NOC-Red CUDI

Hans Ludwing Reyes Chávez
hans@noc.cudi.edu.mx

Centro de Operación de CUDI/CLARA, DGSCA
UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

Abril 2008
Tuxtla Gutiérrez
UNACH

Mapa en una Universidad

Comodity Internet

Red de Voz

IP-PBX

Firewalls/ Seguridad

Usuarios remotos

Internet2

WLANs

UNIVERSITY

Red de Multimedia y Video Conferencia

Computo de Alto Desempeño

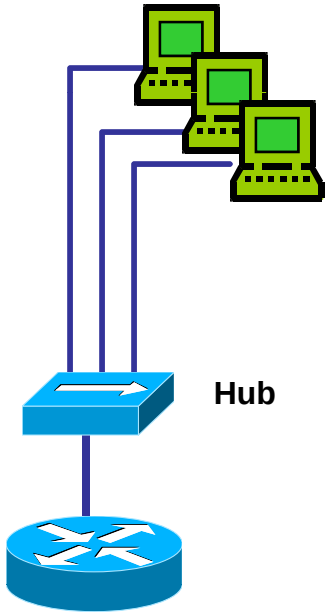
Otros Campus Remotos

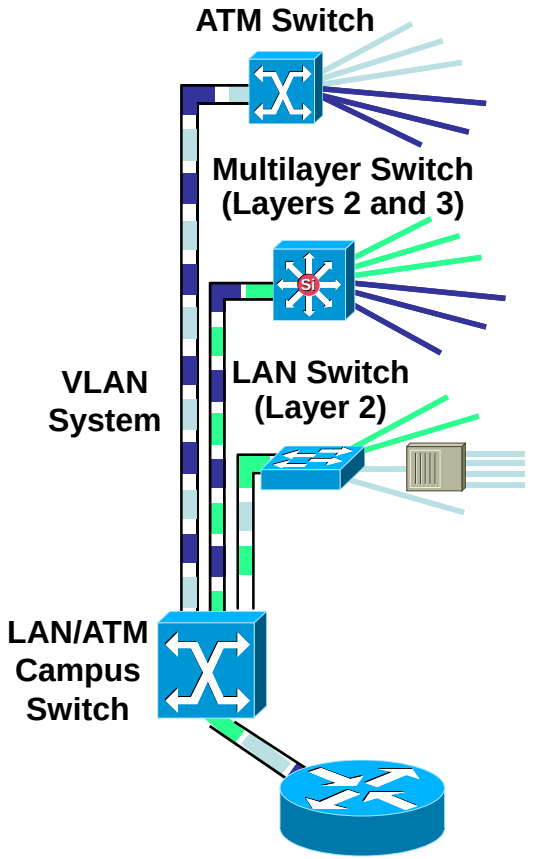
Mejores practicas

LAN

Ambientes de Red

Compartido → **Switcheado**



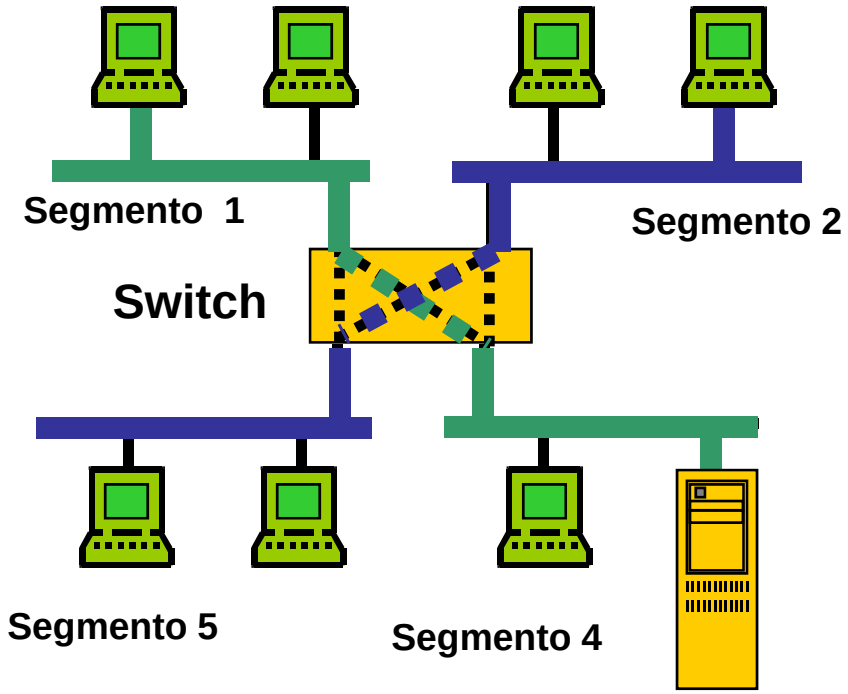


Características

- Trabaja en la capa 2 y 3 del modelo OSI.
- Provee ancho de banda dedicado en cada uno de sus puertos, es decir, los dispositivos conectados a él obtienen acceso inmediato a TODO el ancho de banda.
- Segmenta el tráfico de colisiones (en otras palabras: elimina las colisiones)
- Aprende y genera una tabla direcciones MAC de los dispositivos que “ve” por cada uno de sus puertos.
- Gracias a que provee de un ancho de banda de dedicado para cada dispositivo, permite “conversaciones” simultaneas.
- Funciones de enrutamiento en capa 3
- Balanceadores switches capa 7

Ambiente switcheado

- No hay colisiones
- Ancho de banda dedicado



Fordwarding

- Después de revisar la dirección destino el switch lee la dirección origen para determinar por qué puerto va a reenvíar ese paquete.
  - Si la dirección destino está en la tabla, reenvía el paquete por el puerto correspondiente.
  - Si la dirección destino no está en la tabla, el switch reenvía elpaquete por todos los puerto excepto por el que lo recibió .
- Los switches pueden implementar diferentes métodos para el reenvío de paquetes (fordwarding), estos son:
  - Store and fordward
  - Cut-Through

Fordwarding (cont.)

- Store and Fordward
  - Se lleva a cabo el chequeo de errores en el frame
  - Se desechan los frames corruptos

- En el método store and forward, el swtich lee y copia el frame entero dentro de un buffer y lleva acabo el algoritmo CRC (Cyclic Redundancy Check) y el frame se desecha si el resultado es erróneo o si el frame es enano o (*runts,* menores a 64 bytes) o si es gigantes o (*gigants*, mayores a 1518 bytes) .

Fordwarding (cont.)

- Cut-Through
  - El switch solo lee y copia a un buffer hasta la dirección destino, es decir, solo procesa los primeros 14 bytes del frame .
  - Busca la dirección reenvía.
- Este método, lógicamente es mucho más rápido que el Store and Forward, pero es menos confiable (nadie es perfecto).

- Algunos switches se pueden configurar para que mientras no se alcance a un umbral de errores definido, implemente Cut-Through, y si se alcanza el umbral utilice Store and Forward.

Ejemplo

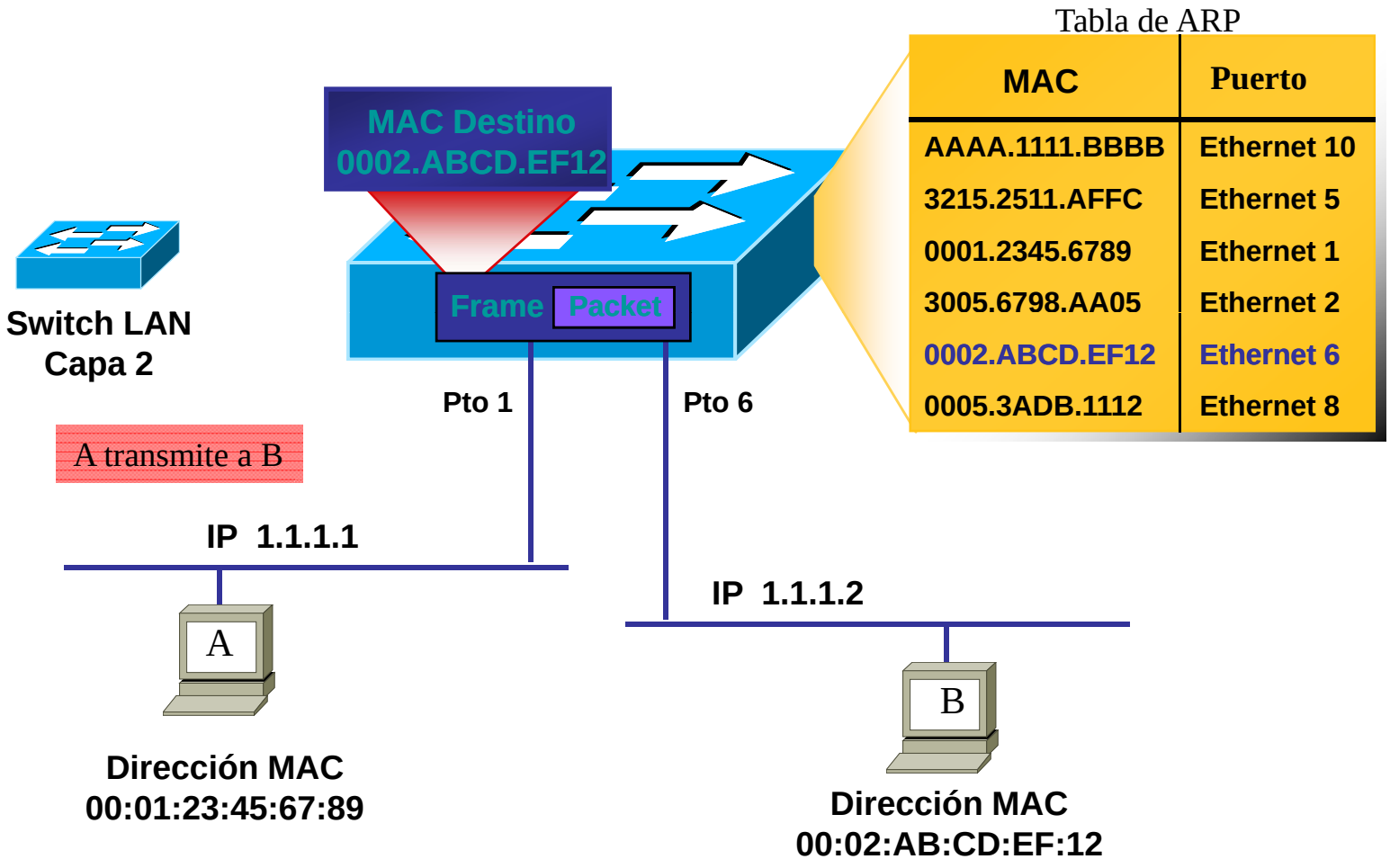
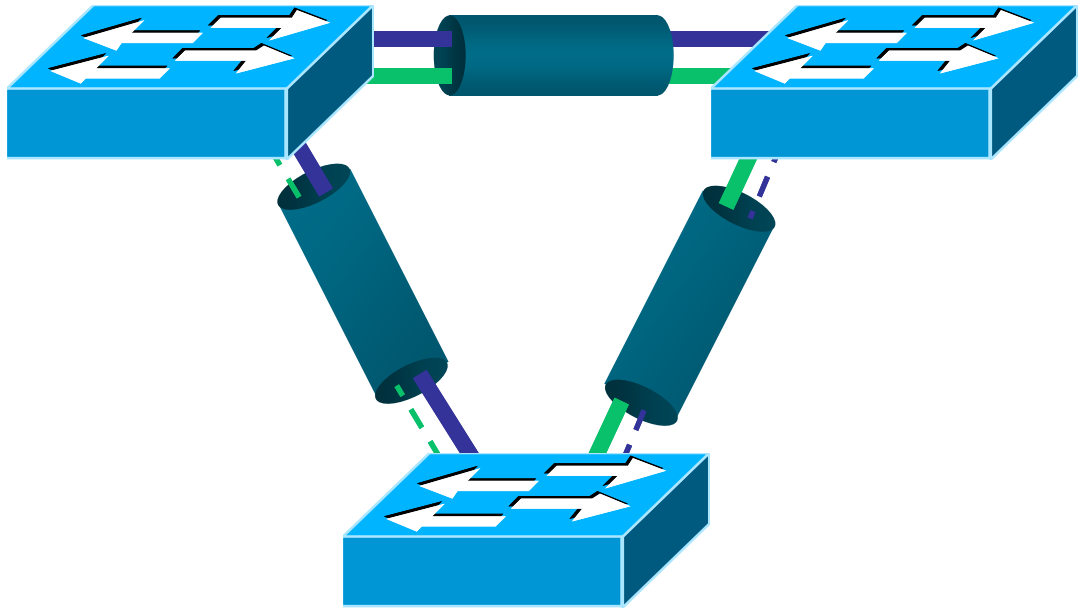


Tabla de ARP
MAC
Puerto
AAAA.1111.BBBB
Ethernet 10
3215.2511.AFFC
Ethernet 5
0001.2345.6789
Ethernet 1
3005.6798.AA05
Ethernet 2
0002.ABCD.EF12
Ethernet 6
0005.3ADB.1112
Ethernet 8
MAC Destino
0002.ABCD.EF12
Frame
Packet
Switch LAN
Capa 2
Pto 1
Pto 6
A transmite a B
IP 1.1.1.1
IP 1.1.1.2
A
B
Dirección MAC
00:01:23:45:67:89
Dirección MAC
00:02:AB:CD:EF:12

Redundancia

Redundancia

- También se puede implementar redundancia en capa 2 a través del protocolo STA (Spanning Tree Algorithm)



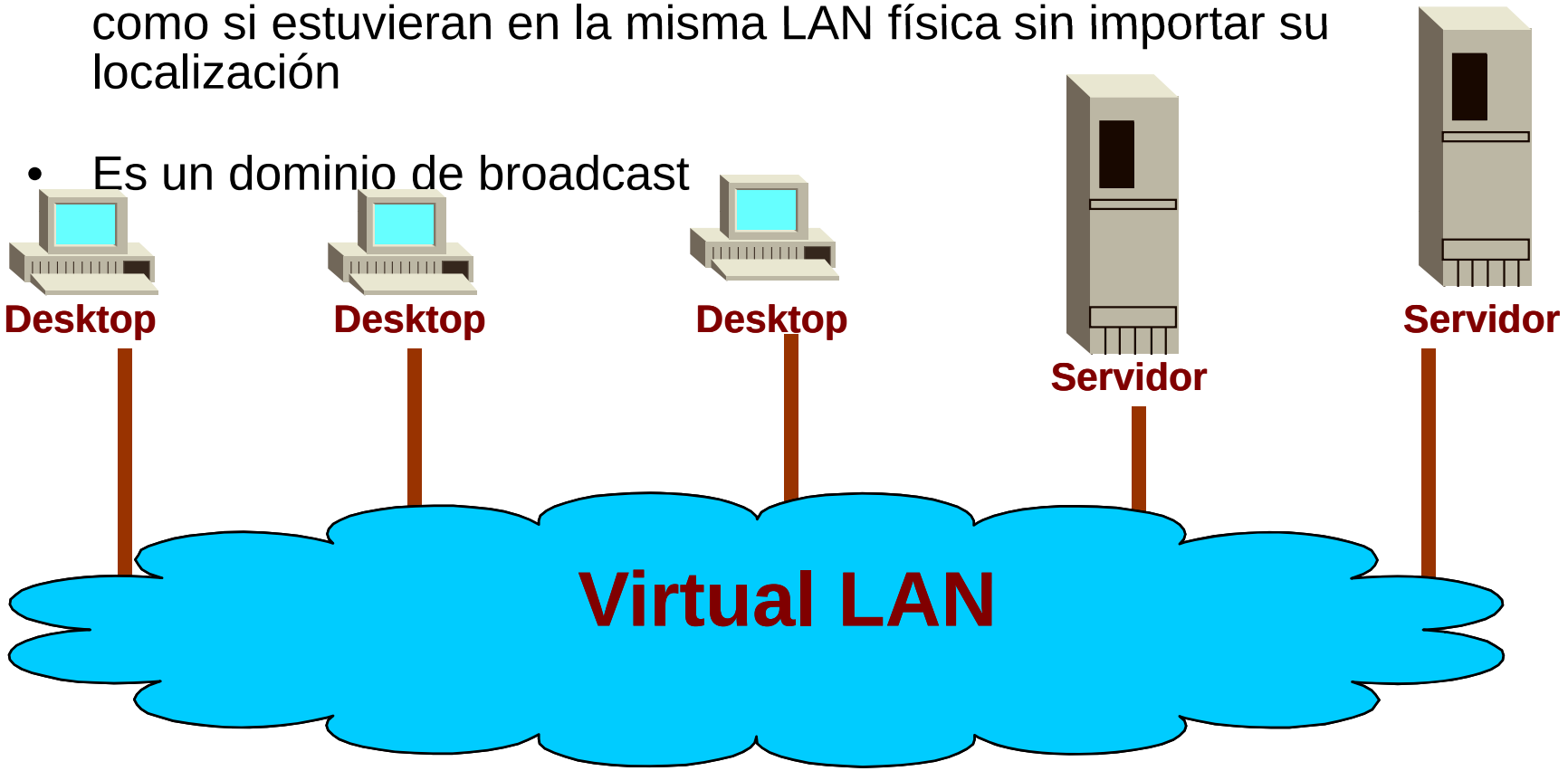
VLAN's

¿Qué es una LAN?

• Es un medio compartido que interconecta a computadoras por medio de un sistema de broadcasting de frames transmitidos por una computadora al resto de las computadoras en el segmento. Cada computadora decide individualmente si recibe o descarta el frame.

¿Qué es una VLAN?

- Un grupo flexible de estaciones que se comunican entre si como si estuvieran en la misma LAN física sin importar su localización
- Es un dominio de broadcast

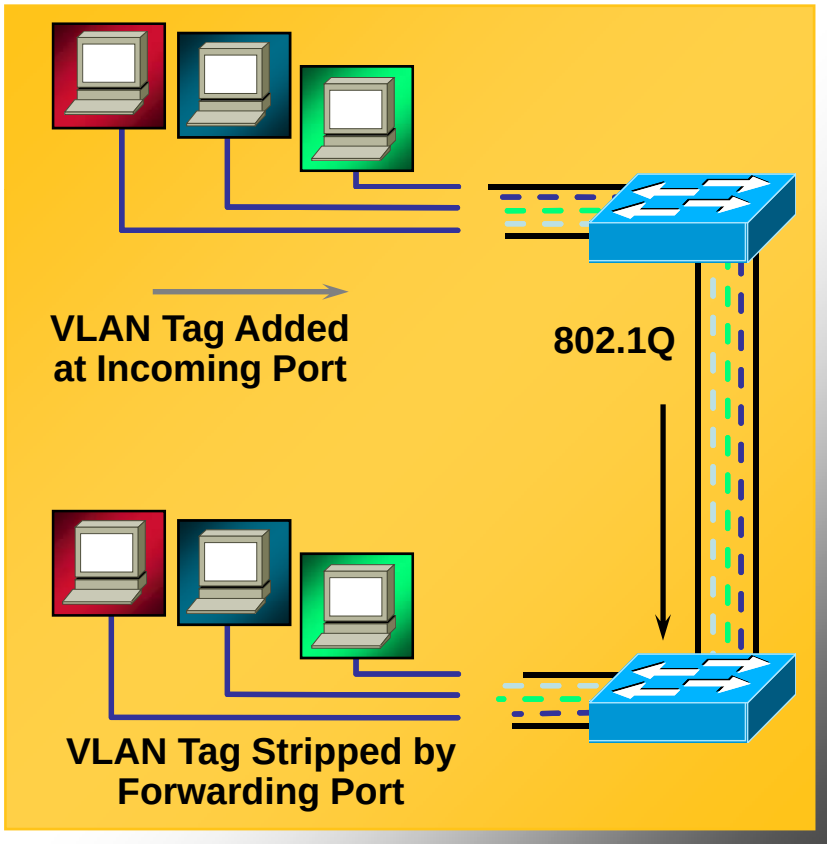


Tipos de VLAN´s

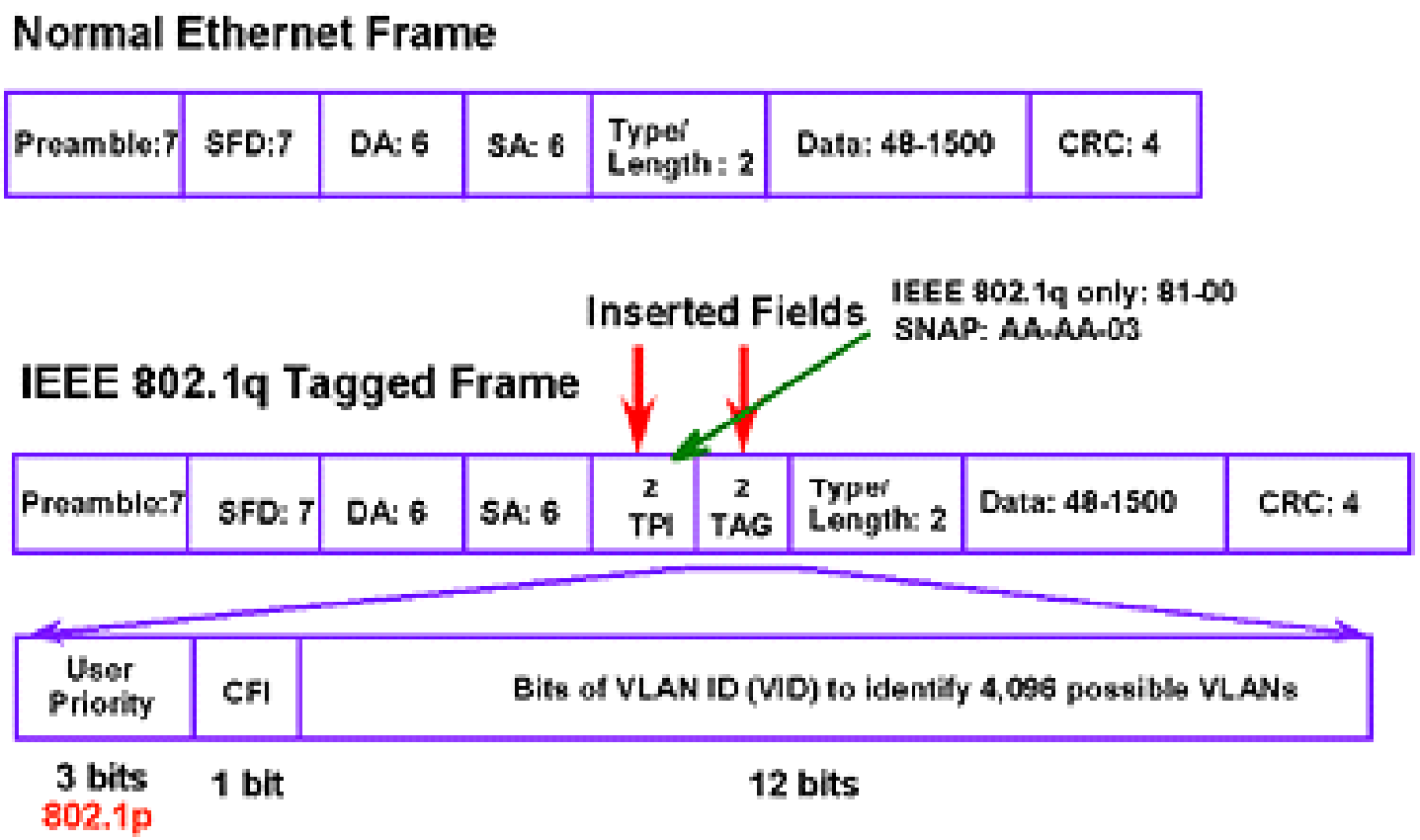
- **Basadas en Puertos.**
  - Cada Interfase Fisica del switch esta configurada como miembro de una VLAN.
- **Basadas en direcciones MAC**
  - En el switch o por medio de una base de datos, cada MAC se registra como miembro de una VLAN especifica. Relacion UNO a UNO
- **Basadas por Protocolo.**
  - Se identifica a que protocolo de capa 3 pertenece y se le asocia a uno VLAN.
    - Por ejemplo IPX, IP, Appletalk

