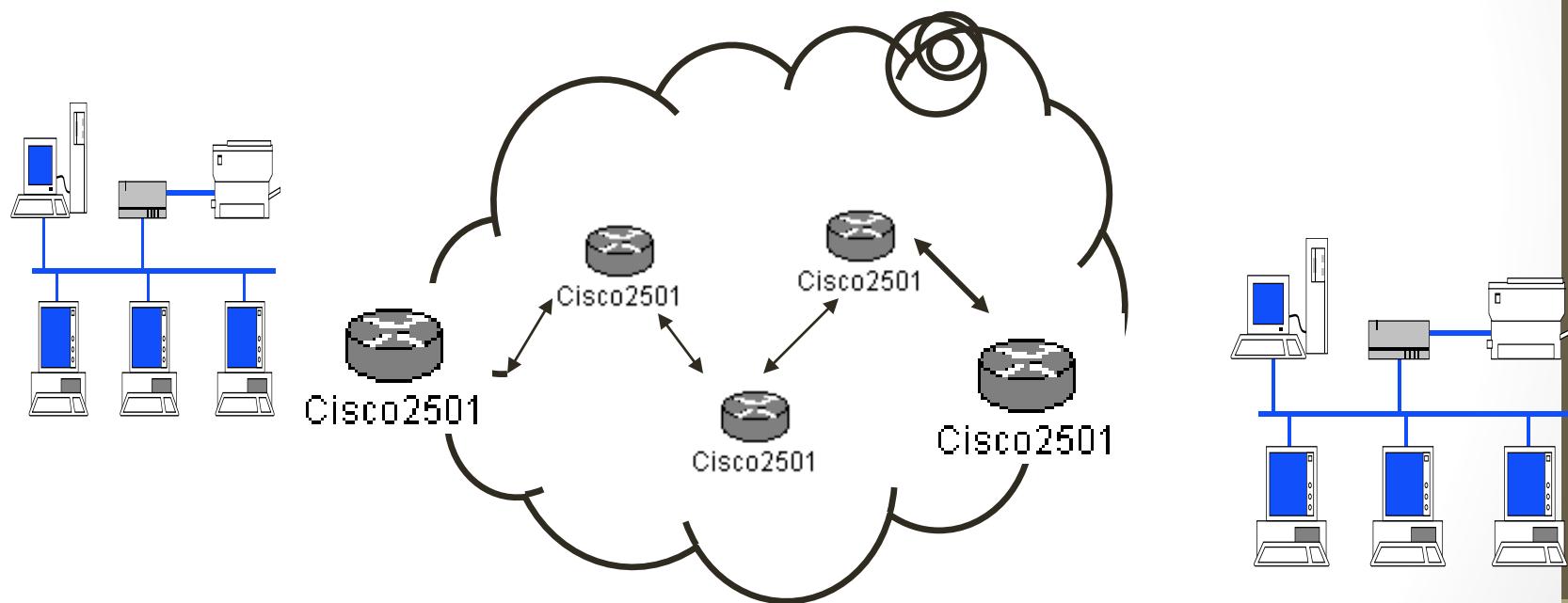
# Função das Camadas

## Camada 3 - Rede

- Responsável pelo endereçamento lógico dos pacotes fim a fim, independente dos programas.
- Determina a rota que os pacotes irão seguir para atingir seu destino (roteamento).
- Faz o controle de congestionamento e podem fazer controle de fluxo também. Não garante a entrega (sem confirmação).
- Ex. Protocolos X25 / Roteadores / Protocolo IP / IPX / BGP / OSPF / RIP



# Camada de Rede



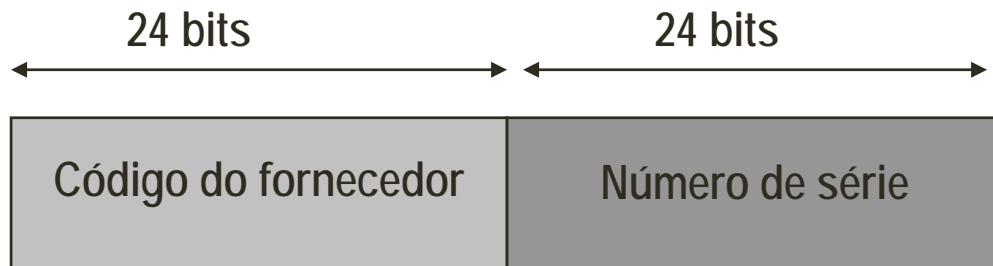
# Função das Camadas

## Camada 2 - Enlace

- Responsável por detectar e corrigir erros de transmissão.
- Restringe-se a dois nós de rede somente – Função principal, fazer com que os dados transmitidos de um computador cheguem ao outro diretamente ligado a ele com integridade
- Faz o endereçamento físico
- Exemplo: Protocolo HDLC e LAPB do protocolo X25 / Switches / Bridges



# Camada de Enlace



00AA00.2CFACA

Exemplos de códigos de fornecedores:

00-00-0C Cisco

00-00-1B Novell

00-00-1D Cabletron

00-AA-00 Intel

00-80-48 Compex

# Função das Camadas

## Camada 1 - Física

- Define os processos e os mecanismos necessários para inserir os sinais nos meios de transmissão e para receber os sinais desses meios (não inclui os meios).
- Por ex.: especificações elétricas, mecânicas, níveis de tensão, taxas de transmissão, etc.
- Parâmetros físicos das interfaces (cabos, conectores, etc.);
- Exemplo: Ethernet 802.3 / RS232 / RS-449 / V-35 / Cabamento / Hubs



# Resumo



- Funções especializadas referentes aos aplicativos (envio de arquivos, terminal virtual, e-mail, etc...)
- Formatação de dados (compactação e criptografia) e conversão de caracteres e códigos (ASCII)
- Negociação e estabelecimento de conexão (atividades com início, meio e fim) – Autenticação
- Divisão da mensagem em pacotes; meios e métodos para a sua entrega de modo adequado
- Roteamento de pacotes através de uma ou várias redes tendo uma visão de endereçamento fim-a-fim
- Trata de comunicação entre dois equipamentos apenas, interconectados entre si
- Transmissão dos bits (sinais elétricos) através do meio físico

# Modelos de Referência



Modelo de Referência OSI



TCP/IP

# Evolução Histórica

- No início dos anos 60, uma associação entre o DARPA (Defense Advanced Research Projects Agency) e um grupo de universidades e algumas instituições, criaram o "ARPANET Network Working Group".
- Em 1969, a rede ARPANET entrou em operação, consistindo inicialmente de quatro nós e utilizando a comunicação baseada em pacotes
- O objetivo era estudar técnicas para implementar sistemas de comunicação de dados robustos e independentes de fornecedores
- ARPANET foi tão bem sucedida que várias organizações ligadas à rede passaram a usá-la cotidianamente

# Evolução Histórica

- Em 1974, foi proposto um grupo de protocolos centrais para satisfazer as seguintes necessidades:
  - Permitir o roteamento entre redes diferentes (chamadas subnets ou subredes)
  - Independência da tecnologia de redes utilizada para poder conectar as subredes
  - Independência do hardware
  - Possibilidade de recobrar-se de falhas
- Originalmente, esses protocolos foram chamados de NCP (Network Control Program), mas, em 1978, passaram a ser chamados de TCP/IP

# Evolução Histórica

- Em 1980, o DARPA começou a implementar o TCP/IP na ARPANET, dando origem à Internet. Em 1983, o DARPA finalizou a conversão de todos seus computadores e exigiu a implementação do TCP/IP em todos os computadores que quisessem se conectar à ARPANET
- Além disso, o DARPA também financiou a implementação do TCP/IP como parte integral do sistema operacional Unix, exigindo que este fosse distribuído de forma gratuita.
- Dessa forma o Unix e, consequentemente, o TCP/IP, se difundiram, cobrindo múltiplas plataformas

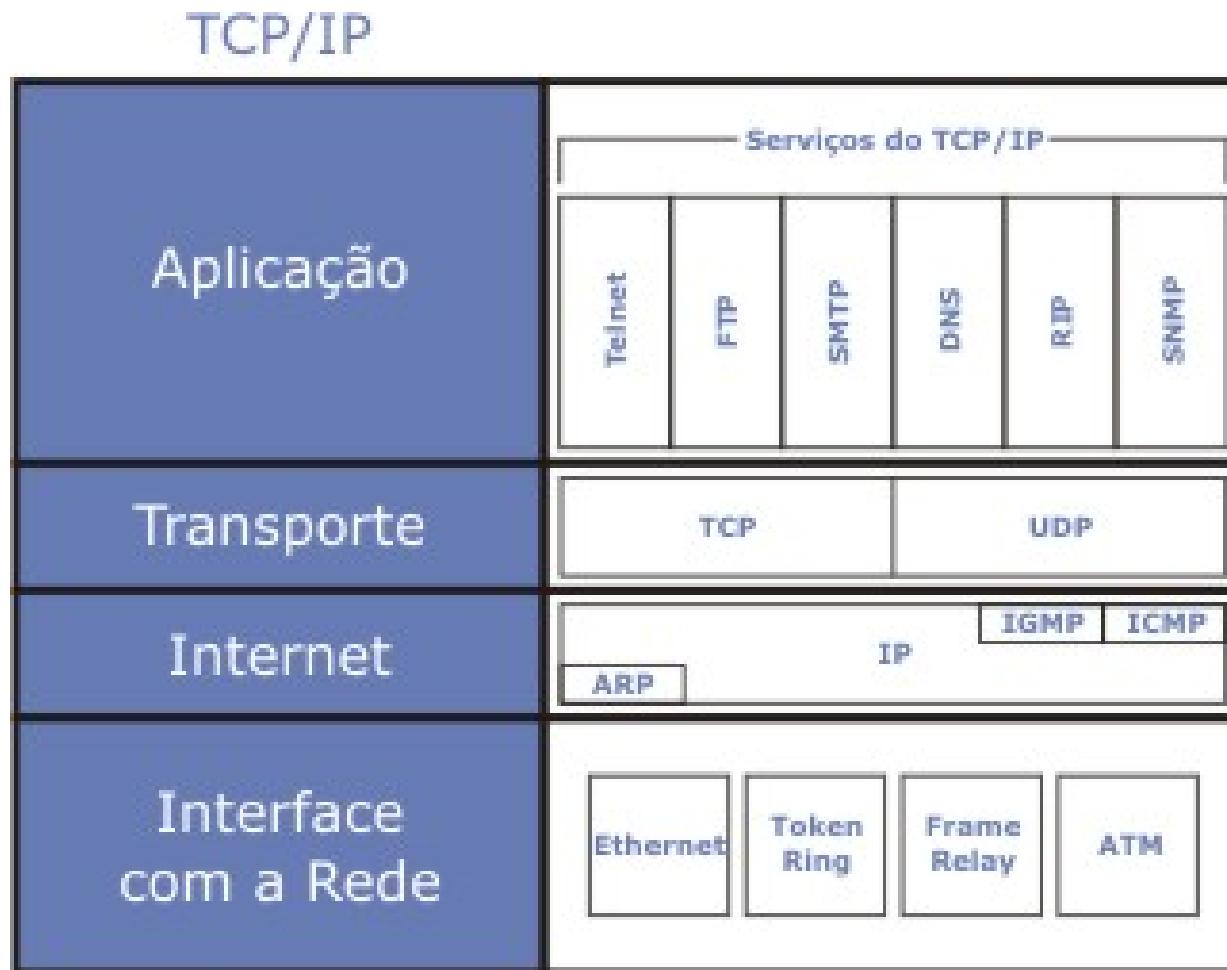
# Protocolos TCP/IP

- Um conjunto de protocolos que permite que computadores possam se comunicar, não importando o fabricante ou o sistema operacional
- Os dois protocolos mais importantes deram seus nomes à arquitetura: Transmission Control Protocol / Internet Protocol
- Os protocolos TCP/IP podem ser utilizados sobre qualquer estrutura de rede. Ex. Ethernets, Token Ring, PPP, X25, Frame Relay, etc.
- A arquitetura TCP/IP, assim como o Modelo OSI, realiza a divisão de funções do sistema de comunicação em estruturas de camadas

# Camadas TCP/IP

- O modelo TCP/IP é formado por 4 camadas conforme abaixo:
  - Aplicação
  - Transporte
  - Inter-Rede
  - Rede
- Diferentemente do modelo OSI, o modelo TCP/IP não é um modelo apenas didático ou conceitual pois ele especifica os protocolos a serem utilizados em cada camada

# Camadas do Modelo TCP/IP



# Camada Aplicacão

- O TCP/IP reúne os protocolos que fornecem serviços de comunicação ao sistema e ao usuário
- Inclui os detalhes das camada de apresentação, sessão e aplicação do Modelo OSI
- Inclui os protocolos de Serviços Básicos **DNS / DHCP** e de serviços ao usuário **Telnet / FTP / Http / SMTP / Etc.**

# Camada de Transporte

- Realiza o transporte de dados fim-a-fim, sem se preocupar com os elementos intermediários (endereços e caminhos).
- As suas atribuições envolvem a qualidade de serviços (confiabilidade), controle de fluxo de pacotes e a detecção e correção de erros.
- Principais Protocolos:
  - **UDP: User Datagram Protocol**
  - **TCP: Transmission Control Protocol**

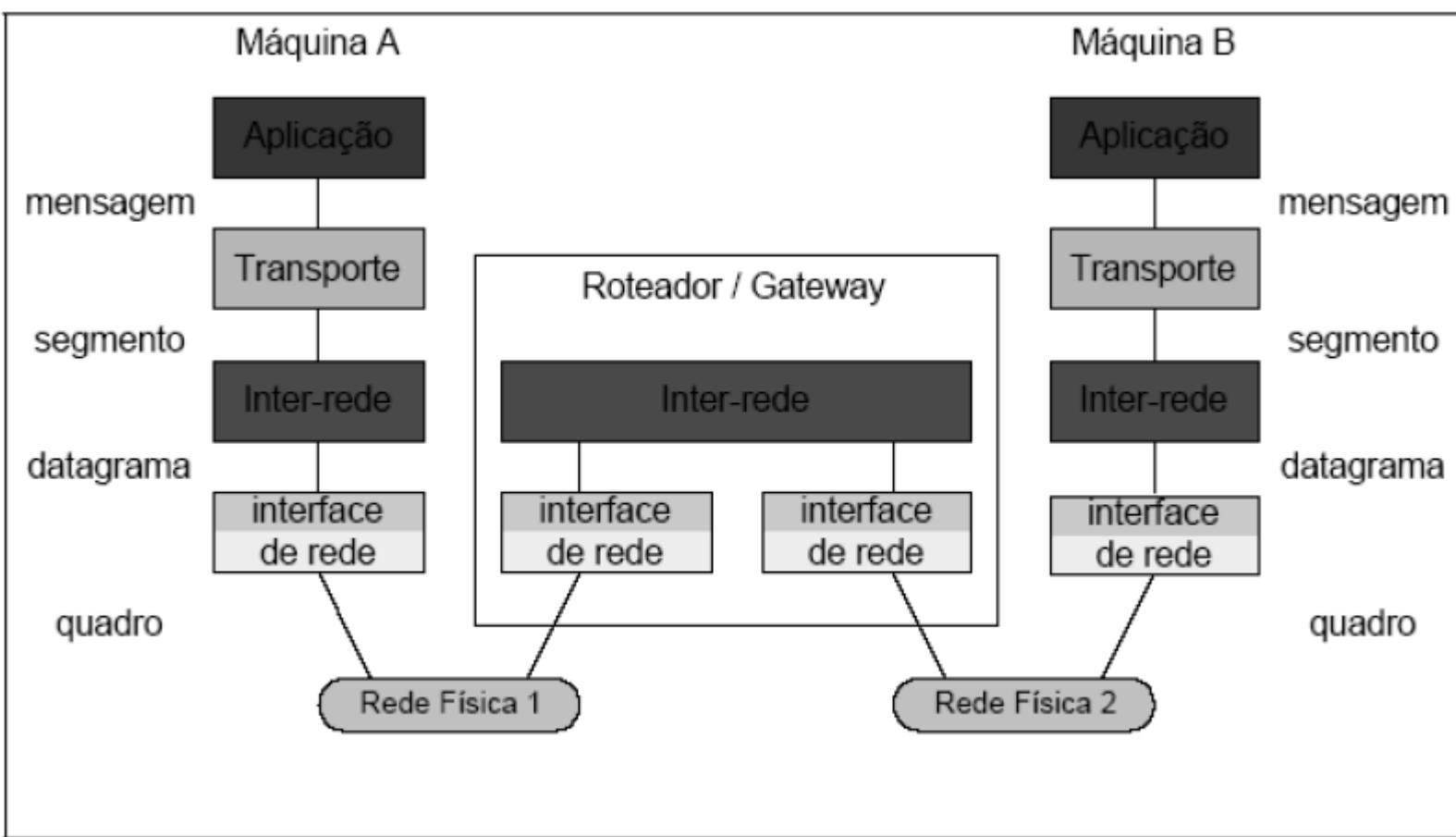
# Camada Inter-Rede

- Gerencia o movimento (comutação) e o roteamento dos pacotes na rede
- Sua finalidade é enviar pacotes da origem de qualquer subrede na inter-rede e fazê-los chegar ao destino, independentemente do caminho e das redes que tomem para chegar lá, usando um identificador, o endereço IP
- Principal Protocolo: ***IP (Internet Protocol)***
- Outros Protocolos: ICMP (Internet Control Message Protocol ) / IGMP (Internet Group Management Protocol)

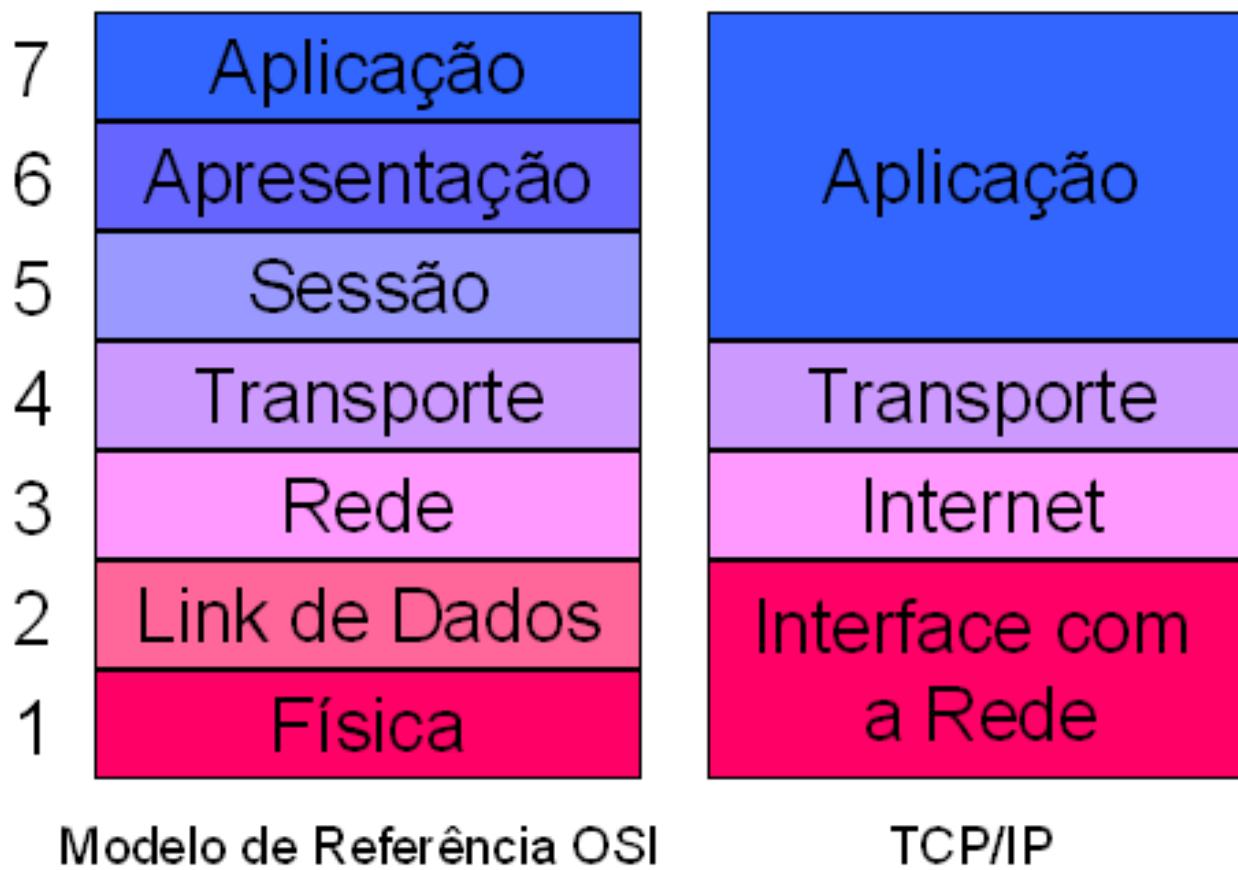
# Camada Rede

- Este nível abrange o driver de dispositivo no SO, a correspondente placa de rede e outros detalhes de hardware necessários para o interfaceamento físico com a rede (Ex. V24 / V35 / RS422, etc)
- Essa camada se relaciona com tudo aquilo que um pacote necessita para realmente estabelecer um link físico entre a origem e o destino
- Inclui detalhes das tecnologias de LAN e WAN que foram empregadas
- Equivalente às camadas física e de enlace do Modelo OSI
- Exemplos de protocolos desta camada: X25 / Frame Relay / ATM / PPP / Ethernet / Token Ring / ARP / RARP

# Camadas TCP/IP



# Modelo OSI x Modelo TCP/IP



# Semelhanças Modelo OSI x Modelo TCP/IP

- Os dois modelos são organizados em camadas
- Ambos modelos possuem camadas de Aplicação, embora incluam serviços muito diferentes
- Ambos modelos possuem camadas de Transporte e de Rede (inter-rede) com funções comparáveis
- Os dois modelos pressupõe o fluxo de pacotes e o encapsulamento dos dados
- Os profissionais da área precisam conhecer ambos

# Diferenças Modelo OSI x Modelo TCP/IP

- O modelo OSI definiu com clareza os conceitos de serviços, interfaces e protocolos.
- O modelo OSI foi concebido antes dos protocolos terem sido inventados, tornando-o mais flexível, porém trouxe uma carência de noção de funcionalidade das camadas.
- O modelo TCP/IP foi criado com base nos protocolos, gerando a vantagem destes protocolos adaptarem-se ao modelo. A desvantagem é que o modelo não se adapta a outras pilhas de protocolo.

