

Redes

Tema 4: Capa de rede

Oscar García Lorenzo

Escola Politécnica Superior de Enxeñería

Índice

- 1 Introducción
- 2 Redes de conmutación de paquetes
- 3 Algoritmos de encamiñamento
- 4 Encamiñamento na Internet
- 5 Protocolo de Internet
- 6 ICMP: Protocolo de mensaxes de control de Internet
- 7 DHCP: Protocolo de configuración dinámica de hosts
- 8 NAT: Traducción de direcciones de rede

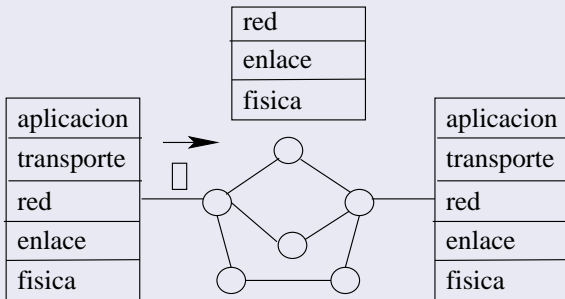
Índice

- 1 **Introducción**
- 2 Redes de conmutación de paquetes
- 3 Algoritmos de encamiñamento
- 4 Encamiñamento na Internet
- 5 Protocolo de Internet
- 6 ICMP: Protocolo de mensaxes de control de Internet
- 7 DHCP: Protocolo de configuración dinámica de hosts
- 8 NAT: Traducción de direcciones de rede

Introducción

Capa de rede

- Encargase de levar os paquetes que lle pasa a capa de transporte do host orixe ao host destino
- Implementada tanto nos sistemas finais coma nos routers



Índice

- 1 Introducción
- 2 Redes de conmutación de paquetes**
- 3 Algoritmos de encamiñamento
- 4 Encamiñamento na Internet
- 5 Protocolo de Internet
- 6 ICMP: Protocolo de mensaxes de control de Internet
- 7 DHCP: Protocolo de configuración dinámica de hosts
- 8 NAT: Traducción de direcciones de rede

Redes de conmutación de paquetes

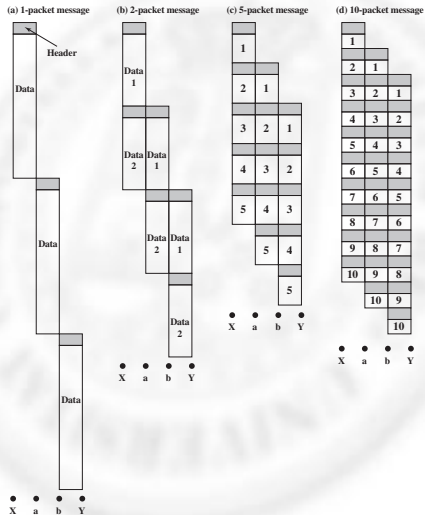


Figure 10.2 Effect of Packet Size on Transmission Time

Redes de conmutación de paquetes

Redes de datagramas

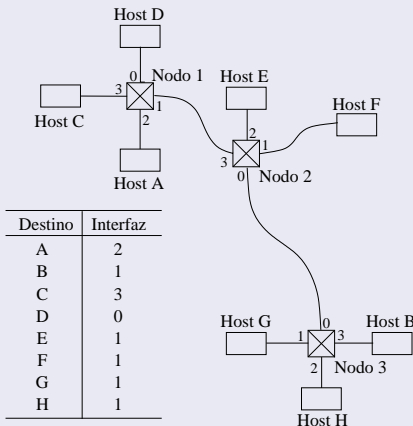
- Cada paquete inclúe na cabeceira a IP destino
- Reenvío: o router examina a cabeceira e o coloca na saída máis apropiada (táboa de reenvío)
- Non manteñen información de estado: unha secuencia de paquetes encamiñanse de forma independente

Redes de circuitos virtuais

- Establecese a conexión planificando unha ruta ao destino: un circuito virtual (CV)
- A cada paquete escríbeselle o identificador de CV: os routers o usan para o reenvío
- Os routers manteñen información de estado (táboa de circuitos virtuales)

Redes de datagramas

Exemplo



Destino	Interfaz
A	2
B	1
C	3
D	0
E	1
F	1
G	1
H	1

Tabla de encaminamiento del nodo 1

Destino	Interfaz
A	3
B	0
C	3
D	3
E	2
F	1
G	0
H	0

Tabla de encaminamiento del nodo 2

Destino	Interfaz
A	0
B	3
C	0
D	0
E	0
F	0
G	1
H	2

Tabla de encaminamiento del nodo 3

Introducción

Capa de rede en Internet: IP

- Tipo datagrama: encamiñanse os paquetes en función da dirección destino que conteñen
- Sen estado: cada paquete tratase de forma independente
- Rede non fiábel: servizo de mellor esforzo.
 - Non se garante a entrega de paquetes (nin o orde)
 - Nin a entrega nun tempo determinado
 - Entrega o maior número de paquetes, aínda que algúns se perdan
- Permite a interconexión de redes de diferentes tecnoloxías (interred)

