Redes y servicios avanzados en Internet

Optativa: Redes y servicios avanzados en Internet

Licenciatura en Informática
Plan 2003-07 / Plan 2012 / Plan 2015

Licenciatura en Sistemas
Plan 2003-07 / Plan 2012 / Plan 2015

Introducción

- Sobre la cátedra:
  - Profesor: Nicolás Macia
  - Profesor: Alejandro Sabolansky
  - Adscripto: Carlos Damián Piazza Orlando
- Horario:
  - Jueves de 14 a 17 hs
- Lugar:
  - Aula 8

Régimen de cursada

- Se alternarán teorías y prácticas durante el horario de cursada

Fechas	Clase	Contenido/Actividades	Actividad Práctica
15/03/18	1	Teoria: Repaso & Intro	Práctico 1: Ruteo estático
22/03/18	2	Teoria: Ruteo Interno I	Práctico 2: Ruteo dinámico - RIP
29/03/18		FERIADO	Práctico 3: OSPF Parte 1
05/04/18	3	Teoria: Ruteo Interno II	Práctico 3: OSPF Parte 1
12/04/18	4		Práctico 3: OSPF Parte 2
19/04/18	5		Consulta
26/04/18	6	Teoria: Ruteo Externo I	Práctico 4: BGP – Parte I
03/05/18	7	Teoria: Ruteo Externo II	Práctica 4: BGP – Parte II
10/05/18	8	Consulta	
17/05/18	9	Presentación Primer Trabajo integrador	Consulta
24/05/18	10	Teoria: ISP, NAP, IXs, Tiers	Consulta
31/05/18	11		Consulta
07/06/18	12		Taller Integrador 1
14/06/18	13	Teoría: Optimizaciones de ruteo y servicios	Presentación Segundo Trabajo integrador
21/06/18	14		Consulta
28/06/18	15		Taller Integrador 2
05/07/18	16	Presentación: Trabajos finales de promoción	Test escrito
A definir	17	Exposición de trabajos finales	

Régimen de cursada

- Aprobación de cursada:
  - Entrega de ejercicios entregables de cada práctica en tiempo y forma
  - Aprobar el primer taller integrador
  - Participar del segundo taller integrador
  - Rendir un test sobre conceptos teórico/prácticos

Nota final de la materia

- El final puede aprobarse de alguna de las siguientes maneras:
  - Rendir una evaluación final de carácter teórico/práctica
  - Promoción:
    - Realizar un trabajo final sobre alguno de los temas propuestos al final de la materia
    - Exposición del mismo en clase al resto de los alumnos
    - Nota final: promedio de diversas notas (ver reglamento)

Contenidos mínimos

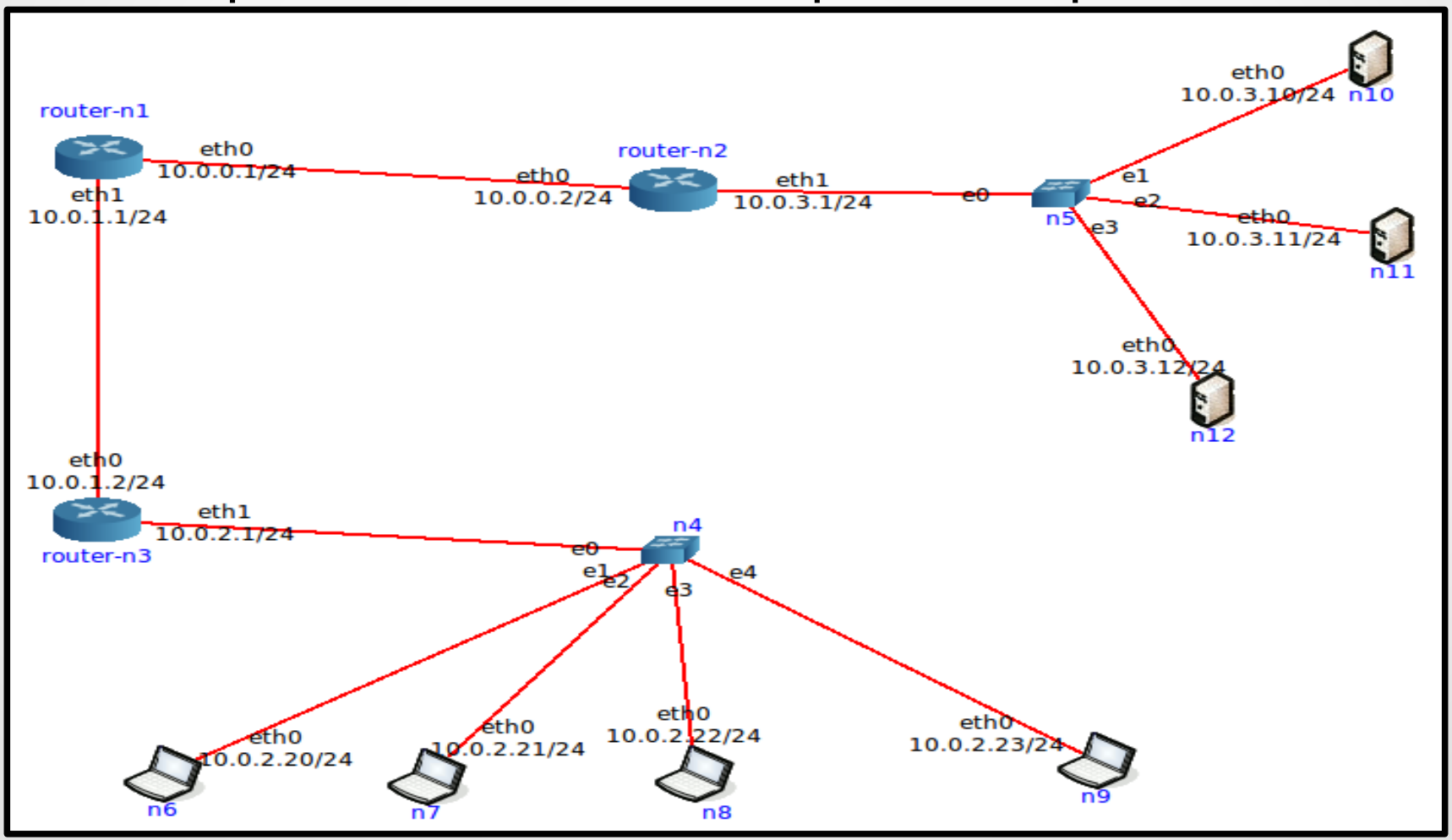
- Protocolos enrutados:
  - IPv4
  - IPv6
- Protocolos de Enrutamiento:
  - Internos
  - Externos
- Estructura de Internet: (Sistemas Autónomos / ISPs / NAP)
- Servicios distribuidos
- Optimizaciones de ruteo

Resumen

- Resumen de aspectos importantes en el funcionamiento de cualquier red
- Utilización IPv4
- Subnetting
- VLSM
- IPv6
- Herramienta a utilizar durante la cursada

