

RCOM Network

up201606673-André Esteves

18 January 2019

1 Network

Network label - camada responsável pela transferência de pacotes

1.1 Exercises

(1º part) (2º part)

1. 2018 Recurso (7,9) (3)
2. 2018 Normal (2,7,9) (3)
3. 2017 Normal (1,8) (3)
4. 2016 Recurso (6,7) (3)
5. 2016 Normal (7) (3)
6. 2015 Normal (1,7) (3)
7. 2014 Normal (2,7,9) (3)
8. 2013 Normal (7) (3)
9. 2012 Normal (6,7,8) (3)
10. 2011 Normal (6,7,8) (3)
11. 2010 Normal (2,4) (3)

1.2 Overview

- Camada de Network (Network layer)
 - Transporta os pacotes(datagrams)
 - ”from sending host to receiving host”
 - funções localizadas em todos os hosts e routers
- Transmissor(Sender):

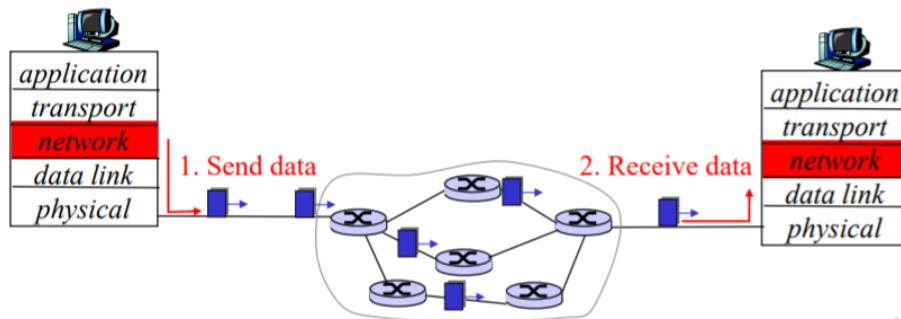
- Encapsula a informação em pacotes
- Cria os pacotes
- Receptor(Receiver):
 - Recebe os pacotes
 - Envia a informação para o transport layer
- Router:
 - Recebe os pacotes pela linha de input
 - Examina o cabeçalho dos pacotes
 - Reencaminha os pacotes para o sítio certo
 - Tem de saber o caminho mais curto para determinar o caminho

1.3 Funções principais da camada de rede

- Forwarding
 - router trata de enviar o pacote desde a porta de entrada(input) até à porta de saída(output)
- Routing
 - determina a rota definida pelos packets
 - algoritmos, caminho mais curto

1.4 Rede de datagramas

- Serviço não orientado à ligação
- Não há o conceito de circuito
- Os pacotes são redirecionados de acordo com a fonte e o destino
- Pacotes com o mesmo par fonte-destino podem seguir caminhos diferentes



9

<u>Destination Address Range</u>	<u>Output Link Interface</u>
11001000 00010111 00010000 00000000 through 11001000 00010111 00010111 11111111	0
11001000 00010111 00011000 00000000 through 11001000 00010111 00011000 11111111	1
11001000 00010111 00011001 00000000 through 11001000 00010111 00011111 11111111	2
otherwise	3

2^{32} possible entries in IPv4

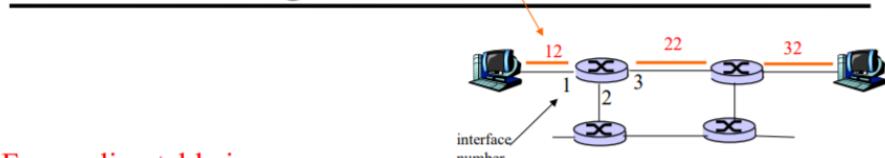
1.5 Circuitos Virtuais

- Serviço orientado à ligação
- Fases:
 1. Estabelecer o circuito
 2. Transferência de dados
 3. Terminação do circuito
- Cada pacote carrega um identificador do circuito virtual
- Caminho da fonte ao destino - ; sequência de identificadores virtuais, um para cada ligação
- Estado de cada circuito mantido pelo router, que pode alocar recursos (bandwidth, buffers) por circuito virtual

1.5.1 Forwarding Table

Contém prefixos e a respetiva porta de saída ;Endereço/Mask, port;

VC - Forwarding Table



Forwarding table in northwest router:

Incoming interface	Incoming VC #	Outgoing interface	Outgoing VC #
1	12	3	22
2	63	1	18
3	7	2	17
1	97	3	87
...

Routers maintain connection state information!

8

1.5.2 Ex: Maior correspondência de prefixo

<u>Prefix Match</u>	<u>Link Interface</u>
11001000 00010111 00010	0
11001000 00010111 00011000	1
11001000 00010111 00011	2
otherwise	3

Examples. Which Interface?

DA: 11001000 00010111 00010110 10100001 → 0

DA: 11001000 00010111 00011000 10101010 → 1,2 → 1

longest prefix

1.6 Circuitos Virtuais versus Rede de Datagramas

Issue	Datagram subnet	Virtual-circuit subnet
Circuit setup	Not needed	Required
Addressing	Each packet contains the full source and destination address	Each packet contains a short VC number
State information	Routers do not hold state information about connections	Each VC requires router table space per connection
Routing	Each packet is routed independently	Route chosen when VC is set up; all packets follow it
Effect of router failures	None, except for packets lost during the crash	All VCs that passed through the failed router are terminated
Quality of service	Difficult	Easy if enough resources can be allocated in advance for each VC
Congestion control	Difficult	Easy if enough resources can be allocated in advance for each VC

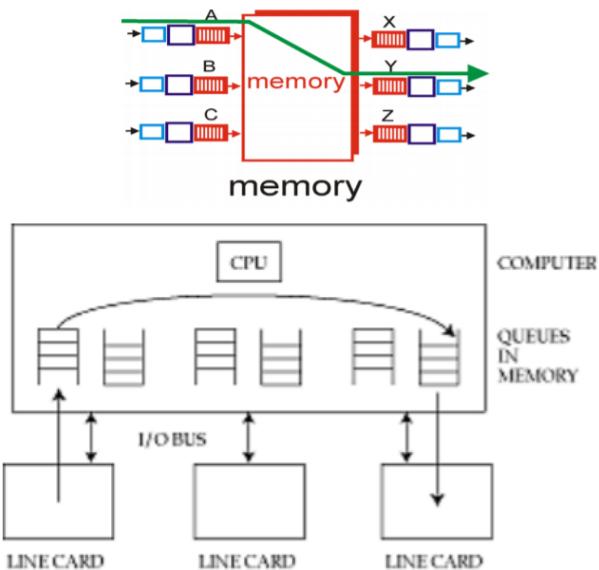
1.6.1 Exame 2016 Recurso - Ex:6

6. Uma rede composta por um conjunto de routers IP interligados entre si que transporta apenas tráfego TCP constitui
- a) Uma rede de comutação de pacotes e oferece um serviço não orientado às ligações.
 - b) Uma rede de comutação de pacotes e oferece um serviço orientado às ligações.
 - c) Uma rede de circuitos virtuais e oferece um serviço não orientado às ligações.
 - d) Uma rede de circuitos virtuais e oferece um serviço orientado às ligações.

