Capa de Red

Redes de Computadores

FIEC04705

Sesión 17

Agenda

- Terminología
- Implementación de subredes
- Funcionamiento de los routers
- Ruteo Jerárquico
- Ruteo en TCP/IP
- IPSec
- VPN
- Mapeo de direcciones físicas a lógicas
- Internet Control Message Protocol
- NAT

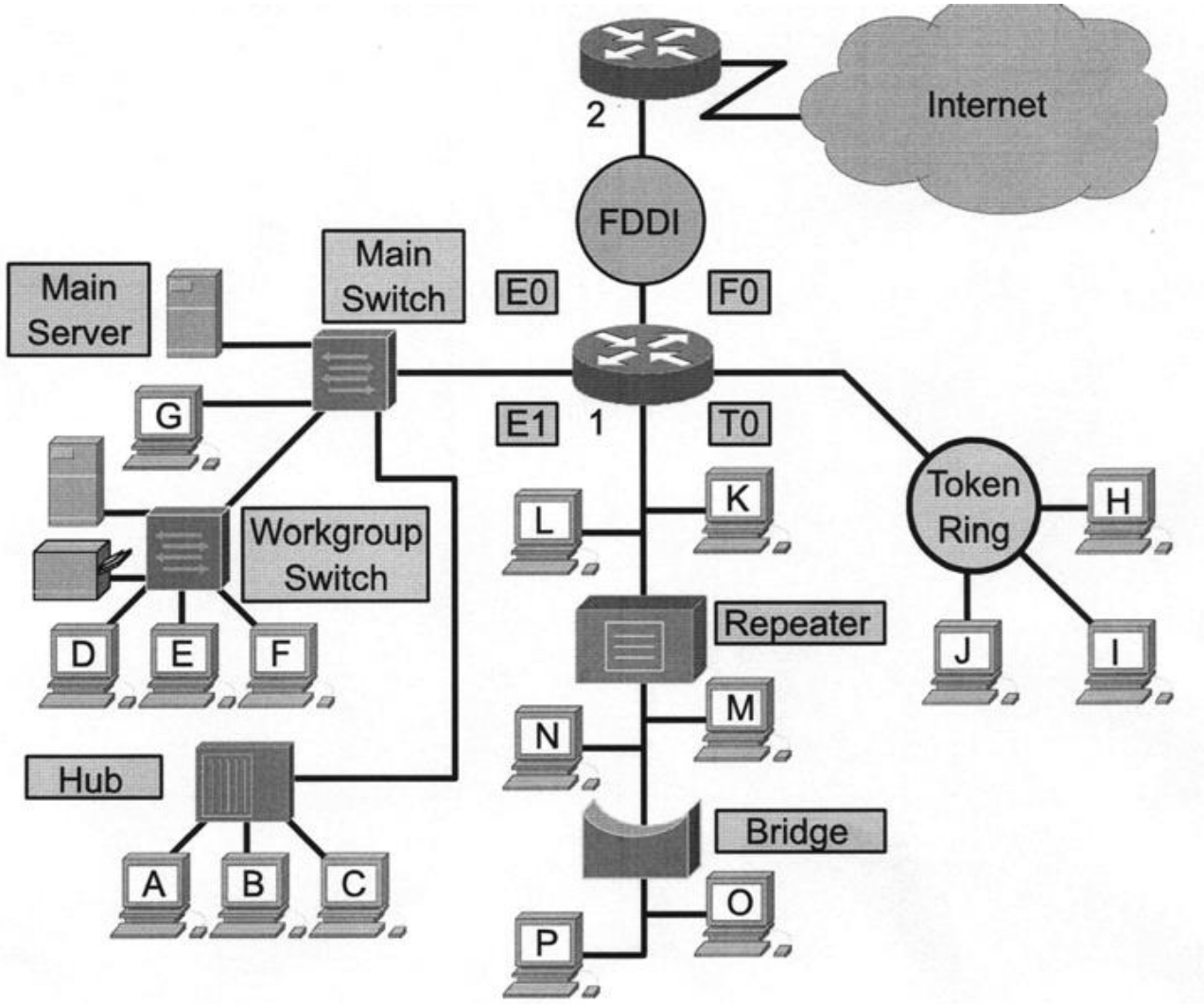
Terminología

Terminología

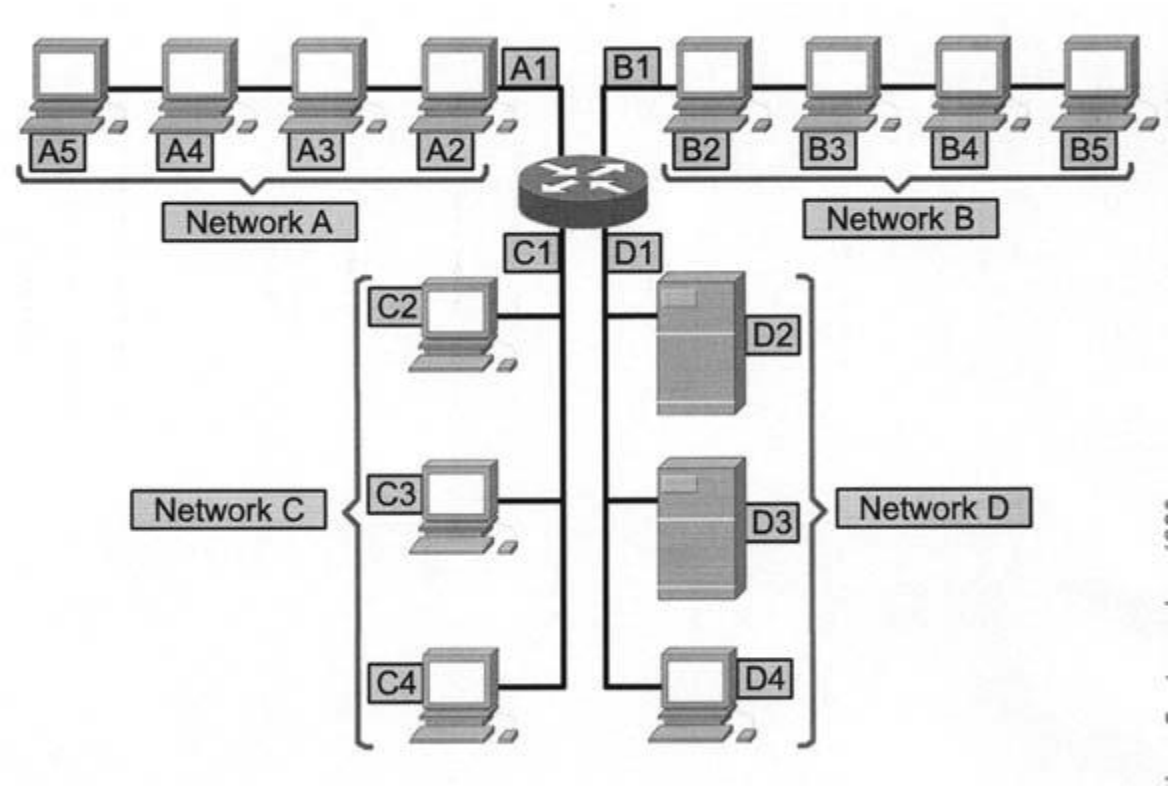
- **Gateway**: dispositivo utilizado para conectar dos redes separadas que utilizan **diferentes protocolos** de comunicación.
- **Internetwork** (internet): una red de redes.

Implementación de redes y subredes

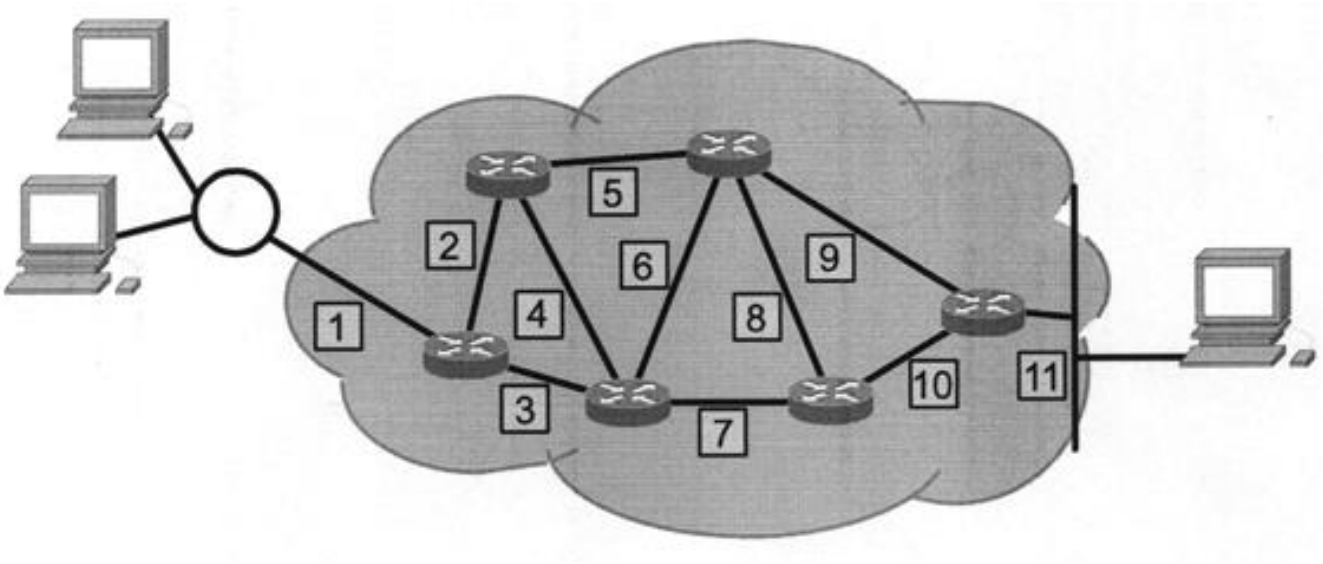
Red


Internet
2
FDDI
Main Server
Main Switch
E0
F0
E1
1
T0
G
Workgroup Switch
D
E
F
L
K
Token Ring
H
J
I
Repeater
M
N
Hub
A
B
C
Bridge
O
P

Subredes


A1
B1
A5
A4
A3
A2
B2
B3
B4
B5
Network A
Network B
C1
D1
C2
D2
Network C
C3
D3
Network D
C4
D4

Subredes



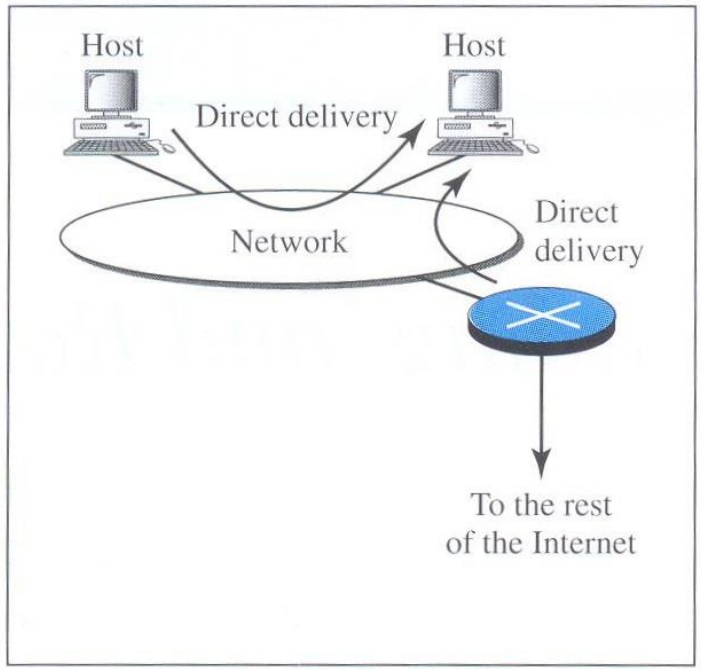
Funcionamiento de los routers

Direct vs. Indirect delivery

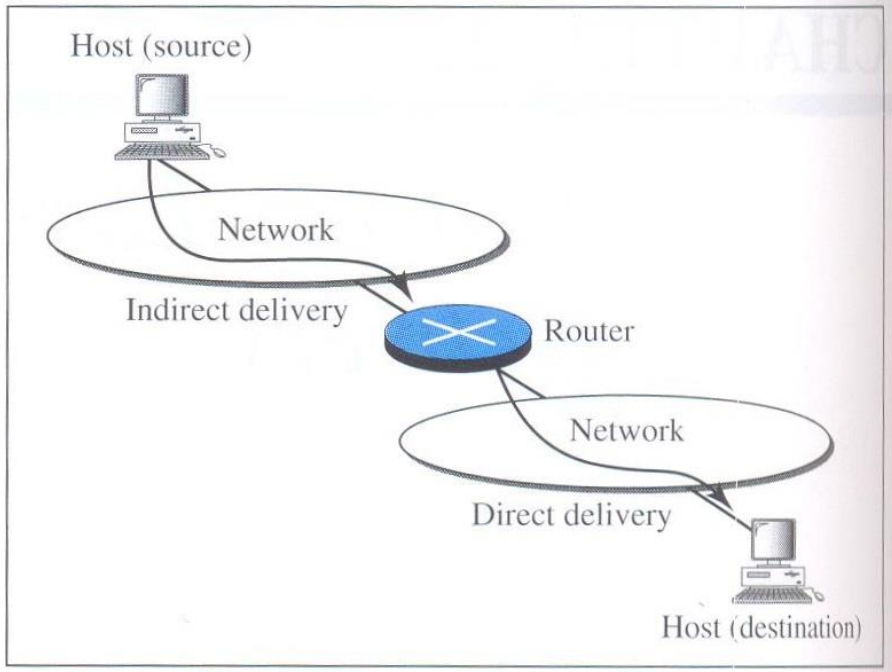
- **Entrega directa**: el destino final del paquete es una estación conectada a la misma red física del remitente. El remitente determina que es una entrega directa extrayendo la dirección de red de destino (por medio de la máscara) y compara esta dirección con la dirección de la red a la cual está conectado. Si coinciden, la entrega es directa.
- **Entrega indirecta**: Si la estación de destino, no está en la misma red que el remitente, el paquete es entregado indirectamente, es decir, el paquete va de un router a otro hasta que alcanza uno conectado directamente a la misma red física del destinatario.

