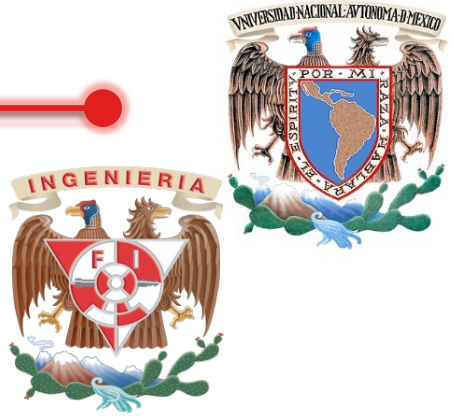
REDES DE DATOS



Facultad de Ingeniería

Capítulo 5. Capa de Red

5.1 Protocolos de Nivel de Red

5.2 Redes y Subredes

5.3 Administración de tablas de ruteo

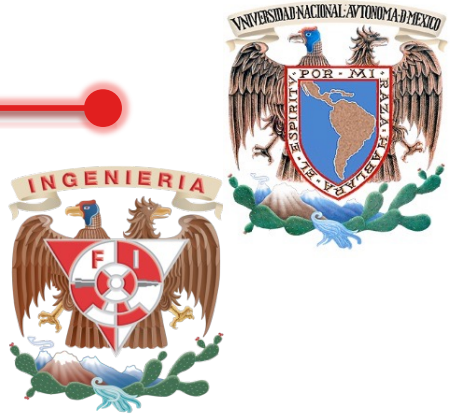
5.4 Protocolos de enrutamiento

5.5 Control de la congestión

5.6 Servicios orientados a conexión

5.7 Servicios no orientados a conexión

5.8 Ruteadores



Capa de Red

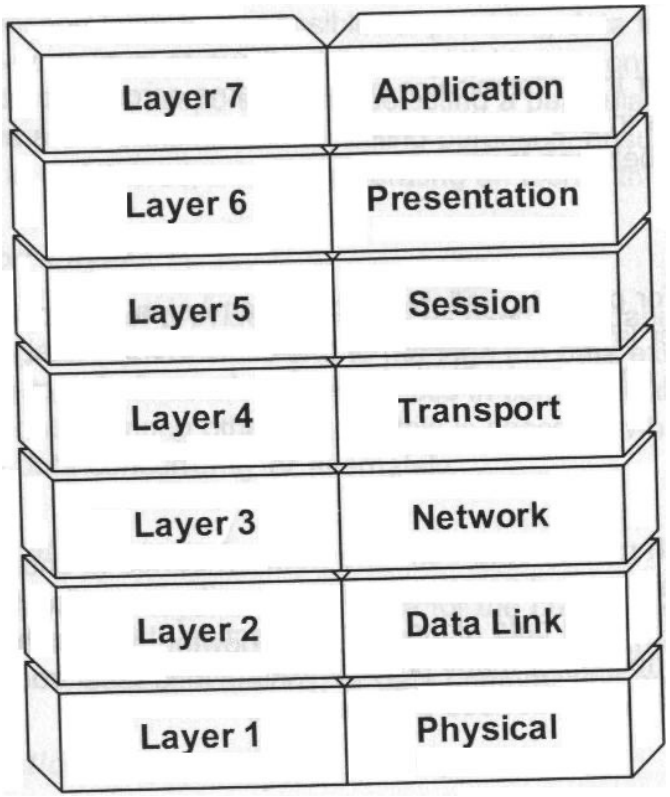
La capa de red es la encargada de la conectividad entre dos computadoras (hosts) cualesquiera, sin importar su ubicación física dentro de la red.

Esta accesibilidad se logra al ocultar los detalles físicos de la red bajo una abstracción lógica de la misma. Para ello, esta capa define las direcciones lógicas que permiten identificar inequívocamente a todo host.

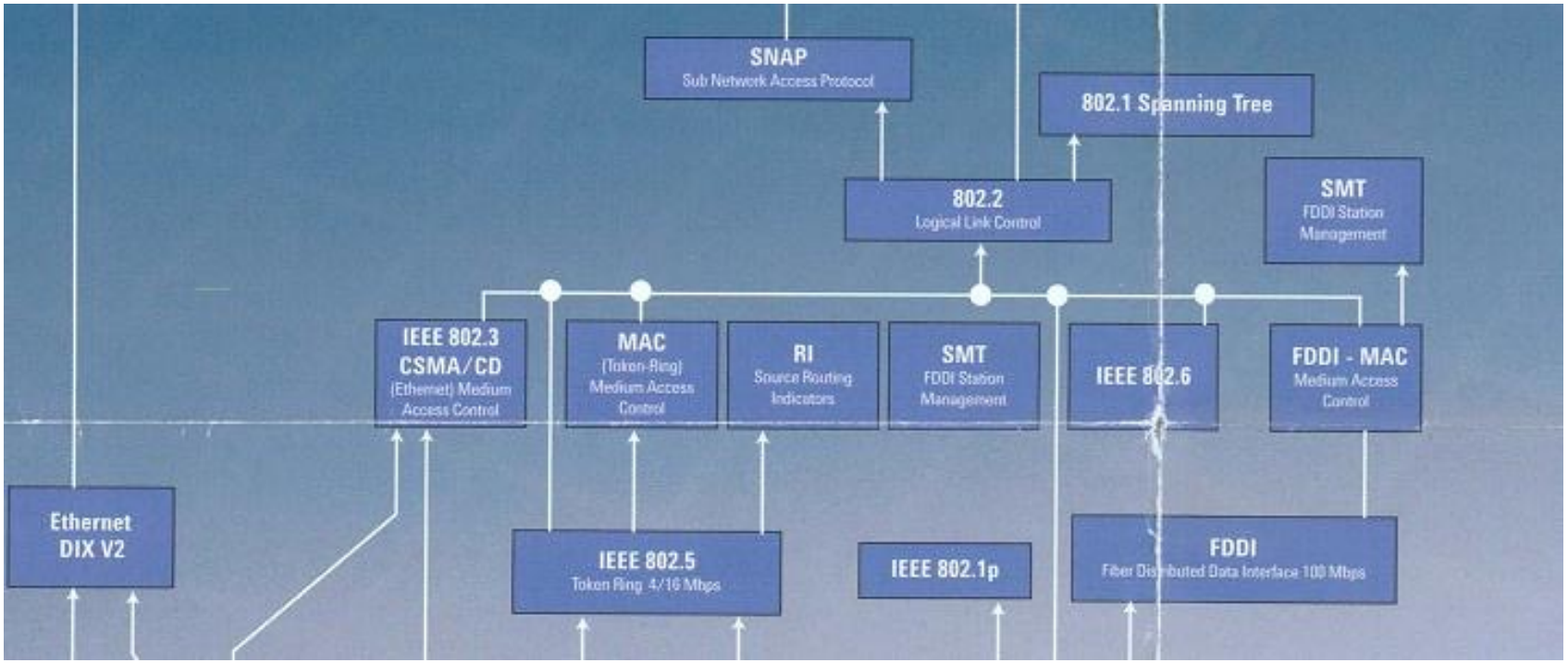
En esta etapa también se define la unidad lógica mínima de transferencia (datagrama), la cual se caracteriza por su independencia de la tecnología (en algunos casos) y todas las funciones de routing.

Modelo OSI

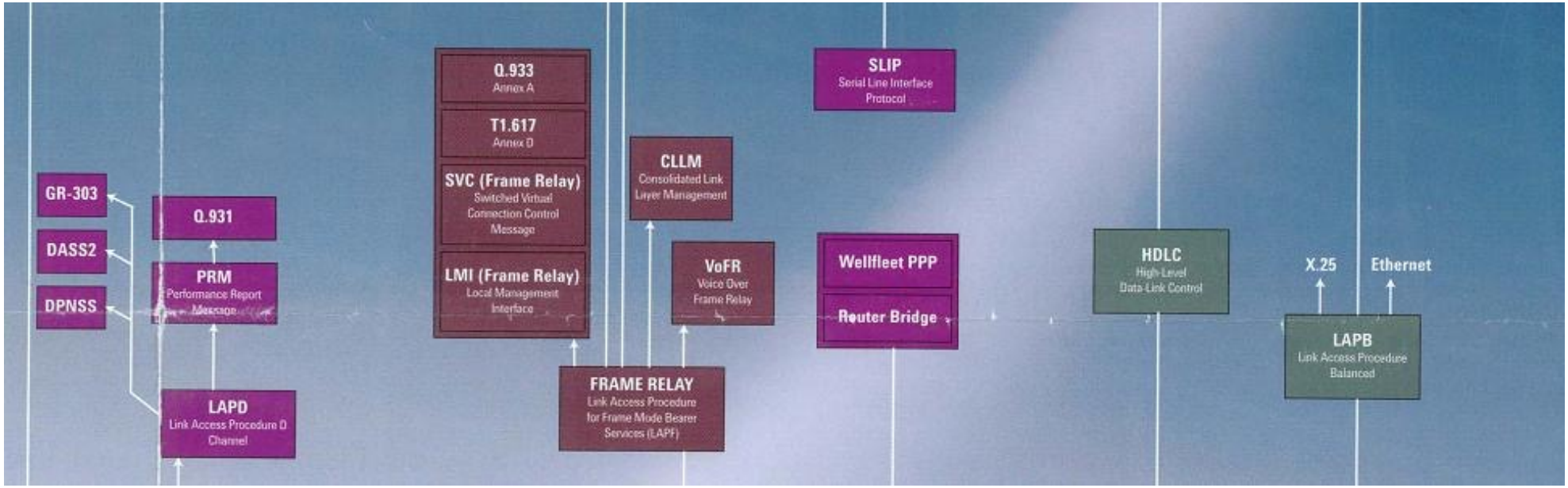
La capa de red tiene la función de “routing” de datos de un dispositivo de red hacia otro. Es la responsable de establecer, mantener y terminar la conexión de red entre cualquier número de dispositivos y la transferencia de datos sobre esta conexión.



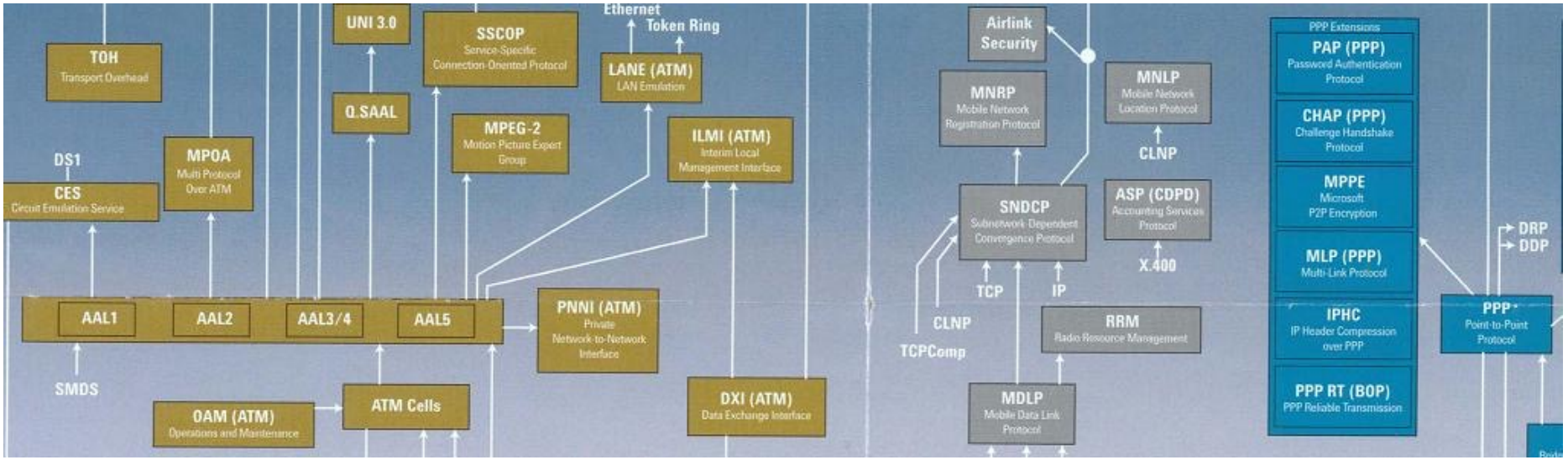
Antecedentes



Antecedentes



Antecedentes



5.1 Protocolos de Nivel de Red

5.1.1 Protocolos IP

El Protocolo de Internet (IP) se encuentra en la capa de red (Capa 3 del modelo OSI), dicho protocolo contienen información de direccionamiento y alguna información de control para habilitar paquetes para ser “envíados a la mejor ruta” (routing) en una red.

IP es el protocolo primario de la capa de red del protocolo TCP/IP. Dentro del Protocolo de Control de Transmisión (TCP), IP representa el corazón de los protocolos de Internet.

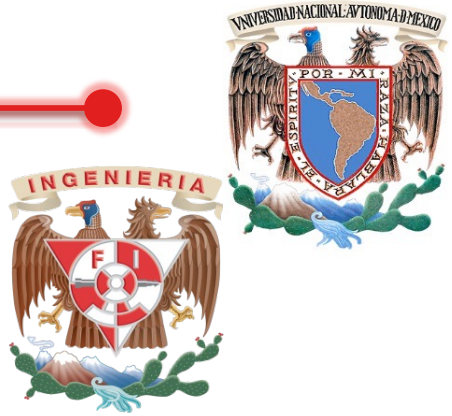
IP tiene dos responsabilidades primarias:

•Proveer servicios no orientado a conexión, realizando el mejor esfuerzo en la entrega de los datagramas a través de la red.

•Proveer fragmentación y reensamble de los datagramas para soportar los enlaces de datos con diferentes tamaños a las unidades máximas de transmisión (MTU).

Datagrama

Los datagramas son básicamente unidades de información que pasa sobre TCP/IP. Contiene información como es el origen y destino de los hosts.



Internet

Internet es una red virtual mundial constituida por subredes físicas (o redes LAN, MAN y WAN) interconectadas.

La interconexión se realiza por medio de “routing” que utilizan el protocolo IP para transmitir datagramas entre las computadoras de las redes conectadas.

Evolución

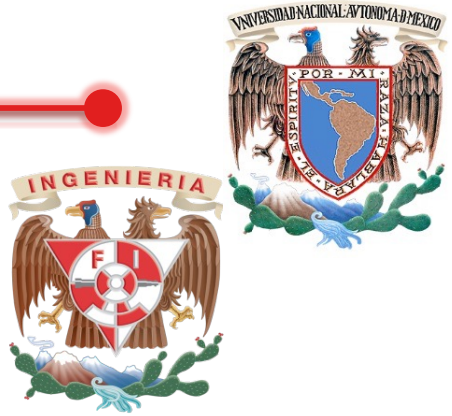
- Red Militar 70’s
- Red Académica 80’s
- Red Comercial 90’s

Protocolo de Internet (RFC 791)

RFC(Request For Comments) son una serie de documentos que abarcan nuevas investigaciones, innovaciones y tecnologías aplicables a las tecnologías de Internet.

La iniciación del formato RFC fue en 1969 parte del proyecto Arpanet. Hoy en día la publicación la realiza el IETF (Internet Engineering Task Force).

RFC 1661 - The Point-to-Point Protocol (PPP)



IP

Define el esquema de direccionamiento lógico

Especifica un servicio de entrega de paquetes sin conexión

Define el formato de los datagramas

Fragmenta y reensambla los datagramas

Enruta los datagramas

Direccionamiento Lógico Modelo TCP/IP

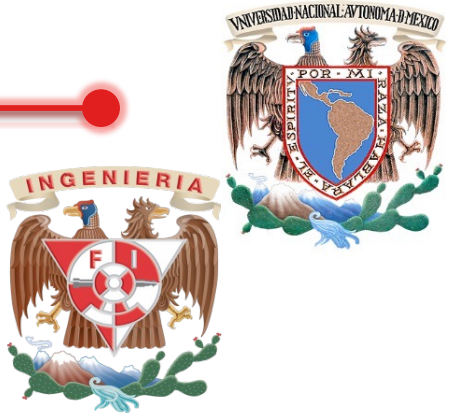
Clasificación de las Direcciones IP

Se llama Dirección IP al número único asignado a un “host” en la red. Dicho número consta de 32 bits dividido en cuatro campos de 8 bits.

Cada campo de 8 bits, es representado por un número decimal entre 0 y 255, separado por periodos.

Cada dirección IPv4 identifica una red y un host único en cada red. El valor del primer campo determina cual porción de la dirección IP es el número de la red y cual porción es el número del host. Los números de red están divididos en cuatro clases:

Clase A Clase B Clase C Clase D



Clase A

0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0

0.0.0.0

0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1

127.255.255.255

Clase B

1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0

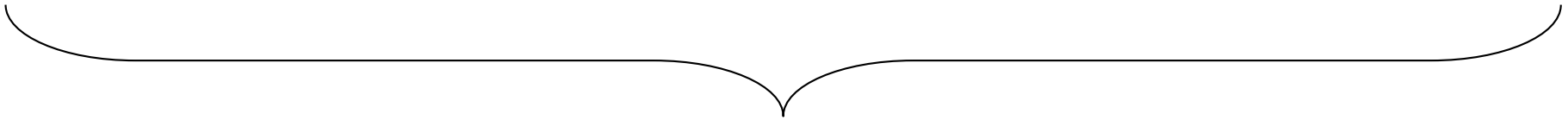
128.0.0.0

1 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1

191.255.255.255

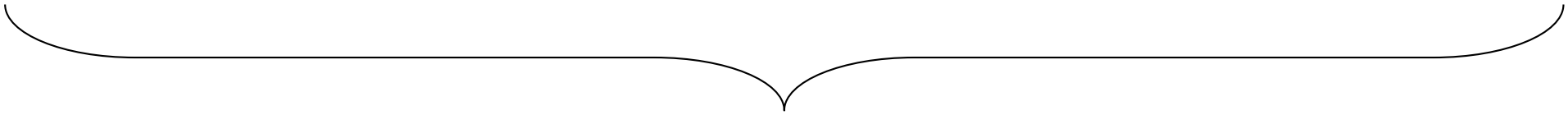
Clase C

1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0

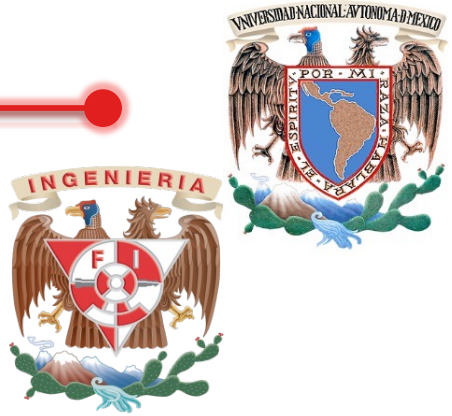


192.0.0.0

1 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1



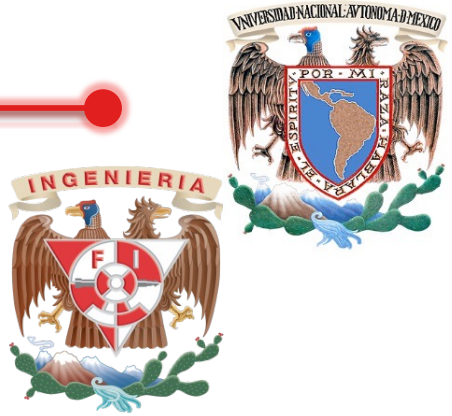
223.255.255.255



Clase A a.b.c.d. Donde “a” es el número de la red y el resto es el número de host.

Clase B a.b.c.d. Donde “a.b” es el número de la red y el resto es el número de host.

Clase C a.b.c.d. Donde “a.b.c” es el número de la red y el resto es el número de host.

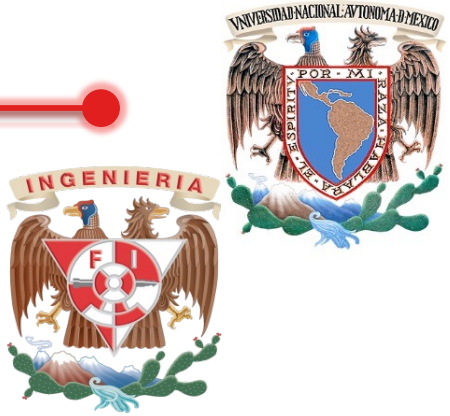


Mascara de Red

Clase A 255.0.0.0

Clase B 255.255.0.0

Clase C 255.255.255.0



Al contar con una mascara de red, nuestra posibilidad de host son la combinación de los bits “sin activar”:

Clase A: 255.0.0.0 $(256)^3$ = 16777216 millones de hosts

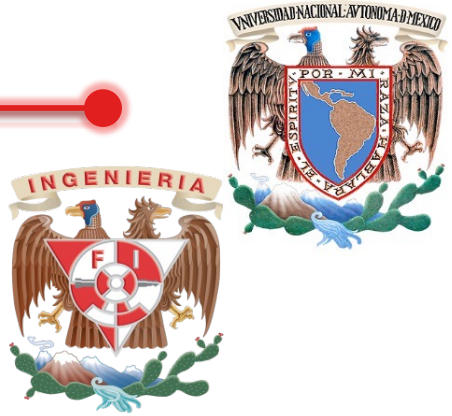
- 16777214 millones de hosts (1 IP Seg. Red y 1 broadcast)

Clase B: 255.255.0.0 $(256)^2$ = 65536 hosts

- 65534 de hosts (1 IP Seg. Red y 1 broadcast)

Clase C: 255.255.255.0 $(256)^1$ = 256 hosts.

- 254 de hosts (1 IP Seg. Red y 1 broadcast)



Ejemplo de estos tres rangos. La dirección IP 140.24.23.17 es una dirección IP Clase B. Red → Dos primeros segmentos de bits. Host → Los dos últimos segmentos de red.