Conceptos generales de redes

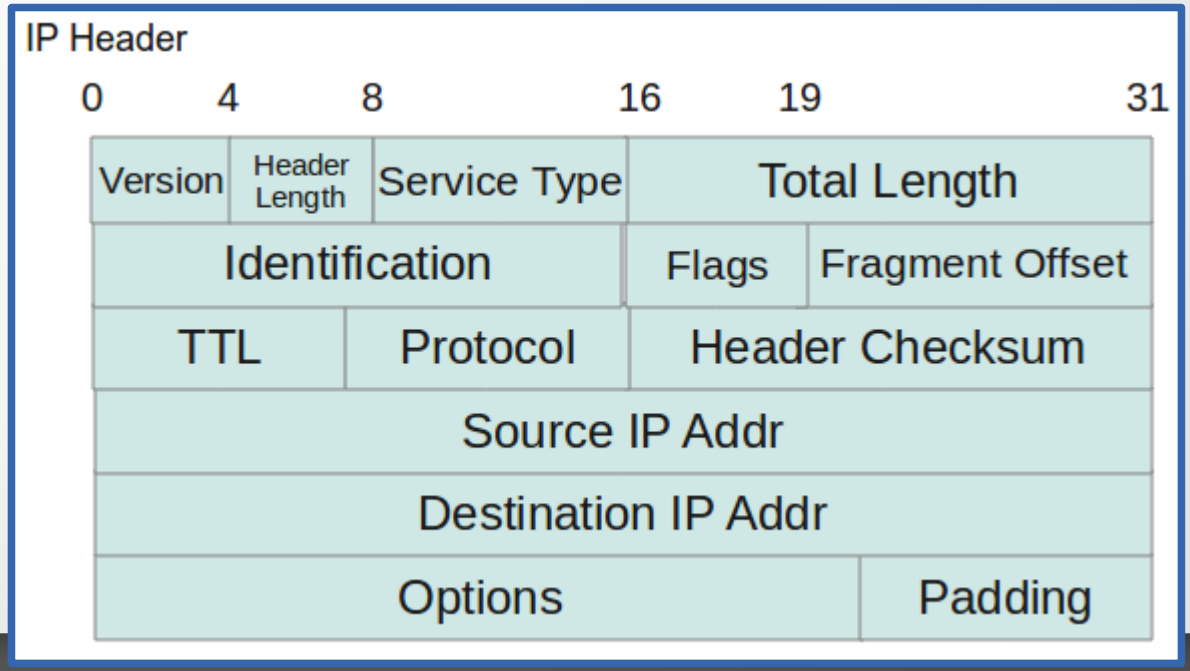
- Cuando pensamos en una red podemos pensar en:



¿Por qué funcionan las comunicaciones?

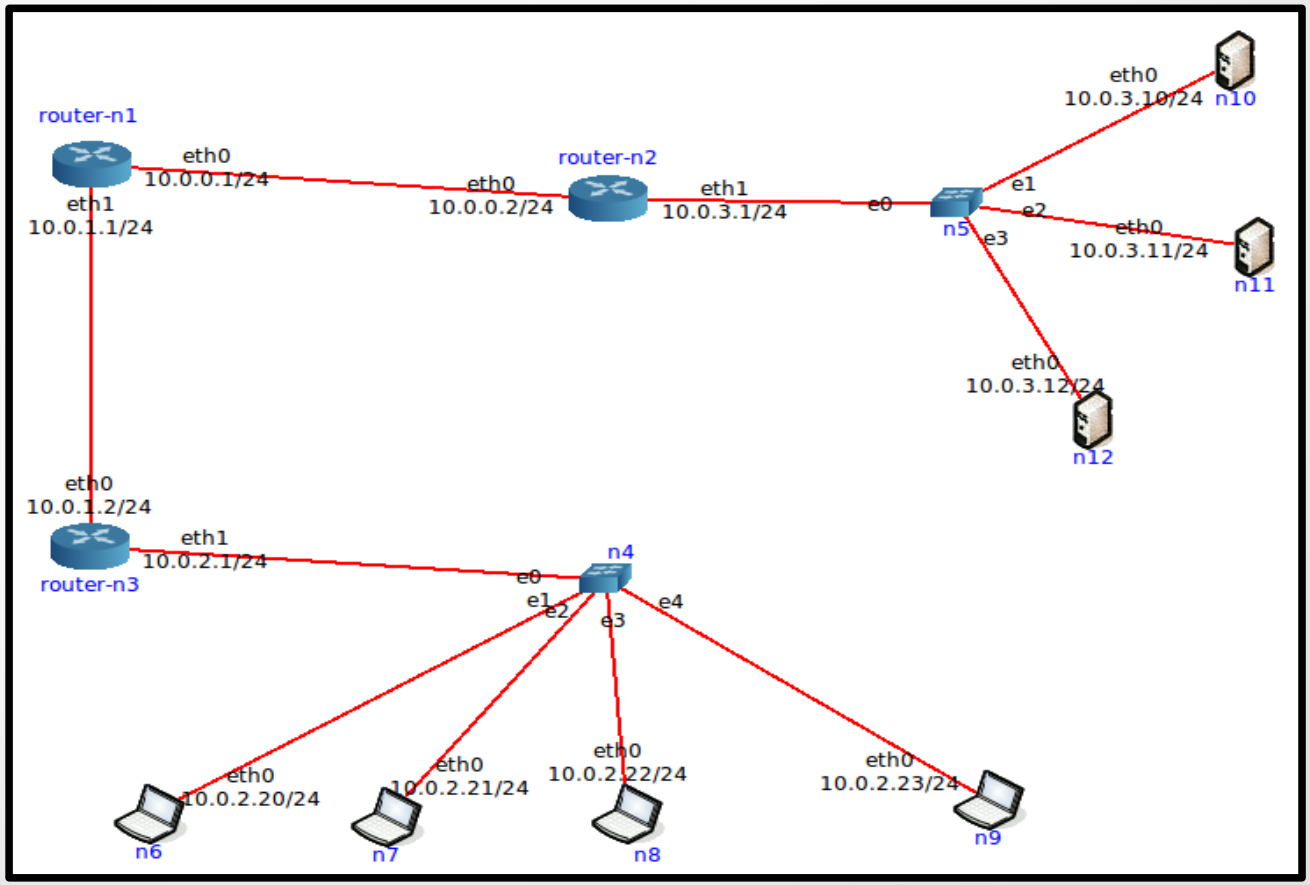
En redes y comunicaciones vimos que:

- Se usa un protocolo enrutado (IPv4)
- IPv4 hace el mejor esfuerzo para el envío de datagramas
- No hay garantías que los datagramas lleguen a destino



¿Por qué funcionan las comunicaciones?