Entrega directa vs. indirecta

Figure 22.1 *Direct and indirect delivery*



a. Direct delivery



b. Indirect and direct delivery

Técnicas de reenvío

Técnicas de reenvío

- Reenviar significa poner al paquete en su ruta hacia su destinatario.
- Requiere que el host o el router dispongan de una tabla de ruteo.
- Entre las técnicas de reenvío tenemos:
  - Next-Hop vs. Route Method
  - Network-Specific Method vs. Host-Specific Method
  - Default Method

Route method vs. next-hop method

Figure 22.2 *Route method versus next-hop method*

a. Routing tables based on route

Routing table for host A

Destination	Route
Host B	R1, R2, host B

Routing table for R1

Destination	Route
Host B	R2, host B

Routing table for R2

Destination	Route
Host B	Host B

b. Routing tables based on next hop

Routing table for host A

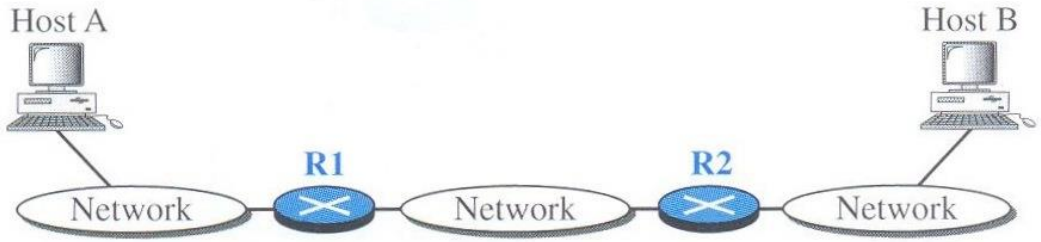
Destination	Next hop
Host B	R1

Routing table for R1

Destination	Next hop
Host B	R2

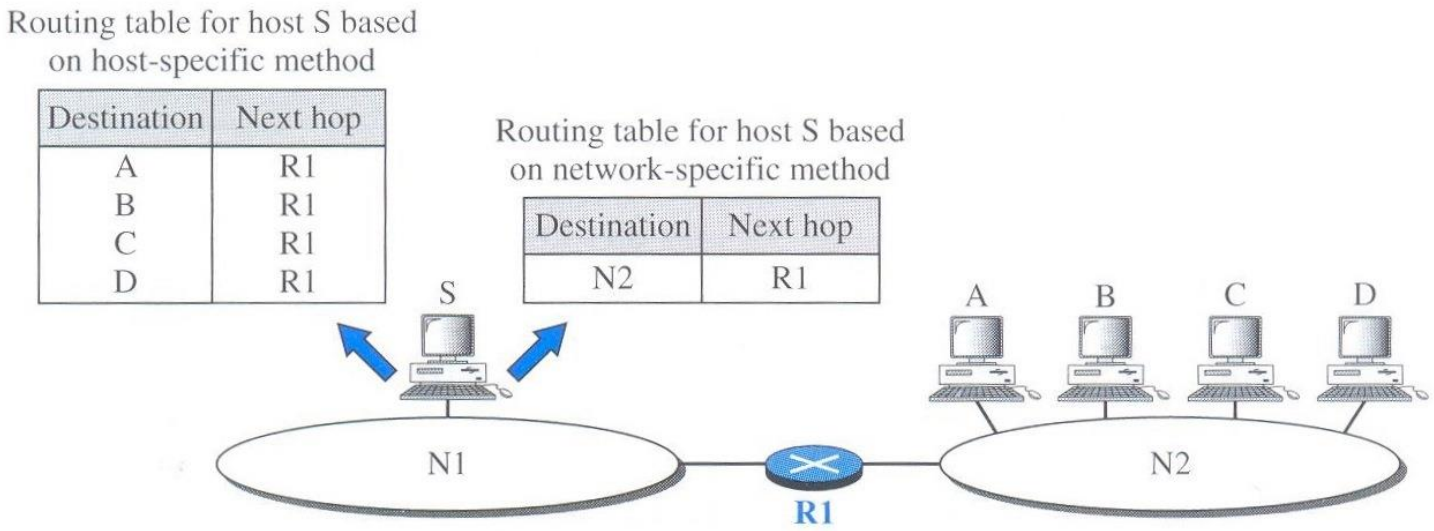
Routing table for R2

Destination	Next hop
Host B	---



Host-specific vs. network-specific method

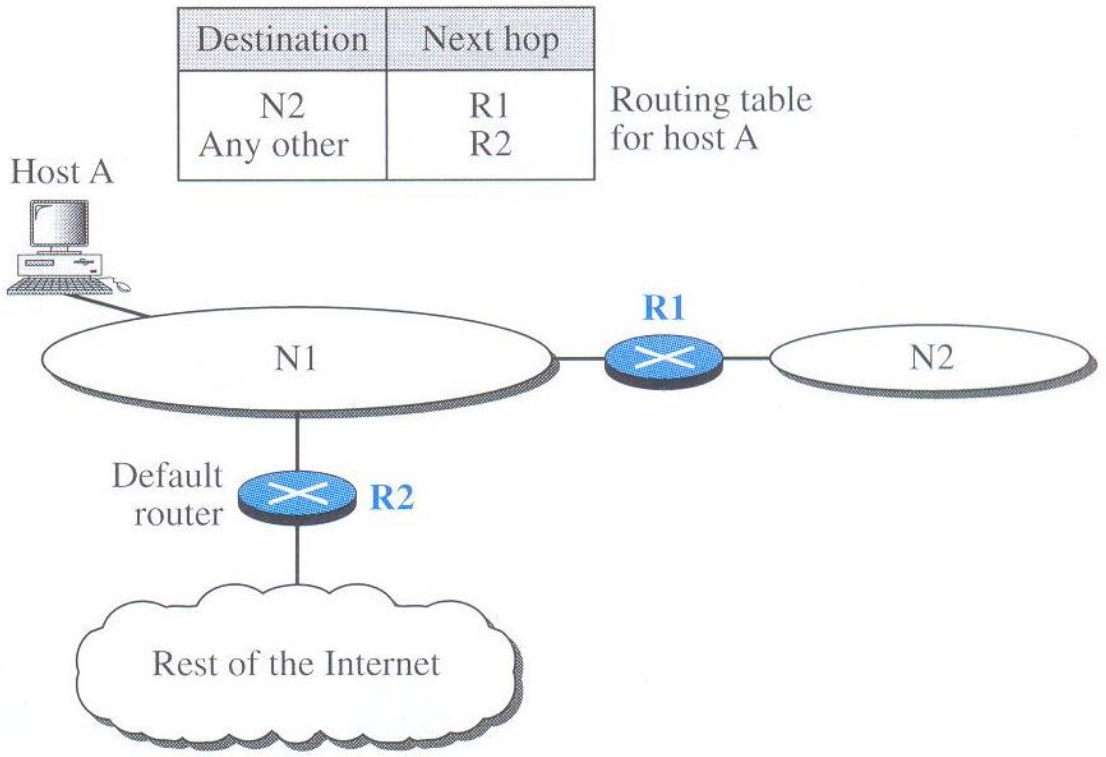
Figure 22.3 *Host-specific versus network-specific method*



Host-specific routing is used for purposes such as checking the route or providing security measures.

Default method

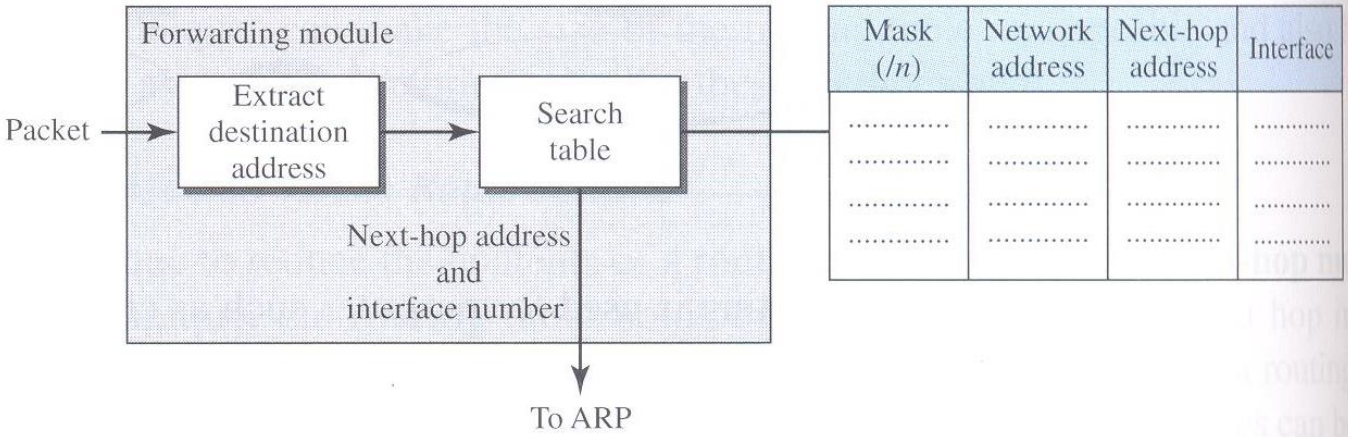
Figure 22.4 *Default method*



Proceso de reenvío

Proceso de reenvío

Figure 22.5 *Simplified forwarding module in classless address*



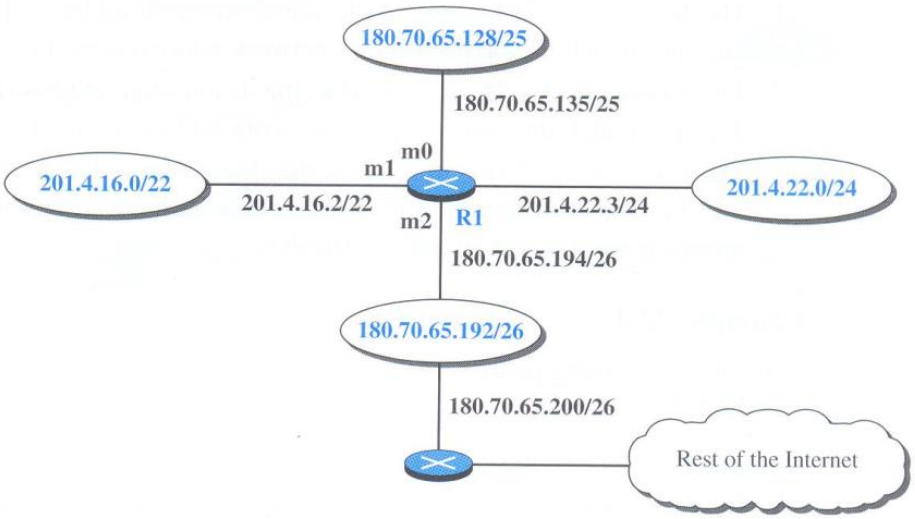
Note that we need at least four columns in our routing table; usually there are more.

In classless addressing, we need at least four columns in a routing table.

