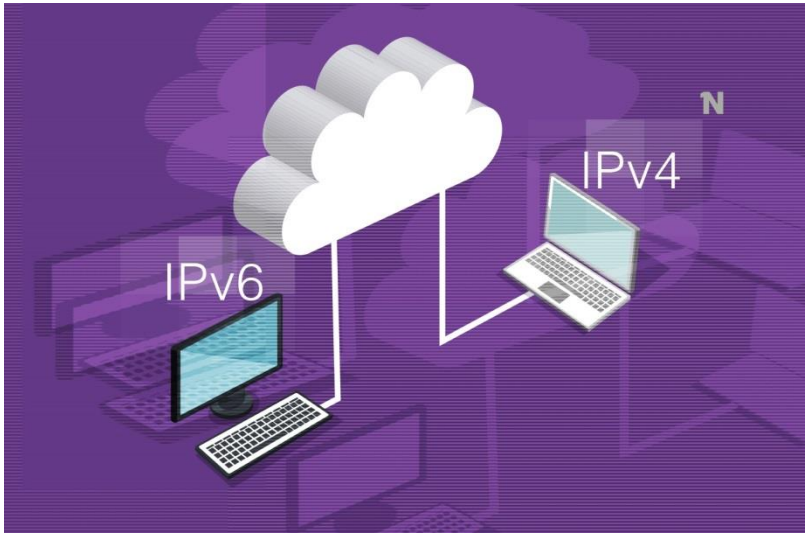
Redes de Computadores

Endereçamento IP



IPv4 x IPv6

Tecnologias como:

- CIDR (roteamento sem uso de classes – permite um melhor aproveitamento dos endereços disponíveis)
- RFC 1918 (endereços privados – permite o uso de endereços não válidos na Internet nas redes corporativas)
- NAT (tradução de endereços – permite que com um endereço válido na Internet apenas, toda uma rede de computadores usando endereços privados seja conectada, mas com várias restrições)
- DHCP (alocação dinâmica de endereços IP – permite que provedores reutilizem endereços Internet para conexões não permanentes)

... foram (e ainda são) usadas como soluções paliativas e ajudaram a manter a Internet funcionando até agora, tempo para "desenvolver" o **IPv6**.

Estimativa de máquinas

Domínio	Hosts	Descrição
.net	376265314	Networks
.com	193223063	Commercial
.jp	74914275	Japan
.de	44875251	Germany
.br	36948579	Brasil
.it	25159545	Italy
.fr	21216185	France
.cn	21385254	China
	...	
.edu	10996207	Educational
Total	1077730537	

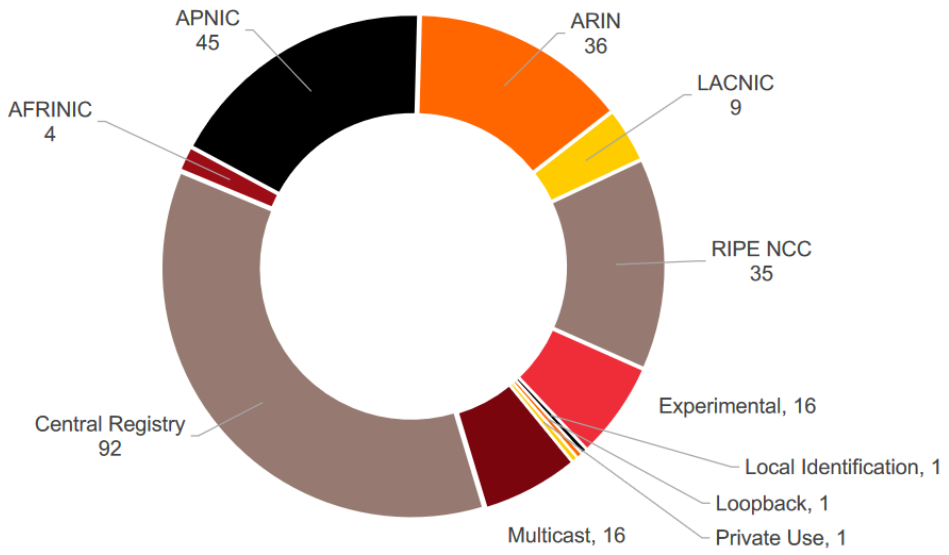
http://ftp.isc.org/www/survey/reports/current/bynum.txt
Dados 2019

Hoje ...

Internet number resource status report

All IPv4 Address Space

Distribution of the 256 /8s



- American Registry for Internet Numbers (ARIN): América do Norte e partes do Caribe;
- Réseaux IP Européens Network Coordination Centre (RIPE NCC): Europa, Oriente Médio e Ásia Central;
- Asia-Pacific Network Information Centre (APNIC):Ásia e Pacífico;
- Latin American and Caribbean Internet Addresses Registry (LACNIC): América Latina e partes do Caribe;
- African Network Information Centre (AfriNIC): África.

https://www.nro.net/wp-content/uploads/NRO-Statistics-2020-Q3-FINAL.pdf

Dados setembro 2020

Estimativas...

- O IPv4 continuará a coexistir com o IPv6 por muitos anos.
- Nem todos os endereços alocados estão em uso, então poderá haver formas de acesso alternativas a endereços, após o esgotamento dos estoques oficiais, provavelmente com alto custo.

A razão principal para o IPv6 é, então...

- A necessidade de mais endereços Internet!
  - Para suportar seu crescimento:
    - Possibilitando a interligação de mais redes, de forma que a expansão da economia, com novas empresas, novos negócios seja suportada.
    - A fim de que todos possam ser incluídos digitalmente, em especial nos países em desenvolvimento
    - Com o uso de novas aplicações, como sua utilização em dispositivos móveis com tecnologia 3G, por exemplo, ou em elétro-domésticos e outros aparelhos com eletrônica embarcada
    - Com a eliminação de tecnologias como o NAT, que dificultam o funcionamento de várias aplicações

Quais as diferenças entre IPv4 e IPv6?