# Diferenças Modelo OSI

- O TCP/IP combina os aspectos das camadas de Apresentação e de Sessão dentro da sua camada de Aplicação
- O TCP/IP combina as camadas Física e de Enlace do Modelo OSI em uma camada (Inter-Rede), adicionando algumas funções da camada de rede nesta camada
- O TCP/IP parece ser mais simples por ter menos camadas, mas pode desempenhar funções equivalentes

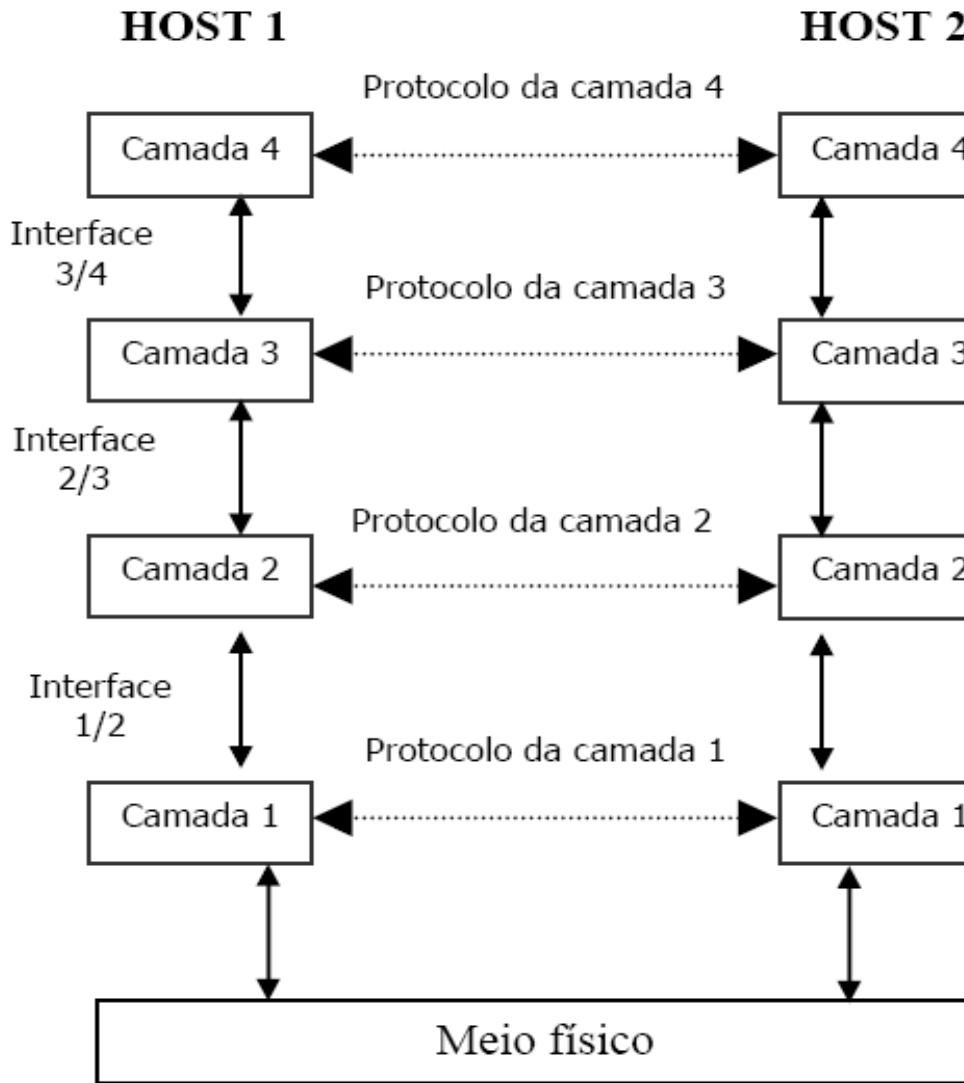
# Diferenças Modelo OSI

- Os protocolos TCP/IP são os padrões em torno dos quais a Internet se desenvolveu, enquanto que o modelo OSI foi desenvolvido para padronizar interconexões de redes diversas
- Geralmente as redes não são desenvolvidas de acordo com o protocolo OSI, embora ele seja usado como um guia

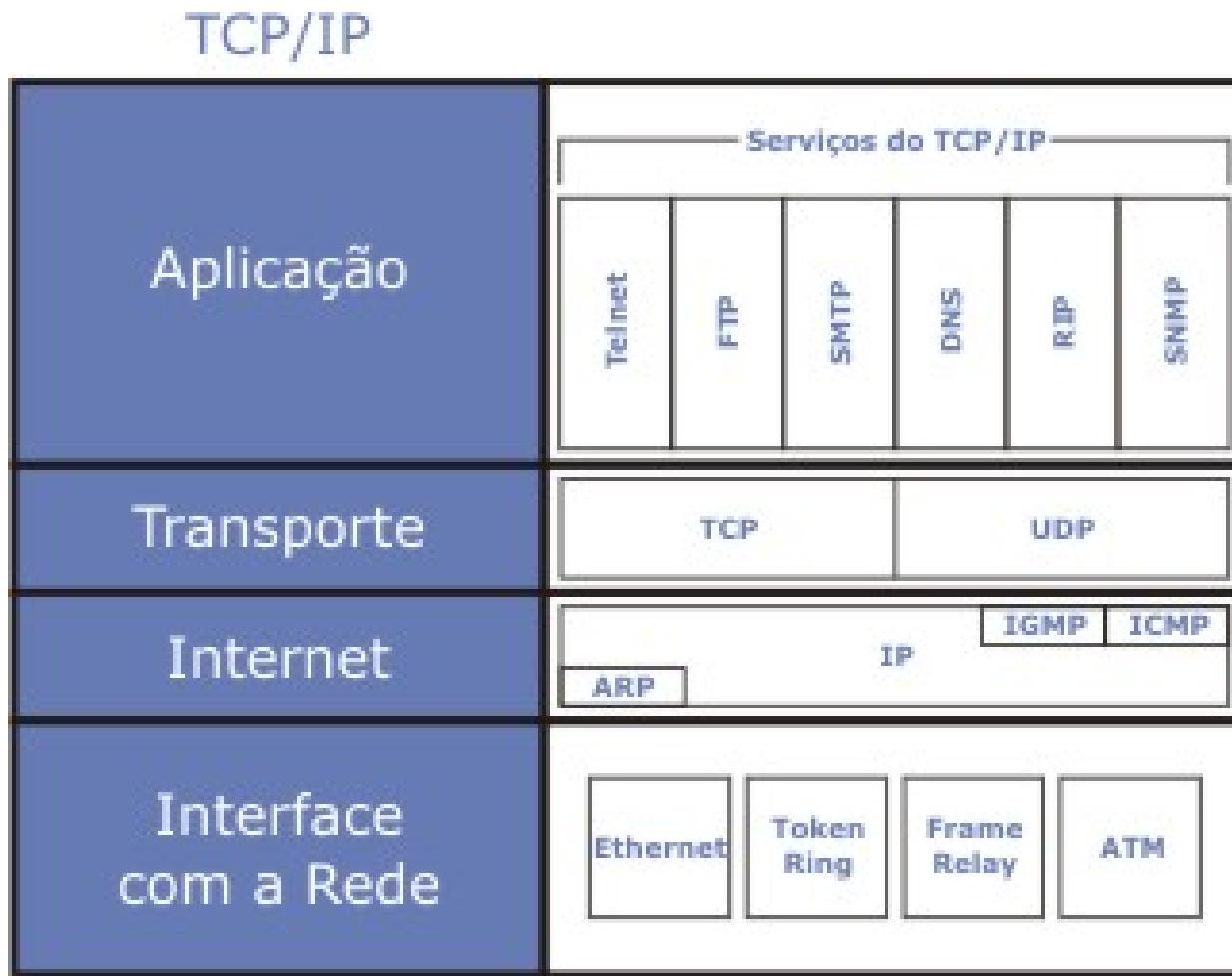
# Protocolos?

- Um dos assuntos mais importantes em relação a redes locais é protocolos.
- São os protocolos que definem como a rede irá funcionar de verdade, pois são eles que definem como os dados enviados por programas serão transferidos pela rede.
- Definição → "*linguagem*" usada pelos dispositivos de uma rede de modo que eles consigam se entender, isto é, trocar informações entre si.

# Comunicação

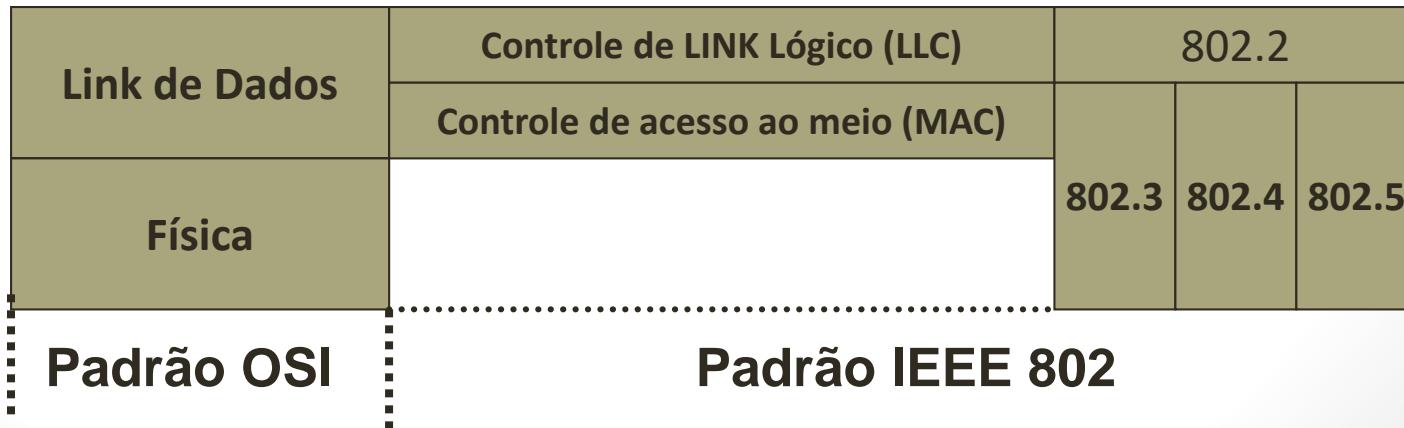


# Modelo TCP / IP



# Protocolos de Camada Física/Enlace

- Padrão IEEE 802 – é um conjunto de protocolos, que se encaixa nas camadas física e de enlace do modelo OSI.
- IEEE – Institute of Electrical and Electronic Engineers
- Divide a camada de enlace em duas subcamadas conforme figura:



# IEEE 802.2

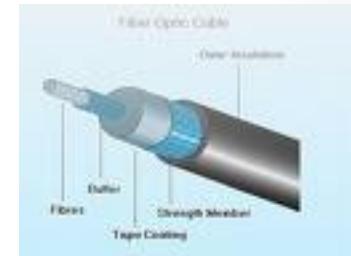
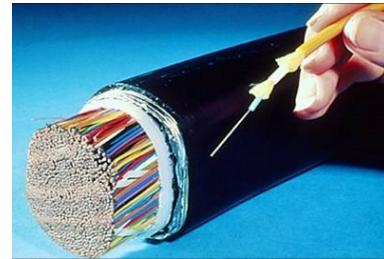
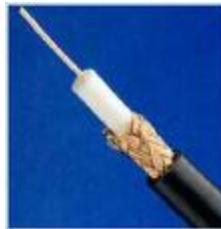
- Também chamado de **LLC (Logical Link Control – Controle Lógico para Conexão)**, este protocolo roda em cima das demais especificações do (IEEE 802.3, IEEE 802.5, etc) determinando a metade superior da camada de Conexão de Dados (Data Link).
- Desta forma, o IEEE 802.2 providencia uma barreira que separa os mecanismos envolvidos com o meio físico da camada de Rede (Network), controlando o fluxo de dados e a detecção e correção de possíveis erros de transmissão.
- Resumindo → é este protocolo que irá fazer a **interface** entre os protocolos de camada física e a camada de rede.

# IEEE 802.3

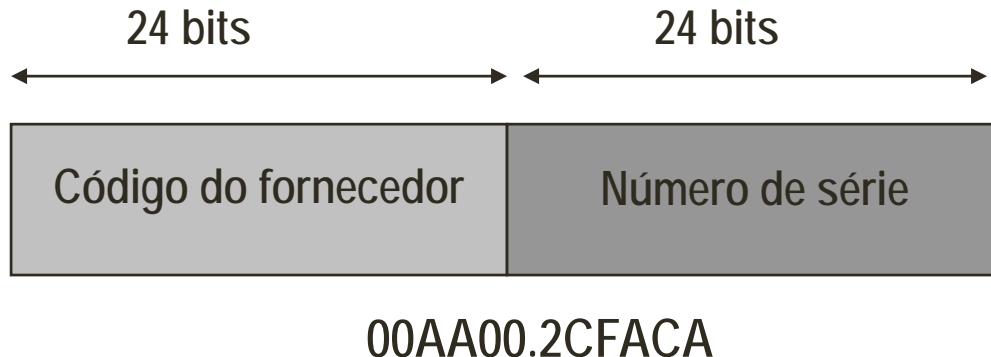
- É o padrão tradicional das redes LAN's com acesso físico que suporta velocidade de 10Mbps (Ethernet), 100Mbps (FastEthernet – 802.3u) e 1Gbps (GigaBitEthernet – 802.3z).
- Utiliza o conceito já estudado de ***detecção de colisão***, chamado ***CSMA/CD***, onde todos os computadores compartilham o mesmo meio e somente um máquina pode transmitir de cada vez, sendo que se duas transmitirem ao mesmo tempo ocorrerá a colisão.
- Utiliza os padrões **10base5** (Cabo coaxial grosso), **10base2** (Cabo coaxial fino), **10baseF** (fibra óptica), 100baseT (UTP), e outros.

# IEEE 802.3

Name	Cable	Max. segment	Nodes/seg.	Advantages
10Base5	Thick coax	500 m	100	Good for backbones
10Base2	Thin coax	200 m	30	Cheapest system
10Base-T	Twisted pair	100 m	1024	Easy maintenance
10Base-F	Fiber optics	2000 m	1024	Best between buildings



# IEEE 802.3



Endereços MAC – (*Media Access Control*) - endereço físico da estação, ou melhor, da interface de rede.

Exemplos de códigos de fornecedores (3 primeiros octetos):

00-00-0C Cisco

00-00-1B Novell

00-00-1D Cabletron

00-AA-00 Intel

00-80-48 Compex

Exemplos do número de série:

00:01:03

# IEEE 802.4

- Pouco utilizado.
- Padrão IEEE para redes locais do tipo Token Bus.
- Basicamente, padroniza o protocolo MAP, que controla o acesso ao meio no protocolo Token Bus.
- Nos meados dos anos 80, a empresa GM (General Motors) cansada das dificuldades encontradas na informatização da empresa, resolveu desenvolver um padrão para a automação fabril.
- Este padrão foi batizado como MAP ("Manufacturing Automation Protocol")

# IEEE 802.5

- Utilizam o método de passagem de bastão, as redes 802.5 e ***Token Ring*** são chamadas de determinísticas, já que é possível calcular o tempo necessário para que a informação flua de um nó até outro.
- Essas redes também possuem alguns mecanismos para a resolução de erros que as redes do tipo Ethernet não possuem, além de evitar colisões.
- Usado em topologia do tipo anel.

# IEEE 802.11

- Padrão ***Ethernet Sem Fio / Wireless / WLan / Wi-Fi***
- Também utiliza o 802.2 para camada de acesso ao nível lógico (LLC)
- Utiliza ***autenticação*** para verificar se uma estação está autorizada a se comunicar com outra estação em uma dada área de cobertura ou entre um AP (Access Point) e cada estação.
- O método de ***criptografia*** é conhecido como WEP (Wireless Equivalent Privacy), que se destina a fornecer às redes sem fio o mesmo nível de segurança das redes convencionais.
- Utiliza Método de acesso ***CSMA/CA*** - Antes de transmitir efetivamente um pacote, a estação avisa sobre a transmissão e em quanto tempo a mesma irá realizar a tarefa, evitando colisões e retransmissões.

# IEEE 802.11

PADRÃO	TAXA DE BITS	ALCANCE	FREQUÊNCIA	COMPATIBILIDADE	CUSTO
802.11a	54Mbps	25m a 100m	5GHz	Incompatível com o 802.11b e 802.11g	Alto
802.11b	11Mbps	100m a 150m	2.4GHz	Adoção generalizada.	Mais Baixo de todos
802.11g	108Mbps	100m a 150m	2.4GHz	Compatibilidade com o 802.11b a 11Mbit/s	Baixo
802.11 n	300Mbps (MIMO)	400m	2.4GHz ou 5GHz	Compatível com os demais, dependendo da frequência	Alto

# IEEE 802.11n



# IEEE 802.11

## Intervalo de Freqüência

- **2.4 GHz** é muito propenso a interferências devido a alta penetração
  - WLAN
  - Telefones sem fio
  - Dispositivos Bluetooth
- **5 GHz** implica em menos interferência mas,
  - Alta taxa de absorção (chuva, prédios, pessoas)
  - Células menores

# IEEE 802.15

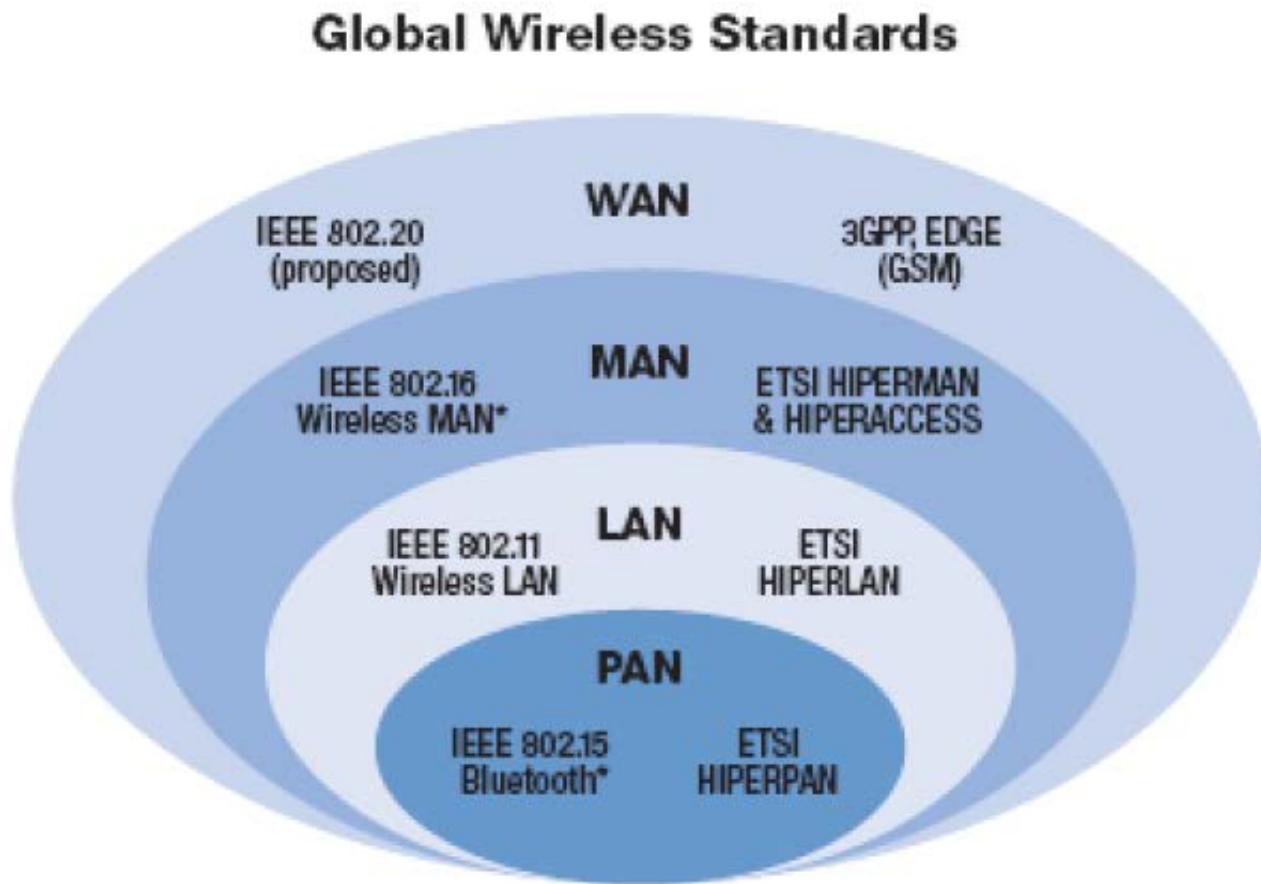
- Também conhecido como ***Redes Pan*** (personal area network)
- ***Bluetooth***
- Diâmetro inferior a 10m
- Substituição de cabos (mouse, teclado, fones)
- Frequência: 2,45 GHz
- Velocidade de 1Mbps



# IEEE 802.16

- Também conhecido como padrão WiMax
- Características Principais:
  - Não há necessidade de Visada
  - Alto Alcance (pode atingir 50 Km)
  - Altas Velocidades (pode atingir 75 MBps)
- Em fase de implantação no Brasil. Utilizará, principalmente a faixa de frequência de 3,5GHz.
- A Embratel adquiriu licenças em todo o Brasil e já está operando em várias regiões desde Março de 2008.