Example 22.1

Make a routing table for router R1, using the configuration in Figure 22.6.

Figure 22.6 *Configuration for Example 22.1*



Solution

Table 22.1 shows the corresponding table.

Table 22.1 *Routing table for router R1 in Figure 22.6*

Mask	*Network Address*	*Next Hop*	*Interface*
/26	180.70.65.192	—	m2
/25	180.70.65.128	—	m0
/24	201.4.22.0	—	m3
/22	201.4.16.0	....	m1
Any	Any	180.70.65.200	m2

Proceso de reenvío

Example 22.2

Show the forwarding process if a packet arrives at R1 in Figure 22.6 with the destination address 180.70.65.140.

Solution

The router performs the following steps:

1. The first mask (/26) is applied to the destination address. The result is 180.70.65.128, which does not match the corresponding network address.
2. The second mask (/25) is applied to the destination address. The result is 180.70.65.128, which matches the corresponding network address. The **next-hop address** (the destination address of the packet in this case) and the interface number m0 are passed to ARP for further processing.

Proceso de reenvío

Example 22.3

Show the forwarding process if a packet arrives at R1 in Figure 22.6 with the destination address 201.4.22.35.

Solution

The router performs the following steps:

1. The first mask (/26) is applied to the destination address. The result is 201.4.22.0, which does not match the corresponding network address (row 1).
2. The second mask (/25) is applied to the destination address. The result is 201.4.22.0, which does not match the corresponding network address (row 2).
3. The third mask (/24) is applied to the destination address. The result is 201.4.22.0, which matches the corresponding network address. The destination address of the packet and the interface number m3 are passed to ARP.

Proceso de reenvío

Example 22.4

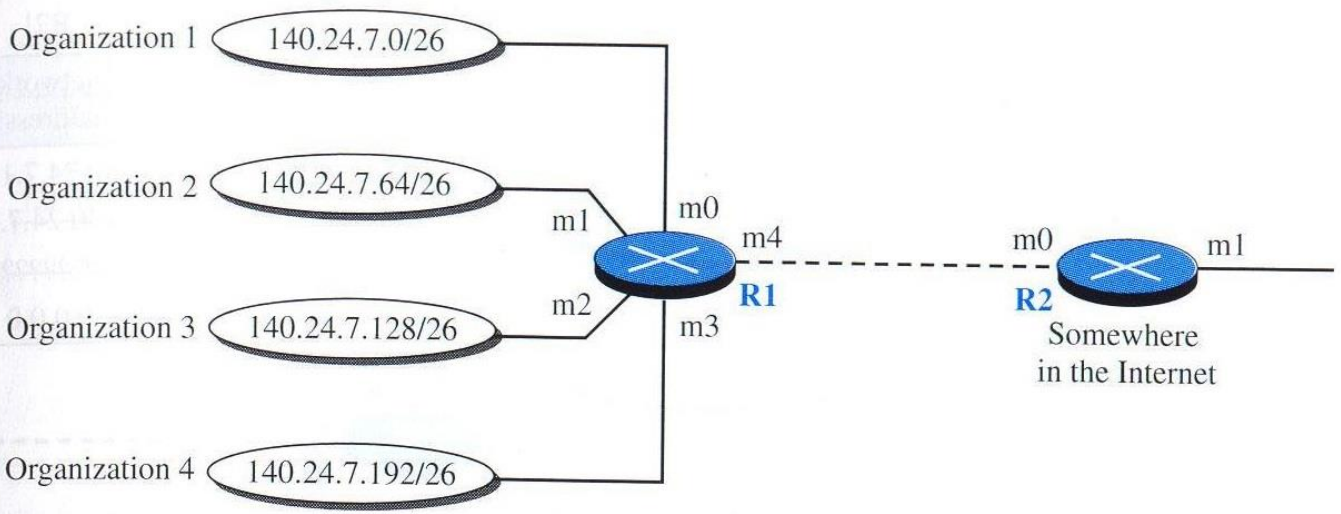
Show the forwarding process if a packet arrives at R1 in Figure 22.6 with the destination address 18.24.32.78.

Solution

This time all masks are applied, one by one, to the destination address, but no matching network address is found. When it reaches the end of the table, the module gives the next-hop address 180.70.65.200 and interface number m2 to ARP. This is probably an outgoing package that needs to be sent, via the default router, to someplace else in the Internet.

Address aggregation

Figure 22.7 *Address aggregation*



Mask	Network address	Next-hop address	Interface
/26	140.24.7.0	----------	m0
/26	140.24.7.64	----------	m1
/26	140.24.7.128	----------	m2
/26	140.24.7.192	----------	m3
/0	0.0.0.0	Default	m4

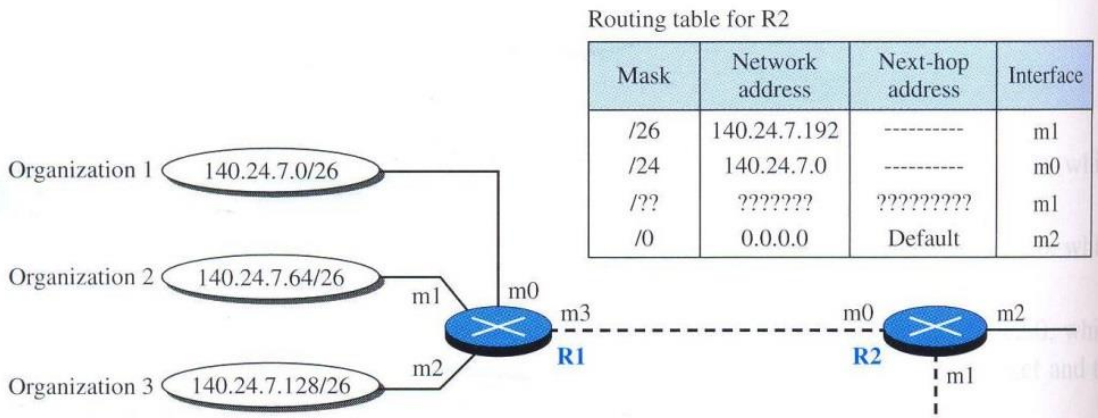
Routing table for R1

Mask	Network address	Next-hop address	Interface
/24	140.24.7.0	----------	m0
/0	0.0.0.0	Default	m1

Routing table for R2

Longest mask matching

Figure 22.8 *Longest mask matching*



Routing table for R2

Mask	Network address	Next-hop address	Interface
/26	140.24.7.192	----------	m1
/24	140.24.7.0	----------	m0
/??	???????	?????????	m1
/0	0.0.0.0	Default	m2

Mask	Network address	Next-hop address	Interface
/26	140.24.7.0	----------	m0
/26	140.24.7.64	----------	m1
/26	140.24.7.128	----------	m2
/0	0.0.0.0	Default	m3

Routing table for R1

Mask	Network address	Next-hop address	Interface
/26	140.24.7.192	----------	m0
/??	???????	?????????	m1
/0	0.0.0.0	Default	m2

Routing table for R3

Ruteo Jerárquico

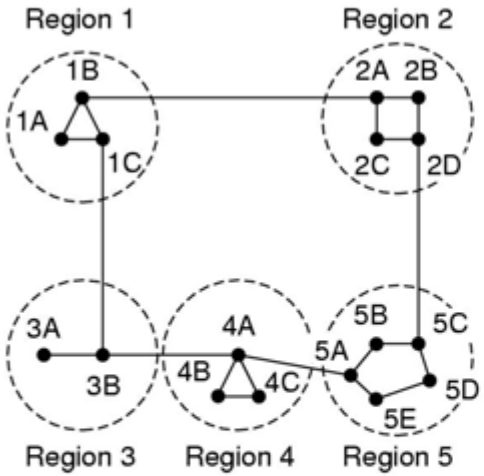
Ruteo jerárquico

- Cuando las redes crecen, el tráfico de ruteo de paquetes y las tablas de ruteo crecen proporcionalmente. Una solución es tener algunos routers para que hagan ruteo a otros: **Ruteo jerárquico.**
- Los routers están divididos en grupos denominados **dominios, regiones o autonomous systems (ASs)**. Cada región podría ser considerada como una red separada e independiente.

Ruteo jerárquico

- Cada router tiene información acerca de la forma de rutear paquetes en su propia región.
- Cada región tiene designados uno o más routers que determinan rutas entre regiones.
- Regiones grandes son divididas en subregiones, etc.

Ruteo jerárquico



(a)

Full table for 1A

Dest.	Line	Hops
1A	–	–
1B	1B	1
1C	1C	1
2A	1B	2
2B	1B	3
2C	1B	3
2D	1B	4
3A	1C	3
3B	1C	2
4A	1C	3
4B	1C	4
4C	1C	4
5A	1C	4
5B	1C	5
5C	1B	5
5D	1C	6
5E	1C	5

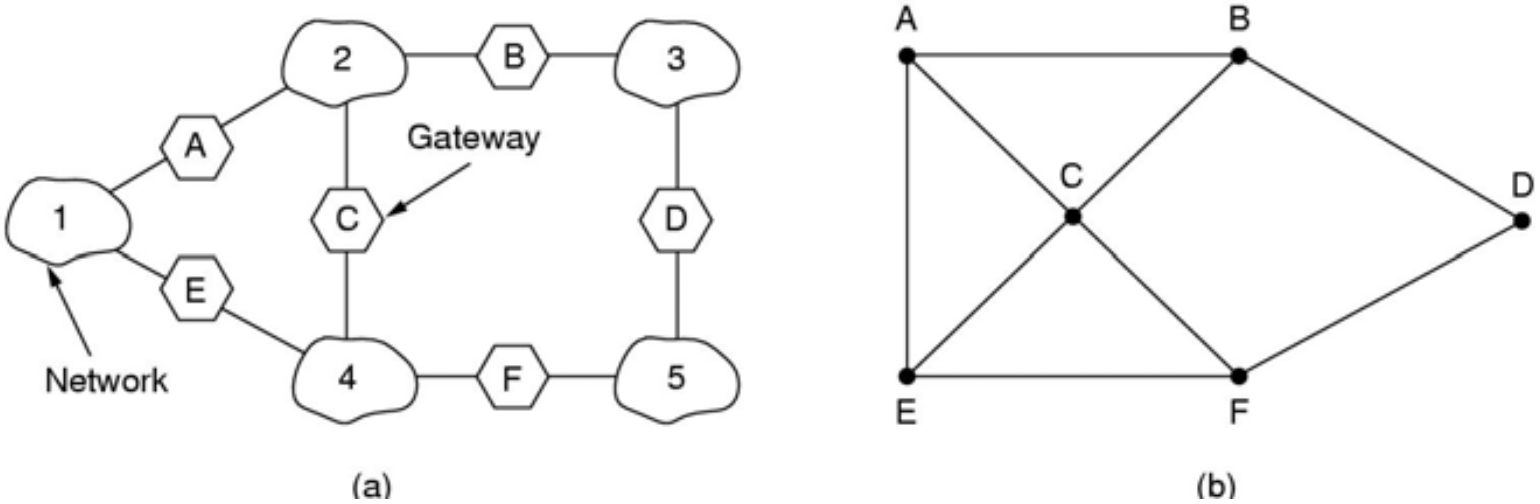
(b)

Hierarchical table for 1A

Dest.	Line	Hops
1A	–	–
1B	1B	1
1C	1C	1
2	1B	2
3	1C	2
4	1C	3
5	1C	4

(c)