802.1Q

- 802.1 es un estándar de la IEEE que establece el método para etiquetado de los frames de ethernet dentro de una VLAN.
- 802.1Q fue desarrollado para poder segmentar redes demasiado extensas, permitiendo seccionarlas en segmentos pequeños, asi evitar grupos de broadcast demasiado extensos.
- Proporcionan seguridad



802.1Q - Virtual LANs



Beneficios

Desempeño

- segmentación
- control de dominio de broadcast
- prevención de tormentas de broadcast
- “eficiencia”
- modelado de flujos de tráfico
- QOS
- eliminar los cuellos de botella en los ruteadores
- soporte de granjas de servidores (centralización)
- escalabilidad

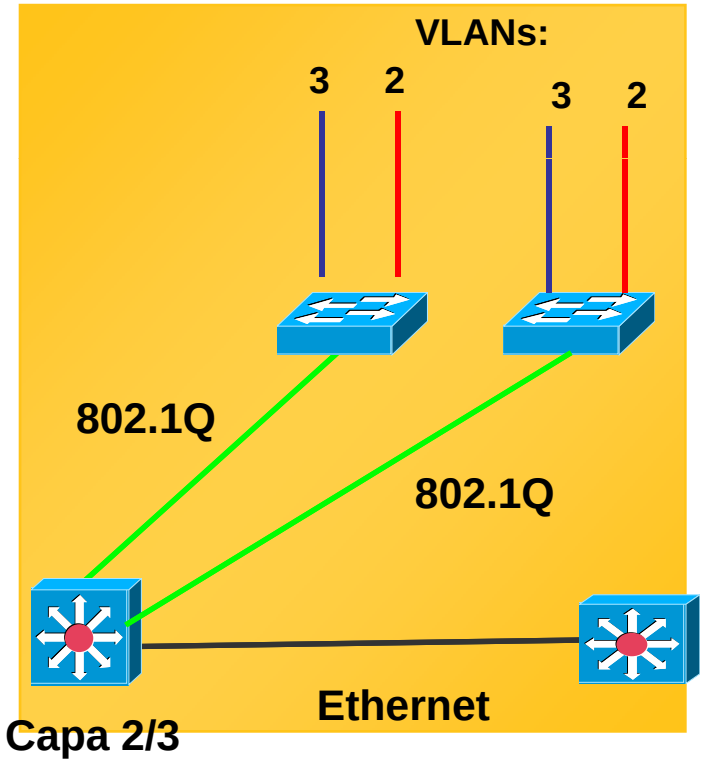
Beneficios (cont.)

- Administración
  - simplificación de la admón.
  - adiciones/movimientos/cambios
  - grupos de trabajo distribuidos
  - infraestructura de admón.
  - escalabilidad
  - reducir el tiempo para hacer cambios
- Seguridad
  - control de acceso

Ruteo entre VLAN´s

- Para que exista comunicación entre VLAN´s diferentes (Vlan ID) es necesario contar con un equipos de capa 3.

```
interface FastEthernet0/0
 no ip address
 no ip directed-broadcast
!
interface FastEthernet0/0.1
 encapsulation dot1Q 1
 ip address 132.248.204.254 255.255.255.0
 no ip directed-broadcast
!
interface FastEthernet0/0.2
 description Ingenieria
 encapsulation dot1Q 100
 ip address 132.248.200.254 255.255.255.0
 no ip directed-broadcast
```



Redes WAN

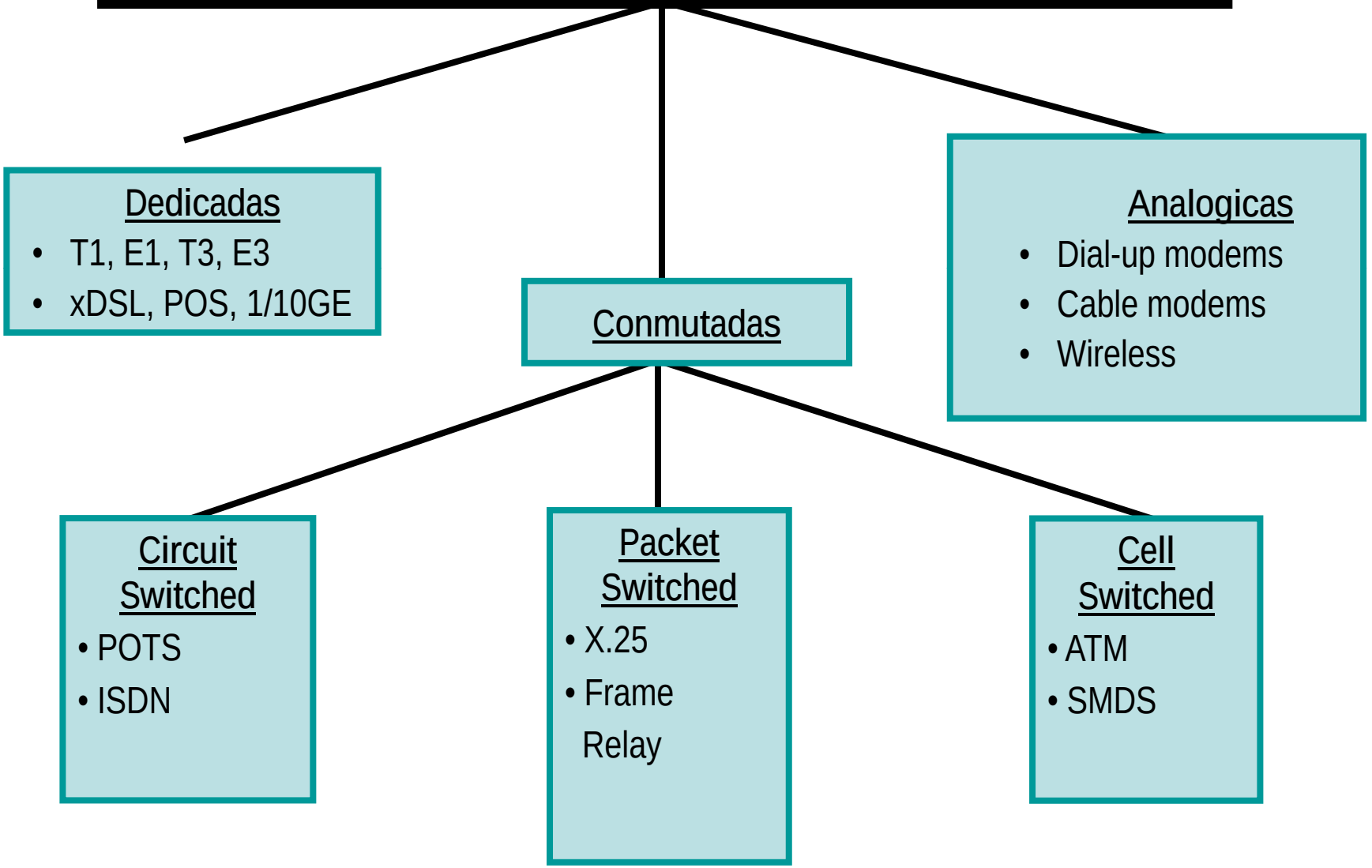
Servicios WAN

- Las WAN proporcionan el intercambio de información entre diferentes LAN que se encuentran geograficamente separadas.
- Las WAN interconecta diferentes dispositivos

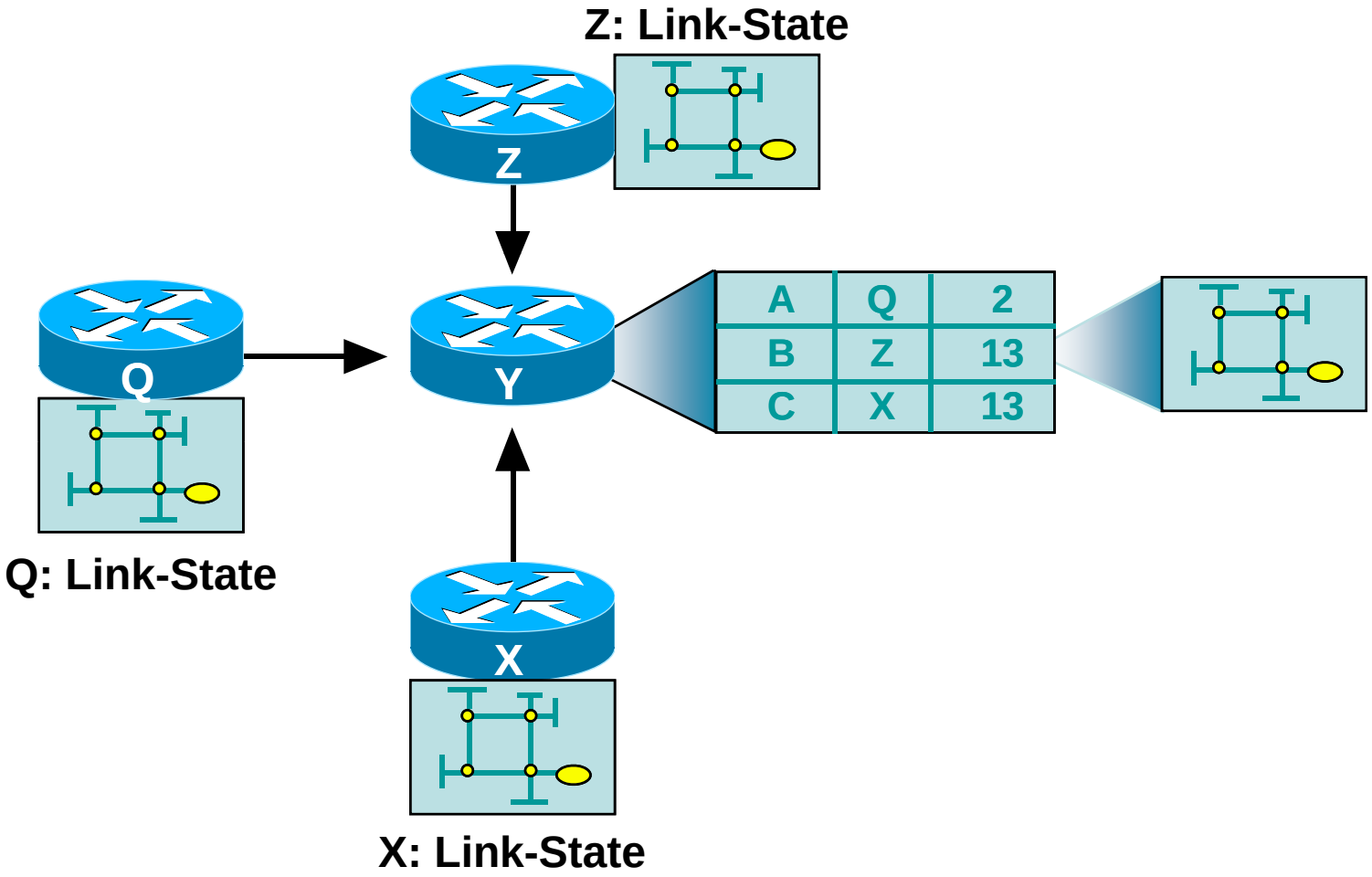
Estándares WAN

- Que capas del modelo OSI describen a los estándares WAN ?
  - Capa Física
  - Capa de Enlace

Tecnologías WAN

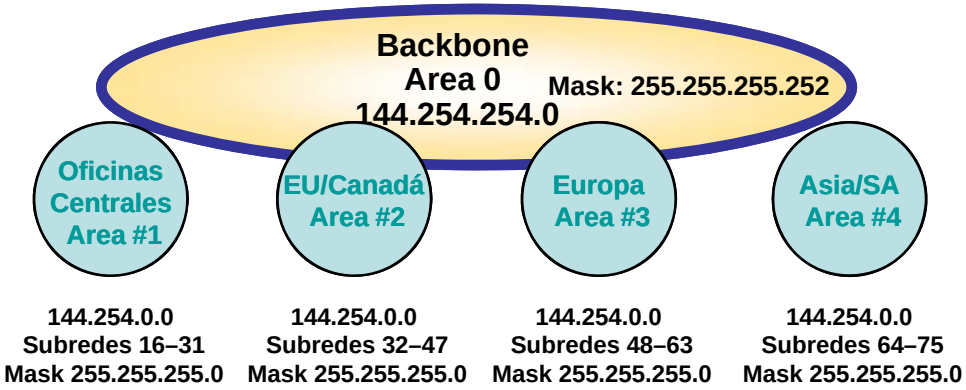


OSPF - Link-State

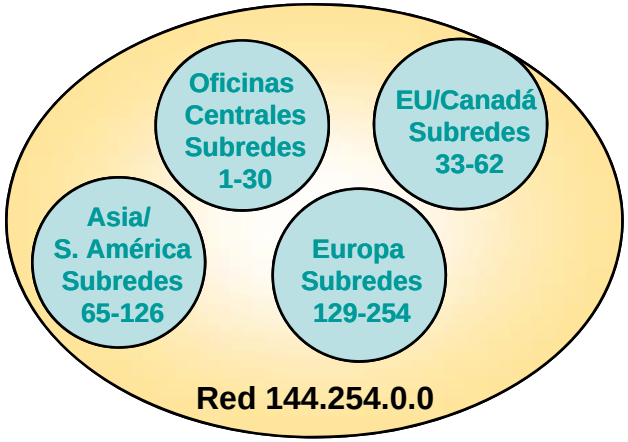


Configuración

Link State



Distance Vector



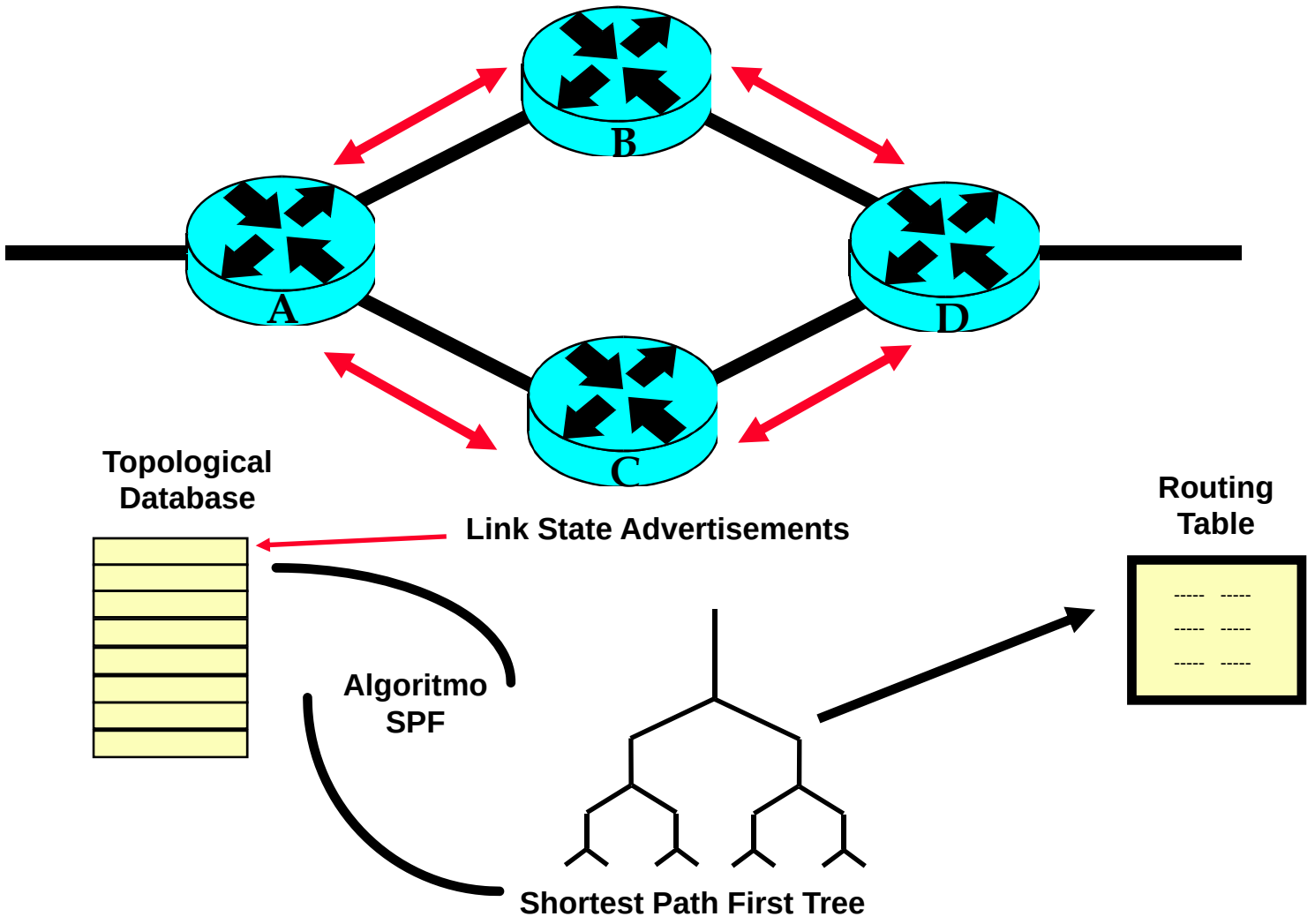
	Link State	Traditional Distance Vector	Advanced Distance Vector
Configuración	Difícil	Fácil	Fácil

OSPF

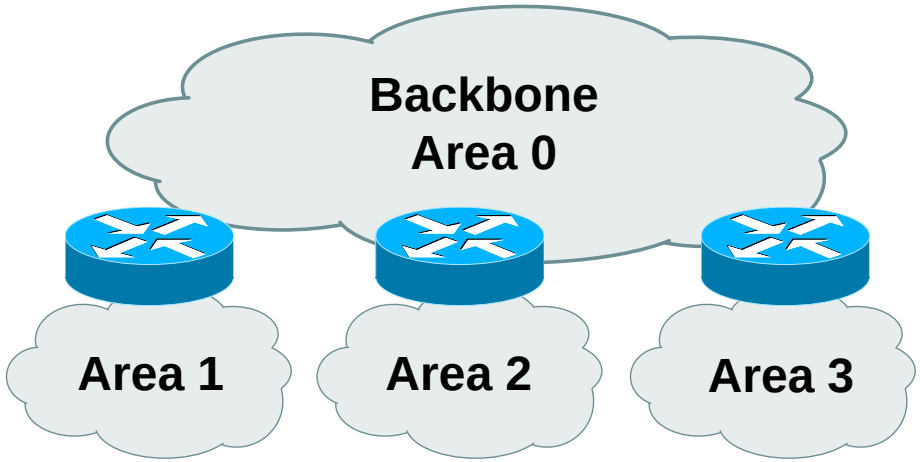
Open Shortest Path First:

- Desarrollado por el IETF en 1988.
- Intradominio.
- Link-State.
- Maneja VLSM.
- Soporta redes discontiguas.
- Utiliza multicast para el envío de su información de ruteo.

