



Ciência da Computação

Redes

Camada de Rede

1º Semestre de 2018
Prof. Vaine Luiz Barreira
<http://bit.ly/unipcc18>

Camada de Rede

A camada de rede está relacionada à transferência de pacotes da origem para o destino.

Chegar ao destino pode exigir vários ***hops*** (saltos) em roteadores intermediários ao longo do percurso.

Essa função contrasta com a função da camada de enlace de dados que tem como função principal mover quadros de uma extremidade de um fio para a outra.

Camada de Rede

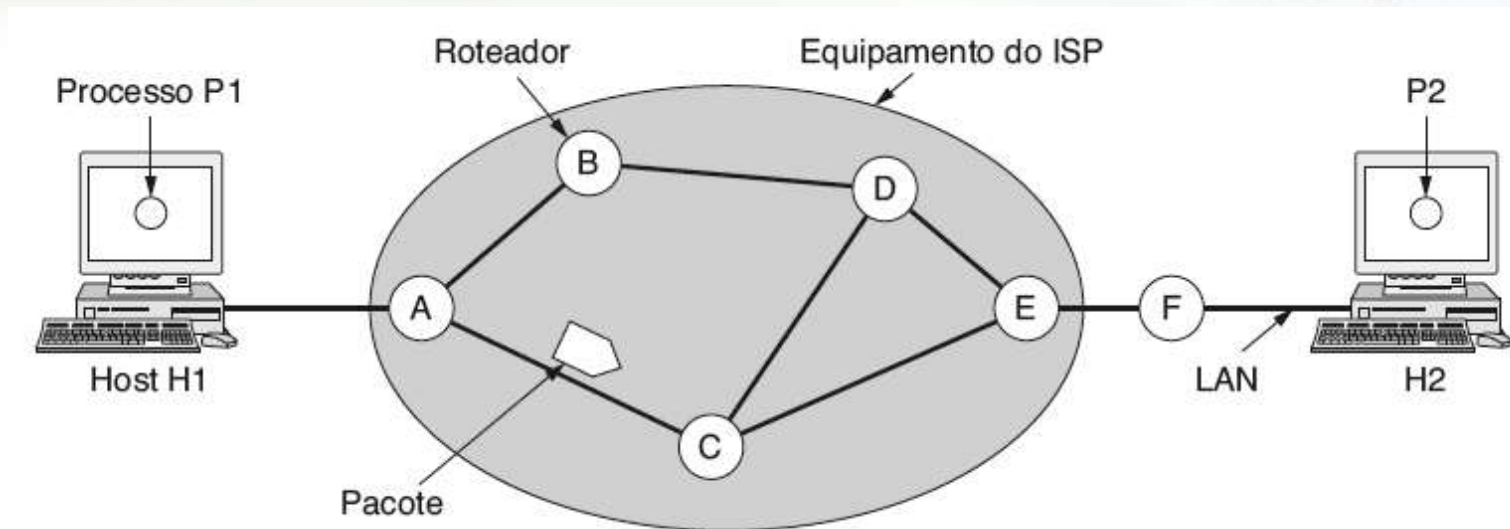


A camada de rede deve conhecer a topologia da rede (ou seja, o conjunto de todos os roteadores e enlaces) e escolher os caminhos mais apropriados que a compõem.

Deve ter o cuidado de escolher rotas que evitem sobrecarregar algumas das linhas de comunicação e roteadores enquanto deixa outras ociosas.

Quando a origem e destino estão em redes diferentes, ocorrem novos problemas, e cabe à camada de rede lidar com eles.

Comutação de pacotes Store-and-Forward



- Um host com um pacote a enviar o transmite para o roteador mais próximo.
- O pacote é armazenado ali até chegar totalmente, de forma que o *checksum* possa ser conferido.
- Em seguida, ele é encaminhado para o próximo roteador ao longo do caminho, até alcançar o host de destino, onde é entregue.

Serviços oferecidos à Camada de Transporte

- Os serviços devem ser independentes da tecnologia de roteadores.
- A camada de transporte deve ser isolada do número, do tipo e da topologia dos roteadores presentes.
- Os endereços de rede que se tornaram disponíveis para a camada de transporte devem usar um plano de numeração uniforme, mesmo nas LANs e WANs.

Questionamento: a camada de rede deve fornecer serviço orientado a conexões ou não orientado a conexões?

Serviço orientado a conexões ou não?



Ponto de vista da Comunidade da Internet:

- A tarefa dos roteadores é tão somente movimentar pacotes.
- Os hosts devem aceitar o fato de que a rede é pouco confiável e fazerem eles próprios o controle de erros (ou seja, detecção e correção de erros) e o controle de fluxo.
- Preferência por um serviço sem conexões.

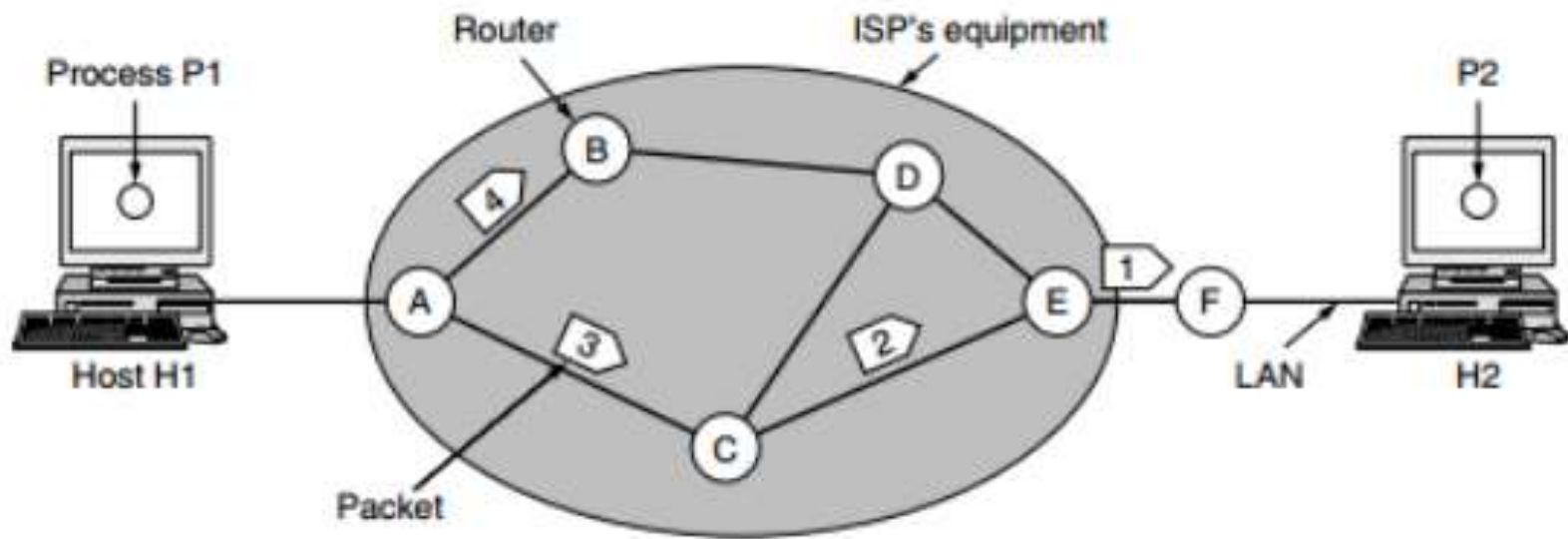
Serviço orientado a conexões ou não?

Ponto de vista das Companhias Telefônicas (ISPs):

- A sub-rede deve fornecer um serviço orientado a conexões confiável.
- A qualidade de serviço é o fator dominante e, sem conexões na sub-rede, é muito difícil alcançar qualidade de serviço.
- Preferência por um serviço orientado a conexões.

Rede de Datagramas

Implementação do serviço não orientado a conexões.



