

Redundancia

Ing. José Restaino

Ing. Alvaro Sánchez

Objetivo

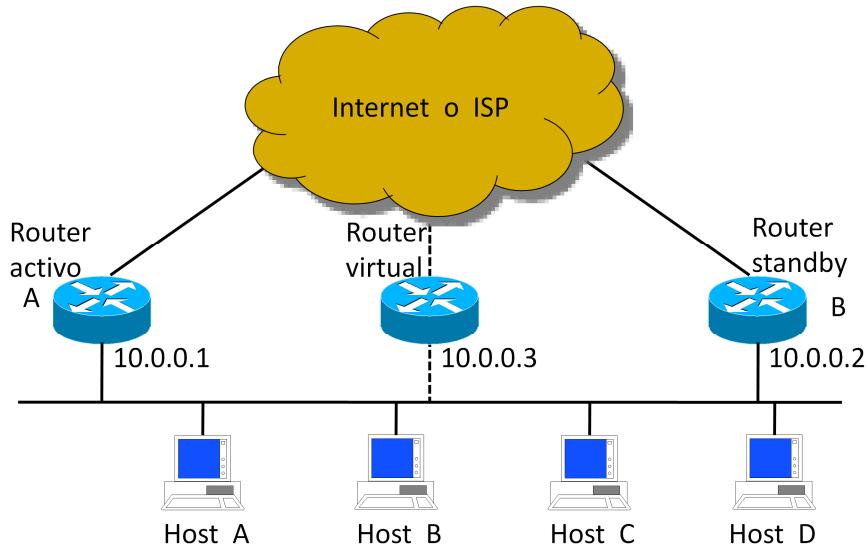
- Asegurar la continuidad del funcionamiento ante un fallo simple.
- En el caso de dispositivos de redes implica prever caminos alternativos que se utilicen automáticamente en caso de indisponibilidades de los caminos actuales

Redundancia

- Redundancia en LAN
- Redundancia en WAN
- Redundancia entre sistemas autónomos
- Redundancia en sistemas de servidores

Redundancia en LAN - HSRP

Funcionamiento básico



Elementos y funcionamiento

Hot Standby Routing Protocol es un mecanismo ideado por Cisco en 1994 (RFC 2281), para proveer una salida redundante a los hosts de una Lan. Para éstos, la configuración sólo debe prever que se defina como default gateway la dirección IP del HSRP, en lo demás, se trata de una configuración estándar.

El mecanismo involucra dos routers, uno de los cuales será el activo y el otro permanecerá en standby para intervenir en caso de fallo del activo (se define por medio de la especificación de prioridades).

Los dos equipos se comunicarán a través de la Lan (es requisito que exista este tipo de conectividad), e intercambiarán sus parámetros de configuración. Esa interconexión se utilizará para mantener un envío periódico de paquetes de "heart beat", con hello timer de 3 segundos, y hold timer de 10 segundos, que le permite determinar al standby si le corresponde entrar en acción. El router standby entrará en acción si se supera el hold timer sin escuchar ningún paquete de hello.

Ambos routers podrán tener configuradas direcciones IP en la Lan que comparten, pero la dirección de default gateway podrá ser una de ellas o bien otra diferente. La última opción es la usual y la recomendable.

El router activo responderá las solicitudes de ARP que especifiquen la dirección IP del default gateway (la dirección virtual de HSRP) con una dirección MAC virtual, independiente de la dirección MAC propia del router. En caso que el router que está en standby pase al estado activo, responderá por las mismas direcciones virtuales, la IP y la MAC. De ese modo, los hosts no percibirán más que una pequeña interrupción en la conectividad, correspondiente al tiempo que le insume al standby detectar la situación y asumir su nuevo rol de activo.

Debe notarse que el HSRP afecta solamente al tráfico saliente. La redundancia para el tráfico entrante se logra por medio de los anuncios de las rutas de la Lan a través de ambos routers.

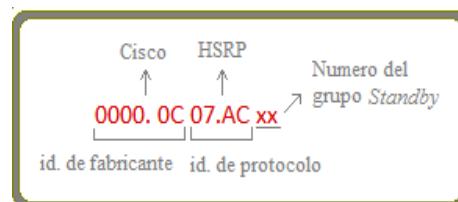
Ejemplo de configuración

Configuración del Router A

```
Router A (config)# interface Ethernet0/0
Router A (config-if)# ip address 10.0.0.1 255.255.255.0
Router A (config-if)# standby 1 preempt
Router A (config-if)# standby 1 priority 110
Router A (config-if)# standby 1 ip 10.0.0.3
```

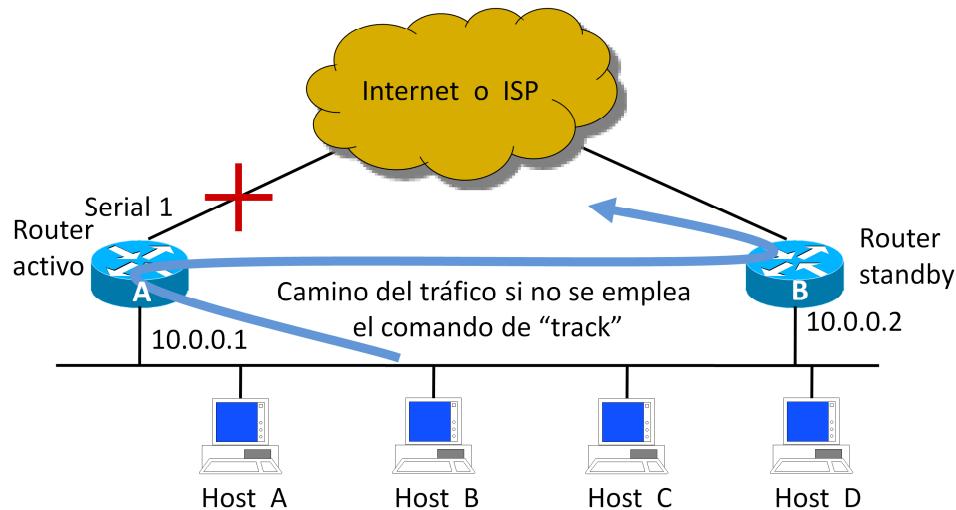
Configuración del Router B

```
Router B (config)# interface Ethernet0/0
Router B (config-if)# ip address 10.0.0.2 255.255.255.0
Router B (config-if)# standby 1 preempt
Router B (config-if)# standby 1 priority 105
Router B (config-if)# standby 1 ip 10.0.0.3
```



Redundancia en LAN - HSRP

Funcionamiento básico



Fallo en interfaz de salida

En caso de un fallo en la interfaz de salida del router activo (A), debido a que dicho equipo tiene en funcionamiento un protocolo de enrutamiento que le permite intercambiar información con el standby (B), redirigirá el tráfico a este último router. Si se desea evitar que el router A participe en el envío del tráfico, y que el mismo se curse directamente a través de B, se puede configurar a A para que en caso de fallo de la interfaz de salida, disminuya su prioridad para ser activo, de modo que permitirá que el standby lo releve (comando “standby n°grupo track interfaz”, disminuye en 10 la prioridad en caso de caída de la interfaz).

