

# Reunión de primavera

**Hans Ludwing Reyes Chávez**

**[hans@internet2.unam.mx](mailto:hans@internet2.unam.mx)**

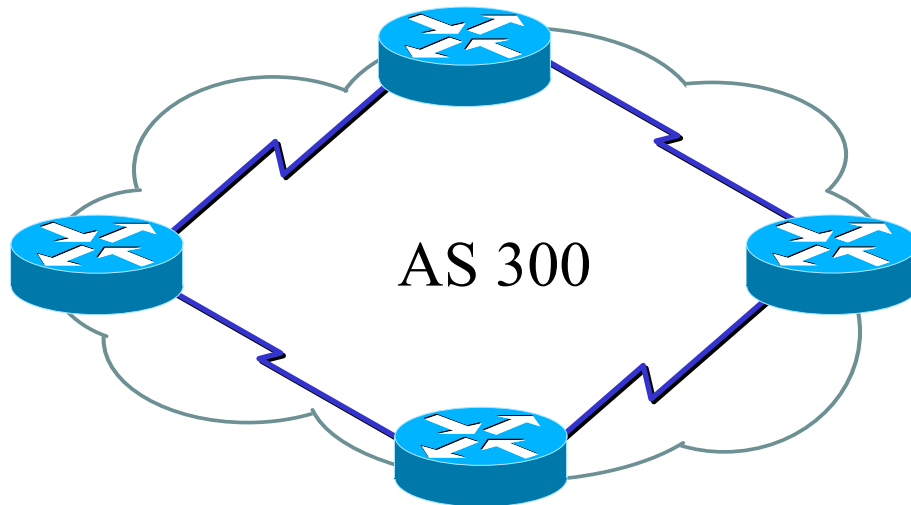
**Centro de Operación de CUDI  
UNAM**

**Abril 2006  
Oaxaca, Oaxaca**



# Sistema Autónomo (AS)

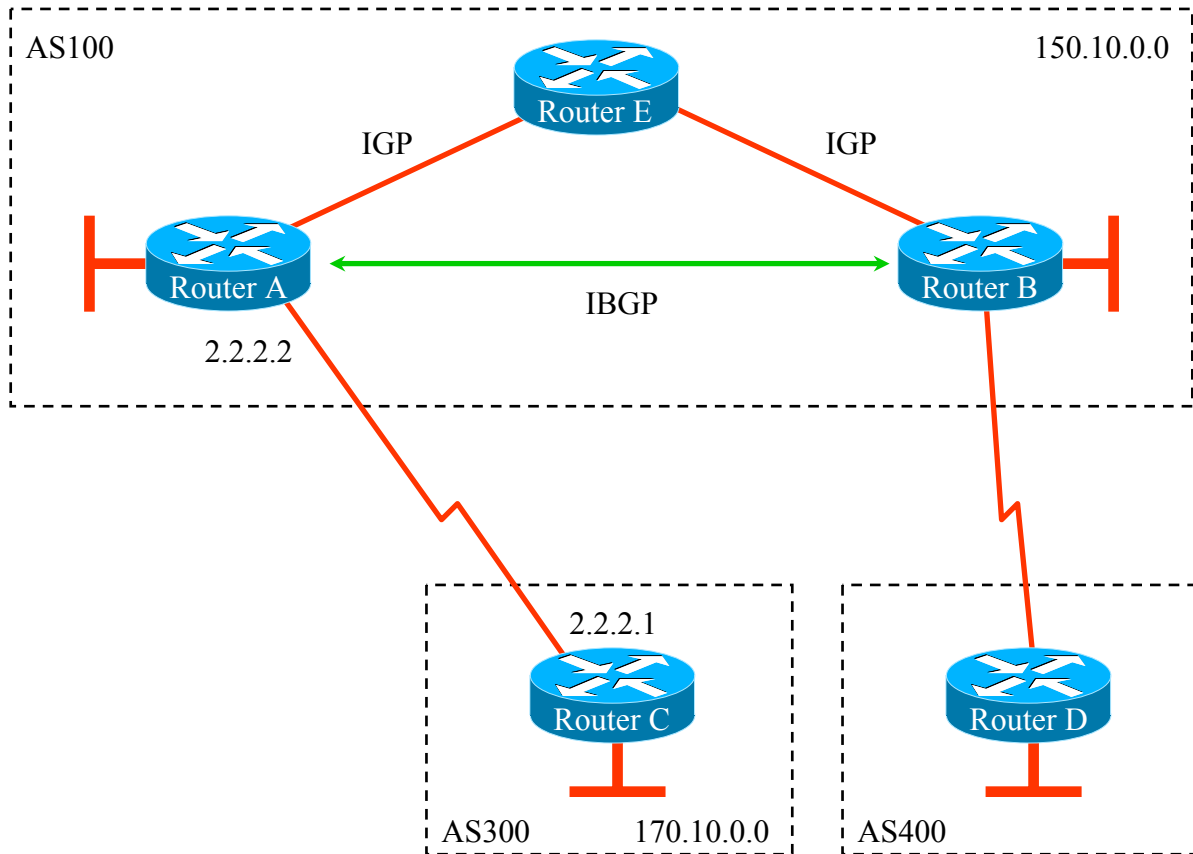
- Conjunto de routers (y redes) bajo una misma administración y con la mismas políticas de ruteo
- Al exterior, un AS se ve como una sola entidad
- Cada AS posee un identificador único.



