

#### NOTAS:

- Para un mismo switch, dos hosts pueden tener la misma IP mientras esten en VLANs distintas (para los switches mas nuevos)
- La ventaja de una VLAN por sobre una subred es que la VLAN es una separacion FISICA entre puertos. Esto implica mas seguridad, porque los hosts de una VLAN no pueden comunicarse con los de otra VLAN ni por broadcast ni haciendose pasar por otra IP (y estas dos cosas si se pueden hacer si en vez de dos VLAN hubiera dos subredes). Sin embargo, es posible conectar dos VLAN dentro del mismo switch.
- Yo le puedo asignar una IP de red a cada VLAN, y tambien puedo asignar una IP para ese switch por cada VLAN que tenga
- Un switch de capa 3 no es un router porque no rutea. Esto significa que NO agarra paquetes IP por una interfaz y los envia por otra interfaz. Los paquetes que manda son ethernet.
- Los switches capa 3 tienen IP propia por cada VLAN porque esto les permite ser configurados por ssh o similares
- Cuando hacemos ping desde un switch de capa 3 a un host en una VLAN, este no es un comportamiento normal, para probar la red es mejor hacerlo al reves.
- Cuando quiero hablar con una IP que esta en la misma subred que yo, internamente no hace falta consultar la tabla de ruteo
- La logica por detras del modo privilegiado en un switch es que en la vida real SI me pide una clave para entrar. La diferencia es que en el simulador, simula que yo estoy entrando por la interfaz especial que tiene todo switch para configuracion.

## Protocolos de Ruteo

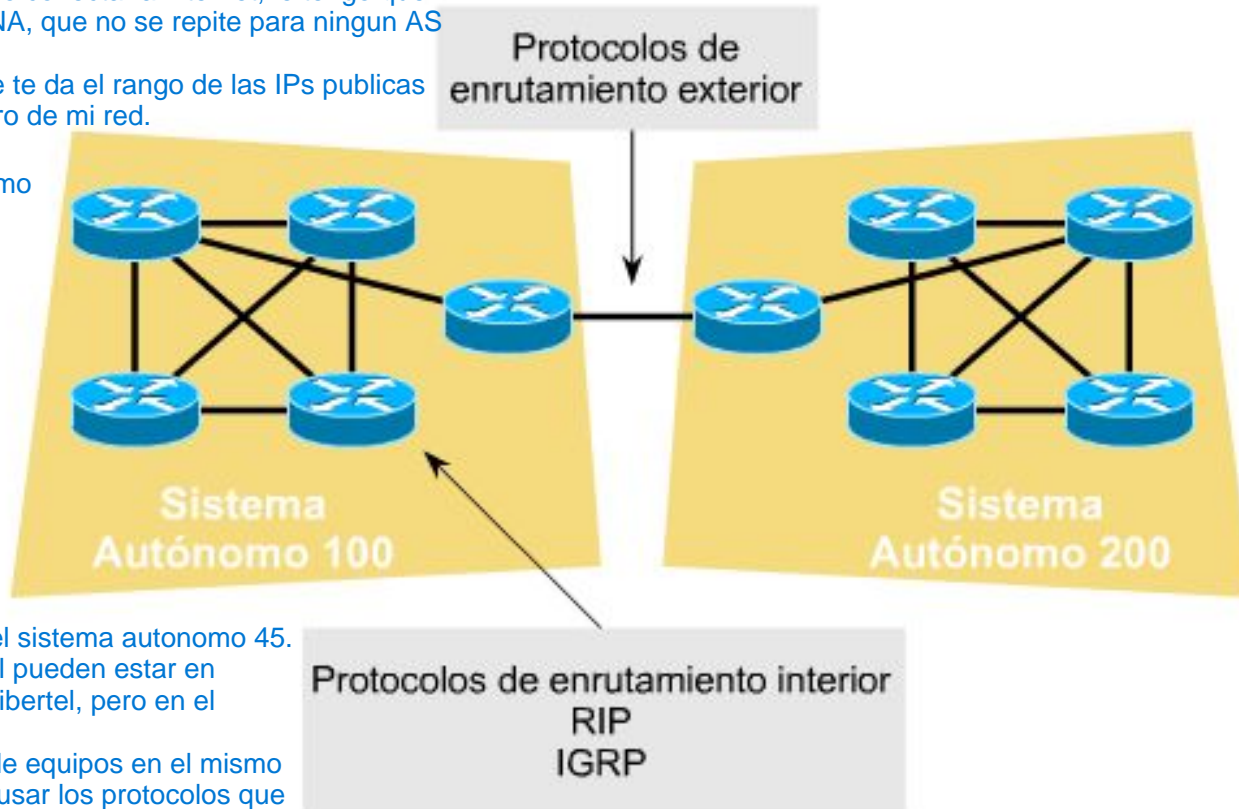
# Sistema Autónomo (AS)

- Un AS es un conjunto de redes administradas por el mismo ente.
- Rige una sola política de ruteo

El nombre "sistema autónomo" viene dado por el IANA, que es el consorcio que regula todos los SAs en internet. Cuando yo tengo un SA lo quiero conectar a internet, le tengo que pedir un ID unico al IANA, que no se repite para ningún AS en todo el mundo. IANA también es el que te da el rango de las IPs publicas que yo voy a usar dentro de mi red.

Si yo armo una red, como Banelco (que no esta registrado en IANA), entonces no es un AS.

El internet es un conjunto de sistemas autonomos conectados entre si. Empresas crean sus propias redes regionales y se conectan con otras empresas que hacen lo mismo en otras ciudades cercanas.



Ejemplo: fibertel tiene el sistema autonomo 45. Dos usuarios de fibertel pueden estar en distintas subredes de fibertel, pero en el mismo SA.

Para la comunicacion de equipos en el mismo SA, la empresa puede usar los protocolos que quiera. Sin embargo, para comunicarse entre distintos SA, el protocolo tiene que ser el mismo.

# IANA

ASN: numero de sistema autonomo

- Otorga direcciones **IP** y **ASN** a entidades regionales
  - AfriNIC (African Network Information Centre)
  - APNIC (Asia Pacific Network Information Centre) Argentina usa APNIC. Si fibertel quiere pedir IPS, se tiene que comunicar con ese organismo.
  - ARIN (American Registry for Internet Numbers) - North America Region
  - LACNIC (Regional Latin-American and Caribbean IP Address Registry)
  - RIPE NCC (Réseaux IP Européens) - Europe, the Middle East, and Central Asia

# LACNIC

## ■ Ejemplos de búsquedas de WHOIS en LACNIC

### ■ Ejemplo 1

- 190.188/15
- owner: Prima S.A. Subsidiaria de Fibertel
- responsable: Miguel Fernandez
- address: La Rioja, 301
- address: C1214ADG - Buenos Aires –
- aut-num: 10834 Numero de sistema autonomo

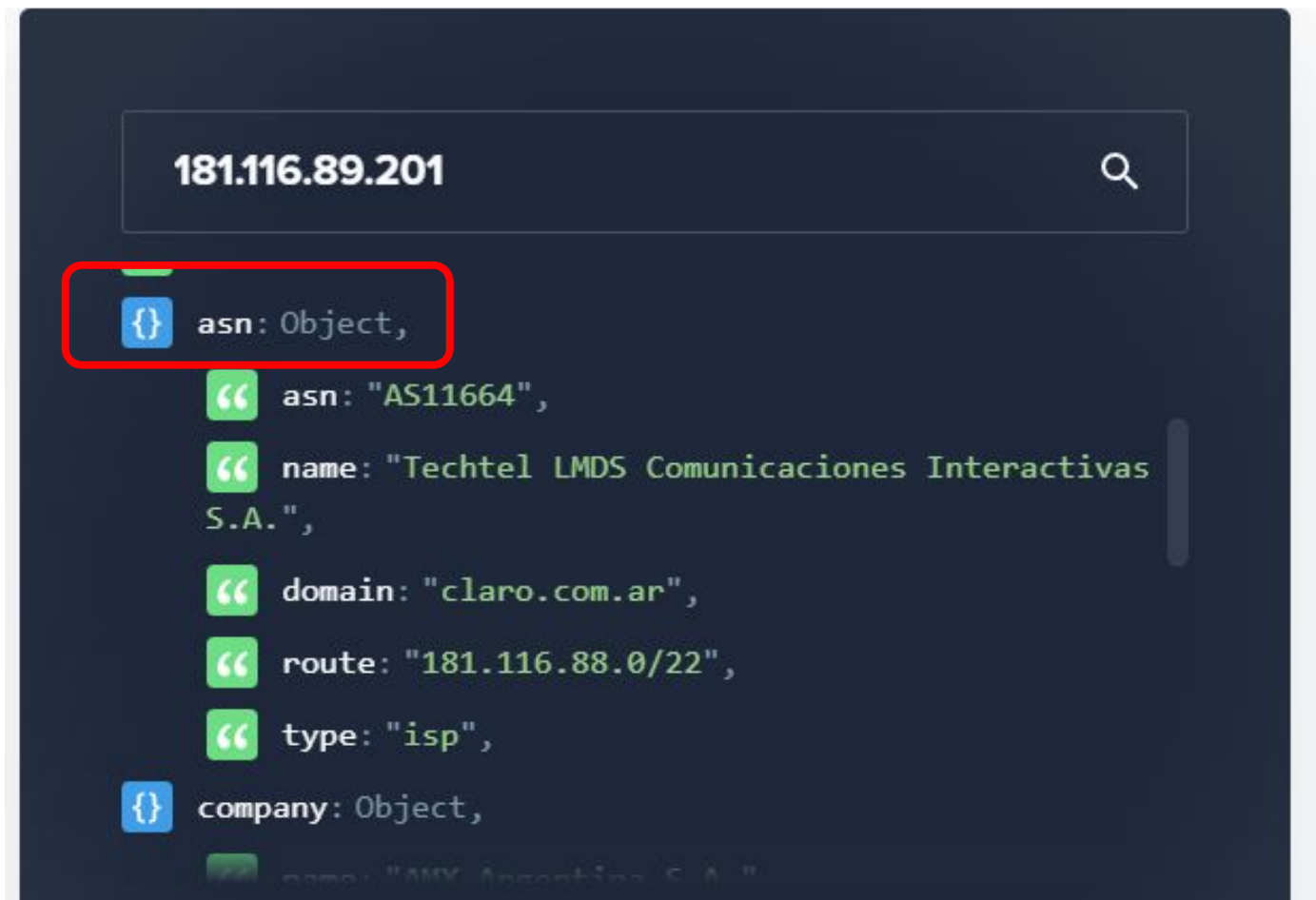
whois es un protocolo. el de la terminal de linux es solo una app que usa ese protocolo

### ■ Ejemplo 2

- 209.13/16
- owner: Telefonica Data Argentina S.A.
- responsable: ip master
- address: Corrientes, 707, piso 8 Ind
- address: C1043AAH - Buenos Aires –
- aut-num: 7934

# ipinfo.io

- Ejemplo IP hogareña



# ipinfo.io

- Pido info del AS



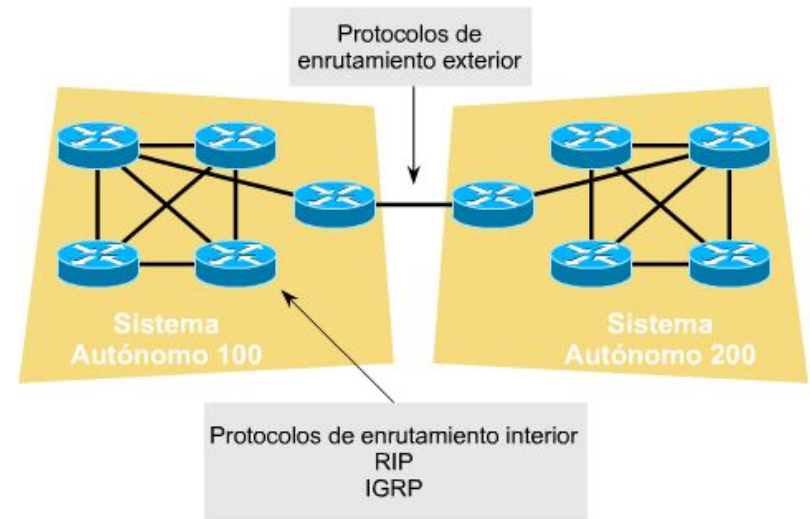
```
AS11664

{
  "asn": "AS11664",
  "name": "Techtel LMDS Comunicaciones Interactivas S.A.",
  "country": "AR",
  "allocated": "1998-11-09",
  "registry": "lacnic",
  "domain": "claro.com.ar",
  "# num_ips": 733440,
  "type": "isp",
}
```

Claro tiene 733 440 IPs publicas

# Sistema Autónomo (AS)

- Protocolo exterior (EGP)
- Cada uno se identifica por un ASN (lo provee IANA)
- Los EGP se suelen usar al cambiar de países, o empresas, por ejemplo



EGP: exterior gateway protocol. Se usa cuando cambias de ente, SA, país. No siempre un SA es un proveedor de internet. Por ejemplo, el ITBA podría registrar su SA sin ser proveedor de internet.