Ejemplo de configuración

Configuración del Router A

```

Router A (config)# interface Ethernet0/0
Router A (config-if)# ip address 10.0.0.1 255.255.255.0
Router A (config-if)# standby 1 preempt
Router A (config-if)# standby 1 priority 110
Router A (config-if)# standby 1 ip 10.0.0.3
Router A (config-if)# standby 1 track Serial1      <- indicación de la interfaz a monitorear

```

Configuración del Router B

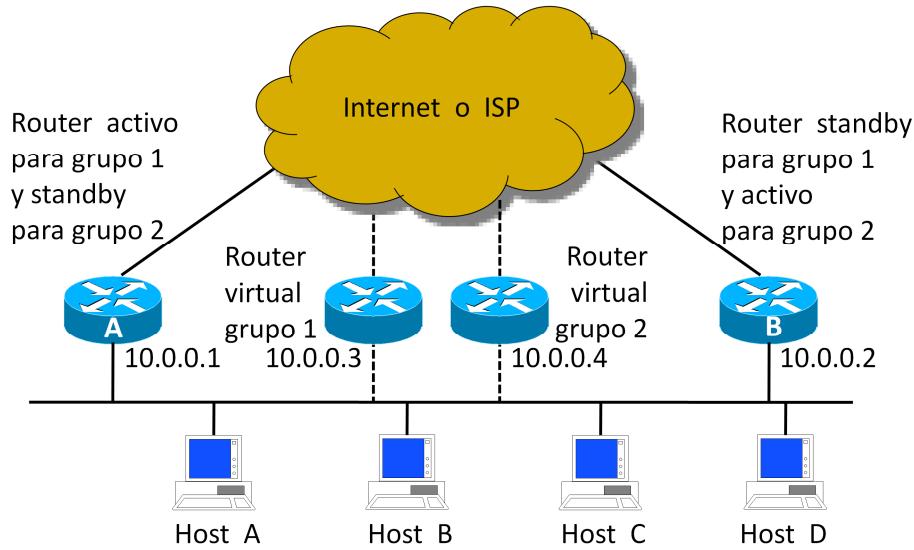
```

Router B (config)# interface Ethernet0/0
Router B (config-if)# ip address 10.0.0.2 255.255.255.0
Router B (config-if)# standby 1 preempt
Router B (config-if)# standby 1 priority 105
Router B (config-if)# standby 1 ip 10.0.0.3

```

Redundancia en LAN - HSRP

Grupos (MHSRP)



Balance de carga mediante grupos de HSRP (Multi-group HSRP, MHSRP)

En HSRP es posible definir instancias (grupos) independientes, de modo de tener dos parejas diferentes de direcciones IP y MAC. Uno de los routers será el activo para una de esas parejas, y el otro lo será para la otra pareja. En parte de los hosts se configurará como default gateway una de las direcciones IP virtuales, y en el resto la otra dirección IP virtual. De ese modo el tráfico de una parte de los hosts será enviada por uno de los routers y el restante tráfico por el otro router.

Ejemplo de configuración

Configuración del Router A

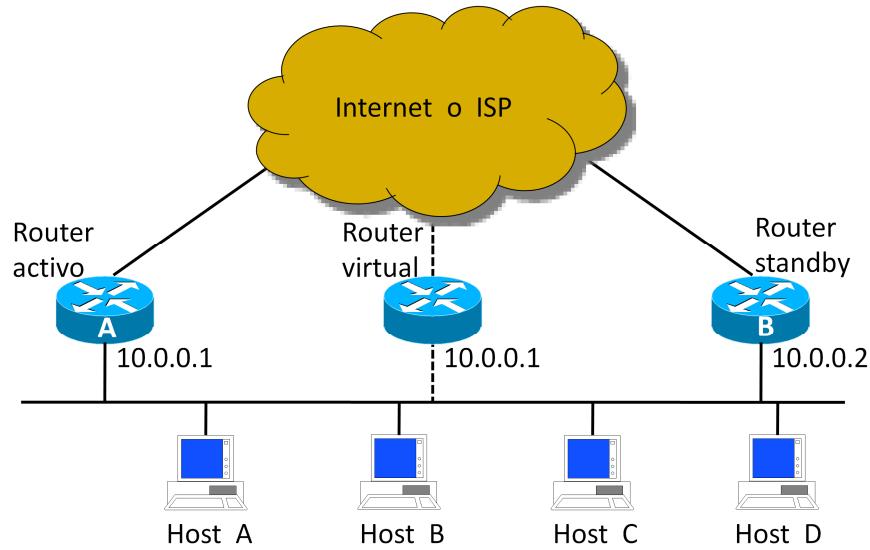
```
Router A (config)# interface Ethernet0/0
Router A (config-if)# ip address 10.1.0.1 255.255.0.0
Router A (config-if)# standby 1 priority 110
Router A (config-if)# standby 1 preempt
Router A (config-if)# standby 1 ip 10.0.0.3
Router A (config-if)# standby 2 priority 95
Router A (config-if)# standby 2 preempt
Router A (config-if)# standby 2 ip 10.0.0.4
```

Configuración del Router B

```
Router B (config)# interface Ethernet0/0
Router B (config-if)# ip address 10.1.0.2 255.255.0.0
Router B (config-if)# standby 1 preempt
Router B (config-if)# standby 1 priority 105
Router B (config-if)# standby 1 ip 10.0.0.3
Router B (config-if)# standby 2 priority 110
Router B (config-if)# standby 2 preempt
Router B (config-if)# standby 2 ip 10.0.0.4
```

Redundancia en LAN - VRRP

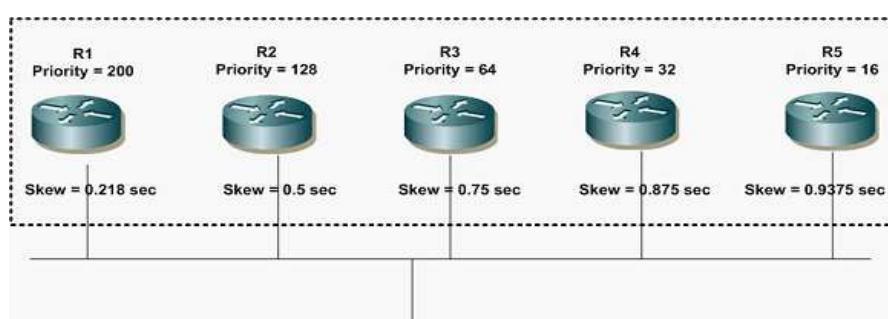
Funcionamiento básico



Elementos y funcionamiento

Virtual Router Redundancy Protocol es un mecanismo creado por IETF en 1999 (RFC 3768). Similar a HSRP, permite emplear equipamiento de múltiples proveedores, ya que no se trata de un protocolo propietario. Tiene temporizadores más rápidos que HSRP: por defecto emplea hello cada 1 segundo.

El hold timer se calcula del siguiente modo: Hold time = 3 x Advertisements + tiempo skew, donde el tiempo skew permite que cada router difiera del resto en el tiempo total que espera. El valor del tiempo de skew es inversamente proporcional a la prioridad. En la figura se muestra un ejemplo.