# 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

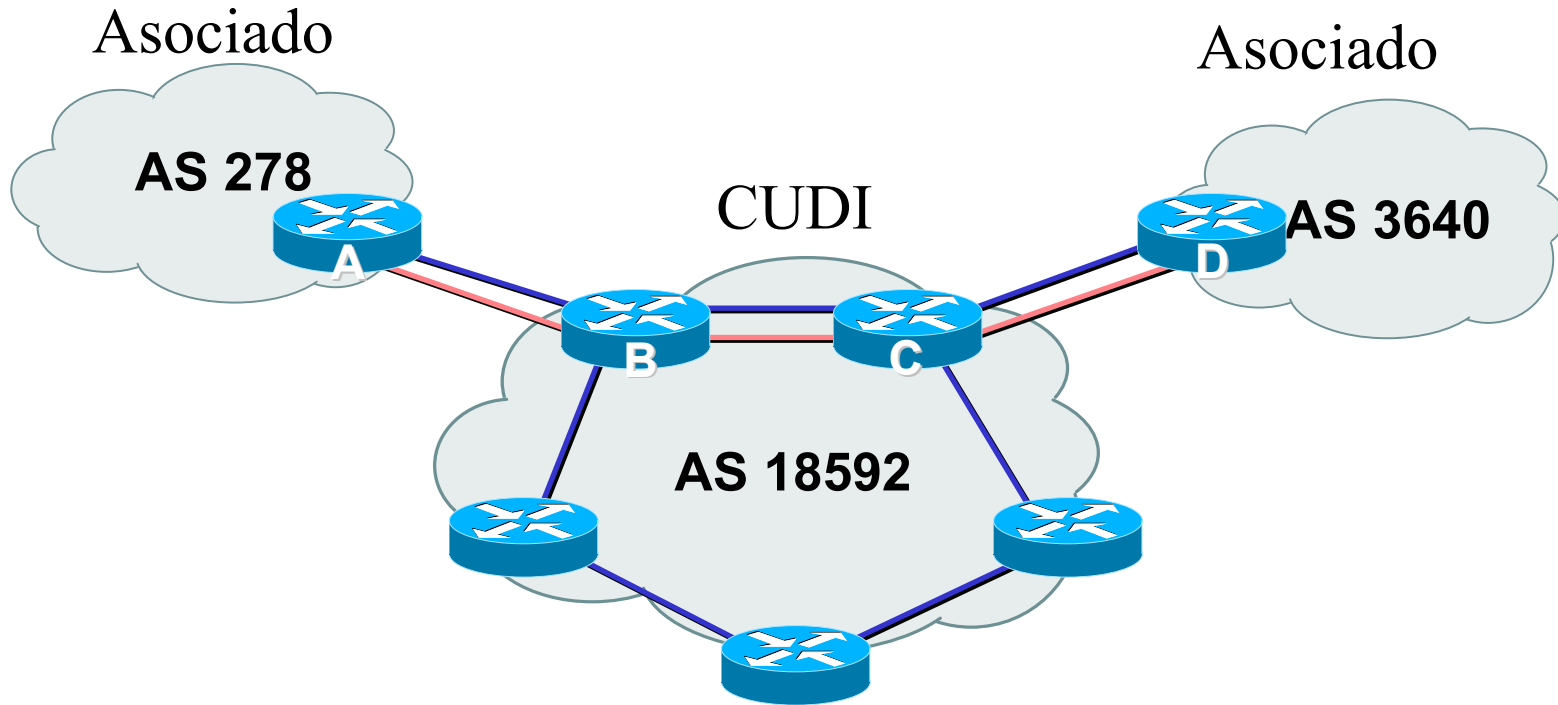
## Sincronización



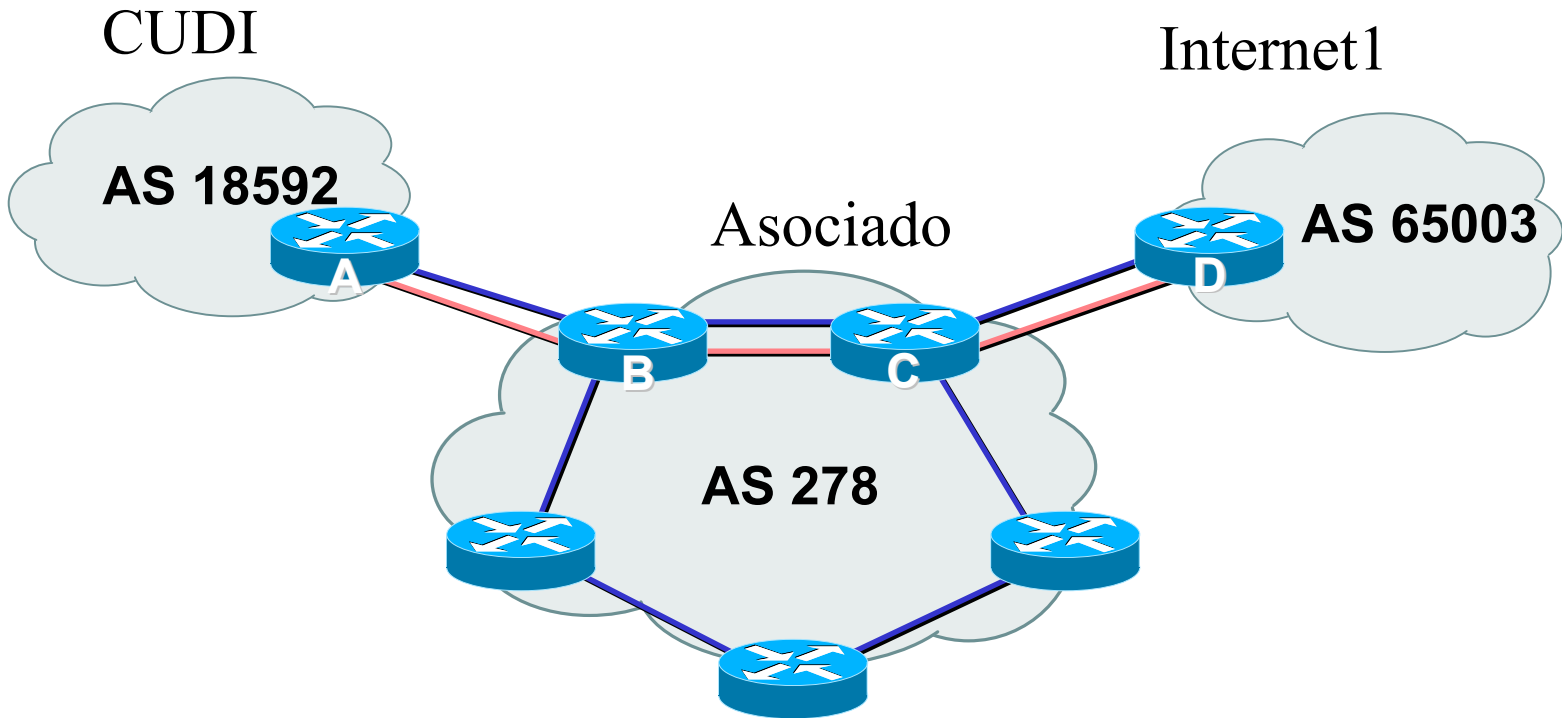
# Definiciones

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

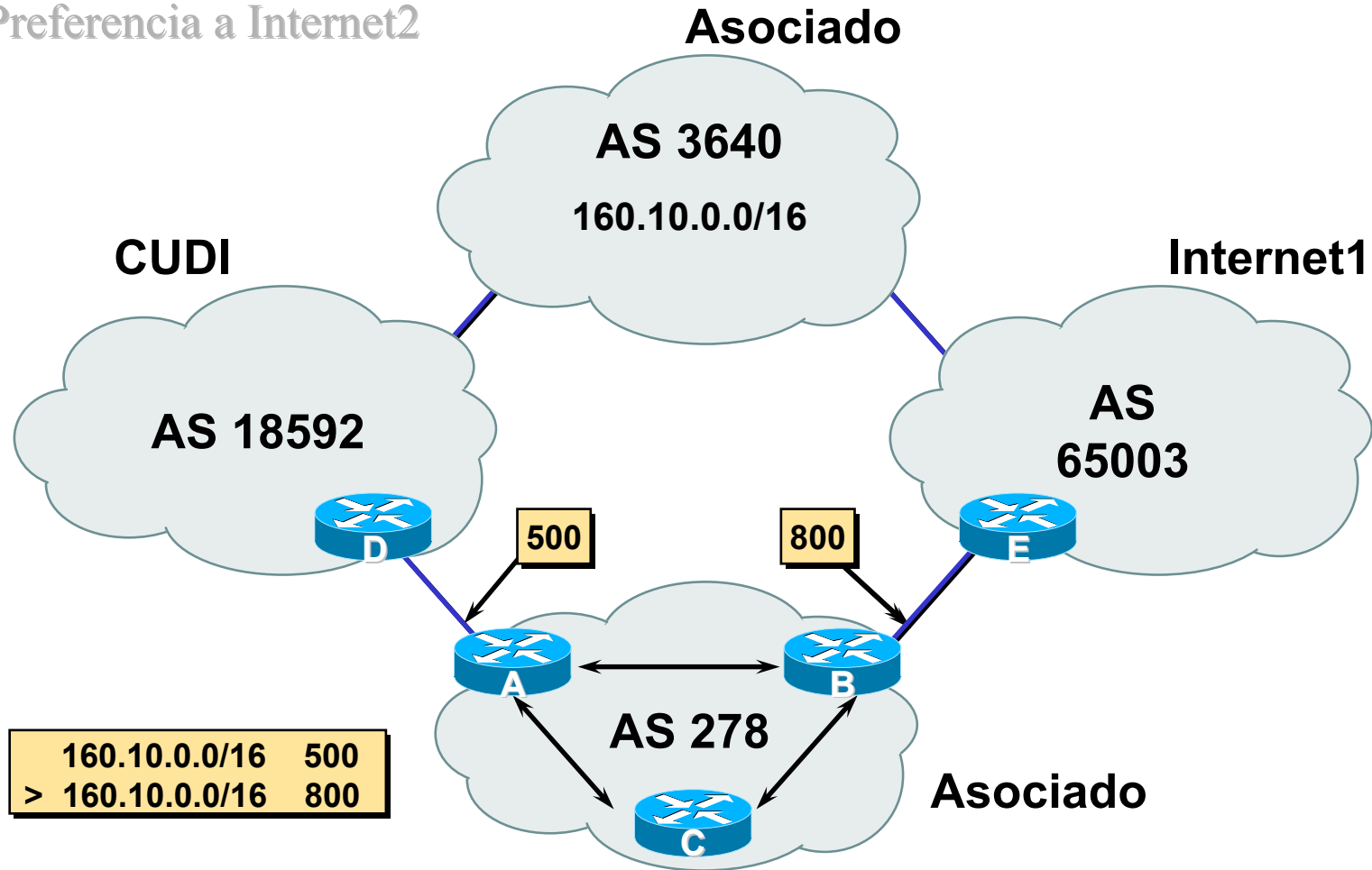
# Transito



# No Transito



## Preferencia a Internet2





# Aplicando Políticas de Ruteo

- Aplicando Políticas 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 200.200.1.1 distribute-list 10 in
```

```
neighbor 200.200.1.1 distribute-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 línea inicie con
- \$ Que la línea termine con
- | Or (pipe)
- () que contenga la expresión

*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 (Confederación)

# Políticas 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 ...

# Políticas 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
  
```



# Políticas de Control - Route-Map

```

router bgp 100
  neighbor 220.200.1.2 route-map filter-on-as-path in
  !
route-map filter-on-as-path permit 10
  match as-path 1
  set local-preference 80
  !
route-map filter-on-as-path permit 20
  match as-path 2
  set local-preference 200
  !
route-map filter-on-as-path permit 30
  !
ip as-path access-list 1 permit _150$
ip as-path access-list 2 permit _210_
    
```

# Políticas de Control - Route-Map

Ejemplo. Uso de PREEND

```

router bgp 300
  network 215.7.0.0
  neighbor 2.2.2.2 remote-as 100
  neighbor 2.2.2.2 route-map SETPATH out
!
route-map SETPATH permit 10
  set as-path prepend 300 300
    
