Apontamentos para redes- teste 2



NETWORK LAYER:

-NETWORK LAYER OVERVIEW

-WHAT IS INSIDE A ROUTER

-IP: INTERNET PROTOCOL



NETWORK LAYER OVERVIEW:

O sender encapsula os segmentos da camada de transporte para datagramas quando passa para a link layer e o receiver entrega o segmento na transport layer protocol (TCP)

Network Layer está em todos os dispositivos que estão interligados à internet como hosts e routers

ROUTERS: examinam os headers de todos os IP datagramas que passam por ele, move os datagramas dos input ports para os outports para os transferir.

Funções da network layer:

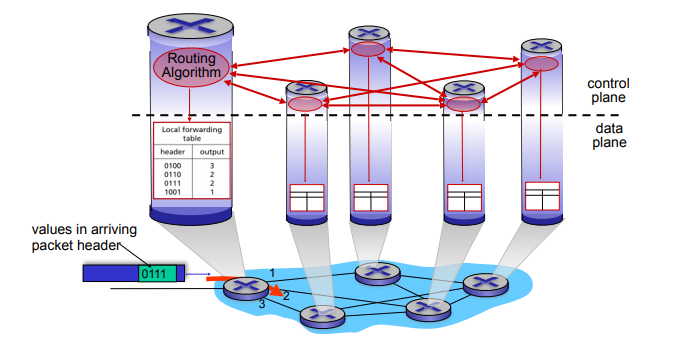
1. FORWARDING: move o pacotes que estão à entrada de um certo router para a sua apropriada saída
2. ROUTING: determina qual o caminho a ser tomado para o pocote desda source até à destination

Exemplo: Numa viagem, o processo de sair num certa saída na autoestrada é forwarding, o processo de planeamento da rota de onde estamos para onde vamos é routing.

DATA PLANE: determina como o datagrama chega à entrada do router e como o mesmo vai ser transferido para a sua saída, isto é algo que acontece em cada router, localmente

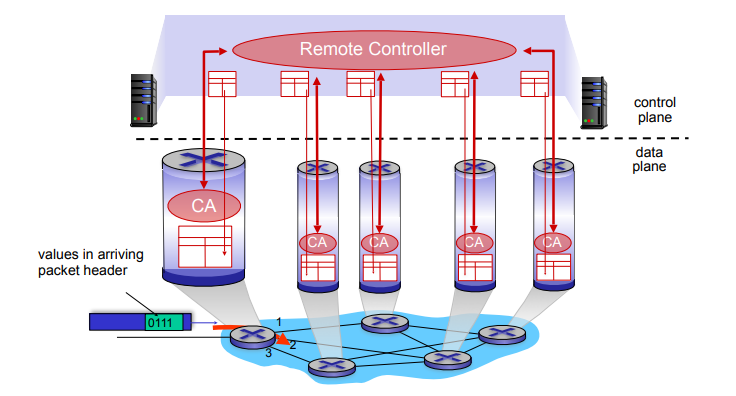
CONTROL PLANE: determina como o datagrama é roteado entre os routers de source até chegada, isto é algo que acontece na nível da network (network-wide) e este tâm duas approaches: Tradicional routing (implementada nos routers) e Software Defined Networking (implementada nos servidores)

PER ROUTER CONTROL PLANE:



Cada router interage com a control plane e com isso tem então acesso a uma routing table do pacote para saber qual saída terá que encaminhar o pacote

LOGICALLY CENTRALIZED CONTROL PLANE:



Em cada router é remotamente colocado uma forwarding table em cada um dos routers de forma a ter as informações do pacote

NETWORK SERVICE MODEL:

**Q: What service model for channel transporting datagrams from sender to receiver?**

Exemplo de serviços para **datagramas individuais**: garante a entrega e garante a entrega em menos de 40 milisegundos.

Exemplo de serviços para o **flow de datagramas**: são entregues em ordem, garante a utilização de mínima largura de banda para transferir e restringe as mudanças dos pacotes.

O network service model não garante a entrega do datagram, o tempo, a ordem e a largura de banda necessária para a entrega de um certo pacote.

REFLEXÕES SOBRE O BEST-EFFORT SERVICE:

1. SIMPLICIDADE DO MECANISMO
2. LARGURA DE BANDA
3. DISTRIBUIÇÃO DE SERVIÇOS DA APLICATION LAYER (REPLICA)
4. CONGESTION CONTROL

WHAT’S INSIDE A ROUTER:

Input ports, switching, outport ports

INPORT PORTS: recebe uma line termination da physical layer, o link layer protocol (para receber o pacote) e tem o lookup,forwarding queueing (switching descentralizado na qual usa os headers para encontrar qual é o output port do pacote; input port queuing- se o datagrama chega mais rapidamente que a forwarding rate)

DESTINATION-BASES FORWARDING: encaminha baseado no ip address tradicional

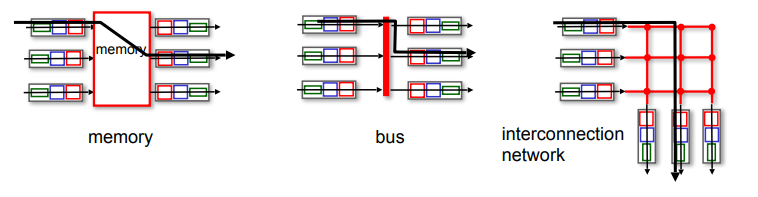
GENERALIZED FORWARDING: encaminha baseado nos valores do header

LONGEST PREFIX MATCHING: quando olhamos para uma entrada da forwarding table dada pelo destination address, usa o maior endereço que faz correspondência ao endereço de destino.

