



Universidad del Cauca
Facultad de Ingeniería Electrónica y Telecomunicaciones
Departamento de Telemática



Sistemas de Conmutación

Introducción a las Redes IP



Dr. Ing. Álvaro Rendón Gallón
Popayán, abril de 2013

Temario



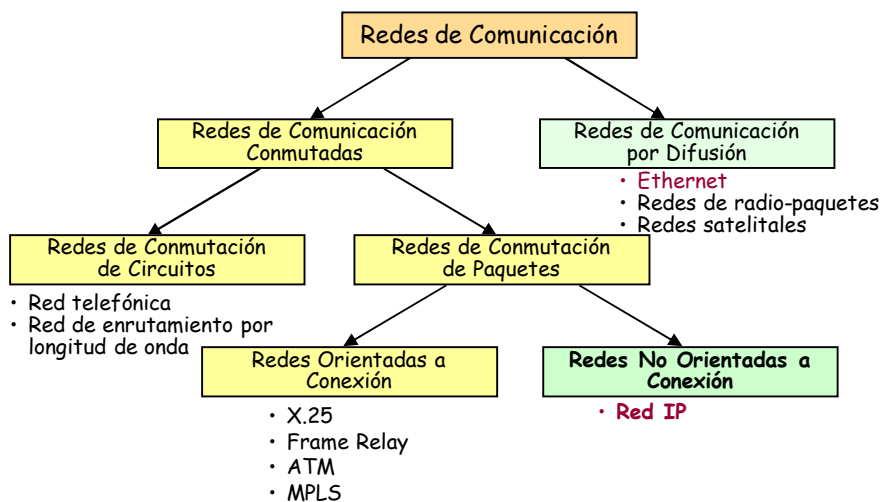
2

- Generalidades del modelo TCP/IP
- Capa de acceso a la red: Ethernet
- Capa de red: Internet
- Capa de transporte: TCP y UDP
- Protocolos de enrutamiento
- Dispositivos de red

Temario

- **Generalidades del modelo TCP/IP**
 - Comunicación orientada y no orientada a conexión
 - Redes de datagramas y de circuitos virtuales
 - Tipos de redes
 - Arquitectura de protocolos TCP/IP
- Capa de acceso a la red: Ethernet
- Capa de red: Internet
- Capa de transporte: TCP y UDP
- Protocolos de enrutamiento
- Dispositivos de red

Redes de comunicaciones

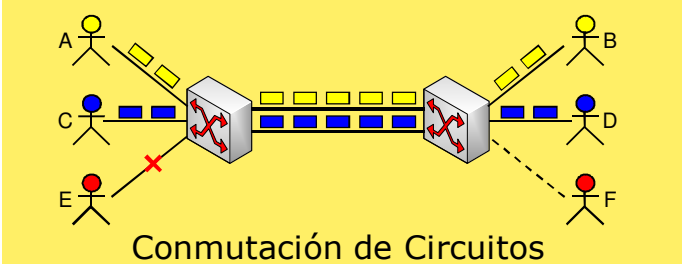


H.G. Perros. Connection-Oriented Networks: SONET/SDH, ATM, MPLS and Optical Networks. John Wiley & Sons, Chichester (England), 2005. (Fig. 1-1, pag. 2).

5

**Conmutación de Circuitos vs
Conmutación de Paquetes**

Departamento de
Telemática



Conmutación de Circuitos

Un circuito (físico o un canal) dedicado para la comunicación entre los usuarios (apropiado para telefonía)

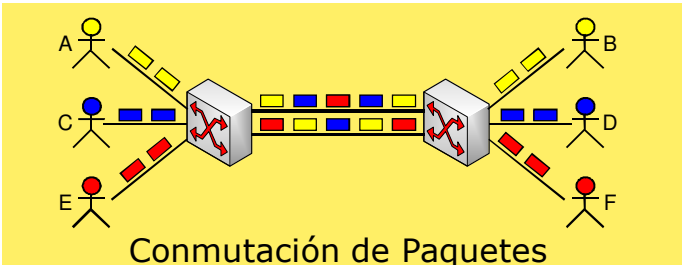
Requiere establecimiento y liberación

El establecimiento requiere capacidad disponible de circuitos y conmutadores

6

**Conmutación de Circuitos vs
Conmutación de Paquetes**

Departamento de
Telemática



Conmutación de Paquetes

Los circuitos son compartidos entre las diferentes conexiones (uso más eficiente en transmisión de datos)

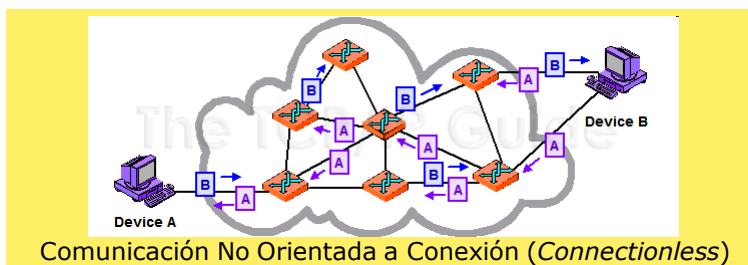
Todos los datos son agrupados en paquetes

La velocidad de transferencia de los paquetes varía en función del estado de la red

Comunicación Orientada a Conexión vs No Orientada a Conexión



7



Cada paquete se procesa en forma independiente en los nodos y puede seguir una ruta distinta: **Datagrama**

Cada paquete lleva la identificación del **destino**

Los paquetes pueden llegar en desorden o perderse

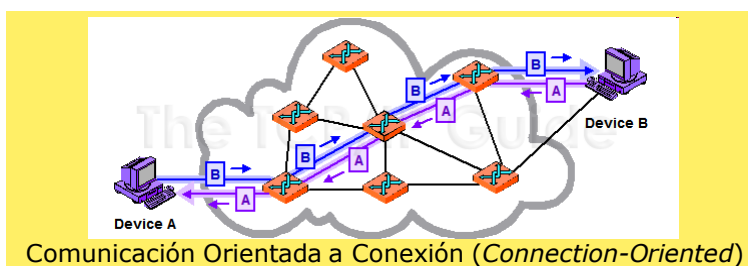
El receptor reordena y recupera los paquetes

http://www.tcpipguide.com/free/t_CircuitSwitchingandPacketSwitchingNetworks.htm

Comunicación Orientada a Conexión vs No Orientada a Conexión



8



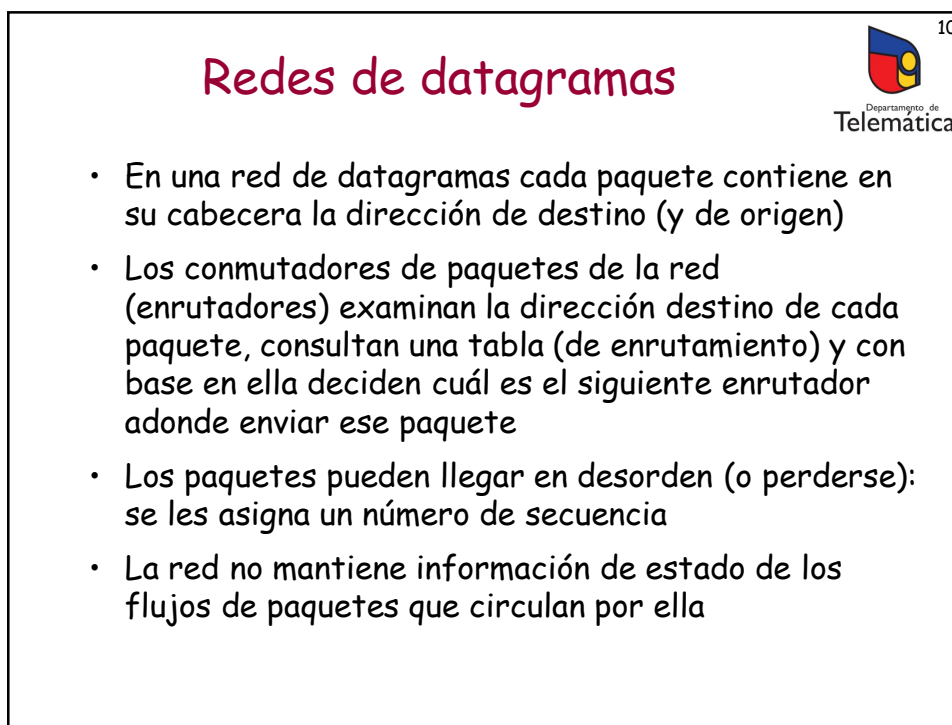
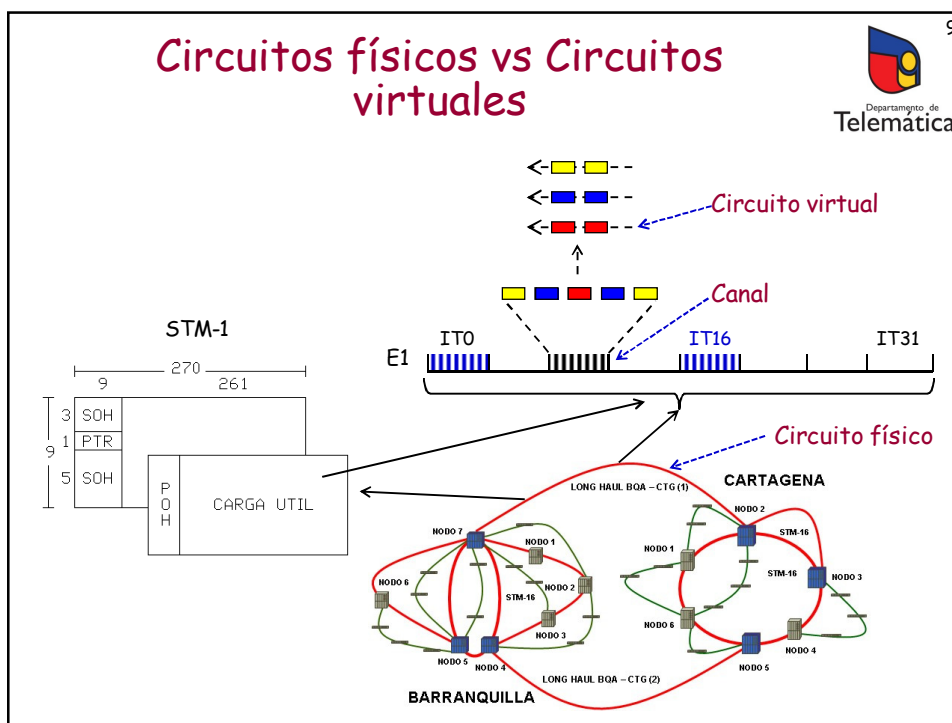
Los paquetes siguen una ruta establecida antes de iniciar la transferencia: **Circuito Virtual** (conmutado o permanente)

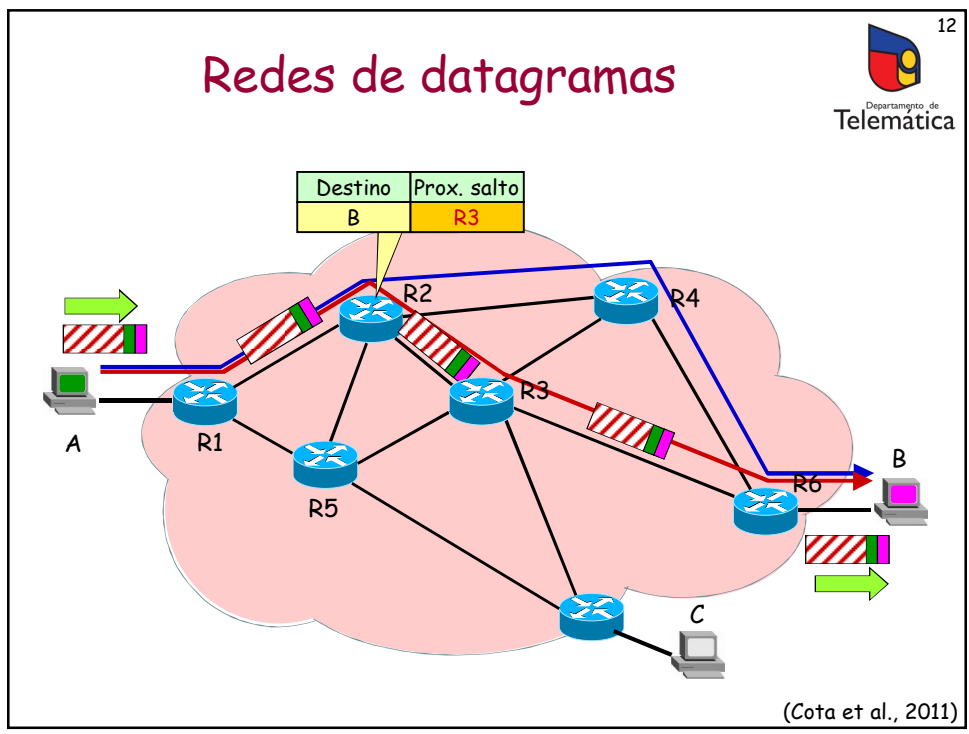
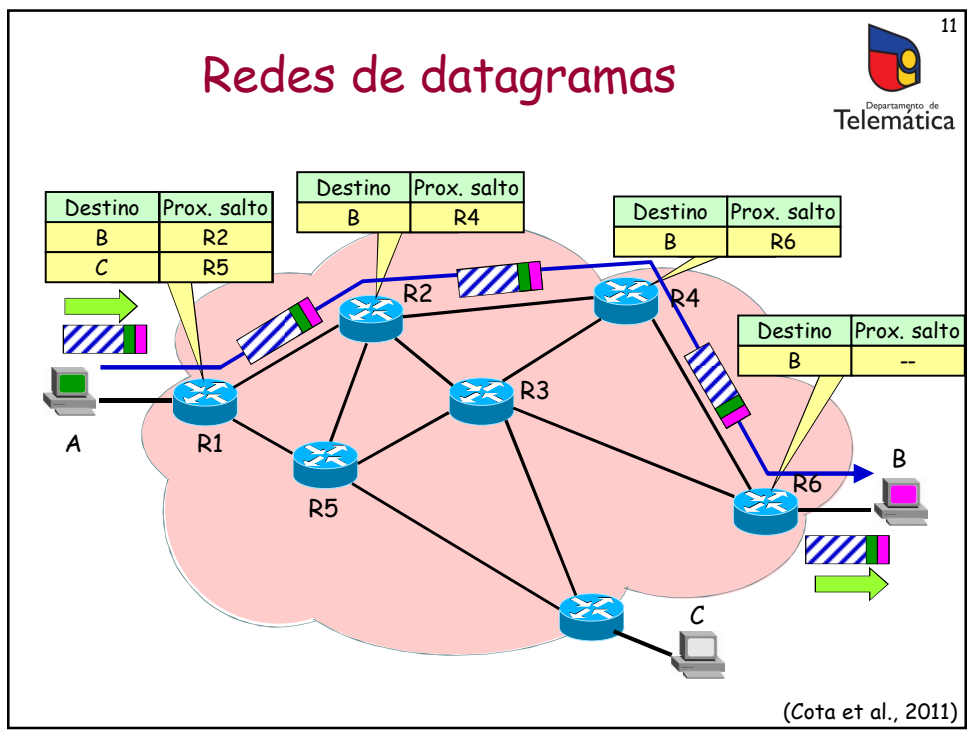
Requiere establecimiento y liberación

Cada paquete lleva la identificación del **circuito virtual**

La red puede hacer secuenciación y control de errores

http://www.tcpipguide.com/free/t_CircuitSwitchingandPacketSwitchingNetworks.htm





Redes de circuitos virtuales



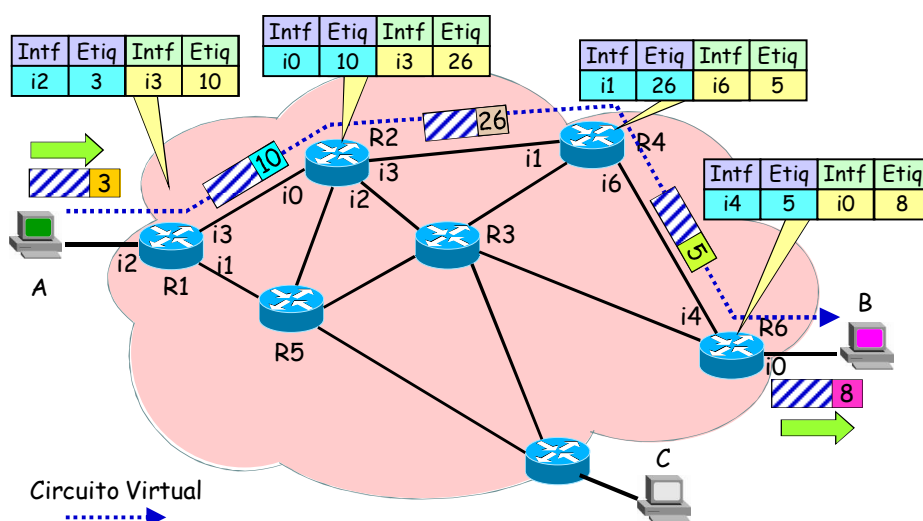
13

- Los paquetes viajan de origen a destino siguiendo un Circuito Virtual (VC: Virtual Circuit)
- El VC está conformado por los conmutadores/enrutadores y las conexiones virtuales entre ellos (saltos)
- Cada paquete contiene en su cabecera la identificación de la conexión virtual asignada (**etiqueta**) en cada salto
- Los conmutadores/enrutadores mantienen una tabla de asignación interfaz-etiqueta de entrada a interfaz-etiqueta de entrada salida para cada VC
- Con la interfaz y la etiqueta de entrada del paquete, el conmutador/enrutador obtiene la interfaz y la etiqueta de salida (próximo salto)
- Las tablas de interfaz-etiqueta controlan el estado de los flujos de paquetes que circulan por la red

Redes de circuitos virtuales



14



(Cota et al., 2011)

15

Departamento de Telemática

Redes de circuitos virtuales

- El establecimiento del VC se hace **antes** de empezar a enviar los paquetes. Al terminar el envío se libera
- El establecimiento y liberación de VC se realiza con paquetes de control (señalización)
- En el establecimiento, para elegir el próximo salto (interfaz-etiqueta de salida) se usan tablas de enrutamiento, igual que en redes de datagramas

Tabla interfaz-etiqueta

Intf	Etq	Intf	Etq
i0	10	i3	26

Tabla de enrutamiento

Destino	Prox. salto
B	R4

16

Departamento de Telemática

Datagramas vs Circuitos Virtuales

	Datagramas	Circuitos Virtuales
Establecimiento	No	Si
Dirección	Global	Solo ID de CV
Estado	No	Tabla de CV
Encaminamiento	Por tabla de rutas	Por tabla de CVs
Ruteo	Estático/dinámico	SVC/PVC
Fallas routers	No afectan ?	Cortan CV
Calidad de servicio	Difícil	Posible (se pueden reservar recursos y hacer ingeniería de tráfico)
Cont. Congestión	Difícil	Posible (se pueden reservar recursos)

Tipos de redes



17

LAN: Local Área Network (red de área local)

- Desde una habitación al tamaño de un campus

MAN: Metropolitan Área Network (red de área metropolitana)

- Hasta el tamaño de una ciudad

WAN: Wide Área Network (red de área extensa)

- Generalmente abarcan continentes

Internetworking (interconexión de redes)

- Interconexión de redes WAN y LAN

Redes avanzadas

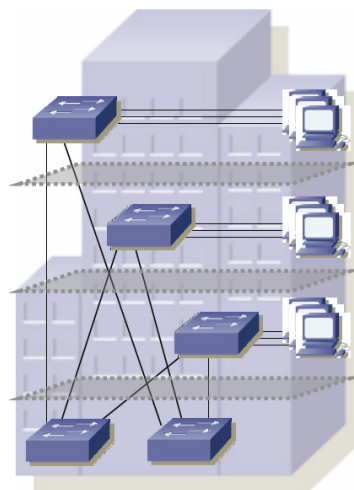
- Académicas y de investigación

Redes de área local (LAN)



18

- Son redes privadas
- Principalmente para datos
- Voz usa otra red en paralelo (hasta llegar VoIP)
- Se limitan a un edificio o una zona local (1 ó 2 Km)
- Velocidades 10-1.000Mbps
- Conectan estac. de trabajo, periféricos, terminales, etc.
- Muchos usuarios
- Se producen pocos errores
- Suelen ser tecnologías basadas en medios de difusión
- Ejemplos: Ethernet, WiFi, FDDI, Token Ring, etc.