IP: 140.24.23.17

Segmento de Red (La primera dirección IP)	140.24.0.0
Broadcast (La última dirección IP)	140.24.255.255

Otra clasificación de las redes IP son:

Homologadas (real o pública)

No Homologadas (privada o reservada)

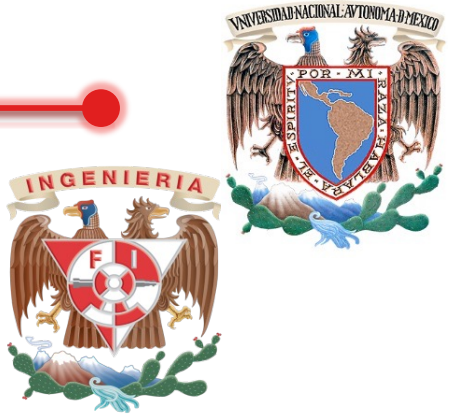
RFC 1918 (Mas detalles)

Rango de direcciones No Homologadas

Clase A: 10.0.0.0 a 10.255.255.255 o 10/8

Clase B: 172.16.0.0 a 172.31.255.255 o 172.16/12

Clase C: 192.168.0.0 a 192.168.255.255 o 192.168.0/16



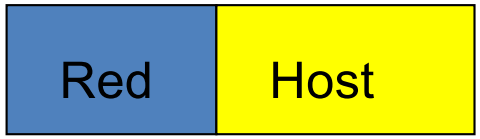
Ejemplo. Conocer la clase (ambas clasificaciones) de las siguientes direcciones IP

54.84.15.34	IP dentro de Clase A, IP Homologada
10.4.56.1	IP dentro de Clase A, IP No Homologada
172.20.12.3	IP dentro de Clase B, IP No Homologada
200.84.15.34	IP dentro de Clase C, IP Homologada

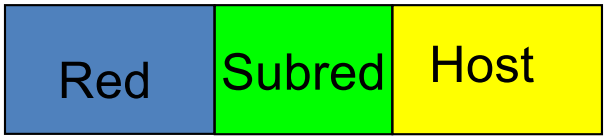
Subred. Se define una subred como un subconjunto de redes de tipo A, B o C

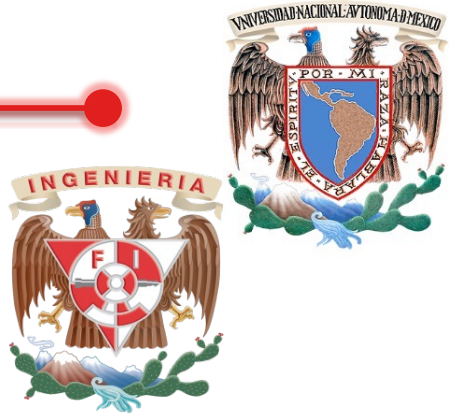
Jerarquías de Red

1) Jerarquía de dos niveles



2) Jerarquía de tres niveles



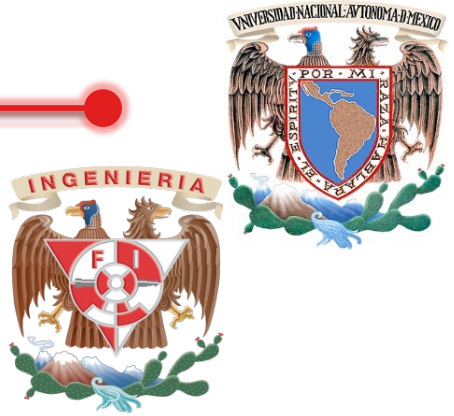


Razones para crear una subred

Dividir el tráfico de la red entre varias subredes. En cada subred habrá tráfico local.

Seguridad o accesos limitados a una subred

Dividir el trabajo administrativo al crear redes locales y distribuir dichas funciones a “administradores locales”



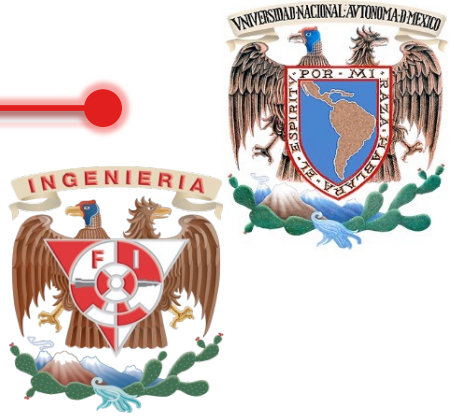
Creación de subredes. Modificar los bits de izquierda a derecha en cuanto a los “bits móviles” y se crearán redes en múltiplos de 2.

Ejemplo. Clase C

Máscara Decimal	Mascara Binario	No. de Redes	No. de Hosts
255.255.255.0	11111111.11111111.11111111.00000000	1	254
255.255.255.128	11111111.11111111.11111111.10000000	2	126
255.255.255.192	11111111.11111111.11111111.11000000	4	62
255.255.255.224	11111111.11111111.11111111.11100000	8	30
255.255.255.240	11111111.11111111.11111111.11110000	16	14
255.255.255.248	11111111.11111111.11111111.11111000	32	6
255.255.255.252	11111111.11111111.11111111.11111100	64	2

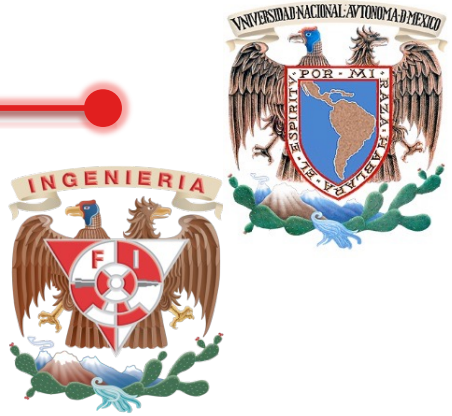
Ejemplo. Clase B

Máscara Decimal	Mascara Binario	No. de Redes	No. de Hosts
255.255.0.0	11111111.11111111.00000000.00000000	1	65534
255.255.128.0	11111111.11111111.10000000.00000000	2	32766
255.255.192.0	11111111.11111111.11000000.00000000	4	16382
255.255.224.0	11111111.11111111.11100000.00000000	8	8190
255.255.240.0	11111111.11111111.11110000.00000000	16	4094
255.255.248.0	11111111.11111111.11111000.00000000	32	2046
255.255.252.0	11111111.11111111.11111100.00000000	64	1022
255.255.254.0	11111111.11111111.11111110.10000000	128	510
255.255.255.0	11111111.11111111.11111111.00000000	256	254
255.255.255.128	11111111.11111111.11111111.10000000	512	126
255.255.255.192	11111111.11111111.11111111.11000000	1024	62
255.255.255.224	11111111.11111111.11111111.11100000	2048	30
255.255.255.240	11111111.11111111.11111111.11110000	4096	14
255.255.255.248	11111111.11111111.11111111.11111000	8192	6
255.255.255.252	11111111.11111111.11111111.11111100	16384	2



Clase A

Tarea



Ejercicio. Crear una subred si el número de nodos es igual a 95.

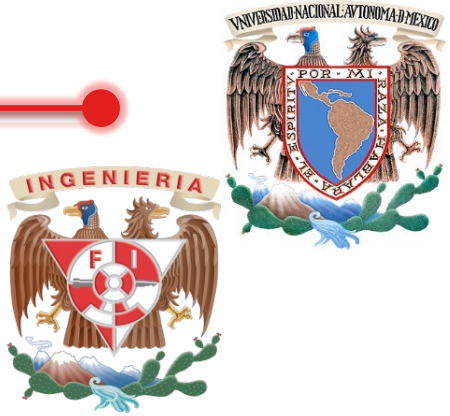
Solución 1. Suponiendo que “no se cuenta” con direcciones reales, se utilizará las direcciones IP privadas.

Segmento de Red = 192.168.14.0

Mascara de Red = 255.255.255.0

No. de Subredes = 1

No. de Hosts disponibles = 254



Solución 2. Suponiendo que “no se cuenta” con direcciones reales, se utilizará las direcciones IP privadas, en la Clase B.

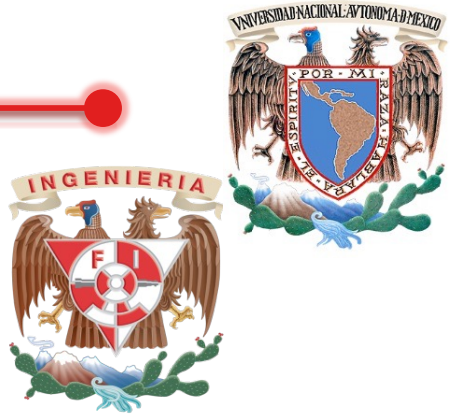
Segmento de Red = 172.28.0.0

Mascara de Red = 255.255.0.0

No. de Subredes = 1

No. de Hosts disponibles = 65534

Broadcast = 172.28.255.255



Solución 3. Suponiendo que “no se cuenta” con direcciones reales, se utilizará las direcciones IP privadas, en la Clase A.

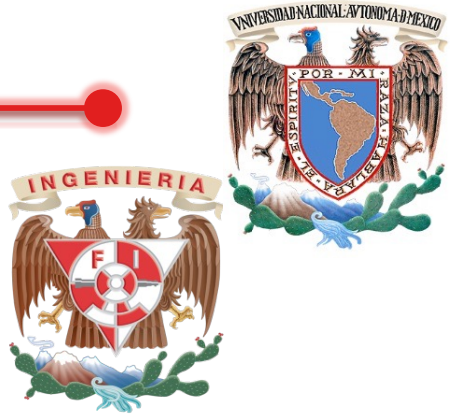
Segmento de Red = 10.0.0.0

Mascara de Red = 255.0.0.0

No. de Subredes = 1

No. de Hosts disponibles = $(256)^3$ -2

Broadcast = 10.255.255.255



Solución 4. Suponiendo la solución 1, además de limitar el número de redes con respecto al número de nodos.

No. de nodos =95 64<95<128 128 Host por red

Máscara Decimal	No. de Redes	No. de Hosts
255.255.255.128	2	126

Segmento de Red1 = 192.168.14.0

Mascara de Red1 = 255.255.255.128

Broadcast1 = 192.168.14.127

Segmento de Red2 = 192.168.14.128

Mascara de Red2 = 255.255.255.128

Broadcast2 = 192.168.14.255

Ejercicio (aumentado). Crear una subred si el número de nodos es igual a 95, se deben crear 4 subredes, usando parte de la solución 1.

Comprobar si los rangos fueron realizados correctamente.

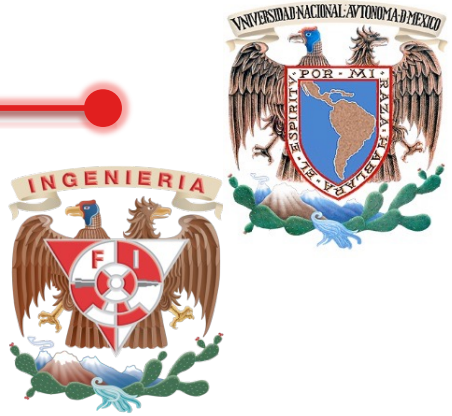
Operación AND

(IP)(AND)(MascaraDeRed)=SegmentoDeRed

IP(Binario)

AND MR(Binario)

SR(Binario)



Ejercicio (aumentado). Crear una subred si el número de nodos es igual a 95, se deben crear 4 subredes en la clase B.

Comprobar si los rangos fueron realizados correctamente.

Operación AND

(IP)(AND)(MascaraDeRed)=SegmentoDeRed

IP(Binario)

AND MR(Binario)

SR(Binario)

Solución 5. Suponiendo la solución 1, además de limitar el número de redes con respecto al número de nodos (95) y dividiendo las 4 subredes de la siguiente forma:

Red 1. 63 Nodos

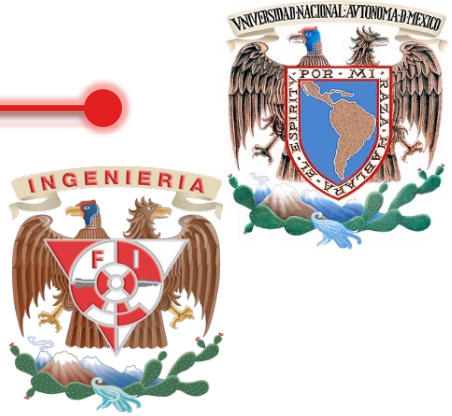
Red 2. 20 Nodos

Red 3. 10 Nodos

Red 4. 2 Nodos

Solución: Ejercicio

RFC: 959, 1817, 1518 y 1519



Definición de CIDR (Classless Inter-Domain Routing)

CIDR (Routing de Inter-Dominios sin Clases). Es un estándar de red para la interpretación de direcciones IP. CIDR facilita el routing al permitir agrupar bloques de direcciones en una sola entrada en la tabla de rutas. Estos grupos se llaman comúnmente Bloques CIDR, comparten una misma secuencia inicial de bits en representación binaria de sus direcciones IP.

Con esta mejora se cuenta con un uso más eficiente de las escasas direcciones IPv4.
Mayor uso de la jerarquía de direcciones (agregar de prefijos de subred o jerarquía de tres niveles), disminuyendo la sobrecarga de los routers principales de Internet.

Tablas de CIDR

CIDR	No. de redes por clase	Hosts	Máscara
/32	1/256 C	1	255.255.255.255
/31	1/128 C	2	255.255.255.254
/30	1/64 C	4	255.255.255.252
/29	1/32 C	8	255.255.255.248
/28	1/16 C	16	255.255.255.240
/27	1/8 C	32	255.255.255.224
/26	1/4 C	64	255.255.255.192
/25	1/2 C	128	255.255.255.128
/24	1/1 C	256	255.255.255.0
/23	2 C	512	255.255.254.0
/22	4 C	1,024	255.255.252.0
/21	8 C	2,048	255.255.248.0
/20	16 C	4,094	255.255.240.0
/19	32 C	8,192	255.255.224.0
/18	64 C	16,384	255.255.192.0

Tablas de CIDR

CIDR	No. de redes por clase	Hosts	Máscara
17	128 C	32,768	255.255.128
/16	256 C, 1 B	65,536	255.255.0.0
/15	512 C, 2 B	131,072	255.254.0.0
/14	1,024 C, 4 B	262,144	255.252.0.0
/13	2,048 C, 8 B	524,288	255.248.0.0
/12	4,096 C, 16 B	1,048,576	255.240.0.0
/11	8,192 C, 32 B	2,097,152	255.224.0.0
/10	16,384 C, 64 B	4,194,304	255.192.0.0
/9	32,768 C, 128B	8,388,608	255.128.0.0
/8	65,536 C, 256B, 1 A	16,777,216	255.0.0.0
/7	131,072 C, 512B, 2 A	33,554,432	254.0.0.0
/6	262,144 C, 1,024 B, 4 A	67,108,864	252.0.0.0
/5	524,288 C, 2,048 B, 8 A	134,217,728	248.0.0.0
/4	1,048,576 C, 4,096 B, 16 A	268,435,456	240.0.0.0
/3	2,097,152 C, 8,192 B, 32 A	536,870,912	224.0.0.0

Definición de VLSM (Variable Length Subnet Mask)

VLSM (Mascara de Subred de Longitud Variable). Es el método por el cual la convencionales mascaras de dos niveles IP son reemplazadas por el esquema flexible de tres niveles.

Debido a que los administradores dejan de asignar direcciones IP a los “hosts” basados que están conectados en redes físicas, la subred es una verdadera brecha para las grandes redes IP que mantengan. Tiene sus propias consideraciones, sin embargo, todavía están investigando para su mejora. La principal consideración de la “subred” es el hecho de identificar a la subred representada a un nivel jerárquico adicional y cómo las direcciones IP se interpretan y utilizan para realizar routing.

Solución 5. Suponiendo la solución 1, además de limitar el número de redes con respecto al número de nodos (95) y dividiendo las 4 subredes de la siguiente forma:

Red 1. 63 Nodos

Red 2. 20 Nodos

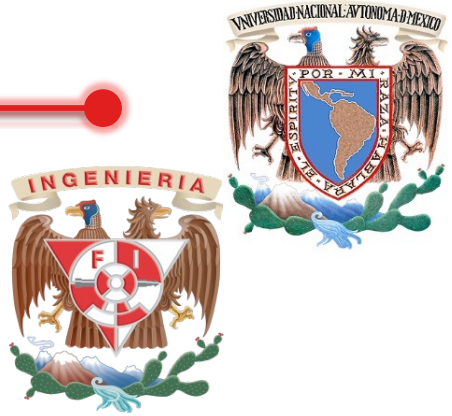
Red 3. 10 Nodos

Red 4. 2 Nodos

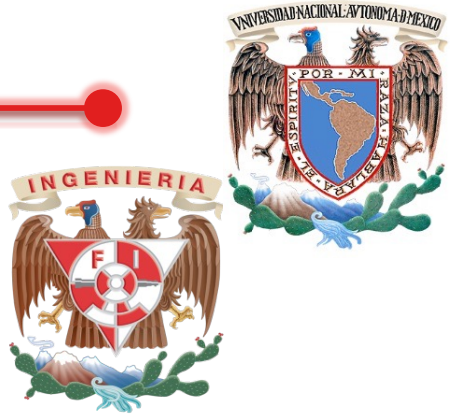
Solución: Subredes

VLMS

RFC: 959, 1817, 1518 y 1519



Tarea. Crear subredes si el número de nodos es igual a 14300, se deben crear 4 subredes en las clases A y B. Así como dar una solución para tipos C.



Protocolo de Internet

Direccionamiento Multicast

El rango de direcciones multicast es de 224.0.0.1 a 239.255.255.254

La dirección 224.0.0.1 se asigna al grupo de todos los hosts y routers en una subred física que participan en IP multicast.

La dirección 224.0.0.2 se asigna a todos los routes en una subred física.

IP(Cabecera)

Versión: 4 bits, v4,v6

Longitud del encabezado: 4 bits

Longitud Total: 16 bits

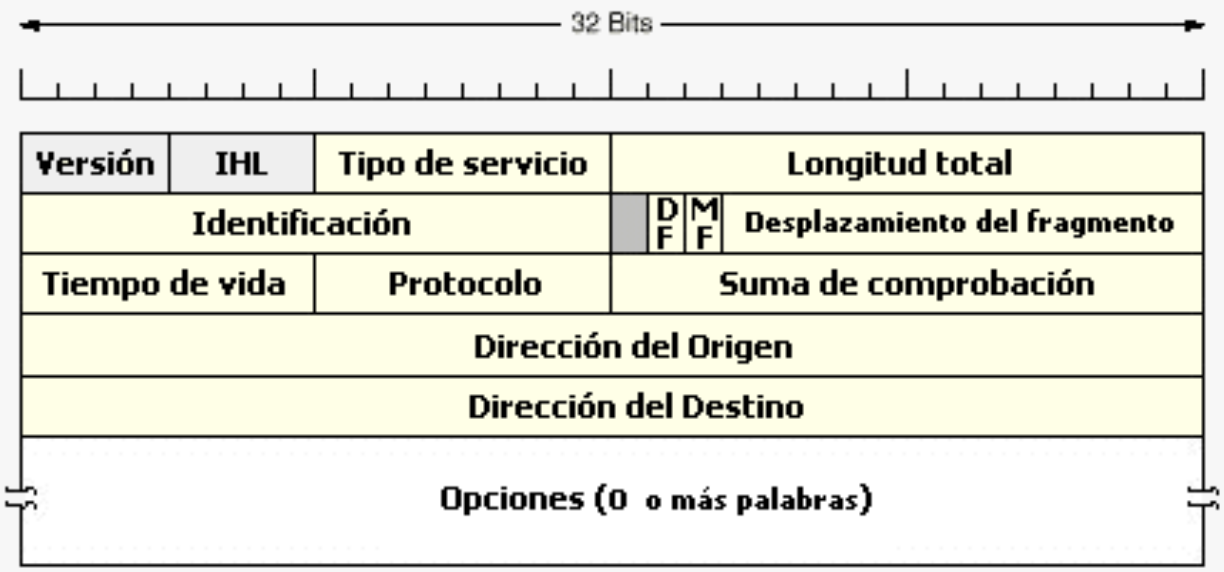
Identificación: 16 bits

Banderas, 3 bits:

El primer bit no se usa.

DF Do not Fragment(1)

MF More Fragment (1)

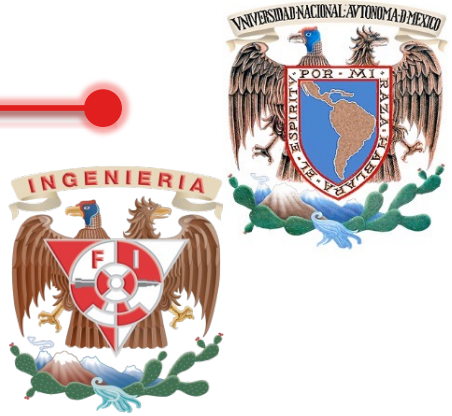


Offset: 13 bits, indica la posición de este fragmento en el datagrama (en bytes)

Checksum: 16 bits, Este campo se calcula considerando el encabezado como una secuencia de enteros de 16 bits, sumando estos enteros y tomando el complemento a 1 del resultado.

TTL:8 bits, especifica el tiempo que le queda de vida al datagrama. Cada router le quita 1 segundo de vida.

Protocolo: 8 bits el cual va dirigido al datagrama (1-ICMP,6-TCP, 17-UDP)



IP(Cabecera)

Tipo de Servicio: Permite especificar como debe tratarse el datagrama (QoS)

Precedencia	D	T	R	Reservado

Precedencia (Bits 0-2), indica el QoS deseado:

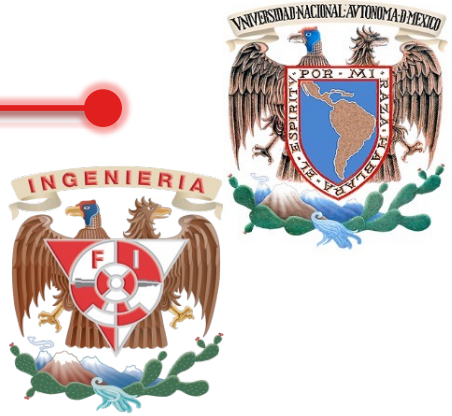
111 Network control

110 Internetwork control

010 Inmediate

001 Priority

000 Routine Data



IP(Cabecera)

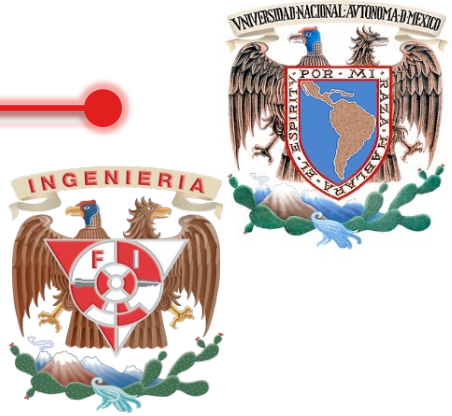
Los Bits D, T y R especifican el tipo de transporte deseado

Delay (Retardo): 0=Normal 1=Bajo

Throughput (Rendimiento): 0=Normal 1=Alto

Reliability (Confiabilidad) :0=Normal 1=Alto

Esta especificación puede ayudar a los algoritmos de enrutamiento a escoger un camino hacia el destino.



