Redes

Tema 4: Capa de red

José Carlos Cabaleiro Domínguez

Escola Técnica Superior de Enxeñería

Índice

- Introducción
- Redes de conmutación de paquetes
- Algoritmos de encaminamiento
- Encaminamiento en Internet
- Protocolo de Internet
- 6 ICMP: Protocolo de mensajes de control de Internet
- DHCP: Protocolo de configuración dinámica de hosts
- 8 NAT: Traducción de direcciones de red



Índice

Intro

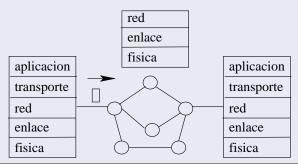
- Introducción
- 2 Redes de conmutación de paquetes
- 3 Algoritmos de encaminamiento
- 4 Encaminamiento en Internet
- Protocolo de Internet
- 6 ICMP: Protocolo de mensajes de control de Internet
- 7 DHCP: Protocolo de configuración dinámica de hosts
- 8 NAT: Traducción de direcciones de rec



Introducción

Capa de red

- Se encarga de llevar los paquetes que le pasa la capa de transporte del host origen al host destino
- Implementada tanto en los sistemas finales como en los routers



Introducción

Intro

Conceptos

- Reenvío (forwarding)
 - Cuando llega un paquete a un router, el router hace pasar el paquete a la interfaz de salida apropiada
- Encaminamiento o rutado (routing)
 - Determinar la ruta que debe seguir un paquete que se envía desde un emisor a un receptor
 - Algoritmos de encaminamiento
- Tablas de reenvío
 - Tablas que almacenan la información necesaria para el reenvío de paquetes
 - Asigna el valor del campo de la cabecera a la interfaz de salida apropiada
 - Los algoritmos de encaminamiento determinan los valores de las tablas de reenvío

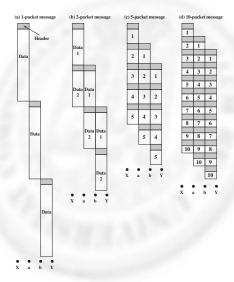


Índice

- Introducción
- Redes de conmutación de paquetes
- Algoritmos de encaminamiento
- 4 Encaminamiento en Internet
- 5 Protocolo de Internet
- 6 ICMP: Protocolo de mensajes de control de Internet
- 7 DHCP: Protocolo de configuración dinámica de hosts
- 8 NAT: Traducción de direcciones de rec



Redes de conmutación de paquetes





Redes de conmutación de paquetes

Redes de datagramas

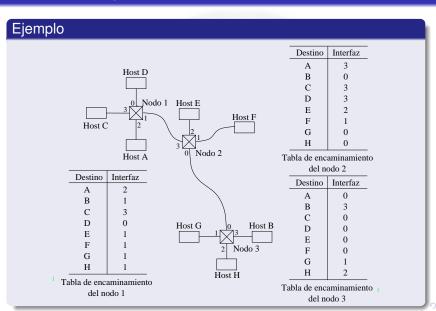
- Cada paquete incluye en la cabecera la IP destino
- Reenvío: el router examina la cabecera y lo coloca en la salida más apropiada (tabla de reenvío)
- No mantienen información de estado: una secuencia de paquetes se encaminan de forma independiente

Redes de circuitos virtuales

- Se establece la conexión planificando una ruta al destino: un circuito virtual (CV)
- A cada paquete se le escribe el identificador de CV: los routers lo usan para el reenvío
- Los routers mantienen información de estado (tabla de circuitos virtuales)

Com. paquetes ocioco Encaminamiento Enc. en Internet ocioco de Internet ICMP DHCP NAT ocioco de Internet ocioco de Internet ICMP DHCP NAT ocioco de Internet ocioco

Redes de datagramas



Introducción

Capa de red en Internet: IP

- Tipo datagrama: se encaminan los paquetes en función de la dirección destino que contienen
- Sin estado: cada paquete se trata de forma independiente
- Red no fiable: servicio de mejor esfuerzo.
 - No se garantiza la entrega de paquetes (ni el orden)
 - Ni la entrega en un tiempo determinado
 - Entrega el mayor número de paquetes, aunque algunos se pierdan
- Permite la interconexión de redes de diferentes tecnologías (interred)



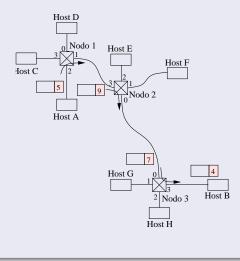
Redes de circuitos virtuales

Tabla de circuitos virtuales

- Cada nodo mantiene una tabla de encaminamiento con la siguiente información:
 - Interfaz de entrada del circuito virtual
 - Identificador del circuito virtual VCI
 - Interfaz de salida por la que los paquetes de ese circuito virtual dejan el nodo
 - Identificador de salida del circuito virtual
- Un paquete que llega por una interfaz con un VCI, se coloca en la interfaz indicada en la tabla con el nuevo VCI