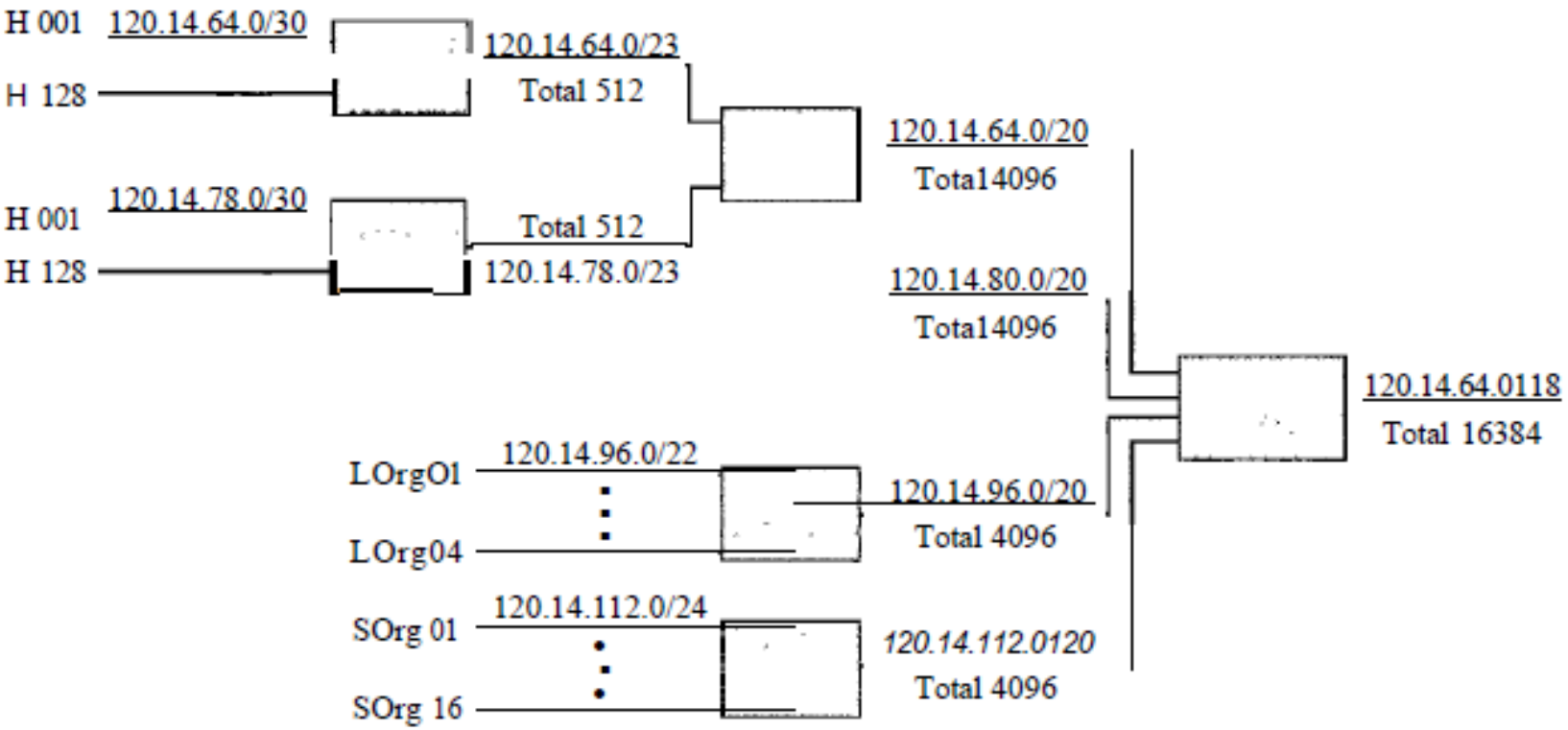
Ruteo jerárquico



Ruteo jerárquico

- Internet tiene jerarquías
- Internet está dividido en ISPs (Internet Service Providers) nacionales e internacionales
- ISPs nacionales son divididos en ISPs regionales, y estos se dividen en ISPs locales.
- Por lo tanto la tabla de ruteo puede decrecer en tamaño.

Ruteo jerárquico

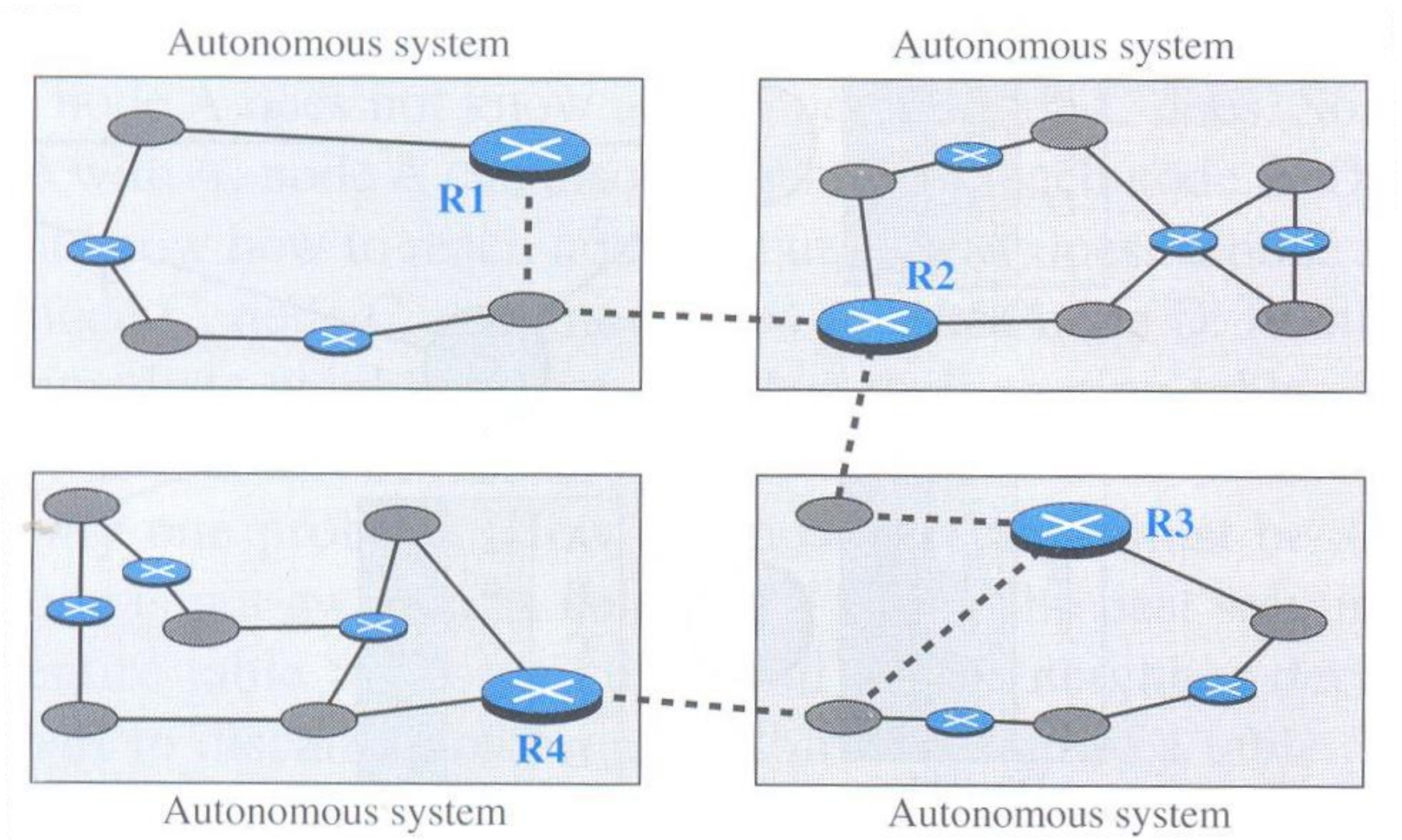


Ruteo en TCP/IP

Ruteo dentro y entre dominios

- Un Autonomous System (AS) es un grupo de redes y routers bajo la autoridad de una única administración.
- Nos referimos al ruteo dentro de un sistema autónomo como **intradomain routing**.
- Nos referimos al ruteo entre sistemas autónomos como **interdomain routing**.

Intra and interdomain routing



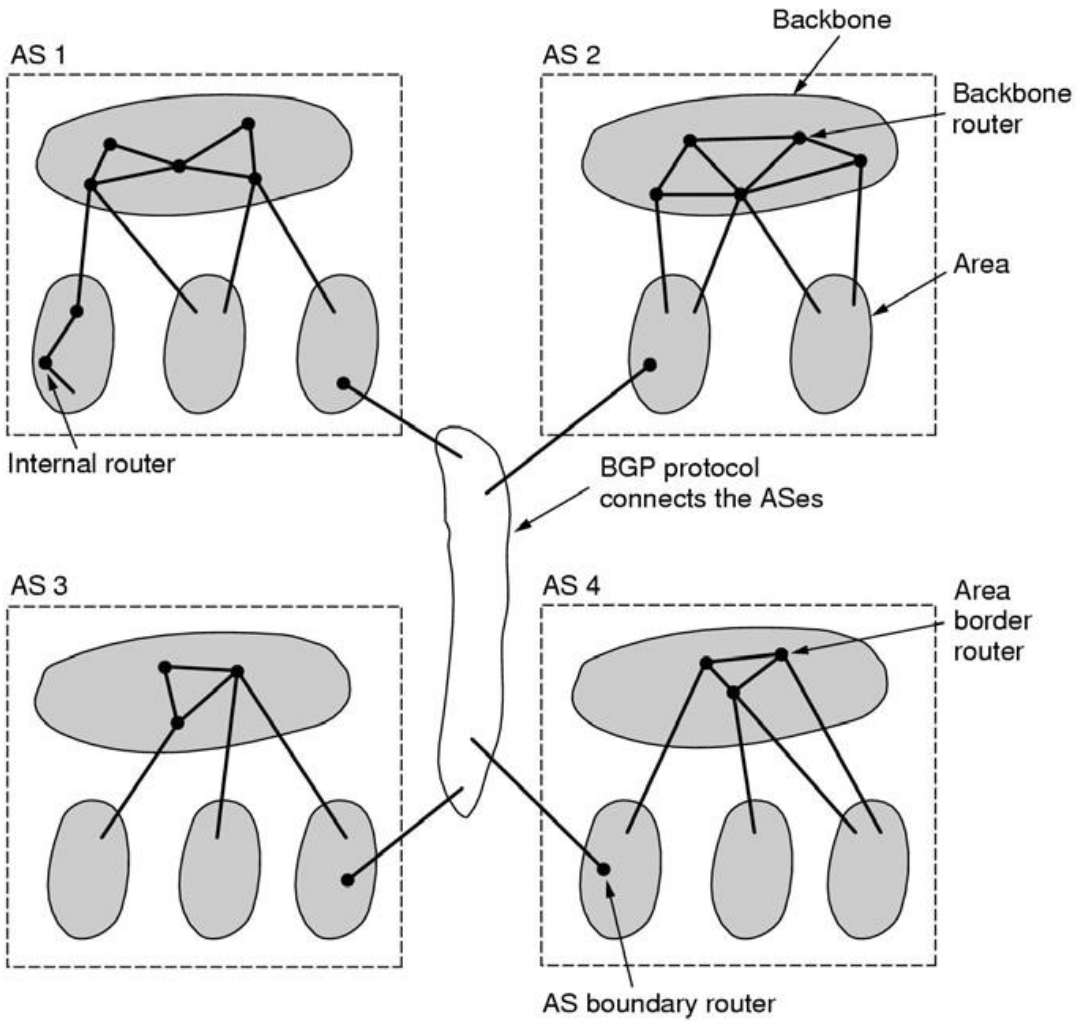
Ruteo en TCP/IP

- Generalmente una interconexión de redes consiste en:
  - Tres tipos de conexiones y redes:
    1. Punto a punto
    2. Redes multiacceso con broadcasting (LANs)
    3. Redes multiacceso sin broadcasting (WANs)
  - Cuatro clases de routers:
    1. Internal
    2. Area Border
    3. Backbone
    4. AS boundary

Ruteo en TCP/IP

- Protocolos de gateway interior (dentro de ASs)
  - IGRP Interior Gateway Routing Protocol, Cisco, Distance Vector
  - RIP, Routing Information Protocol, UNIX BSD systems - el más común de los IGP en el Internet, distance vector.
  - EIGRP, Enhanced Interior Gateway Routing Protocol, Cisco, híbrido.
  - OSPF, Open Shortest Path First, link state
- The exterior protocol (entre ASs)
  - Border Gateway Protocol, fundamentalmente Bellman-Ford

Ruteo en el Internet



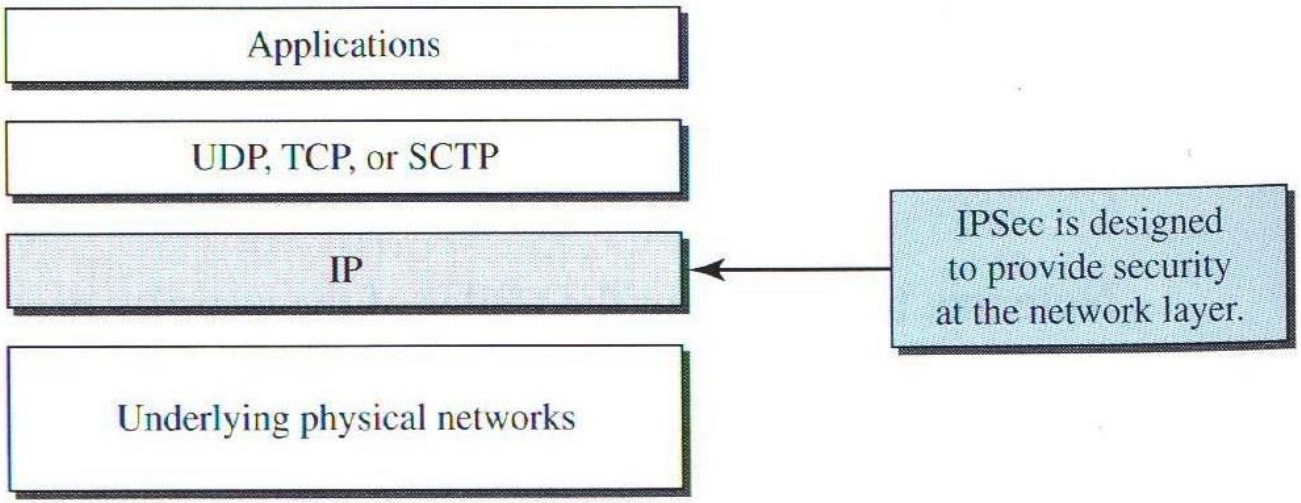
IPSecurity (IPSec)