Una empresa que no quiere ser proveedor de internet le puede pedir a IANA IPs públicas. También es posible contratar IP públicas a un ISP, pero es mejor pedirselas al IANA para no tener que depender de una ISP. Esto hacen las empresas grandes, porque si yo me cambio de ISP pierdo la IP pública que tenía contratada.

Sin embargo, por más que yo sea una empresa con mi propio SA y mis propias IPs públicas, igual necesito pagarle a un ISP para conectarme a internet (la única diferencia es que en este caso el ISP no me da ni una IP ni un router).

# Protocolos EGP

Hay muchos EGP, el que mas se utiliza es el BGP.  
El IGP es el internal gateway protocol.

- Para operar necesitan:
  - Una lista de los routers vecinos, con los que intercambiarán la información de enrutamiento.
  - Una lista de las redes a ser publicadas como de acceso directo.
  - El número de sistema autónomo del router local.





# Protocolos IGP

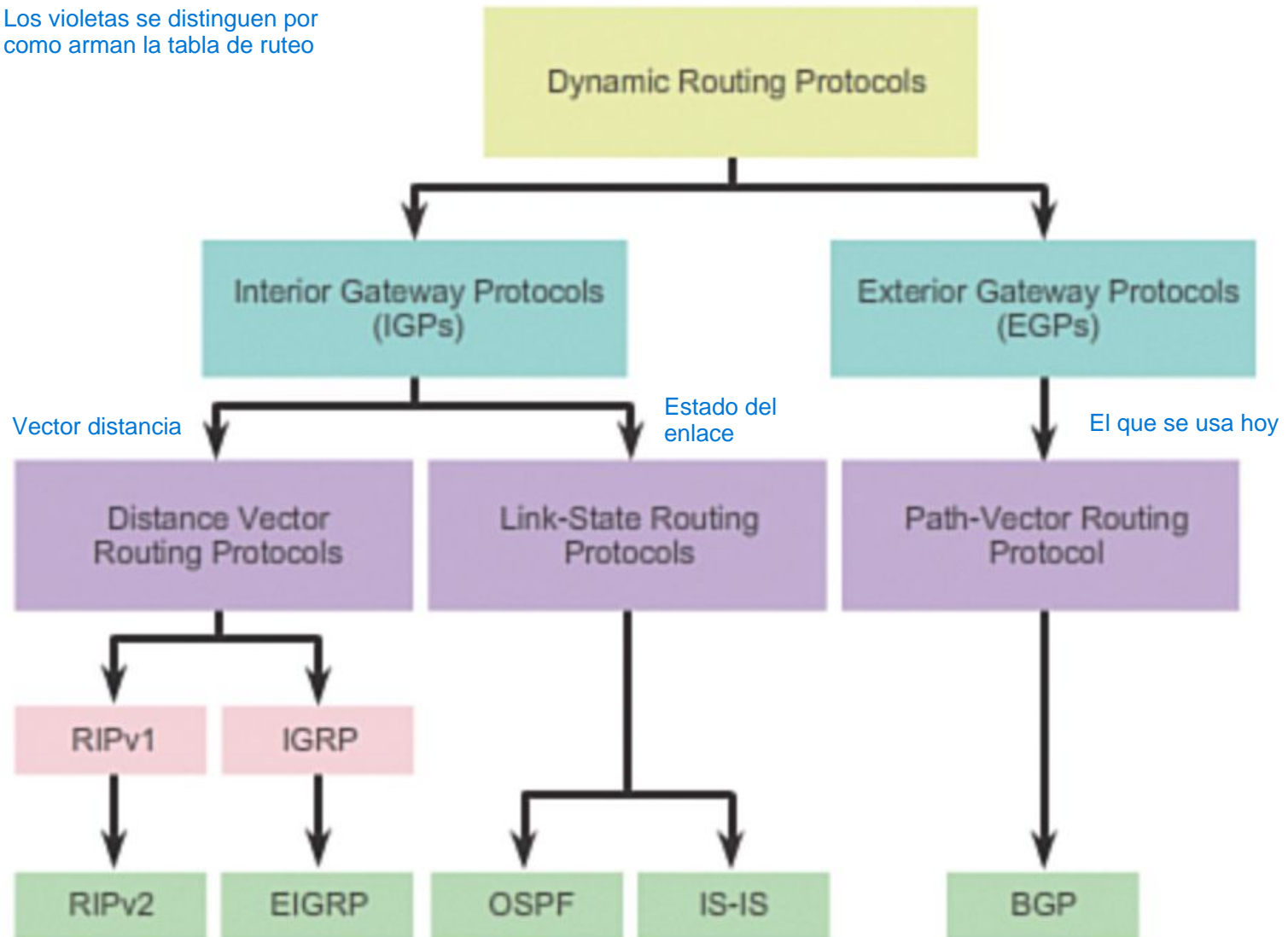
- Se utilizan dentro de un Sistema Autónomo
- Están diseñados para redes pequeñas

# Protocolos de enrutamiento - Repaso

- Toman la decisión de porque interfaz enviar los paquetes recibidos.
- Se puede dividir en dos grupos:
  - Ruteo estático
    - No toma decisiones según estado de la red
  - Ruteo dinámico
    - Cambia las decisiones de ruteo según el estado de la red.

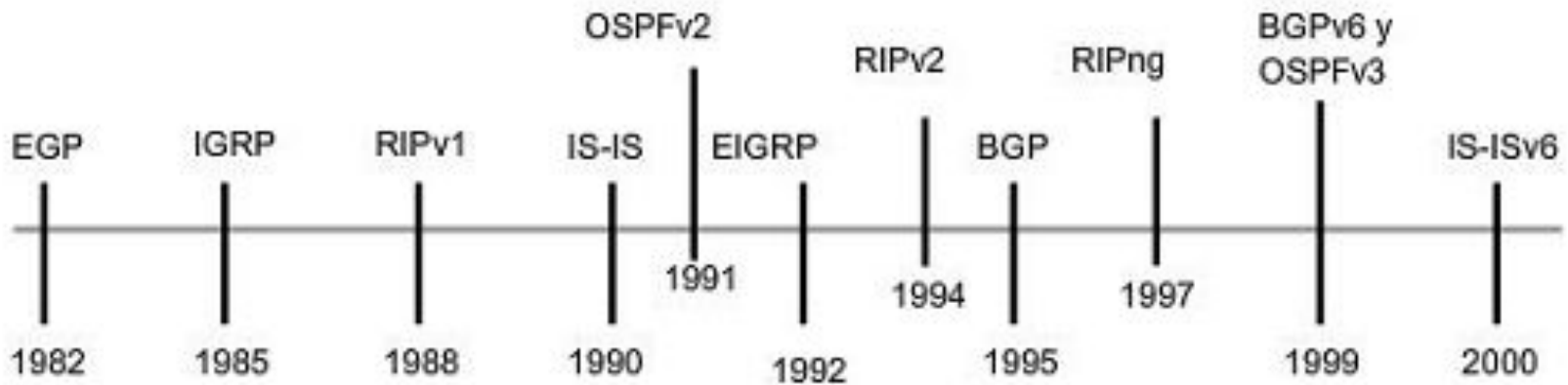
# Tipos de Protocolos

Los violetas se distinguen por  
como arman la tabla de ruteo



# Historia de los Protocolos

Hoy en día se usa BGP. Cuando apareció internet, los protocolos no estaban preparados para tal magnitud de hosts, entonces se tuvo que crear uno nuevo.



Internet aparece alrededor de 1994

Tiempo de convergencia: cuanto tarda la red en enterarse de un cambio.

Los routers únicamente conocen a sus vecinos, y se lo anuncian a otros routers.

En internet hay miles de millones de routers, y tarda un tiempo en actualizarse cuando aparece un router o se cae otro.

# Repaso tabla de ruteo

PC Windows con  
IPs

192.168.100.34

192.168.56.1 (VM)

172.19.208.1 (VM)

172.30.224.1 (VM)

```
IPv4 Tabla de enrutamiento
=====
Rutas activas:
Destino de red      Máscara de red      Puerta de enlace  Interfaz  Métrica
0.0.0.0             0.0.0.0             192.168.100.1     192.168.100.34    25
127.0.0.0           255.0.0.0           En vínculo        127.0.0.1         331
127.0.0.1           255.255.255.255     En vínculo        127.0.0.1         331
127.255.255.255     255.255.255.255     En vínculo        127.0.0.1         331
169.254.0.0         255.255.0.0         En vínculo        169.254.80.80     9256
169.254.80.80       255.255.255.255     En vínculo        169.254.80.80     9256
169.254.255.255     255.255.255.255     En vínculo        169.254.80.80     9256
172.19.208.0        255.255.240.0       En vínculo        172.19.208.1      5256
172.19.208.1        255.255.255.255     En vínculo        172.19.208.1      5256
172.19.223.255      255.255.255.255     En vínculo        172.19.208.1      5256
172.30.224.0        255.255.240.0       En vínculo        172.30.224.1      5256
172.30.224.1        255.255.255.255     En vínculo        172.30.224.1      5256
172.30.239.255      255.255.255.255     En vínculo        172.30.224.1      5256
192.168.56.0        255.255.255.0       En vínculo        192.168.56.1      281
192.168.56.1        255.255.255.255     En vínculo        192.168.56.1      281
192.168.56.255      255.255.255.255     En vínculo        192.168.56.1      281
192.168.100.0       255.255.255.0       En vínculo        192.168.100.34    281
192.168.100.34      255.255.255.255     En vínculo        192.168.100.34    281
192.168.100.255     255.255.255.255     En vínculo        192.168.100.34    281
224.0.0.0           240.0.0.0           En vínculo        127.0.0.1         331
224.0.0.0           240.0.0.0           En vínculo        192.168.100.34    281
224.0.0.0           240.0.0.0           En vínculo        192.168.56.1      281
224.0.0.0           240.0.0.0           En vínculo        169.254.80.80     9256
224.0.0.0           240.0.0.0           En vínculo        172.19.208.1      5256
224.0.0.0           240.0.0.0           En vínculo        172.30.224.1      5256
255.255.255.255     255.255.255.255     En vínculo        127.0.0.1         331
255.255.255.255     255.255.255.255     En vínculo        192.168.100.34    281
255.255.255.255     255.255.255.255     En vínculo        192.168.56.1      281
255.255.255.255     255.255.255.255     En vínculo        169.254.80.80     9256
255.255.255.255     255.255.255.255     En vínculo        172.19.208.1      5256
255.255.255.255     255.255.255.255     En vínculo        172.30.224.1      5256
=====
```

# Repaso tabla de ruteo

PC con Linux

```
manav@ubuntu: ~  
manav@ubuntu:~$ route -n  
Kernel IP routing table  
Destination      Gateway          Genmask          Flags Metric Ref    Use Iface  
0.0.0.0          10.0.2.2        0.0.0.0          UG    100    0      0 enp0s3  
10.0.2.0         0.0.0.0         255.255.255.0    U     100    0      0 enp0s3  
169.254.0.0      0.0.0.0         255.255.0.0      U     1000   0      0 enp0s3  
manav@ubuntu:~$
```

# Repaso tabla de ruteo

El objetivo de un protocolo de ruteo es crear una tabla de ruteo con “costos” mínimos para llegar a destino

"costo" puede ser economico, politico, de velocidad, etc.