Redes de circuitos virtuales





Nodo 1				
Entra	da	Salida		
Interfaz	VCI	Interfaz	VCI	
2	5	1	9	

Nodo 2			
Entra	da	Sali	da
Interfaz	VCI	Interfaz	VCI
3	9	0	7
•	•		

Nodo 3			
Entrada		Salida	
Interfaz	VCI	Interfaz	VCI
0	7	3	4
•	•		

Redes de circuitos virtuales

Construcción de la tabla de VC

- A envía una Petición de llamada dirigida a B
- Esta llega al nodo 1 por la interfaz 2, que debe saber como reenviarla para que llegue a B (similar a datagramas)
- El nodo 1 decide marcar esta petición con un VCI de 5 (aleatorio), y la envía por la interfaz 1
- 2 lo recibe, lo marca con VCI 9 y lo coloca en la interfaz 0;
 3 lo marca con VCI 7 y lo coloca en 3; y B lo marca con VCI 4, que identificará los paquetes de A
- B devuelve una Llamada aceptada con VCI 4 al nodo 3 por el interfaz 3
- El nodo 3 puede completar su entrada en la tabla (VCI salida = 4); lo mismo los nodos 2 y 1
- 1 manda el ACK a A que lo recibe con VCI 5
 - ⇒ A marca el resto de paquetes a B con VCI 5

Índice

- Introducción
- Redes de conmutación de paquetes
- 3 Algoritmos de encaminamiento
- 4 Encaminamiento en Internet
- Protocolo de Internet
- 6 ICMP: Protocolo de mensajes de control de Internet
- 7 DHCP: Protocolo de configuración dinámica de hosts
- 8 NAT: Traducción de direcciones de red



Algoritmos de encaminamiento

Conceptos

- Algoritmo de encaminamiento o rutado: el encargado de encontrar el camino mínimo entre el origen y destino
 - Cada host está conectado a un router (router por defecto)
 - El problema se limita a encontrar el camino mínimo entre routers
- Equivalente a encontrar el camino mínimo en un grafo
 - Routers: nodos del grafo
 - Enlaces: aristas del grafo
 - Se les asigna un peso (coste)
 - Coste: distancia, velocidad, carga del enlace, coste económico, etc.

Algoritmos de encaminamiento

Clasificación

- Globales. De estado de los enlaces
 - Cada nodo dispone de toda la información sobre la red: todos los nodos y el coste de todos los enlaces
 - A partir de esta información, cada nodo puede calcular su tabla de encaminamiento (o de rutas)
- Descentralizados. De vector de distancias
 - El cálculo de los caminos mínimos se hace en colaboración de todos los nodos
 - Los nodos intercambian información sólo con sus vecinos
 - Solo conocen la distancia a los demás nodos y por dónde empezar

Algoritmos de encaminamiento

Clasificación

- Estáticos o dinámicos
 - Estáticos: solo cambian cuando cambia la topología de red o se modifican manualmente parámetros
 - Dinámicos: se ejecutan periódicamente de forma automática. Los usados actualmente en Internet
- Sensibles o insensibles a la carga
 - Sensibles: el coste de los enlaces varía dinámicamente
 - Pueden provocar que los mensajes queden atrapados en un ciclo
 - En Internet son insensibles a la carga

Encaminamiento de estado de los enlaces

Algoritmo de Dijkstra (1959)

- Busca el camino más corto entre dos vértices de un grafo pesado
- Variante del algoritmo, forward search:
 - El nodo N quiere calcular su tabla de routing a partir de los LSP (link state packet) que ha recibido
 - Cada nodo tiene 2 listas: Confirmado y Provisional
 - Cada elemento de las listas indican el coste para alcanzar un nodo y el siguiente salto
 - (M, 5, L), indica que de N se alcanza M a coste 5 a través de l
 - Inicializa la tabla Confirmado con una entrada para N con coste 0 ((N, 0, -))
 - Sigue el siguiente algoritmo:



Encaminamiento de estado de los enlaces

Algoritmo de Dijkstra

- Para el último nodo añadido a Confirmado (nodo S) examina su LSP
- 2 Para cada vecino (V) de S, calcula el coste (Coste) para alcanzar V como la suma del coste de N a S y de S a V
 - Si v no está en ninguna lista, añádelo a la lista Provisional de la forma (V, Cost, SigSalto)
 - Si V está en Provisional, y Coste es menor que el indicado, reemplázalo por (V, Cost, SigSalto)
- Si Provisional está vacía, acaba; si no pasa la entrada de Provisional con menor coste a Confirmado
- Vuelve al paso 1

