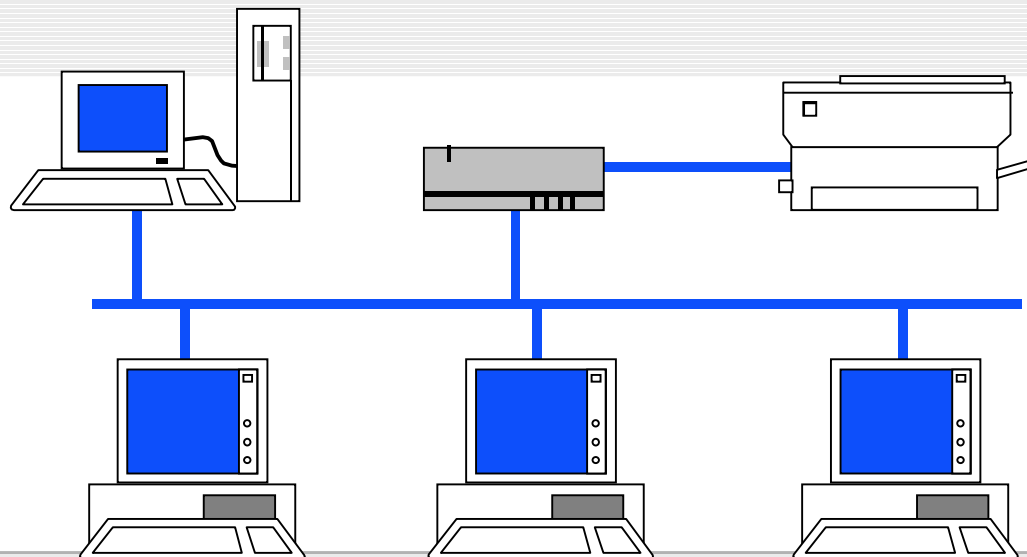
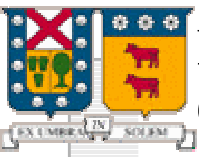


Redes de Computadores

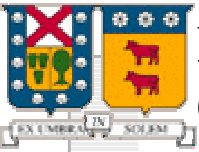
Capa de Red Internet Protocol (IP)





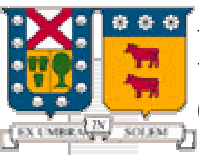
IP provee...

- Servicio sin conexión
- Direccionamiento
- Enrutamiento de Paquetes
- Fragmentación y Re-ensamble
- Paquetes de largo variable (hasta 64kb)
- Entrega de mejor esfuerzo: retardo, fuera de orden, corrupción y pérdidas son posibles. Tareas para capas superiores...

