

PROTOSCOLOS DE INTERCONEXIÓN DE REDES

1.3

INDICE:

1. Interconexión de redes

- 1.1 Interconexión a Nivel Físico (repetidores y concentradores)
- 1.2 Interconexión a Nivel de Enlace (puentes)
- 1.3 Interconexión a Nivel de Red (enrutadores)
- 1.4 Interconexión por Encima del Nivel de Red (pasarelas)

2. El Protocolo de Internet (IPv4)

- 2.1 Servicios y Protocolo IPv4
- 2.2 Protocolos de Resolución de Direcciones. Gestión de grupos
- 2.3 Protocolo de control y notificación de errores
- 2.4 Encaminamiento
- 2.5 Protocolos de encaminamiento dinámico en Internet

3. La siguiente generación de IP

- 3.1 Problemática del crecimiento de Internet
- 3.2 El Protocolo IPv6

1. INTERCONEXIÓN DE REDES

Las redes de área local no se encuentran normalmente aisladas

Conexiones entre segmentos de una misma LAN, a otras LAN o a Internet

Los dispositivos de interconexión operan a distintos niveles

Dispositivos de Conexión

Cinco categorías dependiendo del nivel al que operen en la red

Nivel Físico

- Repetidor
- Concentrador (Hub)

Nivel de Enlace

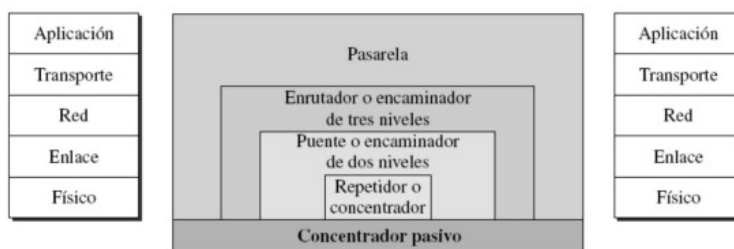
- Conmutador (Switch)
 - Puente (Bridge)
- Transparente: De aprendizaje
De traducción

Nivel de Red

- Router IP

Nivel superior

- Pasarela (Gateway)



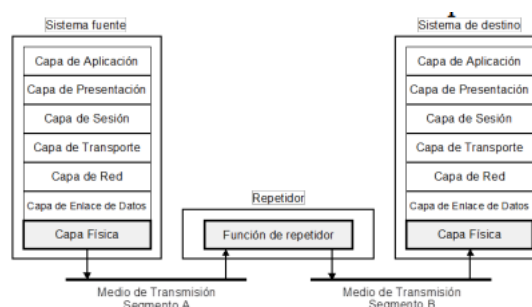
1.1. Interconexión a Nivel Físico

REPETIDORES - HUBS

Regeneran señales eléctricas cuando se usan cables largos (no sólo cables, sino también otros medios de transmisión física). Sólo copian los bits que reciben por su entrada en su(s) salida(s)

Desventajas

- No realizan distribución del tráfico
- Tienen límites de distancia
- No introducen ningún tipo de seguridad
- No es posible realizar una gestión de red
- No interconectan redes de diferentes tipos



1.2. Interconexión a Nivel de Enlace

PUENTES (BRIDGES)

Tienen implementado hasta el nivel de Enlace de Datos

Son dispositivos de Almacén y Envío

Aceptan una trama, verifican checksums, la analizan y se devuelve a la capa física para envío a la otra subred.

Las redes interconectadas se consideran una sola subred.

Ventajas

Segmentación red

Fiabilidad

Seguridad

Tipo de puentes:

Transparentes

Interconectan redes iguales

Dos tipos

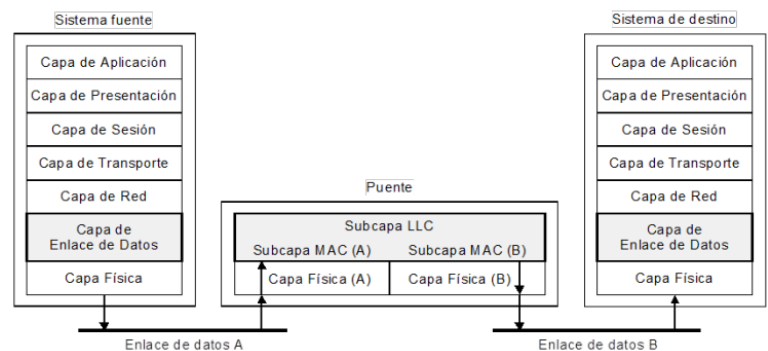
» Básicos

» De aprendizaje (Aísla tráfico)

De Traducción

Conecta redes con protocolos diferentes a nivel de enlace (o MAC en el caso de las LAN)

Antes de reenviar las tramas realiza la conversión de protocolos que sea necesaria

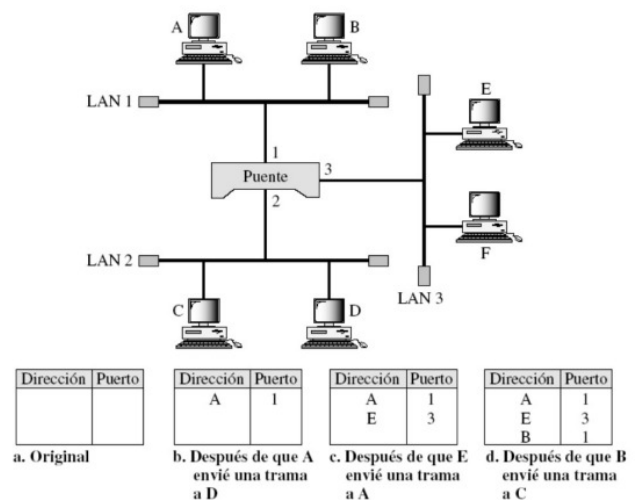


Puentes transparentes de aprendizaje:

Tiene capacidad de filtrado (decide enviar o eliminar la trama)

Decide por qué puerto realizar el envío

Mantiene tabla interna que relaciona direcciones y puertos



Problemas de la interconexión a través de puentes de traducción:

Dificultades para conectar LANs 802.X de distinto tipo

Reformatear trama y calcular nuevo CRC

Invertir el orden de los bits

Inventarse o desechar bits en algunos campos

Generar una prioridad ficticia

Desechar la prioridad

Problema con la congestión, de una red rápida a una lenta

El intercambio de ACK retrasado o imposible

Problema muy grave, trama demasiado larga para el destino

CONMUTADORES (SWITCHES)

Como el puente: nivel de enlace

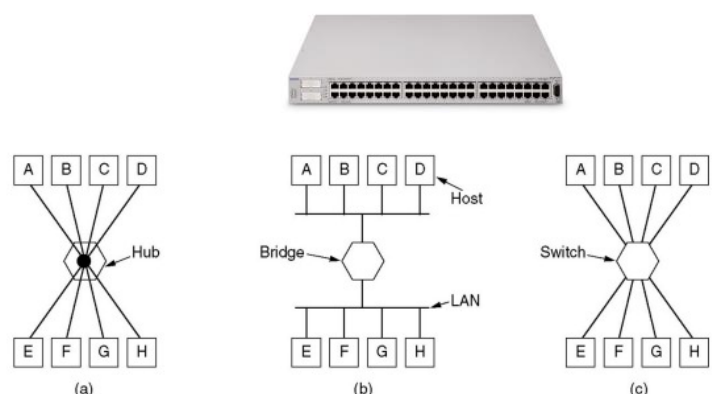
Pero habitualmente

-Un conmutador interconecta ordenadores

-Un puente interconecta redes locales

-Sólo realizan el procesamiento de la trama del nivel de enlace, para distribuir el tráfico pero no comprueban errores...

Hub vs Bridge vs Switch



1.3. Interconexión a Nivel de Red

ENCAMINADOR (ROUTER)

Es un dispositivo que opera en el nivel de red

Puede determinar el mejor camino a través de una serie de enlaces de datos para ir desde una red fuente a una red destino

Es un dispositivo de propósito específico

Se dedica a interconectar redes

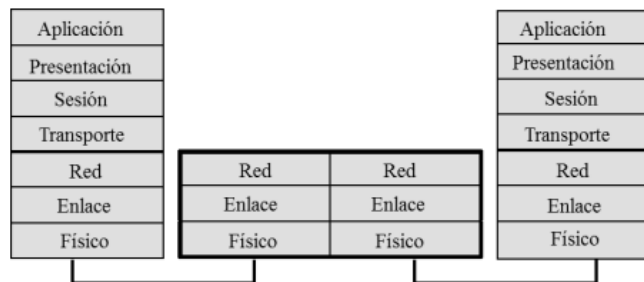
Para la red, un router es un nodo más

Un router puede conectar

Una LAN con una WAN

Dos LANs

Dos WANs



1.4. Interconexión por encima del Nivel de Red

Pasarelas (gateways)

Se usa para hacer referencia a un sistema que opera por encima del nivel de Red (pero a veces es usado como sinónimo de router)

Una ventaja decisiva es que puede conectar redes con formatos de direccionamiento distintos

Realizan funciones de conversión entre protocolos desde el nivel de Red

Pasarelas que operan a nivel de transporte:

Suelen ser multiprotocolo

Ejemplo: conexión de una red TCP/IP con una red ATM

Se pueden usar para conexiones a redes WAN

Pasarelas que operan a nivel de aplicación:

Ejemplo: envío de correo electrónico entre máquinas que usan sistemas de correo diferente

Envío de un mensaje de correo electrónico a un teléfono móvil vía SMS

2. EL PROTOCOLO DE INTERNET (IPV4)

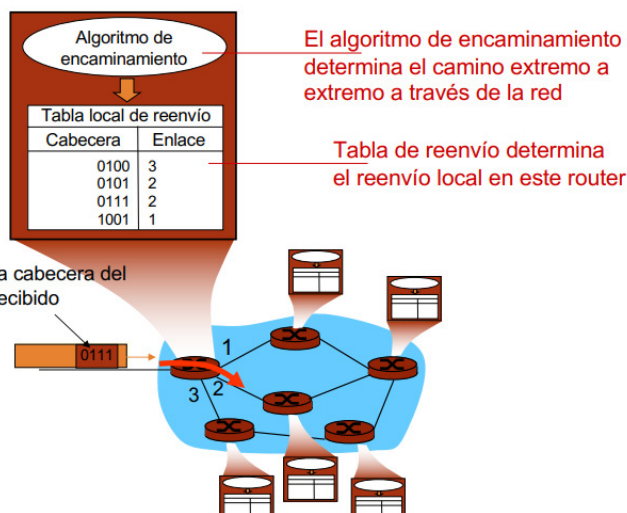
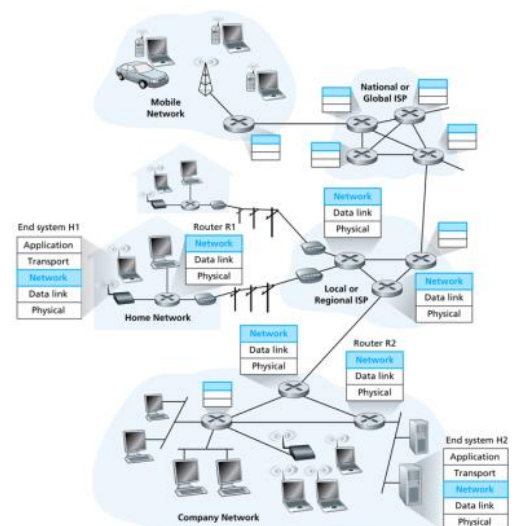
2.1. Internet Protocol (IP) versión 4