Link State

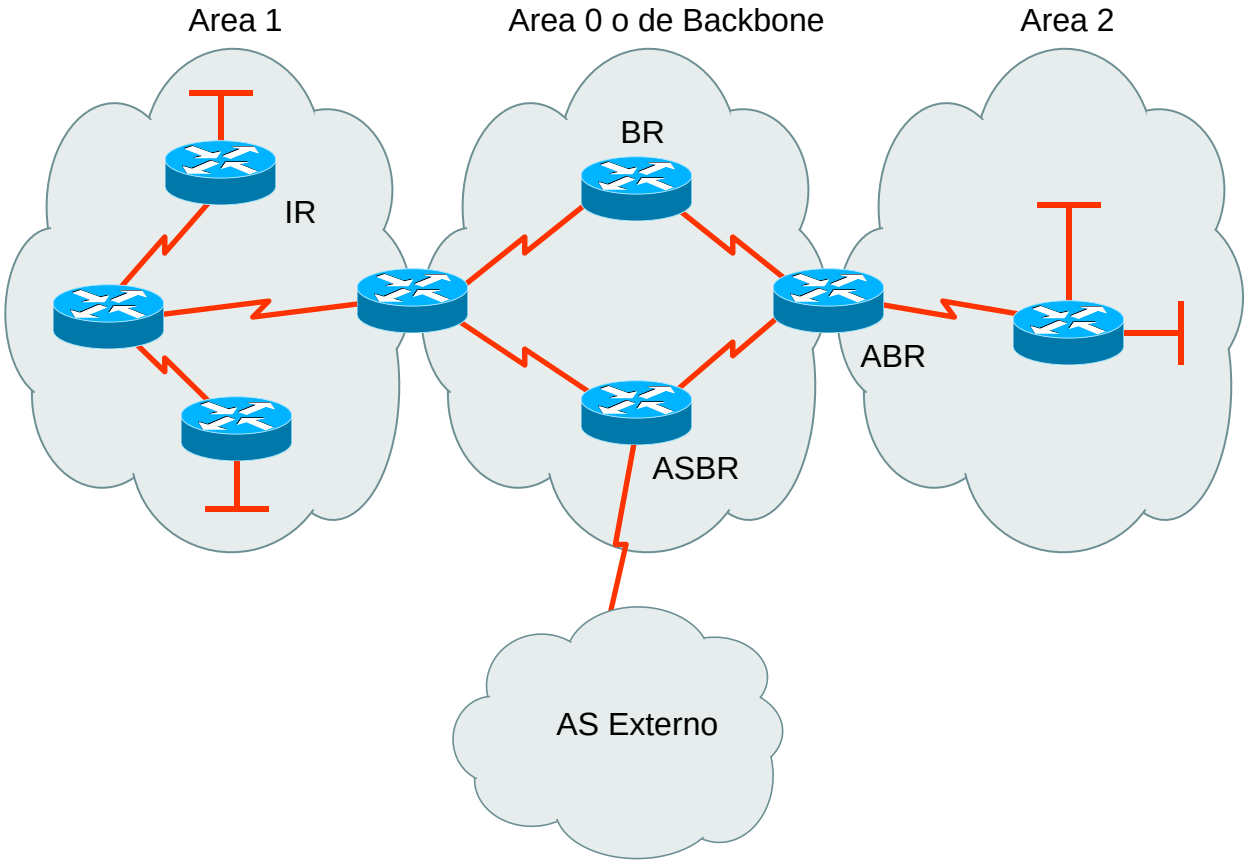

B
A
D
C
Topological Database
Link State Advertisements
Routing Table
Algoritmo SPF
Shortest Path First Tree

Areas en OSPF

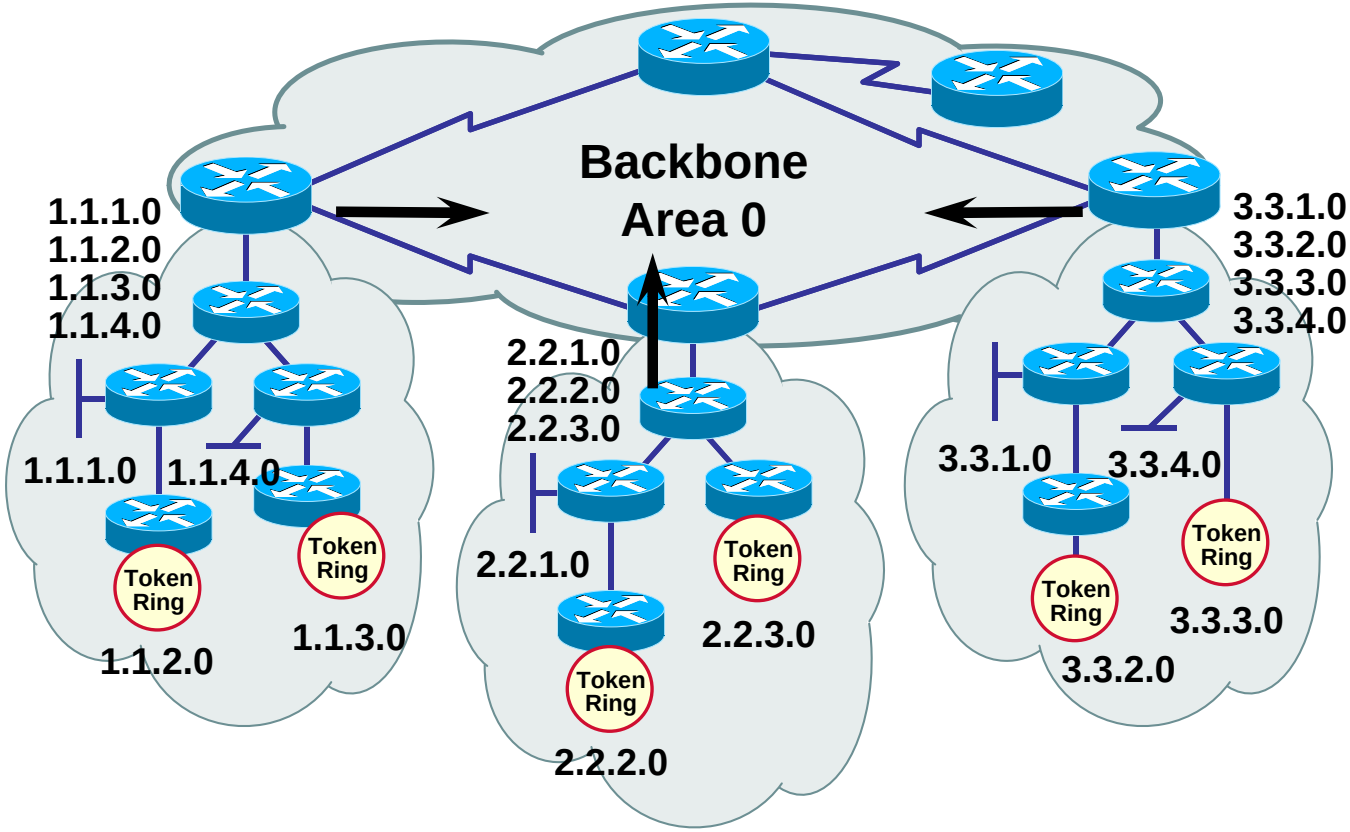


- La topología dentro de un área permanece invisible para las demás áreas.
- Se reduce el tráfico de ruteo.

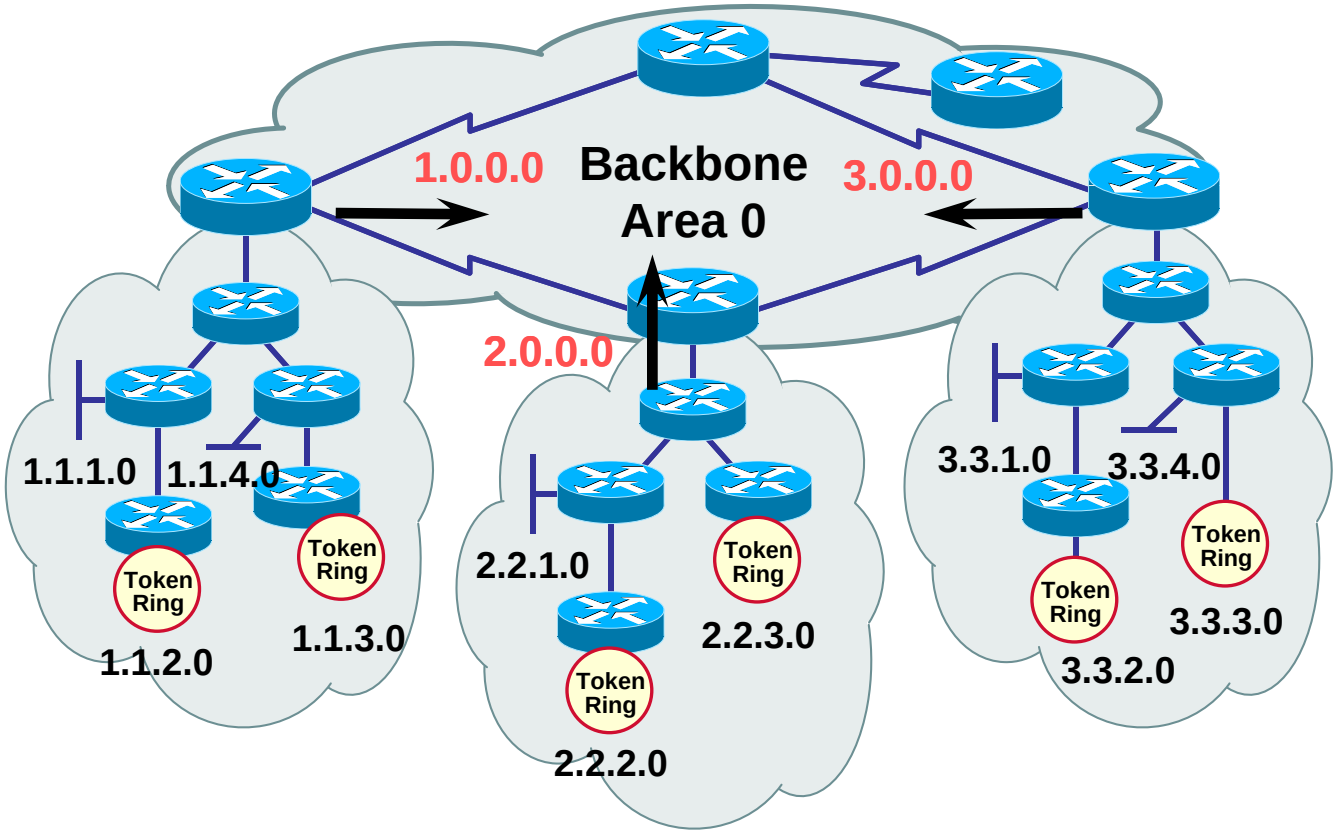
Ruteadores en OSPF



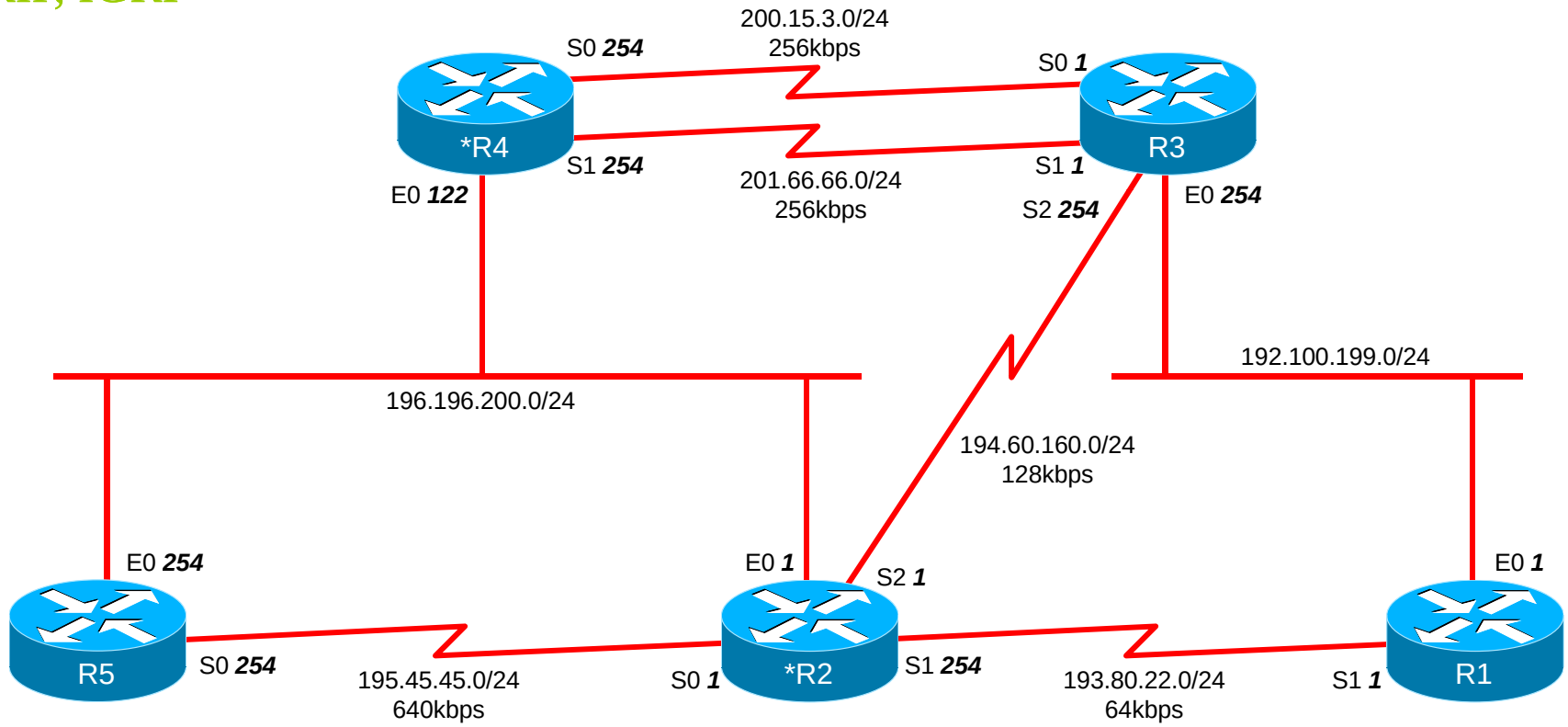
Sin Sumarización



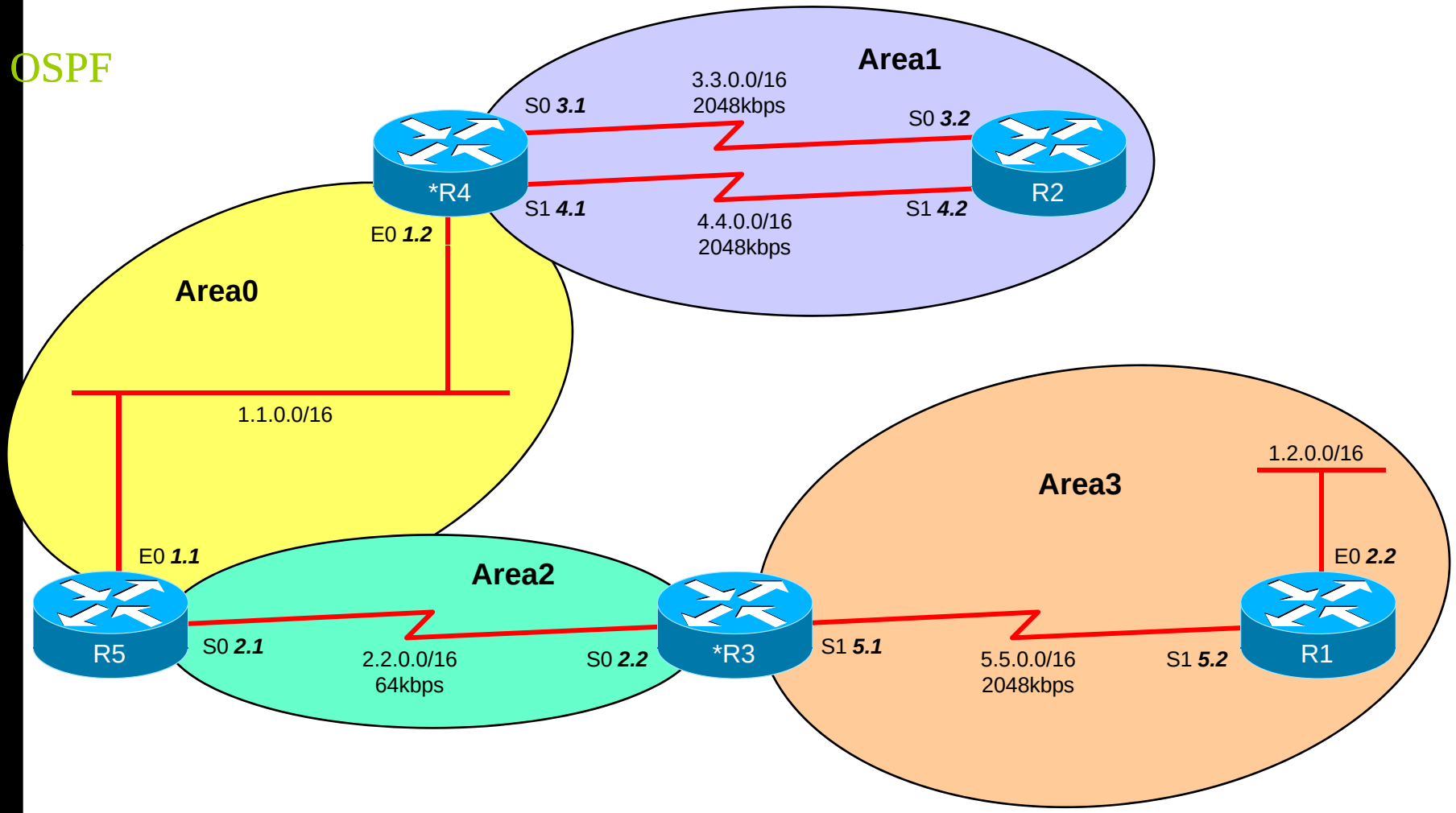
Con Sumarización



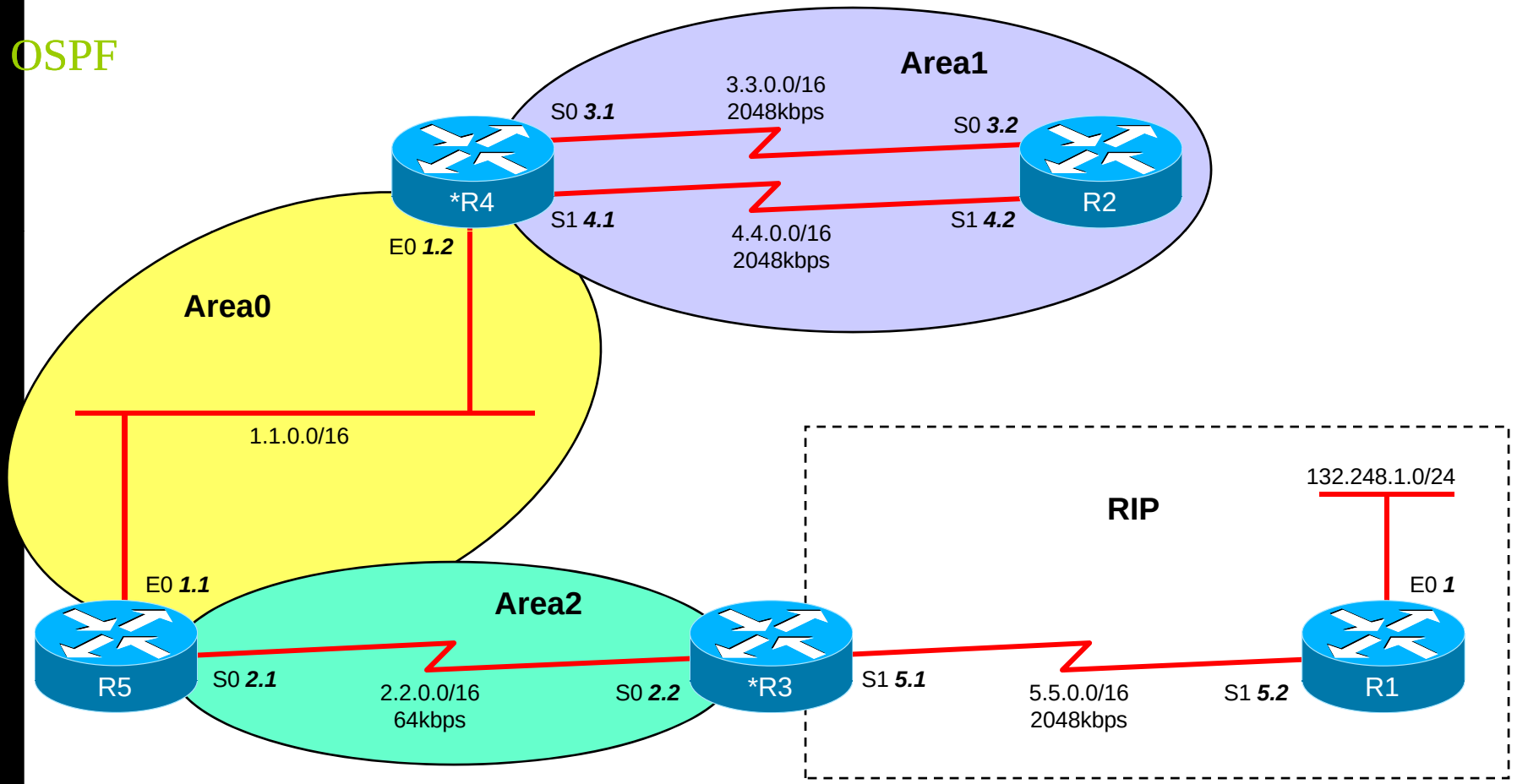
RIP, IGRP


200.15.3.0/24
256kbps
S0 254
S0 1
*R4
R3
S1 254
S1 1
201.66.66.0/24
256kbps
E0 122
S2 254
E0 254
192.100.199.0/24
196.196.200.0/24
194.60.160.0/24
128kbps
E0 254
E0 1
S2 1
E0 1
R5
S0 254
195.45.45.0/24
640kbps
S0 1
*R2
S1 254
193.80.22.0/24
64kbps
S1 1
R1

OSPF


Area1
3.3.0.0/16
2048kbps
S0 3.1
S0 3.2
*R4
R2
S1 4.1
S1 4.2
4.4.0.0/16
2048kbps
E0 1.2
Area0
1.1.0.0/16
1.2.0.0/16
Area3
E0 1.1
E0 2.2
Area2
R5
S0 2.1
2.2.0.0/16
64kbps
S0 2.2
*R3
S1 5.1
5.5.0.0/16
2048kbps
S1 5.2
R1

OSPF


Area1
3.3.0.0/16
2048kbps
S0 3.1
S0 3.2
*R4
R2
S1 4.1
S1 4.2
4.4.0.0/16
2048kbps
E0 1.2
Area0
1.1.0.0/16
RIP
132.248.1.0/24
E0 1.1
Area2
E0 1
R5
S0 2.1
2.2.0.0/16
64kbps
S0 2.2
*R3
S1 5.1
5.5.0.0/16
2048kbps
S1 5.2
R1

Secure OSPF

Router Neighbor Authentication

The primary purpose of router neighbor authentication is to protect the integrity of a routing domain. In this case, authentication occurs when two neighboring routers exchange routing information. Authentication ensures that the receiving router incorporates into its tables only the route information that the trusted sending router really intended to send. It prevents a legitimate router from accepting and then employing unauthorized, malicious, or corrupted routing updates that would compromise the security or availability of a network. Such a compromise might lead to re-routing of traffic, a denial of service, or simply giving access to certain packets of data to an unauthorized person.

Secure OSPF

OSPF Authentication

Router neighbor authentication is a mechanism that, when applied correctly, can prevent many routing attacks. Each router accomplishes authentication by the possession of an authentication key. That is, routers connected to the same network segment all use a shared secret key. Each sending router then uses this key to ‘sign’ each route table update message.

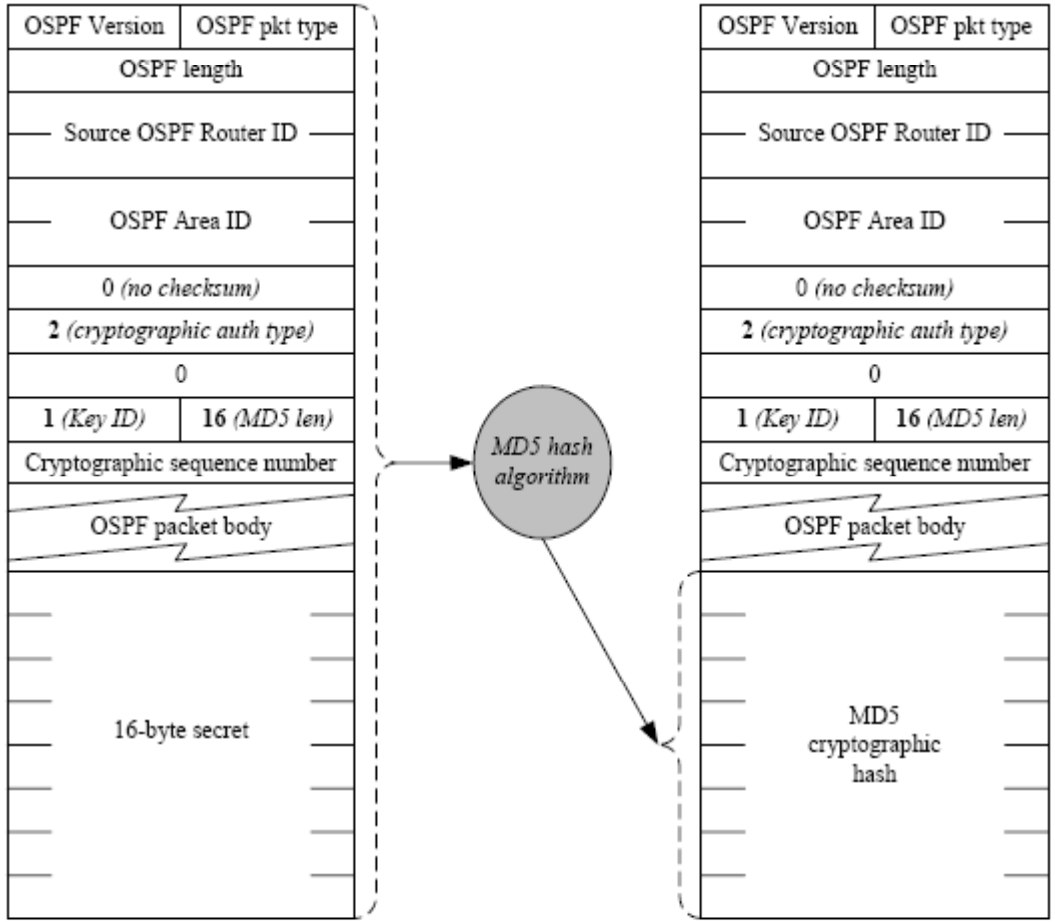
Secure OSPF

OSPF Authentication

- OSPF uses two types of neighbor authentication: plaintext and message digest (MD5)
- Plaintext is no recomended

Secure OSPF

OSPF Calculation of an MD5 Authentication



Secure OSPF

OSPF Configuring Authentication

North# **config t**

Enter configuration commands, one per line. End with CNTL/Z.