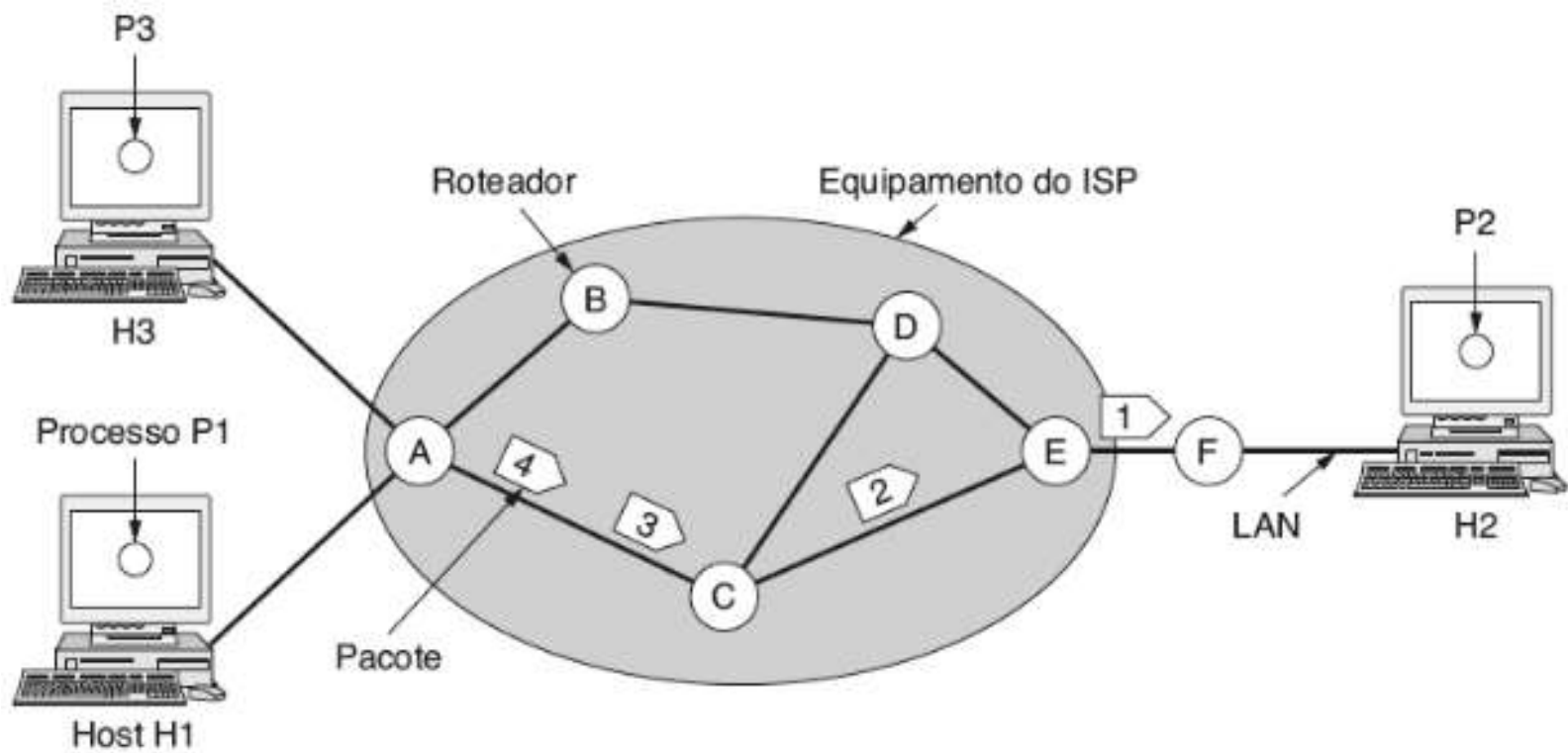
Pacotes (datagramas) são injetados individualmente na sub-rede e roteados de modo independente uns dos outros.
Importante o algoritmo de roteamento.

Implementação do serviço orientado a conexões

- Sub-rede de Circuitos Virtuais.
- Evitar a necessidade de escolher uma nova rota para cada pacote enviado.
- Quando uma conexão é estabelecida, escolhe-se uma rota desde a máquina de origem até a máquina de destino.
- A rota é usada por todo o tráfego que flui pela conexão, exatamente como ocorre no sistema telefônico.
- Quando a conexão é liberada, o circuito virtual também é encerrado.
- Com o serviço orientado a conexões, cada pacote transporta um identificador, informando a que circuito virtual ele pertence.

Rede de Circuitos Virtuais

Implementação do serviço orientado a conexões.



Um exemplo é o **MPLS** (*MutiProtocol Label Switching*)

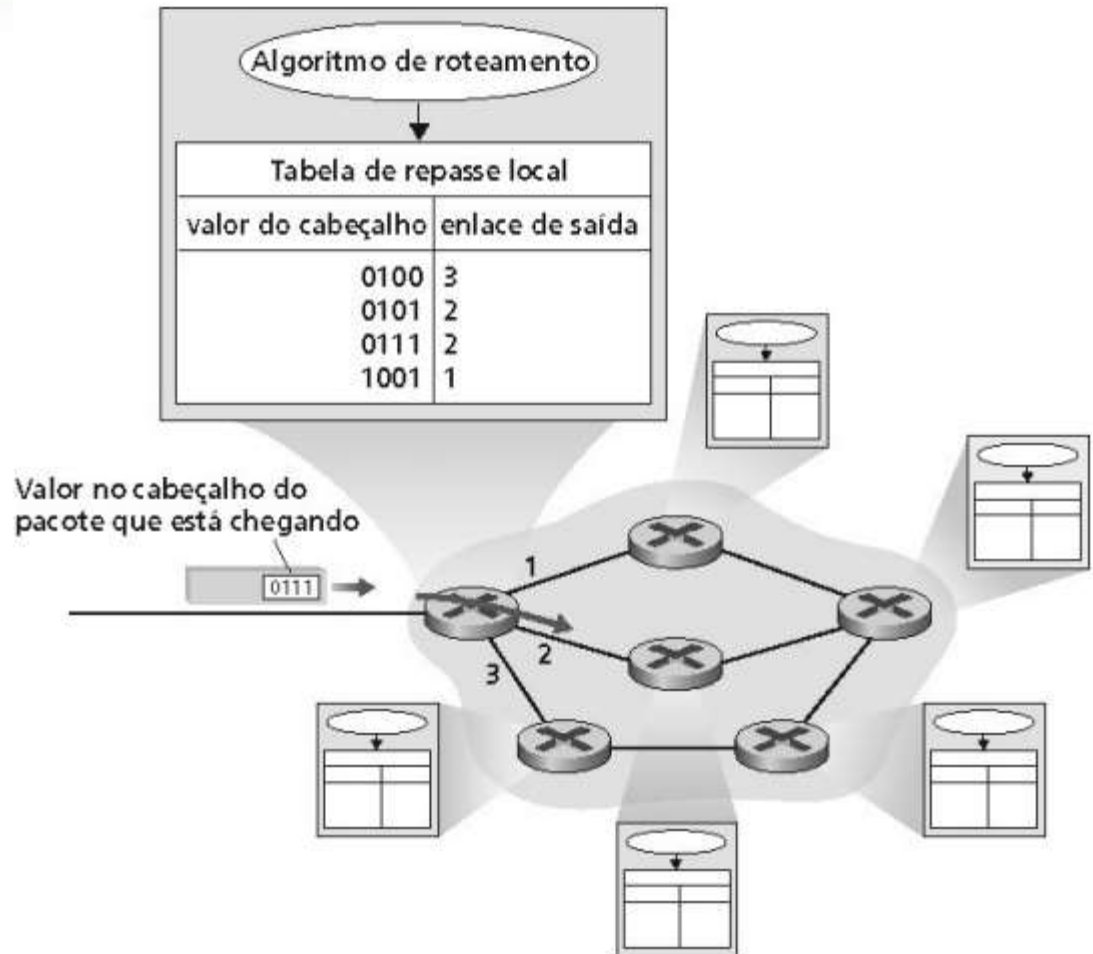


Vídeo

Introdução ao roteamento de pacotes IP

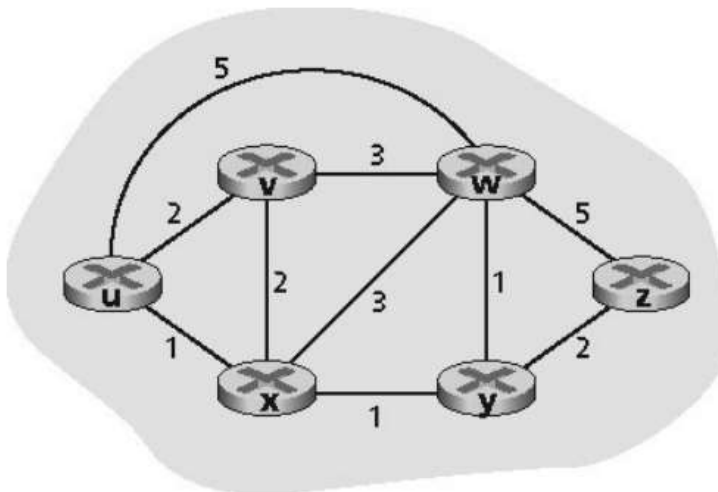
Algoritmos de Roteamento

O algoritmo de roteamento é a parte do software da camada de rede responsável pela decisão sobre a linha de saída a ser usada na transmissão do pacote de entrada.



Algoritmos de Roteamento

- Normalmente um host está ligado diretamente a um roteador, o roteador default;
- Dado um conjunto de roteadores conectados por enlaces, um algoritmo de roteamento descobre um “bom” caminho entre o roteador de origem e o roteador de destino;



Qual seria o caminho de menor custo entre os nós “U” e “Z”?