# Padrões IEEE sem fio



# **Protocolos de Camada de Inter-Rede do Modelo TCP/IP**

# ARP

- *Address Resolution Protocol*
- Tem a finalidade de ***chegar a um endereço físico a partir de um endereço IP.***
- O ARP consulta as máquinas na rede local e procura seus endereços físicos a partir de um IP. O ARP mantém em seu cache o par endereço físico / número de IP. Toda vez que o IP quer se comunicar com o computador o cache do ARP é consultado para checar se este endereço está na rede local.
- Se o endereço físico já estiver no cache do ARP, então o endereço físico correspondente é usado para enviar um datagrama diretamente para o adaptador de rede físico desejado.

# ARP

- *Address Resolution Protocol*
- Se o endereço IP não estiver no cache do ARP, então o ARP faz uma transmissão na LAN.
- O pedido inclui o endereço do IP do computador desejado. Toda máquina LAN examina este pedido.
- Se o endereço corresponder, este computador gerará uma resposta ao ARP que inclui o endereço físico em seu cache, e o IP pode prosseguir e enviar seu datagrama diretamente para o adaptador de rede desejado.

# RARP

- *Reverse ARP*
- Realiza a função oposta do ARP.
- O RARP é usado quando o *endereço físico é conhecido mas o endereço IP não*.
- Ele é ativado quando se conhece o endereço físico e o IP não.

# ICMP

- *Internet Control Message Protocol*
- É usado para notificar o IP e os protocolos das camadas superiores sobre erros no nível da rede e problemas no controle do fluxo.
- O comando de teste **PING** é um protocolo ICMP
- O Ping envia um datagrama para um endereço e solicita que o computador de destino retorne os dados enviados em um datagrama de resposta.

# ICMP

- *Internet Control Message Protocol*
- Outras funções deste protocolo: controlar a velocidade de transmissão de um computador para o outro, para que não haja sobrecarga de dados.
- Aviso de quando um computador de destino não foi achado na rede e avisa quando o TTL de um datagrama chegou a zero.
- TTL → *Time to Live* - número de saltos entre máquinas.

# Exemplo PING

C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\temp>ping www.folha.com.br

Disparando contra ghandi.folha.com.br [200.221.3.135] com 32 bytes de dados:

Resposta de 200.221.3.135: bytes=32 tempo=2639ms TTL=244

Resposta de 200.221.3.135: bytes=32 tempo=35ms TTL=244

Resposta de 200.221.3.135: bytes=32 tempo=43ms TTL=244

Resposta de 200.221.3.135: bytes=32 tempo=21ms TTL=244

Estatísticas do Ping para 200.221.3.135:

Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (0% de perda),

Aproximar um número redondo de vezes em milissegundos:

Mínimo = 21ms, Máximo = 2639ms, Média = 684ms

C:\Documents and Settings\temp>ping 192.168.0.100

Disparando contra 192.168.0.100 com 32 bytes de dados:

Resposta de 192.168.0.100: bytes=32 tempo<1ms TTL=128

Estatísticas do Ping para 192.168.0.100:

Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (0% de perda),

Aproximar um número redondo de vezes em milissegundos:

Mínimo = 0ms, Máximo = 0ms, Média = 0ms

C:\Documents and Settings\temp>

# IP

- ***Internet Protocol*** – Cuida do endereçamento (roteamento) dos computadores em uma rede TCP/IP
- Formado por 4 octetos, representando um endereço único na rede Internet
- Ex. **200.192.055.002**
- Veremos adiante, a explicação do protocolo IP

# Protocolos da Camada de Transporte do Modelo TCP/IP

# TCP

- *Transmission control protocol*
- É o principal protocolo de transporte da Internet. Aceita mensagens de qualquer tamanho de um protocolo da camada superior e oferece transporte Full-duplex.
- Realiza a sincronização de seqüências de transmissão criando caminhos entre origem e destino no momento da transmissão para envio do pacote
  - **Orientado a conexão** (*transporte confiável – controle de fluxo – Ex.: telefonia*) .
- *Confirma entrega dos pacotes*
- O envio de pacotes é realizado atribuindo um identificador de cada segmento, chamado porta, que está relacionado ao protocolo da camada de aplicação que está sendo transportado
- Ex. 21 (FTP) , 80 (Http), 443 (Https), etc.

# UDP

- *User Datagram Protocol*
- *Não é orientado a conexão*, utilizando o conceito de datagramas
- *Não tem confirmação de entrega dos dados*
- Não faz conexões, não faz controle de fluxo, e outras funções que o TCP faz, o UDP é mais rápida que o TCP.

# Protocolos da Camada de Aplicação do Modelo TCP/IP

# Principais Portas

- Ao todo – 65535, começando de 1

:: 21 - FTP;

:: 23 - Telnet;

:: 25 - SMTP;

:: 80 - HTTP;

:: 110 - POP3;

:: 143 - IMAP;

:: 443 – HTTPS, etc ...

# FTP

- *File Transfer Protocol*
- Permite que um usuário transfira arquivos entre dois computadores de rede
- Oferece variedade de Logins, inspeção de relatórios, manipulação de arquivos, execução de comandos e outras funções.
- Pode ser usado para Mover arquivos entre sistemas operacionais

# SMTP/POP3

- *Simple Mail Transfer Protocol*
- *Post Office Protocol*
- Protocolo de roteamento de correio eletrônico, que utiliza TCP no nível de transporte e IP no nível de Rede
- **SMTP** – E-mails de Saída
- **POP3** – E-mails de Entrada

# SNMP

- *Simple Network Management Protocol*
- Protocolo para gerência de rede
- Segue a arquitetura do Modelo TCP/IP
- Utiliza protocolo **UDP** para entrega das mensagens

# Telnet

- *Remote Terminal Emulation*
- Permite que usuários accessem os aplicativos com base em host de rede, com PC's funcioando como se fossem terminais burros
- Ou seja, ocorre uma simulação de terminal no PC Local
- Tem uma função parecida com o com o aplicativo de acesso remoto do Windows

# DNS

- *Domain Name System*
- É um sistema de banco de dados distribuídos que fazem a resolução do endereço/nome para as aplicações do cliente
- Por exemplo: no IE ao digitar [www.escolafontes.com.br](http://www.escolafontes.com.br), o DNS irá realizar uma conversão deste nome para o endereço IP válido desta página, pois na Internet o endereçamento é feita através de endereço IP. Em 24/11/2010 o IP era: 200.209.69.202
- Também realiza a função inversa, convertendo um endereço IP em um domínio válido

# DHCP

- *Dynamic Host Configuration Protocol*
- Quando não é utilizado IP fixo na máquinas da sua rede, deve existir um servidor DHCP na sua rede para conceder dinamicamente endereços IP's para cada nova conexão de uma máquina na rede

# DNS e DHCP

The image displays two side-by-side Windows dialog boxes. The left dialog is titled "Propriedades de Conexão local" (Local Connection Properties) and the right one is titled "Propriedades de Protocolo TCP/IP" (TCP/IP Properties). Both dialogs have standard Windows window controls at the top.

**Propriedades de Conexão local (Left Dialog):**

- Geral:** Shows the selected network adapter as "Realtek RTL8139/810x Family Fast".
- Autenticação:** Contains checkboxes for "Cliente para redes Microsoft", "Compartilhamento de arquivos e impressoras para redes...", "Agendador de pacotes QoS", and "Protocolo TCP/IP".
- Avançado:** Contains checkboxes for "Mostrar ícone na área de notificação quando conectado" and "Notificar-me quando esta conexão não tiver conectividade ou ela for limitada".
- Buttons:** OK, Cancelar.

**Propriedades de Protocolo TCP/IP (Right Dialog):**

- Geral:** Shows the configuration method as "Obter um endereço IP automaticamente".
- Configuração alternativa:** Shows the configuration method as "Usar o seguinte endereço IP:" with fields for "Endereço IP:", "Máscara de sub-rede:", and "Gateway padrão:".
- DNS:** Shows the configuration method as "Obter o endereço dos servidores DNS automaticamente".
- Buttons:** Avançado..., OK, Cancelar.

The text in the dialogs is in Portuguese.

# Endereçamento IP

# Endereçamento IP

- O IP é um protocolo da *Camada de rede*
- É um ***endereço lógico*** único em toda a rede, portanto, quando estamos navegando na Internet estamos utilizando um endereço IP único mundialmente, pois a Internet é uma rede mundial
- Em redes locais podemos utilizar alguns endereços que ***não são válidos na Internet***. Estes são reservados para redes locais, mas cada máquina da rede local utilizará um único IP nesta rede local.

# Endereços Lógicos, Físicos e de Serviço

- **Serviço:** Atribuído na camada de Transporte (TCP) e refere-se a uma aplicação que está sendo transportada (porta);
- **Lógico:** Atribuído na camada de rede (IP) e indica a origem e destino do serviço, independente do serviço que está sendo transportado;
- **Físico:** Atribuído na camada enlace (MAC), e indica o próximo host da rede onde o pacote será entregue.

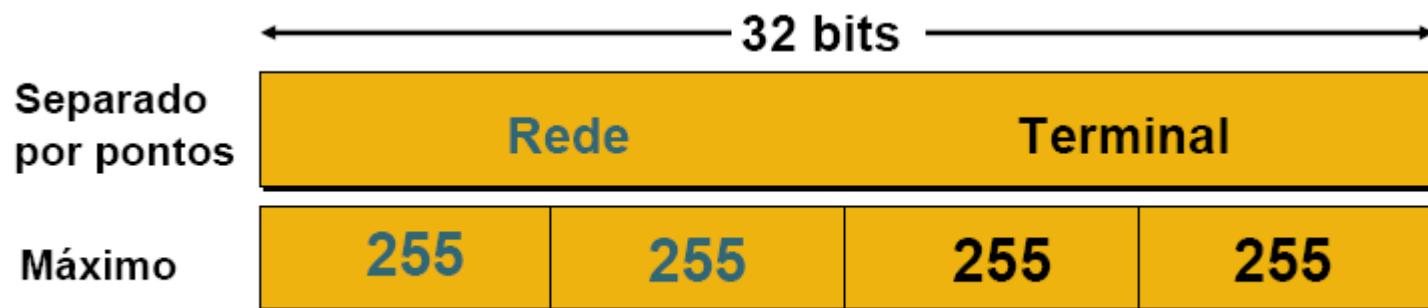
# Endereço IPv4

- Um endereço IP consiste em ***4 bytes ou 32 bits***. Ao invés de trabalhar com 32 bits por vez, é comum a prática de segmentação dos 32 bits de um endereço IP em quatro campos de 8 bits chamados de octetos;
- Cada octeto é convertido em um número de base decimal na escala de 0-255. Estes são separados por um ponto. Este formato é chamado de **notação decimal pontuada**. Em uma rede, estes números devem ser únicos e seguem a algumas regras que veremos a seguir;
- Exemplo.: 74.125.91.104 (www.google.com).

# Host x Rede

- Cada endereço IP inclui uma identificação de ***rede e uma de host (máquina)***:
- A ***identificação de rede*** (também conhecida como endereço de rede) identifica os sistemas que estão localizados no mesmo segmento físico de rede na abrangência de roteadores IPs. Todos os sistemas na mesma rede física devem ter a mesma identificação de rede. A identificação de rede deve ser única na rede;
- A ***identificação de host*** (também conhecido como endereço de host) identifica uma estação de trabalho, servidor, roteador, ou outro host TCP/IP (nó da rede) dentro de uma rede. O endereço para cada host deve ser único para a identificação de rede.

# Host x Rede

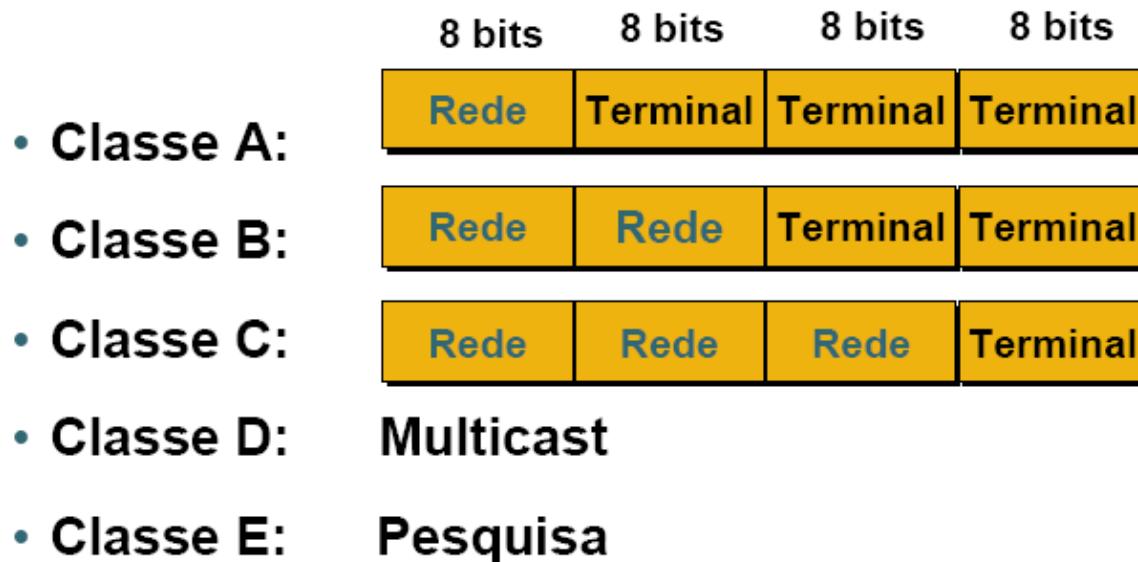


# Classes IP

- Existem 5 ***classes (A,B,C,D,E)*** de endereços IP, que irão variar conforme a quantidade de endereços de rede existente em cada classe;
- O objetivos das classes é determinar qual parte do endereço IP pertence a rede e qual parte do endereço IP pertence ao host, além de permitir uma melhor distribuição dos endereços IP's.

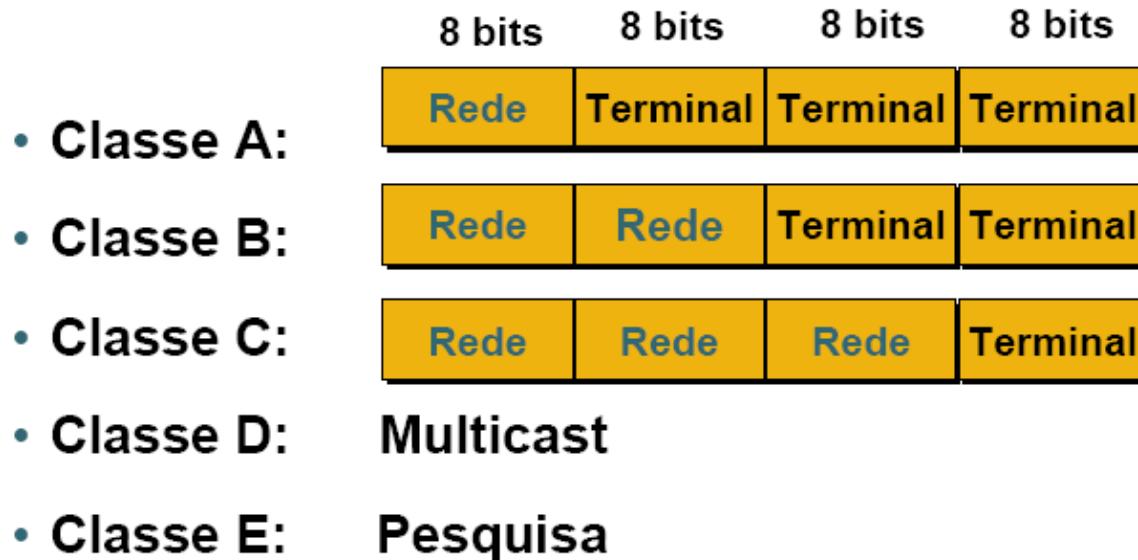
# Classe A

- O primeiro byte do endereço está entre 1 e 127.
- Exemplo: 13.0.0.1 / 80.10.69.12 / 37.25.10.99
- Nos endereços de Classe A, o primeiro número identifica a rede e os outros três números identificam o próprio host.



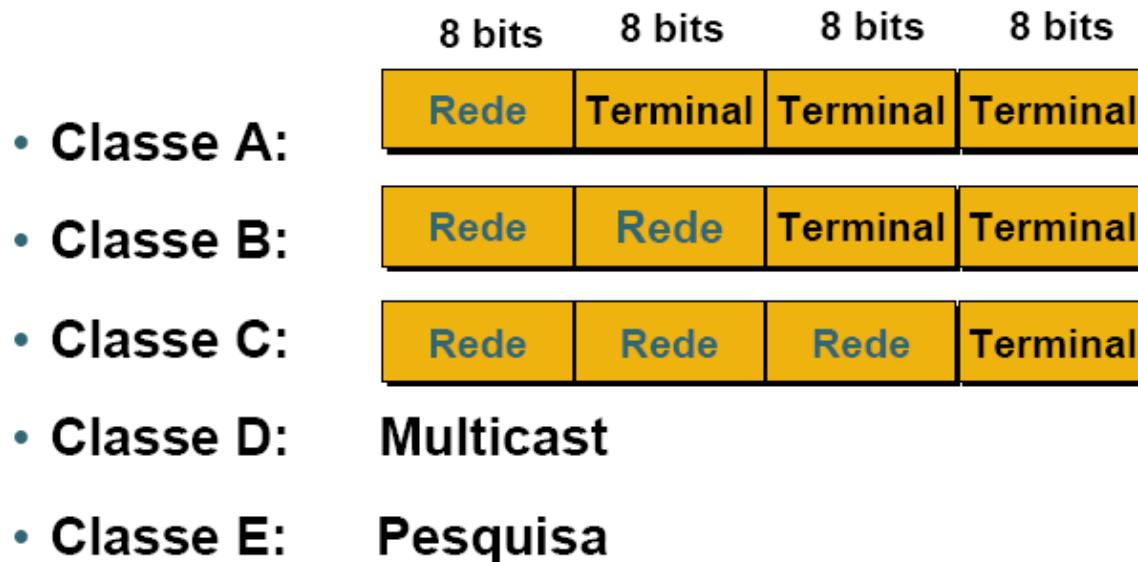
# Classe B

- O primeiro byte do endereço está entre 128 e 191.
- Exemplo: 133.0.0.1 / 140.10.69.12 / 190.25.10.99.
- Nos endereços de Classe B, os dois primeiros números identificam a rede e os outros dois números identificam o host.



# Classe C

- O primeiro byte do endereço está entre 192 e 223.
- Exemplo: 200.0.0.1 / 220.10.69.12 / 195.25.10.99
- Nos endereços de Classe C, os três primeiros números identificam a rede e os últimos números identificam o próprio host.



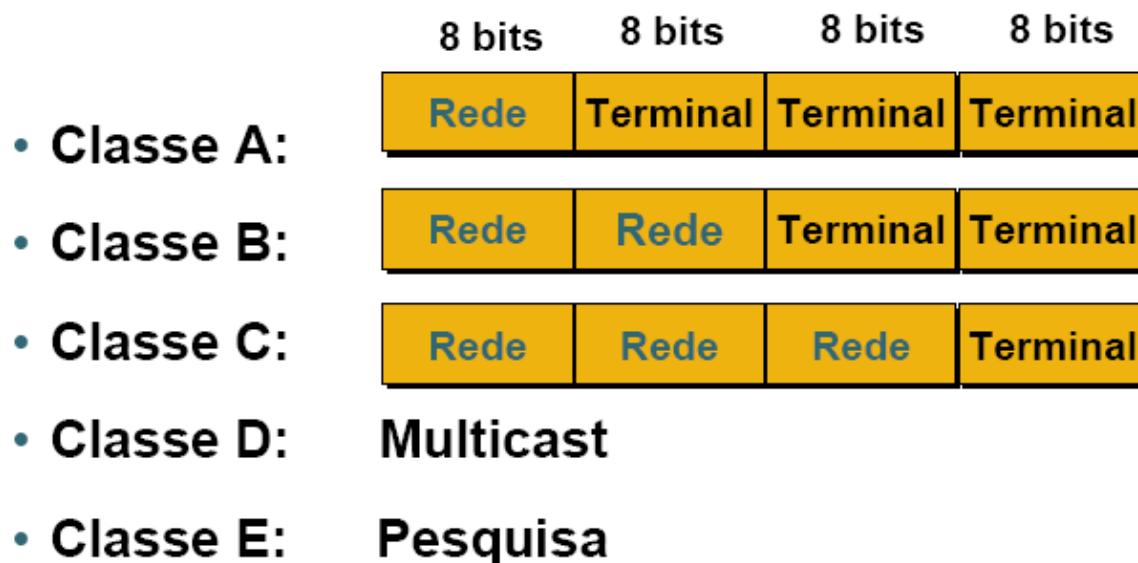
# Classe D

- O primeiro byte do endereço está entre 224 e 239;
- Exemplo: 225.0.0.1 / 239.10.69.12 / 226.25.10.99;
- Esta classe está reservada para criar agrupamentos de computadores para o uso de Multicast (acesso apenas a endereços que estejam configurados para receber os dados). Não podemos utilizar esta faixa de endereços para endereçar os computadores de usuários na rede TCP/IP.

