tutoría Redes de Datos

Capítulo 3: Capa de red

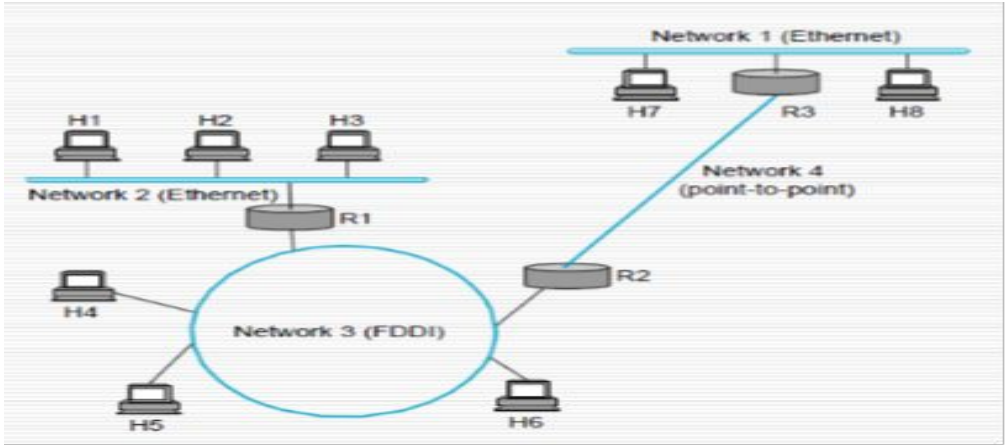
udp Escuela de Informática y Telecomunicaciones
FACULTAD DE INGENIERÍA Y CIENCIAS

Ph.D. Nicolás Boettcher

¿Para qué sirve?

El protocolo IP pretende resolver el problema de conectar diversas redes locales, que además pueden ser de diversos tipos.

A este concepto se le conoce como internet working.

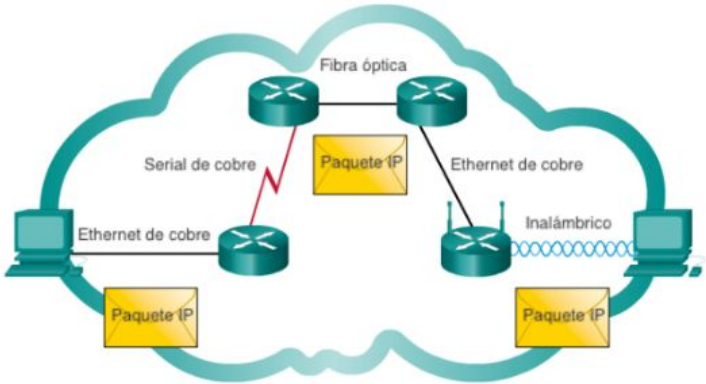


¿Servicio no confiable?

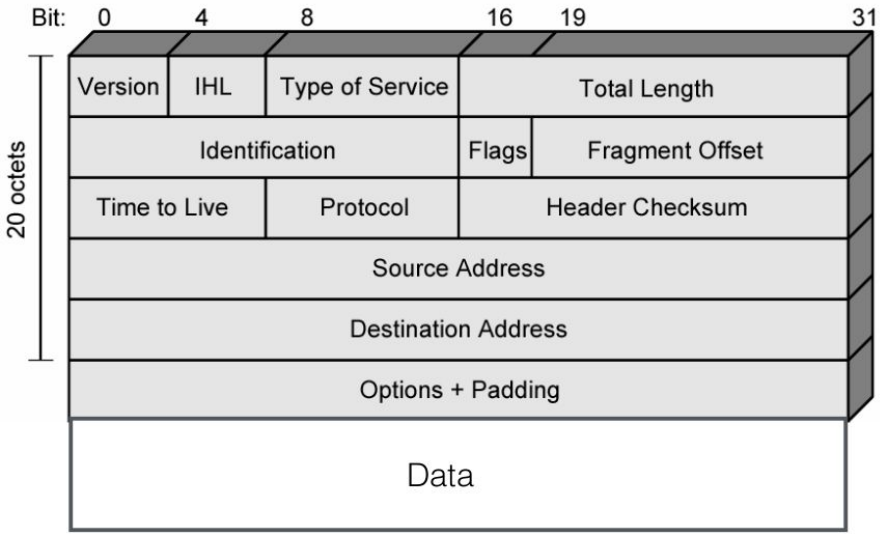
- Cada datagrama contiene suficiente información para permitir que la red se encargue de hacerlo llegar a destino independientemente.
- Si algo anda mal y el datagrama se pierde, corrompe, se despacha a otro lugar y cualquier otra cosa, la red no hace nada para corregirlo. Esto lo convierte en un servicio no confiable.
- Si se ofrece un servicio confiable sobre una red no confiable, es necesario colocar mucha inteligencia en los componentes para sobrellevar el problema.
- Hacer que los routers sean simples es uno de los objetivos iniciales de IP.
- La idea de “mejor esfuerzo” no sólo implica a veces que los datagramas se pierdan, sino que lleguen desordenados o duplicados. Se espera que las capas superiores se encarguen de dichas circunstancias.
- La habilidad de funcionar sobre cualquier cosa es otra de las fortalezas de IP.

Relación con L2

- IP funciona independiente del medio de comunicación.
- Capa de enlace de datos se encarga de prepararlo para su transmisión en la red.
- Hay una restricción! el tamaño máximo del paquete a transmitir.



Datagrama IP




```
Internet Protocol Version 4, Src: 192.168.1.129, Dst:
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN:
    Total Length: 68
    Identification: 0x1aca (6858)
  ▸ 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
  ▸ Time to Live: 1
    Protocol: UDP (17)
    Header Checksum: 0xf841 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.129
    Destination Address: 192.112.36.4
```

```
0000  e4 ab 89 bb 06 a8 dc 21  48 24 f8 56 08 00 45 00
0010  00 44 1a ca 00 00 01 11  f8 41 c0 a8 01 81 c0 70
0020  24 04 50 0b 82 a0 00 30  a6 df 09 33 68 74 74 70
```

Maximum Transmission Unit (MTU)

Source	Destination	Protocol	Length	Info
192.168.31.178	1.1.1.1	ICMP	35	Echo (ping) request id=0x0002, seq=1/256, ttl=64
1.1.1.1	192.168.31.178	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=c8
1.1.1.1	192.168.31.178	ICMP	60	Echo (ping) reply id=0x0002, seq=1/256, ttl=55
192.168.31.178	1.1.1.1	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=27
192.168.31.178	1.1.1.1	ICMP	60	Echo (ping) request id=0x0003, seq=1/256, ttl=64
1.1.1.1	192.168.31.178	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=d8
1.1.1.1	192.168.31.178	ICMP	60	Echo (ping) reply id=0x0003, seq=1/256, ttl=55

ping -s 1473 vs ping -s 1498

Jumbo Packets

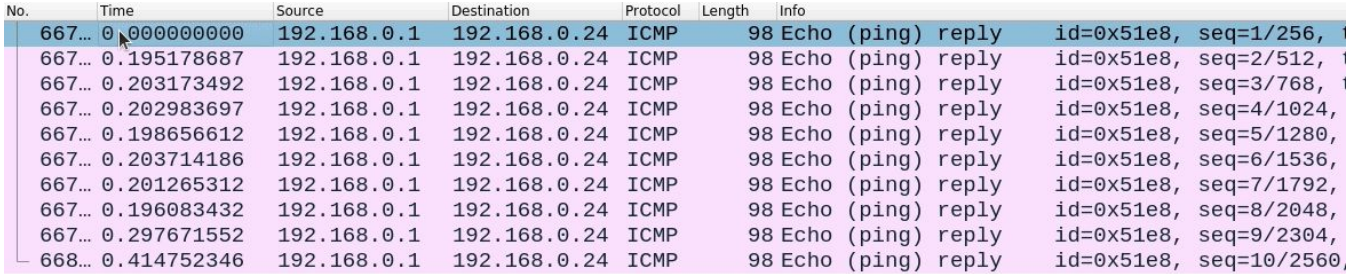
```
ifconfig lo
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
```

No.	Time	Source	Destination	Protocol	Length	Info
1154	0.00006…	127.0.0.1	127.0.0.1	TCP	65549	8000 → 59290
1155	0.00001…	127.0.0.1	127.0.0.1	TCP	66	59290 → 8000
1156	0.00000…	127.0.0.1	127.0.0.1	TCP	119	8000 → 59290
1157	0.00006…	127.0.0.1	127.0.0.1	TCP	65549	8000 → 59290

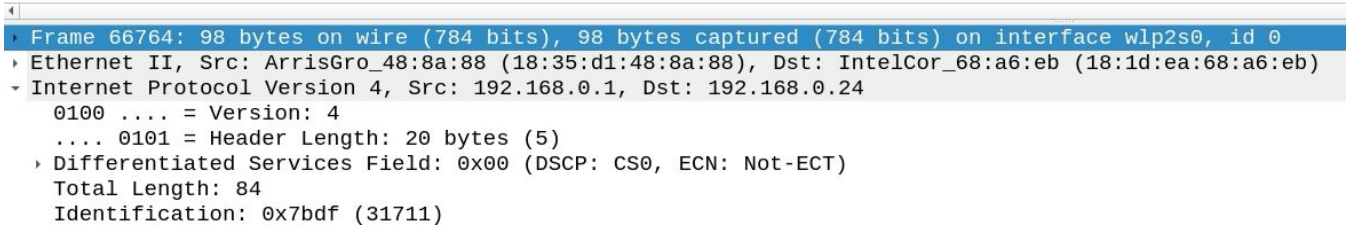
```
▸ Frame 1154: 65549 bytes on wire (524392 bits), 65549 bytes ca
▸ Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst
▾ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▾ Differentiated Services Field: 0x02 (DSCP: CS0, ECN: ECT(0)
      0000 00.. = Differentiated Services Codepoint: Default (0
      .... ..10 = Explicit Congestion Notification: ECN-Capable
    Total Length: 65535
    Identification: 0x8946 (35142)
  ▸ Flags: 0x4000, Don't fragment
```

Estructura Datagrama IP

Identification: contiene el número del datagrama el cual identifica el fragmento para su reconstrucción.