Objetivo básico:

- Enviar los paquetes del nodo emisor al nodo receptor a través de una red de conmutación de paquetes
- Dado que puede haber varias rutas posibles, la capa de red es la encargada del encaminamiento

Reenvío (Forwarding): Mover paquetes de la entrada de un router a la salida del router apropiada

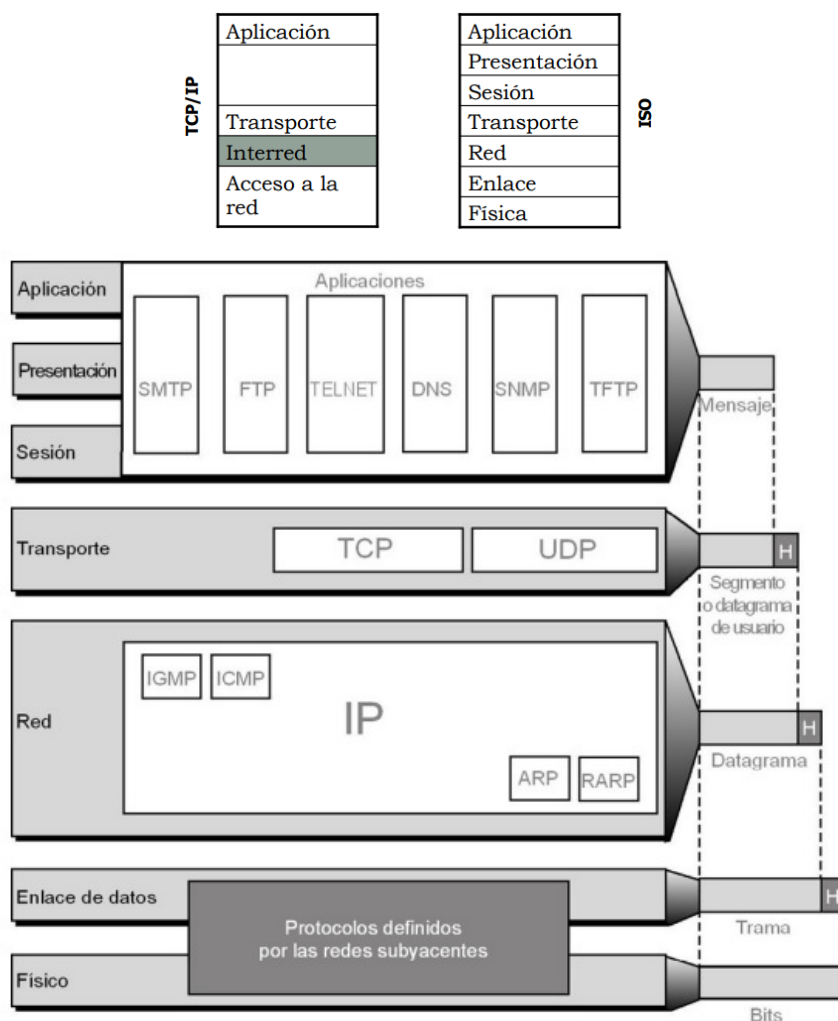
Encaminamiento (Routing): Determinar la ruta que seguirán los paquetes desde el origen al destino. Algoritmos de encaminamiento



El protocolo IP

El protocolo interred (Internet Protocol o IP), RFC 791

Es el corazón de TCP/IP y es el protocolo más importante de la capa de red
IP facilita el servicio de reparto básico de paquetes de las redes TCP/IP



Es un protocolo sin conexión

Deja en manos de las capas superiores el establecimiento de la conexión si se requiere un servicio orientado a la conexión

IP también deja en manos de otras capas la verificación de datos y la recuperación de errores

Detecta errores pero no hace nada por recuperarse de ellos Los routers descartan los paquetes

Los protocolos de otras capas han de proporcionar control de errores si éste es requerido

(Primitivas) Servicio IP

Send: R_DATOS.petición(Origen, Destino, Datos, Calidad de servicio)

Recv: R_DATOS.indicación(Origen, Destino, Datos, Calidad de servicio)

Funciones del protocolo IP

Las funciones básicas son:

Definir el datagrama, que es la unidad básica de transmisión

Definir el esquema de direccionamiento

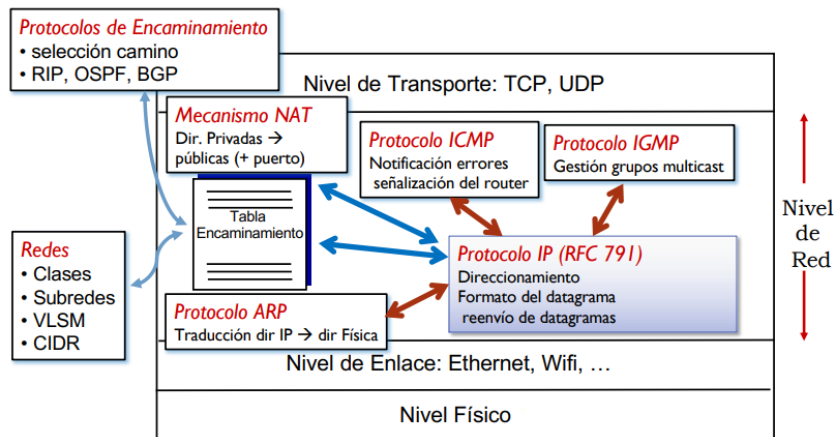
Trasladar los datos entre las capas de acceso a la red y las capas de transporte

Encaminar datagramas a ordenadores remotos

Fragmentación y reensamblado de datagramas

Control de congestión

Descarte de paquetes

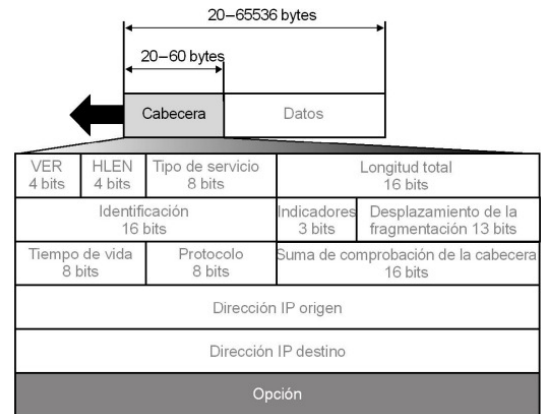


Datagramas IP

Los paquetes se denominan datagramas

Estructura

- Contiene una cabecera y los datos
- La cabecera tiene una parte fija de 20 bytes y una parte variable



Campos (longitudes expresadas en bits)

Versión (4): versión del protocolo

Longitud de la cabecera (4): HLEN:

Longitud total de la cabecera del datagrama en palabras de 4 bytes

Es necesario porque la longitud de la cabecera es variable (20-60 bytes) à (HLEN 5-15)

Tipo de servicio (8): parámetros de velocidad, prioridad, retardo, rendimiento

Longitud total (16): longitud del datagrama. El máximo valor es 65535 bytes (64 KiB)

Campos fragmentación/reensamblado:

Identificación (16): identifica de forma única al datagrama

Flags (3)

DF (1): don't fragment

MF (1): more fragments. Todos los fragmentos menos último lo tienen activado

Un bit no usado

Offset del fragmento (13): indica a qué parte del datagrama pertenece el fragmento (el desplazamiento real se obtiene multiplicando por 8)

Tiempo de vida (8): contador para limitar la vida de los paquetes

Almacena una marca de tiempo que se va decrementando en cada salto

El datagrama se descarta cuando llega a 0

Controla el número máximo de saltos

Campos

Protocolo

Del nivel superior. Indica a qué elemento de la capa de transporte hay que entregar el datagrama (TCP ó UDP)

Checksum de la cabecera: se recalcula en cada salto (hop)

Opciones

Tamaño variable (máx. 40 bytes)

Útiles para probar y depurar la red

Fragmentación de datagramas

Motivación

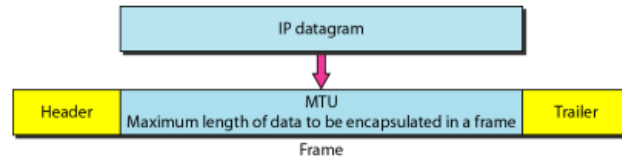
La longitud del datagrama es mayor que la unidad máxima de transmisión (MTU) del nivel del enlace de la interfaz de salida

Solución

- Fragmentar el datagrama en fragmentos de longitud \leq MTU
- La capa IP ha de ser capaz de fragmentar los datagramas
- Cada fragmento es un datagrama completo
- Se deben reensamblar o recomponer el datagrama original antes de entregarlo a la capa de transporte del host destino

Inconveniente

- Costoso de implementar computacionalmente
- Coste que incide en el tiempo de entrega del datagrama original

**Campos de la cabecera relacionados con la fragmentación**

Identificador: El mismo para todos los fragmentos

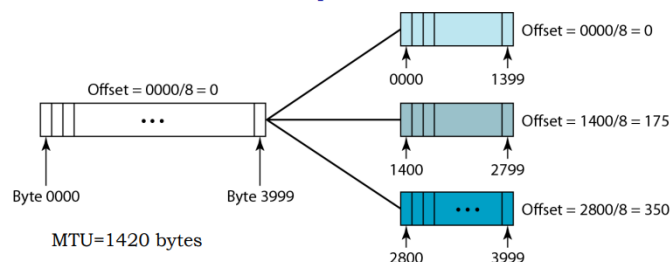
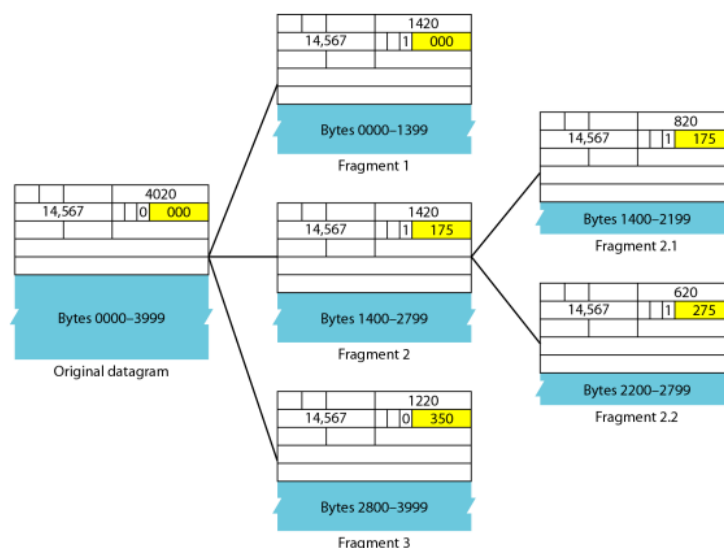
Indicadores