	8 bits	8 bits	8 bits	8 bits
• <b>Classe A:</b>	Rede	Terminal	Terminal	Terminal
• <b>Classe B:</b>	Rede	Rede	Terminal	Terminal
• <b>Classe C:</b>	Rede	Rede	Rede	Terminal
• <b>Classe D:</b>	Multicast			
• <b>Classe E:</b>	Pesquisa			

# Classe E

- O primeiro byte do endereço está entre 240 e 247.
- A Classe E é um endereço reservado e utilizado para testes e novas implementações (IETF – *Internet Engineering Task Force*) e controles do TCP/IP.
- Não podemos utilizar esta faixa de endereços para endereçar os computadores na rede TCP/IP.



# Números Máximos de Hosts em cada Classe

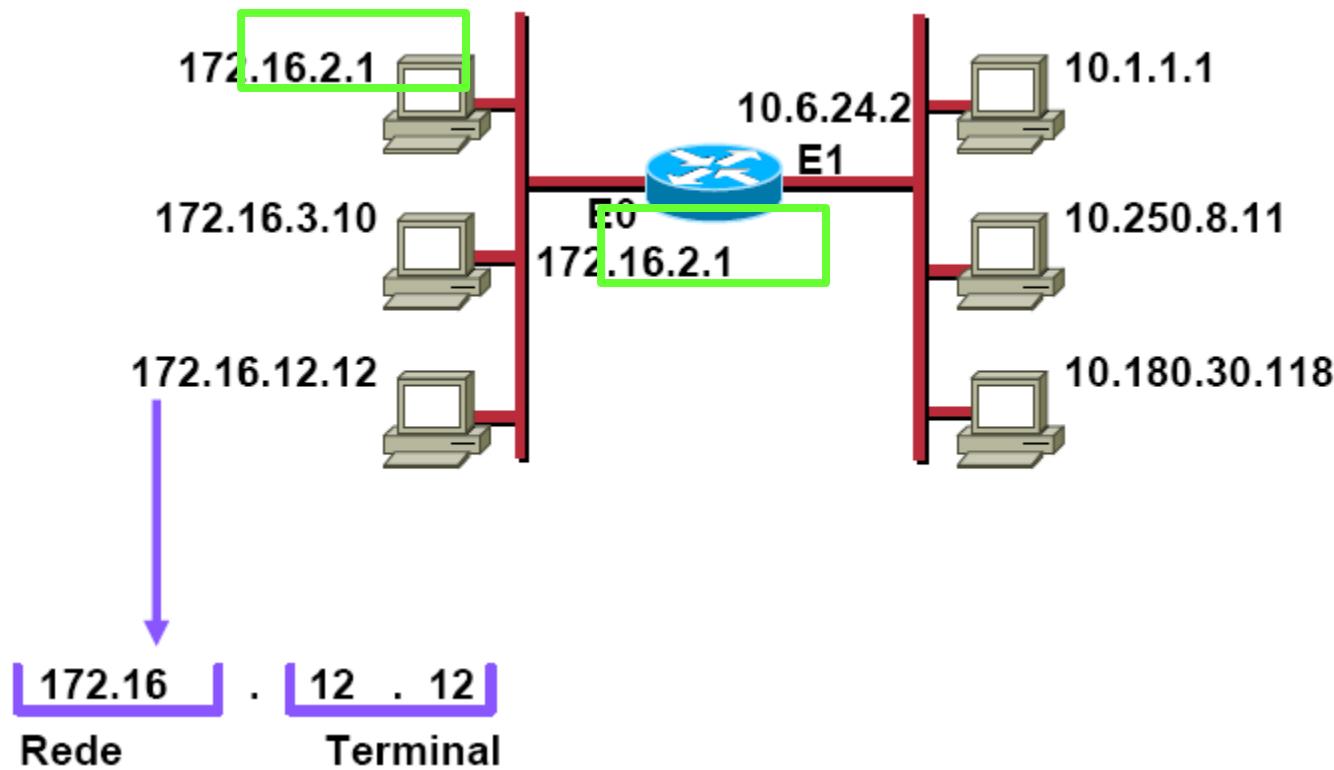
1. Octeto	Max. Redes	Formato	Exemplo	Max. Host
1-126	126	R.H.H.H	100.1.240.28	16.777.214
128-191	16.384	R.R.H.H	157.100.5.195	65.534
192-223	2.097.152	R.R.R.H	205.35.4.120	254
224-239	Multicast			
240-247	Reservado			

# Conflitos IP

- Para definirmos os IP's de uma rede, precisamos seguir estas duas regras:
  - Na mesma rede, os IP's de todas as máquinas devem estar na mesma rede.

Por exemplo: Endereços Classe A. (13.0.0.1, onde o 13 é rede e 0.0.1 é host);  
Todos os hosts desta rede devem estar na mesma rede, ou seja, com IP's começados por 13;
  - Numa mesma rede não poderá haver endereços IP's iguais.

# Conflitos IP



# Máscara de Sub-Rede

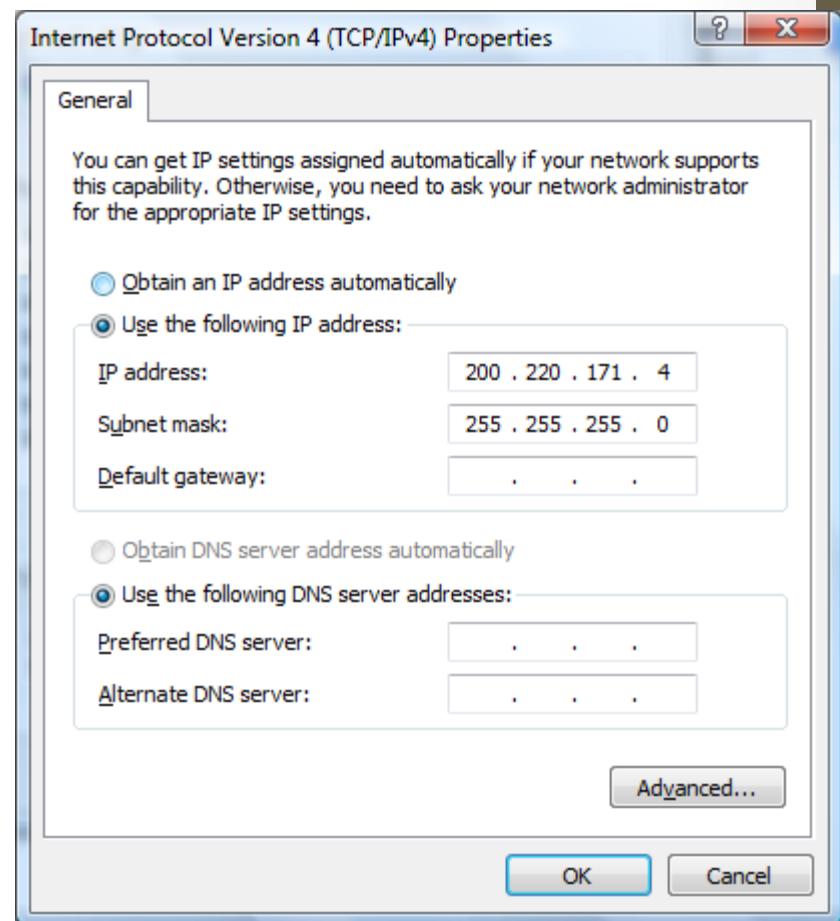
- Existem casos onde faz-se necessário subdividir uma rede em redes menores. Imagine o administrador de uma rede que contém 16 milhões de hosts. Ele deverá utilizar uma rede Classe A;
- A máscara de rede foi criada para formar sub-redes menores, e também possibilitar uma melhor utilização dos endereços IP disponíveis;
- Em resumo, o parâmetro Máscara de Sub-rede serve para confirmar ou alterar o funcionamento das Classes de endereços padrões do TCP/IP;
- Sempre deverá ser configurado o IP e a máscara em uma rede.

# Máscara de Sub-Rede

Endereço	Máscara	Classe	Sub-rede
131.108.2.10	255.255.255.0	B	131.108.2.0
15.6.24.20	255.255.0.0	A	15.6.0.0
168.124.36.12	255.255.255.0	B	168.124.36.0

# Máscara de Sub-rede

- Em uma rede, o primeiro endereço da rede identifica o endereço da rede em si, e não poderá ser utilizado em nenhum equipamento;
- O último endereço também não poderá ser utilizado, pois é reservado para broadcast dentro daquela rede;
- Exemplo:
  - IP: 200.220.171.4
  - Máscara: 255.255.255.0
  - Rede: 200.220.171.0
  - Broadcast: 200.220.171.255



# Máscara de Sub-Rede

- Também pode ser necessário, em casos especiais, subdividir ainda mais as classes de endereços IP;
- Para isso existem outras máscaras de IP conforme exemplos abaixo:
  - IP: **200.220.171.0** Mask: **255.255.255.0**  
Endereços entre: **200.220.171.0** e **200.220.171.255**
  - IP: **200.220.171.0** Mask: **255.255.255.128**  
Endereços entre: **200.220.171.0** e **200.220.171.127**
  - IP: **200.220.171.0** Mask: **255.255.255.192**  
Endereços entre: **200.220.171.0** a **200.220.171.63**
  - Etc.

# Endereços não válidos na Internet

- Quando quiser configurar uma rede local, você deve usar um dos endereços reservados; endereços que não existem na Internet e que por isso podemos utilizar à vontade em nossas redes particulares;
- As faixas abaixo são reservadas para uso em redes locais:

Faixa	Máscara
10.X.X.X	255.0.0.0
172.16.X.X até 172.31.X.X	255.255.0.0
192.168.X.X	255.255.255.0



# Endereço IPv5

- Protocolo de fluxo em tempo real (experimental);
- Nunca foi amplamente utilizado.

# Endereço IPv6

- Com a explosão da Internet e com o surgimento constante de novos serviços, os atuais IPv4 estão se tornando escassos. Surge então, a necessidade de implementarmos um novo padrão de endereçamento (IPv6);
- Ele é um número que foi criado para substituir o antigo IPv4. Possui 128bits, enquanto que o IPv4 possui apenas 32bits;
- Exemplo em representação hexadecimal:  
**1080:0:0:0:8:800:200C:417A**

# Endereços IPv6 - Benefícios

- **Capacidade expandida de Roteamento e Endereçamento:** o endereço IP foi aumentado de 32 para 128 bits;
- **Simplificação do formato do Cabeçalho (Header):** alguns campos do cabeçalho IPv4 foram retirados ou tornaram-se opcionais, para reduzir o processamento dos pacotes de dados mais comuns, e para manter o custo de banda do cabeçalho do IPv6 o mais reduzido possível, apesar do aumento do campo de endereços;
- **Outros benefícios:**
  - Qualidade de Serviço;
  - Autenticação e Privacidade.

# Endereço IPv6 - Interoperabilidade

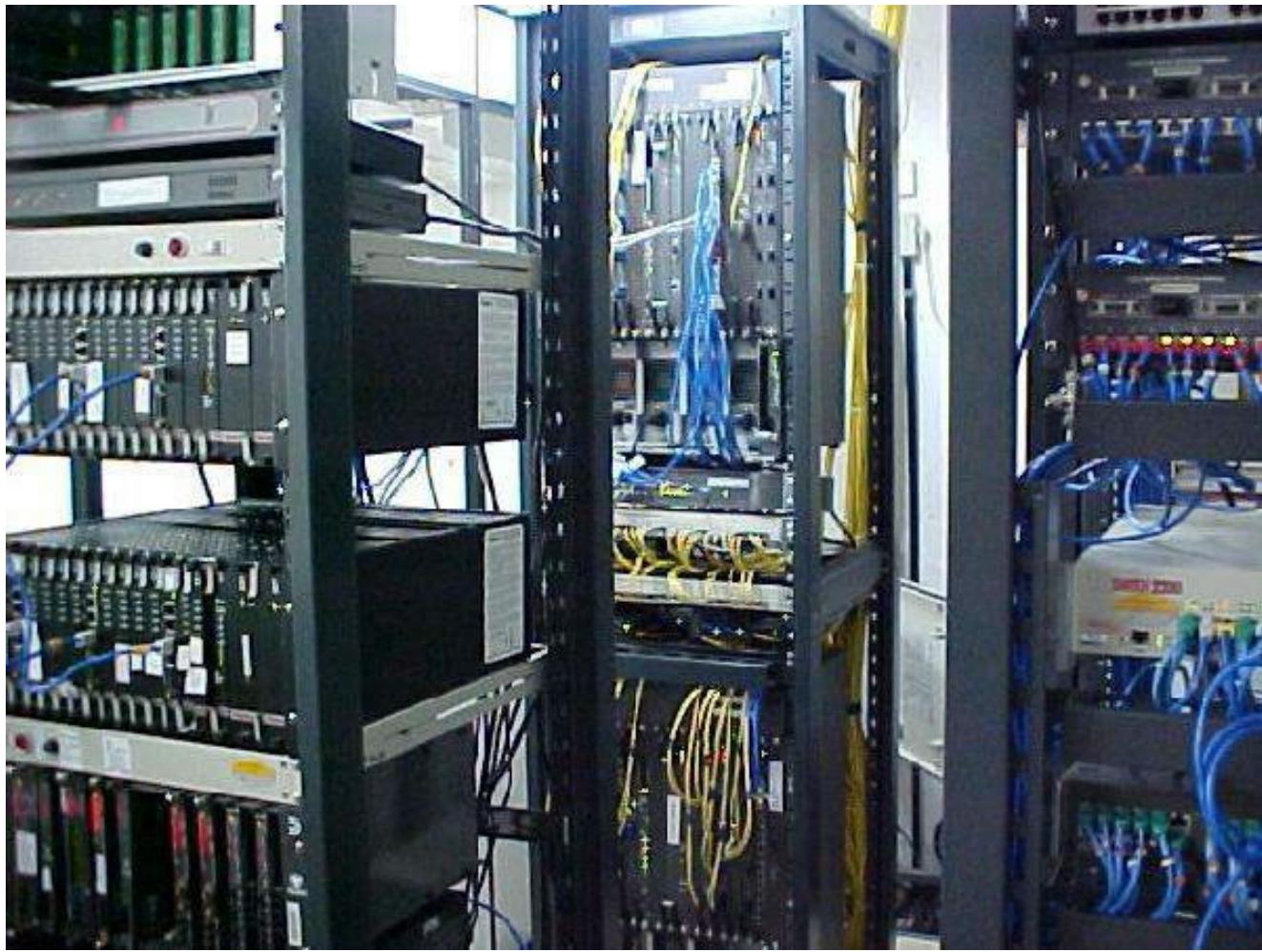
- Este padrão também foi criado para permitir que redes IPv4 possam se conectar em redes IPv6;
- Ex.: convertendo o endereço IPv4 (192.168.20.30) para IPv6:

**0:0:0:0:0:192.168.20.30**

# Broadcast

- Difusão, transmissão;
- Em redes, um endereço de *broadcast* é um endereço IP (e este é sempre o último endereço da rede);
- Permite que a informação seja enviada para todas as máquinas de uma TAN, LAN, MAN e WAN.

# Visão Geral de Equipamentos de Rede



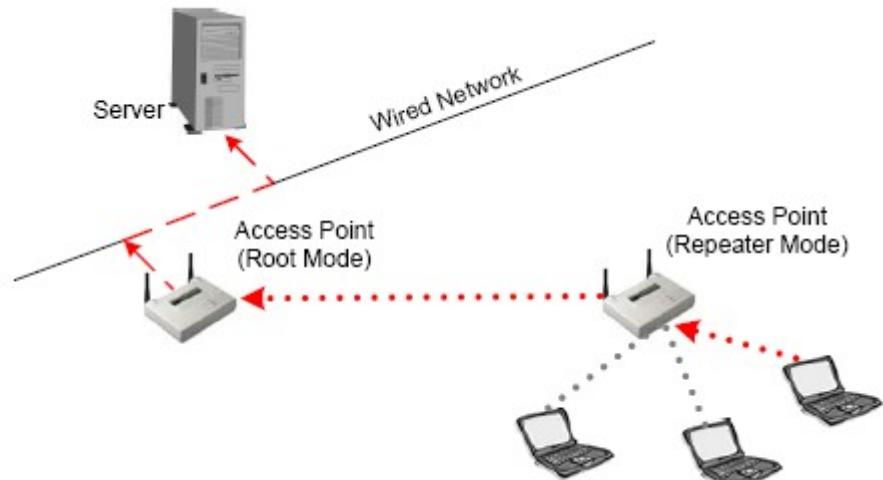
# Repetidor (Camada Física)

- O repetidor é um dispositivo responsável por *amplificar os sinais*, regenerando os sinais recebidos e transmitindo esses sinais para outro segmento da rede;
- Como o nome sugere, *ele repete as informações* recebidas em sua porta de entrada na sua porta de saída. Ele não faz análise dos quadros de dados para verificar para qual segmento o quadro é destinado;
- Apesar de aumentar o comprimento da rede, o repetidor pode interferir no seu desempenho, pois ele também amplifica “ruídos” que podem existir no sinal;
- Atualmente, os repetidores não são encontrados como equipamentos independentes, mas sim embutidos dentro de outros equipamentos, especialmente dentro dos hubs e switches.

# Repetidor (Camada Física)



Fonte:  
[http://sweet.ua.pt/~a35438/Otros/Redes%20de%20Computadores\\_ficheiros/repetidor.jpg](http://sweet.ua.pt/~a35438/Otros/Redes%20de%20Computadores_ficheiros/repetidor.jpg)  
Acesso em: 08 mar. 2009



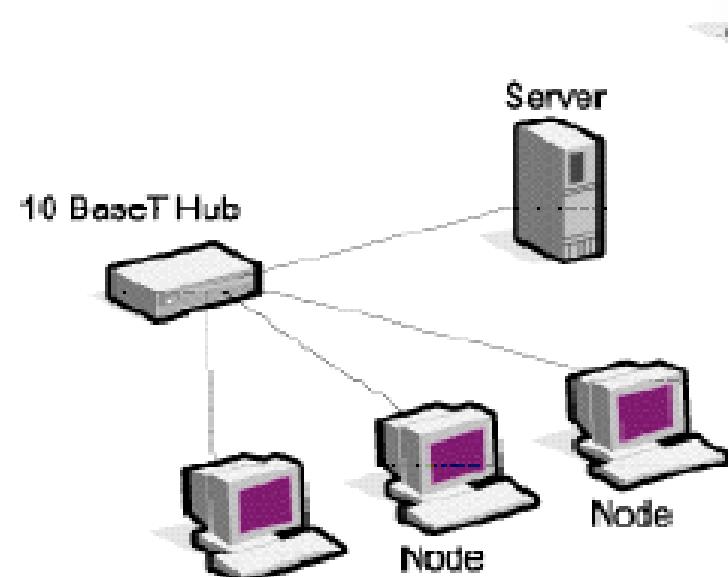
Fonte:  
[http://www.juliobattisti.org/tutoriais/paulocfarias/redeswireless008\\_clip\\_image014.jpg](http://www.juliobattisti.org/tutoriais/paulocfarias/redeswireless008_clip_image014.jpg)  
> Acesso em: 08 mar. 2009

# Hub (Camada Física)

- Os hubs são dispositivos concentradores, responsáveis por centralizar a distribuição dos pacotes nas redes fisicamente ligadas em *estrela*, apesar de funcionarem, do ponto de vista lógico, como **barramento**;
- Podemos conectar dois ou mais hubs entre si, num processo conhecido como [cascateamento](#);
- A maioria dos hubs possui uma porta chamada “Up Link”, que se destina justamente a esta conexão. Ela deve ser ligada numa porta comum de um outro hub com um cabo comum;
- Se o hub não possuir a porta de “Up Link”, podemos interligar os dois equipamentos através de um cabo de rede do tipo “[crossover](#)” conectado em portas comuns.

# Hub (Camada Física)

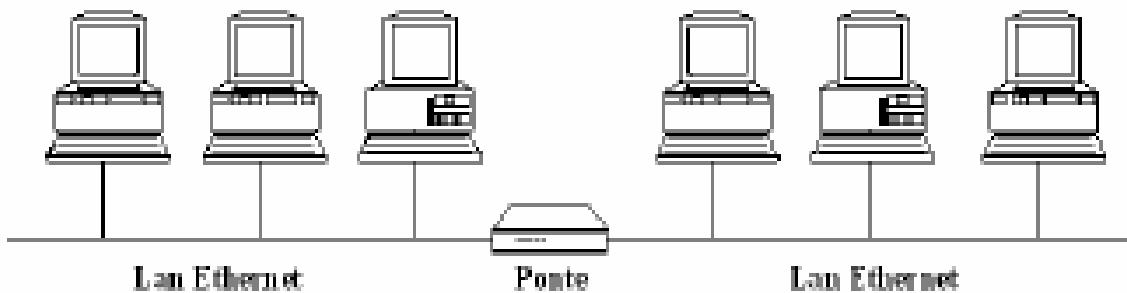
- O recurso de conectar hubs é recomendável somente em redes pequenas, pois qualquer sinal transmitido por um computador da rede será retransmitido para todos os outros. Quanto mais computadores existirem na rede, maior será o tráfego e mais lenta a rede será devido ao número crescente de “colisões”;
- Atualmente, existem hubs 10/100 com detecção automática de velocidade.