Por ejemplo, yo tal vez no quiero que mis paquetes pasen por un sistema autonomo de determinado pais. Esto es un costo politico.

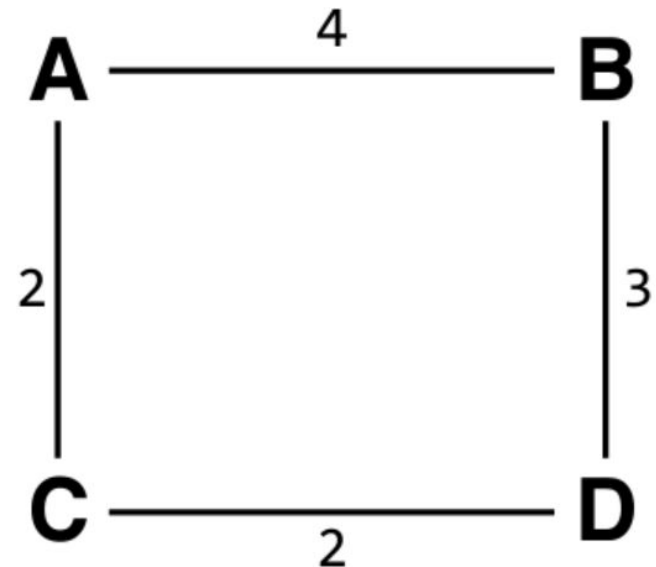
## A's routing table

```
routing_table[A] = self ; 0  
routing_table[B] = A->B ; 4  
routing_table[C] = A->C ; 2  
routing_table[D] = A->C ; 4
```

Para llegar a D, paso por C.

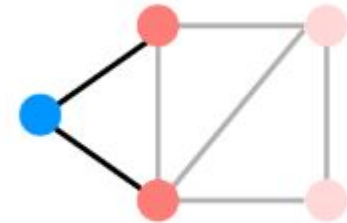
El protocolo elige almacenar que es mejor pasar por C que por B para ir a D.

Generalmente, estos pesos se ponen de manera manual



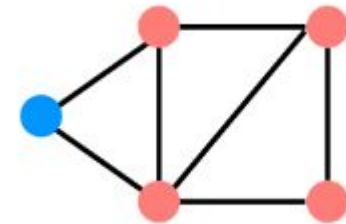
# Ruteo distribuido

Los **nodos** aprenden que **vecinos** tienen usando protocolo “Hello”

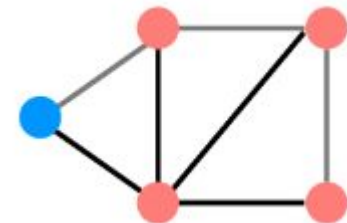


Los **nodos** aprenden **rutas** de sus vecinos por **anuncios**

Es parecido al gossip de cassandra como funciona esto



Los **nodos** crean sus tablas de ruteo con costos mínimos



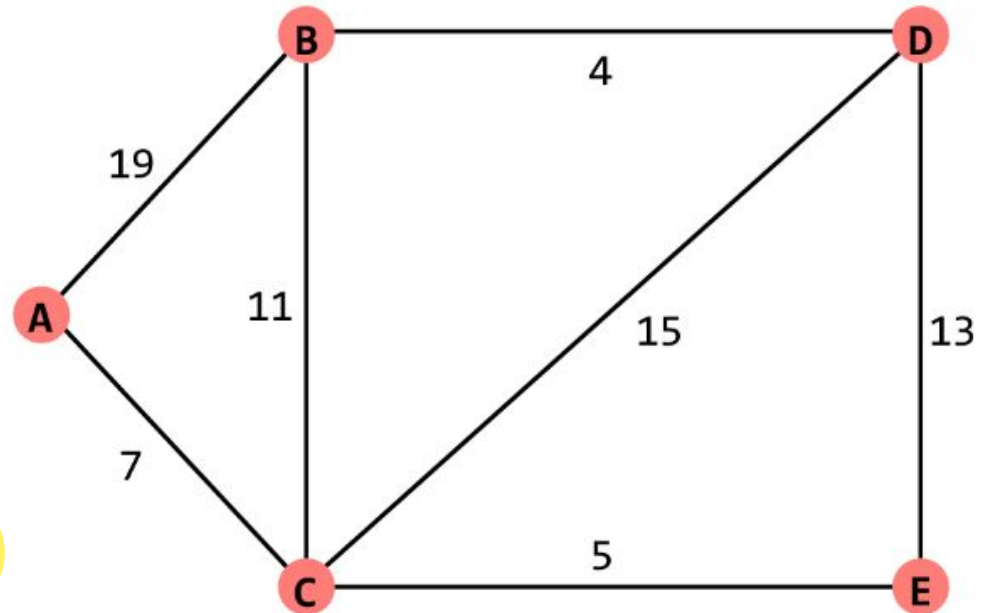




# Ruteo por **ESTADO DE ENLACE**

# Ruteo por estado de enlace

Los anuncios de un nodo contienen las redes a las que llega y el costo de cada una



From A: [(B,19), (C,7)]  
From B: [(A,19), (C,11), (D,4)]  
From C: [(A,7), (B,11), (D,15), (E,5)]  
From D: [(B,4), (C,15), (E,13)]  
From E: [(C,5), (D,13)]

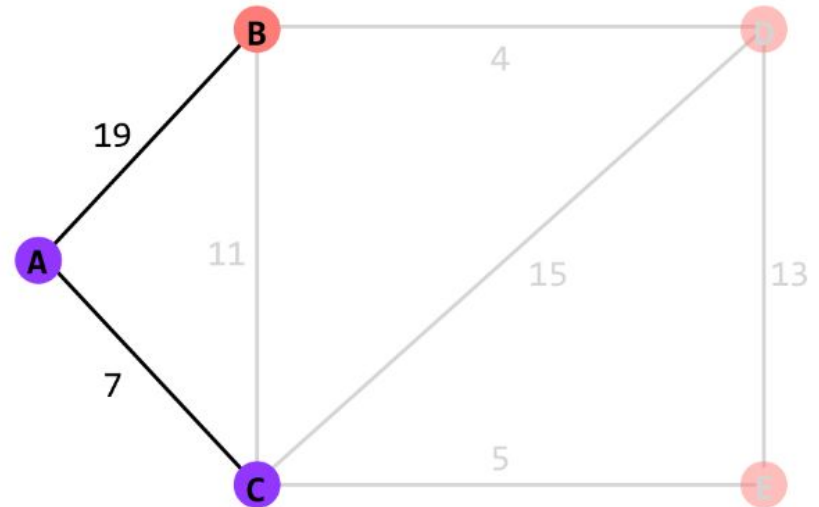
Esta es la información que envía cada nodo sobre si mismo

# Ruteo por estado de enlace

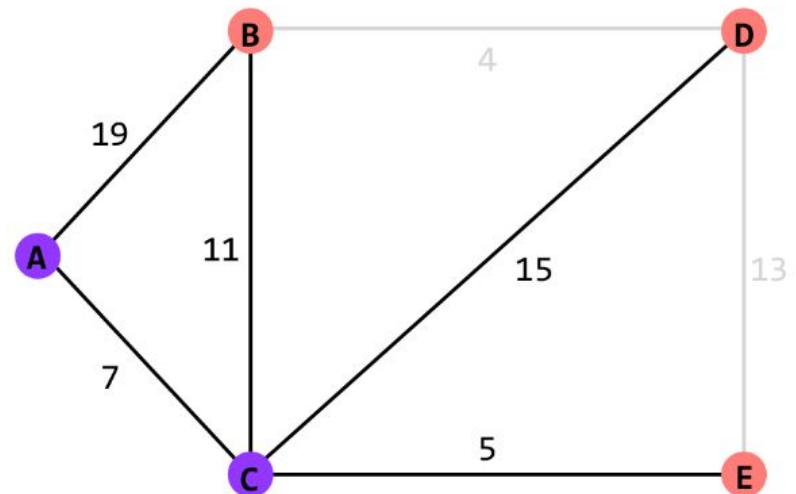
Cada **nodo**, obtiene información, **toma el menor costo**, comienza a iterar y actualiza la información de cada camino si encuentra uno menor:

(A elige C entre C y B y luego continúa aprendiendo por el lado de C)

A: Self, 0  
B: A->B, 19  
C: A->C, 7



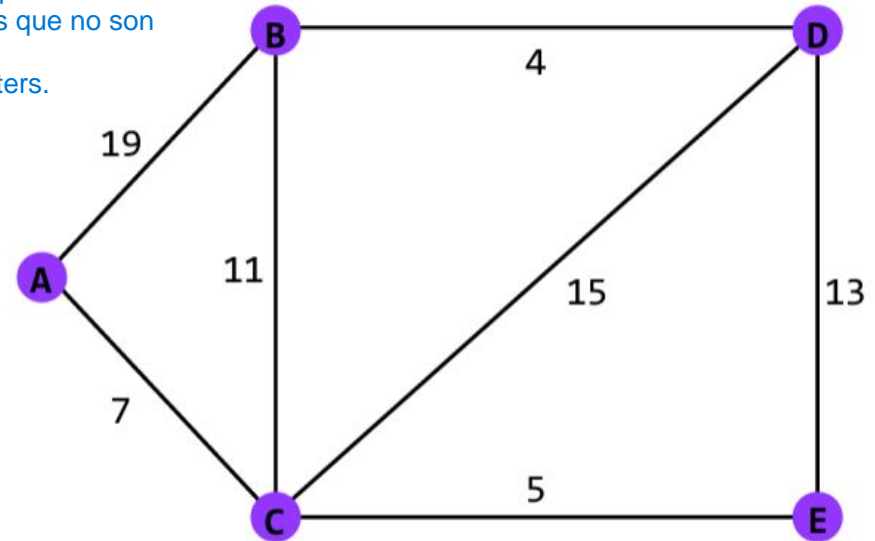
A: Self, 0  
B: A->B, 19  
C: A->C, 7



# Ruteo por estado de enlace

Este que estamos viendo ahora es el primer tipo de protocolo que se creo.  
La idea es que A le pide a B y a C su tabla de ruteo con los distintos pesos, pero no se queda ahi, sino que averigua TODAS las tablas de ruteo de todos los routers que no son sus vecinos (como D y E, que los encontro mientras hablaba con B y C).  
Este protocolo ya no se usa en la actualidad, porque hay MILLONES de routers.

**A:** Self, 0  
**B:** A->C, 18  
**C:** A->C, 7  
**D:** A->C, 22  
**E:** A->C, 12



Obtiene el ruteo final luego de las iteraciones para el nodo A.

Para ver: B luego de iterar decidiría ir a A a través de C

# Ruteo por estado de enlace

Los nodos envían anuncios a TODOS los nodos con su información

Cada nodo arma un mapa de toda la red

Genera mucho tráfico

Poco recomendado para grande redes.

Optimización: Si uno quiere viajar de Bs. As. a La Plata, no analiza las rutas de Córdoba.

La idea de esto es pedir la menor cantidad de informacion posible. No me interesa saber de routers que no llegan a donde yo quiero llegar.



# Ruteo por **VECTOR DISTANCIA**

# Ruteo por *vector distancia*

## Los nodos envían anuncios solo a sus vecinos

La desventaja de este algoritmo es que yo estoy confiando que el camino con el menor costo va a seguir teniendo el menor costo, y no va a cambiar mas adelante

From A: [(A,0), (B,19), (C,7)]

From C: [(A,7), (B,11), (C,0), (D,15), (E,5)]

From D: [(B,4), (C,15), (D,0), (E,13)]

From B: [(A,19), (B,0), (C,11), (D,4)]

From E: [(C,5), (D,13), (E,0)]

From C: [(A,7), (B,11), (C,0), (D,15), (E,5)]

A termina aprendiendo que para llegar a B, es mejor pasar por C que ir directo

From B: [(A,19), (B,0), (C,11), (D,4)]

From C: [(A,7), (B,11), (C,0), (D,15), (E,5)]

En el ruteo dinamico, el protocolo resuelve el camino segun los costos.