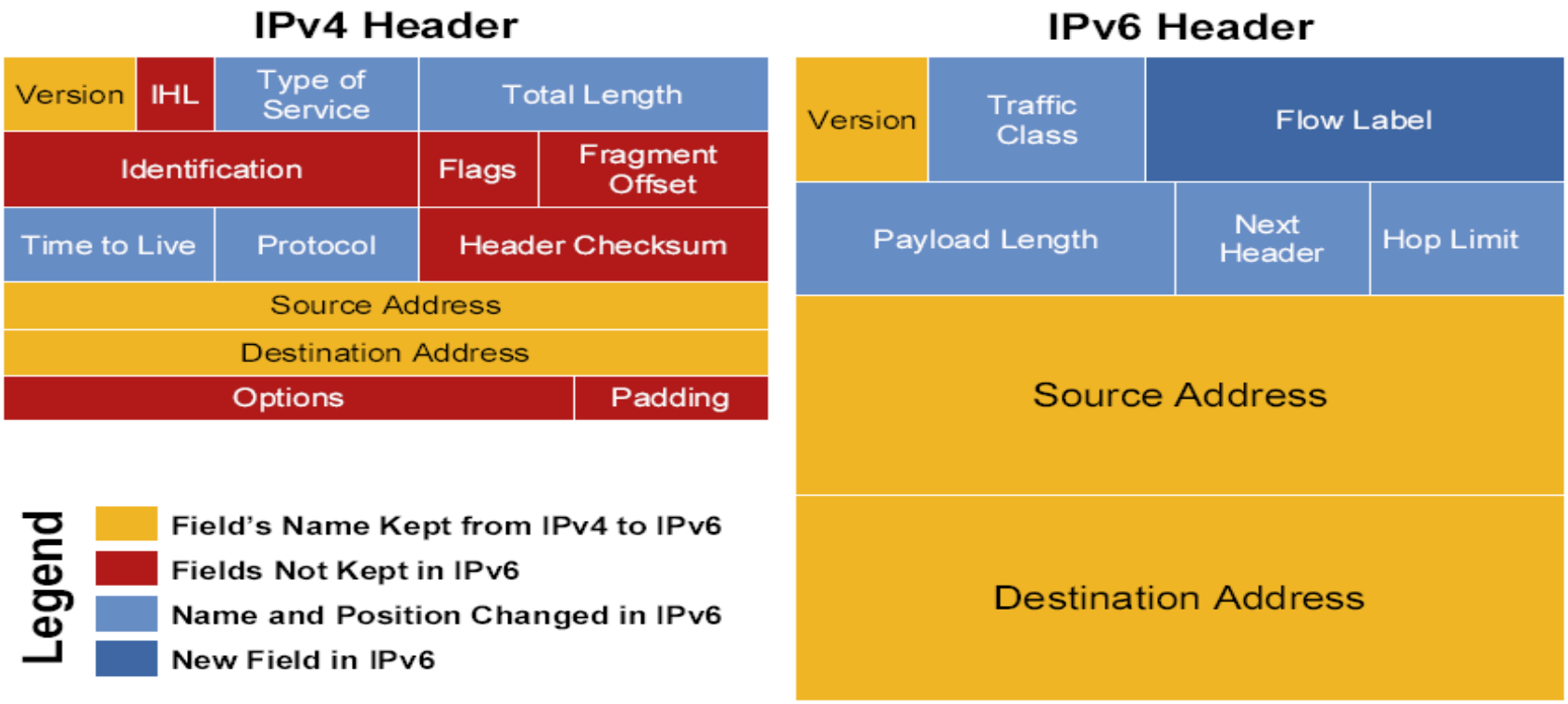
Números...

- Se a questão principal é ter mais endereços:

- Um endereço IPv4 é formado por 32 bits.
  - 2^32 = 4.294.967.296 endereços
    aproximadamente 4 trilhões de endereços

- Um endereço IPv6 é formado por 128 bits.
  - 2^128 = 340.282.366.920.938.463.463.374.607.431.768.211.456 endereços
  - ~ 79 trilhões de trilhões de vezes mais que no IPv4.
  - ~ 5.6 x 1028 endereços IP por ser humano.
  - ~ 66.557.079.334.886.694.389 de endereços por cm2 na superfície da Terra.

Formato


IPv4 Header
Version
IHL
Type of Service
Total Length
Identification
Flags
Fragment Offset
Time to Live
Protocol
Header Checksum
Source Address
Destination Address
Options
Padding
IPv6 Header
Version
Traffic Class
Flow Label
Payload Length
Next Header
Hop Limit
Source Address
Destination Address
Legend
Field's Name Kept from IPv4 to IPv6
Fields Not Kept in IPv6
Name and Position Changed in IPv6
New Field in IPv6

Endereços

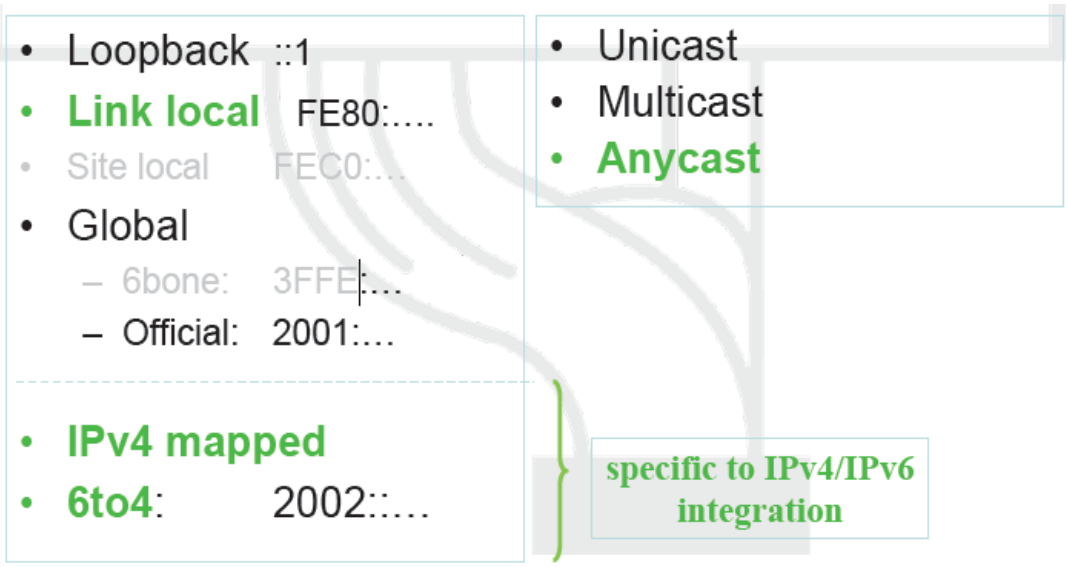
- Representação
  - Números hexadecimais de 16bits
  - Separados por “ : “
  - Podem ser maiúsculos ou minúsculos
  - Abreviações são possíveis:
    - Zeros à esquerda podem ser omitidos
    - Zeros contínuos são representados por ::
    - Exemplo:
      - 2001:0db8:0000:130F:0000:0000:087C:140b
      - 2001:0db8:0:130F::087C:140b