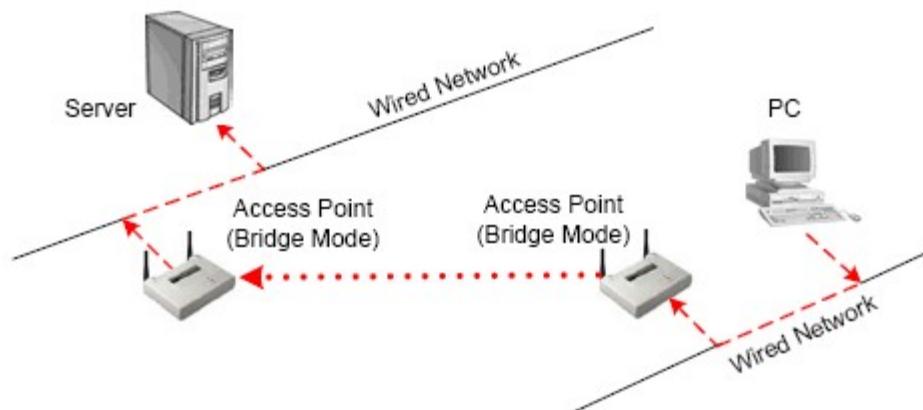
# Ponte (Bridge) - (Camada Enlace)

- A ponte é um equipamento “inteligente”, pois ela analisa os pacotes recebidos e verifica qual o destino. Se o destino for o trecho atual da rede, ela não replica o pacote nos demais trechos, diminuindo a colisão e aumentando a segurança;
- A verificação de um pacote para a determinação de qual trecho da rede ele pode trafegar é baseado no endereço **MAC** (*Media Access Control*), um número identificador único para cada interface de rede.

# Ponte (Bridge) - (Camada Enlace)



Fonte:  
[http://www.juliobattisti.org/tutoriais/paulocfarias/redeswireless08\\_clip\\_image002.jpg](http://www.juliobattisti.org/tutoriais/paulocfarias/redeswireless08_clip_image002.jpg) Acesso em: 08 mar. 2009

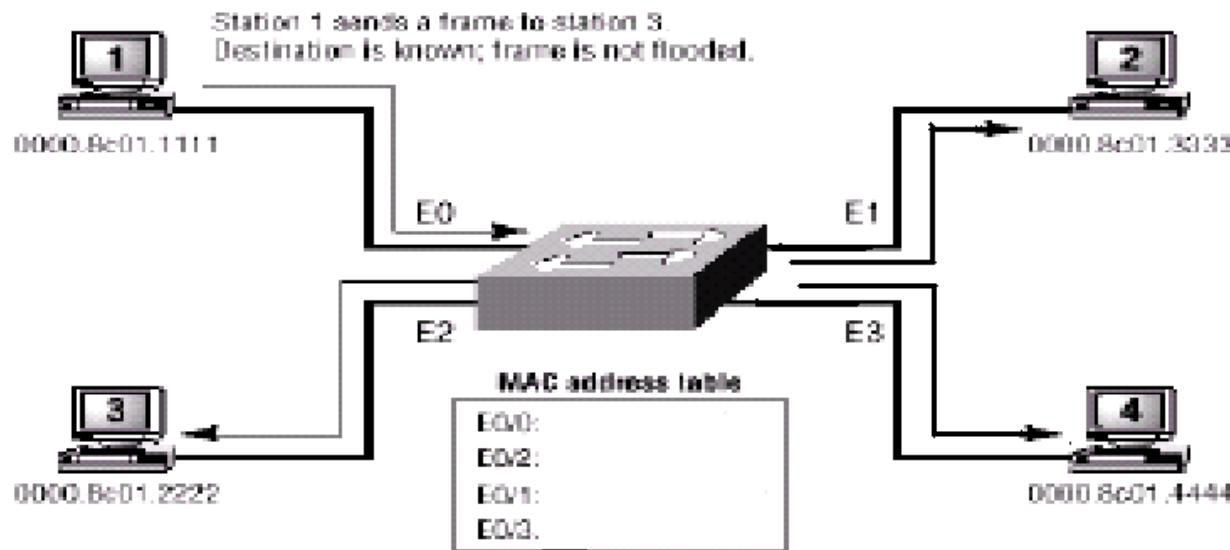


# Switch (Camada Enlace)

- O Switch é um equipamento que *envia os pacotes somente para o computador que os requisitou através da análise do endereço MAC* contido no cabeçalho do pacote, da mesma forma que uma Bridge;
- De maneira geral, a função do switch é muito parecida com a de uma ponte, com a exceção que ele tem mais portas e um melhor desempenho;
- Outra vantagem é que mais de uma comunicação pode ser estabelecida simultaneamente, desde que as comunicações não envolvam portas de origem ou destino que já estejam sendo usadas em outras comunicações.

# Switch (Camada Enlace)

## Aprendizagem de Endereços

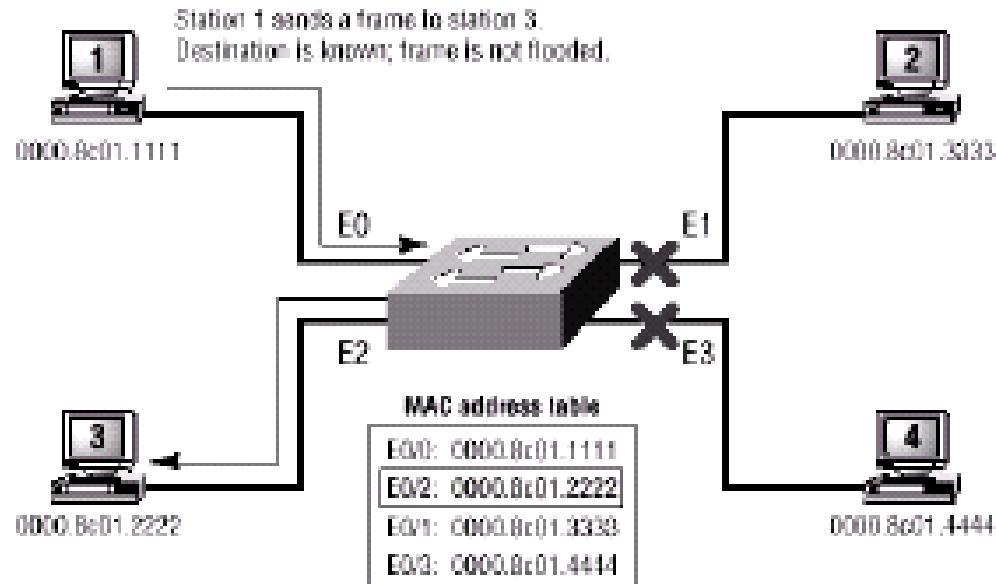


# Switch - Aprendizagem de Endereços

- O switch recebe o pacote que vem por um cabo, armazena o pacote, lê seu cabeçalho para saber origem e destino. Em seguida monta uma tabela com os valores dos endereços encontrados em cada cabo;
- Os switches possuem tabelas onde armazenam os endereços MAC “conhecidos” da rede, e sua correspondente porta de origem, chamadas de Source Address Tables (SAT);
- Estes endereços MAC são das estações de trabalhos, hubs “inteligentes”, outros switches, bridges ou roteadores;
- Se os endereços de (origem e destino) já existem na SAT, os switches implementam o repasse dos quadros de acordo com a informação do endereço de destino nele contida, e na porta de saída correspondente ao endereço MAC armazenado na SAT;
- Caso o endereço de origem não conste na SAT, esta será atualizada;
- Caso o endereço de destino não conste na SAT, o switch enviará os quadros para todos os cabos.

# Switch (Camada Enlace)

## Aprendizagem de Endereços



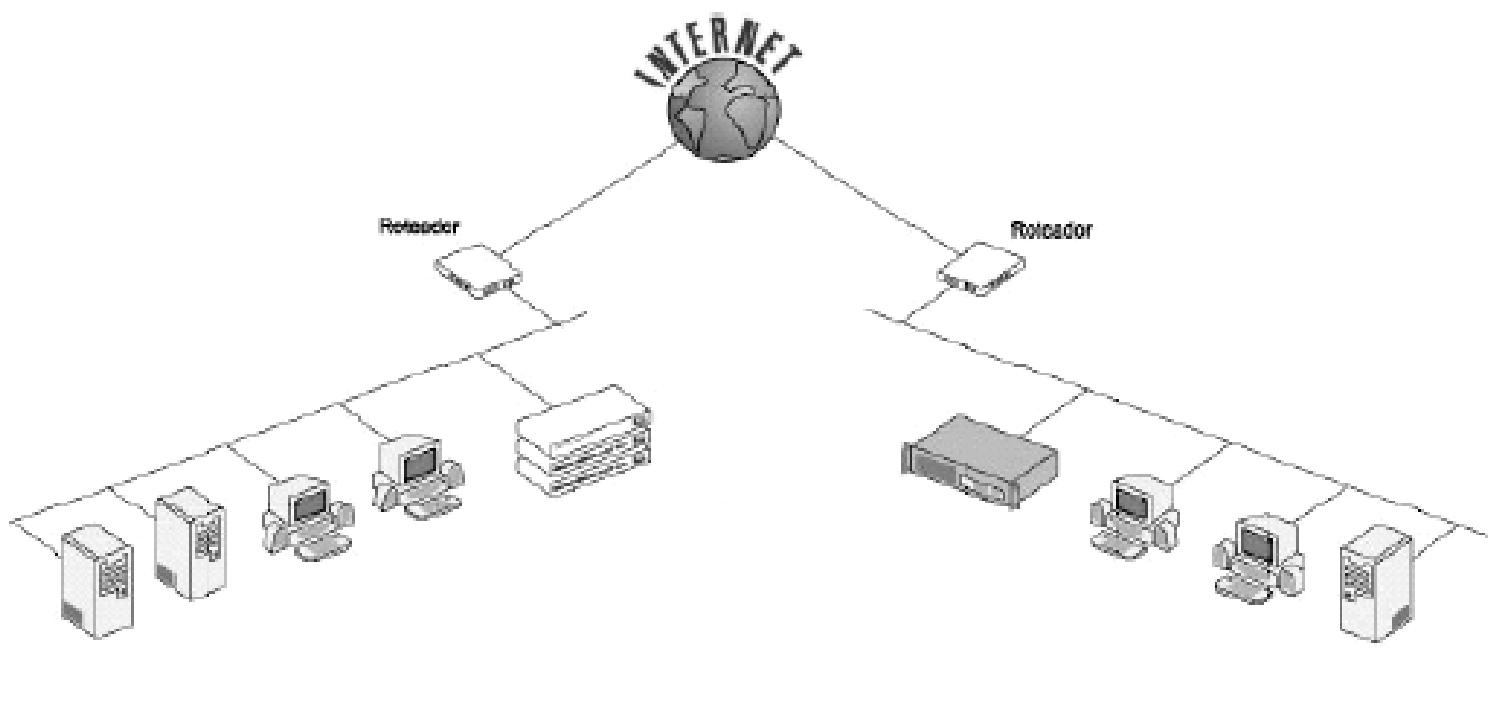
# Roteadores (Camada Rede)

- Os roteadores são responsáveis pelo *roteamento dos pacotes entre redes locais (LAN's) e redes de longa distância (WAN's);*
- Realizam o roteamento baseado em endereços IP's, e utilizam protocolos de roteamento (RIP, OSPF, BGP) para *escolha do melhor caminho;*
- É importante notar que o papel do roteador é interligar redes diferentes (redes independentes), enquanto que papel dos repetidores, hubs, pontes e switches são de interligar segmentos pertencentes a uma mesma rede.

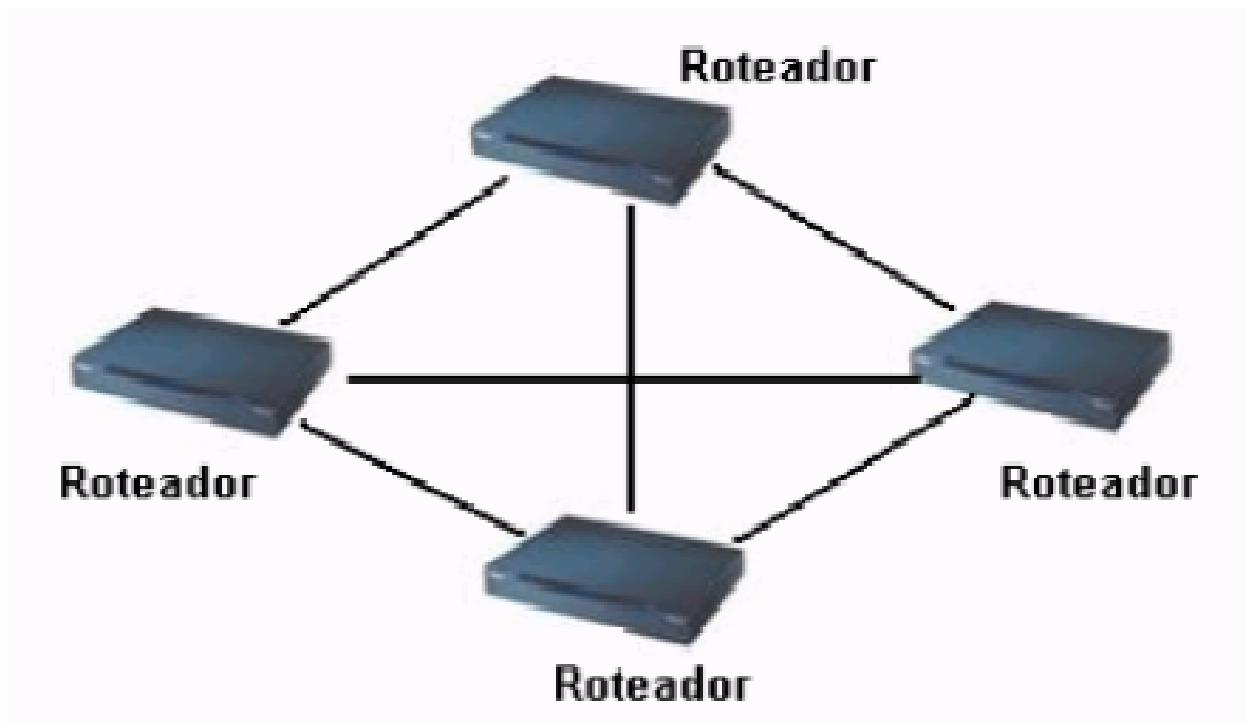
# Roteadores (Camada Rede)

- As etapas de um roteamento:
  1. O roteador recebe dados de uma de suas redes conectadas;
  2. O roteador passa os dados para a camada rede;
  3. O roteador verifica o endereço de destino do cabeçalho IP;
  4. O roteador consulta uma tabela de roteamento para determinar para onde encaminhará os dados.

# Roteadores (Camada Rede)



# Roteadores (Camada Rede)



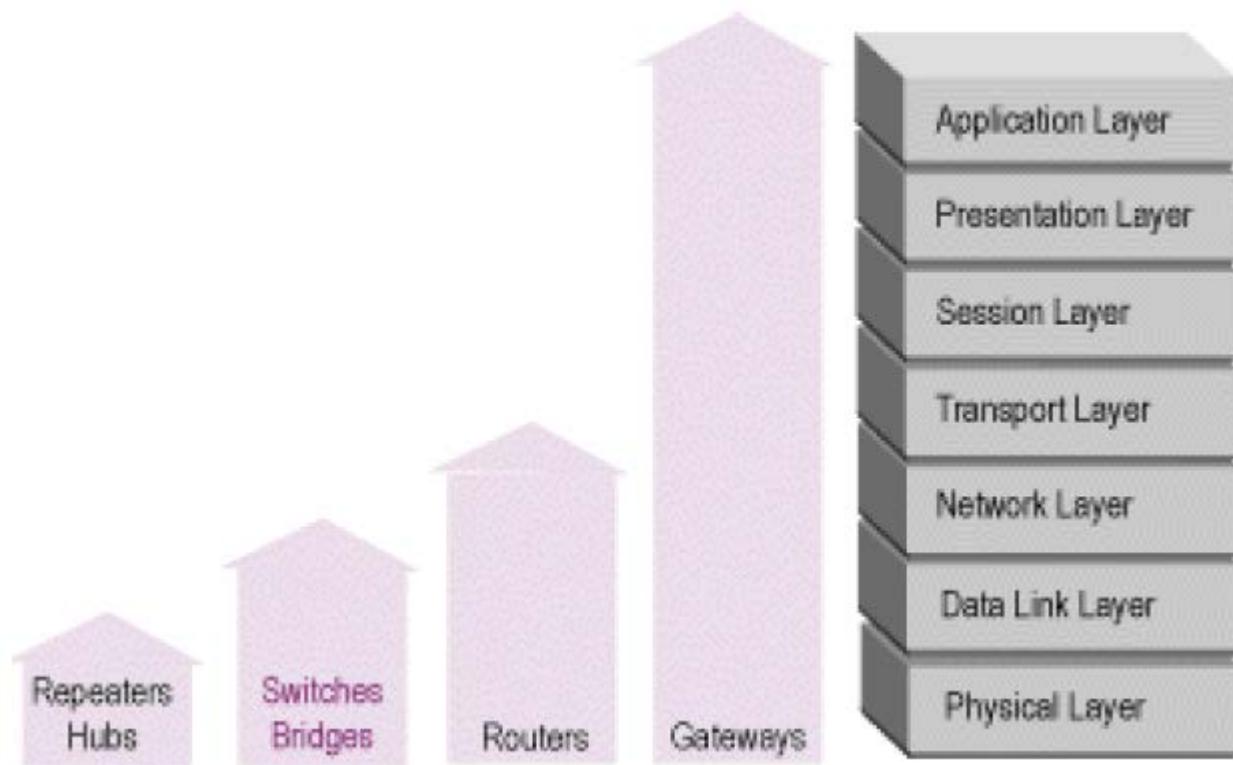
# Switch Camada 3 (Camada Rede)

- Existem alguns switches que atuam na camada 3 do modelo OSI (Rede), pois fazem a segmentação de rede através do endereço IP ao invés de utilizar a segmentação através do endereço MAC;
- Diferencia do roteador, pois o switch não faz escolha do melhor caminho para os pacotes.

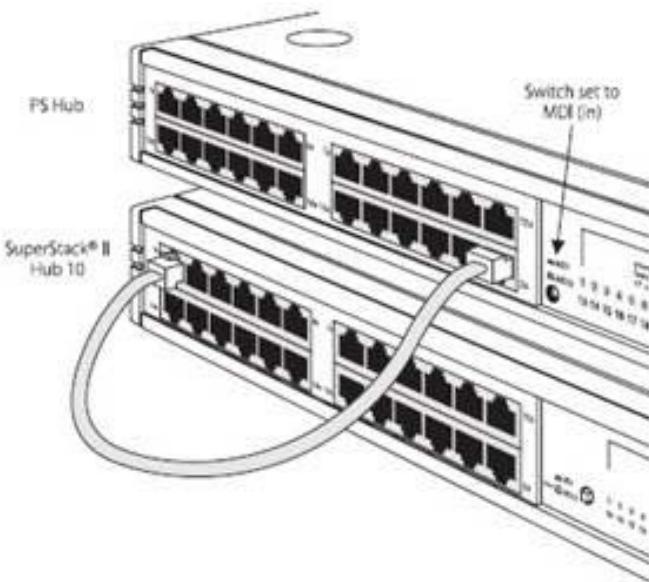
# Gateway

- Os gateways são constituídos por software e hardware necessário para unir dois ou mais tipos de rede. ***Eles atuam em todas as camadas do modelo OSI***, onde recompõem os pacotes de dados e os transmitem entre as redes;
- Um “gateway” é um equipamento intermediário, geralmente destinado a interligar redes de naturezas diferentes ou mesmo converter protocolos. Realizam a conversão de protocolos;
- Podemos considerar um “Access Point”, por exemplo, como um gateway, já que ele serve de intermediário entre duas redes de tecnologia diferentes.

