



T2:

Nivel de Red

Tema 2: Nivel de RED IP

Interconexión de Redes

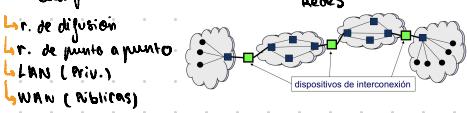
No hay ninguna red q pueda conectar a TODOS

- Dispersion usuarios
- ≠ Redes servicios
- ≠ Redes modos de funcionamiento
- ≠ Redes tecnologías

InterNetworking !!

conectar redes de cualquier tipo

conjunto de redes



Terminología

Intranet: internet interna, aislada, con conexión a Internet

Subred

Sistema Final: ES/host

Sistema Intermedio: IS (conecta 2 o más subredes)

Bridge (puente): conecta 2 o más LAN en alta 2. Subred única

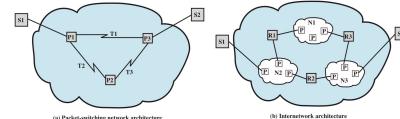
Router (encaminador): conecta redes heterogéneas en alta 3

Requisitos

Dispositivo de Interconexión → debe tener:

- direccionamiento
- tamaño mas grande
- mecanismos acceso red
- explotación de temporizadores
- recuperación de errores
- informes de estado

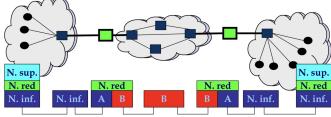
- técnicas de encaminamiento
- control de acceso al bufero
- conexión/sin conexión



Arquitectura de Protocolos

• de Redes + dispositivos Interconexión
y Protocolos en las superiores en los los multilayeres

cada interconexión termina a b almp de todas las redes q. posibliza avanzar el datagrama paso a paso hasta el destino



Redes NO Orientadas a Conexión

Internet: conectadas mediante IP

Diseño IP

No orientado a función

- sencillito
- flexibilidad de enrutamiento ante fallos y congestiones

Servicio no fiable (best-effort)

TCP
Resolución de problemas de extremo a extremo

Interconexión de Red de Redes

Internet → considerarse como una red

- IS → los nodos
- subredes → enlaces entre los nodos

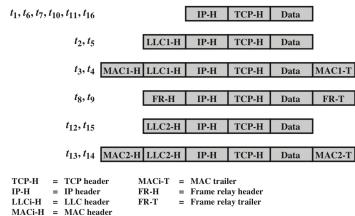
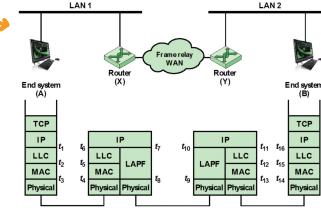
Redes Orientadas a Conexión

Cuando todos los nodos son orientados a conexión:



IS → reenviar paquetes recibidos por dicho trío
cada uno de los cuales es conectado a cada una de las redes
pero
solicitando conexión virtual con el siguiente IS
seco utilizado
salvo redes con = tecnología

Fig. Interconexión con IP



Internet Protocol (IP)

IP v4 definido en RFC 791:

- servicios ofrecidos a la capa superior (transporte)
- Protocolo: formato del paquete

Servicios IP

- la capa IP ofrece un solo servicio → a la capa de transporte
- terminología OSI: servicio no confirmado
- Primitivas

Send (request)

- Dirección origen
- Dirección destino
- Protocolo
- Indicadores de tipo de servicio
- Identificador
- Indicador de no fragmentación
- O de mida
- Longitud de datos
- Opciones
- Datos

Tiempo de vida (TTL)

→ si el encaminamiento gira correctamente
datagrama alcanza su destino

→ Si no → pueden existir bucles
• encaminamiento **estático** mal configurado
• encaminamiento **dinámico** en transiciones entre los momentos de establecimiento

→ Para q el datagrama no circule en la red (consumo recursos)
se marca en el datagrama → @ max de vida

se ✓ en cada ROUTER

Tema 2: Nivel de RED IP

Internet Protocol (IP)

Fragmentación y reensamblado

- Las distintas redes → pueden tener máx. de paquetes
MTU = Maximum Transfer Unit
- Routers → pueden tener q+ un datagrama en varios
FRAGMENTACIÓN → datagrama + fragmentos
- Recompuesto en el destino
REENSAMBLADO

Campos del datagrama utilizados:

- Identificador de la unidad de datos
dirección origen dirección destino identificador en protocolo tráfico portado ID.
- Largo de datos