ARP (Address Resolution Protocol)

En la red virtual de Internet cada host tiene una dirección lógica IP.

En las subredes físicas cada host tiene una dirección de hardware.

Para transmitir un datagrama al destino (host o enrutador) que se encuentre en la misma subred física, el datagrama debe encapsularse en un paquete que contenga la dirección hardware del destino.

¿Cómo se mapea una dirección lógica en una dirección hardware?

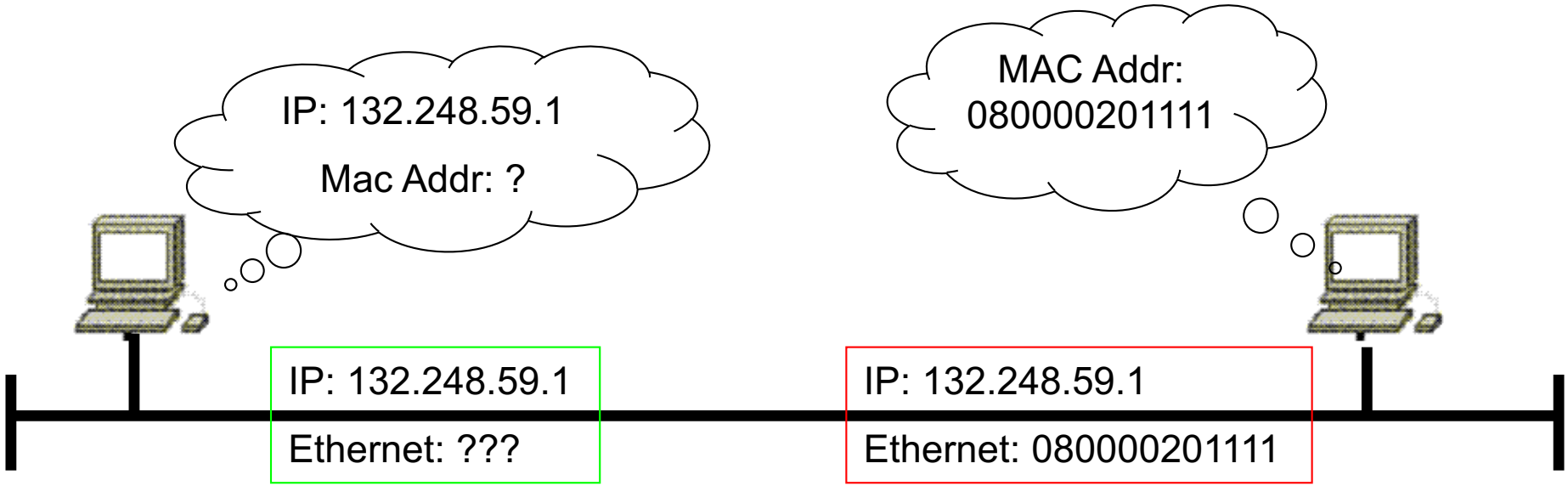
Por ejemplo, ¿Cómo se mapea una dirección IP de 32 bits en una dirección ethernet de 48 bits?

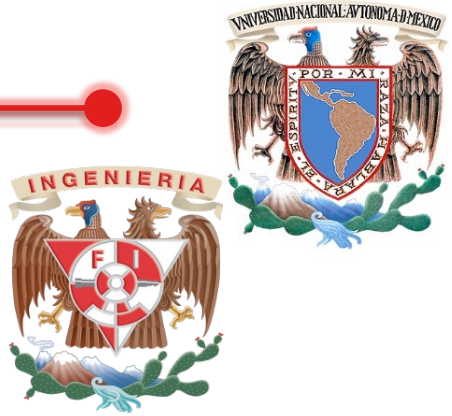
ARP

Permite a una fuente encontrar la dirección de hardware de un destino que se encuentre en la misma subred física

Recibe como entrada la dirección IP del destino y regresa su dirección hardware.

Funciona en subredes que tienen la capacidad de difusión





ARP

El Address Resolution Protocol (ARP) permite “mapear” de una dirección IP a una dirección física del equipo (MAC address para Ethernet) que esta en una red local.

Por ejemplo en IPv4, la dirección es de 32 bits. En una red de área local, sin embargo, las direcciones de la MAC son de 48 bits. Usualmente se utiliza un tabla llamada “cache ARP”, que se usa para mantener la correlación entre la dirección MAC y la correspondiente IP address. ARP provee reglas para hacer dicha correlación y proveer las dirección en conversión en ambos sentidos.

ARP

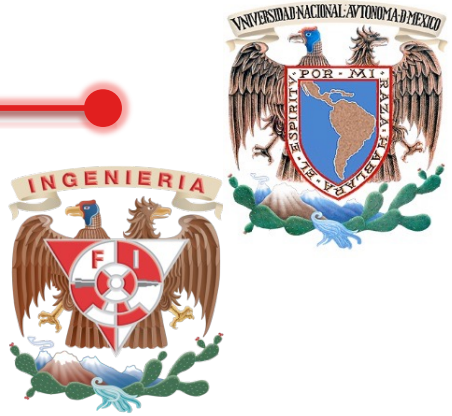
0	8	16	24	31
TIPO DE HARDWARE		TIPO DE PROTOCOLO		
HLEN	PLEN	OPERACION		
SENDER HA (octeto 0 - 3)				
SENDER HA (OCTETO 4 – 5)		SENDER IP (OCTETO 0 – 1)		
SENDER IP (OCTETO 2 – 3)		TARGET HA (OCTETO 0 – 1)		
TARGET HA (octeto 2 - 5)				
TARGET IP (octeto 0 - 3)				

Tipo de Hardware. Especifica un tipo de interfaz de hardware por el cual el envío requiere una respuesta. Ejemplo: Ethernet 1.

El tipo de Protocolo. Especifica el tipo del protocolo de dirección del alto-nivel donde el remitente lo ha provisto. Ejemplo: 0x800 IP

HLen. La longitud de la dirección de hardware.

PLen. La longitud de la dirección del protocolo.



ARP

Operación. Las operación son las siguientes:

1.ARP request 2. ARP response 3. RARP request 4. RARP response

5. Dynamic RARP request 6. Dynamic RARP reply 7. Dynamic RAR error

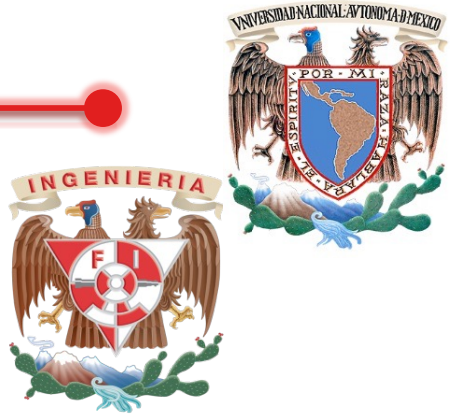
8. InARP request 9. InARP reply

Dirección del Hardware del origen. Longitud en bytes de la longitud del HW.

Dirección del Protocolo del origen. Longitud en bytes de la longitud del Protocolo.

Dirección Hardware destino. Longitud en bytes de la longitud del HW.

Dirección del Protocolo destino. Longitud en bytes de la longitud del Protocolo.



ARP

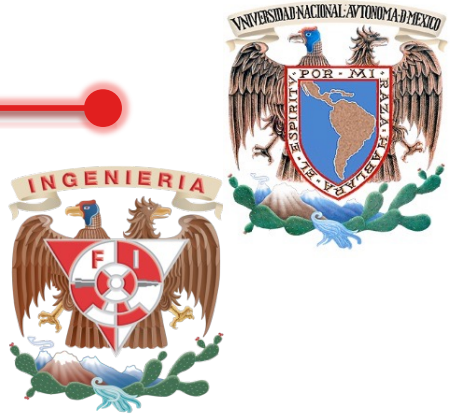
El mensaje ARP se encapsula en un paquete de la subred física que se difunde por todas las máquinas de la subred. La difusión es muy costosa ya que todos los receptores deben procesar el paquete.

Cada fuente mantiene en caché una tabla con la pareja de direcciones (IP, hardware) que ha adquirido recientemente.

El mensaje ARP incluye la pareja de dirección de emisor para que los receptores puedan guardarla en su propia tabla.

Cuando se configura la interfaz de red de un equipo se emite un ARP (gratuito) para actualizar las tablas de las máquinas de la subred y asegurar la unicidad de una dirección IP.

Capa de Red



brahm@root>arp -a

telematica1.fi-b.unam.mx (132.248.59.82) at 0:1:2:c9:23:91 [ethernet]

puide1.fi-b.unam.mx (132.248.59.85) at 0:50:da:59:20:25 [ethernet]

lcomp89.fi-b.unam.mx (132.248.59.89) at 0:20:af:4d:a6:40 [ethernet]

isis.fi-b.unam.mx (132.248.59.15) at 0:f:fe:b1:67:b9 [ethernet]

lestat.fi-b.unam.mx (132.248.59.42) at 0:50:da:59:20:1e [ethernet]

? (132.248.59.244) at 0:7:50:e2:12:0 [ethernet]

puide2.fi-b.unam.mx (132.248.59.95) at 0:50:da:59:1f:57 [ethernet]

medusa.fi-b.unam.mx (132.248.59.20) at 0:60:97:6c:1c:87 [ethernet]

dctrl.fi-b.unam.mx (132.248.59.22) at 0:e:c:85:50:be [ethernet]

estigia.fi-b.unam.mx (132.248.59.98) at 0:a0:24:34:f1:76 [ethernet]

perseo.fi-b.unam.mx (132.248.59.24) at 0:4:76:f0:5b:e3 [ethernet]

kaos.fi-b.unam.mx (132.248.59.26) at 0:4:75:37:f0:6a [ethernet]

cronos.fi-b.unam.mx (132.248.59.2) at 8:0:20:75:99:54 [ethernet]

zeus.fi-b.unam.mx (132.248.59.3) at 0:50:da:59:20:6e [ethernet]

fe3-15-iimas-core.fi-b.unam.mx (132.248.59.254) at 0:c:db:ac:1c:0 [ethernet]

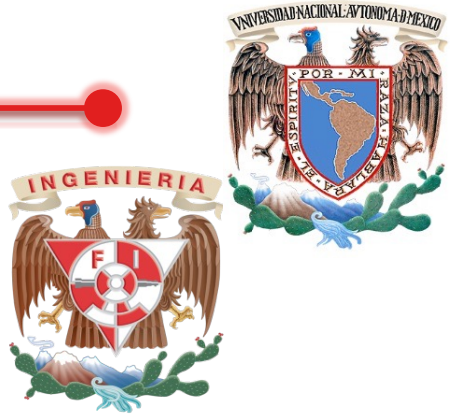
rha.fi-b.unam.mx (132.248.59.5) at 0:60:97:2e:5a:a5 [ethernet]

Internet Control Message Protocol (ICMP)

El ICMP es parte del Modelo TCP/IP. Los mensajes ICMP, entrega mensajes IP, son usados “fuera de banda” para conocer la operación o “la no operación” de la red. Los paquetes entregados ICMP no son fiables, así que los hosts no pueden contar un paquete recibido ICMP para cualquier problemas de la red. Las funciones claves de ICMP son:

- Anunciar errores en la red, tal como el host o una porción de la red (o completa) sean “inalcanzables”, esto solamente muestra algún tipo de falla. Un paquete TCP o UDP directos a un número de puertos con adjunto de recepción no puestos, están también reportados vía ICMP.

- Anuncia congestión de la red. Cuando un “router” empieza a tener “buffering” de muchos paquetes, debido a la no disponibilidad de transmitir estos tan rápido como se están recibiendo, se genera un mensaje ICMP de apagar el origen. Con esto ocasiona que la fuente mande “mas despacio” los paquetes a transmitir.



Internet Control Message Protocol (ICMP)

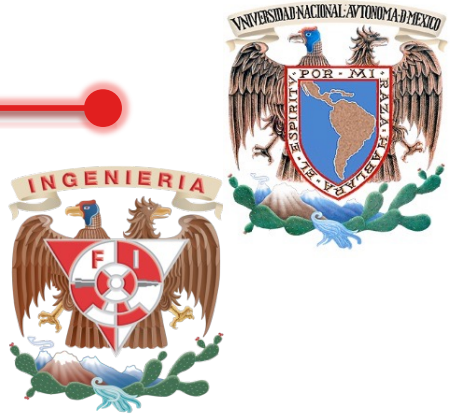
Asistencia a Fallas. ICMP soporte una función “echo”, el cual envía justamente un paquete round-trip entre dos hosts. El comando “ping” (Packet InterNet Groper) es una utilería muy común en la administración de redes, que esta basado en la siguiente característica. Ping transmitirá una serie de paquetes, calculando el valor promedio del vía round-trip en tiempo y porcentaje de paquetes perdidos.

Anuncia tiempos fuera (timeout). Si unos paquetes IP tienen el campo “TTL” borrados (tienen el valor en cero), el router descarta los paquetes que fueron generados con esta configuración. Traceroute es una utilería del cual mapea rutas de red que envían paquetes con valores pequeños de TTL y se miran los “timeouts” de los ICMP anunciados.

ICMP

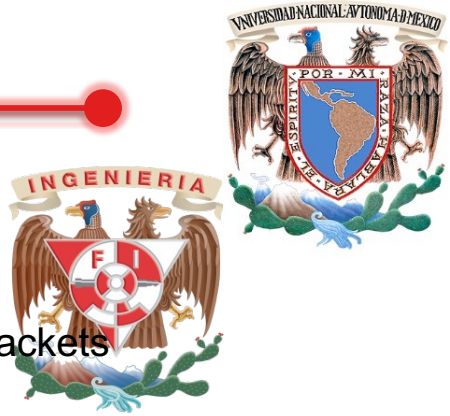
```
root@aries>ping www.ipn.mx
PING www.ipn.mx (148.204.103.161) 56(84) bytes of data.
64 bytes from www.ipn.mx (148.204.103.161): icmp_seq=0 ttl=245 time=65.7 ms
64 bytes from www.ipn.mx (148.204.103.161): icmp_seq=1 ttl=245 time=70.3 ms
64 bytes from www.ipn.mx (148.204.103.161): icmp_seq=2 ttl=245 time=81.7 ms
64 bytes from www.ipn.mx (148.204.103.161): icmp_seq=3 ttl=245 time=67.1 ms
64 bytes from www.ipn.mx (148.204.103.161): icmp_seq=4 ttl=245 time=75.7 ms
64 bytes from www.ipn.mx (148.204.103.161): icmp_seq=5 ttl=245 time=73.6 ms
64 bytes from www.ipn.mx (148.204.103.161): icmp_seq=6 ttl=245 time=59.6 ms
64 bytes from www.ipn.mx (148.204.103.161): icmp_seq=7 ttl=245 time=55.9 ms
64 bytes from www.ipn.mx (148.204.103.161): icmp_seq=8 ttl=245 time=69.9 ms
64 bytes from www.ipn.mx (148.204.103.161): icmp_seq=9 ttl=245 time=59.3 ms
64 bytes from www.ipn.mx (148.204.103.161): icmp_seq=10 ttl=245 time=62.8 ms
--- www.ipn.mx ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 11161ms
rtt min/avg/max/mdev = 55.922/67.465/81.735/7.438 ms, pipe 2
```

ICMP




```
root@aries>ping www.ipn.mx -s 128
PING www.ipn.mx (148.204.103.161) 128(156) bytes of data.
136 bytes from www.ipn.mx (148.204.103.161): icmp_seq=0 ttl=245 time=30.4 ms
136 bytes from www.ipn.mx (148.204.103.161): icmp_seq=1 ttl=245 time=38.6 ms
136 bytes from www.ipn.mx (148.204.103.161): icmp_seq=2 ttl=245 time=32.2 ms
136 bytes from www.ipn.mx (148.204.103.161): icmp_seq=3 ttl=245 time=36.0 ms
136 bytes from www.ipn.mx (148.204.103.161): icmp_seq=4 ttl=245 time=32.3 ms
136 bytes from www.ipn.mx (148.204.103.161): icmp_seq=5 ttl=245 time=21.4 ms
136 bytes from www.ipn.mx (148.204.103.161): icmp_seq=6 ttl=245 time=37.7 ms
136 bytes from www.ipn.mx (148.204.103.161): icmp_seq=7 ttl=245 time=13.1 ms
136 bytes from www.ipn.mx (148.204.103.161): icmp_seq=8 ttl=245 time=26.6 ms
136 bytes from www.ipn.mx (148.204.103.161): icmp_seq=9 ttl=245 time=41.1 ms
136 bytes from www.ipn.mx (148.204.103.161): icmp_seq=10 ttl=245 time=53.6 ms
--- www.ipn.mx ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 10009ms
rtt min/avg/max/mdev = 13.140/33.042/53.636/10.144 ms, pipe 2
```

ICMP



root@aries>traceroute www.yahoo.com

traceroute to www.yahoo-ht3.akadns.net (209.191.93.52), 30 hops max, 38 byte packets

1 126.inverso.unam.mx (132.247.249.126) 0.294 ms 0.205 ms 0.195 ms

2 132.247.251.137 (132.247.251.137) 0.302 ms 0.225 ms 0.272 ms

3 132.247.251.130 (132.247.251.130) 4.040 ms 0.361 ms 0.286 ms

4 132.247.251.236 (132.247.251.236) 0.618 ms 0.444 ms 0.852 ms

5 reg-mex-nextengo-49-pos10-3.uninet-ide.com.mx (200.79.4.142) 0.948 ms reg-mex-nextengo-49-pos1-4.uninet-ide.com.mx (201.117.71.134) 1.380 ms reg-mex-nextengo-49-pos10-3.uninet-ide.com.mx (200.79.4.142) 1.189 ms

6 bb-mex-nextengo-25-pos5-2.uninet.net.mx (201.125.74.218) 172.166 ms 203.403 ms 218.917 ms

7 bbint-la-onewilshire-2-pos-6-0.uninet.net.mx (200.38.192.229) 42.837 ms 42.885 ms 42.686 ms

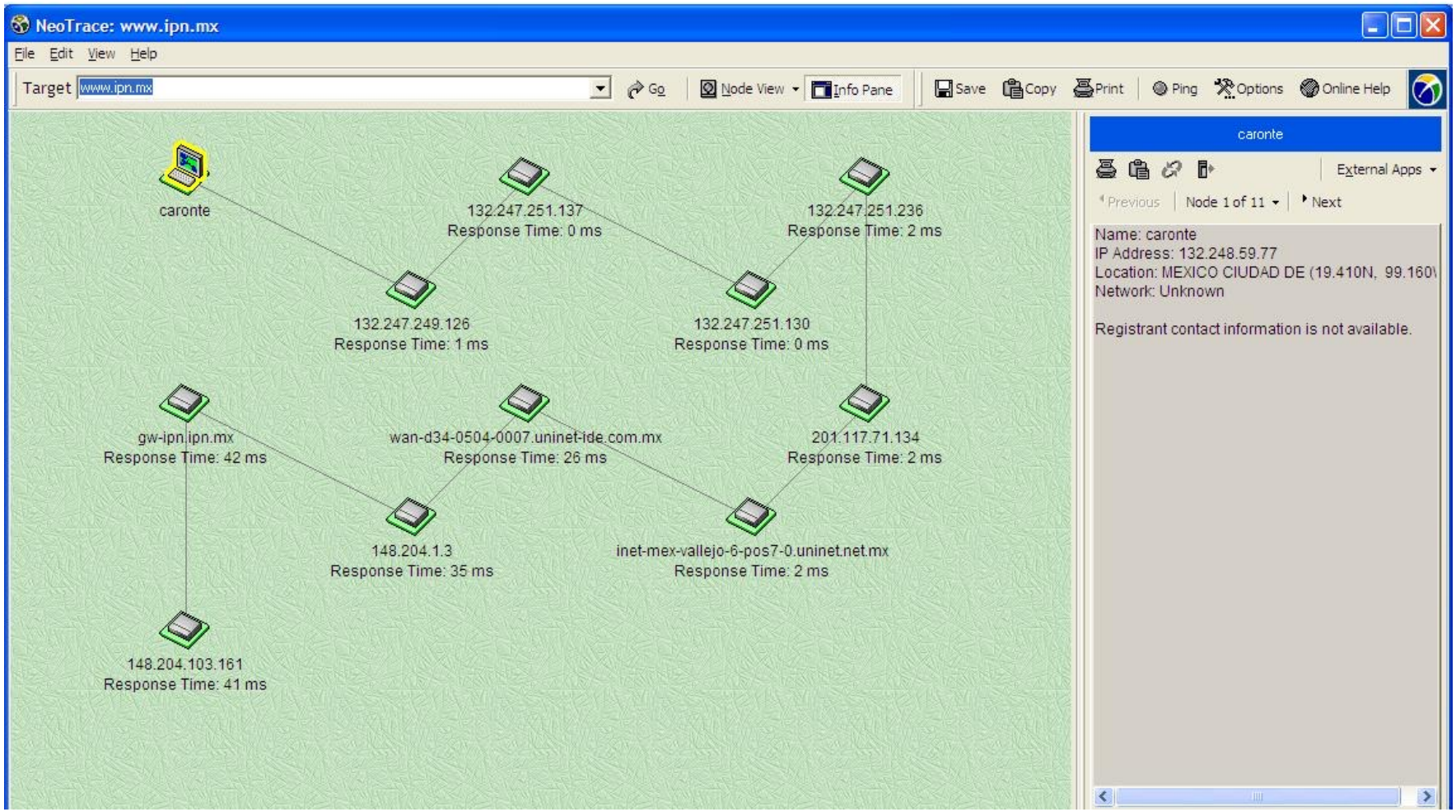
8 64.213.78.21 (64.213.78.21) 42.931 ms 43.946 ms 43.152 ms

9 yahoo-5.ar2.SJC2.gblx.net (64.215.195.98) 51.750 ms 52.161 ms 53.845 ms

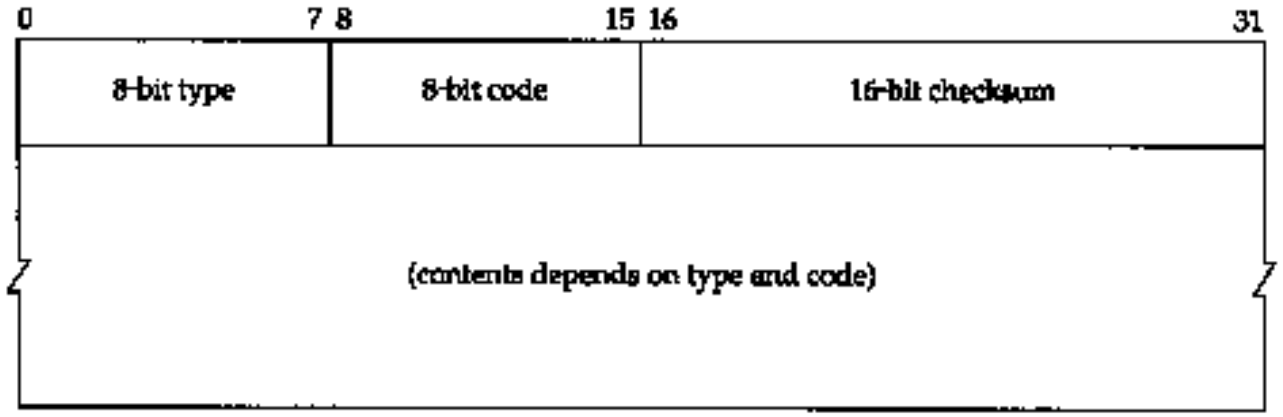
10 so-0-0-0.pat1.da3.yahoo.com (216.115.101.137) 90.311 ms 90.315 ms 90.382 ms

11 ge-0-1-0-p130.msr2.mud.yahoo.com (216.115.104.85) 90.763 ms ge-0-1-0-p120.msr1.mud.yahoo.com (216.115.104.81) 91.110 ms ge-1-1-0-p130.msr2.mud.yahoo.com (216.115.104.93) 90.654 ms

ICMP


NeoTrace: www.ipn.mx
File Edit View Help
Target www.ipn.mx
Go
Node View
Info Pane
Save
Copy
Print
Ping
Options
Online Help
caronte
132.247.251.137
Response Time: 0 ms
132.247.251.236
Response Time: 2 ms
132.247.249.126
Response Time: 1 ms
132.247.251.130
Response Time: 0 ms
gw-ipn.ipn.mx
Response Time: 42 ms
wan-d34-0504-0007.uninet-ide.com.mx
Response Time: 26 ms
201.117.71.134
Response Time: 2 ms
148.204.1.3
Response Time: 35 ms
inet-mex-vallejo-6-pos7-0.uninet.net.mx
Response Time: 2 ms
148.204.103.161
Response Time: 41 ms
caronte
External Apps
Previous
Node 1 of 11
Next
Name: caronte
IP Address: 132.248.59.77
Location: MEXICO CIUDAD DE (19.410N, 99.160
Network: Unknown
Registrant contact information is not available.