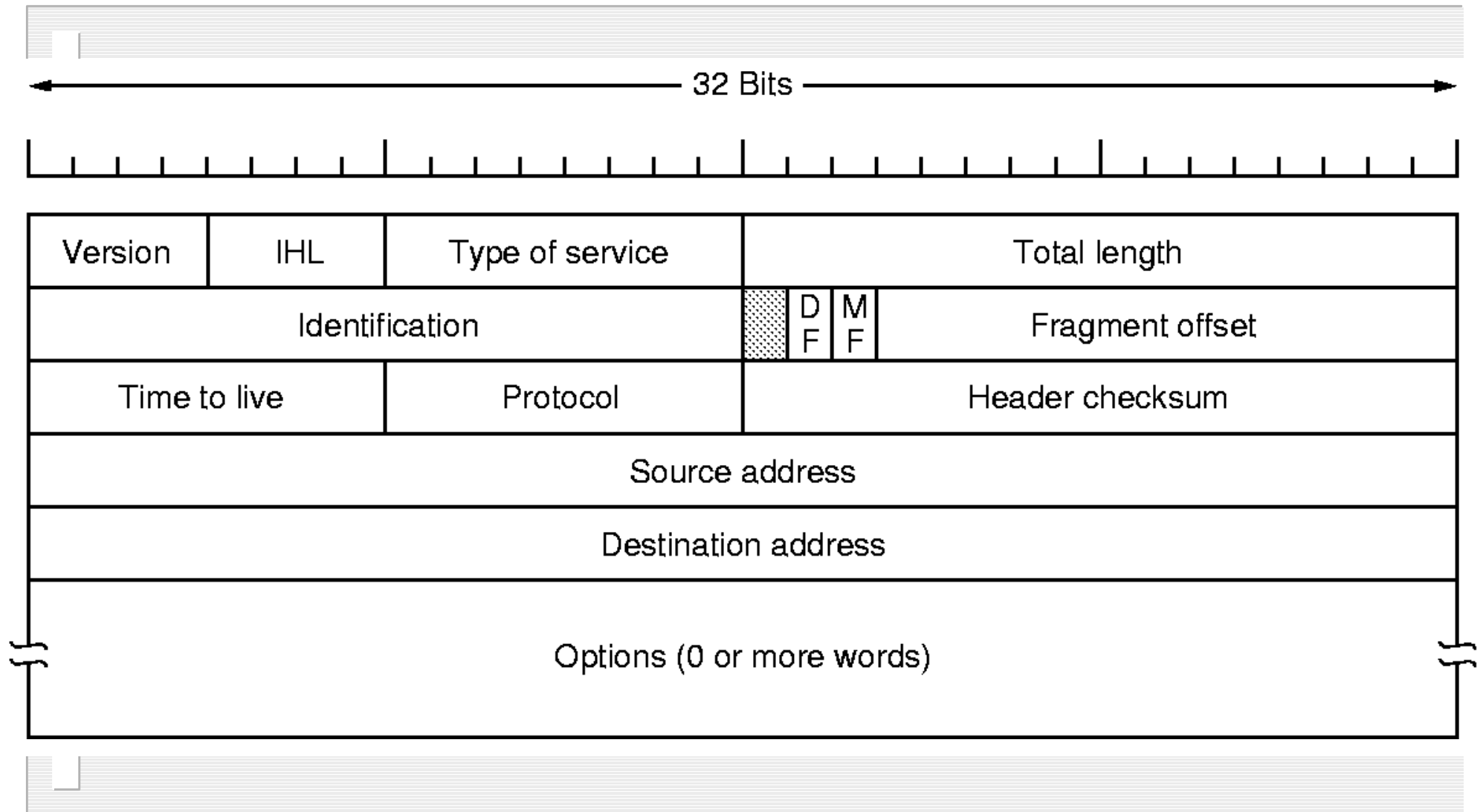


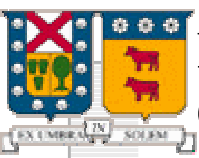
IP no provee...

- Confiabilidad ni Control de Flujo extremo a extremo (hecho por TCP o Capa Aplicación)
- Numeración de Paquetes
- Detección de errores de la data (lo hace TCP)
- Reporte de Errores (ICMP)
- Confección de Tablas de Ruteo (RIP, OSPF, BGP, etc)
- Seteo de conexión (es sin conexión)
- Resolución de Nombres (ARP, RARP, DNS)
- Configuración (BOOTP, DHCP)
- Multicast (IGMP, MBONE)



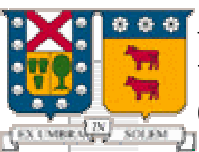
Encabezado IP versión 4 (actual)





Encabezado IP versión 4 (actual)

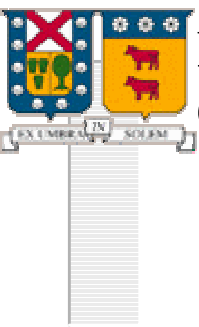
- Version: versión de protocolo IP
- IHL: largo del encabezado en palabras de 32 bits. Min=5, Max=15, limita las opciones a 40 bytes.
- Service Type: indica el tipo de servicio que se desea. Confiabilidad v/s velocidad
- Total Length: largo total del datagrama. Max=65.535 bytes
- Identification: necesaria cuando hay fragmentación (todos los fragmentos de un paquete poseen este valor idéntico)
- DF: Don't Fragment (algunos paquetes no conviene fragmentar)
- MF: More Fragment. Todos los fragmentos excepto el último poseen este bit en 1
- Fragment offset: indica donde se ubica este fragmento dentro del paquete IP. Max # fragmentos = 8192
- Time to live: limita la cantidad de routers (hops) por los cuales puede pasar
- Protocol: indica a cuál capa 4 entregarle el paquete (RFC 1700)
- header checksum: calculado en cada salto.