- Prefixos
  - Como o CIDR (IPv4)
  - Exemplo:
    - 2001:db8:12::/48

Endereços

Uma mesma interface de rede tem vários endereços, com funções diversas:

Loopback: válido para o host
Link Local: válido para a rede local, assinalado automaticamente com base no MAC Address.
Global: válido na Internet



Mudanças

- O IPv6 não é só um “upgrade” do IP. Ele é um protocolo novo. Do ponto de vista dos equipamentos é um protocolo diferente.
  - Para implantar o IPv6, provavelmente serão necessárias mudanças:
    - Em boa parte dos equipamentos de redes
      - Roteadores
      - Switches
      - Firewalls
    - Em alguns dos programas
      - Para alguns, legados, não será possível mudar
    - Em alguns dos sistemas operacionais
    - Nas características das conexões à Internet

Como fazer a implantação?
IPv4 e IPv6 podem conviver?

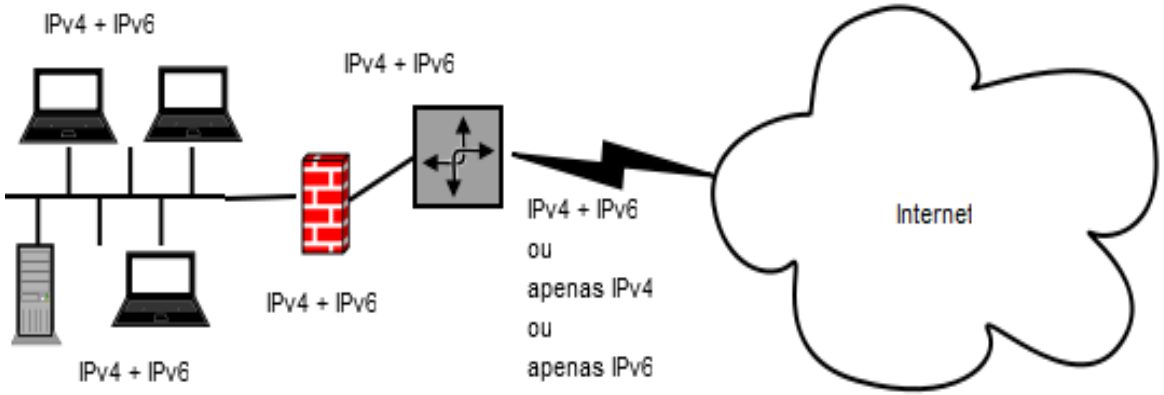
Existem várias abordagens para a transição

- Pilha dupla (dual stack)
  - Os equipamentos usam simultaneamente IPv4 e IPv6
  - Quanto à conectividade à Internet, pode ser:
    - Só IPv4
    - Só IPv6
    - IPv4 e IPv6
- Túneis (conectando ilhas IPv6 entre si)
  - O IPv6 pode ser encapsulado dentro de conexões IPv4
  - Os pacotes IPv6 podem ser transmitidos dentro de pacotes IPv4
  - IPv6-over-IPv4 / Tunnel Broker / 6to4 / ISATAP / Teredo
- Tradução de pacotes (redes IPv4 conversando com redes IPv6)
  - Reescrevendo os cabeçalhos dos pacotes IP
  - Reescrevendo os cabeçalhos dos pacotes TCP
- Tradução de aplicações

Pilha Dupla

Os equipamentos funcionam com IPv4 e IPv6 simultaneamente
Exige suporte para IPv4 e IPv6 em praticamente todos os equipamentos de rede e computadores

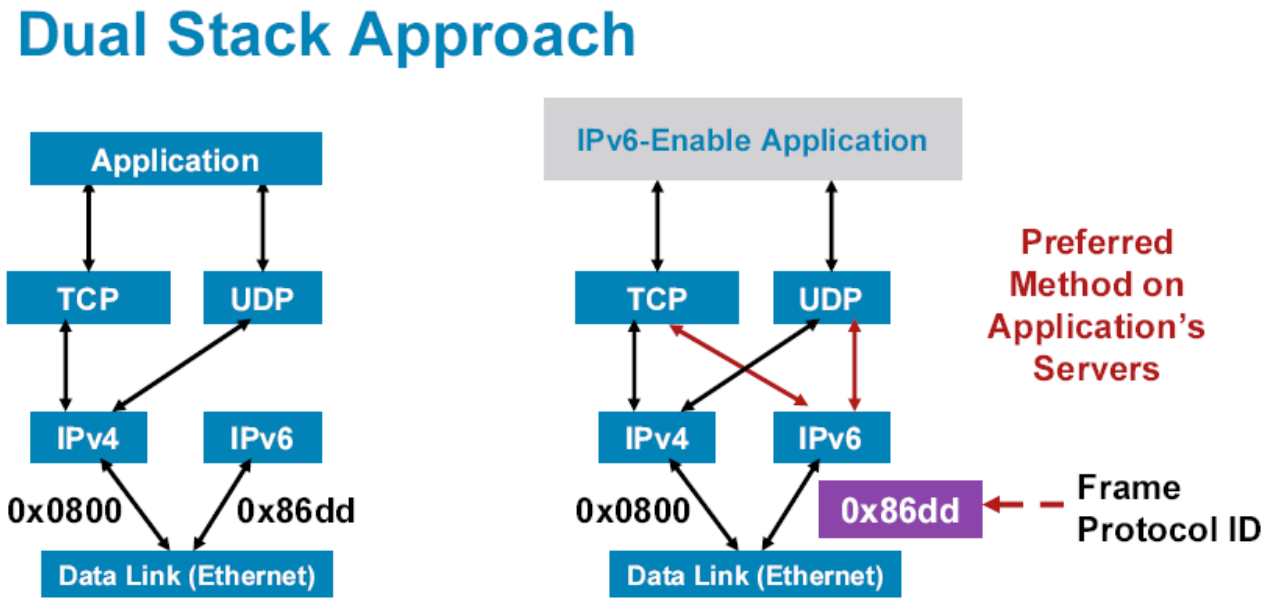
- Permite que a implantação do IPv6 seja feita sem mudar a topologia da rede IPv4
- Pode ser implementada com ou sem conectividade IPv6 à Internet.
- Pode utilizar endereços válidos IPv6, em conjunto com NAT para IPv4



Pilha Dupla

As aplicações têm os dois protocolos à disposição.