Reensamblado en el destino

- memoria temporal → ir almacenando fragmentos recibidos
- routers no miran en orden
- no puede perderse algún fragmento

criterio

- @ de vida reensamblado
- Utilizac. @ vida datagrama
- si vence @ vida antes de recibir el ult fragmento → devolver fragmentos recibidos

Control de Errores

Un datagrama puede ser desvirtuado por un router

- Erros de bit
- Expiración @ de vida
- No pueden encaminarlos
- congestión

Desearle → notificar al ES fuente de error

IP: protocolo ICMP

Control de Flujo

Permite al ES que los IS limiten velocidad a q+ reciben info.
(por ejemplo)  el caudal"

EN IP se realiza mediante ICMP

Formato del datagrama IP

Bit:	0	4	8	16	19	31
Version	4 bits	III	Type of Service	Total Length		
Identification			Flags	Fragment Offset		
Time to Live					Header Checksum	
					Source Address	
					Destination Address	
					Options + Padding	

Versión → del Protocolo IP 4 bits: IPv4 6 bits: IPv6

IHL → [Internet Header length] longitud cabecera. [nun 20 bytes]

Total Length → del datagrama

Identification → nº secuencial único (identifica un datagrama)

- Entre cada par origen-destino
- Para cada protocolo superior

TOS: Type of Service → especificación origen

routine, Priority, Immediate, Flash...

Flags → paraímetro q+ podemos establecer con un solo bit

- Above fragments: indica q+ tienen más fragmentos q+ el datagrama original

- Don't Fragment por ejemplo cuando se sabe q+ destino no es capaz de reensamblar router q+ recibe datagrama. Don't Fragment de tamaño superior al MTU → lo desvirtua

Fragmet offset, TTL

- fragment offset (13 bits)

→ lugar donde se sitúa este fragmento dentro del datagrama original (de 64 bits)

TTL (Time To Live)

→ lim. del @ q+ un datagrama puede permanecer en la red → N° de saltos

→ hasta datagrama circule

→ router → documenta una unidad de TTL = 0 → router lo desvirtua

Protocol (8 bits)

→ identifica el protocolo situado inmediatamente por encima de IP en pila

→ suele pasar dentro del nivel 3

Campo protocol: indica q+ protocolo llevamos dentro uno del nivel 4 como TCP uno del nivel 3 como ICMP

Header Checksum (16 bits)

→ redundancia para la detección de errores → añade 80b a la cabecera

→ operación q+ haga con el nº de bits q+ tengo

↳ si me da el mismo número → cabecera está bien (reenvío)

↳ Si no me da el mismo número → cabecera está mal (desvirtua paquete)

el checksum puede variar (router puede modificar cabecera a propósito)

Source / Destination addresses

→ Source address (32 bits) → dirección IP host de origen

→ Destination Address (32 bits) → dirección IP destino

Options → opciones de usuario

campo optional no incluido en estos 20 bytes

end of options → Security, Extended Security...



Padding / Data

→ padding (longitud variable) → relleno q+ asegura q+ la cabecera IP tiene un nº entero ... 32 bits

datos de protocolo nivel superior

longitud no entero de 8 bits

longitud max. del datagrama: 64 Kbytes

Tema 2: Nivel de RED IP

Direccionamiento IP

dirección IP designa de forma única conexión un host \rightarrow red
 debe agrupar + examinamiento
 Direccionamiento jerárquico
 debe ser \rightarrow configurable
 cambio host Subred
 cambiar IP

Direcciones N₂ y N₃

N₂ address:
 identificador de forma única: una estación \rightarrow red local (a nivel 2)
 basa en un identificador que sea único (red de difusión)
 (normalmente) nº \rightarrow asignado: fábrica
 \rightarrow nº en el firmáculo

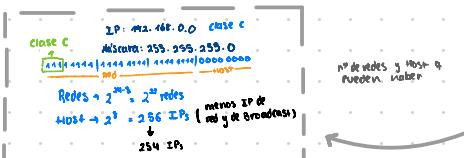
N₃ Address:
 identificador de forma única: un host una internet (a nivel 3)
 dirección \rightarrow localizar dicho host [para facilitar examinamiento]
 dirección debe ser: configurable (según donde se sitúe el host)

Algoritmos de dirección son necesarios,
 y hace falta traducir entre ellos: ARP, RARP

Asignación de direcciones

IANA: Internet Assigned Numbers Authority

delega en regional... \rightarrow African..., Asia-Pacific,...
 National...
 Local...