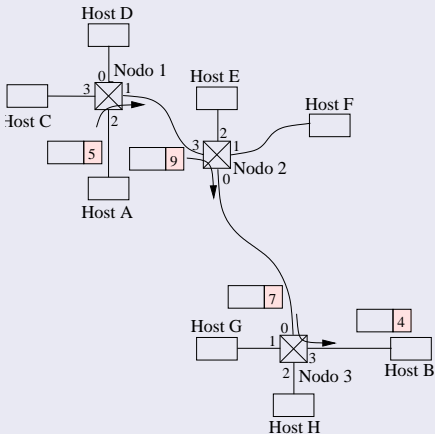
Redes de circuitos virtuais

táboa de circuitos virtuais

- Cada nodo mantén unha táboa de encamiñamento coa seguinte información:
 - Interface de entrada do circuito virtual
 - Identificador do circuito virtual **VCI**
 - Interface de saída pola que os paquetes dese circuito virtual deixan o nodo
 - Identificador de saída do circuito virtual
- Un paquete que chega por unha interface cun VCI, colócase na interface indicada na táboa co novo VCI

Redes de circuitos virtuales

Exemplo



Nodo 1			
Entrada		Salida	
Interfaz	VCI	Interfaz	VCI
2	5	1	9
.	.	.	.
.	.	.	.
.	.	.	.

Nodo 2			
Entrada		Salida	
Interfaz	VCI	Interfaz	VCI
3	9	0	7
.	.	.	.
.	.	.	.
.	.	.	.

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

Redes de circuitos virtuais

Construcción da táboa de VC

- A envía unha *Petición de chamada* dirixida a B
- Esta chega ao nodo 1 pola interface 2, que debe saber como reenviala para que chegue a B (similar a datagramas)
- O nodo 1 decide marcar esta petición cun VCI de 5 (aleatorio), e a envía pola interface 1
- 2 o recibe, o marca con VCI 9 e o coloca na interface 0; 3 o marca con VCI 7 e o coloca en 3; e B o marca con VCI 4, que identificará os paquetes de A
- B devolve unha *Chamada aceptada* con VCI 4 ao nodo 3 pola interface 3
- O nodo 3 pode completar a sua entrada na táboa (VCI saída = 4); o mesmo os nodos 2 e 1
- 1 manda o ACK a A que o recibe con VCI 5
 - \Rightarrow A marca o resto de paquetes a B con VCI 5

Índice

- 1 Introducción
- 2 Redes de conmutación de paquetes
- 3 Algoritmos de encamiñamento**
- 4 Encamiñamento na Internet
- 5 Protocolo de Internet
- 6 ICMP: Protocolo de mensaxes de control de Internet
- 7 DHCP: Protocolo de configuración dinámica de hosts
- 8 NAT: Traducción de direcciones de rede

Algoritmos de encamiñamento

Conceptos

- Algoritmo de encamiñamento ou rutado: o encargado de atopar o camiño mínimo entre a orixe e o destino
 - Cada host está conectado a un router (*router por defecto*)
 - O problema limítase a atopar o camiño mínimo entre routers
- Equivalente a atopar o camiño mínimo nun grafo
 - Routers: nodos do grafo
 - Enlaces: aristas do grafo
 - Asignaselles un peso (custo)
 - Custo: distancia, velocidade, carga do enlace, custo económico, etc.

Algoritmos de encamiñamiento

Clasificación

- **Globais. De estado dos enlaces**
 - Cada nodo dispón de toda a información sobre a rede: todos os nodos e o custo de todos os enlaces
 - A partir desta información, cada nodo pode calcular a súa táboa de encamiñamento (ou de rutas)
- **Descentralizados. De vector de distancias**
 - O cálculo dos camiños mínimos faise en colaboración de todos os nodos
 - Os nodos intercambian información so cos seus veciños
 - So coñecen a distancia aos demais nodos e por onde empezar

Algoritmos de encamiñamento

Clasificación

- Estáticos ou dinámicos
 - Estáticos: so cambian cando cambia a topoloxía de rede ou modificanse manualmente parámetros
 - Dinámicos: execútanse periódicamente de forma automática. Os usados actualmente en Internet
- Sensíbeis ou insensíbeis á carga
 - Sensíbeis: o custo dos enlaces varía dinamicamente
 - Poden provocar que as mensaxes queden atrapadas nun ciclo
 - En Internet son insensíbeis á carga

Encamiñamento de estado dos enlaces

Algoritmo de Dijkstra (1959)

- Procura o camiño máis curto entre dous vértices dun grafo pesado
- Variante do algoritmo, *forward search*:
 - O nodo N quiere calcular a súa táboa de routing a partires dos LSP (*link state packet*) que recibiu
 - Cada nodo ten 2 listas: *Confirmado* e *Provisional*
 - Cada elemento das listas indica o custo para alcanzar un nodo e o seguinte salto
 - $(M, 5, L)$, indica que de N alcanzase M a custo 5 a través de L
 - Inicializa a táboa *Confirmado* cunha entrada para N con custo 0 ($(N, 0, -)$)
 - Segue o seguinte algoritmo:

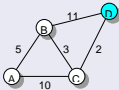
Encamiñamento de estado dos enlaces

Algoritmo de Dijkstra

- 1 Para o último nodo engadido a Confirmado (nodo S) examina o seu LSP
- 2 Para cada veciño (V) de S , calcula o custo (Custo) para alcanzar V como a suma do custo de N a S e de S a V
 - Se V non está en ningunha lista, engadeo á lista Provisional da forma $(V, \text{Cust}, \text{SegSalto})$
 - Se V está en Provisional, e Custo é menor que o indicado, reemplázao por $(V, \text{Cust}, \text{SegSalto})$
- 3 Se Provisional está baleira, acaba; se non pasa a entrada de Provisional con menor custo a Confirmado
- 4 Volve ao paso 1

Encamiñamiento de estado dos enlaces

Algoritmo de Dijkstra



Destino	Coste	SigSalto
A	10	C
B	5	C
C	2	C

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, así que reemplaza (B,11,B) por (B,5,C). El LSP de C indica que 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.