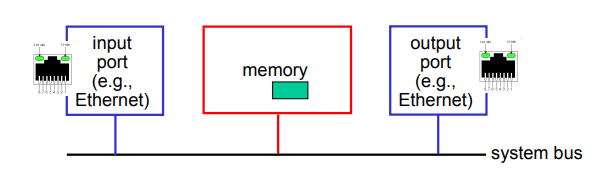
SWITCHING FABRICS: transfere os pacotes do input link mais apropriado para o output link.

SWITCHING RATE: avalia quais pacotes podem ser transferidos da entrada para a saída

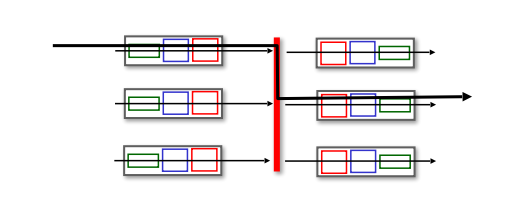
Existem 3 grandes switching fabrics: Em memória, em bus e em interconnection network



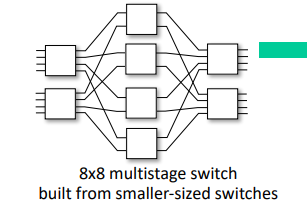
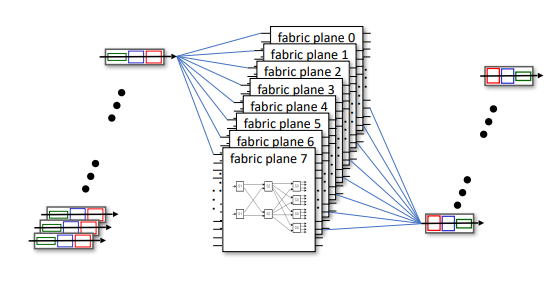
SWITCHING VIA MEMORY: nos computadores tradicionais com switching diretamente controlado pelo CPU, o pacote é copiado para o sistema de memória e a velocidade é limitada de acordo a largura de banda da memória em questão



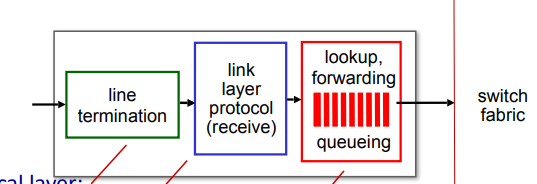
SWITCHING VIA BUS: o datagrama vai da memória do inport para o outport da memória partilhando um bus, bus contetion (velocidade do switching é limitada em largura de banda)



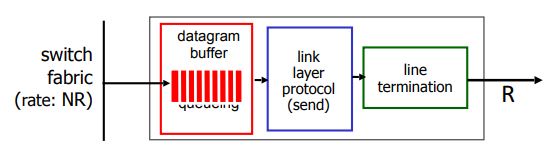
SWITCHING VIA INTERCONNECTION NETWORK: um multitask switch (n\*n) e exploiting parallelism (fragmentos do datagrama são de tamanho fixo nas células de entrada), a disposição (usamos vários switches planes em paralelo de maneira a aumentar a velocidade)



INPUT PORT QUEUING: se a switch fabric for mais lenta que os inpout ports combinados poderá haver queueing (input queues). Se houver um delay e perda de queueing é devido ao input buffer overflow.



OUTPUT PORT QUEUING: **Buffering** é necessário quando o datagrama chega da malha (fabric) mais rapidamente que a transmissão de link rate (este datagram pode ser perdido por causa de congestão ou falta de buffers), **Scheduling discipline** escolhe de entre os queued dtatagramas para transmitir (a prioridade via para os que tem melhor performance e network neutrality)



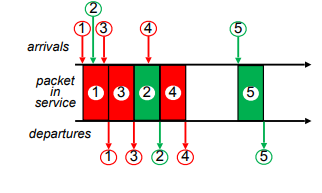
BUFFER MANAGEMENT, SCHEDULING:

BUFFERING MANAGEMENT: Drop (qual pacote devemos adicionar ou largar quando os buffers estão cheios; Tail Drop: largar o pacote que chega; Priority: largar em questão de prioridade), Marking (na qual marca os pacotes com um sinal de congestão ECN, RED)

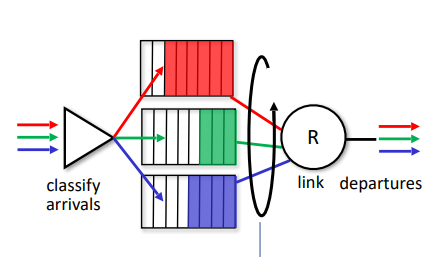
PACKET SCHEDULING (FCFS) : decide qual pacote enviar depois, no caso o primeiro a ser enviado é o primeiro a ser servido, tem prioridade, tem um peso que queueing aceitável.

FCFS: pacotes transmitidos em ordem de chegada ao output port, first-in-first-out

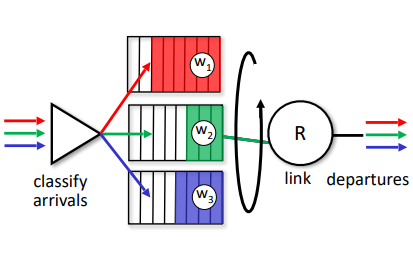
SCHEDULING POLICIES: Priority Schedulign- quando o trafégo chega é classificado numa queed class, usando os headers para classificar os pacotes, e envia pacotes de maior prioridade quele que foram bufferizados em pacotes



Round Robin Sheduling- o servidor é cíclico, repetindo os scans de cada class (das queued), mandando um pacote completo para cada class se disponíveis



Weighted Fair Queuing (WFQ)- é um Round Robin generalizados, em que cada class i tem um peso Wi e é pesado cada serviço de ciclo por pacote

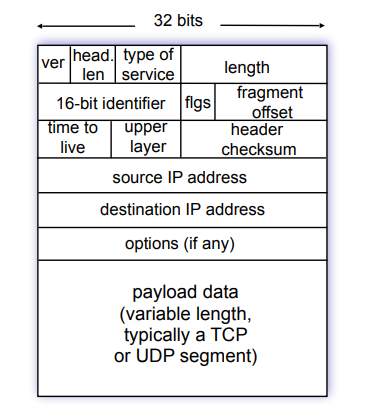


IP: INTERNET PROTOCOL:

FORMATO DO DATAGRAMA:

Dentro da network layer temos 3 assuntos bastante importantes: o Path-selection algorithms que são implementados com protocolos de routing e SDN controller, na qual obtemos as forwarding tables, temos o IP protocol que nos fala do formato do datagrama, do endereçamento e de manuseamento de pacotes.