Encabezado IP versión 4 (actual)

Option	Description
Security	Specifies how secret the datagram is
Strict source routing	Gives the complete path to be followed
Loose source routing	Gives a list of routers not to be missed
Record route	Makes each router append its IP address
Timestamp	Makes each router append its address and timestamp

- security: opción ignorada en la práctica
- strict: indica la ruta exacta por donde debe ir el paquete
- loose: indica una lista de routers por los cuales debe pasar el paquete como mínimo
- record: campo en que cada router agrega su IP. Para debugging
- timestamp: campo en que cada router indica la hora. Para debugging.



Encabezado IP versión 6

Características

- Dirección IP de 128 bits
- Clases de direcciones basadas en topologías y subclases para NSAP, IPX e IPv4
- Mayor flexibilidad para direccionamiento multicast
- Header simplificado que privilegia ruteamiento
- Soporta mecanismos de privacidad y autenticación
- Facilidades para especificar tipo de tráfico (o tratamiento deseado).

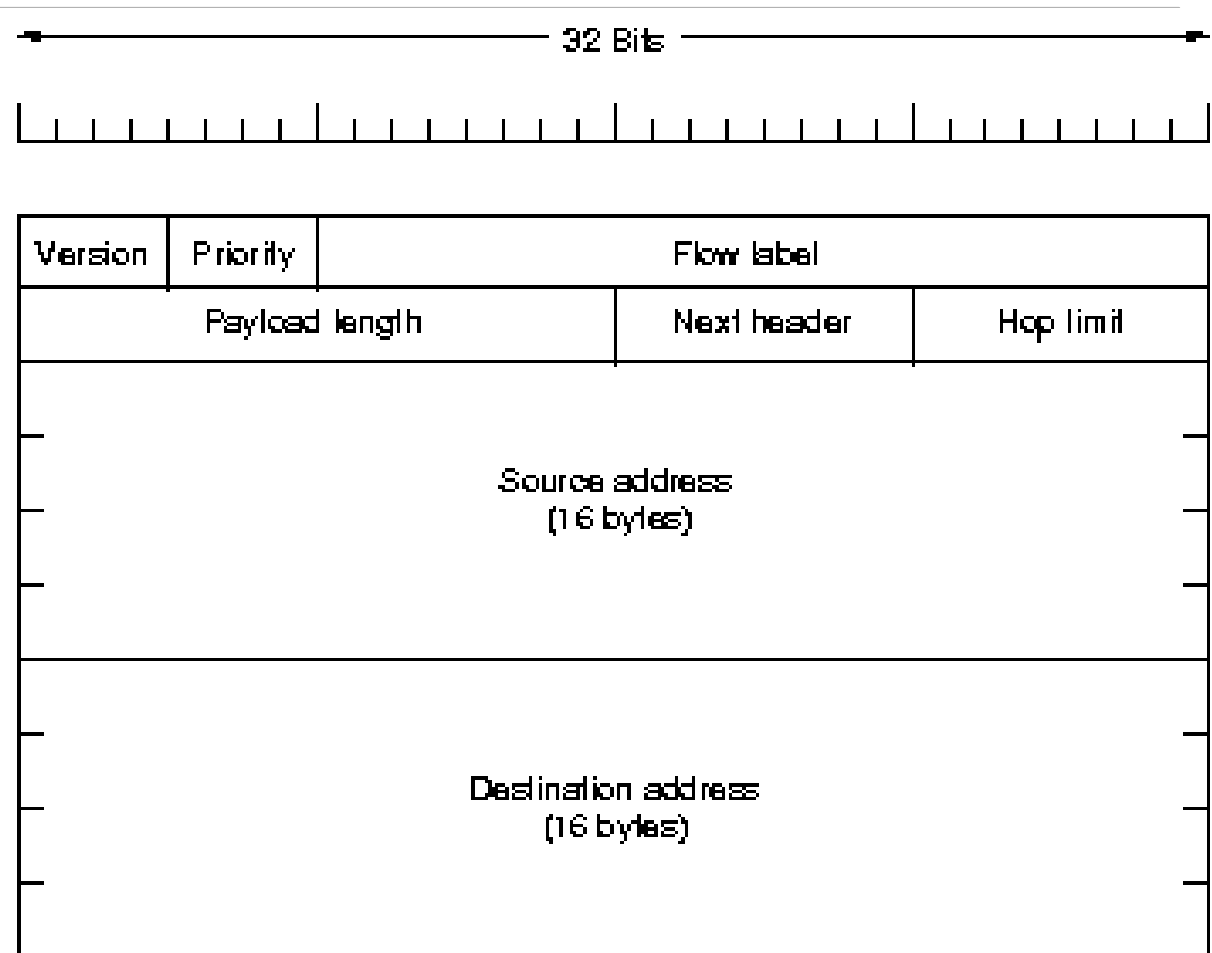
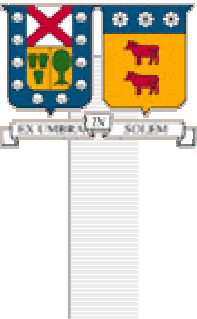


Fig. 5-56. The IPv6 fixed header (required).



