

Redes de Computadores

Camada de Rede

Prof. Everthon Valadão

Material baseado nos slides de:
Dorgival Guedes (UFMG) e Fábio Costa (UFG)

(última modificação: 26/10/2020)



Camada de rede

Nosso objetivo:

- entender os princípios dos serviços da camada de rede:
 - Modelo de serviço
 - Endereçamento
 - Roteamento
 - IPv6

Tópicos abordados:

- Endereçamento (IPv4), máscaras e sub-redes
- Expedição de pacotes
- Protocolos auxiliares
- Roteamento interno (RIP, OSPF) e entre sistemas autônomos (BGP)
- Protocolo IPv6



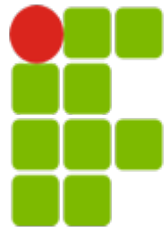
Camada de rede

Nosso objetivo:

- entender os princípios dos serviços da camada de rede:
 - Modelo de serviço
 - Endereçamento
 - Roteamento
 - IPv6

Tópicos abordados:

- Endereçamento (IPv4), máscaras e sub-redes
- Expedição de pacotes
- Protocolos auxiliares
- Roteamento interno (RIP, OSPF) e entre sistemas autônomos (BGP)
- Protocolo IPv6



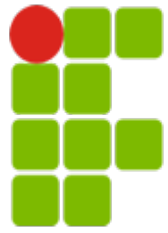
Funções básicas da camada de rede:

- **Endereçamento**

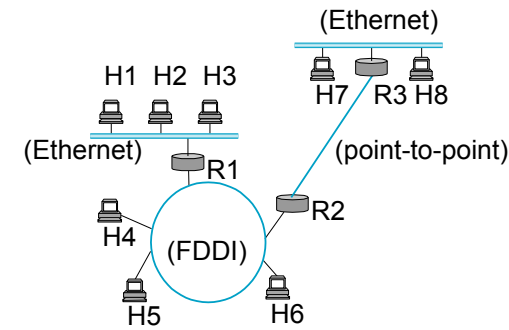
- identificação de cada máquina, independente de sua localização ou da tecnologia

- **Roteamento**

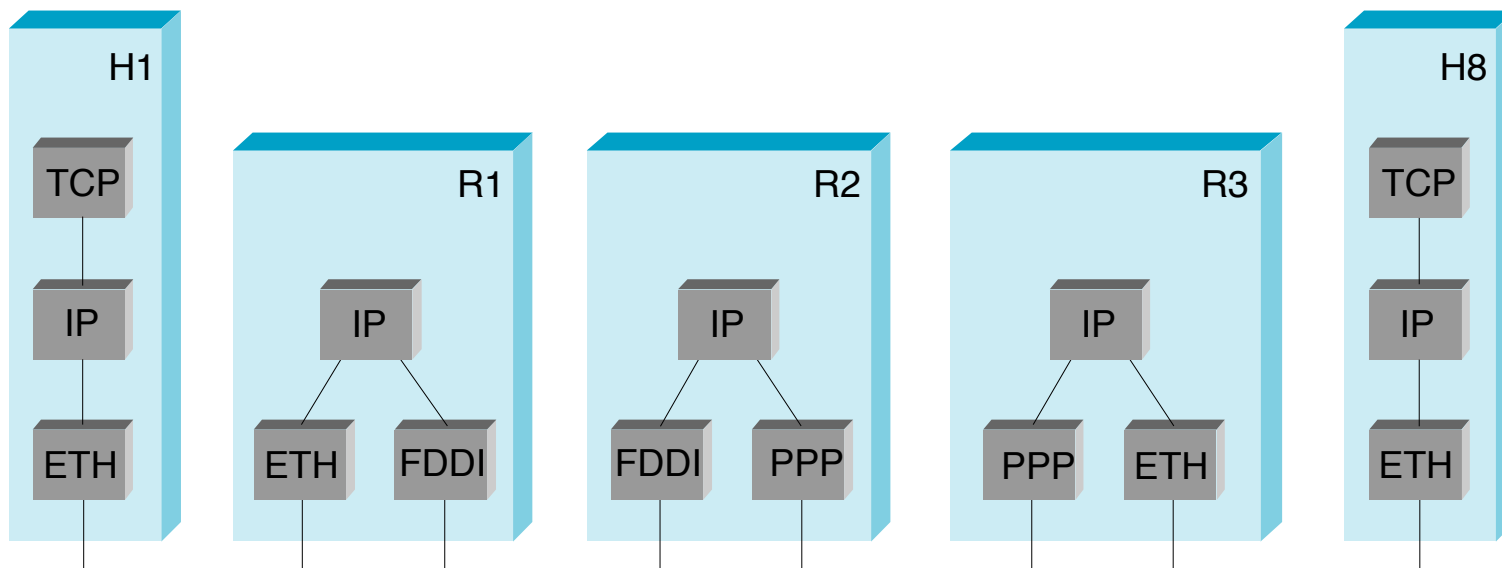
- determinação de um caminho entre duas máquinas quaisquer da internet

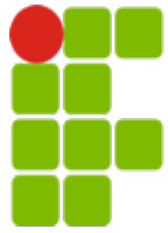


Interconexão



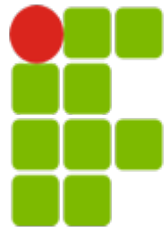
- Conexão entre as redes é feita por roteadores
 - Equipamento com finalidade especial: interconexão
 - Deve ser capaz de lidar com diferentes tecnologias (“ponte”)
- A rede virtual resultante deve oferecer os mesmos serviços em todos os seus pontos





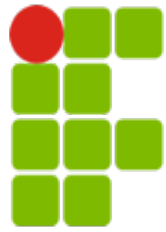
Modelo de serviço da Internet

- **Sem conexão** (baseado em datagramas)
- Entrega segundo “**melhor esforço**” possível
 - faz o melhor que pode, mas não garante a entrega
- **Serviço não confiável:**
 - Pacotes podem ser perdidos
 - Pacotes podem ser entregues fora de ordem
 - Várias cópias de um pacote podem ser entregues
 - Pacotes podem ser atrasados por muito tempo



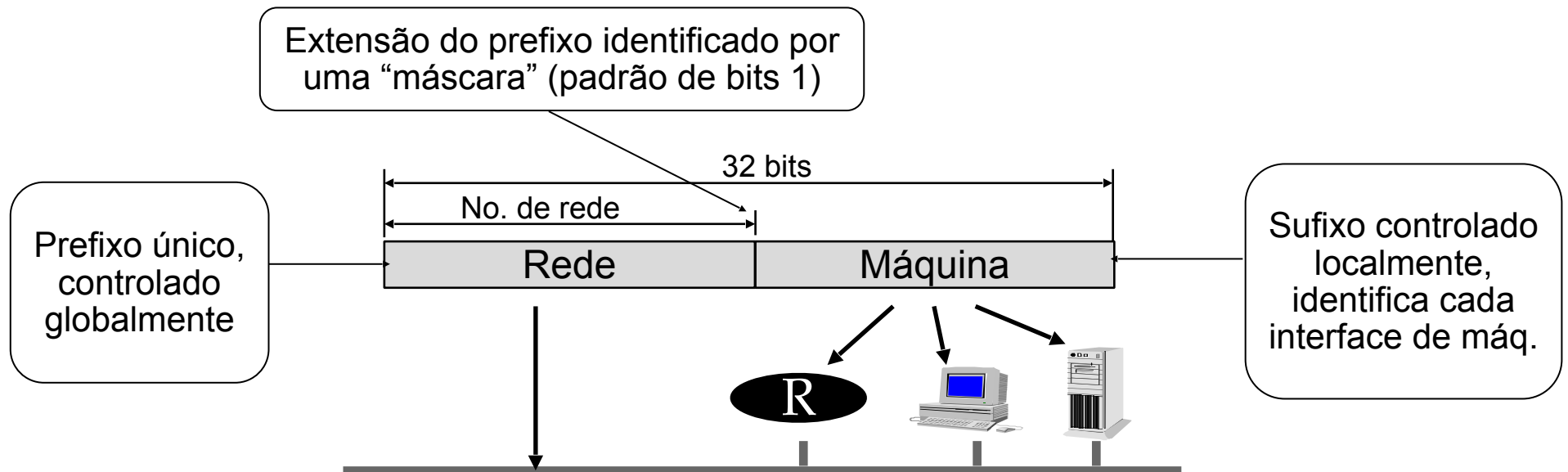
Endereçamento global dos nós

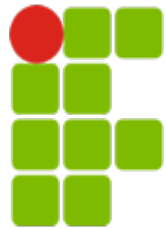
- Componente crítico da abstração fornecida pela Internet
- O IP é um endereço lógico, independente de endereços físicos como os usados em redes locais (MAC)
 - o IP pode mudar quando se muda de rede, o MAC sempre é o mesmo
- Ajuda a criar a ilusão de uma **rede única e integrada**
- Usuários, aplicações e protocolos de alto nível usam endereços lógicos (IP) para se comunicar



Endereço IPv4

- Dividido em endereço de rede (prefixo) e endereço de máquina (sufixo)

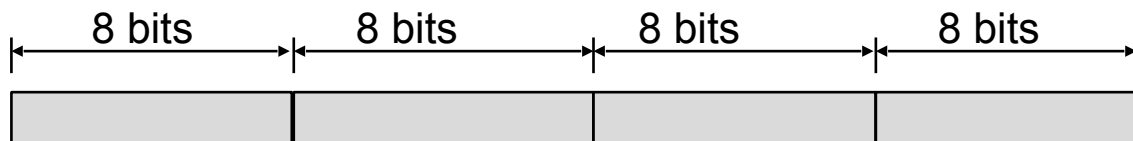




Endereço IPv4: máscara de rede

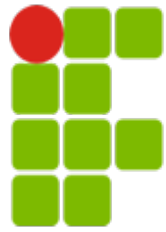
- Notação de ponto decimal

- 32 bits normalmente visualizados como quatro grupos de 1 byte (8 bits)
- Máscara identificada pelo seu comprimento ou como padrão de 1's



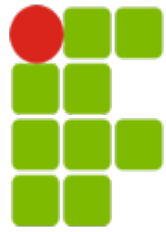
- Exemplos:

IP (binário)	IP (decimal)	Máscara
<u>10000001 00110100 00000110</u> 00000000	-> 129.52.6.0	<u>255.255.255.0</u>
<u>10000001 00110100 00000110</u> 00000000	-> 129.52.6.0	/24
<u>10000000 00001010</u> 00000010 00000011	-> 128.10.2.3	<u>255.255.0.0</u>
<u>10000000 00001010</u> 00000010 00000011	-> 128.10.2.3	/16
<u>11000000 00000101 00110000</u> 00000011	-> 192.5.48.3	/26
<u>00001010 00000010 00000000</u> 00100101	-> 10.2.0.37	/20
<u>10000000 10000000 11111111</u> 00000000	-> 128.128.255.0	/18



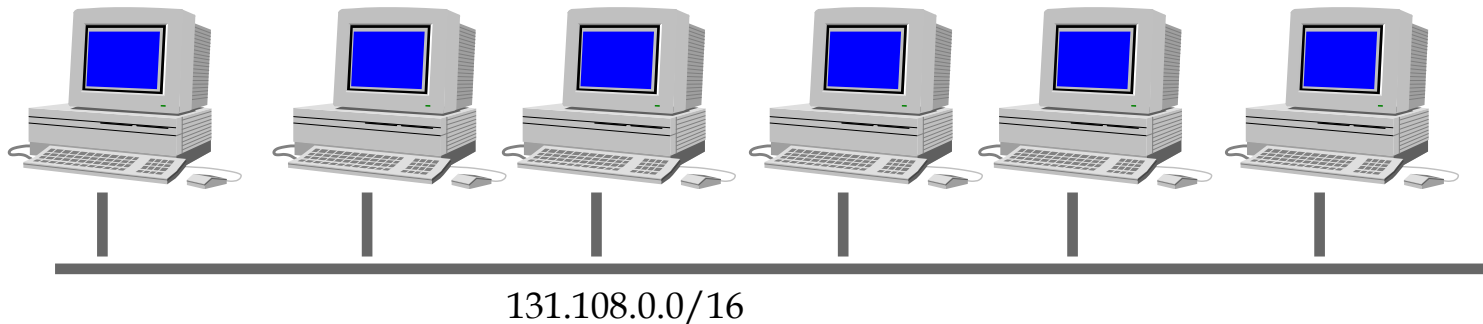
Endereços IPv4 “especiais”

- Alguns endereços são especiais e reservados:
 - Sufixo todo em zeros (*.0): endereço identifica uma subrede
 - ex.: 200.131.160.0 /24
 - Sufixo todo em uns (*.255): endereço de *broadcast* (envia o pacote a todas as máquinas daquela subrede)
 - ex.: 200.131.160.255 /24
 - Existem faixas especiais de IPv4 para **redes privadas** ([RFC-1918](#)), de uso apenas local pois **não são publicamente roteadas** na Internet global:
 - ex.:
 - **10.0.0.0/8** de **10.0.0.0** até **10.255.255.255**
 - **172.16.0.0/12** de **172.16.0.0** até **172.31.255.255**
 - **192.168.0.0/16** de **192.168.0.0** até **192.168.255.255**
- OBS.: pacotes com destinatário nesses endereços **não são roteados para fora da rede local**, ou seja, não são “endereços válidos na Internet”!