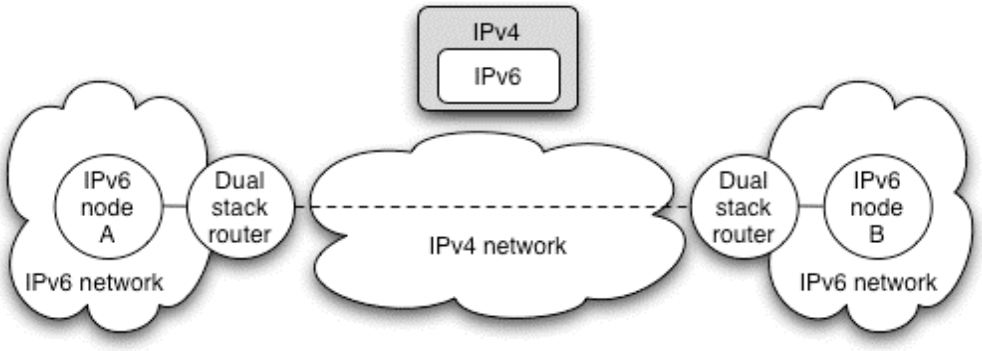
- Quando acessa um serviço disponível através de ambos, a aplicação deve escolher um deles:



Túneis

Hoje: Ilhas IPv6 conectem-se através de redes IPv4
No futuro: Ilhas IPv4 conectem-se através de redes IPv6
Vários tipos:

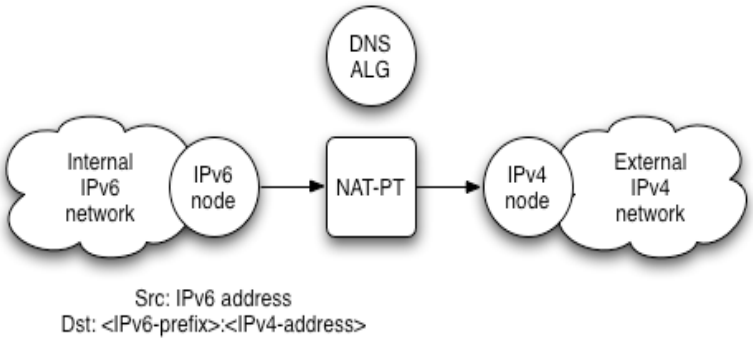
- IPv6-over-IPv4
- Tunnel Broker
- 6to4
- ISATAP
- Teredo

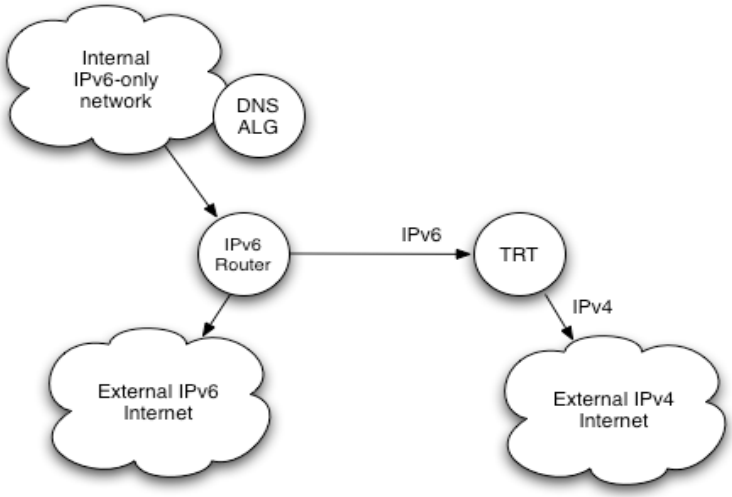


Tradução de pacotes

Serve para permitir a comunicação de uma rede que “fala” somente IPv4 com outra, que “fala” somente IPv6.

- Pode ser usada, por exemplo, se você tem uma rede IPv6 e precisa acessar recursos na Internet v4.
- Para suportar aplicações ou sistemas operacionais que somente funcionam com IPv4
- Usa protocolos como NAT-PT e TRT