Redes

Capa de Red

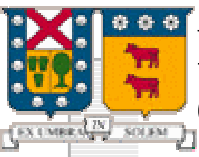
IPv4

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Version (4)				Hdr Length				Type of Service							
Total Length															
Identification															
0	D	M	Fragment Offset												
Time to Live								Protocol							
Header Checksum															
Source Address															
Destination Address															
Options															
Data															

IPv6

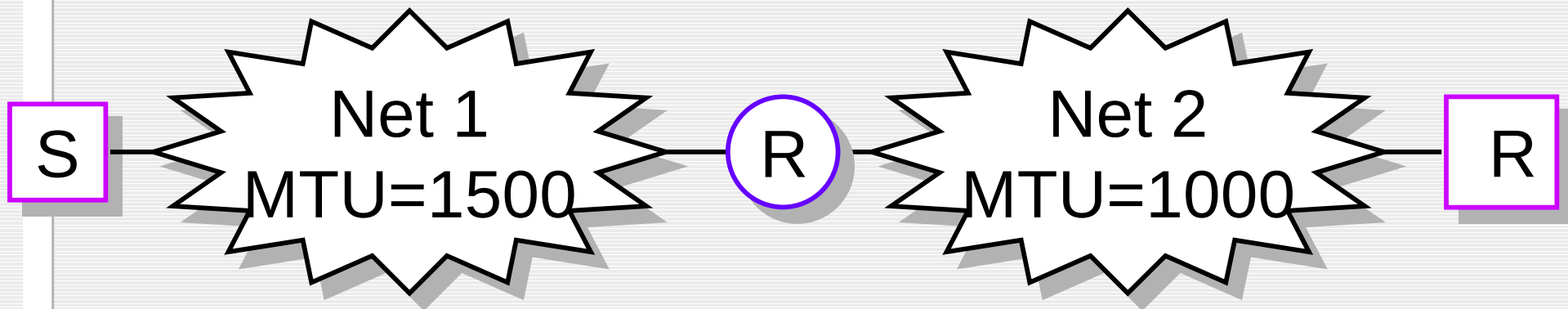
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Version (6)				Flow Label											
Flow Label															
Total Length															
Next Header								Time to Live							
Source Address															
Destination Address															
Other Headers															
Data															

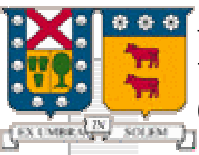
Comparación



MTU

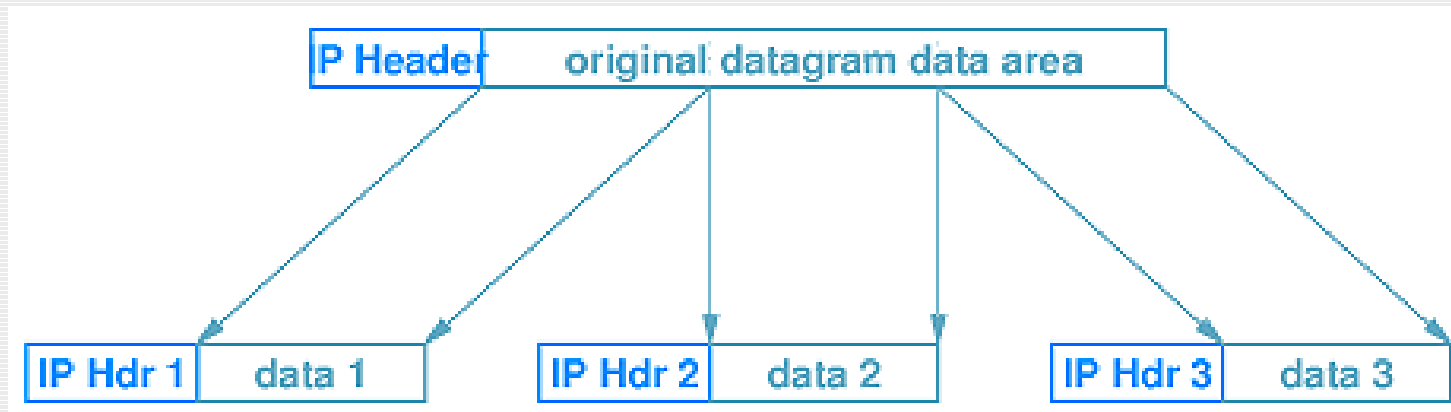
- Cada red LAN posee un tamaño máx. de frame
 - Ethernet: 1522 bytes (802.1Q)
 - FDD: 4500 bytes
 - Token Ring: 2 a 4 Kb
- Cada subred ajusta su tamaño máx de paquete a la MTU de su red LAN