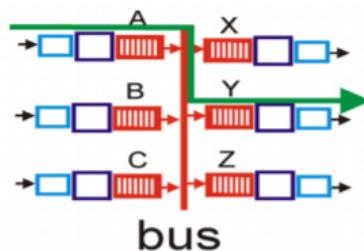
1.7 Arquitetura do router

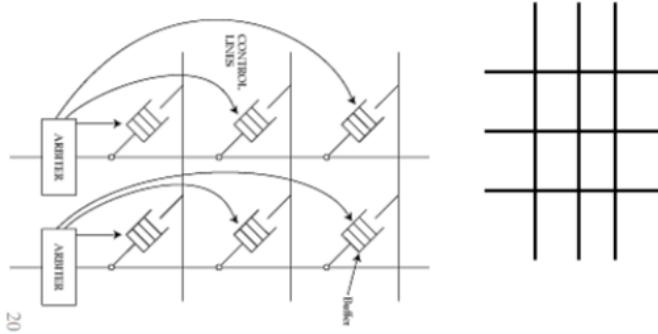
- Funções principais:
 - Correr algoritmos de roteamento e protocolos (RIP, OSPF, BGP)
 - Reencaminhar pacotes
- Componentes principais:
 - Input Port
 - * Physical Layer (bit-level)
 - * Data Link Layer (e.g., Ethernet)
 - * Queuing (se os pacotes chegarem rápido demais)
 - * Lookup + Forwarding (faz algum reencaminhamento imediatamente)
 - Output Port
 - * Buffering (quando é excedida a velocidade de saída)

- * Queuing (com disciplina de agendamento) (Queuing perda e espera - devido ao overflow do buffer da porta de input)
- * Data Link Layer (protocol, desencapsulação)
- * Physical Layer (linha de terminação)
- Switching Fabric
 - * Controla o reencaminhamento (fisicamente ou através dum CPU)
 - * Switching Via Memória do Computador
 - Router de primeira geração
 - Em computadores tradicionais, switching é controlado pelo CPU
 - Cada pacote é copiado para a memória do sistema e transferida duas vezes pelo bus

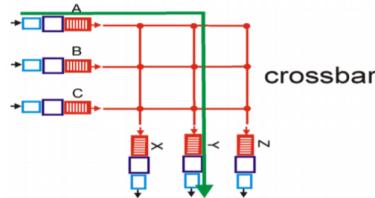


- * Switching via a Bus
 - Os pacotes são processados por um bus partilhado
 - A transferência dos pacotes desde a linha de input e output é realizada de forma direta
 - A taxa da conexão do bus é limitada pela bus bandwidth





- * Switching via a Crossbar
 - $2N$ buses
 - Possibilita transferências simultâneas de pacotes
 - a cross bar pode conter buffers intermos
 - Ultrapassa os limites da bus bandwidth



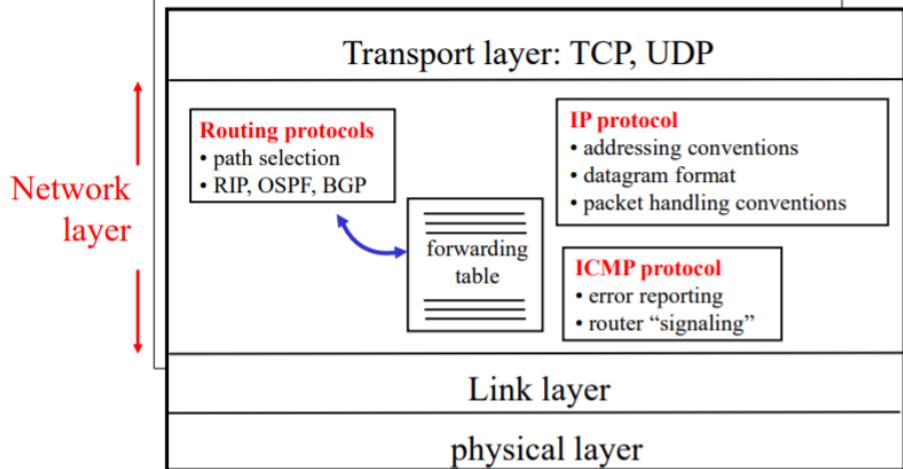
Exame 2016 Normal - Ex.7

7. Quando uma trama é recebida por um *Switch Ethernet* e a tabela de encaminhamento do *Switch* não contém uma entrada para o endereço de destino da trama, o *Switch*
 - a) Elimina a trama.
 - b) Invoca um procedimento do *Address Resolution Protocol* (ARP).
 - c) Envia a trama para todas as portas ativas exceto a porta através da qual a trama foi recebida.
 - d) Envia a trama para através da porta ligada ao *default gateway* do *Switch*.

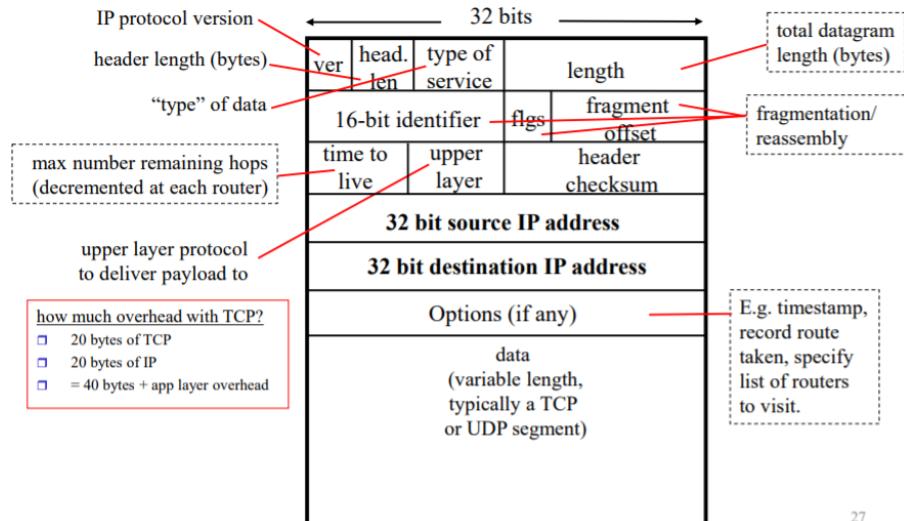
1.8 Protocolo Internet

1. Camada de rede Internet

Host, router network layer functions



2. Formato datagramma IP



27

3. Internet Checksum

Internet Checksum

- ♦ The Internet (not layer 2) uses a checksum
 - » easily implementable in software →
 - » 1's complement sum of 16 bit words
 - » Performance: d=2

```
u_short
cksum(u_short *buf, int count)
{
    register u_long sum = 0;
    while (count--)
    {
        sum += *buf++;
        if (sum & 0xFFFF0000)
        {
            /* carry occurred,
             so wrap around */
            sum &= 0xFFFF;
            sum++;
        }
    }
    return ~(sum & 0xFFFF);
}
```

- ♦ One's complement sum
 - » Mod-2 addition with carry-out
 - » Carry-out in the most-significant-bit is added to the least-significant bit
 - » Get one's complement of “one's complement sum”

1010011	
0110110	
carry-out ① 0001001	
Carry wrap-around 0000001	
0001010	
One's complement = 1110101	

1.8.1 Cada pacote contém:

- Versão do protocolo IP
- Tamanho do Header
- Tipo de serviço
- Tamanho da informação
- Identificador + Flags + Offset de Fragmento (Permite fragmentar mensagens em vários pacotes)
- Time To Live (para os pacotes não ficarem indefinidamente perdidos na rede)
- Upper Layer Protocol
- Checksum do Header
- IP de Origem
- IP de Destino
- Opções (opcional)
- Informação (Normalmente pacote TCP ou UDP)

1.8.2 Fragmentação IP e Reassembly

- Identificador i - Identifica o pacote
- fragflag i - 1 se houver mais informação, 0 se for o último fragmento
- Offset i - Offset do fragmento em bytes / 8

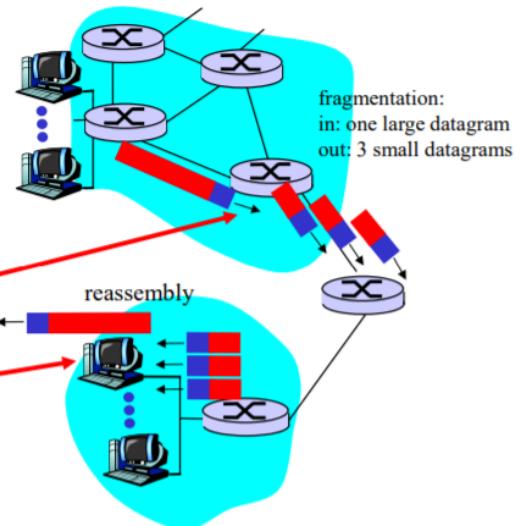
IP Fragmentation and Reassembly

♦ Network links have MTU

- » MTU - max. transfer size
- » largest possible link-level frame
- » different link types, different MTUs