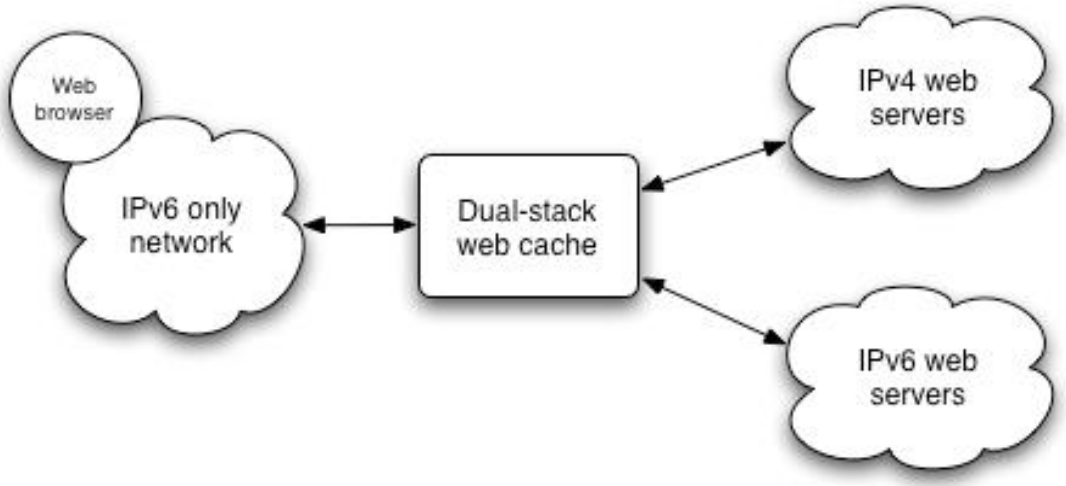




Tradução de aplicações

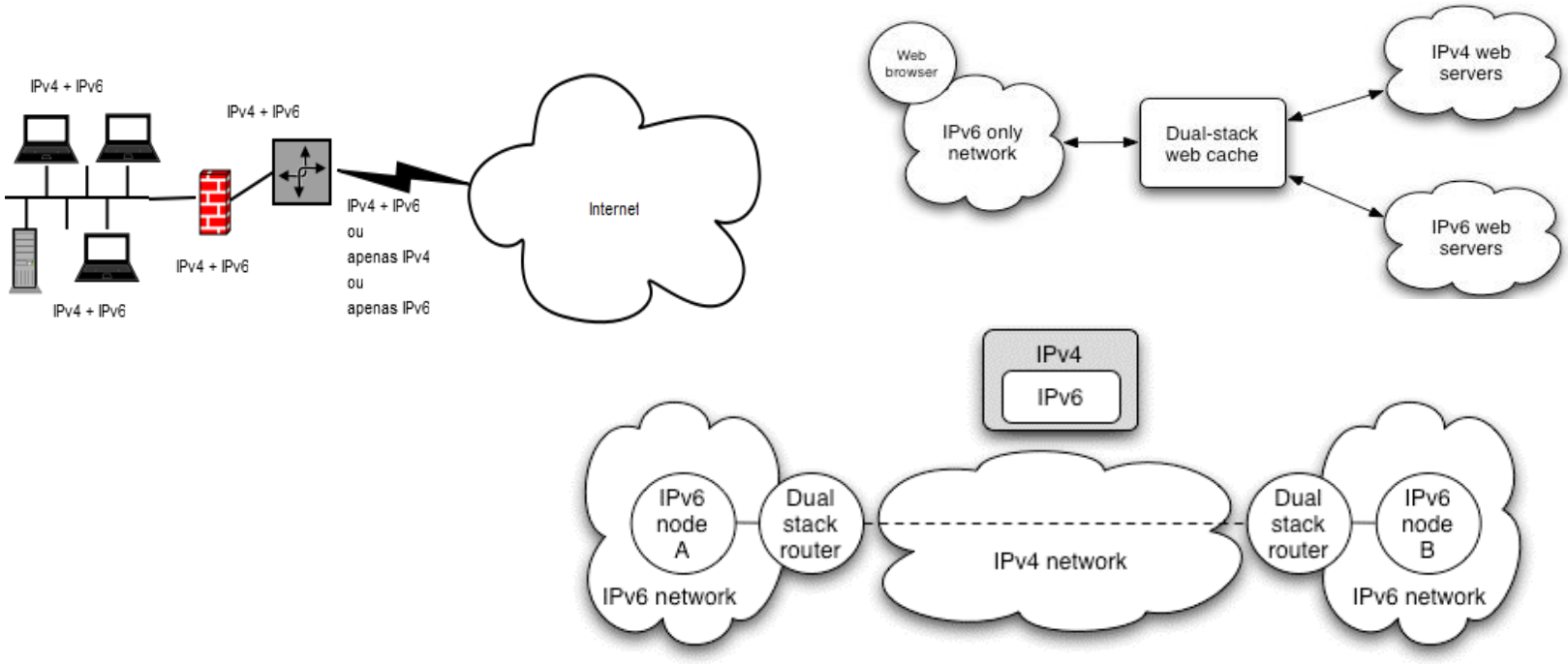
Como a tradução de pacotes é um tanto complicada, pode-se prover a conectividade para aplicações específicas:

- Existem gateways que operam no nível das aplicações (ALGs) e oferecem alternativas mais simples.
- Aplicações que suportam ALG:
  - Cache web
  - Gateway SMTP
  - Resolver DNS
  - Proxy SIP
  - etc



O que usar na implantação?

A resposta deve ser dada caso a caso...
Mas, provavelmente: Um pouco de cada tecnologia!



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 Tráfico (prioridade): permite definir prioridades diferenciadas para vários fluxos de informação

- Checksum: 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

ENVIO DE DATAGRAMAS– ROTEAMENTO

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;