Desplazamiento

**Desplazamiento:**

Mide el desplazamiento de los datos con respecto al datagrama original (unidades de 8 bytes)

El desplazamiento (tamaño de datos) de los fragmentos intermedios debe ser múltiplo de 8

**Ejemplo de fragmentación****Direcciones IP**

Las direcciones IPv4 son únicas e universales

Una dirección IPv4 tiene una longitud de 32 bits

El espacio de direcciones es 2³² (4.294.967.296)

Tres tipos de direcciones: – Unicast (individual – uno) – Multicast (grupo – muchos) – Broadcast (difusión – todos)

Notaciones: – Binaria – Decimal-punto (punto-decimal)

Direccionamiento IP

El encaminamiento en IP es un encaminamiento jerárquico

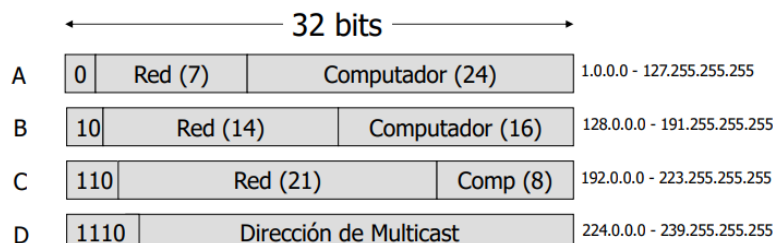
Encaminamiento basado en el direccionamiento jerarquizado

En IP se realiza una jerarquía de encaminamientos de dos niveles, según la cual una dirección IP se divide en una parte para la red y otra para el host (dispositivo) <id.Red><id.host>

Los routers usan únicamente la parte de la red hasta que un datagrama IP llega a un router que puede entregar el paquete directamente

Formatos de direcciones IP

Clases: El espacio de direcciones se divide en 4 clases A, B, C y D



Las direcciones de red son asignadas por el ICANN

Internet Corporation for Assigned Names and Numbers

Delega partes del espacio de direcciones a entidades regionales

Direcciones IP especiales

00000000000000000000000000000000	La máquina local
Red 0000 . . . 0000	Identificador de Red
0000 . . . 00000 Host	Una máquina en la red local
11111111111111111111111111111111	Broadcast en la red local
Red 1111 . . . 1111	Broadcast en una red remota
127 (irrelevante)	Test loopback. Ej: 127.0.0.1

Notaciones IP – Representación

Binaria

La dirección IP se muestra como 32 bits

10000000	00001011	00000011	00011111
128.11.3.31			

Decimal-punto

Se separan por puntos en 4 grupos de 8 bits. Cada grupo se representa en decimal (0-255)

- #C0290614 -> 192.41.6.20

Subredes

Motivación: Cuando una red se compone de varias subredes, usar directamente direcciones tipo A, B o incluso C puede ser ineficiente

Idea básica:

Se puede dividir un bloque de direcciones (de clase A, B o C) en varios grupos de direcciones más pequeños

Se usan varios bits del identificador de host para constituir un identificador subred

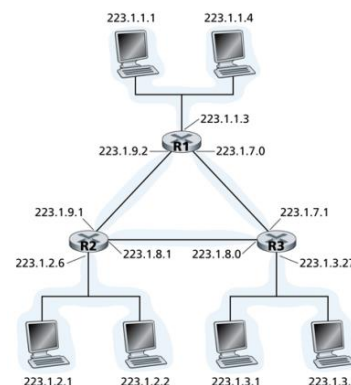
Si tomo 'n' bits, entonces puedo definir 2^n subredes

Asignar cada grupo a redes más pequeñas à subredes

El tamaño de cada subred disminuye según el número de bits asignados para identificador de subred

Máscara de subred: Patrón de 0s y 1s para calcular el identificador de subred a la que pertenece un equipo

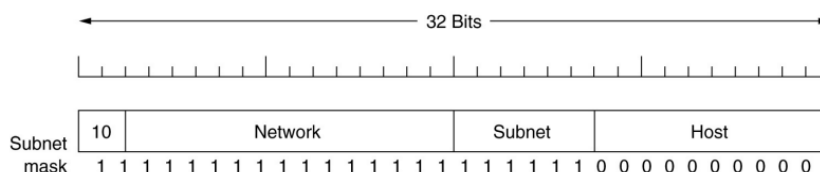
Ventaja: No hace falta pedir nuevas direcciones al ICANN. Aprovechamiento de direcciones IP



de
de

Máscara de subred. Ejemplo

dirección de clase B dividida en 64 subredes



Notación prefijo

Máscaras de bits contiguos

Notación identificador de subred: a.b.c.d/prefijo – Ej: 159.110.128.0/18

Ejemplo

IP destino: 192.228.17.57

	Representación Binaria	Representación Decimal
Dirección IP	11000000.11100100.00010001.00111001	192.228.17.57
Máscara de subred	11111111.11111111.11111111.11100000	255.255.255.224 (equivalente a prefijo /27)
Operación AND de dirección y máscara	11000000.11100100.00010001.00100000	192.228.17.32
Número/Identificador de subred	11000000.11100100.00010001.00100000	1/192.228.17.0 (hay 8 posibles)
Número/identificador de máquina	00000000.00000000.00000000.00011001	25

Direccionamiento IP

La longitud de los identificadores de red/subred dependen de la clase a la que pertenecen (en las clases A, B y C)

Máscaras por defecto según la clase de dirección

Clase	Binario	Punto-Decimal	Prefijo
A	11111111 00000000 00000000 00000000	255.0.0.0	/8
B	11111111 11111111 00000000 00000000	255.255.0.0	/16
C	11111111 11111111 11111111 00000000	255.255.255.0	/24

Subredes

La primera dirección de un bloque NO se asigna normalmente a un dispositivo -> se usa como la dirección de red que representa la organización ante el resto del mundo

Es necesaria para la función de encaminamiento

Número de IPs por subred:

IH: bits del identificador del host.

N: bits de extensión

Número de IPs/subred: $IP = 2^{(IH-N)} - 2$

No es una IP asignable a un host la dirección de subred (id. de host todo a 0)

No es una IP asignable a un host la dirección de broadcast (id. de host todo a 1)

Encaminamiento CIDR

CIDR (enrutamiento entre dominios sin clase - Classless Interdomain Routing)

En este esquema no hay clases, pero las direcciones se asignan en bloques (rango) de direcciones

El tamaño del bloque (nº de direcciones) varía

Restricciones en la definición de bloques

Las direcciones del bloque deben de ser contiguas

El nº de direcciones en un bloque debe ser potencia de 2 (1,2,4,8,16,32, ...)

Definición de bloques

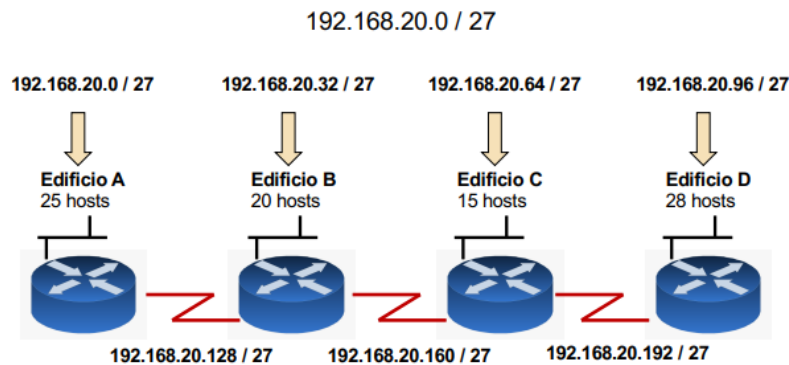
dirección -> x.y.z.t/n -> máscara (nº de bits compartidos por las direcciones que pertenecen al bloque)

Subredes con tamaño de máscara variable (VLSM)

Motivación: Definir subredes de tamaño variable para no desaprovechar subredes (VLSM – Variable Length Subnet Mask)

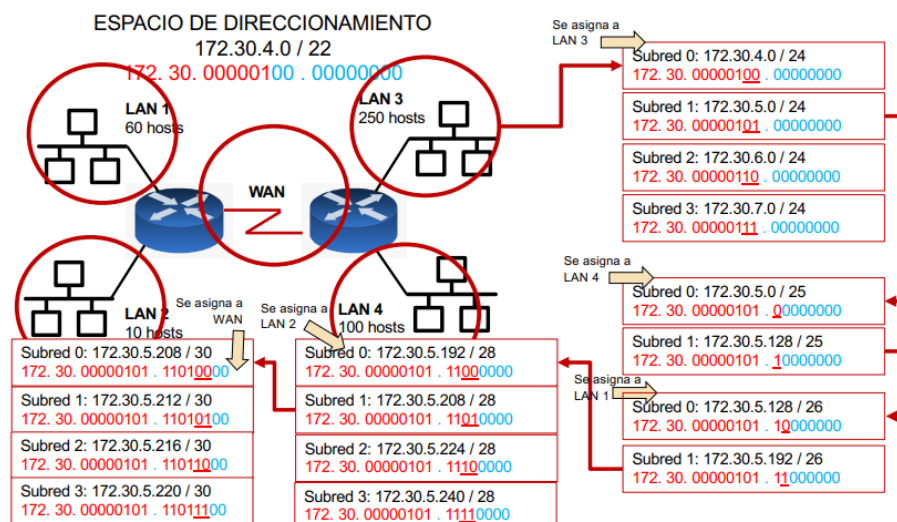
Subredes con máscara de tamaño fijo (FLSM)	Subredes con máscara de tamaño variable (VLSM)
Antiguas	Modernas
Subredes de igual tamaño	Subredes de tamaño variable
Soporta protocolos de enrutamiento con y sin clases de direcciones	Soporta protocolos de enrutamiento solo sin clases de direcciones
Desperdicia más direcciones IP	Desperdicia menos direcciones IP
Todas las subredes usan la misma máscara	Las subredes utilizan distintas máscaras
Configuración y administración sencilla	Configuración y administración más compleja

ESQUEMA DE SUBRED TRADICIONAL



Cada subred tiene 30 direcciones disponibles ($5 \text{ bits de host id} \rightarrow 2^5 - 2$)

Desperdicio de direcciones (p.ej: IPs necesarias en enlaces WAN 2 (sobran 28 direcciones/enlace WAN, 84 en total)



Funciones de IP: Encaminamiento con datagramas

La función más importante de la capa IP es el encaminamiento de datagramas extremo a extremo a través de Internet

Características

El envío de mensajes mediante datagramas tiene la ventaja de adaptarse fácilmente ante fallos en los nodos
Los paquetes serán (relativamente) largos

Hay que incluir la dirección de destino en cada datagrama

Cada paquete de un mismo flujo de datos se encamina de forma independiente

Estrategia: Cada host o router tiene una tabla de encaminamiento

El método utilizado por un router o un host para averiguar la IP a la que debe enviar un determinado datagrama se denomina genéricamente como el “algoritmo de encaminamiento”.

En las tablas de encaminamiento se almacena información sobre los posibles destinos y sobre cómo alcanzarlos.