```

- Cuando se utilice el Preend utilizar su propio AS
  - De lo contrario BGP puede detectar un loop que provoca una desconexión

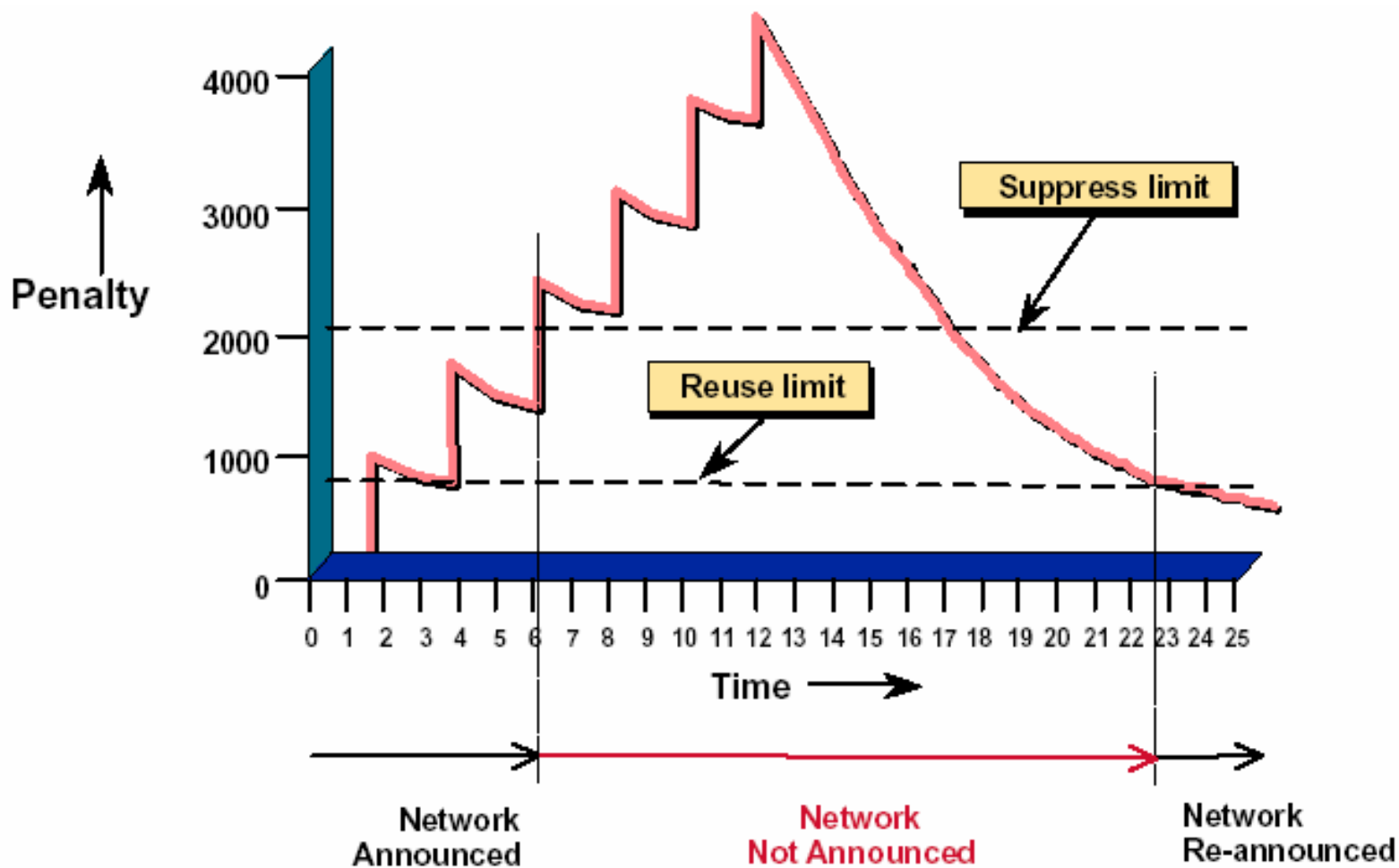
# Route Flap Damping

- Route Flap
  - Cada vez que un camino va a up, down o se modifica un Atributo
  - Las oscilaciones son a través de toda la Internet
  - Desperdicio de CPU
- La penalizaciones reduce la propagación de la oscilación.
- Documentado el uso de penalizaciones en el RFC-2439

# Route Flap Damping

- Se suma a una penalidad (1000) por cada oscilación
  - Un cambio en Atributo 500
- Exponencialmente decae la penalidad
- Penalida arriba del limite se supreción
  - No se propaga el anuncio a los vecinos
- Penalidad abajo del limite de Reuso
  - Se propaga el anuncio a los vecinos
  - Las penalidades se reinician a cero cuando estas caen debajo de la mita del limite de Reuso

# Route Flap Damping



# Route Flap Damping

- Se aplica solamente de entrada a los anuncios de los eBGP
- Los caminos alternos son todavia utiles
- Esta normalmente definido:
  - Half-life (default 15 minutos)
  - Reuse-limit (default 750)
  - Supress-limit (default 2000)
  - Maximun suppress limit (default 60 minutos)

*Recomendación de su uso [www.ripe.net/docs/ripe-210.html](http://www.ripe.net/docs/ripe-210.html)*

# BGP vs IGP

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

# BGP vs IGP

- BGP usar internamente (iBGP) y externamente (eBGP)
- iBGP usado para transportar
  - Los prefijos de Internet a través del Backbone
  - Los prefijos de los clientes
  - Utilizar /32 para las interfaces loopbacks de enrutamiento y levantar las sesiones de IBGP con ellas
  - Usar Peer Groups
  - Usar Passwords en la sesiones de IBGP



# BGP vs IGP

- IGP
  - El IGP debe contener a las redes de la DMZ o usar  
neighbor x.x.x.x next-hop-self
- eBGP usados para
  - Intercambiar prefijos con otros AS
  - Implementar políticas de Ruteo

# BGP

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

# BGP

- Herencia de BGP
  - Sincronización
    - En redes grandes es mejor apagarla
      - router bgp 278  
no synchronization
  - Auto-Sumarización
    - router bgp 278  
no auto-summary
  - *Hacer la distancia administrativa mas grande que cualquier IGP*
    - *Distance bgp 200 200 200*

# 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

# BGP

- Que anuncios no debo de recibir