Encamiñamento de vector de distancias

Algoritmo descentralizado

- Todos os nodos colaboran

Funcionamento

- Inicialmente, os nodos só coñecen o custo a os seus veciños
- Iterativamente, os nodos comunican a os seus veciños todo o que saben
- Os nodos computan distancias a novos nodos ou actualizan as que teñen con menores valores
- As actualizacións continúan ata que converge
- A información que un nodo z comunica a os seus veciños son as distancias $d_{z,i}$
- Almacenase o veciño que enviou dita información (seguinte salto)

Encamiñamento de vector de distancias

Funcionamento

Sexa o nodo x cun veciño z , cuxo enlace ten custo $c_{x,z}$, e que z envía $d_{z,y} \Rightarrow$

$D_{x,y}(z) =$	$c_{x,z}$	+	$d_{z,y}$
distancia de x	custo do		distancia
a y a través	enlace que		de z
da saída z	une x con z		a y

táboa de distancias do nodo x

		distancia por	
		z	z'
destino	y	$D_{x,y}(z)$	$D_{x,y}(z')$
	y'	$D_{x,y'}(z)$	$D_{x,y'}(z')$

Encamiñamento de vector de distancias

Exemplo

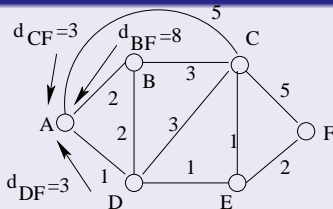
- Nodos B, C e D envían a A a distancia a F
- A calcula as distancias

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

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

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

- A táboa de distancias para A



		distancia por		
		B	C	D
destino
	F	10	8	4

Encamiñamento de vector de distancias

Ejemplo

- A comunica a os seus veciños a distancia a F,
 $d_{A,F} = \min_z D_{A,F}(z) = 4$
- Despois de certas iteracións, converge

		distancia por		
		B	C	D
destino	B	2	8	3
	C	5	5	3
	D	4	7	1
	E	5	6	2
	F	7	8	4

táboa de distancias de A

destino	saída
B	B
D	D
C	D
E	D
F	D

táboa de rutas de A

Encamiñamento de vector de distancias

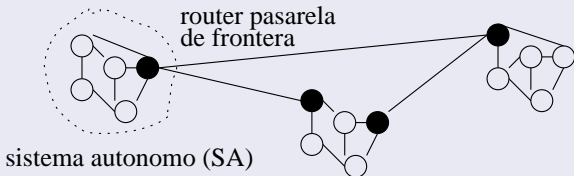
Características

- Intercambio de actualizacións cos veciños
 - Periódicamente
 - Cando un cambio na súa táboa ou no custo dun enlace
 - Disminución do custo dun enlace: actualización rápida das táboas
 - Aumento do custo dun enlace: algúns problemas. Resólvese con diversas técnicas: horizonte dividido e inverso envenenado
- Iterativo: pode precisar moitas iteracións. Peor que EE.
- Menos robusto que EE: se un nodo calcula mal as súas distancias, todos usarán eses valores incorrectos

Encamiñamento xerárquico

Sistemas autónomos (SA)

- Rexións nas que se dividen as redes grandes como Internet
- Operados por empresas u organismos
- Os routers so coñecen un encamiñamento na súa rexión
- *Routers pasarela fronteira*: centralizan o tráfico de saída do SA



- Dous niveis de encamiñamento:
 - Intradominio: cada SA pode elixir algoritmo
 - Interdominio: común para todos os SA

Índice

- 1 Introducción
- 2 Redes de conmutación de paquetes
- 3 Algoritmos de encamiñamento
- 4 Encamiñamento na Internet**
- 5 Protocolo de Internet
- 6 ICMP: Protocolo de mensaxes de control de Internet
- 7 DHCP: Protocolo de configuración dinámica de hosts
- 8 NAT: Traducción de direcciones de rede

Encamiñamento na Internet

Protocolos usados na Internet

- Intradominio ou internos ao SA (IGP): RIP y OSPF
- Interdominio ou entre SAs: BGP

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

- Protocolos da capa de aplicación

RIP (*Routing Information Protocol*)

Protocolo de información de encamiñamento

- Encamiñamento intradominio basado en vector de distancias
- Considera que o custo dos enlaces é 1 e distancia máxima 15
- Mensaxes RIP so aos nodos veciños
 - Mensaxes de petición RIP: solicitan información
 - Mensaxes de resposta RIP: lista de ata 25 redes internas ao SA
 - Tamén de forma automática cada 30 s. aos seus veciños. Se non se recibe resposta en 180 s., considerase caído

