

Resumo Redes Prova III

Calculando IPs, máscaras e subredes.

Em quatro blocos: 4x 64 ips

Máscara: 255.255.255.192

Endereço de subrede: 192.168.0.0

192.168.0.64

192.168.0.128

192.168.0.192

Endereço do primeiro host: 192.168.0.1

192.168.0.65

192.168.0.129

192.168.0.193

Endereço do último host: 192.168.0.62

192.168.0.126

192.168.0.190

192.168.0.254

Endereço de broadcast: 192.168.0.63

192.168.0.127

192.168.0.191

192.168.0.255

no enunciado nós temos um bloco de ips assim:

192.168.0.0 com uma mascara /24 (255.255.255.0).

isso quer dizer que, com essa mascara, essa rede tem 256 ips! como tu sabe disso? a mascara eh assim por causa dos bits "ativos" dela. um ipv4 tem 8 bits pra cada numero. 8bits.8bits.8bits.8bits, se tds os 8 bits do octeto forem 1, esse octeto vale 255! (ver conversao binaria, bem simples).

um bit ativo na mascara quer dizer q aquele bit nao muda na rede. assim, uma mascara /24 (tem os primeiros octetos totalmente ativos e o ultimo nulo) diz q a rede tem 192.168.0 como partes FIXAS e o .0 final VARIA TOTALMENTE. todos os 8 bits podem ser 1 ou 0, entao podem ser qualquer numero de 0 a 255.

quando vc cria subredes, vc ta aumentando o numero de bits fixos. (bota diminuir tmb e criar redes maiores, mas n eh o caso da atividade).

com isso o ultimo octeto da mascara deixa de ser 00000000 e passa a começar com 1.

a quantidade de 1s depende do tamanho da rede q vc quer.

com 8 bits negativos, nos temos 256 ips pq 2 elevado a 8 é 256

se 7 bits foram negativos, temos 2 elevado a 7, entao 128 ips na rede q tem mascara /25.

pra 6 bits negativos, msm coisa e ficamos com 64.

nessa atividade ele pediu pra dividir o bloco em 2 e 4 subredes, entao eu assumi q fossem igualmente e fiz 2 de 128 e 4 de 64.

primeira pergunta, como definimos a mascara?

com a explicacao anterior, fica bem obvio. pra cada octeto vc monta o numero referente

$10000000 = 128$

$11000000 = 128+64 = 192$

entao:

mascara de rede com 128 ips:

255.255.255.128

mascara de rede cm 64 ipa:

255.255.255.192

segunda pergunta, o endereço da rede. o endereço q se refere a rede SEMPRE eh o primeiro. esse endereço nem eh considera um endereço "valido", pois nunca eh usado por uma maquina.

na primeira subrede fica obvio, o endereço eh 192.168.0.0. na segunda, dependendo na tamanho da sua rede/mascara, eh o proximo q fica FORA da rede. no caso de 128, a primeira subrede tem 128 ips do 0 ao 127, entao 192.168.0.128 eh o primeiro endereço da segunda subrede. vendo as respostas na atividade vc consegue entender isso facilmente.

pulando pra ultima pergunta, endereço de broadcast. ele eh a msm coisa q o endereço de rede, n eh considerado um endereço valido. em serve pra ser enviado um pacote para TODOS os ips da rede, e em SEMPRE o ultimo possivel na rede. no exemplo anterior q a subrede tinha 128 ips de 0 a 127, o endereço de broadcast era o 192.168.0.127. alias, o endereço de broadcast SEMPRE eh um numero impar.

assim, endereço de primeiro e último host fica meio obvio. sao o primeiro e ultimo endereço valido, ou seja, endereço q n eh o da rede ou o de broadcast. ve na atividade.

<https://www.freecodecamp.org/portuguese/news/ficha-informativa-de-sub-redes-mas-cara-de-sub-rede-24-30-26-27-29/>

Capítulo 4 - Camada de Rede, plano de dados

Serviços e protocolos da camada de rede:

Transporta segmento do hospedeiro emissor ao receptor

- emissor: encapsula segmentos em datagramas, passa para a camada de enlace
- receptor: entrega segmentos para protocolo da camada de transporte

Protocolos de camada de rede em todos os dispositivo de Internet: hospedeiros e roteadores

- Roteadores:
 - examinam campos de cabeçalho em todos os datagramas IP que passam por eles

- move datagramas de portas de entrada para portas de saída para transferi-los ao longo do caminho final

Duas funções-chave da camada de rede:

- Encaminhamento: move pacotes do enlace de entrada de um roteador para o enlace de saída apropriado (processo de passar por um único cruzamento)
- Roteamento: determina rota tomada por pacotes da origem para o destino (processo de planejar a viagem da origem ao destino)



Plano de dados e plano de controle:

Plano de dados:

- função local, por roteador
- determina como o datagrama que chega em uma porta de entrada do roteador é encaminhado para uma porta de saída

Plano de controle:

- lógica em toda a rede
- determina como o datagrama é roteado entre roteadores ao longo do caminho fim-a-fim do hospedeiro de origem ao de destino.
- duas abordagens de plano de controle:
 - (I) algoritmos de roteamento tradicionais implementados em roteadores
 - (II) SDN – rede definida por software implementada em servidores (remotos)

(I) Plano de controle por roteador = Componentes individuais do algoritmo de roteamento em todo e cada roteador interagem no plano de controle

(II) Plano de controle de SDN = Controlador remoto computa e instala tabelas de encaminhamento nos roteadores

Funções da porta de entrada:

Comutação descentralizada:

- usando valores de campo de cabeçalho, procurar porta de saída usando tabela de encaminhamento na memória da porta de entrada (“correspondência mais ação”)
- objetivo: processamento completo da porta de entrada na ‘velocidade da linha’
- enfileiramento na porta de entrada: ocorre se os datagramas chegarem mais rápido do que a taxa de encaminhamento para a estrutura de comutação
- encaminhamento baseado em destino: encaminha com base apenas no endereço IP de destino (tradicional)
- encaminhamento generalizado: encaminha com base em qualquer conjunto de valores de campo de cabeçalho

Correspondência com prefixo mais longo: ao procurar a entrada da tabela de encaminhamento para determinado endereço de destino, use o prefixo de endereço mais longo que corresponde ao endereço de destino.