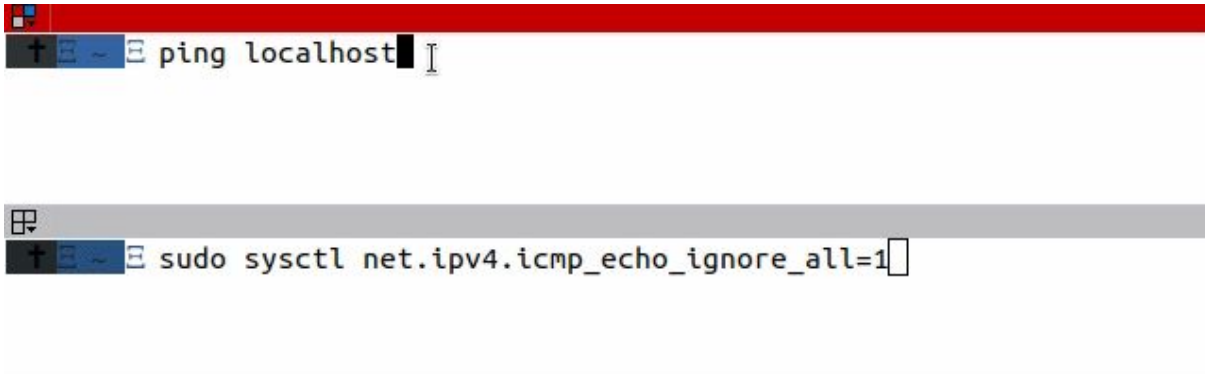


No.	Time	Source	Destination	Protocol	Length	Info
667…	0.000000000	192.168.0.1	192.168.0.24	ICMP	98	Echo (ping) reply id=0x51e8, seq=1/256,
667…	0.195178687	192.168.0.1	192.168.0.24	ICMP	98	Echo (ping) reply id=0x51e8, seq=2/512,
667…	0.203173492	192.168.0.1	192.168.0.24	ICMP	98	Echo (ping) reply id=0x51e8, seq=3/768,
667…	0.202983697	192.168.0.1	192.168.0.24	ICMP	98	Echo (ping) reply id=0x51e8, seq=4/1024,
667…	0.198656612	192.168.0.1	192.168.0.24	ICMP	98	Echo (ping) reply id=0x51e8, seq=5/1280,
667…	0.203714186	192.168.0.1	192.168.0.24	ICMP	98	Echo (ping) reply id=0x51e8, seq=6/1536,
667…	0.201265312	192.168.0.1	192.168.0.24	ICMP	98	Echo (ping) reply id=0x51e8, seq=7/1792,
667…	0.196083432	192.168.0.1	192.168.0.24	ICMP	98	Echo (ping) reply id=0x51e8, seq=8/2048,
667…	0.297671552	192.168.0.1	192.168.0.24	ICMP	98	Echo (ping) reply id=0x51e8, seq=9/2304,
668…	0.414752346	192.168.0.1	192.168.0.24	ICMP	98	Echo (ping) reply id=0x51e8, seq=10/2560,



```
Frame 66764: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface wlp2s0, id 0
Ethernet II, Src: ArrisGro_48:8a:88 (18:35:d1:48:8a:88), Dst: IntelCor_68:a6:eb (18:1d:ea:68:a6:eb)
Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.24
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x7bdf (31711)
```

Disable/Enable ICMP reply



¿Qué ventajas tiene segmentar?

- Eficiencia
  - Un segmento IP requiere estar en el mismo dominio de broadcast.
  - Si tenemos muchos nodos en el mismo segmento, aumentamos las posibilidades de colisión y disminuimos el rendimiento.
- Seguridad
  - Podemos aplicar reglas o filtros de tráfico entre segmentos IP.
- Administración
  - Definimos segmentos IP en base a funciones, que requieren tipos de servicio diferentes.
  - Cada red IP puede recibir un tratamiento diferente, distintos servicios, etc.

IPs para una LAN

- IANA define un bloque de IPs reservados que permiten a las organizaciones su utilización en redes privadas sin solicitud alguna.
- Estos bloques reservados se les conoce como **direcciones privadas**, pues está prohibido su uso en redes públicas como Internet.

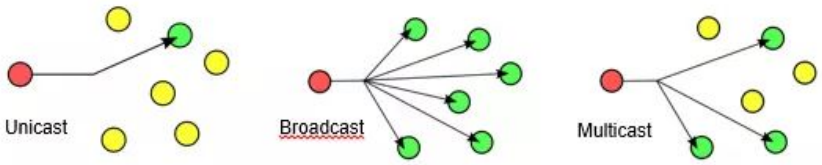
Podríamos decir que las frecuencias de libre uso del espacio radioeléctrico son una analogía a las ips privadas dentro del espacio de la totalidad de las ips.

	Octeto	Octeto	Octeto	Octeto
Binario	11000000	00000101	00100010	00001011
Decimal	192	5	34	11

Públicas vs Privadas

- **Direcciones IP públicas:** Son visibles en todo Internet. Un nodo con una IP pública es accesible (visible) desde cualquier otro nodo conectado a Internet. Para conectarse a Internet es necesario tener una dirección IP pública.
- **Direcciones IP privadas (reservadas):** Son visibles únicamente por otros nodos de su propia red o de otras redes privadas interconectadas por routers. Se utilizan en las empresas para los puestos de trabajo. Los nodos con direcciones IP privadas pueden salir a Internet por medio de un router (o proxy) que tenga una IP pública.