Com. paquetes Encaminamiento ocooco O

Encaminamiento de estado de los enlaces

Algoritmo de Dijkstra



Destino	Coste	SigSalto
A	10	С
В	5	С
С	2	С

Tabla de routing del nodo D

Paso	Confirmado	Provisional	Comentarios
1	(D,0,-)		D es el único elemento inicial de Confirmado
2	(D,0,-)	(B,11,B) (C,2,C)	El LSP de D dice que puede alcanzar B a coste 11, y C a coste 2. Lo pone en Provisional .
3	(D,0,-) (C,2,C)	(B,11,B)	Pasa el miembro de Provisional con menor coste (C) a Confirmado , y examina su LSP.
4	(D,0,-; (C,2,C)	(B,5,C) (A,12,C)	El coste de alcanzar B a través de C es 5, asi que reemplaza (B,11,B) por (B,5,C). El LSP de C indica qu puede alcanzar A con coste 10+ 2 a través de C.
5	(D,0,-; (C,2,C) (B,5,C)	(A,12,C)	Pasa el miembro de Provisional con menor coste (B) a Confirmado , y examina su LSP.
6	(D,0,-) (C,2,C) (B,5,C)	(A,10,C)	El LSP de B dice que puede alcanzar A a coste 5, así que cambia (A,12,C) por (A,10,C) (el coste D–B es 5 a través de C)
7	(D,0,-) (C,2,C) (B,5,C) (A,10,C)		Pasa el miembro de Provisional con menor coste (A) a Confirmado , y ya está.

Encaminamiento de estado de los enlaces

Complejidad algorítmica del algoritmo de Dijkstra

Complejidad cuadrática, O(n²)

Ventajas

- Se estabiliza rápidamente
- No genera mucho tráfico
- Responde rápidamente a cambios en la topología o fallos de nodos

Inconvenientes

- La cantidad de información (LSPs) almacenada en cada nodo puede ser bastante grande ⇒
 - Problemas de escalabilidad



Algoritmo descentralizado

Todos los nodos colaboran

Funcionamiento

- Inicialmente, los nodos solo conocen el coste a sus vecinos
- Iterativamente, los nodos comunican a sus vecinos todo lo que saben
- Los nodos computan distancias a nuevos nodos o actualizan las que tienen con menores valores
- Las actualizaciones continúan hasta que converge
- La información que un nodo z comunica a sus vecinos son las distancias $d_{z,i}$
- Se almacena el vecino que envió dicha información (siguiente salto)

Funcionamiento

Sea el nodo x con un vecino z, cuyo enlace tiene coste $c_{x,z}$, y que z envía $d_{z,y} \Rightarrow$

$$D_{x,y}(z) = c_{x,z} + d_{z,y}$$

distancia de x coste del distancia
a y a través enlace que de z
de la salida z une x con z a y

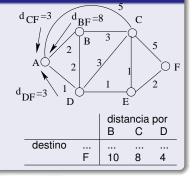
Ejemplo

- Nodos B, C y D envían a A la distancia a F
- A calcula las distancias

$$D_{A,F}(B) = c_{A,B} + d_{B,F} = 2 + 8 = 10$$

 $D_{A,F}(C) = c_{A,C} + d_{C,F} = 5 + 3 = 8$
 $D_{A,F}(D) = c_{A,D} + d_{D,F} = 1 + 3 = 4$

La tabla de distancias para A



Ejemplo

- A comunica a sus vecinos la distancia a F,
 d_{A,F} = min_zD_{A,F}(z) = 4
- Después de ciertas iteraciones, converge

		distancia por		
		В	С	D
destino	В	2	8	3
	С	5	5	3
	D	4	7	1
	Ε	5	6	2
	F	7	8	4

destino	salida
В	В
D	D
С	D
E	D
F	D

Tabla de rutas de A

Tabla de distancias de A



Características

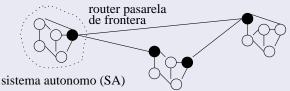
- Intercambio de actualizaciones con los vecinos
 - Periódicamente
 - Cuando un cambio en su tabla o en el coste de un enlace
 - Disminución del coste de un enlace: actualización rápida de las tablas
 - Aumento del coste de un enlace: algunos problemas. Se resuelve con diversas técnicas: horizonte dividido e inverso envenenado
- Iterativo: puede necesitar muchas iteraciones. Peor que EE.
- Menos robusto que EE: si un nodo calcula mal sus distancias, todos usarán esos valores incorrectos



Encaminamiento jerárquico

Sistemas autónomos (SA)

- Regiones en las que se dividen las redes grandes como Internet
- Operados por empresas u organismos
- Los routers solo conocen en encaminamiento en su región
- Routers pasarela frontera: centralizan el tráfico de salida del SA



- Dos niveles de encaminamiento:
 - Intradominio: cada SA puede elegir algoritmo
 - Interdominio: común para todos los SA

Índice

- Introducción
- 2 Redes de conmutación de paquetes
- Algoritmos de encaminamiento
- Encaminamiento en Internet
- Protocolo de Internet
- 6 ICMP: Protocolo de mensajes de control de Internet
- 7 DHCP: Protocolo de configuración dinámica de hosts
- 8 NAT: Traducción de direcciones de rec



Encaminamiento en Internet

Protocolos usados en Internet

- Intradominio o internos al SA (IGP): RIP y OSPF
- Interdominio o entre SAs: BGP

Categoría	Protocolo	Tipo	Protocolos transporte/red
intra-autónomo	RIP	VD	UDP/IP (puerto 520)
	OSPF	EE	propio/IP (puerto 89)
inter-autónomo	BGP	VD	TCP/IP (puerto 179)