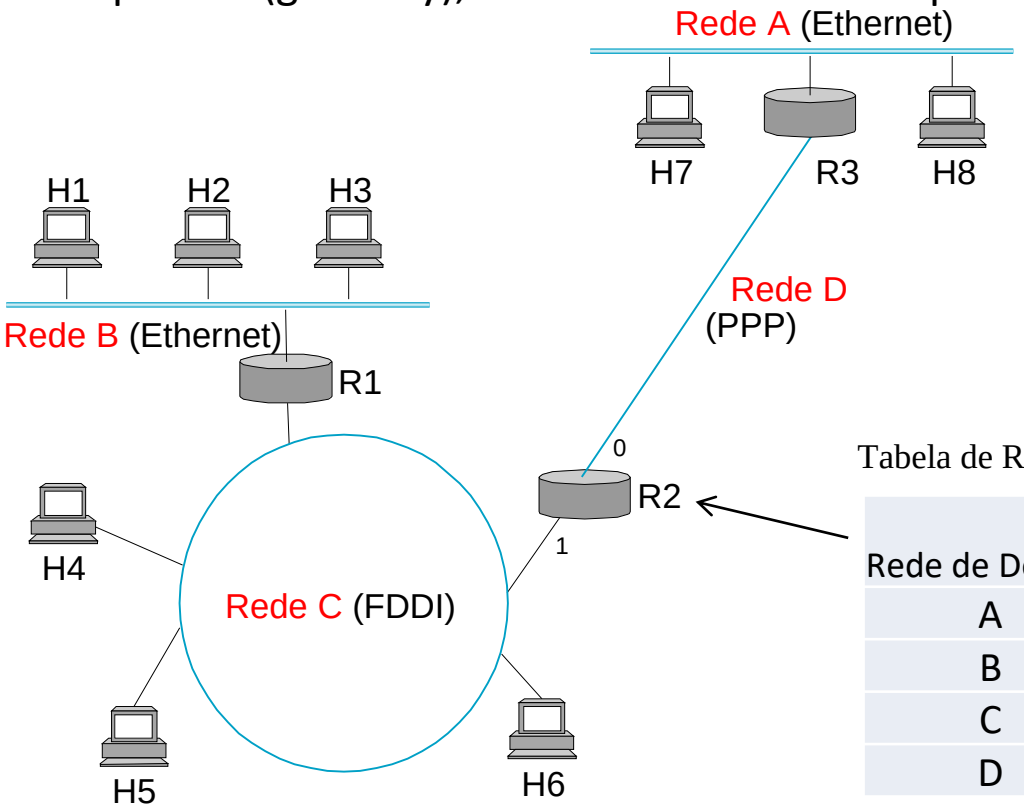


Tabela de Roteamento do roteador R2

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

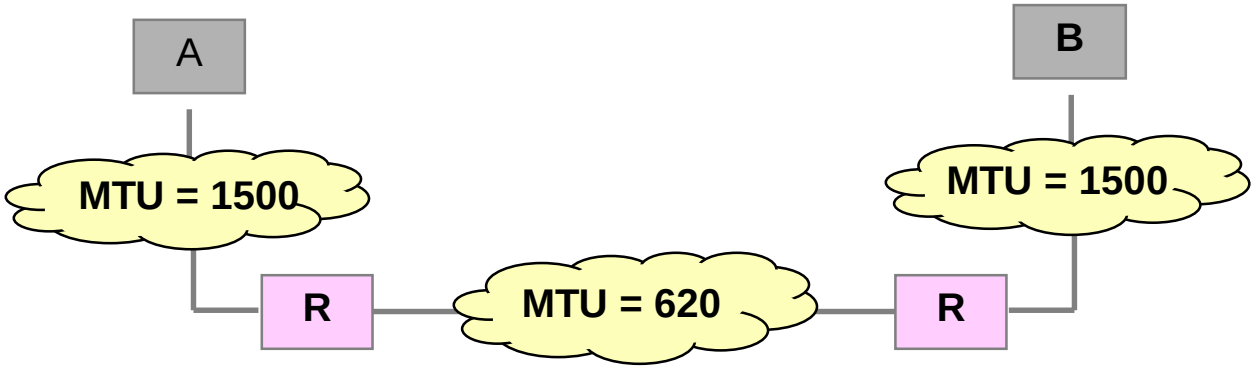
Problemas associados à expedição

- Cada rede pode ter limites diferentes para o tamanho máximo de pacotes
  - É preciso ser capaz de enviar pacotes grandes em qualquer rede
  - 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 rede de cada protocolo especifica um pacote máximo que pode ser enviado de cada vez:
  - MTU (*Maximum Transfer Unit*)



Qual o tamanho do datagrama neste caso?

Fragmentação e Remontagem

- Enlaces de rede têm MTU correspondente ao **maior quadro que pode** ser transportado pela camada de enlace.

tipos de enlaces diferentes possuem MTU diferentes

Ethernet: 1492 bytes

Wi-Fi: 2304 – 7981 bytes

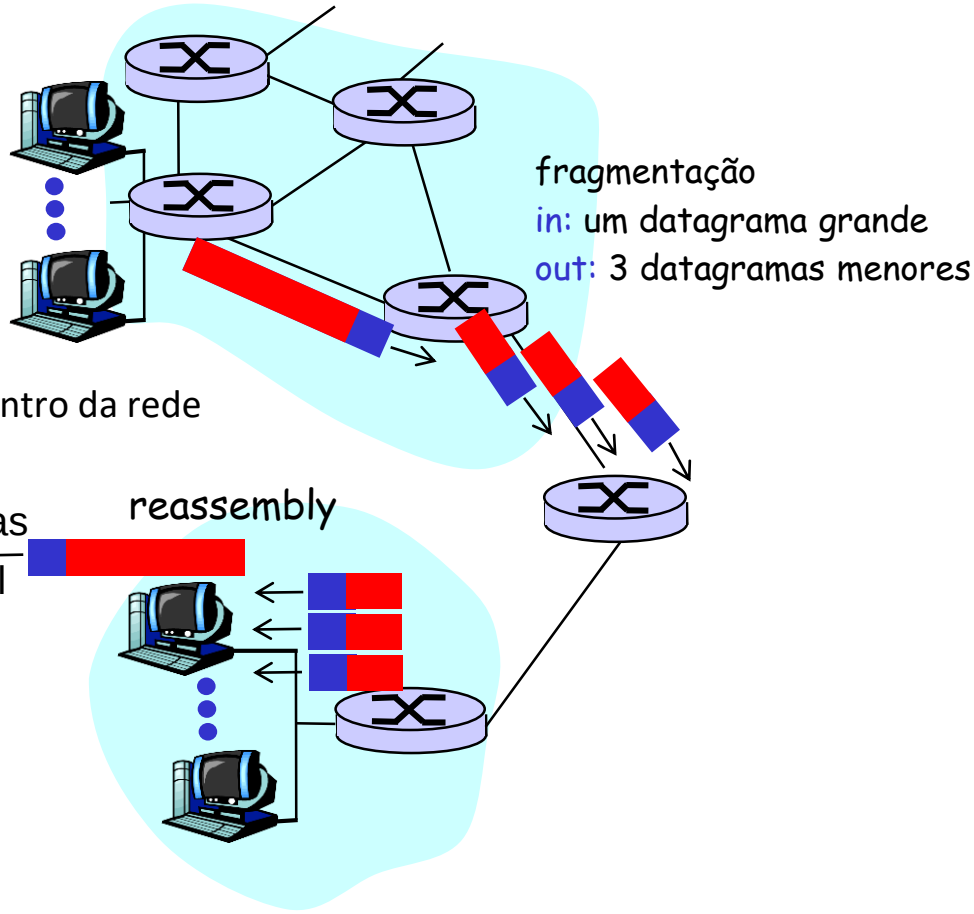
FDDI: 4352 bytes

- Datagramas IP grandes devem ser divididos dentro da rede (fragmentados)

um datagrama dá origem a vários datagramas

"remontagem" ocorre apenas no destino final

O cabeçalho 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

- Fragmentar apenas se necessário (MTU < pacote)
  - tentar evitar fragmentação já no próprio nó de origem
  - nos intermediários é permitido re-fragmentar, se necessário
  - remontagem é feita só no nó de destino

- OBS.: 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

O que ocorre se fragmentos são perdidos,
chegam foram 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: (Tamanho datagrama)/(Tamanho cabeçalho)
  - o datagrama deve 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 endereços IP locais a endereços físicos

Como localizar 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

Tradução de Endereços: endereço lógico (IP) para físico (MAC)

- Protocolo ARP (Address Resolution Protocol)
  - protocolo da cama de enlace
  - traduz 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

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 DCHP (camada de aplicação)

Configuração de máquinas

Qual a informação mínima para uma máquina operar na rede?