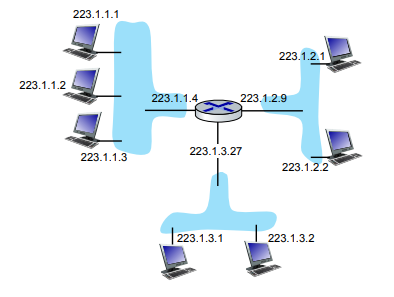
O formato do datagrama IP é constituído pela length (tamanho do datagrama em bytes), as flags, fragment offset, 16-bit identifier de forma a tratar da fragementação (reassemble of packets), o TTL, upper layer (TCP ou UDP) header checksum, source IP address (32bits), destination IP address (32 bits). Pode ver a ter 40 bytes



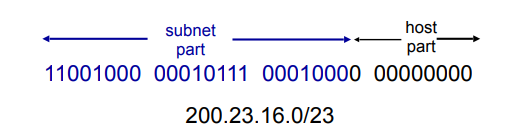
IPv4 ADDRESSING:

É um identificador a 32 bits no qual é associado a cada host ou router interface.

INTERFACE: conexão entre o host e o router e a physical layer, os routers normalmente têm várias interfaces, os hosts normalmente têm uma ou duas interfaces



CIDR (Classless InterDomain Routing): a porção da subnet é arbitrária e o seu formato de endereço é de a,b,c,d/x na qual o x é o número de bits na subnet.

Endereço de Subnet: 

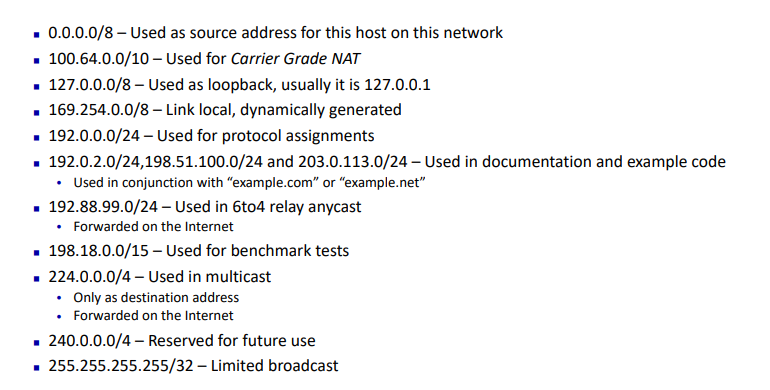
Endereço de BroadCast seriam todos os bits da host part a 1

SUBNET: São dispositivos de interfaces que conseguem chegar um ao outro sem ter que passar no router

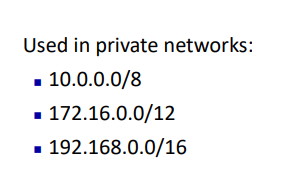
STRUCTURE OF IP ADDR: Subnet part (devices in the same subnet have common high order bits) e Host part (os restantes bits menos significativos)

HOW TO DEFINE A SUBNET: separar cada interface desde o router ao host criando ilhas isoladas de network, sendo cada ilha uma subnet

IP ADDRESSES (SPECIAL ADDRESSES):



IP ADDRESSES (PRIVATE ADDRESSES):



HOW TO GET A IP ADDRESS: Através do protocol DHCP (Dynamic Host Configuration Protocol) no qual recebemos um IP address através do server quando nos juntamos à rede

DHCP- habilita a reutilização de endereços IP, e suporta dos users de mobile

O host primeiro faz um request dum IP Address (DHCP request) e o DHCP server manda um endereço de IP ao host (DHCP ack)

NETWORK ADDRESS TRANSLATION:

NAT- todos os serviços de rede local partilham apenas um endereço IPv4

Todos os datagramas que saem da rede local levam um source NAT address mas dentro da rede local os datagramas com a origem e destino na rede têm o endereço local como source e destination.

Todos os dispositivos na rede têm o endereço IP privado no qual só pode ser usado dentro da rede local. Com isto temos vantagens como, apenas um endereço IP é necessário do ISP para todos os dispositivos, podemos alterar os IP dos hosts na rede local sem ter preocupações coma rede fora, pode mudar o ISP sem mudar o endereço do dispositivo na rede local e os dispositivos dentro da rede local não são diretamente endereçáveis/visíveis pelo mundo.