Ejemplo de configuración

Configuración del Router A

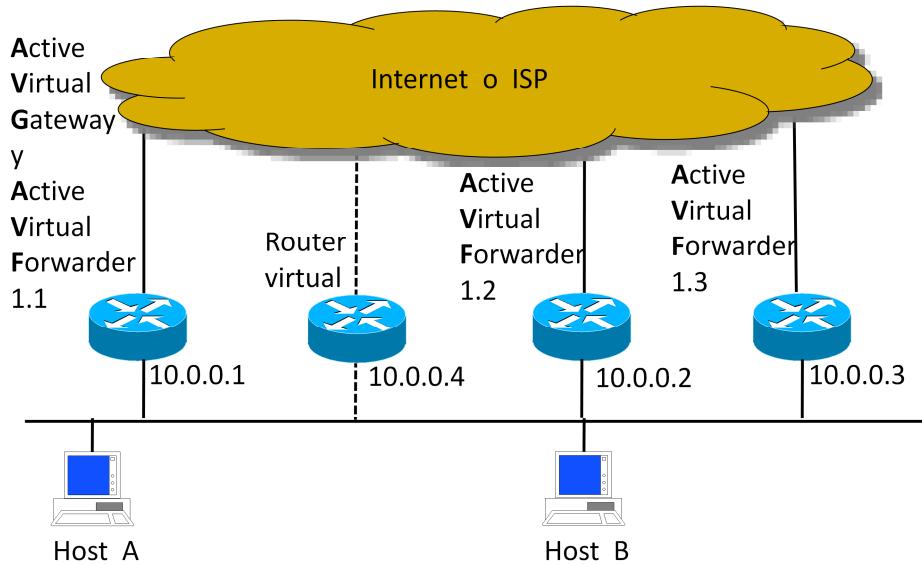
```
Router A (config)# interface Ethernet0/0
Router A (config-if)# ip address 10.0.0.1 255.255.255.0
Router A (config-if)# vrrp 1 preempt
Router A (config-if)# vrrp 1 priority 110
Router A (config-if)# vrrp 1 ip 10.0.0.1
```

Configuración del Router B

```
Router B (config)# interface Ethernet0/0
Router B (config-if)# ip address 10.0.0.2 255.255.255.0
Router B (config-if)# vrrp 1 preempt
Router B (config-if)# vrrp 1 priority 105
Router B (config-if)# vrrp 1 ip 10.0.0.1
```

Redundancia en LAN - GLBP

Funcionamiento básico



Elementos y funcionamiento

Gateway Load Balancing Protocol es un mecanismo de Cisco de 2005., desarrollado a partir de HSRP, que permite efectuar balance e carga sin necesidad de crear múltiples grupos (hasta 1024 grupos) como en el caso de MHSRP. Permite el envío de mensajes autenticados mediante MD5.

Puede emplear diferentes algoritmos de balance de carga para adaptarse a distintos entornos de redes y necesidades de clientes:

- 1) Round-Robin: cada dirección MAC de router virtual activo (*Active Virtual Forwarder*) es incluida en turnos para responder a la solicitud ARP de la dirección IP del router virtual. Puede haber hasta 4 AVF's por grupo.
- 2) Por Peso: la cantidad de carga enviada a un router virtual activo (AVF) depende del valor de peso publicado por el gateway que contiene ese AVF.
- 3) Dependiente del Host: se garantiza que un cliente use la misma dirección MAC virtual mientras ésta esté participando en el grupo GLBP.

Terminología

AVG (Active Virtual Gateway): Asigna a cada router dentro del grupo una dirección MAC virtual única, siguiendo el formato: 0007.B400.XXYY (xx es el número del grupo GLBP, yy es el número diferente propio de cada router; 01,02,...). Es responsable de la operación del protocolo.

AVF (Active Virtual Forwarder): Dentro de cada grupo se elige un router virtual AVF para una dirección MAC virtual específica que es responsable de reenviar los paquetes enviados a esa dirección MAC. Pueden existir múltiples AVF dentro de un grupo (hasta 4).

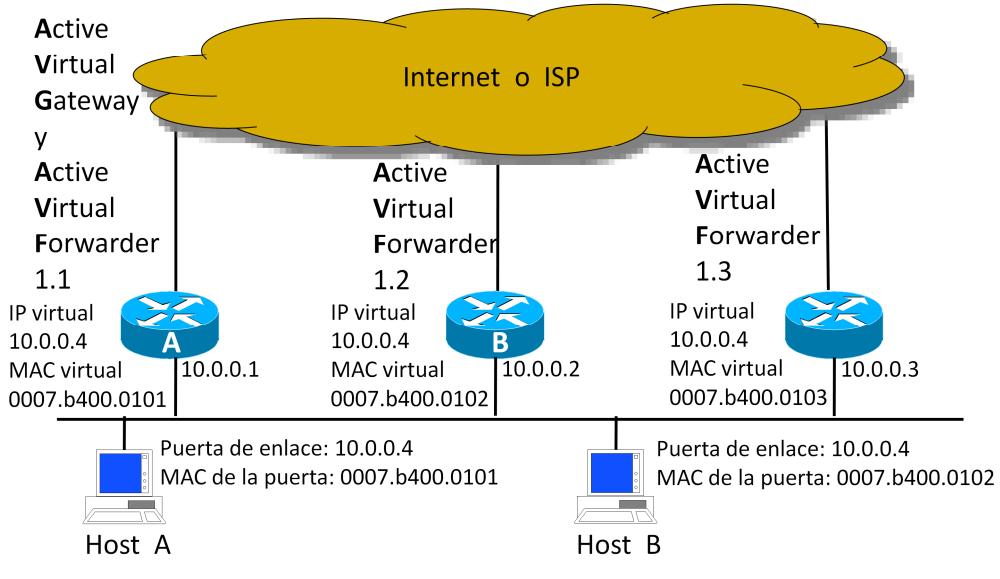
Por defecto, los routers GLBP emplean la dirección de multicast 224.0.0.102 para enviar paquetes de hello a sus peers, cada 3 segundos, mediante UDP: 3222 (origen y destino).

Puerta de enlace GLBP: Es un router con GLBP. Cada puerta de enlace GLBP puede participar en uno o más grupos GLBPs.

vIP: dirección IP virtual, ip v.4. Sólo puede haber una vIP por cada grupo configurado y éste debe tener al menos un miembro.

Redundancia en LAN - GLBP

Funcionamiento básico



Configuración

Ejemplo de configuración básica

Configuración del Router AVG

```
Router A (config)# interface Ethernet0/0
Router A (config-if)# ip address 10.0.0.1 255.255.255.0
Router A (config-if)# glbp 1 preempt
Router A (config-if)# glbp 1 priority 110 <- prioridad de AVG
Router A (config-if)# glbp 1 ip 10.0.0.4
Router A (config-if)# glbp 1 timers 6 20 <- valores de hello timer y de hold timer
```

Configuración del Router AVF1

```
Router B (config)# interface Ethernet0/0
Router B (config-if)# ip address 10.0.0.2 255.255.255.0
Router B (config-if)# glbp 1 preempt
Router B (config-if)# glbp 1 priority 105
Router B (config-if)# glbp 1 ip 10.0.0.4
Router B (config-if)# glbp 1 timers 6 20 <- valores de hello timer y de hold timer
```

Ejemplo de configuración de balance ponderado

Configuración del Router AVG

```
Router A (config)# track 1 interface Ethernet0/0
Router A (config)# interface Ethernet0/0
Router A (config-if)# ip address 10.0.0.1 255.255.255.0
Router A (config-if)# glbp 1 preempt
Router A (config-if)# glbp 1 priority 110
Router A (config-if)# glbp 1 ip 10.0.0.4
Router A (config-if)# glbp 1 timers 6 20
Router A (config-if)# glbp 1 load-balancing weighted.
Router A (config-if)# glbp 1 weighting 100 lower 85 upper 95
Router A (config-if)# glbp 1 weighting track 1 decrement 20
```