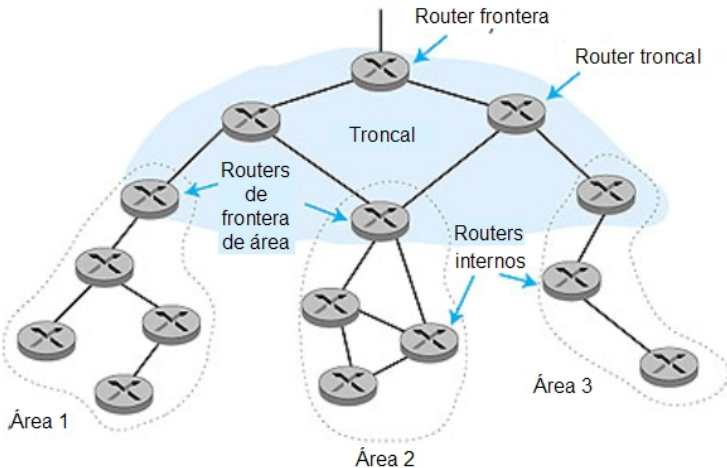
OSPF (*Open Shortest Path First*)

Protocolo aberto de primeiro o camiño máis curto

- Aberto: algoritmo libre
- Encamiñamento intradominio baseado en estado dos enlaces
- Máis avanzado que RIP, pensado para reemplazalo
- Mensaxes OSPF difúndense a todos os nodos
 - Cando se producen cambios
 - Periódicamente, ao menos cada 30 minutos
 - Cada router obtén información completa do SA
- Mensaxes HELLO a cada veciño, para comprobar que o enlace está OK
- Posibilidade de interrogar a un veciño para obter toda a información
- O custo das mensaxes os pon o administrador

OSPF (*Open Shortest Path First*)

OSPF xerárquico



BGP (*Border Gateway Protocol*)

Protocolo de pasarela de frontera

- Protocolo similar ao de vector de distancias, intercambianse rutas completas (vector de rutas)
- Cada SA identifícase por un número de sistema autónomo único
- Os administradores poden decidir as políticas de encamiñamento

rede destino	métrica
x	4

Exemplo de mensaxe en RIP

rede destino	ruta
x	SA1/SA2/SA3/S4

Exemplo de mensaxe en BGP

Índice

- 1 Introducción
- 2 Redes de conmutación de paquetes
- 3 Algoritmos de encamiñamento
- 4 Encamiñamento na Internet
- 5 Protocolo de Internet**
- 6 ICMP: Protocolo de mensaxes de control de Internet
- 7 DHCP: Protocolo de configuración dinámica de hosts
- 8 NAT: Traducción de direcciones de rede

Protocolo de Internet

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

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

- Protocolo de rede: IP
 - Define o formato das direccións
 - Formato dos datagramas
 - Accións dos routers en base aos campos dos datagramas
- Protocolo de encamiñamento
- Protocolo de mensaxes de control de Internet (ICMP)

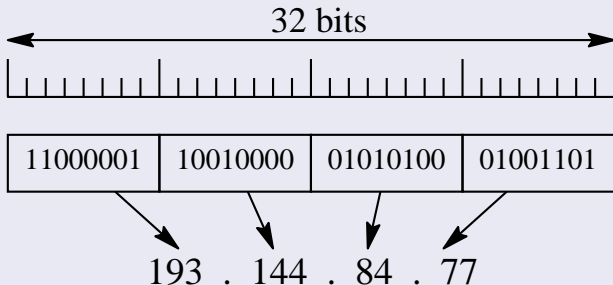
IP (*Internet Protocol*)

Direccionamiento IPv4

- Os nodos nunha rede teñen unha dirección IP por interface
- Interface: a unión dun host ou router cun enlace

Codificación da dirección IP

- En IPv4, cada dirección IP codifícase mediante 4 bytes, xeralmente escritos en notación decimal



A	0	Red	Estación
---	---	-----	----------

B	10	Red	Estación
---	----	-----	----------

C	110		Red		Estación
---	-----	--	-----	--	----------

D	1110		Dirección multicast
---	------	--	---------------------

E	11110	Reservado para uso futuro
---	-------	---------------------------

> 240.0.0.1

Direccionamiento IPv4

Proporción redes-máquinas

- Restricción: un campo de rede ou de host non pode estar todo a 1s ou todo a 0s
- Segundo isto temos:
 - Clase A:** 126 ($2^7 - 2$) redes con ≈ 16 millones de estacións cada unha ($2^{24} - 2 = 16777214$)
 - Clase B:** 16384 (2^{14}) redes con 65534 ($2^{16} - 2$) estacións cada unha
 - Clase C:** ≈ 2 millones de redes ($2^{21} = 2097152$) con 254 estacións cada unha ($2^8 - 2$)

Direccionamiento IPv4

Direcciones especiales reservadas

- Identificación de redes: o nº de rede e o resto a 0
- Exemplos:
 - Clase A → 10.0.0.0
 - Clase B → 172.16.0.0
 - Clase C → 193.144.84.0
- Dirección de broadcast: o nº de rede e o resto a 1
- Exemplos:
 - Clase A → 10.255.255.255
 - Clase B → 172.16.255.255
 - Clase C → 193.144.84.255

Direccionamiento IPv4

Direccións especiais reservadas

- Algunhas direccións reservadas polo IANA:
 - 0.0.0.0 → *Esta red*. Para arrincar sistemas sen disco (protocolo DHCP, tamén encamiñamento por defecto)
 - 127.0.0.0–127.255.255.255 → a propia estación (dirección de *loopback*), soese usar a 127.0.0.1
 - 240.0.0.0–255.255.255.254 → reservadas para uso futuro
 - 255.255.255.255 → difusión a toda a rede (protocolo DHCP)
- Descritas no RFC 3330

Direccionamiento IPv4

Subredes

- Problema: o número de estaciones nunha rede pode ser demasiado grande \Rightarrow dificultades de administración
- Solución: dividir a rede en subredes, que se xestionen de forma independente pero que actúen como unha soa de cara ao exterior