IMPLEMENTATION: NAT router deve:

* Ter um outgoing datagrama que muda cada outgoing datagrama source IP address, port# para NAT IP address, novo port#
* Lembrar-se de cada par de tradução de (source IP address, port#) para (NAT IP address, novo port#)
* Nos incoming datagramas mudar o para (NAT IP address, novo port#) no destination fields de cada incoming datagrama com a correspondente (source IP address, port#) guardado na NAT table

CONTROVERSIAL TOPICS ABOUT NAT:

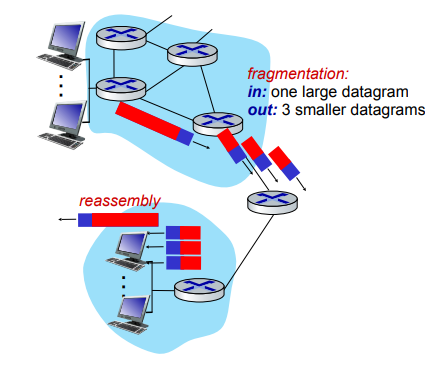
* Routers should only be processed in layer 3
* Address shortage should be solved by IPv6
* Violates end-to-end argument
* NAT traversal -VER AINDA A PARTE DA HIERARQUIA

FRAGMENTATION:

Network links have MTU (max segment size- maior link possível), logo cada link diferente tem um MTU diferente também

Quando o IP datagrama é muito grande há uma necessidade de o dividir em pequenas parcelas pelas quais podem ser transferidas, isto quando são enviadas. Quando chegam ao destino são reassembladas de novo ao IP datagrama inicial.

No header do IP vai a ordem pela qual conseguimos identificar cada fragmento



FAZER OS EXERCÍCIOS DE FRAGMENTAÇÃO !!!!

ICMP (Internet control message protocol):

Este protocolo é usado para os hosts e os routers comunicarem a informação do nível da network, ao qual partilham os erros (quando não conseguimos alcançar um host, network, porto ou protocolo)

As mensagens do protocolo ICMP são transferidas em IP datagramas

Estas mensagens contêm o type, um código e os primeiros 8 bytes do IP datagrama que está a causar problemas

TRACEROUTE E ICMP: Quando enviamos um segmento UDP para um certo destino, quando o nth datagrama passa nth router.

Quando router descarta o datagrama, o protocolo ICMP manda uma mensagem à source com o type 11 e o código 0, na qual esta mensagem pode ter o nome do router e o IP address.

Stopping criteria:

1. Quando eventualmente o segmente UDP chega ao destino
2. Quando o destino retorna uma mensagem ICMP com o type 3 e o código 3 (“port unreachable)
3. Quando a origem acaba

IPv6:

Este foi criado com o intuito de resolver o problema de esgotamento de endereços no IPv4

O seu header tem 40 bytes fixos de tamanho e permite diferentes tratamentos de flow na network layer.

IPv6 DATAGRAM FORMAT: tem uma flow label (consegue identificar datagramas com o mesmo flow), priority (identifica a prioridade entre datangramas na flow), source address (tem 128 bits) e destination address (tem 128 bits), payload (onde transporta os dados)

QUAIS AS DIFERENÇAS PARA O IPv4:

1. Não tem checksum, para termos mais velocidade nos routers em questão de processamento do endereço
2. Não tem fragmentation/reassembly
3. Não tem opções

LINK LAYER:

- INTRODUCTION

- ERROR DETECTION, CORRECTION

- MULTIPLE ACESS PROTOCOL

- LAN’S

- DATACENTER NETWORKING

- A DAY IN A LIFE OF A WEB REQUEST

INTRODUTION:

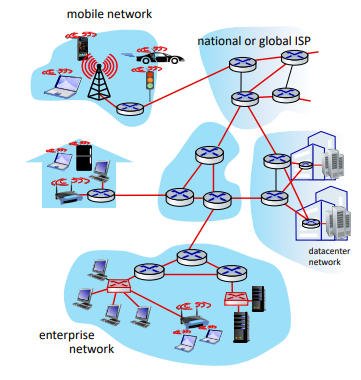
A Layer que trata da última ligação com a rede local do cliente (Last Mile), que se encarrega de encontrar o dispositivo certo onde tem que entregar o pacote e que faz a adaptação do datagrama para a rede local

Todos os dispositivos têm sempre o mesmo MAC Address (este varia de dispositivo para dispositivo).

À entrada de cada router que está ligado a vários dispositivos, a LINK LAYER vai ver de acordo o IP Address do router qual o MAC Address associado a esse IP (IP ao qual pretende entregar o pacote)

TERMINOLOGY:

1. HOSTS AND ROUTERS: nós
2. CANAIS DE COMUNICAÇÃO QUE SE CONECTÃO ATRAVÉS DOS NÓS AO LONGO DO CAMINHO DA COMUNICAÇÃO (Links- wired, wireless, LANs)
3. LAYER 2 PACKET: Frame (trama) que encapsula o datagrama IP da Layer 3



A Link Layer tem como responsabilidade transferir o datagrama de um nó para o outro através do seu MAC Address

CONTEXT: O datagrama é transferido por diferentes protocolos de link para diferentes links (WiFi on first lnik, Ethernet on the next link)

Cada protocolo de link fornece diferentes serviços, que pode ou não dar dados reliable através da transferência por link

Analogia de transporte do datagrama:

Viagem de Princeton para Lausanne

Tourista = Datagrama

Segmento de Transporte = Communication Link

Transport mode = Link Layer Protocol

Travel Agent = Routing Algorithm

SERVIÇOS DA LINK LAYER:

FRAMING, LINK ACESS: Encapsula um datagram num frame, adicionando-lhe o header, garante meios partilhados, multiplexa vários users numa rede, o MAC Address no header do frame identifica qual é a origem e o destino (diferente do IP Address)

RELIABLE DELIVERY BETWEEN ADJANCENT NODES: Entre o ponto A e o ponto B ele assegura a transferência segura de todos os bits.

Tem End-to-End reliability pois o protocol TCP conhece as pontas (onde deve de entre o pacote).

O Link atua localmente quando há um erro na passagem de bits, já o TCP só vê a saída e chegada deles ao destino.

FLOW CONTROL: Assegura que não há um excesso de fluxo na rede.

ERROR DETECTION: Deteta erros causados por ruído, e o receiver deteta erros (ao qual pede retransmissão).

ERROR CORRECTION: Consegue alterar um bit (dar flip), em vez de fazer retransmissão do pacote, tendo o pacote correto.