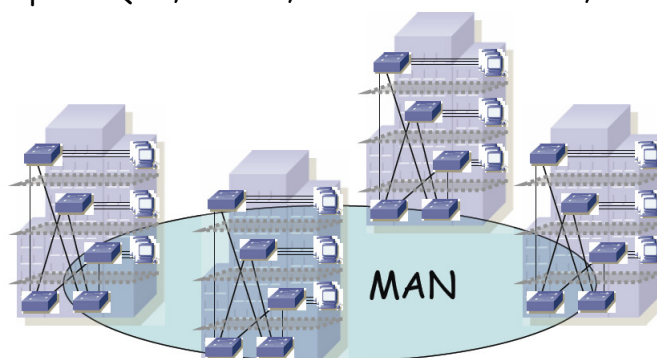
(Morató, 2010)

Redes de área metropolitana (MAN)



19

- Se extienden por áreas metropolitanas
- Interconectan LAN separadas
- Pueden ser públicas o privadas
- Las velocidades típicas van de centenares de Mbps a Gbps
- Ejemplo: DQDB, WiMax, Ethernet conmutada, MPLS, etc.



(Morató, 2010)

Redes de área extensa (WAN)



20

- Cubre un área muy amplia: un país, un continente, el mundo
- Interconecta LAN y MAN
- Usa conmutadores de circuitos/paquetes
- Normalmente controlada por un operador
- Ejemplo: ATM, SDH, Frame Relay, MPLS, etc.



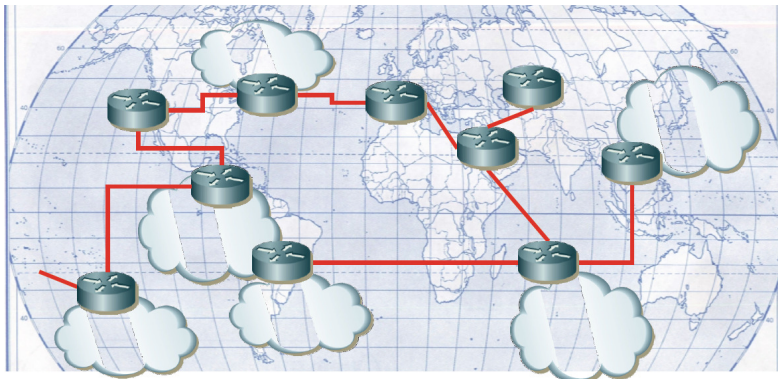
(Morató, 2010)

Interconexión de redes (Internetworking)



21

- Puede interconectar LAN, MAN, WAN, etc..
- Las redes pueden ser de tecnologías diferentes
- Puede abarcar el globo: **Internet**-working



(Morató, 2010)

Redes avanzadas

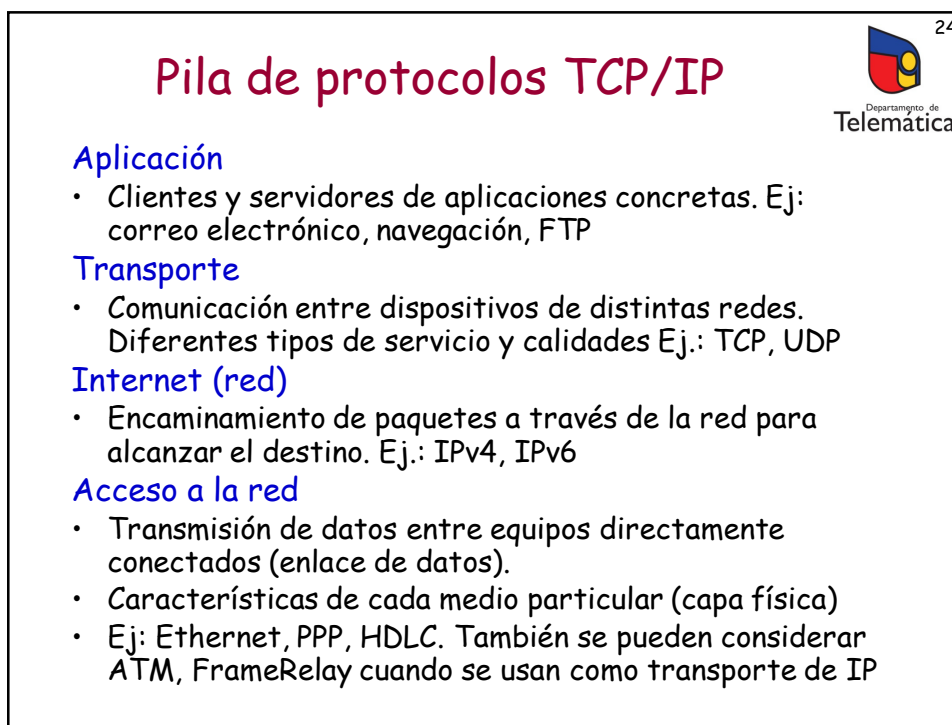
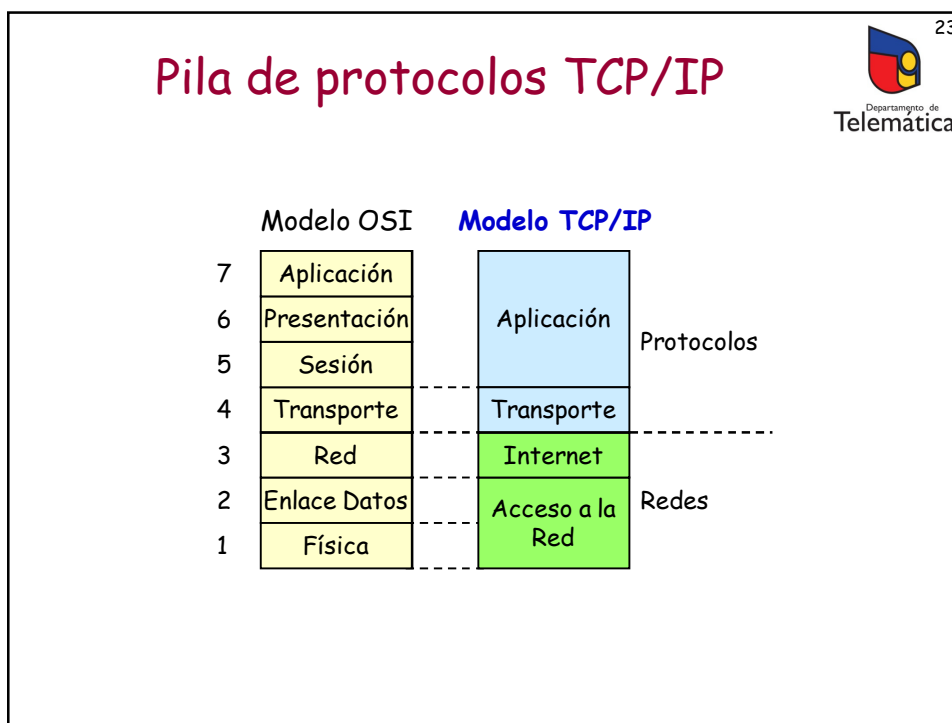


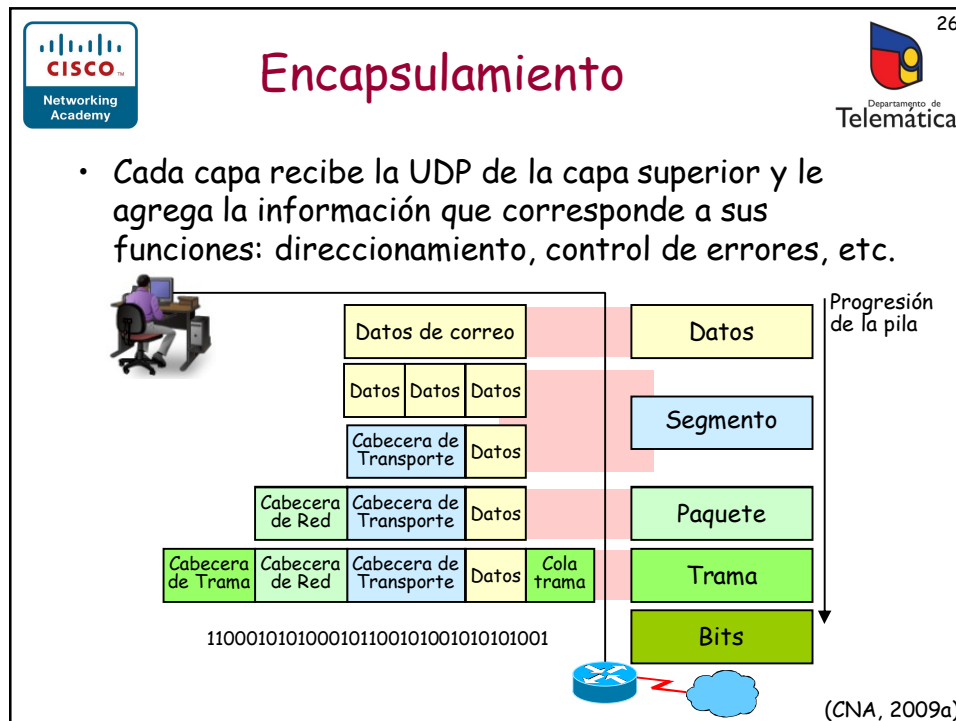
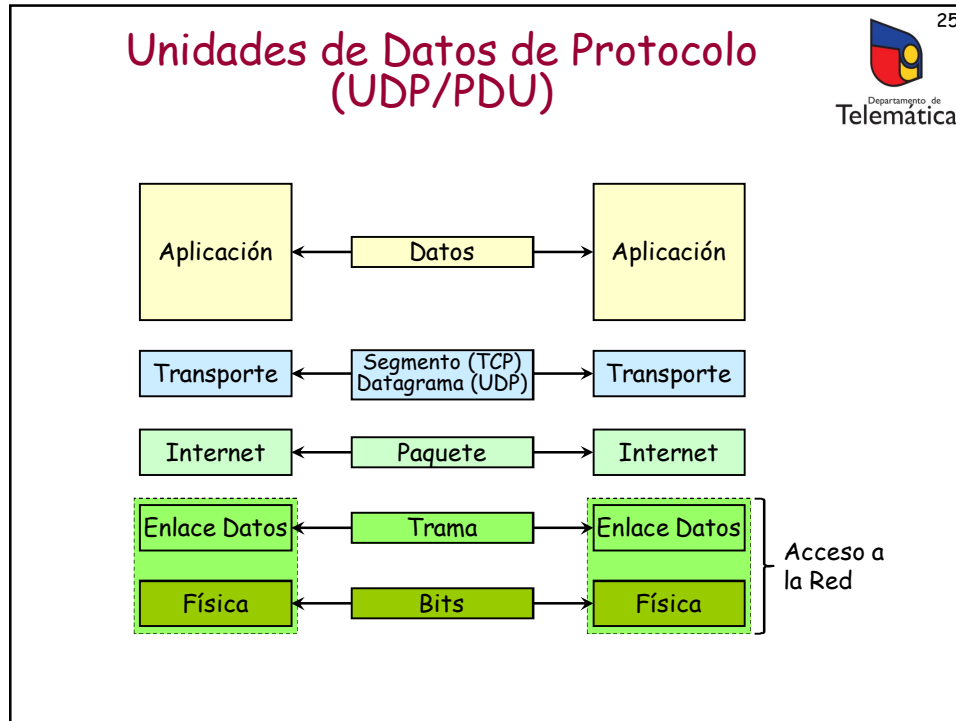
22

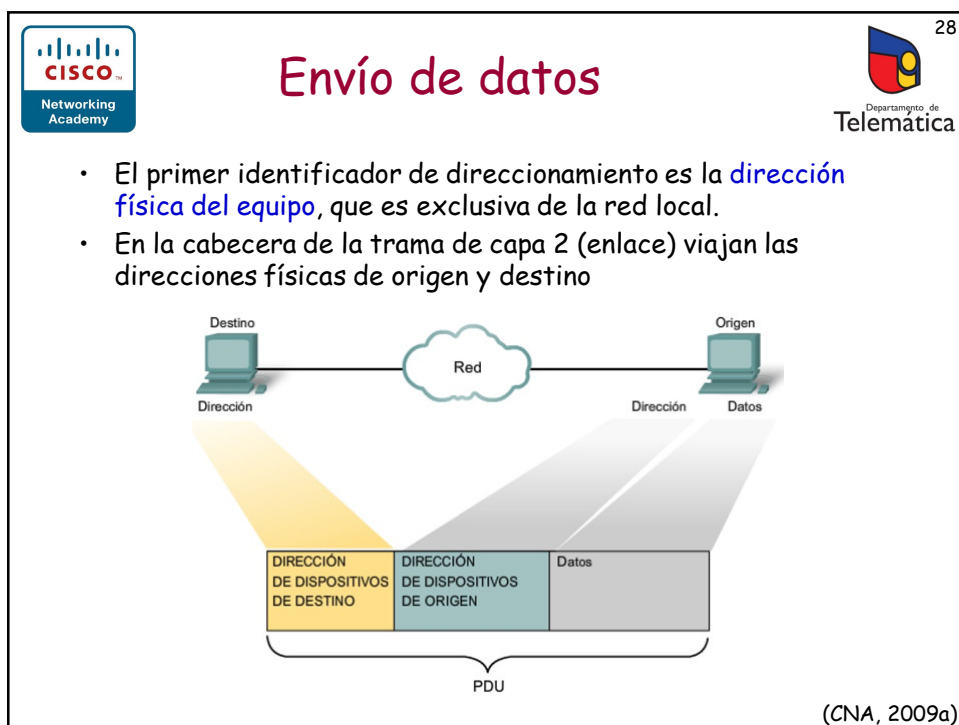
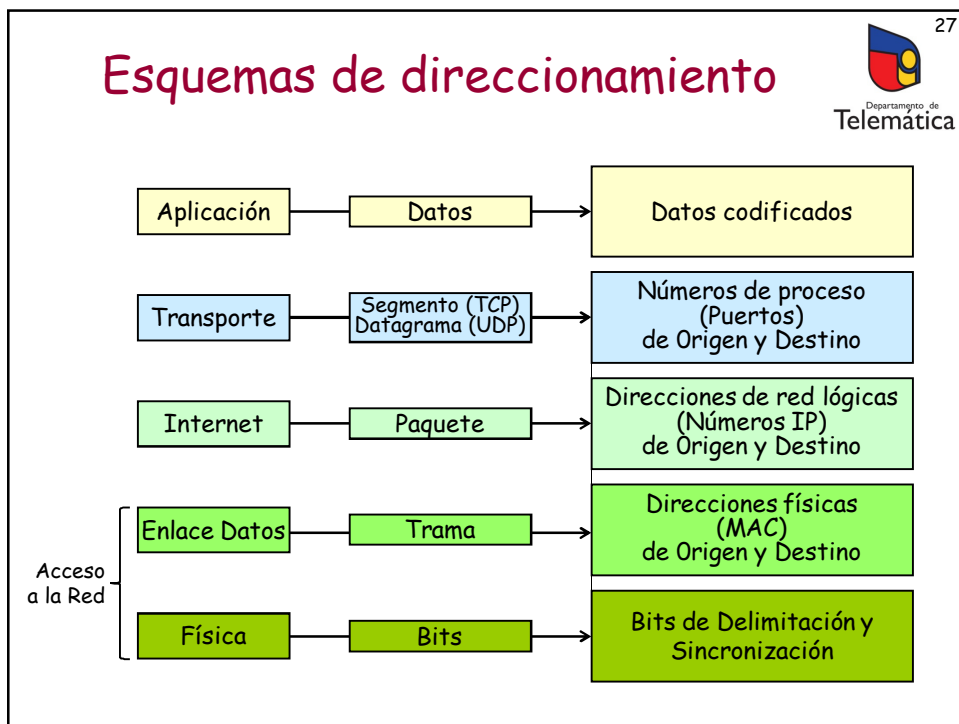


Europa: GEANT
 USA: Internet2
 Latinoamérica: RedCLARA
 Colombia: RENATA
 Popayán: RUP

http://www.redclara.net/index.php?option=com_content&task=view&id=51&Itemid=236







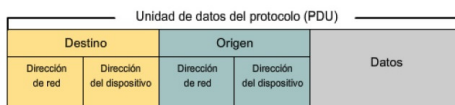


Transporte de datos entre redes

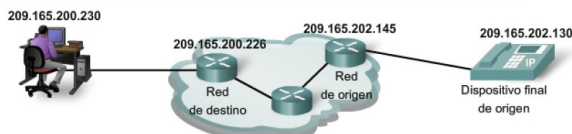


29

- Los protocolos de capa 3 (red) están diseñados para la transferencia de datos de una red local a otra
- Por tanto, las direcciones de capa 3 deben permitir identificar distintas redes y los equipos ubicados en ellas
- En los límites de cada red local, un dispositivo de red (por lo general un enrutador) lee la dirección de destino para determinar la ruta que se debe asignar al paquete de datos



El encabezado de la Unidad de datos del protocolo también contiene la dirección de red.



(CNA, 2009a)

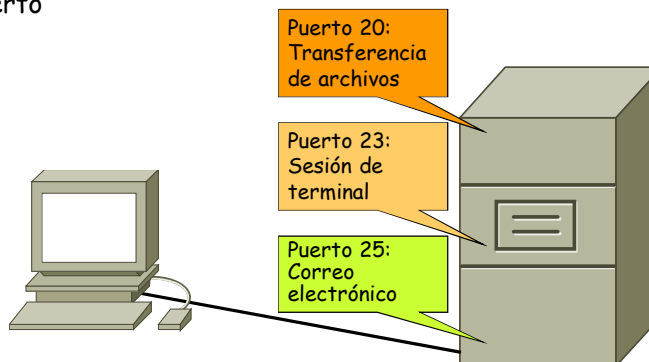


Entrega de datos a la aplicación



30

- Cuando los datos llegan al equipo de destino, es preciso determinar a cuál aplicación deben entregarse
- El direccionamiento de la capa 4 (transporte) identifica el servicio o proceso que recibe los datos en el equipo de destino
- Cada aplicación o servicio es representado por un número de puerto



(CNA, 2009a)

Temario



31

- Generalidades del modelo TCP/IP
- **Capa de acceso a la red: Ethernet**
 - Capa física
 - Subcapa MAC
 - Subcapa LLC
- Capa de red: Internet
- Capa de transporte: TCP y UDP
- Protocolos de enrutamiento
- Dispositivos de red

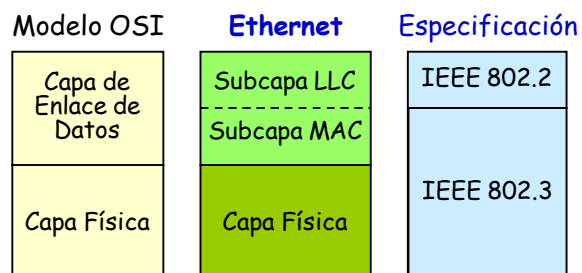
Ethernet



32


Define las funciones de las capas 1 y 2 del modelo OSI.
Ether-net: red *éter*, la "sustancia que lo llena todo".