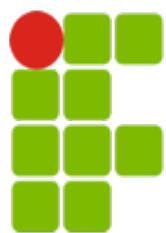


Segmentação de rede (*subredes*)

- Cada número de rede tem sua **máscara de rede**
- A máscara permite definir se um endereço IP é local ou não

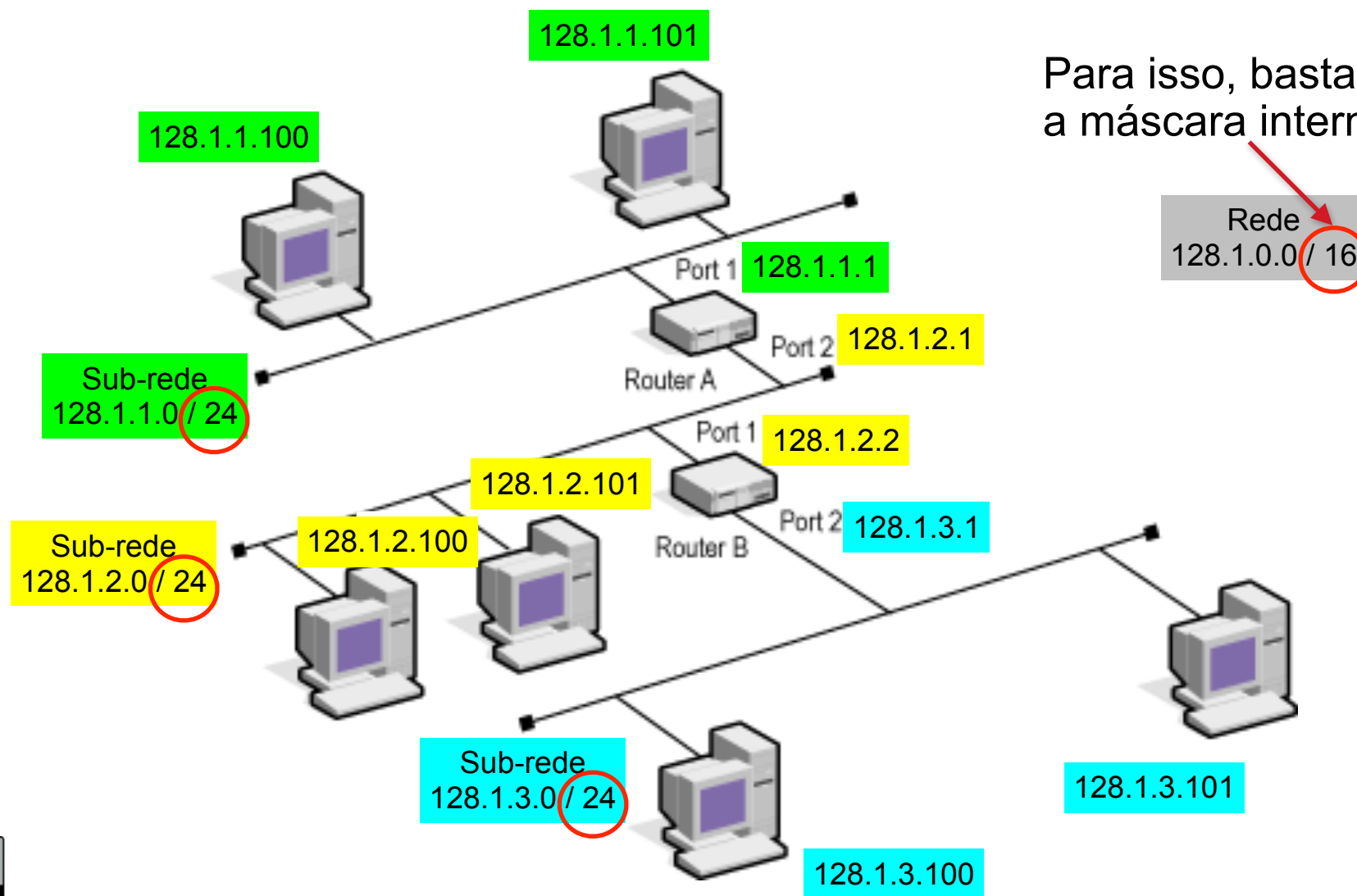


- Exemplos para a rede **131.108.0.0 /16**
 - **131.108.1.1** **está** na mesma rede local que **131.108.1.2**
 - mas **131.109.1.3** **NÃO está** na mesma rede que **131.108.1.4**
 - **131.108.2.2** **está** na mesma rede local que **131.108.100.200**
 - mas **130.108.100.200** **NÃO está** na mesma rede que **131.108.100.200**



Segmentação de rede (*subredes*)

- Uma entidade pode subdividir sua faixa de endereços IP entre sub-redes





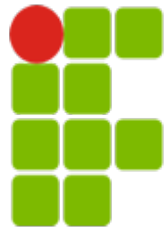
Camada de rede

Nosso objetivo:

- entender os princípios dos serviços da camada de rede:
 - Modelo de serviço
 - Endereçamento
 - Roteamento
 - IPv6

Tópicos abordados:

- Endereçamento (IPv4), máscaras e sub-redes
- Expedição de pacotes
- Protocolos auxiliares
- Roteamento interno (RIP, OSPF) e entre sistemas autônomos (BGP)
- Protocolo IPv6



Expedição de datagramas

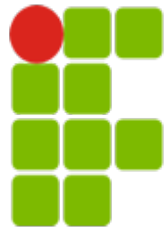
- cada datagrama contém o endereço do destino
- cada interface tem seu endereço e sua máscara
- comportamento depende de o endereço de destino estar na mesma rede a que pertence a interface:

SE ((end_destino & mascara) == (end_interface & mascara))

envia datagrama diretamente ao host de destino, pois ele está na mesma rede local que o roteador

SENÃO

determina próximo passo para o pacote, de acordo com as redes as quais o roteador tem acesso



Expedição de datagramas

- A tabela de expedição controla o roteamento
 - mapeia endereços de rede para o próximo roteador
 - pode haver uma rota de saída padrão (*gateway*), na falta de uma rota específica

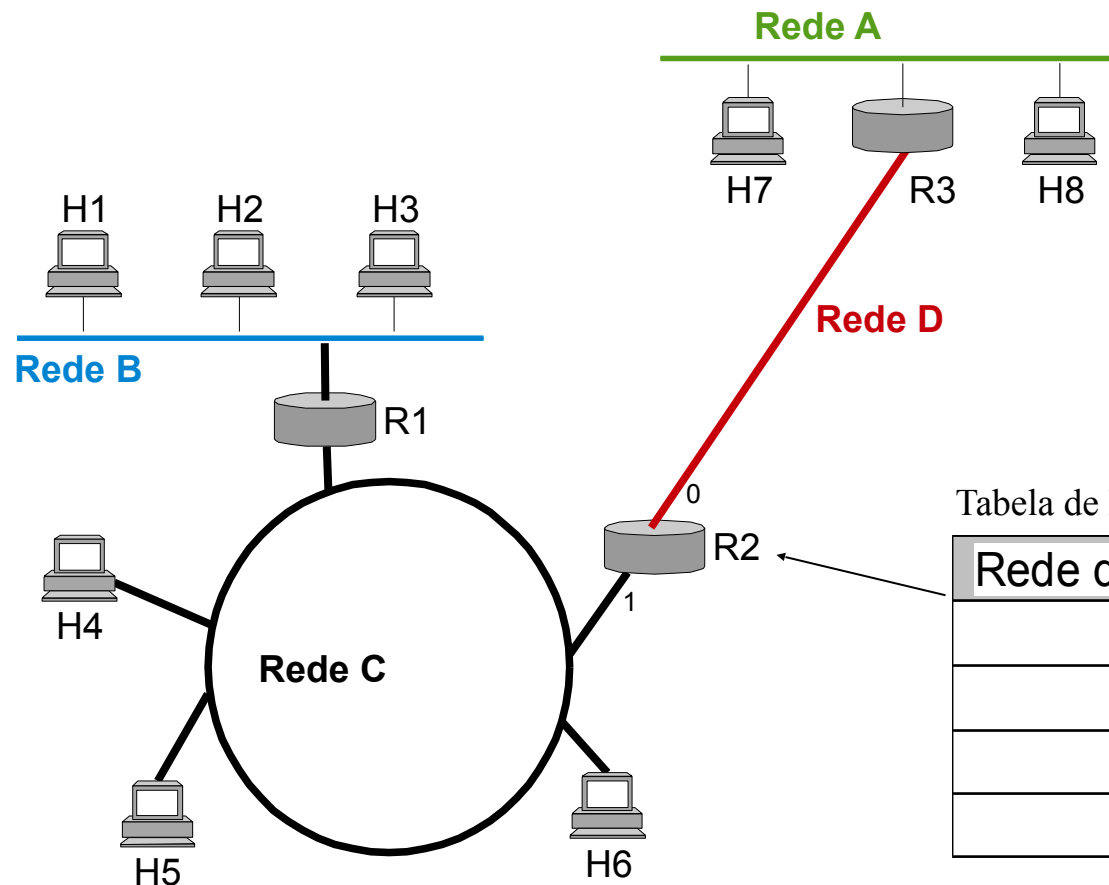
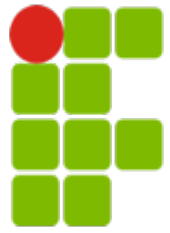