HALF-DUPLEX AND FULL-DUPLEX: Ambos os nós de cada ponta, transmitem mas não ao mesmo tempo.

WHERE IS THE LINK LAYER IMPLEMENTED: Em cada host separadamente. Esta layer é implementada no NIC (network interface card) ou chip (Ethernet, WiFi card ou chip). Já se encontra no data bus dos dispositivos dos hosts. Combinação de hardware, software e firmware.

INTERFACES COMMUNICATING:

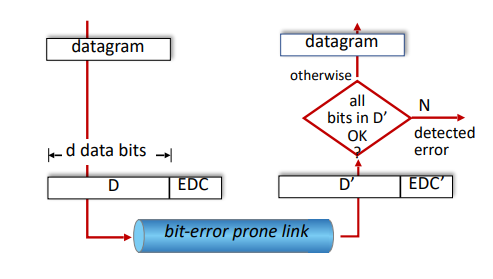
- SENDING SIDE: Encapsula o datagrama para um frame, e adiciona um x de bits para correção de erros de modo a transferir dados de maneira segura, assegura flow control, entre outros

. RECEIVING SIDE: Procura por erros, assegura o recebimento de data segura, assegura flow control, extraí o datagrama e passa-o para a layer superior do lado que vai receber o datagrama

ERROR DETECTION, CORRECTION:

EDC: Deteta errões e fornece bits de correcção (redundante)

D: data protegida pela correção de erros



Um datagrama qua vai ser transmitido num canal pode ter erros. No caso do datagrama chegar ao receiver com erros, temos que perceber onde poderá estar o erro, logo a deteção de erros não é 100% reliable.

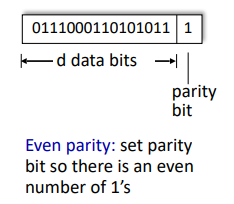
PARITY CHECKING:

UM BIT DE PARIDADE:

Qualquer datagrama que chegar com um x de bits a 1, se o número de bits for ímpar adicionamos um 1, se já for par, adicionamos um zero

Quando é feito o set up da ligação é feita a paridade (decide-se)

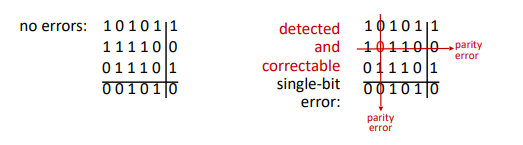
Se a paridade não bater certo há erros no pacote mas não se sabe ao certo onde



TWO DIMENSIONAL BIT PARITY:

Pegamos na mensagem e dividimo-la por dois.

Deteta erros e corrige um bit individual

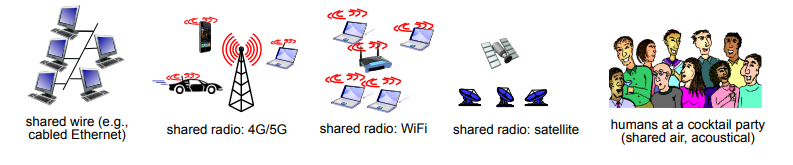


INTERNET CHECKSUM: deteta erros mas não os corrige, no transporte de pacotes através do protocolo UDP temos este campo

CRC (CYCLIC REDUNDANCY CHECK) – De todos os meios, é o qual a correção de erros é mais eficiente, os dados em bits fornecidos e o padrão dos bits dados por r+1 se a soma desse dois mod 2 não der resto zero, significa que há um erro no pacote enviado.

MULTIPLE ACCESS PROTOCOLS:

Existem 2 tipos de links, o point-to-point (ligação de um ponto a outro, Ethernet switch a um host), e Broadcast (como o WiFi, 4G/5G entre outros) que são meios partilhados.

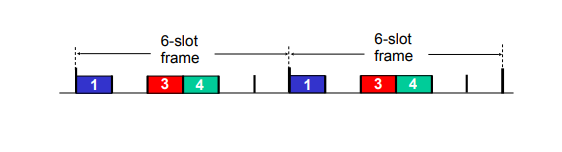


Quando temos apenas uma transmissão num canal partilhado de Broadcast não haverá colisões pois apenas temos uma pessoa a fazer uma transmissão mas quando há um ou mais dispositivos a fazer transmissão num mesmo nó há probabilidade de haver colisão de bits. Temos o chamado collision domain que faz parte da rede onde podem estar n bits ( se não existisse este domain os bits iriam chocar fazendo a partilha de um canal complicado posi a informação nunca chegará ao receiver)

A situação ideal seria se um nó quer transmitir bits ele envia um x no temos que tem de envio, passando para outro nó e assim todos os nós têm um x de bits que podem enviar,, havendo assim uma **PARTIÇÃO DO CANAL** (time slots) – exemplo- num apartamento, todos temos um mês sozinhos para estar lá, nossa time slot é um mês, e quando acaba temos que dar as chaves do apartamento a outra pessoa, usamos o apartamento à vez - **TAKING TURNS**.

**RANDOM ACCESS**: o canal não é dividido longo há possibilidade de colisão

CHANNEL PARTITIONING MAC PROTOCOLS: TDMA(TIME DIVISION MULTIPLE ACCESS)



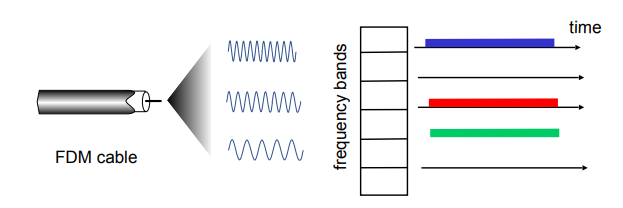
Acedemos ao canal em rondas, à vez

Cada vez, isto é por cada slot, tem um slot de bits que pode enviar fixa.

Durante o meu time slot há a intuição que a rede é só minha, mas não, a rede é nossa naquela time slot, após essa passar, já não tenho permissão para enviar mais bits pois não estou na minha time slot.