• Protocolos de la capa de aplicación

RIP (Routing Information Protocol)

Protocolo de información de encaminamiento

- Encaminamiento intradominio basado en vector de distancias
- Considera que el coste de los enlaces es 1 y distancia máxima 15
- Mensajes RIP solo a los nodos vecinos
 - Mensajes de petición RIP: solicitan información
 - Mensajes de respuesta RIP: lista de hasta 25 redes internas al SA
 - También de forma automática cada 30 s. a sus vecinos. Si no se recibe respuesta en 180 s., se considera caído

OSPF (Open Shortest Path First)

Protocolo abierto de primero el camino más corto

- Abierto: algoritmo libre
- Encaminamiento intradominio basado en estado de los enlaces
- Más avanzado que RIP, pensado para reemplazarlo
- Mensajes OSPF se difunden a todos los nodos
 - Cuando se producen cambios
 - Periódicamente, al menos cada 30 minutos
 - Cada router obtiene información completa del SA
- Mensajes HELLO a cada vecino, para comprobar que el enlace está OK
- Posibilidad de interrogar a un vecino para obtener la toda la información
- El coste de los mensajes los pone el administrador

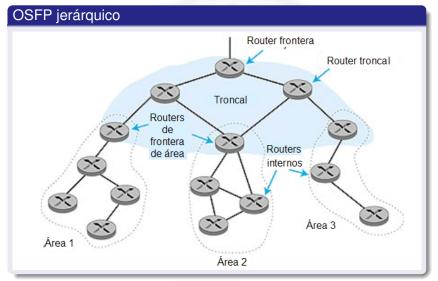
OSPF (Open Shortest Path First)

Protocolo abierto de primero el camino más corto

- Seguridad: implementa un protocolo de transporte propio
 - Con todos los mensajes autentificados
 - Solo considera los routers autenticados
- Múltiples caminos de mismo coste: permite repartir el tráfico
- Soporte de jerarquía: permite subdividir los SA en áreas
 - Cada área ejecuta OSPF sobre los routers de ese área
 - Las áreas se comunican entre sí mediante los routers de frontera de área
 - Paquetes con destino fuera del área se encaminan al router de frontera de área
 - Interconectados entre sí en un área troncal
 - En el SA existe un router de frontera para salir fuera del SA



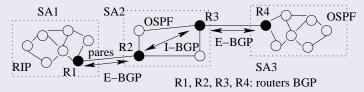
OSPF (Open Shortest Path First)



BGP (Border Gateway Protocol)

Protocolo de pasarela de frontera

- Protocolo interdominio estándar en Internet (BGP4)
- Comunica routers pasarela de frontera



- Cada SA puede usar el protocolo intradominio que desee
- Dos tipos de comunicaciones:
 - Entre routers BGP vecinos, pares BGP. Se usa E-BGP
 - Entre routers del mismo SA, considerados vecinos lógicos.
 Se usa I-BGP

BGP (Border Gateway Protocol)

Protocolo de pasarela de frontera

- Protocolo similar al de vector de distancias, se intercambian rutas completas (vector de rutas)
- Cada SA se identifica por un número de sistema autónomo único
- Los administradores pueden decidir las políticas de encaminamiento

red destino	métrica	
X	4	

red destino	ruta
Х	SA1/SA2/SA3/S4

Ejemplo de mensaje en RIP

Ejemplo de mensaje en BGP



Índice

- 1 Introducción
- Redes de conmutación de paquetes
- 3 Algoritmos de encaminamiento
- Encaminamiento en Internet
- Protocolo de Internet
- 6 ICMP: Protocolo de mensajes de control de Internet
- 7 DHCP: Protocolo de configuración dinámica de hosts
- 8 NAT: Traducción de direcciones de red



IP (Internet Protocol)

Protocolo de Internet

- Protocolo basado en datagramas: servicio sin conexión
- La fiabilidad recae en capas superiores (TCP)
- Diseñado para interconectar redes diferentes

Componentes de la capa de red en Internet

- Protocolo de red: IP
 - Define el formato de las direcciones
 - Formato de los datagramas
 - Acciones de los routers en base a los campos de los datagramas
- Protocolo de encaminamiento
- Protocolo de mensajes de control de Internet (ICMP)



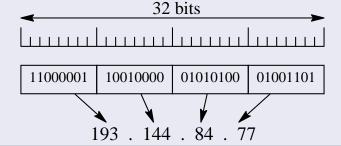
IP (Internet Protocol)

Direccionamiento IPv4

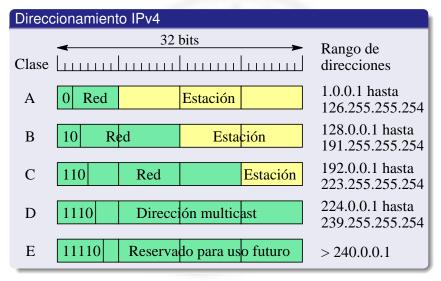
- Los nodos en una red tienen una dirección IP por interfaz
- Interfaz: la unión de un host o router con un enlace