Como el esquema de direccionamiento en IP es jerárquico, en las tablas de encaminamiento IP los posibles destinos se identifican por el identificador de red

De esta forma se ocultan los detalles de qué hosts y cómo están conectados a las diferentes redes y se minimiza el tamaño de las tablas de encaminamiento.

Tabla de Encaminamiento

El contenido de las tablas de encaminamiento suelen ser pares del tipo .

Donde N es un identificador de red y R es la dirección IP del router en el siguiente salto para alcanzar dicha red por tanto el router debe estar conectado a la misma red física

Identificador de red	Siguiente salto
----------------------	-----------------

Cuando hay subredes

Se incluye como información una columna con la máscara que hay que aplicar para comparar correctamente la dirección destino del datagrama con la dirección destino de la entrada

Identificador de red/subred	Máscara	Siguiente salto
-----------------------------	---------	-----------------

Si un router está conectado a varias redes

Se necesita el identificador de interfaz de salida, ej: hme0, le1, etc

Identificador de red/subred	Máscara	Siguiente salto	Identificador de interfaz
-----------------------------	---------	-----------------	---------------------------

entrada envío directo

1. La IP destino pertenece a la misma red/subred

- El envío directo (entrega directa) es la transmisión de un datagrama desde el host origen hasta el host destino a través de una sola red física (un único enlace – punto a punto o multipunto)
- 2 hosts sólo pueden comunicarse mediante entrega directa si ambos están conectados directamente a la misma red física (por ejemplo, una sola red Ethernet)

Básicamente en la entrega directa el emisor encapsula el datagrama dentro de una trama de enlace/física, transforma la dirección IP destino en una dirección física y envía la trama resultante al destino a través de la interfaz física correspondiente

entrada envío indirecto

El envío indirecto (entrega indirecta) es necesario cuando el host destino no está conectado directamente a la red del origen, lo que implica que el datagrama deberá atravesar varias redes físicas, y para ello es necesario atravesar routers

La entrega indirecta es más compleja ya que hay que determinar:

- el host origen ha de identificar al primer router al que debe entregar el datagrama
- el primer router debe identificar cuál será el siguiente router al que debe enviar el datagrama, esto también se denomina identificar el “siguiente salto”
- La comunicación entre dos routers consecutivos de la ruta se realiza siempre mediante entrega directa:
 - Dos routers deben estar conectados a la misma red física
 - A su vez, el último router de la ruta que sigue el datagrama debe estar conectado a la misma red física que el host destino

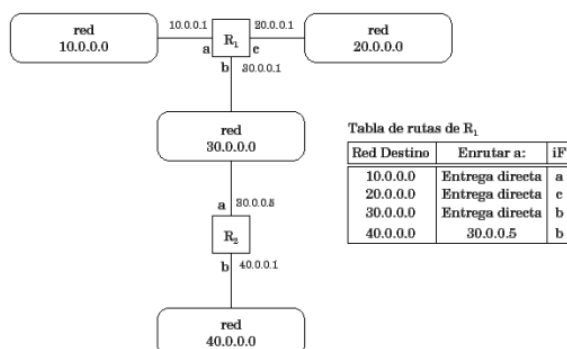
entrada por defecto

Para simplificar más las tablas de encaminamiento aparece el concepto de “ruta por defecto” - default

La ruta por defecto contiene la dirección del router del siguiente salto al que se deben enviar los datagramas (también denominado router por defecto) si tras recorrer la tabla de encaminamiento no se encontró ninguna ruta específica para el identificador de red al que va dirigido el datagrama

La tabla de encaminamiento permite especificar una ruta especial para una dirección IP (individual o multicast) en particular

Ejemplo



Algoritmo de Encaminamiento IP

```

1 IF hay ruta específica en el campo de Opciones THEN
2   Enviar según ruta específica
3   RETURN
3 ELSE
4   Extraer IP destino (IPd) del datagrama
5   FOREACH entrada en la Tabla de encaminamiento (hasta entrada por defecto)
6     Calcular el Identificador de red (Id_red) o subred (Id_subred): IPd AND Mascara
7     IF Id_red o Id_subred coincide con entrada en la tabla THEN
8       IF envío Directo THEN
9         Enviar a IPd directamente (Usar ARP con IPd para obtener dir. enlace)
10        RETURN
11      ELSE
12        Enviar al Siguiente Router con IPr (Usar ARP con IPr para obtener dir. enlace)
13        RETURN
14    END
15  IF entrada por Defecto THEN
16    Enviar al Router por defecto con IPr (Usar ARP con IPr para obtener dir. enlace)
17  ELSE
18    Error de encaminamiento (Notificación por parte de ICMP)

```

En la mayor parte de implementaciones, el tráfico dirigido a una determinada red desde un host origen va a seguir el mismo camino aunque existan diversas posibilidades

Los datagramas que viajen de A a B pueden seguir rutas diferentes a los datagramas que viajen de B a A

A excepción de la disminución del campo TTL (y el recálculo del checksum de forma oportuna), el encaminamiento no modifica la cabecera del datagrama original

En particular, las direcciones IP origen y destino permanecen fijas durante toda la ruta.

Protocolos asociados a IP

IP es de tipo best-effort y necesita de otros protocolos

Clasificación de los protocolos asociados a IP

Asociar direcciones lógicas a físicas -> ARP, DHCP, etc

Gestión de grupos (envíos multicast) -> IGMP

Alertar situaciones de congestión y errores -> ICMP

Actualización de tablas de encaminamiento -> RIP, OSPF

Protocolos de resolución de direcciones – ARP

La entrega de un paquete requiere el uso de una dirección lógica y de una dirección física

Por tanto, debemos ser capaces de traducir una dirección lógica a su correspondiente dirección física y viceversa.

Address Resolution Protocol

Asocia direcciones lógicas (IP) a direcciones físicas

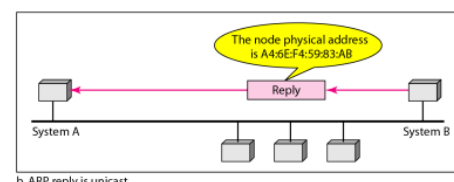
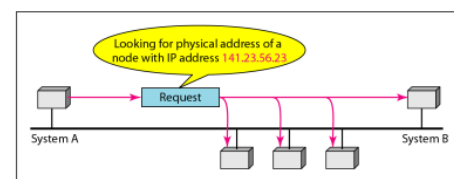
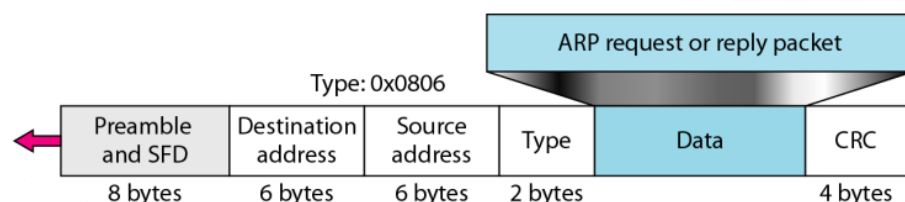
-La consulta es enviada a toda la red (broadcast)

-La respuesta es enviada sólo a la máquina que realizó la consulta (unicast)

-Las últimas asociaciones son almacenadas

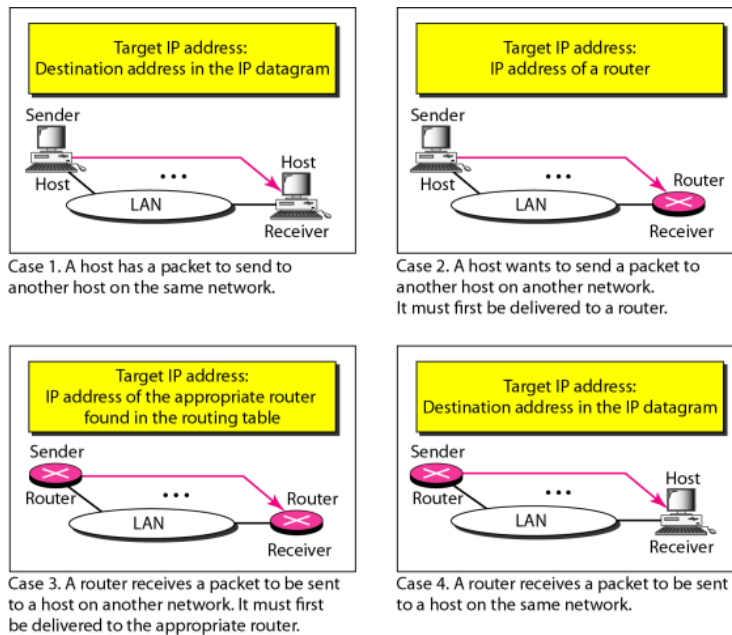
-El destinatario también actualiza su tabla con las direcciones de origen

Las últimas asociaciones son almacenadas temporalmente en una memoria caché interna. Antes de enviar una petición se consulta la caché
Un paquete ARP se encapsula directamente en una trama del nivel de enlace



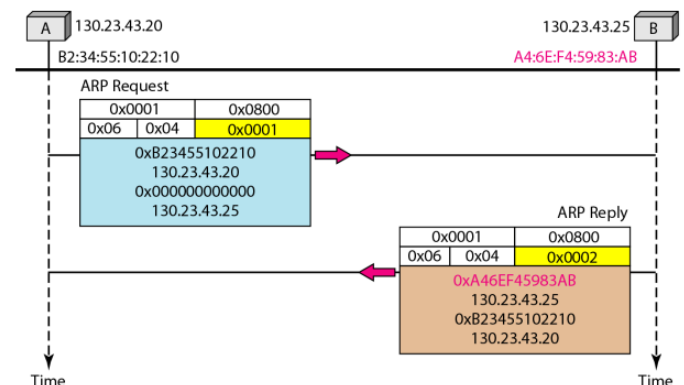
32 bits		
8 bits	8 bits	16 bits
Hardware Type	Protocol Type	
Hardware length	Protocol length	Operation Request 1, Reply 2
Sender hardware address (For example, 6 bytes for Ethernet)		
Sender protocol address (For example, 4 bytes for IP)		
Target hardware address (For example, 6 bytes for Ethernet) (It is not filled in a request)		
Target protocol address (For example, 4 bytes for IP)		

4 casos de uso de ARP



Ejemplo de resolución ARP

Un host con dirección IP 130.23.43.20 y dirección física B2:34:55:10:22:10 tiene que enviar un paquete a otro host con dirección IP 130.23.43.25 y dirección física A4:6E:F4:59:83:AB. Los dos hosts están en la misma red Ethernet. Muestra los paquetes ARP request y reply encapsulados en las tramas Ethernet.



Protocolos de asignación de direcciones – DHCP

Mecanismos para asociar IPs

Asignación manual

Asignar una IP fija con ifconfig, ipconfig, ip address, etc

Asignación automática

Asignar una IP permanentemente cuando se solicita (ej: RARP, BOOTP y DHCP)

Asignación dinámica

Asignar una IP temporalmente cuando se solicita (DHCP)

Utilidad asignación IPs automática y dinámica

Estaciones móviles (ej: portátiles, teléfonos móviles, etc.)