Dirección IP

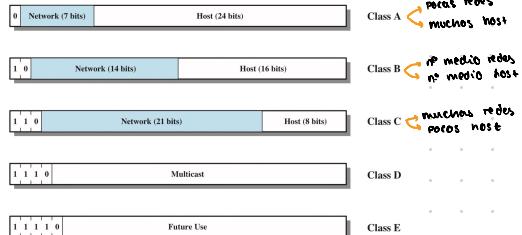
Largo: 32 bits

Notación: punto decimal ["Dotted decimal"]

\downarrow dirección en 4 bytes
 traduce a decimal

31	24 23	16 15	8 7	0
11001100	00001111	10001000	00110010	
204	15	136	50	
			204.15.136.50	

Direccionamiento con clase



Máscara de Red

network mask

nº binario a 32 bits

Señala la parte de red de la dirección IP

Parte red: 1

Parte host: 0

11001100	00001111	10001000	00110010
204	15	136	50

11111111	11111111	11111111	00000000
255	255	255	0

Valores Permitidos

dirección IP con todo unos \rightarrow difusión (broadcast) en esa red local

Primer dirección IP en una red \rightarrow host todo a cero

\hookrightarrow la dirección de la red

Otro: AND binary dirección IP y dirección red

Última dirección IP \rightarrow host todo a uno

\hookrightarrow dirección broadcast dirigida

HOST \rightarrow todo 1
 red \rightarrow todo 0 \rightarrow para un HOST

Bloques de direcc. reservadas

0.0.0.0/8

10.0.0.0/8 \rightarrow privado

127.0.0.0/8 \rightarrow loopback

Para mandarnos cosas a nosotros mismos, \rightarrow no se puede asignar a ningún dispositivo

192.16.0.0/12] privado

192.168.0.0/16

169.254.0.0/16

Cálculo de las Redes

Caract. de la dirección

Nº bits red: Bn

Nº bits host: Bn

Nº bits clase: Bn

+ 32 bits

Clase A \rightarrow 0... \rightarrow 2²⁴-2

Clase B \rightarrow 10... \rightarrow 2¹⁶-2

Clase C \rightarrow 110... \rightarrow 2⁸-2

Caract. de las redes

Nº redes : Nn

Nº host en cada red: Nn

los partes red/host \rightarrow 2³²⁻ⁿ - 2

Nn = 2⁸ - 2

Nn = 2⁸ - 2

Direcciones IP públicas y privadas

Direcciones Públicas

(las de Internet)

únicas a nivel global

Adjudicación regulada

Direcciones Privadas

→ ocultados (no conectados a Internet)

→ pueden repetirse en toda red

→ No DCC con una dirección Pública (directamente)

→ Rangos de direcciones IP para uso interno y privado (no se encuentran red Pública)

Clase	Direcciones privadas RFC 1918
A	10.0.0.0
B	172.16.0.0 a 172.31.0.0
C	192.168.0.0 a 192.168.255.0

Nivel de RED IP

Direccionamiento IP

Agregación



CIDR (Classes, InterDomain Routing)

- Esquema de direccionamiento IP
- Reemplaza estructura directa IP original (con clase)
 - enrutar mejor directo existentes
 - intercambio info. rutas
- Combinación VLSM + Organiza jerárquicamente direcciones IP globales
- Nuevos protocolos de encaminamiento CIDR
 - classless routing implementan máscaras
 - dejan obsoletas versiones originales (classful routing)

Direccionamiento Estático y dinámico

Asignación dirección IP a un host:

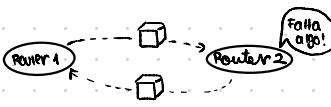
- Dirección estática \rightarrow establecida por config. manual
- Dirección dinámica \rightarrow asignada automáticamente
 - equipo se conecta temporalmente a la red
 - hay conjunto limitado direcciones

Mecanismos de agrupación dinámica de direcciones

- DHCP: Dynamic Host Configuration Protocol
- IPCP: IP Configuration Protocol
- RARP: Reverse Address Resolution Protocol

Internet Control Message Protocol (ICMP)

- Protocolo
 - control flujo
 - notificación de errores
 - ayuda IP \rightarrow para hacer retenciones
- Sobresalto
 - nivel 3
 - mensajes info y error