```

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
    
```

# BGP

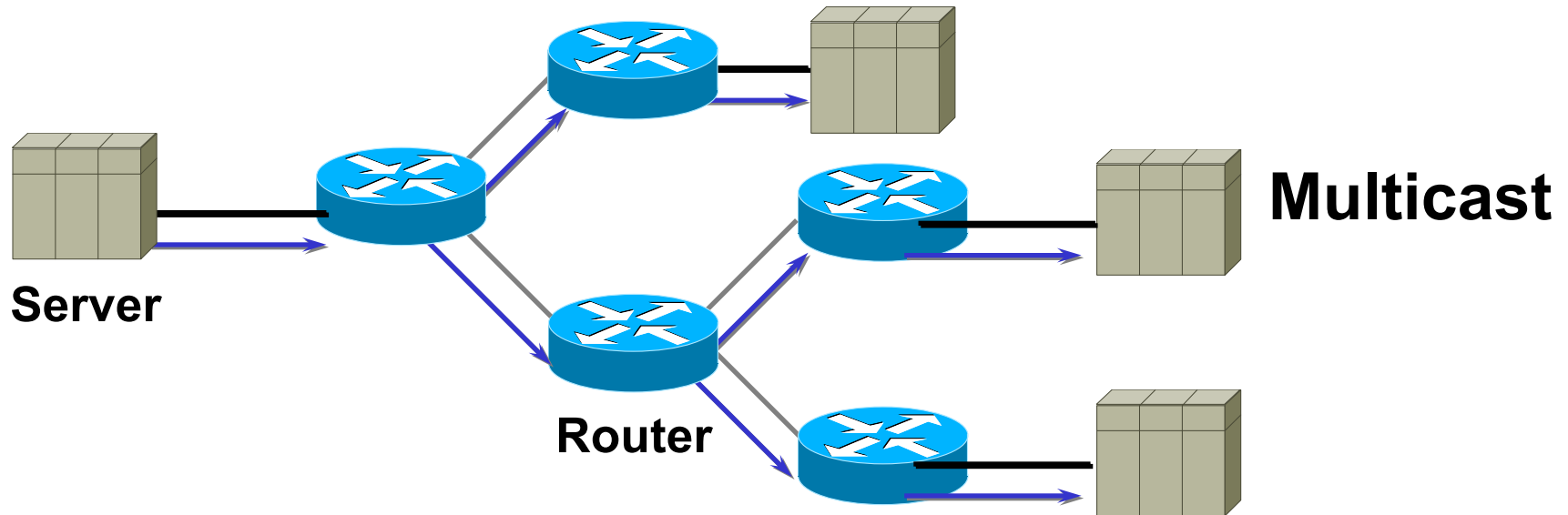
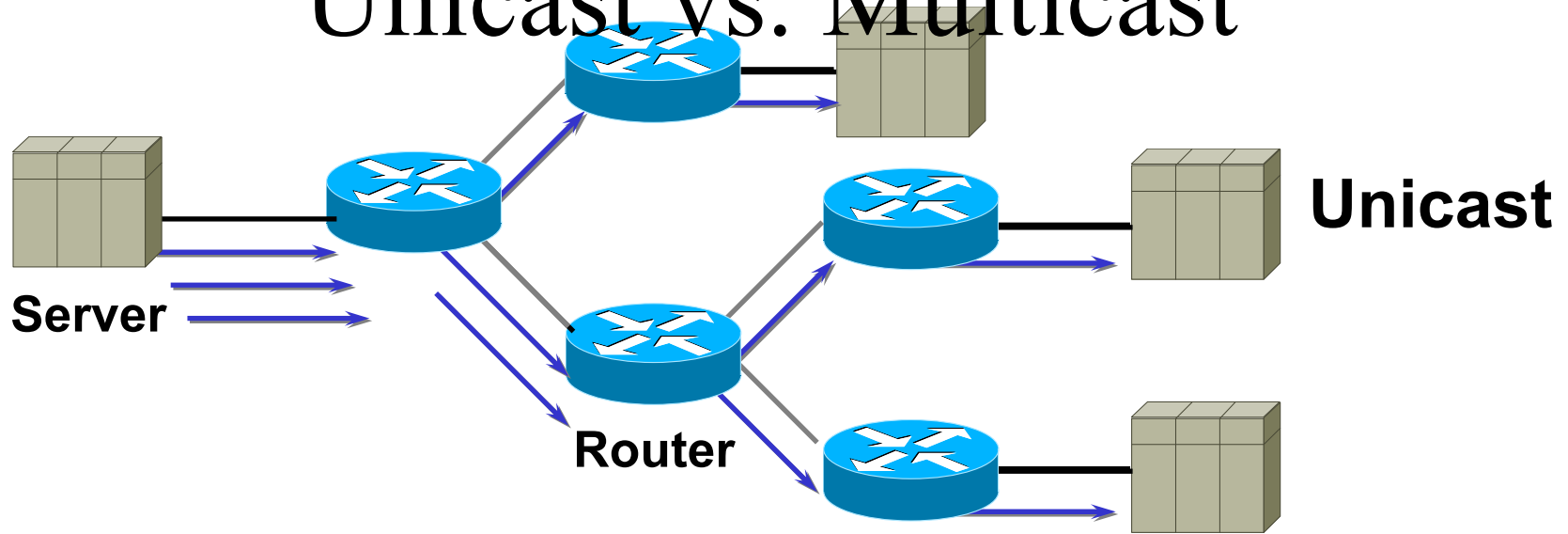
- Como debo crear los anuncios
    - Usar el comando Network
    - Mientras exista una ruta estatica el anuncio se mantendra en BGP
      - Estatica de Pull-Up  
ejemplo
- ```
ip route 200.15.0.0 255.255.0.0 null0
router bgp 100
    network 200.15.0.0 mask 255.255.0.0
```

# BGP