Pila de protocolos:




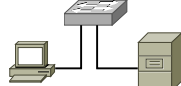
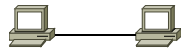
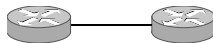
LLC: Logical Link Control (Control del Enlace Lógico)
 MAC: Media Access Control (Control de Acceso al Medio)

33



Departamento de
Telemática

Ethernet: capa física

- UTP: Unshielded Twisted Pair (par trenzado sin blindaje)
- STP: Shielded Twisted Pair (par trenzado apantallado)
- 4 pares de hilos con código de colores
- Hilos 1, 2: Transmisión de datos
- Hilos 3, 6: Recepción de datos
- **Cable directo (Straight-Through):**
 - pin 1-pin 1, pin 2-pin 2, ... (Tx-Tx, Rx-Rx)
 - Conecta un equipo (PC/servidor) a un dispositivo de red (e.g. enrutador, conmutador, concentrador)
- **Cable cruzado (Cross-Over):**
 - pin 1-pin 3, pin 2-pin 6, ... (Tx-Rx, Rx-Tx)
 - Conecta entre sí dos equipos o dos dispositivos de red
- Velocidad de conexión: 10 Mbps, 100 Mbps, 1 Gbps, 10 Gbps

34


Departamento de
Telemática

Ethernet: capa de enlace


Subcapa MAC (Control de acceso al medio)

- Establece a cuál nodo se le permite acceder al medio (único) de comunicación en un instante dado
- Ensambla los datos en tramas con campos de direccionamiento y detección de errores

Subcapa LLC (Control del enlace lógico)

- Control de errores y de flujo
- Interfaz con los niveles superiores
- Hace posible tener varios protocolos de red sobre el mismo medio
- Basado en HDLC (igual que PTM2/SS7)

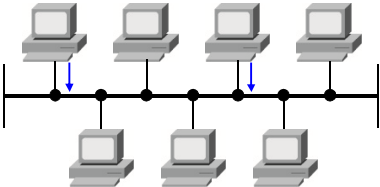
35




Departamento de
Telemática

Ethernet: subcapa MAC

- Protocolo **CSMA/CD** (*Carrier Sense Multiple Access with Collision Detection*): Acceso Múltiple Sensible a Portadora, con Detección de Colisión
- Cuando una estación desea transmitir, **escucha la portadora** para saber si el medio está libre. Si está ocupado, espera hasta que se libere
- Cuando el medio está libre, la estación empieza a transmitir
- Si **detecta una colisión** (otra estación transmitiendo), se detiene, espera un tiempo aleatorio, y empieza desde el principio



36



Departamento de
Telemática

Ethernet: subcapa MAC

Formato de la trama (IEEE 802.3)

Preamb	SOF	Destino	Origen	Long	Datos	Relleno	FCS	
bytes	7	1	6	6	2	0-1.500	0-46	4

Preámbulo: 101010101010... (7 bytes alternando 1 y 0)

SOF (Start Of Frame): 101010**11**

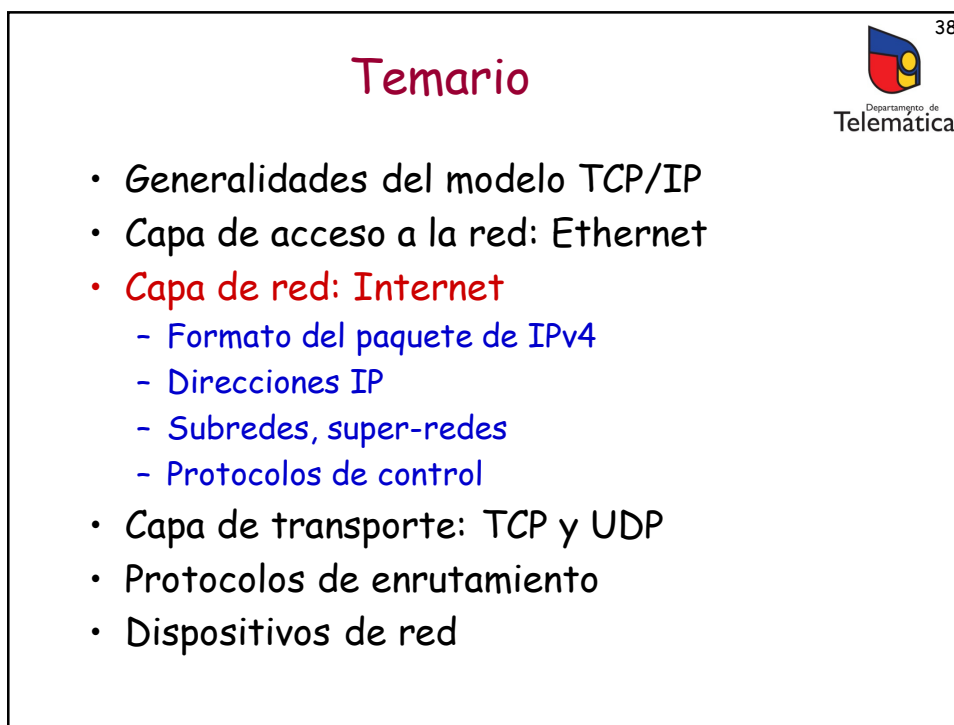
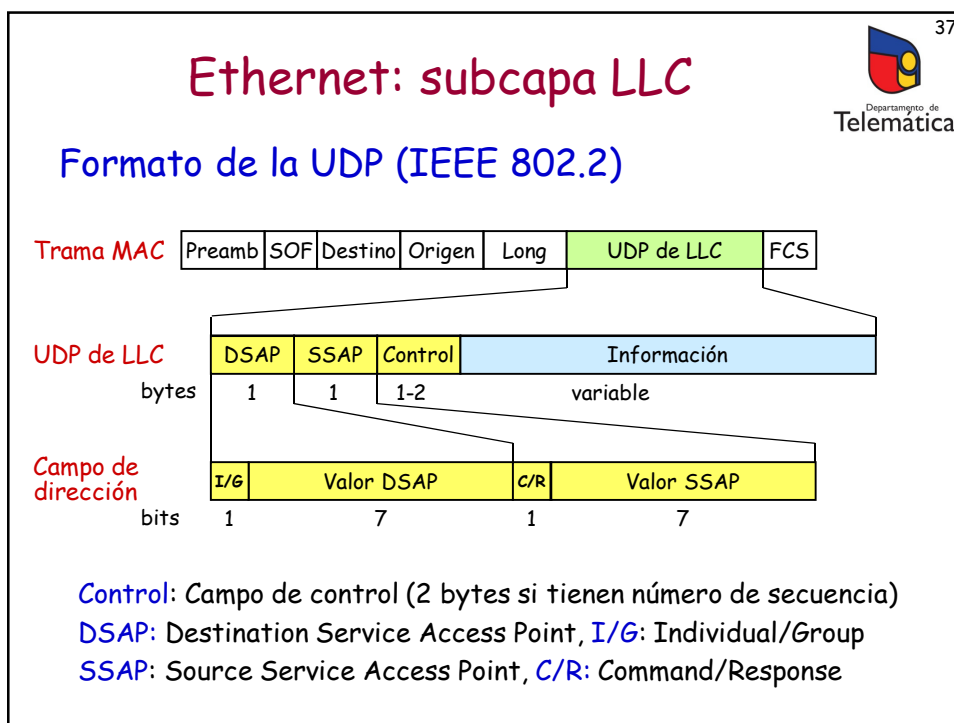
Destino/Origen: Direcciones MAC (Ej: 00-B0-D0-86-BB-F7)


Longitud: del campo de datos

Relleno: trama ≥ 64 bytes (datos+relleno ≥ 46)

FCS: Frame Check Sequence

Direcciones MAC: 3 bytes asignados por IEEE al fabricante
3 bytes asignados por el fabricante a la tarjeta





39
 Departamento de
Telemática

Capa de red: Internet

Tres tipos de protocolo

- **Protocolos de red:**
 - Transportan las UDP de niveles superiores
 - IPv4, IPv6
- **Protocolos de control:**
 - Intercambio de información de control entre dispositivos de la red
 - ICMP, ARP, RARP, BOOTP, DHCP, IGMP
- **Protocolos de enrutamiento:**
 - Intercambio de información de enrutamiento
 - RIP, OSPF, IS-IS, IGRP, EIGRP, BGP

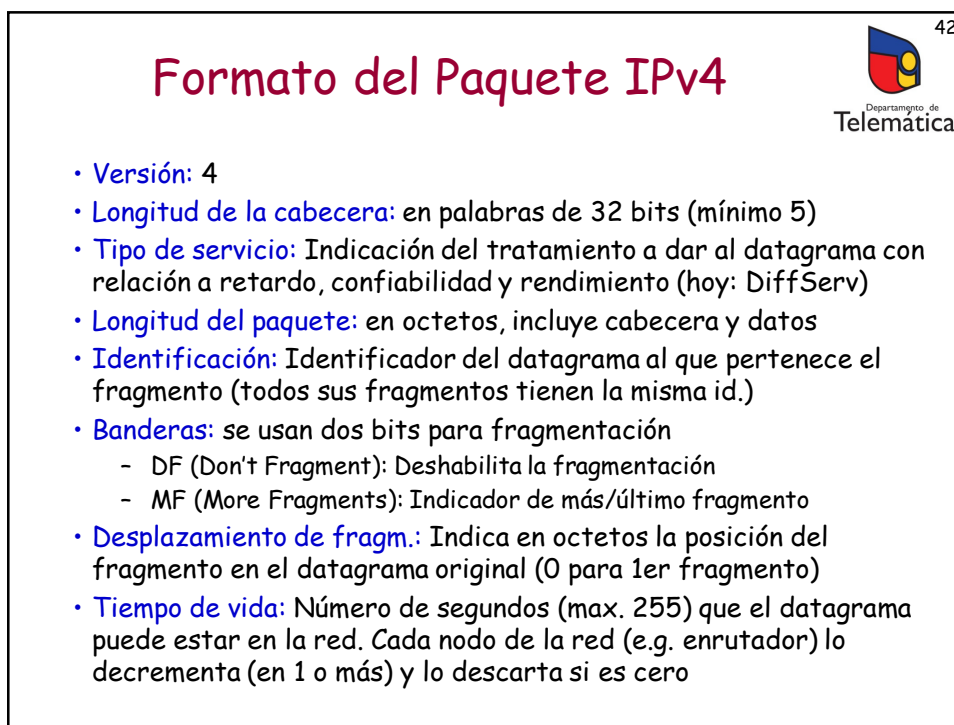
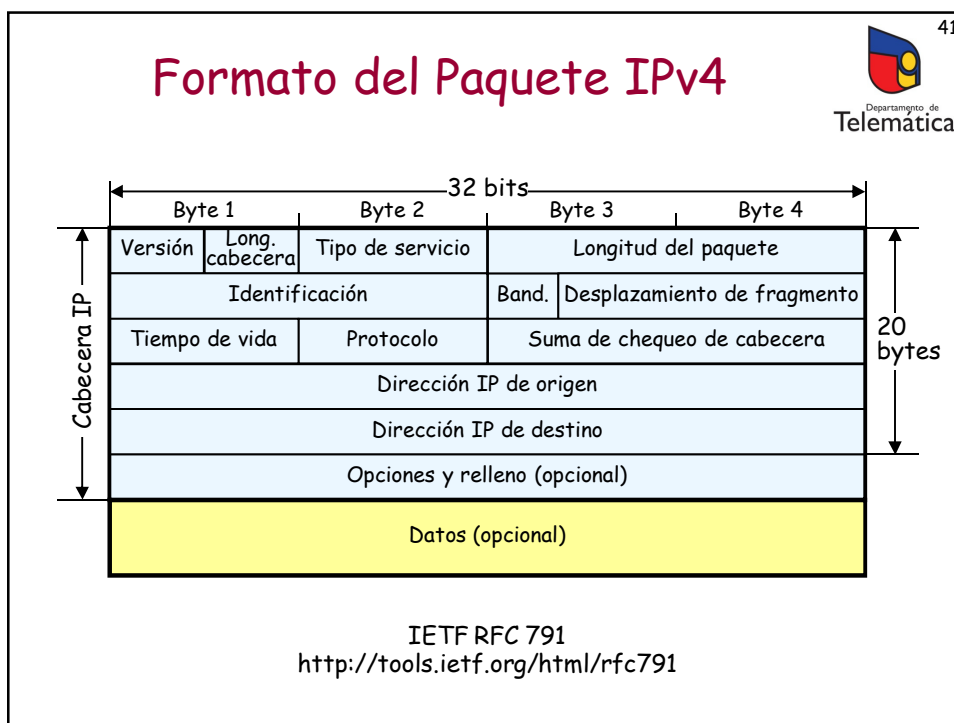
Aplicación
Transporte
Internet
Acceso a la Red


40
 Departamento de
Telemática


Protocolo de Internet (IP)

Suministra un servicio no orientado a conexión:

- Un computador puede enviar a otro paquetes sin haber establecido una conexión, como tiene que hacerse en X.25, FR, ATM y MPLS
- Cada paquete IP es enrutado de modo independiente, y en teoría pueden seguir rutas distintas
- En la práctica, los enrutadores usan tablas de enrutamiento que no cambian con frecuencia, luego típicamente los paquetes siguen el mismo camino
- Las tablas de enrutamiento son refrescadas periódicamente teniendo en cuenta enlaces congestionados y fallas en enrutadores y enlaces



43


 Departamento de
 Telemática

Formato del Paquete IPv4

Protocolo: Indica a qué protocolo debe entregarse el paquete

Ejemplos:

Valor	Protocolo	Descripción
1	ICMP	Internet Control Message Protocol
2	IGMP	Internet Group Management Protocol
3	GGP	Gateway-to-Gateway Protocol
4	IP	IP en IP (encapsulado)
5	ST	Stream
6	TCP	Transmission Control Protocol
8	EGP	Exterior Gateway Protocol
17	UDP	User Datagram Protocol
29	ISO-TP4	ISO Transport Protocol Clase 4
80	CLNP	Connectionless Network Protocol
88	IGRP	Interior Gateway Routing Protocol
89	OSPF	Open Shortest Path First


Aplicación

Transporte

Internet

Acceso a la Red

44


 Departamento de
 Telemática

Fragmentación en IP

- El nivel de red debe acomodar cada datagrama en una trama del nivel de enlace.
- Cada tecnología de nivel de enlace tiene un valor máximo de datagrama que puede aceptar, Ej.:
 - Ethernet: 1.500 bytes (DIX), 1.492 (LLC-SNAP).
 - Token Ring: 4.440 bytes (4 Mb/s, THT 8 ms).
- Este valor es la MTU (Maximum Transfer Unit).

Token Ring

Cab. ABCDEF GHIJKL MNOP

↓

E-net DIX


Cab. ABCDEF

Cab. GHIJKL

Cab. MNOP

(Araya, 2006)

45


Departamento de
Telemática

Fragmentación en IP

- Si el datagrama no cabe, debe fragmentarse. Ej: datagrama de 4.000 bytes creado en red Token Ring que pasa a Ethernet. El enrutador lo fragmenta
- A veces el equipo ha de fragmentar de entrada pues genera datagramas demasiado grandes, ej: NFS construye datagramas de 8 KB, incluso en Ethernet

Token Ring

Cab.	ABCDEF GHIJKL MNOP
------	--------------------


↓

E-net DIX

Cab.	ABCDEF	Cab.	GHIJKL	Cab.	MNOP
------	--------	------	--------	------	------

(Araya, 2006)


46


Departamento de
Telemática


Fragmentación en IP

- Los fragmentos reciben la misma cabecera que el datagrama original salvo por los campos 'MF' y 'Desplazamiento del fragmento'.
- Los fragmentos de un mismo datagrama se identifican por el campo 'Identificación'.
- Todos los fragmentos, menos el último, tienen a 1 el bit MF (More Fragments).
- La unidad básica de fragmentación es 8 bytes. Los datos se reparten en tantos fragmentos como haga falta, todos ellos múltiplos de 8 bytes (salvo quizá el último).
- Toda red debe aceptar un MTU de al menos 68 bytes. El mínimo recomendado es de 576 bytes.

(Araya, 2006)



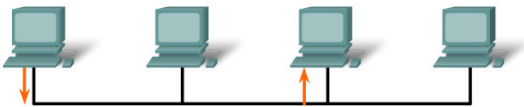
Modos de direccionamiento



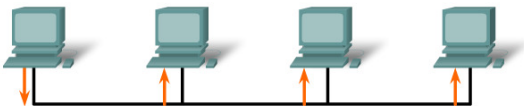
Departamento de Telemática

47

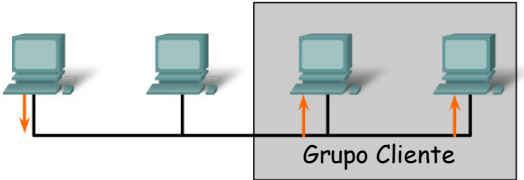
Unidifusión (Unicast)
Un emisor y un receptor



Difusión (Broadcast)
Un emisor hacia todas las demás direcciones




Multidifusión (Multicast)
Un emisor hacia un grupo de direcciones
(grupo gestionado por IGMP)




IGMP: Internet Group Management Protocol

(CNA, 2009c)



Clases de direcciones IP




Departamento de Telemática

48

- Las clases A, B y C son llamadas **clases primarias** porque son usadas para las direcciones de los computadores y servidores, llamados en forma genérica hosts (equipos), y los dispositivos de la red (enrutadores, etc.)
- La clase D es para **multidifusión**
- La clase E está reservada para usos futuros

	8 Bits	8 Bits	8 Bits	8 Bits
Clase A	0	Red	Sufijo	
Clase B	10	Red	Sufijo	
Clase C	110	Red	Sufijo	
Clase D	1110 Dirección de Multidifusión			
Clase E	11110 Reservado para uso futuro			

49



Departamento de Telemática

Clases de direcciones IP

- El primer campo determina la clase de dirección (A, B, C, D, E)
- El segundo campo indica la **dirección de la red**
- Primer más segundo campo: **prefijo**
- El tercer campo (**sufijo**) indica la dirección del equipo

	8 Bits	8 Bits	8 Bits	8 Bits
Clase A	0	Red	Sufijo	
Clase B	10	Red	Sufijo	
Clase C	110	Red	Sufijo	
Clase D	1110	Dirección de Multidifusión		
Clase E	11110	Reservado para uso futuro		

50


Departamento de Telemática

Clases de direcciones IP

- Cada octeto se escribe en decimal, de 0 a 255
- Clase A - Direcciones de red: 1.0.0.0 a 126.0.0.0
126 redes, 16,7 millones de equipos por red
- Clase B - Direcciones de red: 128.0.0.0 a 191.255.0.0
16.384 redes, 65.536 equipos por red
- Clase C - Direcciones de red: 192.0.0.0 a 223.255.255.0
2 millones de redes, 256 equipos por red

	8 Bits	8 Bits	8 Bits	8 Bits
Clase A	0	Red	Sufijo	
Clase B	10	Red	Sufijo	
Clase C	110	Red	Sufijo	
Clase D	1110	Dirección de Multidifusión		
Clase E	11110	Reservado para uso futuro		

Internet Assigned Numbers Authority (IANA)

51

Departamento de Telemática

Direcciones IP especiales

← 32 Bits →

Red		Equipo	
-----	--	--------	--

Dirección de la red (bits de equipo = 0)

← 8 Bits
1 Byte

← 8 Bits
1 Byte

← 8 Bits
1 Byte

← 8 Bits
1 Byte

N	N	H	H
172	16	0	0

Dirección de difusión (bits de equipo = 1)