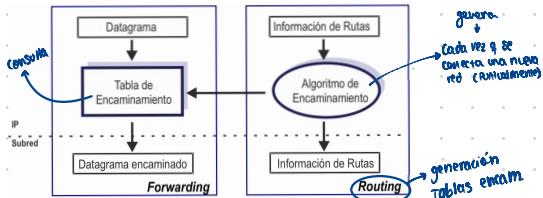


Encaminamiento IP

Objetivo: del Ruta a seguir Implementación: Tabla encaminamiento en los routers

- En IP \rightarrow Modelo Salto a Salto: solo interesa el Siguiente Salto
- Métrica e Coste: Permite seleccionar ruta más óptima \rightarrow redes de otro operador \rightarrow EC
- Protocolo de encaminamiento
 - obtiene info. sobre encaminamiento \rightarrow actualiza tabla encom.
 - Requiere intercambio info. con otros encaminadores
 - dinámico \rightarrow otra posibilidad: estático

Forwarding y Routing



Tablas de encaminamiento

- Contiene Mejores Rutas
 - estícticas (B manejable)
 - dinámicas (obtenidas) routers encaminam.)
- Cada fila en la Tabla incluye
 - Red o host del destino (dirección y másc./negro)
 - Dirección IP Prox. Salto
 - Métrica de la Ruta (saltos, retraso, ancho banda...)
 - Interfaz Salida

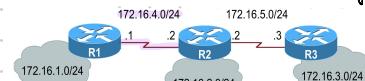
Selección de Rutas

- Menor Coste
- distancia administrativa \rightarrow asociar pesos a primaria entre otras
- Routers \rightarrow Rutas con \leftarrow coste \rightarrow activa balanceo de carga

conexión directa = 0
ruta estática = 1
IGRP = 100

Encaminamiento estático

Se asocian redes conocidas \rightarrow indicando IP del siguiente Salto

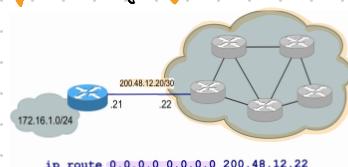


En el router R2:

ip route 172.16.1.0 255.255.255.0 172.16.4.1
ip route 172.16.3.0 255.255.255.0 172.16.4.1

saliente a través

Ruta por defecto



ip route 0.0.0.0 0.0.0.0 200.48.12.22

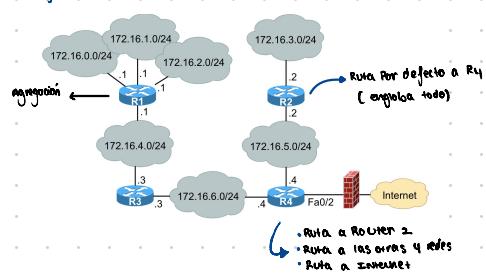
Nivel de RED IP

Encaminamiento IP

CIDR. Longest Match

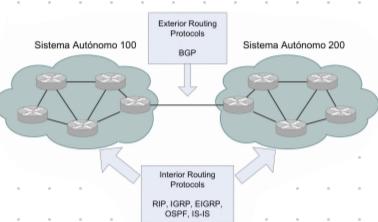
- Redes con direccionamiento SIN Clases \rightarrow intercambian máscaras y direcc. destino (CIDR, Classless Inter-Domain Routing)
- Tabla enrutamiento \rightarrow (puede) rutas = destino \leftrightarrow máscaras
 - \downarrow del Salto
 - Ruta más específica o longest match \rightarrow Ruta más larga

Ejemplo:



Sistema Autónomo (SA o AS)

- Conjunto Subredes conectadas con una administración estrategia enrutamiento común
- Cada SA establece protocolo intercambia info con otros SA
- Internet formada SA's interconectados
- Clasificación
 - \hookrightarrow Interior Gateway Protocol [IGP]
 - \hookrightarrow Exterior Gateway Protocol [EGP]



Protocolos: Requerimientos y Clasificación

objetivos

- Optimización
- Simplicidad
- Estabilidad
- Flexibilidad
- Convergencia rápida

Tipos

- Vector-Distancia
- Estado del enlace
- Vector-Camino

Vector-Distancia (VD)

Info Mantenida:

- vector de costos
- vector distancias
- vector siguiente salto

Info. intercambiada:

- \downarrow Router 2 \rightarrow Vector distancias
- \downarrow Router 2 \rightarrow Routers vecinos

funcionamiento:

Router 2 \rightarrow Router 2 \rightarrow Vector distante.
Router 2 recibe vector distante.