```

interface loopback 0
  ip address 215.17.3.1 255.255.255.255
!
interface Serial 5/0
  ip unnumbered loopback 0
  ip verify unicast reverse-path
!
ip route 215.34.10.0 255.255.252.0 Serial 5/0
!
router bgp 100
  network 215.34.10.0 mask 255.255.252.0
  
```

## Unicast vs. Multicast





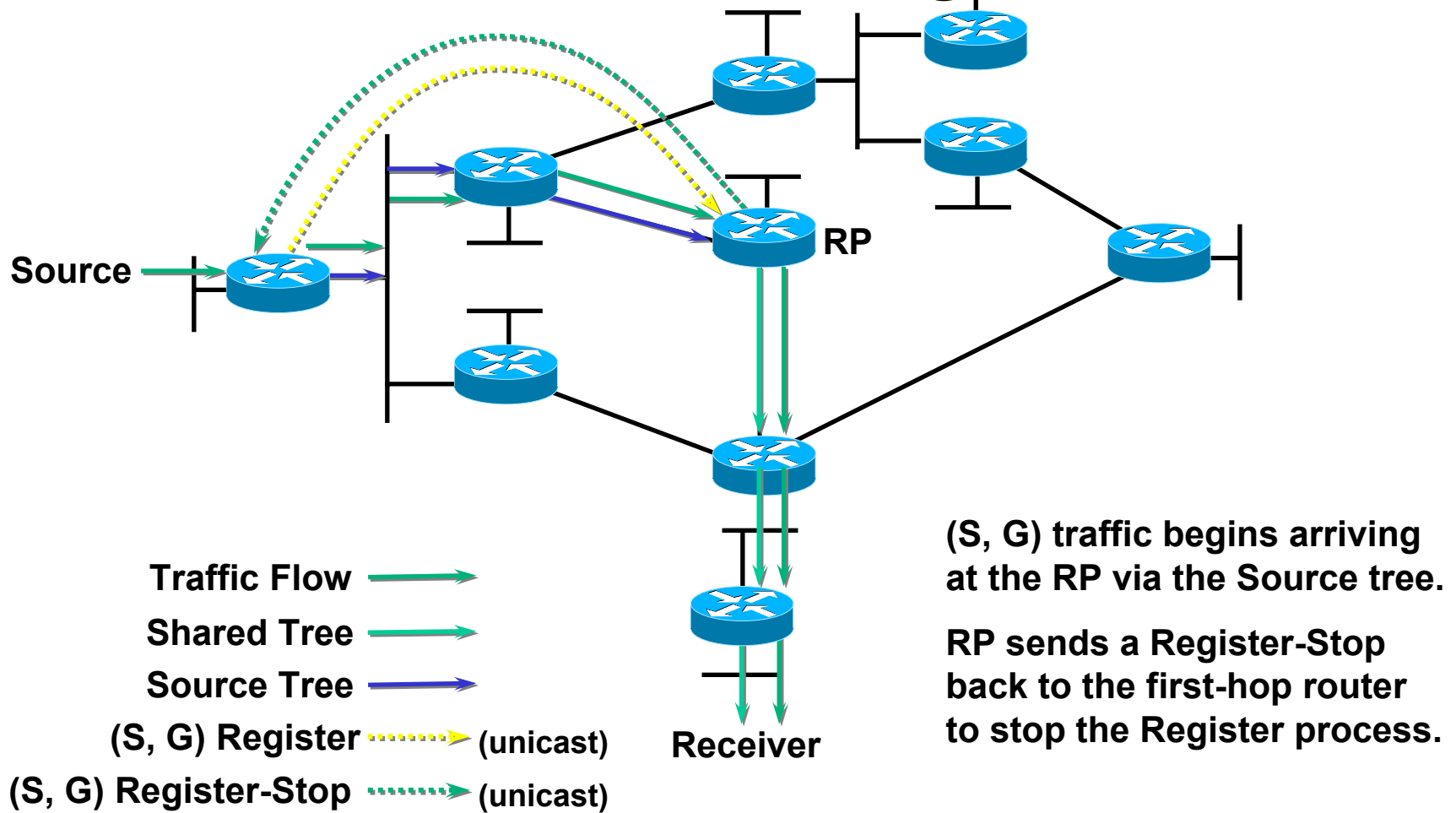
# Que necesito para tener Multicast

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

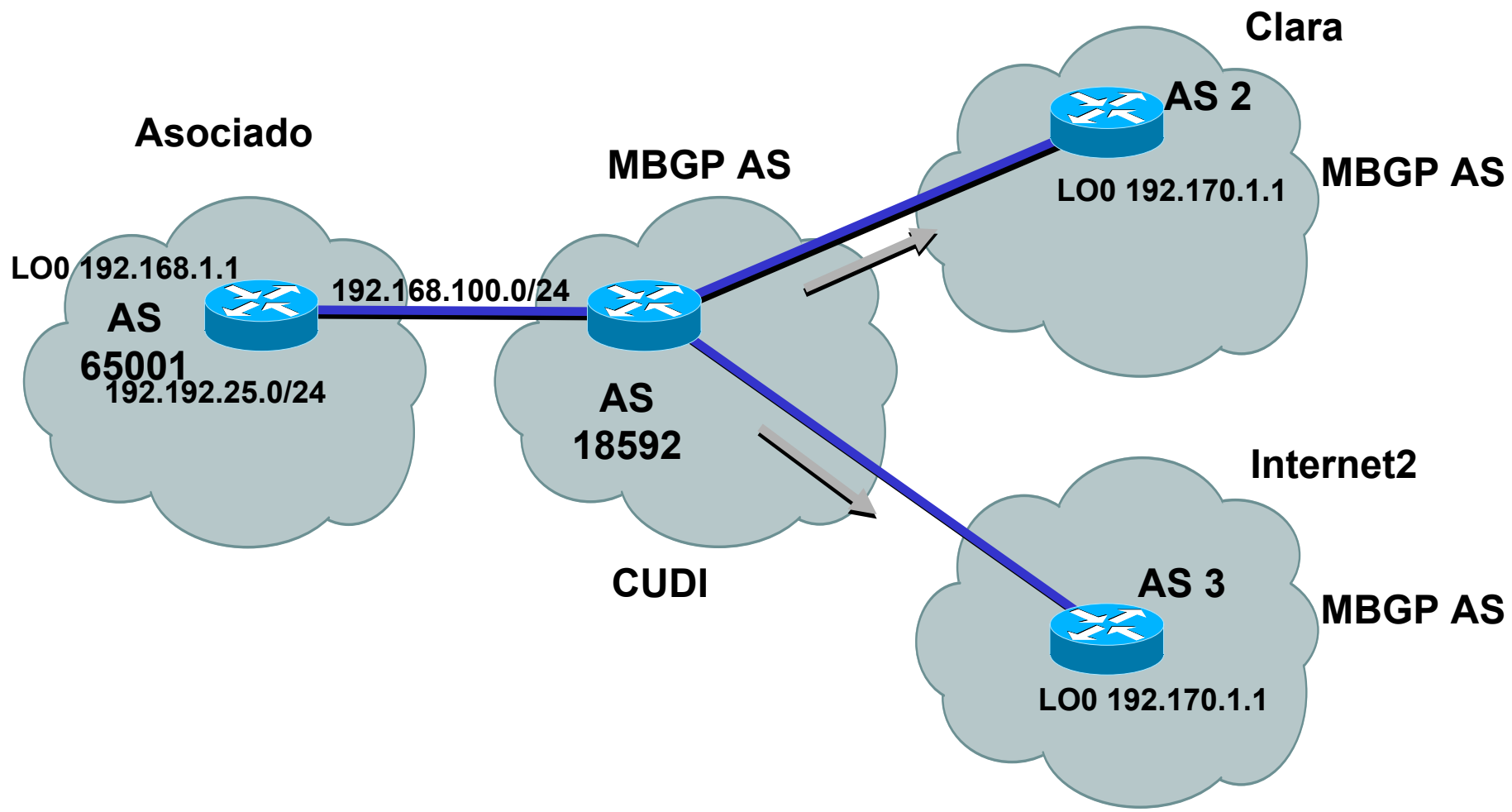
**PIM-SM (forwarding)**

- **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

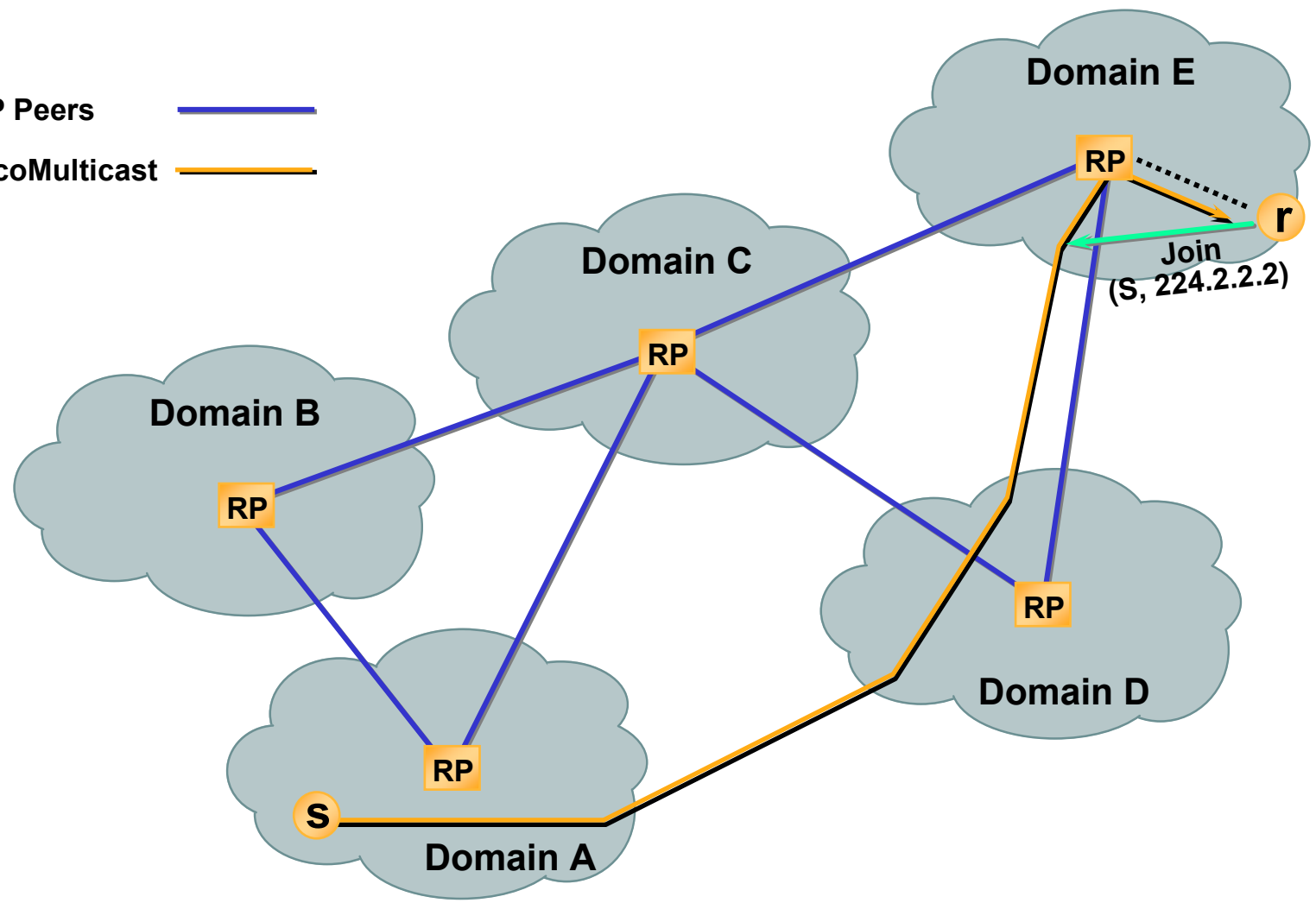


# Funcionamiento MBGP



# Funcionamiento MSDP

MSDP Peers   
TraficoMulticast 



# Multicast v4

- Habilitar multicast en el router
  - ip multicast-routing
- Habilitar PIM en las interfaces