IPSec

- Es una colección de protocolos diseñados por la Internet Engineering Task Force (IETF) para proveer seguridad a un paquete a nivel de red.
- IPSec ayuda a crear paquetes autenticados y confidenciales en la capa de red.
- IPSec opera en dos diferentes modos:
  - **Transport mode**
  - **Tunnel mode**

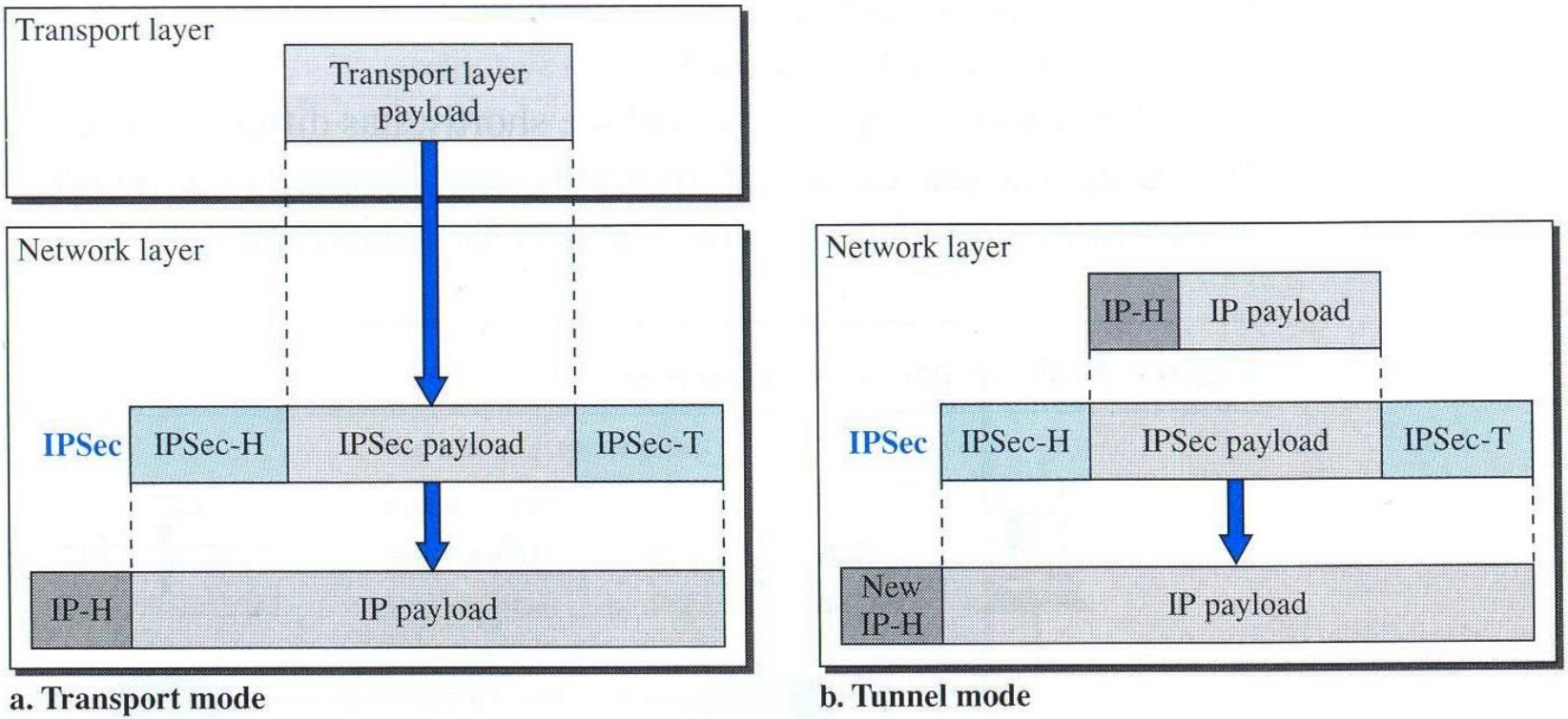
IPSec

Figure 32.2 *TCP/IP protocol suite and IPSec*



IPSec: Modos de operación

Figure 32.3 *Transport mode and tunnel modes of IPSec protocol*

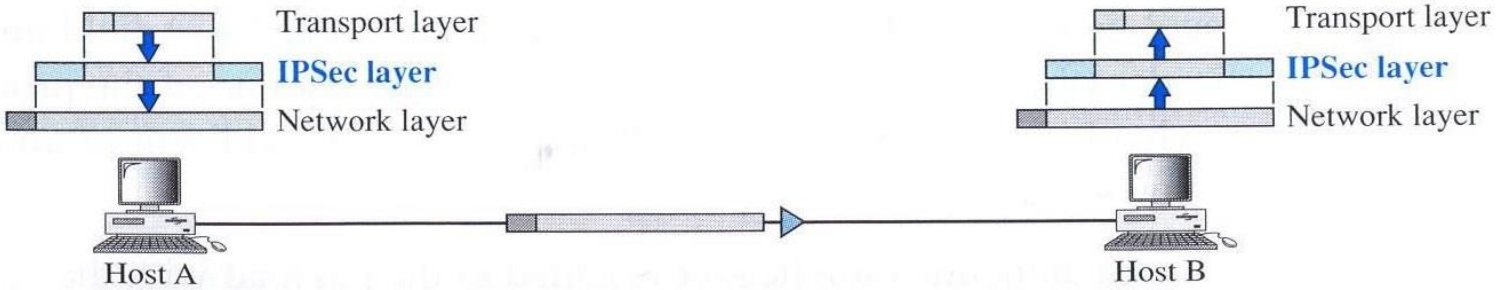


Transport mode

- Protege lo que se entrega desde la capa de transporte a la capa de red. No protege la cabecera IP, solamente el payload de la capa de red (lo que viene de la capa de transporte).
- Usualmente se utiliza cuando se necesita proteger datos en una comunicación entre hosts (host-host).
- El remitente usa IPSec para autenticar y/o encriptar el payload entregado desde la capa de transporte.
- El destinatario usa IPSec para chequear la autenticación y/o desencriptar el paquete IP y entregarlo a la capa de transporte

Transport mode

Figure 32.4 *Transport mode in action*

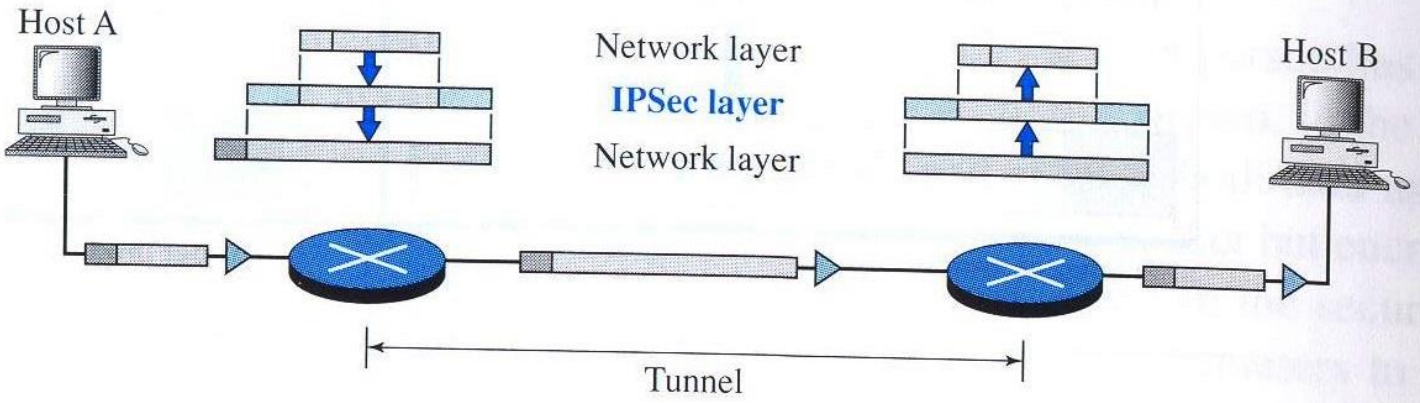


Tunnel mode

- En este modo, IPSec protege todo el paquete IP, incluyendo la cabecera. Aplica IPSec a todo el paquete y luego agrega una nueva cabecera IP. Esta nueva cabecera IP tiene información diferente que la original.
- Este modo se emplea para la comunicación entre routers, o cuando ya sea el remitente o el destinatario no es un host.

IPSec

Figure 32.5 *Tunnel mode in action*



Virtual Private Network (VPN)

VPN

- VPN es una tecnología que usa el Internet para la comunicación dentro y entre organizaciones (intra and interorganizations), pero que requiere privacidad para sus comunicaciones internas.
- VPN usa IPSec para proveer seguridad a los datagramas IP.

Redes privadas

- Una red privada está diseñada para ser usada dentro de una organización. Brinda acceso a recursos compartidos y al mismo tiempo provee privacidad. Definamos dos conceptos: intranet y extranet.
- **Intranet**: es una red privada (LAN) que usa el modelo Internet. Sin embargo, el acceso a a la red está limitado para los usuarios dentro de la organización.

Redes privadas

- **Extranet**: los mismo que la Intranet con una diferencia: Algunos recursos pueden accedidos por grupos específicos de usuarios fuera de la organización bajo el control del administrador de la red. Por ejemplo: estudiantes de una universidad que remotamente accedan a ciertos computadores luego de verificar sus credenciales.

Privacidad en las redes

- **Direccionamiento**: Una red privada que usa Internet debe utilizar direcciones IP. Tiene tres alternativas:
  1. La red puede aplicar a un conjunto de direcciones de las Internet authorities y usarlas sin estar conectados a Internet.
  2. La red puede usar cualquier conjunto de direcciones sin registarlas con las Internet authorities.
  3. Utilizar los conjuntos de direcciones reservados por las Internet authorities.
     1. 10.0.0.0. a 10.255.255.255
     2. 172.16.0.0 a 172.31.255.255
     3. 192.168.0.0 a 192.168.255.255

Privacidad en las redes

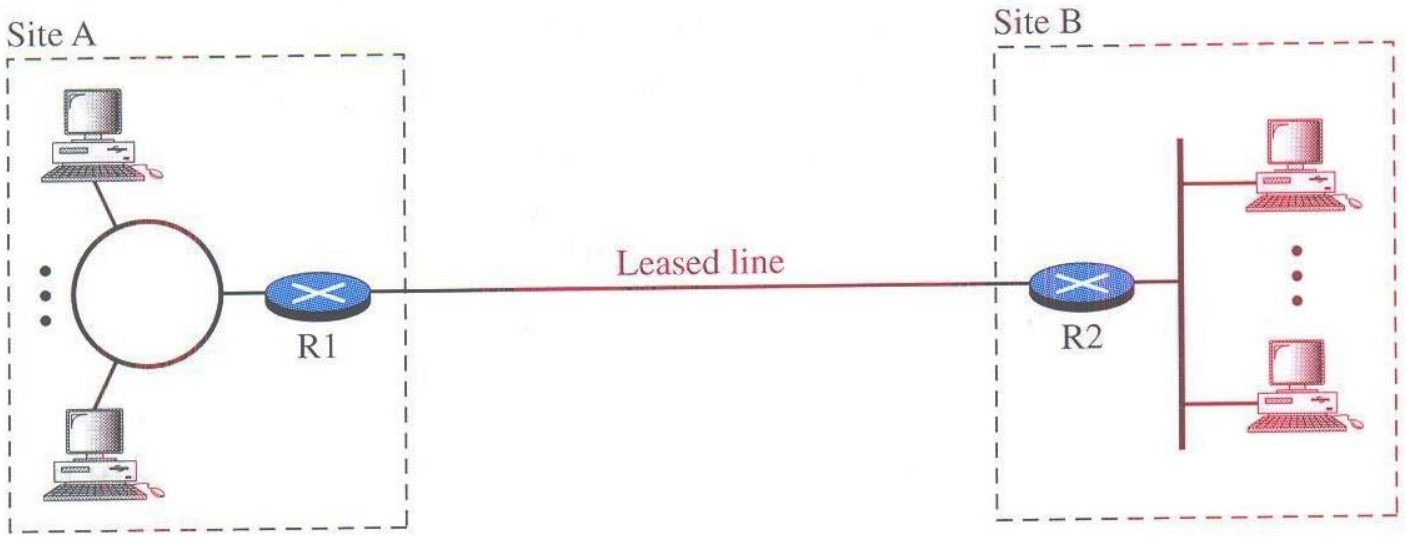
- Con la finalidad de tener privacidad las organizaciones tienen tres estrategias:
  1. Redes privadas
  2. Redes híbridas
  3. Redes privadas virtuales

Redes privadas

- Una organización que necesita privacidad al rutear información dentro de la organización puede utilizar una red privada.
- Una organización grande con varios sitios puede crear una internet privada.
- Las LANs en cada sitio se conecta a los otros por medio de routers y líneas rentadas.