- Quem sou eu?
  - Endereço e máscara locais
- 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)

- 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.: 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

- **Notificação de erros e controle**
  - problemas na operação da rede podem ser notificados
  - protocolo de controle geral deve ser reconhecido: ICMP (camada de rede)

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
  - Notificação de falhas (*ex.: destino inalcançável, checksum, remontagem*)
  - Redirecionamento de rotas
  - Requisição de informações

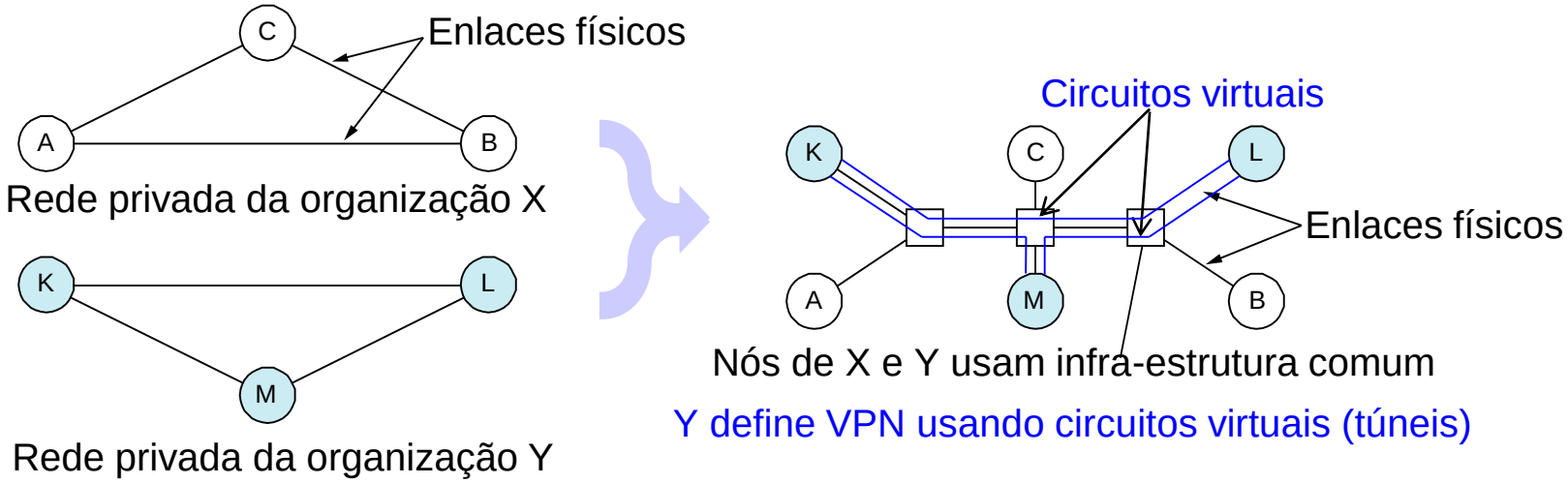
Protocolos auxiliares na operação da rede

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*



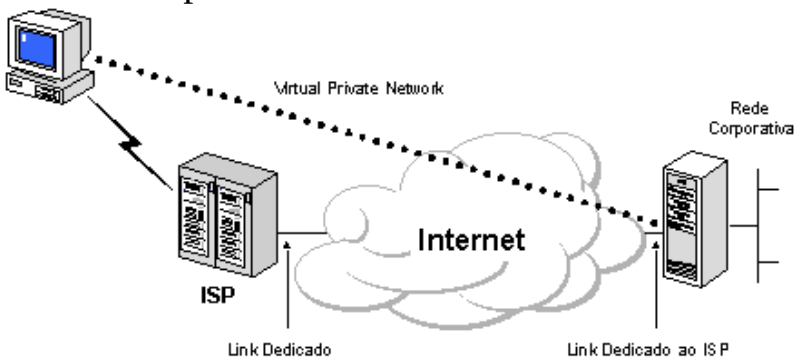
Redes virtuais (VPNs)

- 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
- 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.

Exemplos de VPN

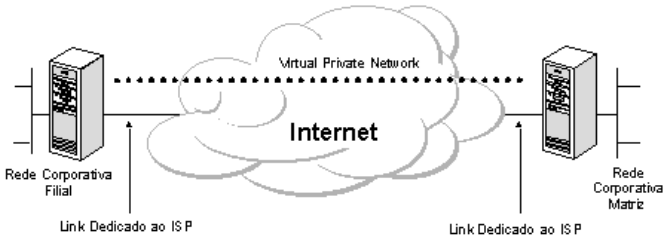
Acesso Remoto (via Internet)

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



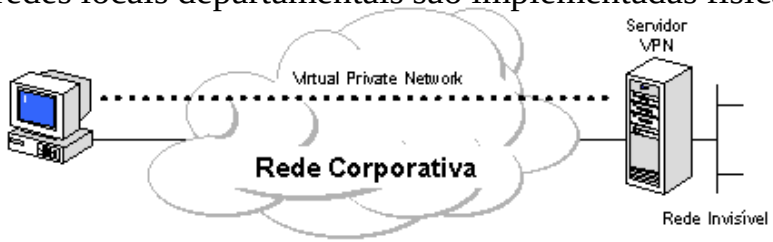
Conexão de LANs (via Internet)

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



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, este é criptografado

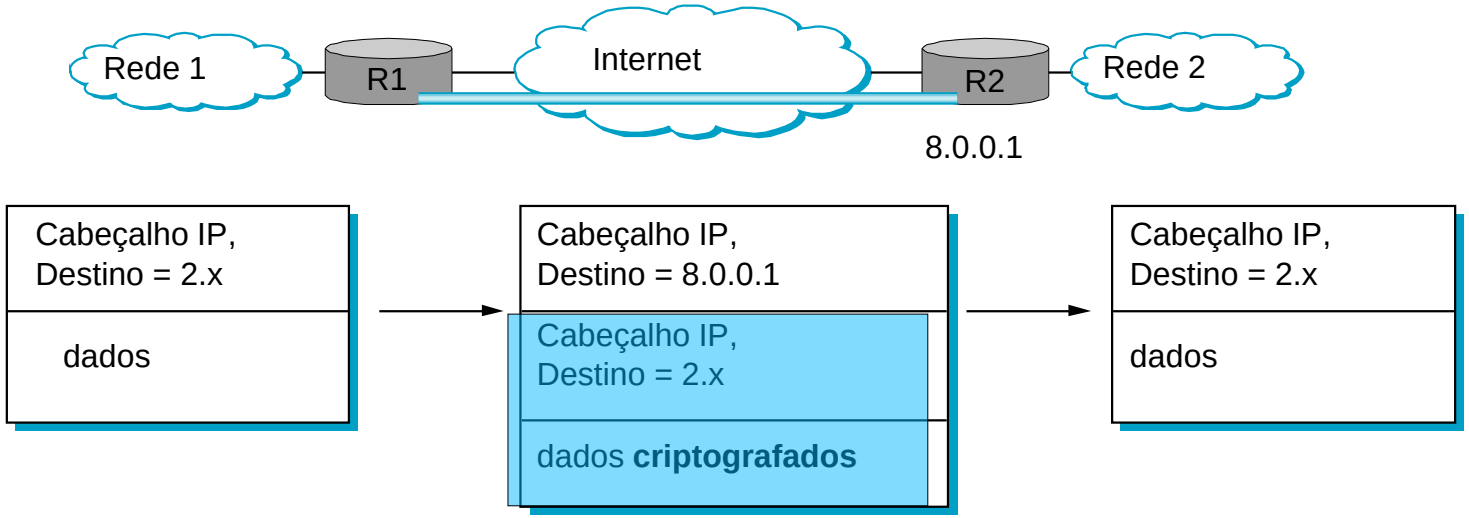
- Pacote IP pode trafegar dentro de um outro pacote IP