Codificación de la dirección IP

 En IPv4, cada dirección IP se codifica mediante 4 bytes, generalmente escritos en notación decimal



IP (Internet Protocol)



Proporción redes-máquinas

- Restricción: un campo de red o de host no puede estar todo a 1s o todo a 0s
- Según esto tenemos:

Clase A: 126 ($2^7 - 2$) redes con \approx 16 millones de estaciones cada una ($2^{24} - 2 = 16777214$)

Clase B: $16384 (2^{14})$ redes con $65534 (2^{16} - 2)$

estaciones cada una

Clase C: \approx 2 millones de redes ($2^{21} = 2097152$) con

254 estaciones cada una $(2^8 - 2)$

Direcciones especiales reservadas

- Identificación de redes: el nº de red y el resto a 0
- Ejemplos:
 - Clase A → 10.0.0.0
 - $\bullet \ \, \text{Clase B} \rightarrow 172.16.0.0$
 - Clase C → 193.144.84.0
- Dirección de broadcast: el nº de red y el resto a 1
- Ejemplos:
 - Clase A → 10.255.255.255
 - Clase B → 172.16.255.255
 - Clase C → 193.144.84.255

Direcciones especiales reservadas

- Algunas direcciones reservadas por el IANA:
 - 0.0.0.0 → Esta red. Para arrancar sistemas sin disco (protocolo DHCP, también encaminamiento por defecto)
 - 127.0.0.0–127.255.255.255 \rightarrow la propia estación (dirección de *loopback*), se suele usar la 127.0.0.1
 - 240.0.0.0–255.255.255.254 → reservadas para uso futuro
 - 255.255.255.255 → difusión a toda la red (protocolo DHCP)
- Descritas en el RFC 3330

Subredes

- Problema: el número de estaciones en una red puede ser demasiado grande ⇒ dificultades de administración
- Solución: dividir la red en subredes, que se gestionen de forma independiente pero que actúen como una sola de cara al exterior

Máscara de subred

- Utilizamos parte del campo estación para indicar la subred
- Empleamos máscaras para delimitar la subred
- Formato de máscara: 32 bits de los que los n más significativos están a 1 y los 32 – n restantes a 0
- Ejemplo: máscara de 27 bits, se denota como sufijo /27 255.255.255.224 = 111111111111111111111111111111100000

Ejemplo de máscara

- Dirección clase C 193.168.17.0/27 (o máscara 255.255.255.224)
 - Los 24 primeros bits indican la red (192.168.17)
 - Los 3 siguientes la subred
 - Los 5 últimos la posición de la estación en la subred
 - Tenemos $2^3 = 8$ subredes, con $2^5 2 = 30$ estaciones por subred
 - En total, podemos direccionar 8 x 30 = 240 estaciones (254 en clase C sin máscara)

Ejemplo de máscara

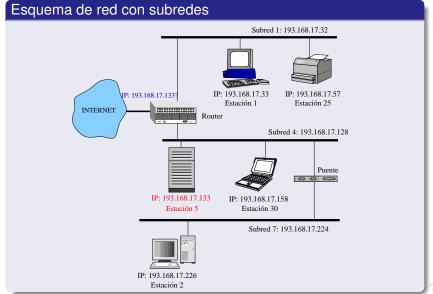
Dirección 193.168.17.0/27 (clase C)

Nº de subred	Dir. base	Dir. broadcast
0	193.168.17.0	193.168.17.31
1	193.168.17.32	193.168.17.63
2	193.168.17.64	193.168.17.95
3	193.168.17.96	193.168.17.127
4	193.168.17.128	193.168.17.159
5	193.168.17.160	193.168.17.191
6	193.168.17.192	193.168.17.223
7	193.168.17.224	193.168.17.255

Ejemplo de subredes

- Dirección 193.168.17.133/27
 - ¿A qué subred pertenece?

¿Qué posición ocupa en la subred?



Redes sin clase

- En 1993, se suprimen las clases
- Direcciones CIDR (Classless Inter-Domain Routing)
 - Sufijo $/s \Rightarrow s$ bits para indicar la red y 32 s para indicar la estación ($2^{(32-s)} 2$ estaciones)
- Ejemplos: 193.168.17.0/18, 130.15.0.0/8
- También se conocen como superredes
- Ejemplo: 193.168.173.253/18
 - Nº de red: 11000001.10101000.10000000.000000000 = 193.168.128.0
 - Broadcast: 11000001.10101000.10111111.11111111 = 193.168.191.255
 - Nº estación: 11000001.10101000.10101101.11111101 = estación nº 11773
 - N^0 total de estaciones: $2^{14} 2 = 16382$

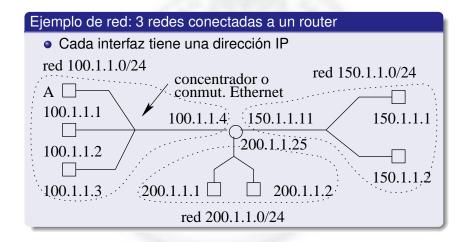


Subredes en redes sin clase

- Las redes con clase serían: A/8, B/16 y C/24
- Se pueden establecer también subredes