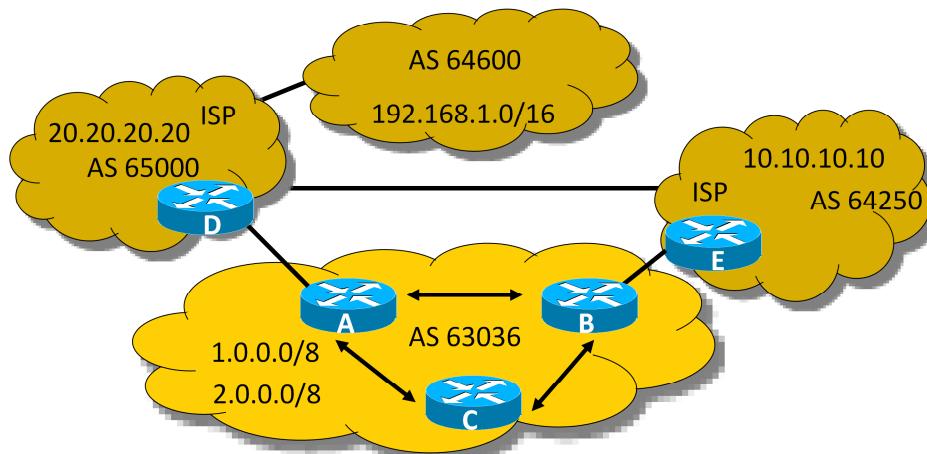
Configuración del Router AVF1

```
Router B (config)# track 1 interface Ethernet0/0
Router B (config)# interface Ethernet0/0
Router B (config-if)# ip address 10.0.0.2 255.255.255.0
Router B (config-if)# glbp 1 preempt
Router B (config-if)# glbp 1 priority 105
Router B (config-if)# glbp 1 ip 10.0.0.4
Router B (config-if)# glbp 1 timers 6 20
Router B (config-if)# glbp 1 load-balancing weighted.
Router B (config-if)# glbp 1 weighting 50 lower 35 upper 45
Router B (config-if)# glbp 1 weighting track 1 decrement 20
```

peso y límites ->
para dejar de ser AVF y volver a serlo

Redundancia entre sistemas autónomos

Multihoming



Multihoming

Cuando se desea disponer de redundancia de proveedores de acceso a Internet, se debe emplear BGP en modalidad de multihoming, lo cual implica que se emplee un número de Sistema Autónomo público para identificar el origen de las publicaciones de direcciones.

A continuación de presentan tres alternativas de acceso:

- recepción de sólo rutas default
- recepción de sólo rutas directamente conectadas y eventualmente rutas default
- recepción de full routing table

En cualquiera de las alternativas, interesa en general que se evite el tránsito de tráfico de otros AS a través del AS propio, lo cual resultaría en un consumo indeseado de recursos de la red.

Comandos

Sintaxis de route map:

```
route-map nombre_de_route_map acción numeral
  match ip address prefix-list nombre_de_lista
  set metric métrica
```

Ejemplo:

```
route-map ospf-to-eigrp permit 20
  match ip address prefix-list pfx
  set metric 40000 1000 255 1 1500
```

Sintaxis de prefix list:

```
ip prefix-list nombre_de_prefix-list seq nº_de_secuencia acción prefijo
```

Aplicación:

```
neighbor dirección_IP_del_vecino prefix-list nombre_de_prefix-list sentido
```

Ejemplo:

```
ip prefix-list DEFAULT seq 5 permit 0.0.0.0/0
```

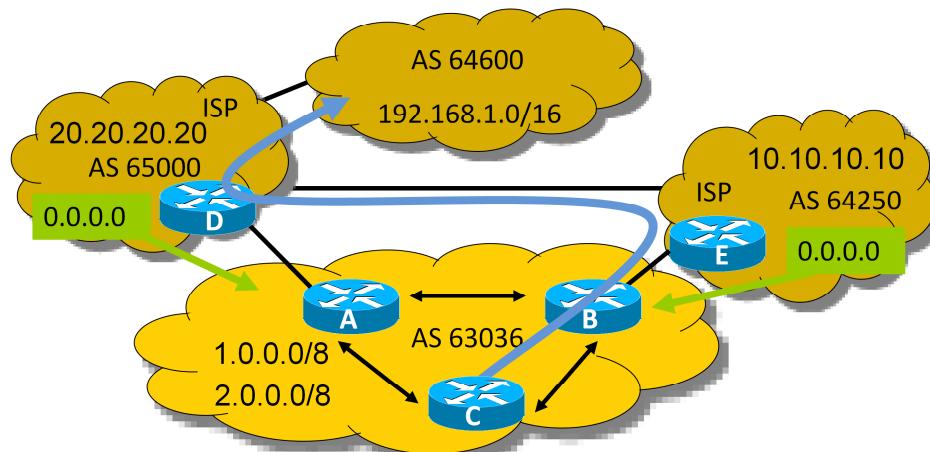
Aplicación:

```
neighbor 10.10.10.10 prefix-list DEFAULT in
```

Redundancia entre sistemas autónomos

Tráfico saliente de un sistema

A- Rutas por defecto de todos los proveedores (default routing)



C elige la menor métrica IGP de las rutas por defecto

Fuente: Curso BSCN de Cisco Systems

Configuración para recibir sólo rutas default:

```
router bgp 63036
network 1.0.0.0
network 2.0.0.0
neighbor 10.10.10.10 remote-as 64250
neighbor 10.10.10.10 route-map sololocal out
neighbor 10.10.10.10 prefix-list DEFAULT in
neighbor 20.20.20.20 remote-as 65000
neighbor 20.20.20.20 route-map sololocal out
neighbor 20.20.20.20 prefix-list DEFAULT in
```

#La siguiente prefix-list permite sólo actualizaciones de rutas default:

```
ip prefix-list DEFAULT seq 5 permit 0.0.0.0/0
```

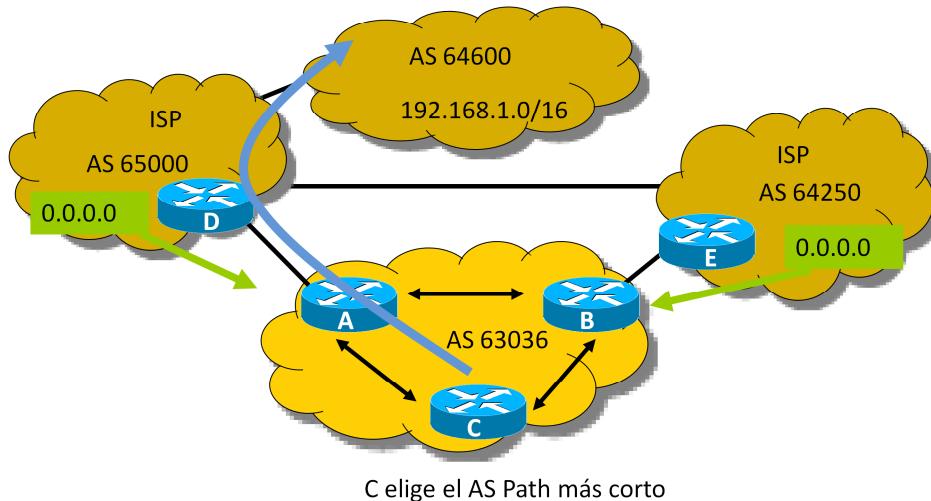
#La prefix-list se aplica a los neighbors de la siguiente manera:

```
neighbor 10.10.10.10 prefix-list DEFAULT in
neighbor 20.20.20.20 prefix-list DEFAULT in
```

Redundancia entre sistemas autónomos

Tráfico saliente de un sistema

B- Rutas por defecto y rutas de clientes de todos los proveedores (partial routing)



Fuente: Curso BSCN de Cisco Systems

Configuración para recibir sólo rutas directamente conectadas:

```
router bgp 300
network 1.0.0.0
network 2.0.0.0
neighbor 10.10.10.10 remote-as 100
neighbor 10.10.10.10 route-map sololocal out
neighbor 10.10.10.10 route-map soloas100 in
neighbor 20.20.20.20 remote-as 200
neighbor 20.20.20.20 route-map sololocal out
neighbor 20.20.20.20 route-map soloas200 in
```