Algoritmos de Roteamento

As algoritmos de roteamento podem ser agrupados em duas classes principais:

Não Adaptativos ou Roteamento Estático

Não baseiam suas decisões de roteamento em medidas ou estimativas do tráfego e da topologia atuais, mas sim num cálculo off-line, sendo transmitida para os roteadores quando a rede é iniciada.

Algoritmos de Roteamento

Algoritmos Adaptativos ou Roteamento Dinâmico

A tabela de roteamento será preenchida dinamicamente com base em protocolos de encaminhamento. Usa-se essencialmente para redes com mudanças frequentes de topologia ou de grandes dimensões. O preenchimento será então baseado em Métricas que podem variar entre:

- Número de saltos (hops);
- Atraso (delay);
- Custo dos caminhos - valor atribuído arbitrariamente pelo administrador da rede;
- Largura de banda - velocidade de transmissão;
- Congestionamento;
- Confiabilidade;
- Etc.

Rotas Estáticas X Dinâmicas

Rotas Estáticas

Vantagens

Maior segurança, uma vez que existe apenas um caminho de entrada/saída da rede;
Processamento da informação no router mais rápido.

Desvantagens

Sem redundância ou tolerância a falhas – no caso de um link falhar, perde-se a comunicação por completo, já que o router não irá tentar descobrir um caminho alternativo;
Em redes de grandes dimensões torna-se impraticável configurar todas as rotas manualmente.

Rotas Dinâmicas

Vantagens

Garante redundância e tolerância a falhas;
Boa aplicabilidade para redes de grandes dimensões.

Desvantagens

Falta de controle nas rotas escolhidas (tarefa do protocolo de encaminhamento);
Processamento da informação no router mais lento devido aos cálculos impostos pelo protocolo de encaminhamento.

Comando ROUTE

Comando "ROUTE" (Windows)

```
IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
0.0.0.0                    0.0.0.0          10.2.0.1         10.0.0.1         35
10.0.0.0                    255.0.0.0        On-link          10.0.0.1         291
10.0.0.1                    255.255.255.255  On-link          10.0.0.1         291
10.255.255.255              255.255.255.255  On-link          10.0.0.1         291
127.0.0.0                    255.0.0.0        On-link          127.0.0.1        331
127.0.0.1                    255.255.255.255  On-link          127.0.0.1        331
127.255.255.255             255.255.255.255  On-link          127.0.0.1        331
192.168.56.0                 255.255.255.0    On-link          192.168.56.1     281
192.168.56.1                 255.255.255.255  On-link          192.168.56.1     281
192.168.56.255              255.255.255.255  On-link          192.168.56.1     281
224.0.0.0                    240.0.0.0        On-link          127.0.0.1        331
224.0.0.0                    240.0.0.0        On-link          192.168.56.1     281
224.0.0.0                    240.0.0.0        On-link          10.0.0.1         291
255.255.255.255             255.255.255.255  On-link          127.0.0.1        331
255.255.255.255             255.255.255.255  On-link          192.168.56.1     281
255.255.255.255             255.255.255.255  On-link          10.0.0.1         291
=====
Persistent Routes:
None
```

Comando ROUTE

Comando "ROUTE" (Windows)

Examples:

```
> route PRINT
> route PRINT -4
> route PRINT -6
> route PRINT 157*          .... Only prints those matching 157*

> route ADD 157.0.0.0 MASK 255.0.0.0 157.55.80.1 METRIC 3 IF 2
      destination^      ^mask      ^gateway      metric^      ^
                                   Interface^
  If IF is not given, it tries to find the best interface for a given
  gateway.
> route ADD 3ffe::/32 3ffe::1

> route CHANGE 157.0.0.0 MASK 255.0.0.0 157.55.80.5 METRIC 2 IF 2

  CHANGE is used to modify gateway and/or metric only.

> route DELETE 157.0.0.0
> route DELETE 3ffe::/32
```

Algoritmos de Roteamento



Menos utilizados nas redes atuais:

- Roteamento de caminho mais curto
Número de hops, distâncias, etc.
Algoritmo de Dijkstra
- Flooding (Inundação)
Cada pacote de entrada é enviado para cada interface de saída, exceto para aquela em que chegou.

Roteamento por Vetor de Distância

Mais utilizados nas rede atuais:

Roteamento por Vetor de Distância (Distance Vector - DV)

Cada roteador mantém uma tabela (isto é, um vetor) que fornece a melhor distância conhecida até cada destino e determina qual enlace deve ser utilizado para chegar lá. Essas tabelas são atualizadas por meio da troca de informações com os vizinhos. No fim, cada roteador saberá o melhor enlace para alcançar cada destino.

Algoritmo de **Bellman-Ford**. Foi o algoritmo de roteamento original da ARPANET e também foi utilizado na Internet com o nome de **RIP** (*Routing Information Protocol*);

Roteamento de Estado de Enlace

Mais utilizados nas rede atuais:

Roteamento de Estado de Enlace (Link State - LS):

Dividida em 5 partes, onde cada roteador deve fazer o seguinte:

1. Descobrir seus vizinhos e aprender seus endereços de rede;
2. Medir a distância ou o custo até cada um de seus vizinhos;
3. Criar um pacote que informe tudo o que ele acabou de aprender;
4. Enviar esse pacote e receber pacotes de todos os outros roteadores;
5. Calcular o caminho mais curto até cada um dos outros roteadores.

OSPF (*Open Shortest Path First*) é muito utilizado.

Algoritmos de Roteamento

Estado de enlace, vetor de distância e outros algoritmos contam com o processamento em todos os roteadores para calcular as rotas.

Problemas com o hardware ou com o software, até mesmo com um pequeno número de roteadores, podem causar grandes complicações na rede.

Se um roteador alegar ter um enlace que na realidade não tem, ou se esquecer de um enlace que tem, o grafo da rede ficará incorreto.

Algoritmos de Roteamento



Se um roteador deixar de encaminhar pacotes ou danificá-los enquanto os encaminhar, a rota não funcionará como se espera.

Se a memória do roteador se esgotar ou se ele calcular o roteamento incorretamente, as falhas serão inúmeras.

Roteamento Hierárquico

À medida que as redes aumentam de tamanho, as tabelas de roteamento dos roteadores crescem proporcionalmente.

Não apenas a memória do roteador é consumida por tabelas cada vez maiores, mas também é necessário dedicar maior tempo de CPU para percorrê-las e mais largura de banda para enviar relatórios de status sobre elas.

Em determinado momento, a rede pode crescer até o ponto em que deixará de ser viável cada roteador ter uma entrada correspondente a cada outro roteador, de forma que o roteamento terá de ser feito de forma hierárquica.

Roteamento Hierárquico

Nos algoritmos Link State e Distance Vector, consideramos a rede simplesmente como uma coleção de roteadores interconectados, todos rodando o mesmo algoritmo.

Na prática, temos:

Escalabilidade: aumento no número de roteadores, sobrecarga relativa ao cálculo, ao armazenamento e à comunicação da tabela de roteamento.

Autonomia administrativa: empresas desejam controlar seus roteadores como bem entendem.

Roteamento Hierárquico



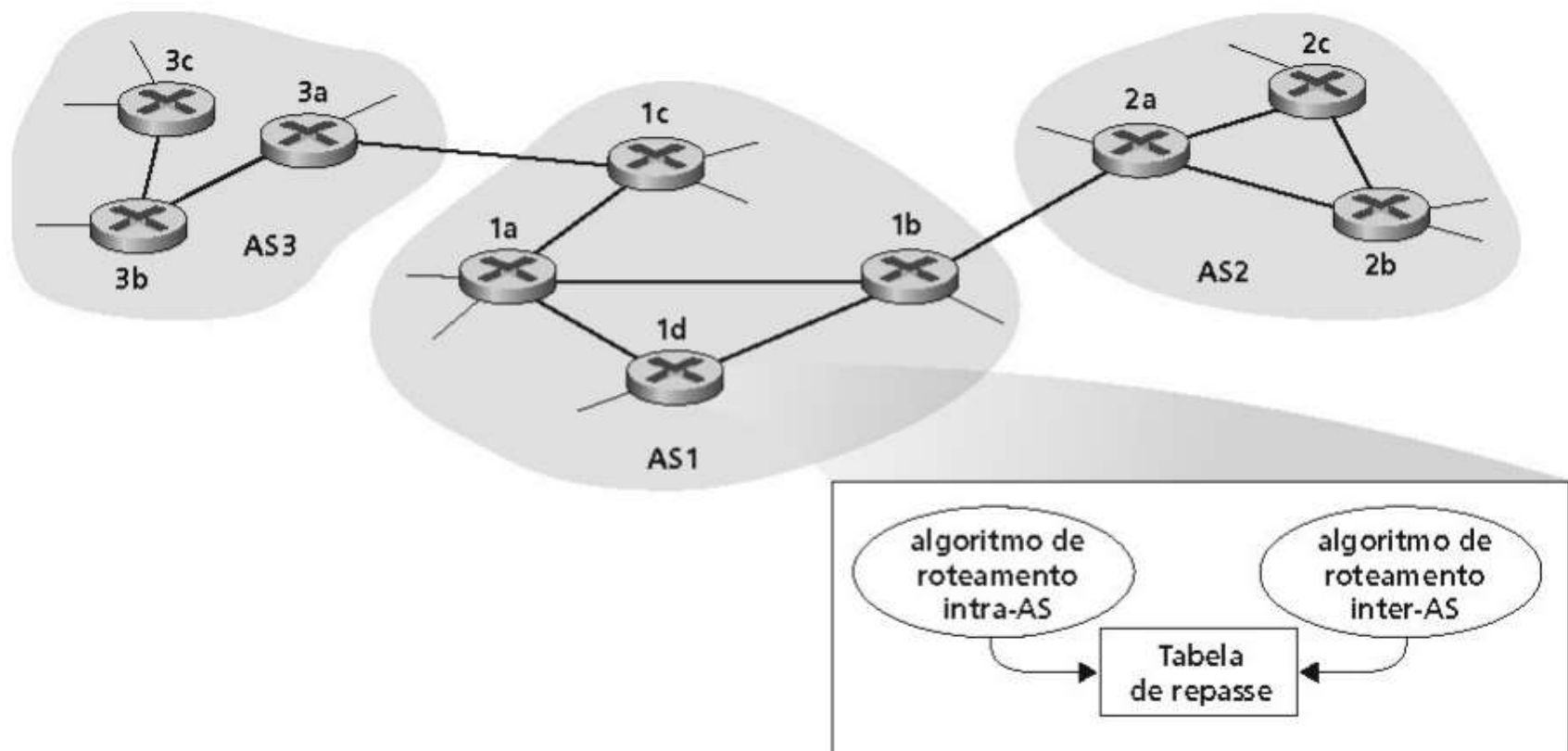
Para resolver essas questões práticas, agrupamos os roteadores em:

Sistemas Autônomos (Autonomous Systems – AS):
roteadores sob o mesmo controle administrativo rodando o mesmo algoritmo de roteamento (roteamento intra-sistema autônomo – Intra-AS);

Roteadores de Borda (Gateway Routers):
roteadores responsáveis em conectar os AS entre si;

Roteamento Hierárquico

Exemplo de sistemas autônomos interligados.



Roteamento na Internet

Protocolos de roteamento Intra-AS também são conhecidos como **Internet Gateway Protocols - IGP**.

Os mais comuns:

RIP: Routing Information Protocol (DV)

OSPF: Open Shortest Path First (LS)

ISIS: Intermediate System to Intermediate System (LS)

IGRP: Interior Gateway Routing Protocol (proprietário da Cisco)

Routing Information Protocol - RIP

O RIP foi um dos primeiros protocolos de roteamento intra-AS da Internet, e seu uso é ainda amplamente disseminado.

A versão 1 do RIP está definida na RFC 1058 e a versão 2, compatível com a versão 1, na RFC 1723.

O RIP é um protocolo de vetor de distâncias (DV).

Routing Information Protocol - RIP

Alguns aspectos da implementação do RIP:

Se não há um aviso depois de 180 segundos, o vizinho e o enlace são declarados mortos;

Então, novos anúncios são enviados aos vizinhos;

Os vizinhos por sua vez devem enviar novos anúncios (se suas tabelas de rotas foram alteradas);

Reversão envenenada (*poison reverse*) é usada para prevenir loops (distância infinita = 16 saltos);

Open Shortest Path First - OSPF

O OSPF foi concebido como sucessor do RIP e como tal tem uma série de características avançadas:

Protocolo de estado de enlace que usa broadcasting;

Algoritmo de caminho de menor custo de Dijkstra;

Os custos dos enlaces são configurados pelo administrador da rede: Custo de enlace em 1 ou pesos inversamente proporcionais à capacidade do enlace (menor tráfego em banda baixa);

Open Shortest Path First - OSPF

A versão mais recente do OSPF, versão 2, está definida no RFC 2178. Nela é especificado que:

Um roteador transmite informações do estado de enlace sempre que houver uma mudança no estado de um enlace;

O roteador transmite o estado do enlace periodicamente (pelo menos a cada 30 minutos), mesmo que o estado não tenha mudado;

O protocolo OSPF verifica se os enlaces estão operacionais (via uma mensagem HELLO).

Roteamento na Internet



Protocolos de roteamento entre diversos AS são conhecidos como **Exterior Gateway Protocols - EGP**.

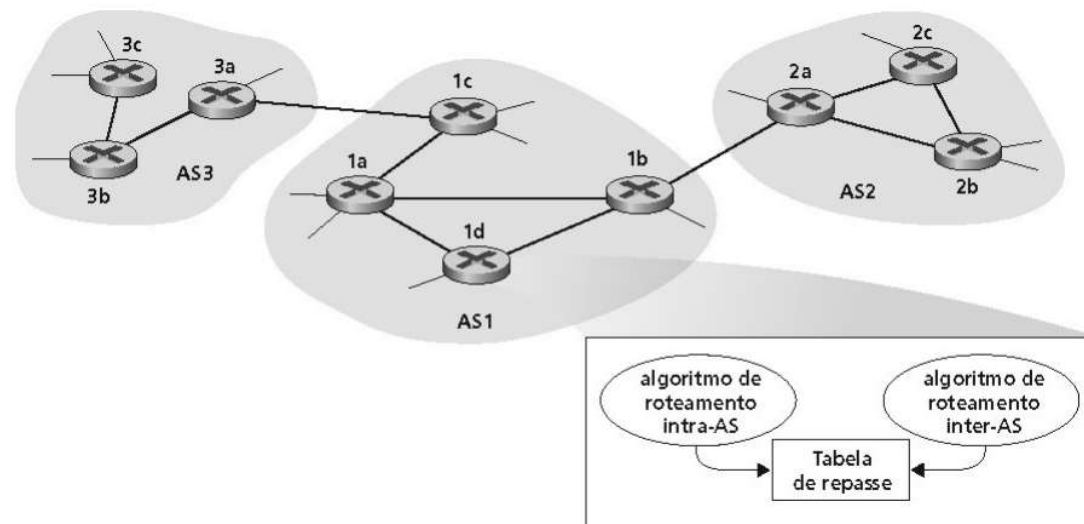
O mais comum:

BGP4: Border Gateway Protocol versão 4

Border Gateway Protocol - BGP

A versão 4 do Protocolo de Roteamento de Borda (BGP), especificada na RFC 1771, é o padrão, de fato, para roteamento entre sistemas autônomos na Internet de hoje.

É extremamente complexo e permite que cada sub-rede anuncie sua existência ao restante da Internet e como chegar até lá.





Vídeo

Como funciona a Internet? O protocolo IP.

Vídeo

Endereçamentos IPs

Host



Em informática, **host** ou hospedeiro, é qualquer máquina ou computador conectado a uma rede, podendo oferecer informações, recursos, serviços e aplicações aos usuários ou outros nós na rede.

É o responsável por implementar a estrutura da camada de rede de endereçamento.

Cada host deve ter um endereço único na rede.

Endereço IP



Número único atribuído a cada computador (host) em uma rede que use o modelo TCP/IP, para distingui-los, independente do sistema operacional ou hardware utilizado.

O endereço IP é definido ou configurado especificamente no protocolo IP do TCP/IP do sistema operacional.

Endereço IPv4

O endereço IPv4 é representado por um número de 32 bits (4 bytes).

Para melhor uso, foi criada uma notação chamada *dot quad* ou ponto quadrante, na qual o número de 32 bits tem quatro grupos de 8 bits separados por ponto. Ex.:

10000000 . 00001010 . 00000010 . 00011110

Com 8 bits podemos ter números de 0 a 255, portanto são 256 possíveis números em cada grupo (0 a 255).

Cada grupo é chamado de octeto (oito bits).

Temos portanto $2^{32} = 4.294.967.296$ (quatro bilhões de endereços).