North(config)# **router ospf 1**

North(config-router)# **network 14.1.0.0 0.0.255.255 area 0**

North(config-router)# **area 0 authentication message-digest**

North(config-router)# **exit**

North(config)# **int eth0/1**

North(config-if)# **ip ospf message-digest-key 1 md5 r0utes-4-all**

North(config-if)# **end**

North#

Secure OSPF

OSPF Configuring Authentication

East# **config t**

Enter configuration commands, one per line. End with CNTL/Z.

East(config)# **router ospf 1**

East(config-router)# **area 0 authentication message-digest**

East(config-router)# **network 14.1.0.0 0.0.255.255 area 0**

East(config-router)# **network 14.2.6.0 0.0.0.255 area 0**

East(config-router)# **exit**

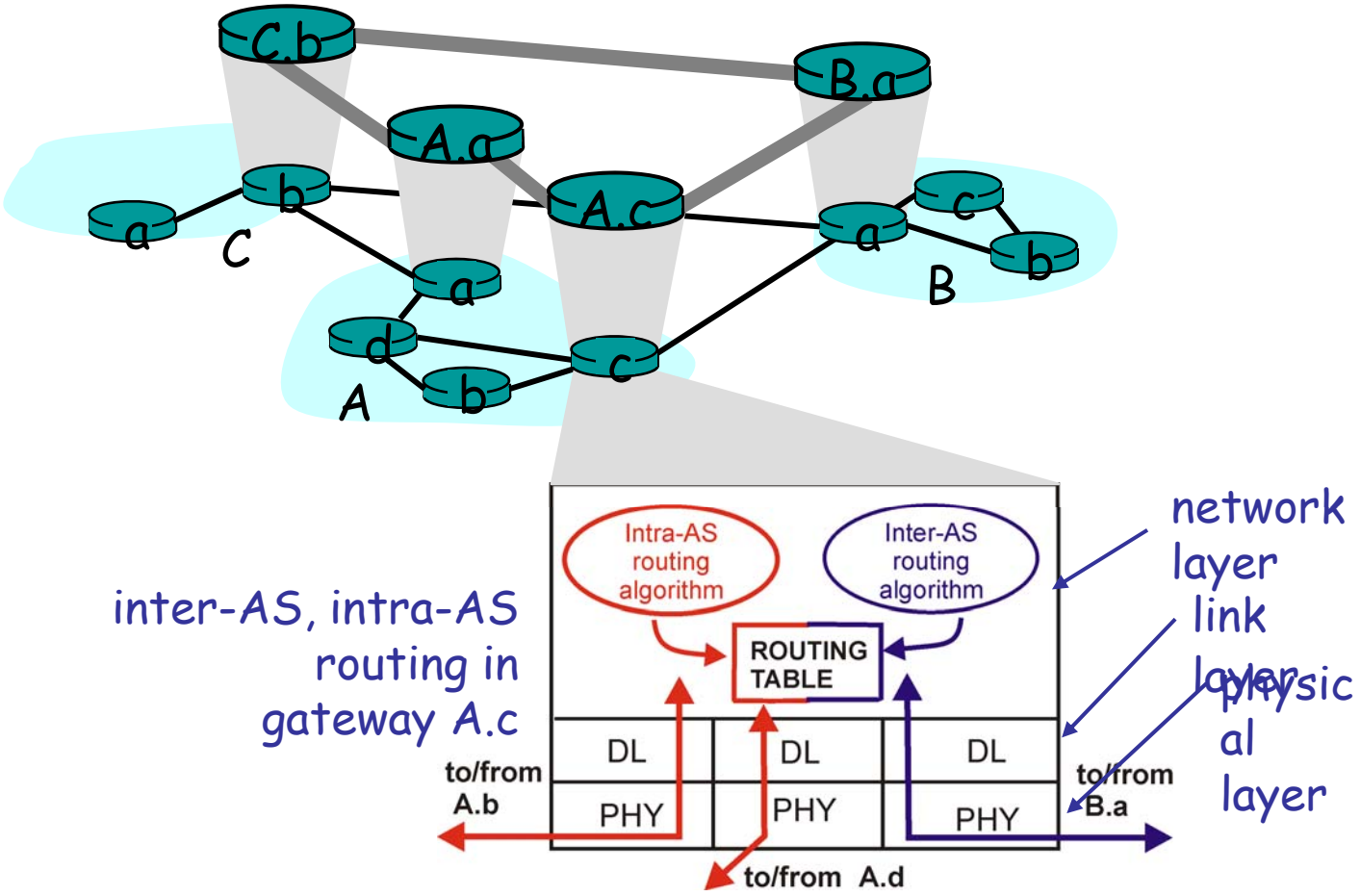
East(config)# **int eth0**

East(config-if)# **ip ospf message-digest-key 1 md5 r0utes-4-all**

East(config-if)# **end**

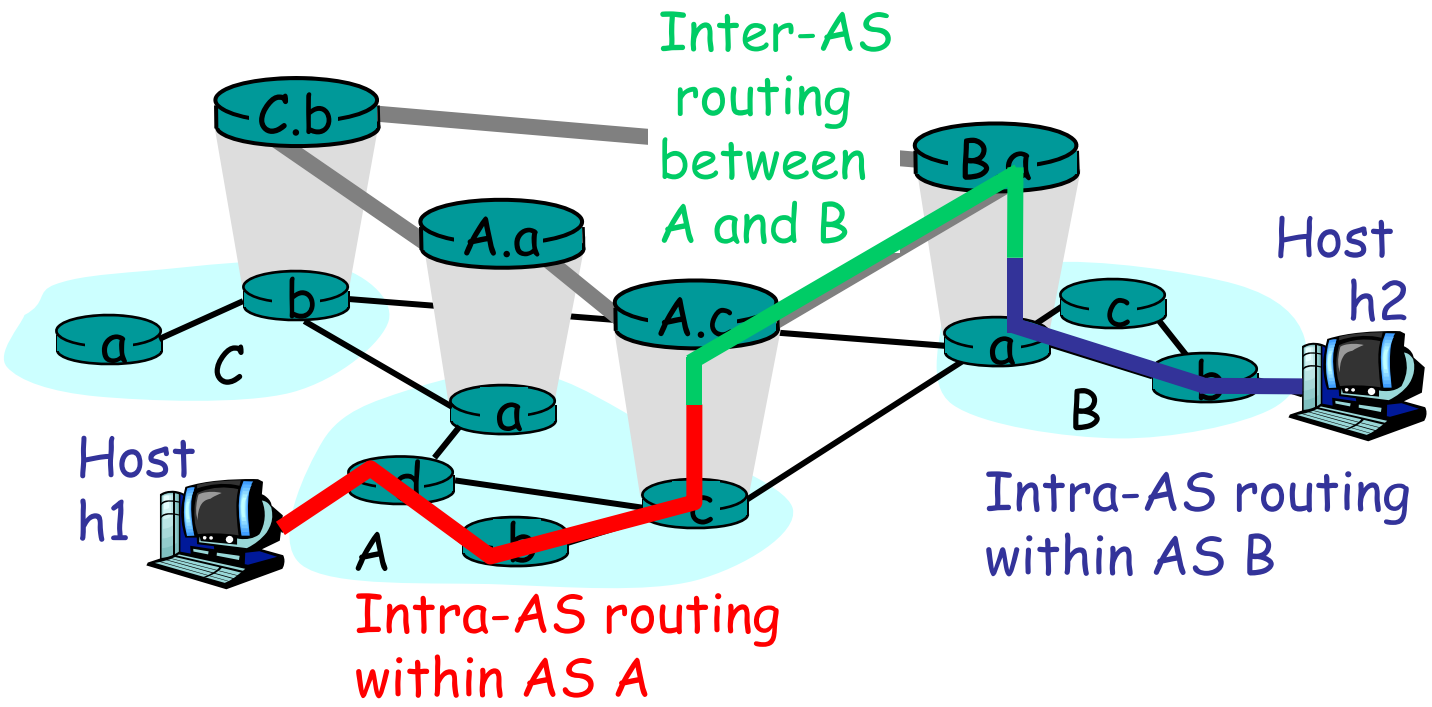
Internet Routing

- Inter-AS and Intra-AS routing



Internet Routing

- Inter-AS and Intra-AS routing



Aplicando Politicas de Ruteo

- Aplicando Politicas de Ruteo
  - Basadas de AS-PATH, Prefijos y comunidades
  - Rechazando/Aceptando rutas
  - Modificando Atributos para la selección de Rutas
- Herramientas
  - Lista de acceso ACL/Prefix-list (Prefijos)
  - Filtro de AS Filter-list
  - Route-Maps y comunidades

Filtrado de Prefijos - ACLs


```
router bgp 200
  neighbor 200.200.1.1 remote-as 210
  neighbor 200.200.1.1distribute-list 10 in
  neighbor 200.200.1.1distribute-list 11 out


access-list 10 deny 218.10.0.0    0.0.255.255
access-list 10 permit any

access-list 11 permit 215.7.0.0     0.0.255.255
```

Filtrado de Prefijos - Prefix-list


```
router bgp 200
 neighbor 220.200.1.1 remote-as 210
 neighbor 220.200.1.1 prefix-list PEER-IN in
 neighbor 220.200.1.1 prefix-list PEER-OUT out
!
ip prefix-list PEER-IN deny 218.10.0.0/16
ip prefix-list PEER-IN permit 0.0.0.0/0 le 32
ip prefix-list PEER-OUT permit 215.7.0.0/16
```

Filtrado de AS-PATHs


```
router bgp 100
 neighbor 220.200.1.1 remote-as 210
 neighbor 220.200.1.1 filter-list 5 out
 neighbor 220.200.1.1 filter-list 6 in
!
ip as-path access-list 5 permit ^200$
ip as-path access-list 6 permit ^150$
```

Expresiones Regulares

- . Cualquier carácter (pero solo uno)
- * Cualquier conjunto de Caracteres
- + Al menos uno en la siguiente cadena
- ^ Que la linea inicie con
- $ Que la linea termine con
- | Or (pipe)
- () que contenga la expreción

Similar a UNIX

Ejemplos

- .* Match con cualquier cosa
- .+ Match con al menos un carácter
- ^$ Match con las rutas de mi AS
- _1400$ Originado en este AS
- ^1400_ Recibido por el AS
- _810_ Pasa por el AS
- _810_1400_ Pasa por cualquiera de los AS
- _(1400_)+_ Match al menos una vez
- _\(65350\)_ Via 65350 (Conferederación)

Politicas de Control - Route-Map

- Un Route-Map es como un programa
- Tiene numeros de secuencia
- Cada linea es un condicion separada
  - If (condicion) then (sentencia)
    else
    If (condicion) then (sentencia)
    etc ...

Politicas de Control - Route-Map


```
router bgp 100
 neighbor 1.1.1.1 route-map infilter in
!
route-map infilter permit 10
 match ip address prefix-list HIGH-PREF
 set local-preference 120
!
route-map infilter permit 20
 match ip address prefix-list LOW-PREF
 set local-preference 80
!
route-map infilter permit 30
!
ip prefix-list HIGH-PREF permit 10.0.0.0/8
ip prefix-list LOW-PREF permit 20.0.0.0/8
```

Peer Groups ejemplo


```
router bgp 100
 neighbor ibgp-peer peer-group
 neighbor ibgp-peer remote-as 100
 neighbor ibgp-peer update-source loopback 0
 neighbor ibgp-peer send-community
 neighbor ibgp-peer route-map outfilter out
 neighbor 1.1.1.1 peer-group ibgp-peer
 neighbor 2.2.2.2 peer-group ibgp-peer
 neighbor 2.2.2.2 route-map  infilter in
 neighbor 3.3.3.3 peer-group ibgp-peer
```

BGP con Autenticación MD5

BGP peers can be protected from DoS, spoofing, and man-in-the-middle attacks by implementing RFC 2385, “Protection of BGP Sessions via the TCP MD5 Signature Option” [34]. This security mechanism operates between two BGP peers and requires the configuration of a shared key on each of these peers. The shared key is used to create and verify the MD5 signature (i.e. one-way hash) for each segment transmitted and received during the BGP session respectively. The shared key takes the form of a password configured on each peer router.

BGP con Autenticación MD5

North (config)# **router bgp 26625**
North(config-router)# **neighbor 14.2.0.250 remote-as 27701**
North(config-router)# **neighbor 14.2.0.250 password r0utes4All**
North(config-router)# **end**
North#

BGP vs IGPs

- Internal Routing Protocols
  - Ejemplos OSPF, RIP, etc..
  - Usados para transportar las direcciones de la infraestructura de la organización
  - No usados para transportar los prefijos de Internet or clientes
  - Desiñados de tal forma que se minimice el numero de prefijos

BGP vs IGPs

- BGP usar internamente (iBGP) y externamente (eBGP)
  - Intercambio de prefijos con los clientes (Afiliados)
- iBGP usado para transportar
  - Los prefijos de Internet a través del Backbone
  - Los prefijos de los clientes (Afiliados)
  - Utilizar /32 para las interfaces loopbacks de enrutamiento y levantar las sesiones de IBGPcon ellas

BGP

- Nunca hacer
  - Redistribuir BGP en un IGP
  - Redistribuir un IGP (OSPF) dentro de BGP
  - Usar IGP (OSPF) para transportar los prefijos de los clientes

BGP

- Que anuncios no debo de recibir
  - No recibir los prefijos definidos en el RFC1918
  - No aceptar tus propios prefijos
  - No aceptar el default (a menos que se requiera)
  - No aceptar prefijos mayores de /24
  - Lista de Martian-Networks (Bogus)

BGP

- Que anuncios no debo de recibir (Bogus list)

```
ip prefix-list in-filter deny 0.0.0.0/0           ! Block default
ip prefix-list in-filter deny 0.0.0.0/8 le 32
ip prefix-list in-filter deny 10.0.0.0/8 le 32
ip prefix-list in-filter deny 127.0.0.0/8 le 32
ip prefix-list in-filter deny 169.254.0.0/16 le 32
ip prefix-list in-filter deny 172.16.0.0/12 le 32
ip prefix-list in-filter deny 192.0.2.0/24 le 32
ip prefix-list in-filter deny 192.168.0.0/16 le 32
ip prefix-list in-filter deny 221.10.0.0/19 le 32 ! Block local prefix
ip prefix-list in-filter deny 224.0.0.0/3 le 32   ! Block multicast
ip prefix-list in-filter deny 0.0.0.0/0 ge 25     ! Block prefixes >/24
ip prefix-list in-filter permit 0.0.0.0/0 le 32
```

Configuracion de Politicas

- Supocición
  - Los prefix-list son usados en lugar de las ACL por ser mas faciles, rapidos.
- Las tres herramientas Basicas
  - Prefix-list (o ACL) para filtrar Prefijos
  - Filter-list para Filtrar ASNs
  - Route-map para aplicar Politicas de Ruteo

Suposiciones Basicas

- Se deben anunciar a Internet/Internet2 bloques de direcciones que previamente hallan sido asignado.
- Se pueden anunciar subprefijos, pero su alcance no esta garantizado.
- En RIR la maxima longitud es de /20 y en EU mucho ISP estan siguiendo esta politica, en Internet2 la maxima longitud es de /24

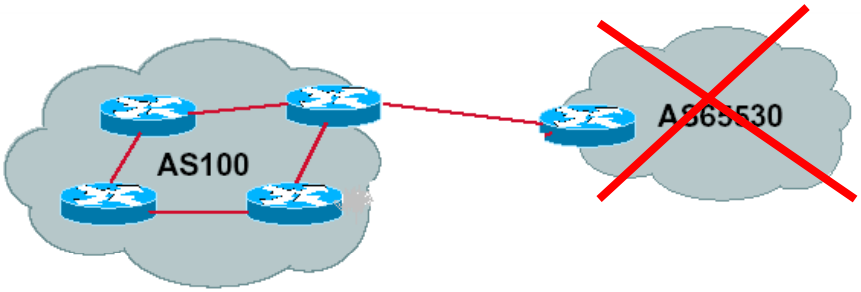
Route Flap Damping

- Esta característica fue desechada recientemente debido a que se penaliza al usuario por usar la red lo cual contradice contratos donde se garantizan la disponibilidad de la red (LSA-Level Service Agremment)

Formas de Multihoming

- Stub-homed stub Network
- Multi-home stub network
- Multi-home network

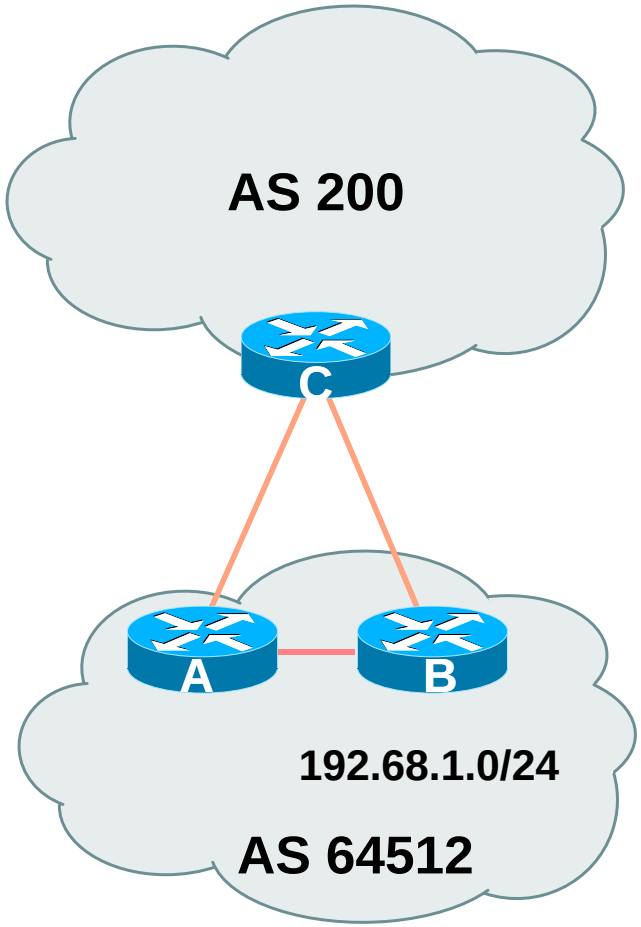
Stub Network



- No requiere de BGP
- Requiere que se genere solamente el default al Upstream ISP

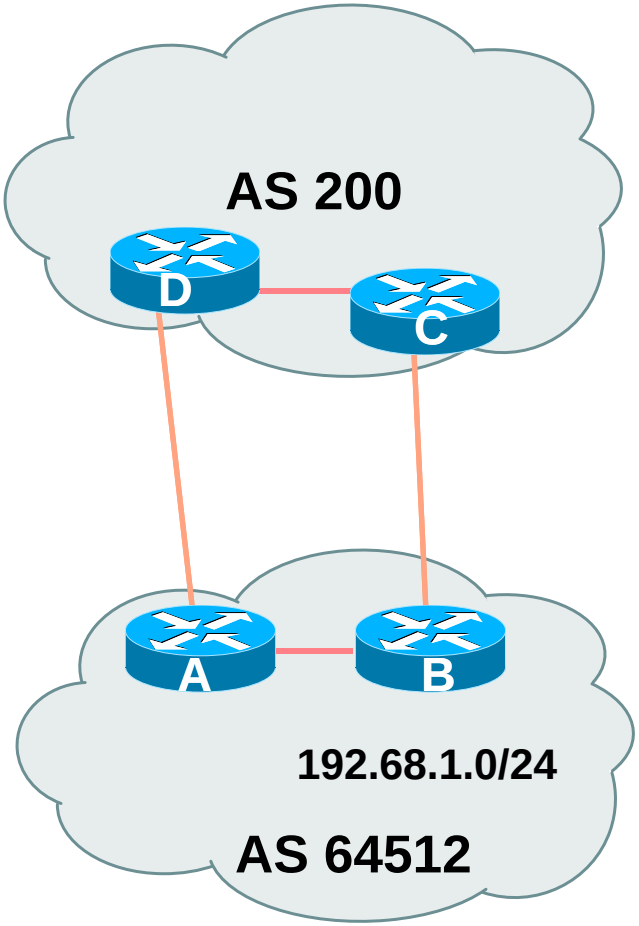
  El Upstream ISP debe anunciar la stub network
- Las politicas dependen de las politicas del Upstream ISP

Multi-homed Stub Network



- Utilizar BGP (no un IGP o estaticas) para balancear
- Utilizar un As privado (ASN >64511)
- Upstream ISP debe anunciar la stub network
- Las politicas dependen de las politicas del Upstream ISP

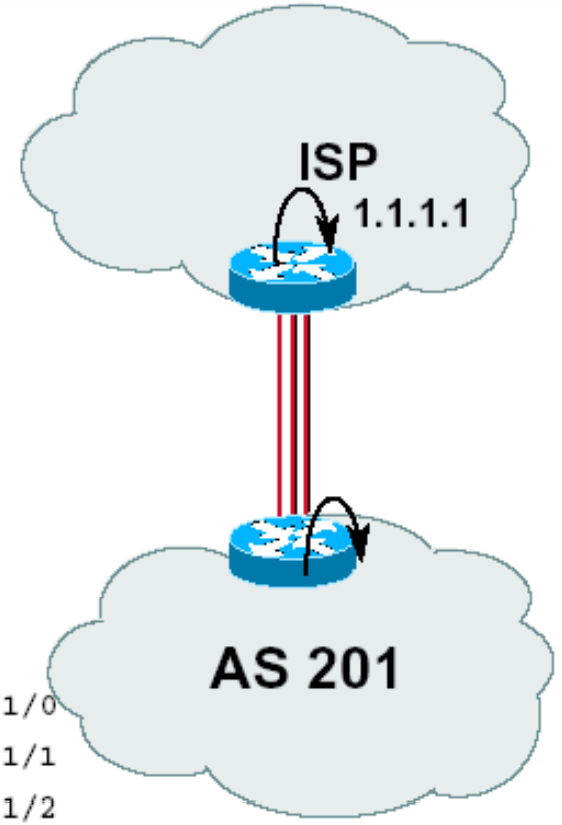
Multi-homed Network



- Muchas situaciones posibles
  - Multiples sesiones a un mismo ISP
  - Un secundario como backup solamente
  - Balanceo entre el primario y el secunario
  - Selectivamente user un ISP