Clases de direcciones IPs



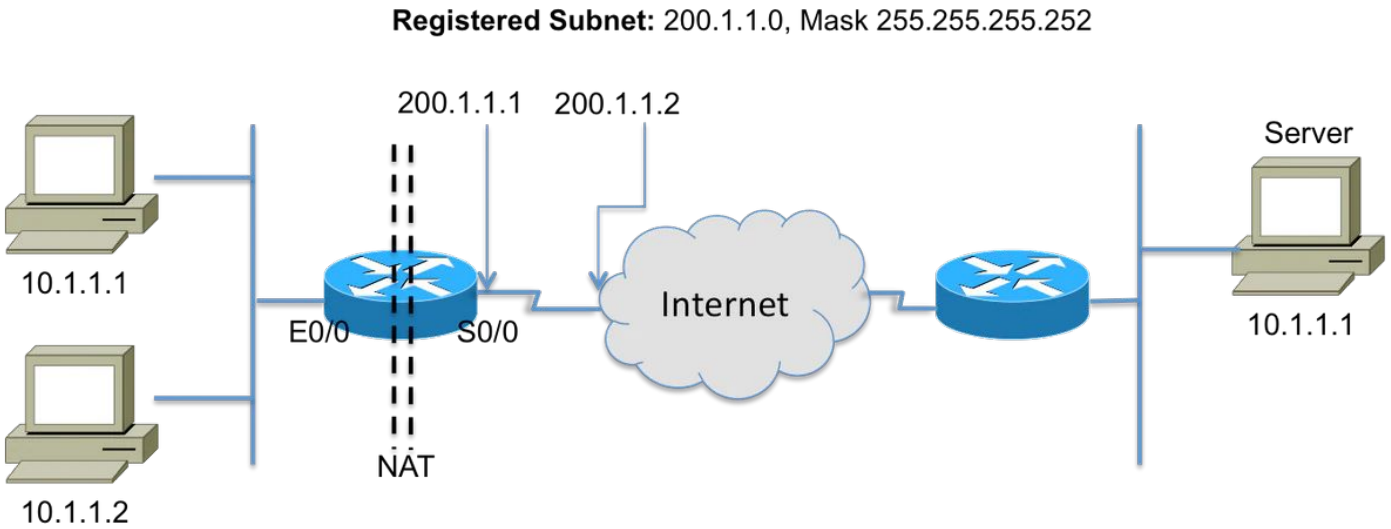
Red o rango	Uso
127.0.0.0	Reservado (fin clase A)
128.0.0.0	Reservado (ppio. clase B)
191.255.0.0	Reservado (fin clase B)
192.0.0.0	Reservado (ppio. clase C)
224.0.0.0	Reservado (ppio. clase D)
240.0.0.0 – 255.255.255.254	Reservado (clase E)
10.0.0.0	Privado clase A
172.16.0.0 – 172.31.0.0	Privado clase B
192.168.0.0 – 192.168.255.0	Privado clase C

```
curl ifconfig.me/ip
186.156.125.25%
ifconfig wlp2s0
wlp2s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.24  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::49e7:4e54:dfa:4014  prefixlen 64  scopeid 0x20<link>
        ether 18:1d:ea:68:a6:eb  txqueuelen 1000  (Ethernet)
        RX packets 285150  bytes 303044989 (303.0 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 152143  bytes 41931840 (41.9 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

NAT: Network Address Translation

- Solución para la escasez de IPs
- ISP asigna 1 IP para cada hogar o empresa
- Dentro de la red, cada equipo tiene un IP único perteneciente a la red privada
- Para lograr comunicar con el resto de las redes, se realiza un proceso de traducción entre las IP privadas a la IP pública

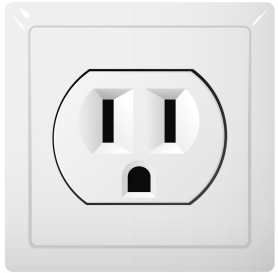
Dynamic NAT



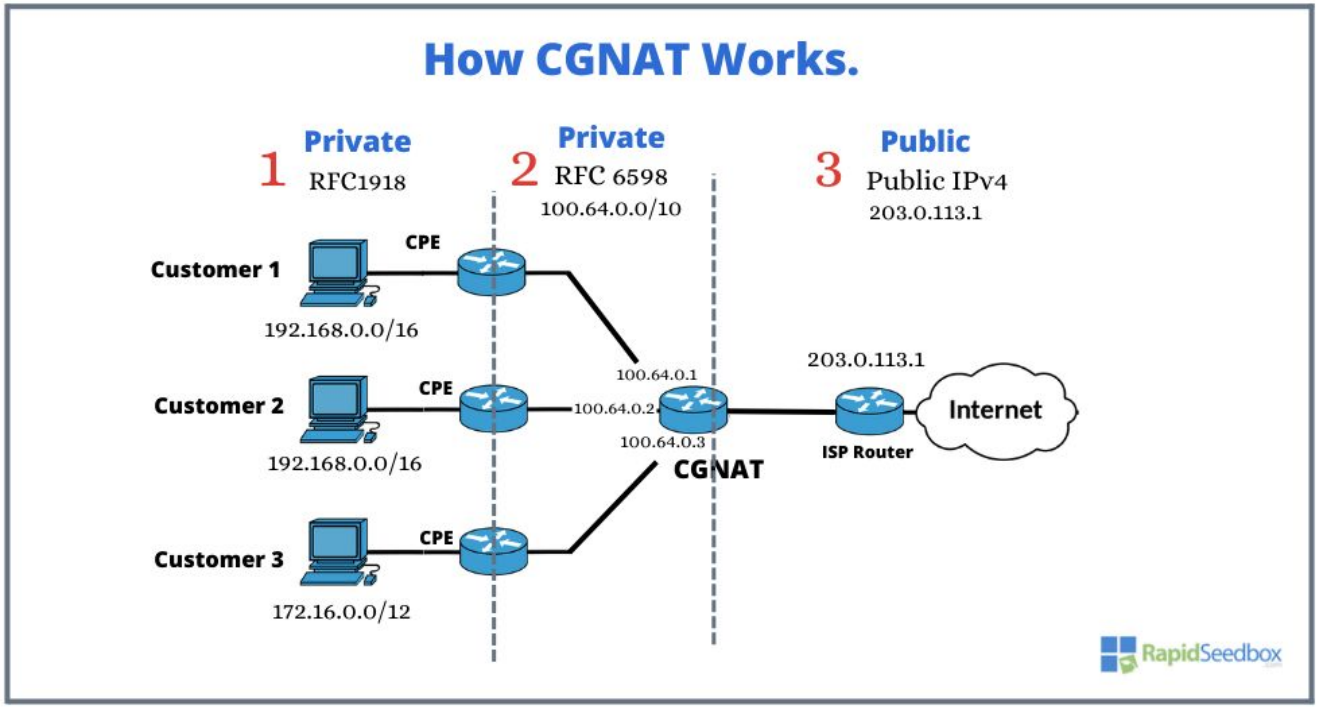
Inside Local	Inside Global
10.1.1.1:3212	200.1.1.1:3212
10.1.1.1:3213	200.1.1.1:3213
10.1.1.2:38913	200.1.1.1:38913

Inside

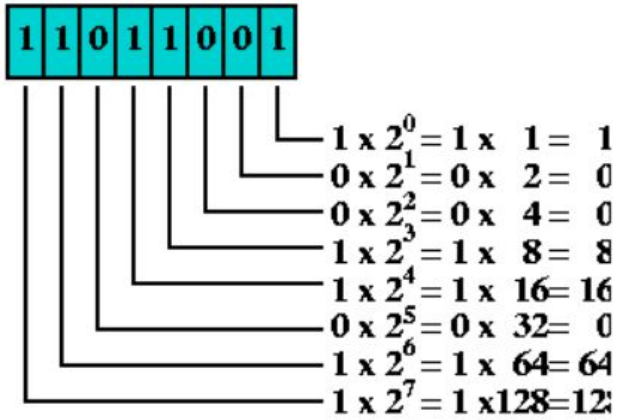
Outside



CGNAT (Carrier-Grade NAT)



Binario & decimal



$$1 + 8 + 16 + 64 + 128 = 217$$

Decimal number 225

Division	Quotient	Remainder	
225 / 2	112	1	← LSB
112 / 2	56	0	
56 / 2	28	0	
28 / 2	14	0	
14 / 2	7	0	
7 / 2	3	1	
3 / 2	1	1	
1 / 2	0	1	

Binary number 1 1 1 0 0 0 0 1

Decimal number 8

Division	Quotient	Remainder	
8 / 2	4	0	← LSB
4 / 2	2	0	
2 / 2	1	0	
1 / 2	0	1	
		0	
		0	
		0	
		0	

Binary number 0 0 0 0 1 0 0 0

Decimal number 77

Division	Quotient	Remainder	
77 / 2	38	1	← LSB
38 / 2	19	0	
19 / 2	9	1	
9 / 2	4	1	
4 / 2	2	0	
2 / 2	1	0	
1 / 2	0	1	
		0	

Binary number 0 1 0 0 1 1 0 1

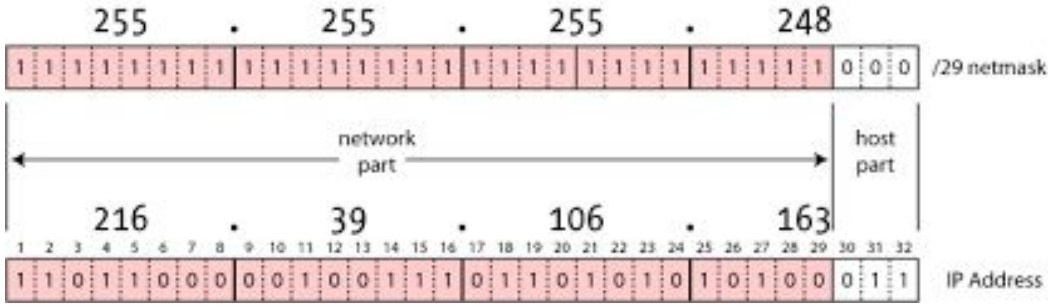
Decimal number 254

Division	Quotient	Remainder	
254 / 2	127	0	← LSB
127 / 2	63	1	
63 / 2	31	1	
31 / 2	15	1	
15 / 2	7	1	
7 / 2	3	1	
3 / 2	1	1	
1 / 2	0	1	

Binary number 1 1 1 1 1 1 1 0

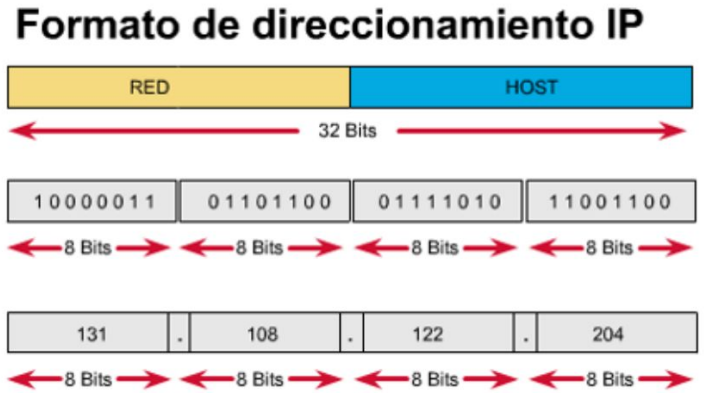
Máscara de red

- Está compuesta por una secuencia de 1s y 0s
- Permite conocer rangos de IPs
- Al hacer un AND con una dirección IP de una red, permite obtener la IP inicial y final de la red.



Prefijo

- Formado por IP/Mask
- Tamaño del prefijo no puede ser calculado solo con la IP
- IP + tamaño: 131.108.0.0 / 16, se debe enviar el tamaño igualmente
- Subnet Mask → 16 representa número de 1’s incluidos en la máscara
- IP AND Mask → Parte que representa la red



Ventajas del esquema jerárquico

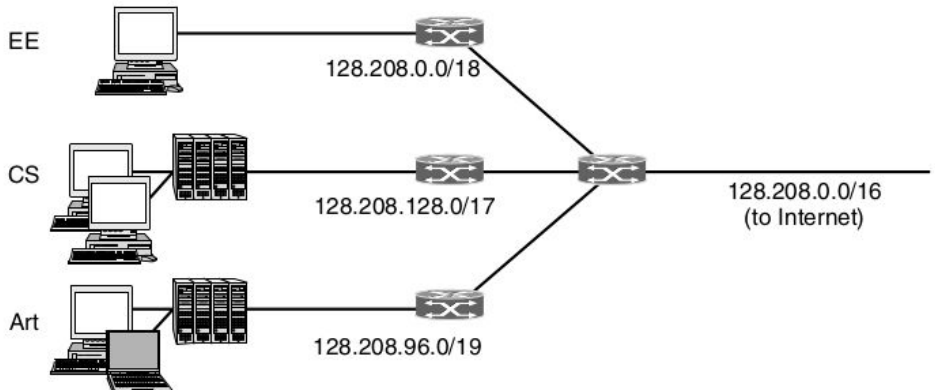
- Solo utiliza la parte de red para “rutear” paquetes disminuyendo los tamaños de las tablas de los routers
- Cuando llega a la red de destino, se utiliza la información del host para entregar el paquete
- Tamaño de las tablas son del orden de 300.000 prefijos, con Internet actual, lo cual le permite escalar

Desventajas del esquema jerárquico

- Uso ineficiente de las IPs a menos que haya una cuidadosa administración
- Si se asignan bloques de direcciones muy grandes pueden quedar muchos IPs sin uso
- Con el crecimiento de internet las IPs son un bien escaso

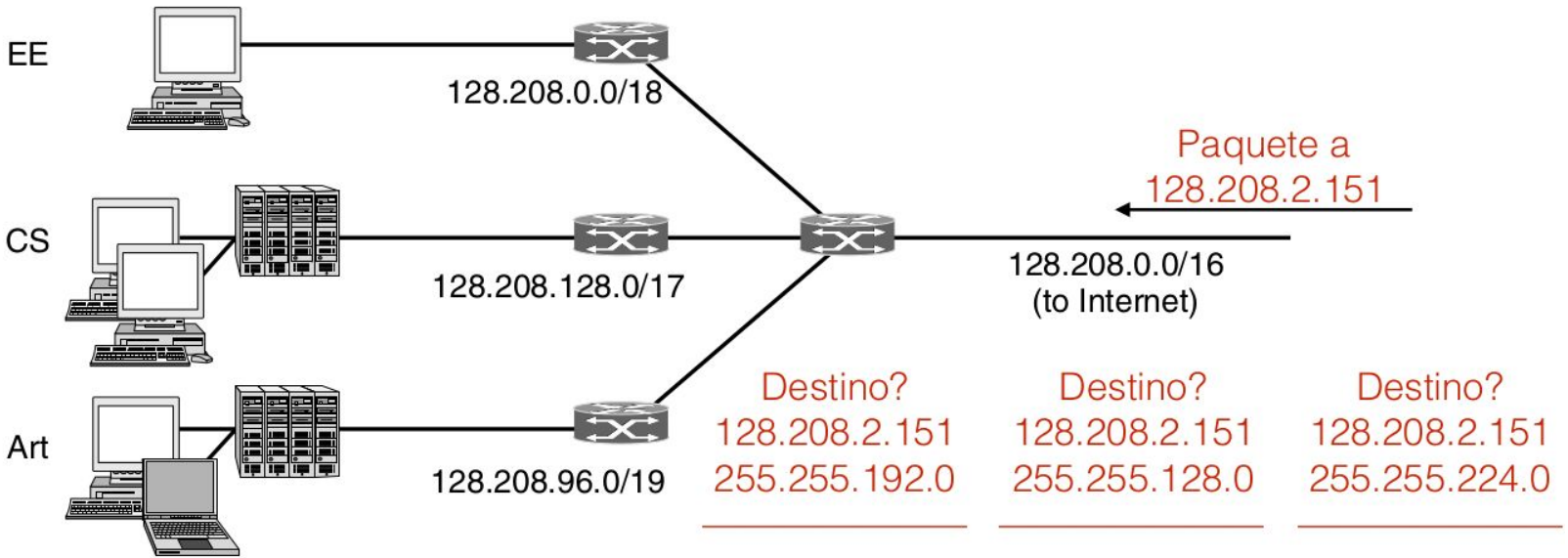
Subredes

- Subredes son segmentos de nodos de la red
- Cada segmento de la red está identificado por un prefijo de red
- Todos los host de dicho segmento poseen el mismo prefijo
- ¿Para qué sirven?

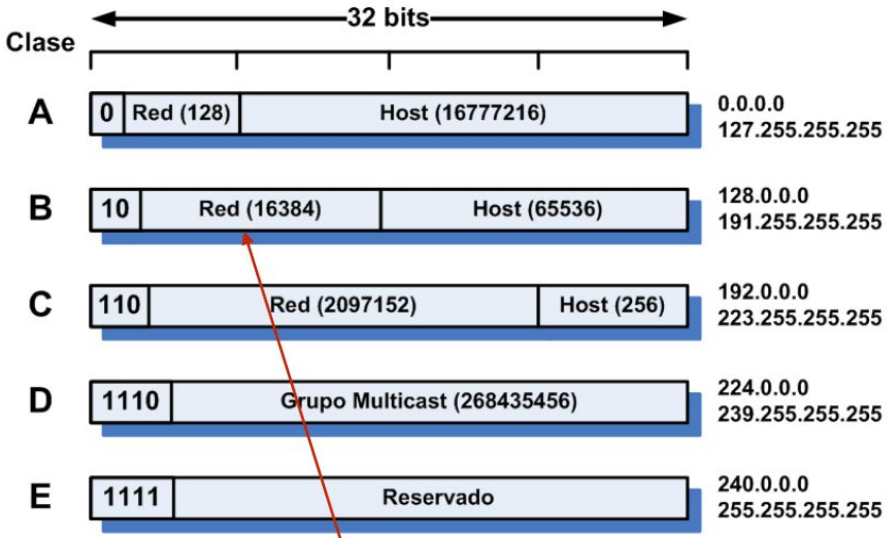


Ejemplo de subred

Computer Science:	10000000	11010000	1lxxxxxxx	xxxxxxxx
Electrical Eng.:	10000000	11010000	00lxxxxxx	xxxxxxxx
Art:	10000000	11010000	011lxxxxx	xxxxxxxx



Clases de IPs



Class	Leading bits	Size of *network*	Size of *rest* bit field	Number of networks	Addresses per network	Start address	End address