- Para el ruteo, cada red tiene definida su dirección de red (netaddress/netmask):
  - 10.0.0.0/24
  - 10.0.1.0/24
  - 10.0.2.0/24
  - 10.0.3.0/24

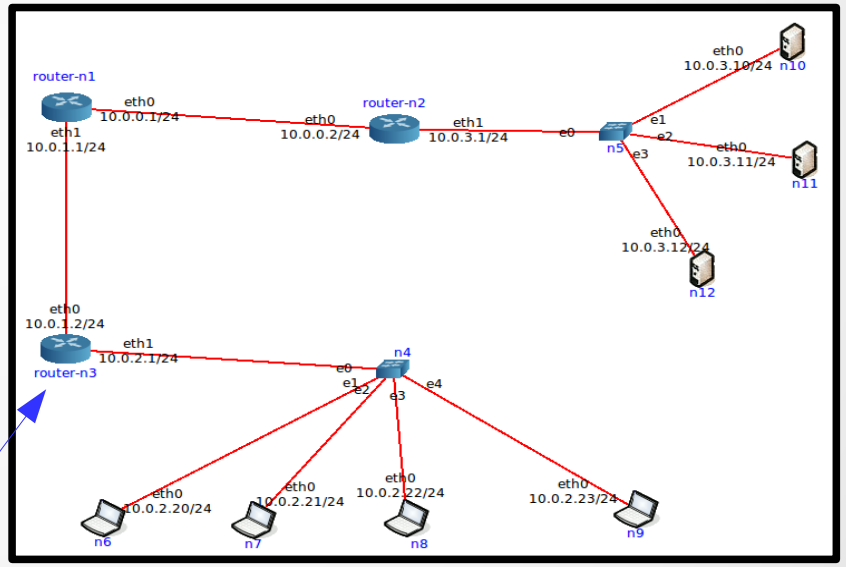


¿Por qué funcionan las comunicaciones?

- Toda dirección IP tiene una máscara de red asociada que indica si la dirección IP es:
  - de host
  - de red
  - de broadcast
- Los distintos hosts y servidores tienen configurado:
  - Dirección IP
  - Máscara de red
  - Gateway
  - Resolver (servidor de DNS)

¿Por qué funcionan las comunicaciones?

- Los routers tienen tablas de rutas que les dicen qué camino deben tomar los paquetes para les llegan:
  - Los router hacen el forwarding, los hosts no deberían
- ¿como se rutea un paquete dirigida a la IP 10.0.3.56?

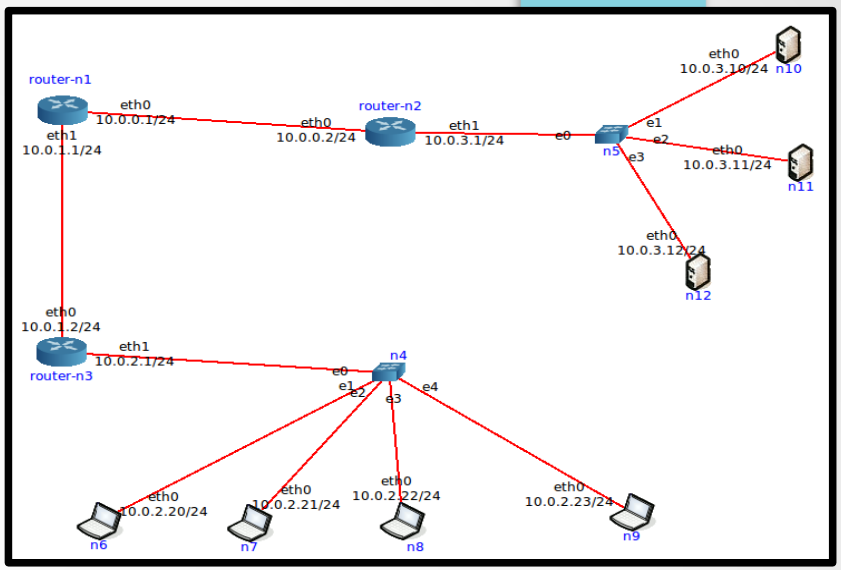



```
router n3$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
10.0.0.0        10.0.1.1        255.255.255.0   UG    20     0        0 eth0
10.0.1.0        0.0.0.0         255.255.255.0   U     0      0        0 eth0
10.0.2.0        0.0.0.0         255.255.255.0   U     0      0        0 eth1
10.0.3.0        10.0.1.1        255.255.255.0   UG    30     0        0 eth0
router n3$
```

¿Por qué funcionan las comunicaciones?

Los routers, usan la máscara de red para determinar si una dirección IP pertenece a una red o no

- ¿como ruteo la IP 10.0.3.56?



AND	10	0	3	56	← Dirección IP a consultar
	255	255	255	0	← Máscara de red
	10	**0**	**3**	**0**	← Dirección de red ???

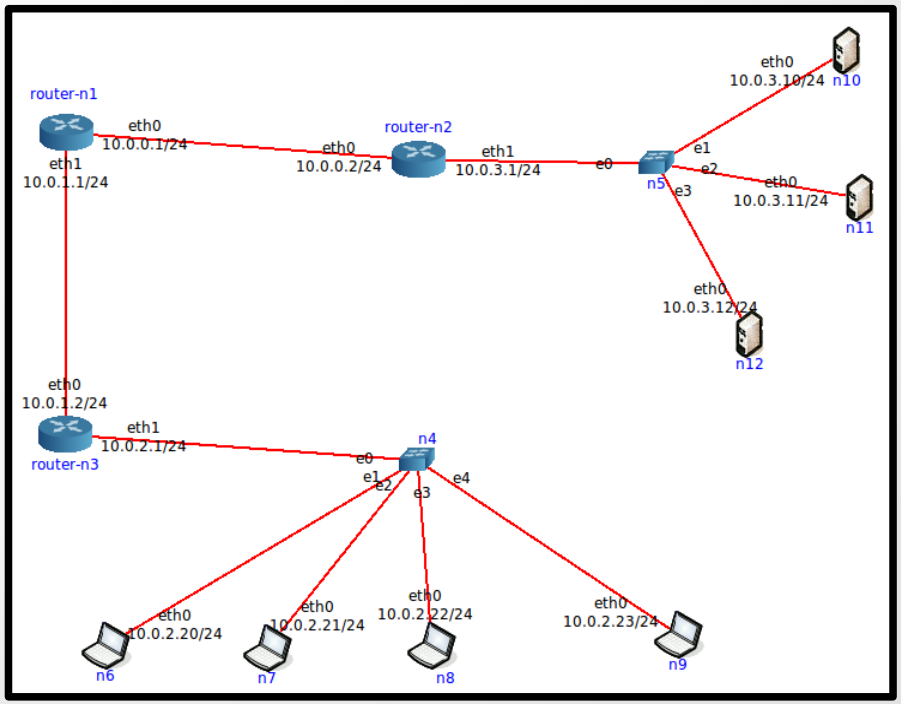
```
router n3$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
10.0.0.0        10.0.1.1        255.255.255.0   UG    20     0        0 eth0
10.0.1.0        0.0.0.0         255.255.255.0   U     0      0        0 eth0
10.0.2.0        0.0.0.0         255.255.255.0   U     0      0        0 eth1
10.0.3.0        10.0.1.1        255.255.255.0   UG    30     0        0 eth0
router n3$
```

¿Por qué funcionan las comunicaciones?