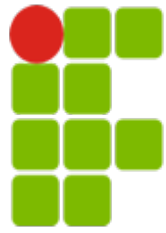
Tabela de Roteamento do roteador R2

Rede de Destino	Próximo passo
A	R3
B	R1
C	Interface 1
D	Interface 0



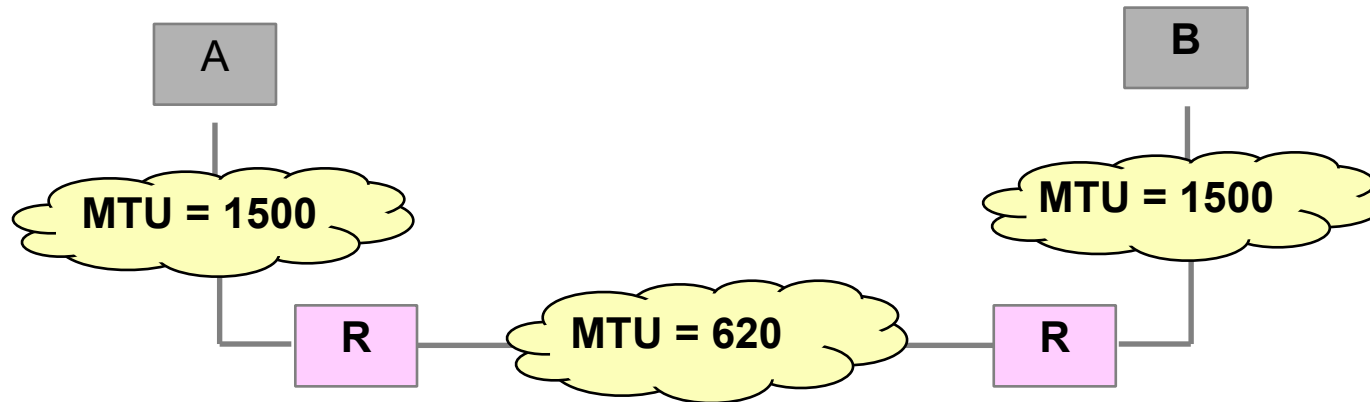
Problemas associados à expedição

- Cada rede pode ter limites diferentes para o tamanho máximo de pacotes
 - É preciso ser capaz de enviar pacotes grandes em qualquer rede
 - Consequência: fragmentação e remontagem de pacotes
- Em uma rede, a entrega de pacotes depende dos endereços de enlace (rede local)
 - É preciso associar endereços IP locais a endereços físicos
 - Protocolo ARP

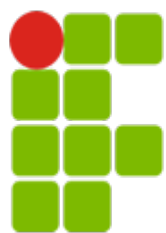


Fragmentação de pacotes

- A camada de interface de rede (enlace/física), conforme o protocolo da tecnologia de acesso, especifica um **tamanho máximo** do pacote que pode ser nela enviado:
 - MTU (*Maximum Transfer Unit*)

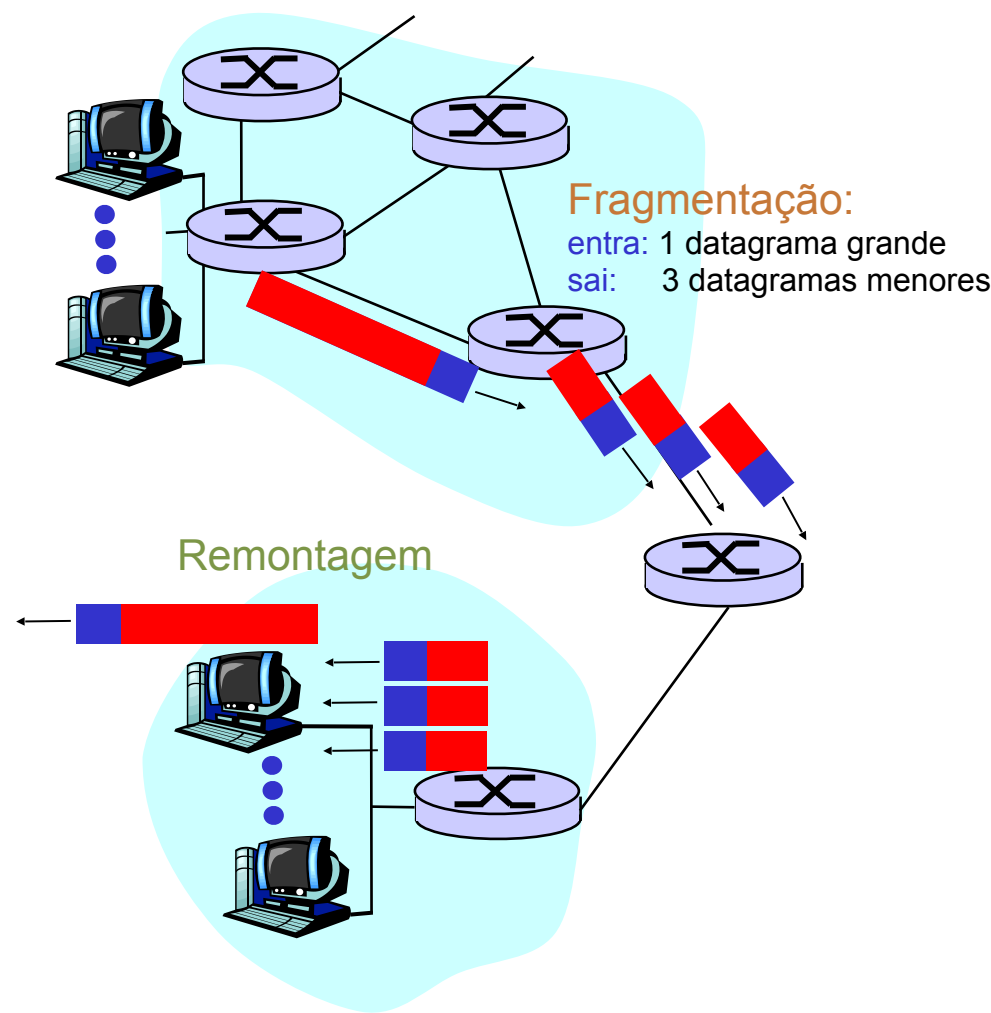


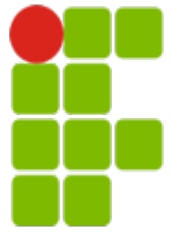
Qual o tamanho ideal do datagrama neste caso?



Fragmentação e Remontagem

- Enlaces de rede têm MTU correspondente ao **maior quadro que pode ser** transportado pela camada de enlace:
- Exemplos de tecnologias de enlace que possuem MTU diferentes
 - Ethernet: 1492 bytes
 - FDDI: 4352 bytes
 - Wi-Fi: 2304 – 7981 bytes
- Datagramas IP **grandes demais** devem ser divididos (fragmentados) pelos roteadores
 - um datagrama dá origem a vários datagramas
 - “remontagem” ocorre apenas no destino final
 - O cabeçalho do protocolo IP é usado para identificar e ordenar datagramas relacionados



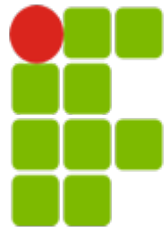


Fragmentação: princípios básicos

- A informação do cabeçalho original é mantida
 - mantém o end.fonte, end.destino e nº de identificação do datagrama
 - ajusta o FLAG para 1 nos fragmentos e 0 no último
 - o deslocamento (OFFSET) determina a posição do fragmento no datagrama original
- Fragmenta apenas se for necessário ($MTU < \text{pacote}$)
 - tentar evitar fragmentação já no próprio nó de origem (como?)
 - nos intermediários é permitido re-fragmentar, se necessário
 - porém, a remontagem é feita só no nó de destino

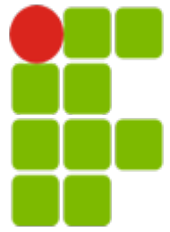
OBS.: o IP não tenta recuperar fragmentos perdidos!

→ a camada de transporte é que deverá se preocupar com isso...



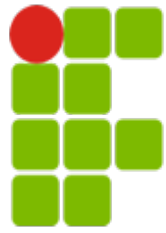
Remontagem de pacotes

- Processo inverso ao da fragmentação
 - responsável: computador **destino**
 - “culpado”: roteadores intermediários
- O que ocorre se fragmentos são perdidos, chegam fora de ordem ou atrasados?
 - RX não tem como informar TX para re-enviar um fragmento pois TX *não conhece nada sobre a fragmentação!*
- Solução:
 - RX ao receber o primeiro fragmento inicializa um temporizador
 - Se todos os fragmentos não chegam antes do temporizador se esgotar então **os fragmentos recebidos são descartados**



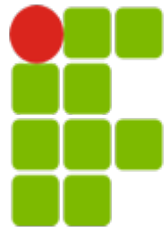
Problemas associados à expedição

- Cada rede pode ter limites diferentes para o tamanho máximo de pacotes (MTU)
 - não podemos simplesmente estabelecer uma MTU global como a menor MTU
 - é preciso ser capaz de enviar pacotes grandes em qualquer rede
 - Razão de (in)eficiência = $(\text{Tamanho datagrama})/(\text{Tamanho cabeçalho})$
 - porém, o datagrama deveria ser tão grande quando possível?
 - Fragmentação e remontagem de pacotes: *perda “parcial” é na verdade total*
- Em uma rede, a *entrega de pacotes ao destino final depende dos endereços físicos de enlace (rede local)*
 - é preciso associar o endereço IP na rede local a um endereço físico



Como identificar o destino na rede física?

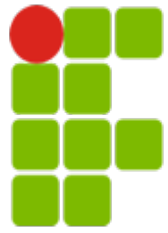
- A entrega local de pacotes (IP) na LAN depende dos endereços de enlace (MAC)
- Pacotes IP trazem endereços IP, mas para entregá-los a um destino na LAN é preciso conhecer o endereço físico!
 - endereço físico (MAC) *não tem nada a ver* com endereço IP
 - os programas usam endereço IP (end. lógico) pra se comunicar e as placas de rede usam o endereço MAC (end. físico)
- Em redes Ethernet, por ex., uma máquina só recebe um pacote se ele contém o **seu** endereço físico
 - é preciso “perguntar” às máquinas da rede qual é o endereço físico da máquina que se deseja alcançar
 - protocolo utiliza mensagens *broadcast* para que todas as máquinas participem do processo



Resolução de Endereços:

endereço lógico (IP) para físico (MAC)