Multiples Sesiones a un ISP

- ebgp Multihop
- eBGP a loopbacks
- Prefijos a prendidos a través de las loopbacks

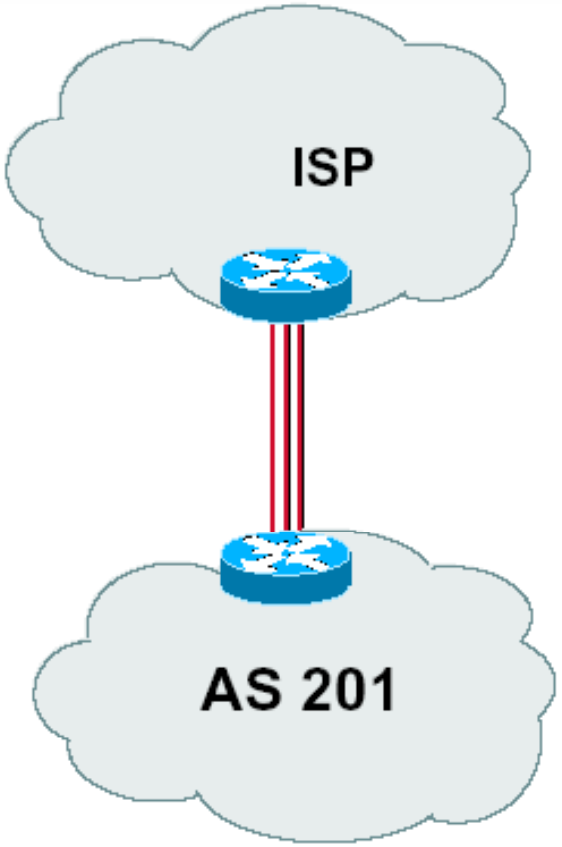



```
router bgp 201
 neighbor 1.1.1.1 remote-as 200
 neighbor 1.1.1.1 ebgp-multihop 5
ip route 1.1.1.1 255.255.255.255 serial 1/0
ip route 1.1.1.1 255.255.255.255 serial 1/1
ip route 1.1.1.1 255.255.255.255 serial 1/2
```

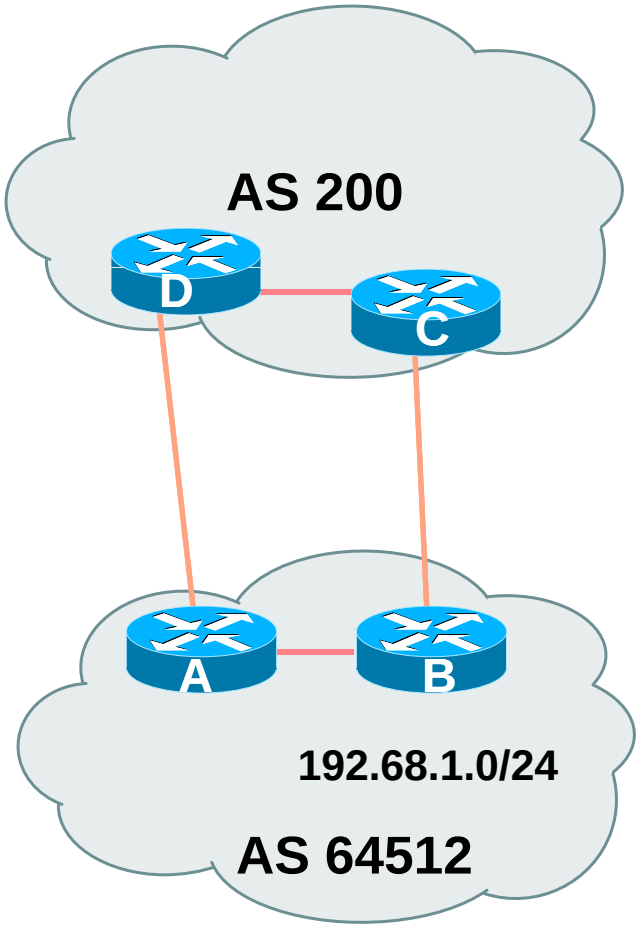
Multiple Sessiones a un ISP
BGP Multi-Path

- Tres sessions de BGP requeridas
- Limitado a 6 caminos paralelos

```
router bgp 201
 neighbor 1.1.2.1 remote-as 200
 neighbor 1.1.2.5 remote-as 200
 neighbor 1.1.2.9 remote-as 200
 maximum-paths 3
```



Multiples Sesiones a un ISP



- Usar eBGP multi-path para crear multiples paths en la tabla de ruteo
- Hacer balanceo entre los caminos

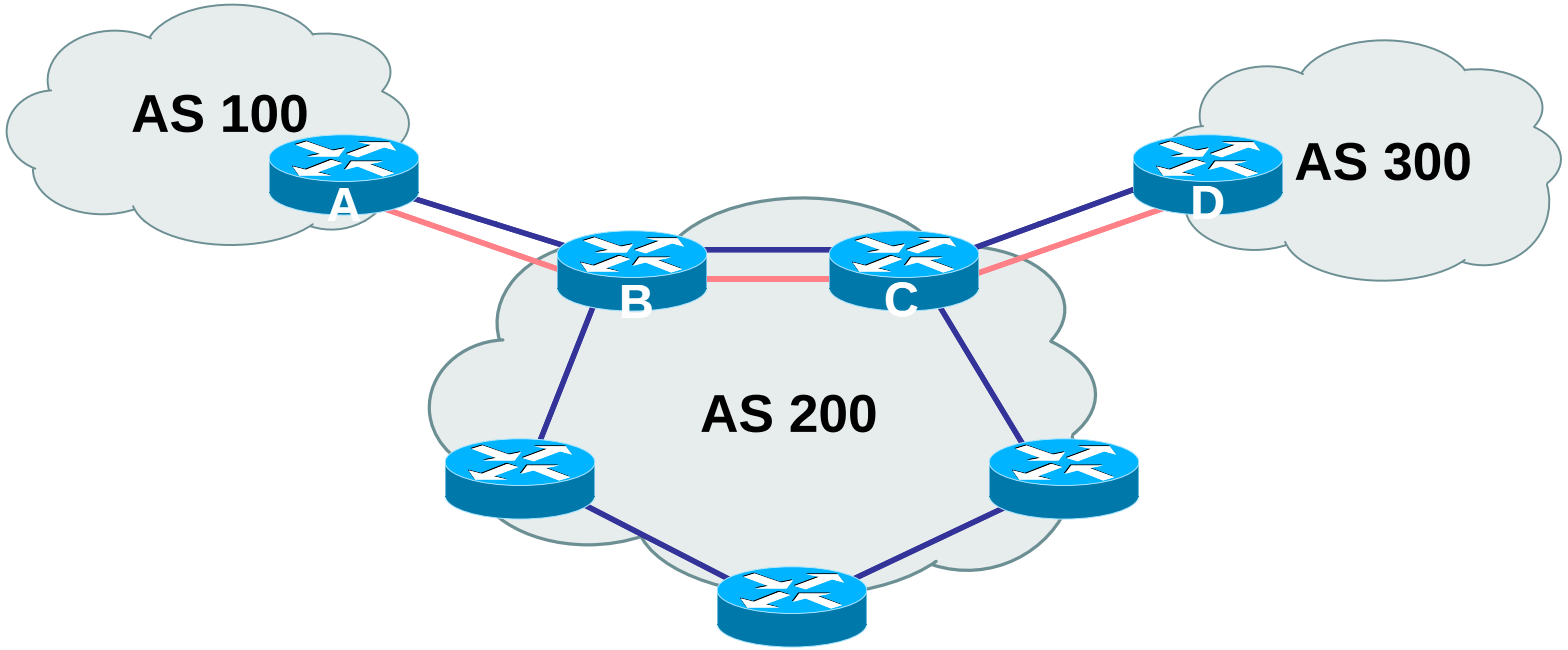
Multiples sesiones a un ISP

- Planeacion y algo de trabajo para lograr el balanceo
  - Definición del Default
  - Modificar el numero de prefijos que se aprenden en cada
- No hay una solución Magica

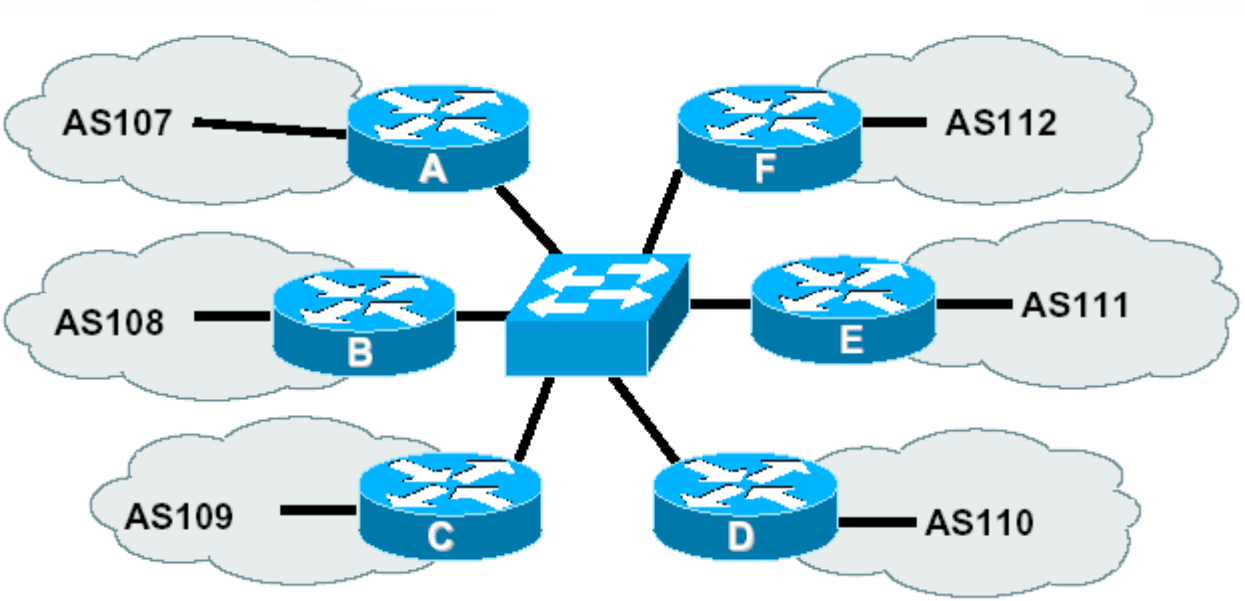
Definiciones

- Transit
  - Transporta trafico a través de su red normalmente por un pago
- Exchance Points
  - Punto en comun donde varios Ases intercambian información de routeo y trafico

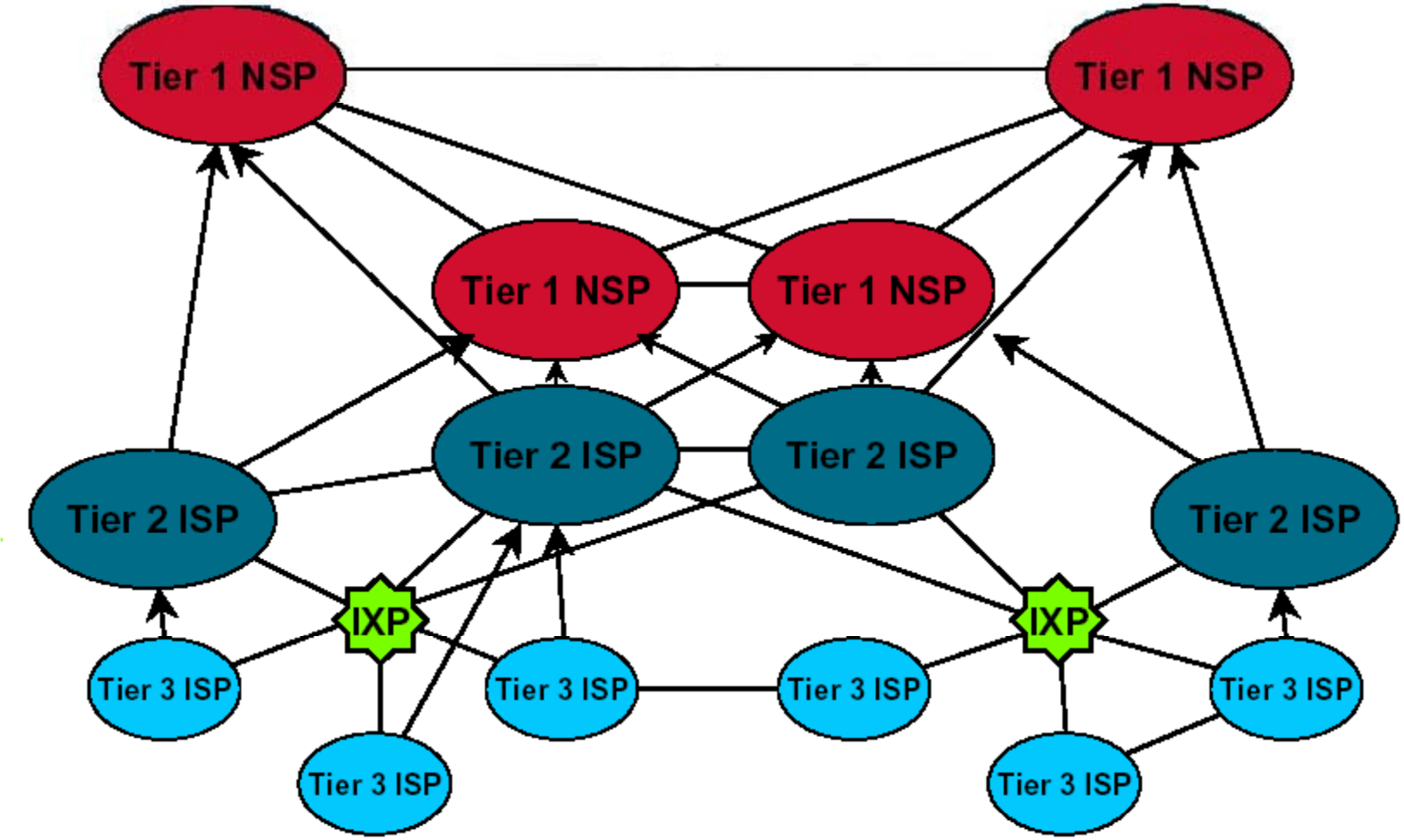
Transito



Exchange Points



Topologia de Tiers



BlackHoles

Una alternativa a las ACLs para el control de tráfico es una tecnica conocidad como BlackHole-routing o Null-Routing. Null-Routing sacrifica la granularidad de una ACL pero puede ser llevar todo el tráfico de una red o de una dirección espesifica.

BlackHoles

Configuring Null Routing

Central# **config t**

Central(config)# **interface null0**

Central(config-if)# **no ip unreachables**

Central(config-if)# **exit**

Central(config)# **ip route 10.0.0.0 255.0.0.0 null0**

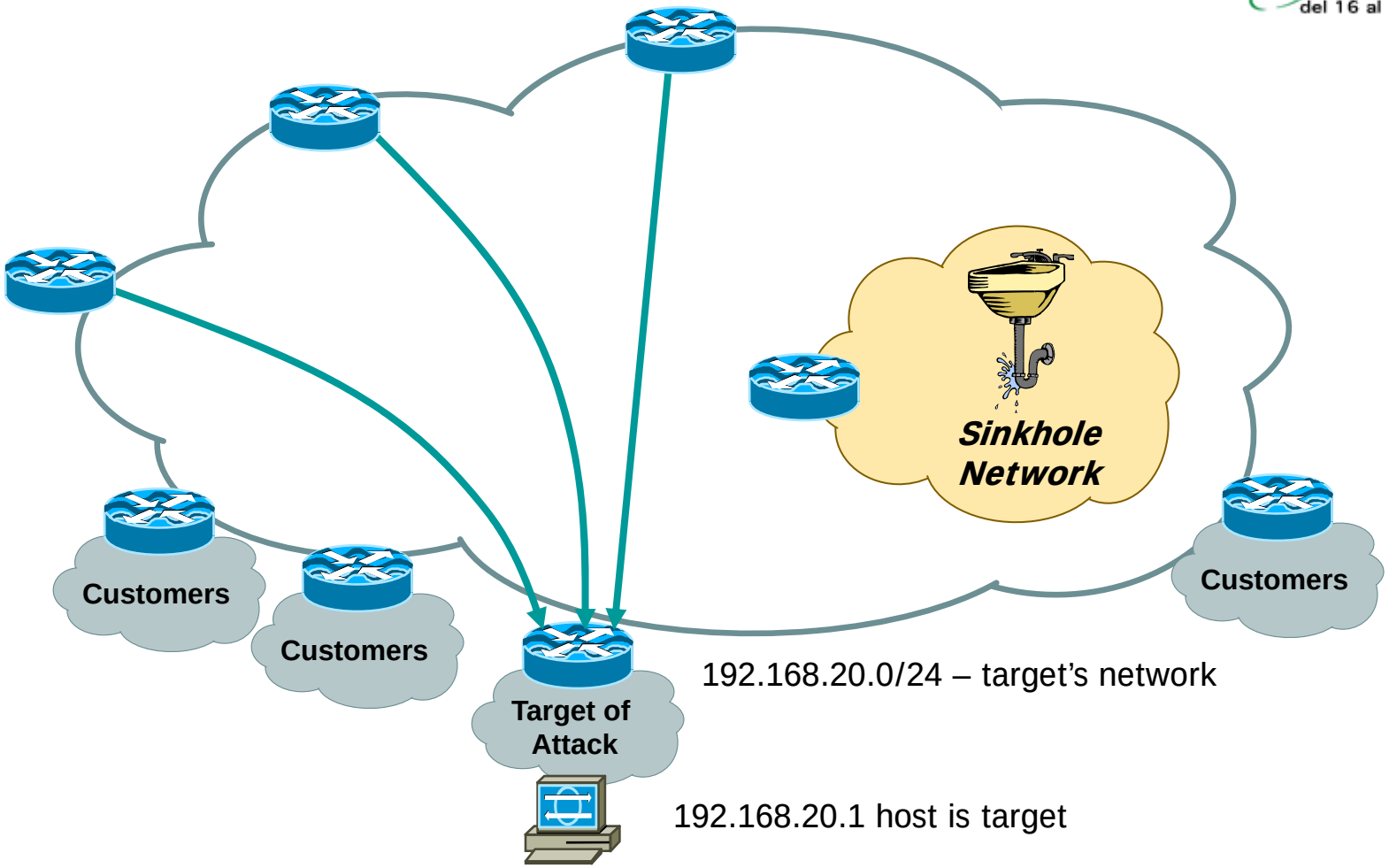
Central(config)# **exit**

Central#

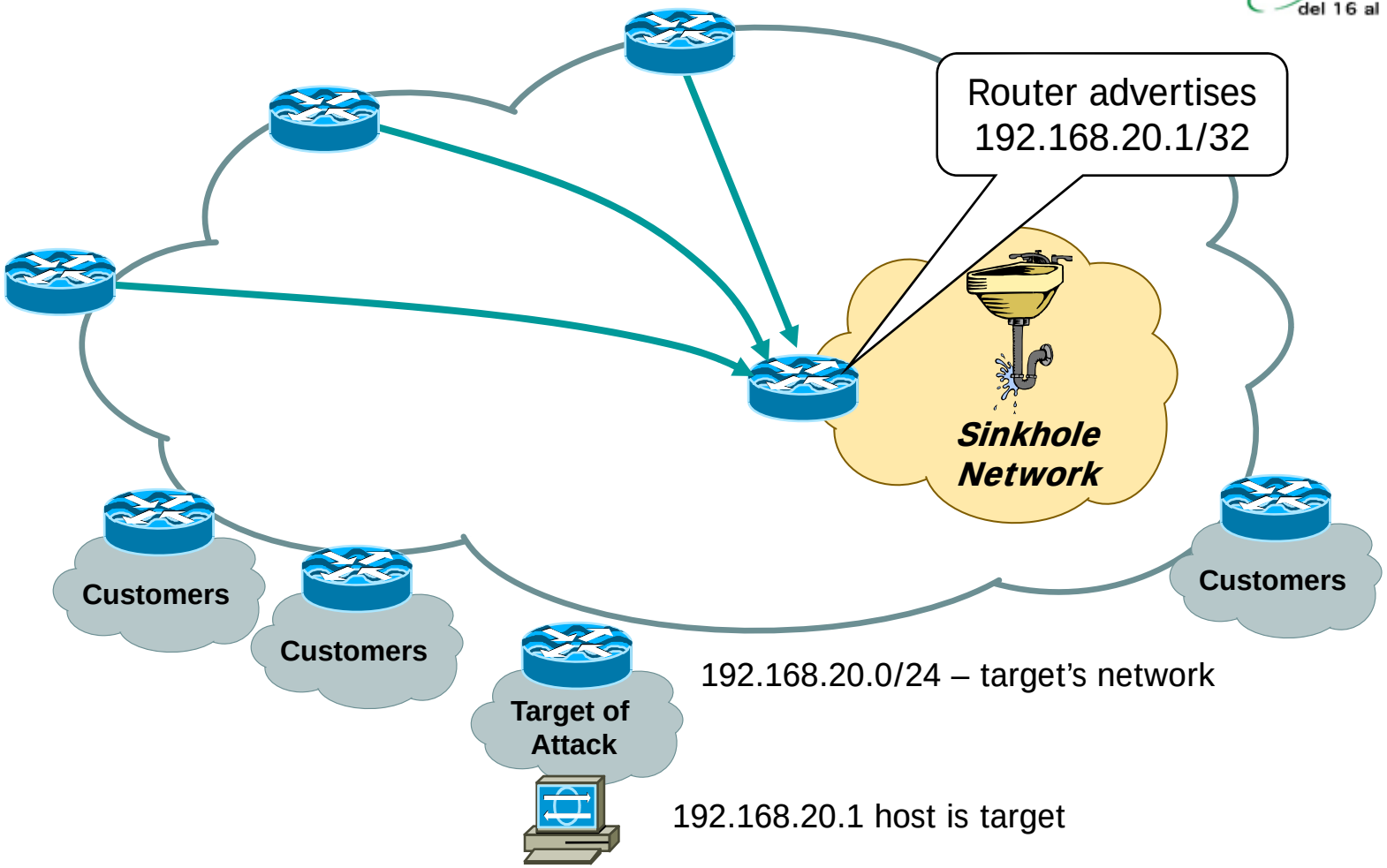
Sinkhole Routers/Networks

- Sinkholes are the network equivalent of a ***honey pot***, also commonly referred to as a ***tar pit***, sometimes referred to as a ***blackhole***.
  - Router or workstation built to *suck in* and assist in analyzing attacks.
  - Used to redirect attacks away from the customer – working the attack on a router built to withstand the attack.
  - Used to monitor *attack noise, scans, data from mis-configuration* and other activity (via the advertisement of default or unused IP space)
  - Traffic is typically diverted via BGP route advertisements and policies.