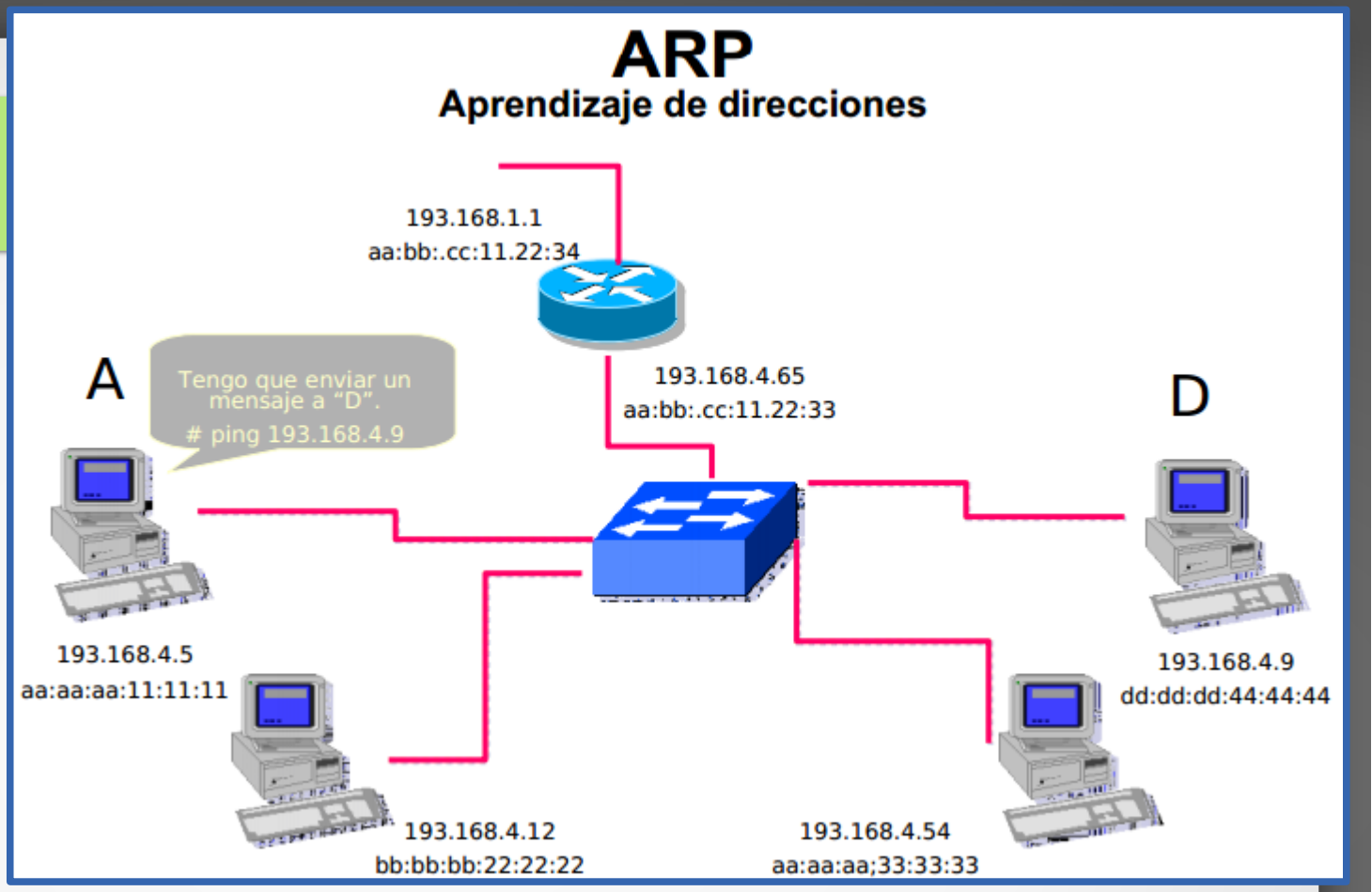
- Lo anterior ilustra el funcionamiento del ruteo de red (capa de red o layer 3), sin embargo ….
- Es también importante recordar las cuestiones de capa de enlace (layer 2) que permiten que las comunicaciones funcionen:
  - Se utilizan las direcciones MAC
  - No hay jerarquía u organización en la asignación de direcciones MAC
  - Una dirección MAC puede estar en cualquier red
  - Para que dos dispositivos dentro de la misma LAN se comuniquen necesitan conocer la dirección MAC del otro dispositivo

¿Por qué funcionan las comunicaciones?

- La capa de enlace nos permite comunicarnos con otros dispositivos que están en la misma LAN
- Existe un protocolo dinámico (ARP) para averiguar dinámicamente las direcciones MAC de otros elementos conectados a la red
  - Se utiliza el protocolo ARP



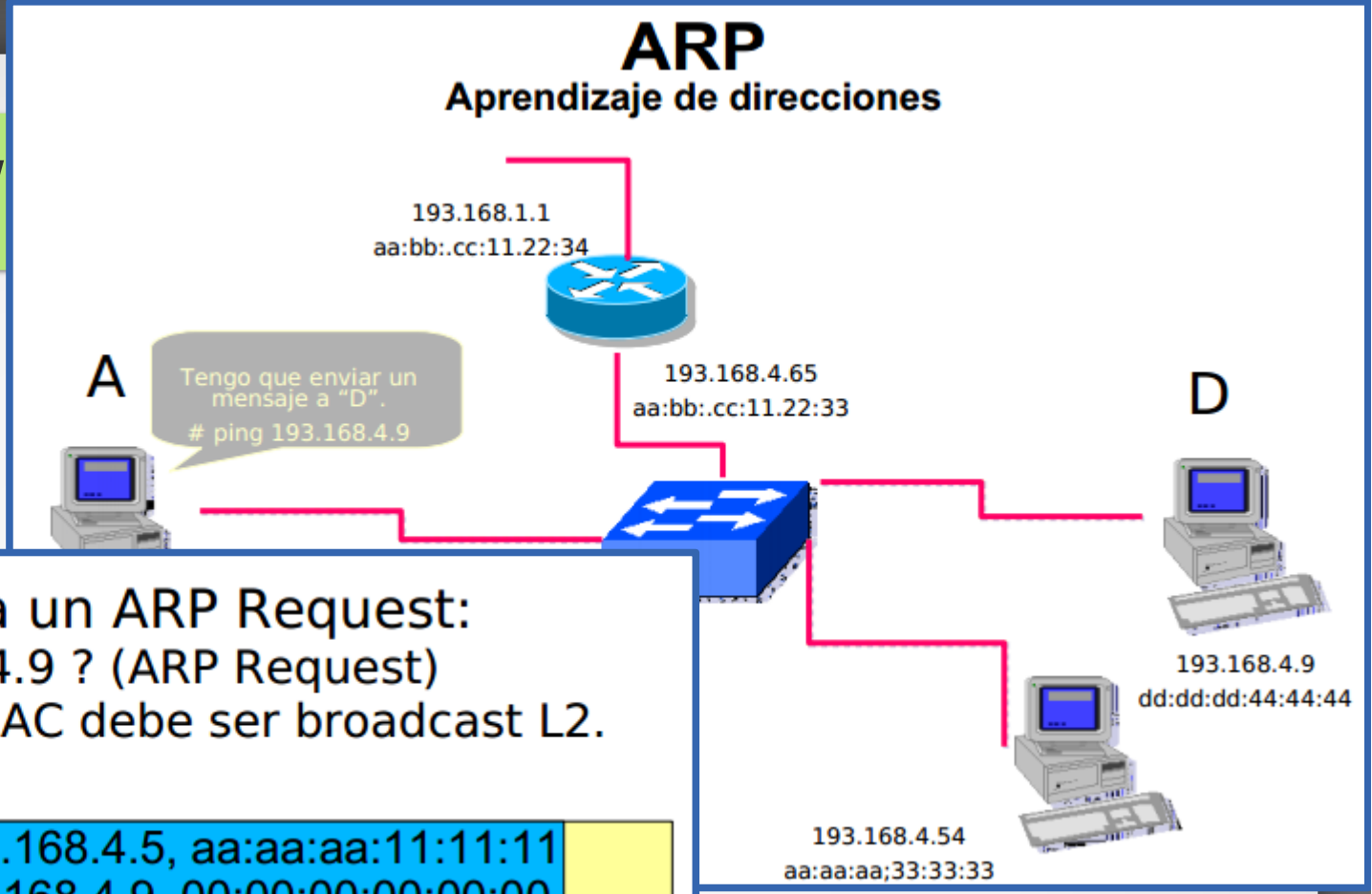
ARP




```
andres@h1(paraguil):~$ arp -a -n
(?) 193.168.4.65  at  aa:bb:cc:11.22:33 on eth0
(?) 193.168.4.62  at  <incomplete> on eth0
```