En el ruteo estatico, el ISP puede poner una ruta fija o un valor fijo de costo pasando por encima de lo que dice el protocolo.

Algunos protocolos trabajan por congestion, por lo que los costos se van actualizando

From A: [(A,0), (B,19), (C,7)]

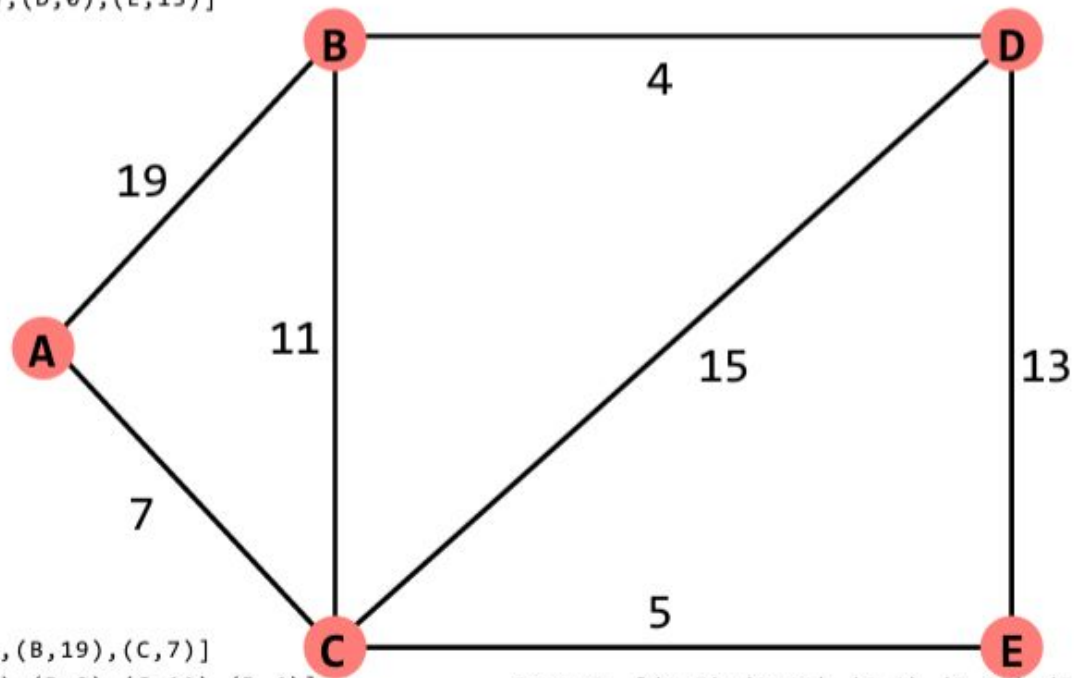
From B: [(A,19), (B,0), (C,11), (D,4)]

From D: [(B,4), (C,15), (D,0), (E,13)]

From E: [(C,5), (D,13), (E,0)]

From C: [(A,7), (B,11), (C,0), (D,15), (E,5)]

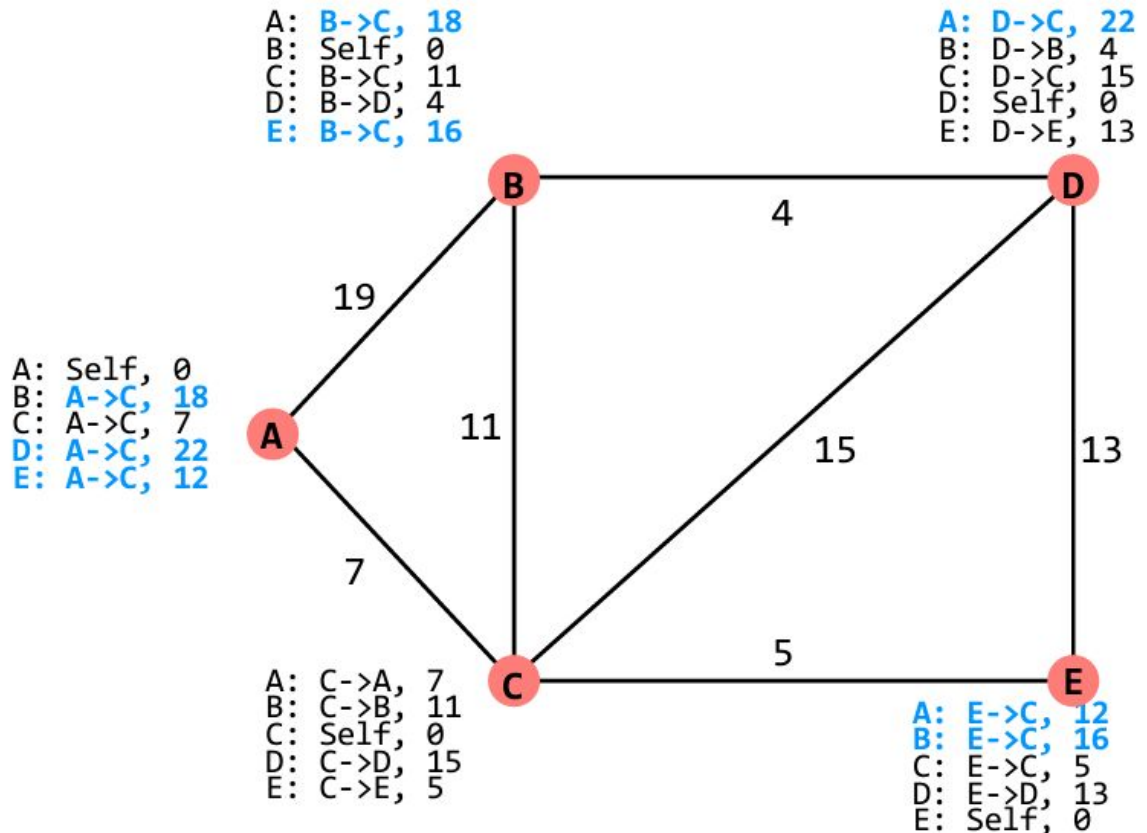
From D: [(B,4), (C,15), (D,0), (E,13)]



# Ruteo por vector

Se anuncian los **costos** de llegar a las redes en lugar de la topología

Cuando un nodo actualiza su tabla la vuelve a anunciar.





# Ruteo por *vector distancia*

Los protocolos tienen un heartbeat que se hace entre routers, para que sepan cuando se cayó el vecino

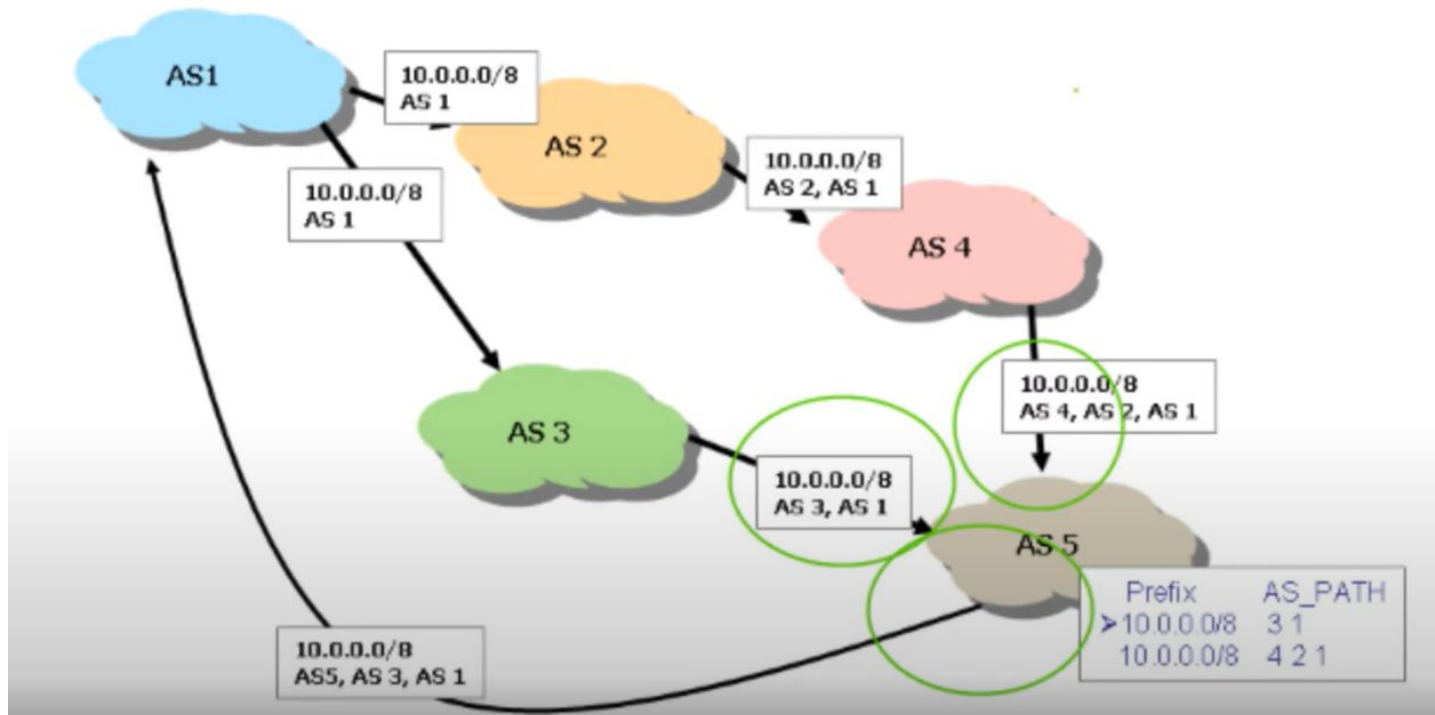
Es muy rápido para sumar nuevos nodos y actualizar la red.

Cuando un nodo “muere” es lento en actualizarse y aparecen problemas (Ej. Distancia Infinita)

# PROBLEMA

Ni estado de enlace ni vector distancia escalan bien para el tamaño que tiene internet.

Muchos AS, muchos caminos posibles



# Solución

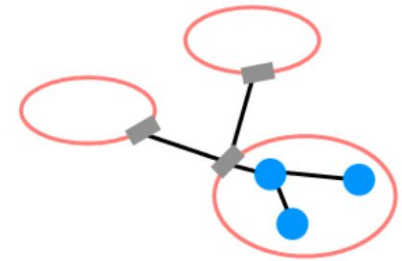
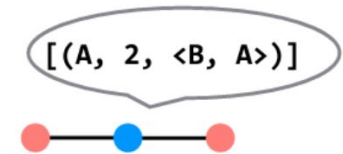
En vez de avisar todo lo que conoce, el router solo avisa el path que ya decidió para llegar a otro router

**Ruteo por path:** Los anuncios incluyen el path que decidió el router y sirve para detectar loops

**Ruteo jerárquico:** Se rutea dentro de los AS y fuera de los AS de manera independiente.

No todos los routers de un SA hablan con Internet

**Direccionamiento topológico:** Se asignan ruteo por bloques de direcciones y no por IPs.



18.0.0.0, ... , 18.0.0.255



18.0.0.0/24



Ruteo por

**PATH VECTOR**

# Ruteo por path vector

Es una mejora al *vector distancia*

La mejora es que cada nodo pasa el path completo que conoce

Un nodo pasa su path pero su decisión de armado puede ser:

- distancia
- ancho de banda
- económico
- etc

El protocolo por excelencia que usa path vector es BGP.

# Ruteo por path vector

**BGP** usa path vector

Su configuración es **manual**

Uno de los factores más importantes es el económico.

No siempre se evitan caminos congestionados (casi nunca).