Redes privadas

Figure 32.10 *Private network*

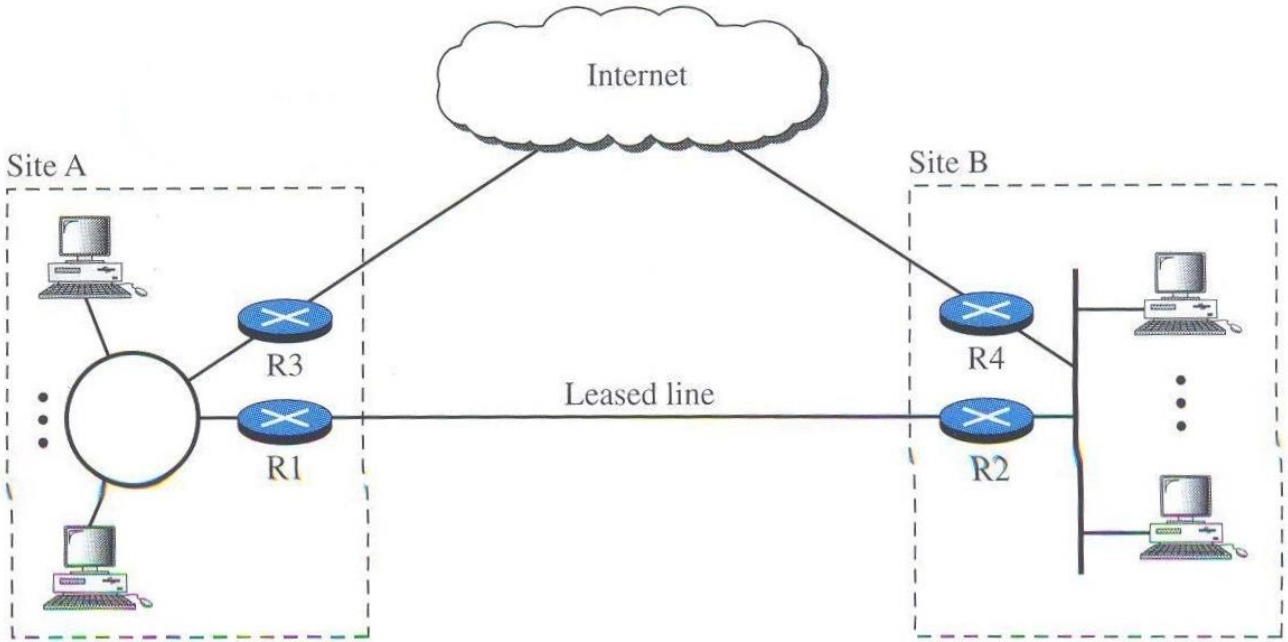


Redes híbridas

- En la actualidad, la mayoría de las organizaciones necesitan privacidad en el intercambio de información entre organizaciones, pero al mismo tiempo necesitan estar conectados al Internet global. La solución es usar redes híbridas.
- La red híbrida permite que la organización tenga su propia internet privada y al mismo tiempo tener acceso al Internet global.

Redes híbridas

Figure 32.11 *Hybrid network*

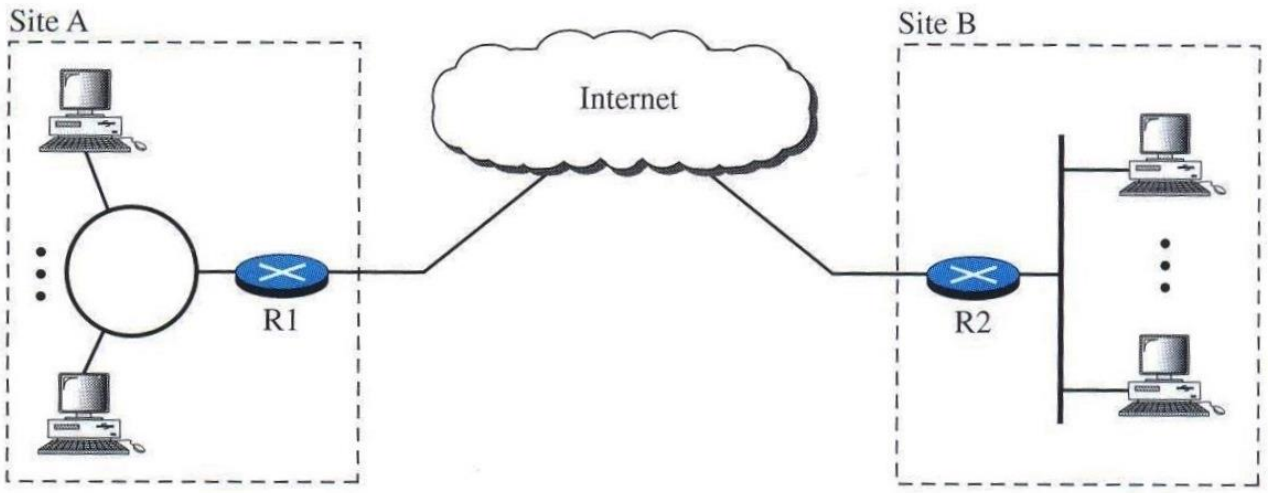


Redes privadas virtuales (VPN)

- El costo es la principal desventaja de los alternativas anteriores. Las redes WANs son costosas y para interconectar varios sitios se necesita varias enlaces rentados, lo cual implica altos costos mensuales.
- La idea de la tecnología VPN es utilizar el Internet global para comunicaciones públicas y privadas.

Redes privadas virtuales (VPN)

Figure 32.12 *Virtual private network*

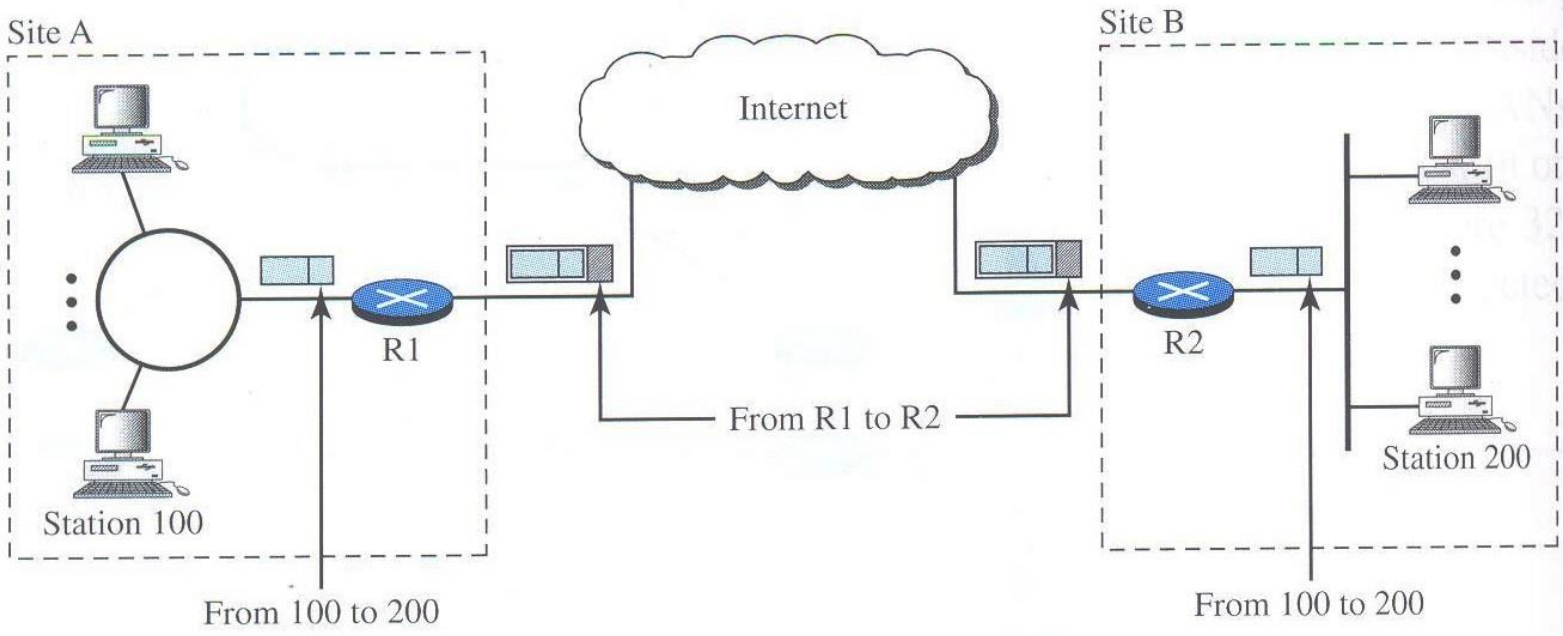


Redes privadas virtuales (VPN)

- VPN crea una red que es privada pero virtual. Es privada porque garantiza privacidad dentro de la organización. Es virtual porque no tiene una verdadera WAN privada, la red es físicamente pública pero virtualmente privada.
- La tecnología VPN usa IPSec en tunnel mode para proveer autenticación, integridad y privacidad.
- Tunneling

Redes

Figure 32.13 *Addressing in a VPN*



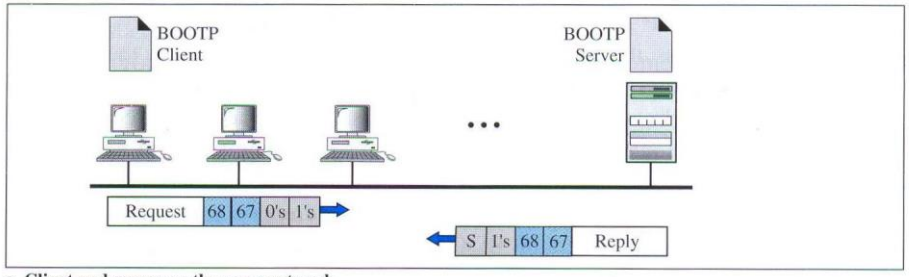
Mapeo de direcciones físicas a lógicas

Mapeo de direcciones físicas a lógicas

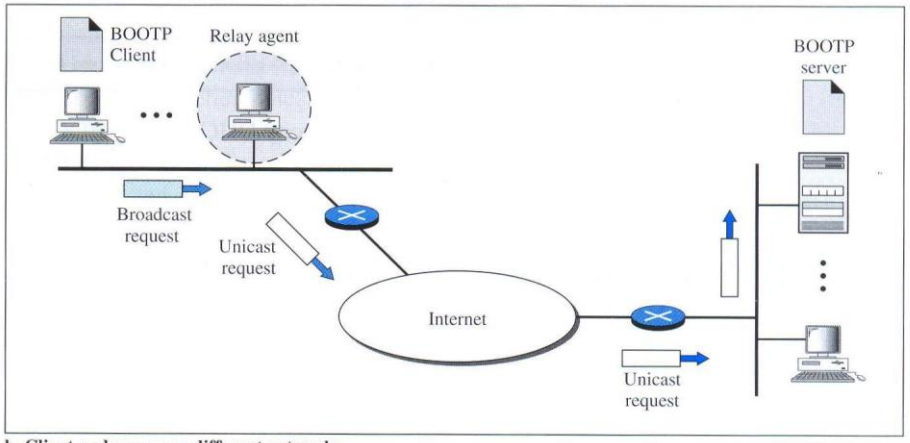
- **Reverse Address Resolution Protocol (RARP)**: encuentra la dirección lógica para una máquina que conoce solo su dirección física. Está casi obsoleto en vista que funciona a nivel de capa de enlace de datos y por lo tanto se requeriría un RARP server para cada red.
- **Bootstrap Protocol (BOOTP)**: es un protocolo cliente/servidor diseñado para proveer un mapeo de direcciones físicas a lógicas. Es un protocolo de capa de aplicación que le permite al administrador mantener una tabla que relaciona fija y estáticamente direcciones físicas y lógicas.