# Resumo

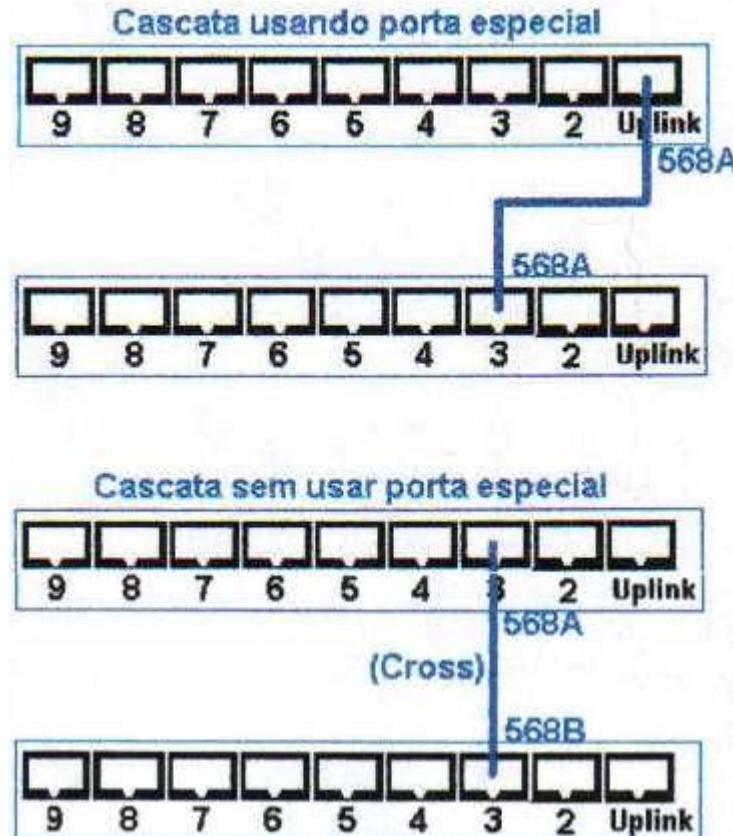


# Cascateamento de Hubs



Fonte:

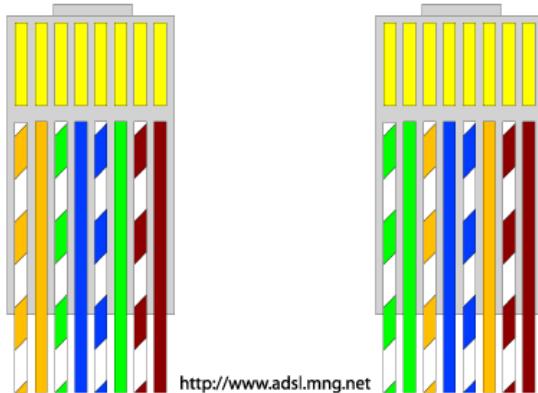
<[http://www.jullobattisti.org/tutoriais/paulocfarias/redesbasico019\\_clipping\\_image005.jpg](http://www.jullobattisti.org/tutoriais/paulocfarias/redesbasico019_clipping_image005.jpg)> Acesso em: 08 mar. 2009



Fonte: <<http://flipper.do.sapo.pt/files/rede/rede.h8.jpg>>  
Acesso em: 08 mar. 2009

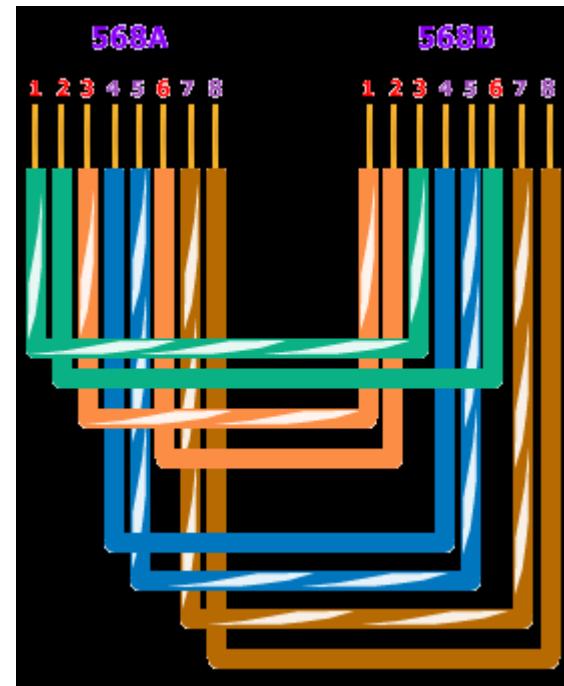
# Cabo Crossover

RJ45 Crossover Cable Standard



<http://www.adsl.mng.net>

Fonte:  
<<http://www.adsl.mng.net/zaavruud/rj45/crossover.png>> Acesso em: 08 mar. 2009



Fonte:  
<<http://www.conniq.com/images/Crossover.gif>>  
Acesso em: 08 mar. 2009



# Access Point

## Dual-Band Wireless Access Point Linksys a Division of Cisco Systems, Inc.



Fonte:

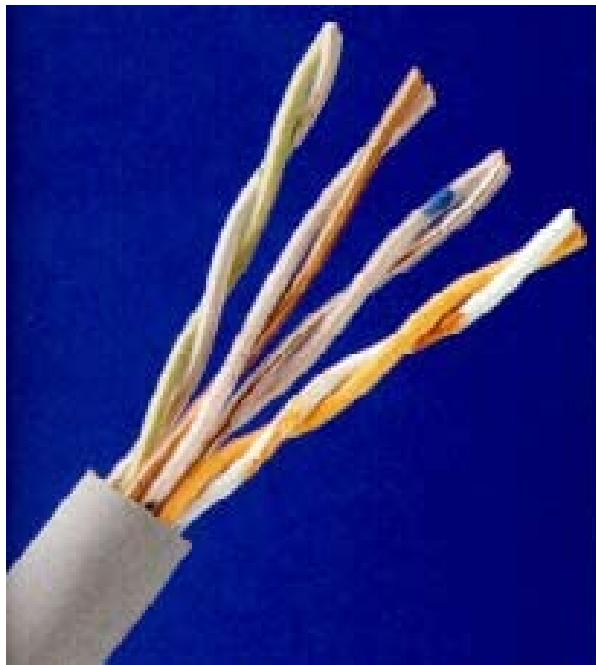
<<http://www.computercablestore.com/images/products/Linksys%20a%20Division%20of%20Cisco%20Systems%20Inc/WAP51AB.jpg>> Acesso em: 08 mar. 2009

# Visão Geral de Meios de Transmissão

# Meios de Transmissão

- Os meios de transmissão são tecnologias que provêm ***conexões entre as estações de uma rede LAN ou WAN;***
- Qualquer meio capaz de transportar informações eletromagnéticas pode ser usado em redes de computadores, sendo os mais utilizados os pares metálicos, cabos coaxiais, fibra óptica, sinais de rádio, satélites, telefonia celular, dentre outros.
- A maioria dos meios de acesso podem ser utilizados tanto em redes LAN's, quanto em redes WAN's

# Cabo Metálico - Par Trançado



Par Trançado sem Blindagem (UTP)



Par Trançado com Blindagem (STP)

Fonte: <<http://www.clubedohardware.com.br/printpage/181>> Acesso em: 09 mar. 2009

# Cabo Metálico - Par Trançado

- São dois fios enrolados em espiral, de forma a reduzir o ruído e manter constante as propriedades elétricas do meio, por todo o seu comprimento;
- Os tipos mais usuais em redes LAN's são:
  - Cabo sem blindagem (**UTP – Unshielded Twisted Pair**);
  - Cabo com blindagem (**STP – Shielded Twisted Pair**);
- São utilizados em Redes LAN's 100baseT / 10BaseT (onde T significa trançado);
- Utilizado também em redes externas para conexões telefônicas ou de última milha de redes WAN (última milha ou Last Mile é a conexão do cliente ao ponto de presença da empresa de telefonia mais próxima).

# Cabo Metálico - Par Trançado

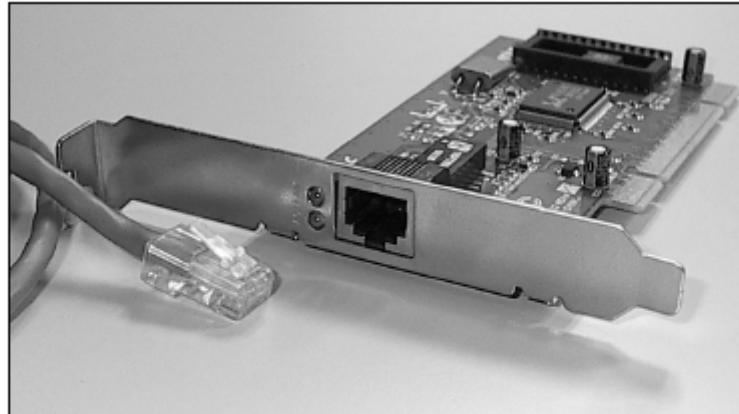
- **Vantagens**

- Baixo Custo;
- Facilidade de Instalação;

- **Desvantagens**

- Pequenas distâncias em rede LAN's (100 m).

# Cabo Metálico – Par Trançado

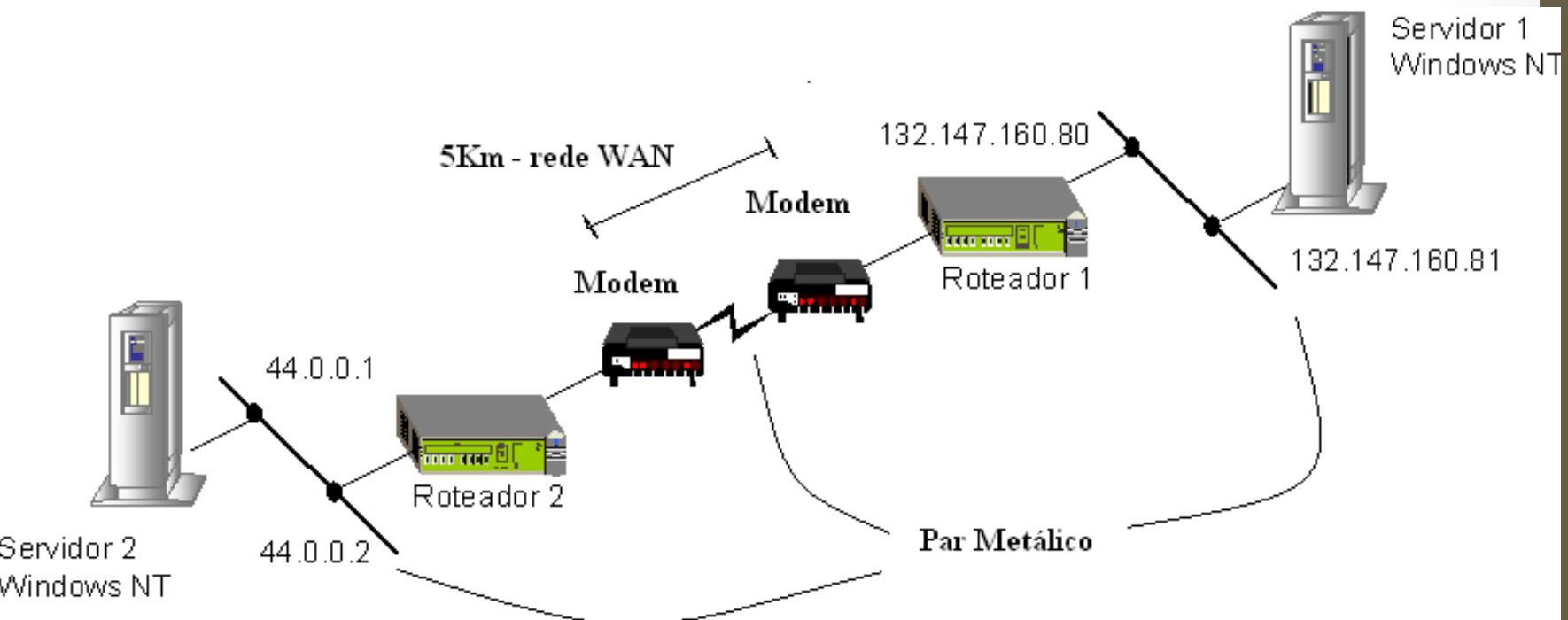


Conectores RJ-45 macho (montado no cabo UTP) e  
fêmea (montado na placa de rede)

# Cabo Metálico – Par Trançado

- **Modem:** Equipamentos utilizado em redes WAN para realizar a conversão do sinal proveniente do equipamento de rede (roteador, por exemplo) para um sinal capaz de trafegar no meio de acesso físico, no caso, par metálico (conf. figura no próximo slide);
- Exemplos:
  - Modem padrão V92 utilizado em linhas discadas com velocidade máxima de 56Kbps;
  - Modem ADSL – utilizado no serviço Velox da Telemar, Speed da Telefônica e etc.

# Cabo Metálico - Par Trançado



Padrão TIA EIA-  
568B

# Padrões

TIA/EIA 568A Wiring

1		White and Green
2		Green
3		White and Orange
4		Blue
5		White and Blue
6		Orange
7		White and Brown
8		Brown

TIA/EIA 568B Wiring

1		White and Orange
2		Orange
3		White and Green
4		Blue
5		White and Blue
6		Green
7		White and Brown
8		Brown

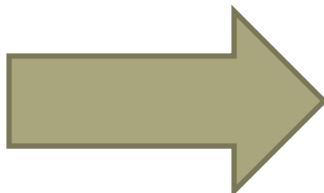
# Cabo Direto

- Utiliza somente os pinos 1 e 2 (TX) / 3 e 6 (RX);
- Cabo direto significa que a ligação é feita pino a pino;
- Utilizado para conectar equipamento diferentes. Ex.: Computador ao Hub.

Pin No.	Cor do fio	Nome do sinal
1	white and orange	TX_D1+
2	orange	TX_D1-
3	white and green	RX_D2+
4	blue	BI_D3+ **
5	white and blue	BI_D3- **
6	green	RX_D2-
7	white and brown	BI_D4+ **
8	brown	BI_D4- **

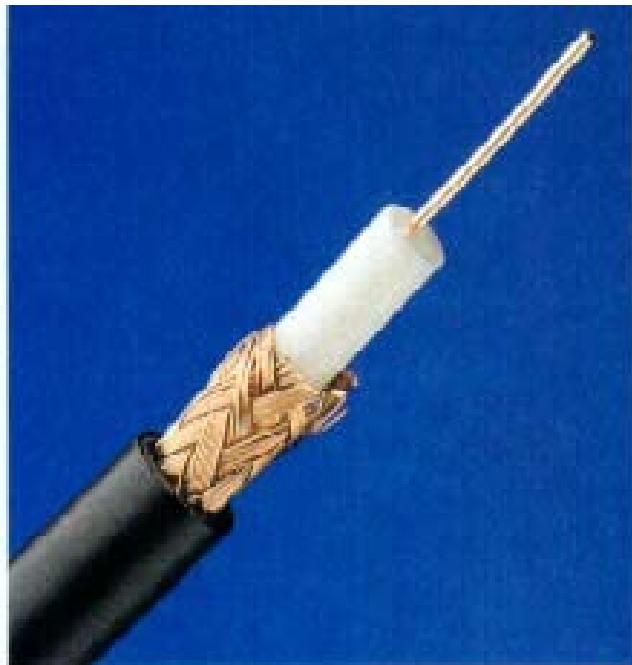
# Cabo Crossover (Cruzado)

- Cabo cruzado utilizado para conectar equipamento iguais. Exemplos:  
Hub/Hub e/ou  
Computador/Computador;
- Os pinos 1 e 2 (TX) são conectados aos pinos 3 e 6 (RX) e vice-versa.

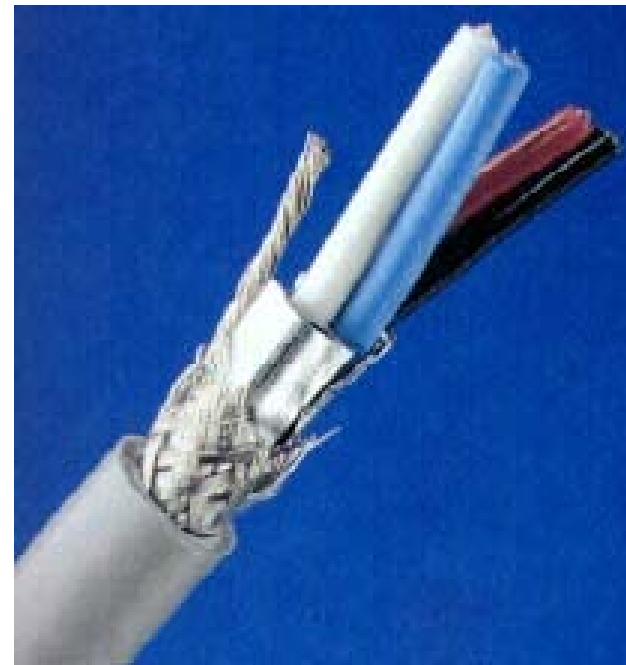


Ficha RJ45 num lado	Ficha RJ45 no outro lado
1	3
2	6
3	1
4 *	5 *
5 *	4 *
6	2
7 *	8 *
8 *	7 *

# Cabo Coaxial



**Cabo Coaxial Fino (10Base2)**



**Cabo Coaxial Grosso (10Base5)**

Fonte: <<http://www.clubedohardware.com.br/printpage/181>> Acesso em 09 mar. 2009

# Cabo Coaxial

- Cabo formado por um condutor central envolvido por uma malha externa;
- Os cabos coaxiais de maior qualidade não são maleáveis, sendo mais difíceis de instalar;
- Mais utilizados em redes LAN's:
  - 10base2 – 200mts – Cabo coaxial fino;
  - 10base5 – 500mts – Cabos coaxial grosso;
- Outras utilizações:
  - Interligações de sistemas E1 de voz (conexões entre PABX's);
  - Redes de TV a CABO.

# Cabos Coaxial

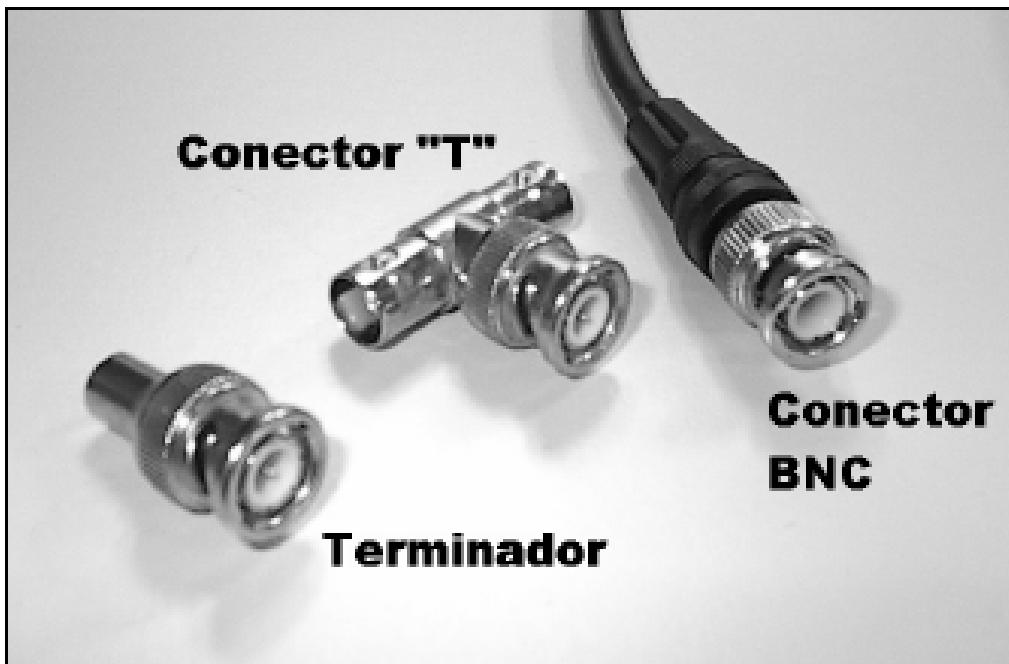
- **Vantagens:**

- Maiores distâncias;
- Maior imunidade a ruído;

- **Desvantagens:**

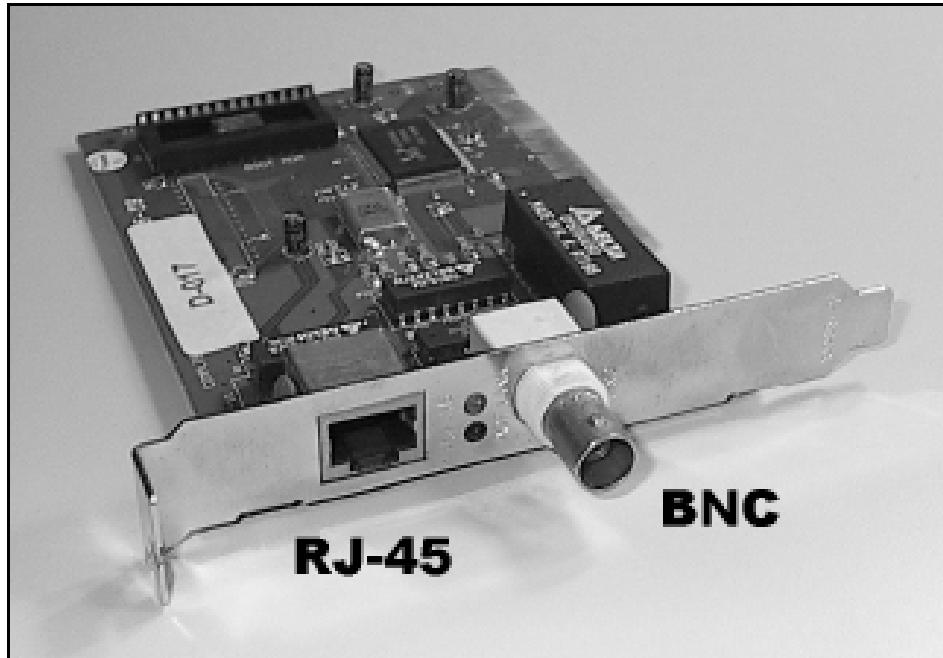
- Não é flexível, dificultando a instalação;
- Maior custo se comparado ao par metálico.