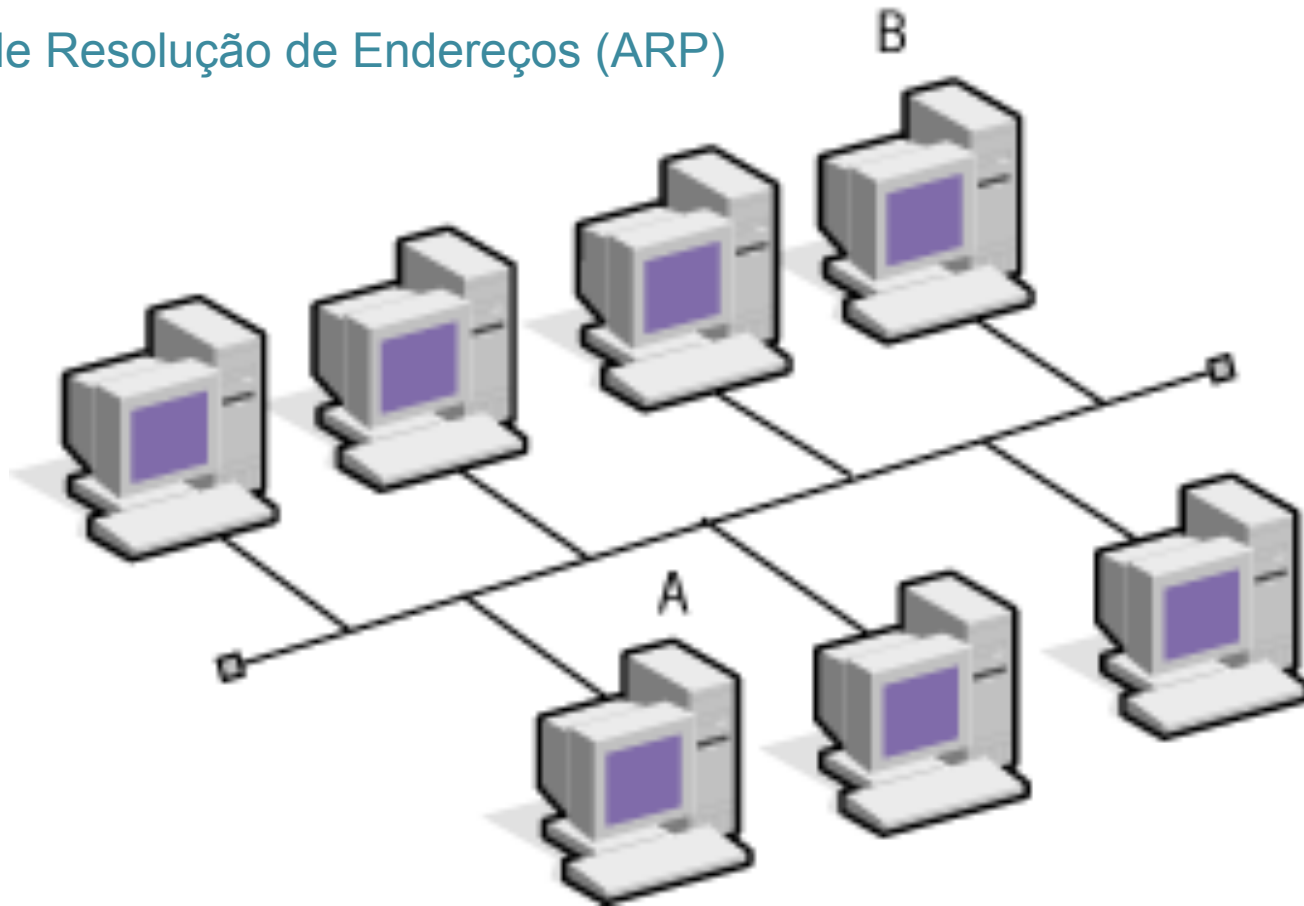
- Protocolo ARP (*Address Resolution Protocol*)
 - protocolo da camada de **enlace**
 - ~~traduz~~ resolve o endereço lógico (IP) em físico (MAC)
 - gerencia *cache* de associações entre endereços IP e MAC
 - entradas são descartadas após 10 min. (aprox.) sem utilização
 - tabela é atualizada mesmo se a entrada já existe



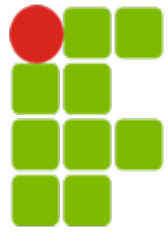
ARP:

resolução de endereço lógico (IP) em físico (MAC)

Protocolo de Resolução de Endereços (ARP)



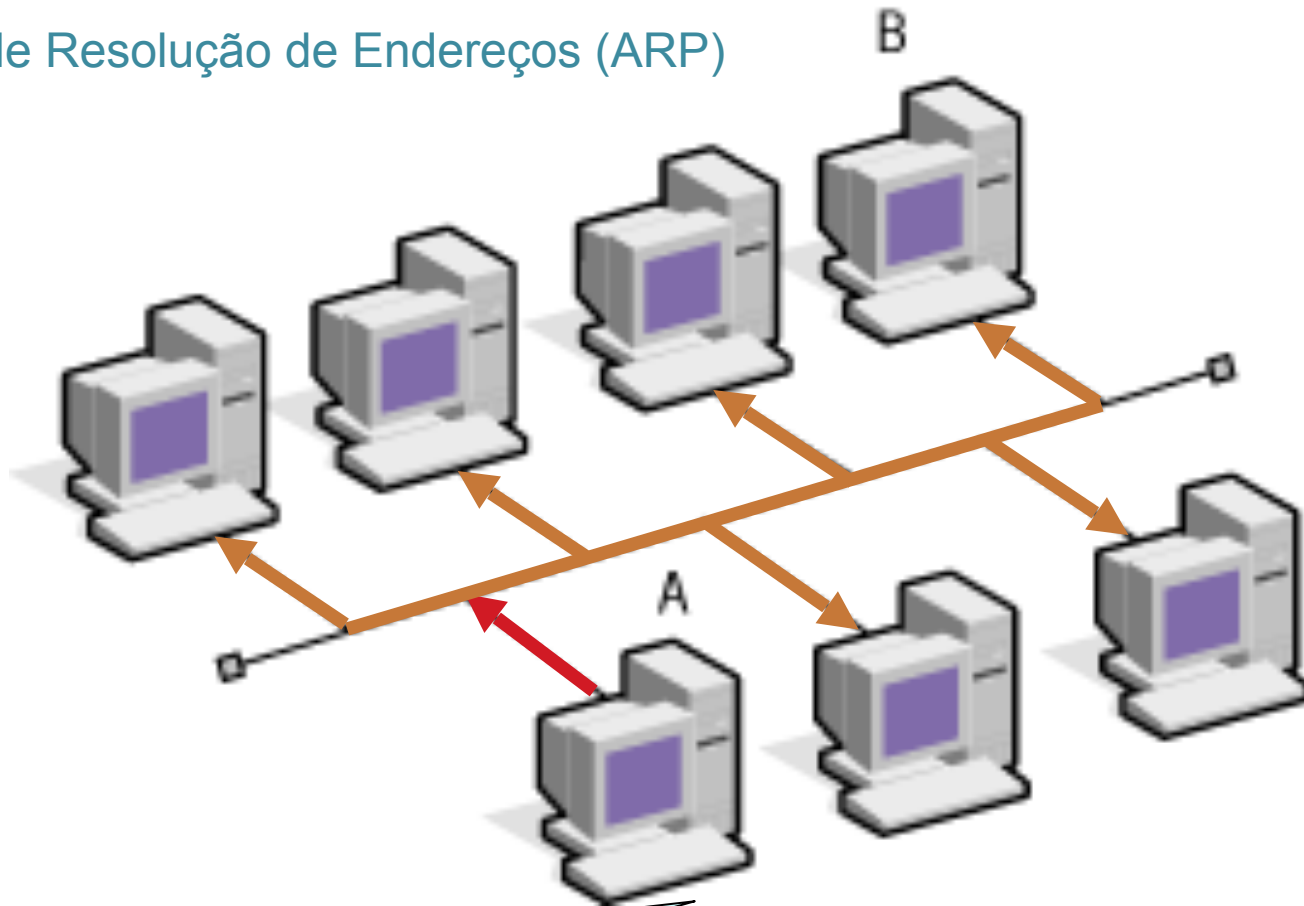
Como o host A determina endereço físico (hardware) do host B?



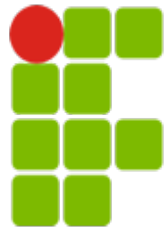
ARP:

resolução de endereço lógico (IP) em físico (MAC)

Protocolo de Resolução de Endereços (ARP)



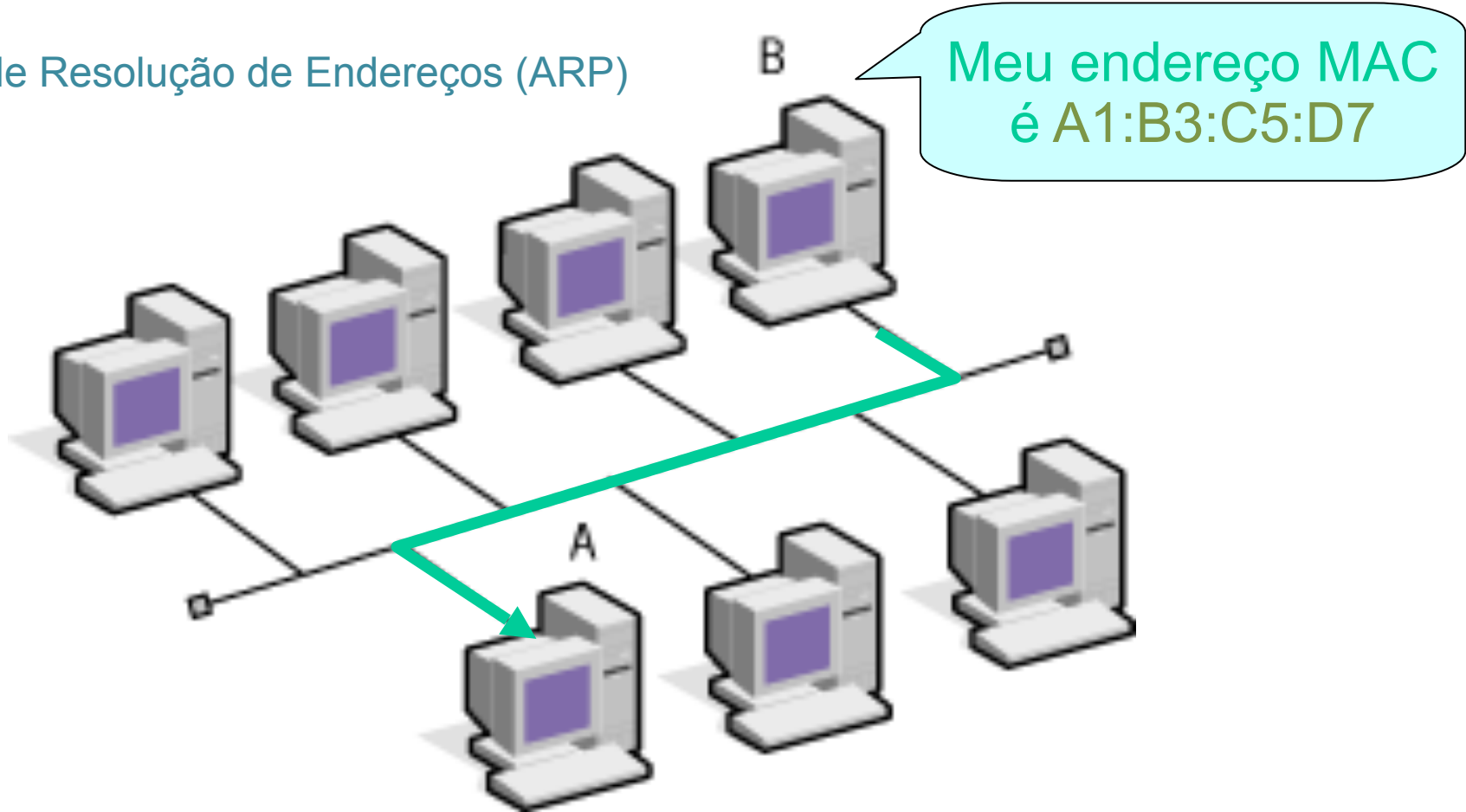
Qual o endereço MAC cujo IP
é 192.168.1.101 (host B)?