A	0	8	24	128 (2^7)	16,777,216 (2^{24})	0.0.0.0	127,255,255,255
B	10	16	16	16,384 (2^{14})	65,536 (2^{16})	128.0.0.0	191,255,255,255
C	110	24	8	2,097,152 (2^{21})	256 (2^8)	192.0.0.0	223,255,255,255

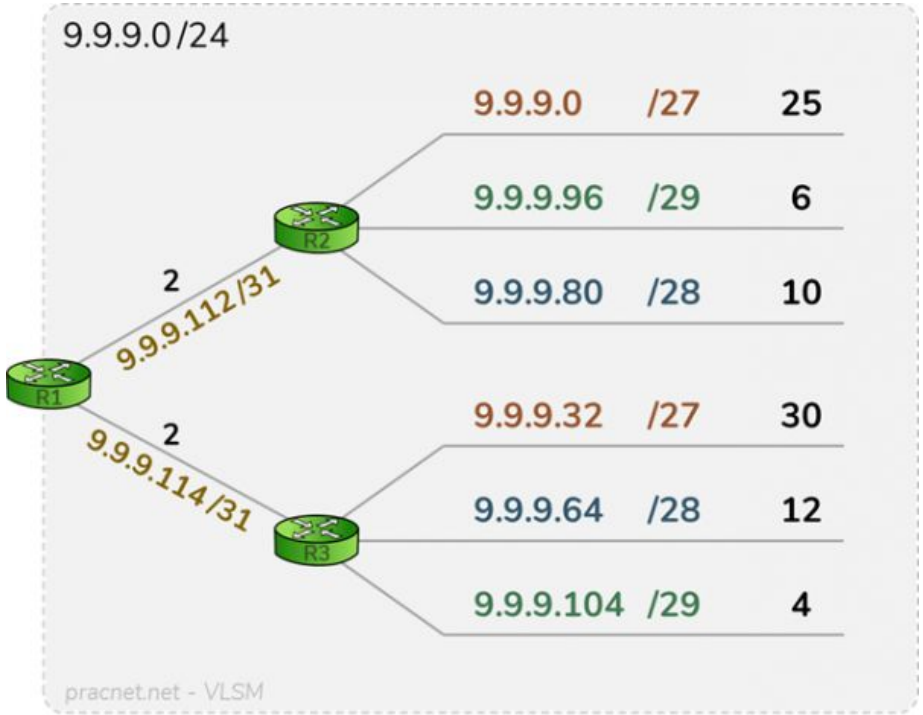
CIDR (Classless Inter Domain Routing)

Clase	Prefijo CIDR	Rango	
A	10.0.0.0/8	10.0.0.0 – 10.255.255.255	1 dirección clase A
B	172.16.0.0/12	172.16.0.0 - 172.31.255.255	16 direcciones clase B
C	192.168.0.0/16	192.168.0.0 - 192.168.255.255	256 direcciones clase C

Subnet Mask

Suffix	Hosts	32-Borrowed=CIDR	2^Borrowed = Hosts	Binary=> dec = Suffix
.255	1	/32	0	11111111
.254	2	/31	1	11111110
.252	4	/30	2	11111100
.248	8	/29	3	11111000
.240	16	/28	4	11110000
.224	32	/27	5	11100000
.192	64	/26	6	11000000
.128	128	/25	7	10000000

VLSM (Variable Length Subnet Masking)



- Lo que tradicionalmente se utiliza es un tamaño de máscara variable.
- Máscara variable permite adaptarse a las necesidades y reducir el desperdicio de IPs.
- La parte red y la parte host no son iguales en todas las subredes.
- Aunque las subredes pueden tener diferente tamaño no pueden solaparse.

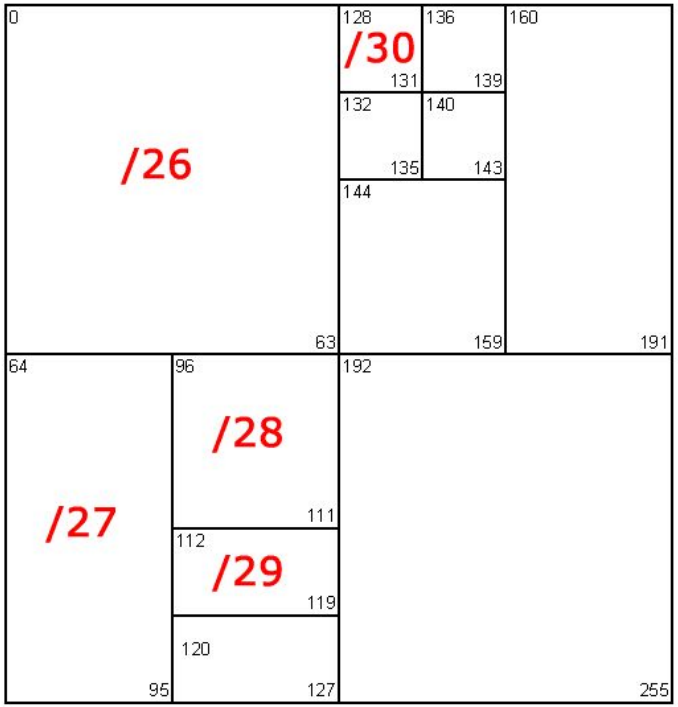
Ejemplo VLSM

Se tiene una red **clase C** cuya dirección base es **192.168.10.0/24**. Se quiere dividir dicha red en 4 subredes. Subred **A** con 50 host, subred **B** con 20 host, subred **C** con 10 host, y subred **D** con 10 host. Determine una manera de asignar direcciones utilizando VLSM. Identifique número de hosts, rango de IPs disponibles, dirección de broadcast, y máscara de cada subred.

Ejemplo VLSM

RED:#	Host (2^n)	n	Red	Mascara	Rango Util	Broadcast
A: 50	64	6	192.168.10.0	255.255.255.192 /26	192.168.10.1 - 192.168.10.62	192.168.10.63
B: 20	32	5	192.168.10.64	255.255.255.224 /27	192.168.10.65 - 192.168.10.94	192.168.10.95
C:10	16	4	192.168.10.96	255.255.255.240 /28	192.168.10.97 - 192.168.10.110	192.168.10.111
D:10	16	4	192.168.10.112	255.255.255.240 /28	192.168.10.113 - 192.168.10.126	192.168.10.127

VLSM - Técnica cuadro



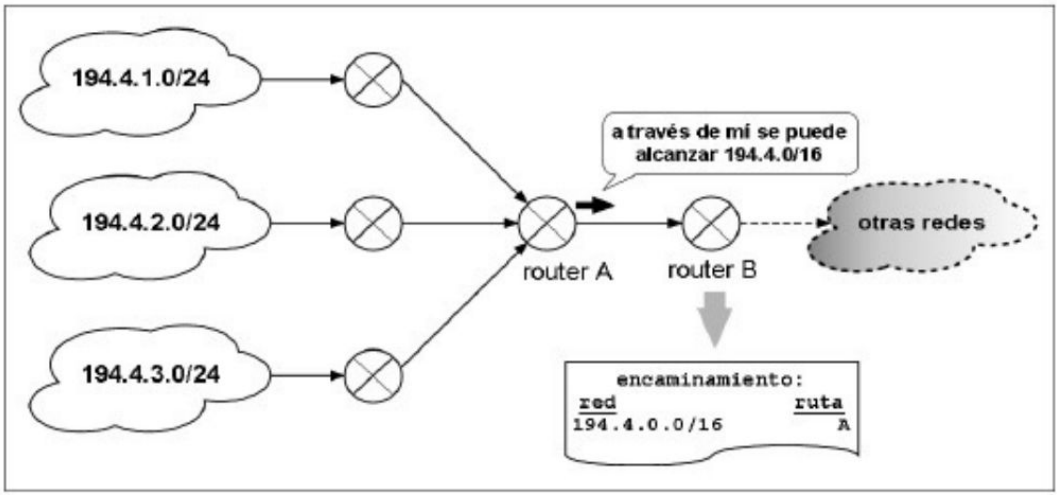
Agregación de dominios

Ventajas:

- Hace más pequeñas las tablas de enrutamiento.
- Esto hace que las búsquedas en la tabla sean más rápidas.
- Vuelve más legible la información.
- Oculta información específica acerca de las redes agregadas
- Las redes más pequeñas incluídas pueden caerse sin que esto afecte a publicación.
- Los protocolos de enrutamiento dinámico pueden evitar consumir ancho de banda para las actualizaciones.

Agregación de dominios

Proceso consiste en encontrar el máximo prefijo común entre las redes



Encontrar un prefijo que considere los 3 sub prefijos indicados y minimice la cantidad de IPs no disponibles.

Agregación de dominios

- Pasar a binario todas las redes a sumarizar.
- Identificar el número de bit n hasta el cual todos los bits de todas las redes son iguales. los bits contenidos entre este y los bits de host iniciales deben formar un recubrimiento completo.
- Para obtener el número de la super red se dejan los n bits primeros como están y el resto se pone a 0 obteniendo una red X.Y.Z.K
- La superred será X.Y.Z.K/n

Problema

Una organización recibe desde su ISP el bloque de direcciones 63.78.2.0/23 y necesita satisfacer los siguientes requerimientos:

- 8 equipos de comunicación
- 26 servidores de diversos tipos
- 1 router
- 12 equipos en finanzas
- 20 equipos en desarrollo
- 10 equipos en gerencia
- 40 equipos para administración y contabilidad
- 32 equipos de laboratorio de pruebas

Solución 1

- Mantener una jerarquía plana o único segmento IP. Así todos los equipos estarán configurados con la máscara 255.255.128.0
- Se ahorran interfaces de red en el router.
- Se ahorran problemas si hay que cambiar algún equipo.
- Todos los equipos tienen que estar en el mismo dominio de broadcast.

Solución 2

- Dividir el bloque usando máscaras más pequeñas.
- Se determina la máscara en base al número de hosts esperados en dicho bloque.

¿Cómo se comunican las distintas redes?