Máscara de subrede

- Utilizamos parte do campo estación para indicar a subrede
- Empleamos *máscaras* para delimitar a subrede
- Formato de máscara: 32 bits dos que os n máis significativos están a 1 e os $32 - n$ restantes a 0
- Exemplo: máscara de 27 bits, denotase como sufixo /27
 $255.255.255.224 \equiv 11111111.11111111.11111111.11100000$

Direccionamiento IPv4

Exemplo de máscara

- Dirección clase C 193.168.17.0/27 (ou máscara 255.255.255.224)
 - Os 24 primeros bits indican a rede (192.168.17)
 - Os 3 seguintes a subrede
 - Os 5 últimos a posición da estación na subrede
 - Temos $2^3 = 8$ subredes, con $2^5 - 2 = 30$ estacións por subred
 - En total, podemos direccionar $8 \times 30 = 240$ estacións (254 en clase C sen máscara)

Direccionamiento IPv4

Exemplo de máscara

- Dirección 193.168.17.0/27 (clase C)

Nº de subrede	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

Direccionamiento IPv4

Exemplo de subredes

- Dirección 193.168.17.133/27

- A qué subrede pertenece?

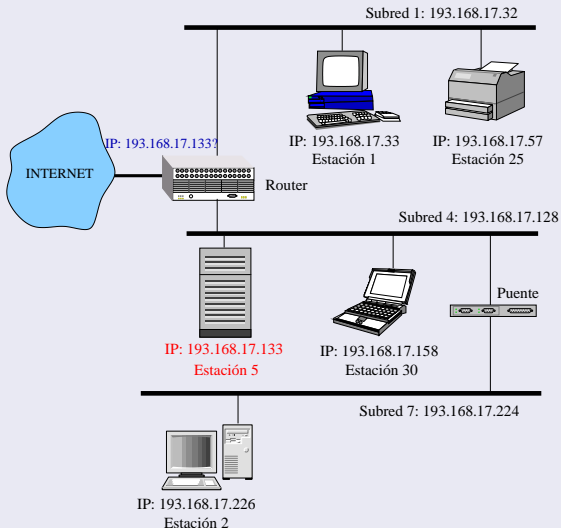
193.168.17.133	→	11000001.10101000.00010001.10000101	⊗
255.255.255.224	→	11111111.11111111.11111111.11100000	
<hr/>			
		11000001.10101000.00010001.10000000	
		<div style="display: flex; justify-content: space-around; align-items: center;"> Red Subred 4 </div>	

- Que posición ocupa na subrede?

193.168.17.133	→	11000001.10101000.00010001.10000101	⊗
255.255.255.224	→	00000000.00000000.00000000.00011111	
<hr/>			
		00000000.00000000.00000000.00000101	
		<div style="display: flex; justify-content: space-around; align-items: center;"> Estación 5 </div>	

Direcccionamiento IPv4

Esquema de red con subredes



Direcccionamiento IPv4

Redes sen clase

- En 1993, suprimense as clases
- Direccíons CIDR (*Classless Inter-Domain Routing*)
 - Sufijo /s \Rightarrow s bits para indicar a rede e $32 - s$ para indicar a estación ($2^{(32-s)} - 2$ estaciones)
- Exemplos: 193.168.64.0/18, 130.0.0.0/8
- Tamén se coñecen como *superredes*
- Exemplo: 193.168.173.253/18
 - N° de rede: 11000001.10101000.10000000.00000000 = 193.168.128.0
 - Broadcast: 11000001.10101000.10111111.11111111 = 193.168.191.255
 - N° estación: 11000001.10101000.10101101.11111101 = estación n° 11773
 - N° total de estaciones: $2^{14} - 2 = 16382$

Direccionamiento IPv4

Subredes en redes sen clase

- As redes con clase serían: A/8, B/16 y C/24
- Pódense establecer tamén subredes

193.144.48.0/20 en dúas subredes				
193	144	0011-0-000	0	subrede 193.144.48.0/21
193	144	0011-1-000	0	subrede 193.144.56.0/21

193.144.48.0/20 en 8 subredes				
193	144	0011-000-0	0	subrede 193.144.48.0/23
193	144	0011-001-0	0	subrede 193.144.50.0/23
...				
193	144	0011-111-0	0	subrede 193.144.62.0/23

◀ ◻ ▶ ◀ ◻ ▶ ◀ ≡ ▶ ◀ ≡ ▶ ≡

Direccionamiento IPv4

Exemplo de rede: 3 redes conectadas a un router

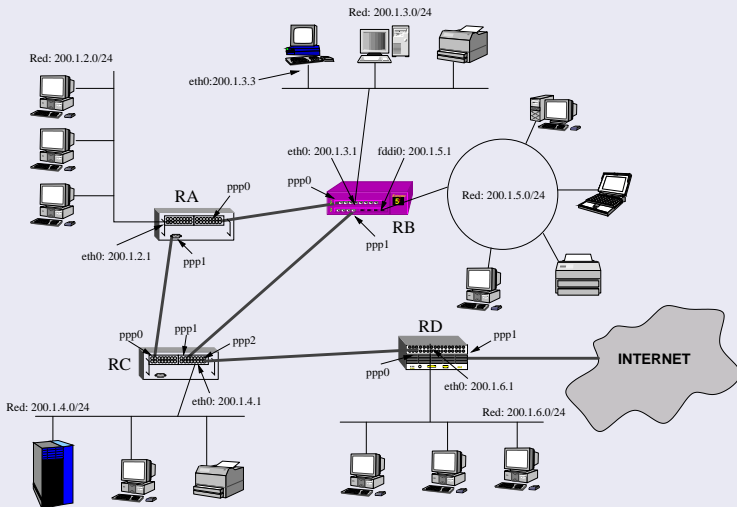
- Cada interface ten unha dirección IP

táboa de rutas do host A			
destino	interface	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

táboa de rutas do router			
destino	interface	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