193.144.48.0/20 en dos subredes				
				subred 193.144.48.0/21
193	144	0011-1-000	0	subred 193.144.56.0/21

		193.144.48.0/	′20 e	en 8 subredes
193	144	0011-000-0	0	subred 193.144.48.0/23
193	144	0011-001-0	0	subred 193.144.48.0/23 subred 193.144.50.0/23
193	144	0011-111-0	0	subred 193.144.62.0/23



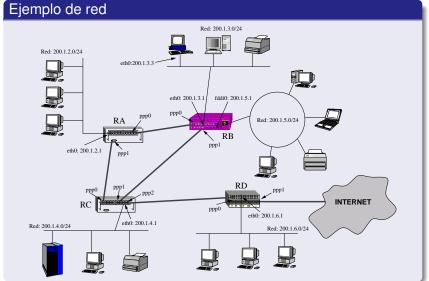
Ejemplo de red: 3 redes conectadas a un router

Cada interfaz tiene una dirección IP

	Tabla de rutas del I	nost A	
destino	interfaz	gateway	métrica
100.1.1.0/24	eth0 (=100.1.1.1)	*	0
150.1.1.0/24	eth0 (=100.1.1.1)	100.1.1.4	1
200.1.1.0/24	eth0 (=100.1.1.1)	100.1.1.4	1

	Tabla de rutas del ro	outer	
destino	interfaz	gateway	métrica
100.1.1.0/24	eth0 (=100.1.1.4)	*	0
150.1.1.0/24	eth1 (=150.1.1.11)	*	0
200.1.1.0/24	eth2 (=200.1.1.25)	*	0





Ejemplo de	e red: tabla:	s de reenv	⁄ío de los roι	uters	
	ROUTER A			ROUTER B	
Red destino	Gateway	Interfaz	Red destino	Gateway	Interfaz
200.1.2.0	200.1.2.1	eth0	200.1.2.0	*	ppp0
200.1.3.0	*	ppp0	200.1.3.0	200.1.3.1	eth0
200.1.4.0	*	ppp1	200.1.4.0	*	ppp1
200.1.5.0	*	ppp0	200.1.5.0	200.1.5.1	fddi0
200.1.6.0	*	ppp1	200.1.6.0	*	ppp1
0.0.0.0	*	ppp1	0.0.0.0	*	ppp1
	ROUTER C			ROUTER D	
Red destino	Gateway	Interfaz	Red destino	Gateway	Interfaz
200.1.2.0	*	ppp0	200.1.2.0	*	ppp0
200.1.3.0	*	ppp1	200.1.3.0	*	ppp0
200.1.4.0	200.1.4.1	eth0	200.1.4.0	*	ppp0
200.1.5.0	*	ppp1	200.1.5.0	*	ppp0
200.1.6.0	*	ppp2	200.1.6.0	200.1.6.1	eth0
0.0.0.0	*	ppp2	0.0.0.0	*	ppp1

Ejemplo de red: tablas de reenvío de un host

Sistema 200.1.3.3

Red destino	Gateway	Interfaz
127.0.0.1	*	lo
200.1.3.0	*	eth0
0.0.0.0	200.1.3.1	eth0

• Consulta de las tablas de rutas en linux: route [-n]

Tabla de reenvío de los routers

Tabla de re	envío de	un router	
destino	interfaz	gateway	métrica
• • •			
194.24.0.0/21	int _i	*	i saltos
194.24.8.0/22	int _i	*	j saltos
194.24.16.0/20	int_k	*	k saltos
0.0.0.0 (por defecto)	int _x	*	x saltos

- Coincidencia del prefijo más largo
- Agregación de rutas



Reenvío de un paquete: coincidencia del prefijo más largo

- ¿Qué ocurre cuando le llega un paquete a 194.24.17.4?
 - Coincidencia de prefijo: se realiza un AND con cada máscara hasta que se produzca la coincidencia de prefijo
 - Con 194.24.0.0/21

```
194. 24.00010001.00000100 = 194.24.17.4
255.255.111111000.00000000 = 255.255.248.0
194.24.00010000.00000000 = 194.24.16.0
```

No coincide con la dirección base de la red (194.24.0.0)

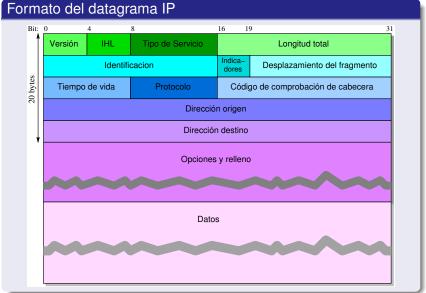
Con 194.24.16.0/20

```
194. 24.00010001.00000100 = 194.24.17.4
255.255.11110000.00000000 = 255.255.240.0
194.\ 24.00010000.000000000 = 194.24.16.0
Sí coincide con la dirección base de la red (194.24.16.0)
```

⇒ se envía por la interfaz correspondiente

 Si hubiese otra coincidencia con un prefijo más largo (máscara más grande), se reenviaría por la interfaz asociada a esa entrada