Arranque de estaciones sin disco

Protocolo DHCP (Dynamic Host Configuration Protocol)

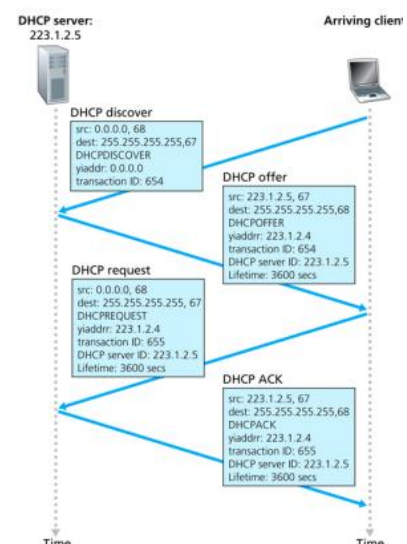
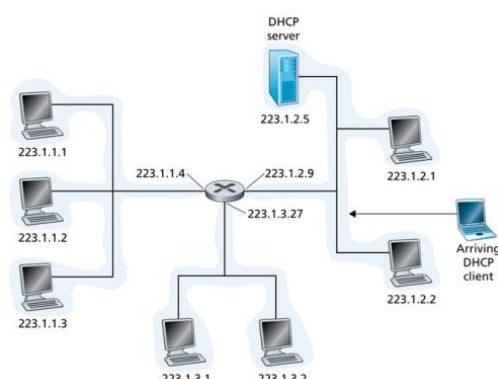
Permite, dada una dirección física, obtener la dirección IP

Funcionamiento básico

Se difunde la dirección Ethernet

El servidor DHCP responde con la IP

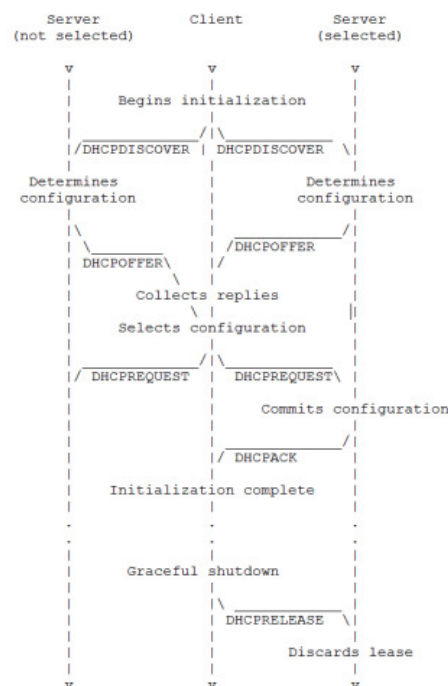
Protocolo DHCP



Protocollo DHCP

Asignación dinámica

- Lease time (LT) : Tiempo completo durante el cual se “arrienda” una configuración dada
- T1: Temporizador para iniciar el renovado de una configuración ($T1 < LT$)
- T2: Temporizador para iniciar la segunda solicitud de una nueva configuración, antes de perder la conexión ($T1 < T2 < LT$)



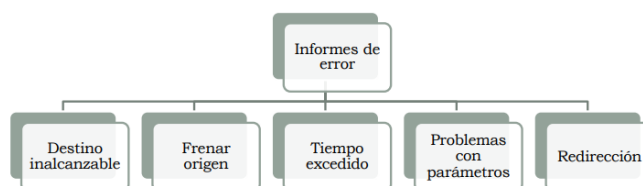
Protocolo de control y notificación de errores - ICMP

Protocolo de Control de Mensajes de Internet

Mensajes de monitorización y de informes de error

Mensajes de informe de error

- Informan (NO CORRIGEN) errores que un dispositivo de encaminamiento o la máquina destino han encontrado en un datagrama
- Se envían al origen de la transmisión



Sin embargo no se generará un mensaje de error ICMP...

En respuesta a un datagrama que lleve un mensaje de error ICMP

Para un datagrama fragmentado que no sea el primer fragmento

Para un datagrama que tenga una dirección multicast

Para un datagrama que tenga una dirección especial (0.0.0.0)

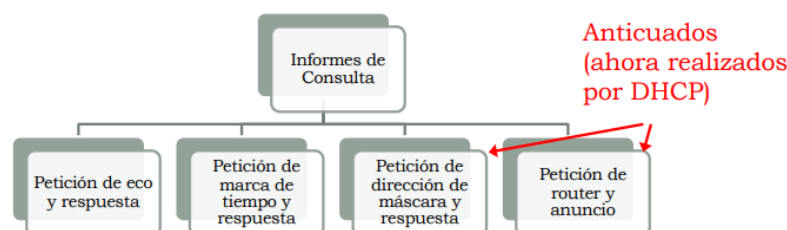
Mensajes de monitorización y consulta

Para diagnosticar problemas en la red

Se envían por pares

Un nodo envía un mensaje que es respondido por otro nodo destino

Ayudan a obtener información específica acerca de un router u otra máquina



Encaminamiento

Una de las objetivos principales del nivel de Red es facilitar la interconexión de redes, y una de las funciones principales del nivel de red es el encaminamiento:

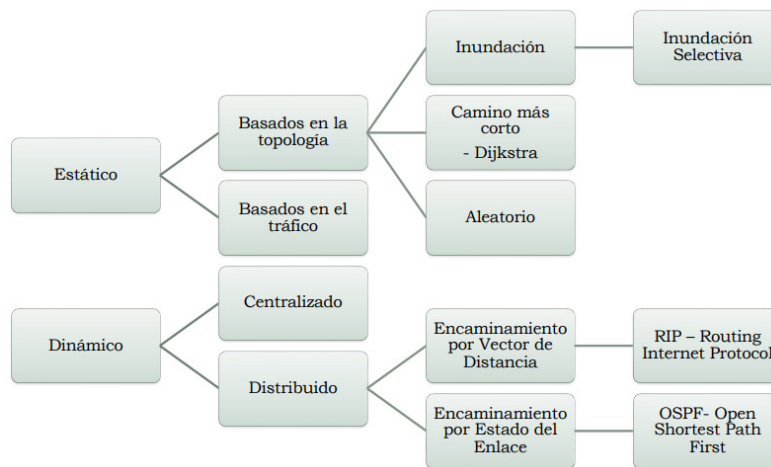
Encaminamiento (o enrutamiento) es la función de buscar un camino entre todos los posibles en una red de paquetes cuyas topologías poseen una gran conectividad

Dado que se trata de encontrar la mejor ruta posible, lo primero será definir qué se entiende por mejor ruta y en consecuencia cuál es la métrica que se debe utilizar para medirla

La base del encaminamiento es el algoritmo que decide el camino a seguir -> algoritmo de encaminamiento

No Adaptables – Estático: Las decisiones de encaminamiento se toman por adelantado

Adaptables – Dinámico: Las decisiones cambian en función del tráfico y de la conectividad de la red



Encaminamiento estático por inundación

Fundamento: cada paquete recibido por una estación se envía al resto de estaciones adyacentes

Con la excepción de la que envió el paquete

Características

Se generan paquetes duplicados

El número de paquetes puede ser infinito sin ningún tipo de control

Es necesario usar una estrategia de control de paquetes duplicados

Estrategias de control de paquetes

Los paquetes llevan un contador con la distancia máxima (diámetro de la red)

Cuando llegan a un nuevo nodo, el contador se decrementa

Los paquetes se desechan cuando el contador llega a cero

Registrar los paquetes enviados

Para evitar enviarlos más una vez

Ventajas

-Se prueban todos los caminos posibles entre el origen y el destino (robustez)

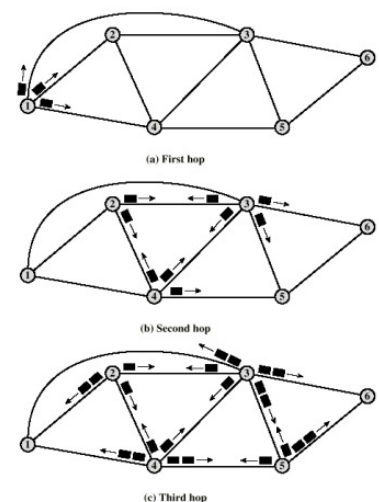
-Al menos una ruta tendrá la longitud mínima

Se puede usar para establecer circuitos virtuales

-Todos los nodos conectados al nodo origen son visitados

Desventaja

-Genera mucho tráfico de mensajes



Encaminamiento estático por camino más corto

Características:

-Las rutas son fijas si no hay cambios en la topología de la red

-En cada nodo existe una tabla que indica la ruta a seguir para que un paquete llegue al nodo destino

El problema a resolver es cómo rellenar las tablas

Manualmente, por el administrador de la red

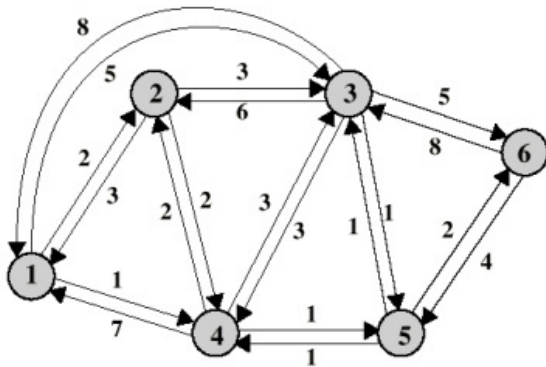
Automáticamente, mediante algún algoritmo

Algoritmo de Bellman-Ford

Algoritmo de Dijkstra

Algoritmos de encaminamiento

Encaminamiento estático



CENTRAL ROUTING DIRECTORY

		From Node					
		1	2	3	4	5	6
To Node	1	—	1	5	2	4	5
	2	2	—	5	2	4	5
	3	4	3	—	5	3	5
	4	4	4	5	—	4	5
	5	4	4	5	5	—	5
	6	4	4	5	5	6	—

Node 1 Directory			Node 2 Directory			Node 3 Directory		
Destination	Next Node		Destination	Next Node		Destination	Next Node	
2	2		1	1		1	5	
3	4		3	3		2	5	
4	4		4	4		4	5	
5	4		5	4		5	5	
6	4		6	4		6	5	

Node 4 Directory			Node 5 Directory			Node 6 Directory		
Destination	Next Node		Destination	Next Node		Destination	Next Node	
1	2		1	4		1	5	
2	2		2	4		2	5	
3	5		3	3		3	5	
5	5		4	4		4	5	
6	5		6	6		5	5	

Encaminamiento aleatorio

Característica principal:

Quando un paquete llega a un nodo, éste elige un camino de forma aleatoria

Se excluye el camino por el que llegó el paquete

Se pueden asignar probabilidades a los caminos (por ejemplo, dependiendo de la velocidad de transmisión)

Ventajas

No necesita información sobre la red

Algoritmo simple

Tráfico inferior al algoritmo de inundación, pero mayor que el óptimo

Algoritmos de encaminamiento dinámicos y distribuidos

Las decisiones cambian en función del tráfico y de la conectividad de la red

La información utilizada por cada nodo para decidir el encaminamiento proviene de otros nodos de la red