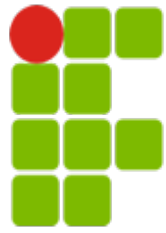


ARP:

resolução de endereço lógico (IP) em físico (MAC)

Protocolo de Resolução de Endereços (ARP)

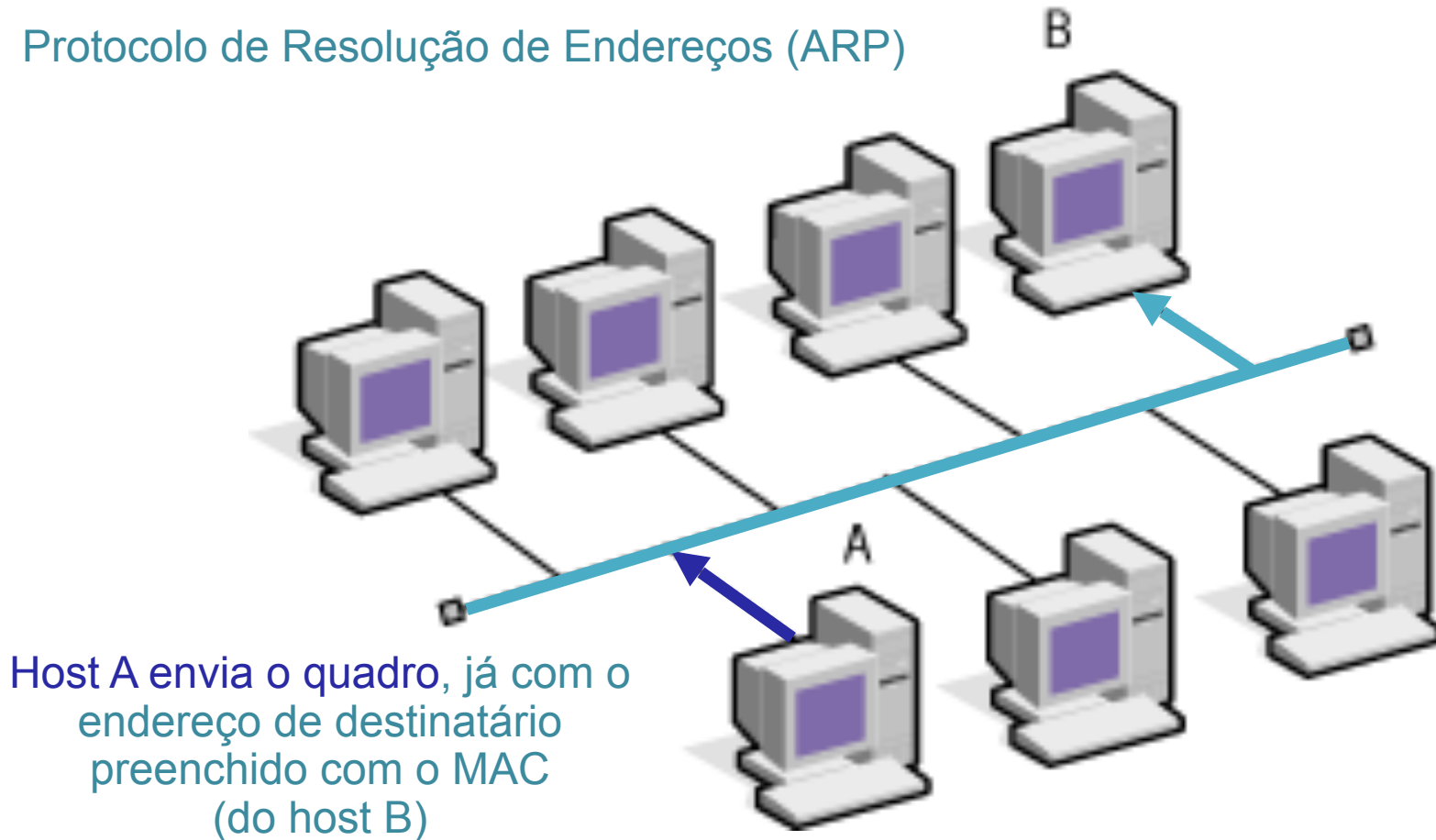




Protocolo de enlace (ex.: Ethernet)

realiza a entrega do quadro com o endereço físico (MAC)

Protocolo de Resolução de Endereços (ARP)



É possível consultar endereços MAC dos computadores vizinhos (na sua rede local) com o comando
arp -n



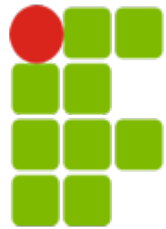
Camada de rede

Nosso objetivo:

- entender os princípios dos serviços da camada de rede:
 - Modelo de serviço
 - Endereçamento
 - Roteamento
 - IPv6

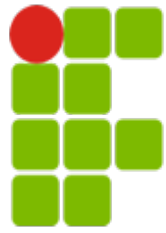
Tópicos abordados:

- Endereçamento (IPv4), máscaras e sub-redes
- Expedição de pacotes
- Protocolos auxiliares
- Roteamento interno (RIP, OSPF) e entre sistemas autônomos (BGP)
- Protocolo IPv6



Protocolos auxiliares na operação da rede

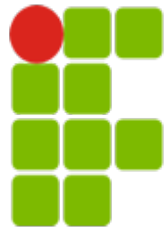
- Gerência de configuração
 - cada máquina deve receber informações básicas para operar
 - endereço e rota padrão (caminho de saída dos dados)
 - isso pode ser feito
 - manualmente, portanto propenso a enganos e conflitos
 - automaticamente, através do protocolo DHCP (camada de **aplicação**)
- Notificação de erros e controle
 - problemas na operação da rede podem ser notificados
 - protocolo de controle geral deve ser reconhecido: ICMP (camada de **rede**)
- Transporte de pacotes sobre outras redes
 - em alguns casos, os pacotes de uma rede devem passar sobre uma rede intermediária sem serem processados
 - criam-se “túneis” onde pacotes entram e só aparecem em outro ponto
 - princípio de redes virtuais (VPNs)



Configuração de máquinas

Qual a informação mínima para uma máquina operar na rede?

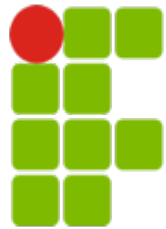
- Quem sou eu?
 - Endereço IP e máscara de subrede
- Pra onde vou?
 - Caminho *default* de saída dos pacotes destinados a outras redes
- Cadê os outros?
 - Processo de descobrimento de endereços de outras máquinas



DHCP

(*Protocolo de Configuração Dinâmica de Hospedeiros*)

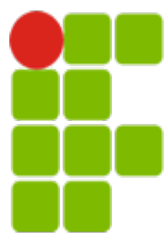
- Permite que um hospedeiro obtenha um endereço IP **automaticamente**
- Extremamente útil para estações móveis (ex.: notebooks, smartphones)
 - se conectam a diferentes redes a cada nova localização
 - muitos usuários em trânsito, endereços utilizados por tempo limitado
- Também é muito útil para ISPs, ex.: tem 2.000 clientes mas só 400 *online*



DHCP

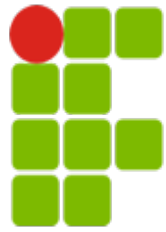
(*Protocolo de Configuração Dinâmica de Hospedeiros*)

- O IP recebido através de DHCP é “emprestado” por um intervalo de tempo definido (*leasing*), devendo portanto ser renovado
 - o hospedeiro pode receber um IP temporário diferente cada vez que se conectar à rede!
 - é possível “amarrar” a oferta do endereço IP ao MAC, de maneira que o hospedeiro sempre receba o mesmo endereço.
- O DHCP permite que o hospedeiro descubra informações adicionais:
 - Máscara de subrede;
 - Endereço do primeiro roteador (default gateway);
 - Endereço do servidor DNS local



Protocolos auxiliares na operação da rede

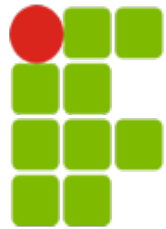
- Gerência de configuração
 - cada máquina deve receber informações básicas para operar
 - endereço e rota padrão (caminho de saída dos dados)
 - isso pode ser feito
 - manualmente, portanto propenso a enganos e conflitos
 - automaticamente, através do protocolo DHCP (camada de **aplicação**)
- Notificação de erros e controle
 - problemas na operação da rede podem ser notificados
 - protocolo de controle geral deve ser reconhecido: ICMP (camada de **rede**)
- Transporte de pacotes sobre outras redes
 - em alguns casos, os pacotes de uma rede devem passar sobre uma rede intermediária sem serem processados
 - criam-se “túneis” onde pacotes entram e só aparecem em outro ponto
 - princípio de redes virtuais (VPNs)



Relato de erros (ICMP)

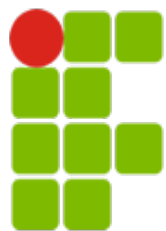
Internet Control Message Protocol (ICMP)

- Troca de mensagens entre elementos da rede IP para controle da transmissão e roteamento
 - Controle de fluxo (*source quench*)
 - Notificação de falhas (*ex.: destino inalcançável, checksum, remontagem*)
 - Redirecionamento de rotas
 - Requisição de informações (*ping*)



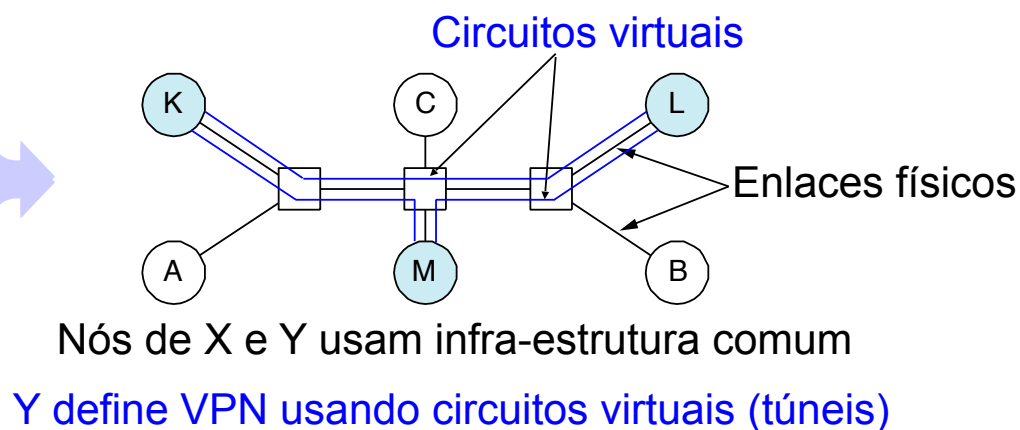
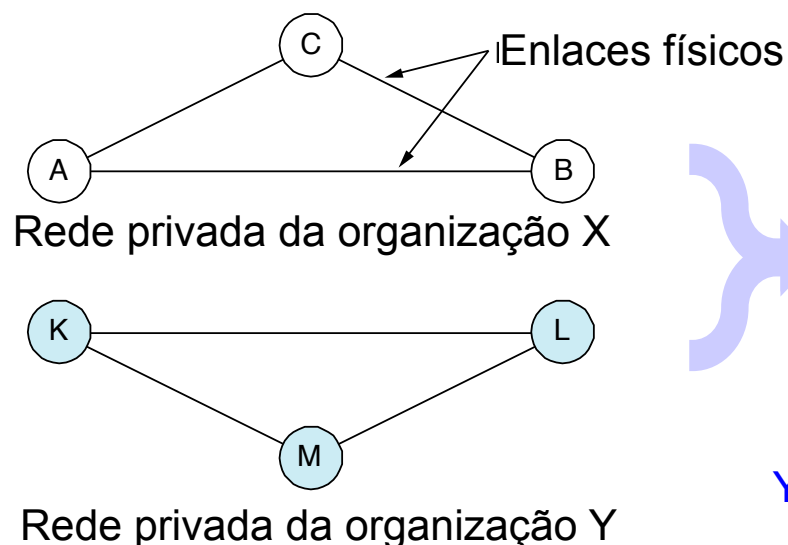
Protocolos auxiliares na operação da rede

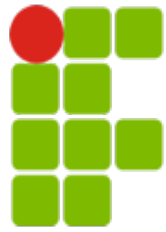
- Gerência de configuração
 - cada máquina deve receber informações básicas para operar
 - endereço e rota padrão (caminho de saída dos dados)
 - isso pode ser feito
 - manualmente, portanto propenso a enganos e conflitos
 - automaticamente, através do protocolo DHCP (camada de **aplicação**)
- Notificação de erros e controle
 - problemas na operação da rede podem ser notificados
 - protocolo de controle geral deve ser reconhecido: ICMP (camada de **rede**)
- Transporte de pacotes sobre outras redes
 - em alguns casos, os pacotes de uma rede devem passar sobre uma rede intermediária (ex.: rede insegura, outra tecnologia)
 - criam-se “túneis” onde pacotes entram e só aparecem em outro ponto
 - princípio de redes virtuais (VPNs)