♦ Large IP datagram is fragmented

- » one datagram → n datagrams
- » “reassembled” at final destination
- » IP header bits used to identify, order related fragments



Example

- 4000 byte datagram
- 3980 bytes data + 20 bytes IP header
- MTU = 1500 bytes

	length =4000	ID =x	fragflag =0	offset =0	
--	-----------------	----------	----------------	--------------	--

One large datagram becomes several smaller datagrams

1480 bytes in data field

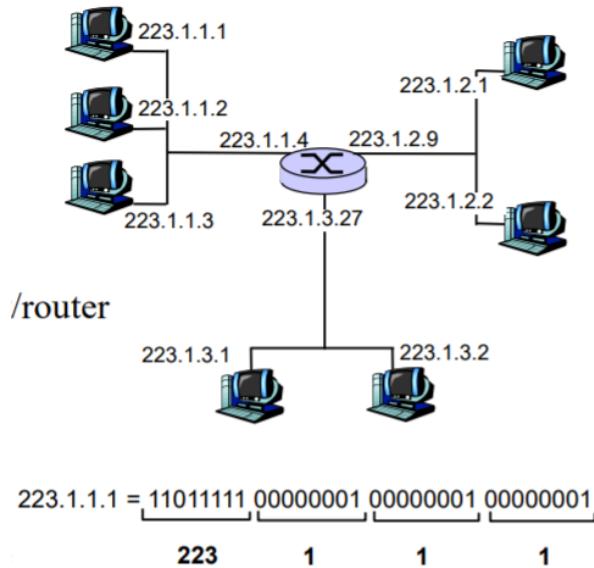
offset =
1480/8

	length =1500	ID =x	fragflag =1	offset =0	
	length =1500	ID =x	fragflag =1	offset =185	
	length =1040	ID =x	fragflag =0	offset =370	

1.8.3 Endereço IP

Endereço IP - é formado por um identificador de 32-bit para uma interface host/router Interface possuem:

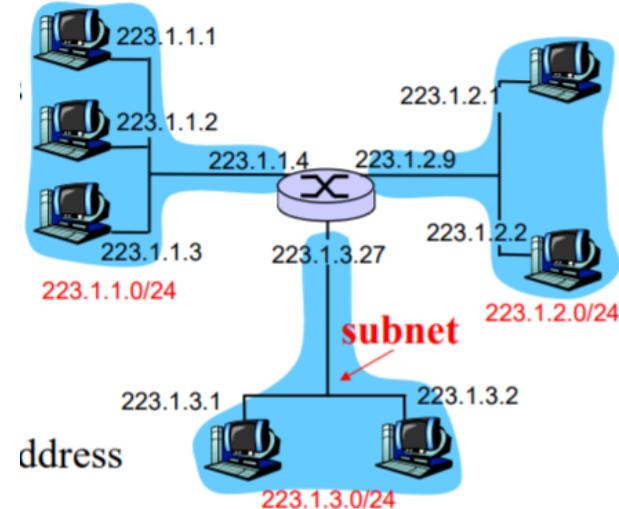
- conexão entre host/router e link físico(physical link)
- routers com multiplas interfaces
- endereços IP associados com as interfaces



1.8.4 Subnets

- Parte mais significativa do IP: Subnet parte
- Parte menos significativa: host(interface) parte
- Subnet é um set de interfaces
- cada um tem a subnet parte do IP igual para comunicação
- Cada computador consegue aceder a outro sem intervenção do router

Network consisting of 3 subnets



CIDR - Classless InterDomain Routing

- a porção de bits do endereço subnet tem tamanho arbitrário
 - formato $-i\ a.b.c.d/x$, em que x é o número de bits na porção do endereço subnet



200.23.16.0/23

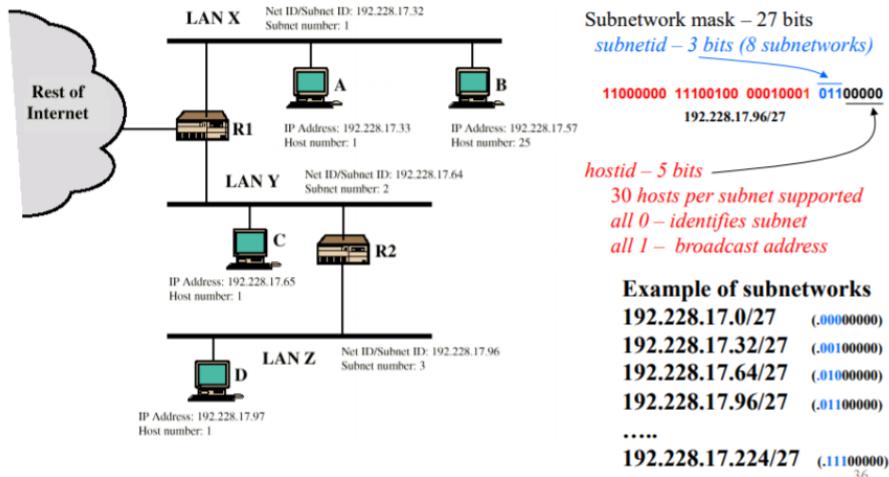
1.8.5 Endereços especiais

- 0.0.0.0 - este host
- 127.0.0.0 - loopback
- 255.255.255.255 - broadcast
- x.x.255.255 - broadcast na subnet x.x.0.0/16
- x.x.0.0 - subnet x.x.0.0/16

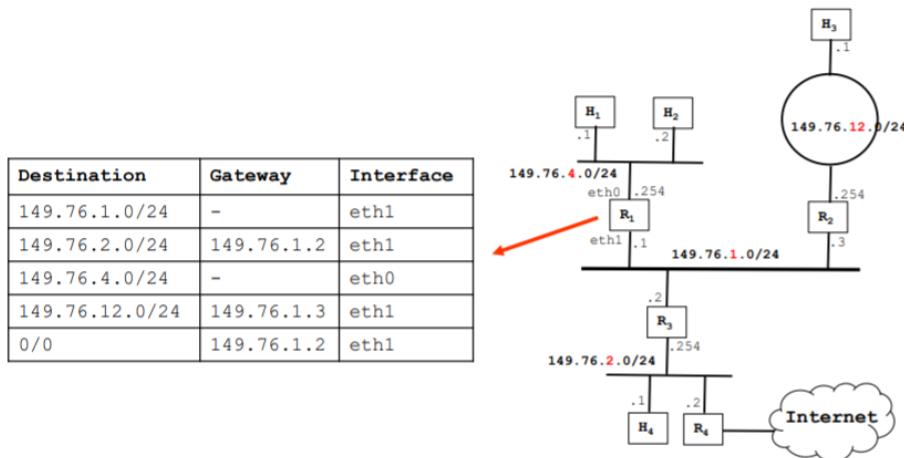
De Notar: - Uma subrede xx.xx.xx.0/24 suporta 255 endereços, no entanto, dois já estão reservados (xx.xx.xx.0 e xx.xx.xx.255), logo só suporta 253 máquinas.