Sinkhole Routers/Networks

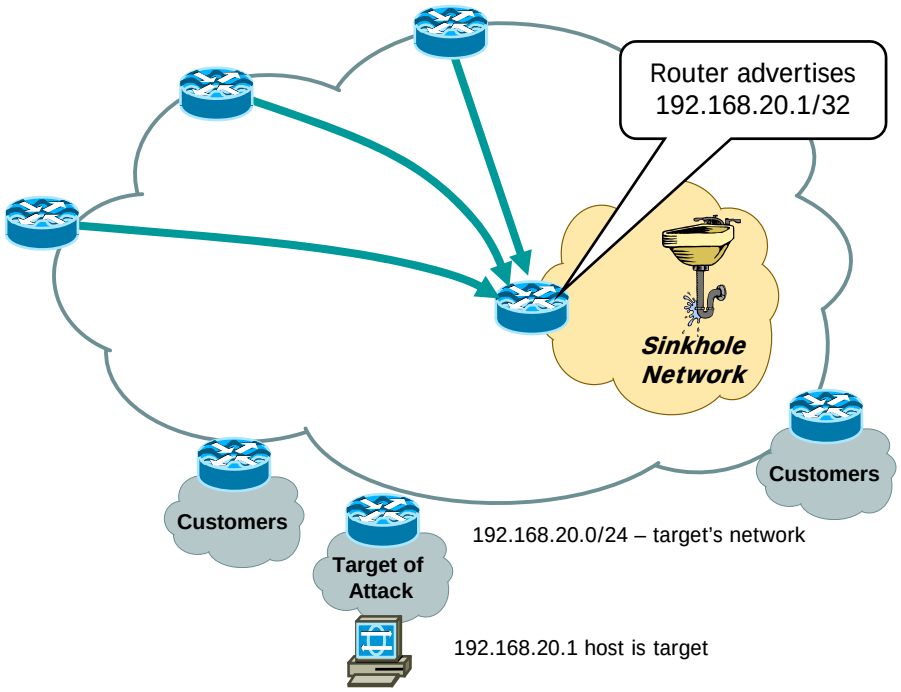


Sinkhole Routers/Networks



Sinkhole Routers/Networks

- Attack is pulled away from customer/aggregation router.
- Can now apply classification ACLs, Packet Capture, Etc…
- Objective is to minimize the risk to the network while investigating the attack incident.

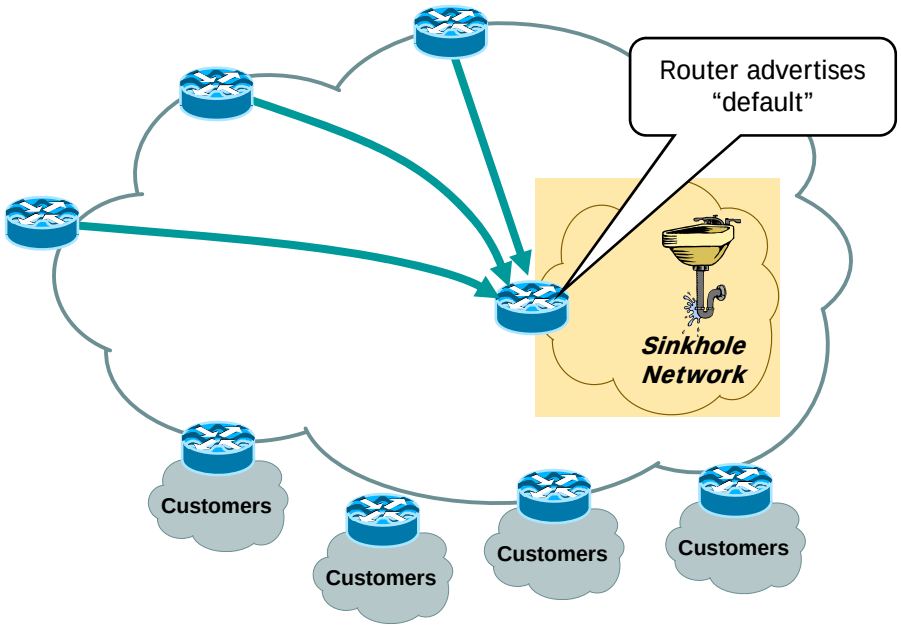


Sinkhole Routers/Networks

Advertising “default” from the Sinkhole will pull down all sorts of *garbage* traffic:

- Customer Traffic when circuits flap
- Network Scans to unallocated address space
- Code Red/NIMDA/Worms
- Backscatter

Can place tracking tools in the Sinkhole network to monitor the noise.



Scaling Sinkhole Networks

Multiple Sinkholes can be deployed within a network

Combination of IGP with BGP Trigger

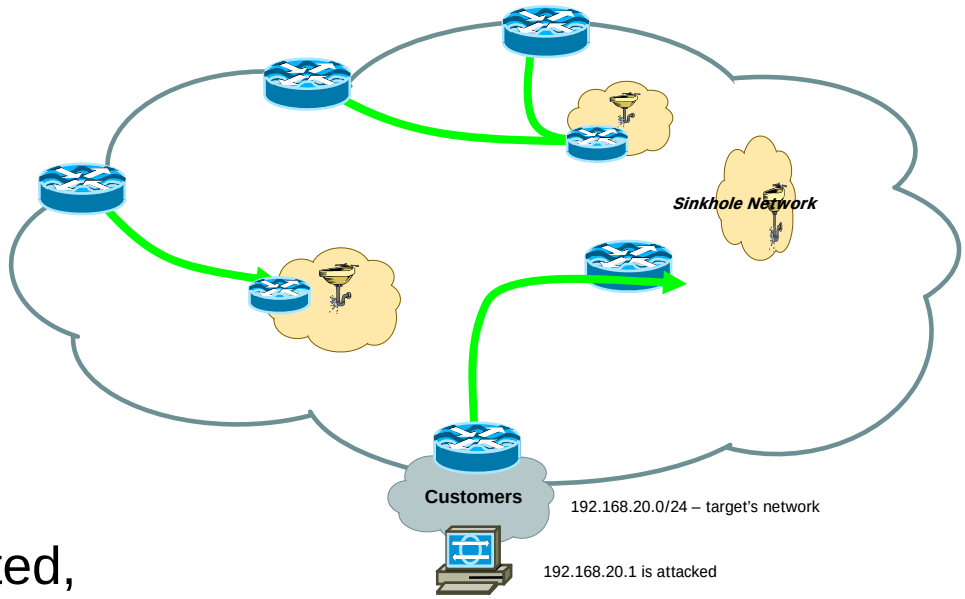
Regional deployment

- Major PoPs

Functional deployment

- Peering points
- Data Centers

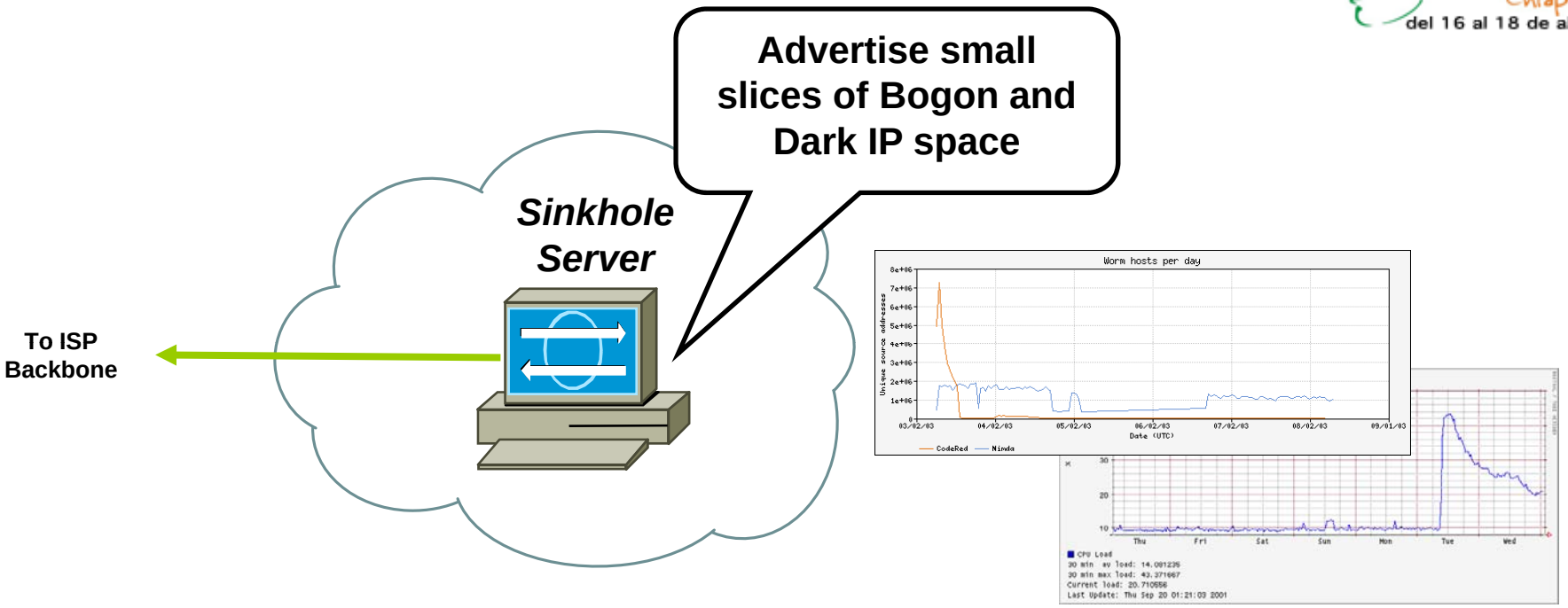
Note: Reporting more complicated, need aggregation and correlation mechanism



Why Sinkholes?

- They work! Providers and researchers use them in their network for data collection and analysis.
- More uses are being found through experience and individual innovation.
- Deploying Sinkholes correctly takes preparation.

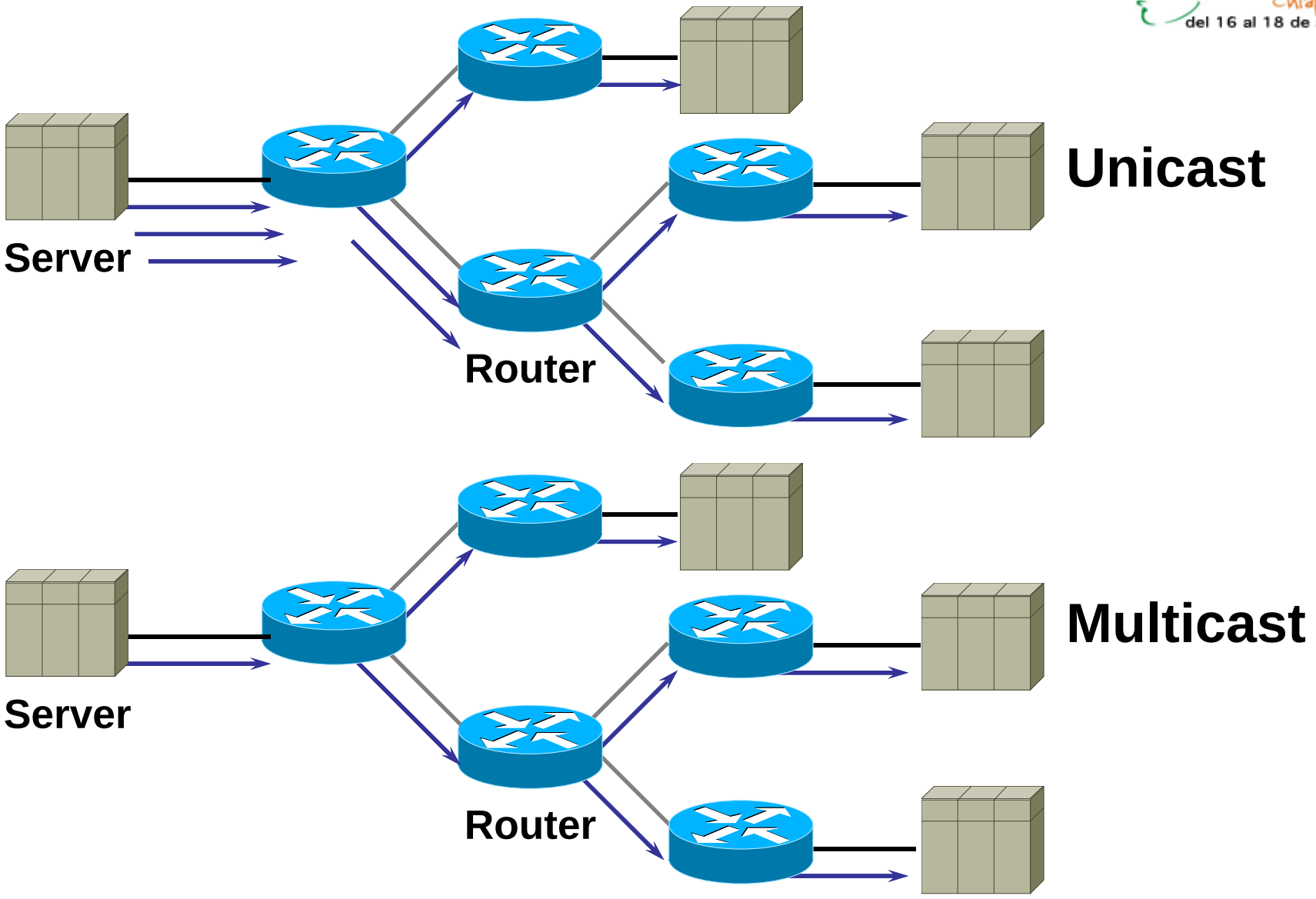
The Basic Sinkhole



- Sinks Holes do not have to be complicated.
- Some large providers started their Sinkhole with a spare workstation with free unix, Zebra, and TCPdump.
- Some GNU or MRTG graphing and you have a decent sinkhole.

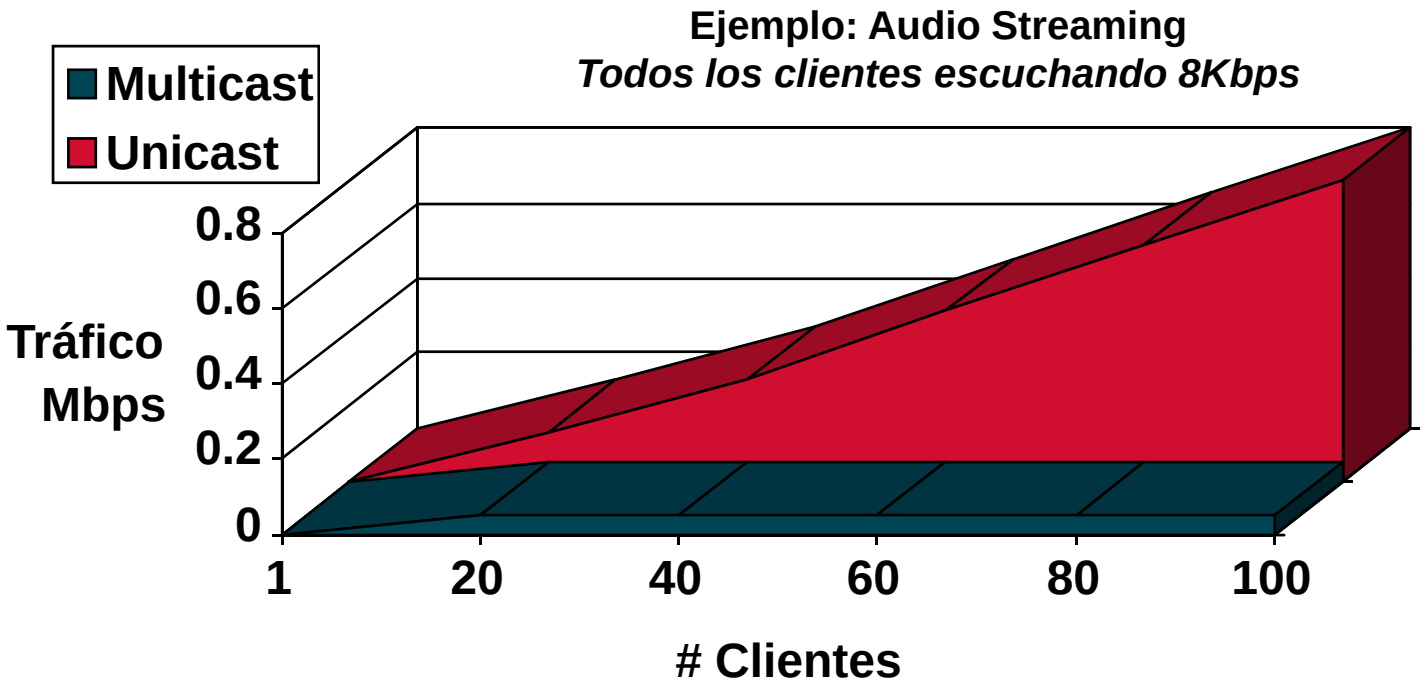
Multicast

Unicast vs. Multicast



Multicast Ventajas

- ***Mejora la Efficiencia*: Contralar el trafico de la red y reducir la carga de cpu**
  ***Optimizar el Funcionameinto* : Elimina el trafico redundante**
- ***Aplicaciones Distribuidas* : hace posible aplicaciones multipuntoes**



Multicast Desventajas

Multicast esta basado en UDP !!!

- ***Best Effort Delivery*: Dlas perdidas no son recuperadas. Las aplicaciones de multicast no son diseñadas para una entrega no confiable. Un multicast confiable esta un en desarrollo.**
- ***No Congestion Avoidance*: La falta de un TCP windowing y un "slow-start" son mecanismos que pueden resultar en una congestion de la red . De ser posible las aplicaciones Multicast deberian de detectar y evitar congestiones**
- ***Duplicates*: Algunos mecanismo de los protocolos de Multicast pueden generar el que se dupliquen paquetes (ejem. Asserts, Registers y SPT Transitions). La aplicaciones de multicas se diseñan para que acepten paquetes duplicados.**
- ***Out of Order Delivery* : Algunos mecanismo pueden ocasionar la entrega de paquetes no solicitados.**

Aplicaciones que se Benefician de IP Multicast

- Multimedia
  - Streaming media
  - Educacion a Distancia, comunicaciones corporativas
  - Conferencias—video/audio
- Data warehousing
- Aplicaciones Financieras
- Cualquier aplicación de datos de uno a muchos

Mitos de Multicast

- Es solo para Streamings de Audio y Video
- Multicast es UDP y UDP es peligroso
- Multicast no es implementado a nivel mundial

Multicast Addressing

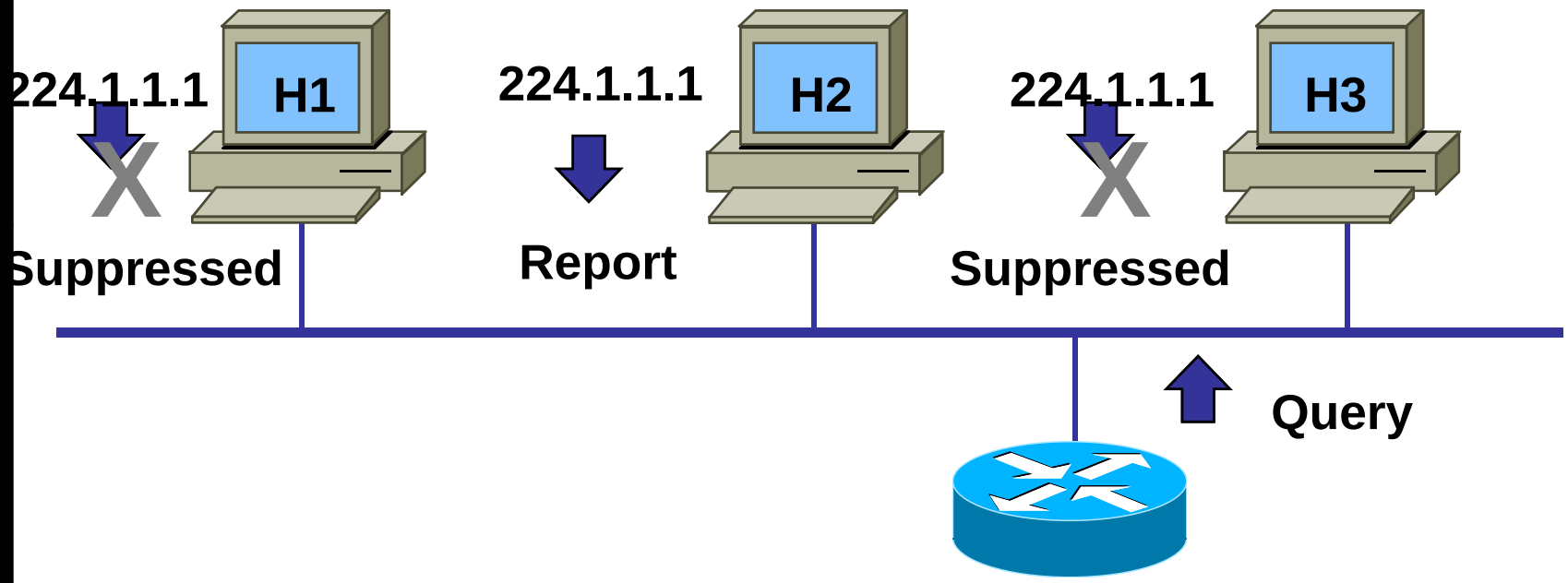
- **P Multicast Group Addresses**
  - **224.0.0.0–239.255.255.255**
  - **Class “D” espacio de direccionamiento**
    - **Los bist de mayor orden del 1er Octeto = “1110”**
- **eservados para uso local**
  - **224.0.0.0–224.0.0.255**
  - **Trasmirtir con TTL = 1**
  - **Ejemplos:**
    - **224.0.0.1** **Todos los systemas en esta subred**
    - **224.0.0.2** **Todos los routers en esta subnet**
    - **224.0.0.4** **DVMRP routers**
    - **224.0.0.5** **OSPF routers**
    - **224.0.0.13** **PIMv2 Routers**

Multicast Addressing

- Alcance Administrativo de las direcciones
  - 239.0.0.0–239.255.255.255
  - Espacio de direcciones Privado
    - Similar a RFC1918 unicast
    - No usadas para uso global en Internet
    - Uso de alcance limitado
    - Las mismas direcciones pueden ser utilizadas en diferentes localidades.
  - Eejmplos:
    - Alcance local: 239.253.0.0/16
    - Alcance Corporativo: 239.192.0.0/14