Redes virtuais (VPNs)

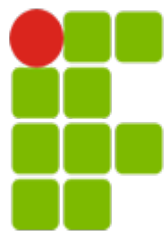
- Organizações podem ter políticas de segurança/acesso definidas em termos de suas redes “privativas”
- Na prática, partes de cada organização podem estar em pontos diferentes da Internet
- VPN: *Virtual Private Network*



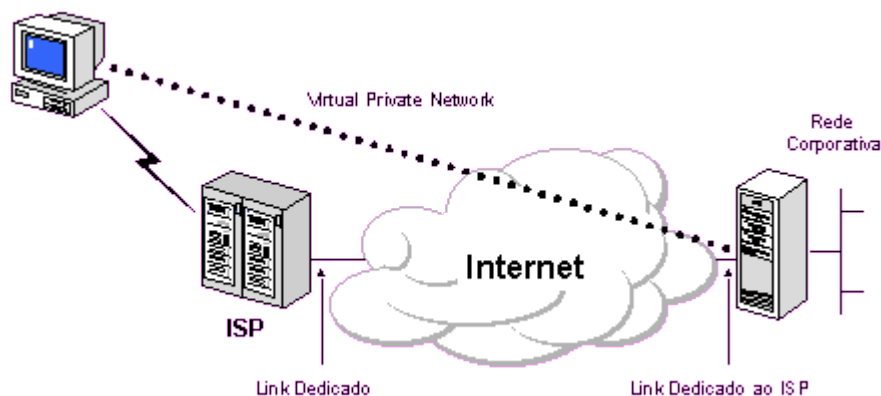


Redes virtuais (VPNs)

- São **túneis de criptografia** entre pontos autorizados
 - criados através da Internet (rede pública) e/ou redes privadas
 - visam a transferência de informações de **modo seguro**, entre redes corporativas ou usuários remotos.
- A **segurança** é a primeira e mais importante função da VPN
 - dados privados serão transmitidos pela Internet (meio inseguro)
 - não se deve permitir que sejam modificados ou interceptados
 - oferecem recursos de autenticação e criptografia (ex.: extensão [IPSec](#))
- Outra função é a **conexão entre corporações** (“Extranets”) através da Internet
 - ex.: conectar filiais distantes de uma empresa
 - redução de custos, pois elimina a necessidade de links dedicados
 - simplifica a operacionalização da WAN: a conexão LAN-Internet-LAN fica parcialmente a cargo dos provedores de acesso.
- Mais informações: <http://www.rnp.br/newsgen/9811/vpn.html>



Exemplos de VPN

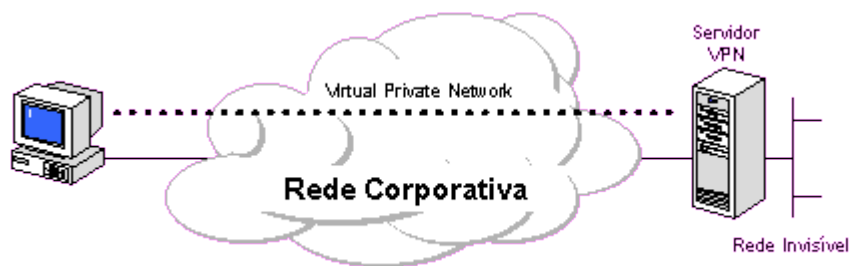
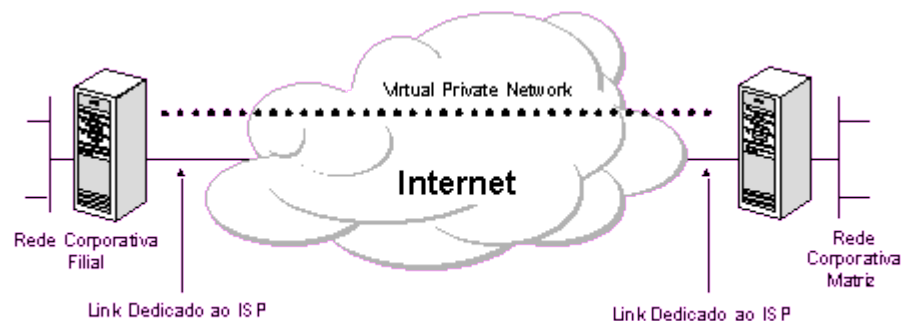


Conexão de LANs (via Internet)

substitui as conexões entre LANs através de circuitos dedicados de longa distância

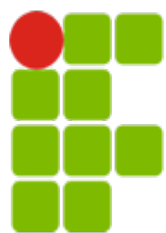
Acesso Remoto (via Internet)

rede virtual privada entre o usuário remoto e o servidor de VPN corporativo através da Internet.



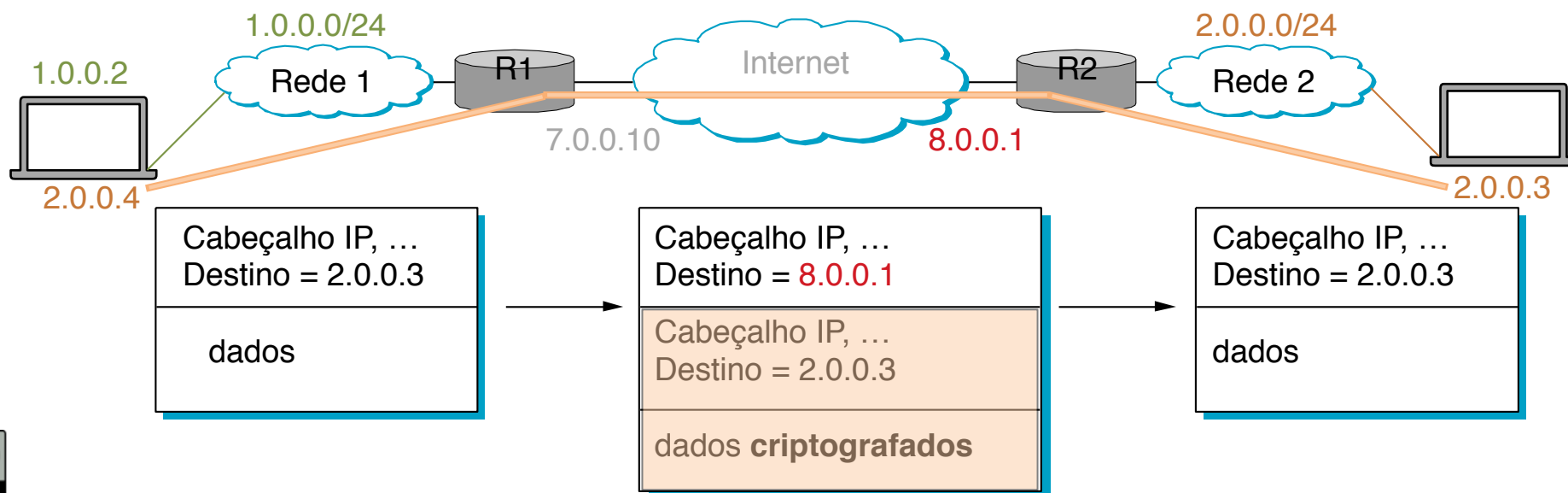
Conexão de PCs (via INTRANet)

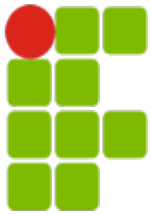
redes locais departamentais são implementadas fisicamente separadas da LAN corporativa (dados confidenciais)



Redes virtuais e túneis (tunelamento)

- As VPNs baseiam-se na tecnologia de tunelamento cuja existência é anterior a elas.
 - mas antes de encapsular o pacote que será transportado, seu conteúdo **é criptografado**
- Pacote IP pode trafegar dentro de um outro pacote IP
 - máquina origem (na rede 1) gera pacote como se estivesse na rede 2
 - roteador empacota-o dentro de outro pacote IP e envia para a rede 2
 - na rede 2, pacote original é desempacotado no servidor da VPN e segue normalmente
 - para todos os efeitos, máquina origem parece estar na rede 2





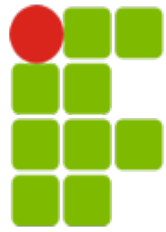
Camada de rede

Nosso objetivo:

- entender os princípios dos serviços da camada de rede:
 - Modelo de serviço
 - Endereçamento
 - Roteamento
 - IPv6

Tópicos abordados:

- Endereçamento (IPv4), máscaras e sub-redes
- Expedição de pacotes
- Protocolos auxiliares
- Roteamento interno (RIP, OSPF) e entre sistemas autônomos (BGP)
- Protocolo IPv6



Roteamento

- Diferença de **Repasse** x Roteamento

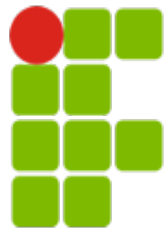
- **Repasse**: selecionar um porto de saída baseado no endereço de destino e na tabela de rotas

SE (**(end_destino & mascara) == (end_interface & mascara)**)

envia datagrama diretamente ao host de destino

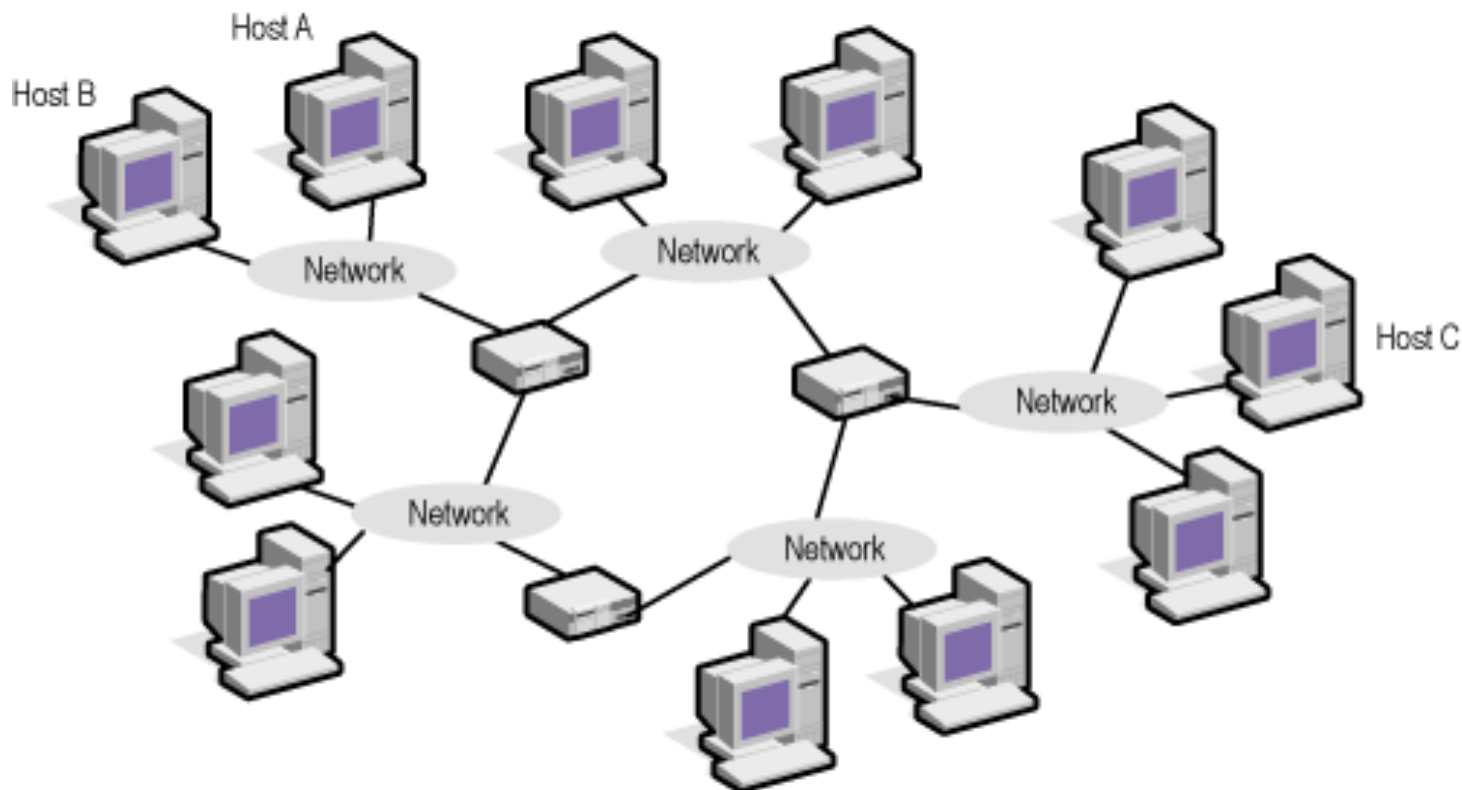
SENÃO

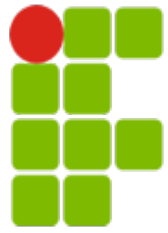
determina próximo passo (roteador) pela tabela de rotas