```
interface ATM1/0.3 point-to-point
ip pim bsr-border
ip pim sparse-dense-mode
ip multicast ttl-threshold 32
ip multicast boundary 50
```

- Definir el filtro de frontera

```
access-list 50 deny 224.0.1.39
access-list 50 deny 224.0.1.40
access-list 50 deny 239.0.0.0 0.255.255.255
access-list 50 permit any
```

# Multicast v4 Cont.

- Definir el vecino de MBGP
 

```
router bgp 18592
address-family ipv4 multicast
neighbor 137.164.27.88 activate
neighbor 137.164.27.88 soft-reconfiguration inbound
neighbor 137.164.27.88 prefix-list ABILENE_OUT out
neighbor 137.164.27.88 route-map Mabilene out
network 200.23.60.0
exit-address-family
```
- Definir el RP
 

```
ip pim rp-address 200.23.60.1
```
- Definir el vecino de MSDP
 

```
ip msdp peer 200.23.60.109 connect-source ATM1/0.3 remote-as 3640
ip msdp description 200.23.60.109 CICESE
ip msdp sa-filter out 200.23.60.109 list 111
```

# Multicast v4 Cont.

- Definir el Filtro de MSDP (acl 111)

```

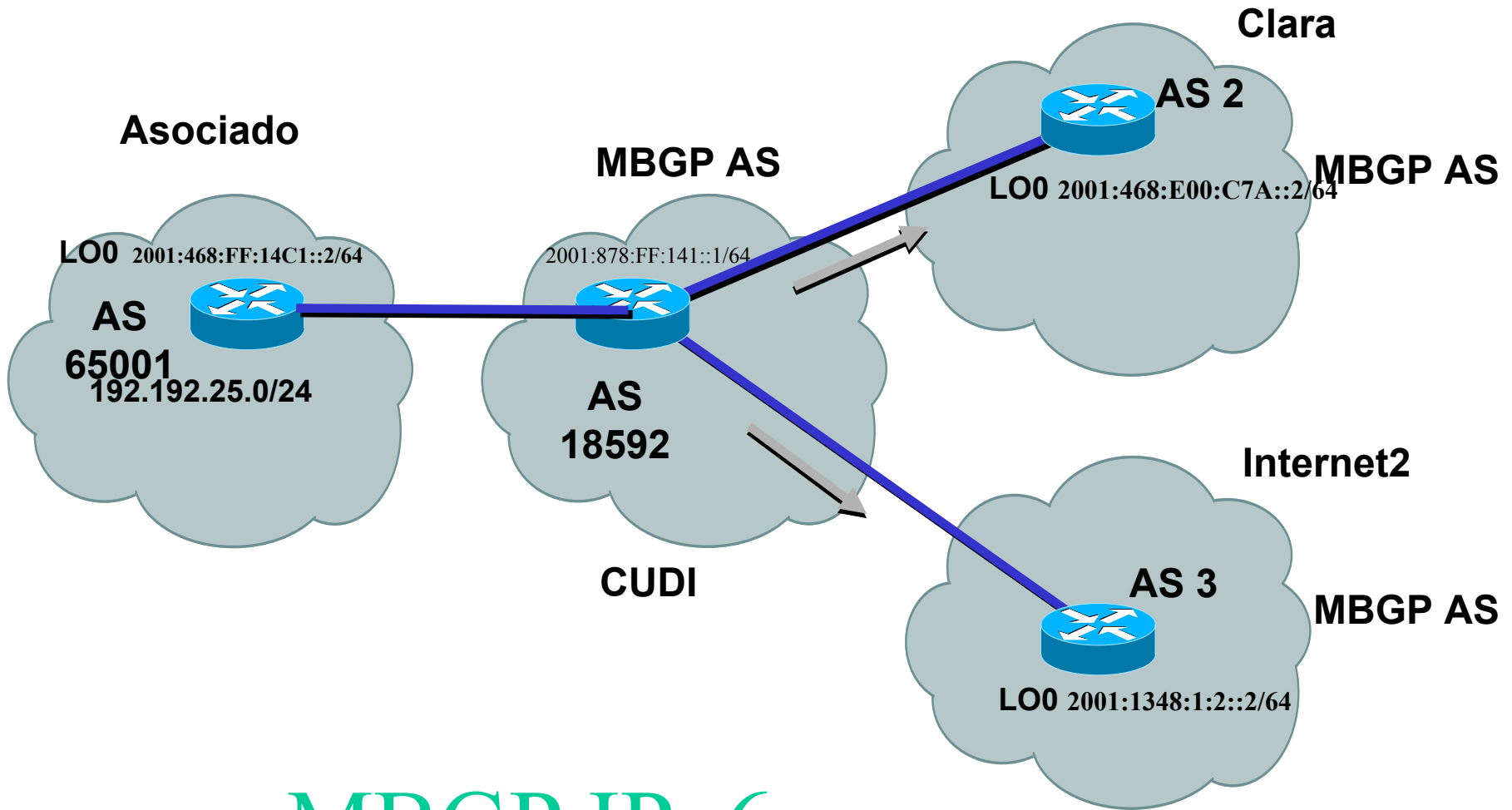
access-list 111 deny ip any host 224.0.1.2
access-list 111 deny ip any host 224.0.1.3
access-list 111 deny ip any host 224.0.1.22
access-list 111 deny ip any host 224.0.1.24
access-list 111 deny ip any host 224.0.1.35
access-list 111 deny ip any host 224.0.1.60
access-list 111 deny ip any host 224.0.2.2
access-list 111 deny ip any host 234.42.42.42
access-list 111 deny ip any host 229.55.150.208
access-list 111 deny ip any host 234.142.142.142
access-list 111 deny ip any host 225.1.2.3
access-list 111 deny ip any host 224.0.1.39
access-list 111 deny ip any host 224.0.1.40
access-list 111 deny ip any 239.0.0.0 0.255.255.255
access-list 111 deny ip 10.0.0.0 0.255.255.255 any
access-list 111 deny ip 127.0.0.0 0.255.255.255 any
access-list 111 deny ip 172.16.0.0 0.15.255.255 any
access-list 111 deny ip 192.168.0.0 0.0.255.255 any
access-list 111 deny ip any 232.0.0.0 0.255.255.255
access-list 111 permit ip any any
    