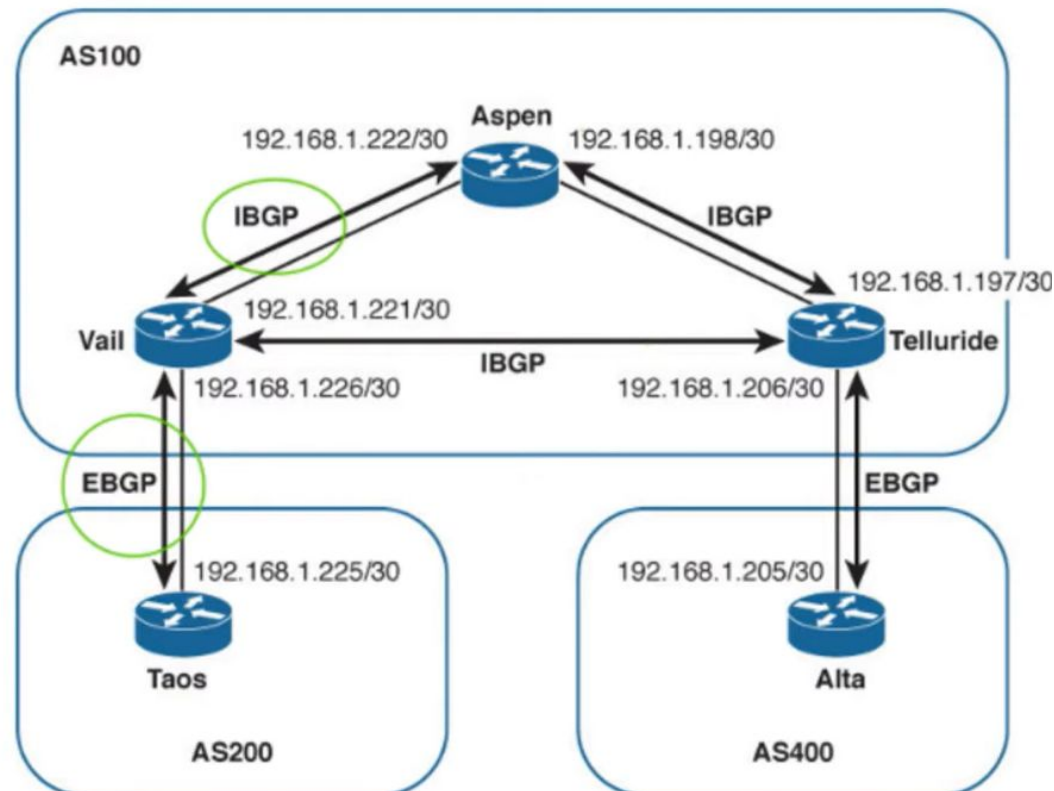
En internet, siempre me van a rutear por los caminos mas economicos, que no siempre son los mas baratos

# BGP – Border Gateway Protocol

- Protocolo estándar de conexión entre AS
- El objetivo de fondo es “limitar” conexiones
  - Los ISP quieren que solo pase por ellos el tráfico que corresponda (Ej. Cuestiones económicas)
  - Filtrar por origen, por destino o por otras cuestiones.
- No siempre es el “camino más corto”
- Corre sobre TCP puerto 179 Es algo loco que es un protocolo de ruteo de IP que corre sobre TCP.
- Maneja dos tipos de BGP:
  - iBGP para los routers del AS i de internal, e de external
  - eBGP para los routers fuera del AS

# BGP – Border Gateway Protocol

- Peers: Vecinos con los que comparto información de BGP
  - Si un Peer tiene el mismo número de AS uso iBGP
  - Si el número de AS es distinto uso eBGP





# BGP – Border Gateway Protocol

- En Internet hay 3 tipos de redes

- Red Stub

- Tienen solo una conexión a la red BGP
    - No se utilizan para tránsito de paquetes porque solo tiene una red

Ejemplo: toyota saca un SA y se conecta a internet.  
Ellos son stub porque no rutean.  
Tienen solo una interfaz y varias IP publicas (en algun sentido se puede comparar con una red hogareña)

- Red de multiconexión

- Tienen más de una conexión
    - Pero rechazan paquetes que tienen origen un AS desconocido y un AS destino desconocido.

Son las menos comunes. Son como una stub pero con mas de una interfaz (estan conectadas a multiples SA)

Ejemplo: toyota se conecta a nissan y solo forwarda paquetes a la red de nissan

- Transit Networks

Ejemplo: algun ISP como fibertel

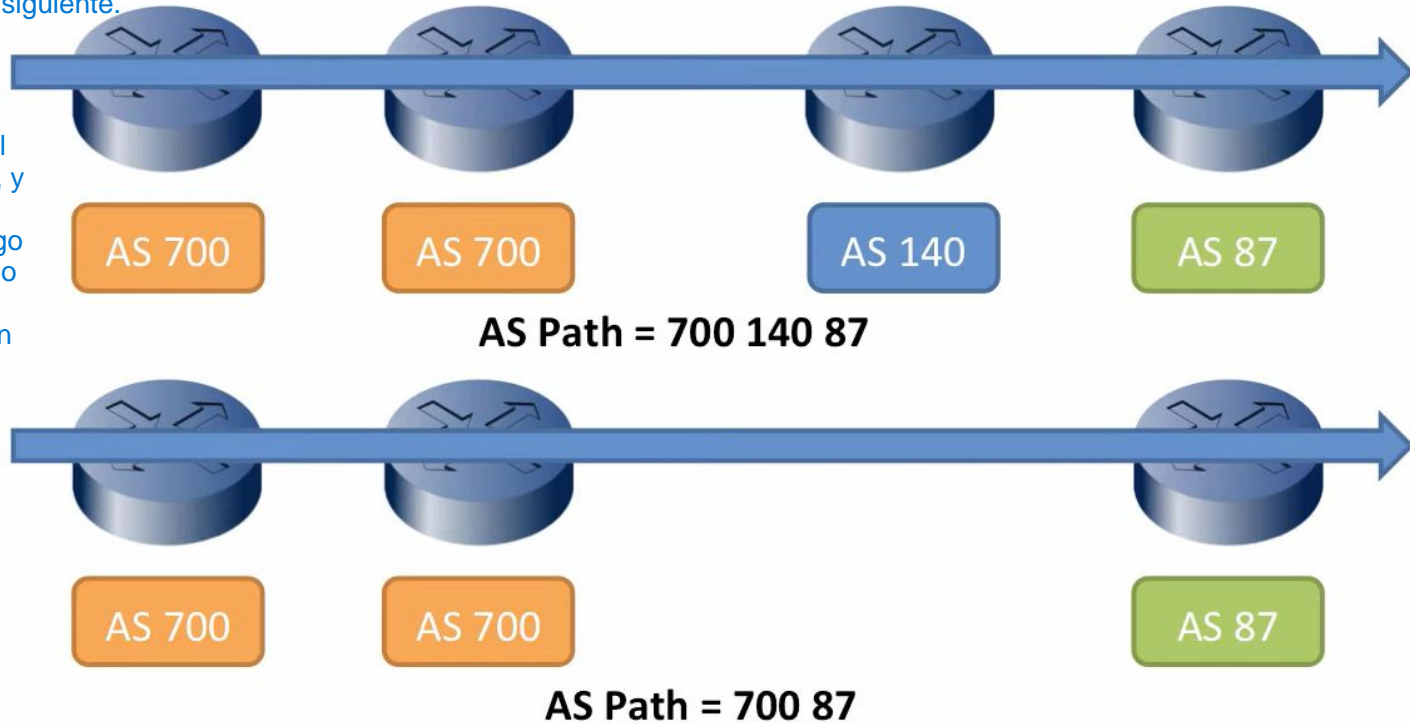
- Dejan transitar paquetes de terceros
    - Pueden aplicar restricciones
    - Cobran por el tránsito

# BGP – Border Gateway Protocol

- BGP tuvo éxito en Internet porque maneja políticas de tránsito
- Las políticas pueden ser de carácter
  - Seguridad
  - Político
  - Económico
- Ejemplos
  - No pasar tráfico a ciertos AS
  - Solo transitar por Albania si no hay otro destino posible
  - Tráfico de origen o destino IBM no debe transitar por Microsoft

# BGP – Decisión

## AS Path



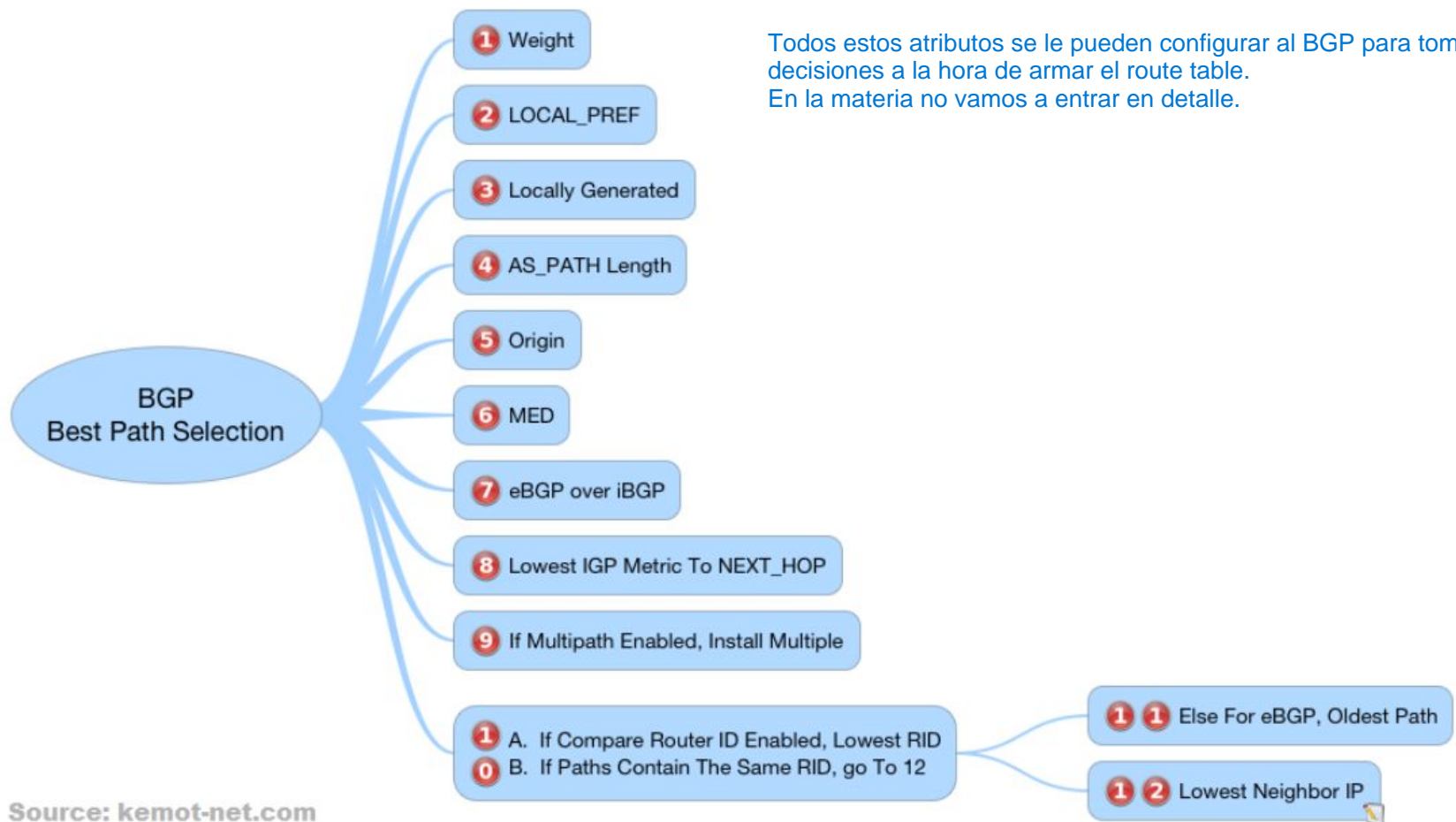
Para estos dos caminos posibles BGP elige el que tiene menos sistemas autónomos (700-87)

A la izquierda tengo dos routers que pertenecen al SA 700. Lo que termina armando BGP es una red de sistemas autónomos. En vez de fijarse IPs específicas, se fija en particular por que sistemas autónomos pasar para llegar a otro. El objetivo es no saber todas las IP por las que va a pasar el paquete, yo se lo paso a un SA y que el se encargue de pasarlo al siguiente.