No caso de haver um dispositivos mais ativo que os outros, ele tem que esperar na mesma posi é a time slot que o mesmo tem disponível apesar de os outros dispositivos que estão a partilhar a rede com ele não esejam tão ativos.

CHANNEL PARTITIONING MAC PROTOCOLS: FDMA (FREQUENCY DIVISION MULTIPLE ACCESS)



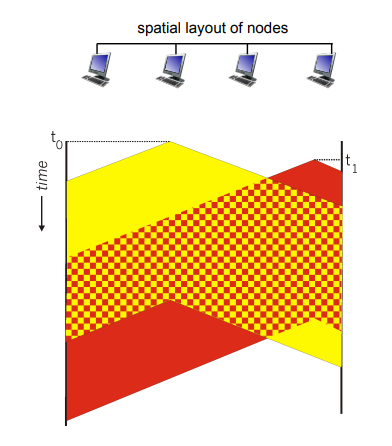
Quando escolhemos as nossas rádios favoritas associamos diferentes frequências a diferentes canais para podermos aceder às mesmas. O espectro é dividido em canais de frequência.

RANDOM ACCESS PROTOCOL: Não há regras, transmitimos quando queremos, sem coordenação entre os nós, podemos mandar quando e quanto quisermos.

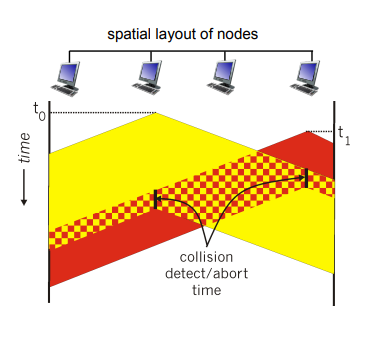
Random Access MAC protocol: deteta colisões e como recuperar de uma colisão (delayed retransmissions) – exemplos – CSMA, ALOHA, CSMA/CD, CSMA/CA

CSMA (CARRIER SENSE MULTIPLE ACCESS):

* SIMPLE CSMA: Olho para a janela e vejo se há tráfego ou não e vejo qual o melhor momento para sair (ouvir antes de transmitir)



* CSMA/CD (CSMA WITH COLLISION DETECTION): As colisões são detetadas num curto período de tempo. Em caso de colisão, abortamos a transmissão, ao qual o processo é tranquilo, isto é, estável, mas em redes WiFi a qualidade fica comprometida devido à largura de banda disponível



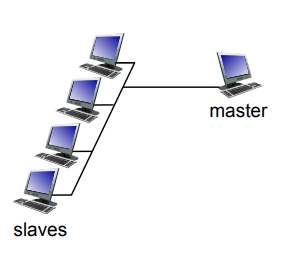
TAKING TURNS MAC PROTOCOL:

- CHANNEL PARTITITONING MAC PROTOCOL: A partilha do canal de forma eficiente e com uma grande carga. Este é ineficiente para pequenas cargas.

- RANDOM ACCESS MAC PROTOCOL: Eficiente com uma carga menor, num único nó de forma a usar todo o canal. Este é ineficiente no caso de uma grande carga pois há risco de colisão

- TAKING TURNS PROTOCOL:

- POLLING: Determina quem tem a permissão para enviar informação, em que temos um nó que faz a determinação de quem tem permissão.



- TOKEN PASSING: Passa de máquina em máquina dando a conhecer que tem a vez para enviar informação, isto de forma sequencial.

SUMMRY OF MAC PROTOCOLS: Temos 3 protocols de MAC

- CHANNEL PARTITIONING: Pode ser por tempo (TDMA) ou por frequência (FDMA)

- RANDOM ACCESS: CSMA, CSMA/CD, CSMA/CA, ALOHA

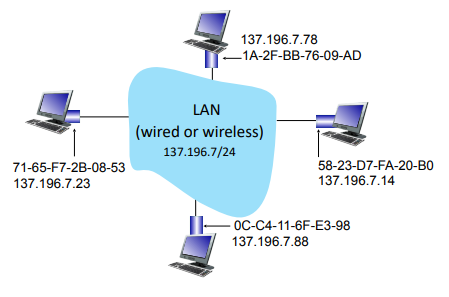
- TAKING TURNS: Polling do site central e passage do token (Bluetooth)

LAN’S : ADDRESSING, ARP

O MAC Address complementa o endereço IP. Este tem 48 bits e é o identificar de um dispositivo físico. Com 6 blocos com 2 números ou letras cada tem 4 bits de informação.

Exemplo: 1A-2F-BB-76-09-AD

Cada interface LAN tem um único MAC Address a 48 bits e tem um único endereço IP localmente

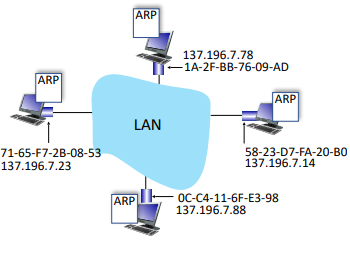


MAC ADDRESS: É administrado pelo IEEE, o fabricante do equipamento, são os bits mais significativos do MAC Address – exemple- 00 60 2F código de equipamento Cisco

IEEE- Gere os MAC Addresses usados nos mesmo devices

Logo analogicamente: Um IP address diz onde moro (podemos mudar) e este pertence a uma determinada rede, um MAC address diz quem eu sou (nunca muda) e é portável, vai connosco para onde for.