°máquina origem (na rede 1) gera pacote como se estivesse na rede 2

°roteador empacota o pacote dentro de outro IP e envia para a rede 2

°na rede 2, pacote original é desempacotado e navega normalmente

Para todos os efeitos, máquina origem parece estar na rede 2



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**))

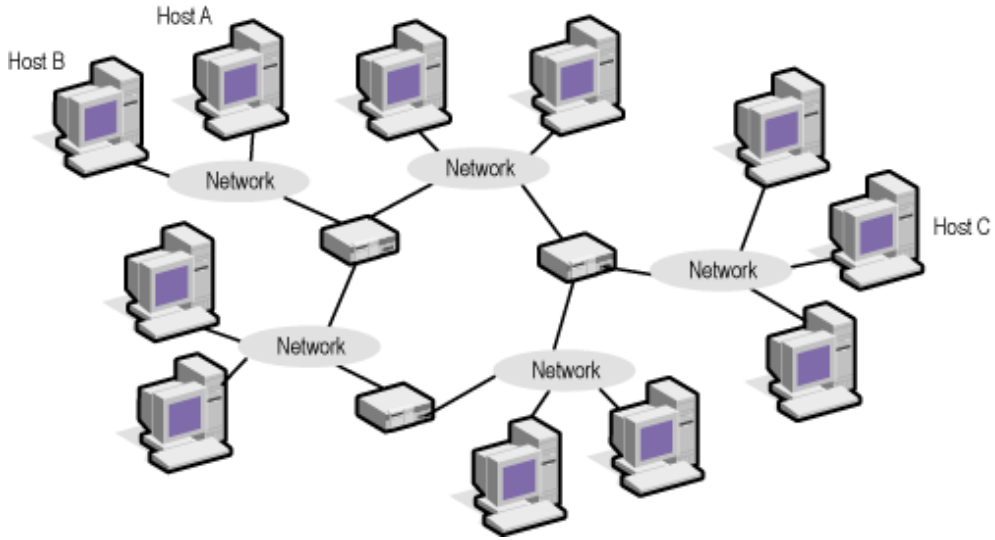
envia datagrama diretamente ao host de destino

°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
  - 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: A*utonomous System*)
  - um AS corresponde a um domínio administrativo
  - 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*), padrão comum a toda a Internet

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

°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

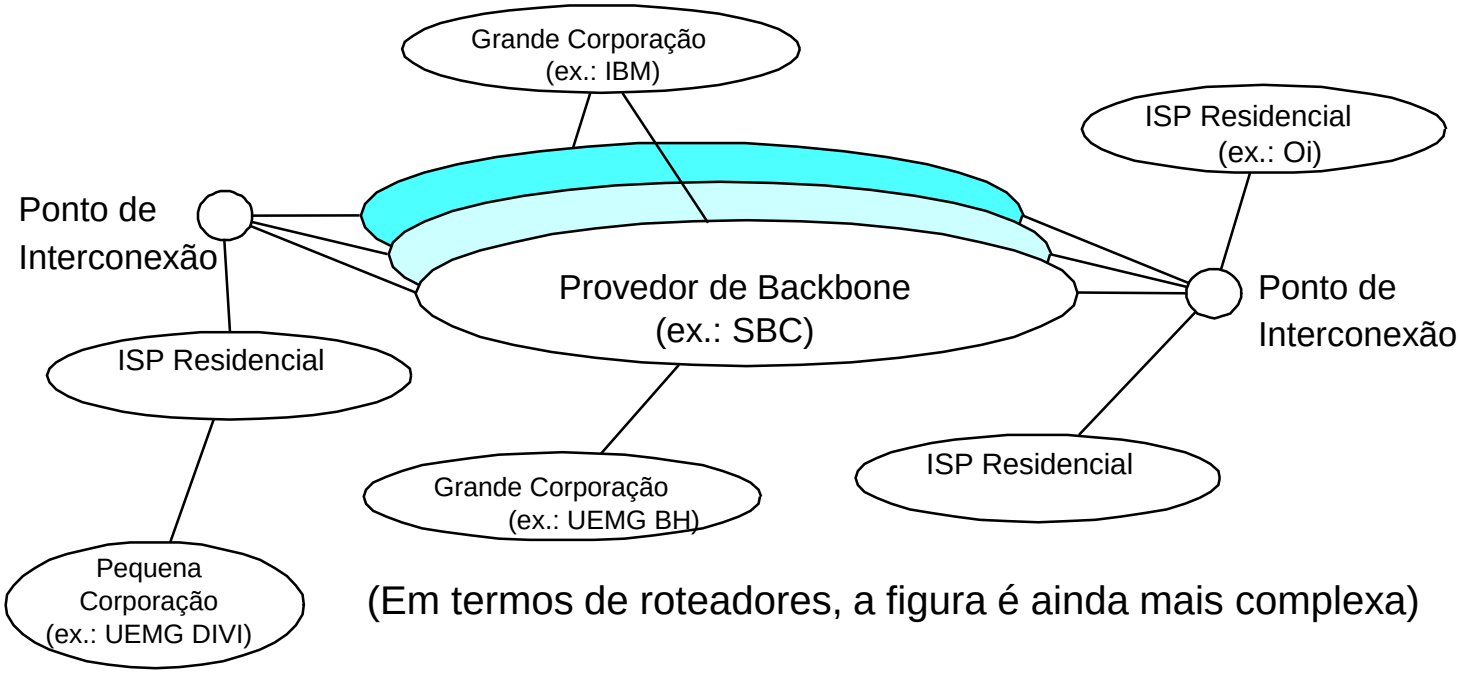
- Protocolos de roteamento simples (RIP)
  - contagem de saltos (links/roteadores) no caminho

- 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

Atualmente:



(Em termos de roteadores, a figura é ainda mais complexa)

- Dúvidas?

Interessantes para consultas:

- https://www.iana.org/numbers
- https://www.nro.net/about/rirs/statistics/

Redes de Computadores

Endereçamento IP