Forming Sub-Networks (importante)

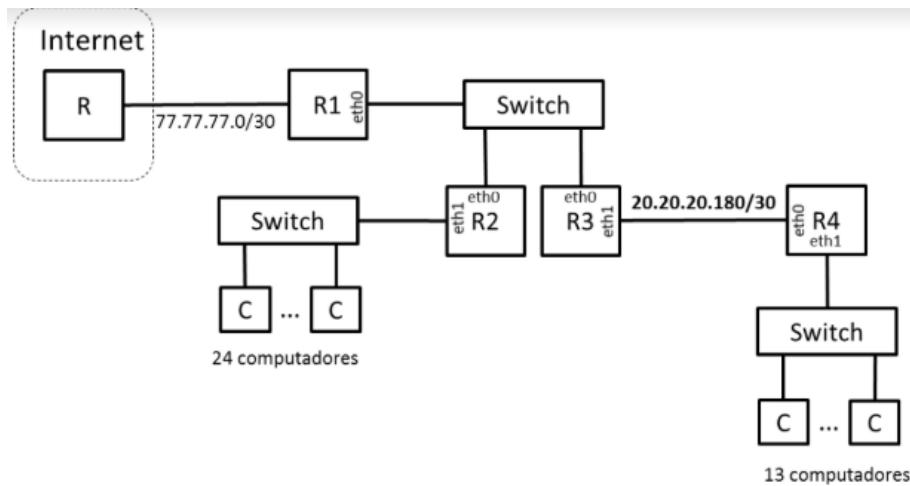
Network **192.228.17.0/24** is divided in **8 subnetworks** → masks of 27 bits



Criar table em R1 (importante)



Exercício: Exame 2018R-ultima questao (3) Considere que a uma empresa foi atribuído o bloco de endereços IP 20.20.20.128/26. A empresa tem um rede de comunicações com a arquitetura descrita na figura, composta por 4 routers (R1, R2, R3, R4) e 3 switches Ethernet. Um dos switches serve 24 computadores, outro serve 13 computadores e o terceiro interliga os routers R1, R2 e R3. Os routers R3 e R4 estão interligados por uma ligação ponto-a-ponto, à qual foi atribuído o endereço de rede 20.20.20.180/30.



a) Calcule os endereços de rede associados às redes indicadas

	Endereço da subrede (endereço/máscara)	Endereço de broadcast da subrede	Nº de endereços de interfaces
Rede dos 24 computadores	20.20.20.128/27	20.20.20.159	30
Rede dos 13 computadores	20.20.20.160/28	20.20.20.175	14
Rede dos routers R1, R2 e R3	20.20.20.184/29	20.20.20.191	6

b) Atribua endereços IP às interfaces dos routers R1, R2, R3 e R4. Use os endereços mais baixos de cada sub-rede. Numa sub-rede atribua os endereços mais baixos aos routers de índice Ri mais baixo. Por exemplo, o endereço de R3.eth1 deverá ser inferior ao endereço R4.eth0.

Router.interface	Endereço(s) IP
R1.eth0	20.20.20.185
R2.eth0	20.20.20.186
R2.eth1	20.20.20.129
R3.eth0	20.20.20.187
R3.eth1	20.20.20.181
R4.eth0	20.20.20.182
R4.eth1	20.20.20.161

c) Escreva a tabela de encaminhamento do router R2. Este router deverá ser capaz enviar pacotes para todos os endereços IP unicast. Use o menor número possível de entradas na tabela.

Destino (endereço/máscara)	Gateway	Interface
20.20.20.128/27	-	eth1
20.20.20.184/29	-	eth0
20.20.20.180/30	20.20.20.187	eth0
20.20.20.160/28	20.20.20.187	eth0
0/0	20.20.20.185	eth0

Fazer pergunta 3 (last question) de todos os exames. É igual, apenas alterando os valores dos IPs
função IP forwarding (importante)

- ◆ Forwarding table has entries in format
 $\langle \text{networkAddress}/\text{mask}, \text{ port} \rangle$
- ◆ Forwarding function
 - » When a datagram arrives with destination address **A**, then
 - For each entry of the forwarding table
 - ◆ $\text{val} = A \& \text{ mask}^*$ (e.g., $\text{mask}=8$, $\text{mask}^*=255.0.0.0$)
 - ◆ if ($\text{val} == \text{networkAddress} \& \text{mask}^*$)
 - add corresponding output port to the set of candidate ports
 - Select the port with the largest mask → most specific route
 - » Example
 - `frdTbl={<128.32.1.5/16,1>, <128.32.225.0/18,3>, <128.0.0.0/8,5>}`
 - Datagram with destination address **A=128.32.195.1**
 - Set of candidate output ports → {1, 3, 5}.
 - Selected port → **3** ← largest mask, 18 bits

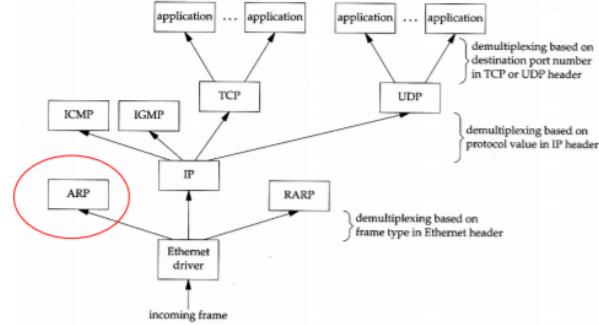
Exame 2018N - Exercicio 7

7. Admita que a tabela de encaminhamento de um router IP contém entradas no formato $\langle \text{endereçoRede}/\text{máscara}, \text{portaSaída} \rangle$ e que a tabela contém as seguintes entradas $\{<222.0.0.0/8, 1>, <222.0.0.0/16, 2>, <222.0.128.0/18, 3>\}$. Assuma que ao router chega um pacote com o endereço de destino **222.0.127.8**. Nesta situação o pacote
- É encaminhado para a porta 1.
 - É encaminhado para a porta 2.**
 - É encaminhado para a porta 3.
 - É eliminado.

1.9 Address Resolution Protocol APR

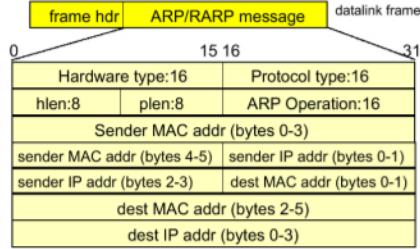
Demultiplexing

- ◆ Ethernet header (type)
 - » IP - 0x0800
 - » ARP - 0x0806
 - » RARP - 0x8035
 - » IPX- 0x8037
 - » IPv6 - 0x86DD
 - » MPLS - 0x8847
- ◆ IP header (protocol)
 - » ICMP - 1
 - » IGMP - 2
 - » TCP - 6
 - » UDP - 17
- ◆ TCP/UDP header (port)
 - » FTP - 21
 - » Telnet - 23
 - » HTTP - 80
 - » SMTP - 25

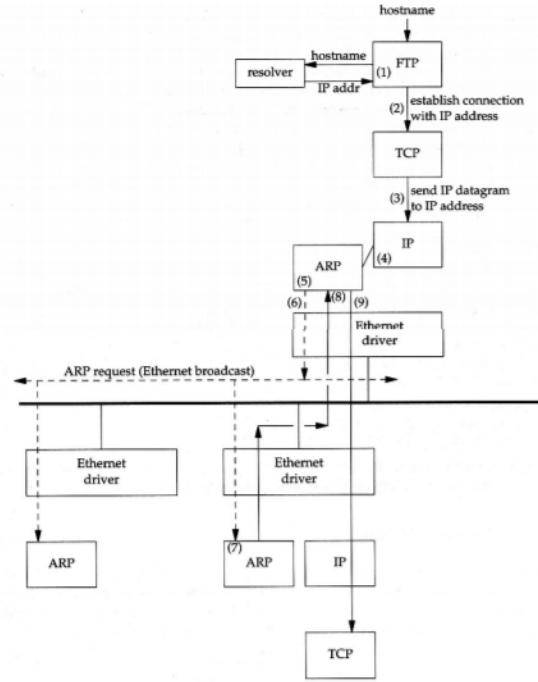


- Uma interface de rede tem 1 endereço MAC e 1 (ou mais) endereços IP
- ARP - protocolo usado para obter o endereço MAC associado a um endereço IP dado
- RARP - reverso de ARP - protocolo usado para obter o endereço IP associado ao endereço MAC