Faixa de Endereços de Destino	Interface do enlace
11001000 00010111 00010*** *****	0
11001000 00010111 00011000 *****	1
11001000 00010111 00011*** *****	2
caso contrário	3

11001000 00010111 00010110 10100001 qual interface? 0

11001000 00010111 00011000 10101010 qual interface? 1

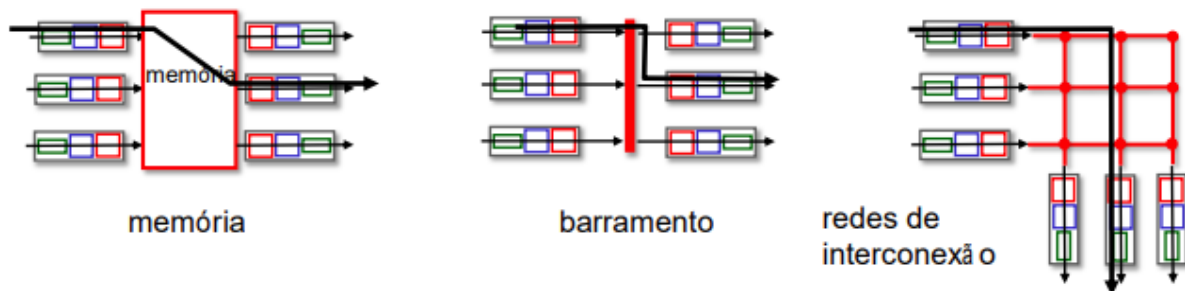
Estruturas de comutação:

Transferem pacotes do enlace de entrada para o enlace de saída apropriado

Taxa de comutação: taxa em que pacotes podem ser transferidos de entradas para saídas

- frequentemente medida como múltiplos da taxa de linha de entrada/saída
- N entradas: taxa de comutação de N vezes a taxa de linha é desejável

Três principais tipos de estruturas de comutação:



Fila da porta de entrada:

- Se a estrutura de comutação for mais lenta do que as portas de entrada combinadas
 - Atraso na fila e perda devido ao estouro do buffer!
- Bloqueio de cabeça de linha (Head-of-the-Line - HOL): datagrama na primeira posição da fila impede que outros na fila avancem

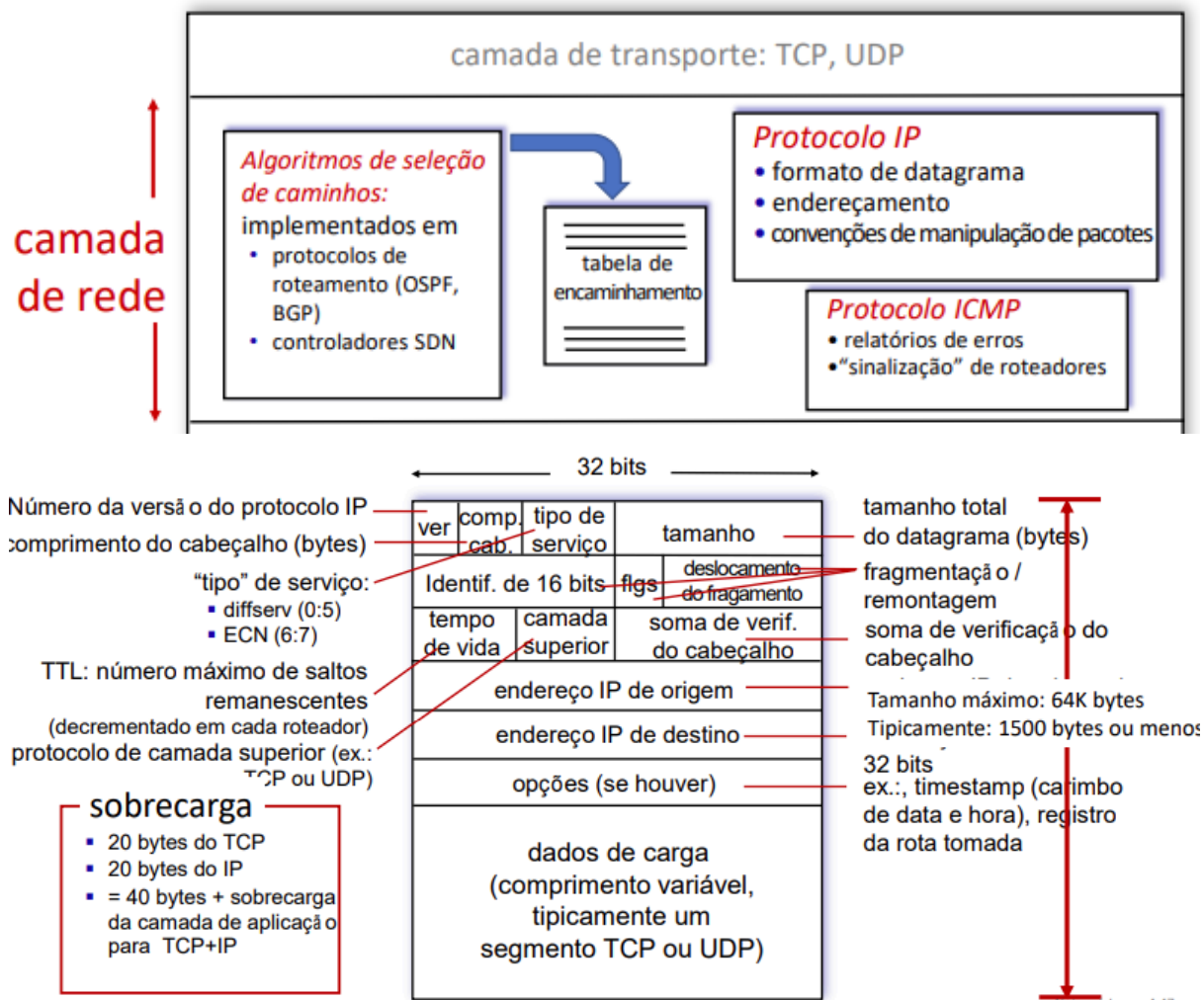
Fila da porta de saída:

- Buffering necessário quando os datagramas chegam da estrutura de comutação mais rápido do que a taxa de transmissão de enlace. Política de perda: quais datagramas descartar se não houver buffers disponíveis? -> Datagramas podem ser perdidos devido ao congestionamento, falta de buffers
- Disciplina de agendamento escolhe entre datagramas enfileirados para transmissão -> Agendamento prioritário – quem obtém melhor desempenho, neutralidade da rede

Gerenciamento de buffer

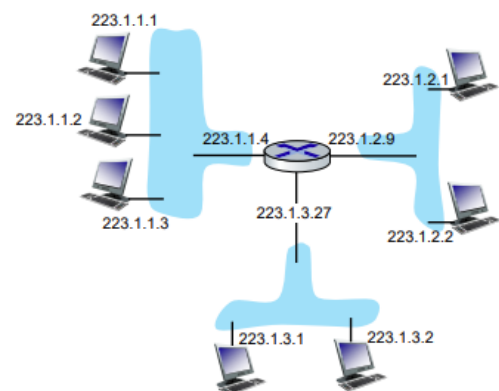
- perda: quais pacotes adicionar/descartar quando buffers estão cheios
 - tail drop: descarta pacote que está chegando
 - priority: descarta/remove com base em prioridades
- marcação: quais pacotes marcar para sinalizar congestionamento (ECN, RED)

Camada de Rede: Internet



Endereçamento IP: introdução

- endereço IP: identificador de 32 bits associado a cada interface de hospedeiro ou roteador
- interface: conexão entre hospedeiro / roteador e enlace físico
 - roteador normalmente tem várias interfaces
 - hospedeiro tipicamente tem uma ou duas interfaces (ex.: Ethernet cabeada, 802.11 sem fio)



Notação decimal de um endereço IP: 223.1.1.1 = 11011111 00000001 00000001 00000001

Sub-redes:

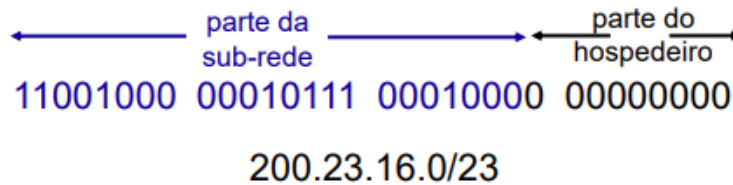
Interfaces de dispositivo que podem se alcançar fisicamente sem passar por um roteador intermediário

Endereços IP têm a estrutura:

- parte da sub-rede: dispositivos na mesma sub-rede têm bits comuns de alta ordem
- parte do hospedeiro: bits de baixa ordem remanescentes

CIDR:

- parte da sub-rede de endereço de comprimento arbitrário
- formato de endereço: a.b.c.d/x, onde x é o número de bits na parte da sub-rede de endereço



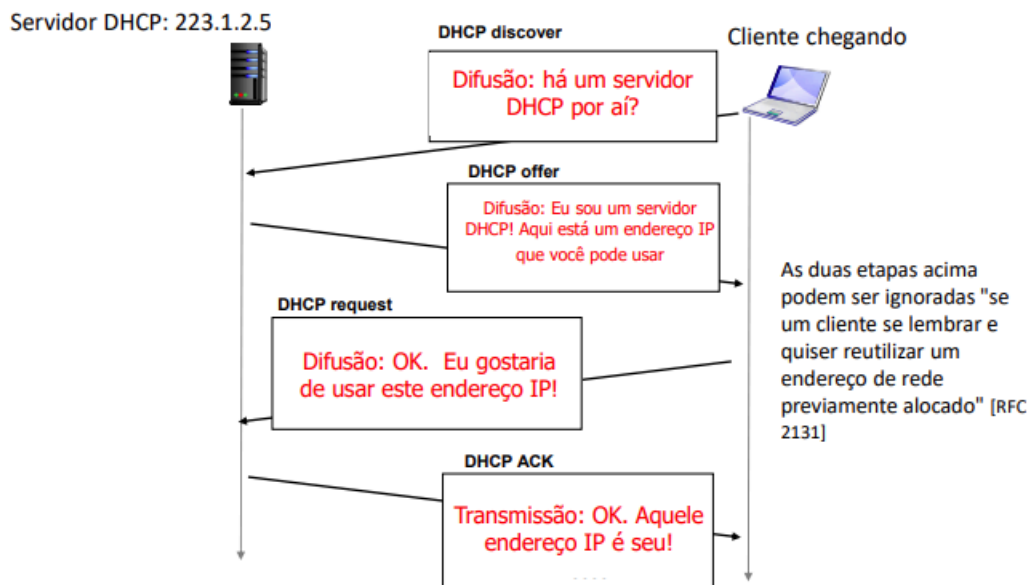
DHCP: Dynamic Host Configuration Protocol

Objetivo: o hospedeiro obtém dinamicamente o endereço IP do servidor de rede quando “entra” na rede

- pode renovar sua concessão sobre o endereço em uso
- permite a reutilização de endereços (apenas mantém o endereço enquanto conectado / ligado)
- suporte para usuários móveis que ingressam / saem da rede

Visão geral:

- hospedeiro difunde (broadcasts) mensagem DHCP discover [opcional]
- servidor DHCP responde com mensagem, DHCP offer [opcional]
- hospedeiro requisita endereço IP: mensagem DHCP request
- servidor DHCP envia endereço: mensagem DHCP ack



O DHCP pode retornar mais do que apenas o endereço IP alocado na sub-rede: endereço do roteador de primeiro salto para o cliente, nome e endereço IP de servidor DNS, máscara de sub-rede (indicando porção de rede versus porção de hospedeiro do endereço).