D: (?) S: aa:aa:aa:11:11:11	S:193.168.4.5 D:193.168.4.9	ICMP (echo request)	

ARP request /



- "A" debe recurrir a un ARP Request:
  - Quién es 192.168.4.9 ? (ARP Request)
  - Como no sabe la MAC debe ser broadcast L2.

D: ff:ff:ff:ff:ff:ff S: aa:aa:aa:11:11:11	YO: 193.168.4.5, aa:aa:aa:11:11:11 RQ:193.168.4.9, 00:00:00:00:00:00

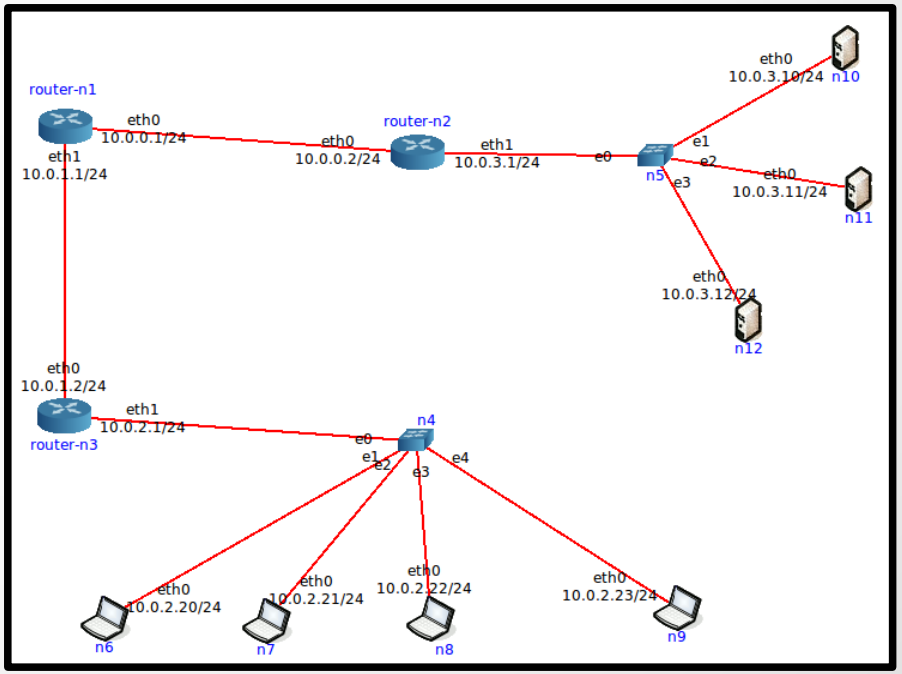
- "D" procesa el requerimiento y responde con ARP Reply:
  - Yo soy dd:dd:dd:44:44:44 de forma unicast.

D: aa:aa:aa:11:11:11 S: dd:dd:dd:44:44:44	YO: 193.168.4.9, dd:dd:dd:44:44:44 RP: 193.168.4.5, aa:aa:aa:11:11:11

```
andres@h1(paraguil):~$ arp -a -n
(?) 193.168.4.65  at  aa:bb:cc:11.22:33 on eth0
(?) 193.168.4.62  at  <incomplete> on eth0
(?) 193.168.4.9   at  dd:dd:dd:44:44:44 on eth0
```

¿Por qué funcionan las comunicaciones?

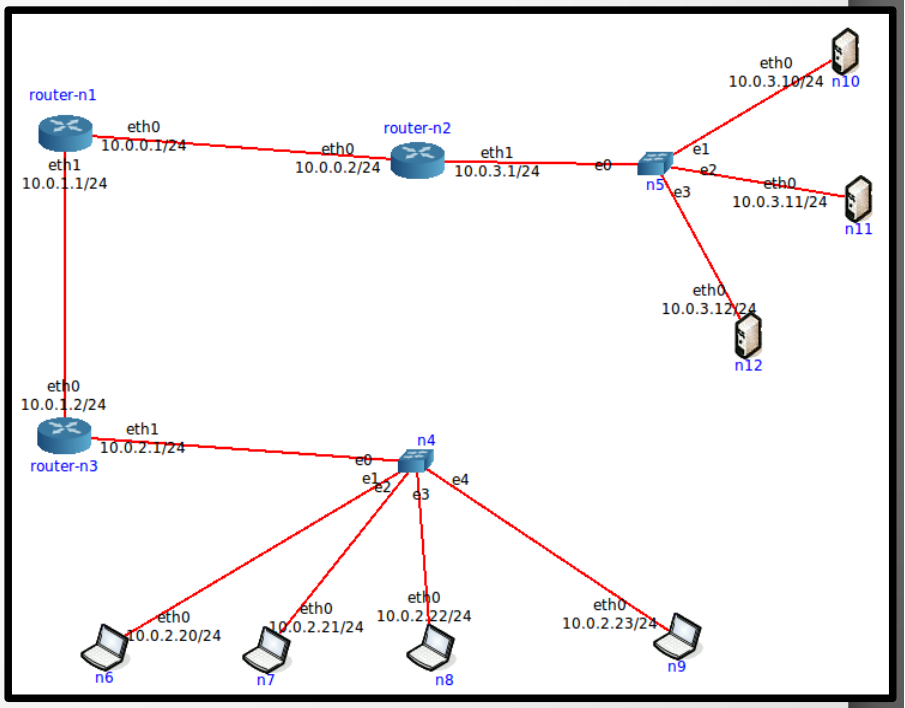
- Layer 2 y Layer 3 funcionando en conjunto
- Cuando una PC se quiere comunicar con una IP determinada, debo determinar si dicha IP está en la misma red que yo:
  - **Si lo está**, se usa ARP para averiguar la MAC de la IP destino
  - Luego puedo comunicarme directamente



D: (?) S: aa:aa:aa:11:11:11	S:193.168.4.5 D:193.168.4.9	ICMP (echo request)	

¿Por qué funcionan las comunicaciones?