Lo que pasa en la practica, es que yo se al SA que yo quiero llegar, y se el primer SA del camino al que se lo tengo que mandar. En el medio puede pasar por un monton de SA que estan fuera de mi control.

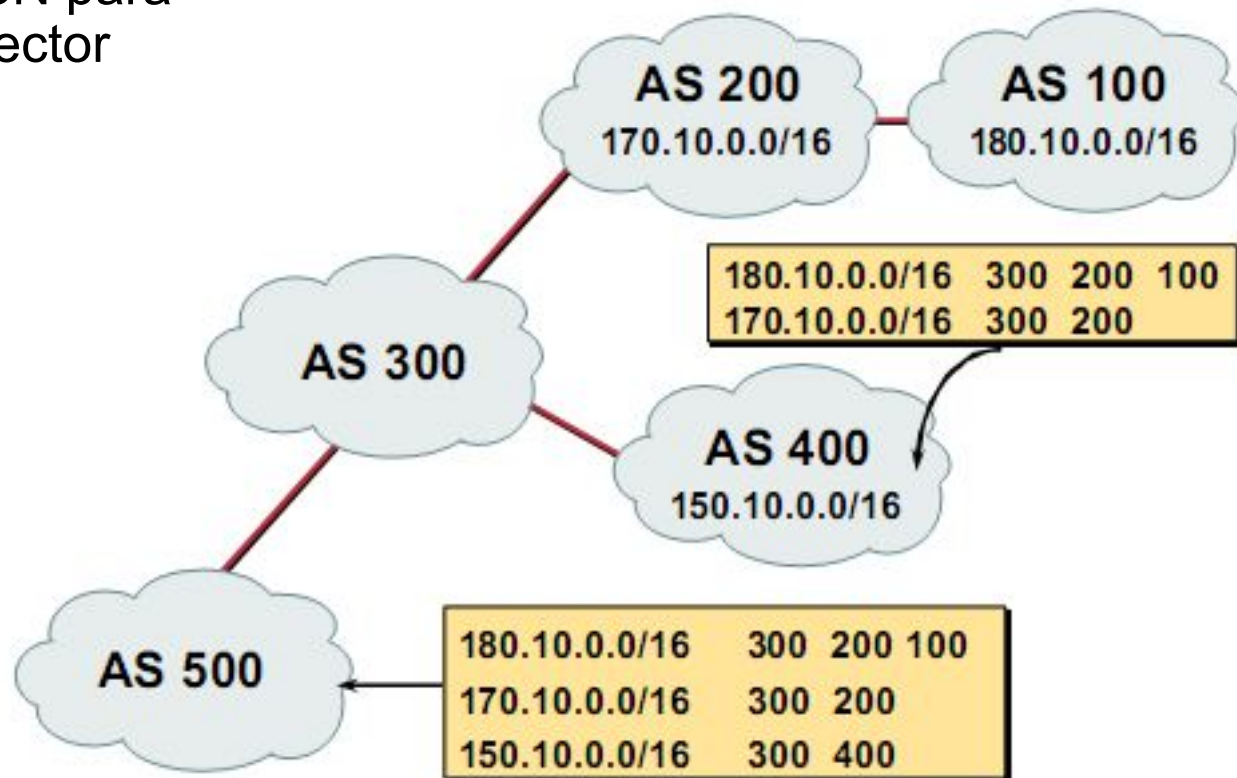
# BGP – Atributos

- Un router puede aprender un prefijo con diferentes atributos múltiples veces. Luego decide cual lo transforma en RUTA



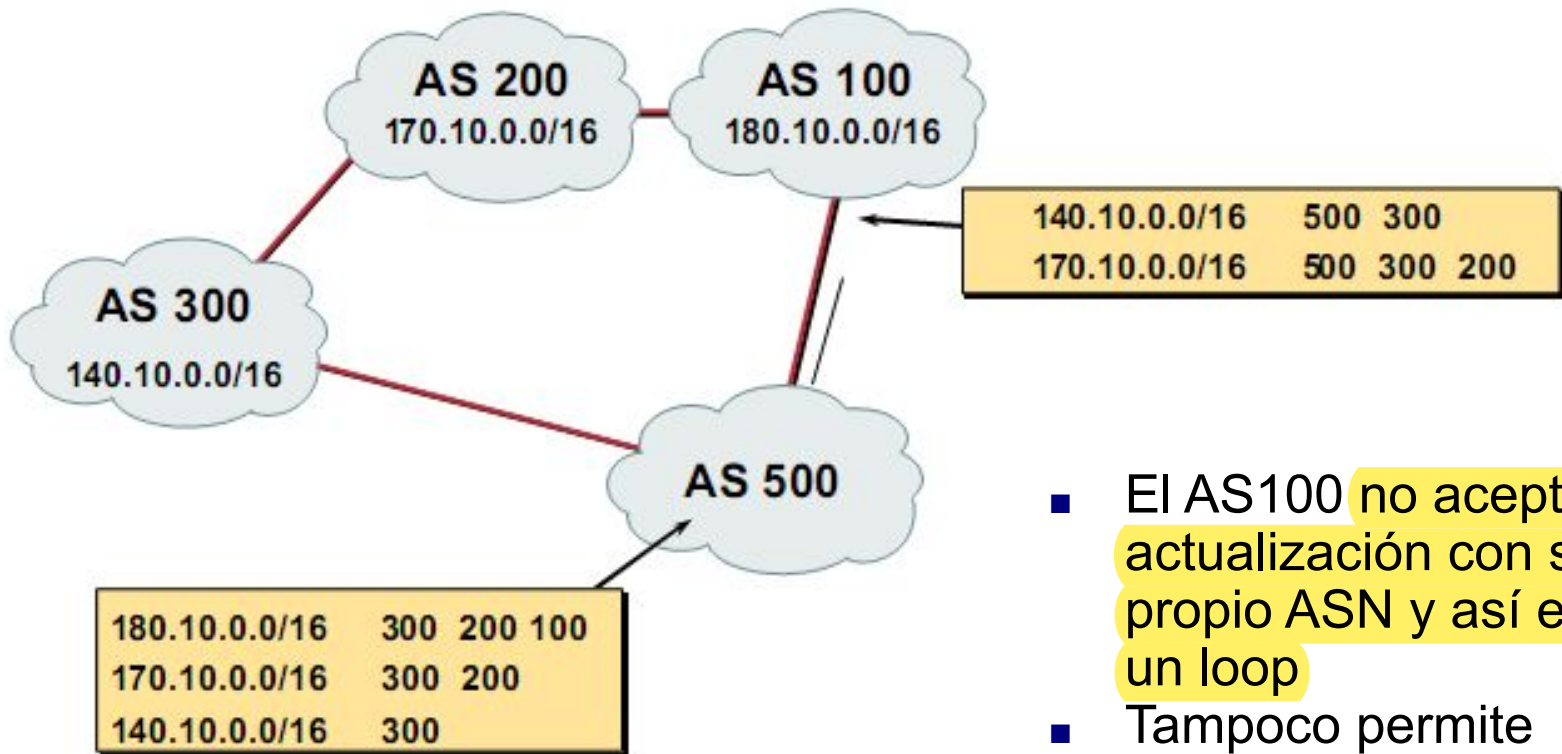
# BGP – Rutas

- Al pasar actualizaciones de rutas cada router añade su ASN para agregar al vector



# BGP – Loops

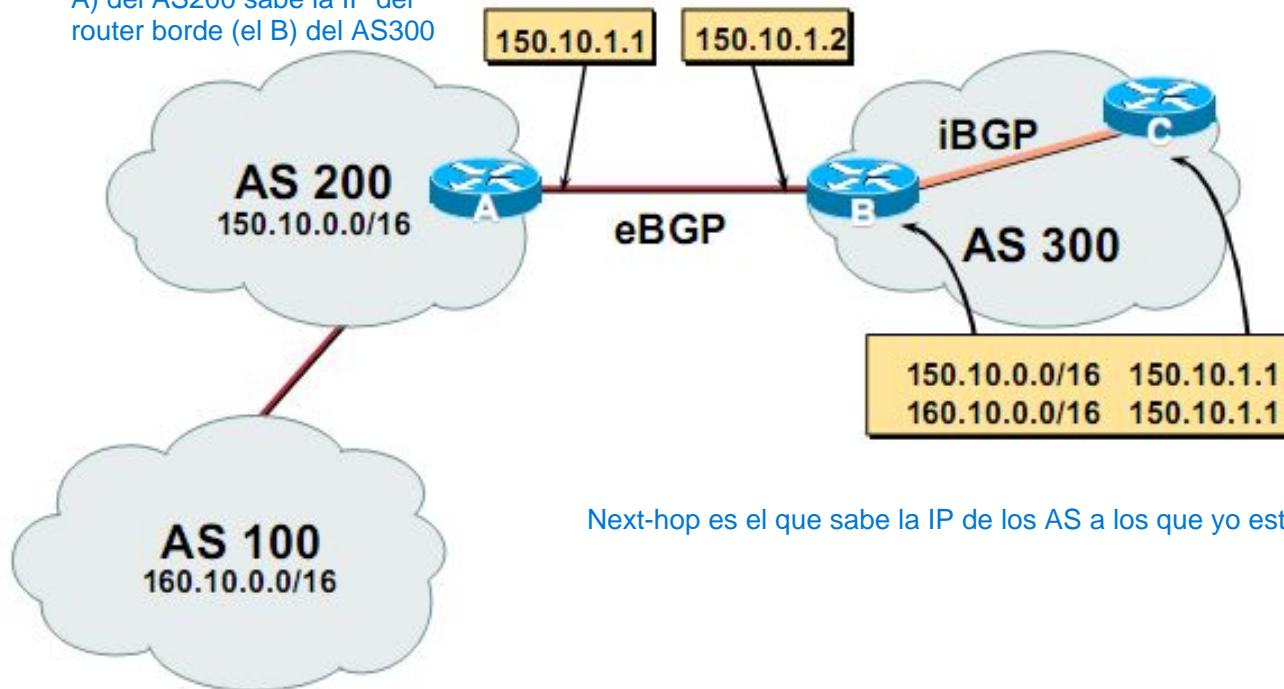
El BGP autodetecta y evita el formado de loops al armar las tablas



- El AS100 no acepta la actualización con su propio ASN y así evita un loop
- Tampoco permite actualizar el path con un AS por donde ya pasó

# BGP – Next Hop

En este caso un solo router (el A) del AS200 sabe la IP del router borde (el B) del AS300



Next-hop es el que sabe la IP de los AS a los que yo estoy conectados.

- Los routers dentro del AS tienen las mismas tablas por iBGP
- El router C, para saber como llegar a la red 150.10.0.0, deberá utilizar un protocolo IGP o una ruta estática.