Cabeceras ICMP



Tipo. Los mensajes pueden ser un error o de información. Los errores de mensaje pueden ser

0/8. Solicitud/Respuesta Eco.

3. Destino inalcanzable

5. Redirección (enrutamiento)

11. Tiempo excedido.

9/10. Anuncio/Solicitud de enrutador

17/18. Solicitud/Respuesta de máscara.

ICMP

Código. Para cada tipo de mensaje diferentes códigos están definidos. Donde los mensajes son:

- No routing hacia el destino
- Comunicación con destino administrativamente prohibido
- No es un vecino
- Dirección inalcanzable
- Puerto inalcanzable

Checksum. Los 16 bits en complemento a 1 de la suma de los mensajes ICMP iniciando con el tipo ICMP. Al calcular el valor del checksum debe ser cero.

Identificador. Un identificador para ayudar a encontrar peticiones respuestas; debe ser cero.

ICMP

Número de secuencia. Número de secuencia para ayudar a encontrar peticiones respuestas; debe ser cero.

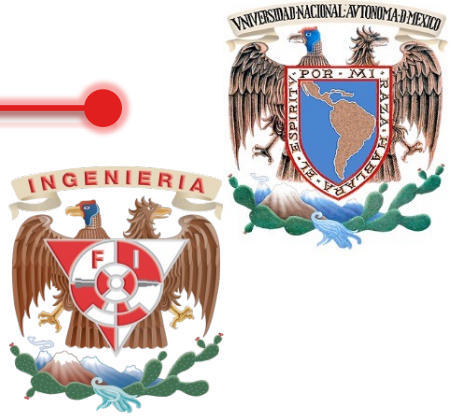
Dirección de la mascara. Una dirección de 32 bits.

Redirección

Cuando un enrutador recibe un host un datagrama cuya mejor “ruta” hacia el destino pasa por otro enrutador de la misma subred física, envía un mensaje de “redirección” al host fuente para pedirle que los siguientes datagramas que envíe al mismo destino los dirija directamente al otro enrutador.

Los códigos de redirección son:

0 para una red	2 para una red con un tipo de servicio
1 para un host	3 para un host con un tipo de servicio



ICMP

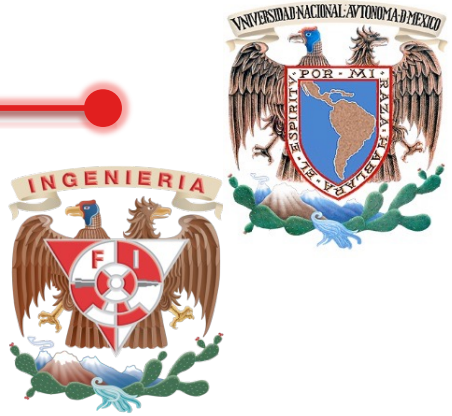
Tiempo Excedido

Cuando se descarta un datagrama debido a que su TTL llega a cero, se envía un mensaje “tiempo excedido” hacia la fuente.

El código del mensaje indica si el datagrama se descartó en un salto (0) o durante el reensamblado (1)

El mensaje “tiempo excedido” se utiliza para implementar el comando “traceroute”

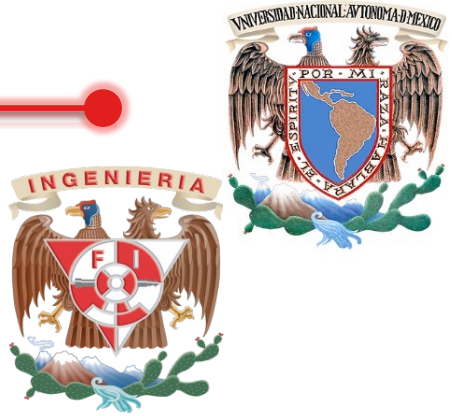
Este comando imprime que enrutadores se encuentran en la ruta hasta cierto destino.



Fragmentación

Los fragmentos son unidades de datos que tienen adentro unidades pequeñas de datos.

El tamaño del fragmento es determinado por el MTU de la interfaz de Red y las capas de hardware (capa física). En IPv4 se especifica la fragmentación y ocurre en el “routing” basado en la interfaz IP.



5.4 Protocolo de Enrutamiento

- Internet se compone de múltiple subredes físicas interconectadas por enrutadores.

•A cada subred física se asigna una dirección de red IP: (netid, 0)

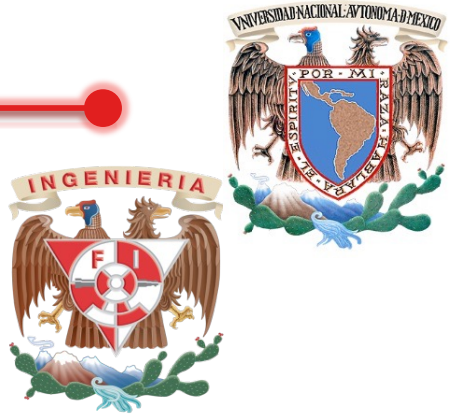
Por convención, el hostid 0 nunca se asigna a un host individual

La dirección que tiene el hostid 0 se reserva para referirse a la red IP

•Entrega directa de datagramas

La transmisión de un datagrama entre dos computadoras conectadas a la misma red IP no involucra routers

La fuente encapsula el datagrama en un paquete de la subred física, agrega la dirección “hardware” correspondiente y envía el paquete directamente al destino.



Entrega indirecta de datagramas.

La transmisión de un datagrama entre dos computadoras conectadas a diferentes redes IP involucra el uso de enrutadores.

La fuente envía el datagrama a un router de su red IP encapsulándolo en un paquete de la subred física.

El datagrama pasa de router a router a través de diferentes subredes físicas hasta que llega a un router directamente conectado a la red destino.

Este router entrega directamente el datagrama al destino encapsulándolo en un paquete de la subred física.

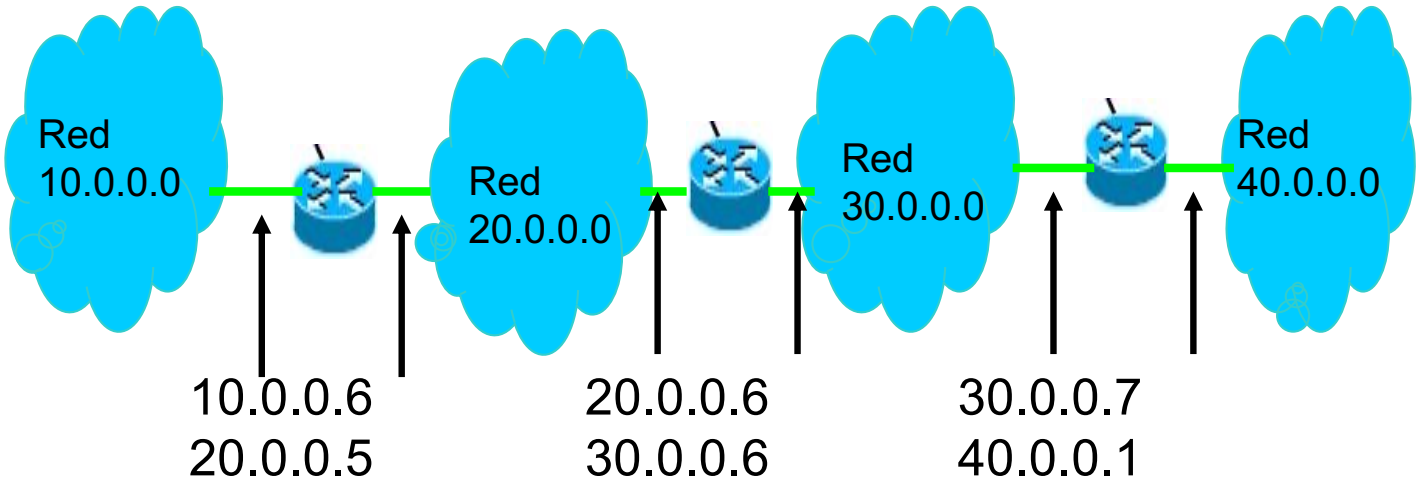
- ¿Cómo sabe la fuente a que enrutador enviar el datagrama?
- ¿Cómo saben los routers la ruta por la que debe pasar el datagrama hasta llegar a la red destino?

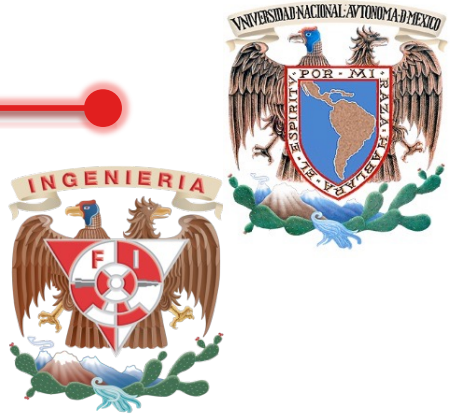
Enrutamiento

Tanto las computadoras como los routers emplean tablas de enrutamiento que contienen una por cada posible red IP destino en la que se indica

Que la entrega es directa. El Algoritmo estático conoce una ó mas rutas si no se encuentran en el destino.

La dirección IP del router que constituye el siguiente salto en la ruta hasta el destino. El Algoritmo dinámico.





Enrutamiento Estático

Como el nombre lo implica, las tablas de “routing” no se cambian. Estas son tablas que se establecen y se construyen manualmente por el administrador de la red.

Una entrada de la base de datos debe estar hecha para cada uno de los segmentos de cada posible ruta a través de la red. Ningún cambio se agrega de la base de datos debe ser hecho manualmente.

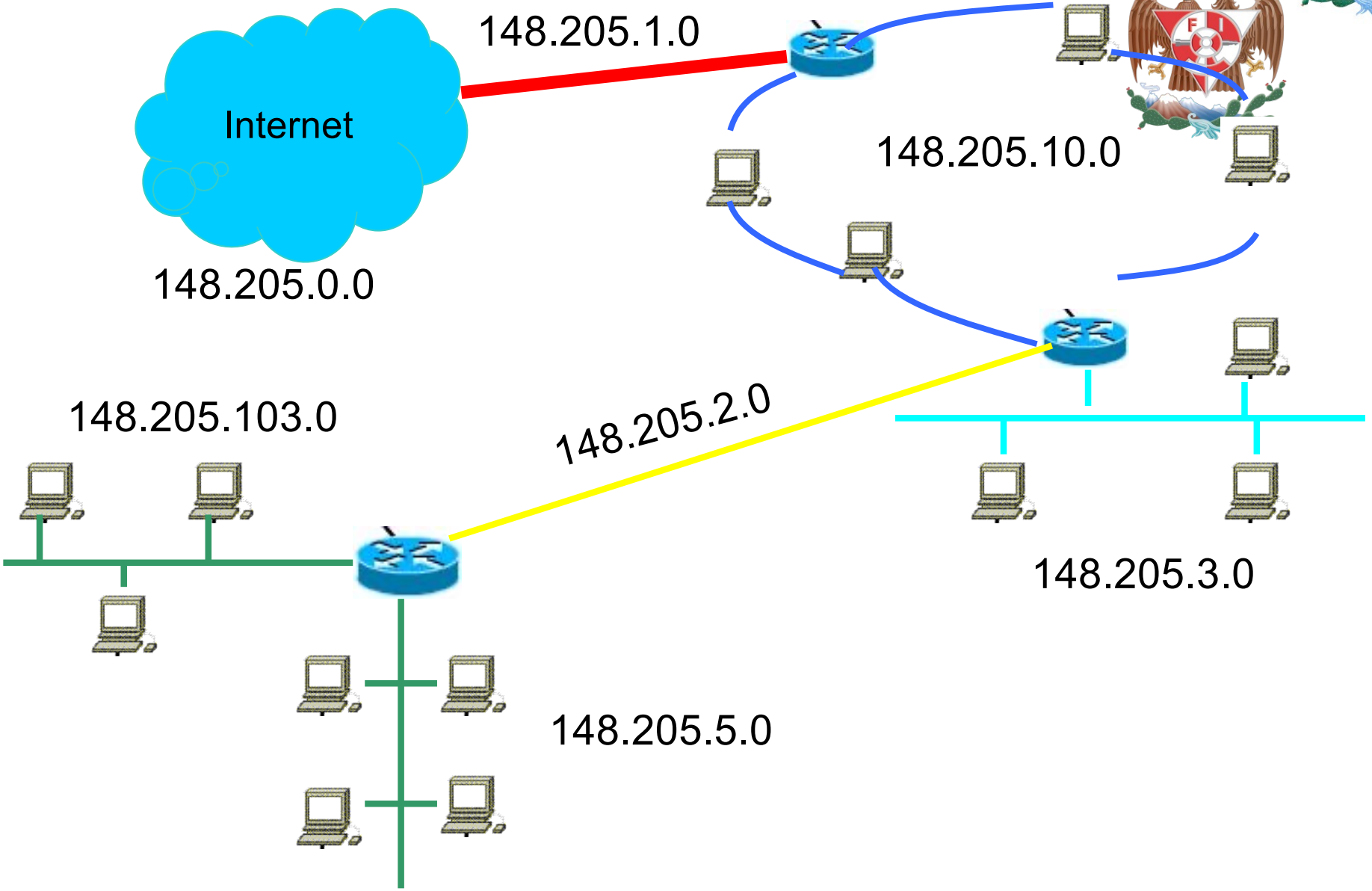
Tabla de routing estáticas debe estar considerada con ventajas en ambientes que requiere absoluta seguridad.

Enrutamiento Dinámico

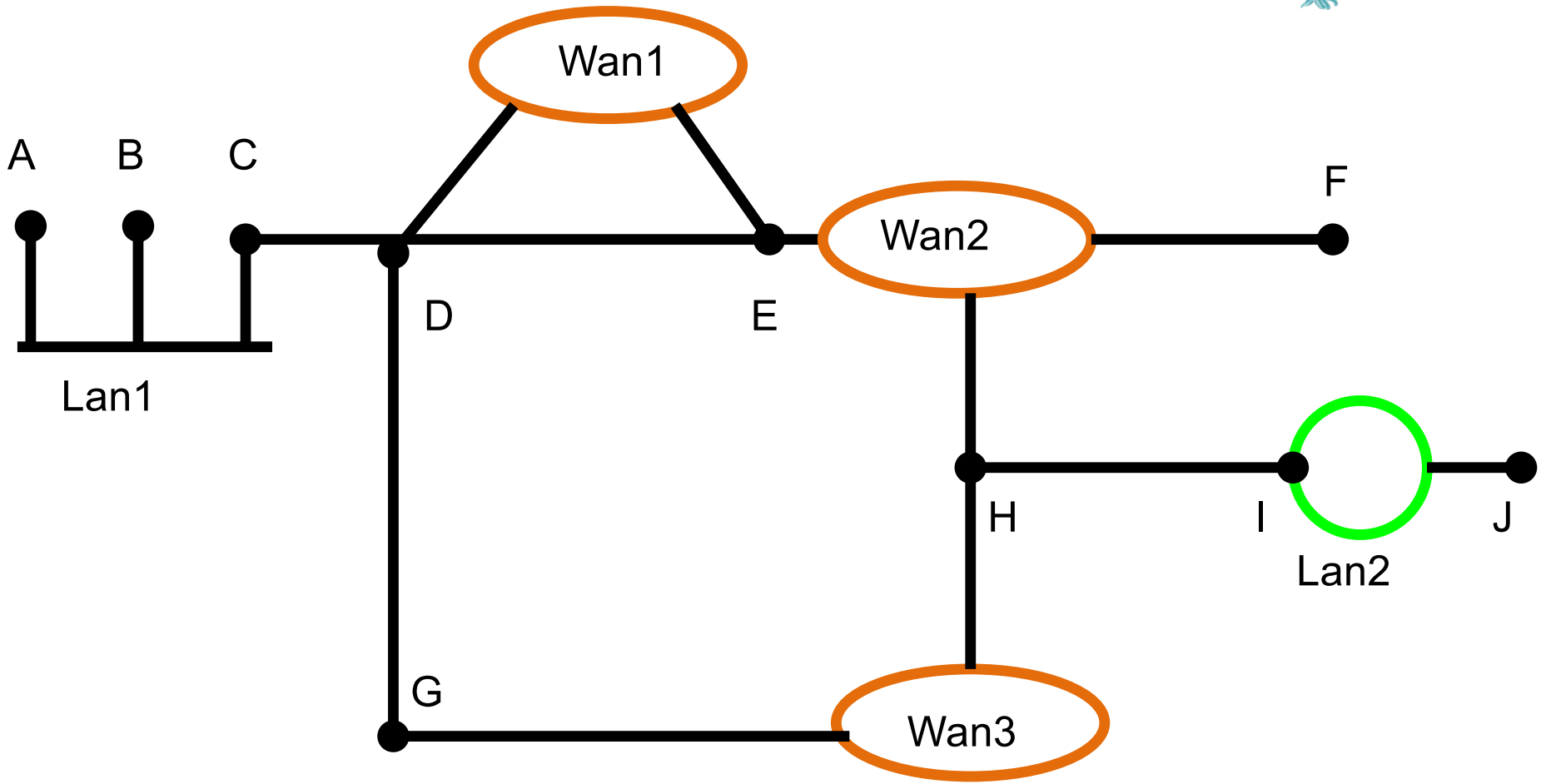
La tablas de routing “dinámico” se generan “dinámica” o automáticamente, se adapta a los cambios de ambiente. Estos tipos de tablas de “routing” son construidas automáticamente por los routers durante la inicialización y son mantenidas y actualizadas por los routers en intervalos regulares. Los Routers contienen paquetes especiales de tipo broadcast que contiene información orientada a las rutas para mantener la tabla de routing.

El camino por el cual las tablas de routings dinámico son creadas y mantenidas esta determinadas por los protocolos de routing o algoritmos a usar.