NAT: network address translation

Todos os dispositivos em uma rede local compartilham apenas um endereço IPv4 no que diz respeito ao mundo exterior

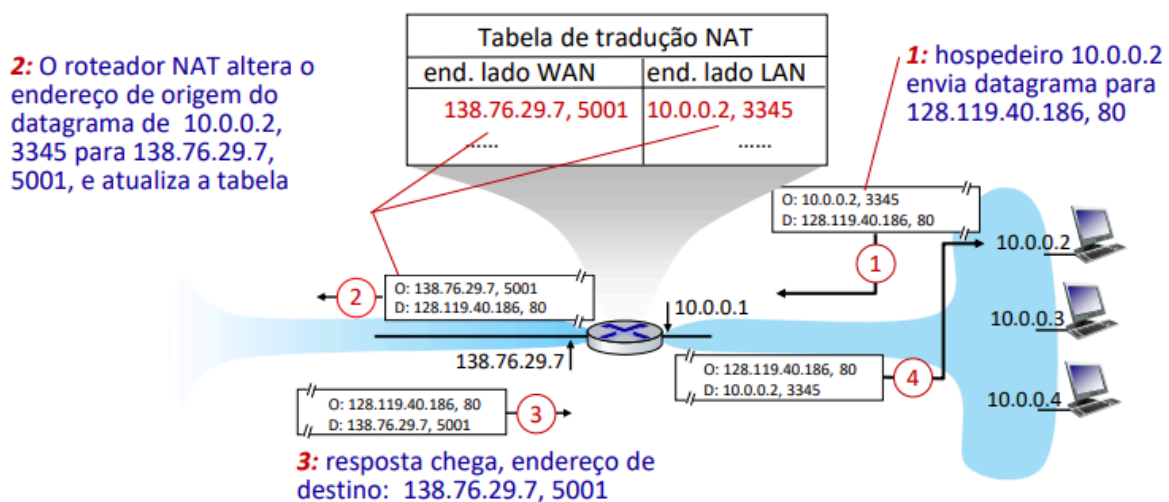
- Todos os datagramas deixando a rede local tem o mesmo endereço IP NAT fonte: 138.76.29.7, mas diferentes números de porta de origem
- Datagramas com origem ou destino nesta rede tem endereços 10.0.0/24 para origem e destino (como de costume)
- Todos os dispositivos na rede local têm endereços de 32 bits em um espaço de endereço IP “privado” (prefixos 10/8, 172.16/12, 192.168/16) que só podem ser usados em redes locais

Vantagens:

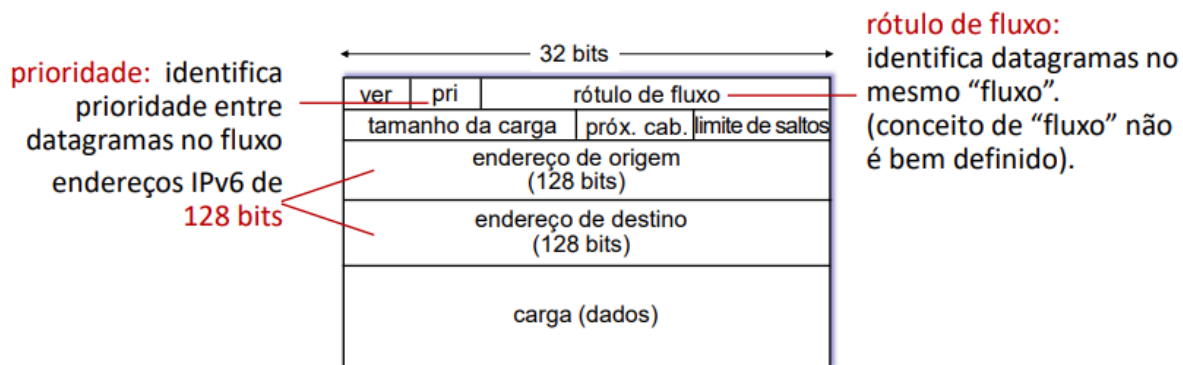
- *apenas um endereço IP do provedor é necessário para todos os dispositivos*
- é possível mudar endereços de hospedeiro em redes locais sem notificar o exterior
- pode alterar o provedor sem alterar endereços de dispositivos na rede local
- segurança: dispositivos dentro da rede local não são diretamente endereçáveis ou visíveis pelo mundo exterior

Implementação:

- datagramas de saída: substituir (endereço IP de origem, número de porta) de cada datagrama de saída para (Endereço IP NAT, novo número de porta)
 - clientes/servidores remotos responderão usando (endereço IP NAT, novo número de porta) como endereço de destino
- lembrar (na tabela de tradução NAT) todo par de tradução (endereço IP de origem, número de porta) para (Endereço IP NAT, novo número de porta)
- datagramas de entrada: substituir (Endereço IP NAT, novo número de porta) em campos de destino de cada datagrama de entrada com os correspondentes (endereço IP de origem, número de porta) armazenados na tabela NAT



IPv6: Endereçamento com numeração hexadecimal



O que está faltando (comparado com IPv4): sem soma de verificação (para acelerar o processamento em roteadores), sem fragmentação/remontagem, sem opções (disponíveis como protocolo de próximo cabeçalho de camada superior no roteador)

Capítulo 5 - Camada de Rede, plano de controle

Protocolos de roteamento:

- Objetivo do protocolo de roteamento: determinar caminhos "bons" (equivalentemente, rotas), do hospedeiro de origem ao hospedeiro de destino, por meio da rede de roteadores
- caminho: sequência de roteadores que os pacotes atravessam de um dado hospedeiro de origem até um hospedeiro de destino final
- "bom": menor "custo", "mais rápido", "menos congestionado"
- roteamento: um desafio de rede "top10"!