- **Si no lo está en la misma red que yo**, se usa ARP para averiguar la MAC del default gateway
  - Luego se envian las comunicaciones a través del default gateway
    - Destino layer 3: *X.X.X.X*
    - Destino layer 2: MAC del default gateway

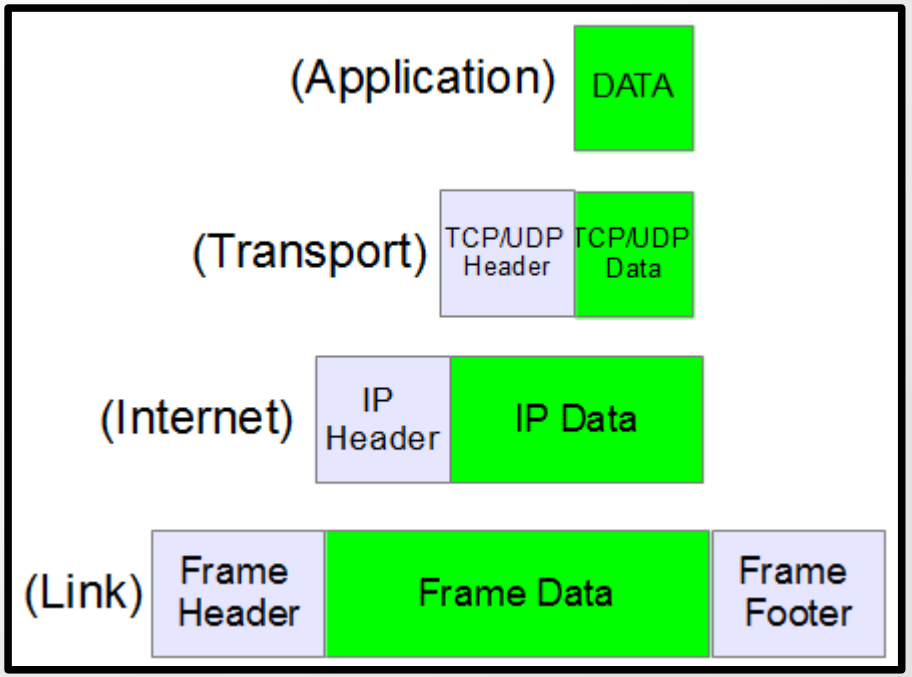


D: (?) S: aa:aa:aa:11:11:11	S:193.168.4.5 D:193.168.4.9	ICMP (echo request)	

¿Por qué funcionan las comunicaciones?

La comunicación entre distintos hosts, funciona por el trabajo en conjunto de distintos tipos de protocolos:

- Protocolos de aplicación: DNS, HTTP, SMTP, etc
- Protocolos de transporte: UDP, TCP
- Protocolos de red: IP
- Protocolos de enlace: Ethernet, ARP



¿Por qué funcionan las comunicaciones?

Por todo esto, por ejemplo, para poder realizar una comunicación HTTP, antes se tienen que dar una serie de cosas:

1) Comunicación HTTP a www.google.com → ¿quién es www.google.com?
2) Comunicación DNS a mi resolver →
   ¿Cuál es la IP de mi servidor DNS? →
   Comunicación ARP para determinar su dirección MAC

- Ethernet se utiliza para efectivamente enviar las tramas al medio

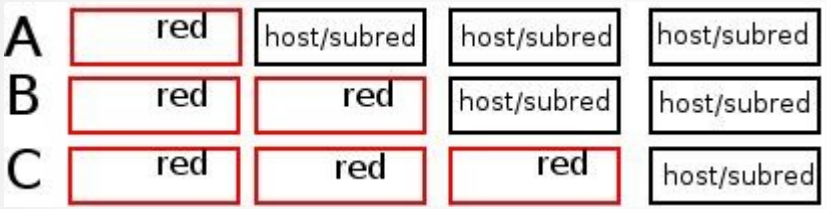
veamos la secuencia de paquetes enviados y su protocolo

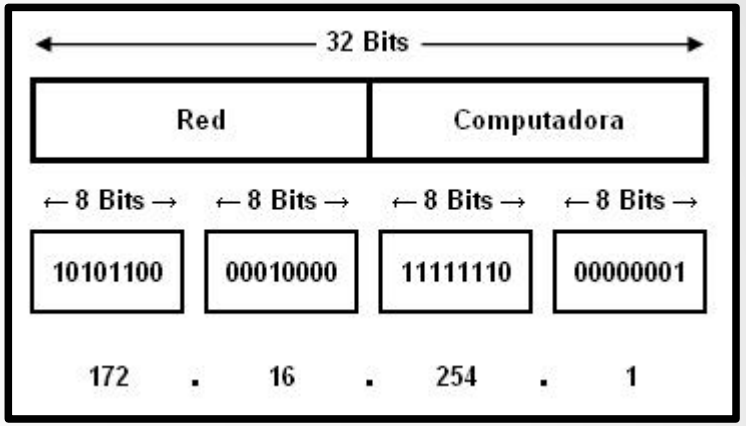
Resumen

- Resumen de aspectos importantes en el funcionamiento de cualquier red
- Utilización IPv4
- Subnetting
- VLSM
- IPv6
- Herramienta a utilizar durante la cursada

Mejor utilización de direcciones IPv4

- Las direcciones IPv4:
  - Son direcciones de 32 bits





  - Dependiendo de el tipo de dirección que sea (A, B o C) los octetos de la misma se usan para determinar la red o el host dentro de la red:

Características	Clase A	Clase B	Clase C
Rango	1 - 127	128 - 191	192 - 223
Bits del 1er octeto	00000000- 01111111	10000000-10111111	11000000-11011111
Máscara de red	255.0.0.0	255.255.0.0	255.255.255.0
Cant.hosts	16.777.214	65.534	254
N°de redes	128	16.384	2.097.152
Broadcast	x.255.255.255	x.x.255.255	x.x.x.255

Subnetting

- Es una técnica utilizada generar redes dentro de redes
- Mejora la utilización de los bloques de red
- Para llevarlo a cabo se incrementan los bits de la máscara de red, tomando bits de la porción de host
- Hay un desperdicio de direcciones IP debido a que para cada red distinta:
  - La primer dirección de la red no se puede utilizar porque es la dirección de la red propiamente dicha
  - La última dirección de la red no se puede utilizar porque es la dirección de broadcast

Ejemplo subnetting

Dado que la dirección **192.168.10.0/24** es una dirección clase **C**

3 octetos clase 1 octeto hosts

$\overbrace{192.168.10.}\ \overbrace{0}$

Con **3** bits adicionales podemos generar hasta 8 subredes.
el último octeto se separa en dos partes:

$\underbrace{xxx}_{\text{subred}}\ \underbrace{xxxxx}_{\text{hosts}}$

Máscara:255.255.255.224 o /27
Cantidad máxima de subredes: $2^3 = 8$
Cantidad máxima de hosts por red: $2^5 - 2 = 32 - 2 = 30$

Ejemplo subnetting (cont)

Subredes generadas con **3 bits**: $2^3 = 8$.