Algoritmo Bellman-Ford

Ventajas: Algoritmo simple

Desventajas:

- Gran cantidad de routers
- Convergencia lenta
- Genera bucles algunos veces
- Ineficiente \rightarrow redes grandes
- No obtiene visión topológica de la red

Estado de Enlaces (LS)

Info Mantenida:

- Estado y coste de los enlaces

Info. intercambiada:

- \downarrow Router 2 \rightarrow Estado enlaces routers vecinos
- \downarrow Router 2 \rightarrow Routers de la red

funcionamiento:

- Router 2 \rightarrow Router 2 \rightarrow Estado
- Router 2 recibe Estado
- obtiene topología de la red \rightarrow calcula mejores rutas

Vector Camino (VC)

Info. mantenida:

- vector de caminos

Info. intercambiada:

- \downarrow Router 2 \rightarrow vectores caminos
- \downarrow Router 2 \rightarrow Routers vecinos

funcionamiento:

- VD
- Presente métricas (costos)
- se relacionan todos los AS a través SAR

Algoritmo Dijstra & SPF

Ventajas:

- Envío \rightarrow menos info.
- convergencia más rápida
- más eficiente \rightarrow redes grandes
- se puede simular \rightarrow visión topográfica

Inconvenientes:

- Algoritmo más complejo
- Mayor consumo recursos

Ventajas:

- evitan problemas de intransitividad (no métricas)
- lista AS a atravesar.

un AS tiene tener políticas internas q morgan en cuenta
los ciclos de todo AS
 \downarrow
seguimiento, rendimiento, calidad, facilidad

Bucle de Encaminamiento

bucle / loops: se generan por inconsistencias en la tabla de enrutamiento

Soluciones para limitar su efecto:

- Guiente al oo \rightarrow infinity
- Horizonte dividido: SPF+Horizon
- Enrutamiento inverso: poison Reverse
- Actualización por eventos triggers
- Temporizadores de espera holdown timers

Protocolos Classful y classless

Protocolos classless \rightarrow incluyen prefijo asociado a los rétes de destino (comparte con CIDR)

- IPv4 \rightarrow si usamos másc: no extienden \Rightarrow classless
- IPv6 \rightarrow siempre classless

te queremos +3:3

NIVEL DE RED IP

Resolución de direcciones. ARP

Necesidad: Hacer corresponder direcciones de N₃ → N₂

- Conocida dirección N₃ (global) averiguar N₂ (local) → N₂ local
- ESTÁ en la misma LAN → si no → N₂ local no necesita la dirección N₂ de una estación en otra LAN
- "Envía datos a dir MAC_D"



- Si 3 correspondencia directa N₂ ↔ N₃
- Producir 3 fxs q mapean N₂ a partir N₃
- Dir N₃: 192.5.49.2 → iguales
- Dir N₂: 2 → iguales

+ Podrían introducirse en la red nuevas máquinas → nuevas direcc. → sin tener q añadir info.

+ Requiere q la direc. MAC sea configurable

- Si 3 correspondencia directa N₂ ↔ N₃

+ Tabla estática de correspondencias (config. manualmente)

- Laborioso + propenso errores
- Habría q act tablas → introduce nueva
- Habría q borrar Tabla → lleva a otra LAN

+ Tabla dinámica de correspondencias (actualiz. autom.)

correspondencia dinámica "Dynamic binding"

Address Resolution Protocol (ARP)

FU(Ch)amiento basado en difusión

diseñado de forma genérica → varios niveles 3 → varios niveles 2

Materialización más típica:

$$\begin{array}{l} N_3 = \text{IP} \\ N_2 = \text{Ethernet} \end{array}$$

FU(Ch)amiento de ARP

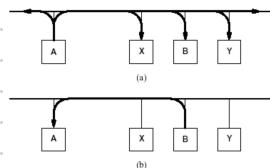
- Estación A → ARP REQUEST → por broadcast → "¿Quién tiene la dirección IP q. q. querer saber?"

contiene → direc. MAC y IP origen

Estación q. la tiene:

- Estación B → responde → ARP RESPONSE a Estación A
- mensaje unicast

- Estación A → apunta la correspondencia entre direcc. N₃ y N₂ en su tabla ARP (nuevos usos)



Temporizador de la tabla ARP

Controlar crecimiento → cada entrada se elimina tras cierto tiempo @ no utilización

Valor del temporizador suele ser configurable

Windows → 2 min.
Unix → 30 min

Refinamientos de ARP

evitar necesidad de difundir ARP REQUEST

- Host al q. va dirigido un ARP REQUEST

↓ apunta direc. Mac + IP del origen

- Cualquier otro host → ↓ apunta correspondencia

- Cuando host arranca → ↓ ARP REQUEST

toda la red ↓ correspondencia entre sus direcc. IP y MAC

Reverse ARP (RARP)

- Permite averiguar direcc. IP → correspondiente a una direcc. MAC

- OpCode: Request y Response

- FU(Ch)amiento inverso a ARP