Los nodos se intercambian información de encaminamiento

Dos estrategias principales:

Encaminamiento por Vector Distancia (Bellman-Ford)

Envía información sólo a nodos adyacentes

Encaminamiento por Estado del Enlace (Dijkstra)

La información de un nodo llega a todos los nodos de la red

Protocolos de encaminamiento dinámico

Encaminamiento basado en el vector de distancia:

El camino de menor coste es el camino de mínima distancia

Cada nodo mantiene un vector (tabla) de las distancias mínimas a cada nodo

Cada nodo tiene conocimiento de toda la red

Envía información sólo a nodos adyacentes

Comparte información a intervalos regulares

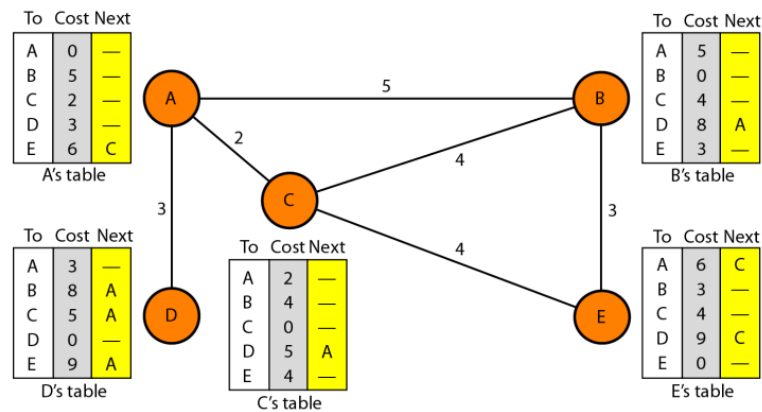
Se asume un coste en cada enlace (de una unidad en la mayoría de los casos)

Tablas de Encaminamiento

Estructura

Identificador de nodo	Coste	Siguiente salto
-----------------------	-------	-----------------

Ejemplo de Encaminamiento basado en el vector de distancia



```

1. Distance_Vector_Routing ( )
2. {
3.     // Initialize (create initial vectors for the node)
4.     D[myself] = 0
5.     for (y = 1 to N)
6.     {
7.         if (y is a neighbor)
8.             D[y] = c[myself][y]
9.         else
10.            D[y] = ∞
11.     }
12.     send vector {D[1], D[2], ..., D[N]} to all neighbors
13.     // Update (improve the vector with the vector received from a neighbor)
14.     repeat (forever)
15.     {
16.         wait (for a vector Dw from a neighbor w or any change in the link)
17.         for (y = 1 to N)
18.         {
19.             D[y] = min [D[y], (c[myself][w] + Dw[y])] // Bellman-Ford equation
20.         }
21.         if (any change in the vector)
22.             send vector {D[1], D[2], ..., D[N]} to all neighbors
23.     }
24. } // End of Distance Vector

```

Encaminamiento basado en el estado del enlace

Para la construcción local de las tablas de encaminamiento, cada nodo recibe información del resto de nodos de la red.

Cada nodo difunde información acerca del estado de sus enlaces

->paquete de estado del enlace (LSP – Link State Packet)

Diseminación de los LSP por inundación

Con los paquetes LSP se conoce la topología de la red

Formación del árbol de camino más corto para cada nodo

Cálculo de una tabla de encaminamiento basado en el árbol de camino más corto

El nodo que crea el paquete envía una copia por cada interfaz de salida

Un nodo que recibe el paquete lo compara con la copia que tiene

Si el nuevo paquete LSP es más viejo (por el nº de secuencia) lo descarta

Si es más nuevo

Descarta el viejo paquete y almacena el nuevo

Envía una copia por cada interfaz excepto por la que llegó

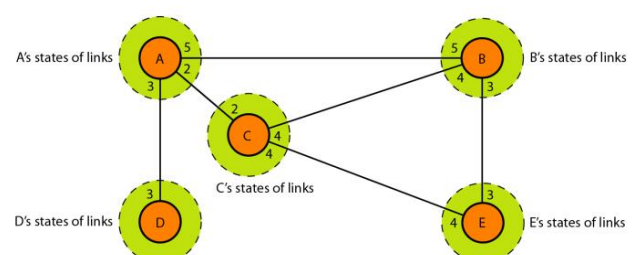
Un LSP transporta

Identidad del nodo, lista de enlaces, un nº de secuencia y la edad

Se generan en dos ocasiones

Un cambio en la topología

De forma periódica (rango de 60 minutos a 2 horas)

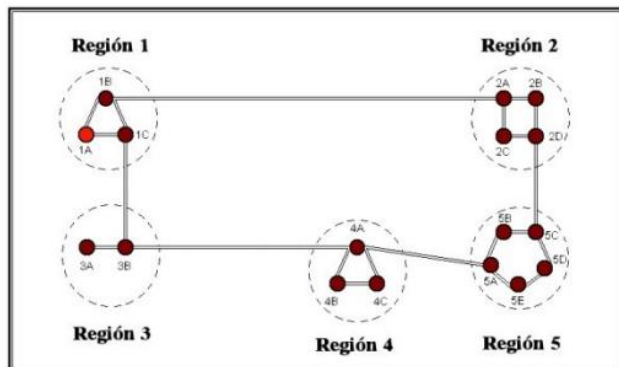


Encaminamiento Jerárquico

A medida que crece el tamaño de las redes, las tablas de encaminamiento crecen proporcionalmente

Aumenta el consumo de memoria y CPU para su procesamiento

Llega un momento en que no es viable mantener una entrada para cada nodo de la red



DESTINO	LINEA	SALTOS
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

TABLA DE 1A COMPLETA

Característica principal:

Los nodos se pueden organizar en torno a dominios/regiones y subdominios

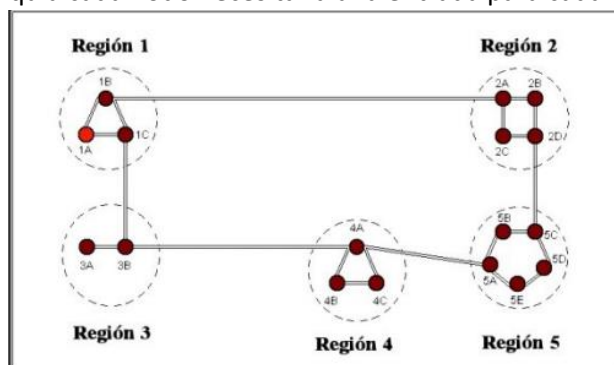
Requiere un sistema de nombres jerárquico. Id. Dominio/id. host

Cada nodo tiene una tabla de encaminamiento

Especifica por qué nodo vecino debe enviar los paquetes destinados a cada uno de los otros M-1 nodos en su mismo dominio, y a cada uno de los K-1 dominios restantes

El tamaño de la tabla con encaminamiento jerárquico es $(M-1) + (K-1)$

Sin la jerarquía cada nodo necesitaría una entrada para cada uno de los N-1 nodos restantes



DESTINO	LINEA	SALTOS
1A	-	-
1B	1B	1
1C	1C	1
R. 2	1B	2
R. 3	1C	2
R. 4	1C	3
R. 5	1C	4

TABLA DE 1A JERÁRQUICA

DESTINO	LINEA	SALTOS
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

TABLA DE 1A COMPLETA

Ejemplo: – Si $M=K=100$, la tabla de encaminamiento en cada nodo tendría:

Jerárquico -> 198

No Jerárquico -> 9.999 entradas

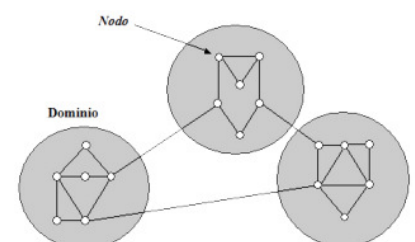
Siendo N = número de nodos K = número de dominios M = número de nodos por dominio $N=K \cdot M$

Ventaja

-Los nodos no tienen que conocer diferentes caminos a localizaciones remotas individuales

-En su lugar los nodos se agrupan en dominios y un nodo sólo necesita saber el nodo al cual debe enviar los próximos paquetes destinados a un dominio remoto

Este es el encaminamiento que se utiliza en Internet (protocolo IP)



Protocolos de encaminamiento dinámico en Internet

La tabla de encaminamiento IP puede actualizarse manualmente

- No es posible adaptarse a las condiciones cambiantes de la red: topología y tráfico
- Es recomendable utilizar un protocolo de encaminamiento que se encargue de actualizar las tablas de encaminamiento de forma dinámica

Protocolos de encaminamiento:

Facilitan el intercambio de información de encaminamiento entre routers (dispositivos de encaminamiento)

Un router tiene acceso a varias redes

Esta información se expresa en términos de qué redes son accesibles a través de qué routers

Cuando hay varias posibilidades, las decisiones de encaminamiento tratan de OPTIMIZAR

Para optimizar, se asigna un COSTE de pasar a través de una red -> MÉTRICA

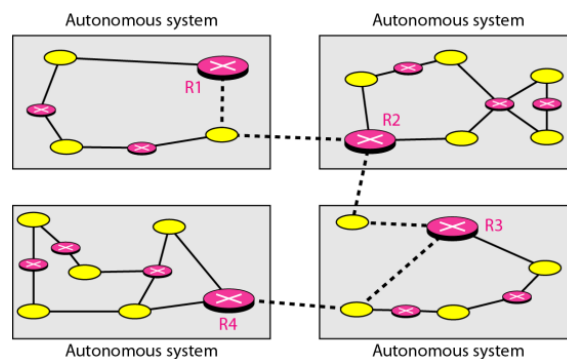
Cada protocolo de encaminamiento define su propia métrica.