```
[redacted] route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.31.1    0.0.0.0         UG    100    0        0 eno2
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 eno2
172.17.0.0      0.0.0.0         255.255.0.0     U     0      0        0 docker0
192.168.31.0    0.0.0.0         255.255.255.0   U     100    0        0 eno2
```

- Se puede completar la tabla de forma estática o dinámica

Tipos de enrutamiento

	Enrutamiento dinámico	Enrutamiento estático
Complejidad de la configuración	Por lo general es independiente del tamaño de la red	Se incrementa con el tamaño de la red
Conocimientos requeridos del administrador	Se requiere de un conocimiento avanzado	No se requieren conocimientos adicionales
Cambios de topología	Se adapta automáticamente a los cambios de topología	Se requiere la intervención del administrador
Escalamiento	Adecuado para las topologías simples y complejas	Adecuada para topologías simples
Seguridad	Es menos seguro	Más segura
Uso de recursos	Utiliza CPU, memoria y ancho de banda de enlace	No se requieren recursos adicionales
Capacidad de predicción	La ruta depende de la topología actual	La ruta hacia el destino es siempre la misma

Protocolos para caminos dinámicos

	Distance Vector	Link State
Internos	RIP, RIPv2, EIGRP	OSPF, IS-IS
Externos	BGP	

Distance Vector

- Cada nodo mantiene un arreglo que contiene las distancias a todos los otros nodos y se la comunica a todos sus vecinos.
- Inicialmente la tabla tiene la información para los vecinos directos y para los otros el valor es infinito.
- Utiliza el algoritmo de Bellman-Ford para calcular las rutas.
- Lo usa el protocolo RIP (Routing Information Protocol), que hasta 1988 era el único utilizado en Internet.

Situación inicial

Destination	Cost	NextHop
B	1	B
C	1	C
D	INF	--
E	1	E
F	1	F
G	INF	--

Information Stored at Node	Distance to Reach Nodes						
	A	B	C	D	E	F	G
A	0	1	1	INF	1	1	INF
B	1	0	1	INF	INF	INF	INF
C	1	1	0	1	INF	INF	INF
D	INF	INF	1	0	INF	INF	1
E	1	INF	INF	INF	0	INF	INF
F	1	INF	INF	INF	INF	0	1
G	INF	INF	INF	1	INF	1	0

Situación final

Destination	Cost	NextHop
B	1	B
C	1	C
D	2	C
E	1	E
F	1	F
G	2	F

Information Stored at Node	Distance to Reach Nodes						
	A	B	C	D	E	F	G
A	0	1	1	2	1	1	2
B	1	0	1	2	2	2	3
C	1	1	0	1	2	2	2
D	2	2	1	0	3	2	1
E	1	2	2	3	0	2	3
F	1	2	2	2	2	0	1
G	2	3	2	1	3	1	0

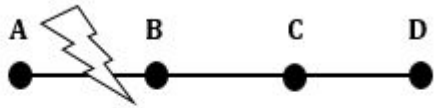
Distance Vector

- El proceso necesario para que todos los nodos tengan una visión consistente de la red, se llama convergencia.
- Se envían actualizaciones a los vecinos en dos circunstancias: periódicamente a intervalos regulares y cuando se recibe una notificación de cambio desde un vecino.
- RIP cuenta los saltos efectuados hasta llegar al destino mientras que IGRP utiliza otra información como el retardo y el ancho de banda.
- Este proceso se conoce también como “enrutamiento por rumor” ya que los nodos utilizan la información de sus vecinos y no pueden comprobar a ciencia cierta si ésta es verdadera o no.

Problemas en Distance Vector

Éste problema se llama count-to-infinity.

Link Between A & B is Broken



	A	B	C	D
A	0, -	1, A	2, B	3, C
B	1, B	0, -	2, C	3, D
C	2, B	1, C	0, -	1, C
D	3, B	2, C	1, D	0, -

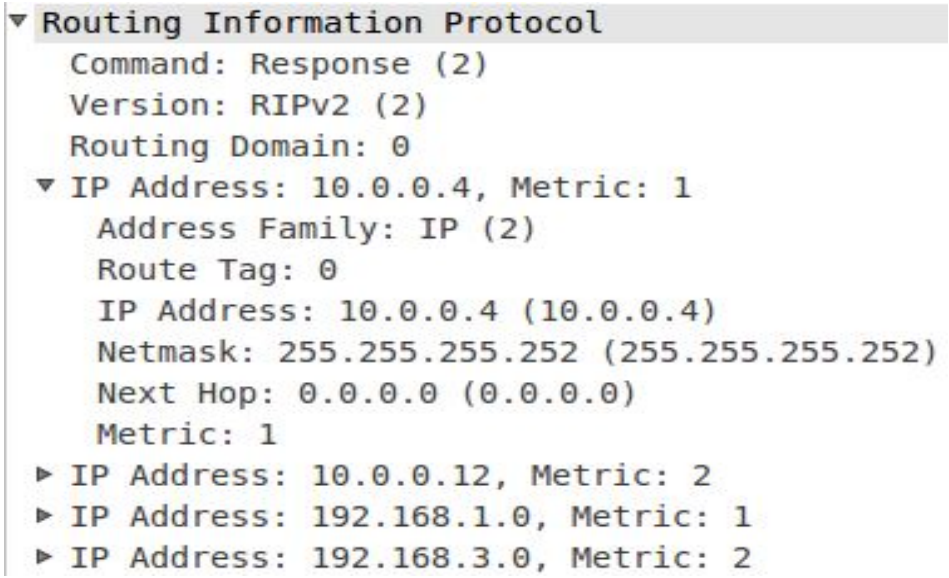
	B	C	D
Sum of Weight to A after link cut	∞, A	2, B	3, C
Sum of Weight to A after 1st updating	3, C	2, B	3, C
Sum of Weight to A after 2nd updating	3, C	4, B	3, C
Sum of Weight to A after 3rd updating	5, C	4, B	5, C
Sum of Weight to A after 4th updating	5, C	6, B	5, C
Sum of Weight to A after 5th updating	7, C	6, B	7, C
Sum of Weight to A after nth updating	.....	....	....
∞	∞	∞	∞

Distance Vector

- Una primera aproximación es definir INF=16, lo que reduce el tiempo de convergencia.
- Otra técnica llamada split horizon, consiste en no enviar las actualizaciones de ruta al vecino del cual se aprendieron.
- Otra técnica más fuerte es split horizon with poison reverse, que consiste en que un nodo sí le envía la actualización aprendida al nodo de quién la aprendió, pero con distancia INF.
- Éstas técnicas afectan la velocidad de convergencia del protocolo, y por lo mismo no se usa en redes grandes.

RIPv2 (RFC 1723) 1994

- Para elegir una ruta, compara las métricas (al recibir una tabla, le suma 1 a todas sus métricas, puesto que las redes están a un router más de distancia) y se queda con la más pequeña.
- En caso de igualdad, se queda con la ruta antigua, para evitar cambios permanentes en las rutas.
- Soporta subredes, resumen de rutas, posee mecanismos de autenticación mediante texto plano o codificación MD5, realiza actualizaciones desencadenadas por eventos.



Actualización de tabla

RIP actualiza cada 30 segundos utilizando el protocolo UDP y el puerto 520, enviando la tabla de enrutamiento completa a sus vecinos.

Las rutas tienen un TTL (tiempo de vida) de 180 segundos, es decir que si en 6 intercambios la ruta no aparece activa, esta es borrada de la tabla de enrutamiento.

No.	Time	Source	Destination	Protocol	Info
201	716.882045	192.168.1.2	224.0.0.9	RIPv2	Response
209	744.879940	192.168.1.2	224.0.0.9	RIPv2	Response
219	773.215155	192.168.1.2	224.0.0.9	RIPv2	Response
227	802.353044	192.168.1.2	224.0.0.9	RIPv2	Response
235	828.653489	192.168.1.2	224.0.0.9	RIPv2	Response
243	856.169863	192.168.1.2	224.0.0.9	RIPv2	Response
253	884.428621	192.168.1.2	224.0.0.9	RIPv2	Response
262	912.934441	192.168.1.2	224.0.0.9	RIPv2	Response

Distancia Administrativa

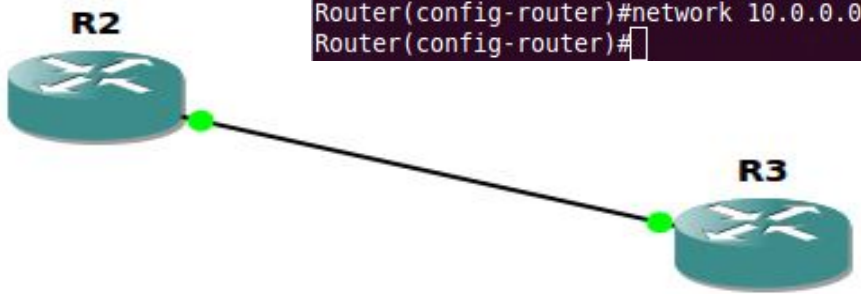
RIP es un protocolo de enrutamiento con una distancia administrativa de 120 (cuanto menor sea la distancia administrativa el protocolo se considera más confiable) y utiliza un algoritmo de vector distancia utilizando como métrica el número de saltos.