1. 00000000: 192.168.10.0/27
2. 00100000: 192.168.10.32/27
3. 01000000: 192.168.10.64/27
4. 01100000: 192.168.10.96/27
5. 10000000: 192.168.10.128/27
6. 10100000: 192.168.10.160/27
7. 11000000: 192.168.10.192/27
8. 11100000: 192.168.10.224/27

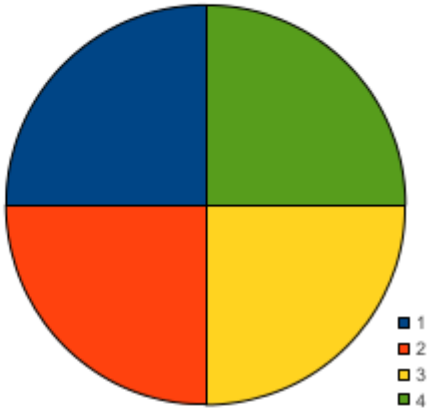
VLSM

- VLSM significa Variable Length Subnet Mask
- La longitud de la máscara no tiene que ser la misma para las distintas subredes
- Útil cuando se tienen redes con distintas cantidades de hosts
- Un ejemplo de VLSM, sería volver a realizar subnetting sobre una de las subredes generadas

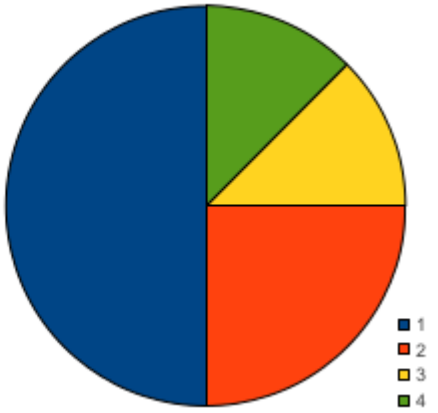
VLSM – Ejemplo gráfico

VLSM Subnetting

- Subredes iguales: /26
  255.255.255.192
  255.255.255.192
  255.255.255.192
  255.255.255.192



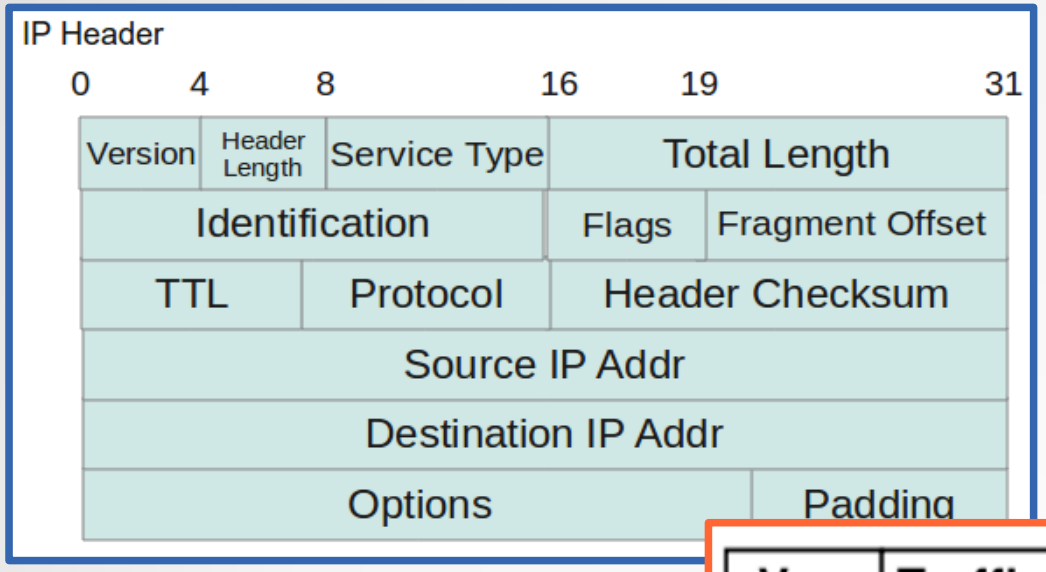
- VLSM: /25, /26, /27, /27:
  255.255.255.128
  255.255.255.192
  255.255.255.224
  255.255.255.224

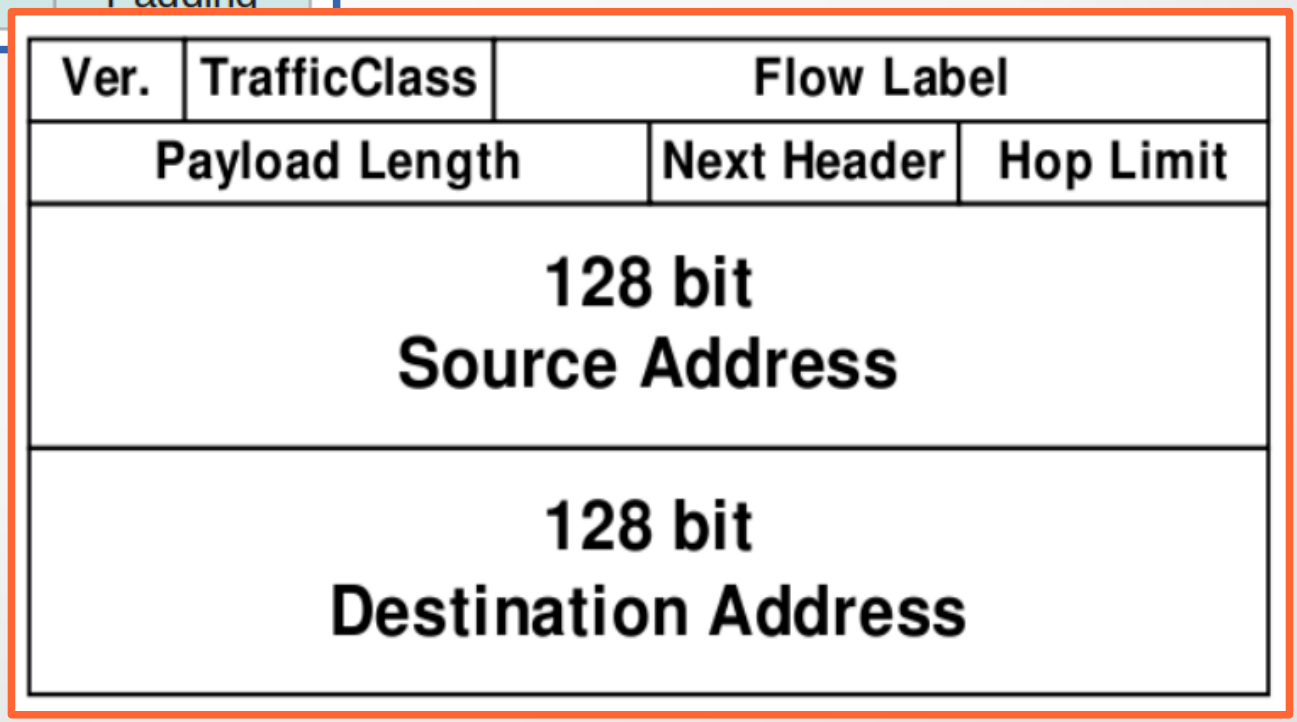


IPv6

- Debido al problema del agotamiento de direcciones IPv4, surge IPv6 como su reemplazo
- Algunos de los beneficios de IPv6:
  - Mayor espacio de direcciones (128 bits)
  - Formato de cabecera simplificado
  - Auto-configuración de direcciones (plug and play)
  - Arquitectura de red jerárquica para un ruteo eficiente