ARP Example



- hardware type : Ethernet=1 ARCNET=7, localtalk=11
- protocol type : IP=0x800
- hlen : length of hardware address, Ethernet=6 bytes
- plen : length of protocol address, IP=4 bytes
- ARP operation : ARP request = 1, ARP reply = 2
RARP request = 3, RARP reply = 4



1.10 Obter endereço IP

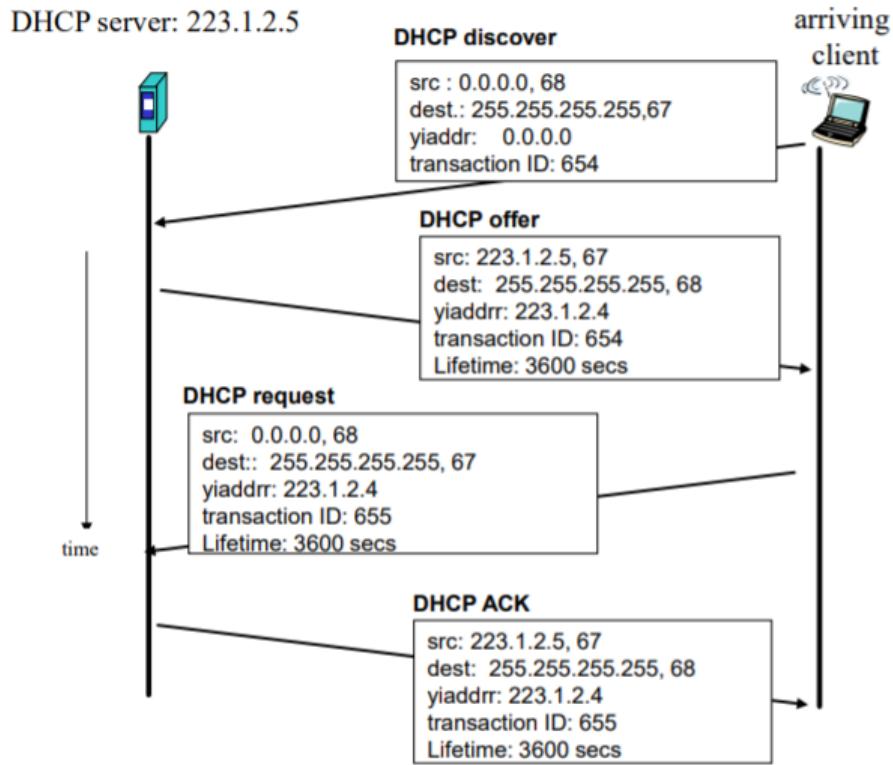
- Parte do endereço da subnet é definido pelo ISP

ISP's block	<u>11001000 00010111 00010000 00000000</u>	200.23.16.0/20
Organization 0	<u>11001000 00010111 0001<u>0000</u> 00000000</u>	200.23.16.0/23
Organization 1	<u>11001000 00010111 0001<u>0010</u> 00000000</u>	200.23.18.0/23
Organization 2	<u>11001000 00010111 0001<u>0100</u> 00000000</u>	200.23.20.0/23
...
Organization 7	<u>11001000 00010111 0001<u>1110</u> 00000000</u>	200.23.30.0/23

- endereçamento hierárquico permite eficiência da informação do router
- O ISP depois trata internamente das suas subredes
- O ISP obtém endereços pela ICANN
- ICANN: Internet Corporation for Assigned Names and Numbers
 - aloca endereços

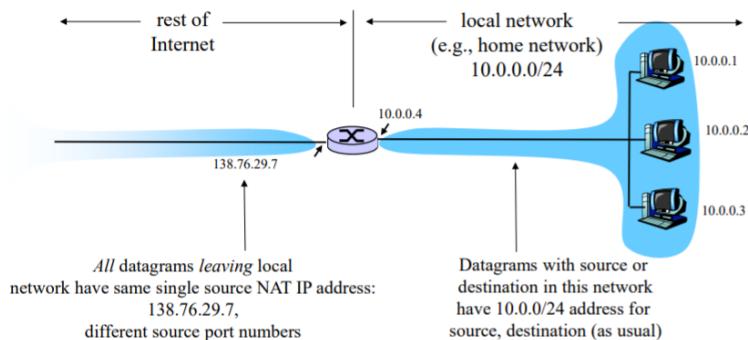
- controla o Domain Name Service (DNS)
- associa os nomes do domínio
- resolve conflitos
- o host obtém endereços IP de forma hard-coded pelo sistema admin num ficheiro ou pelo DHCP
- DHCP: Dynamic Host Configuration Protocol
 - Dinamicamente recebe endereços do servidor
 - ”plug-and-play”
 - permite descobrir e obter endereços da rede do servidor
 - reusa os endereços
 - Overview:
 - * O host faz broadcast de ”DHCP discover” (msg)
 - * O servidor DHCP oferece um endereço, enviando em broadcast ”DHCP offer” (msg)
 - * O host pede esse endereço enviando em broadcast ”DHCP request” (msg)
 - * Se tudo estiver em ordem, o DHCP responde em broadcast com um ”DHCP ACK” (msg)
 - * Todas as mensagens entre o host e o DHCP possuem um id de transação

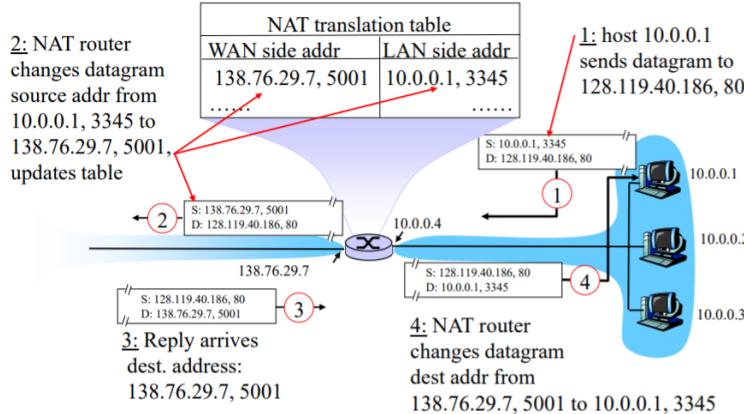
(Com o seguinte gráfico analisar pergunta 7 do exame 2018N)



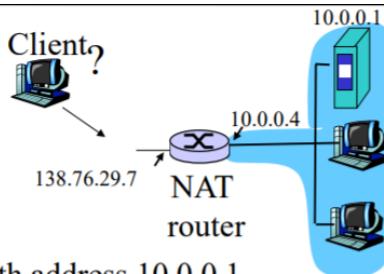
1.11 NAT - Network Address Translation

- Permite que cada computador tenha um IP interno numa rede, sendo o IP externo diferente
- Para isso, possui uma hash table a que associa um IP interno e uma porta a um número, que será a porta de saída
- Caso um cliente se queira ligar a um servidor dentro de uma rede com NAT, é necessário configurar o port forwarding





1.11.1 NAT Transversal



- ◆ Client wants to connect to server with address 10.0.0.1
 - » but server address 10.0.0.1 is private
 - » only one externally visible NATed address: 138.76.29.7
- ◆ Possible solution – **Port forwarding**
 - » statically configure NAT
 - to forward incoming connection requests at given port to server
 - » e.g., (138.76.29.7, port 2500) always forwarded to 10.0.0.1 port 25000

1.11.2 Question 8 - Exame 2017N

- Assuma que a tabela NAT de um router tem a seguinte entrada <(140.76.29.6, 80), (10.0.1.4, 8080)>. A rede privada tem o endereço 10.0.0.0/16 e existe um servidor HTTP na porta 8080 da máquina com o endereço 10.0.1.4. Nesta situação, os endereços IP e TCP de origem de um pacote observado na rede privada para este servidor são os seguintes
 - IP=140.76.29.6, Port= 80.
 - IP=140.76.29.6, Port= 8080.
 - Os endereços IP e TCP da máquina da rede pública que está a contactar o servidor.**
 - Nenhuma das anteriores.