Roteamento

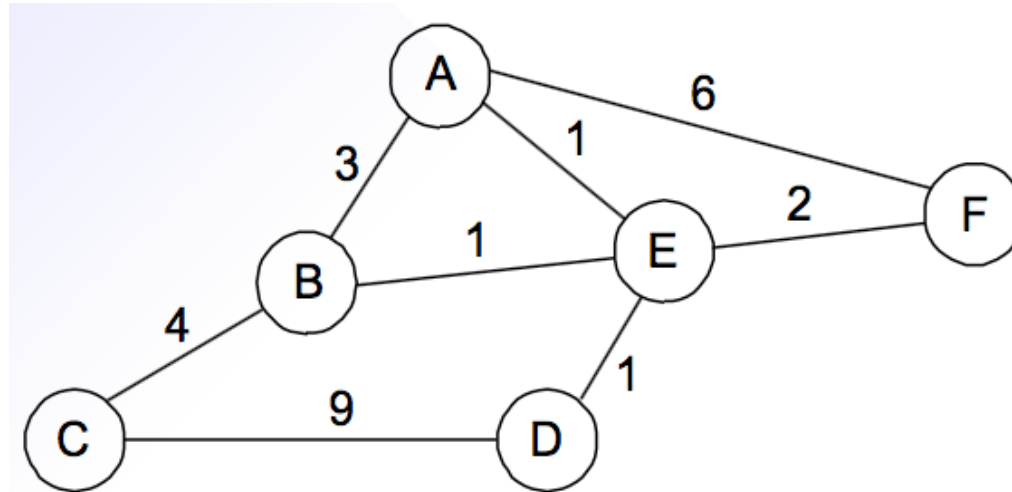
- Diferença de Repasse x **Roteamento**
 - **Roteamento**: processo de construção da tabela de rotas
 - É como os roteadores passam a conhecer as “redes vizinhas”



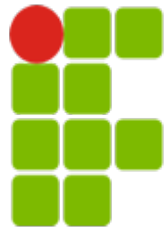


Roteamento

- Diferença de Repasse x **Roteamento**
 - **Roteamento**: processo de construção da tabela de rotas
 - Para isso, a rede deve ser vista como um grafo:

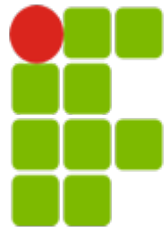


- Problema: encontrar o caminho de menor custo entre nós do grafo
- Fatores relevantes: estáticos (**topologia**) e dinâmicos (**carga**)



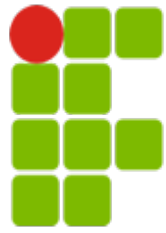
Determinação de rotas

- Responsabilidade de cada entidade ligada à rede: Sistema Autônomo (AS: Autonomous System)
 - um AS corresponde a um domínio administrativo
 - recebe do órgão regulador um nº exclusivo de 16 bits
 - tem controle absoluto sobre **caminhos internos**
 - exemplos: universidades, empresas, ISPs, *backbones*
- Hierarquia de propagação de rotas em dois níveis
 - protocolo **interior** (IGP, *interior gateway protocol*), cada AS pode escolher o seu (ex.: RIP, OSPF)
 - protocolo **exterior** (BGP, *exterior gateway protocol*), todo AS deve utilizar esse protocolo padrão (comum a toda a Internet) para comunicar suas rotas aos demais



Protocolos interiores populares (intra-AS)

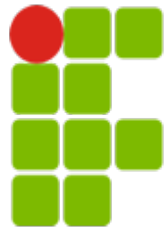
- RIP: *Protocolo de Informação de Roteamento*
 - desenvolvido para a rede da Xerox ([1988](#)) e distribuído com o Unix
 - compara matematicamente rotas para identificar o melhor trajeto
 - baseado na contagem de roteadores (*hop-count*)
 - OSPF: *Menor Rota Livre Primeiro*
 - criado ([1991](#)) para substituir o protocolo RIP
 - padrão Internet mais recente, é o mais utilizado atualmente
 - cada nó constrói uma visão da topologia da rede e descobre sozinho qual é a melhor rota
- **BÔNUS:** permite balanceamento de carga e suporta autenticação de roteadores



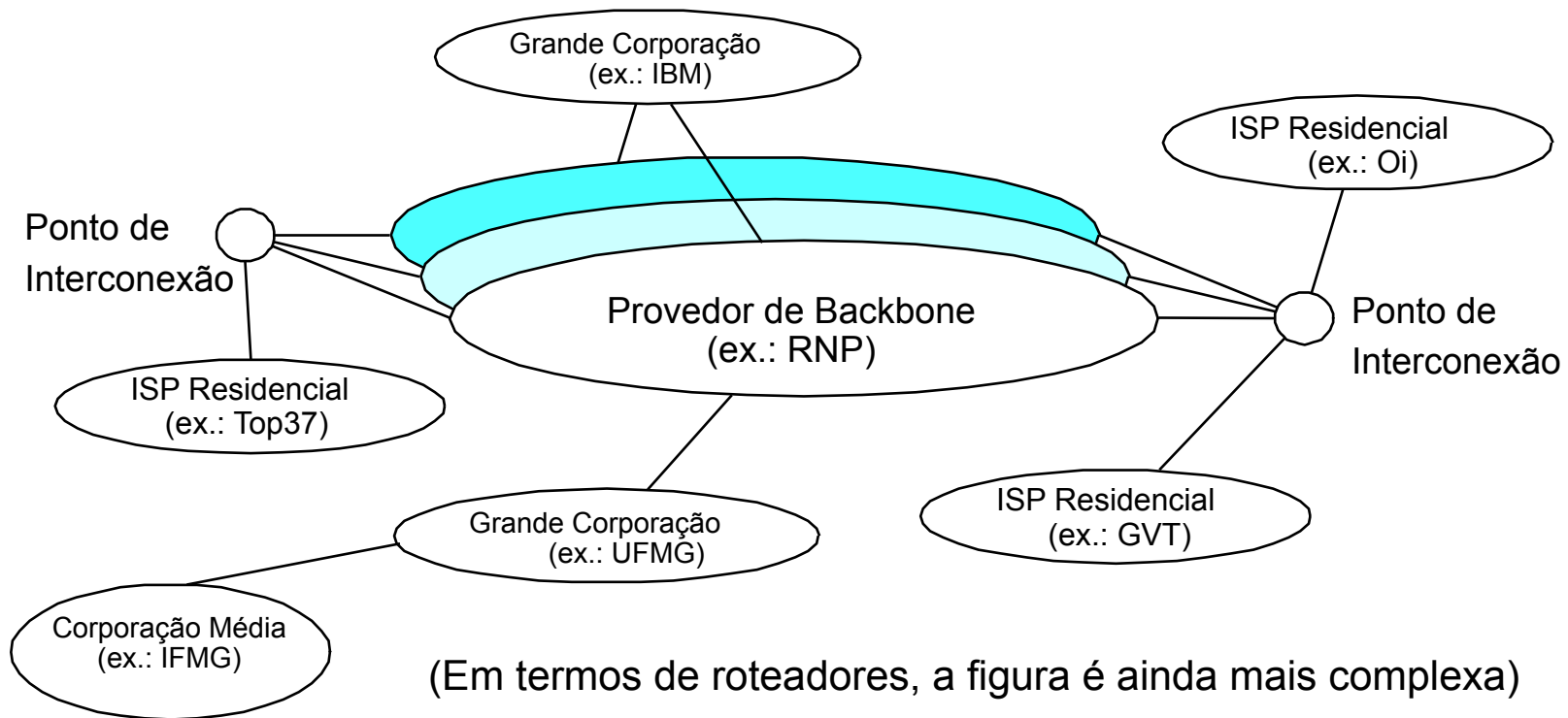
Métricas usadas para o roteamento

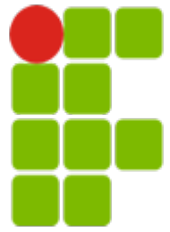
- Métrica original da ARPANET
 - número de pacotes enfileirados em cada link (“engarrafamento”)
 - MAS.... não considerava latência (atraso) nem banda
- Protocolos de roteamento simples (RIP)
 - contagem de saltos (links/roteadores) no caminho
- Novas métricas
 - **atraso** = tempo na fila + tempo de transmissão + latência
 - custo do link = **atraso** médio por algum período de tempo
 - sintonia fina: faixa de valores limitada, inclui utilização do link

→ em suma: escolher a “melhor” rota pode ser complicado, não há uma resposta trivial



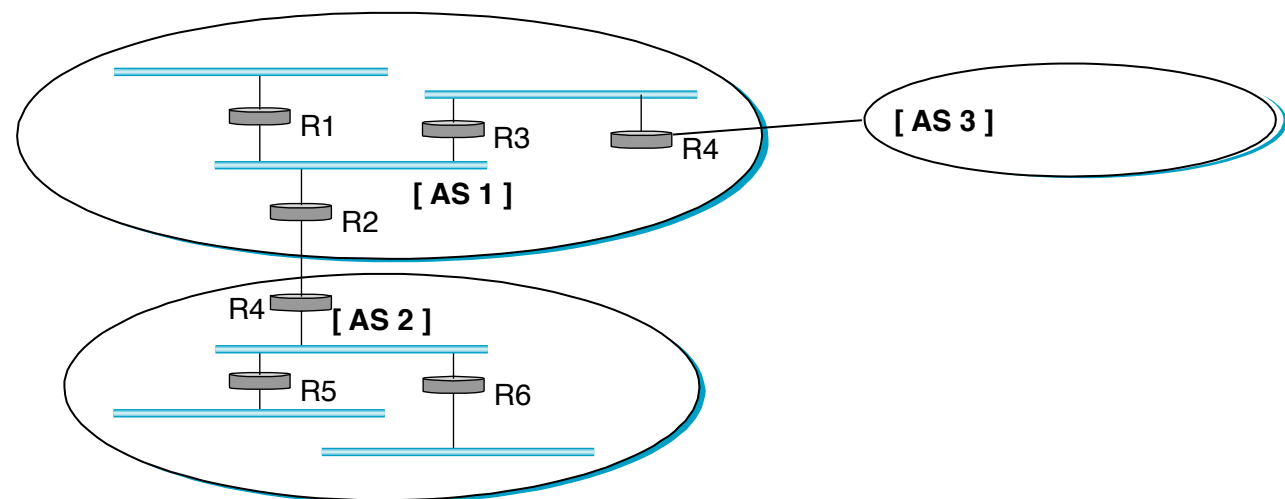
Estrutura da Internet





BGP-4: *Protocolo de Roteador de Borda*

- Cada Sistema Autônomo (AS) tem:
 - um ou mais roteadores de borda (onde os pacotes saem da rede)
 - um “porta-voz” BGP, que anuncia:
 - redes locais internas ao AS
 - outras redes alcançáveis através dele
 - informações sobre caminhos conhecidos (tabela de rotas)
 - porta-voz pode também revogar caminhos previamente anunciados