← 8 Bits
1 Byte

← 8 Bits
1 Byte

← 8 Bits
1 Byte

← 8 Bits
1 Byte

N	N	H	H
172	16	255	255


52

Departamento de Telemática

Direcciones IP especiales

Dirección de la red: 172.16.0.0

Destino	Prox. salto
172.16.0.0	R3
220.138.45.0	R5


53
 Departamento de
 Telemática

Direcciones IP especiales

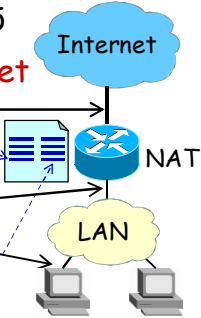
Direcciones privadas

- Clase A: 10.0.0.0 a 10.255.255.255
- Clase B: 172.16.0.0 a 172.31.255.255
- Clase C: 192.168.0.0 a 192.168.255.255


Equipos que **no están conectados a Internet**

Ej.: Red local con servidor proxy NAT

- Dirección pública asignada: 190.69.2.116
- Dirección interna del proxy: 10.200.7.4
- Dirección del computador: 192.168.210.140



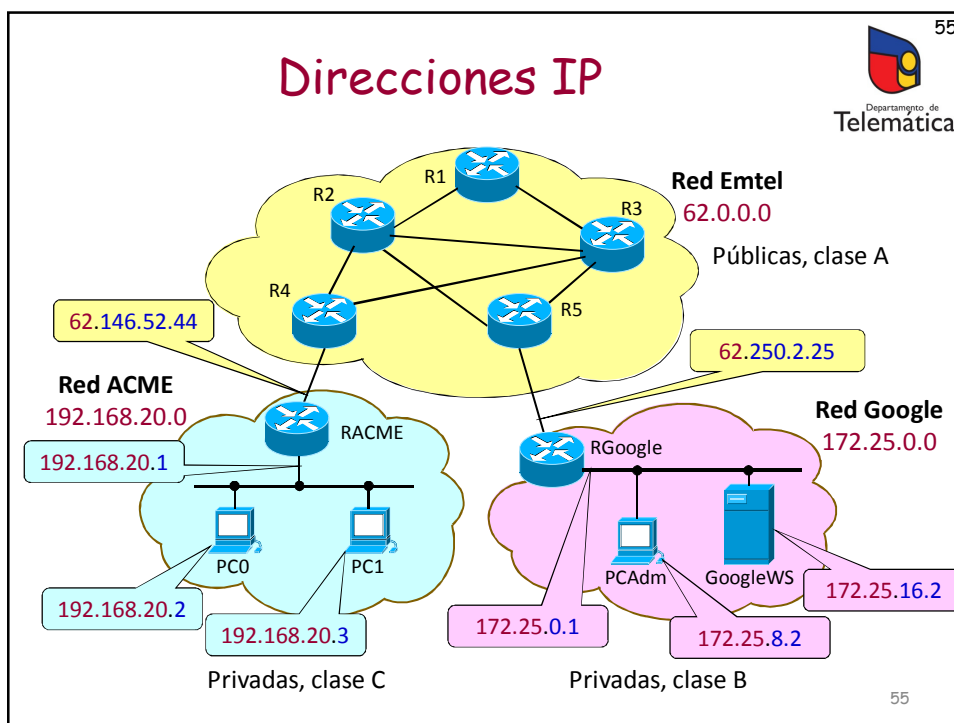
NAT: Network Address Translation


54
 Departamento de
 Telemática

Direcciones IP especiales

- **0.0.0.0** - Identificación local ("este dispositivo")
 Usada cuando se está iniciando el sistema y aún no se conoce la dirección asignada al dispositivo.
 No está permitido su uso como dirección de destino.
- **127.x.x.x** - Bucle de retorno (loopback)
 Usadas en las pruebas de la pila TCP/IP (127.0.0.1)
- **169.254.X.X/16** - Autoconfiguración
 Asignadas cuando en el arranque no se encuentra configurada una dirección estática o dinámica
 También son privadas
- Otras...

Consultar RFC 5735 - "Special Use IPv4 Addresses"

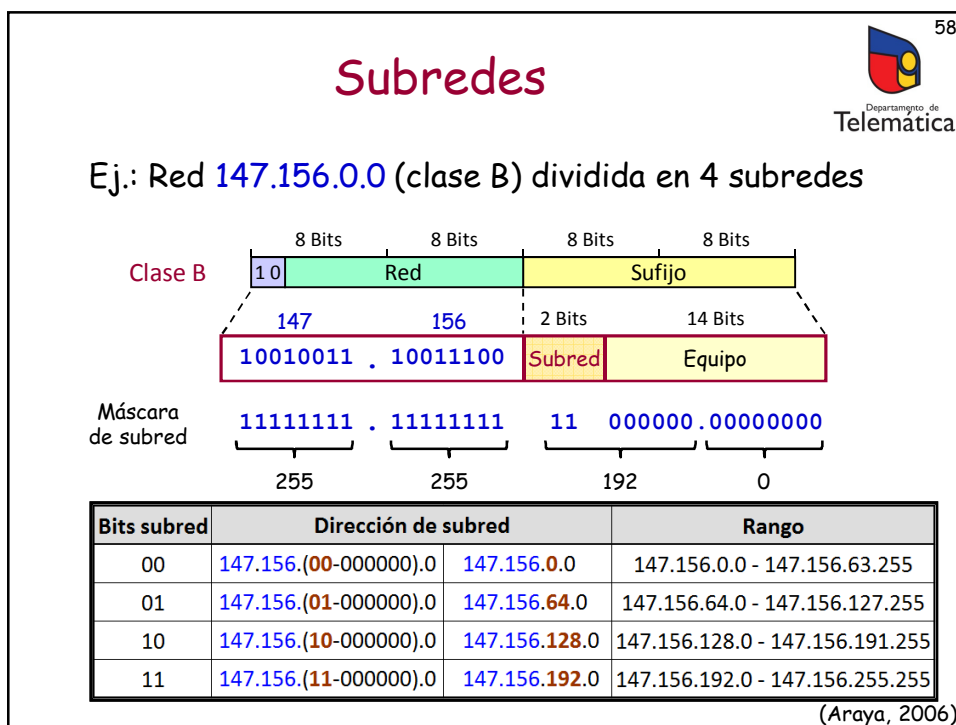
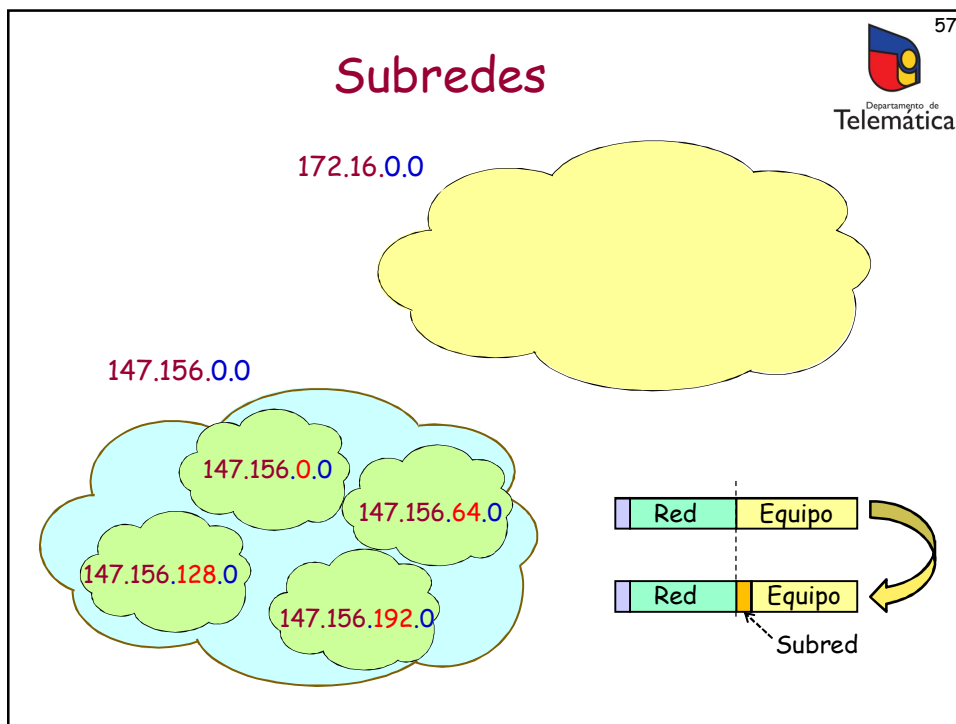


56


Subredes

Departamento de Telemática

- La estructura de las direcciones IP establece una jerarquía de dos niveles:
 - Direcciones de red (prefijos)
 - Direcciones de equipos (sufijos)
- En muchos casos esta jerarquía es insuficiente
 - Un gran organización con una dirección clase B, cuyas dependencias tienen sus propias LAN
- Se divide el sufijo de la dirección IP en:
 - **Parte de subred:** dirección asignada a cada LAN
 - Parte de dirección de equipos
- Para determinar cómo se divide el sufijo de la dirección IP entre subred y equipos se usa la **máscara de subred** (*subnet mask*)



59



 Departamento de
Telemática

Subredes

- La máscara de subred identifica qué parte de la dirección IP es red-subred y qué parte es equipo.
- En cada subred hay siempre dos direcciones reservadas: la primera y la última.
 - Si la parte equipo es cero la dirección es la de la propia subred
 - La dirección con la parte equipo toda a unos está reservada para difusión en la subred
- Ejemplo:
 - Red 156.134.0.0, máscara de subred 255.255.255.0.
 - 256 subredes identificadas por el tercer byte:
156.134.subred.equipo
 - 156.134.subred.0 identifica la subred
 - 156.134.subred.255 es para difusión en la subred

(Araya, 2006)

60


 Departamento de
Telemática

Subredes

Administrador: Símbolo del sistema

Microsoft Windows [Versión 6.1.7600]
 Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Users\arendon>ipconfig

Configuración IP de Windows

Adaptador de LAN inalámbrica Conexión de red inalámbrica:


Sufijo DNS específico para la conexión. . . : unicauca.edu.co
 Dirección IPv4. : 10.200.9.233
 Máscara de subred : 255.255.252.0
 Puerta de enlace predeterminada : 10.200.8.254

C:\Users\arendon>

Ejercicio:

- Obtener la dirección de la subred a la que pertenece el equipo
- Obtener la dirección de difusión dentro de esa subred

Subredes


61
 Departamento de
 Telemática

```

Administrador: Símbolo del sistema
Microsoft Windows [Versión 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Users\arendon>ipconfig


Configuración IP de Windows

Adaptador de LAN inalámbrica Conexión de red inalámbrica:

    Sufijo DNS específico para la conexión. . . : unicauca.edu.co
    Dirección IPv4. . . . . : 10.200.9.233
    Máscara de subred . . . . . : 255.255.252.0
    Puerta de enlace predeterminada . . . . . : 10.200.8.254
  
```

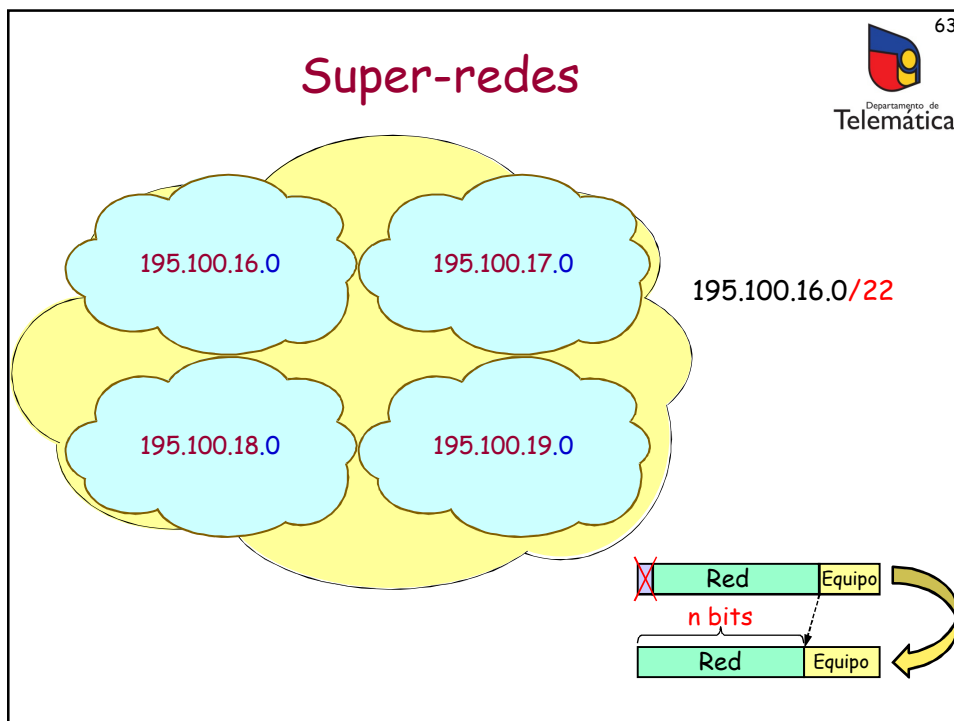
Dirección IP:	10 . 200 . 00001001 . 11101001	10.200.9.233
Máscara de subred:	255 . 255 . 11111100 . 00000000	255.255.252.0
Dirección de subred:	10 . 200 . 00001000 . 00000000	10.200.8.0
Dirección de difusión:	10 . 200 . 00001011 . 11111111	10.200.11.255

Super-redes


62
 Departamento de
 Telemática

- Problema: agotamiento del espacio de direcciones IP
- Causa:
 - Clase A inaccesible (16 millones de equipos por red!)
 - Clase B excesiva (65.536 equipos por red)
 - C demasiado pequeña (256 equipos por red)
 - Muchas organizaciones solicitaban clases B y usaban solo una pequeña parte.
- Solución: asignar **grupos de clases C** a una organización
- Nuevo problema: explosión de las tablas de rutas
- Nueva solución: considerar **un grupo contiguo de redes clase C como una sola red, una super-red**

(Araya, 2006)



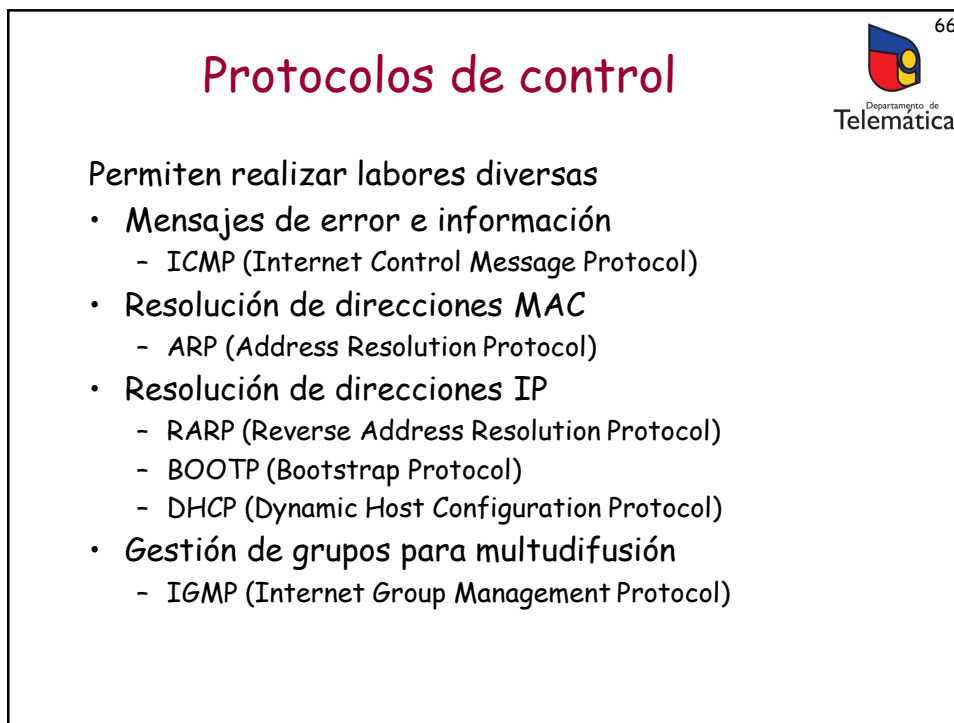
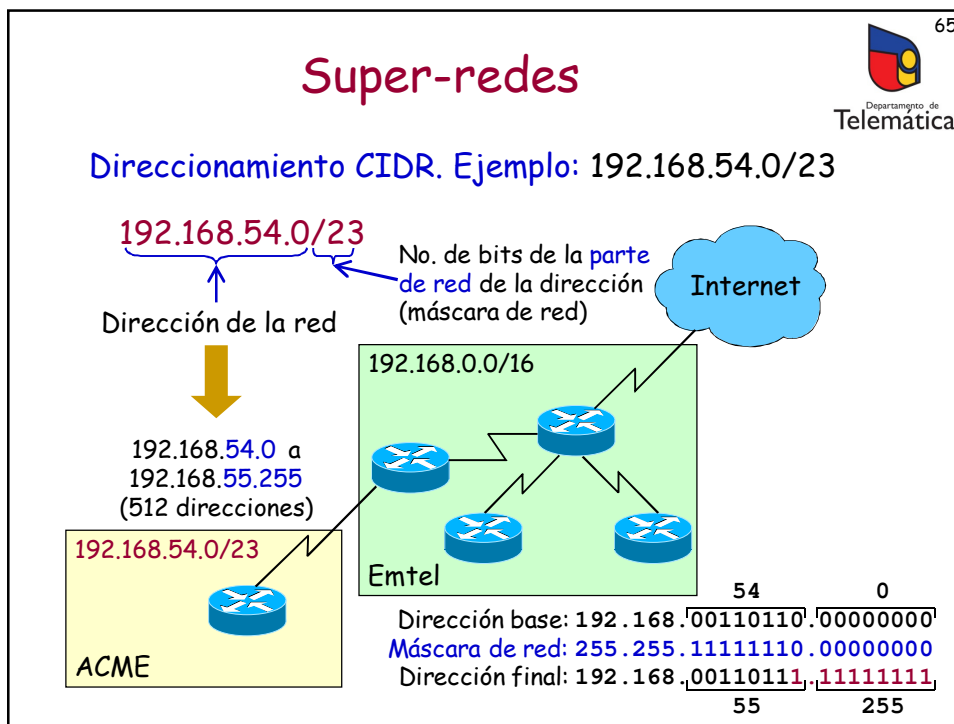
Super-redes

64
Departamento de Telemática


Super-redes Subredes

Red Equipo

- Las super-redes se definen mediante máscaras, como en las subredes, **pero aplicadas a la parte de red**
- Formato: **Dirección base/máscara de red (prefijo)**
- Ej.: Red **195.100.16.0/22**
 - 22: número de bits disponibles en la parte de red
 - Máscara = **11111111.11111111.11111100.00000000**
 - Rango: 195.100.16.0 hasta 195.100.19.255 (1.024 direcciones)
- Normalmente, para 195.100.16.0 (Clase C):
 - Rango: 195.100.16.0 hasta 195.100.16.255 (256 direcciones)
- Ya no se asignan direcciones por clases: enrutamiento sin clases: **CIDR (Classless InterDomain Routing)**



Protocolo de Mensajes de Control de Internet (ICMP)



67
Departamento de Telemática

Define varios mensajes de error e información


Paquete IP

	Cabecera IP	Mensaje ICMP
--	-------------	--------------


Mensaje ICMP

	Tipo	Código	Suma de chequeo	Datos ICMP
bytes	1	1	2	variable

- **Tipo:**
 - 08/00: Solicitud/respuesta de eco (comandos ping y traceroute)
 - 03: Destino inaccesible
 - 04: Disminución de origen
 - 05: Redireccionar
 - 11: Tiempo excedido
 - 12: Problema de parámetros
 - 13/14: Solicitud/respuesta de marca de tiempo
 - 17/18: Solicitud respuesta de máscara de dirección (de subred)
- **Código:** Subtipo de mensaje