1.12 ICMP - Internet Message Control Protocol

- Usado pelo router ou host para mandar mensagens de erro ou de controlo (como o ping)

1.12.1 Exame 2017N Ex:1

1. O programa **ping** usado nas aulas laboratoriais gera pacotes de informação do
- a) protocolo UDP, que por sua vez são encapsulados em pacotes IP, que por sua vez são encapsulados em tramas Ethernet.
- b) protocolo ICMP, que por sua vez são encapsulados em pacotes IP, que por sua vez são encapsulados em tramas Ethernet.
- c) protocolo IP, que por sua vez são encapsulados em tramas Ethernet.
- d) protocolo ARP, que por sua vez são encapsulados em tramas Ethernet.

1.12.2 Exame 2018N Ex:2

2. O protocolo Internet Control Message Protocol (ICMP) usa serviços oferecidos pelo protocolo
- a) TCP.
- b) UDP.
- c) IP.
- d) Ethernet 802.3.

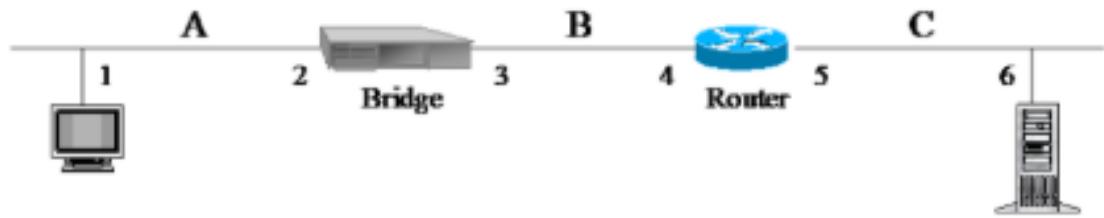
1.12.3 Exame 2016 Recurso - Ex:7

7. Assuma o seguinte cenário de ligações: $[C_1] \rightarrow [S] \rightarrow [R] \rightarrow [C_2]$. Neste cenário o computador C_1 está ligado à porta 0 do switch S, a porta 1 do switch S está ligada à porta 0 do router R, e o computador C_2 está ligado diretamente à porta 1 do router R. Nesta situação, quando o **computador C_1 envia um pacote IP com destino ao computador C_2 , os endereços IP e MAC de origem constantes do pacote recebido por C_2 são:**
- a) Endereço IP de C_1 , endereço MAC de C_1 .
- b) Endereço IP de C_1 , endereço MAC de R.porta1.
- c) Endereço IP de R.porta1, endereço MAC de C_1 .
- d) Endereço IP de R.porta1, endereço MAC de R.porta1.

1.12.4 Exame 2013 Recurso - Ex:7

7. Assuma o seguinte cenário de ligações: $[C_A] \rightarrow [L_A] \rightarrow [R_{NAT}]_{1, \text{pub}} \rightarrow [L_B] \rightarrow [C_B]$. Neste cenário, o computador C_A está ligado à porta 0 do router R_{NAT} através da LAN L_A e o computador C_B está ligado à porta 1 do router R_{NAT} através da LAN L_B . O router R_{NAT} implementa NAT e a sua porta 1 encontra-se ligada à Internet pública. Nesta situação, quando o computador C_A **envia um pacote de dados para o computador C_B , os endereços IP e MAC de origem constantes do pacote recebido em C_B são os seguintes:**
- a) Endereço IP de C_A , endereço MAC de C_A .
- b) Endereço IP de C_A , endereço MAC de $R_{NAT}.\text{porta}_1$.
- c) Endereço IP de $R_{NAT}.\text{porta}_1$, endereço MAC de C_A .
- d) Endereço IP de $R_{NAT}.\text{porta}_1$, endereço MAC de $R_{NAT}.\text{porta}_1$.

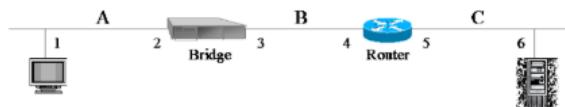
- 1.12.5 se o computador do segmento C fizer ping ao Computador do segmento A, indique os endereços IP e MAC constantes do pacote que transporta a mensagem ICMP Echo Request no segmento A. (Questão 2018R-ex:9)



R: IP origem = 6, IP destino = 1, MAC origem = 4, MAC destino = 1.

1.12.6 Exame 2014 Normal - Ex:9)

9. Na Figura seguinte, se o computador do segmento C fizer ping ao Computador do segmento A, indique os endereços IP e MAC constantes do pacote que transporta a mensagem ICMP Echo Reply no segmento B.



- a) IP_{orig}=1, IP_{dest}=6, MAC_{orig}=1, MAC_{dest}=4.
- b) IP_{orig}=1, IP_{dest}=6, MAC_{orig}=3, MAC_{dest}=4.
- c) IP_{orig}=1, IP_{dest}=4, MAC_{orig}=1, MAC_{dest}=4.
- d) IP_{orig}=1, IP_{dest}=4, MAC_{orig}=3, MAC_{dest}=4.

1.12.7 Exame 2010 Normal - Ex:4 e 5)

4. Admita que uma *bridge* transparente Ethernet / IEEE 802.3 recebe uma trama MAC com endereço de destino que não está presente na sua tabela de comutação (*forwarding table*). Neste caso a *bridge*:
- Transmite uma cópia inalterada da trama em todas as portas, com exceção da porta onde foi recebida.
 - Transmite uma cópia da trama em todas as portas, com exceção da porta onde foi recebida, após alterar o endereço de destino para *broadcast*.
 - Descarta a trama.
 - Retém a trama temporariamente, inicia um processo de resolução de endereços para localizar a estação de destino e, em caso de sucesso, actualiza a tabela de comutação e envia a trama pela porta correspondente.
5. No protocolo TCP o emissor controla uma janela de congestionamento; no inicio da sessão TCP ou após *time-out* entra-se numa fase de *slow start*, que é seguida, após se atingir um limiar, por uma fase de *congestion avoidance*.
- A janela do emissor aumenta durante *slow start* e mantém-se constante durante *congestion avoidance*.
 - A janela do emissor aumenta mais rapidamente durante *slow start* do que durante *congestion avoidance*.
 - A janela do emissor aumenta mais lentamente durante *slow start* do que durante *congestion avoidance*.
 - A janela do emissor aumenta rapidamente durante *slow start*; ao entrar na fase de *congestion avoidance* a janela é reduzida a metade, após o que aumenta mais lentamente até se atingir de novo o limiar (e o processo repete-se).