```

# IPv6

MBGP Extenciones para IPv6

Unicast





## MBGP IPv6

# IPv6 configuración

- **Habilitar IPv6**

```
ipv6 unicast-routing
ipv6 cef
```

- **Habilitar IPv6 en la interfaces**

```
interface ATM1/0.2 point-to-point
ipv6 address 2001:448:3:66::2/64
```

- **Establecer el peer de MBGP**

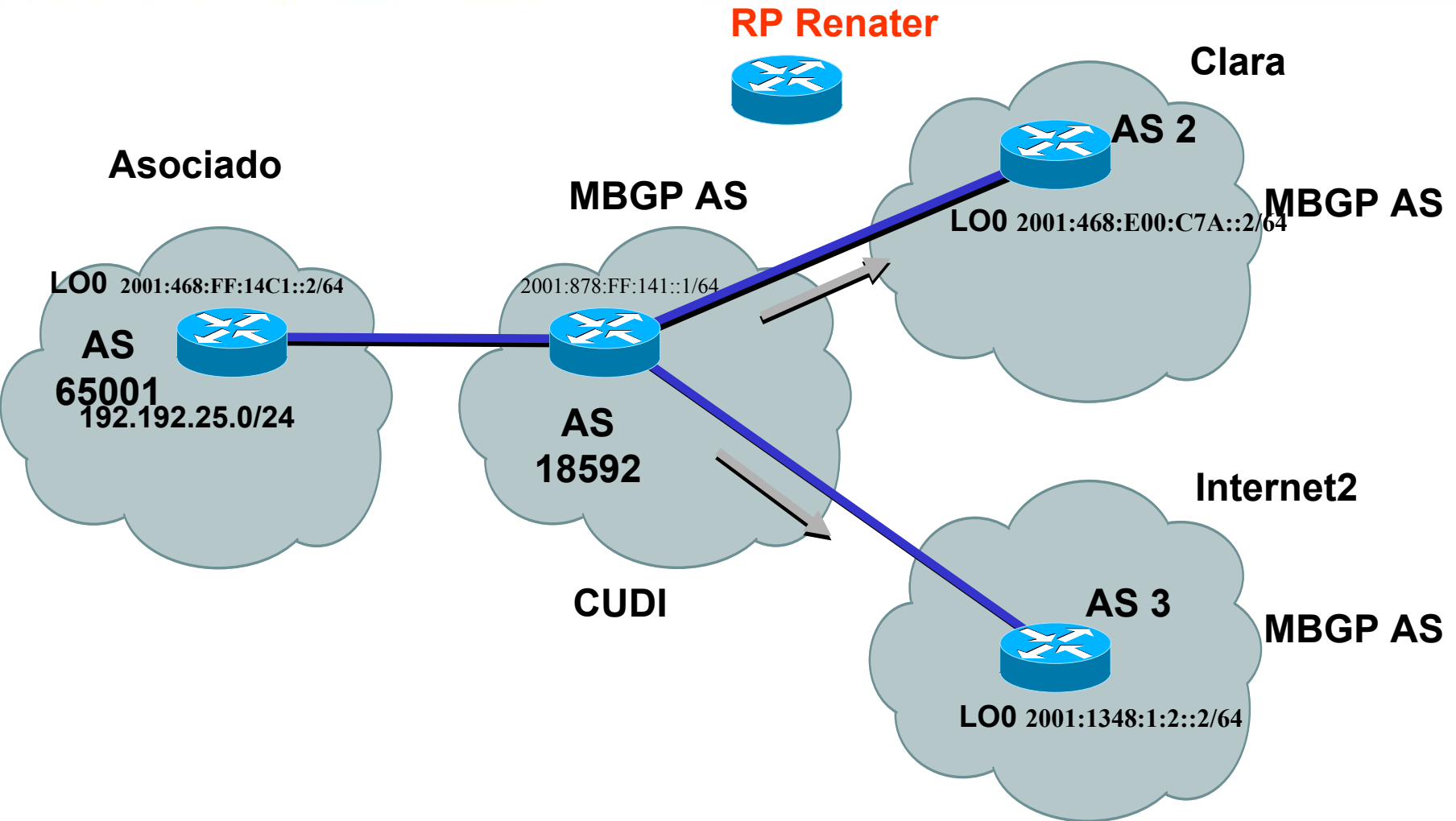
```
router bgp 18592
address-family ipv6
neighbor 2001:448:3:66::1 remote-as 278
neighbor 2001:448:3:66::1 description UNAMIPv6
neighbor 2001:448:3:66::1 prefix-list UNAM in
network 2001:448:3:66::1/48
exit-address-family
```

- **Definir un protocolo IGP (RIP/OSPFv3/ISIS)**

# IPv6

MBGP Extenciones para IPv6

Multicast



## MBGP IPv6 Multicast

# IPv6 Multicast configuración

- Habilitar IPv6

```
ipv6 multicast-routing
ipv6 cef
```

- Definir el RP

```
ipv6 pim rp-address 2001:660:3007:300:1::
```

- Establecer el peer de MBGP

```
router bgp 18592
address-family ipv6 multicast
neighbor 2001:448:3:66::1 remote-as 278
neighbor 2001:448:3:66::1 description UNAMIPv6
neighbor 2001:448:3:66::1 prefix-list UNAM in
network 2001:448:3:66::1/48
exit-address-family
```

- Definir un protocolo IGP (RIP/OSPFv3/ISIS)

!!!! Gracias !!!!