Endereço IPv4

Abaixo temos a representação de um endereço IP com números no formato binário e seu correspondente no formato decimal:

10000000 . 00001010 . 00000010 . 00011110

ou

128 . 10 . 2 . 30

ou

128.10.2.30

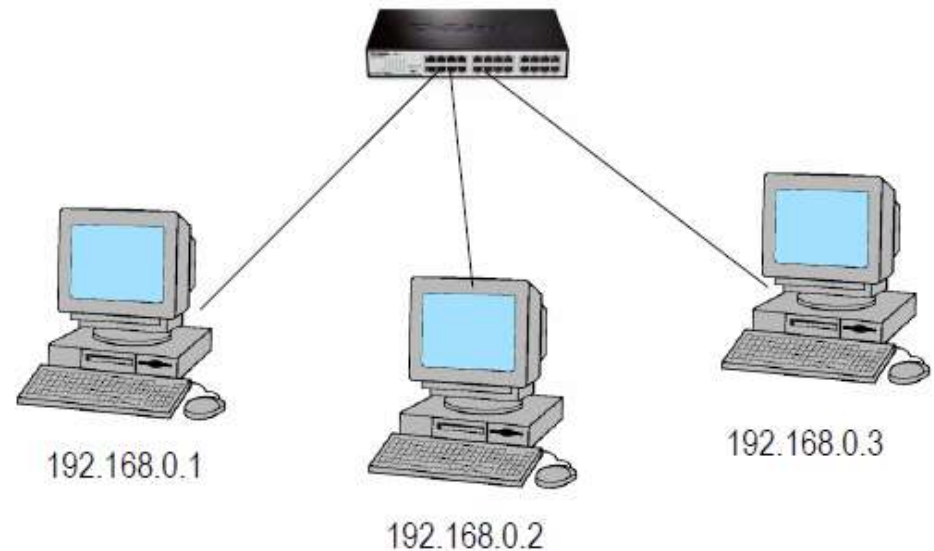
Endereço IPv4

Observe que no exemplo a seguir podemos identificar duas partes nos endereços dos computadores:

Uma parte igual (3 octetos), que representa a rede.

Uma parte variável, que identifica o computador na rede (host).

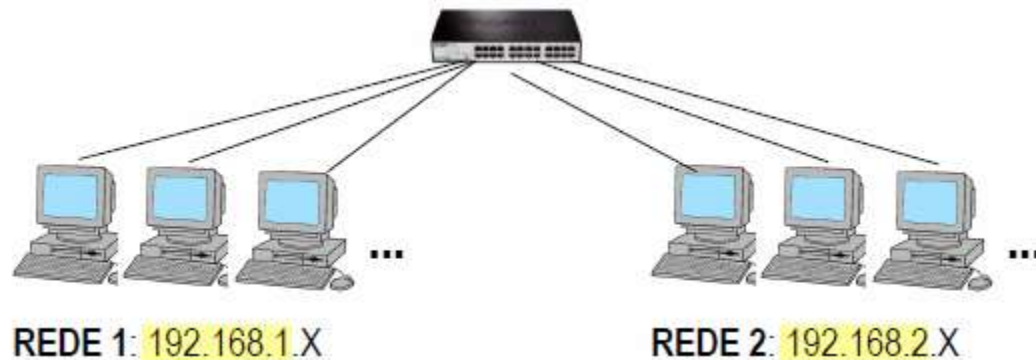
Endereço IP de 32 bits			
Identificador da rede			Ident. do host
192	168	0	1
192	168	0	2
192	168	0	3



Endereço IPv4

Só é possível a comunicação (sem um roteador) entre computadores que estão na mesma rede (mesmo identificador da rede).

A quantidade de octetos que identificam a rede e o host depende da máscara de sub-rede.



Endereço IPv4

Endereços IP privados ou internos são visíveis apenas dentro da rede local onde estão configurados.

Endereços públicos ou externos são visíveis na internet.

Ex: se digitar “http://200.147.67.142” no navegador de Internet, chegará ao site do UOL, indicando que é um endereço visível na Internet, em qualquer parte do mundo.

Unicast, Multicast e Broadcast



São formas de comunicação em uma rede de dados, no que diz respeito à qual(is) hosts ou endereço serão entregue os dados enviados.

Unicast

No **Unicast** os dados são enviados de um host e endereçado a um destino específico.

Há apenas um remetente e um receptor.

É a forma predominante de transmissão em redes locais e na Internet.

Exemplos de protocolos que usam transmissões Unicast:
HTTP, SMTP, FTP e Telnet.

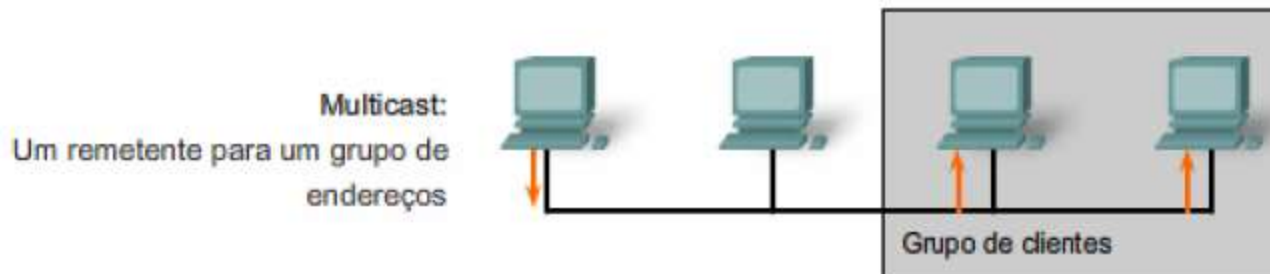


Multicast

No **Multicast** os dados são enviados para um grupo específico de dispositivos ou clientes.

Os clientes da transmissão Multicast devem ser membros de um grupo Multicast lógico para receber as informações.

Um exemplo de transmissão Multicast é a transmissão de vídeo e de voz associada a uma reunião de negócios colaborativa, com base em rede.



Broadcast

No **Broadcast** os dados são enviados de um endereço para todos os outros endereços.

Apenas um remetente enviando para todos hosts da rede.

É essencial para o envio da mesma mensagem para todos os dispositivos na rede local.

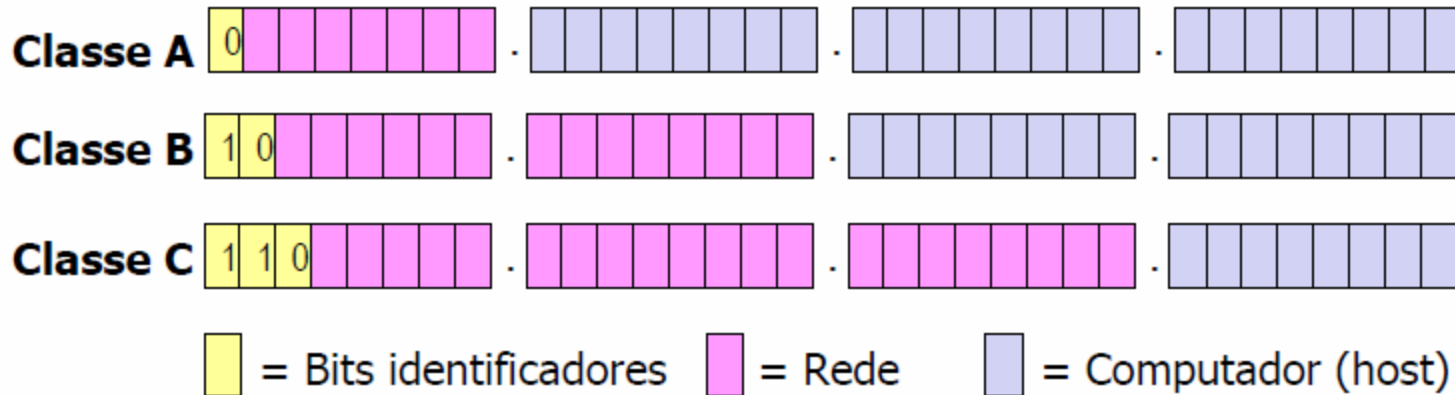
Exemplo: consulta de resolução de endereço que o protocolo ARP envia para todos os computadores em uma rede local.



Classes de Endereçamento

No protocolo IP (IPv4) foram estabelecidas cinco classes de endereços:
A, B, C, D e E

As classes **A, B e C** são usadas p/ endereçamento, com uma parte identificando a rede e outra o host:



As classes **D e E** são para endereços especiais.

Redes Classe A

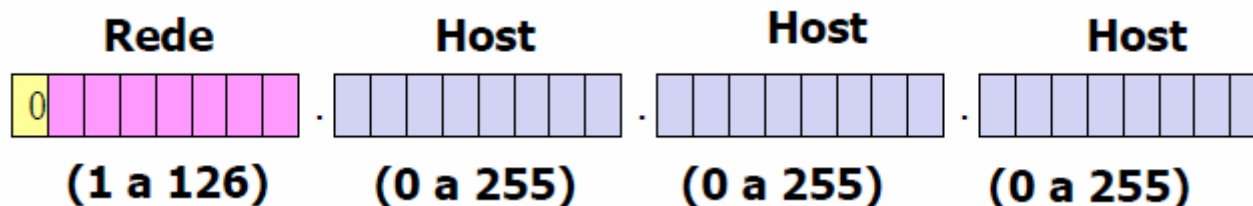
O primeiro octeto identifica a rede, os outros, o host.

O primeiro octeto tem o primeiro bit fixado em zero e seu valor varia de 1 a 126.

Os três outros octetos não podem ser todos 0 (zero) nem todos 255.

Capacidade: 126 redes com até 16.777.214 hosts cada.

Exemplos: 70.35.22.14, 110.25.8.4.