Host-Router Señalizacion: IGMP

Manteniendo un grupo



- El Router envia peticiones (Queries) periodicas en to 224.0.0.1

Multicast Forwarding

- Multicast Routing es al contrario de Unicast Routing
  - En Unicast Routing es importante a donde van los paquete (Ruteo por destino).
  - En Multicast Routing es importante de donde se originan los paquetes(Ruteo por origen).
- Multicast Routing usa “Reverse Path Forwarding”

Que necesito para tener Multicast en mi universidad

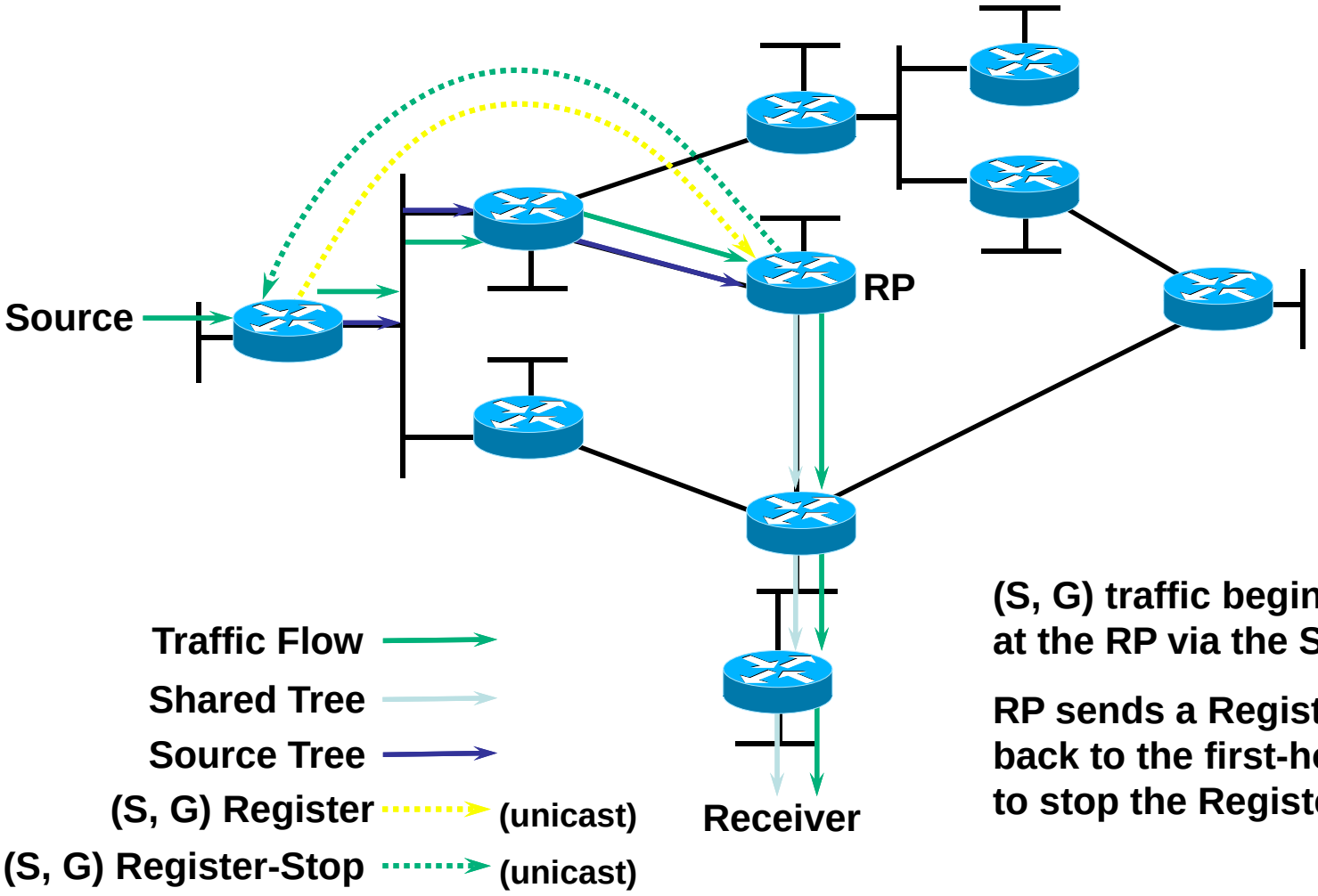
- **Tener un protocolo eficiente para el registro de los grupos(creacion de share-trees)**

  PIM-SM (forwarding)

- **Usar el modelo de unicast de ruteo**
  MBGP (routing)

- **Tener un metodo para descubrir fuentes de multicast en otros dominios**
  MSDP - Interdomain source discovery

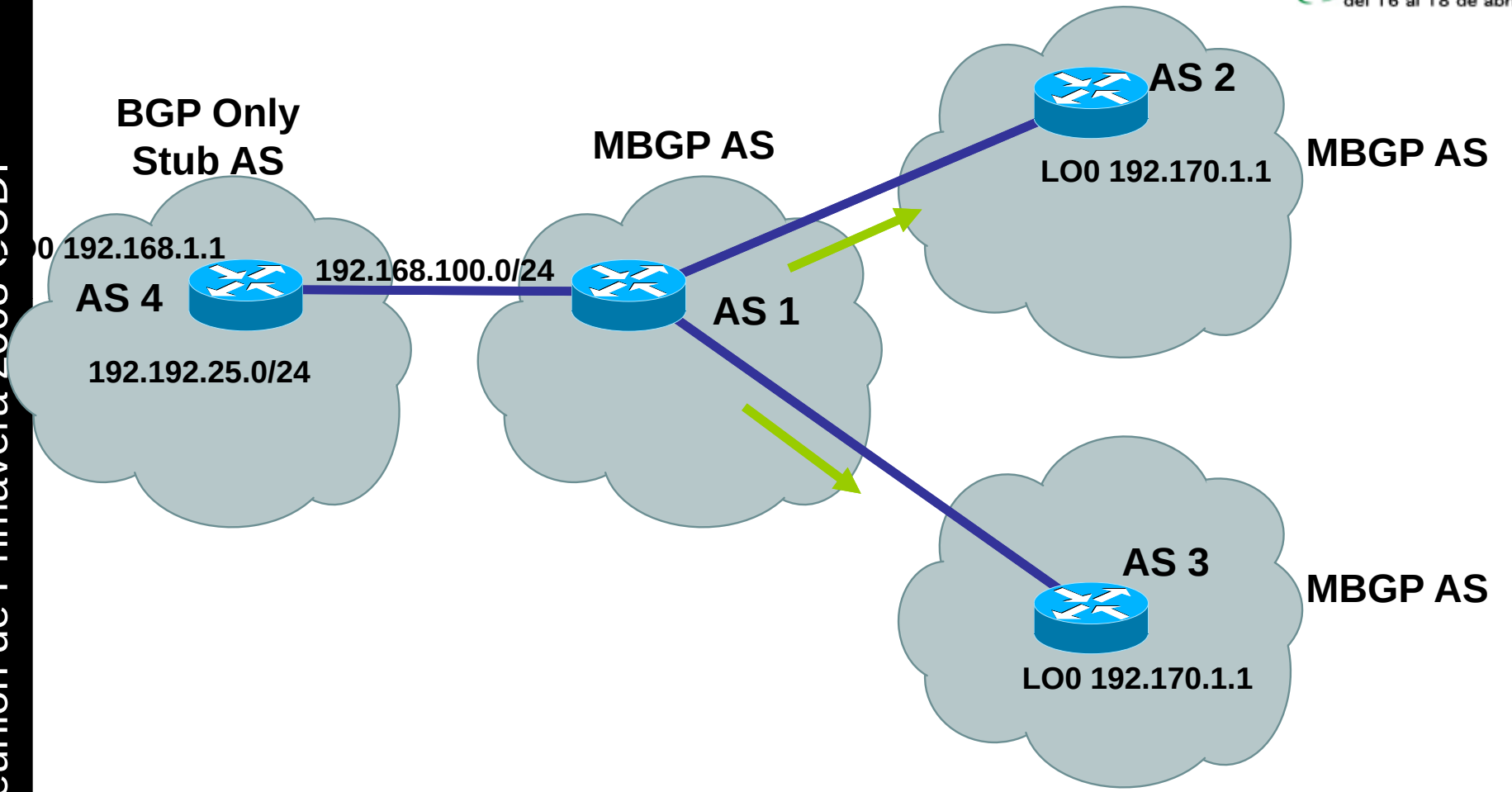
PIM-SM Sender Registration



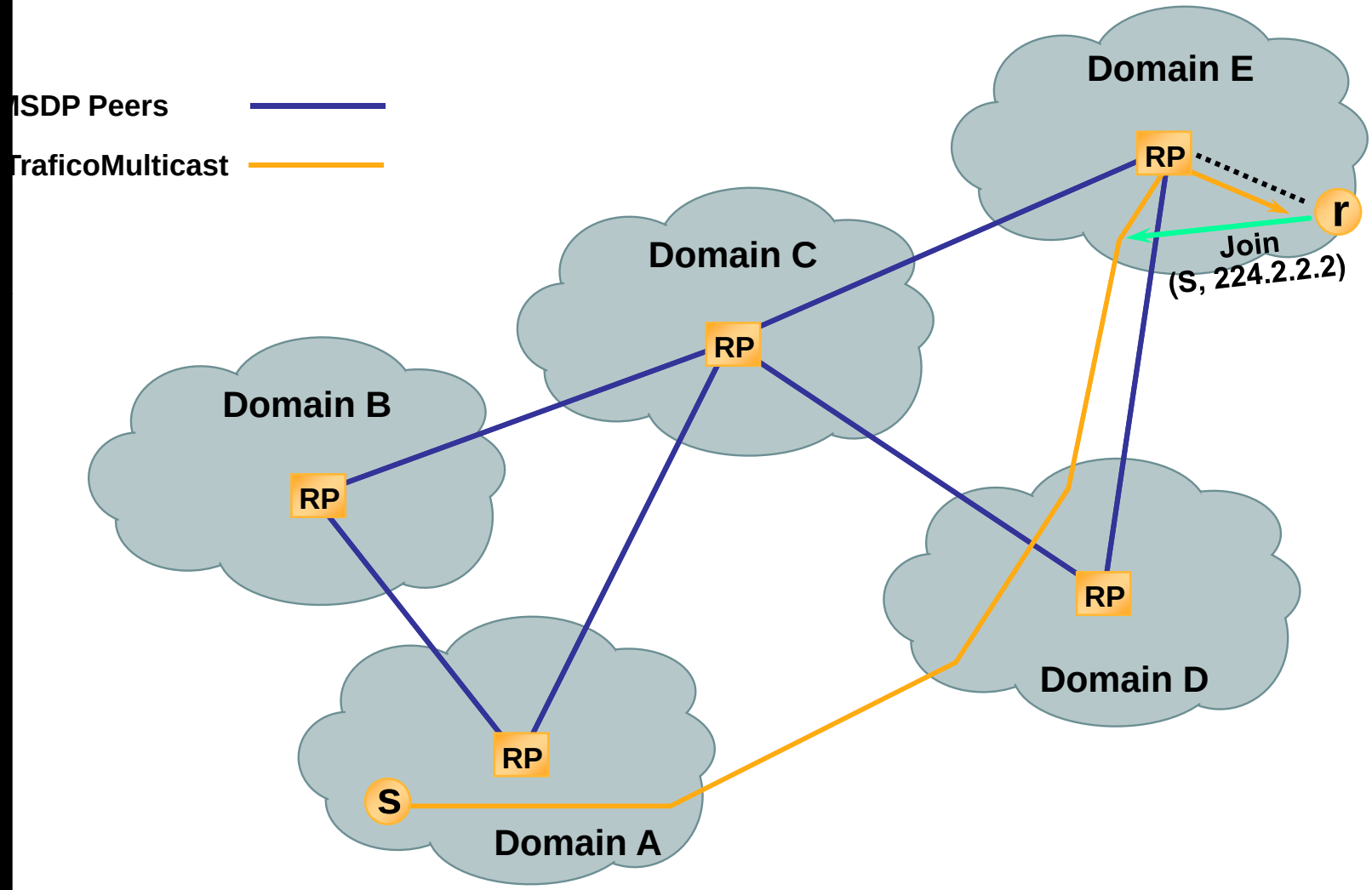
(S, G) traffic begins arriving at the RP via the Source tree.

RP sends a Register-Stop back to the first-hop router to stop the Register process.

Funcionamiento MBGP



Funcionamiento MSDP



BGP with IPv6

- BGP uses a router ID to identify BGP-speaking peers
- The BGP router ID is 32-bit value that is often represented by an IPv4 address
- By default, the Cisco IOS software sets the router ID to the IPv4 address of a loopback interface on the router
- If the process will use IPv6 only it is necessary to manually configure BGP Routing Process and BGP Router ID

BGP with IPv6

- Configuring BGP with peer group
  1. enable
  2. configure terminal
  3. router bgp ***xxxx***
  4. neighbor ***peer-group-name*** peer-group
  5. neighbor ***peer-group-name*** remote-as ***autonomous-system-number***
  6. neighbor ***peer-group-name*** update-source ***interface-type***
  7. address-family ipv6 [unicast | multicast]
  8. neighbor ***ipv6-address*** peer-group ***peer-group-name***
  9. neighbor ***peer-group-name*** activate

BGP with IPv6

- Basic prefix-list for Bogus Routes

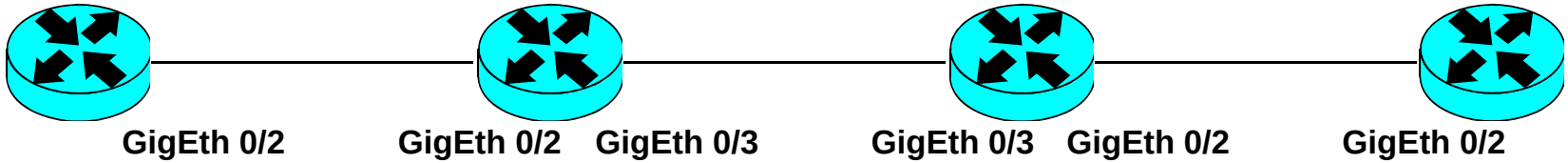
  ipv6 prefix-list IPv6-BOGUS deny 2001:db8::/32 le 128
  ipv6 prefix-list IPv6-BOGUS permit 2002::/16
  ipv6 prefix-list IPv6-BOGUS deny 2002::/16 le 128
  ipv6 prefix-list IPv6-BOGUS deny 0000::/8 le 128
  ipv6 prefix-list IPv6-BOGUS deny fe00::/9 le 128
  ipv6 prefix-list IPv6-BOGUS deny ff00::/8 le 128
  ipv6 prefix-list IPv6-BOGUS permit 0::/0 le 48
  ipv6 prefix-list IPv6-BOGUs deny 0::/0 le 128

BGP with IPv6

- Prefix-list rationale
  - 2001:db8::/32 – IPv6 documentation prefix (RFC3849)
  - 2002::/16 – only permits the /16 - no more-specifics
  - 0000::/8 – is denied (loopback, unspecified, v4-mapped)
  - FE00::/9 and FF00::/8 – multicast ranges are denied (RFC3513)
  - 0::0/0 – all the rest of the IPv6 unicat address space is permitted
  - 3FFE::/16 (6bone) has special treatment according to the 6bone rules

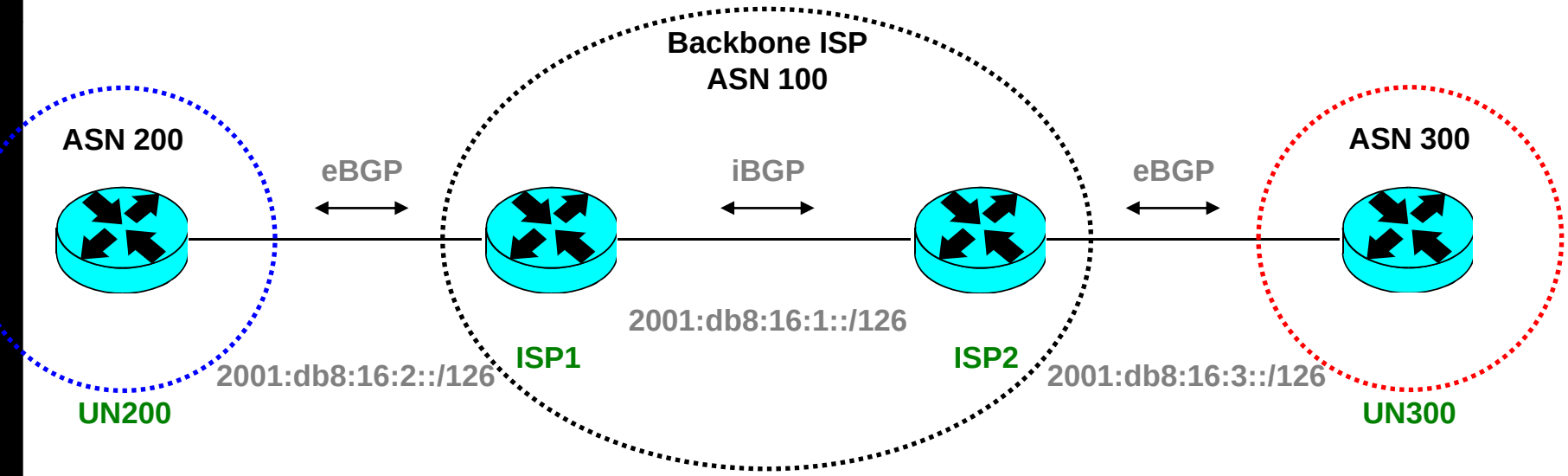
BGP configuration

- Topology for the lab – BGP with IPv6 network
  - two groups of trainees
  - same topology for the two labs

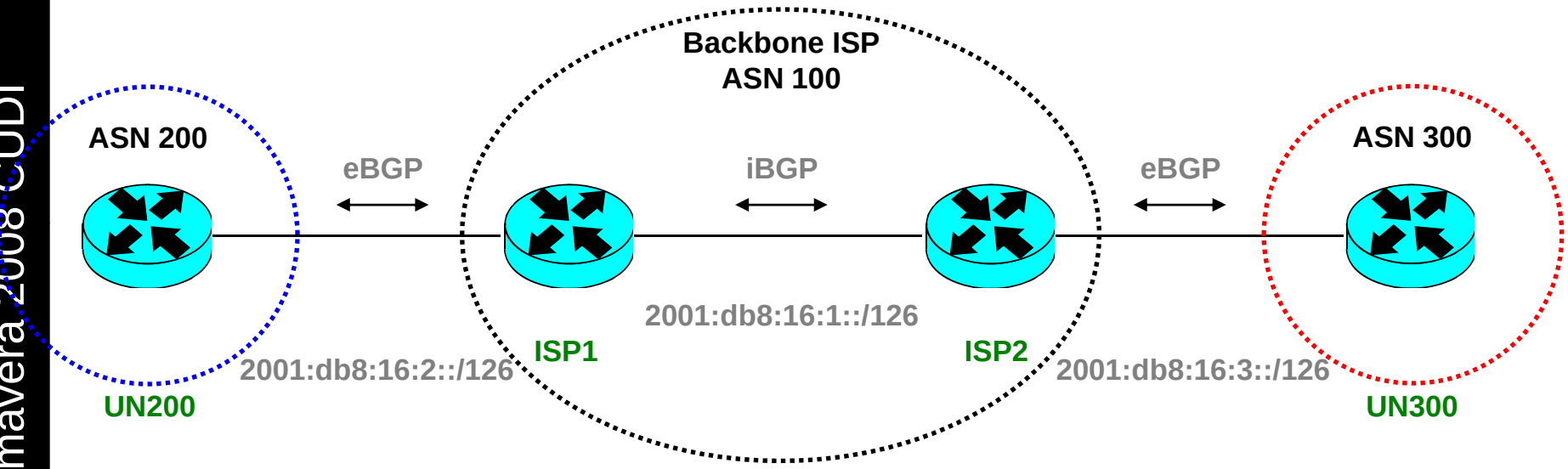


BGP configuration

- BGP topology



Loopback ISP1 – 2001:0db8:16:100::101/128
Loopback ISP2 – 2001:0db8:16:100::102/128
Loopback UN200 – 2001:0db8:17:20::1/128
Loopback UN300 – 2001:0db8:18:30::1/128



Loopback ISP1 – 2001:0db8:16:100::101/128
Loopback ISP2 – 2001:0db8:16:100::102/128
Loopback UN200 – 2001:0db8:17:20::1/128
Loopback UN300 – 2001:0db8:18:30::1/128

Configuration Template

- ISP1 – interfaces and IGP configuration using IS-IS

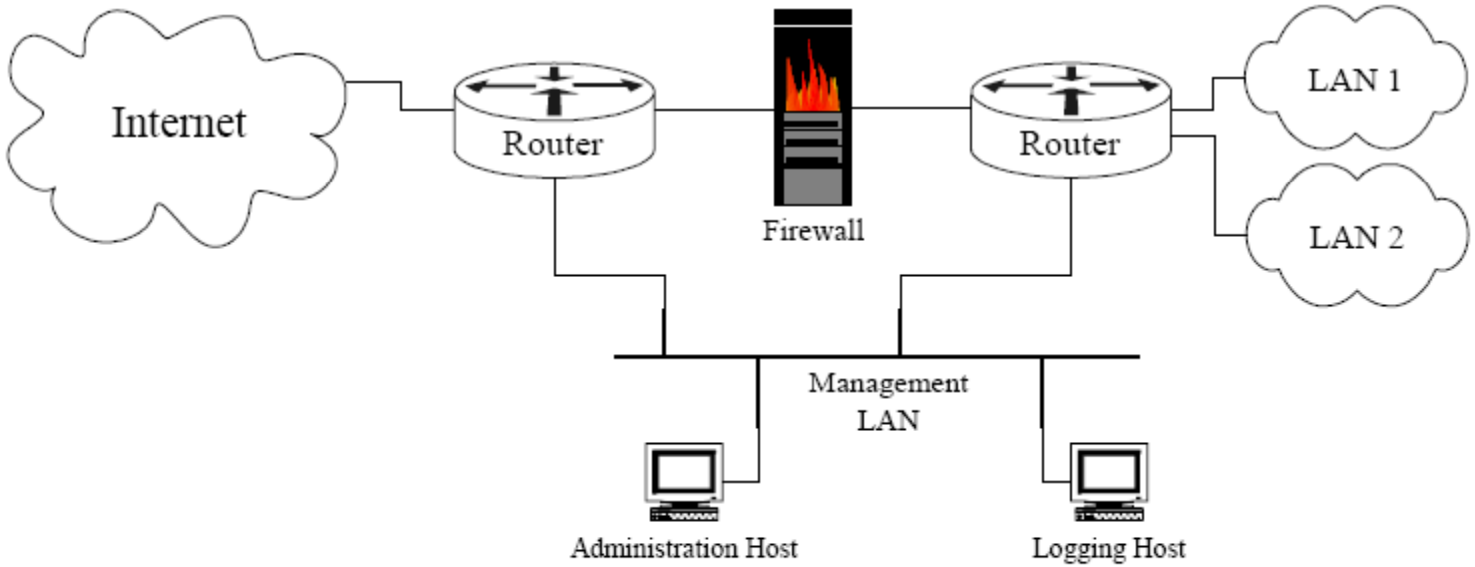
```
!
hostname isp1
!
interface loopback 0
 ipv6 addr 2001:db8:16:100::101/128
 ipv6 router isis
interface giga 0/1
 ipv6 addr 2001:db8:200::x/64
interface giga 0/2
 ipv6 addr 2001:db8:16:2::1/126
 ipv6 router isis
interface giga 0/3
 ipv6 addr 2001:db8:16:1::1/126
 ipv6 router isis
!
router isis
 net 49.0001.1720.1610.0101.00
 metric-style wide
 is-type level-2-only
 passive-interface Giga 0/0
!
```