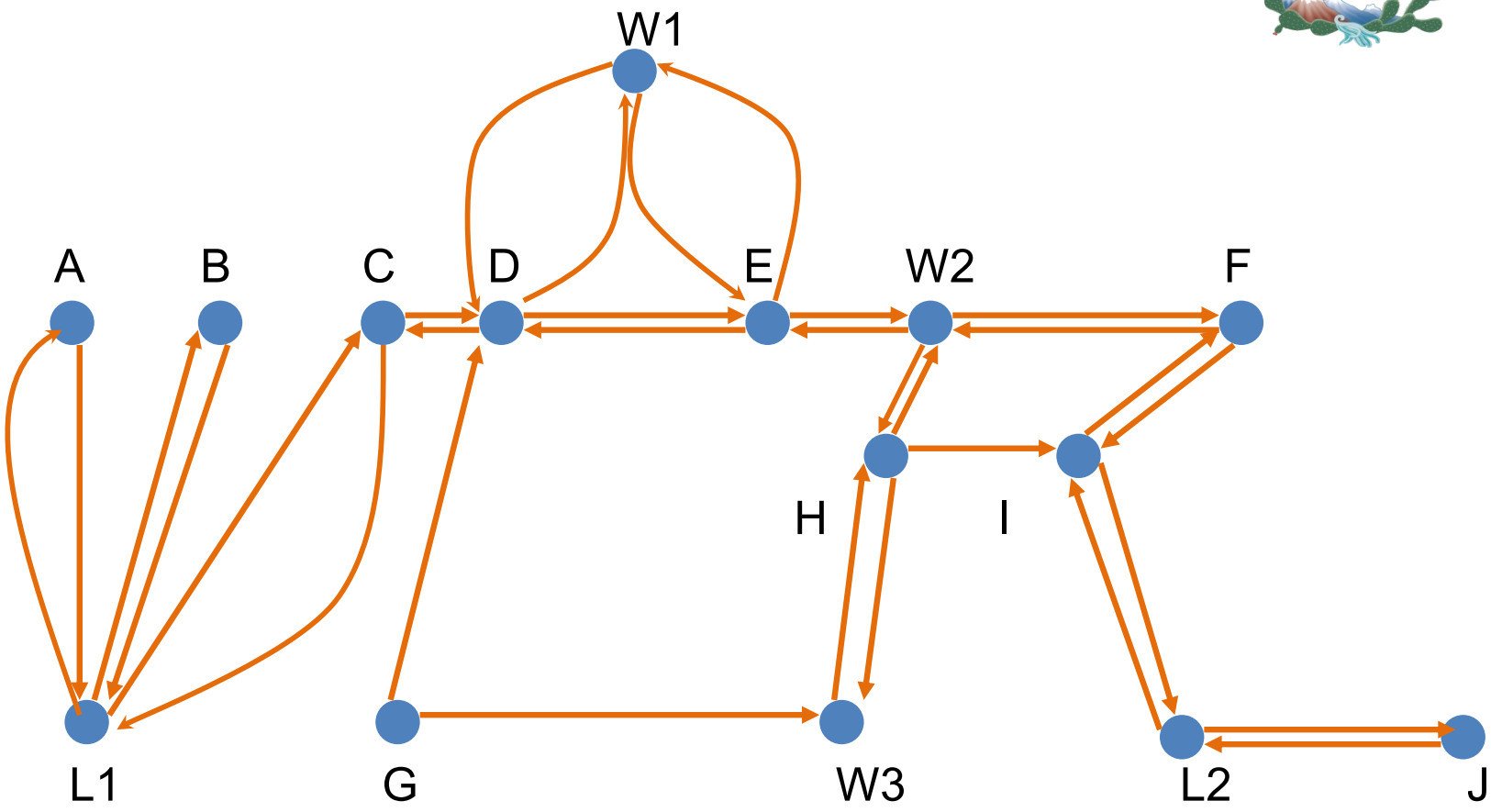
Capa de Red

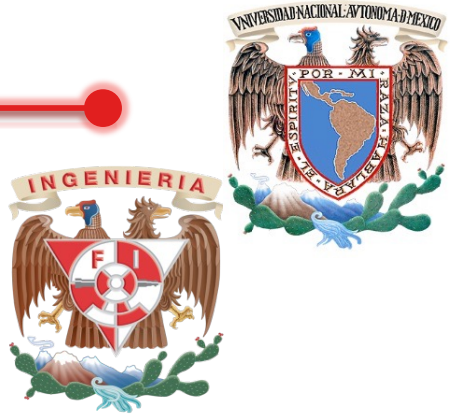

Internet
148.205.1.0
148.205.0.0
148.205.10.0
148.205.103.0
148.205.2.0
148.205.3.0
148.205.5.0

Sistema Autónomo (AS)



Sistema Autónomo con Grafos





Sistema Autónomo

Un sistema autónomo es un conjunto de redes conectadas por dispositivos de “encaminamiento” homogéneos; normalmente estos dispositivos de encaminamiento están bajo el control administrativo de una entidad única.

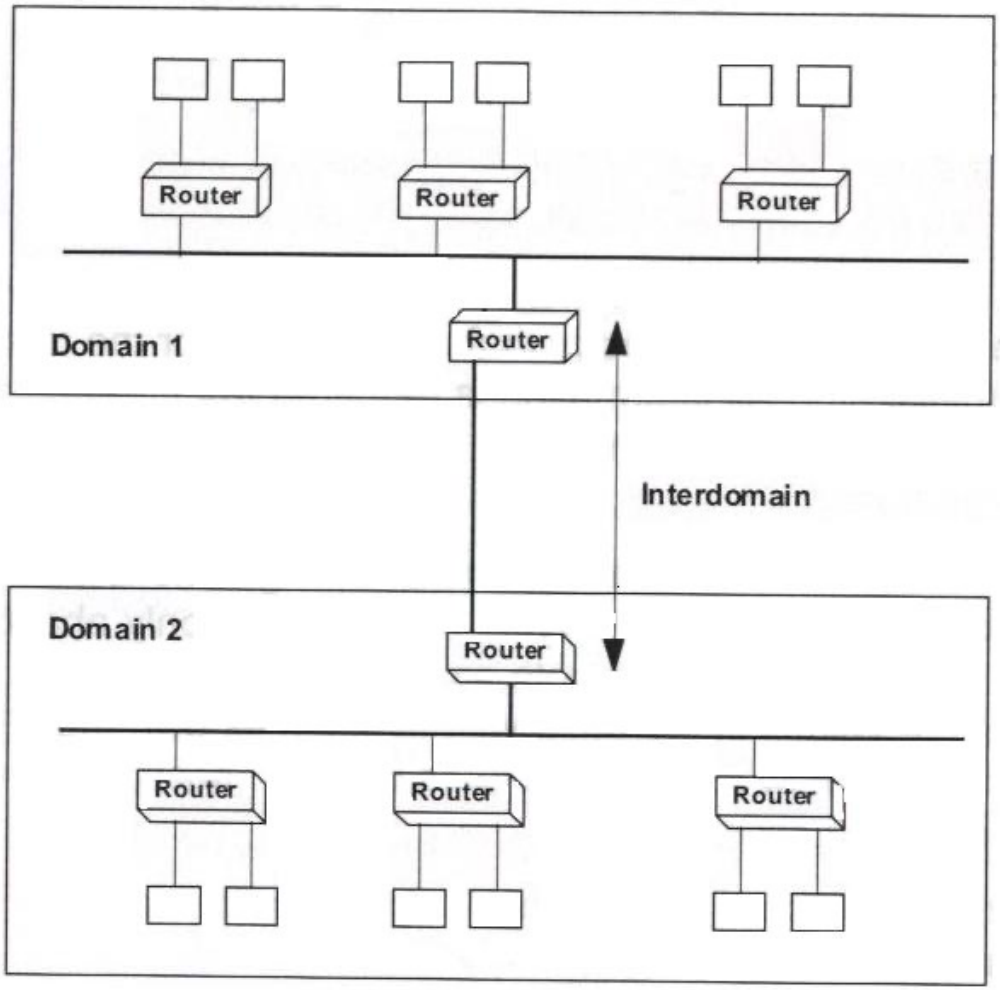
Existen tres protocolos de enrutamiento o encaminamiento

Interior Gateway Protocol (IGP)

Exterior Gateway Protocol (EGP)

Border Gateway Protocol (BGP)

Sistema Autónomo



Protocolo de Enrutamiento

Tipo de Protocolo	Vector-Distancia	Estado del Enlace
IGP	GGP Hello RIP IGPR	OSPF Integrated IS-IS
EGP	EGP BGP	IDRP

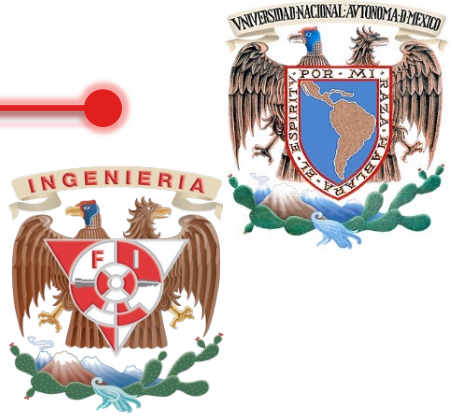
OSPF: Open Shortest Path First

EGP: Exterior Gateway Protocol

BGP: Border Gateway Protocol

IDRP: Interdomain Routing Protocol

IGRP: Interior Gateway Routing Protocol



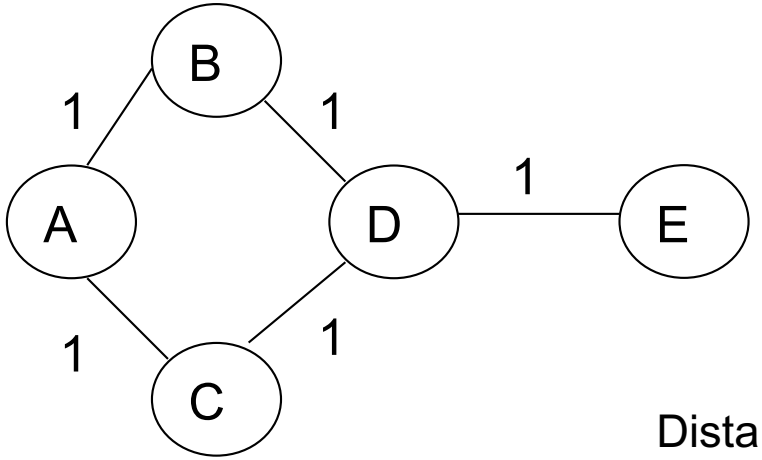
Algoritmo por Vector-Distancia

Fue el primer algoritmo original utilizado en ARPANET y es la base del protocolo RIP I y II, utilizado para calcular la ruta más corta. Utiliza el algoritmo de distancia de Bellman-Ford.

Cada nodo informa a sus vecinos de todas las distancias conocidas por él, mediante vectores de distancia (de longitud variable según los nodos conocidos).

El nodos conoce solo la distancia a los distintos nodos de la red pero no la topología.

Estos vectores de distancia se envía periódicamente, y cada vez que varía su vector de distancias.



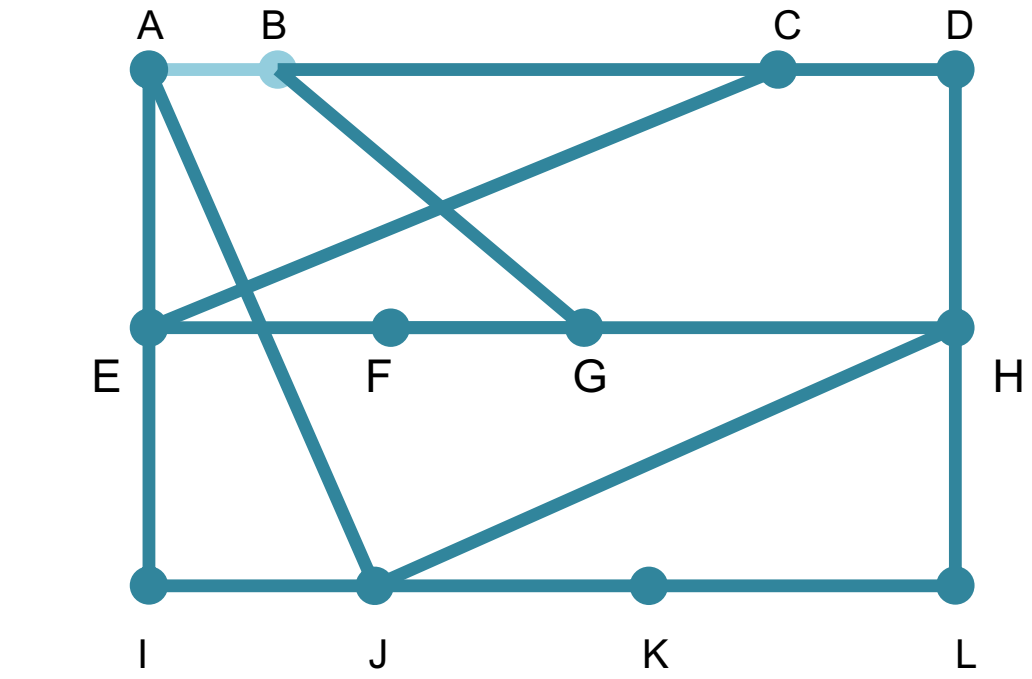
$VD_A=(A=0;B=1;C=1)$

Distancia de A → A

Distancia de A → B

$VD_B=(B=0;A=1;D=1)$ ⟶ $VD_B=(B=0;A=1;C=2;D=1)$

Ejemplo. Utilizando la métrica del retardo. El router conoce el retardo a sus vecinos. Cada T_{msg}, cada router envía a sus vecinos una lista de retardos estimados y recibe lo propio de estos. Con la información recibida cada router recalcula su tabla de enrutamiento.



JA → 8 JI → 10 JH →12 JK →6

	A	I	H	K	J
A	0	24	20	21	8
B	12	36	31	28	20
C	25	18	19	36	28
D	40	27	8	24	20
E	14	7	30	22	17
F	23	20	19	40	30
G	18	31	6	31	18
H	17	20	0	19	12
I	21	0	14	22	10
J	9	11	7	10	0
K	24	22	22	0	6
L	29	33	9	9	15

Enrutamiento Vector Distancia

Ventajas

•Muy sencillo

•Muy robusto (debido al envío periódico de la información)

•Consumo de memoria bajo: Cada nodo solo ha de almacenar distancias con el resto de los nodos

Desventajas

•Convergencia lenta

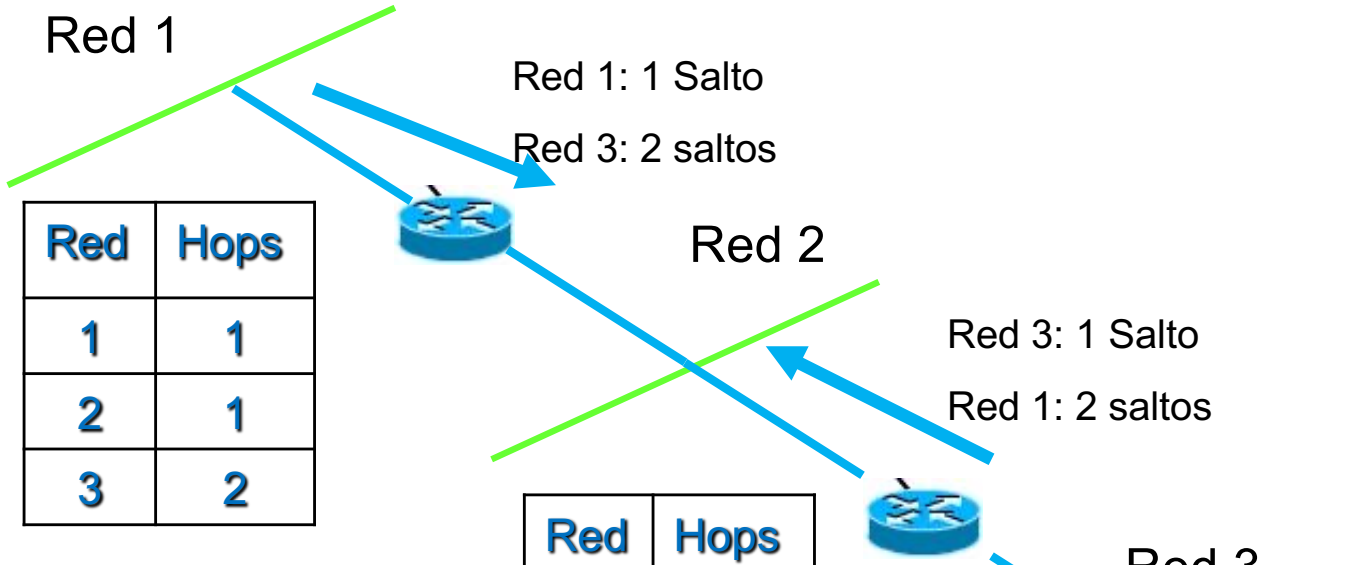
•Pueden aparecer bucles (ciclos infinitos)

•Adaptabilidad a los cambios, ya que solo sabe a quien tiene que enviar un paquete (no se cuenta con la topología de la red)

•Consumo alto de capacidad: se transmiten vectores cuyo tamaño es del orden del número de nodos de la red pues cada nodo comunica a su vecino todas las distancias que conoce.

25 nodos por vector (sino sobrepasa los paquetes)

Enrutamiento Vector Distancia



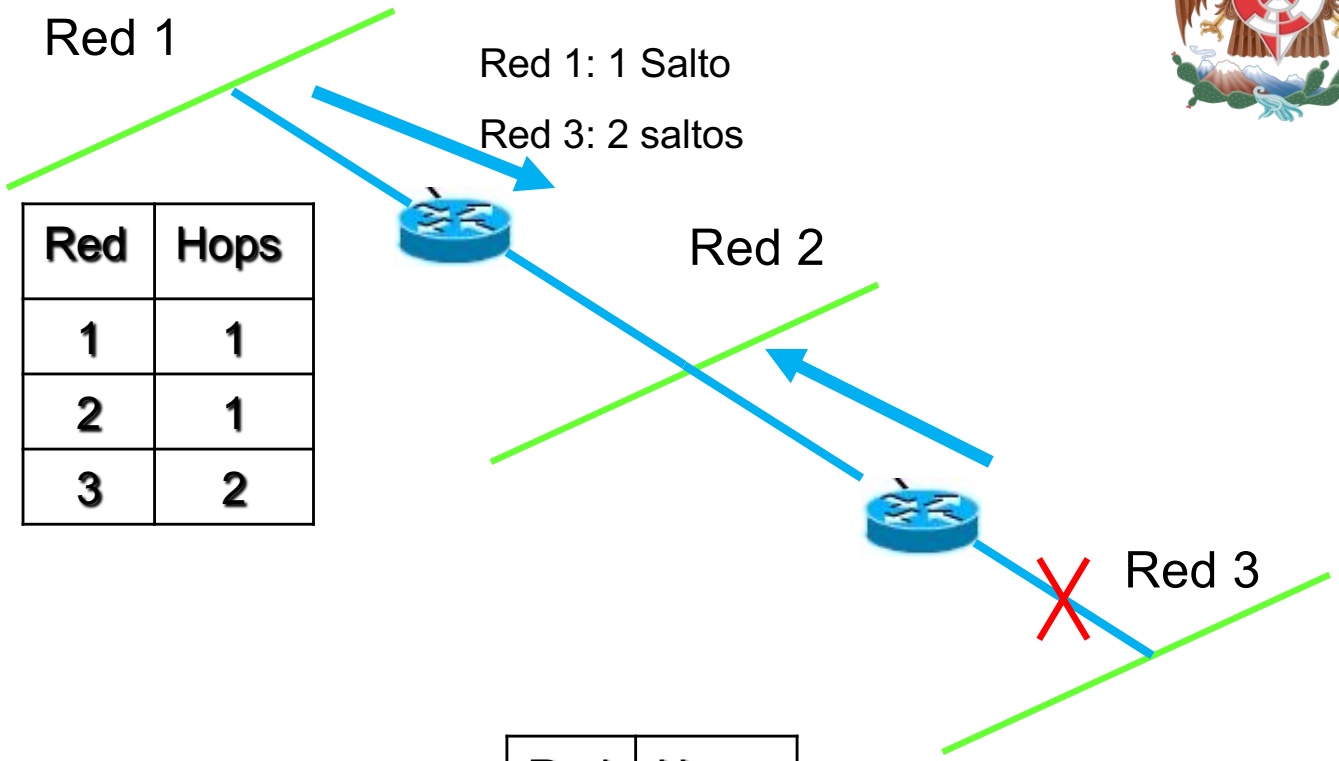
Red	Hops
1	1
2	1
3	2

Red	Hops
1	2
2	1
3	1

Red	Hops
1	2
2	1
3	16

Tabla cuando el enlace hacia la Red 3 falla

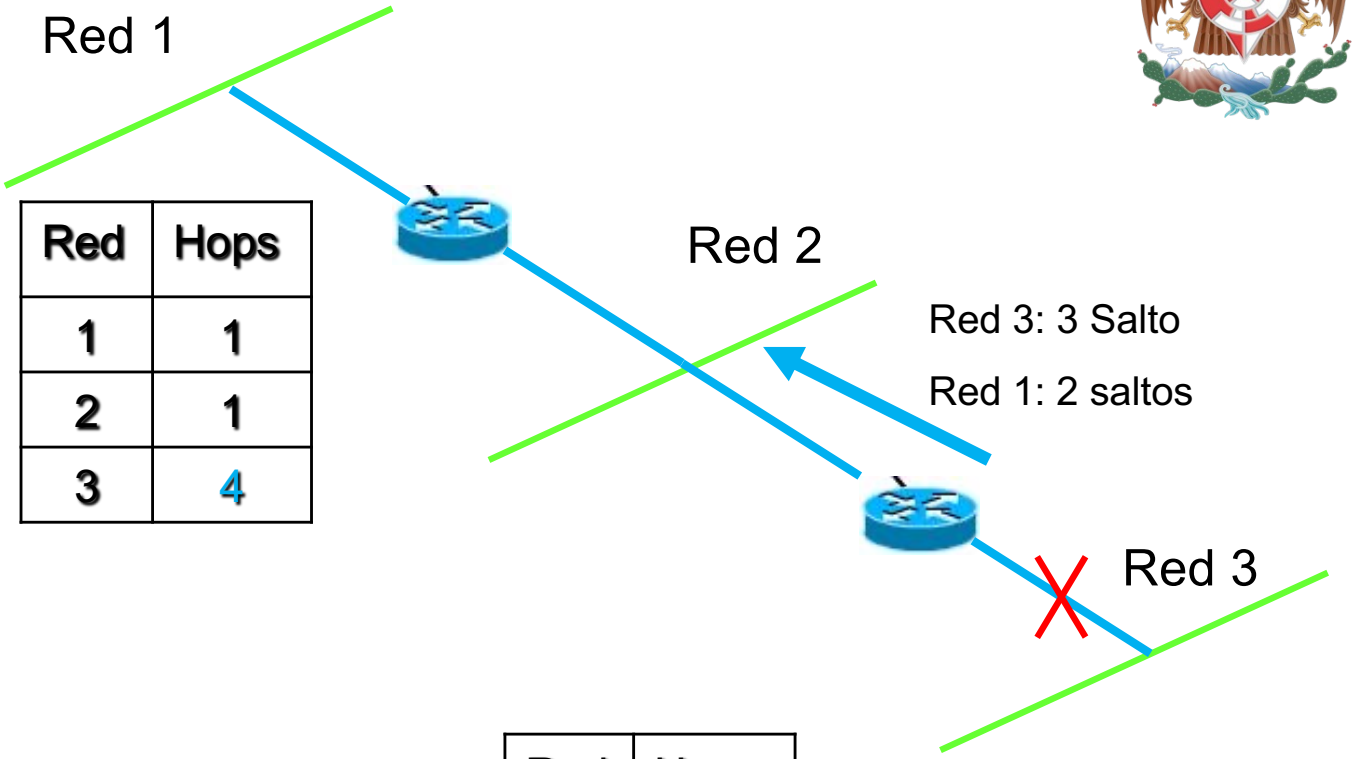
Enrutamiento Vector Distancia



Red	Hops
1	1
2	1
3	2

Red	Hops
1	2
2	1
3	3

Enrutamiento Vector Distancia

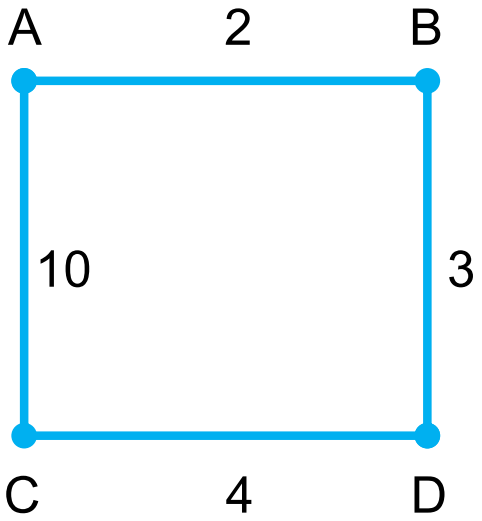


Red	Hops
1	1
2	1
3	4

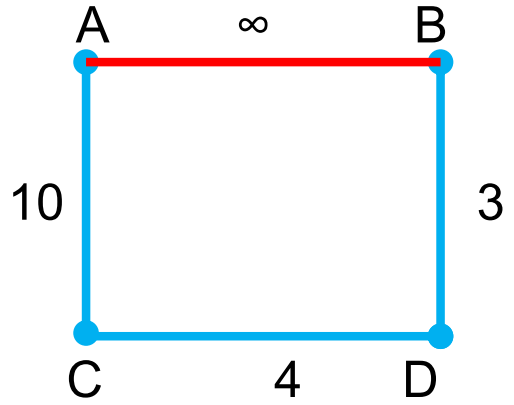
Red	Hops
1	2
2	1
3	3

Enrutamiento Vector Distancia

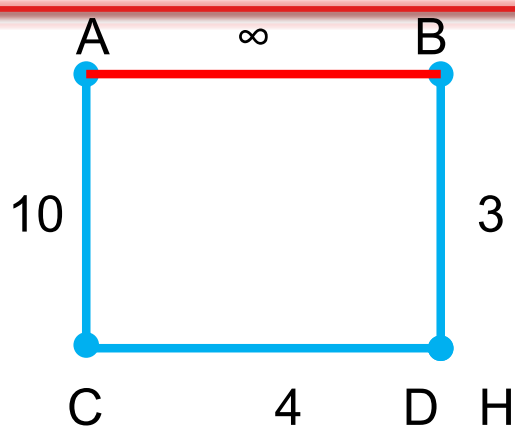
Hold Down (Espera): Espera cuando un router detecta que un enlace se ha caído, éste no acepta mensajes de enrutamiento por un periodo determinado. Esto permite que la actualización inmediatamente se propague. Por ejemplo:



Dest	IMP A Coste por	IMP B Coste por	IMP C Coste por	IMP D Coste por
A	0 ---	2 A	9 D	5 B
B	2 B	0 ---	7 D	3 B
C	9 B	7 D	0 ---	4 C
D	5 B	3 D	4 D	0 ---



Vector Distancia **Hold Down**



Primer intercambio

HD1

DEST	A
A	-----
B	∞ B
C	∞ B
D	∞ B

HD1

DEST	B
A	∞ A
B	----
C	7 D
D	3 D

HD1

DEST	C
A	9 D
B	7 D
C	----
D	4 D

HD1

DEST	D
A	5 B
B	3 B
C	4 C
D	----

Segundo intercambio

HD2

DEST	A
A	-----
B	∞ B
C	∞ B
D	∞ B

HD2

DEST	B
A	∞ A
B	----
C	7 D
D	3 D

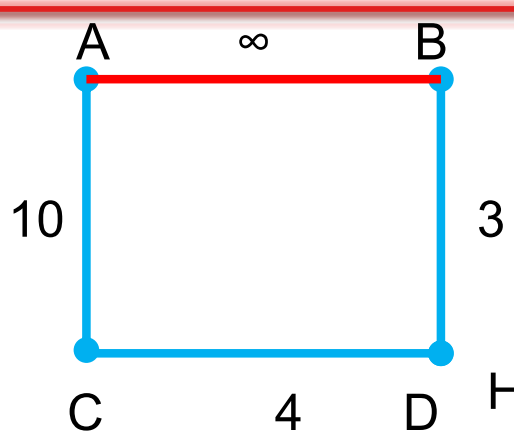
HD2

DEST	C
A	9 D
B	7 D
C	----
D	4 D

HD1

DEST	D
A	∞ B
B	3 B
C	4 C
D	----

Vector Distancia **Hold Down**



HD3

DEST	A
A	-----
B	∞ B
C	∞ B
D	∞ B

HD3

DEST	B
A	∞ A
B	----
C	7 D
D	3 D

HD1

DEST	C
A	∞ D
B	7 D
C	----
D	4 D

HD2

DEST	D
A	∞ B
B	3 B
C	4 C
D	----

Tercer intercambio

Actualiza

DEST	A
A	-----
B	17 C
C	10 C
D	14 C

No Actualiza

DEST	B
A	∞ D
B	----
C	7 D
D	3 D

HD2

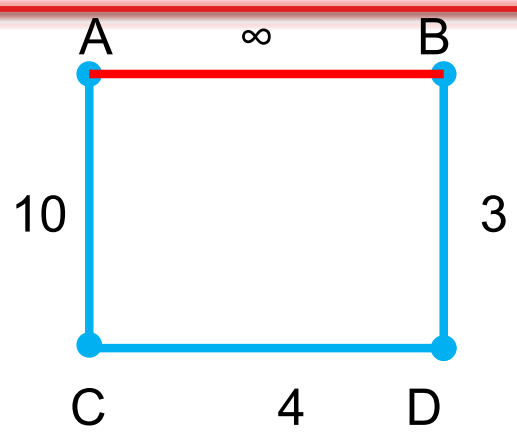
DEST	C
A	∞ D
B	7 D
C	----
D	4 D

HD3

DEST	D
A	∞ B
B	3 B
C	4 C
D	----

HD expiro

Vector Distancia **Hold Down**



No puede porque todavía no llega C

HD3

Actualiza

HD expiro

DEST	A
A	-----
B	17 C
C	10 C
D	14 C

DEST	B
A	∞ D
B	----
C	7 D
D	3 D

DEST	C
A	∞ D
B	7 D
C	----
D	4 D

DEST	D
A	∞ B,C
B	3 B
C	4 C
D	----

Actualiza

HD expiro

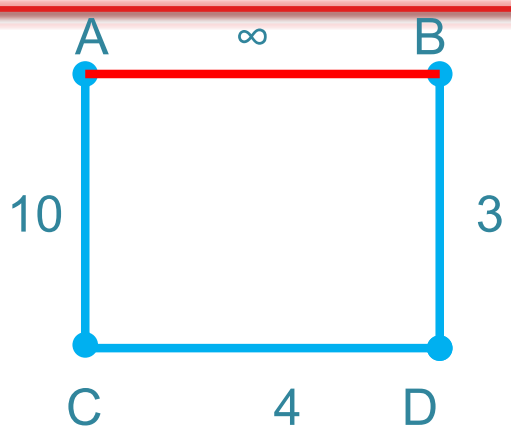
DEST	A
A	-----
B	17 C
C	10 C
D	14 C

DEST	B
A	∞ D
B	----
C	7 D
D	3 D

DEST	C
A	10 A
B	7 D
C	----
D	4 D

DEST	D
A	∞ B
B	3 B
C	4 C
D	----

Vector Distancia **Hold Down**



Actualiza

HD expiro

DEST	A
A	-----
B	17 C
C	10 C
D	14 C

DEST	B
A	∞ D
B	----
C	7 D
D	3 D

DEST	C
A	10 A
B	7 D
C	----
D	4 D

DEST	D
A	14 C
B	3 B
C	4 C
D	----

HD expiro

DEST	A
A	-----
B	17 C
C	10 C
D	14 C

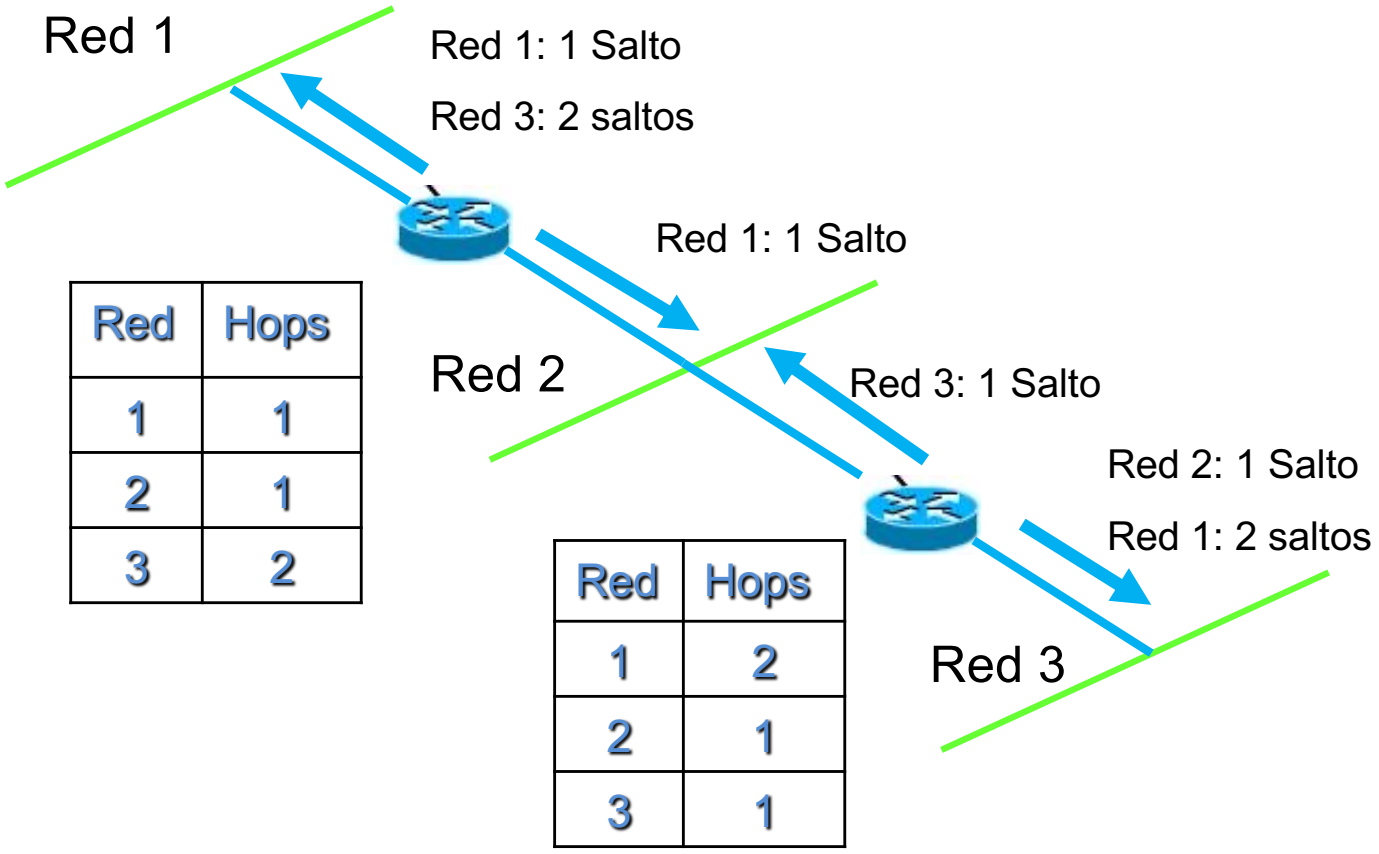
DEST	B
A	17 D
B	----
C	7 D
D	3 D

DEST	C
A	10 A
B	7 D
C	----
D	4 D

DEST	D
A	14 B
B	3 B
C	4 C
D	----

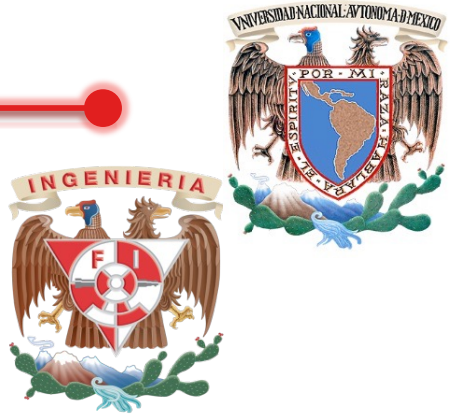
Vector Distancia **Split Horizont**

El protocolo de Horizontes divididos (Split horizont). Si un enrutador no anuncia rutas por la misma interfaz en el que le llegaron. Con esto se elimina el problema de tener que contar hasta “infinito”.



Red	Hops
1	1
2	1
3	2

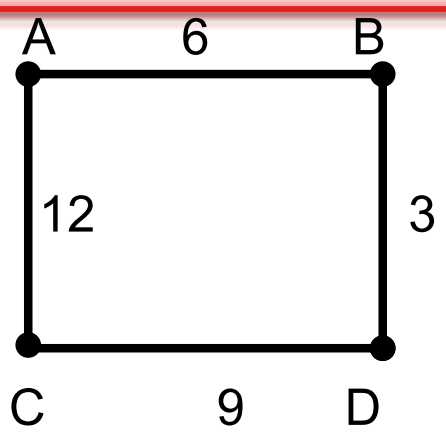
Red	Hops
1	2
2	1
3	1

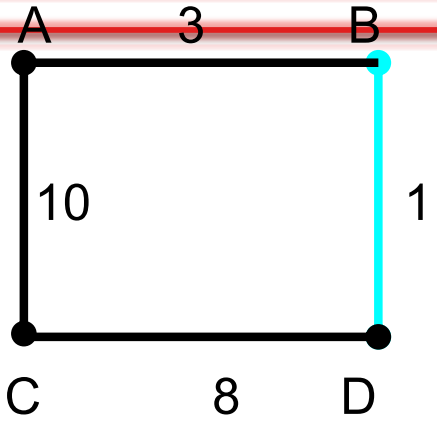


Triggered Updates (Actualizaciones Desencadenadas)

Cuando uno de los enlaces del router se “cae”, un mensaje de actualización es enviado sin la necesidad de esperar los 3 intentos reglamentarios: Mejora tiempo de convergencia. Disminuye el tráfico de difusión.

Vector Distancia **Triggered Updates**





Solamente los routers se dan cuenta de los enlaces adyacentes

Original

DEST	A
A	-----
B	6,A
C	12,A
D	9,B

DEST	B
A	6,B
B	----
C	12,D
D	3,B

DEST	C
A	12,A
B	12,D
C	----
D	9,C

DEST	D
A	9,B
B	3,D
C	9,D
D	----

Primer intercambio

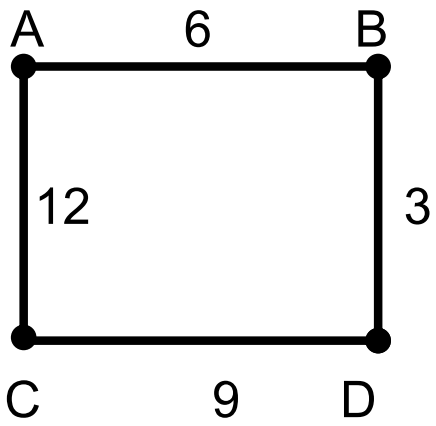
DEST	A
A	----
B	3,A
C	10,A
D	6,B

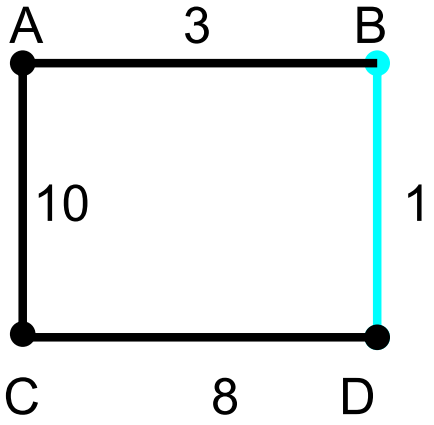
DEST	B
A	3,B
B	----
C	10,C
D	1,B

DEST	C
A	10,C
B	11,D
C	----
D	8,C

DEST	D
A	7,B
B	1,D
C	8,D
D	----

Vector Distancia **Triggered Updates**





Segundo intercambio

DEST	A
A	----
B	3,A
C	10,A
D	4,B

DEST	B
A	3,B
B	----
C	9,D
D	1,B

DEST	C
A	10,C
B	9,D
C	----
D	8,C

DEST	D
A	4,B
B	1,D
C	8,C
D	----

Enrutamiento Vector Distancia

•Cada enrutador envía a sus vecinos su vector de distancias cada 30 segundos.

•En un mensaje RIP pueden enviarse hasta 25 entradas del vector de distancias.

•Para transportar vectores grandes se utilizan varios mensajes.

•Los algoritmos de vectores de distancias son buenos para redes estables y pequeñas.

•Su principal desventaja es que no escalan bien: su desempeño es bajo en Sistemas Autónomos grandes ya que el tamaño de sus mensajes es directamente proporcional al número de redes existentes.

Protocolo de Enrutamiento OSPF

OSPF: Open Shortest Path First

Es el protocolo de enrutamiento más usado en Internet

Utilizan un algoritmo de “Estado del Enlace” (Link State)

La métrica utilizada por omisión por los enrutadores es inversamente proporcional a la velocidad de transmisión del enlace:

$$\text{Distancia} = 10^8 / \text{velocidad de Transmisión}$$

Por ejemplo, para una red Ethernet a 10 Mbps, la distancia es 10

Cada enrutador verifica continuamente los enlaces que lo unen con enrutadores adyacentes intercambiando mensajes Hello.

Típicamente, los mensajes se envían cada 10 segundos y se considera que ha ocurrido una falla en un vecino si no se recibe un mensaje de él durante 40 segundos.

Protocolo de Enrutamiento OSPF

OSPF: Open Shortest Path First

Cada enrutador difunde cada 30 segundos, o cuando hay un cambio en el estado de uno de sus enlaces, Link State Advertisements a todos los enrutadores del Sistema Autónomo para notificarles el estado de sus enlaces.

Cada enrutador conoce entonces la topología completa del Sistema Autónomo (link-state database) y se utiliza el algoritmo del camino más corto de Dijkstra para construir su tabla de enrutamiento.

Cada enrutador construye un árbol de caminos más cortos con él como raíz.

Protocolo de Enrutamiento OSPF

Algoritmo Dijsktra

1. Inicio
2. N={A}
3. For all nodes V
4. If V adyacente de A
5. then D(V) = C(A,V)
6. Else D(V)= infinito
7. .
8. *Loop*
9. Find w not in N tal que D(w) es un mínimo
10. Add w to N.
11. Update D(V) para todo V adyacente a W y no este en N
12. D(V)=min[D(V),D(W)+c(w,v)]
13. /* Nuevo costo para V sea cualquier viejo costo de V o la conocida ruta mas corta en costo para w mas el costo de w a v */
14. *Mientras haya nodos en N*

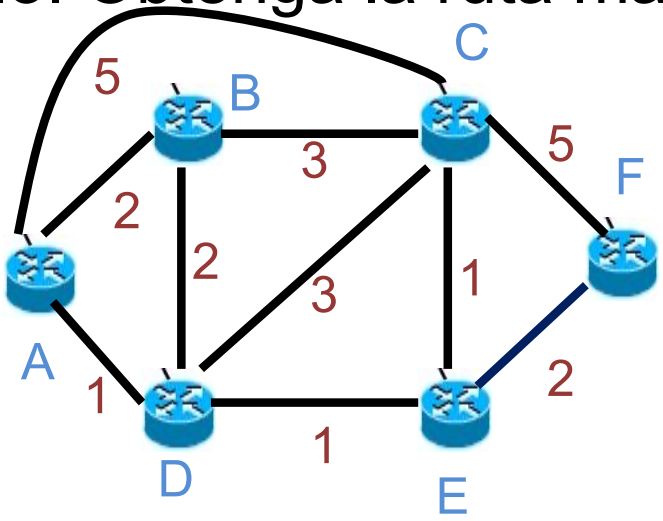
N es el conjunto de nodos por el cual se tienen los pasos de la ruta del costo mínimo

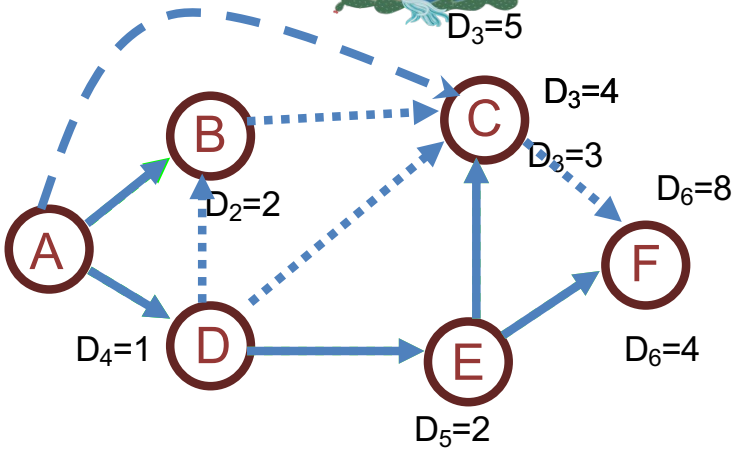
D(x) es la ruta del costo mínimo actual hacia X

C(n,m) es el costo del enlace de n a m

Algoritmo Dijsktra

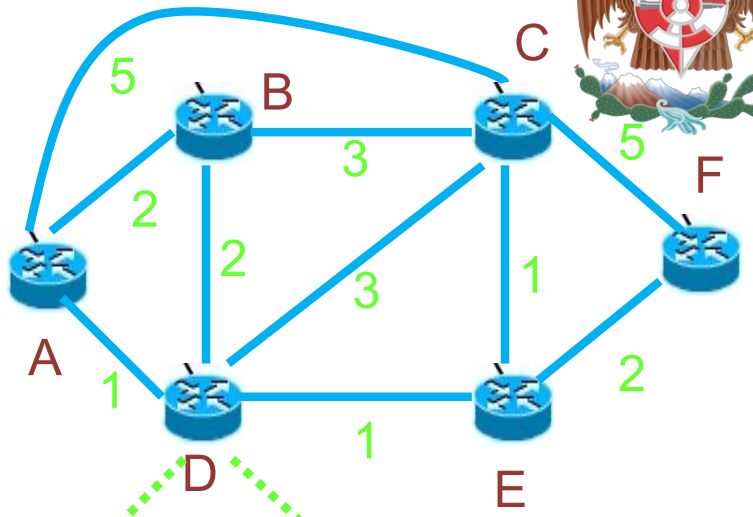
Ejemplo. Obtenga la ruta más corta de A → F