Redes Classe B

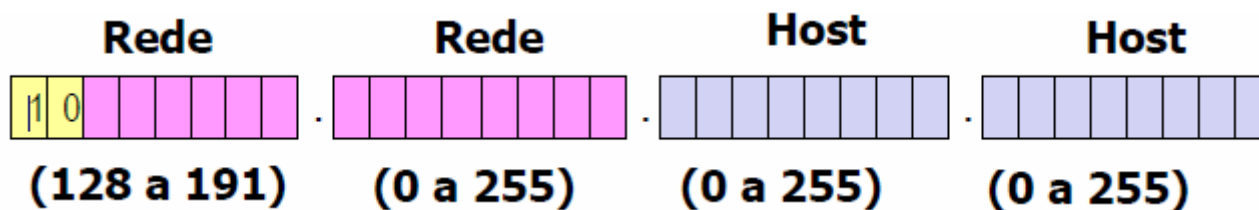
Os dois primeiros octetos identificam a rede, os outros, o host.

O primeiro octeto tem os dois primeiros bits fixados em 10 e seu valor varia de 128 a 191.

Os dois últimos octetos (do host) não podem ser todos 0 (zero) nem todos 255.

Capacidade: 16.384 redes com até 65.536 hosts cada.

Exemplos: 190.15.14.17 130.25.8.4.



Redes Classe C

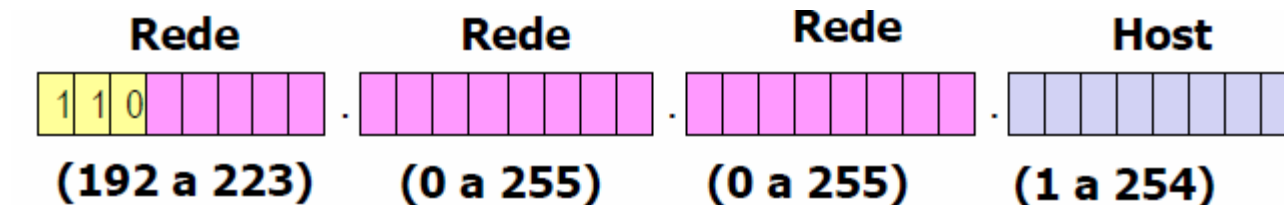
Os três primeiros octetos identificam a rede, o último, o host.

O primeiro octeto tem os três primeiros bits fixados em 110 e seu valor varia de 192 a 223.

Os dois outros octetos não podem ser todos 0 (zero) nem todos 255.

Capacidade: 2.097.152 redes com 256 hosts cada

Exemplos: 200.15.14.17 192.168.0.1.



Redes Classe D

Classe de endereços reservada para criar agrupamentos de computadores para uso em transmissões multicast.

O primeiro octeto tem os quatro primeiros bits fixados em 1110 e seu valor varia de 224 e 239.

Os bits restantes compõem o endereço de multicast.

Os três outros octetos não podem ser todos 0 (zero) nem todos 255.

Redes Classe E

Classe de endereços reservados, que não podem ser usados para equipamentos (hosts) na rede. É para uso futuro e atualmente reservada a testes pela IETF (*Internet Engineering Task Force*).

Variam de 240.0.0.0 a 255.0.0.0

O primeiro octeto tem os quatro primeiros bits fixados em 1111 e seu valor varia de 240 e 255.

Os três outros octetos não podem ser todos 0 (zero) nem todos 255.

Controle de distribuição de endereços

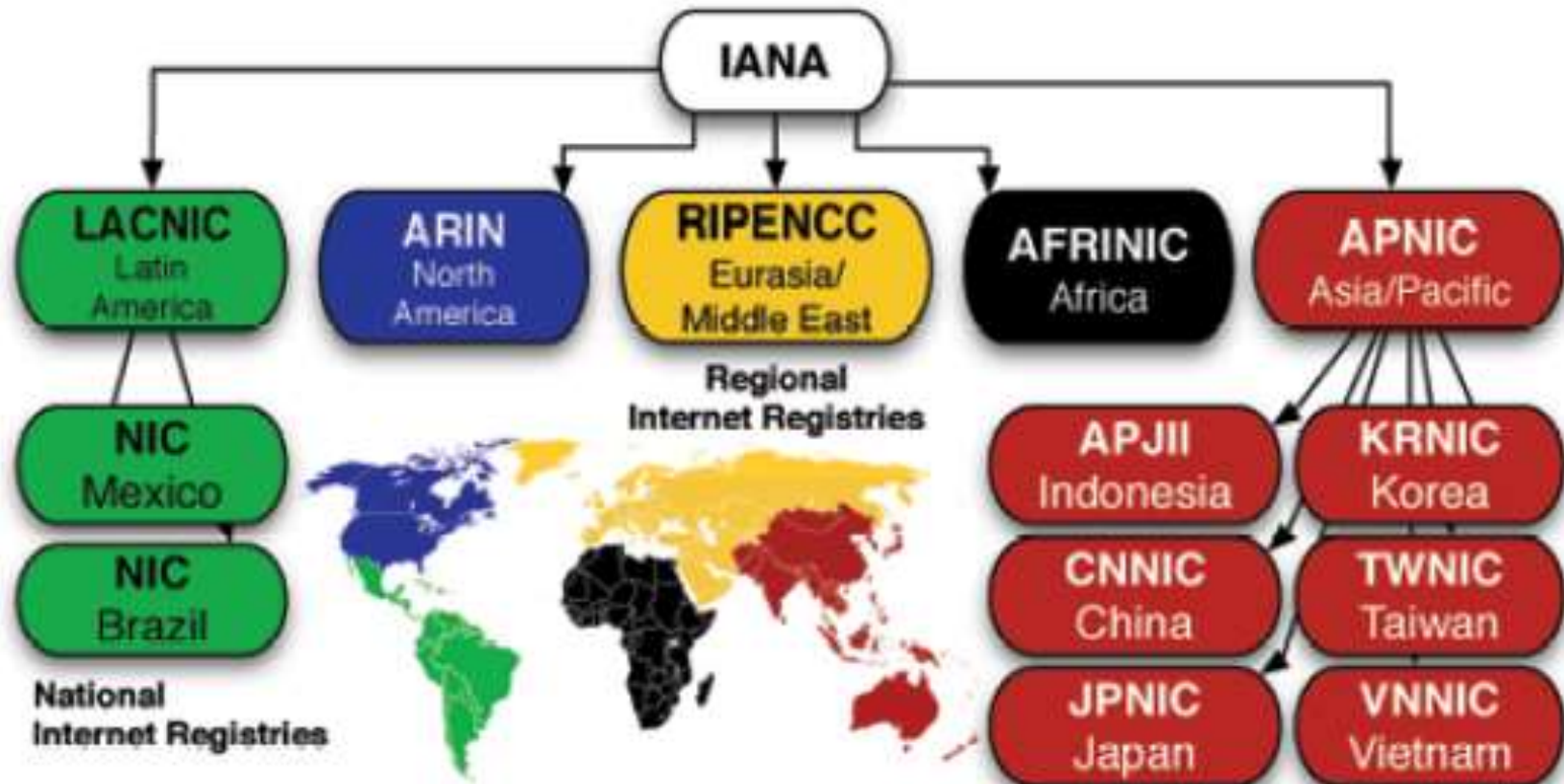
O controle e distribuição de endereços IP é feito pelo **IANA** (*Internet Assigned Numbers Authority*), que:

- Regulamenta o uso da internet em todo o mundo;
- Distribui IP's por países;
- Reserva faixas de IP a pedido de empresas.

Nenhum endereço está mais disponível. Todos já foram distribuídos a empresas usuárias da Internet.

No Brasil, quem recebe os blocos do IANA e distribui internamente é o **NIC.br**, e está subordinado ao Registro de Endereçamento da Internet para a América Latina e o Caribe (LACNIC).

Controle de distribuição de endereços





Controle de distribuição de endereços

Exemplos de redes classe A reservadas por empresas:

Rede	Empresa proprietária	Faixas de IP
3	General Eletric	3.0.0.0 a 3.255.255.255
12	AT & T	12.0.0.0 - 12.255.255.255
15	Hewlett-Packard	15.0.0.0 - 15.255.255.255
19	Ford	19.0.0.0 - 19.255.255.255
54	Marck	54.0.0.0 - 54.255.255.255
55	Boeing	55.0.0.0 - 55.255.255.255
56	U.S. Postal Service	56.0.0.0 - 56.255.255.255

Resumo das Classes

Classe A	1 a 126	.	0 a 255	.	0 a 255	.	0 a 255
Classe B	128 a 191	.	0 a 255	.	0 a 255	.	0 a 255
Classe C	192 a 223	.	0 a 255	.	0 a 255	.	1 a 255

 = Rede  = Computador (host)

Endereços reservados internos

Em cada uma das classes estudadas (A, B e C) o IANA definiu endereços internos e externos.