Internet se divide en SISTEMAS AUTÓNOMOS

Un sistema autónomo (AS) es un grupo de redes y dispositivos de encaminamiento bajo una autoridad común

Excepto en momento de fallos, un AS está conectado

Existe un camino entre cualquier par de nodos



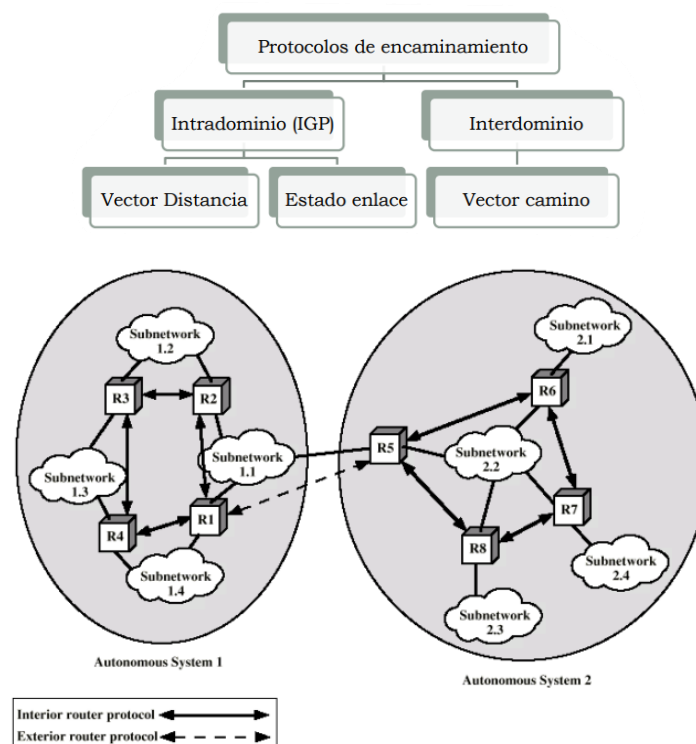
El encaminamiento dentro de un sistema autónomo se conoce como encaminamiento INTRADOMINIO

Cada AS puede elegir uno o más protocolos para determinar el encaminamiento dentro del AS

También denominados Interior Gateway Protocols (IGP)

El encaminamiento entre sistemas autónomos se conoce como encaminamiento INTERDOMINIO

Sólo un protocolo gestiona el encaminamiento interdominio



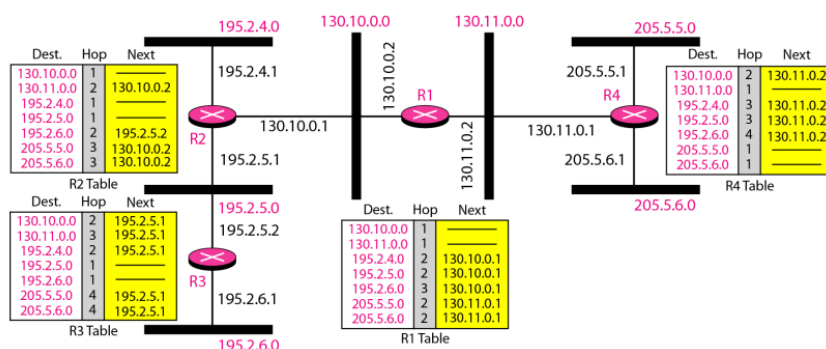
Protocolo de encaminamiento intradominio: RIP

Protocolo de Información de Encaminamiento (Routing Information Protocol, RIP)

Protocolo de encaminamiento intradominio (RFC 1058)

Se basa en el encaminamiento basado en el vector de distancia

- RIP agrega la columna “métrica” a la tabla de encaminamiento
- La métrica empleada es el número de saltos que hay entre el router origen y la subred destino:
- El infinito (∞) se define como 16 – Cualquier camino no puede tener más de 15 saltos
- Cada router difunde su vector de distancias cada 30 segundos a los routers vecinos.
- El vector distancia contiene una lista de hasta 25 subredes de destino pertenecientes al AS, así como la distancia desde el router emisor a cada una de esas subredes
- Si un router no recibe ningún mensaje en 180 segundos considera que el enlace/nodo ha caído.



Ejemplo

Sea un aparte de un sistema autónomo

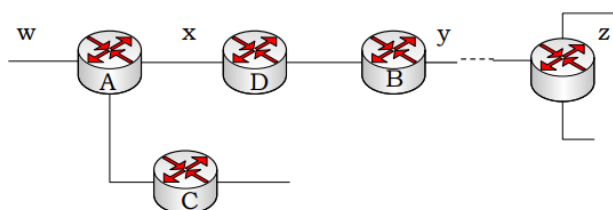


Tabla de encaminamiento de D antes de recibir un anuncio del router A

Subred de destino	Nº de saltos hasta el destino	Siguiente router
w	2	A
y	2	B
z	7	B
x	1	-

30 segundos más tarde, D recibe el siguiente anuncio de A

Subred de destino	Nº de saltos hasta el destino
w	1
y	3
z	4
x	1

Ruta más corta

D actualiza su tabla para tener en cuenta la nueva ruta más corta de encaminamiento

Subred de destino	Nº de saltos hasta el destino	Siguiente router
w	2	A
y	2	B
z	5	A
x	1	-

Protocolo de encaminamiento interdominio: BGP

Protocolo de Pasarela Frontera (BGP –Border Gateway Protocol)

- Permite el intercambio de información entre pasarelas (dispositivos de encaminamiento) de SA diferentes (RFC1771)
- Opera en términos de mensajes que se envían utilizando conexiones TCP -> sesiones BGP
- Utiliza el encaminamiento basado en el vector camino
 - Pasarelas vecinas de diferentes AS se intercambian información
 - Dos pasarelas son vecinas si están conectadas a la misma subred

3. LA SIGUIENTE GENERACIÓN DE IP

Estado Actual de Internet

Internet a día de hoy y cómo puede evolucionar en un futuro próximo (Informe de Morgan Stanley, mayo 2010)
 Cinco Países tienen el 48% de los usuarios de internet (China e India motores del crecimiento futuro)

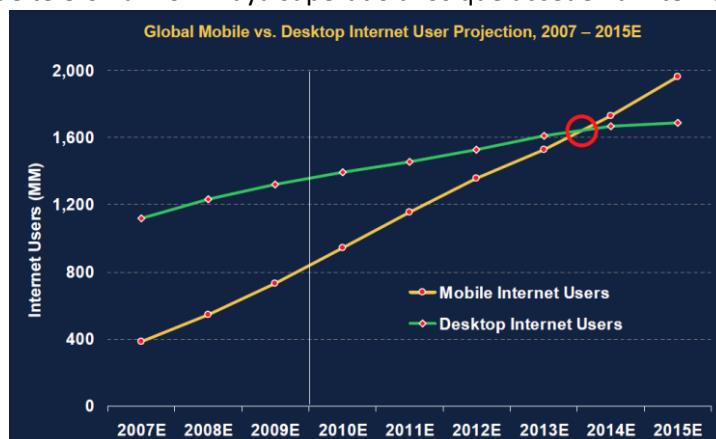
- EEUU: 238 M usuarios, crecimiento anual del 4%.
- Brasil: 67M usuarios, crecimiento anual del +14%
- Rusia: 39M usuarios, crecimiento anual del +13%
- China: 384M usuarios, crecimiento anual del +29%
- India: 130M usuarios, crecimiento anual del +23%.

Internet Móvil

Todo apunta a que la principal herramienta de conexión a Internet serán dispositivos móviles

El crecimiento del acceso a internet desde dispositivos móviles está siendo vertiginoso

Se espera que a finales del año 2013, el número de usuarios que acceden a internet desde un dispositivo de telefonía móvil haya superado a los que acceden a internet desde un PC.



3.1. Problemática del crecimiento del Internet

A principios de 2010, quedaban menos del 10% de IPs sin asignar. En la semana del 3 de febrero del 2011, la IANA (Agencia Internacional de Asignación de Números de Internet, por sus siglas en inglés) entregó el último bloque de direcciones disponibles (33 millones) a la organización encargada de asignar IPs en Asia, un mercado que está en auge y no tardará en consumirlas todas.

IPv4 posibilita 4.294.967.296 (2^{32}) direcciones de red diferentes, un número inadecuado para dar una dirección a cada persona del planeta, y mucho menos a cada vehículo, teléfono, tablet, etcétera.

Agotamiento total de direcciones IP

Agotamiento de direcciones IP de clase B (medianas)

Explosión en las tablas de encaminamiento en los routers frontera

Soluciones

A corto plazo

Fomento del uso de subredes

Encaminamiento sin clases – VLSM – CIDR

NAT

A largo plazo (grupo de trabajo IPnG)

IPv6

Protocolos de resolución de direcciones – NAT

Problema a resolver:

las direcciones IPv4 son insuficientes hoy día

Ejemplos:

- Una empresa tiene asignada un conjunto de IPs < IPs que necesita
- Un ISP – Internet Service Provider – puede tener asignada una dirección de tipo B, pero podría tener más de 65535 clientes
- En las casas es habitual tener varios ordenadores y tener contratada una sola línea ADSL

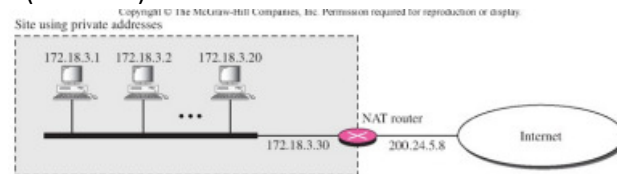
NAT (RFC 3022) Network Address Translation - es una solución para resolver estas cuestiones

Idea básica:

Dentro de la entidad (ej: empresa), cada ordenador tiene una IP única privada

Cuando un paquete sale de la entidad hacia Internet, se lleva a cabo un proceso de traducción a una IP global (pública)

Hace uso de direcciones privadas (o locales)



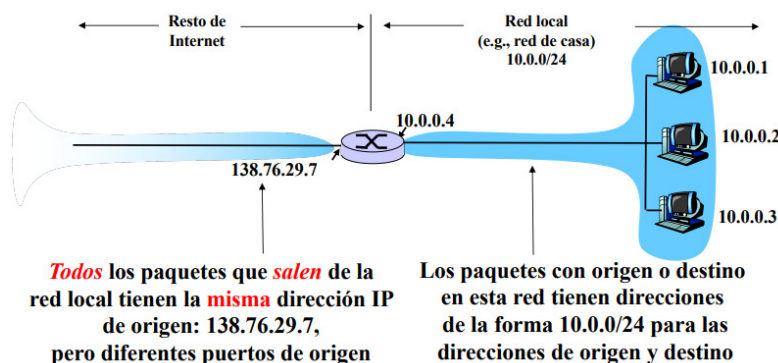
Se denominan redes privadas:

Rango	Total
10.0.0.0 a 10.255.255.255	2^{24}
172.16.0.0 a 172.31.255.255	2^{20}
192.168.0.0 a 192.168.255.255	2^{16}

Son únicas dentro de una organización

Ningún router reenvía al exterior un paquete con direcciones origen privadas

Esquema de funcionamiento



Cuestión a resolver

Número de equipos con acceso a Internet > IPs globales disponibles

Escenario doméstico: 1 IP global del ISP y varios equipos conectados (ej: portátiles, teléfonos móviles, etc.)

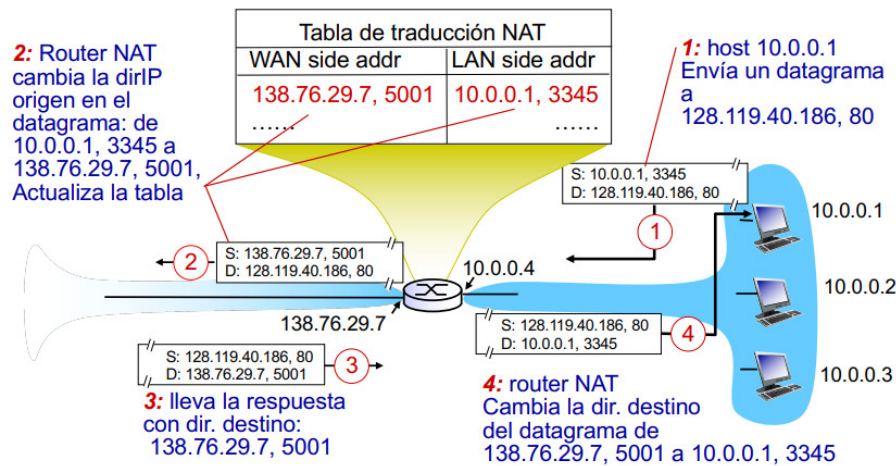
Cuando se recibe una IP global, ¿cómo se sabe a qué máquina local enviarla?