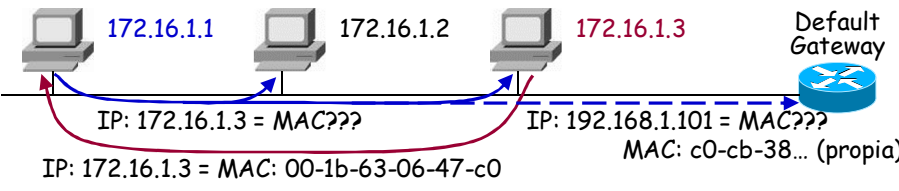


Protocolo de Resolución de Dirección (ARP)



68
Departamento de Telemática

- Permite obtener la dirección MAC del equipo que tiene asignada una dirección IP
- Solicitud por difusión, respuesta directa
- Cuando el equipo de destino está en otra LAN, la resolución de la dirección IP está a cargo de la puerta de enlace predeterminada (*default gateway*)



Resolución de direcciones IP



69

Protocolo de Resolución Inversa de Dirección (RARP)

- Obtiene la dirección IP de un computador del que se conoce la dirección física (MAC)
- Ejemplo: Estaciones de trabajo sin disco (diskless) que al arrancar no conocen su dirección IP; sólo su MAC.
- Se requiere un servidor RARP en la LAN, que administra las correspondencias MAC-IP
- Solicitud por difusión, respuesta directa

Resolución de direcciones IP



70

Protocolo de Inicialización (BOOTP)

- Similar a RARP, pero:
 - Suministra todos los parámetros de configuración de red del cliente, no sólo la dirección IP (e.g. máscara de subred, puerta de enlace y servidores DNS)
 - El servidor puede estar en una LAN distinta
En la LAN del cliente debe haber un agente (e.g. un enrutador) que captura la solicitud BOOT para re-enviarla al servidor remoto
- Cada dirección MAC tiene asignada una dirección IP en forma estática

Resolución de direcciones IP



71

Protocolo de Configuración Dinámica de Equipos (DHCP)

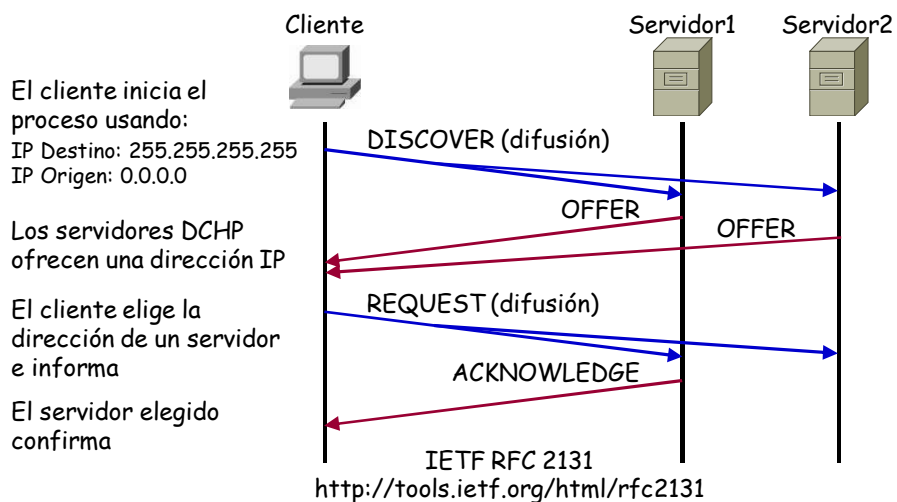
- Similar a BOOTP, pero la asignación de las direcciones IP puede ser:
 - **Manual (estática):** direcciones configuradas por el administrador de la red, y usadas por tiempo indefinido (equivalente a BOOTP)
 - **Automática:** direcciones asignadas según llegan las peticiones. El cliente las usa hasta que las libera.
 - **Dinámica:** direcciones asignadas de un rango disponible, por un intervalo de tiempo predefinido. Los clientes deben solicitar la renovación de su dirección transcurrido el 50% del tiempo de concesión.
- Facilita a un administrador cambiar las direcciones de los equipos en su red o a un portátil configurar su dirección al cambiar de red.

Resolución de direcciones IP



72

Protocolo de Configuración Dinámica de Equipos (DHCP)



Temario



73

- Generalidades del modelo TCP/IP
- Capa de acceso a la red: Ethernet
- Capa de red: Internet
- **Capa de transporte: TCP y UDP**
 - Protocolo TCP
 - Protocolo UDP
- Protocolos de enrutamiento
- Dispositivos de red

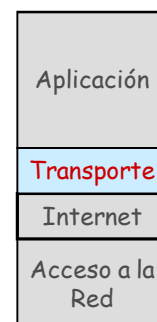
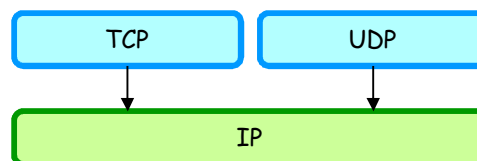
Capa de Transporte




74

Los protocolos más importantes y utilizados son:

- TCP: Transmission Control Protocol
- UDP: User Datagram Protocol





75
 Departamento de Telemática

Protocolo TCP

Transmission Control Protocol (Protocolo de Control de Transmisión)

- RFC 793 (1981)
- Orientado a conexión
 - Se establece una conexión antes de transferir información y se libera al final
- Garantiza un flujo confiable de información entre un cliente y un servidor
 - Corrección de errores
 - Control de flujo

Aplicación
Transporte
Internet
Acceso a la Red


76
 Departamento de Telemática

Formato del segmento TCP

32 bits			
Byte 1	Byte 2	Byte 3	Byte 4
Puerto de Origen		Puerto de Destino	
Número de Secuencia			
Número de Confirmación			
Long. cabecera	Reserva	Banderas	Tamaño de Ventana
Suma de Chequeo		Apuntador Urgente	
Opciones (opcional)			
Datos (opcional)			

IETF RFC 793
<http://tools.ietf.org/html/rfc793>

Formato del segmento TCP



77

- **Puerto de Origen y Destino:** identificador de la entidad de capa 4 (proceso o servicio). Ejs.: 21: FTP; 23: Telnet; 80: HTTP
- **Número de Secuencia:** identificador del primer byte del segmento en el sentido de ida (hacia adelante)
- **Número de Confirmación:** identificador del próximo byte que se espera recibir (confirma n-1)
- **Longitud de la cabecera TCP:** en palabras de 32 bits
- **Tamaño de Ventana:** cantidad máxima de bytes que se aceptan en el sentido de vuelta (control de flujo)
- **Suma de chequeo:** verificación de integridad del segmento
- **Apuntador Urgente:** Posición a partir del Número de Secuencia donde terminan los datos urgentes

Formato del segmento TCP



78

- **Banderas:**
 - CWR (Congestion Window Reduced): control de congestión
 - ECE (ECN Echo): Control de congestión
 - URG: Indica que el Apuntador Urgente es significativo
 - ACK: Indica que el Número de Confirmación es significativo
 - PSH (Push): Indica al receptor que debe entregar de inmediato los datos transportados a la capa superior
 - RST (Reset): Reiniciar la conexión
 - SYN (Synchronize): Indica fase de establecimiento de conexión
 - FIN: Indica fase de terminación de la conexión

Byte 2

C	E	U	A	P	R	S	F
W	C	R	C	S	S	Y	I
R	K	G	K	H	T	N	N

Establecimiento de conexión



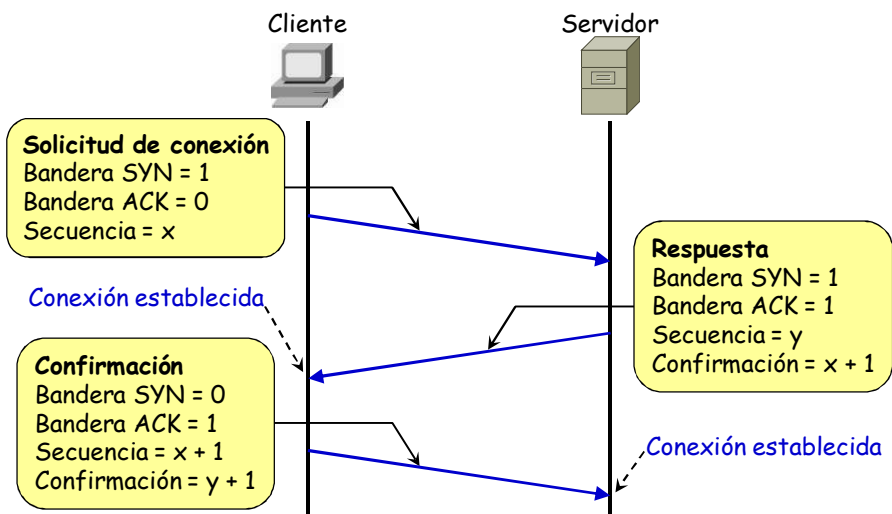
79

- Antes del establecimiento de conexiones, las aplicaciones deben abrir una conexión con TCP
- TCP está basado en el modelo cliente/servidor
 - El servidor espera peticiones: función pasiva
 - El cliente hace las peticiones: función activa
- Así mismo las aplicaciones abren las conexiones:
 - Servidor: **Apertura pasiva** (Passive OPEN). Se abre la conexión pero se permanece a la espera de peticiones
 - Cliente: **Apertura activa** (Active OPEN). La aplicación solicita a TCP iniciar la conexión con el otro equipo
- Cuando se abre la conexión en un extremo, se crea una estructura de datos para brindar soporte a la conexión: TCB (Transmission Control Block)

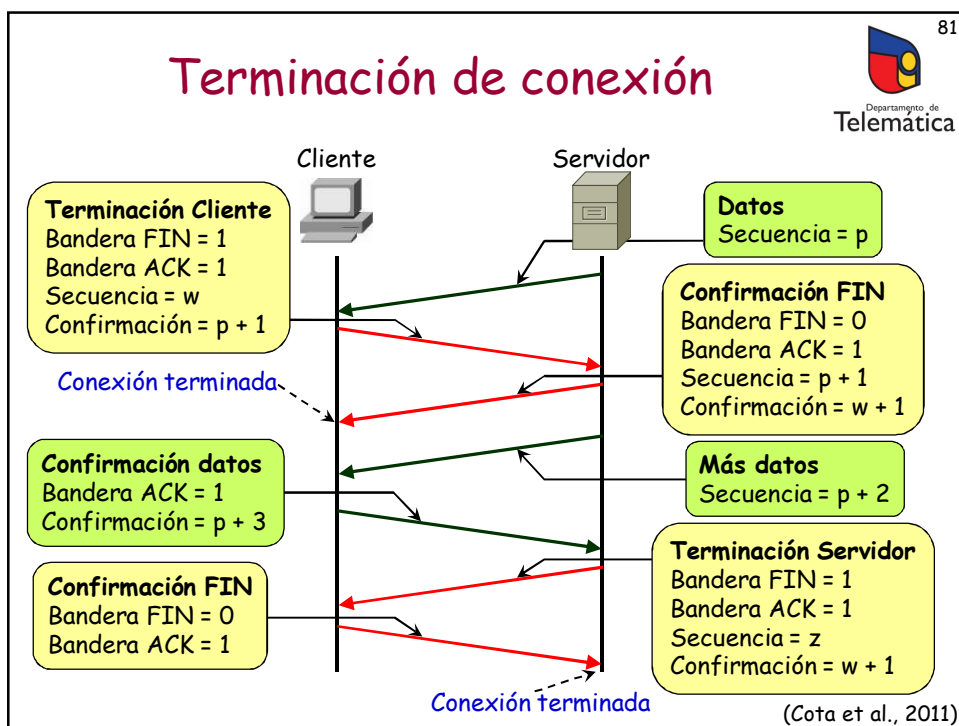
Establecimiento de conexión



80



(Cota et al., 2011)



Control de flujo

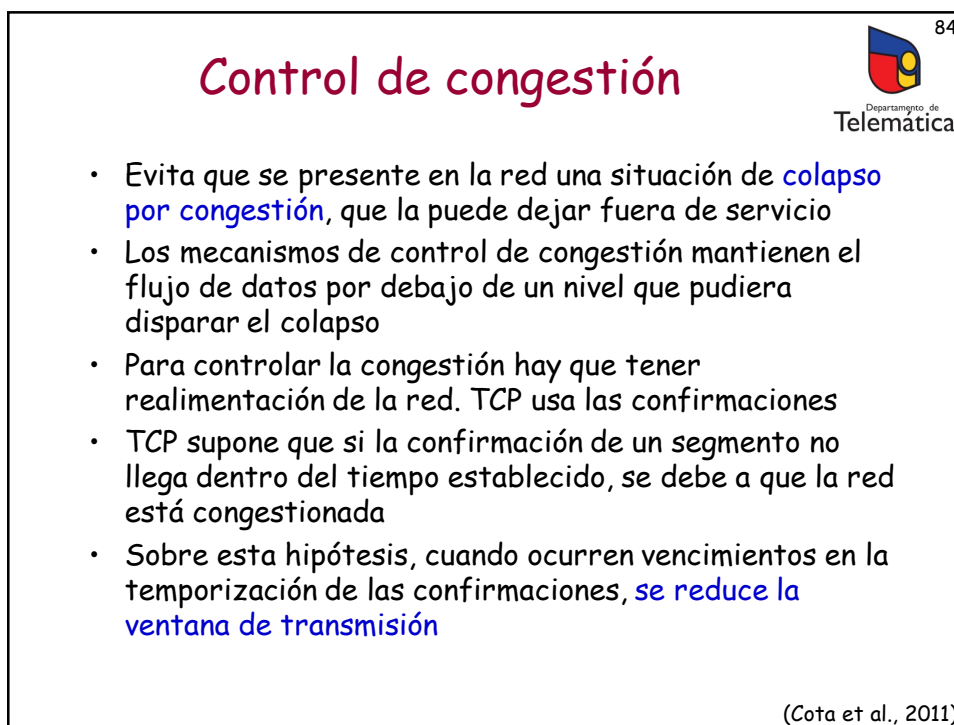
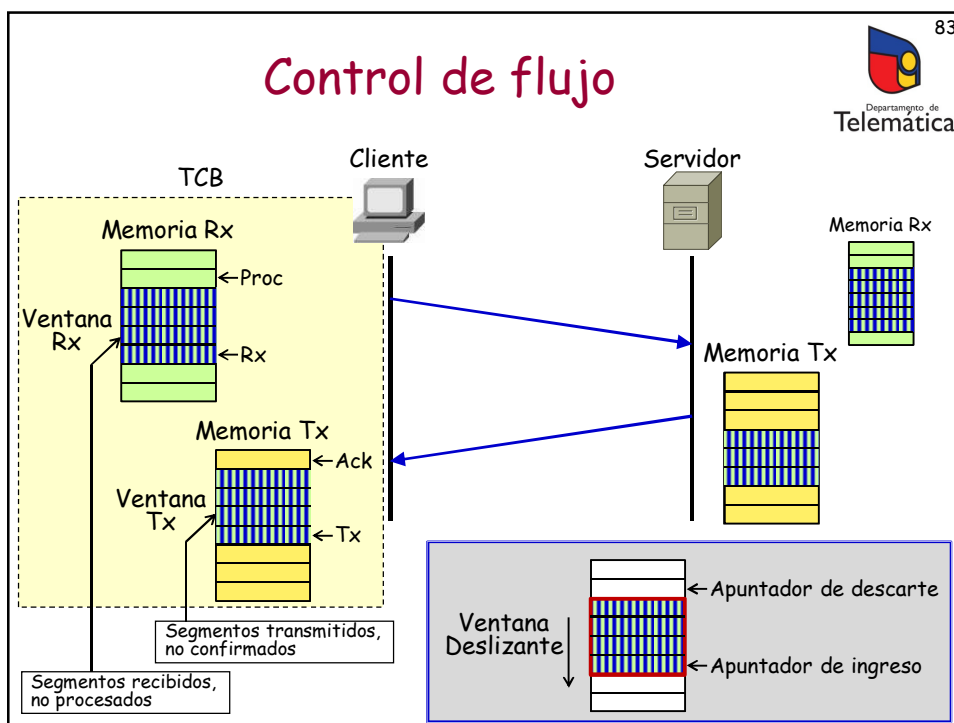
82
Departamento de Telemática

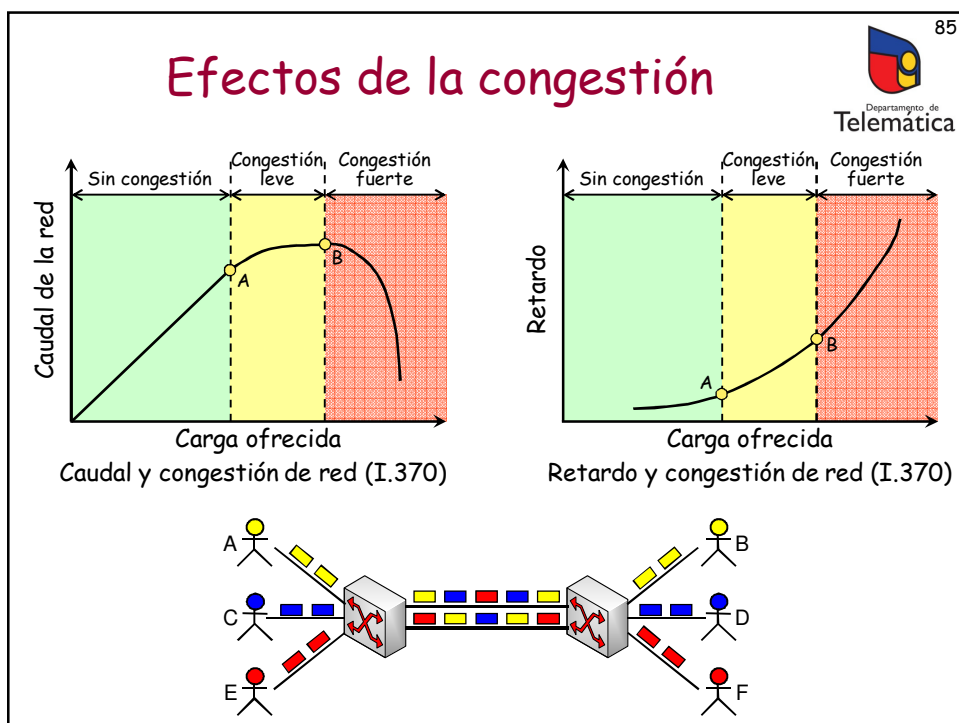
- Evita que el transmisor envíe datos demasiado rápido y no puedan ser procesados por el receptor
- TCP utiliza un protocolo de **ventana deslizante variable**
- Cada segmento tiene una indicación en octetos del tamaño de la **ventana de recepción** (bytes recibidos que no han sido entregados a las aplicaciones)
- El transmisor no puede tener una ventana de transmisión (bytes enviados pendientes de confirmación) mayor a la capacidad indicada para la ventana de recepción

Long. cabecera	Reserva	Banderas	Tamaño de Ventana
----------------	---------	----------	-------------------

Tamaño de Ventana: cantidad máxima de bytes que se aceptan en el sentido de vuelta (control de flujo)

(Cota et al., 2011)