# Cabo Coaxial



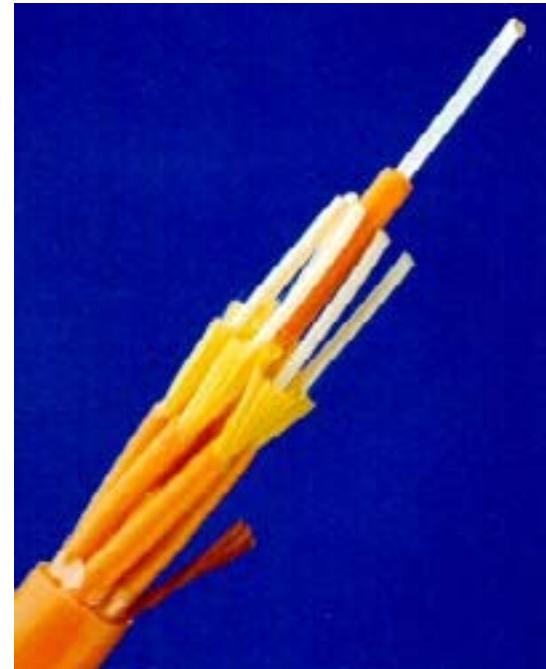
Utilizados para conexões no meio do cabo  
(conector "T") ou nas extremidades

# Cabos Coaxiais



Utilizado normalmente em redes de cabos coaxiais

# Fibra Óptica

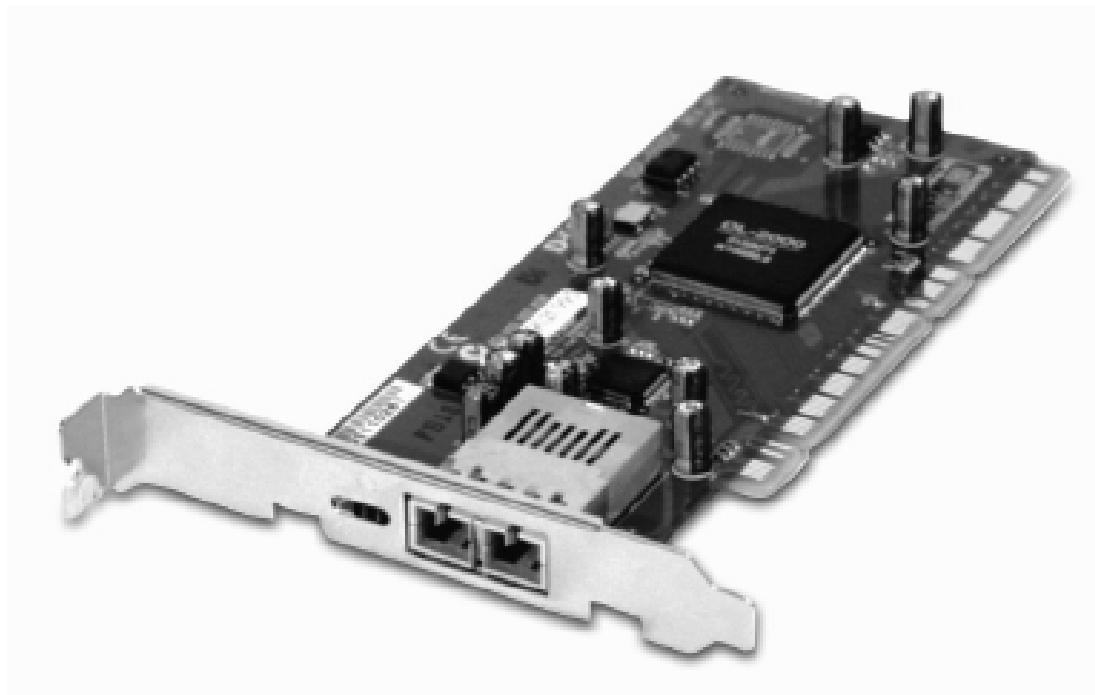


Fonte: <<http://www.clubedohardware.com.br/printpage/181>> Acesso em 09 mar. 2009

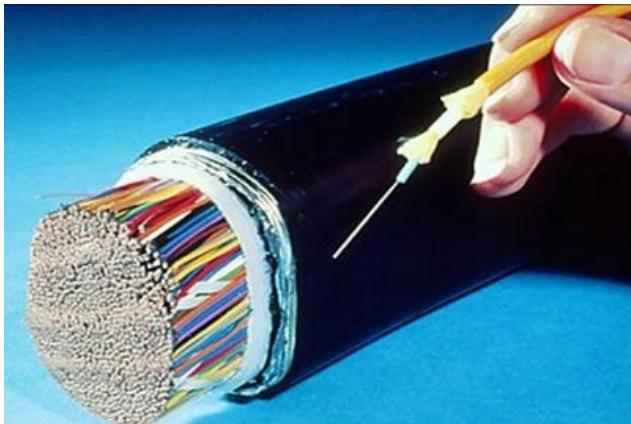
# Fibra Óptica

- A transmissão da informação é feita através de sinais luminosos infravermelho ou visível;
- As fibras ópticas são imunes a interferências eletromagnéticas, ruídos elétricos e sofrem menos atenuações de sinal;
- Devido a estas características, as fibras possuem grandes capacidades de transmissão de sinais (altas velocidades) e atingem grandes distâncias;
- Podem ser utilizadas em redes WAN's e LAN's ([10BaseFL](#), [100baseFX](#), [1000BaseSX](#), [1000BaseLX](#)).

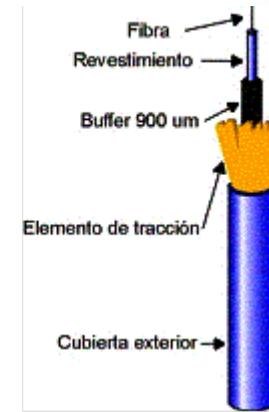
# Fibra Óptica



# Fibra Óptica



Cabo de uso externo



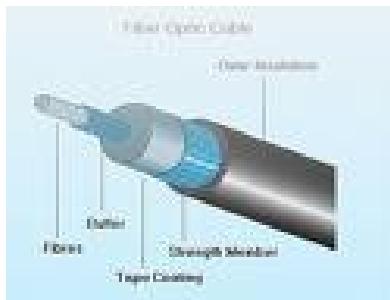
Cabo de uso interno



Cabos anti-roedores



Cabos auto-sustentável



# Sistemas Rádio

# Sistemas Rádio

- Utiliza ondas eletromagnéticas entre Transmissor e receptor.  
Exemplos: Rede Wireless e Redes Celulares;
- Em redes LAN's, temos o padrão IEEE 802.11 (a,b ou g) já estudado, utilizado já em grande escala;
- Em rede WAN's, além do padrão ainda em fase de estudos IEEE 802.20 para conexões de alta velocidade (ponto multiponto), temos vários soluções ponto-a-ponto utilizadas para conexões de rede dedicadas.

# Sistemas Rádio

- **Ponto-a-ponto:** ligação de dois pontos através de um par de freqüências (ida e volta), nas faixas de 400 MHz, 900 MHz, 8,5 GHz, 15 GHz, 18 GHz, 23 GHz e 38 GHz (Modulação FDD), ou de uma única freqüência, na faixa de 2,4 GHz (Modulação TDD);
- **Ponto Multiponto:** ligação de um ponto a vários pontos através de um par de freqüências (ida e volta), nas faixas de 400 MHz e 2 GHz. Será utilizado no padrão IEEE 802.20 (somente o conceito de multiponto, pois a freqüências a serem utilizadas serão outras).

# Sistemas Rádio

- Acess Point de uma rede IEEE 802.11 (ponto-multiponto)

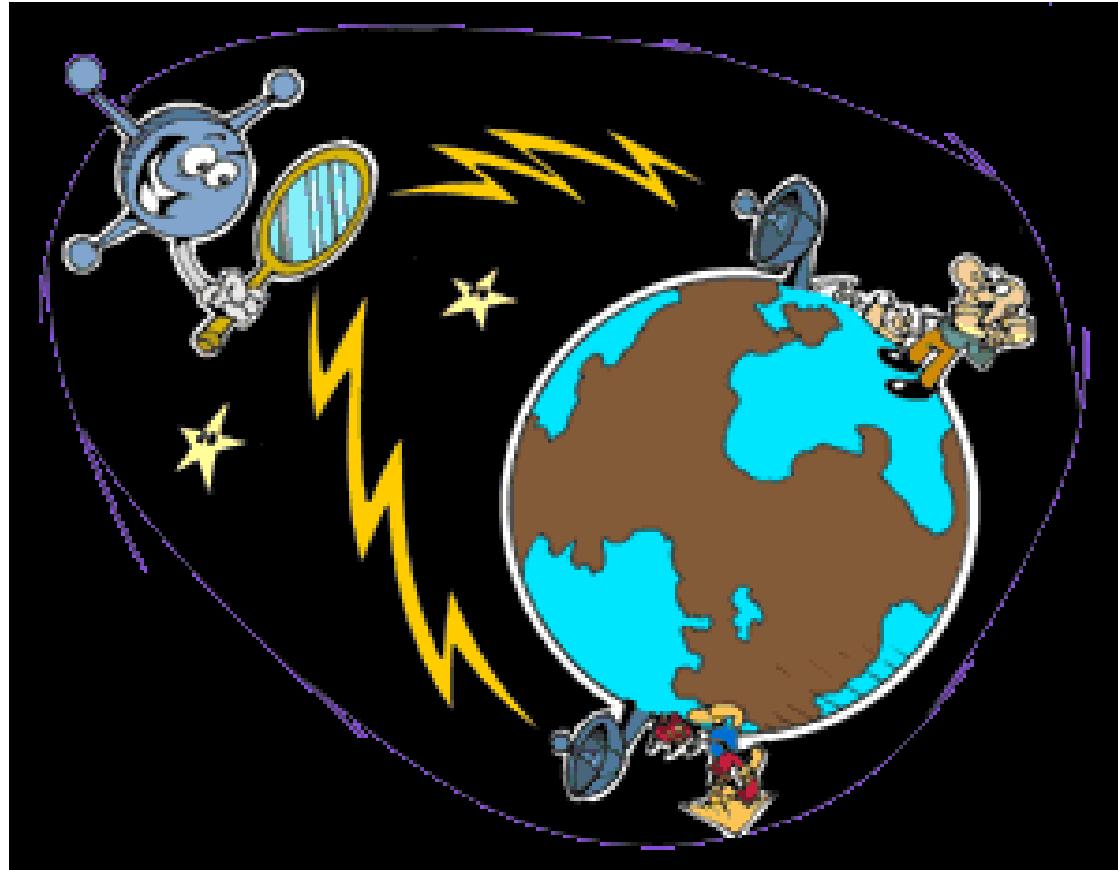


# Sistemas Rádio

Antenas Ponto a Ponto para  
Conexões WAN



# Satélite



Fonte: <<http://www.canalkids.com.br/tecnologia/invencoes/imagens/telstar.gif>> Acesso em: 09 mar. 2009

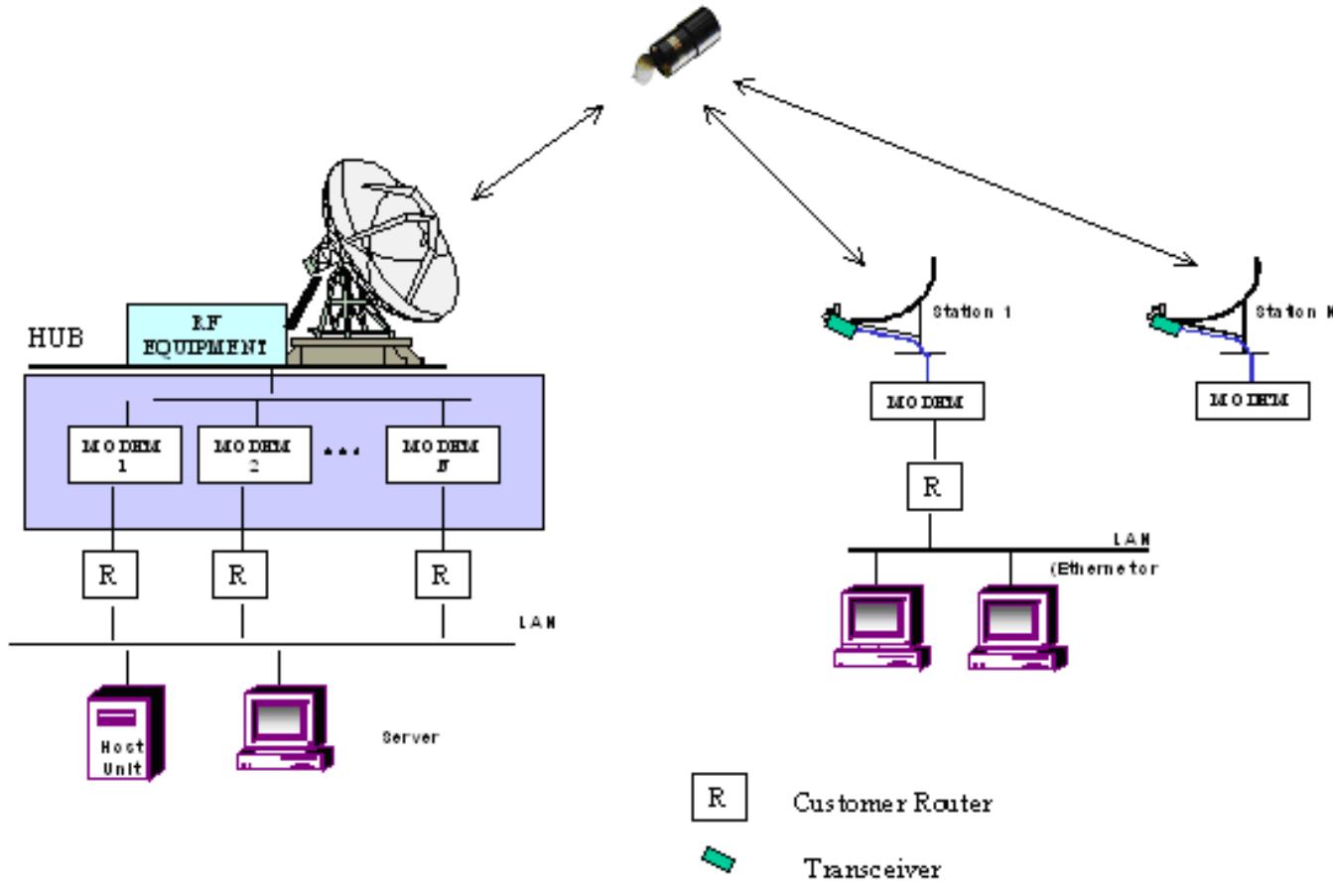
# Satélites

- Utiliza comunicação via Satélite entre Receptor e Transmissor. Indicado para locais onde a chegada dos demais meios de acesso não é viável, pois trata-se da solução mais cara existente;
- Os Sistemas Satélite são constituídos de duas partes bem definidas: Segmento Espacial (Satélite) e Segmento Terrestre (Estações Terrenas);
- Freqüências utilizadas: faixa de 5MHz (banda C - antenas maiores), 12MHz (banda Ku – antenas menores) e outras.

# Satélites

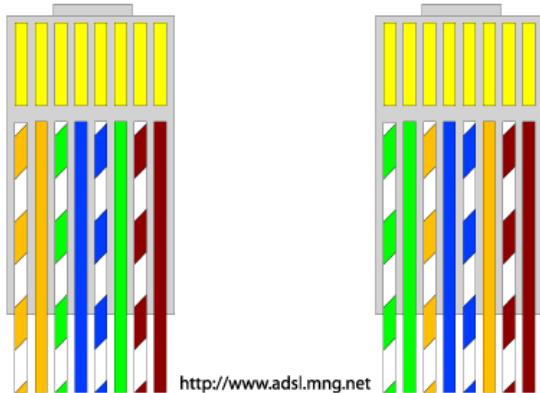


# Satélite



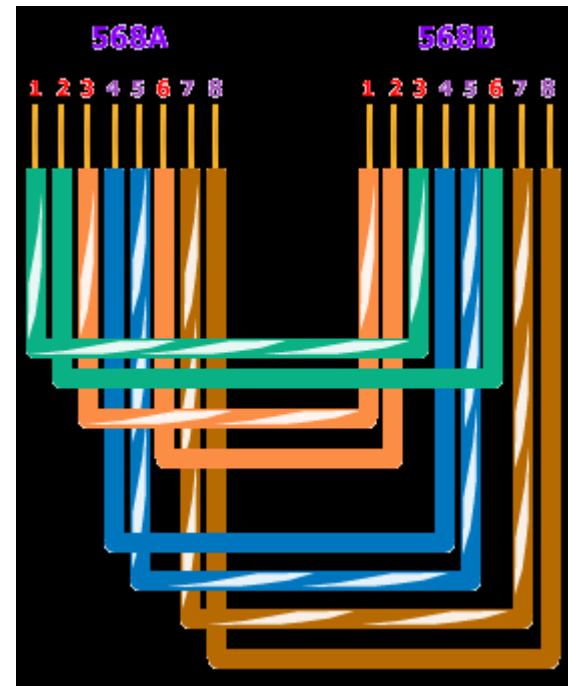
# Cabo Crossover

RJ45 Crossover Cable Standard



<http://www.adsl.mng.net>

Fonte:  
<<http://www.adsl.mng.net/zaavruud/rj45/crossover.png>> Acesso em: 08 mar. 2009

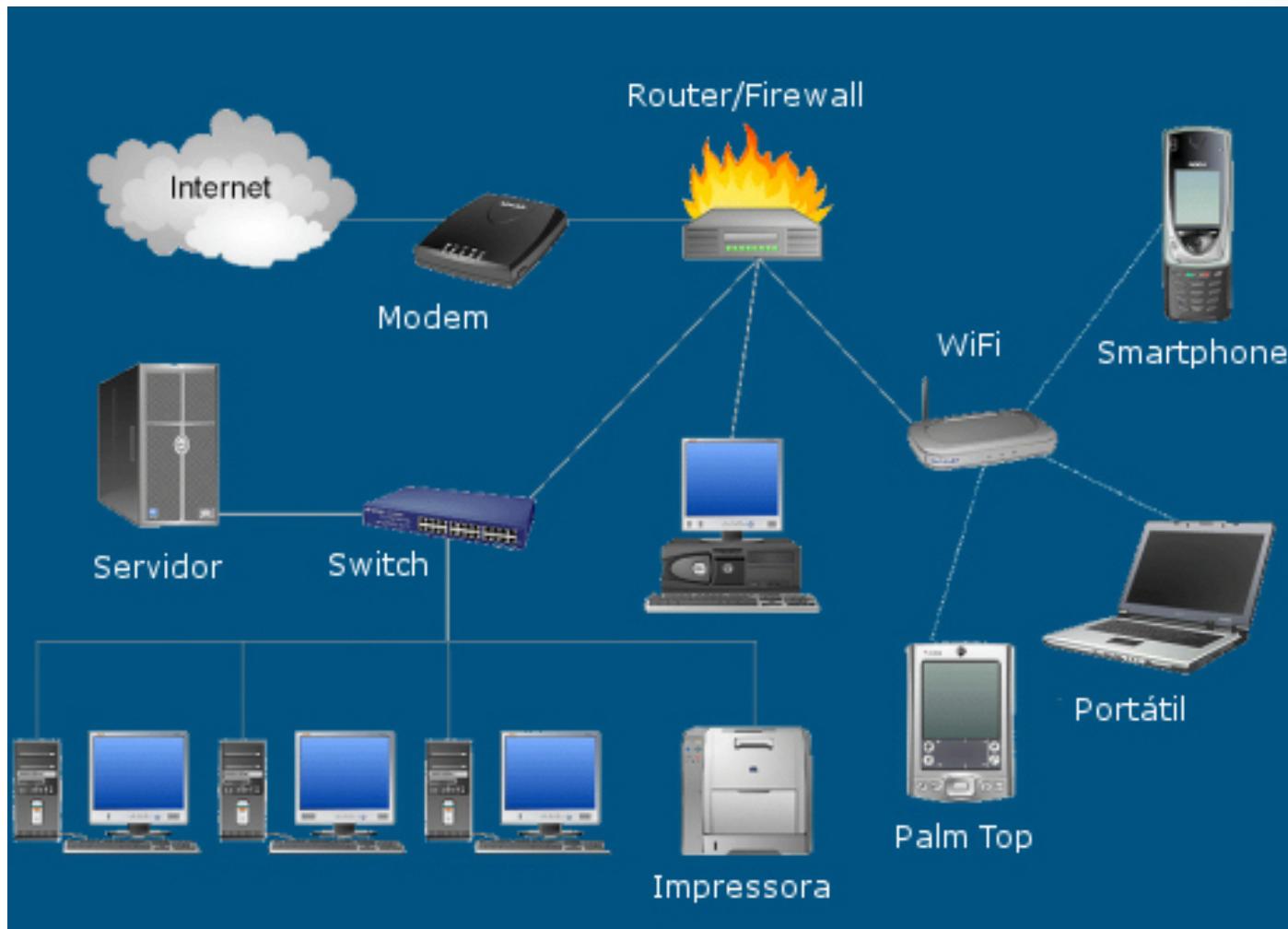


Fonte:  
<<http://www.conniq.com/images/Crossover.gif>>  
Acesso em: 08 mar. 2009



# Utilitários de Redes

# Utilitários de Redes



# **Utilitários de Redes**

- No windows existem alguns utilitários de rede disponíveis através do prompt do DOS;
- São baseados em programas originados do sistema operacional UNIX, com a mesma função;
- Os utilitários mostrados são idênticos aos do Unix, com as exceções do traceroute (que no Windows tem o nome de tracert, devido à antiga limitação de 8 caracteres para nomes de programas do DOS) e o comando ipconfig (que no Unix/Linux é ifconfig);

- 1. Ping**
- 2. Traceroute/tracert**
- 3. Route**
- 4. Nslookup**
- 5. Ipconfig**
- 6. Netstat.**

# Ping

- O utilitário ping (analogia com o jogo de ping-pong) serve para verificar a resposta de um outro servidor na rede até a camada de rede (endereço IP);
- O ping envia pacotes **ICMP** (Internet Control Message Protocol), requisitando uma resposta do servidor remoto. A resposta do servidor normalmente é o mesmo pacote enviado. Ou seja, a máquina remota simplesmente devolve os dados que ela recebeu;
- O objetivo é testar se além da rede estar funcionando corretamente até a camada de rede, a mesma não está fazendo nenhuma tradução nos bytes enviados;
- **Sintaxe:** ping endereço ou IP

# Ping

- No caso de um endereço não responder aos pacotes enviados, isto não indica necessariamente que o computador consultado está fora do ar. Pode ter sido configurado um filtro que impeça que a máquina responda através do Firewall.