Direcccionamiento IPv4

Exemplo de rede



Direccionamiento IPv4

Exemplo de rede: táboas de reenvío dos routers

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

Rede: táboas de reenvío dun 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

Lista das táboas de rutas en linux: `route`

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 das táboas de rutas en linux: `route [-n]`

Direcccionamiento IPv4

táboa de reenvío dos routers

táboa de reenvío dun router			
destino	interface	gateway	métrica
...
194.24.0.0/21	int_i	*	i saltos
194.24.8.0/22	int_j	*	j saltos
194.24.16.0/20	int_k	*	k saltos
...
0.0.0.0/0 (por defecto)	int_x	*	x saltos

- Coincidencia do prefixo máis longo
- Agregación de rutas

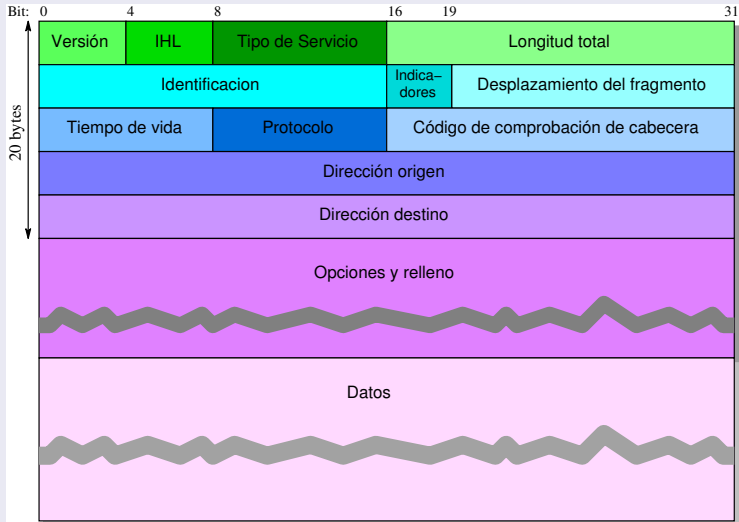
Direccionamiento IPv4

Reenvío dun paquete: coincidencia do prefixo máis longo

- Que ocorre cando lle chega un paquete a 194.24.17.4?
 - Coincidencia de prefixo: realizase un AND con cada máscara ata que se produza a coincidencia de prefixo
 - Con 194.24.0.0/21
 - 194. 24.00010001.00000100 = 194.24.17.4
 - 255.255.11111000.00000000 = 255.255.248.0
 - 194. 24.00010000.00000000 = **194.24.16.0**
 - Non coincide coa dirección base da rede (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. 24.00010000.00000000 = **194.24.16.0**
 - Si coincide coa dirección base da rede (194.24.16.0) \implies envíase poa interface correspondente
 - Se houbera outra coincidencia cun prefixo máis longo (máscara máis grande), reenviaríase pola interface asociada a esa entrada

Datagrama IP

Formato do datagrama IP

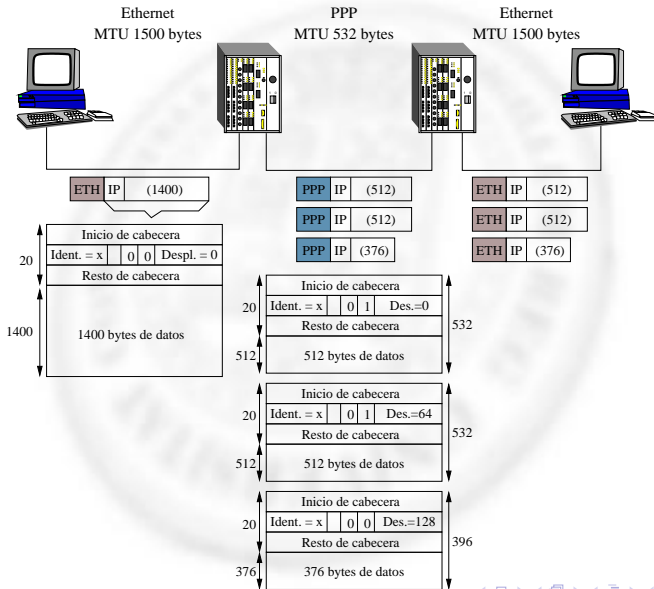


Datagrama IP

Fragmentación

- As redes poden especificar un tamaño máximo para os paquetes ⇒
 - Necesidade de fragmentar os datagramas en unidades máis pequenas
 - MTU: *Maximun transmission unit*, tamaño máximo de datagrama IP que pode enviarse nunha trama
- Dous niveis de numeración: nº de datagrama e desprazamento dentro do mesmo
 - Uso dun bit MF *Máis fragmentos* (1 en todos menos o último)
 - Bit NF indica que non se fragmenta
- O reensamblado realizase no sistema destino
- Intentase evitar a fragmentación, facendo que TCP e UDP xeren segmentos pequenos (536 o 1460 bytes)