```
Router#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 1 subnets
C       172.16.0.0 is directly connected, FastEthernet0/1
R    10.0.0.0/8 [120/1] via 192.168.1.3, 00:00:22, FastEthernet0/0
C    192.168.1.0/24 is directly connected, FastEthernet0/0
```

En la práctica

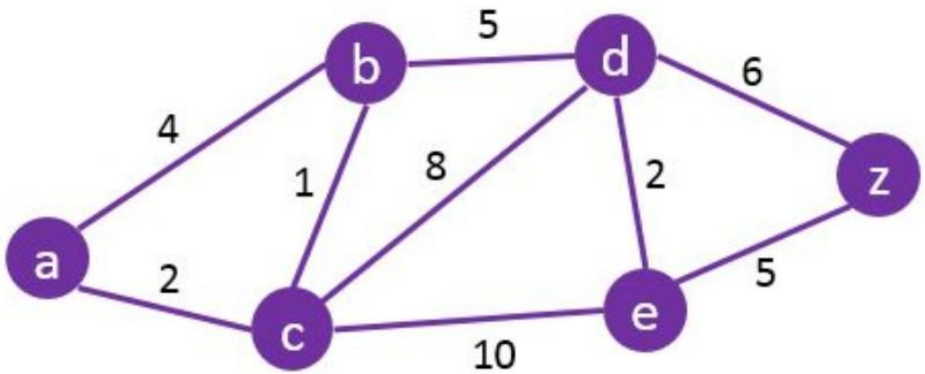
```
Router#ping 10.0.0.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.3, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
Router#ping 10.0.0.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/11/28 ms
Router#
```