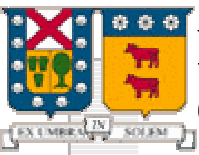




Fragmentación

Fragmentación debido a que redes (Capa 2) intermedias poseen MTU (Maximum Transfer Unit) diferentes

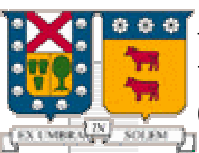




Router Multiprotocolo

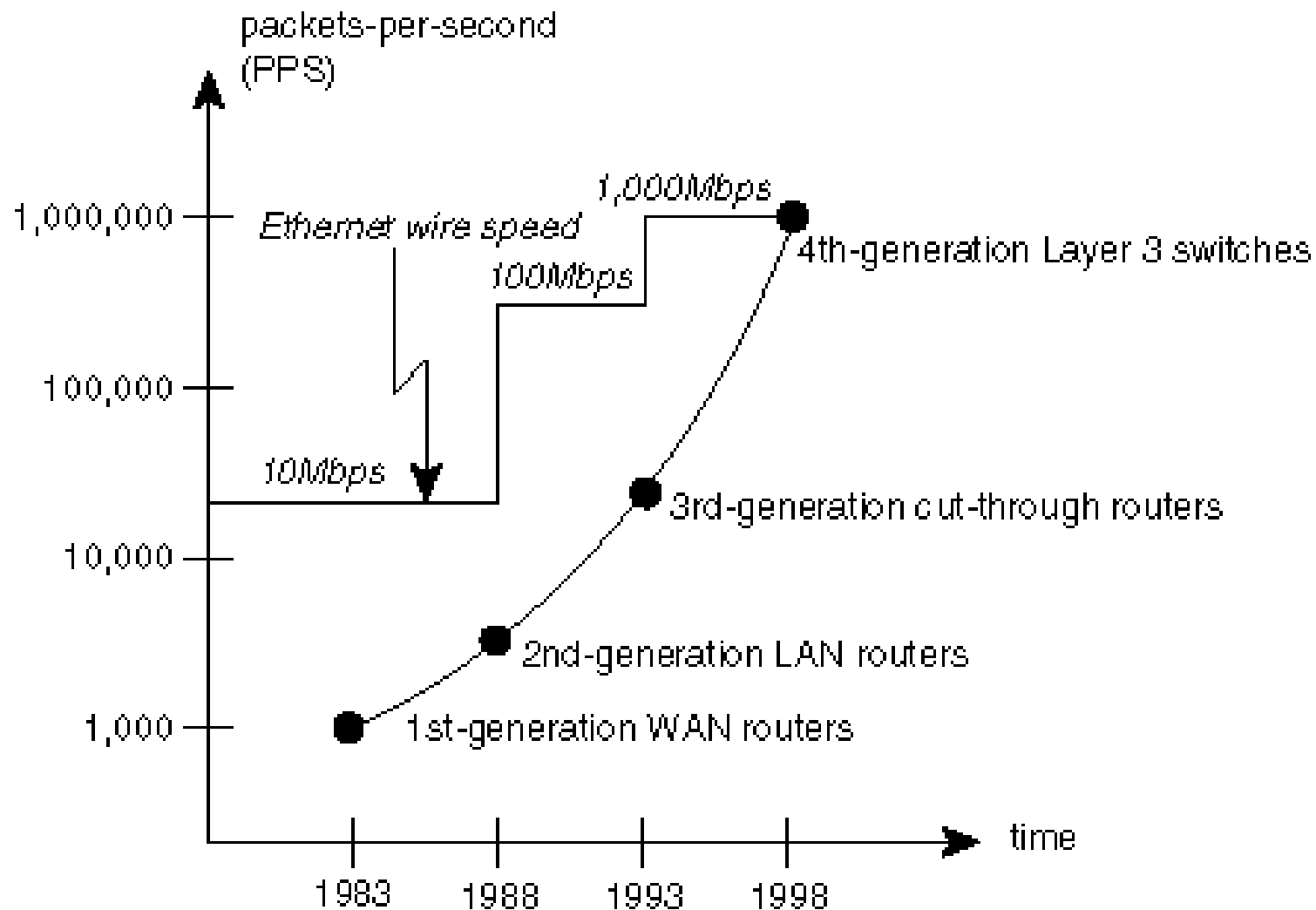
- Pueden comunicar redes de diferente capa 3.
- Generalmente realizan tareas de bridging convirtiendo entre redes LAN y WAN de capa 2.