#La siguiente lista y el siguiente route map permiten publicar sólo rutas originadas localmente

```
ip as-path access-list 10 permit ^$  
route-map sololocal permit 10  
match as-path 10
```

#La siguiente lista y el siguiente route map permiten aceptar sólo rutas originadas en el AS 100

```
ip as-path access-list 20 permit ^100$  
route-map soloas100 permit 10  
match as-path 20
```

#La siguiente lista y el siguiente route map permiten aceptar sólo rutas originadas en el AS 200

```
ip as-path access-list 30 permit ^200$  
route-map soloas200 permit 10  
match as-path 30
```

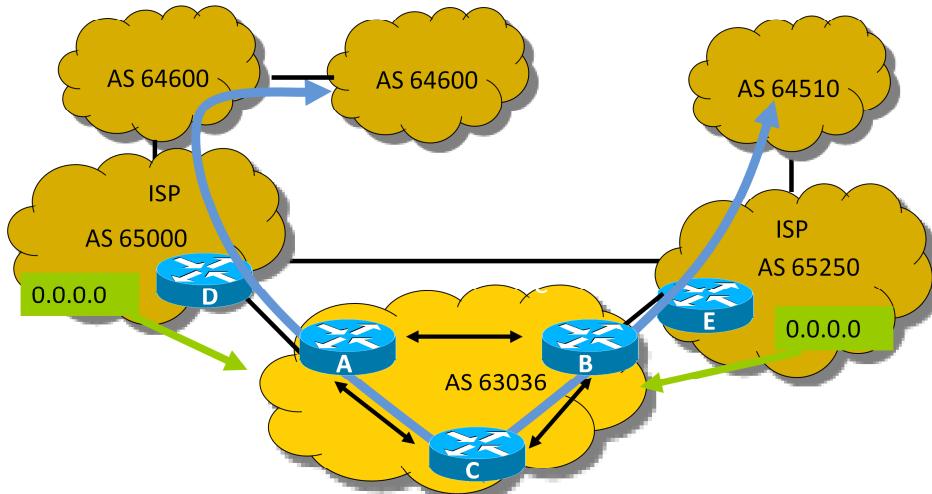
#Las siguientes rutas default apuntan a cada punto de ingreso de los service providers y se distribuyen en el resto de la red:

```
ip route 0.0.0.0 0.0.0.0 10.10.10.10  
ip route 0.0.0.0 0.0.0.0 20.20.20.20
```

Redundancia entre sistemas autónomos

Tráfico saliente de un sistema

C- Rutas completas de todos los proveedores (full routing)



Fuente: Curso BSCN de Cisco Systems

Configuración para recibir Full Routing Table:

```
router bgp 300
network 1.0.0.0
network 2.0.0.0
neighbor 10.10.10.10 remote-as 100
neighbor 10.10.10.10 route-map sololocal out
neighbor 20.20.20.20 remote-as 200
neighbor 20.20.20.20 route-map sololocal out
```

#La siguiente lista permite sólo rutas originadas localmente:

```
ip as-path access-list 10 permit ^$
```

#El siguiente route map permite publicar sólo rutas locales:

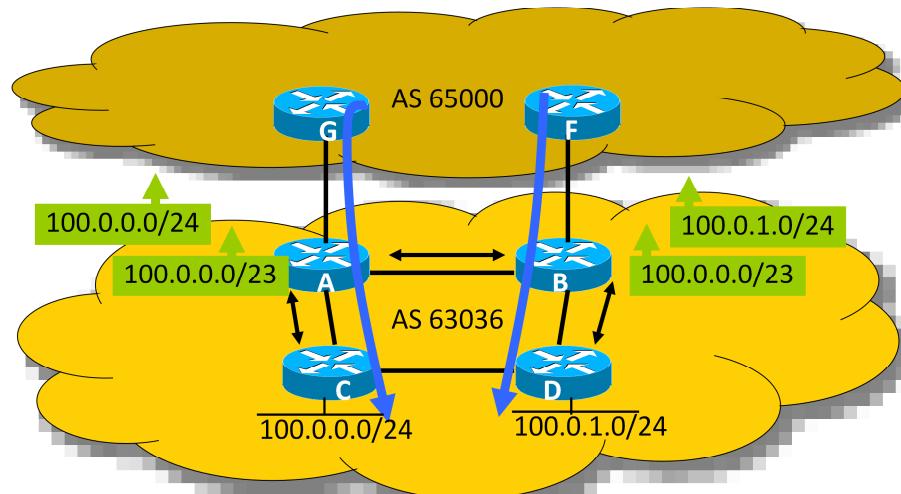
```
route-map sololocal permit 10
```

```
match as-path 10
```

Redundancia entre sistemas autónomos

Tráfico entrante a un sistema

Empleo de publicaciones de distinto grado de especificidad



Anuncios con redundancia

Si se desea que el tráfico a distintos destinos de una red tenga distintos puntos de ingreso, pero con posibilidad de redundancia en caso de fallos, se puede emplear el esquema de publicaciones siguiente. Por cada punto de ingreso se publican las rutas específicas a las cuales se desea que se dirija el tráfico entrante por ese punto. Además, por todos los puntos de ingreso se publica la sumarización de los bloques.

En condiciones normales, las rutas específicas primarán y el tráfico ingresará por los puntos deseados. En caso de fallo de un punto de ingreso, el tráfico que normalmente entra por dicho punto lo hará por los restantes, porque el bloque de direcciones específico ya no se publicará, pero está incluido en la sumarización que seguirá publicándose por los demás puntos.

Configuración para publicar bloques más y menos específicos:

```
router bgp 300
network 1.0.0.0 mask 255.255.255.0
network 2.0.0.0 mask 255.255.255.0
neighbor 10.10.10.10 remote-as 100
neighbor 10.10.10.10 prefix-list trafico_a_C out
neighbor 20.20.20.20 remote-as 200
neighbor 20.20.20.20 prefix-list trafico_a_D out
```

#La siguiente lista permite publicar una ruta específica de C y el bloque sumarizado:

```
ip prefix-list trafico_a_C seq 5 permit 100.0.0.0/24
ip prefix-list trafico_a_C seq 5 permit 100.0.0.0/23
```

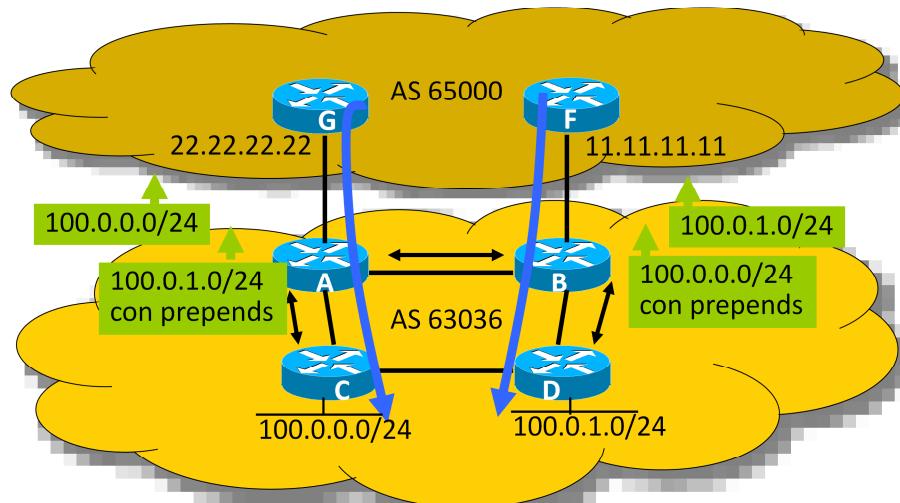
#La siguiente lista permite publicar una ruta específica de D y el bloque sumarizado:

```
ip prefix-list trafico_a_D seq 5 permit 100.0.1.0/24
ip prefix-list trafico_a_D seq 5 permit 100.0.0.0/23
```

Redundancia entre sistemas autónomos

Tráfico entrante a un sistema

Empleo de publicaciones con y sin prepends



Anuncios con redundancia

Otra posibilidad para publicar anuncios de modo de lograr reparto de carga con redundancia, consiste en el empleo de prepends.