Endereços da faixa interna (RFC 1918):

- Podem ser usados sem pedir permissão para a IANA
- São ignorados por roteadores ao tratarem pacotes que tenham um desses endereços como origem ou destino (são endereços não roteáveis)

Classe do Endereço	Endereços	N.º de Redes	N.º de Hosts
A	1.0.0.0 – 126.0.0.0	126	16 777 214
B	128.1.0.0 – 191.255.0.0	16 384	65 534
C	192.0.1.0 – 223.255.255.0	2 097 151	254
D	224.0.0.0 – 239.255.255.255	—	—
E	240.0.0.0 – 247.255.255.255	—	—

Endereços reservados

São endereços usados para se referir à própria rede (não podem ser usados para um host específico).

Tipos mais comuns de endereços reservados:

- Loopback address
- Microsoft APIPA
- Rota padrão
- Endereço de broadcast

Loopback

Endereços reservados para receber informações de retorno dos servidores.

O primeiro byte é o valor 127 e qualquer mensagem de dados enviada para 127.X.X.X retornará para o emitente.

A resposta é dada pelo próprio emitente.

Útil para efetuar testes e otimizar a comunicação entre processos no mesmo computador.

Se a resposta não retornar, indica um possível problema de software ou de hardware.

Microsoft APIPA - Automatic Private IP Addressing

Endereço: 169.254.0.0

Em computadores que são configurados para obter um IP dinâmico, o APIPA aparece quando nenhum DHCP está disponível na rede.

O APIPA interroga automaticamente os outros computadores de forma a garantir que não há uma duplicação de IPs e então assigna ao computador um IP único no 169.254.x.y com a subnet mask de 255.255.0.0.

Rota Padrão – Default Gateway

Endereço: 0.0.0.0

Se um destino for requisitado e não estiver presente na rede local (ex: seu IP é de outra rede), a rota padrão será usada pelo roteador para tentar localizar o destino.




Broadcast

Endereço: 255.255.255.255

É reservado para enviar pacotes em broadcast (para todos os computadores da rede).

Endereços reservados

Blocos de Endereços Reservados

CIDR Bloco de Endereços	Descrição	Referência
0.0.0.0/8	Rede corrente (só funciona como endereço de origem)	RFC 1700 
10.0.0.0/8	Rede Privada	RFC 1918 
14.0.0.0/8	Rede Pública	RFC 1700 
39.0.0.0/8	Reservado	RFC 1797 
127.0.0.0/8	Localhost	RFC 3330 
128.0.0.0/16	Reservado (IANA)	RFC 3330 
169.254.0.0/16	Zeroconf	RFC 3927 
172.16.0.0/12	Rede privada	RFC 1918 
191.255.0.0/16	Reservado (IANA)	RFC 3330 
192.0.2.0/24	Documentação	RFC 3330 
192.88.99.0/24	IPv6 para IPv4	RFC 3068 
192.168.0.0/16	Rede Privada	RFC 1918 
198.18.0.0/15	Teste de benchmark de redes	RFC 2544 
223.255.255.0/24	Reservado	RFC 3330 
224.0.0.0/4	Multicasts (antiga rede Classe D)	RFC 3171 
240.0.0.0/4	Reservado (antiga rede Classe E)	RFC 1700 
255.255.255.255	Broadcast	

Máscara de sub-rede (subnet mask)

Conjunto de quatro números similares ao IP que servem para indicar em uma rede qual é a parte fixa e qual é a parte variável dos endereços IP dessa rede.

É um parâmetro necessário ao configurar uma rede TCP/IP, seja qual for o sistema operacional.

Usa 0 ou 255 nos octetos.

- 0 (zeros) indicam a parte variável dentro da rede
- O valor 255 indica a parte fixa

Classe	Máscara usada
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Máscara de sub-rede (subnet mask)

A máscara de sub-rede padrão acompanha a classe de rede, conforme tabela anterior.

Exemplos:

Endereço IP	Classe	Rede	Host	Máscara de sub-rede padrão
98.158.201.128	A	98.	158.201.128	255.0.0.0
158.208.189.45	B	158.208.	189.45	255.255.0.0
208.183.34.89	C	208.183.34	89	255.255.255.0

Máscara de sub-rede (subnet mask)

A máscara possui uma faixa de 32 bits contendo bits 1 para a ID da rede e da sub-rede, e bits 0 para a ID do host.

Formas de se representar as máscaras:

Classe A - 255.0.0.0 ou 11111111.00000000.00000000.00000000 ou /8
(notação CIDR - *Classless Inter-Domain Routing*)

Classe B - 255.255.0.0 ou 11111111.11111111.00000000.00000000 ou /16
(CIDR)

Classe C - 255.255.255.0 ou 11111111.11111111.11111111.00000000 ou /24 (CIDR)

Máscara de sub-rede (subnet mask)

Tabela 1. Subdivisões de uma identificação de rede classe A.

Número de sub-redes	Número de bits para sub-rede	Máscara de sub-rede	Número de hosts por sub-rede
1-2	1	255.128.0.0 ou /9	8,388,606
3-4	2	255.192.0.0 ou /10	4,194,302
5-8	3	255.224.0.0 ou /11	2,097,150
9-16	4	255.240.0.0 ou /12	1,048,574
17-32	5	255.248.0.0 ou /13	524,286
33-64	6	255.252.0.0 ou /14	262,142
65-128	7	255.254.0.0 ou /15	131,070
129-256	8	255.255.0.0 ou /16	65,534
257-512	9	255.255.128.0 ou /17	32,766
513-1,024	10	255.255.192.0 ou /18	16,382
1,025-2,048	11	255.255.224.0 ou /19	8,190
2,049-4,096	12	255.255.240.0 ou /20	4,094
4,097-8,192	13	255.255.248.0 ou /21	2,046
8,193-16,384	14	255.255.252.0 ou /22	1,022
16,385-32,768	15	255.255.254.0 ou /23	510
32,769-65,536	16	255.255.255.0 ou /24	254
65,537-131,072	17	255.255.255.128 ou /25	126
131,073-262,144	18	255.255.255.192 ou /26	62
262,145-524,288	19	255.255.255.224 ou /27	30
524,289-1,048,576	20	255.255.255.240 ou /28	14
1,048,577-2,097,152	21	255.255.255.248 ou /29	6
2,097,153-4,194,304	22	255.255.255.252 ou /30	2

Máscara de sub-rede (subnet mask)

Tabela 2. Subdivisões de uma identificação de rede classe B.

Número de sub-redes	Número de bits para sub-rede	Máscara de sub-rede	Número de hosts por sub-rede
1-2	1	255.255.128.0 ou /17	132,766
3-4	2	255.255.192.0 ou /18	16,382
5-8	3	255.255.224.0 ou /19	8,190
9-16	4	255.255.240.0 ou /20	4,094
17-32	5	255.255.248.0 ou /21	2,046
33-64	6	255.255.252.0 ou /22	1,022
65-128	7	255.255.254.0 ou /23	510
129-256	8	255.255.255.0 ou /24	254
257-512	9	255.255.255.128 ou /25	126
513-1,024	10	255.255.255.192 ou /26	62
1,025-2,048	11	255.255.255.224 ou /27	30
2,049-4,096	12	255.255.255.240 ou /28	14
4,097-8,192	13	255.255.255.248 ou /29	6
8,193-16,384	14	255.255.255.252 ou /30	2

Máscara de sub-rede (subnet mask)

Tabela 3. Subdivisões de uma identificação de rede classe C.

Número de sub-redes	Número de bits para sub-rede	Máscara de sub-rede	Número de hosts por sub-rede
1-2	1	255.255.255.128 ou /25	126
3-4	2	255.255.255.192 ou /26	62
5-8	3	255.255.255.224 ou /27	30
9-16	4	255.255.255.240 ou /28	14
17-32	5	255.255.255.248 ou /29	6
33-64	6	255.255.255.252 ou /30	2

Máscara de sub-rede (subnet mask)