Algoritmo de roteamento de estado de enlace de Dijkstra

- centralizado: topologia de rede e custos de enlace conhecidos por todos os nós
 - realizado via "transmissão de estado de enlace"
 - todos os nós têm as mesmas informações
- calcula os caminhos de menor custo de um nó ("origem") para todos os outros nós
 - dá a tabela de encaminhamento para aquele nó
- iterativo: após k iterações, sabe os caminhos de menores custos para k destinos
- complexidade do algoritmo: n nós
 - cada iteração n: precisa checar todos os nós, w, não em N'
 - $n(n+1)/2$ comparações: complexidade $O(n^2)$
 - implementações mais eficientes possíveis: $O(n \log n)$
- complexidade de mensagem:
 - cada roteador precisa difundir suas informações de estado de enlace para outros n roteadores
 - algoritmos de transmissão eficientes (e interessantes!): $O(n)$ cruzamentos de enlaces para disseminar uma mensagem de difusão a partir de uma origem
 - a mensagem de um roteador cruza $O(n)$ enlaces: complexidade geral de mensagem: $O(n^2)$
- quando os custos do enlace dependem do volume de tráfego, oscilações de rota podem ocorrer

Algoritmo de vetor de distância (Bellman Ford)

- de tempos em tempos, cada nó envia sua própria estimativa de vetor de distância (DV) para os vizinhos
- quando x recebe novo DV estimado de qualquer vizinho, ele atualiza seu próprio DV usando a equação B-F: $D_x(y) \leftarrow \min_v \{c_{x,v} + D_v(y)\}$ para cada nó $y \in N$
- iterativo, assíncrono: cada iteração local causada por:
 - alteração do custo do enlace local
 - mensagem de atualização de DV de vizinho
- distribuído, auto-parada: cada nó notifica os vizinhos apenas quando seu DV muda
 - vizinhos então notificam seus vizinhos – somente se necessário
 - nenhuma notificação recebida, nenhuma ação tomada!

Abordagem da Internet para roteamento escalável

- agregar roteadores em regiões conhecidas como “sistemas autônomos” (AS) (também chamados “domínios”)
- intra-AS (ou “intra-domínio”): roteamento dentro do mesmo AS (“rede”)
 - todos os roteadores no AS devem executar o mesmo protocolo intradomínio
 - roteadores em diferentes AS podem executar diferentes protocolos de roteamento intradomínio
 - roteador gateway: na “borda” de seu próprio AS, tem enlace(s) para roteador(es) em outros AS'es
- inter-AS (ou “inter-domínio”): roteamento entre AS'es
 - gateways executam roteamento entre domínios

Protocolos de roteamento intra-AS mais comuns:

OSPF (Open Shortest Path First)

- “open”: disponível publicamente
- estado de enlace clássico
 - cada roteador inunda anúncios de estado de enlace OSPF (diretamente sobre IP em vez de usar TCP/UDP) para todos os outros roteadores em todo o AS
 - várias métricas de custos de enlace possíveis: largura de banda, atraso
 - cada roteador tem topologia completa, usa o algoritmo de Dijkstra para calcular a tabela de encaminhamento
- segurança: todas as mensagens OSPF são autenticadas (para evitar intrusões maliciosas)
- OSPF hierárquico
 - hierarquia de dois níveis : área local e backbone.
 - anúncios de estado de enlace inundados apenas na área ou backbone
 - cada nó possui topologia de área detalhada; só sabe direção para chegar a outros destinos
 - roteadores de borda de área: “resumem” distâncias para destinos na sua própria área, anunciam no backbone
 - roteadores locais: inundam estado de enlace apenas na área, calculam roteamento dentro da área, encaminham pacotes para fora via roteador de borda de área

Por que diferentes roteamentos Intra-AS e Inter-AS?

- política:

- inter-AS: o administrador quer controlar como o tráfego é roteado, quem roteia pela sua rede
 - intra-AS: administrador único, portanto, a política é menos problemática
- escala:
 - o roteamento hierárquico economiza o tamanho da tabela, reduz o tráfego de atualização
- desempenho:
 - intra-AS: pode focar no desempenho
 - inter-AS: política domina sobre o desempenho

Software defined networking (SDN)

Camada de rede da Internet: historicamente implementada por meio de abordagem de controle distribuído por roteador:

- roteador monolítico contém hardware de comutação, executa implementação proprietária de protocolos padrão da Internet (IP, RIP, IS-IS, OSPF, BGP) no SO de roteador proprietário (por exemplo, Cisco IOS)
- diferentes “middleboxes” para diferentes funções da camada de rede: firewalls, balanceadores de carga, caixas NAT, ..

Por que um plano de controle logicamente centralizado?