```
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#network 192.168.1.0
Router(config-router)#network 10.0.0.0
Router(config-router)#
```



Enrutamiento por estado de enlace

- El algoritmo de Dijkstra permite encontrar la ruta más corta entre dos nodos en un grafo.
- La ruta más corta no se refiere a la ruta con menos cantidad de saltos.



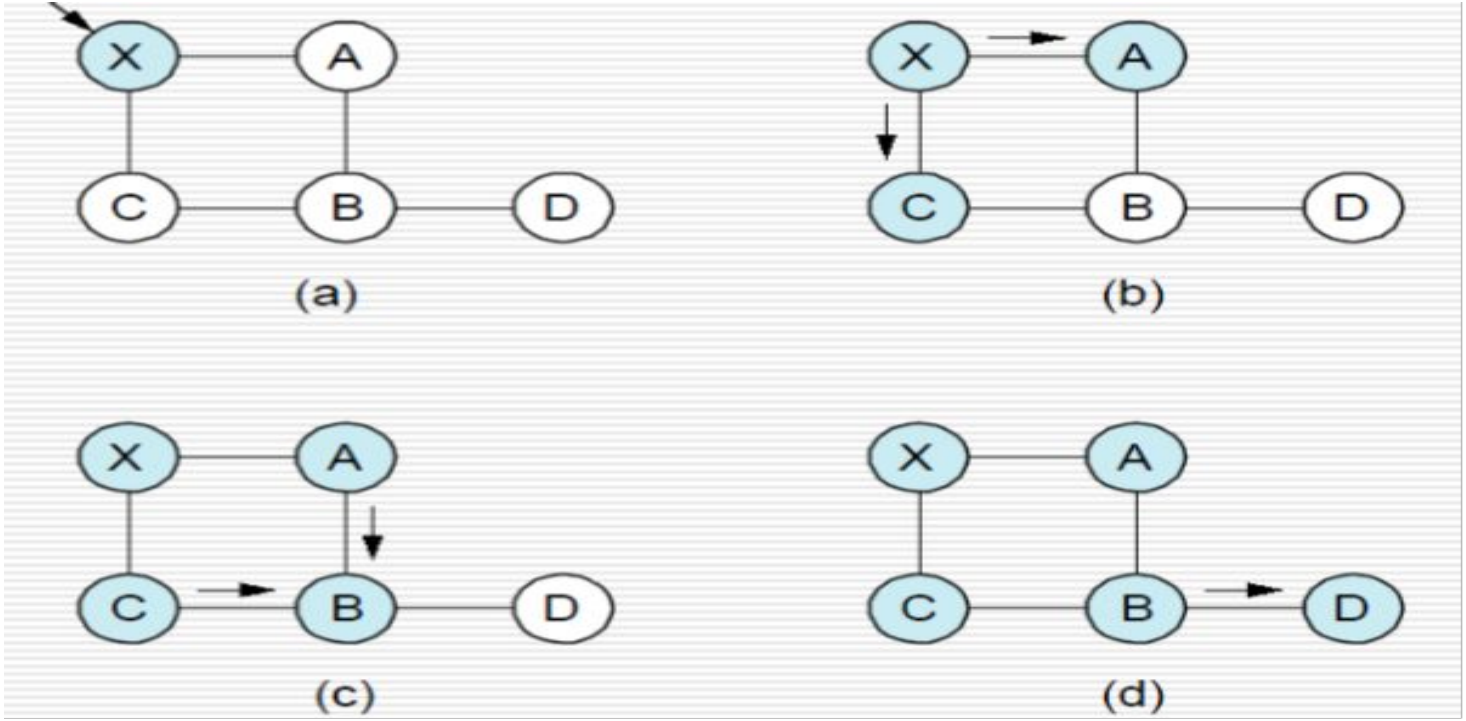
Link State

- Asume que cada nodo es capaz de detectar el “estado” del enlace con sus vecinos.
- Cada nodo sabe como llegar a sus vecinos directos. Toda esa información es diseminada por toda la red.
- Así, cada nodo es capaz de tener una visión completa de la red y con ello poder calcular el camino más corto a cada destino.

Link State

- Este tipo de protocolo se basa en comunicar a todos los miembros la situación de los enlaces.
- Para comunicar esa información, se hace un flooding de la red, que quiere decir que cada nodo le entrega su información a todos sus vecinos y así sucesivamente.

Proceso de flooding



Contenido de LSP (Link-State Packets)

- ID del nodo que creó el LSP.
- Una lista de los vecinos directamente conectados a ese nodo con el costo del enlace a cada uno.
- Un número de secuencia.
- Un TTL para el paquete.
- Los dos primeros campos se usan para calcular las rutas y los dos últimos para asegurar el proceso de flooding. La confiabilidad del proceso incluye asegurarse que todos los nodos tienen la información actualizada.

Proceso LSP

- Si un nodo X recibe una copia de un LSP de parte de un nodo Y, éste verifica si ya tiene información almacenada proveniente de Y.
- Si no tiene, la almacena
- Si tiene, compara el número de secuencia
- Si el nuevo LSP tiene un número mayor, lo considera más nuevo y actualiza su tabla con su información, además de enviarlo a todos sus vecinos, menos aquel que nos lo envió (split-horizon).
- Si la secuencia es menor o igual, se descarta.

Difusión de LSP

Se generan en dos circunstancias:

- A intervalos regulares de tiempo. Estos intervalos son amplios (algunas horas) para reducir el sobrecosto.
- Al producirse un cambio en la topología. Para detectar éstos el protocolo envía mensajes “Hello” regularmente. Si no se ha escuchado un “Hello” desde un vecino en cierto tiempo, se declara el enlace como “fuera de servicio” y se genera un LSP para anunciarlo.

Open Shortest Path First (OSPF)

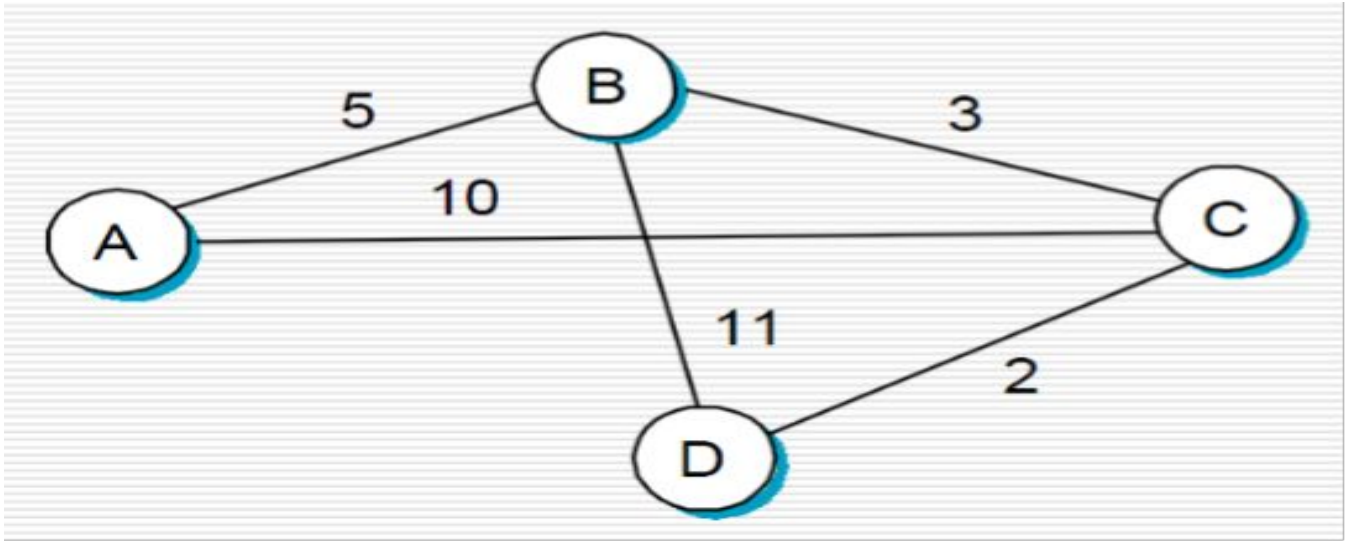
- Se mantienen dos listas: Tentative y Confirmed, donde cada entrada es de la forma <Destination, Cost, NextHop>
- Se inicializa Confirmed con una entrada para mi host, con costo 0.
- Para el nodo recién agregado la lista Confirmed, que llamaremos Next, revisaremos sus LSP.
- Para cada vecino <Neighbor> de Next, calculamos el costo <Cost> de llegar a <Neighbor> como la suma del costo desde mi a Next y desde Next a Neighbor.

Open Shortest Path First (OSPF)

- Si Neighbor no está en la lista Tentative ni en Confirmed, agrego <Neighbor, Cost, NextHop> donde Next Hop es quien permite llegar a Neighbor.
- Si Neighbor está en la lista Tentative y el costo es menor que el actual costo, reemplazo la actual entrada con <Neighbor, Cost, Next Hop>
- Si la lista Tentative está vacía, se detiene. Sino, elijo la entrada de Tentative que tenga el costo más bajo, la muevo a la lista Confirmed y vuelvo al paso 2.

Ejemplo Link State

Haremos el proceso de construcción de la tabla para el nodo D. Nótese que los enlaces tienen costos diferentes.



Paso1

Paso	Confirmed	Tentative	Comentarios
1	(D,0,-)		Debido a que D es el único miembro de la lista, revisamos sus LSP
2	(D,0,-)	(B,11,B) (C,2,C)	D dice que puede alcanzar a B a costo 11, que es mejor que lo que tiene, así que se agrega a la lista `Tentative`; lo mismo para C
3	(D,0,-) (C,2,C)	(B,11,B)	Agregamos el miembro de `Tentative` con menor costo a `Confirmed`. Luego revisamos los LSP para este nuevo miembro.

Paso2

4	(D,0,-) (C,2,C)	(B,5,C) (A,12,C)	Se puede alcanzar a B a través de C con costo 5, así que reemplazamos. C dice que puede alcanzar a A con costo 12.
5	(D,0,-) (C,2,C) (B,5,C)	(A,12,C)	Agregamos el miembro de `Tentative` con menor costo a `Confirmed`. Luego revisamos los LSP para este nuevo miembro.
6	(D,0,-) (C,2,C) (B,5,C)	(A,10,C)	Debido a que podemos alcanzar A con costo 5 a través de B, reemplazamos en `Tentative`
7	(D,0,-) (C,2,C) (B,5,C) (A,10,C)		Agregamos el miembro de `Tentative` con menor costo a `Confirmed`. Con eso terminamos.

Validemos…

Filter: ospf Expression...

No.	Time	Source	Destination	Protocol	Info
200	420.15633	192.168.0.1	224.0.0.5	OSPF	Hello Packet
202	424.36119	192.168.0.2	224.0.0.5	OSPF	Hello Packet
203	425.83858	192.168.0.2	224.0.0.5	OSPF	LS Update
204	428.34420	192.168.0.1	224.0.0.5	OSPF	LS Acknowledge
206	430.15908	192.168.0.1	224.0.0.5	OSPF	Hello Packet
208	434.35959	192.168.0.2	224.0.0.5	OSPF	Hello Packet
211	440.15716	192.168.0.1	224.0.0.5	OSPF	Hello Packet
213	444.35949	192.168.0.2	224.0.0.5	OSPF	Hello Packet
214	448.43864	192.168.0.1	224.0.0.5	OSPF	LS Update
216	450.15878	192.168.0.1	224.0.0.5	OSPF	Hello Packet
218	450.93951	192.168.0.2	224.0.0.5	OSPF	LS Acknowledge
219	454.35974	192.168.0.2	224.0.0.5	OSPF	Hello Packet
221	460.15651	192.168.0.1	224.0.0.5	OSPF	Hello Packet

Distancia administrativa

OSPF tiene una distancia administrativa de valor 110.