Configuración para publicar bloques con y sin pepends:

```
router bgp 63036
network 100.0.0.0 mask 255.255.255.0
network 100.0.1.0 mask 255.255.255.0
neighbor 11.11.11.11 remote-as 65000
neighbor 11.11.11.11 route-map PrePENDs1 out
neighbor 22.22.22.22 remote-as 65000
neighbor 22.22.22.22 route-map PrePENDs2 out
```

#El siguiente route-map aplica prepends a uno de los rangos:

```
route-map PrePENDs1 permit 10
  match ip address 1
  set as-path prepend 63036 63036 63036
```

#El siguiente route-map aplica prepends al otro rango:

```
route-map PrePENDs2 permit 10
  match ip address 2
  set as-path prepend 63036 63036 63036
```

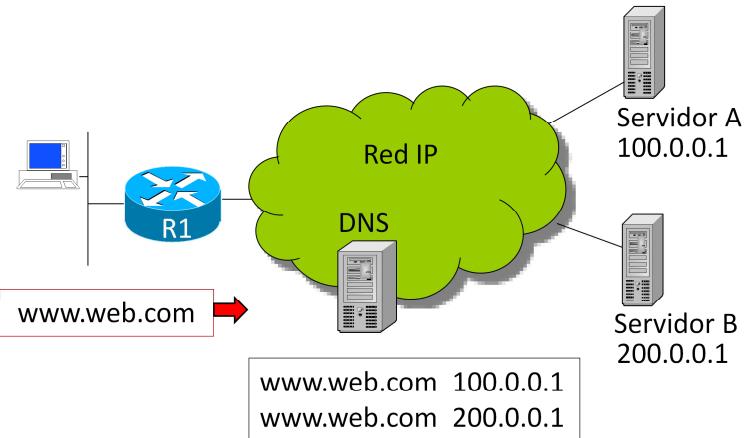
#Las siguientes listas de control de acceso especifican los rangos:

```
access-list 1 permit 100.0.0.0 0.0.0.255
access-list 2 permit 100.0.1.0 0.0.0.255
```

Redundancia en sistemas de servidores

Round Robin de DNS

Mecanismo



Round Robin de DNS

Consiste en tener más de un registro en DNS para un mismo nombre, de modo que cada uno devuelve una dirección IP diferente.

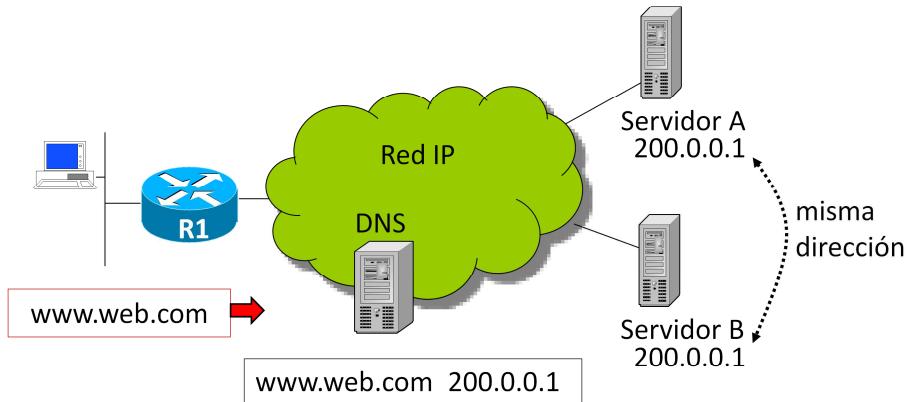
Ante una consulta de un cliente, el DNS devuelve la lista de registros que se corresponden con ese nombre, pero haciendo una permutación circular en cada respuesta, de modo de variar el orden de cada registro. El cliente intentará utilizar en primer lugar la primera opción de la lista, y sólo recurrirá a la siguiente si la primera falla. De ese modo, los sucesivos clientes tenderán a utilizar los posibles servidores repartiendo la carga entre ellos.

Como desventajas hay que tener en cuenta que si un servidor falla, el sistema DNS seguirá informando su dirección y los clientes seguirán intentando establecer contacto con él. Además, el comportamiento de los clientes al recibir la lista de direcciones no está estandarizada. El mecanismo en sí no asegura un balance de carga, sino que apenas intenta un reparto de la misma. Finalmente, si existen sistemas de caché de respuestas de DNS de por medio, la distribución de carga podrá ser desequilibrada, porque se tenderá a reiterar el uso de ciertas direcciones que se tienen en memoria.

Redundancia en sistemas de servidores

Anycast

Mecanismo



Anycast

Consiste en tener replicados los servidores con el mismo direccionamiento IP. De ese modo el cliente accederá al servidor por el camino de menor métrica en la red. Si un servidor falla, es necesario que la ruta al mismo deje de anunciararse. Eso se logra en general, implementando enrutamiento mediante el sistema operativo del servidor, y controlando las rutas que publica según la disponibilidad del servicio.

Una limitación del mecanismo es la falta de "persistencia", que consiste en la necesidad del cliente de seguir dialogando con el mismo servidor en caso de consultas en las cuales envíe más de un paquete. Si la red hiciera balance de carga, podría suceder que un paquete de solicitud de un cliente llegara a un servidor, y que el siguiente llegara a otro, que seguramente no entendería de qué se trata y descartaría ese paquete. Por esa razón, este mecanismo se emplea sólo para consultas que pueden resolverse con un solo paquete de solicitud, tal como suele suceder en servicios de DNS.

ANEXO

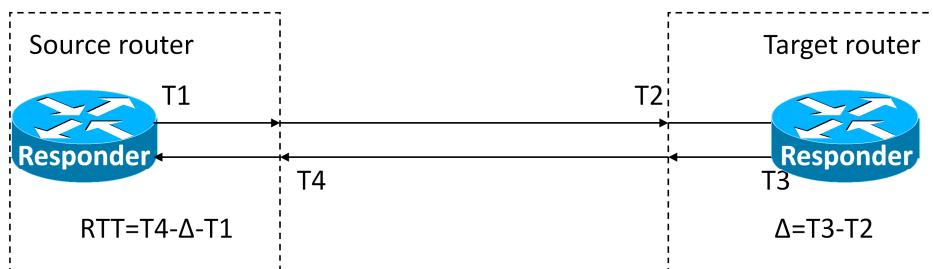
Redundancia

En WAN – Monitoreo e inicio de acciones mediante IP SLA

Funcionamiento

IP Service Level Agreement es un mecanismo que permite medir diversos parámetros de calidad, e iniciar acciones una vez que se supera cierto umbral predefinido.

Entre los parámetros se encuentran: conectividad, retardo, jitter, pérdida de paquetes, secuencia de paquetes, tiempo de descarga, Mean Opinion Score (medida de calidad de voz).