# aplicación MTR (my traceroute)

- Muestra y monitorea los AS por donde pasan los paquetes.
- Ej: Desde mi casa a [www.facebook.com](http://www.facebook.com)

My traceroute [v0.94]								
NB-SRV1 (172.18.86.138) -> www.facebook.com				2024-03-17T18:33:12-0300				
Keys: Help    Display mode    Restart statistics    Order of fields    quit								
		Packets		Pings				
Host		Loss%	Snt	Last	Avg	Best	Wrst	StDev
1. AS???	NB-SRV1	0.0%	75	0.3	0.5	0.3	1.7	0.2
2. AS???	192.168.100.1	0.0%	75	1.1	1.8	1.0	9.3	1.3
3. AS???	100.122.16.4	0.0%	75	5.1	27.0	4.1	656.4	101.8
4. AS19037	be5-2.cf223-br-05.claro.net.ar	0.0%	75	10.5	11.5	7.3	17.4	2.6
5. AS19037	host147.170-51-254.telmex.net.ar	0.0%	75	56.5	41.6	7.5	86.1	19.5
6. AS32934	po204.asw01.eze1.tfbnw.net	0.0%	75	6.5	7.6	5.6	14.2	1.3
7. AS32934	psw03.eze1.tfbnw.net	0.0%	75	7.6	7.5	5.5	13.8	1.0
8. AS32934	173.252.67.107	0.0%	75	7.2	7.5	5.7	11.9	1.1
9. AS32934	edge-star-mini-shv-01-eze1.facebook.com	0.0%	74	7.2	8.0	6.5	18.1	1.5

Es un traceroute que te muestra por los routers que pasas, y el numero de AS de cada uno.

El host 1 es la compu de santiago

El host 2 es el router de santiago

El host 3 es parte de la red 100.64.0.0/10, que hace CGNAT (carrier grade nat). Esta no tiene asignado en un SA porque solo la pueden usar los carriers internamente. Lo que esta pasando es que el carrier me esta haciendo NAT, por lo que la "IP publica" de santiago es una IP dentro del carrier, no una IP publica de internet

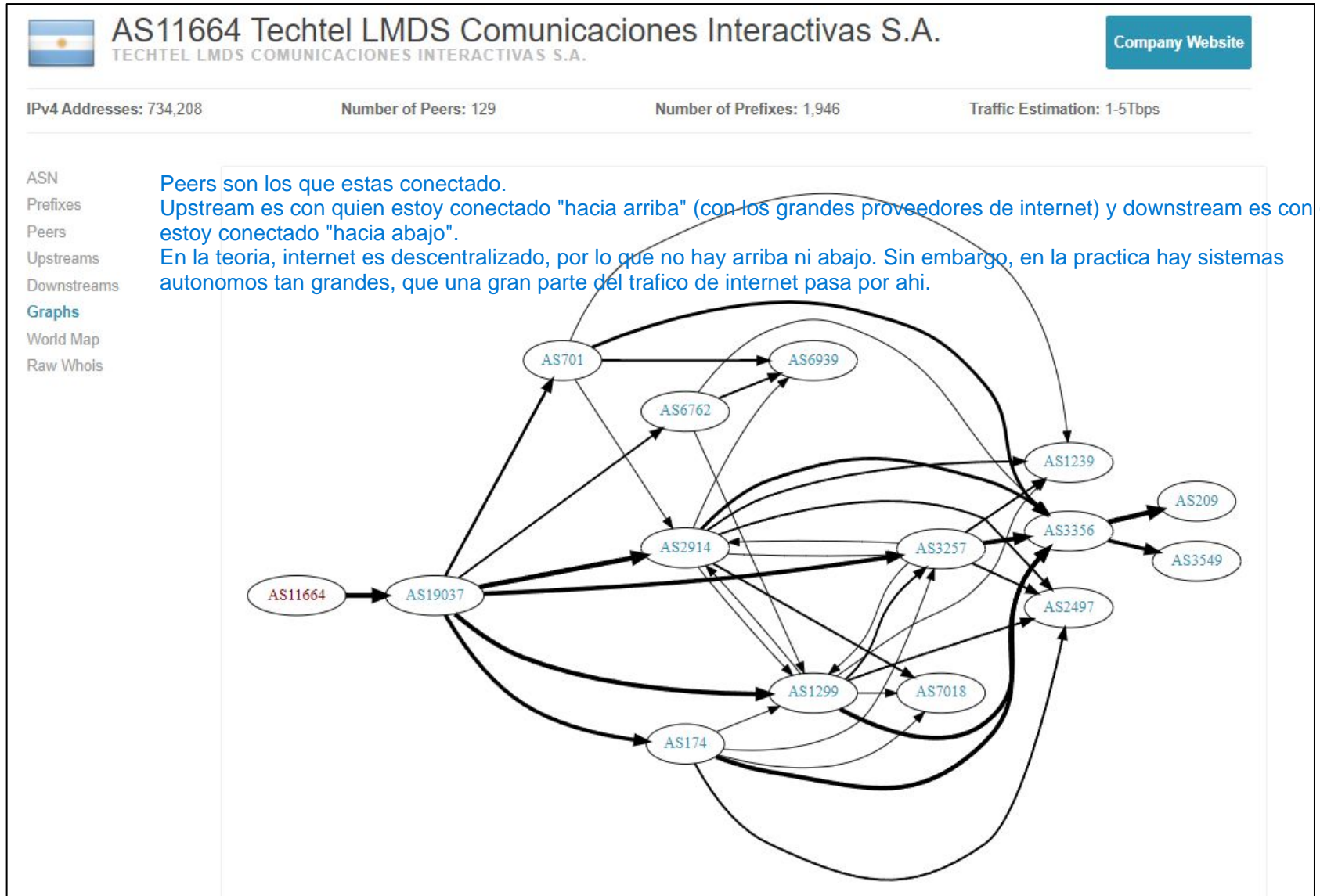
## traceroute -A lo hace también

Los hosts 6 a 9 son todos routers dentro del SA de Facebook



# BGPview.io

## ■ Gráfico de Upstream para el AS de mi casa

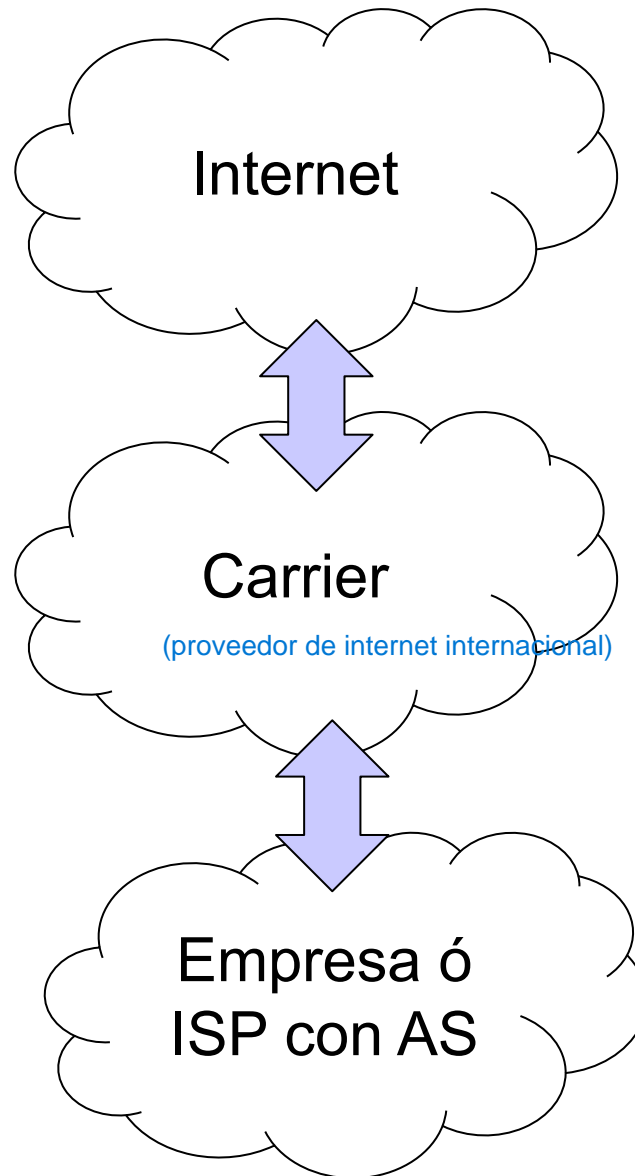


# BGP – BlackHole

- Se utiliza para mitigar ataques de DDoS
- Se puede disparar
  - Local
  - Remoto RTBH (remote triggered black hole)
    - Requiere soporte del proveedor de TRÁNSITO

Cuando te estan atacando, BGP dispara BlackHole

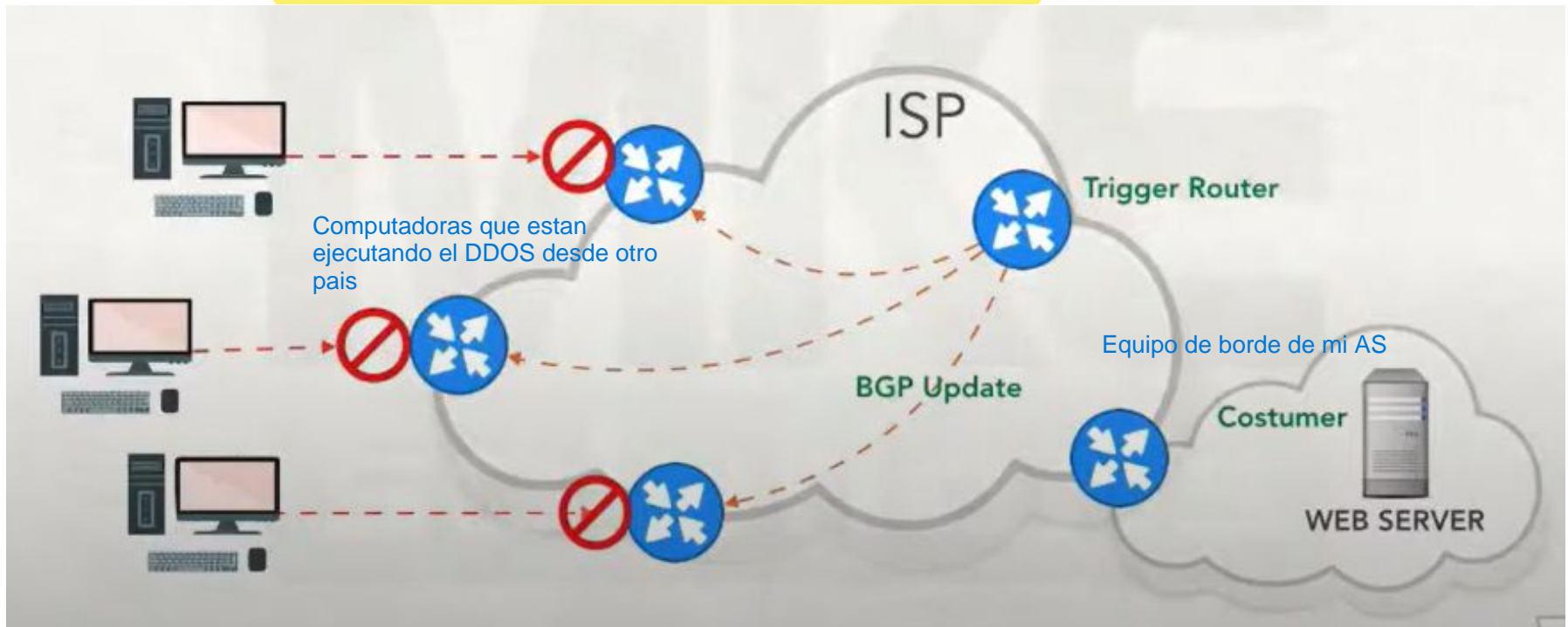
# Carrier



# BGP – BlackHole

- Se publica la dirección IP /32 ó /128
- El Carrier tienen que soportar BGP BlackHole
  - Algunos no lo soportan
  - Otros no lo implementan
  - Otros lo cobran
- El Carrier agrega esa IP a “ruta null” y descarta tráfico

Si a mi me estan atacando, mis equipos que disparan el BlackHole publican su propio IP publico al Carrier, y el carrier deja de mandarme paquetes. La idea es que la mayoría de los DDOS vienen de otros países (tipo Bratislava o lo que sea), entonces yo bloqueo el tráfico entrante de otros países y así me salvo del DDOS.