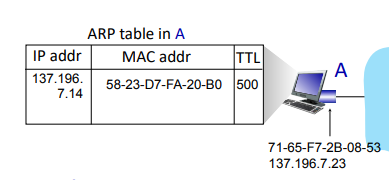
ARP (ADDRESS RESOLUTION PROTOCOL): Cada dispositivo vai preencher a sua ARP table, tendo o IP address, o MAC address e o TTL (Time To Leave- tempo pelo qual o endereço mapeado será esquecido). A ARP table apenas está disponível em dispositivos hosts e routers. <IP address; MAC address; TTL>

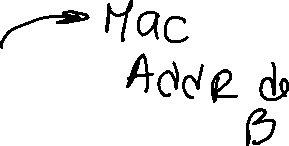
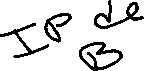


Exemplo: A quer enviar o datagrama para B

O MAC address de B não está na ARP table de A então irá usar o ARP para encontrar o MAC Address de B

1. A faz um pedido de Broadcast com uma ARP Request Query que contem o IP Address de B (o endereço de MAC de Broadcast FF-FF-FF-FF-FF-FF, para todas as portas menos a dele próprio, levando este endereço de Broadcast junto do IP de B) e envia esse request para todos os nós dessa LAN com o objetivo de encontrar o MAC Address de B.
2. B responde a A através de uma ARP Response dando o seu MAC Address, em que agora a ARP message tem o Target IP (o de B) e o Target MAC Address(de B).
3. A recebe a reposta de B, adicionando na ARP table local o MAC Addres de B ficando com esta ARP table.

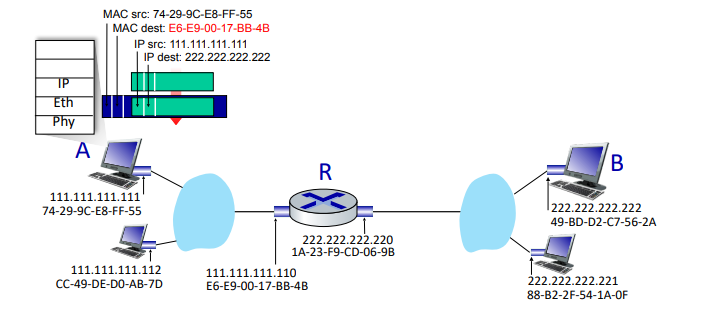




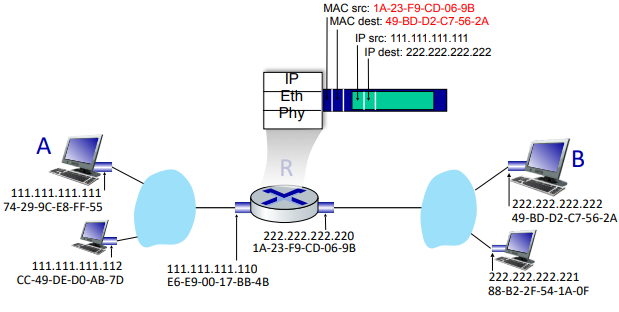
ROUTING TO ANOTHER SUBNET – ADDRESSING:

Mandar um datagrama de A para B passando num router isto é, estando agora os dispositivos em diferentes subnets

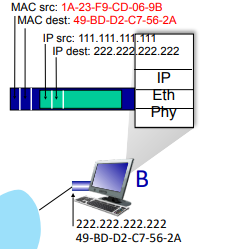
1. Cria um IP datagrama com o source IP de A e destination B
2. Cria um frame contendo o IP datagram de A para B, tendo o MAC Address do router no destino do frame



1. O frame criado será enviado do dispositivo A para o router
2. O router recebe esse mesmo frame, tirado o datagrama e passando o IP para a outra subnet
3. O router vai então determinar para qual interface se dirige, passando agora um datagrama com a source IP de e a destination de D e cria um frame onde tem o frame destination o MAC Address de B



1. Transmite o frame da link layer para o nó onde se contra o B

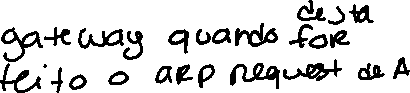


Ambos os lados aprendem com o arp request e response (dispositivos de Layer 3)

Switches guardam o MAC address e a informação das portas (layer 2)

Nenhum ARP request pode sair da rede local.

Quando fazemos um arp request de um dispositivo noutra rede não vamos receber o MAC address desse dispositivos mas sim como resposta vamos obter o MAC address da gateway do router



O protocolo ARP recebe um IP address e transforma-o em MAC Address

TTL não faz parte da arp reply

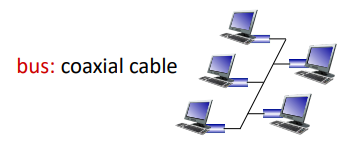
ARP não se aplica aos switches mas sim FDB’s e os switches não têm IP mas têm MAC

No caminho de volta apenas o dispositivo que fez a query é que fica a conhecer os dados do router.

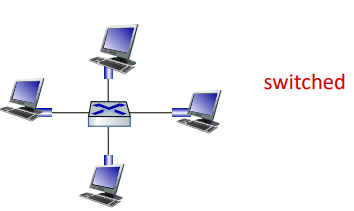
Só aprendemos com a source

LAN’S ETHERNET:

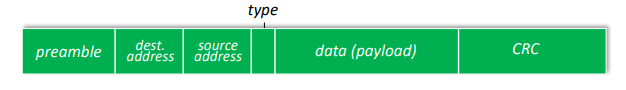
BUS: Popular through mid 90s, em que todos os nós tinham o mesmo domain de colisão por isso havia possibilidade de have choque de bits, isto é, colisão de bits. Esta é feita de um cabo coaxial (CSMA/CD), meio partilhado.



SWITCHED: Prevalece nos dias de hoje, cada nós runs a separate Ethernet protocol, logo os nós não colidem uns com os outros. Não existem troços comuns onde há colisão, distingue o trafego para os diferentes dispositivos.