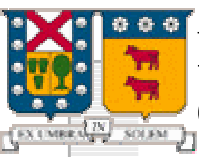
Protocolo			productos	enrutable?
IP	Internet Protocol	IETF Open Standard	todos	si
IPX	Internetwork Protocol Exchange	Novell	NetWare	si
Appletalk	Apple	Apple	Mac PC y Servers	si
NetBIOS	Network Basic Input/Output System	Microsoft, IBM	Windows, LAN Manager, IBM LANServer	no
NetBEUI	NetBIOS Extended User Interface	MS, IBM	Windows, LAN Manager, IBM LANServer	no
SNA	Systems Network Architecture	IBM	Mainframes	no
DECnet	DEC Network	Compaq	Alpha, VAX	si
LAT	Local Area Transport	Compaq	Alpha, VAX	no



Routing Performance

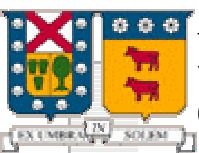
Switches
Layer 3
pueden
rutear
paquetes a
velocidad
de “cable” o
de TX.



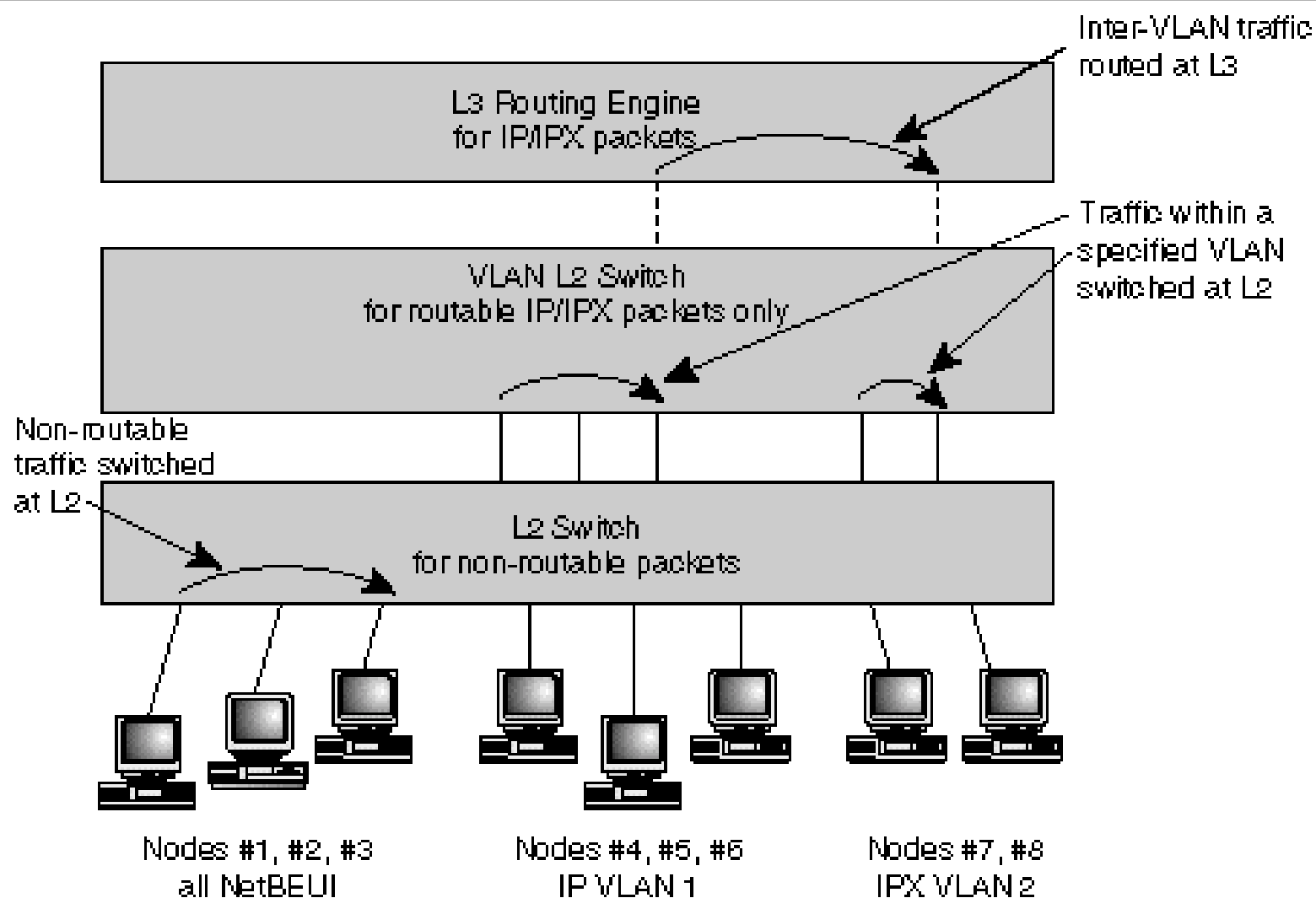


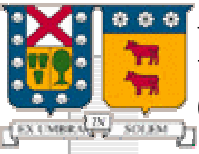
Router v/s Switch Capa 3

característica	Router clásico	Switch Layer 3
Capa OSI	3	3
ruteamiento hecho en	CPU + software	Hardware (chips ASIC)
Layer 2 soportadas	Ethernet, Token Ring, FDDI, ATM, WAN	Fast y Gigabit Ethernet
Performance	lento a medio, depende de CPU y memoria	rápido, cercano a velocidad de TX
precio/puerto	alto	bajo