# BGP – BlackHole

- **Ventajas**

- **Detiene el ataque el carrier no alcanza tu router de borde**

- **Desventaja**

Te dejan sin internet entrante, no internet saliente. Igual estos DDOS no duran mas de unos minutos o horas. El BlackHole va subiendo carrier-grade y se va bloqueando de mas arriba, al lugar especifico de donde proviene el ataque

- **Se deja “sin Internet” a ese cliente atacado**
- **Requiere soporte del carrier** A veces el carrier lo cobra
- **Requiere de un sensor para automatizar la detección y bloqueo** A veces no hace falta un sensor, se hace manual llamando por telefono

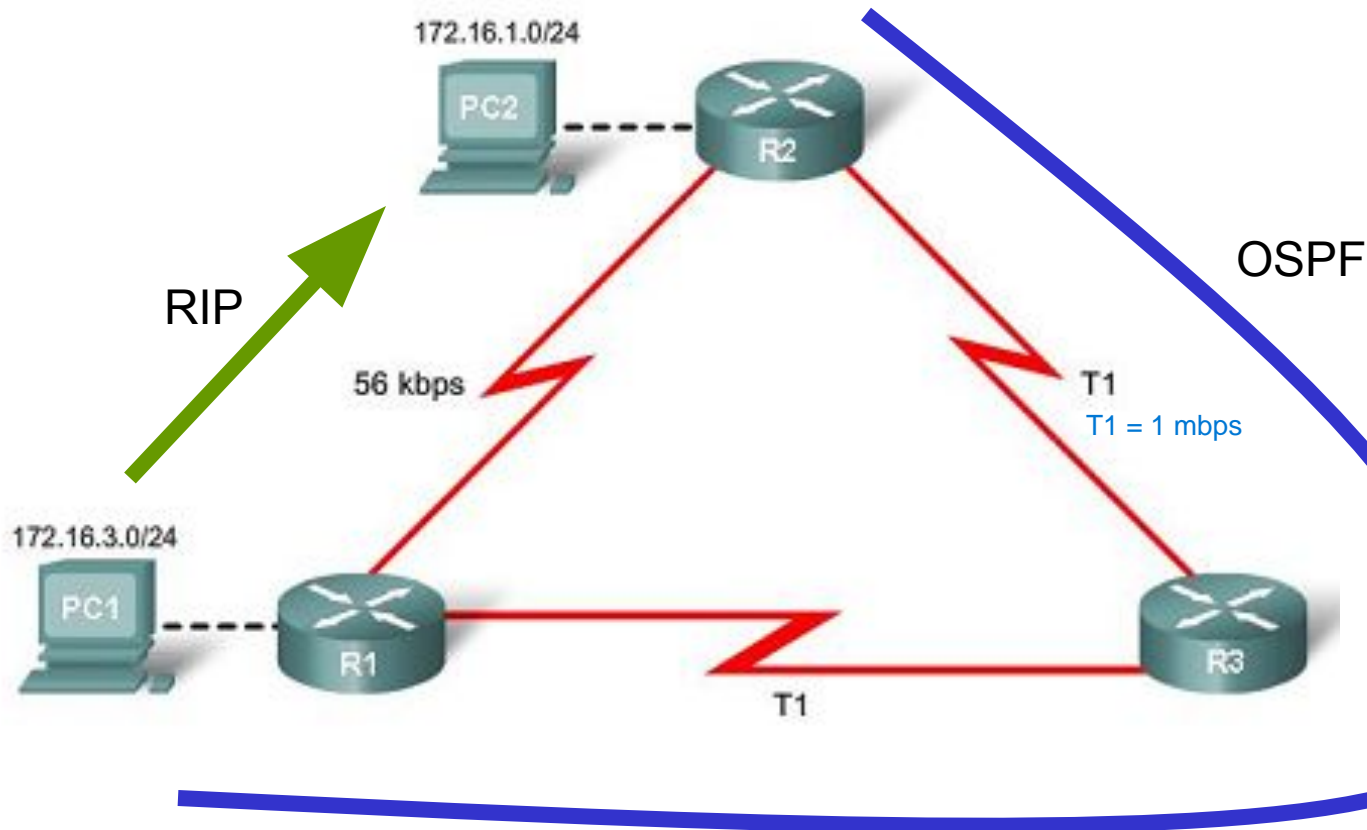
# Métricas

- **Conteo de saltos**
  - Cantidad de routers que un paquete tiene que atravesar
- **Ancho de banda**
- **Carga**
  - Considera la utilización de tráfico de un enlace determinado
- **Retardo** (latencia)
  - Considera el tiempo que tarda un paquete en atravesar una ruta
- **Confiabilidad** (este valor se pone a mano, un enlace que se suele caer tiene menos confiabilidad que uno que no se cae. Un enlace satelital es menos confiable que uno por cable)
  - Evalúa la probabilidad de una falla de enlace calculada a partir del conteo de errores de la interfaz o las fallas de enlace previas
- **Costo** costo economico
  - Un valor determinado ya sea por el IOS o por el administrador de red para indicar la preferencia hacia una ruta.

# Ejemplo

- **RIP y OSPF** informarían rutas diferentes

RIP es un protocolo que solo ve saltos. Va a llegar a la conclusion que la mejor forma de ir de PC1 a PC2 es por el camino verde porque tiene menos saltos. OSPF ve velocidades, entonces la ruta elegida va a ser la azul.



# Distancia Administrativa (AD)

- Que sucede cuando un router conoce una red por distintos caminos mediante diferentes protocolos de enrutamiento ?
- La AD es un valor entero entre 0 y 255

Origen de la ruta	Distancia administrativa
Conectado	0
Estática	1
Ruta sumariada EIGRP	5
BGP externo	20
EIGRP interno	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EIGRP externo	170
BGP interno	200

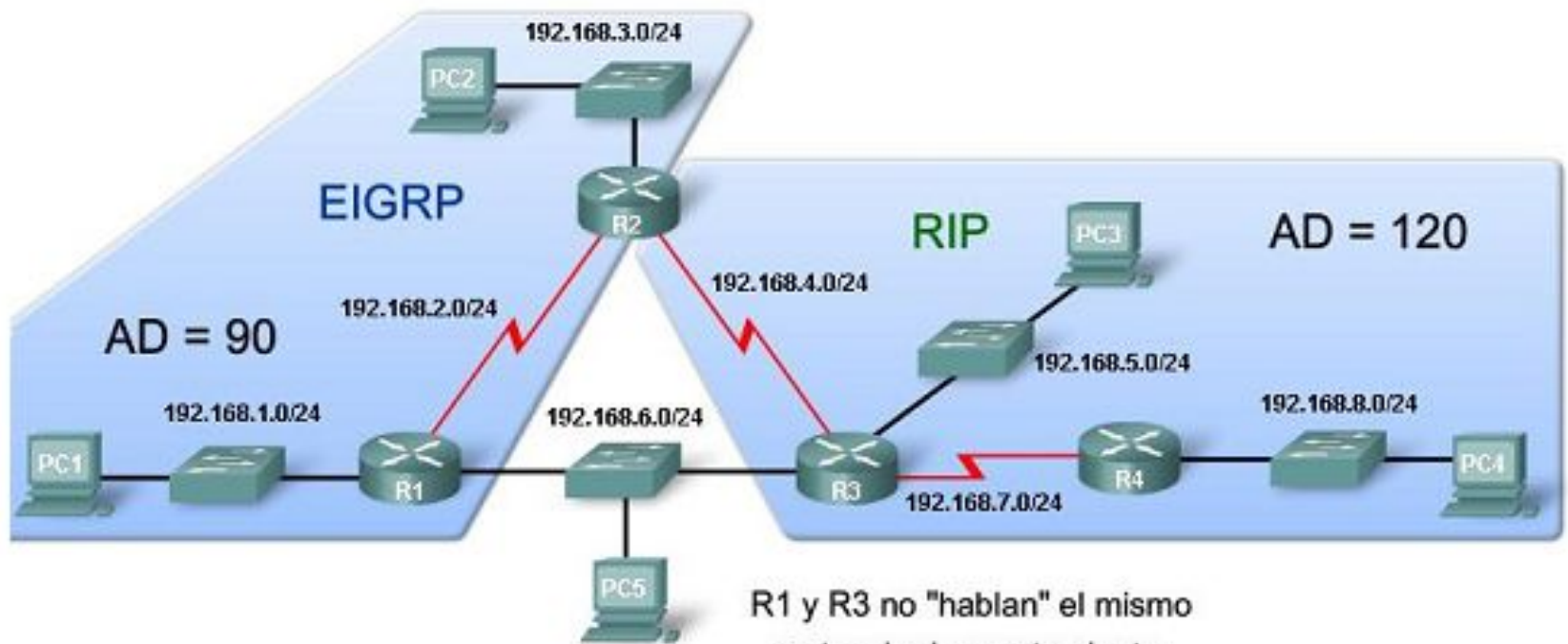
Existe un factor que se llama distancia administrativa, que te da una ponderación de cada protocolo. Cuando es menor, significa que la decisión que voy a tomar es mejor/ mas importante. RIP tiene una AD de 120 y OSPF tiene una de 110, osea que los routers le van a dar prioridad a las decisiones tomadas por OSPF.

La tabla esta preparada para que aparezcan otros protocolos de ruteo, por eso los numeros tienen diferencias.



# Distancia Administrativa (AD)

- Ejemplo: El Router R2 quiere llegar la red 192.168.6.0/24



R1 y R3 no "hablan" el mismo protocolo de enrutamiento.

En este caso, la PC5 se quiere comunicar con el exterior. El camino que toma es el que se ve tirando el comando show ip route

# Distancia Administrativa (AD)

- Al ejecutar **show ip route** en el router se obtiene:

```
R2#show ip route
<output omitted>

Gateway of last resort is not set

D    192.168.1.0/24 [90/2172416] via 192.168.2.1, 00:00:24, Serial0/0/0
C    192.168.2.0/24 is directly connected, Serial0/0/0
C    192.168.3.0/24 is directly connected, FastEthernet0/0
C    192.168.4.0/24 is directly connected, Serial0/0/1
R    192.168.5.0/24 [120/1] via 192.168.4.1, 00:00:08, Serial0/0/1
D    192.168.6.0/24 [90/2172416] via 192.168.2.1, 00:00:24, Serial0/0/0
R    192.168.7.0/24 [120/1] via 192.168.4.1, 00:00:08, Serial0/0/1
R    192.168.8.0/24 [120/2] via 192.168.4.1, 00:00:08, Serial0/0/1
```

- La salida informa: Protocolo, la red, [AD/métrica], dirección para llegar a la red, hora:min:seg de el ultimo update de la ruta, interfaz por la cual llegar a la red.
- Vemos solo la ruta a la red 192.168.6.0 por EIGRP, por tener menor AD que RIP.

# Distancia Administrativa (AD)

- ¿Que sucede si se cae el enlace con R1?
- RIP tiene almacenado las rutas que aprendió

Este comando te dice la tabla entera, no solo las rutas mas importantes.

```
R2#show ip rip database
192.168.3.0/24    directly connected, FastEthernet0/0
192.168.4.0/24    directly connected, Serial0/0/1
192.168.5.0/24
    [1] via 192.168.4.1, Serial0/0/1
192.168.6.0/24
    [1] via 192.168.4.1, Serial0/0/1
192.168.7.0/24
    [1] via 192.168.4.1, Serial0/0/1
192.168.8.0/24
    [2] via 192.168.4.1, Serial0/0/1
```

- Por lo tanto el router puede utilizar ese camino

# IGRP

- Desarrollado por CISCO
- Se considera el ancho de banda, el retardo, la carga y la confiabilidad para crear una métrica compuesta.
- Por defecto, se envía un broadcast de las actualizaciones de enrutamiento cada 90 segundos.
- El IGRP es el antecesor de EIGRP y actualmente se considera obsoleto



# EIGRP

- Desarrollado por CISCO
- No existen actualizaciones periódicas. Las actualizaciones se envían cuando se produce un cambio en la topología.
- Puede realizar un balanceo de carga con distinto costo.
- Establece adyacencia con los vecinos (peers) con el “saludo” EIGRP
- La métrica se basa en el ancho de banda mínimo y en el retardo acumulado de la ruta.
- Mantiene en una base de datos todas las rutas recibidas ( no solo las mejores), por eso ante fallas tiene rápida convergencia