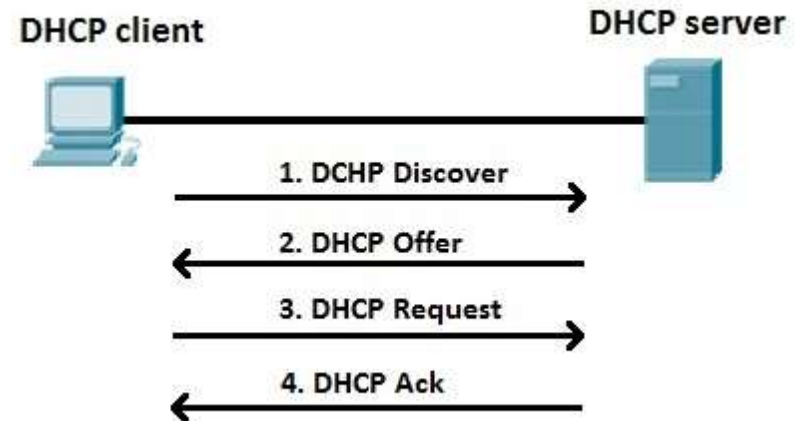
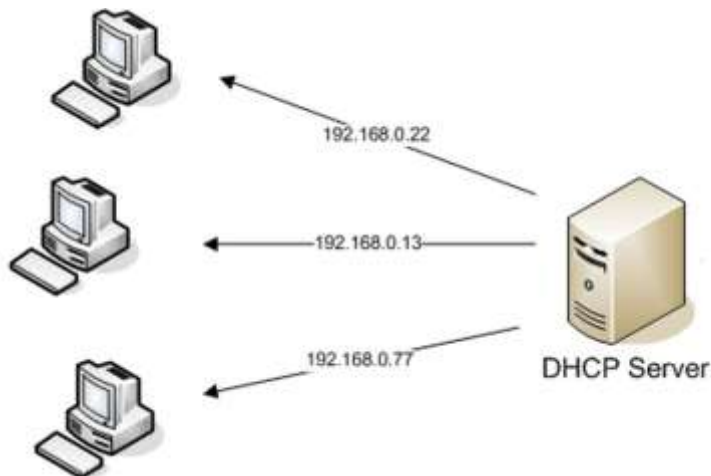
Exercício:

Tenho uma rede Classe C – 192.168.1.0 e preciso montar 8 redes diferentes para as filiais da empresa, sendo que em nenhuma delas terão mais que 20 equipamentos.

Qual a máscara de sub-rede deve ser utilizada para melhor dividir essa rede Classe C?

DHCP – Dynamic Host Configuration Protocol

O DHCP, Dynamic Host Configuration Protocol (Protocolo de configuração dinâmica de host - RFC 2131), é um protocolo de serviço TCP/IP que oferece configuração dinâmica de hosts, com concessão de endereços IP, Máscara de sub-rede, Default Gateway (Gateway Padrão), Número IP de um ou mais servidores DNS, Número IP de um ou mais servidores WINS e Sufixos de pesquisa do DNS. Este protocolo é o sucessor do BOOTP e se tornou padrão em 1993.

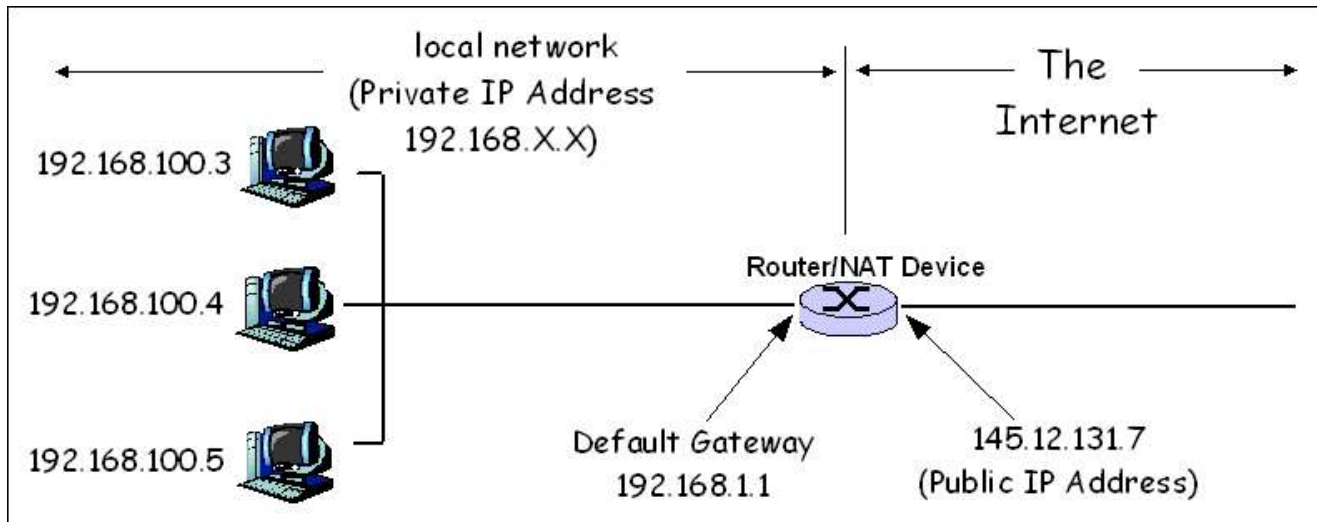


NAT - Network Address Translation

O protocolo NAT surgiu para dar sobrevida ao IPv4.

Com ele foi possível que redes privadas utilizassem IP's de gama privada (ex.: 10.0.0.12) e mesmo assim pudessem acessar uma rede pública (Internet) sem a necessidade de um IP público por computador.

Um único IP público pode ser compartilhado por centenas de equipamentos com IPs privados.



Vídeo

O que é IPv6

IPv6

O endereço IPv6 é representado por um número hexadecimal (0 a 9 e A até F) de 128 bits.

Para melhor uso, foi criada uma notação chamada *hexadecateto*, na qual o número de 128 bits tem oito grupos de 16 bits separados por dois pontos. Ex.:

```
2001:1234:abcd:0000:0000:1111:0db8:0001
```

Pode-se omitir “zeros” à esquerda de cada hexadecateto, reduzindo para:

```
2001:1234:abcd:0:0:1111:db8:1
```

Pode-se substituir sequencias de “zeros” por “::”, mas apenas uma única vez no endereço:

```
2001:1234:abcd::1111:db8:1
```

IPv6

Não diferencia maiúsculas e minúsculas.

Na prática tem 64 bits (outros 64 bits são para implementações futuras).

Temos portanto $2^{128} = 340.282.366.920.938.463.463.374.607.431.768.211.456$

340 undecilhões de endereços, o que representa mais de 48×10^{18} (quarenta e oito quintilhões) de endereços para cada indivíduo do planeta.

Não tem mais Broadcast (pode usar o primeiro e o último endereço) - usa Multicast.

Endereço automático no Linux: segunda parte 32 bits é o MAC address.

Endereço automático no Windows: é aleatório.

Não tem mais o protocolo ARP. No IPv6 está no protocolo ICMP.

Endereços Unicast

Endereços **Unicast**

Os endereços unicast são utilizados para comunicação entre dois nós, por exemplo, telefones VoIPv6, computadores em uma rede privada, etc.

Existem alguns tipos de endereços unicast IPv6:

Global Unicast

Unique-Local

Link-Local

Existem também alguns tipos para usos especiais, como endereços IPv4 mapeados em IPv6, endereço de loopback e o endereço não-especificado, entre outros.

Global Unicast

Global Unicast - equivalente aos endereços públicos IPv4, o endereço global unicast é globalmente roteável e acessível na Internet IPv6

Sua estrutura foi projetada para utilizar os 64 bits mais a esquerda para identificação da rede e os 64 bits mais a direita para identificação da interface.

Portanto, exceto casos específicos, todas as sub-redes em IPv6 tem o mesmo tamanho de prefixo, 64 bits (/64), o que possibilita:

$2^{64} = 18.446.744.073.709.551.616$ dispositivos por sub-rede.

Atualmente, está reservada para atribuição de endereços a faixa:

2000::/3, que corresponde aos endereços de:

2000:: a 3fff:ffff:ffff:ffff:ffff:ffff:ffff:ffff.

Isto representa 13% do total de endereços possíveis com IPv6.

Link Local

Link Local:

Podendo ser usado apenas no enlace específico onde a interface está conectada, o endereço link local é atribuído automaticamente utilizando o prefixo FE80::/64.

Os 64 bits reservados para a identificação da interface são configurados utilizando o formato IEEE EUI-64. Vale ressaltar que os roteadores não devem encaminhar para outros enlaces, pacotes que possuam como origem ou destino um endereço link-local.

Loopback

Endereço Loopback:

Representado pelo endereço unicast `0:0:0:0:0:0:0:1` ou `::1` (equivalente ao endereço IPv4 loopback `127.0.0.1`).

Este endereço é utilizado para referenciar a própria máquina, sendo muito utilizado para teste internos.

IPv6

Quais os riscos da não implantação do IPv6?

- Embora ainda seja pequena, a utilização do IPv6 tem aumentado gradativamente;
- A não implementação do IPv6 irá:
 - Dificultar o surgimento de novas redes;
 - Diminuir o processo de inclusão digital o reduzindo o número de novos usuários;
 - Dificultar o surgimento de novas aplicações;
 - Dificultar o crescimento da IoT (Internet das Coisas);
 - Aumentar a utilização de técnicas como a NAT.
- O custo de não implementar o IPv6 poderá ser maior que o custo de implementá-lo;
- Provedores Internet precisam inovar e oferecer novos serviços a seus clientes.

Bibliografia

TANENBAUM, A. S. Redes de Computadores.
<http://www.nic.br>

Final da aula

Dúvidas?

Contatos:

<http://about.me/vlbarreira>

Cópia da apresentação:

<http://bit.ly/unipcc18>