Mapeo de direcciones físicas a lógicas

Figure 21.7 *BOOTP client and server on the same and different network*



a. Client and server on the same network



b. Client and server on different networks

Mapeo de direcciones físicas a lógicas

- **Dynamic Host Configuration Protocol (DHCP)**: ha sido diseñado para proveer asignación de estática o dinámica de direcciones ya sea de forma manual o automática.
- DHCP tiene una primera base de datos que estáticamente asocia direcciones físicas con direcciones lógicas.
- DHCP tiene una segunda base de datos con un pool de direcciones de IP disponibles y lo hace dinámico al DHCP.

Mapeo de direcciones físicas a lógicas

- Cuando un cliente DHCP envía un requerimiento al DHCP server, este primero chequea la base estática. Si lo encuentra, retorna la dirección IP permanente.
- Caso contrario, el servidor selecciona una IP disponible del pool y agrega la entrada en la base de datos dinámica.
- Las direcciones asignadas desde el pool son temporales. El DHCP server emite una licencia por un tiempo específico. Luego de lo cual expira y el cliente debe renovar su licencia.
- En DHCP las direcciones estáticas son creadas manualmente, mientras que las dinámicas automáticamente.

Internet Control Message Protocol (ICMP)

ICMP

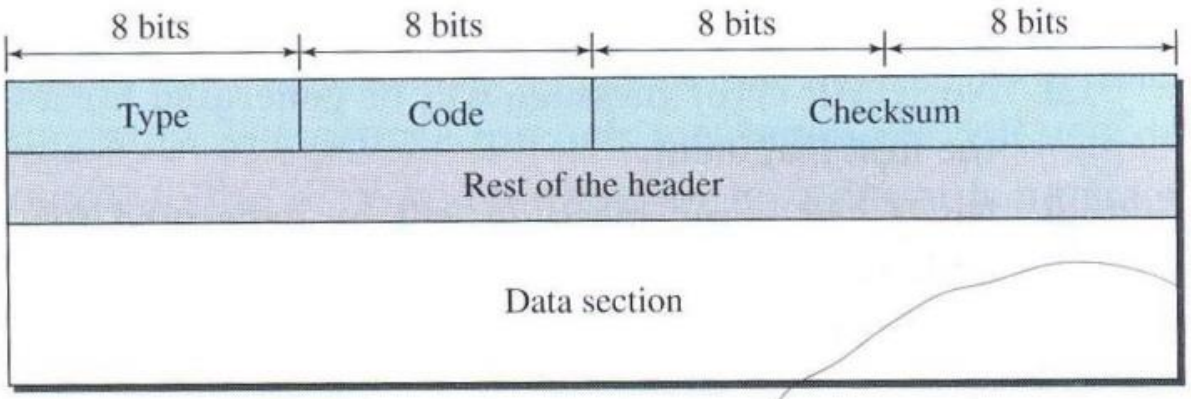
- El protocol IP es un servicio de entrega de datagramas desde un origen hacia un destino.
- Tiene dos deficiencias:
  1. Ausencia de control de errores: No posee mecanismos de reporte ni corrección de errores
  2. Falta de mecanismos de asistencia: Carece de mecanismos de administración y consulta de hosts.
- ICMP fue diseñado para compensar estas dos deficiencias.

Tipo de mensajes ICMP

- Los mensajes ICMP se clasifican en dos categorías:
  1. **Mensajes de reporte de errores**: reportan problemas que un router o un host de destino puede encontrar cuando procesa un paquete IP
  2. **Mensajes de consulta**: ocurre en pares, y ayuda a un administrador de red a obtener información específica desde un router u otro host.

Formato de mensajes ICMP

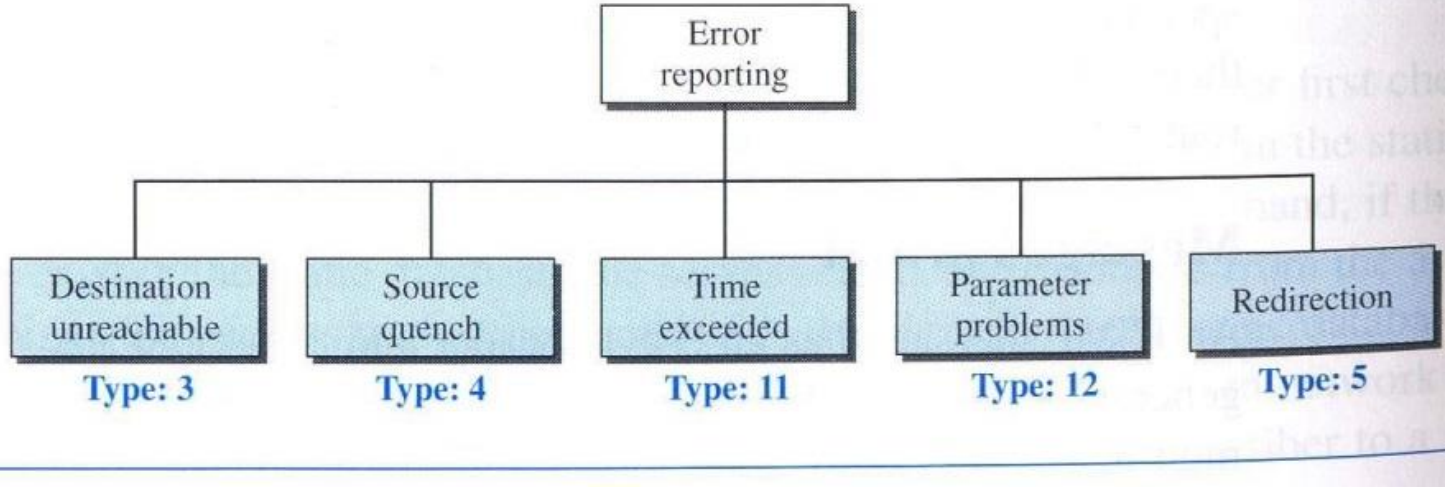
Figure 21.8 *General format of ICMP messages*



- **En caso de mensajes de error**, la sección de datos lleva información para encontrar el paquete original que tiene el error. **En caso de mensajes de consulta**, lleva información adicional dependieno del tipo de consulta.

Mensajes para reporte de errores

Figure 21.9 *Error-reporting messages*

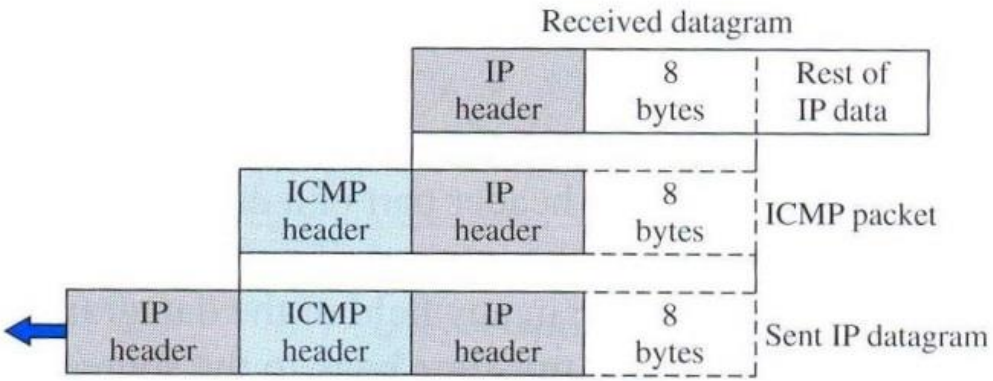


Mensajes para reporte de errores

- No se genera un mensaje de error ICMP en respuesta a un datagrama llevando un mensaje de error ICMP.
- Ningún mensaje de error ICMP será generado para un datagrama fragmentado a menos que sea el primero.
- Ningún mensaje de error ICMP será generado para un datagrama que tenga una dirección de multicasting.
- Ningún mensaje de error ICMP será generado para un datagrama que tenga una dirección especial tal como 127.0.0.0 o 0.0.0.0

Mensajes para reporte de errores

Figure 21.10 *Contents of data field for the error messages*



Mensajes para reporte de errores

- **Destination unreachable**: Si un router o host no puede entregar un datagrama, este envía un mensaje de destino inalcanzable de regreso al host de origen que inicio el datagrama.
- **Source quench**: fue diseñado para agregar una especie de control de flujo al protocol IP. Este mensaje informa al origen que el datagrama ha sido descartado y le advierte de una congestion en alguna parte de la ruta y por lo tanto se debe disminuir la velocidad del proceso de envío.

Mensajes para reporte de errores

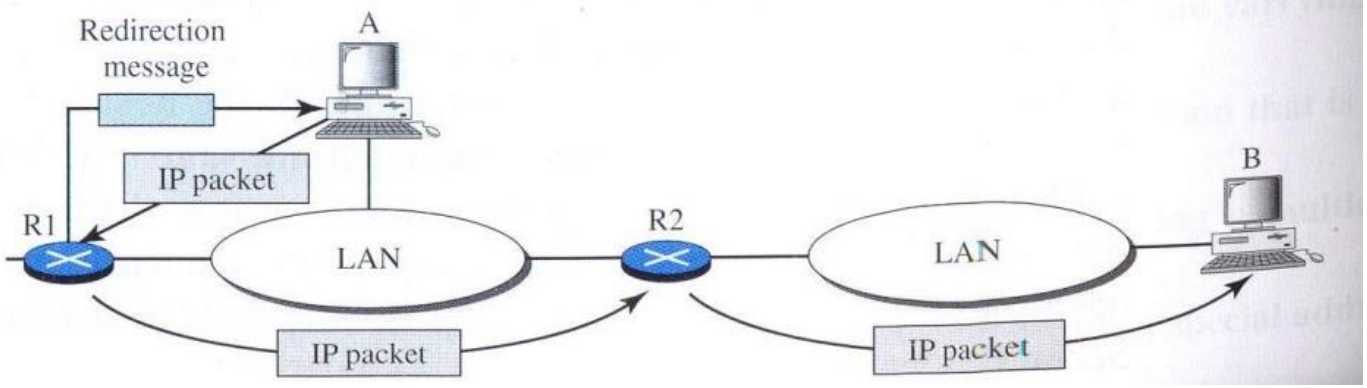
- **Time exceeded**: se genera en dos casos.
  - Cada vez que un datagrama visita un router, el valor del campo ***time to live*** se decrement en uno. Cuando este campo alcanza el valor de 0, luego del decrement, el router descarta el datagrama y en se envía un mensaje de tiempo excedido a la fuente original.
  - Cuando luego de un cierto límite de tiempo, todos los fragmentos que forman un mensaje no han arribado al host de destino.

Mensajes para reporte de errores

- **Parameter problem**: Si un router o host descubre un valor ambiguo o faltante en cualquier campo del datagrama.
- **Redirection**: Un mensaje para actualizar la tabla de ruteo de un host.