latencia	app. 200us	< 10us (100Mbps)
programabilidad	muy alta	poco a nada
protocolos soportados	todos	IP, a veces IPX
protocolos de intercambio rutas	todos	RIP, RIPv2, a veces OSPF y DVMRP
Uso	division de dominio de broadcasts	ruteamiento IP rápido
	conecction WAN	ruteamiento entre VLAN
	ruteamiento multiprotocolo	



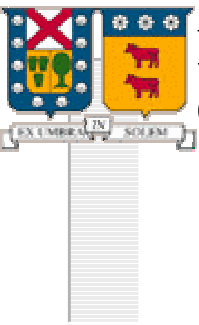
Operación de un Switch Capa 3





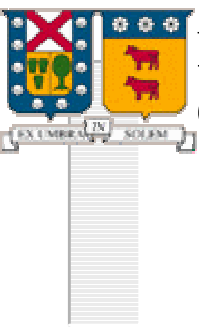
Internet Control Protocols

- En TCP/IP existen varios protocolos anexos que ayudan a las capas IP y TCP/UDP como son:
- ICMP (Internet Control Message Protocol)
- ARP (Address Resolution Protocol)
- RARP (Reverse Address Resolution Protocol)
- BOOTP (BOOT Protocol)
- DHCP (Dynamic Host Configuration Protocol).



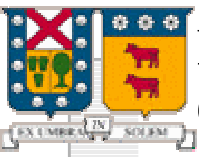
ICMP

- Se usa para comunicar eventos sucedidos en la Red
- Principalmente usado por Routers para enviar msg a los emisores o receptores de paquetes
- ICMP es considerado ser un protocolo de capa 3 por encima de IP
- ICMP es ocupado por los comandos **Ping** y **Traceroute**
- ICMP está definido en RFC 792.