Datagrama IP: fragmentación



IPv6

IP versión 6

- A capacidade de direccionamiento do IP actual (v.4) pronto estará no límite (último grupo rexional asignado en 2011)
- Necesidade de simplificar o protocolo, para que os encamiñadores sexan máis eficientes
- Proporcionar maior seguridade
- Xurde IPv6 como resposta (inicialmente IPng)

Características de IPv6

- Direccións de 128 bits $\Rightarrow 3,4 \times 10^{38}$ direccións
- Non existen clases
- Permite envío multicast
- Servizos en tempo real
- Servizos de autenticación e seguridade

IPv6

Direccións IPv6

- Representación con 8 campos de 16 bits en hexadecimal:
47CD:1234:4422:AC02:0022:1234:A456:0124

- Forma compacta se hai cadeas de ceros:

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

⇔ 47CD::A456:0124

- Direccións IPv4 escritas como IPv6

::FFFF:193.144.84.77

- Facilitan a transición IPv4 → IPv6

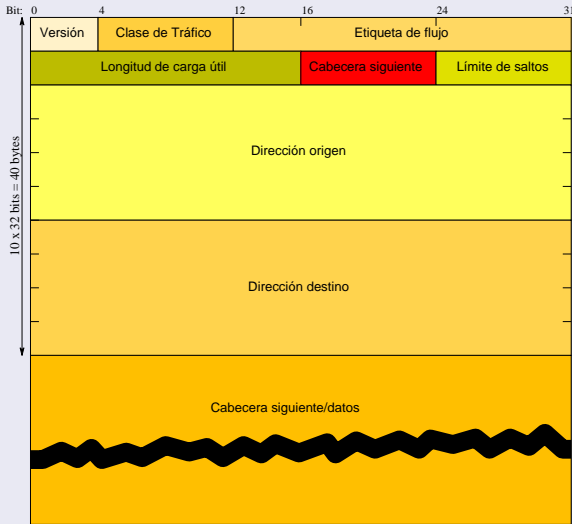
- Uso de máscaras para a parte de rede e de host

dirección:	3ffe:ffff:100:1:2:3:4:5/48
máscara:	ffff:ffff:ffff:0000:0000:0000:0000:0000
rede:	3ffe:ffff:0100:0000:0000:0000:0000:0000

- Direccións *unicast*, *multicast* (comenzan por ff) y *anycast* (a calquera host dunha rede)

IPv6

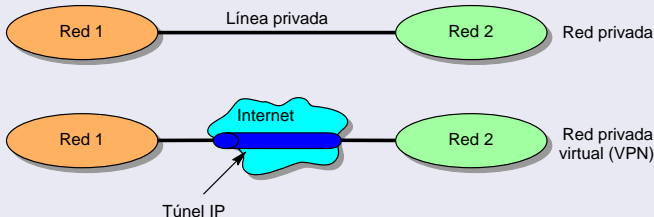
Formato del datagrama IPv6



VPN: *Virtual Private Network*

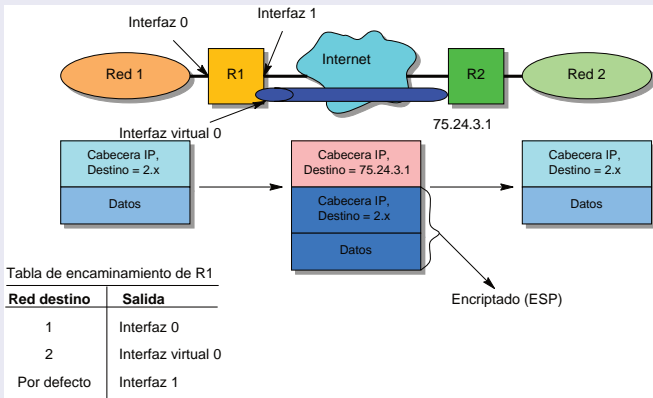
Redes privadas virtuales

- Rede dunha organización que utiliza a rede pública para comunicarse de forma segura
- Usan sistemas de encriptación e autenticación
 - **IPsec**, protocolo de seguridade de IP para soportar comunicacións seguras e implementar VPNs
 - Tamén se poden implementar mediante túneles IP



VPN: Virtual Private Network

Túneles IP



- R1 cifra o datagrama coa chave pública de R2 e lle engade unha cabeceira con destino R2
- R2 o descifra coa súa chave privada e o envía ao destino

Índice

- 1 Introducción
- 2 Redes de conmutación de paquetes
- 3 Algoritmos de encamiñamento
- 4 Encamiñamento na Internet
- 5 Protocolo de Internet
- 6 ICMP: Protocolo de mensaxes de control de Internet**
- 7 DHCP: Protocolo de configuración dinámica de hosts
- 8 NAT: Traducción de direcciones de rede

ICMP: *Internet Control Messages Protocol*

Protocolo de mensaxes de control de Internet

- Usase para que hosts e routers poidan informarse sobre erros ou o estado da rede
- Funciona sobre IP, pero non se garante a súa entrega
- Encapsúlase nun datagrama IP

Mensaxes ICMP

- Tipo e código da mensaxe
- Os 8 primeiros bytes do datagrama que causou a mensaxe