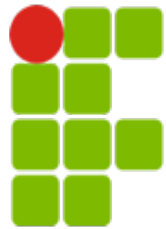
Camada de rede

Nosso objetivo:

- entender os princípios dos serviços da camada de rede:
 - Modelo de serviço
 - Endereçamento
 - Roteamento
 - IPv6

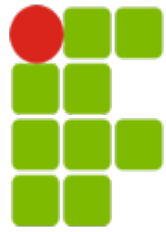
Tópicos abordados:

- Endereçamento (IPv4), máscaras e sub-redes
- Expedição de pacotes
- Protocolos auxiliares
- Roteamento interno (RIP, OSPF) e entre sistemas autônomos (BGP)
- Protocolo IPv6



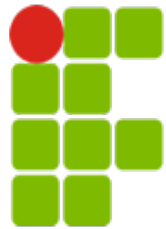
IPv6: motivações

- Motivação básica para criar nova versão de IP: esgotamento dos endereços
 - As pressões por mais endereços haviam diminuído por um tempo com:
 - uso de *firewalls*, *IP forwarding*, NAT, etc.
 - Recentemente, ressurgiram pressões no sentido inverso
 - P2P, multimídia pessoa-a-pessoa (VoIP, vídeo)
- Motivação secundária: suportar novas aplicações, como *vídeo sob demanda* (VoD) e *voz sobre IP* (VoIP)
 - Cabeçalho inclui identificação de fluxo para roteadores com QoS
 - pacotes num fluxo (mesma origem e destino) devem ser tratados da mesma maneira
 - as vantagens relativas ao tratamento de novas aplicações podem justificar adoção



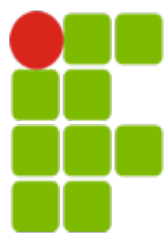
IPv6: características

- Endereços sem classes, com 128 bits
- Previsão para uso eficiente de *multicast*
- Suporte a serviços de tempo real
- O cabeçalho obrigatório foi “enxugado”
 - quão mais simples, mais rápido de processar!
- Adicionados novos campos do cabeçalho IPv6:
 - **Rótulo do Fluxo**: identifica datagramas do mesmo “fluxo” (pacotes de mesma origem/destino), para serem tratados da mesma maneira.
 - **Classe de Tráfego (prioridade)**: permite definir prioridades diferenciadas para vários fluxos de informação
- **Checksum**: foi removido inteiramente para reduzir o tempo de processamento em cada roteador
 - as camadas de Transporte, de Rede e de Enlace fazem um checksum!

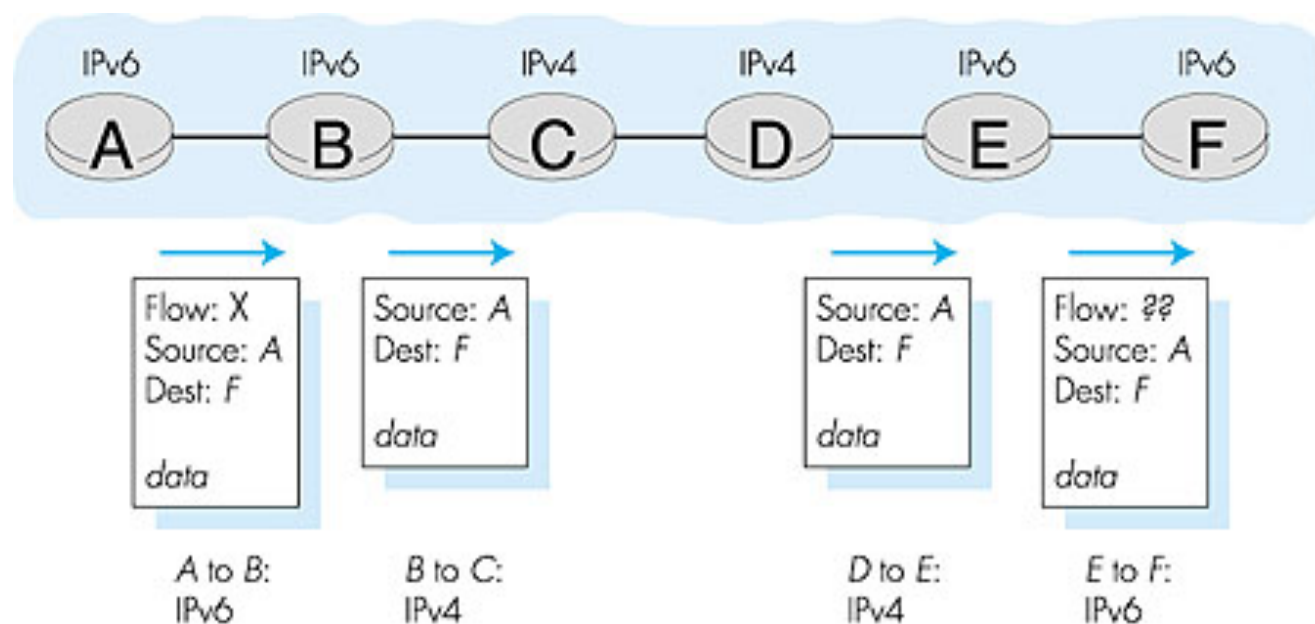


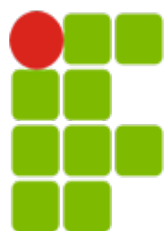
Transição do IPv4 para IPv6

- Nem todos os roteadores poderão ser atualizados simultaneamente
 - não haverá um “dia da vacinação universal”
 - até lá, a rede deverá operar com os dois tipos de datagramas simultaneamente presentes
- Duas abordagens propostas:
 - **pilha de protocolos dupla**: alguns roteadores, com pilhas de protocolos duais (IPv6 e IPv4), podem trocar pacotes nos dois formatos e traduzir de um formato para o outro
 - **tunelamento**: IPv6 transportado dentro de pacotes IPv4 entre roteadores IPv4



Abordagem “pilha dupla com tradução”



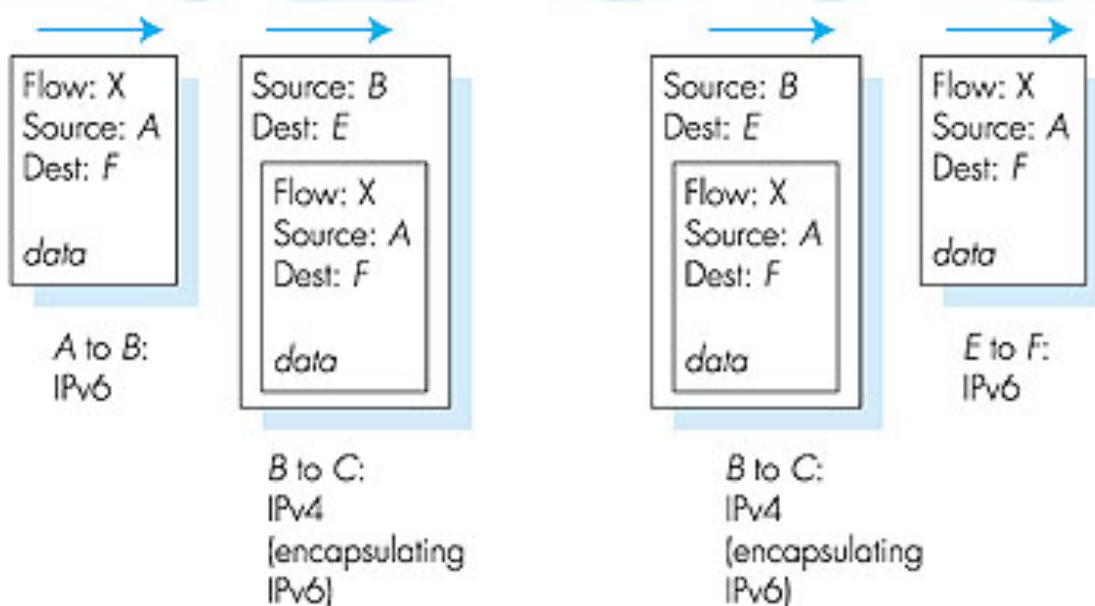
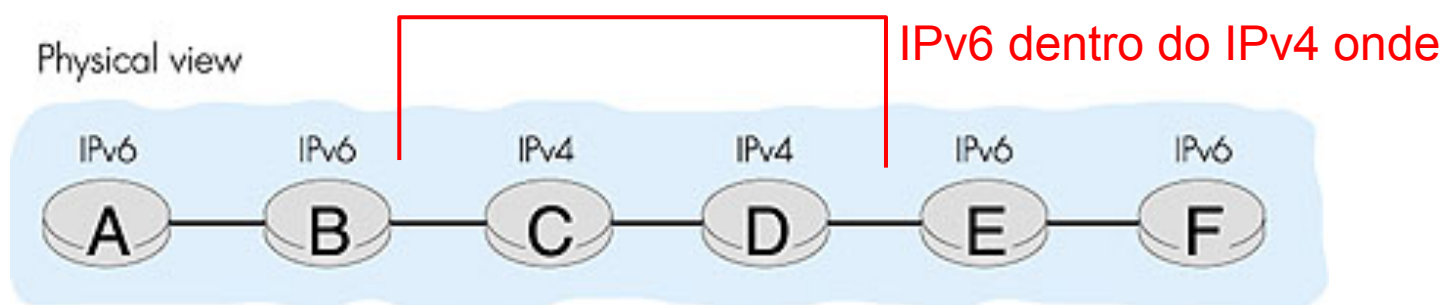


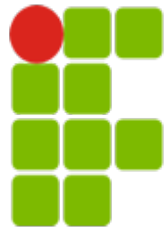
Abordagem de “tunelamento”

Logical view



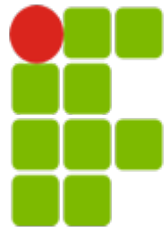
Physical view





NDP: Protocolo de Descoberta de Vizinhos

- Usado com o IPv6, define cinco tipos de pacotes ICMPv6 que desempenham **funções semelhantes** ao ARP e ICMP do IPv4
- O protocolo **NDP** é responsável por:
 - autoconfiguração dos nós
 - descoberta de outros nós no enlace
 - determinação dos endereços físicos de outros nós
 - detecção de duplicação de endereços
 - descoberta de roteadores disponíveis
 - descoberta de servidores DNS
 - descoberta de endereços de prefixo (end. de rede)
 - identificação de indisponibilidade de um vizinho
 - manter informações de alcance sobre os caminhos para nós vizinhos



Saiba mais sobre o IPv6

- <http://www.youtube.com/watch?v=-Uwjt32NvVA>
- <http://www.worldipv6launch.org/measurements/>
- <http://ipv6.br/>
- <http://www.google.com/intl/pt-BR/ipv6/>
- <http://pt.wikipedia.org/wiki/IPv6>
- <http://www.infowester.com/ipv6.php>