- gerenciamento de rede mais fácil: evita configurações incorretas de roteadores, maior flexibilidade nos fluxos de tráfego
- encaminhamento baseado em tabela (lembre-se da API OpenFlow) permite “programação” de roteadores
 - “programação” centralizada mais fácil: calcule tabelas centralmente e distribua
 - “programação” distribuída mais difícil: calcule tabelas como resultado de algoritmo distribuído (protocolo) implementado em cada roteador
- implementação aberta (não proprietária) do plano de controle
 - promover a inovação: não interferir em desenvolvimentos promissores em seus estágios iniciais

Comutadores de plano de dados:

- switches simples e rápidos que implementam o encaminhamento generalizado do plano de dados (Seção 4.4) em hardware
- tabela de fluxo (encaminhamento) computada e instalada sob supervisão do controlador
- API para controle de comutação baseado em tabela (por exemplo, OpenFlow)
 - define o que é controlável e o que não é
- protocolo para comunicação com o controlador (por exemplo, OpenFlow)

Controlador SDN (SO de rede):

- mantém as informações do estado da rede
- interage com aplicativos de controle de rede “acima” via API norte
- interage com comutadores de rede “abaixo” via API sul
- implementado como sistema distribuído para desempenho, escalabilidade, tolerância a falhas, e robustez

Aplicativos de controle de rede:

- “cérebros” de controle: implementa funções de controle usando serviços de nível inferior, API fornecida pelo controlador SDN

- desagregado: pode ser fornecido por terceiros: distinto do fornecedor de roteamento ou controlador SDN

ICMP: internet control message protocol

- usado por hospedeiros e roteadores para comunicar informações em nível de rede
 - relatório de erros: hospedeiro, rede, porta, ou protocolo inacessível
 - solicitação/resposta de eco (usado por ping)
- camada de rede “acima” do IP:
 - mensagens ICMP são transportadas em datagramas IP
- mensagem ICMP: tipo, código mais os primeiros 8 bytes do datagrama IP causando erro

Traceroute e ICMP

- Origem envia conjuntos de segmentos UDP para destino
 - 1º conjunto tem TTL =1, 2º conjunto tem TTL=2, etc.
- Datagrama no n-ésimo conjunto chega ao n-ésimo roteador:
 - roteador descarta datagrama e envia mensagem ICMP para a origem (tipo 11, código 0)
 - a mensagem ICMP possivelmente inclui o nome do roteador e o endereço IP
- Critérios de parada :
 - o segmento UDP eventualmente chega ao hospedeiro de destino
 - destino retorna mensagem ICMP “porta inacessível” (tipo 3, código 3)
 - origem para
- Quando a mensagem ICMP chega à origem: grava RTTs

Capítulo 6 - Camada de Enlace

Terminologia:

- Hospedeiros e roteadores são nós
- Canais de comunicação que conectam nós adjacentes são enlaces
- Pacote da camada 2 é um quadro, que encapsula datagrama
- A camada de enlace tem a responsabilidade de transferir datagramas de um nó para outro nó fisicamente adjacente através de um enlace

Contexto:

- Datagrama é transferido por diferentes protocolos de enlace sobre diferentes enlaces (ex: Ethernet, frame relay, 802.11)
- Cada protocolo de enlace fornece diferentes serviços

Serviços da camada de enlace:

- Enquadramento, acesso ao enlace:
 - Encapsula datagrama no quadro, incluindo cabeçalho
 - Acesso ao canal se o meio é compartilhado
 - Endereços “MAC” usados nos cabeçalhos de quadro para identificar origem, destino
 - Diferente do endereço IP! MAC é um endereço físico, fixo da máquina
- Entrega confiável entre nós adjacentes
 - Raramente é usado em enlace com poucos erros de bit
 - Enlace sem fio: altas taxas de erro
- Controle de fluxo: ritmo de nós de emissão e recepção adjacentes

- Detecção de erro: erros causados por atenuação de sinal e ruído, receptor detecta presença de erro e sinaliza ao remetente para retransmitir ou descarta quadro
- Correção de erro: receptor identifica e corrige erros de bit
- Half-duplex e full-duplex: com half-duplex os nós nas duas extremidades do enlace podem transmitir, mas não ao mesmo tempo

Onde a camada de enlace é implementada?

- Em todo e qualquer hospedeiro
- Implementada no “adaptador” ou placa de interface de rede
- Conecta-se aos barramentos do sistema do hospedeiro
- Combinação de hardware, software e firmware

Comunicação entre adaptadores

- Lado emissor:
 - Encapsula datagrama em quadro
 - Inclui bits de verificação de erro, rdt, controle de fluxo, etc
- Lado receptor:
 - Procura erros, rdt, controle de fluxo, etc
 - Extrai datagrama, passa para camada superior no lado receptor

Protocolos de Acesso Múltiplo

Dois tipos de enlace

- Ponto a ponto: enlace ponto a ponto entre comutador Ethernet e hospedeiro
- Difusão (broadcast - mídia compartilhada): Ethernet à moda antiga, HFC usado pelas TVs a cabo, Wifi

Algoritmos distribuído que determina como os nós compartilham canal, ou seja, determinam quando o nó pode transmitir

- Comunicação sobre compartilhamento de canal deve usar o próprio canal

Protocolos MAC

- Particionamento de canal: divide o canal em “pedaços” menores (intervalos de tempo, frequência, código), aloca pedaço ao nó para uso exclusivo, compartilham canal de modo eficiente e justo quando com alta carga, mas é ineficiente com baixa carga pois há atraso no acesso ao canal
- Acesso aleatório: canal não dividido, permite colisões, se “recupera” da colisões, eficiente com baixa carga mas com alta carga tem sobrecarga de colisão
 - ALOHA, CSMA, etc
- “Revezamento”: os nós se revezam, mas os nós com mais a enviar podem receber mais tempo, procura o melhor dos dois mundos
 - Polling: nó mestre “convida” nós escravos para transmitir em rodadas, tipicamente usado com dispositivos escravos burros, preocupações incluem sobrecarga, latência, ponto de falha único (mestre)
 - Passagem de token: token de controle passado de um nó para outro sequencialmente, preocupações incluem sobrecarga do token, latência, ponto de falha único (token)

Endereços MAC e ARP

- Endereço IP de 32 bits: camada de rede, usado para encaminhamento na camada 3
- Endereço MAC: usado “localmente” para levar quadro de uma interface a outra fisicamente conectada (mesma rede do ponto de vista do IP), 48 bits gravados no

hardware e em notação hexadecimal. Cada interface tem um endereço MAC único com alocação administrada pelo IEEE, os fabricantes que compram os direitos.