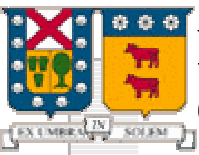
ICMP

Message type	Description
Destination unreachable	Packet could not be delivered
Time exceeded	Time to live field hit 0
Parameter problem	Invalid header field
Source quench	Choke packet
Redirect	Teach a router about geography
Echo request	Ask a machine if it is alive
Echo reply	Yes, I am alive
Timestamp request	Same as Echo request, but with timestamp
Timestamp reply	Same as Echo reply, but with timestamp



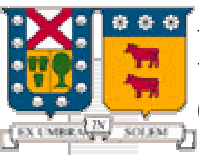
ARP

- El usuario especifica sitios (nombres) que son traducidas a direcciones IP gracias al Servidor de Nombres (DNS)
- La Capa 3 sólo entiende números IP de 32 bits
- La Capa 2 se comunica con otros computadores de la misma red LAN sólo usando la dirección MAC, que en Ethernet es de 48 bits
- **ARP** traduce direcciones IP a direcciones MAC (sea Ethernet, Token Ring, SNA, etc.).



ARP

- Cada máquina pregunta vía broadcast cuál es la dirección MAC de la IP que necesita
- En ese mismo paquete, el emisor adjunta su IP, para que el receptor conozca esta IP y no pregunte vía broadcast
- Cada máquina en Internet debe correr ARP y además:
 - posee un cache de ARP para ahorrar preguntar por cada paquete
 - Al inicializarse pregunta la dirección MAC de su IP. Si una maquina contesta, entonces reporta al usuario que hay otra máquina con la misma IP. Esto además sirve para que el resto de la LAN lo conozca
 - cada entrada del cache posee un tiempo de expiración.

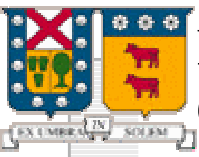


ARP

■ Para máquinas que no están en la LAN hay 2 alternativas:

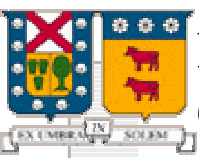
- que el Router sea además un Proxy ARP, quien responde preguntas ARP por otras redes LAN engañando al emisor
- que el emisor deduzca que esa dirección IP no pertenece a la LAN y le envía el paquete a su “Puerta de Enlace” (aquí gateway=router) por defecto
- ejemplo de ARP cache.

IP Address	Hardware Address
197.15.3.2	0A:07:4B:12:82:36
197.15.3.3	0A:9C:28:71:32:8D
197.15.3.4	0A:11:C3:68:01:99
197.15.3.5	0A:74:59:32:CC:1F
197.15.3.6	0A:04:BC:00:03:28
197.15.3.7	0A:77:81:0E:52:FA



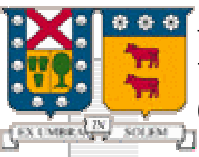
RARP (RFC 903)

- Es el servicio inverso a ARP: Dada una dirección MAC encontrar la IP correspondiente.
- Esta situación se produce cuando estaciones sin disco deben “bootear” desde un disco de un servidor.....
- Una vez booteado, pregunta via broadcast “mi MAC es x.x.x.x, alguien sabe cuál es mi dirección IP?”
- El servidor RARP contesta
- Esto permite que varias máquinas booten desde el mismo servidor con el mismo software, pero tengan diferentes IP.



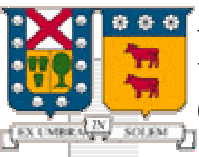
BOOTP (RFC 951, 1048,1084)

- Las peticiones RARP no cruzan los routers, por lo que es necesario tener un RARP server en cada subred IP...
- Existe un protocolo alternativo llamado BOOTP (RFC 951) que utiliza paquetes UDP y entrega a la estación más información que RARP, como es:
 - dirección IP de su servidor de booteo (imagen a bootear)
 - dirección IP de su default router (puerta de enlace)
 - Subred IP a la que pertenece (mask).



DHCP

- BOOTP y RARP requieren que esté la dirección MAC del cliente ya ingresada a la base de datos
- Qué pasa si llega un nuevo computador?
- Qué pasa si un computador es cambiado a otra subred?
- **Dynamic Host Configuration Protocol** posee un grupo de direcciones IP y las asigna a medida que llegan peticiones
 - cliente envía petición DHCP
 - servidor DHCP busca una IP desocupada y la asigna a la MAC
 - servidor responde al cliente su IP asignada.



DHCP

- Qué pasa si el cliente se va de la subred?
- El servidor no supo y queda la dirección ocupada?
- Cada asignación posee un tiempo de expiración
- El cliente no puede usar su IP después de la expiración
- Al cabo de este tiempo, el servidor puede asignar de nuevo esta IP si el cliente no ha pedido “prórroga”
- Se puede asignar siempre la misma IP a una misma MAC, si se desea (asignación estática).