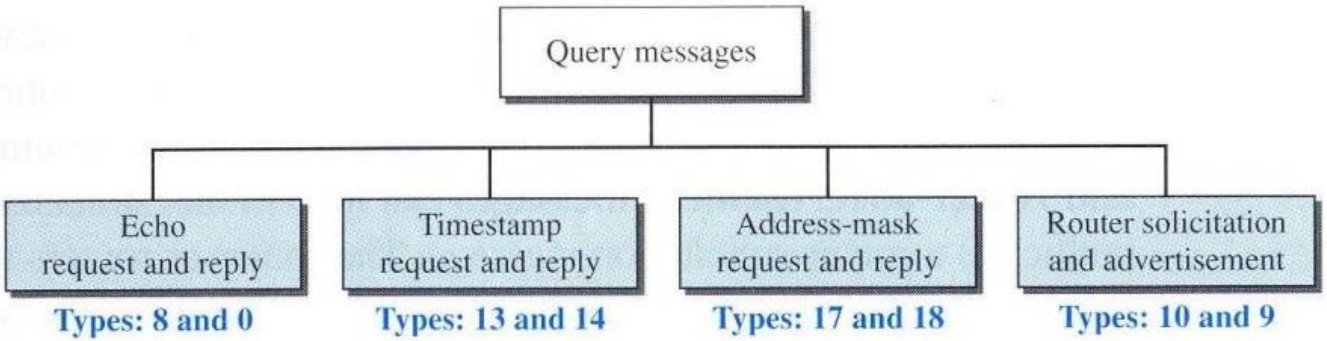
ICMP: Redirection

Figure 21.11 *Redirection concept*



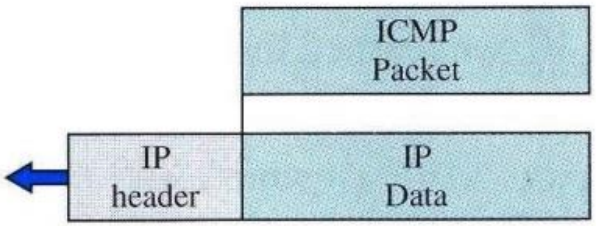
Mensajes para consulta

Figure 21.12 *Query messages*



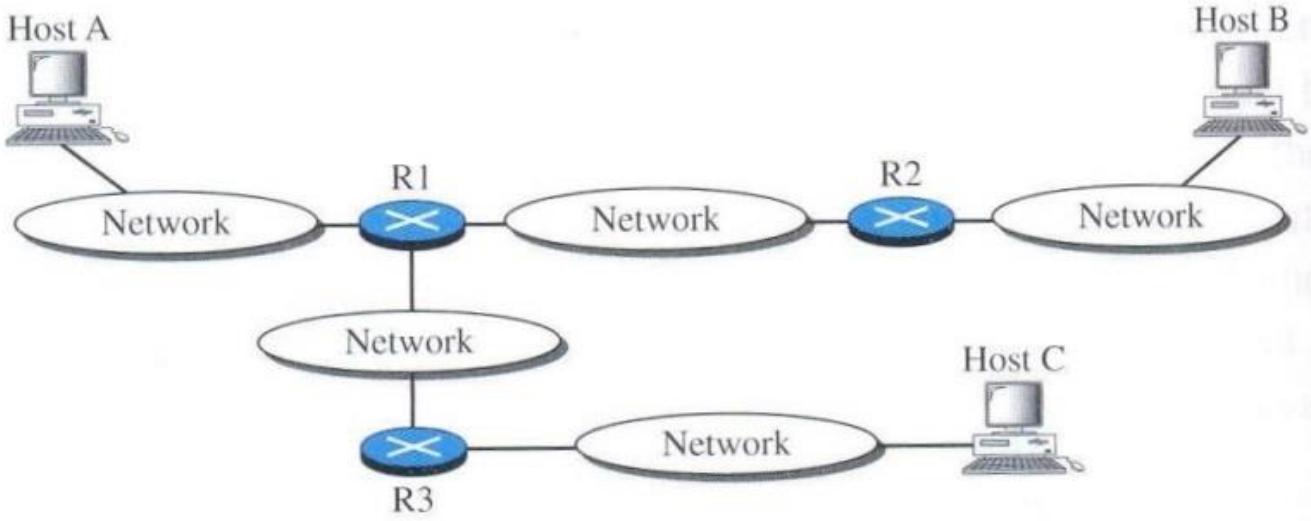
ICMP

Figure 21.13 *Encapsulation of ICMP query messages*



Traceroute

Figure 21.15 *The traceroute program operation*



Network Address Translation - NAT

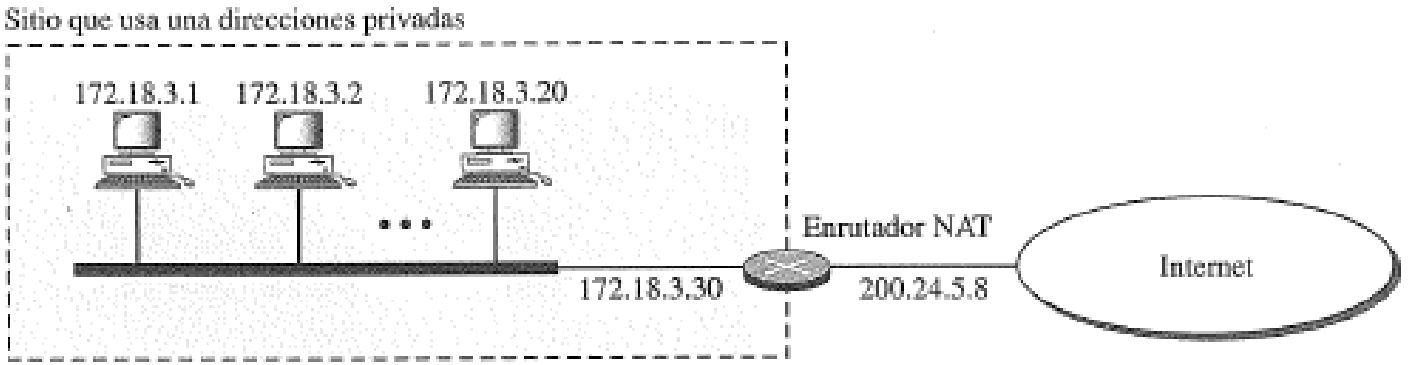
NAT

- Permite que una organización pueda tener internamente un amplio rango de direcciones IP, pero solo una o un pequeño número de direcciones externamente.
- Las direcciones IP para uso privado son únicas dentro de la organización pero no globalmente. Ningún router reenviará un paquete que tiene una de estas direcciones como dirección de destino.

NAT

- Un router de la figura corre un software NAT. En este ejemplo, la Internet ve al router NAT con la dirección 200.24.5.8

Figura 19.10 *Una implementación NAT.*



Traducción de direcciones

- Los paquetes de salida pasan a través del router, el cual reemplaza la dirección de origen con la dirección global NAT.
- Los paquetes entrantes también pasan por el router NAT, el cual reemplaza la dirección de destino con la apropiada dirección privada.

Traducción de direcciones

Figura 19.11 *Direcciones en una NAT.*

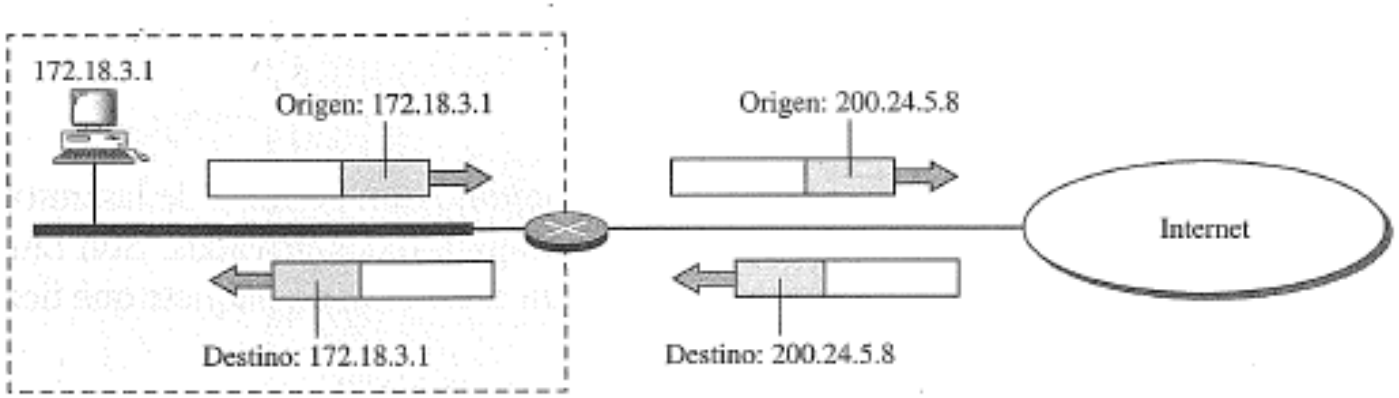


Tabla de traducción

- El router NAT utiliza una tabla de traducción para conocer la dirección de destino de un paquete proveniente de la Internet.

Figura 19.12 *Traducción de direcciones NAT.*

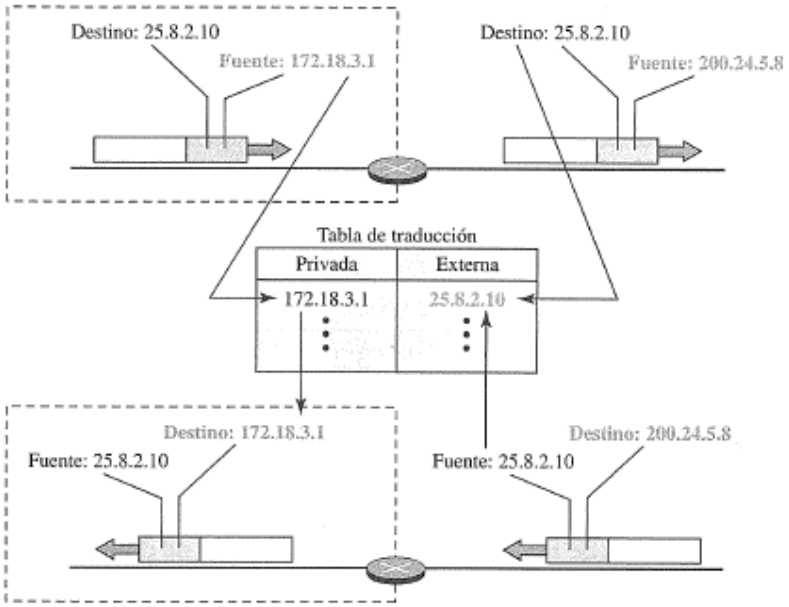


Tabla de traducción

- Existen tres casos:
  1. **Usando una dirección IP**.
     - La tabla tiene dos columnas (la dirección privada y la dirección externa – la del destino del paquete)
     - Solo un host de la red privada puede accede al mismo host externo
  2. **Usando un Pool de direcciones IP**.
     - Se usa un pool de direcciones globales.
     - El número de conexiones a un mismo host externo no puede exceder el número de direcciones en el pool.
     - Ningún host de la red privada puede acceder a dos programas en el host externo (Por ejemplo, HTTP, FTP, etc.)
  3. **Usando las direcciones IP y números de puerto**.
     - Se usan cinco columnas en la tabla para incluir los puertos de origen y destino.

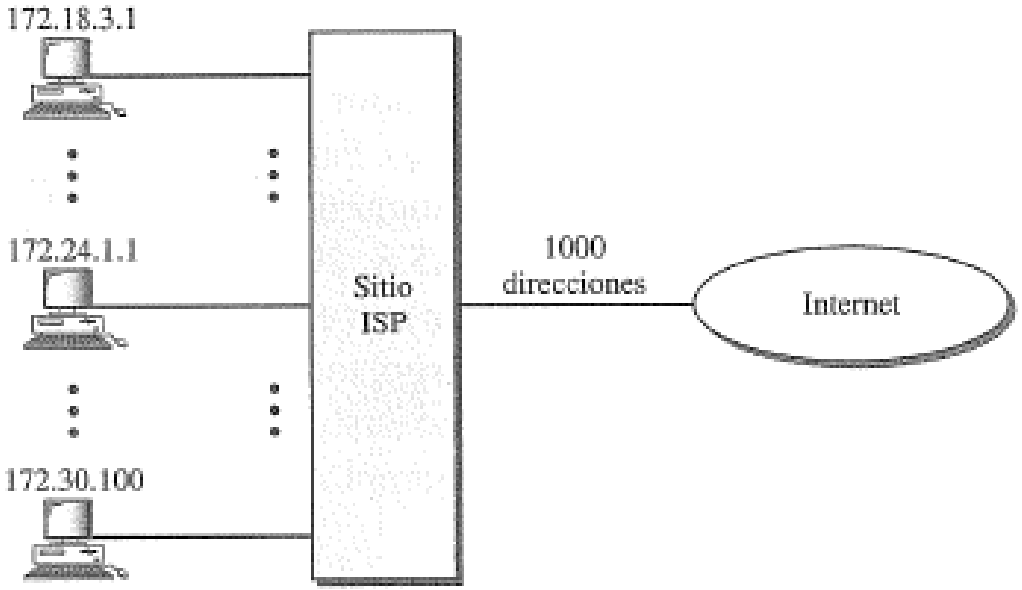
NAT

Tabla 19.4 *Tabla de traducción de cinco columnas*

Dirección privada	*Puerto privado*	*Dirección externa*	*Puerto externo*	*Protocolo de transporte*
172.18.3.1	1400	25.8.3.2	80	TCP
172.18.3.2	1401	25.8.3.2	80	TCP
...	...	...	...	...

NAT e ISPs

Figura 19.13 *Un ISP y NAT.*



Puntos para recordar

- Dominios
- Ruteo en Internet
- Mapeo de direcciones física a lógicas
- IPSec
- VPN
- ICMP
- NAT

Próxima Sesión

- Capa de transporte