86


Departamento de Telemática

Protocolo UDP

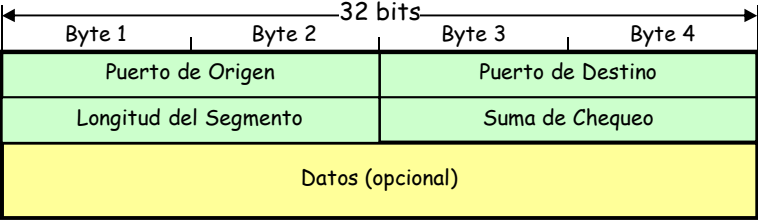
User Datagram Protocol (Protocolo de Datagramas de Usuario)

- RFC 768 (1980)
- Protocolo de transporte no orientado a conexión
 - No se requiere el establecimiento de una conexión para transferir información
- No confiable
 - No garantiza la entrega de la información ni corrige errores
- La única información que requiere de la capa de transporte son los puertos de origen y destino

Aplicación
Transporte
Internet
Acceso a la Red


87
 Departamento de Telemática


Formato del segmento UDP



- **Puerto de Origen y Destino:** identificador de la entidad de capa 4 (proceso o servicio). Ejs.: 53: DNS; 69: TFTP
- **Longitud del segmento:** en octetos
- **Suma de chequeo:** verificación de integridad del segmento

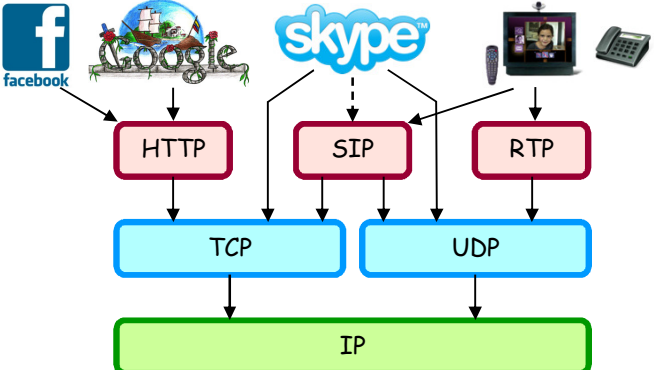
IETF RFC 768
<http://tools.ietf.org/html/rfc768>

DNS: Domain Name System
TFTP: Trivial File Transfer Protocol


88
 Departamento de Telemática

Usuarios de TCP y UDP

Ejemplos de protocolos usuarios



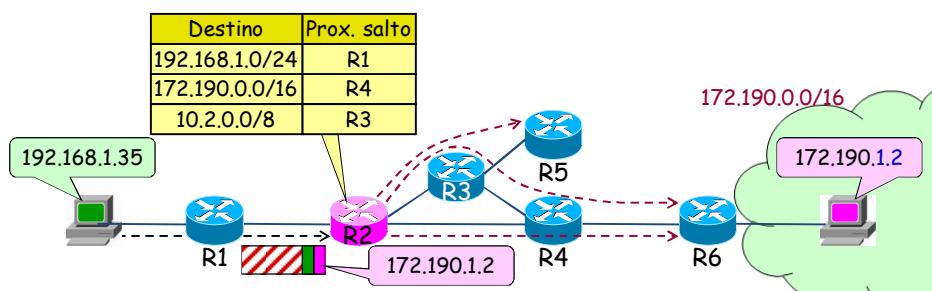
HTTP: Hypertext Transfer Protocol
 SIP: Session Initiation Protocol
 RTP: Real-time Transport Protocol


Temario

- Generalidades del modelo TCP/IP
- Capa de acceso a la red: Ethernet
- Capa de red: Internet
- Capa de transporte: TCP y UDP
- **Protocolos de enrutamiento**
 - Principios del enrutamiento
 - Protocolos de Vector Distancia (Ej.: RIP)
 - Protocolos de Estado del enlace (Ej.: OSPF)
- Dispositivos de red

Tabla de enrutamiento

- Los enrutadores realizan la función de **re-envío (forwarding)** encaminando los paquetes mediante la **Tabla de Enrutamiento**
- La Tabla de Enrutamiento contiene las direcciones y máscaras de las redes de destino y el próximo salto para llegar a ellas
- Los paquetes IP tienen en su cabecera la dirección de destino (dirección del equipo)





93
Departamento de Telemática

Tabla de enrutamiento

Longest prefix match

Dirección de destino= 192.168.2.33

Destino	Máscara	Próximo salto	Resultado AND	
192.168.1.128	/25	IP _{R1}	192.168.2.0	NO
192.168.1.0	/24	IP _{R2}	192.168.2.0	NO
192.168.0.0	/23	IP _{R3}	192.168.2.0	NO
192.168.0.0	/16	IP_{R5}	192.168.0.0	SI
192.0.0.0	/8	IP _{R6}		
0.0.0.0	/0	IP _{R7}		

Próximo salto: R5

Máscara /25

Destino 192.168.00000010.00100001

AND 255.255.11111111.10000000

= 192.168.00000010.00000000


Máscara /16

192.168.00000010.00100001

255.255.00000000.00000000

192.168.00000000.00000000

(Cota et al., 2011)



94
Departamento de Telemática


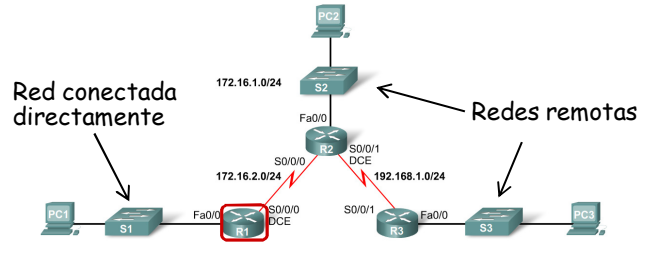


Tabla de enrutamiento

Información en la Tabla de Enrutamiento

- **Redes conectadas directamente:** a una de las interfaces (puertos) del enrutador.
- **Redes remotas:** sólo se pueden alcanzar a través de otro enrutador, mediante rutas estáticas o dinámicas.
- **Información detallada de las redes:** fuente de información (conectado directamente, ruta estática o dinámica), dirección y máscara de red, la interfaz de salida y/o la dirección IP del enrutador del siguiente salto.

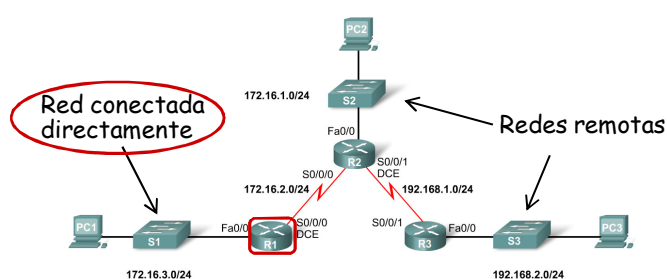


(CNA, 2009b)

Tabla de enrutamiento

Redes conectadas directamente

- Cuando la interfaz de un enrutador se **configura** con una dirección IP y una máscara, **el enrutador entra a hacer parte de la red conectada a dicha interfaz**
- La dirección de red y la máscara, más el tipo y número de interfaz, se registran en la Tabla de Enrutamiento como red conectada directamente

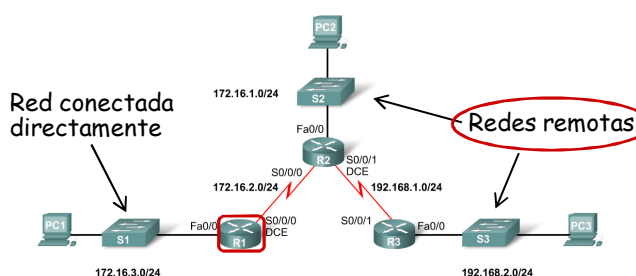


(CNA, 2009b)

Tabla de enrutamiento

Redes remotas

- No están conectadas directamente al enrutador
- Su información es registrada en la Tabla de Enrutamiento:
 - Mediante configuración de **rutas estáticas**
 - Mediante **protocolos de enrutamiento dinámico**



(CNA, 2009b)

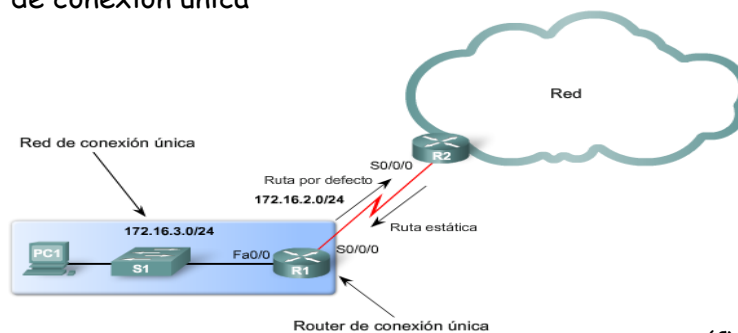


Rutas estáticas



97

- El administrador de la red configura la información de enrutamiento
- Mejor seguridad
- Mayor esfuerzo de administración
- Se usan generalmente cuando se enruta hacia una red de conexión única



(CNA, 2009b)



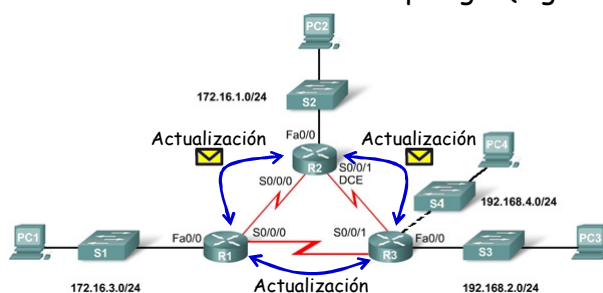
Protocolos de enrutamiento dinámico




98

Funciones:


- Permiten a los enrutadores compartir en forma dinámica información acerca de las redes remotas, y agregarla a sus Tablas de Enrutamiento
- Determinar cuál es la mejor ruta a un destino
- Actualizar de forma automática las Tablas de Enrutamiento cuando cambia la topología (e.g. nueva red)



(CNA, 2009b)




Protocolos de enrutamiento dinámico


99


Componentes:

- **Estructuras de datos.** Tablas o bases de datos, en la RAM del enrutador
- **Algoritmo:** Procesan la información de enrutamiento y determinan la mejor ruta
- **Mensajes:** Usados para descubrir enrutadores vecinos, intercambiar información de enrutamiento y otras acciones para conocer y mantener información precisa sobre la red

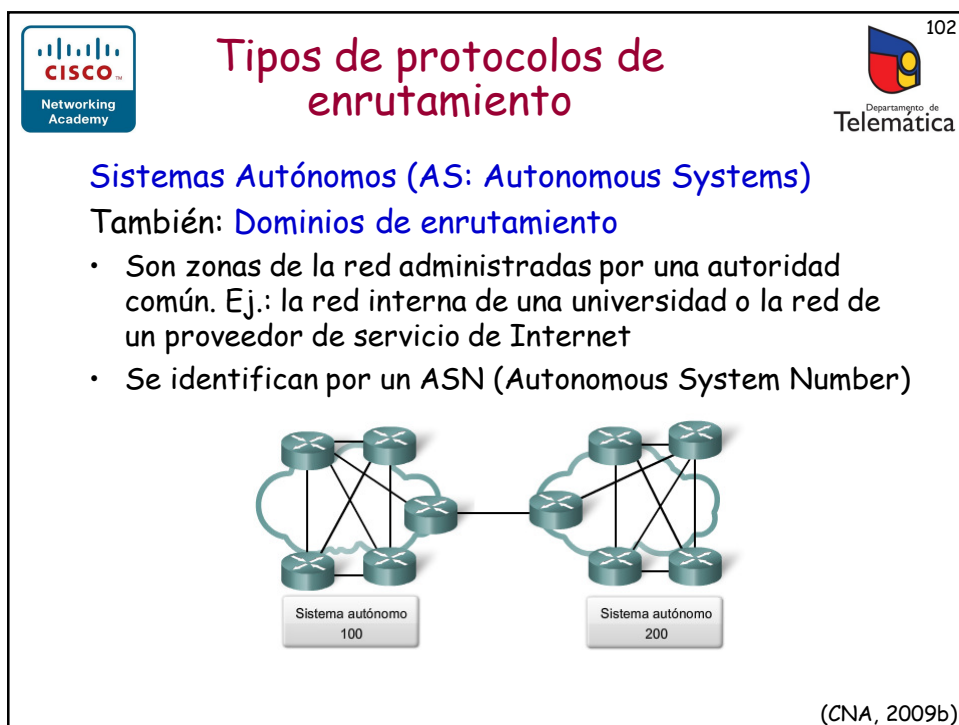
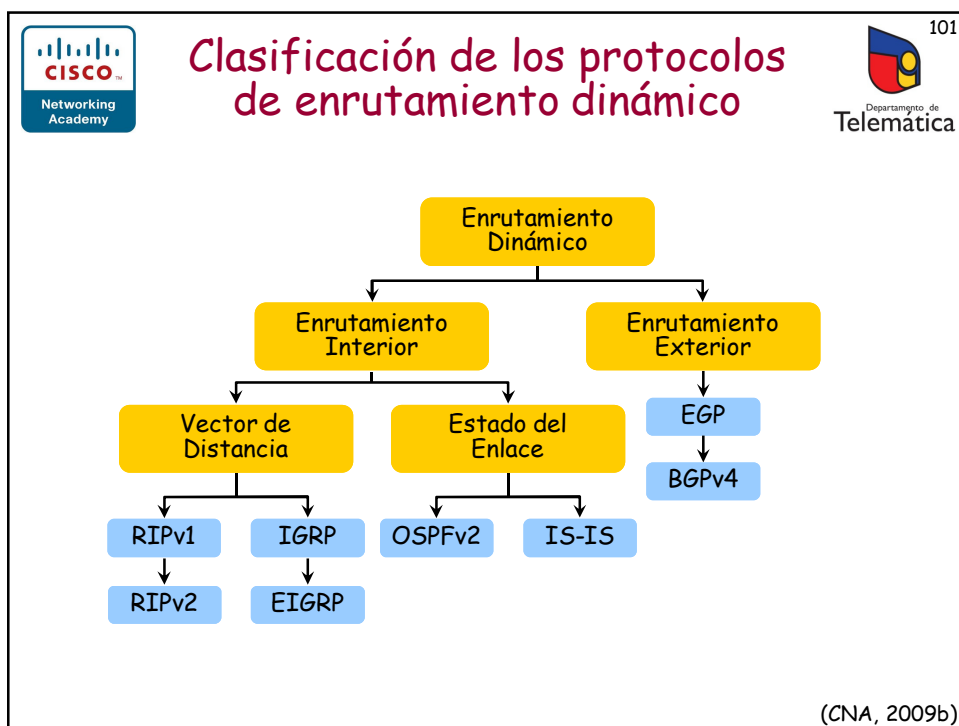
(CNA, 2009b)




Enrutamiento dinámico vs enrutamiento estático



100

Característica	Enrutamiento Dinámico	Enrutamiento Estático
Complejidad de la configuración	Independiente del tamaño de la red	Incrementa con el tamaño de la red
Conocimientos del administrador	Avanzados	No adicionales
Cambios de topología	Se adapta en forma automática	Requiere intervención del administrador
Escalamiento	Para topologías simples y complejas	Para topologías simples
Seguridad	Menos seguro	Más seguro
Uso de recursos	Usa CPU, memoria y ancho de banda	No requiere recursos adicionales
Capacidad de predicción	La ruta depende de topología actual	La ruta es siempre la misma





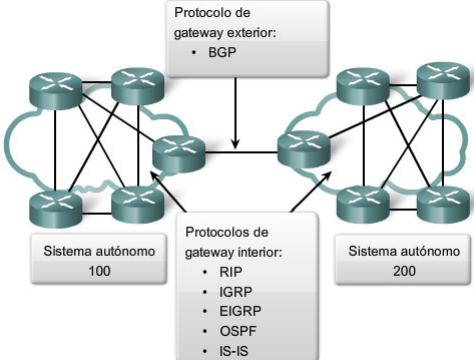
Tipos de protocolos de enrutamiento




103
Departamento de Telemática

Sistemas Autónomos (AS: Autonomous Systems)


- Dentro de las AS se utilizan **Protocolos de Enrutamiento Interior (IGP: Interior Gateway Protocols)**. Ej.: RIP, OSPF
- Entre AS se usan **Protocolos de Enrutamiento Exterior (EGP: Exterior Gateway Protocols)**. Ej.: BGP



(CNA, 2009b)



Tipos de protocolos de enrutamiento



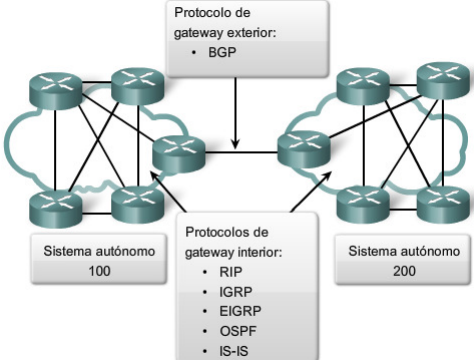
104
Departamento de Telemática

Protocolos de Enrutamiento Interior (IGP)

- Su objetivo es llegar por el mejor camino a todos los destinos dentro del AS. Son los "técnicos"

Protocolos de Enrutamiento Exterior (EGP)

- Hacen enrutamiento por políticas y pueden impedir/preferir ciertos tránsitos. Son los "políticos"



(Cota et al., 2011)

105



Departamento de Telemática

Tipos de protocolos de enrutamiento

Protocolos de Enrutamiento Interior (IGP)

Dos tipos: **Vector Distancia** y **Estado del Enlace**

- **Vector Distancia**
 - Las rutas se anuncian como vectores* de distancia y dirección
 - Distancia:** Valoración de la ruta (e.g. Número de saltos hasta el destino)
 - Dirección:** siguiente enrutador o interfaz de salida
- **Estado del Enlace**
 - Crean una vista completa de la topología de la red

Vector: magnitud (física) definida en términos de longitud y dirección

106

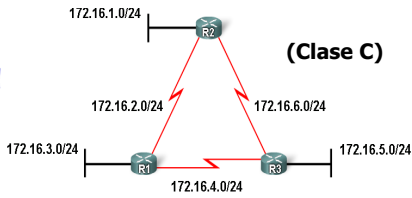
Departamento de Telemática

Cisco Networking Academy

Tipos de protocolos de enrutamiento

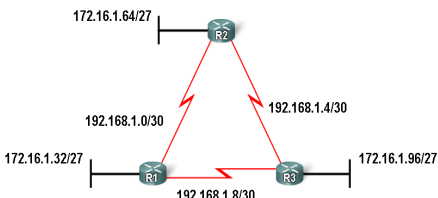
Protocolos con clase (classful) y sin clase (classless)

- **Protocolos con clase**
 - NO envían la máscara de subred en la actualización de las rutas
 - Basados en las direcciones IP clase A, B y C
- **Protocolos sin clase**
 - Envían la máscara de subred en la actualización de las rutas




(Clase C)

Classful: Subnet mask is the same throughout the topology




Classless: Subnet mask can vary in the topology

(CNA, 2009b)




(Otra) clasificación de los protocolos de enrutamiento




107
Departamento de Telemática

	Enrutamiento Interior				Enrutamiento Exterior
	Vector Distancia		Estado del enlace		Vector de Camino
Con clase	RIP	IGRP			EGP
Sin clase	RIPv2	EIGRP	OSPFv2	IS-IS	BGPv4
IPv6	RIPng	EIGRP para IPv6	OSPFv3	IS-IS para IPv6	BGPv4 para IPv6

(CNA, 2009b)

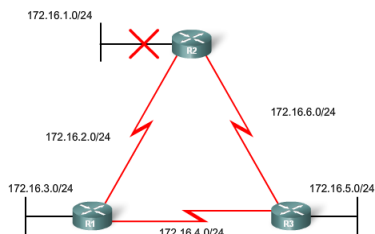


Convergencia



108
Departamento de Telemática

- Es el estado en el cual las Tablas de Enrutamiento de todos los enrutadores son **consistentes**
- Una red ha convergido cuando todos sus enrutadores tienen información completa y precisa sobre la red
- Una red no es completamente operativa hasta que converge
- Una propiedad de los protocolos de enrutamiento es su velocidad de convergencia:
 - RIP, IGRP: Convergencia lenta
 - EIGRP, OSPF: Convergencia rápida