1.12.8 IP datagramas info:

♦ Carried in IP datagrams

Type	Code	Checksum	Unused
IP Header + 64 bits of original datagram			

(a) Destination Unreachable; Time Exceeded; Source Quench

Type	Code	Checksum	Unused
IP Header + 64 bits of original datagram			

(b) Parameter Problem

Type	Code	Checksum	Gateway Internet Address
IP Header + 64 bits of original datagram			

(c) Redirect

Type	Code	Checksum	Identifier
Optional data			

(d) Echo, Echo Reply

Type	Code	Checksum	Identifier
Sequence Number			

(e) Timestamp

Type	Code	Checksum	Identifier
Sequence Number			

(f) Timestamp Reply

Type	Code	Checksum	Identifier
Sequence Number			

(g) Address Mask Request

Type	Code	Checksum	Identifier
Sequence Number			

(h) Address Mask Reply

Type	Code	Description
0	0	echo reply (ping)
3	0	dest. network unreachable
3	1	dest host unreachable
3	2	dest protocol unreachable
3	3	dest port unreachable
3	6	dest network unknown
3	7	dest host unknown
4	0	source quench (congestion control - not used)
5	0	Redirect
8	0	echo request (ping)
9	0	route advertisement
10	0	router discovery
11	0	TTL expired
12	0	bad IP header

62

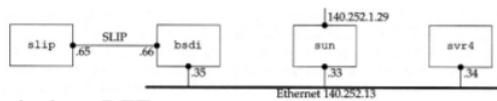
1.12.9 Tracerout and ICMP

- Permite fazer traceroute enviando mensagens com TTL=1,2,3... e esperando respostas de erro "TTL expired" até receber um "Host unreachable"

- ◆ Source sends series of UDP segments to destination
 - » first segment has TTL =1
 - » second segment has TTL=2, ...
 - » unlikely port number
- ◆ When nth datagram arrives to nth router
 - » router discards datagram
 - » sends to source:
 - ICMP TTL expired
 - message includes router name & IP address
- ◆ When ICMP message arrives, source calculates RTT
- ◆ Traceroute does this 3 times for each TTL
- ◆ Stop criterion
 - » UDP segment eventually arrives at destination host
 - » Destination returns ICMP “dest port unreachable” packet
 - » source stops

```
svr4% traceroute slip
traceroute to slip (140.252.13.65), 30 hops max. 40 byte packets
1 bsdi (140.252.13.35) 20 ms 10 ms 10 ms
2 slip (140.252.13.65) 120 ms 120 ms 120 ms
```

```
slip% traceroute svr4
traceroute to svr4 (140.252.13.34), 30 hops max, 40 byte packets
1 bsdi (140.252.13.66) 110 ms 110 ms 110 ms
2 svr4 (140.252.13.34) 110 ms 120 ms 110 ms
```



1.12.10 ICMP Redirect

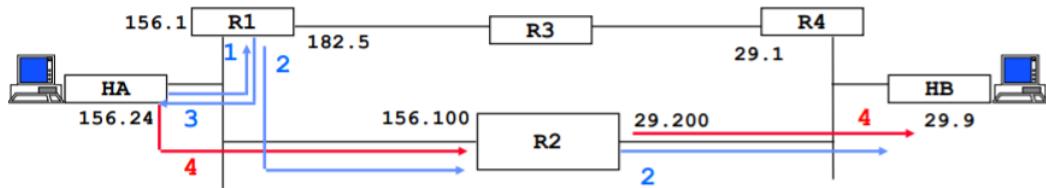
- ICMP Redirect - Permite informar outros hosts do caminho mais rápido para determinado destino

- ◆ General routing principle of the TCP/IP architecture
 - » routers have extensive knowledge of routes
 - » hosts have minimal routing information → learn routes also from ICMP redirects
- ◆ ICMP redirect message
 - » Sent by router R1 to source host A
 - when R1 receives a packet from A with destination = B, and R1
 - ◆ finds that the next hop is R2 and
 - ◆ A is on-link with R2
 - » R1 sends ICMP redirect to A saying next hop for destination B is R2
 - » A updates its forwarding table with a host route

ICMP Redirect Format

/		/
	IP datagram header (prot = ICMP)	
+	-----	-----
	Type=5 code checksum	
+	-----	-----
	Router IP address that should be preferred	
+	-----	-----
	IP header plus 8 bytes of original datagram data	
/		/

ICMP Redirect Example



dest IP addr	srce IP addr	prot	data part
1: 193.154.29.9	193.154.156.24	udp	xxxxxxxx
2: 193.154.29.9	193.154.156.24	udp	xxxxxxxx
3: 193.154.156.24	193.154.156.1	icmp	type=redir code=host cksum 193.154.156.100 xxxxxxxx (28 bytes of 1)
4: 193.154.29.9	193.154.156.24	udp
After 4			

```
HA$ netstat -nr
Routing Table:
Destination          Gateway          Flags Interface
-----              -----
127.0.0.1           127.0.0.1        UH      lo0
193.154.29.9        193.154.156.100   UGH    eth0
193.154.156.0        193.154.156.24    U      eth0
224.0.0.0           193.154.156.24    U      eth0
default              193.154.156.1        UG    eth0
```

Flags:
U - route Up
G - route to a Gateway (next hop router)
H - route to a Host

67

1.13 IPv6

- IPv4
 - espaço reduzido de endereçamento (32 bits)
 - uso não continuo
 - o uso de algumas soluções como private networks (NAT) e classless networks (CIDR) superava os problemas acima

- IETF developed new IP version: IPv6
 - Uso dos mesmos princípios do IPv4
 - muitas melhorias
 - Header foi redefinido

1.13.1 IPv6 - Melhorias

- Endereços 128 bits (16 octets, 8 shorts). No classes
- Melhor QoS suporte (native flow level)
- funções nativas de segurança (autenticação, data encriptação)
- Autoconfiguração (Plug-n-play)
- Routing
- Multicast

1.13.2 Representação dos endereços

- 8 x 16 bit, hexadecimal, separados por:
47CD : 1234 : 3200 : 0000 : 0000 : 4325 : B792 : 0428
- formato comprimido:
FF01:0:0:0:0:0:43 -; FF01::43
- compatibilidade com IPv4:
0:0:0:0:0:13.1.68.3 or ::13.1.68.3
- Loopback endereço:
::1
- Prefixo de rede ”/”, igual ao IPv4:
FEDC:BA98:7600::/40 -; network prefix = 40 bits

1.13.3 Endereços Reservados

Allocation	Prefix (binary)	Fraction of Address Space
Unassigned	0000 0000	1/256
Unassigned	0000 0001	1/256
Reserved for NSAP Allocation	0000 001	1/128
Unassigned	0000 01	1/64
Unassigned	0000 1	1/32
Unassigned	0001	1/16
Global Unicast	001	1/8
Unassigned	010	1/8
Unassigned	011	1/8
Unassigned	100	1/8
Unassigned	101	1/8
Unassigned	110	1/8
Unassigned	1110	1/16
Unassigned	1111 0	1/32
Unassigned	1111 10	1/64
Unassigned	1111 110	1/128
Unassigned	1111 1110 0	1/512
Link-Local Unicast Addresses	1111 1110 10	1/1024
Site-Local Unicast Addresses	1111 1110 11	1/1024
Multicast Addresses	1111 1111	1/256