O ARP é um protocolo que faz o “mapeamento” de endereço IP e endereço MAC! Cria uma tabela de “tradução”.

- Cada nó na LAN tem uma tabela ARP que mapeia os endereços IP/MAC para alguns nós da LAN <end IP, end MAC, TTL>
- TTL (Time to Live) = tempo após qual o mapeamento de endereço será esquecido
- A quer enviar datagrama para B, e o MAC de B não está na tabela ARP de A
- A envia por broadcast pacote ARP de consulta, contendo o endereço IP de B
- MAC de destino: ff-ff-ff-ff-ff-ff (broadcast)
- Todos os nós na LAN recebem essa requisição ARP
- B recebe o pacote ARP e responde para A com seu endereço MAC, quadro é enviado para o MAC de A (unicast)
- A salva no cache o par IP/MAC de B em sua tabela ARP até a informação expirar

Ethernet

- Tecnologia de LAN com fio “dominante”, barata, primeira tecnologia amplamente usada, simples, acompanhou a corrida pela velocidade
- Diferentes topologias
- Estrutura do quadro: adaptador enviando encapsula o datagrama IP em um quadro Ethernet



Preâmbulo - usado para sincronizar as taxas de clock do emissor e do receptor

Endereço - MAC de origem e destino com 6 bytes cada

Tipo - indica o protocolo da camada acima (IP, etc)

CRC - cyclic redundancy check no receptor, se algum erro é detectado o quadro é descartado

Comutador Ethernet

- Dispositivo da camada de enlace, tem um papel ativo
 - Armazena e encaminha quadros Ethernet
 - Examina o endereço MAC dos quadros chegando, seletivamente encaminha quadro para um ou mais enlaces de saída quando o quadro deve ser encaminhado em um segmento, usa CSMA/CD para acessar segmento
- Transparente: hospedeiros não sabem da presença de comutadores
- Plug-and-play, self-learning: comutadores não precisam ser configurados
 - Comutador aprende quais hosts podem ser alcançados através de quais interfaces
 - Quando quadro é recebido, o comutador aprende a localização do emissor
 - Grava o par emissor/localização na tabela de comutação

Comutadores vs roteadores

Ambos armazenam-e-encaminham. Ambos tem tabela de encaminhamento.

- Roteadores: dispositivos da camada de rede (examinam cabeçalhos de datagrama). Computam tabelas usando algoritmos de roteamento e endereço IP.

- Comutadores (switches!): dispositivos da camada de enlace (examinam cabeçalhos de quadros). Aprendem a tabela de encaminhamento usando inundação, aprendizado e endereços MAC.

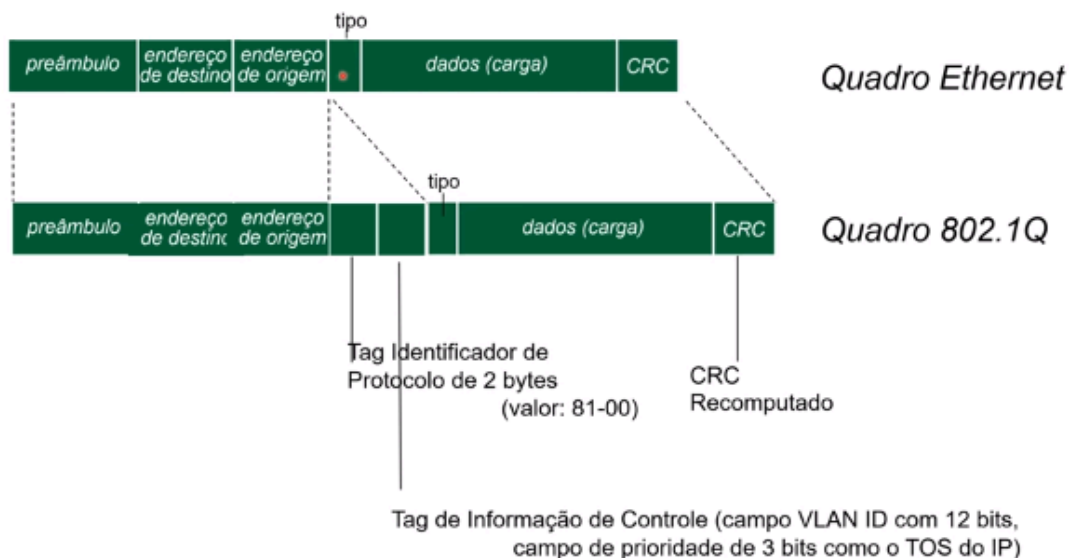
VLANs

Motivação: problemas de segurança/privacidade e eficiências. Criar uma “rede” virtual que isola o tráfego.

- Virtual Local Area Networks = comutadores que suportam capacidades de VLAN podem ser configurados para definir múltiplas LANs virtuais sobre uma única infraestrutura de LAN física.

VLAN baseada em portas: portas do comutador agrupadas (pelo software de gerenciamento do comutador) de forma que um único comutador físico opere como múltiplos comutadores virtuais.