Métricas



109

- Cuando existen varias alternativas para llegar al mismo destino, el enrutador selecciona la **mejor ruta** evaluando el costo de alcanzar el destino
- Los valores usados por el protocolo para asignar este costo se denominan **métricas**
- Cada protocolo tiene sus propias métricas
- Las métricas usadas por los protocolos de enrutamiento IP incluyen:
 - **Número de saltos** para llegar al destino
 - **Ancho de banda** de los enlaces hacia el destino
 - **Carga** de tráfico que manejan los enlaces
 - **Retardo** de los paquetes a través de la ruta
 - **Confiabilidad** de los enlaces
 - **Costo**: indicador de las preferencias del administrador

(CNA, 2009b)



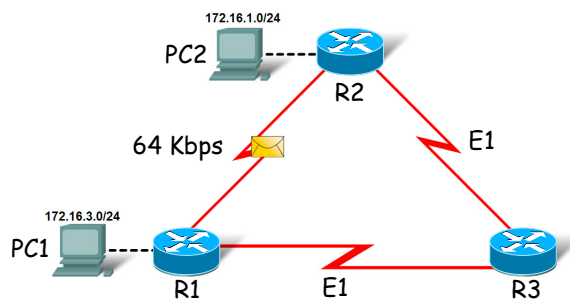
Métricas



110

R1 tiene dos rutas para enviar un paquete de PC1 a PC2

- RIP elige R2 usando la métrica del **número de saltos**
- OSPF elige R3-R2 usando la métrica del **ancho de banda**



(CNA, 2009b)



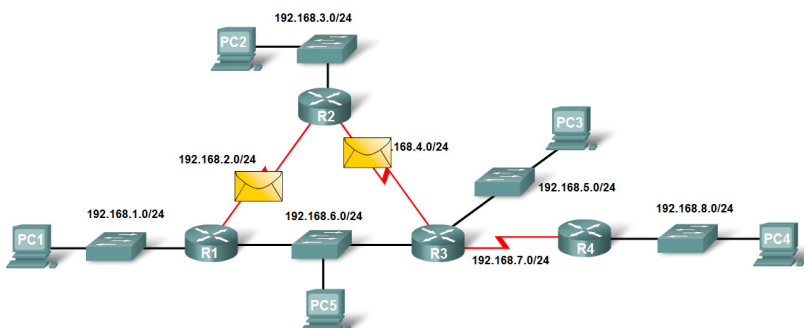
Métricas



111

Balace de carga

- Es la habilidad de un enrutador para distribuir paquetes entre varias rutas que tienen el mismo costo
- En el ejemplo, R2 balaceo el tráfico hacia PC5 sobre dos rutas de igual costo




(CNA, 2009b)

Distancia administrativa




112

- Un enrutador puede obtener de **varias fuentes de información** la ruta hacia un mismo destino.
- Por ejemplo, mediante una configuración de ruta estática y RIP, o usando RIP y OSPF
- Como usan métricas distintas, los costos de cada protocolo no son comparables.
- La **distancia administrativa** define la preferencia por una fuente de información de enrutamiento, calificando su **confiabilidad**.
- Es un valor de 0 a 255 que se asigna a cada fuente de información de enrutamiento, siendo 0 la más confiable.




Distancia administrativa




113

Valores predeterminados

Fuente de información	Distancia administrativa
Interfaz conectada (directa)	0
Ruta estática	1
Ruta resumida EIGRP	5
BGP externo	20
EIGRP interno	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EIGRP externo	170
BGP interno	200



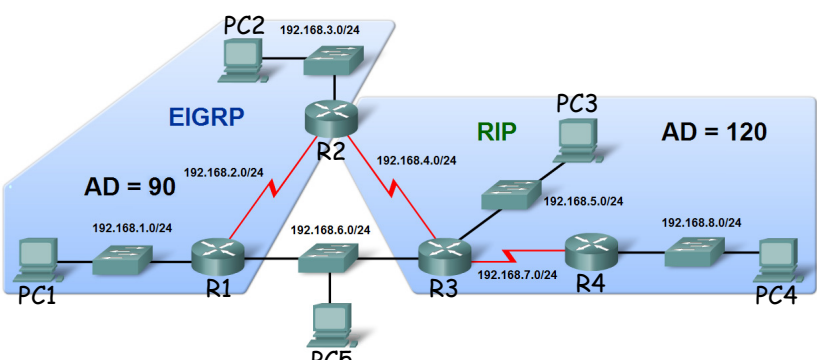
Distancia administrativa



114

R2 tiene dos rutas para enviar paquetes de PC2 a PC5

- La ruta por R1 se obtuvo usando EIGRP (AD=90)
- La ruta por R3 se obtuvo usando RIP (AD=120)
- R2 elige la ruta por R1 y la guarda en su Tabla de Enrutamiento



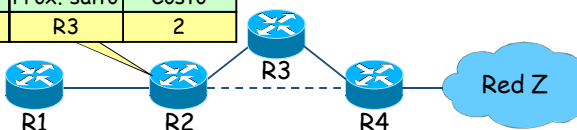
(CNA, 2009b)

Protocolos de Vector Distancia



- Cada enrutador mantiene una tabla con entradas:
destino → [distancia (costo), dirección (próximo salto)]
- Periódicamente envía actualizaciones de rutas a sus vecinos, con los destinos y distancias que conoce
- Cuando recibe una actualización de un vecino, suma el costo recibido de cada destino con el costo del enlace con el vecino
- Si obtiene un costo menor o igual al que tenía para el destino, toma el nuevo
- Si el costo es mayor, descarta la información

Destino	Prox. salto	Costo
Z	R3	2

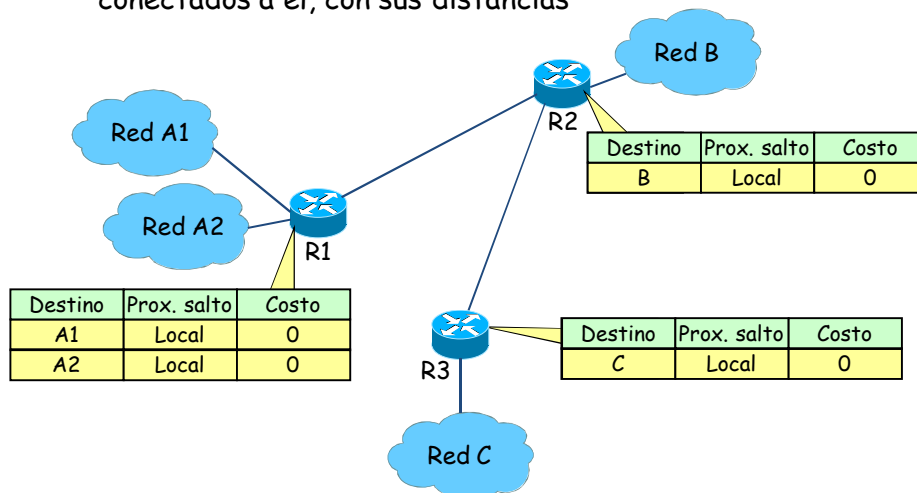


(Cota et al., 2011)

Protocolos de Vector Distancia



- Inicialmente, cada enrutador sólo conoce los destinos conectados a él, con sus distancias



(Cota et al., 2011)

117

Protocolos de Vector Distancia

Departamento de Telemática

- Luego, cada enrutador envía a sus vecinos la información que conoce

Destino	Prox. salto	Costo
A1	Local	0
A2	Local	0

Destino	Prox. salto	Costo
B	Local	0

Destino	Prox. salto	Costo
C	Local	0

(Cota et al., 2011)

118

Protocolos de Vector Distancia

Departamento de Telemática

- Con la información recibida, cada enrutador actualiza su **Tabla de Enrutamiento**

Destino	Prox. salto	Costo
A1	Local	0
A2	Local	0
B	R2	1

Destino	Prox. salto	Costo
B	Local	0
A1	R1	1
A2	R1	1
C	R3	1

Destino	Prox. salto	Costo
C	Local	0
B	R2	1

(Cota et al., 2011)

119

Departamento de Telemática

Protocolos de Vector Distancia

- Se repite el ciclo con la nueva información

Destino	Prox. salto	Costo
A1	Local	0
A2	Local	0
B	R2	1

Destino	Prox. salto	Costo
B	Local	0
A1	R1	1
A2	R1	1
C	R3	1

Destino	Prox. salto	Costo
C	Local	0
B	R2	1

(Cota et al., 2011)

120

Departamento de Telemática

Protocolos de Vector Distancia

- De nuevo se actualizan las Tablas de Enrutamiento

Destino	Prox. salto	Costo
A1	Local	0
A2	Local	0
B	R2	1
C	R2	2

Destino	Prox. salto	Costo
B	Local	0
A1	R1	1
A2	R1	1
C	R3	1

Destino	Prox. salto	Costo
C	Local	0
B	R2	1
A1	R2	2
A2	R2	2

(Cota et al., 2011)

121

Departamento de Telemática

Protocolos de Vector Distancia

- La convergencia se alcanza cuando **todas las Tablas de Enrutamiento** en la red contienen **la misma información**

Destino	Prox. salto	Costo
A1	Local	0
A2	Local	0
B	R2	1
C	R2	2

Destino	Prox. salto	Costo
B	Local	0
A1	R1	1
A2	R1	1
C	R3	1

Destino	Prox. salto	Costo
C	Local	0
B	R2	1
A1	R2	2
A2	R2	2

(Cota et al., 2011)

122

Departamento de Telemática

Protocolos de Vector Distancia

Al **cambiar la topología...**


- Actualización por evento

Destino	Prox. salto	Costo
A1	Local	0
A2	Local	0
B	R2	1
C	R3	1

Destino	Prox. salto	Costo
B	Local	0
A1	R1	1
A2	R1	1
C	R3	1

Destino	Prox. salto	Costo
C	Local	0
B	R2	1
A1	R1	1
A2	R1	1

(Cota et al., 2011)



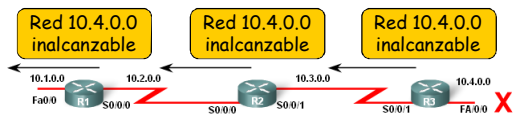
123

Protocolos de Vector Distancia


Departamento de Telemática

Actualizaciones por eventos (triggered updates)

- Se usan para aumentar la velocidad de convergencia cuando hay un cambio de topología
- El enrutador que detecta el cambio no espera el intervalo de actualización. Envía de inmediato un mensaje de actualización a sus vecinos
- Los receptores a su vez propagan la actualización
- Eventos que disparan las actualizaciones:
 - Cambio de estado de una interfaz
 - Una ruta se vuelve inalcanzable
 - Se registra una ruta en la Tabla de Enrutamiento



(CNA, 2009b)



124

Protocolos de Vector Distancia

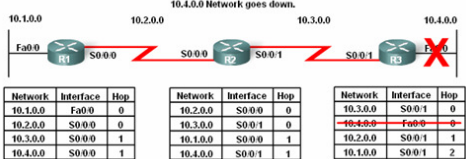
Departamento de Telemática

Bucles de enrutamiento (routing loops)

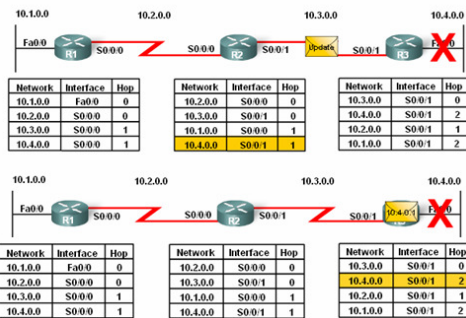
- Es una condición en la cual un **paquete es transferido continuamente** entre una serie de enrutadores, sin alcanzar nunca su destino
- Ocurre cuando varios enrutadores tienen información de enrutamiento que indica que existe una ruta válida a un destino inalcanzable

Routing Loop

10.4.0.0 Network goes down.



Before R3 can send an update, R2 sends an update.



(CNA, 2009b)



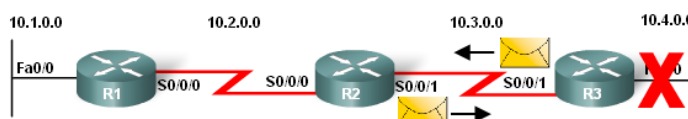
Protocolos de Vector Distancia



125

Conteo a Infinito (count to infinity)

- Se produce como resultado de una actualización imprecisa de las Tablas de Enrutamiento
- En cada ronda de actualización se incrementa el número de saltos hacia un destino
- Produce un **bucle de enrutamiento**



Network	Interface	Hop
10.1.0.0	Fa0/0	0
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/0	1
10.4.0.0	S0/0/0	24

Network	Interface	Hop
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/1	0
10.1.0.0	S0/0/0	1
10.4.0.0	S0/0/1	23

Network	Interface	Hop
10.3.0.0	S0/0/1	0
10.4.0.0	S0/0/1	22
10.2.0.0	S0/0/1	1
10.1.0.0	S0/0/1	2

(CNA, 2009b)



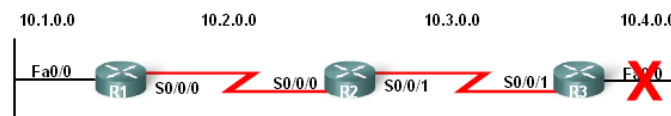
Protocolos de Vector Distancia



126

Conteo a Infinito (count to infinity)

- Los protocolos de Vector Distancia establecen un valor "infinito" para el número de saltos.
- En RIP, infinito = 16
- Cuando un enrutador alcanza el valor "infinito", marca la ruta como inalcanzable.




Network	Interface	Hop
10.1.0.0	Fa0/0	0
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/0	1
10.4.0.0	S0/0/0	16


Network	Interface	Hop
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/1	0
10.1.0.0	S0/0/0	1
10.4.0.0	S0/0/1	16

Network	Interface	Hop
10.3.0.0	S0/0/1	0
10.4.0.0	S0/0/1	16
10.2.0.0	S0/0/1	1
10.1.0.0	S0/0/1	2

(CNA, 2009b)



Protocolos de Vector Distancia



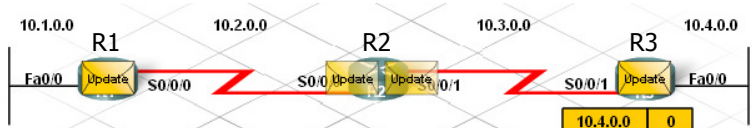
127
Departamento de Telemática

Regla de Horizonte Dividido (Split Horizon Rule)

- Usada para prevenir bucles de enrutamiento.
- Un enrutador no debe anunciar una red a través del enrutador del cual provino la actualización.

Regla de horizonte dividido para 10.4.0.0

- R3 la anuncia a R2
- R2 sólo la anuncia a R1




Network	Interface	Hop
10.1.0.0	Fa0/0	0
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/0	1
10.4.0.0	S0/0/0	1


Network	Interface	Hop
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/1	0
10.1.0.0	S0/0/0	1
10.4.0.0	S0/0/1	1

Network	Interface	Hop
10.3.0.0	S0/0/1	0
10.4.0.0	Fa0/0	0
10.2.0.0	S0/0/1	1
10.1.0.0	S0/0/1	2

(CNA, 2009b)



RIP



128
Departamento de Telemática

Routing Information Protocol (Protocolo de Información de Enrutamiento): Es un protocolo de Vector Distancia

- Basado en los algoritmos de Bellman, Ford y Fulkerson, implementados en 1969 en ARPANET
- Medios de los 70: Xerox desarrolla el protocolo GWINFO, que evolucionó a RIP
- 1982: BSD Unix implementa RIP, haciéndolo popular
- 1988: IETF publica el RFC 1058, documentando el protocolo existente
- 1994: RFC 1723: RIPv2
- 1997: RFC 2080: RIPv2

(CNA, 2009b)

RIP



129

RIPv1 - RFC 1058

- Obsoleto
- Sólo maneja las clases de direcciones IP originales A, B y C (**classful**).
- No soporta máscaras de subred variables (VLSM), es decir, CIDR
- Para cada destino, el enrutador almacena al menos la siguiente información:
 - Dirección IP el destino
 - La métrica (número de saltos) para llegar a él
 - La dirección IP del próximo salto
 - Banderas para indicar el estado de actualización
 - Temporizadores asociados a la entrada en la tabla

(Cota et al., 2011)

RIP



130

RIPv1 - RFC 1058

- Utiliza UDP (puerto UDP 520) para el intercambio de mensajes (por difusión) entre los enrutadores
- Envía actualizaciones de rutas cada 30 segundos
- Implementa actualizaciones por eventos
- Implementa la regla de horizonte dividido
- El número máximo de saltos es 15
- Distancia administrativa = 120
- No soporta autenticación para la actualización de rutas
- Puede hacer balance de carga
- Usado en redes pequeñas o al borde de redes grandes
- Fácil de configurar

RIP



131

RIPv2 - RFC 1723

- Extiende la funcionalidad de RIPv1
- Soporta enrutamiento sin clase (**classless**).
- Envía las máscaras de subred en las actualizaciones de enrutamiento.
- Utiliza una dirección de multidifusión (224.0.0.9) para los mensajes de petición, en lugar la de difusión de RIPv1
- Permite autenticación en la actualización de las rutas
- Usa el mismo formato de mensaje de RIPv1 pero modifica el formato de los parámetros (entradas de ruta) y agrega nuevas entradas de ruta

Protocolos de Estado del Enlace



132

- Idea básica: **construir el grafo de la red**. A partir del grafo, **calcular las mejores rutas** a todos los destinos.
- **Paso 1:** Identificación de las redes conectadas directamente al enrutador (por configuración)
- **Paso 2:** Descubrimiento de los vecinos (y el estado de los enlaces) mediante el protocolo HELLO
- **Paso 3:** Construcción del Paquete de Estado de Enlaces (LSP) con información de cada enlace
- **Paso 4:** Envío del LSP a todos los vecinos, que la guardan y re-envían hasta que todos tienen la misma información
- **Paso 5:** Construcción del grafo de la red y cálculo de los caminos más cortos
- **Paso 6:** Construcción de la Tabla de Enrutamiento