```
     192.168.0.0/30 is subnetted, 1 subnets
C       192.168.0.0 is directly connected, FastEthernet1/0
O    192.168.1.0/24 [110/2] via 192.168.0.2, 00:00:30, FastEthernet1/0
C    192.168.2.0/24 is directly connected, FastEthernet1/1
```

RIP vs OSPF

En un link-state el tiempo de convergencia puede ser de 4 o 5 segundos según la red, en cambio en RIP es de 180 segundos.

Whois | DNS | IRR | Propagation | Visibility | Routes

Announced By		
Origin AS	**Announcement**	**Description**
AS10753	200.14.84.0/24	Universidad Diego Portales

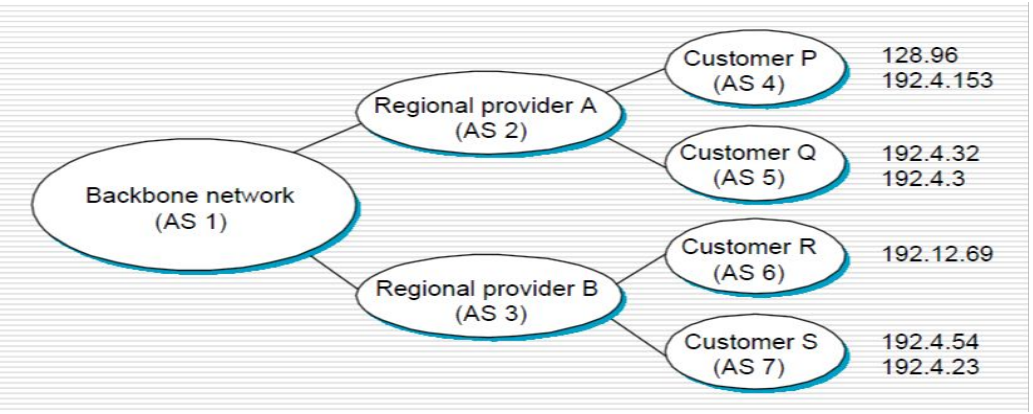
```
inetnum:     200.14.84.0/22
status:      assigned
aut-num:     N/A
owner:       Universidad Diego Portales
ownerid:     CL-UDPO-LACNIC
responsible: Elías Pérez Morales
address:     Manuel Rodriguez sur 333, 415, 3er piso
address:     12345 - Santiago -
country:     CL
phone:       +56 2 6762057
owner-c:     GAE13
tech-c:      GAE13
abuse-c:     GAE13
inetrev:     200.14.84.0/22
nserver:     MBULNES.UDP.CL [lame - not published]
nsstat:      20240630 UH
nslastaa:    20201123
created:     19941117
changed:     20160530

nic-hdl:     GAE13
person:      Gabriel Espinoza
e-mail:      gabriel.espinoza@udp.cl
address:     Manuel Rodriguez sur 333, 333,
address:     123456789 - santiago - No
country:     CL
phone:       +56 2 6768750
created:     20160425
changed:     20160425
```

Autonomous Systems

- Unidades bajo la misma administración, permite agregación de direcciones con el objetivo de reducir la cantidad de información global, y con ello permitir una mejor escalabilidad.
- Dentro de los AS se pueden usar protocolos internos (IGP) o externos, pero entre AS se usan protocolos externos (EGP).

Desafíos

- Autonomía de cada sistema para calcular sus rutas internas. Ello no permite calcular el “costo” de un camino, por lo que sólo se anuncia la capacidad de alcanzar una red.
- Otro desafío involucra las políticas, pues generalmente se quiere privilegiar ciertos caminos para ciertos destinos (métricas y pesos).



Super Looking Glass | Terminal

```
Found 4 more results
200.14.84.0/24 200.14.85.0/24 200.14.86.0/24 200.14.87.0/24

⚠ Please refine your request

Observed 635 results for 200.14.84.0/24

RPKI State: ✔ VALID, ✖ INVALID, - NOT FOUND
Origin codes: i - IGP, e - EGP, ? - incomplete
{ } - Braces enclose AS sets, {x„} - Braces containg an x follo
Network         Neighbor            MED        LocPrf     RPKI
--------------  ------------------- ---------- ---------- ----
200.14.84.0/24  208.51.134.246      24606      100        -
200.14.84.0/24  208.51.134.248      13894      100        -
200.14.84.0/24  208.51.134.255      13894      100        -
200.14.84.0/24  45.68.16.1          0          100        -    21838 3549 10753 ? (pit.scl)
200.14.84.0/24  45.68.16.2          0          100        -    21838 3549 10753 ? (pit.scl)
200.14.84.0/24  168.195.130.2       0          100        -    263702 3549 10753 ? (rrc24.ripe.net)
200.14.84.0/24  12.0.1.63           0          100        -    7018 3356 3549 10753 i (rrc00.ripe.net)
200.14.84.0/24  27.111.228.43      0          100        -    3491 3356 3549 10753 i (route-views.sg)
200.14.84.0/24  27.111.228.217     0          100        -    3257 3356 3549 10753 i (route-views.sg)
200.14.84.0/24  27.111.229.103     0          100        -    9002 3356 3549 10753 i (route-views.sg)
200.14.84.0/24  27.111.229.245     0          100        -    35280 3356 3549 10753 i (rrc23.ripe.net)
200.14.84.0/24  31.204.91.150      0          100        -    56665 3356 3549 10753 i (route-views4)
200.14.84.0/24  37.49.236.32       0          100        -    34177 3356 3549 10753 i (rrc21.ripe.net)
200.14.84.0/24  37.49.236.36       0          100        -    16347 3356 3549 10753 i (rrc21.ripe.net)
200.14.84.0/24  37.49.237.83       201        100        -    25091 3356 3549 10753 i (rrc21.ripe.net)
200.14.84.0/24  37.49.237.143      0          100        -    50628 3356 3549 10753 i (rrc21.ripe.net)
200.14.84.0/24  37.139.139.17      0          100        -    57866 3356 3549 10753 i (route-views)
200.14.84.0/24  45.6.52.62         0          100        -    267613 3356 3549 10753 i (route-views.rio)
200.14.84.0/24  45.6.54.171        0          100        -    199524 3356 3549 10753 i (route-views.rio)
200.14.84.0/24  45.6.54.203        0          100        -    6057 21838 3549 10753 e (route-views.rio)
200.14.84.0/24  45.6.55.6          0          100        -    264409 3356 3549 10753 i (route-views.rio)
200.14.84.0/24  45.6.55.32         0          100        -    52468 7195 3549 10753 i (route-views.rio)
200.14.84.0/24  45.68.16.3         0          100        -    64112 21838 3549 10753 ? (pit.scl)
200.14.84.0/24  45.68.16.19        0          100        -    269956 21838 3549 10753 ? (pit.scl)
200.14.84.0/24  45.127.172.74      0          100        -    4826 3356 3549 10753 i (route-views.sydney)
200.14.84.0/24  45.127.172.80      0          100        -    3491 3356 3549 10753 i (route-views.sydney)
200.14.84.0/24  45.127.173.66      0          100        -    7594 3356 3549 10753 i (route-views.sydney)
Press space to continue, 'n' for no more paging, Ctrl-C or 'q' to exit (6%)
```

AS Info | Graph v4 | Graph v6 | Prefixes v4 | Prefixes v6 | Peers v4 | Peers v6
Whois | IRR | Traceroute

Prefix	Description	Visibility
200.12.130.0/24	UNIVERSIDAD MAYOR	**100%** 647/647
200.14.84.0/24	Universidad Diego Portales	**100%** 647/647
200.14.85.0/24	Universidad Diego Portales	**100%** 647/647
200.14.86.0/24	Universidad Diego Portales	**100%** 647/647
200.14.87.0/24	Universidad Diego Portales	**100%** 647/647