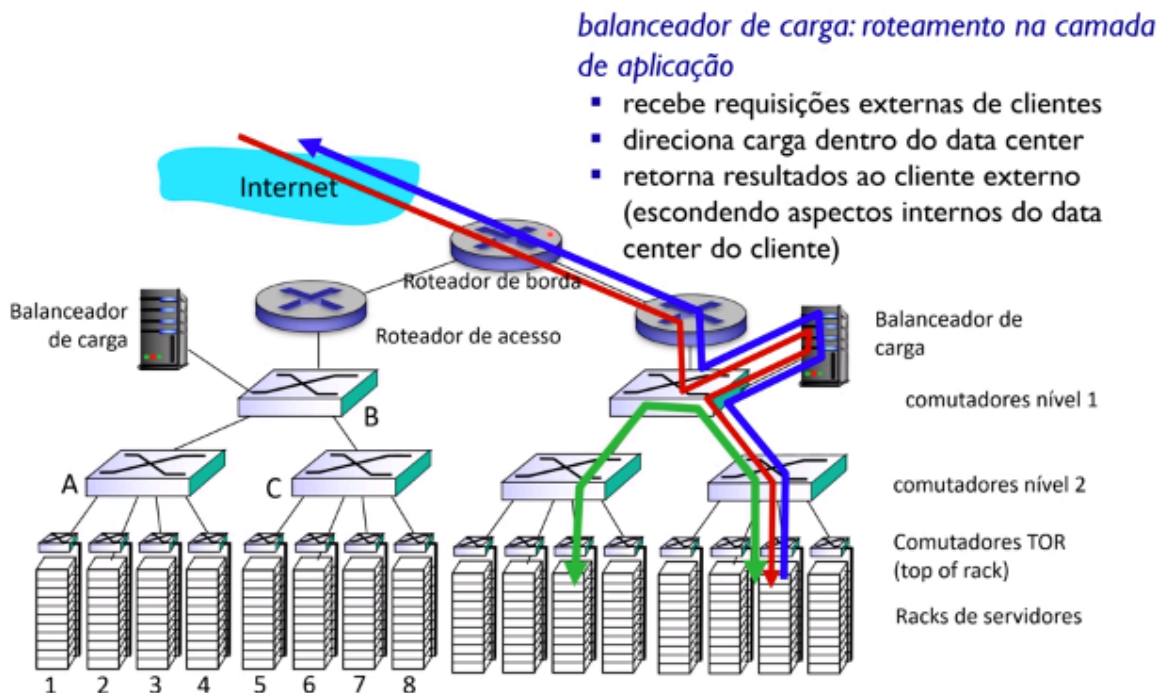
- Isolamento de tráfego: quadros de/para portas na VLAN alcançam somente as portas da VLAN
- Associação dinâmica: portas pode ser dinamicamente atribuídas entre VLANs
- Encaminhamento entre VLANs: feito via roteamento (tal qual como comutadores separados)
 - Na prática, os dispositivos que são vendidos são uma combinação de roteador e comutador
 - Para que as VLANs se espalham por mais de um comutador, faz-se o uso de PORTAS DE TRONCO (mode trunk), que são portas/cabos que conseguem carregar quadros de VLANs (802.1 Q) pois adiciona novos campos no cabeçalho



Redes de data centers

- Dezenas a centenas de milhares de hospedeiros, frequentemente acoplados em locais próximos
- Desafios: múltiplas aplicações, cada uma servindo um número massivo de clientes; gerenciamento/balanceamento de carga, evitando gargalos de processamento, rede e dados

- Rica interconexão entre comutadores e racks: vazão aumentada entre racks (múltiplos caminhos de roteamento possíveis), confiabilidade aumentada via redundância



Síntese: um dia na vida de uma solicitação web

- Jornada através da pilha de protocolos -> Aplicação, transporte, rede, enlace
- Cenário: estudante conecta laptop à rede, solicita/recebe www.google.com
- O laptop conectando precisa obter seu próprio endereço IP, endereço do roteador de primeiro salto e endereço do servidor DNS -> usa o DHCP
- Requisição DHCP encapsulada em UDP, encapsulada em IP, encapsulada em Ethernet 802.3
- Quadro Ethernet enviado por broadcast na LAN, recebido no roteador executando DHCP
- Ethernet demultiplexador para IP, demultiplexador para UDP, demultiplexador para DHCP
- Servidor DHCP formula DHCP ACK contendo endereço IP do cliente, IP do primeiro salto, nome e endereço IP do DNS
- Encapsulamento no servidor DHCP, quadro encaminhado (aprendizado do comutador) através da LAN, demultiplexador no cliente
- Cliente DHCP recebe resposta DHCP ACK
- Cliente agora tem endereço IP, sabe nome e endereço dos servidores DNS e endereço IP do roteador de primeiro salto
- Antes de enviar requisição HTTP, é necessário saber o IP do google -> DNS
- Requisição DNS criada, encapsulada em UDP, IP, Ethernet. Para enviar quadro para roteador, é necessário o endereço MAC da interface do roteador -> ARP
- Broadcast da requisição ARP, recebida pelo roteador, o qual responde com ARP reply dando o endereço MAC da interface do roteador

- Cliente agora sabe endereço MAC do roteador de primeiro salto, portanto agora pode enviar quadro contendo a requisição DNS
- Datagrama IP contendo requisição DNS encaminhado via comutador da LAN do cliente para o roteador de primeiro salto
- Datagrama IP encaminhado da rede do campus para a rede da Comcast, roteado para o servidor DNS
- Demultiplexador para o servidor DNS
- Servidor DNS responde ao cliente com o endereço IP do google
- Para enviar requisição HTTP, cliente primeiro abre socket TCP para o servidor web
- Estabelece conexão TCP com 3-way handshake
- Requisição HTTP enviada no socket TCP
- Datagrama IP contendo requisição HTTP roteada para o google
- Servidor web responde com resposta HTTP (contendo página web)
- Datagrama IP contendo resposta HTTP roteada de volta ao cliente

RESUMO, CAPÍTULO 6

- Princípios por trás dos serviços da camada de enlace:
 - Detecção de erros, correção de erros
 - Compartilhando um canal de broadcast: acesso múltiplo
 - Endereçamento na camada de enlace
- Instanciação e implementação de várias tecnologias da camada de enlace
 - Ethernet
 - LANs comutadas, VLANs