133

Departamento de Telemática

Protocolos de Estado del Enlace

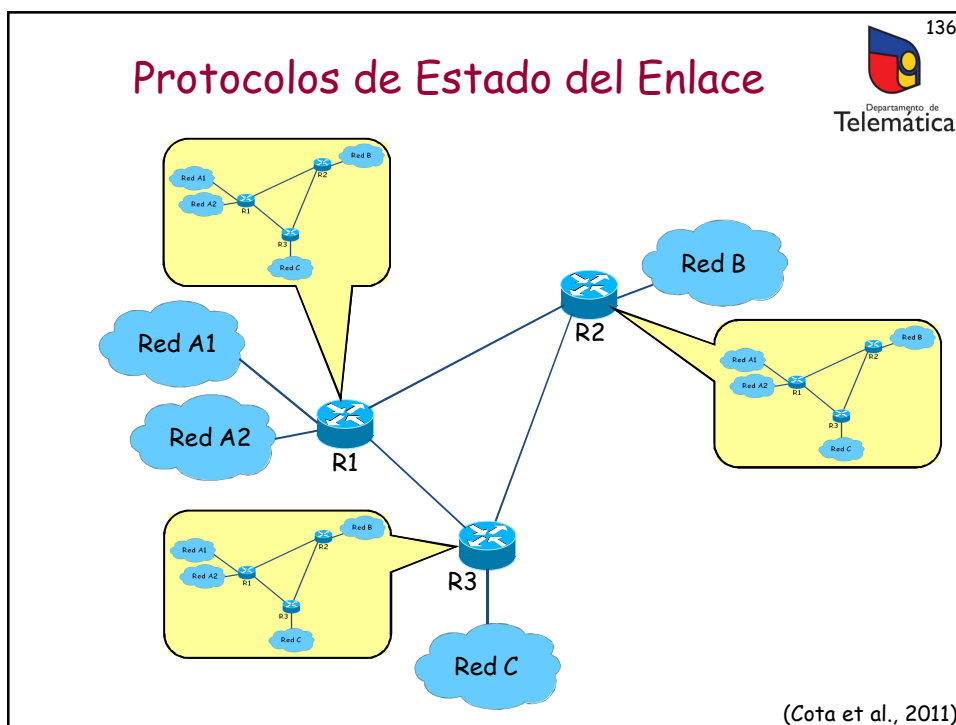
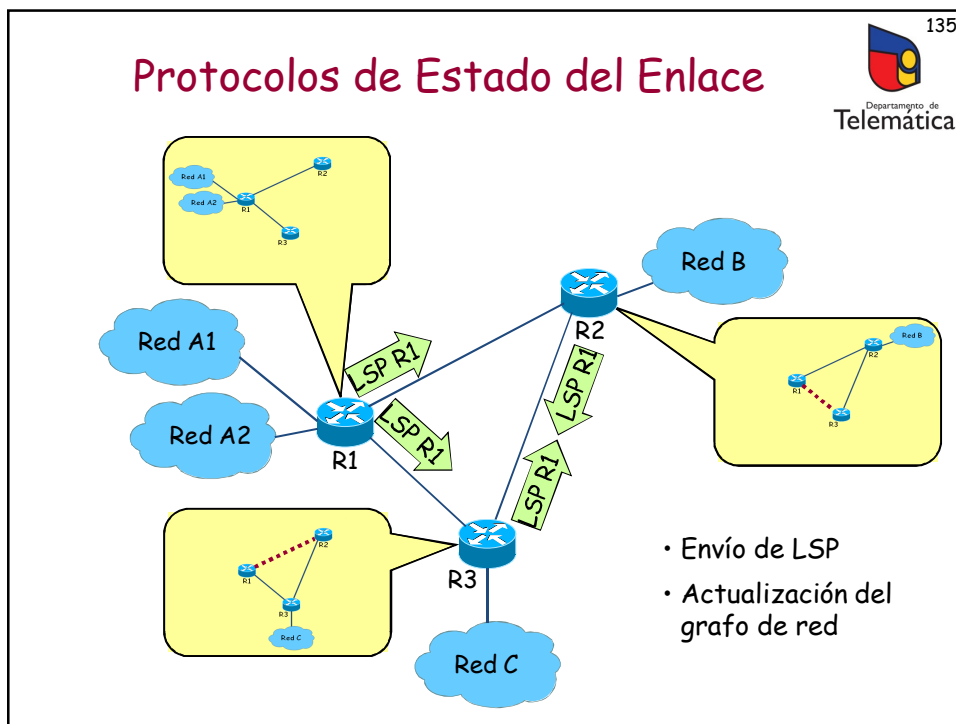
- Cada enrutador conoce sus redes conectadas directamente
- Envían Hello para identificar a sus vecinos

134

Departamento de Telemática

Protocolos de Estado del Enlace

Primer grafo de red construido por cada enrutador





Protocolos de Estado del Enlace



Estado del Enlace: Información sobre una interfaz del enrutador, que contiene:

- Dirección y máscara de subred
- Dirección IP
- Tipo de red (Ethernet, serial, etc.)
- Costo asociado al enlace (e.g. velocidad)
- Enrutadores vecinos del enlace
- El estado de todos los enlaces del enrutador se envía en el Paquete de Estado del Enlace (LSP)
- Después de la avalancha inicial, se envían LSP adicionales cuando ocurre un **cambio en la topología** (no hay envío periódico)

Enlace 1:
 • Red 10.1.0.0/16
 • Dirección IP 10.1.0.1
 • Tipo de red: Ethernet
 • Costo: 2
 • Vecinos: Ninguno



Enlace 2:
 • Red 10.2.0.0/16
 • Dirección IP 10.2.0.1
 • Tipo de red: Serial
 • Costo: 20
 • Vecinos: R2

(CNA, 2009b)



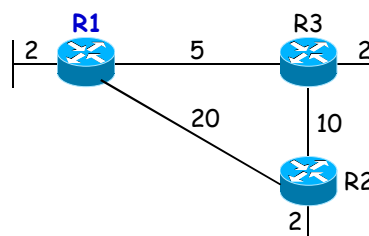
Protocolos de Estado del Enlace



- Para calcular las rutas utilizan algoritmos de "primer camino más corto": Shortest Path First (SPF)
- Se utiliza el algoritmo SPF de Dijkstra*
- El camino más corto no es necesariamente el de menor número de saltos (depende de las métricas)

Análisis en R1


Destino	Camino	Costo
LAN R2	R1 a R2	22
LAN R2	R1 a R3 a R2	17



* Edsger Dijkstra: Investigador en informática holandés, Premio Turing 1972

(CNA, 2009b)

139


Departamento de
Telemática


Comparación


Protocolos de Vector Distancia vs Estado del Enlace

Característica	Vector Distancia	Estado del Enlace
Qué envía ?	Todo lo que aprendió	Solo distancias a sus vecinos
A quién envía ?	A sus vecinos	A todos los enrutadores que participan del protocolo
Convergencia frente a cambios de topología	Lenta (por conteo a infinito)	Rápida
Carga a la red	Mucha (propaga todo periódicamente)	Poca (informa cuando hay cambios)
Necesidad de CPU y memoria	Baja	Alta

(Cota et al., 2011)

140


Departamento de
Telemática

 **CISCO**
Networking Academy

OSPF

Open Shortest Path First (Protocolo Abierto del Primer Camino Más Corto)

- Protocolo de estado del enlace
- Abierto (no depende de un fabricante)
- Inició en 1987
- 1989: OSPFv1, experimental, nunca se desplegó
- 1991: OSPFv2, publicado en RFC 1247
- 1998: OSPFv2 actualizado en RFC 2328
- 1999: OSPFv3 publicado en RFC 2740, para IPv6

(CNA, 2009b)

OSPF



141

OSPF v2


- Realiza enrutamiento jerárquico a dos niveles
- Soporta enrutamiento sin clase (classless), y máscaras de subred de tamaño variable (VLSM)
- Rápida convergencia
- Sólo envía actualizaciones por eventos
- Distancia administrativa = 110 por defecto
- Usa como métrica el "costo del enlace", definido por el administrador
- Cisco usa como costo la velocidad de la interfaz, calculada como $10^8/BW$ (costo= 1 para 100 Mbps)
- Permite cifrado y autenticación de la información de enrutamiento
- No tiene límite de saltos
- Soporta balanceo de carga por múltiples caminos

Temario




142

- Generalidades del modelo TCP/IP
- Capa de acceso a la red: Ethernet
- Capa de red: Internet
- Capa de transporte: TCP y UDP
- Protocolos de enrutamiento
- **Dispositivos de red**
 - Capa 1: Distribuidor
 - Capa 2: Puente y Conmutador
 - Capa 3: Enrutador y Conmutador Capa 3

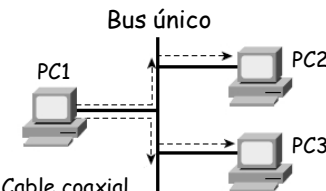


Capa 1: Distribuidor



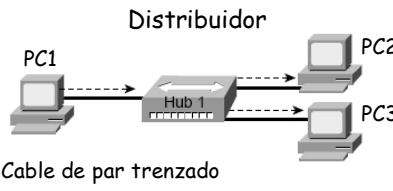
143
Departamento de
Telemática

Bus único



Cable coaxial


Distribuidor




Cable de par trenzado

- En un **dominio de colisión** la trama de una fuente puede colisionar con la trama de otra fuente
- Sólo una fuente puede enviar una trama a la vez
- Las tramas de difusión son escuchadas por todos los otros dispositivos
- El **distribuidor (hub)** actúa como un bus único: reenvía todos los paquetes recibidos en un puerto a los demás puertos

(Odom, 2004)

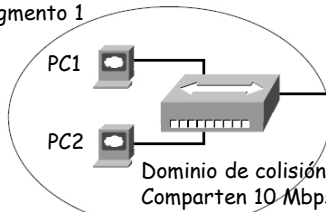



Capa 2: Puente



144
Departamento de
Telemática

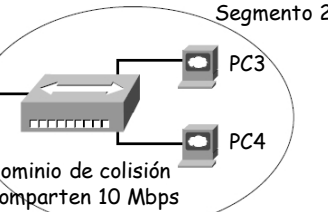
Segmento 1





Bridge


Segmento 2




El **puente (bridge)** separa los dominios de colisión en las redes Ethernet: **segmentación de LAN**

- En cada dominio una fuente puede enviar tramas al tiempo
- El puente registra las MAC de las fuentes (bridge table)
- Usando MAC de destino decide si reenvía las tramas
- Reenvía todas las tramas de unidifusión a MAC desconocida, las de multidifusión y las de difusión

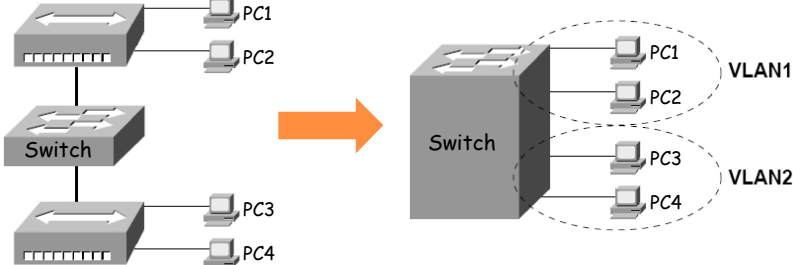
(Odom, 2004)



Capa 2: Conmutador



145
Departamento de Telemática




Dominio de difusión: Conjunto de dispositivos que reciben una trama de difusión enviada por cualquiera de ellos: **subred IP**


El **conmutador (switch)** separa los dominios de difusión: crea **VLAN (LAN virtuales)**

- Agrupa usuarios por departamentos o grupos de trabajo
- Reduce sobrecarga limitando el tamaño de cada dominio
- Mejora la seguridad separando dispositivos sensibles
- Separa tráfico especializado: e.g. teléfonos IP

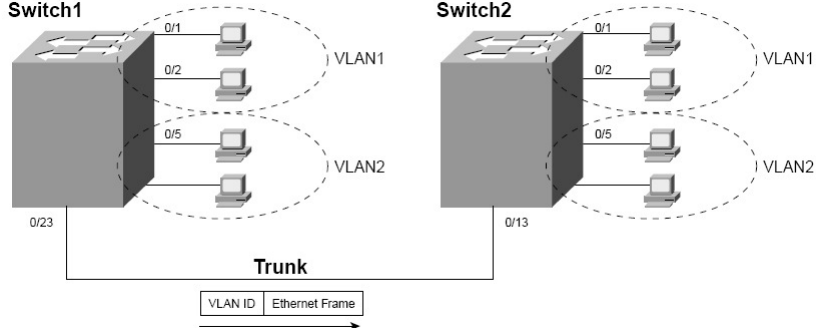
(Odom, 2004)



Entroncamiento de VLAN




146
Departamento de Telemática




Los protocolos para entroncamiento (trunking) de VLAN permiten tener dispositivos de una misma VLAN en uno o más conmutadores:

- CISCO Inter-Switch Link (ISL)
- IEEE 802.1q

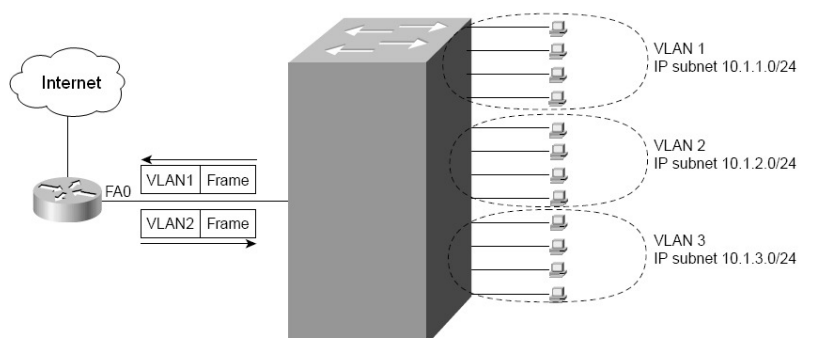
(Odom, 2004)



Interconexión de VLAN




147
Departamento de
Telemática




- El conmutador tiene una tabla de **direcciones MAC** por cada VLAN. No puede reenviar paquetes de una VLAN a otra
- Una VLAN corresponde a una subred IP
- Para enviar tramas de una VLAN a otra se requiere un **enrutador**, que encamina paquetes con base en la dirección IP

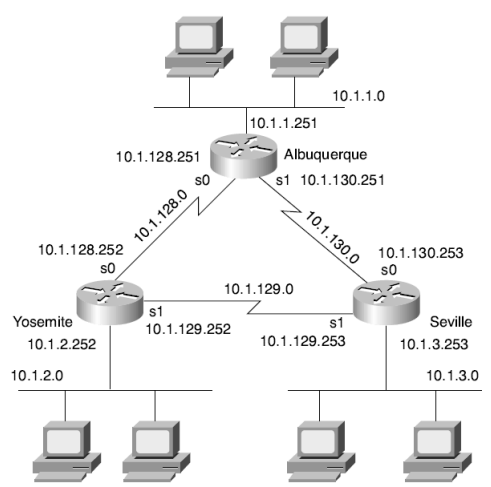
(Odom, 2004)



Capa 3: Enrutador



148
Departamento de
Telemática



El enrutador reenvía paquetes de una LAN/VLAN a otra con base en la **dirección IP**

(Odom, 2004)

149

Departamento de Telemática

Enrutador

Los enrutadores tienen dos componentes:

- Control
- Reenvío

The diagram illustrates a router as a blue cylinder with a white starburst pattern on top. Inside, there are two yellow boxes: 'Control' (containing a dashed 'FIB') and 'Reenvío'. Dotted arrows show 'Información de Enrutamiento' flowing in and out of the Control box. Solid arrows show 'Paquetes' (packets) entering and leaving the Reenvío box.

150

Departamento de Telemática

Enrutador

Componente de Control:

- Intercambia información de enrutamiento usando protocolos como RIP, OSPF, BGP, etc.
- Gestiona la tabla de enrutamiento: **Forwarding Information Base (FIB)**
- FIB asocia los puertos (interfaces) de salida a direcciones de red (prefijos)

Destino	Interfaz
10.0.0.0	FastEthernet0/0
192.168.1.0	FastEthernet1/0
172.190.0.0	FastEthernet0/0

The diagram shows a close-up of the Control component. It features a yellow box labeled 'Control' containing a dashed 'FIB' box, and a yellow box labeled 'Reenvío' below it. Dotted arrows indicate the exchange of 'Información de Enrutamiento' between the Control box and the external environment. A solid double-headed arrow connects the Control and Reenvío boxes.

151

Departamento de Telemática

Enrutador

Componente de Reenvío:

- Extrae de la cabecera del paquete la dirección IP de destino
- Usa el algoritmo de emparejamiento del prefijo más largo (*longest prefix match*) para encontrar una entrada en la FIB que corresponda a la dirección IP de destino
- Obtiene de la FIB el puerto (interfaz) de salida al que debe enviar el paquete

172.190.1.2

Control

FIB

Reenvío

Destino	Interfaz
10.0.0.0	FastEthernet0/0
192.168.1.0	FastEthernet1/0
172.190.0.0	FastEthernet0/0

Paquetes → Paquetes

152

Departamento de Telemática

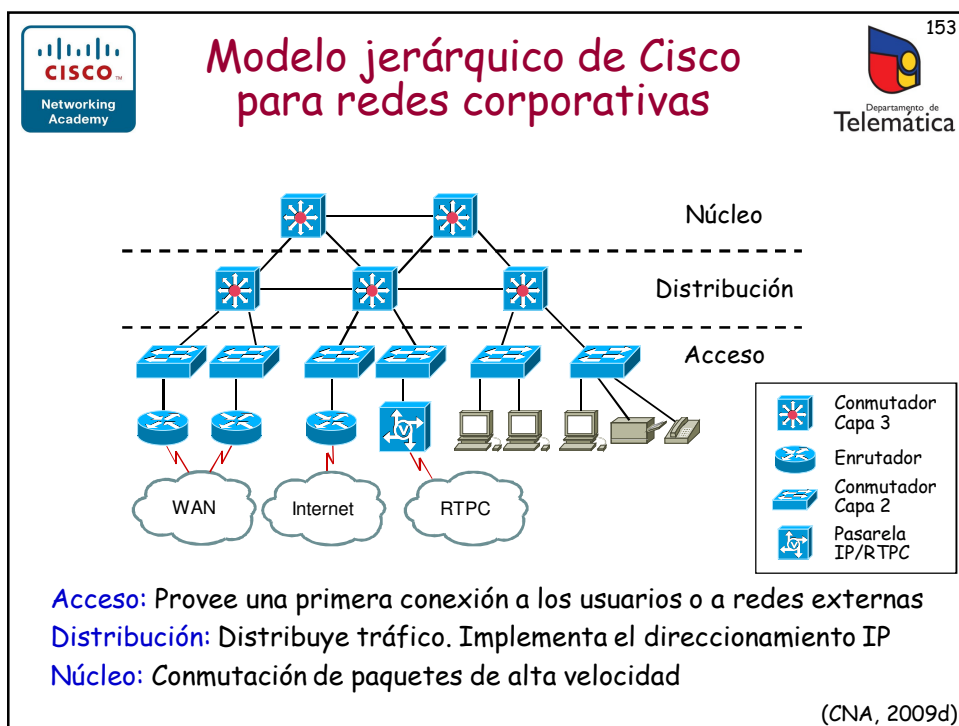
Cisco Networking Academy

Conmutador capa 3

VLAN 1 (PC1) — Conmutador Capa 2 — VLAN 2 (PC2)
 ↓
 VLAN 1 (PC1) — Conmutador Capa 3 — VLAN 2 (PC2)

- Es un conmutador que también tiene funciones de enrutamiento
- Se comporta igual que la combinación:
enrutador + conmutador capa 2
- Gestión de VLAN más interconexión de LAN/VLAN

(Odom, 2004)



154

Departamento de Telemática

Bibliografía

- CNA (2009a). "CCNA Exploration. Network Fundamentals", Version 4.0. Cisco Networking Academy, Cisco Press, Indianapolis, USA
- CNA (2009b). "CCNA Exploration. Routing Protocols and Concepts", Version 4.0. Cisco Networking Academy, Cisco Press, Indianapolis, USA
- W. Odom (2004). "CCNA INTRO Exam Certification Guide". Cisco Press, Indianapolis, USA.
- W. R. Araya (2006). "Tema 3. El Nivel de Red en Internet". Curso "Redes WAN: IP, ATM", Servicios Profesionales, Chile.
- E. Cota et al. (2011). Material del curso "Ruteo IP y tecnologías de transporte". Universidad de la República, Uruguay.
- CNA (2009c). "CCNA Exploration. LAN Switching and Wireless", Version 4.0. Cisco Networking Academy, Cisco Press, Indianapolis, USA
- CNA (2009d). "CCNA Exploration. Accessing the WAN", Version 4.0. Cisco Networking Academy, Cisco Press, Indianapolis, USA
- D. Morató (2010). "Introducción a las redes". Curso "Redes de Banda Ancha". Universidad Pública de Navarra, España.