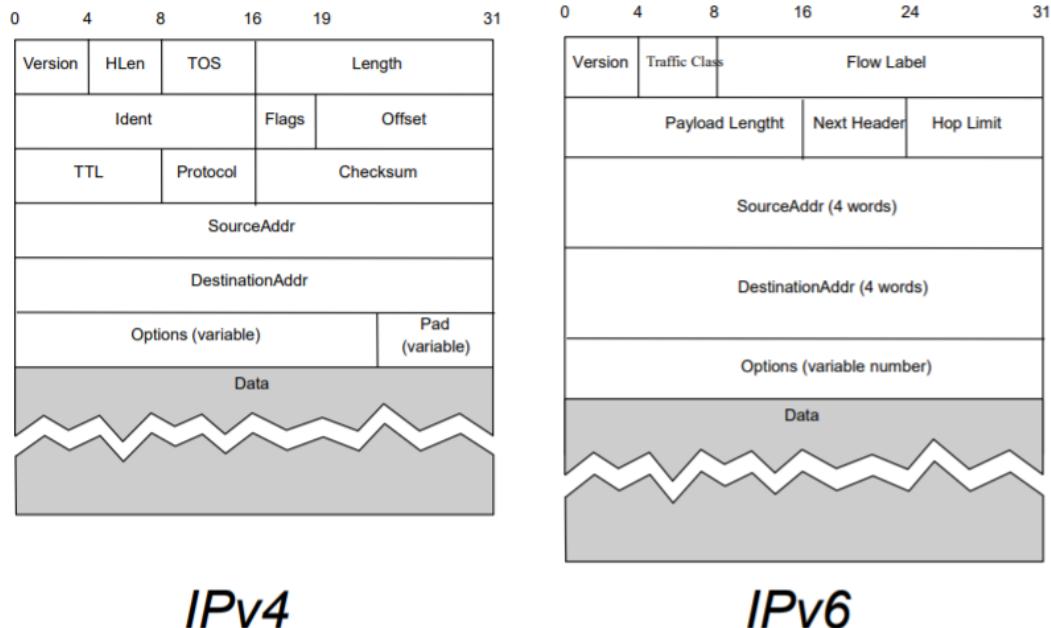
1.13.4 Tipo de Endereços

- Link-Local
 - Usado para a comunicação entre hosts na mesma LAN/link
 - Endereço criado pelo endereço MAC
 - Routers não enviam pacotes tendo endereços de destino Link-Local
- Global Unicast
 - Endereços globais
 - Endereços: prefixo de rede + identificador do computador
 - Prefixos estruturados: Agregação de rede; menos entradas nas router forwarding tables
- Anycast
 - Endereços de grupo
 - Um pacote é recebido por um e um só membro do grupo
- Multicast
 - Endereços de grupo
 - Um pacote pode ser recebido por vários membros do grupo

1.13.5 Formato dos Endereços

n bits	m bits	128-n-m bits	Global Unicast Address (2000::/3)
+-----+ 001 global rout prefix subnet ID interface ID +-----+			
10 bits	54 bits	64 bits	Link-Local Unicast address (fe80::/10)
+-----+ 1111111010 0 interface ID +-----+			
10 bits	54 bits	64 bits	Site-Local Unicast address (fec0::/10) (not used)
+-----+ 1111111011 subnet ID interface ID +-----+			
n bits		128-n bits	Anycast address
+-----+ subnet prefix 0000000000000000 +-----+			
8	4	4	Multicast address Scope - link, site, global, ... (ff::/8)
+-----+ 11111111 flgs scop +-----+		112 bits	
		group ID	

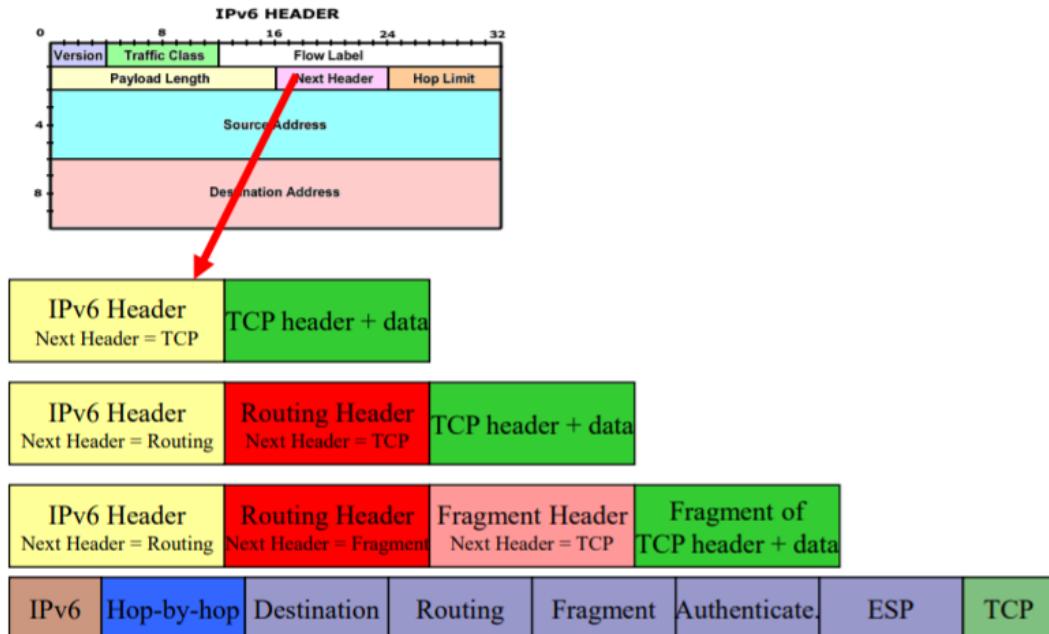
1.13.6 Headers IPv4 e IPv6



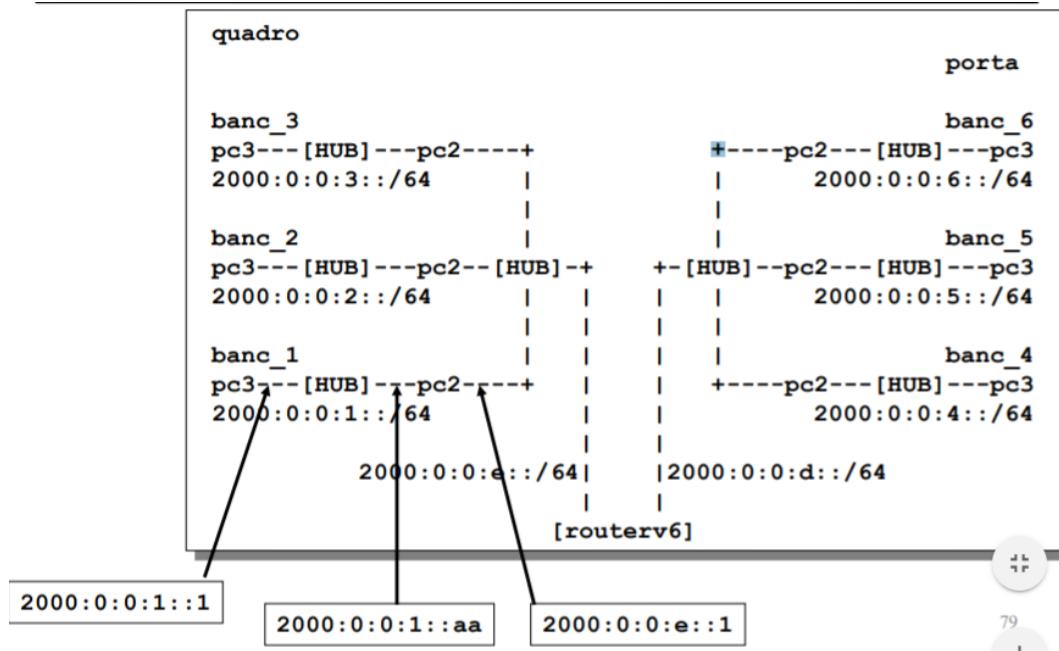
1.13.7 IPv6 Header

- Flow label - identifica o fluxo do pacote
 - QoS, ressalva de recursos
 - Pacotes recebem o mesmo serviço
- Payload lenght - Header não incluído
- Next header - identifica o próximo header/extensão
- Options - incluída nas extensões dos headers

1.13.8 Extension Headers



1.13.9 Exemplo da Rede do Laboratório



1.13.10 Protocol Neighbor Discovery (ND)

IPv6 node usa ND para:

- Encontrar outros nodes no mesmo link/LAN
- Encontrar o node do endereço MAC (ND substitui ARP)
- Encontrar routers na sua rede
- Manter/Segurar a informação sobre os nodes vizinhos

ND similar às funções IPv4:

- ARP IPv4
- ICMP Router Discovery
- ICMP Redirect

1.13.11 ND Mensagens

- ICMP mensagens (over IP), Uso de endereços Link Local
- **Neighbor Solicitation:** Enviado pelo host para obter o endereço MAC de um vizinho/para verificar a sua presença

- **Neighbor Advertisement:** resposta ao pedido
- **Router Advertisement:** Informação sobre o prefixo da rede, periodica ou abaixo do pedido. Enviado pelo router para o endereço IP do Link Local multicast
- **Router Solicitation:** Hosts solicitam do router uma mensagem Router Advertisment
- **Redirect:** Usado pelo router para informar o host acerca da melhor rota para o destino