ETHERNET FRAME STRUTURE:



- O datagrama IP para a zona de data(payload)

- Preamble tem 8 bytes (preamble + SFD) e é usado para sincronização de máquinas

- Dest (destino da próxima rede local) e Source (gateway da última rede local) address tem MAC address da máquina de envio e receção- 6 bytes

- Type: dá informação do protocolo da layer superior (maioritariamente IP (IPv4, IPv6))

- CRC: Cyclic Redundancy Check at the receiver- deteta erros

ETHERNET:

* CONNECTIONLESS: Não tem setup entre o envio e receção do NIC’s
* UNRELIABLE: Recebe os NIC’s sem mandar ACK’s e NACK’s para perceber se chegou ou receiver
* ETHERNET MAC PROTOCOL: CSMA/CD com binary backoff

VLAN (VIRTUAL LAN): Necessidade de pegar numa rede LAN física e torna-la digital

LAN’S – SWITCHES:

ETHERNET SWITCH: Um switch é um dispositivo de layer 3 (link layer), o switch para a rede IP é como se não existe-se

Dispositivo com inteligência, guarda frames (é capaz de aprender para onde vai e a informação sobre o pacote enviado, sabe o MAC Address de origem e o porto de origem, pois mais uma vez, só aprendemos com a source)

É transparente aos olhos do host, o host não tem a noção da existência de switches na rede

Os switches não precisam de ser configurados (self-learning)

SWITCHES - MULTIPLE SIMULTANEOUS TRANSMISSIONS:

Cada host tem uma ligação dedicada e direta a um switch

Switches bufferizão os pacotes

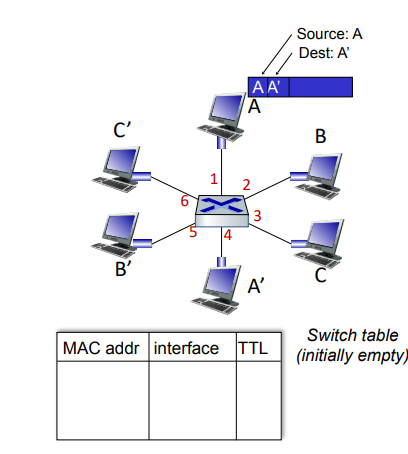
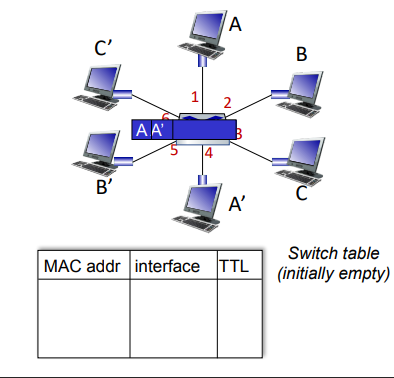
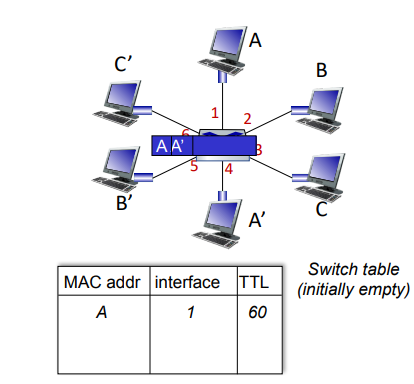
Tem um collision domain independente- todas as interfaces têm um separadamente.

Quando estão a ser enviados pacotes para o mesmo dipositivo pode haver colisão mas quando é enviado de A para A’ e de C para C’ não há colisão de bits

SWITCHES FORWARDING TABLE:

Cada switch tem uma switch table com o MAC address do host, a interface para alcançar o host e o time stamp

SWITCH SELF-LEARNING: O switch aprende qual host quer atingir com uma certa interface

INTERCONNECTING SWITCHES: Os switches aprendem sozinhos logo podem estar conectados

SWITCHES VS ROUTERS: Ambos guardam e encaminham e têm forwarding tables

-ROUTERS: Fazem parte da network layer. Computação de IP Address para as suas interfaces. **Faz a rede.**

-SWITCHES: Faz parte da link layer. Aprende com as forwarding tables usando o flooding, learning e os MAC Addresses. **Divide a rede.**

DATACENTER NETWORKING:

Usados por empresas que têm um número elevado de hosts como a Amazon, o Youtube, a Akamai, a Apple, a Microsoft, a Goodle entre outros.

OBJETIVOS: Múltiplas aplicações servem um vasto número de hosts, ao servirem esses clientes garantindo reliability, e balanciar a carga de modo a não haver excesso de data a ser processado.

DATACENTER NETWORKS- NETWORK ELEMENTS

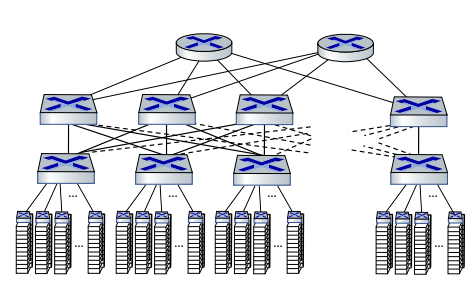
- SERVER RACKS: 20-40 servidores: hosts

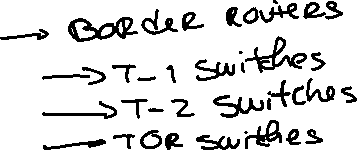
- TOP OF RACK (TOR) SWITCH: Um por cada server rack e com 40-100Gbps

- TIER-2 SWITCHES: Faz conexão de 16 TOR que estão por baixo dele

-TIER-1 SWITCHES: Faz conexão de 16 T-2 que estão por baixo dele

-BORDER ROUTERS: Faz a conexão dos datacenters externos





DATACENTER NETWORKS: PROTOCOL INNOVATIONS

LINK LAYER: remote DMA (RDMA)

TRANSPORT LAYER: ECN

ROUTING/MANAGEMENT: SDN