<http://www.cisco.com/application/pdf/paws/16563/12.pdf>

Medidas

IP SLA permite la medición de los siguientes parámetros:

- Retardo entre una solicitud y la correspondiente respuesta de servidores DHCP, DNS, HTTP, FTP, de respuesta a la solicitud de ICMP echo de extremo a extremo y salto a salto.
- Jitter en respuestas salto a salto a solicitudes de ICMP echo.
- Retardo de extremo a extremo en respuestas a solicitudes de UDP echo.
- Jitter, pérdida de paquetes y conectividad para tráfico UDP.
- Retardo en establecer una conexión TCP.
- Retardo en establecimiento de llamadas de VoIP.
- Retardos en registro de un gateway en un gatekeeper.

Monitoreo de nivel

IP SLA permite monitorear si un parámetro toma cierto estado o supera un cierto nivel predefinido, y ejecutar acciones cuando eso ocurre.

- Permite monitorear:
- Pérdida de conexión
- Temporizado
- RTT
- Jitter promedio
- Pérdida de paquetes en un sentido
- Jitter en un sentido
- Mean Opinion Score en un sentido
- Latencia en un sentido.

Redundancia

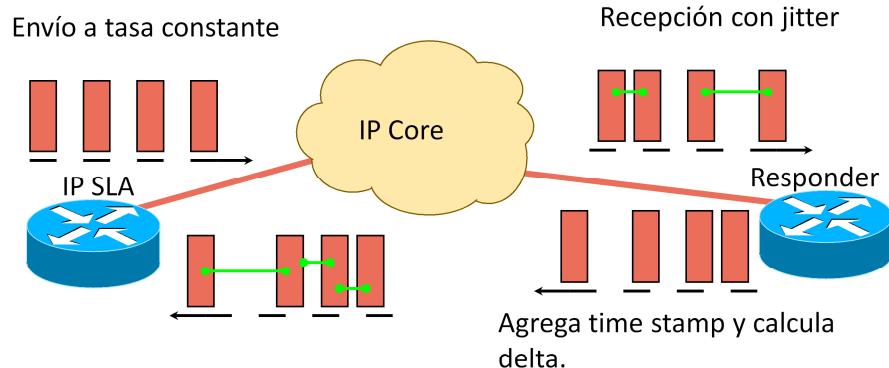
En WAN – Monitoreo e inicio de acciones mediante IP SLA

Mediciones

Per-direction inter-packet delay (Jitter)

Per-direction packet loss

Average Round Trip Delay



http://www.cisco.com/en/US/technologies/tk648/tk362/tk920/technologies_brief0900aec801e3602.ppt

Redundancia

En WAN – Monitoreo e inicio de acciones mediante IP SLA

Requerimientos según la aplicación

	*DATA TRAFFIC	*VoIP	*SERVICE LEVEL AGREEMENT	*AVAILABILITY	**STREAMING VIDEO
REQUIREMENT	<ul style="list-style-type: none"> Minimize Delay, Packet Loss Verify QoS 	<ul style="list-style-type: none"> Minimize Delay, Packet Loss, Jitter 	<ul style="list-style-type: none"> Measure Delay, Packet Loss, Jitter One-way 	Connectivity testing	<ul style="list-style-type: none"> Minimize Delay, Packet Loss
IP SLA MEASUREMENT	<ul style="list-style-type: none"> Jitter Packet loss Latency per QoS 	<ul style="list-style-type: none"> Jitter Packet loss Latency MOS Voice Quality Score 	<ul style="list-style-type: none"> Jitter Packet loss Latency One-way Enhanced accuracy NTP 	<ul style="list-style-type: none"> Connectivity tests to IP devices 	<ul style="list-style-type: none"> Jitter Packet loss Latency

http://www.cisco.com/en/US/technologies/tk648/tk362/tk920/technologies_brief0900aecdb801e3602.ppt

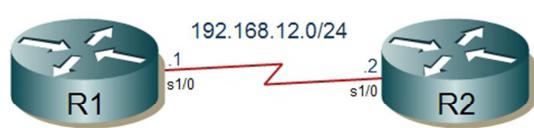
Redundancia

En WAN – Monitoreo e inicio de acciones mediante IP SLA

Ejemplo 1 de configuración

R1:

```
interface Serial1/0
ip address 192.168.12.1 255.255.255.0
!
ip route 2.2.2.2 255.255.255.255 Serial1/0
!
ip sla 1
icmp-echo 192.168.12.2
timeout 250
threshold 250
frequency 1
ip sla schedule 1 life forever start-time now
```



R2:

```
interface Loopback0
ip address 2.2.2.2 255.255.255.255
interface Serial1/0
ip address 192.168.12.2 255.255.255.0
```

<https://rekrowten.wordpress.com/2012/09/21/ip-sla-concepts-part-1/>

Redundancia

En WAN – Monitoreo e inicio de acciones mediante IP SLA

Ejemplo 2 de configuración

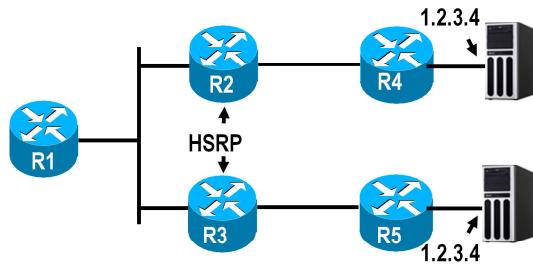
R1:

ip sla 2

http get url http://1.2.3.4

!

ip sla schedule 2 start-time now



<https://rekrowten.wordpress.com/2012/09/21/ip-sla-concepts-part-1/>

Redundancia en WAN - MPLS

Disponibilidad de la red

Protección vs Restauración.

- Protección: Se pre computa un camino alternativo antes de que la falla ocurra.
- Restauración: Se calcula un camino alternativo solamente luego de que una falla ocurra.

Recuperación Local vs Global.

- Local: el nodo encargado de redireccionar el trafico es el inmediato upstream de el punto de falla. La falla se maneja localmente.
- Global: Un nodo que puede estar a algo de distancia de la falla es el responsable en redireccionar el trafico (Es usualmente el extremo final PE). Gestiona la falla donde sea que ella ocurra a lo largo del LSP

Redundancia en WAN - MPLS

Protecciones

Capa física - óptica.

- Parcial o malla completa de sistema de switching óptico

Capa física - protocolo.

- Estrategias automáticas con protección por switching SONET/SDH

Capa IP.

- Algoritmos de convergencia del IGP.

Capa MPLS.

- MPLS TE Reroute
- MPLS TE Path Protection
- MPLS TE Fast Reroute

Redundancia en WAN - MPLS

TE Fast Reroute

Mecanismo local de protección.

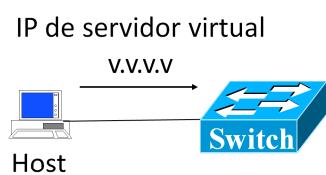
- El nodo es responsable por el rerruteo del tráfico, esto es llamado Point of Local Repair (PLR)
- Preseñalizan túneles de backup en cada nodo
- Los túneles de backup pueden ser establecidos manualmente o automáticamente
- Un simple túnel de backup puede proteger todos los LSPs afectados por una falla. O puede especificarse qué TE LSPs son los seleccionados para la protección Fast Reroute usando RSVP-TE.
- Túnel de backup de next hop (NH) protege contra fallas del link.
- Túnel de backup de next next hop (NNH) protege contra fallas del nodo
- Más amplios métodos de recuperación ante falla desarrollados.
- Provee tiempos de recuperación comparables con SDH si la falla del link se detecta rápidamente.

Redundancia en sistemas de servidores

Server Load Balancing

Topología

Los servidores reales "real 1, real2, ..." responden como un único servidor virtual accesible a través de la dirección v.v.v.v



Plataformas que lo soportan:
Catalyst 6000 Family Switches
Cisco 7200 Series Routers

Server Load Balancing

SLB permite repartir la carga de procesamiento en varios servidores, en lo que normalmente se llama "granja de servidores". Los usuarios (clientes) solicitan servicio a la dirección virtual , el switch envía la solicitud a uno de los servidores reales, y éste responde.