Configuration Template

- ISP1 – interfaces and IGP configuration using OSPF

```
!
hostname isp1
!
interface loopback 0
 ipv6 addr 2001:db8:16:100::101/128
 ipv6 router ospf
interface giga 0/1
 ipv6 addr 2001:db8:200::x/64
interface giga 0/2
 ipv6 addr 2001:db8:16:2::1/126
 ipv6 router ospf
interface giga 0/3
 ipv6 addr 2001:db8:16:1::1/126
 ipv6 router ospf
!
ipv6 router ospf 200
passive-interface Giga 0/1
!
```

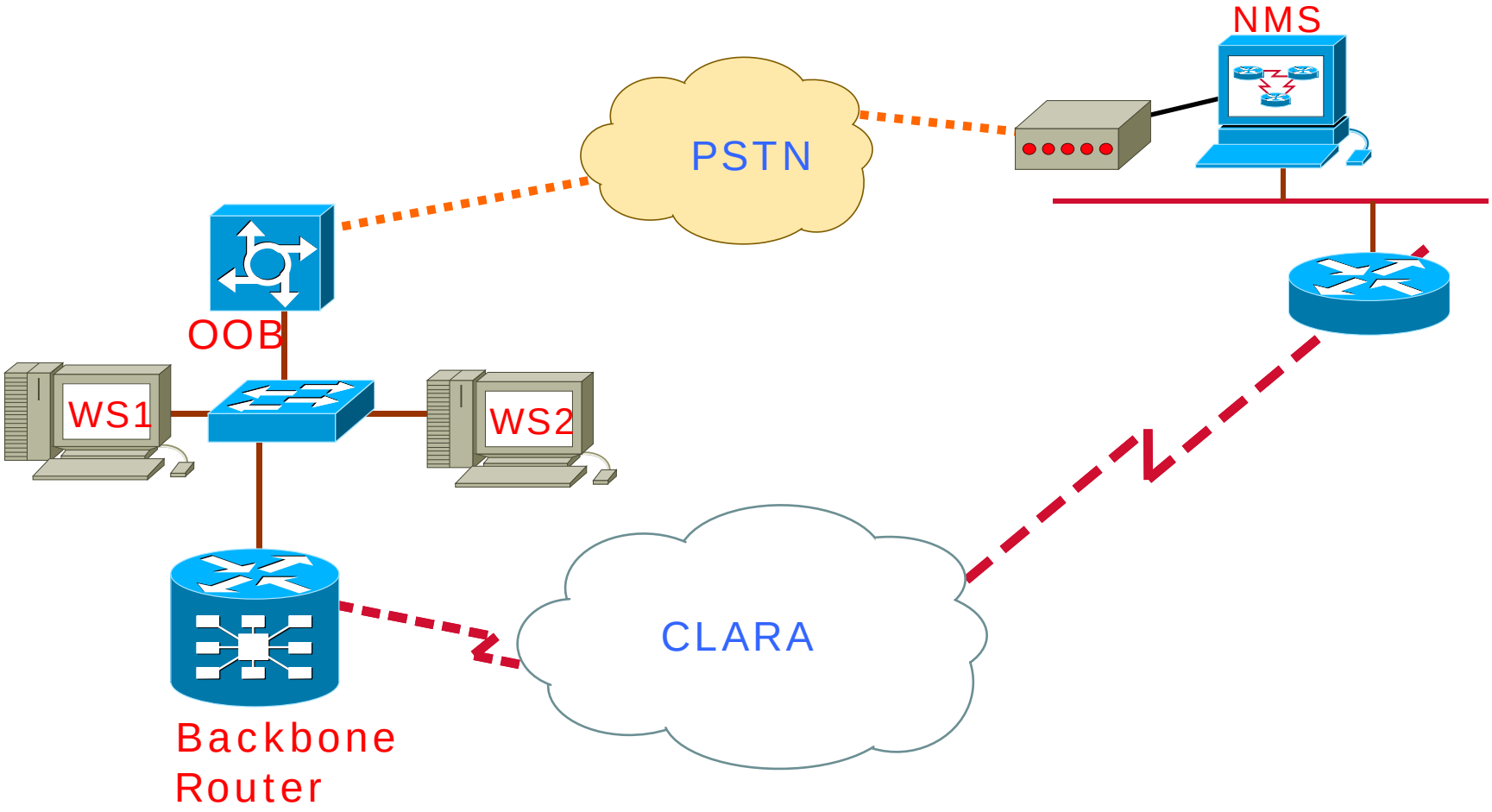
Managing the Router



1.-Establish a dedicated management network. The management network should include only identified administration hosts and a spare interface on each router.

2.-Another method is to encrypt all traffic between the administrator's computer and the router.

Conexión del NOC



Network Operation Center

Administración y Monitoreo de Redes

Definición:

Proceso de controlar una red compleja para maximizar su eficiencia y su productividad.

Se divide en 5 Áreas Funcionales:

- Administración de las Fallas.
- Administración de las Configuraciones.
- Administración de la Seguridad.
- Administración del Rendimiento.
- Administración de la Contabilidad.

Sistema de Administración de Red Plataforma

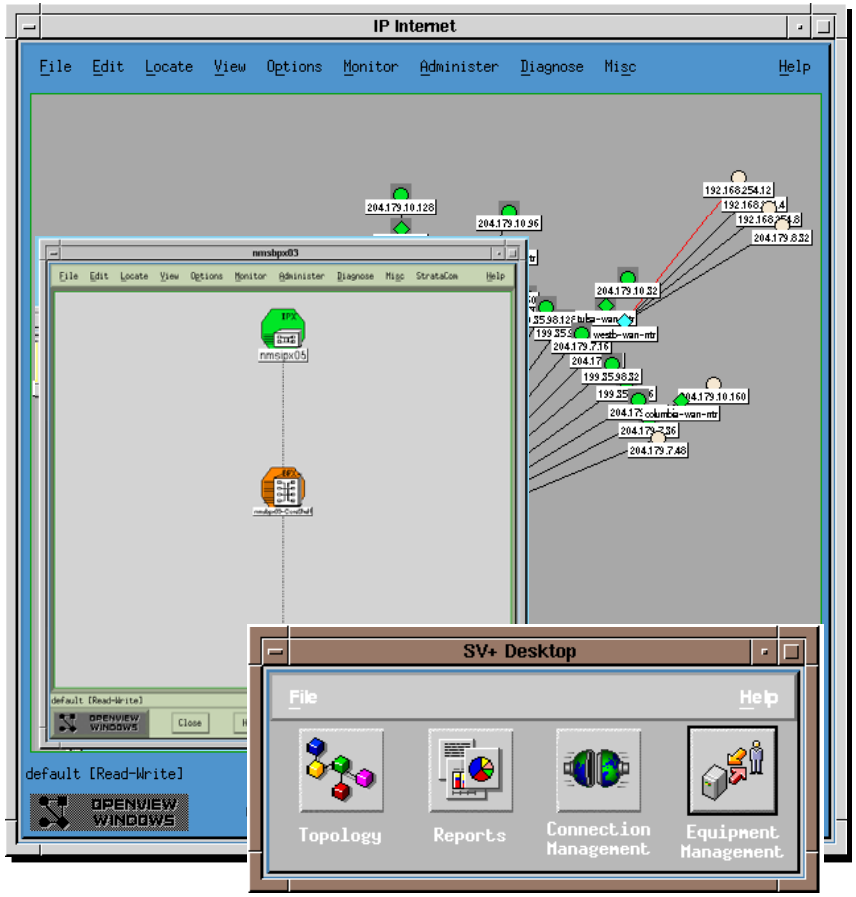
Plataforma de Administración de Red:

Software que provee la funcionalidad para administrar una gran variedad de dispositivos de red.

Funcionalidades Básicas:

- Interfaz Gráfica de Usuario.
- Mapa de la Red.
- Método Estándar para consultar a los diferentes dispositivos (MIBs).
- Sistema de Menú Personalizado.
- Sistema de Administración de Bases de Datos.
- Bitácora de Eventos.

Sistema de Administración de Red Plataforma



Sistema de Administración de Red (Cont.) Plataforma

Características:

- Herramientas para generar gráficas y reportes.
- Interfaz de Programación para Aplicaciones (API).
- Sistemas de Seguridad.

Sistema de Administración de Red Aplicaciones

Objetivo:

Administrar dispositivos o servicios específicos.

Características:

- Administración de dispositivos específicos.
- Evita sobreponerse a las funcionalidades de la plataforma.
- Se integra a la plataforma a través de sistemas de menú y APIs.
- Reside en múltiples plataformas.

Administración y Monitoreo de Redes Fallas

¿Qué es Administración de las Fallas?

Proceso de localizar los problemas o fallas en la red mediante diferentes mecanismos (poleo y/o eventos críticos) y corregirlos.

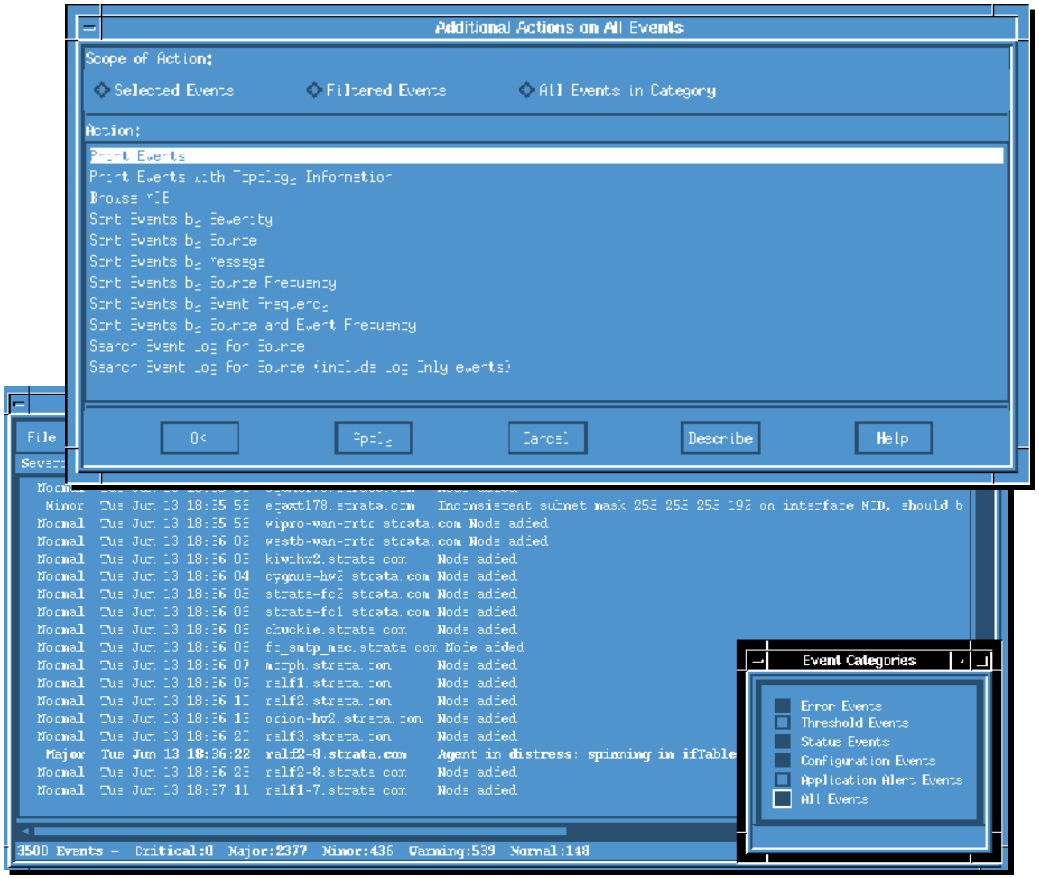
Pasos:

- Identificar el problema.
- Aislar el problema.
- Solucionar el problema.

Beneficios:

Incrementa la confiabilidad de la red dando herramientas para detectar problemas e iniciar procedimientos de recuperación más rápidamente.

Administración y Monitoreo de Redes
Fallas



Administración y Monitoreo de Redes Configuraciones

¿Qué es Administración de las Configuraciones?

Proceso de obtener datos de la red y usarlos para configurar todos los dispositivos.

Pasos:

- Obtener información del estado actual de la red (errores).
- Usar esos datos para modificar la configuración de los dispositivos de red.
- Almacenar los datos y tener un inventario de todos los dispositivos de la red.

Beneficios:

Permite el acceso rápido a la configuración de todos los dispositivos de red.

Administración y Monitoreo de Redes Seguridad

¿Qué es Administración de la Seguridad?

Proceso de proteger la información más importante ubicada en los dispositivos conectados a la red controlando los puntos de acceso.

Pasos:

- Identificar la información a proteger.
- Encontrar los puntos de acceso.
- Proteger los puntos de acceso.
- Mantener la seguridad.

Beneficios:

Evita malos manejos de información que pudieran afectar el desempeño de mi red o la integridad de ésta.

Administración y Monitoreo de Redes Rendimiento

¿Qué es Administración del Rendimiento?

Proceso de verificar el desempeño de la red (hardware, software y el medio) para garantizar que no esté congestionada y que esté accesible.

Pasos:

- Obtener información de la utilización actual de los dispositivos de la red y sus enlaces.
- Analizar la información más relevante para discernir las tendencias de utilización.
- Establecer límites de utilización.
- Simular tráfico para predecir su comportamiento y maximizar su rendimiento.

Beneficios:

Proporciona consistencia en el servicio y permite corregir problemas potenciales.

Administración y Monitoreo de Redes
Contabilidad

¿Qué es Administración de la Contabilidad?

Proceso de determinar la utilización por usuario o grupo de usuarios de los recursos de la red para proporcionarlos en forma suficiente.

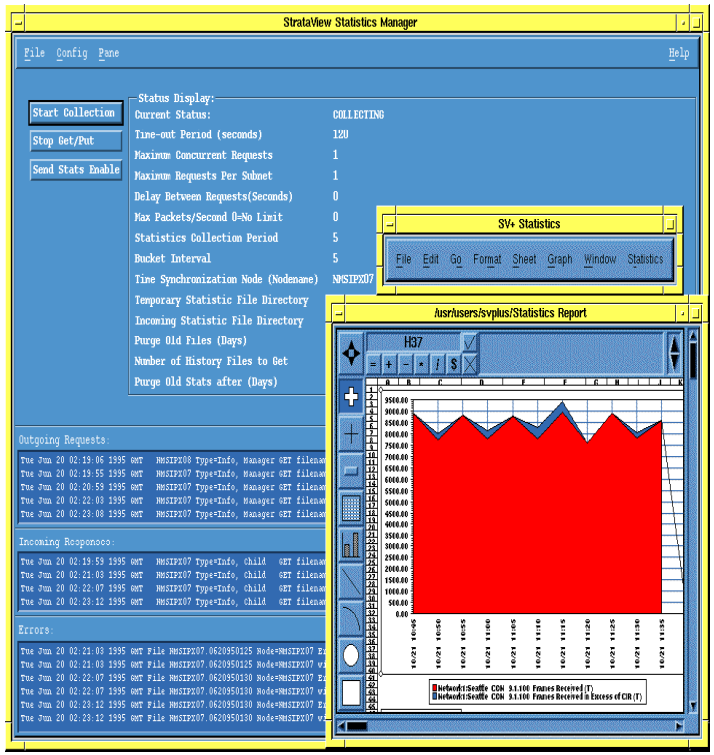
Pasos:

- Obtener información de la utilización de los recursos de la red.
- Establecer cuotas de utilización.
- Realizar el cobro por utilización de la red.

Beneficios:

Da a conocer la utilización de la red para hacerla más productiva, permite medir y reportar la utilización de los recursos por los usuarios y determinar el costo por utilización.

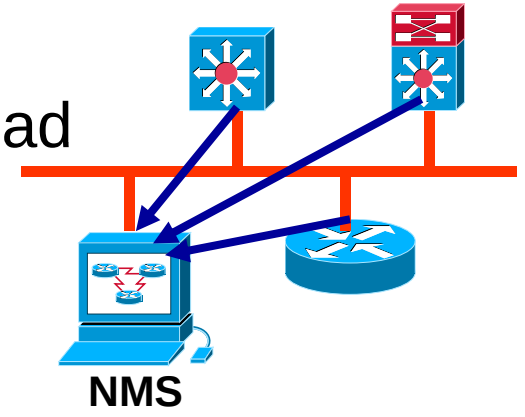
Administración y Monitoreo de Redes
Contabilidad



NMS

Centralizada

- Una plataforma instalada en una sola entidad
  - Una sola entidad recibe todas las alarmas y eventos
  - Única Base de Datos centralizada.
  - En el reciden todas las aplicaciones



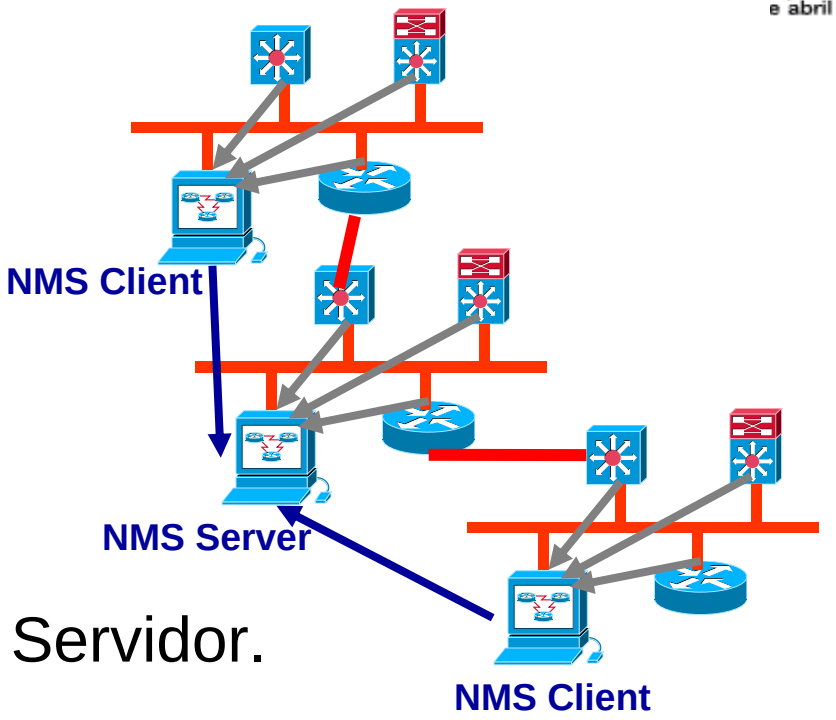
Una sola entidad para accesar todas las aplicaciones de administración

Características:

- Mayor seguridad y control
- Disponible en la mayoría de los proveedores
- Para redes pequeñas

NMS

Jerárquica



- Utiliza múltiples sistemas:
  - Servidor.
  - Clientes.
- DB con tecnología Cliente / Servidor.

Características:

- No depende de una sola entidad.
- Distribuye las tareas de administración de red.
- Distribuye el monitoreo de la red.
- Almacenamiento centralizado de la información.

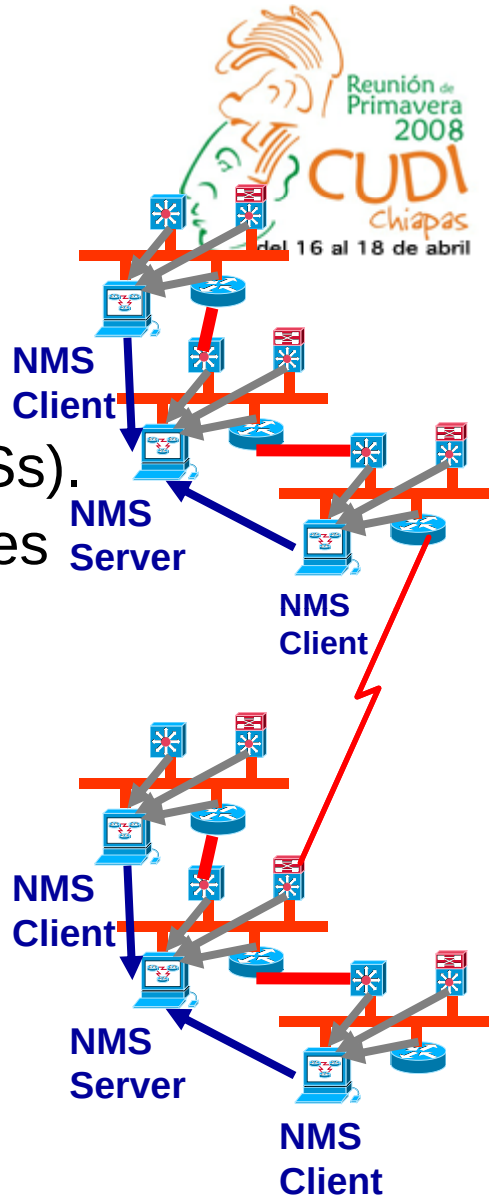
NMS

Distribuida

- Plataforma instalada en múltiples entidades (WSs).
- Múltiples Bases de Datos instaladas en diferentes entidades.

Características:

- Una sola entidad para toda la información de la red, alarmas y eventos.
- Una sola entidad para accesar todas las aplicaciones de administración.
- No depende de una sola entidad.
- Distribuye las tareas de administración de red.
- Distribuye el monitoreo de la red.



Mesa de Ayuda

- Los usuarios deben de tener una forma de contactar a los responsables de la operación de la red.
- Se debe de contar con una base de datos histórica de los eventos de la red.
- Debe tener mecanismos de retroalimentación a los usuarios

Medios de Contacto al NOC

- Se deben tener claramente definidos los medios de contacto.
- Se debe tener definidos quienes pueden contactar al NOC y la forma en que lo pueden hacer.
- Tratar en lo posible de tener un solo punto de contacto para los usuarios.
- Tener un manual de procedimiento para todos lo casos posible que se puedan presentar.
- Incluir horarios

Procedimientos de Escalación

- Se debe de contactar con un proceso de escalación.
- Este debe de tener la información para contactar a todos los involucrados.
- Debe ser conocida por los usuarios.
- Debe ser conocida por los involucrados
- Se deben de tener una clasificación de los incidentes y de preferencia definir periodos de tiempo para escalar al siguiente nivel.