Iteración	N	D_2	Ruta	D_3	Ruta	D_4	Ruta	D_5	Ruta	D_6	Ruta
1	{A}	2	A-B	5	A-C	1	A-D	∞	----	∞	----
2	{A,D}	2	A-B	4	A-D-C	1	A-D	2	A-D-E	∞	----
3	{A,B,D}	2	A-B	4	A-D-C	1	A-D	2	A-D-E	∞	----
4	{A,B,D,E}	2	A-B	3	A-D-E-C	1	A-D	2	A-D-E	4	A-D-E-F
5	{A,B,C,D,E}	2	A-B	3	A-D-E-C	1	A-D	2	A-D-E	4	A-D-E-F
6	{A,B,C,D,E,F}	2	A-B	3	A-D-E-C	1	A-D	2	A-D-E	4	A-D-E-F

Algoritmo Dijsktra



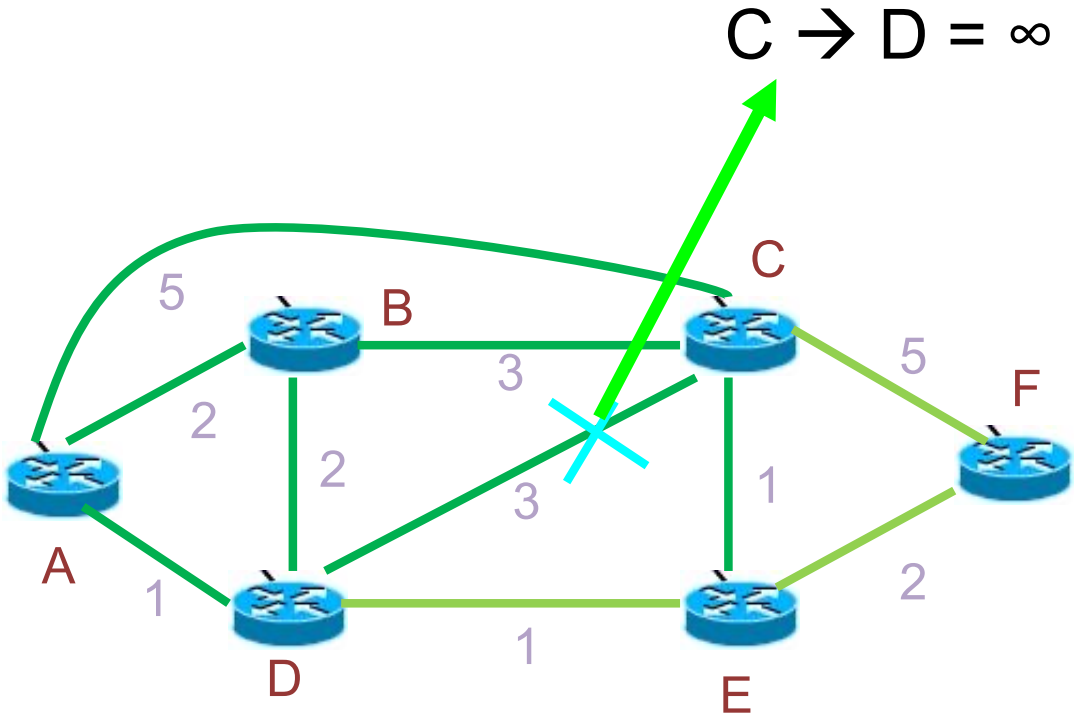
Estado del Enlace del router A

	Primer nodo por la ruta mas corta
B	B
C	D
D	D
E	D
F	D

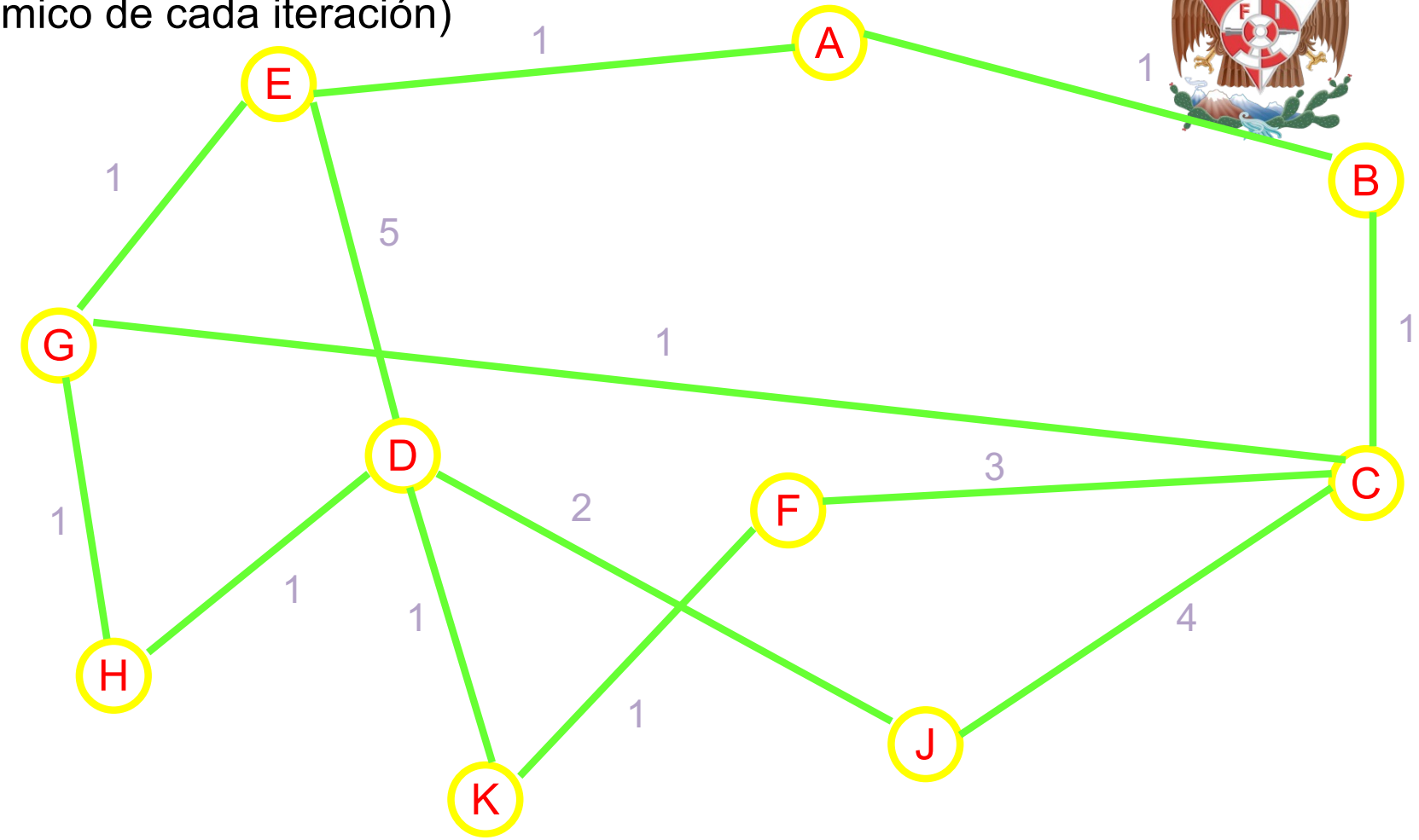
Estado del Enlace del router D

	Primer nodo por la ruta mas corta
A	A
B	B
C	E
E	E
F	E

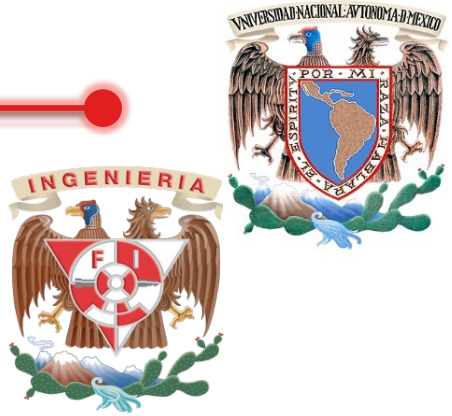
Algoritmo de Inundación del Estado del Enlace (Link State Floading)



Tarea: Obtenga la ruta mas corta de A → K (incluir diagrama dinámico de cada iteración)



Iteración	N	D_2 Ruta	D_3 Ruta	D_4 Ruta	D_5 Ruta	D_6 Ruta



Protocolo OSPF

OSPF soporta un enrutamiento jerárquico

Cada Sistema Autónomo tiene un backbone al cual se conectan todas las demás áreas

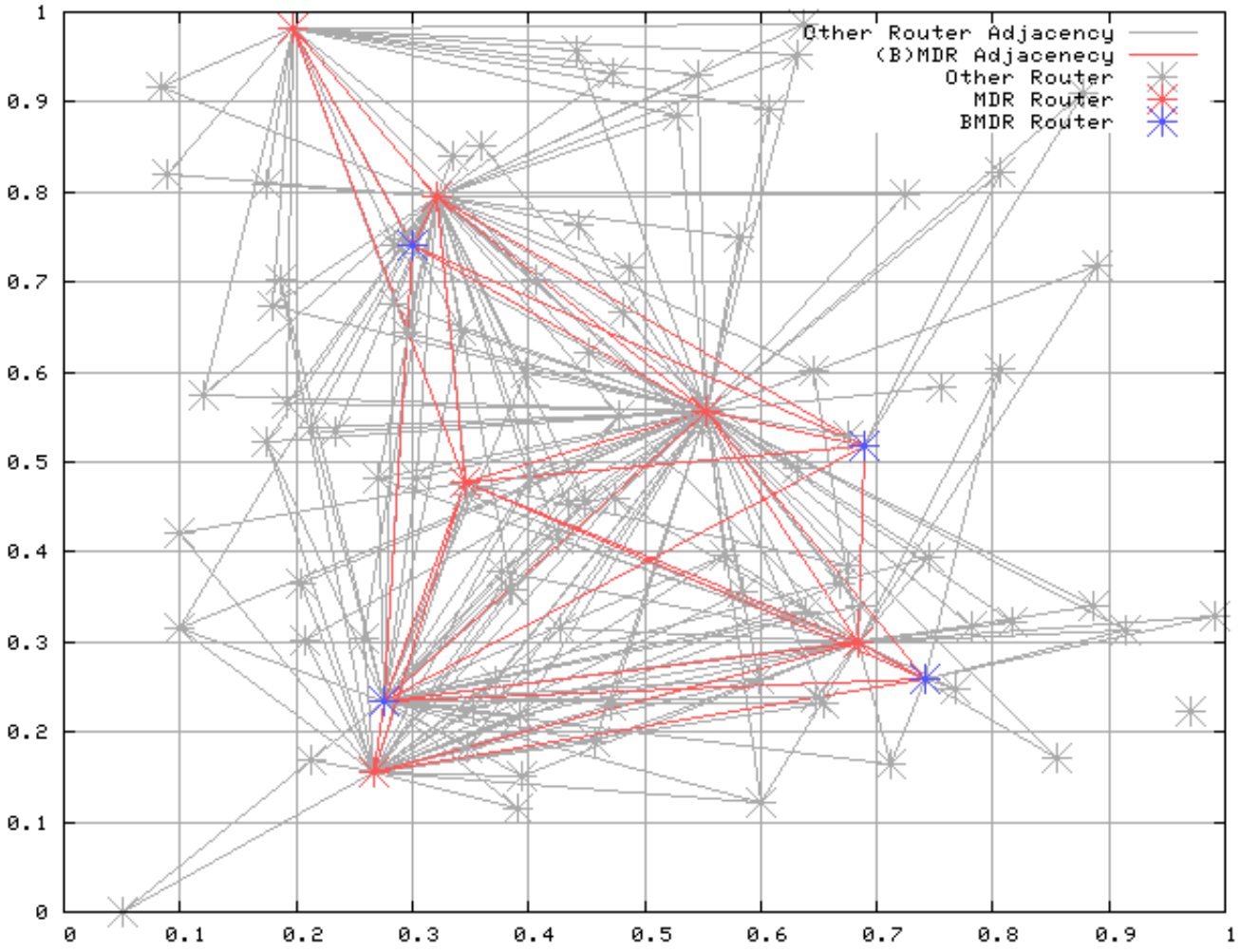
Los routers de cada área conocen completamente su topología interna.

La topología de cada área no es visible desde otras áreas, solo se conoce que redes contiene.

El enrutamiento de un datagrama IP entre áreas consta de tres pasos:

- Desde la fuente hasta un router en su área que forme parte del backbone
- A través del backbone hasta un enrutador que forme parte del área destinataria
- Hasta el destino

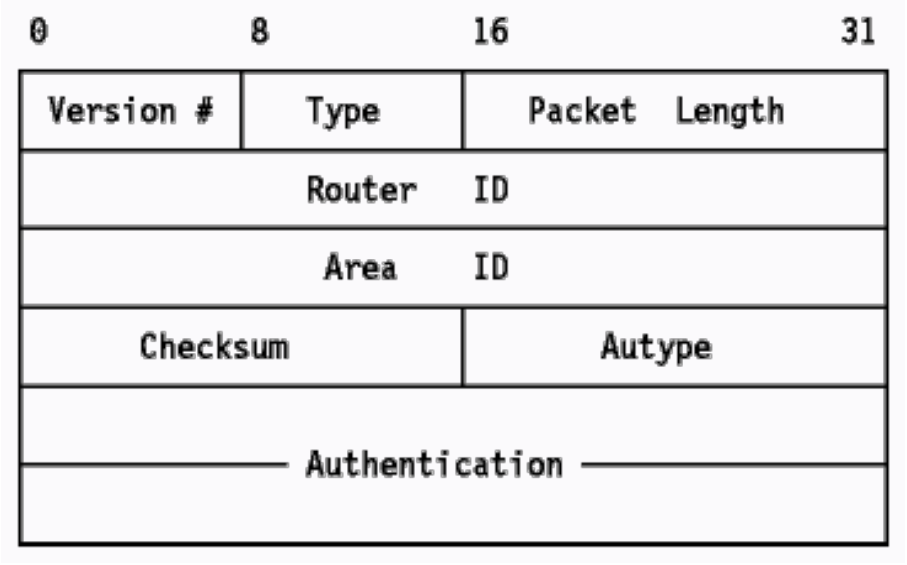
Protocolo OSPF



Protocolo OSPF

Los mensajes OSPF se encapsulan en datagramas IP

Las actualizaciones se envían en multicast a la dirección 224.0.0.5



Protocolo de enrutamiento: OSPF

Versión: Versión del protocolo (2 en la actualidad)

Packet type: Identifica el tipo de mensaje.

1- Hello (pruebas de accesibilidad). Son periodicas y sirven para saber si el vecino es accesible

2-Descripción de la base de datos (Topología)

3-Petición de estado del enlace (para actualizar la Base de Datos Topologica)

4-Actualización del estado del enlace

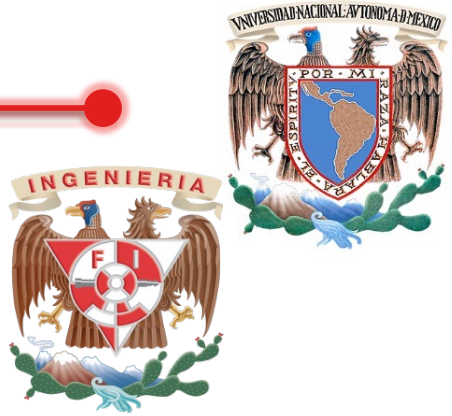
5-Acuse de recibo del estado del enlace

Packet length: Número de bytes del paquete

Router ID: Dirección IP del enrutador del emisor

Area ID: Identificador del área a la que pertenece el paquete

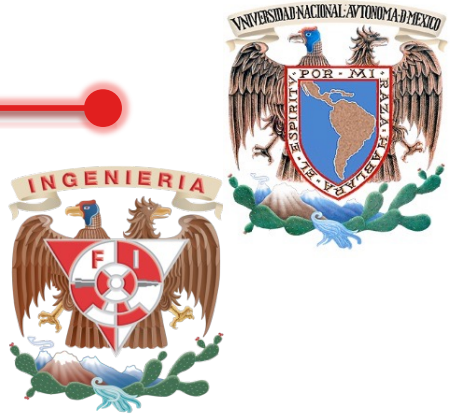
Checksum: código de error (similar al que usa IP)



Protocolo de enrutamiento: OSPF

Conclusión

- OSPF es un protocolo abierto
- Responde rápidamente a cambios en la topología de la red y genera poco tráfico
- Proporciona balanceo de cargas entre múltiples rutas que tenga la misma distancia



Multicast

Unicast. Identifica a un host en una red. (Ejemplo 192.164.34.4)

Broadcast. Identifica a todos los hosts de una red. (Ejemplo 172.16.255.255)

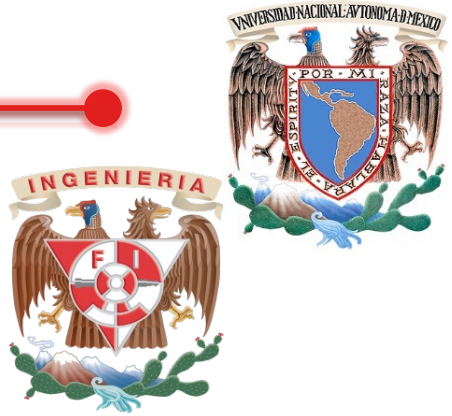
Multicast. Direcciona a un grupo concreto de hosts dentro de una subred (Clase D: 224.0.0.0 – 239.255.255.255)

Dirección 224.0.0.1 → Todos los hosts y routers de una subred

Dirección 224.0.0.2 → Todos los routers con capacidades multicast de una subred

Dirección 224.0.0.0 - 224.0.0.255 → Reservado para protocolos de bajo nivel

Dirección 239.0.0.0 → 239.255.255.255 → Reservado para usos administrativos



Multicast

Si un host se une a un grupo multicast, recibirá todo el tráfico unicast dirigido a él, el broadcast dirigido a toda la subred y el tráfico multicast dirigido al grupo al que se ha unido.

Para participar en IP multicast sobre una subred física, un host debe tener software que le permita mandar y recibir datagramas multicast.

Para participar en multicast sobre internet, un host debe informar a los enrutadores locales multicast.

APLICACIONES

La enseñanza a distancia
La difusión de noticias sobre el escritorio

Las reuniones de empresas virtuales

Otras aplicaciones a considerar en la distribución de software

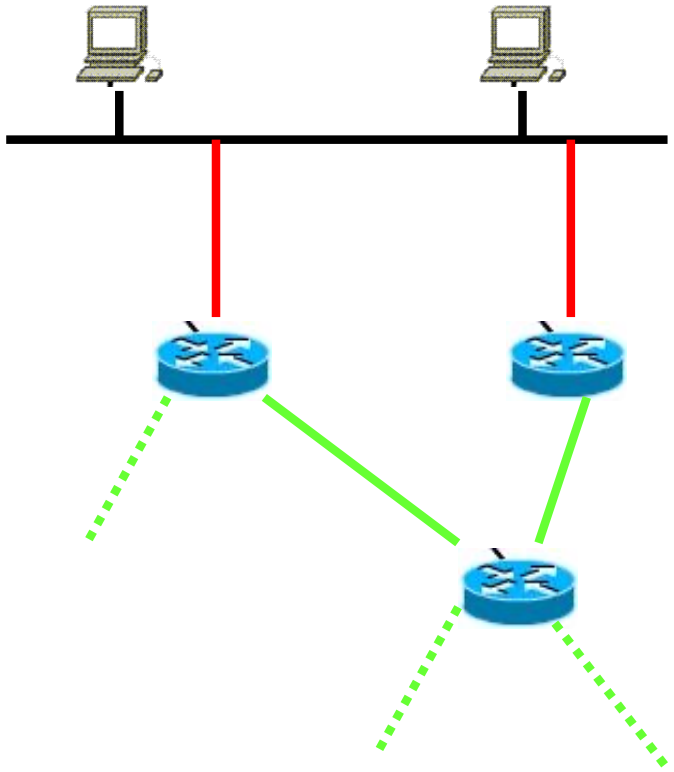
La distribución de pequeños archivos de datos a muchos usuarios

Multicast

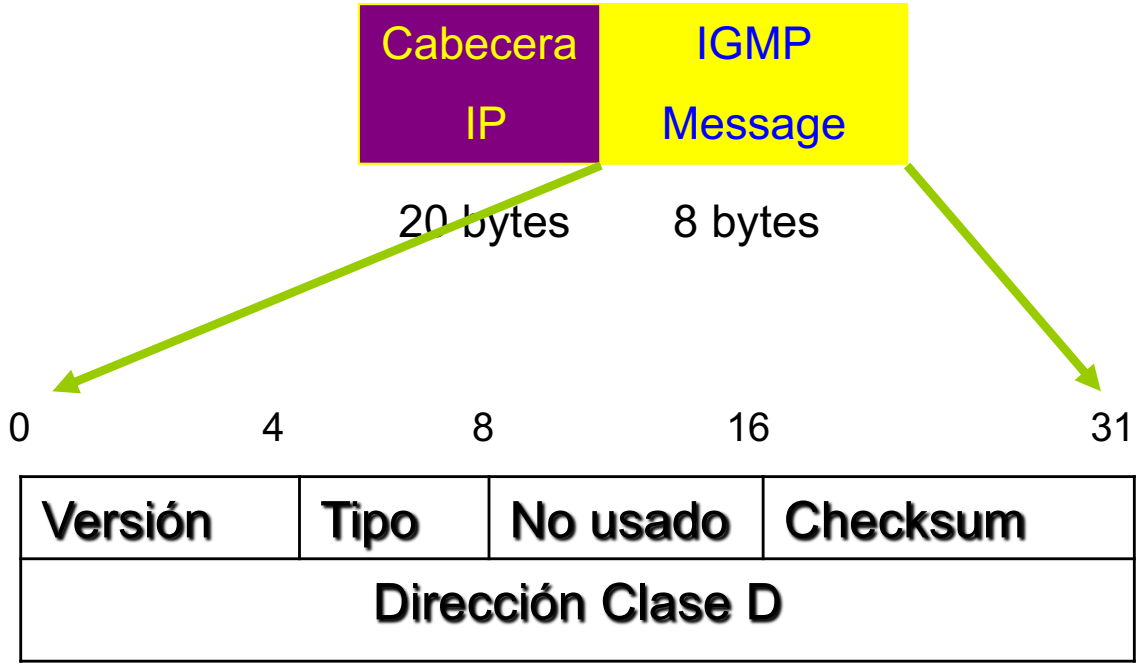
La comunicación de información local de membresía entre hosts y routers multicast se realiza a través de IGMP (Internet Group Management Protocol)