ICMP: *Internet Control Messages Protocol*

Tipos de mensaxes ICMP

- *Destino inalcanzable*: o envía un nodo á estación orixe cando non pode alcanzar o destino ou cando o datagrama non pode fragmentarse e non pode atravesar unha rede (tipo ICMP 3)
- *Tempo excedido*: cando un nodo destrúe un datagrama porque o seu contador chegou a 0 o manda á estación orixe (tipo ICMP 11)
- *Ralentizar fonte*: para limitar o número de datagramas que as estacións introducen na rede e evitar a conxestión (tipo ICMP 4)
- *Solicitud de eco e Resposta de eco*: utilízanse para ver se un destino é alcanzable e atópase activo (uso en ping) (tipos ICMP 8 e 0)

ICMP: *Internet Control Messages Protocol*

Tipos de mensaxes ICMP

- *Problema de parámetro*: indica que se detectou un valor ilegal nun campo da cabeceira (tipo ICMP 12)
- *Redirixir*: utilízase cando un nodo dáse conta de que hai un mellor camiño para enviar o datagrama
- *Marca de tempo e Resposta a marca de tempo*: para medir o retardo da rede
- *Petición de máscara de dirección e Resposta de máscara de dirección*: empregadas cando se usan subredes, permiten a un computador coñecer a máscara de subrede

- Selección
- Métodos de conmutación de paquetes
- Algoritmos de encaminamiento
- Encaminamiento en Internet
- Protocolo de Internet
- ICMP: Protocolo de mensajes de control de Internet
- OSPF: Protocolo de configuración dinámica de host
- Traducción de direcciones de red

- Selección
- Métodos de conmutación de paquetes
- Algoritmos de encaminamiento
- Encaminamiento en Internet
- Protocolo de Internet
- ICMP: Protocolo de mensajes de control de Internet
- OSPF: Protocolo de configuración dinámica de host
- Traducción de direcciones de red

DHCP: *Dynamic Host Configuration Protocol*

Protocolo de configuración dinámica de hosts

- Asignación de direcciones IP aos hosts:
 - Estáticamente: o administrador do equipo
 - Dinámicamente: co protocolo DHCP
 - Cada vez que se inicia, solicita ao servidor unha IP temporal
 - Usado polos ISPs, cando non teñen direccións para todos os seus abonados
 - Tamén usado nas redes inarámicas
- Permite obter información para un host como:
 - a súa dirección IP
 - o *gateway* por defecto
 - servidores DNS dispoñíbeis

DHCP: *Dynamic Host Configuration Protocol*

Pasos do protocolo DHCP

- Descubrimento dun servidor DHCP: mensaxe DHCPDISCOVER
 - IP destino 255.255.255.255 (broadcast)
 - IP orixe 0.0.0.0
- Ofrecemento do servizo DHCP: resposta do servidor cunha IP, máscara de rede, etc. e un tempo de concesión
- Petición DHCP: si hai varias ofertas, o cliente solicita unha
- ACK DHCP: o servidor confirma a solicitude

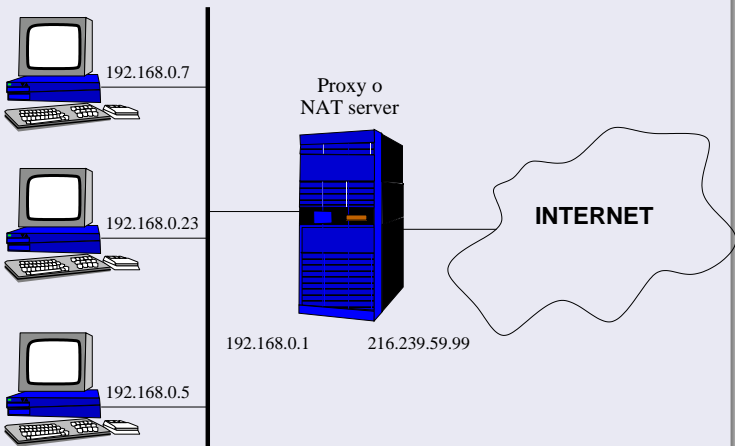
Índice

- 1 Introducción
- 2 Redes de conmutación de paquetes
- 3 Algoritmos de encamiñamento
- 4 Encamiñamento na Internet
- 5 Protocolo de Internet
- 6 ICMP: Protocolo de mensaxes de control de Internet
- 7 DHCP: Protocolo de configuración dinámica de hosts
- 8 NAT: Traducción de direcciones de rede

NAT: Network Address Translation

Traducción de direcciones de red

- Permite usar a mesma IP válida en varios computadores



NAT: Network Address Translation

Direccións sen conexión a Internet

- Direccións especiais para uso en redes privadas:
 - Comunicacións internas dunha empresa
 - Conexión de varias estacións 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)
- Os routers de Internet ignoran os paquetes con estas IPs
- Descritas no RFC 1918

NAT: *Network Address Translation*

Servidor NAT

- Necesita dúas interfaces e dúas IPs
 - Unha para a IP válida para conectar ao exterior
 - Outra cunha IP privada para conectar á rede interna
- Os computadores da red privada terán como gateway a IP privada do servidor NAT
- Encamiña de forma transparente os paquetes entre a rede interna e a rede externa
- Cambia a IP privada e porto orixe dos paquetes internos pola IP do servidor NAT e un porto libre
- Nunha táboa almacena IP orixe, porto orixe e porto usado
 - Polo porto usado sabe a que máquina enviar a resposta
- Pode combinarse fácilmente con filtrado de paquetes
- NAT traversal e UPnP

NAT: Network Address Translation

Funcionamiento