Datagrama IP

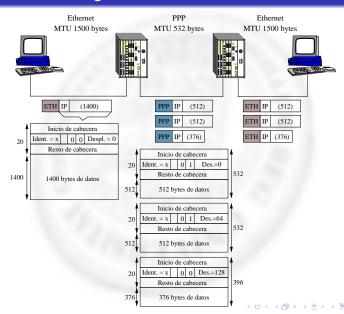


Datagrama IP

Fragmentación

- Las redes pueden especificar un tamaño máximo para los paquetes ⇒
 - Necesidad de fragmentar los datagramas en unidades más pequeñas
 - MTU: Maximun transmission unit, tamaño máximo de datagrama IP que puede enviarse en una trama
- Dos niveles de numeración: nº de datagrama y desplazamiento dentro del mismo
 - Uso de un bit MF Más fragmentos (1 en todos menos el último)
 - Bit NF indica que no se fragmenta
- El reensamblado se realiza en el sistema destino
- Se intenta evitar la fragmentación, haciendo que TCP y UDP generen segmentos pequeños (536 o 1460 bytes)

Datagrama IP: fragmentación



IP versión 6

- La capacidad de direccionamiento del IP actual (v.4) pronto estará en el límite
- Necesidad de simplificar el protocolo, para que los encaminadores sean más eficientes
- Proporcionar mayor seguridad
- Surge IPv6 como respuesta (inicialmente IPng)

Características de IPv6

- Direcciones de 128 bits \Rightarrow 3,4 \times 10³⁸ direcciones
- No existen clases
- Permite envío multicast
- Servicios en tiempo real
- Servicios de autenticación y seguridad

Direcciones IPv6

• Representación con 8 campos de 16 bits en hexadecimal:

47CD:1234:4422:AC02:0022:1234:A456:0124

Forma compacta si hay cadenas de ceros:

47CD:0000:0000:0000:0000:A456:0124

⇔ 47CD::A456:0124

Direcciones IPv4 escritas como IPv6

::FFFF:193.144.84.77

- Facilitan la transición IPv4 → IPv6
- Uso de máscaras para la parte de red y de host

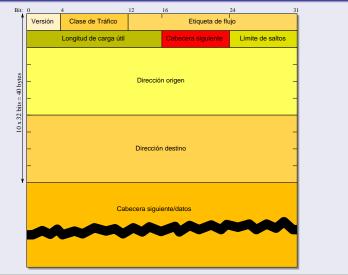
 Direcciones unicast, multicast (comienzan por ff) y anycast (a cualquier host de una red)

Cabecera IPv6

- 40 bytes (desaparece la longitud de cabecera), en 8 campos (menos que IPv4)
- Campos eliminados:
 - Opciones: se indican en cabeceras adicionales
 - Fragmentación: no se fragmentan. Si un datagrama es muy grande, se devuelve un mensaje ICMP
 - Numeración de los paquetes: no se numeran
 - Suma de comprobación: se ahorra procesamiento en los routers
 - Queda en la capa de transporte y posiblemente en la de enlace
- Clase de tráfico y Etiqueta de flujo (8 y 20 bits): relacionados con la QoS



Formato del datagrama IPv6



Transición de IPv4 a IPv6

- Debe ser gradual y coexistirán las dos
- Uso de túneles (tunneling)
 - Cuando los paquetes IPv6 deban pasar por routers que no soportan IPv6
 - Encapsular los paquetes IPv6 dentro de paquetes IPv4
 - Añadir cabeceras IPv4 con las direcciones de los routers que no soportan IPv6
 - Eliminar dichas cabeceras al llegar a zonas con routers IPv6

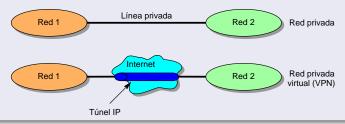
IPv4 IPv6



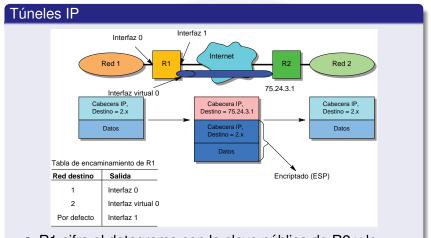
VPN: Virtual Private Network

Redes privadas virtuales

- Red de una organización que utiliza la red pública para comunicarse de forma segura
- Usan sistemas de encriptación y autenticación
 - IPsec, protocolo de seguridad de IP para soportar comunicaciones seguras e implementar VPNs
 - También se pueden implementar mediante túneles IP



VPN: Virtual Private Network



- R1 cifra el datagrama con la clave pública de R2 y le añada una cabecera con destino R2
- R2 lo descifra con su clave privada y lo envía al destino

Índice

- Introducción
- 2 Redes de conmutación de paquetes
- 3 Algoritmos de encaminamiento
- 4 Encaminamiento en Internet
- Protocolo de Internet
- 6 ICMP: Protocolo de mensajes de control de Internet
- 7 DHCP: Protocolo de configuración dinámica de hosts
- 8 NAT: Traducción de direcciones de rec