Host-to-Router-Protocol (IGMP)

Multicast Routing Protocols (PIM)



Multicast: Operación IGMP



Tipo

1) Petición de miembros de un grupo

2) Informe de miembros de grupo

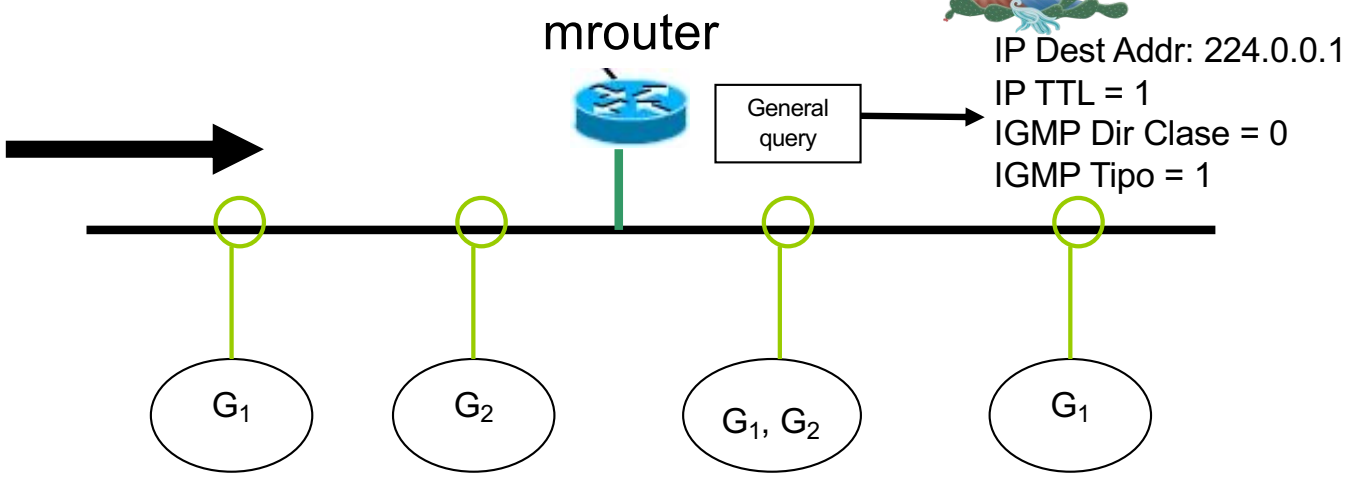
3) Mensaje de salida del grupo (solo en IGMP 2)

4) Mensaje DVMRP (Distance Vector Multicast Protocol)

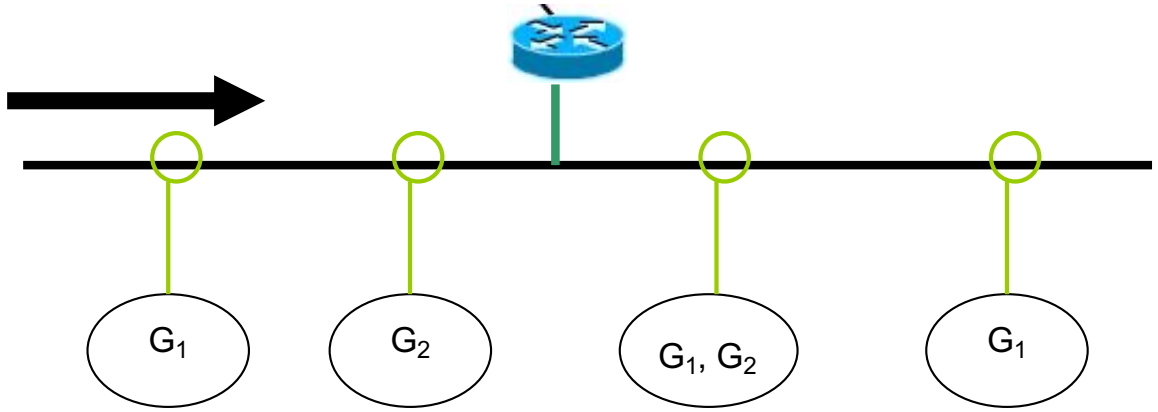
Multicast: Operación IGMP

1) Petición de miembros de un grupo

Periódicamente entre un router multicast (mrouter) local interroga a los hosts para determinar que grupos permanecen activos.



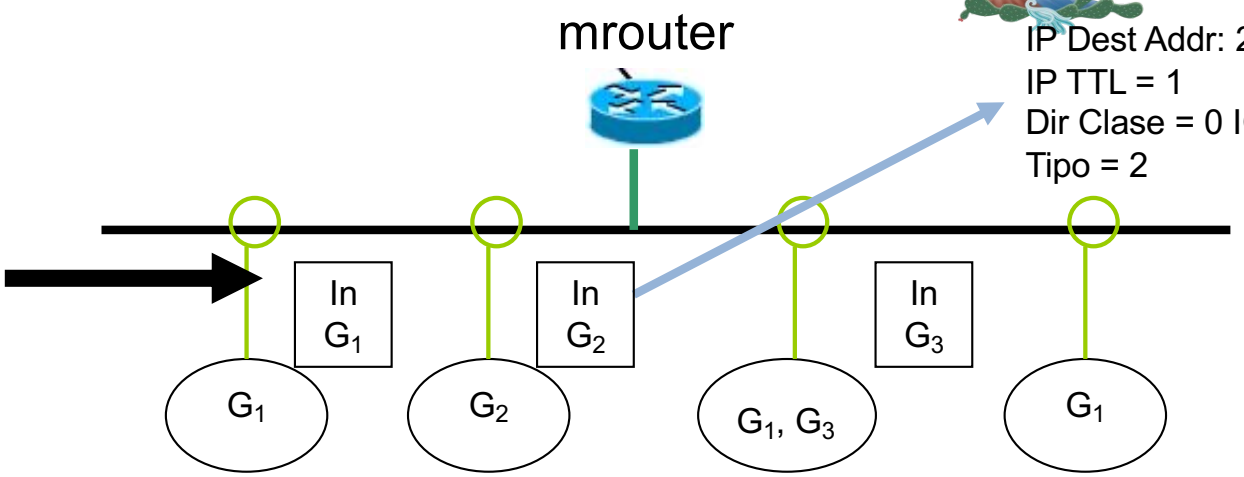
Al recibir la interrogación, cada host calcula aleatoriamente el Tiempo Máximo de Respuesta (entre 0 – 10 seg.)



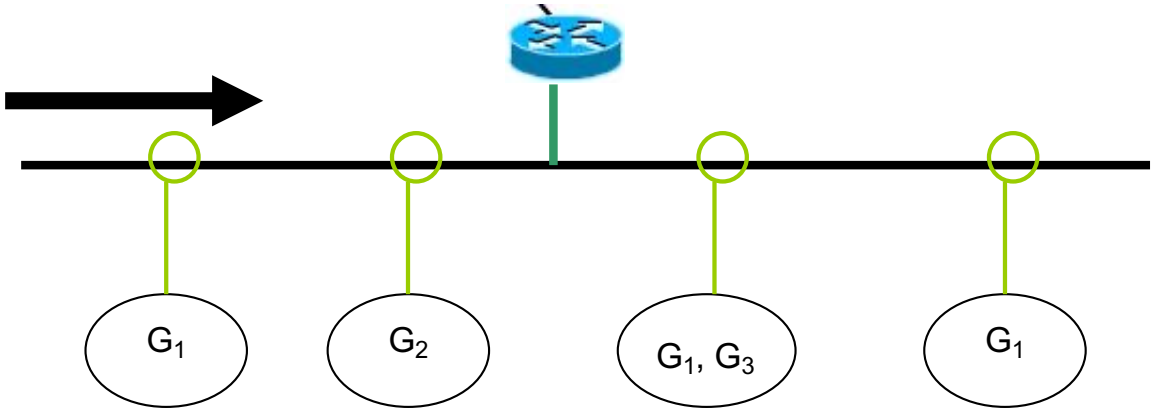
Multicast: Operación IGMP

3) Informe de miembros de grupo

Cuando el temporizador expira, el host envía al Router su dirección multicast al cual pertenece, o al cual quiere pertenecer



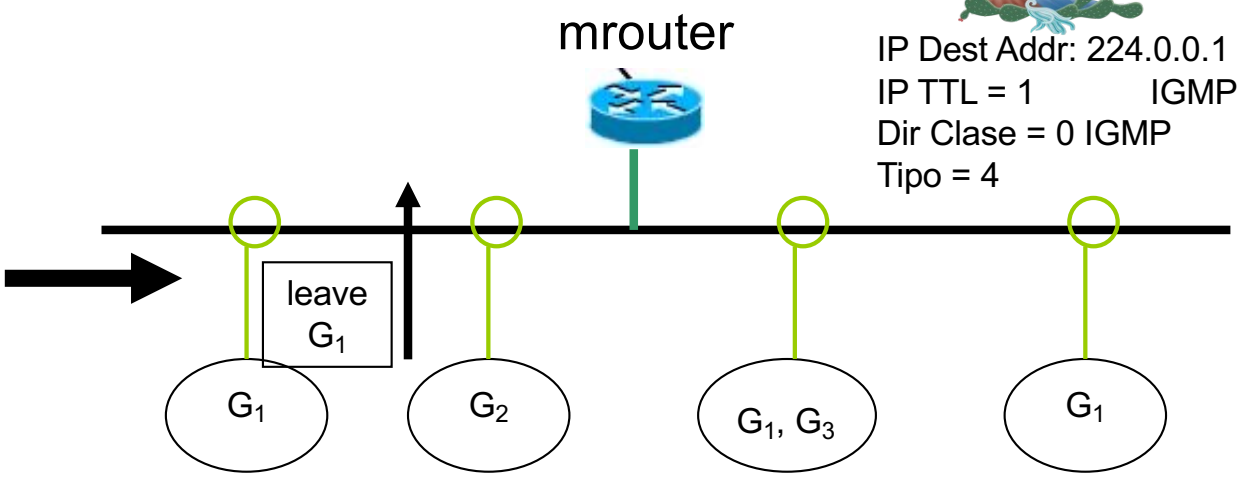
Si un host (en espera) observa que otro de su grupo ya ha enviado un informe al mrouter, no es necesario que este envíe el suyo



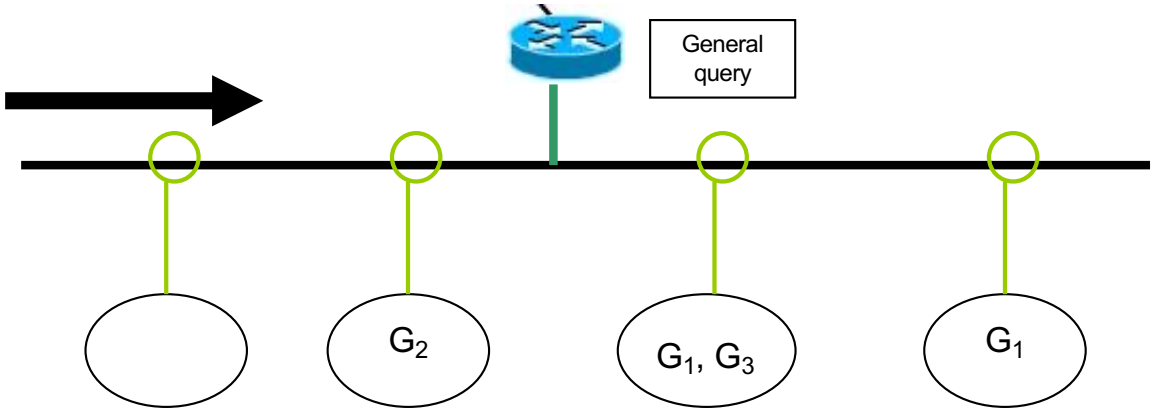
Multicast: Operación IGMP

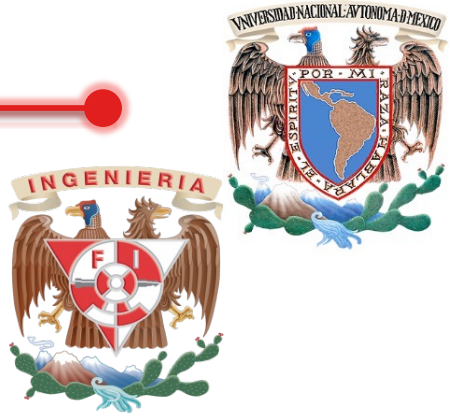
3) Mensaje de salida del grupo (solo en) IGMP 2

Cuando el host que notificó al mRouter acerca el grupo multicast al cual pertenecía, ya no tiene interés de estar en el grupo envía un mensaje de salida.



El mRouter interroga a los hosts para determinar si alguien es miembro grupo



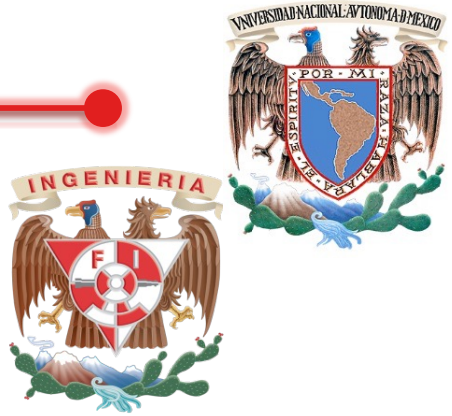


5.8 Routers

Los routers son dispositivos de red que operan en la tercera capa del modelo OSI, la capa de RED. Esto hace que sus operaciones sean diferentes que los repetidores y los puentes MAC. Ambos de estos dispositivos son usados para conectar redes que sean idénticas con respecto del acceso al medio usado.

Sin embargo, la información es transferida basándose en la direcciones MAC. Esto también hace que este dispositivos de protocolo independiente, especifique que ellos son independientes de los protocolos que trabajen en la capa MAC.

Los routers son capaces para proveer conectividad para mezclar ambientes MAC para trabajar con un protocolo en la capa superior. Esto permite la conexión de los segmentos de red que sean diferentes.



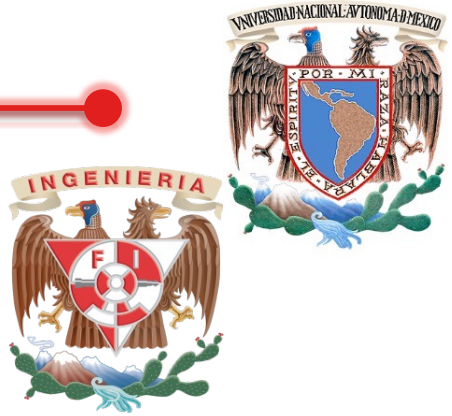
Routers

Sin embargo, se debe notar que las redes que se interconectan comparten algún protocolo similar en dicha pila, los routers no son capaces de traducir un protocolo. El router debe ser equipado con software apropiado para cada protocolo que sea soportado.

Una interred se basa en routers y esta compuesta de diferentes subredes lógicas.

Cada uno de los segmentos de red se conectan a través de un routers que mantiene su identidad lógica.

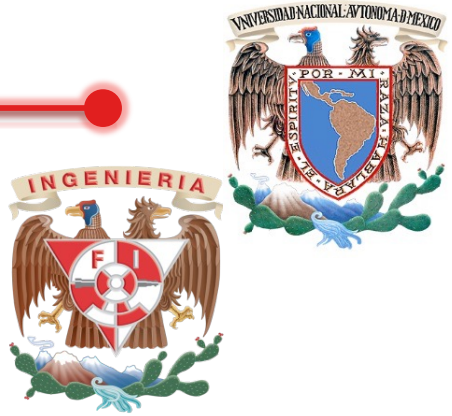
Los routers pueden ser usado para interconectar redes sobre redes locales o amplias. Sea crítico el diseño la instalación de internetworks y de grandes WANs usando enlaces de las telecomunicaciones.



Routers

El rol del router es dirigir paquetes a lo largo de manera eficiente, ruta económica en redes acopladas cuando estos son rutas muy redundantes desde el dispositivo origen al dispositivo destino.

Aunque algunos Sistemas Operativos en Red soportan routing por el servidor de archivo, mas routers son dispositivos “stand-Alone”. La función de routing tiende a ser “lento” el rendimiento del servidor. El rendimiento de procesamiento de un router en gran parte determina por sus componentes internos y arquitectura.



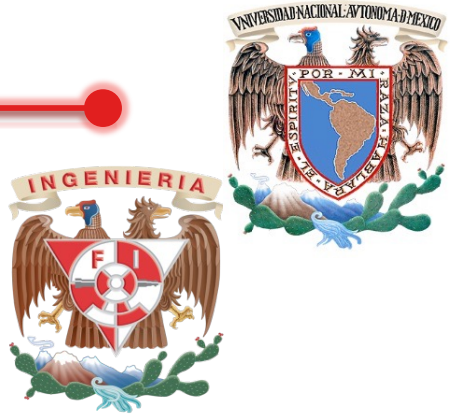
Routers

Funcionalidad

Los routers son considerados son dispositivos activos. Son activos en el sentido que son requeridos para que haga varias decisiones acerca de cada paquete manejado. Sin embargo, los routers necesita conocer mas protocolos que los brigdes.

Una meta del router es obtener un paquete del dispositivo origen hacia el destino. Sin embargo, pero hace primero la determinación que ruta es mejor o porque router debe atravesar la red.

Todos los routers rinde el mismo conjunto de funciones básicas, cueste lo que cueste de los protocolos trabajaron.



Routers

Funcionalidad

La funcionalidad del router puede estar categorizada dentro de tres áreas. Esto son los siguientes:

Permitir la unión de redes heterogéneas (diferentes).

Asegurar que las redes sean capaces de manejar el tráfico de carga.

Escoger la mejor ruta de comunicación a través de la red.

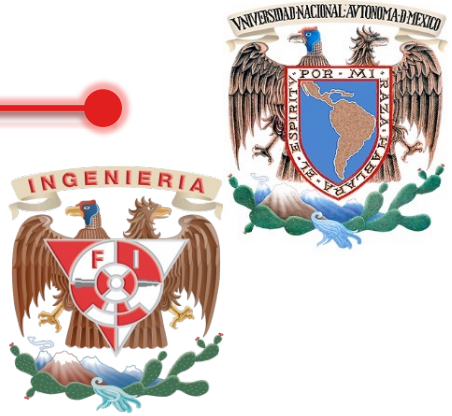
Routers

Uniendo redes

Los routers operan en la capa de red. Esto permite que las redes operen con diferentes protocolos en la capa de enlace de datos que sean interconectados. Por ejemplo, la capa de enlace de datos usados pueden ser: X.25, FDDI, Ethernet, LocalTalk, Token Ring o Frame Relay, mencionando algunos.

En el orden que sean capaces para manejar todos los protocolos diferentes en la capa de enlace de datos, los routers deben ser capaces de trabajar con esquemas diferentes de direcciones, diferentes tamaños de frames y diferentes tasas de datos.

El direccionamiento de la capa de enlace de datos es administrada con un mapeo en la capa de red y usando esquemas de resoluciones de dirección de nombres.



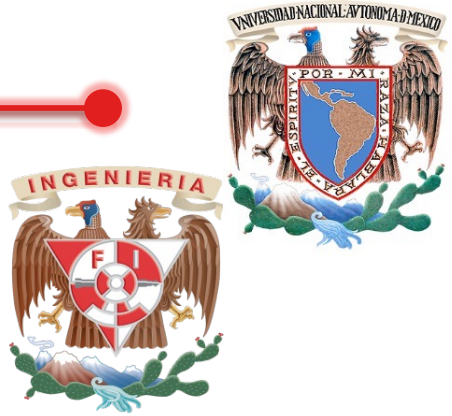
Routers

Uniendo redes

Los frames “largos” son administrados para que los routers rompan frames “largos” dentro de paquetes pequeños. Cada uno de los paquetes obtienen un número de secuencia así deben reensamblar al receptor final.

Carga de tráfico

Las redes basadas en routers consiste en enlazar operacionalmente a diferentes velocidades de transmisión. Esto puede conducir a problemas de congestionamiento de tráfico. Los problemas de congestionamiento pueden ser mas comúnmente cuando las redes operan a diferentes tasas de datos y con estás interconexiones y el exceso de tráfico en uno de estos enlaces.



Routers

Carga de tráfico

Un meta para manejar los problemas de congestión es permitir a los routers borrar paquetes y cuando tienen los sistemas que regenerar estos en un tiempo después. Esto agrega tráfico a la red y puede causar grandes retardos en la transmisión.

Un método más aceptado para manejar las congestiones es usar una técnica llamada “Source Quench”. En esta técnica, el router monitorea la utilización del ancho de banda de las redes adjuntas.

Cuando el promedio de los datos que se están transmitiendo un umbral de alcance preestablecido, el router enviará un paquete de congestión para que los dispositivos que envían reduzcan o paren la salida. Cuando la congestión ha sido liberada, el dispositivo origen “amortiguado” restablece su transmisión de manera normal.

Routers

Selección de la ruta

Los routers proveen ambas funciones: control de tráfico y filtrado. El control de tráfico es importante cuando esto son mas que una ruta entre los dos puntos finales de la red.

Seleccionando una ruta de telecomunicaciones a través de la red es un proceso en dos pasos. El primer paso es crear y mantener una tabla de ruteo y en el segundo caso, seleccionar la mejor ruta para que el siguiente paso sea el viaje del paquete. Este segundo paso esta basado en la información encontrada en los paquetes y en la tabla de ruteo.

Las tablas de ruteo y la selección de rutas a través de la red forman la base de la función de los routers.

“Por mi raza hablará el espíritu”