Solución adoptada

NAPT (network address and port translation)

Los protocolos TCP y UDP tienen un campo de puerto origen

Al enviar, ese campo se reemplaza por un índice en una tabla que contiene el par (IP, puerto) original



Críticas al esquema NAT

- Viola la arquitectura de IP: hay máquinas con direcciones iguales
- Si falla el sistema NAT, todas las conexiones TCP se rompen
- Viola el modelo de capas: Si se modifica TCP o UDP, la solución NAT puede no funcionar
- No funciona si se utilizan protocolos diferentes de TCP y UDP a nivel de transporte

IPv6

El Internet Protocol versión 6 (IPv6) (en español: Protocolo de Internet versión 6) definida en el RFC 2460 y diseñada para reemplazar a IPv4

En cambio, IPv6 admite 340.282.366.920.938.463.463.374.607.431.768.211.456 (2128 o 340 sextillones de direcciones)-cerca de $6,7 \times 10^{17}$ (670 mil billones) de direcciones por cada milímetro cuadrado de la superficie de La Tierra.

Otra vía para la implantación del protocolo es la adopción de éste por parte de instituciones.

El gobierno de los Estados Unidos ordenó el despliegue de IPv6 por todas sus agencias federales en el año 2008.

Lanzamiento mundial de IPv6 (6/6/2012): <http://www.worldipv6launch.org/>

La mayoría de los protocolos de transporte -y aplicaciónnecesitan pocos o ningún cambio para operar sobre IPv6; las excepciones son los protocolos de aplicación que integran direcciones de capa de red, como FTP o NTPv3, NTPv4.

IPv6 especifica un nuevo formato de paquete, diseñado para minimizar el procesamiento del encabezado de paquetes.

Debido a que las cabeceras de los paquetes IPv4 e IPv6 son significativamente distintas, los dos protocolos no son interoperables.

Algunos de los cambios de IPv4 a IPv6 más relevantes son:

- Capacidad extendida de direccionamiento
- Multicast extendido
 - Desaparece el broadcast
- Se define un nuevo tipo de dirección -> Anycast
- Soporte mejorado para las extensiones y opciones
- Procesamiento simplificado en los routers
 - Paquete más simple, no hay checksum, etc.
- Autoconfiguración
 - Mensajes de descubrimiento de routers ICMPv6
- Seguridad de Nivel de Red obligatoria
 - Internet Protocol Security (IPsec)
- Movilidad
 - Al desplazarse se le asigna una segunda dirección (CoA, Care of Address), aparte de la asignada por su ISP (HoA, Home of Address)

Notación de Direcciones IPv6

Ejemplo de una dirección (128 bits o 16 bytes)

1080:0000:0000 :0000:0008:0198: FE1C:418A

 1080: 0 : 0 : 0 : 8 : 198: FE1C:418A
 1080::8:198: FE1C:418A

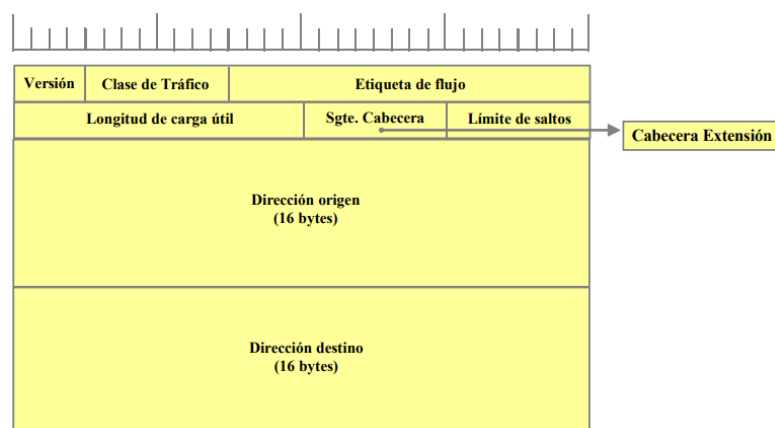
Solamente puede ponerse un :: en una dirección para evitar ambigüedad

Direcciones IPv6 reservadas

Dirección IPv6	Longitud del Prefijo (Bits)	Descripción	Notas
::	128 bits	sin especificar	como 0.0.0.0 en Pv4
::1	128 bits	dirección de bucle local (loopback)	equivalentes a la dirección de loopback de IPv4
::ffff:xx:xx:xx:xx	96 bits	direcciones IPv6 mapeadas a IPv4	Los 32 bits más bajos contienen una dirección IPv4. Se usan para representar direcciones IPv4 mediante direcciones IPv6.
ff01:: o ff02::	8 bits	Multicast reservadas	Sustituyen a las direcciones de broadcast y multicast de IPv4 (ej: todos los nodos, todos los routers, etc.)

Codificación de direcciones IPv4 (32 bits) 0:0:0:0:0:A00:1 ó ::10.0.0.1 y la correspondiente dir. ipv6 ::FFFF:10.0.0.1

Cabecera IPv6



Hop-by-hop

Encaminamiento

Fragmentación

Autenticidad

Datos cifrados

Opciones de destino

Cabecera IPv6 Sgte. Cab. = TCP	Cabecera TCP	Datos ...
--------------------------------------	--------------	--------------

Cabecera IPv6 Sgte. Cab. = Encaminamiento	Cabecera Encaminamiento Sgte. Cab. = TCP	Cabecera TCP	Datos ...
---	--	--------------	--------------

Más simple: 6 campos y 2 direcciones en vez de 10 campos, 2 direcciones y algunas opciones

Cabecera de tamaño fijo

Se eliminó el campo checksum

Se eliminó la fragmentación de paquetes en los routers intermedios

Redefinición de campos clásicos: Longitud de la cabecera y TTL

Nuevos campos 'clase' y 'etiqueta de flujo'

Direcciones IPv6

Tres tipos de direcciones: unicast, anycast y multicast.:

Una dirección unicast identifica un único interface de red

Una dirección anycast es asignada a un grupo de interfaces, normalmente de nodos diferentes.

- Un paquete enviado a una dirección anycast se entrega únicamente a uno de los miembros, típicamente el host con menos coste, según la definición de métrica del protocolo de encaminamiento.
- Las direcciones anycast tienen el mismo formato que las unicast, diferenciándose únicamente por estar presente en varios puntos de la red.

Una dirección multicast también es usada por múltiples hosts, que consiguen la dirección multicast participando en el protocolo de multidifusión (multicast) entre los routers de red.

Un paquete enviado a una dirección multicast es entregado a todos los interfaces que se hayan unido al grupo multicast correspondiente.

IPv6 no implementa direcciones broadcast.

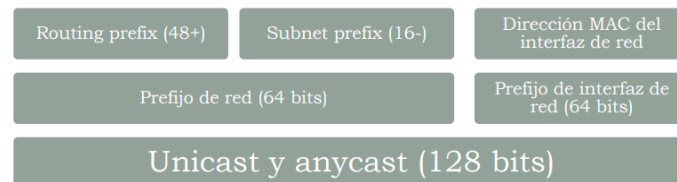
El mismo efecto puede lograrse enviando un paquete al grupo de multicast de enlace-local todos los nodos (all-nodes) ff02::1.

Formato direcciones IPv6 unicast y anycast

Se dividen en 2 grupos lógicos:

Prefijo de red se usa para el encaminamiento (network prefix – routing prefix) junto con el prefijo de subred (subnet prefix)

Los 64 bits del identificador de interfaz (interface identifier) se generan automáticamente con la dirección MAC o DHCP6



Direcciones multicast

Se construyen en función de su aplicación.

Comienzan por un prefijo binario de 8 bits a 1

IPv6 no implementa direcciones broadcast.

El mismo efecto puede lograrse enviando un paquete al grupo de multicast de enlace-local todos los nodos (allnodes) ff02::1.



IPv6

Autoconfiguración de direcciones libres de estado:

Los nodos IPv6 pueden configurarse a sí mismos automáticamente cuando son conectados a una red IPv6 usando los mensajes de descubrimiento de routers de ICMPv6.

La primera vez que son conectados a una red, el nodo envía una solicitud de router de link-local usando multicast (router solicitud) pidiendo los parámetros de configuración; y si los routers están configurados para esto, responderán este requerimiento con un "anuncio de router" (router advertisement) que contiene los parámetros de configuración de capa de red.

Si la autoconfiguración de direcciones libres de estado no es adecuada para una aplicación, es posible utilizar Dynamic Host Configuration Protocol para IPv6 (DHCPv6) o bien los nodos pueden ser configurados en forma estática.

Multicast:

Multicast, la habilidad de enviar un paquete único a destinos múltiples es parte de la especificación base de IPv6. Esto es diferente a IPv4, donde es opcional).

IPv6 no implementa broadcast, que es la habilidad de enviar un paquete a todos los nodos del enlace conectado.

El mismo efecto puede lograrse enviando un paquete al grupo de multicast de enlace-local todos los nodos (all hosts). Por lo tanto, no existe el concepto de una dirección de broadcast y así la dirección más alta de la red (la dirección de broadcast en una red IPv4) es considerada una dirección normal en IPv6.

Seguridad de Nivel de Red obligatoria:

Internet Protocol Security (IPsec), el protocolo para cifrado y autenticación IP forma parte integral del protocolo base en IPv6.

Procesamiento simplificado en los routers:

Las simplificaciones hechas en la cabecera de los paquetes, así como en el proceso de reenvío de paquetes hace el procesamiento de los paquetes más simple y por ello más eficiente.

- El encabezado del paquete en IPv6 es más simple que el utilizado en IPv4, así los campos que son raramente utilizados han sido movidos a opciones separadas; en efecto, aunque las direcciones en IPv6 son 4 veces más largas, el encabezado IPv6 (sin opciones) es solamente el doble de largo que el encabezado IPv4 (sin opciones).
- Los routers IPv6 no hacen fragmentación.
- No hay suma de comprobación (checksum) en la cabecera.

Movilidad:

A diferencia de IPv4 móvil, IPv6 móvil (MIPv6) evita el ruteo triangular y por lo tanto es tan eficiente como el IPv6 normal. Sin embargo, ni MIPv6 ni MIPv4 son ampliamente difundidos hoy, por lo que esta ventaja es más bien teórica.

Soporte mejorado para las extensiones y opciones:

Los cambios en la manera en que se codifican las opciones de la cabecera IP permiten límites menos rigurosos en la longitud de opciones, y mayor flexibilidad para introducir nuevas opciones en el futuro.

Jumbogramas:

IPv4 limita los paquetes a 64 KiB de carga útil.

IPv6 tiene soporte opcional para que los paquetes puedan superar este límite, los llamados jumbogramas, que pueden ser de hasta 4 GB. El uso de jumbogramas puede mejorar mucho la eficiencia en redes de altos MTU.