Formato de cabeceras IPv4 / IPv6



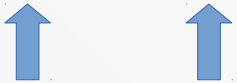


Formato de direcciones IPv6

- Direcciones de 128 bits – Se usa notación hexadecimal
- Ceros contiguos se pueden eliminar solo una vez con “::”

Dirección de alcance local:

- fe80:0000:0000:0000:c685:08ff:fe08:dbcb/64
- inet6 fe80::c685:8ff:fe08:dbcb/64 scope link



Dirección de loopback

- 0000:0000:0000:0000:0000:0000:0000:0001
- inet6 ::1/128 scope host

Tipos de direcciones IPv6

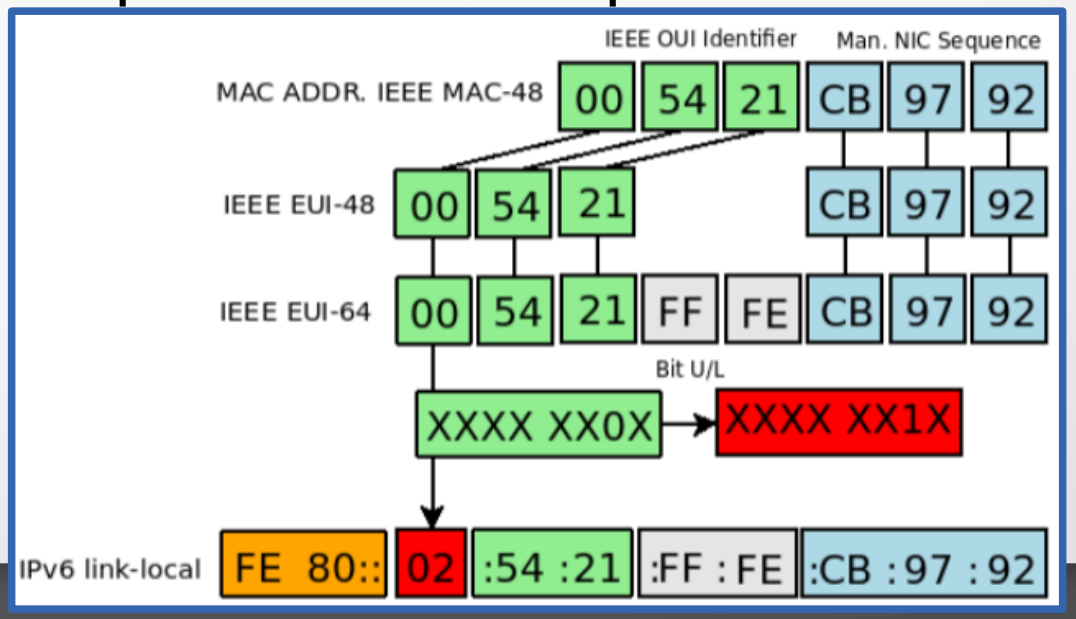
- Tipos:
  - Unicast
  - Anycast
  - Multicast (No hay broadcast): FF00::/8

- Alcance de direcciones Unicast:
  - Local: prefijo FE80::/10
  - Globales: prefijo 2000::/3

SLAAC Autoconfiguración de direcciones

Se lo conoce como SLAAC. Los 64 bits de la porción de host de la dirección se pueden crear:

- EUI-64: mediante el proceso EUI-64, a partir de la dirección MAC de 48 bits.
- De generación aleatoria: se utiliza un número aleatorio generado por el sistema operativo.

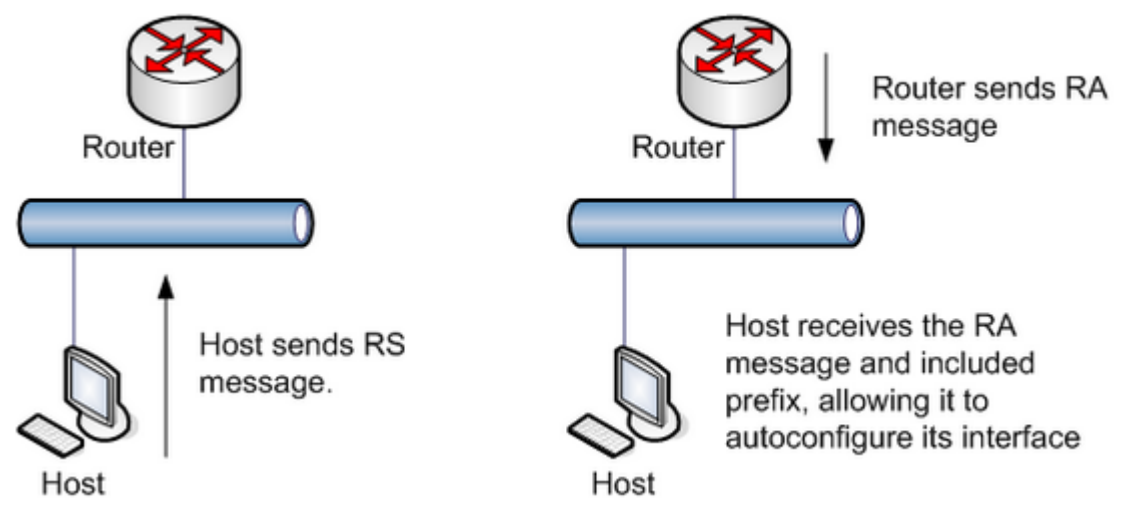


Neighbor Discovery

- El protocolo Neighbor Discovery entre otros:
  - Reemplaza a ARP:
    - Mensajes:
      - NS: Neighbor Solicitation
      - NA: Neighbor Advertisement
  - Cumple otras funciones propias de ICMP, como por ejemplo los mensajes ICMP REDIRECT

Neighbor Discovery (autoconfig)

- Reemplaza la configuración manual
- Alternativa básica al uso de DHCPv6
- Los host auto configuran su dirección local y luego su prefijo de red. Usan paquetes: RS (Router Solicitation) y RA (Router Advertisement)



Herramienta de virtualización

- Se utilizará VirtualBox como plataforma de virtualización
- Se distribuirá una máquina virtual sobre el cuál se podrán realizar todas las actividades prácticas
- Los conceptos abordados podrán ser inspeccionados mediante el uso de la herramienta CORE:
  - http://www.nrl.navy.mil/itd/ncs/products/core
  - https://code.google.com/p/coreemu/
  - https://github.com/coreemu/core

Mostrar