ICMP: Internet Control Messages Protocol

Protocolo de mensajes de control de Internet

- Se usa para que hosts y routers puedan informarse sobre errores o el estado de la red
- Funciona sobre IP, pero no se garantiza su entrega
- Se encapsula en un datagrama IP

Mensajes ICMP

- Tipo y código del mensaje
- Los 8 primeros bytes del datagrama que causó el mensaje

ICMP: Internet Control Messages Protocol

Tipos de mensajes ICMP

- Destino inalcanzable: lo envía un nodo a la estación origen cuando no puede alcanzar el destino o cuando el datagrama no puede fragmentarse y no puede atravesar una red (tipo ICMP 3)
- Tiempo excedido: cuando un nodo destruye un datagrama porque su contador llegó a 0 lo manda a la estación origen (tipo ICMP 11)
- Ralentizar fuente: para limitar el número de datagramas que las estaciones introducen en la red y evitar la congestión (tipo ICMP 4)
- Solicitud de eco y Respuesta de eco: se utilizan para ver si un destino es alcanzable y se encuentra activo (uso en ping) (tipos ICMP 8 y 0)



ICMP: Internet Control Messages Protocol

Tipos de mensajes ICMP

- Problema de parámetro: indica que se ha detectado un valor ilegal en un campo de la cabecera (tipo ICMP 12)
- Redirigir: se utiliza cuando un nodo se da cuenta de que hay un mejor camino para enviar el datagrama
- Marca de tiempo y Respuesta a marca de tiempo: para medir el retardo de la red
- Petición de máscara de dirección y Respuesta de máscara de dirección: empleadas cuando se usan subredes, permiten a un computador conocer la máscara de subred

Índice

- Introducción
- 2 Redes de conmutación de paquetes
- Algoritmos de encaminamiento
- 4 Encaminamiento en Internet
- Protocolo de Internet
- 6 ICMP: Protocolo de mensajes de control de Internet
- DHCP: Protocolo de configuración dinámica de hosts
- NAT: Traducción de direcciones de rec



DHCP: Dynamic Host Configuration Protocol

Protocolo de configuración dinámica de hosts

- Asignación de direcciones IP a los hosts:
 - Estáticamente: el administrador del equipo
 - Dinámicamente: con el protocolo DHCP
 - Cada vez que se inicia, solicita al servidor una IP temporal
 - Usado por los ISPs, cuando no tienen direcciones para todos sus abonados
 - También usado en las redes inalámbricas
- Permite obtener información para un host como:
 - su dirección IP
 - el gateway por defecto
 - servidores DNS disponibles



DHCP: Dynamic Host Configuration Protocol

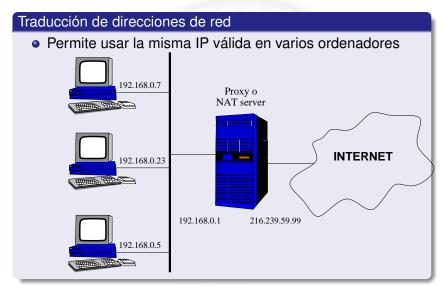
Pasos del protocolo DHCP

- Descubrimiento de un servidor DHCP: mensaje DHCPDISCOVER
 - IP destino 255.255.255.255 (broadcast)
 - IP origen 0.0.0.0
- Ofrecimiento del servicio DHCP: respuesta del servidor con una IP, máscara de red, etc. y un tiempo de concesión
- Petición DHCP: si hay varias ofertas, el cliente solicita una
- ACK DHCP: el servidor confirma la solicitud

Índice

- Introducción
- 2 Redes de conmutación de paquetes
- Algoritmos de encaminamiento
- 4 Encaminamiento en Internet
- Protocolo de Internet
- 6 ICMP: Protocolo de mensajes de control de Internet
- 7 DHCP: Protocolo de configuración dinámica de hosts
- 8 NAT: Traducción de direcciones de red





Direcciones sin conexión a Internet

- Direcciones especiales para uso en redes privadas:
 - Comunicaciones internas de una empresa
 - Conexión de varias estaciones usando una única IP
 - Clase A: 10.0.0.0/8 (10.0.0.0-10.255.255.255)
 - Clase B: 172.16.0.0/12 (172.16.0.0–172.31.255.255)
 - Clase C: 192.168.0.0/16 (192.168.0.0–192.168.255.255)
- Los routers de Internet ignoran los paquetes con estas IPs
- Descritas en el RFC 1918



NAT

Servidor NAT

- Necesita dos interfaces y dos IPs
 - Una para la IP válida para conectar al exterior
 - Otra con una IP privada para conectar a la red interna
- Los ordenadores de la red privada tendrán como gateway la IP privada del servidor NAT
- Encamina de forma transparente los paquetes entre la red interna y la red externa
- Cambia la IP privada y puerto origen de los paquetes internos por la IP del servidor NAT y un puerto libre
- En una tabla almacena IP origen, puerto origen y puerto usado
 - Por el puerto usado sabe a qué máquina enviar la respuesta
- Puede combinarse fácilmente con filtrado de paquetes