# Ping - URL Ok!

```
C:\WINDOWS\system32\cmd.exe
C:\>ping www.terra.com.br

Pinging www.terra.com.br [200.176.3.142] with 32 bytes of data:

Reply from 200.176.3.142: bytes=32 time=64ms TTL=240
Reply from 200.176.3.142: bytes=32 time=79ms TTL=240
Reply from 200.176.3.142: bytes=32 time=73ms TTL=240
Reply from 200.176.3.142: bytes=32 time=86ms TTL=240

Ping statistics for 200.176.3.142:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 64ms, Maximum = 86ms, Average = 75ms

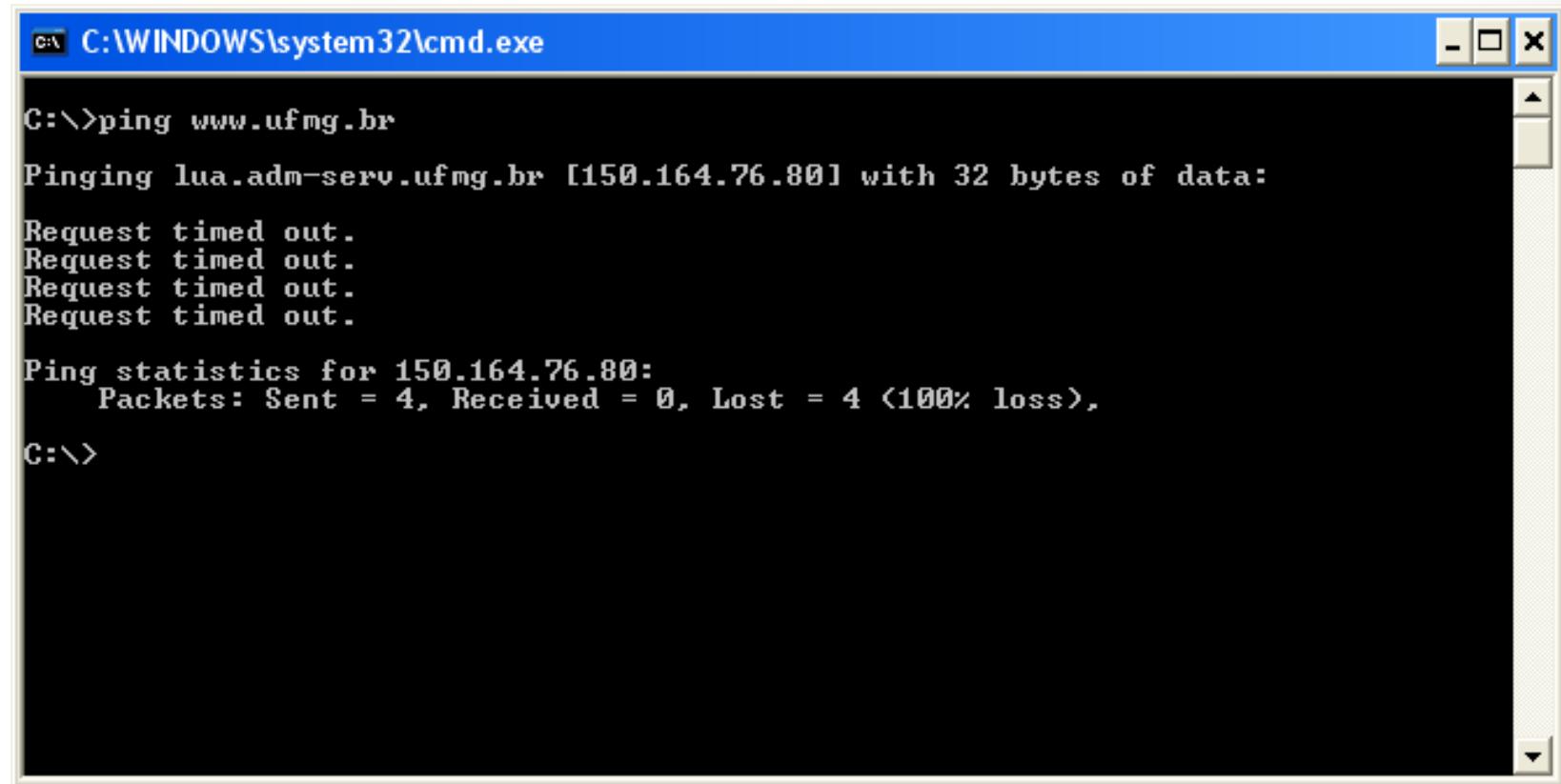
C:\>_
```

# Ping – IP Ok!

```
C:\WINDOWS\system32\cmd.exe
C:\>ping 200.219.214.18
Pinging 200.219.214.18 with 32 bytes of data:
Reply from 200.219.214.18: bytes=32 time=38ms TTL=52
Reply from 200.219.214.18: bytes=32 time=34ms TTL=52
Reply from 200.219.214.18: bytes=32 time=35ms TTL=52
Reply from 200.219.214.18: bytes=32 time=48ms TTL=52

Ping statistics for 200.219.214.18:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 34ms, Maximum = 48ms, Average = 38ms
C:\>
```

# Ping – URL Não Respondendo



C:\WINDOWS\system32\cmd.exe

```
C:\>ping www.ufmg.br

Pinging lua.adm-serv.ufmg.br [150.164.76.80] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 150.164.76.80:
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
```

# Ping – Help!

```
C:\WINDOWS\system32\cmd.exe
C:\>ping

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
           [-r count] [-s count] [[-j host-list] | [-k host-list]]
           [-w timeout] target_name

Options:
  -t             Ping the specified host until stopped.
                  To see statistics and continue - type Control-Break;
                  To stop - type Control-C.
  -a             Resolve addresses to hostnames.
  -n count       Number of echo requests to send.
  -l size        Send buffer size.
  -f             Set Don't Fragment flag in packet.
  -i TTL         Time To Live.
  -v TOS         Type Of Service.
  -r count       Record route for count hops.
  -s count       Timestamp for count hops.
  -j host-list   Loose source route along host-list.
  -k host-list   Strict source route along host-list.
  -w timeout     Timeout in milliseconds to wait for each reply.

C:\>
```

# Ping

- Exemplo ao vivo!

# Tracert

- O utilitário traceroute serve para nos mostrar por onde um pacote IP trafega quando é enviado;
- Esse utilitário é tão útil quanto o **ping** e no Windows está disponível com o nome de **tracert**;
- Com seu resultado um administrador de rede pode verificar em qual ponto uma comunicação pode estar rompida ou com tráfego congestionado;
- **Sintaxe:** tracert endereço ou IP

# Tracert

- O traceroute funciona enviando sucessivos pacotes IP de ping com o valor do TTL iniciando em 1 e aumentando até o ping ser respondido pelo destino. Isso faz com que o pacote IP "morra" cada vez mais longe da origem;
- Para cada vez que o TTL chega a zero (o pacote "morre"), o roteador onde isso ocorreu envia um pacote ICMP para a origem;
- Desta forma, a origem tem como saber qual é o endereço do roteador onde o pacote IP morreu e consequentemente a rota dele até o destino.

# Tracert – URL Ok!

```
C:\WINDOWS\system32\cmd.exe
C:\>tracert www.yahoo.com.br
Tracing route to frontpage.americas.fy5.b.yahoo.com [200.152.161.132]
over a maximum of 30 hops:
 1   1 ms    1 ms    1 ms  192.168.0.1
 2   3 ms    2 ms    2 ms  192.168.1.254
 3   6 ms    9 ms    4 ms  netctr122.netcetera.com.br [192.168.122.1]
 4   21 ms   6 ms   22 ms  10.0.2.1
 5   9 ms   19 ms    9 ms  10.0.5.62
 6   7 ms    7 ms   23 ms  201-048-012-254.static.ctbc.com.br [201.48.12.25
4]
 7   16 ms   27 ms   19 ms  201-048-005-162.static.ctbctelecom.com.br [201.4
8.5.162]
 8   17 ms   18 ms   28 ms  201-048-230-193.static.ctbctelecom.com.br [201.4
8.230.193]
 9   21 ms   16 ms   20 ms  201-048-250-141.static.ctbc.com.br [201.48.250.1
41]
10   21 ms   32 ms   41 ms  201-048-044-006.static.ctbc.com.br [201.48.44.6]
11   35 ms   35 ms   38 ms  201-048-044-014.static.ctbc.com.br [201.48.44.14
]
12   39 ms   51 ms   49 ms  ge-3-2-0-10.ptt.ro002.spo.tivit.net.br [200.185.
4.2]
13   40 ms   52 ms   36 ms  ext-a.ra002.spo.tivit.net.br [200.185.6.8]
14   40 ms   43 ms   62 ms  200.185.6.68
15   65 ms   35 ms   50 ms  200.185.60.34
16   36 ms   63 ms   39 ms  unknown-200-152-162-227.yahoo.com [200.152.162.2
27]
17   39 ms   43 ms   35 ms  slb1.bro.yahoo.com [200.152.160.30]
18   40 ms   38 ms   36 ms  hp2.latam.vip.bro.yahoo.com [200.152.161.132]

Trace complete.

C:\>
```

# Tracert – URL Não Respondendo

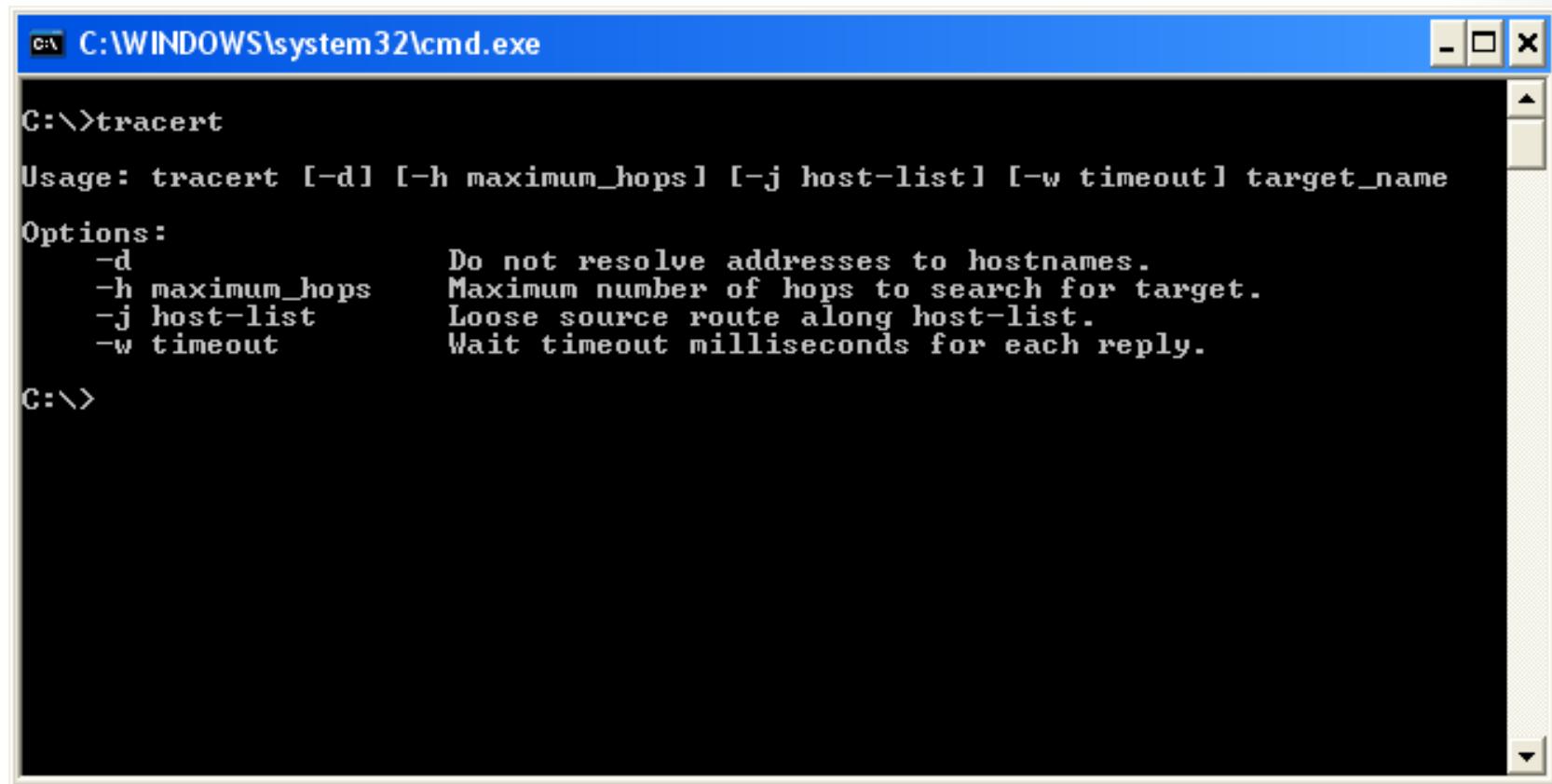
```
C:\WINDOWS\system32\cmd.exe
C:\>tracert www.ufmg.br

Tracing route to lua.adm-serv.ufmg.br [150.164.76.80]
over a maximum of 30 hops:
1       1 ms      1 ms      1 ms  192.168.0.1
2       3 ms      2 ms      2 ms  192.168.1.254
3       6 ms      4 ms      4 ms  netctr122.netcetera.com.br [192.168.122.1]
4      11 ms     20 ms      6 ms  10.0.2.1
5       8 ms      8 ms      6 ms  10.0.5.62
6       9 ms      7 ms      7 ms  201-048-012-254.static.ctbc.com.br [201.48.12.25
4]
7      18 ms     14 ms     20 ms  201-048-005-162.static.ctbctelecom.com.br [201.4
8.5.162]
8      18 ms     19 ms     21 ms  201-048-230-193.static.ctbctelecom.com.br [201.4
8.230.193]
9      17 ms     14 ms      *    201-048-250-141.static.ctbc.com.br [201.48.250.1
411]
10     57 ms     40 ms     39 ms  rnp.ptt.anasp.br [200.136.34.2]
11     55 ms     53 ms     54 ms  so-0-2-0-r1-df.bkb.rnp.br [200.143.252.17]
12     72 ms      *     62 ms  so-0-1-0-r1-mg.bkb.rnp.br [200.143.252.29]
13     69 ms     76 ms     61 ms  s2-mg.bkb.rnp.br [200.143.252.226]
14     64 ms     81 ms     81 ms  pop-mg-novo.rede.ufmg.br [200.131.2.220]
15      *     85 ms    133 ms  pop.central-core.rede.ufmg.br [150.164.164.149]

16      *      *      *    Request timed out.
17      *      *      *    Request timed out.
18      *      *      *    Request timed out.
19      *      *      *    Request timed out.
20      *      *      *    Request timed out.
21      *      *      *    Request timed out.
22      *      *      *    Request timed out.
23      *      *      *    Request timed out.
24      *      *      *    Request timed out.
25      *      *      *    Request timed out.
26      *      *      *    Request timed out.
27      *      *      *    Request timed out.
28      *      *      *    Request timed out.
29      *      *      *    Request timed out.
30      *      *      *    Request timed out.

Trace complete.
C:\>
```

# Tracert – Help!



A screenshot of a Windows Command Prompt window titled "C:\WINDOWS\system32\cmd.exe". The window shows the usage and options for the "tracert" command. The text is as follows:

```
C:\>tracert
Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout] target_name
Options:
  -d           Do not resolve addresses to hostnames.
  -h maximum_hops Maximum number of hops to search for target.
  -j host-list  Loose source route along host-list.
  -w timeout    Wait timeout milliseconds for each reply.
C:\>
```

# Tracert

- Exemplo ao vivo!

# Route

- O utilitário route é usado para listar, adicionar e remover regras da tabela de roteamento de um computador. Esta tabela de roteamento é sempre consultada pela camada de rede do protocolo para determinar qual será o próximo HOP por onde um pacote deve passar;
- Na figura existente no próximo slide, podemos verificar a existência de 4 colunas principais: "Network Destination", "Netmask", "Gateway" e "Interface";
- ***Sintaxe:*** Route print

# Route

```
C:\>route print
=====
Interface List
0x1 ... MS TCP Loopback interface
0x10003 ... 00 08 02 2e 8a 9f .... Realtek RTL8139/810X Family PCI Fast Etherne
t NIC
=====
=====
Active Routes:
Network Destination      Netmask         Gateway       Interface  Metric
          0.0.0.0        0.0.0.0   192.168.0.1  192.168.0.198    20
          127.0.0.0     255.0.0.0   127.0.0.1    127.0.0.1      1
        192.168.0.0    255.255.255.0  192.168.0.198  192.168.0.198    20
  192.168.0.198    255.255.255.255        127.0.0.1    127.0.0.1    20
  192.168.0.255    255.255.255.255  192.168.0.198  192.168.0.198    20
        224.0.0.0     240.0.0.0   192.168.0.198  192.168.0.198    20
 255.255.255.255    255.255.255.255  192.168.0.198  192.168.0.198      1
Default Gateway: 192.168.0.1
=====
Persistent Routes:
  None
C:\>
```

A primeira regra da tabela exemplo apresentada, indica a regra do "Default Gateway". Esta regra é a que determina para onde um pacote vai quando ele não se enquadra em nenhuma outra regra.

# Nslookup

- O utilitário nslookup serve para traduzir nomes de domínios para os números IP correspondentes;
- Este utilitário consulta os servidores de DNS (Domain Name Service), espalhados pela Internet, para resolver uma consulta e descobrir o endereço IP;
- O nslookup ao contrário dos outros utilitários vistos até agora, oferece um prompt para o usuário digitar nomes de domínios para consulta;
- **Sintaxe:** Nslookup endereço ou IP.

# Nslookup - Exemplo

```
C:\>nslookup
*** Can't find server name for address 10.0.5.62: Non-existent domain
Default Server: gateway.netcetera.com.br
Address: 200.202.236.17
Aliases: 17.236.202.200.in-addr.arpa

> www.terra.com.br
Server: gateway.netcetera.com.br
Address: 200.202.236.17
Aliases: 17.236.202.200.in-addr.arpa

Non-authoritative answer:
Name: www.terra.com.br
Address: 200.176.3.142

> www.esj.eti.br
Server: gateway.netcetera.com.br
Address: 200.202.236.17
Aliases: 17.236.202.200.in-addr.arpa

Non-authoritative answer:
Name: esj.eti.br
Address: 200.219.214.18
Aliases: www.esj.eti.br

> www.yahoo.com
Server: gateway.netcetera.com.br
Address: 200.202.236.17
Aliases: 17.236.202.200.in-addr.arpa

Non-authoritative answer:
Name: www-real.wai.b.yahoo.com
Address: 69.147.76.15
Aliases: www.yahoo.com, www.wai.b.yahoo.com

> exit
C:\>
```

# Nslookup

- Exemplo ao vivo!

# Ipconfig

- O utilitário ipconfig é um aplicativo usado para informar a configuração atual de rede da máquina;
- *Sintaxe:* ipconfig

# Ipconfig - Exemplo

```
C:\WINDOWS\system32\cmd.exe
C:\>ipconfig
Windows IP Configuration

Ethernet adapter Hamachi:
  Connection-specific DNS Suffix . . . . .
  IP Address . . . . . : 5.168.17.168
  Subnet Mask . . . . . : 255.0.0.0
  Default Gateway . . . . .

Ethernet adapter Wireless Network Connection:
  Connection-specific DNS Suffix . . . .
  IP Address . . . . . : 192.168.0.101
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 192.168.0.1

Ethernet adapter Local Area Connection:
  Media State . . . . . . . . . : Media disconnected

C:\>
```

# Ipconfig - Help!

# Ipconfig – MAC Address

```
C:\WINDOWS\system32\cmd.exe
C:\>ipconfig /all

Windows IP Configuration

    Host Name . . . . . : Lambda
    Primary Dns Suffix : .
    Node Type . . . . . : Unknown
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No

Ethernet adapter Hamachi:

    Connection-specific DNS Suffix . . . . . :
    Description . . . . . : Hamachi Network Interface
    Physical Address. . . . . : 7A-79-05-A8-11-A8
    DnCp Enabled. . . . . . : Yes
    Autoconfiguration Enabled . . . . . : No
    IP Address . . . . . : 5.168.17.168
    Subnet Mask . . . . . : 255.0.0.0
    Default Gateway . . . . . :
    DHCP Server . . . . . : 5.0.0.1
    Lease Obtained. . . . . : segunda-feira, 9 de março de 2009 11
:28:40
    Lease Expires . . . . . : segunda-feira, 9 de março de 2009 11
:32:55

Ethernet adapter Wireless Network Connection:

    Connection-specific DNS Suffix . . . . . :
    Description . . . . . : ZPlus C361 902.11g WLAN PCI Adapter
    Physical Address. . . . . : 00-05-9E-80-75-43
    Dhcp Enabled. . . . . . : No
    IP Address. . . . . : 192.168.0.101
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.0.1
    DNS Servers . . . . . : 10.0.5.62
                                200.202.236.17

Ethernet adapter Local Area Connection:

    Media State . . . . . . . . . : Media disconnected
    Description . . . . . . . . . : SiS 900-Based PCI Fast Ethernet Adapter
    Physical Address. . . . . . . . . : 00-0C-6E-26-62-F7
    C:\>
```

# Netstat

- O netstat serve para mostrar as conexões ativas atualmente com a máquina em questão. Ele lista na tela todas as conexões TCP/IP em andamento;
- *Sintaxe:* netstat

# Netstat

```
C:\WINDOWS\system32\cmd.exe
C:\>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    lambda:1025            localhost:2002        ESTABLISHED
  TCP    lambda:1209            localhost:1210        ESTABLISHED
  TCP    lambda:1210            localhost:1209        ESTABLISHED
  TCP    lambda:1212            localhost:1213        ESTABLISHED
  TCP    lambda:1213            localhost:1212        ESTABLISHED
  TCP    lambda:2002            localhost:1025        ESTABLISHED
  TCP    lambda:5152            localhost:1211        CLOSE_WAIT
  TCP    lambda:1105            hy1msg3093117.phx.ghl:1863 ESTABLISHED
  TCP    lambda:1143            a72-246-216-49.deploy.akamaitechnologies.com:htt
p  CLOSE_WAIT
  TCP    lambda:1160            app55.logmein.com:https ESTABLISHED
  TCP    lambda:2608            p1079-ipbf3210hodogaya.kanagawa.ocn.ne.jp:5051
ESTABLISHED
  TCP    lambda:2869            192.168.0.1:1026      CLOSE_WAIT

C:\>
```

# Netstat

- Exemplo ao vivo!

Fim