Redundancia en sistemas de servidores

Server Load Balancing

Algoritmos de balance de carga

Weighted Round Robin – A los servidores se les asignan conexiones en un modo circular. Cada servidor S_i tiene definido un peso n_i que representa su capacidad de aceptar conexiones en relación a los demás. En consecuencia, se le asignarán n_i conexiones antes de pasar al siguiente.

Weighted Least Connections – Cada servidor sigue teniendo definido un peso n_i . Su capacidad tope estará dada por $n_i/(n_1+n_2+n_3\dots)$. En el momento de asignar conexiones, se elegirá el servidor que esté más alejado de su tope de conexiones.

Port-Bound Servers

Funcionalidad que consiste en definir un conjunto de servidores reales que responden por un determinado servicio y por una dirección IP dada, otro conjunto de servidores reales que responden por otro servicio y la misma dirección IP anterior, etc.

Client-Assigned Load Balancing

Consiste en definir una lista de clientes que tienen permitido el acceso a un servidor virtual.

Sticky Connections

Esta funcionalidad permite que una conexión de un cliente sea atendida por el mismo servidor que atendió la anterior, siempre que no haya vencido el temporizado *sticky timer* entre conexiones.

Redundancia en sistemas de servidores

Server Load Balancing

Automatic Server Failure Detection

El sistema contabiliza la cantidad de sesiones TCP fallidas dirigidas a un servidor. Si superan el umbral *failure threshold* el servidor se considera caído y es removido de la lista de servidores activos.

Automatic Unfail

Cuando un servidor que ha sido removido de la lista de activos supera el umbral *retry timer* de tiempo de inactividad, es devuelto a la actividad y el sistema le envía nuevamente conexiones. Si la conexión es exitosa, el servidor es incorporado en la lista de servidores activos, de lo contrario, permanece inactivo por el tiempo del *retry timer*, luego de lo cual volverá a ser probado.

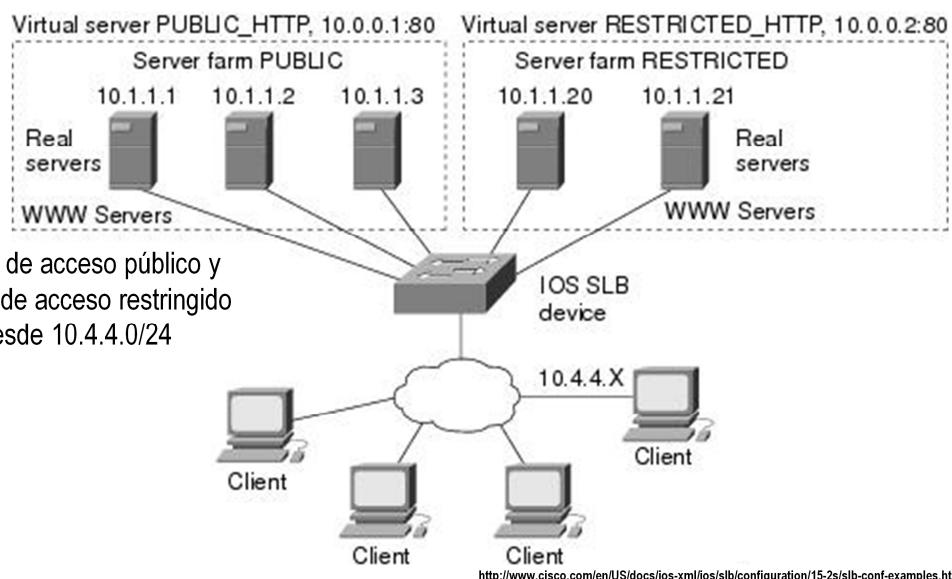
Stateless Backup

Puede tenerse redundancia para SLB mediante HSRP en switches de capa 3.

Redundancia

En sistemas de servidores – Server Load Balancing

Ejemplo de configuración



Configuración completa

```

ip slb probe PROBE2 http
request method POST url /probe.cgi?all
header HeaderName HeaderValue
!
ip slb serverfarm PUBLIC
nat server
real 10.1.1.1
reassign 4
faildetect numconns 16
retry 120
inservice
real 10.1.1.2
reassign 4
faildetect numconns 16
retry 120
inservice
probe PROBE2
!
ip slb serverfarm RESTRICTED
predictor leastconns
bindid 309
real 10.1.1.1
weight 32
maxconns 1000
reassign 4
faildetect numconns 16
retry 120
inservice
real 10.1.1.20
reassign 4
faildetect numconns 16
retry 120
inservice
real 10.1.1.21
reassign 4
faildetect numconns 16
retry 120
inservice
ip slb vserver PUBLIC_HTTP
virtual 10.0.0.1 tcp www
serverfarm PUBLIC
!
ip slb vserver RESTRICTED_HTTP
virtual 10.0.0.2 tcp www
serverfarm RESTRICTED
no advertise
sticky 60 group 1
idle 120
delay 5
client 10.4.4.0 255.255.255.0
synguard 3600000
inservice

```

Redundancia

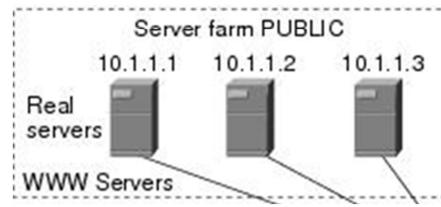
En sistemas de servidores – Server Load Balancing

Ejemplo de configuración - Server Farm Pública

```

ip slb serverfarm PUBLIC identificación de la "serverfarm"
real 10.1.1.1 dirección IP del servidor real
    reassign 2 intentos SYN antes de asignar a otro servidor
    faildetect numconns 4 numclients 2 cantidad de conexiones y clientes fallidos aceptables
    retry 20 lapso en segundos antes de un nuevo intento luego de un fallo
    inservice inclusión del servidor en la granja (por defecto no está incluido)
    exit
real 10.1.1.2
    reassign 2
    faildetect numconns 4
    retry 20
    inservice
    exit
real 10.1.1.3
    reassign 2
    faildetect numconns 4
    retry 20
    inservice
end

```



<http://www.cisco.com/en/US/docs/ios/slbtm/configuration/15.2/slbtm-conf-examples.html>

Redundancia

En sistemas de servidores – Server Load Balancing

Ejemplo de configuración - Server Farm Restringida

```
ip slb serverfarm RESTRICTED
real 10.1.1.20
    reassign 2
    faildetect numconns 4
    retry 20
    inservice
    exit
real 10.1.1.21
    reassign 2
    faildetect numconns 4
    retry 20
    inservice
end
```



<http://www.cisco.com/en/US/docs/ios/xml/ios/slb/configuration/15.2/slbt-conf-examples.html>

Redundancia

En sistemas de servidores – Server Load Balancing

Ejemplo de configuración - Virtual Servers

```
Virtual server PUBLIC_HTTP, 10.0.0.1:80
ip slb vserver PUBLIC_HTTP  definición del servidor virtual
    virtual 10.0.0.1 tcp www   dirección IP y servicio
    serverfarm PUBLIC      identificación de la granja para la que será servidor frontal
    idle 120               tolerancia de ausencia de tráfico en una conexión, antes de finalizarla con RST
    delay 5                tolerancia para el arribo de paquetes de una conexión que ya tuvo su fin en TCP
    inservice
    exit

Virtual server RESTRICTED_HTTP, 10.0.0.2:80
ip slb vserver RESTRICTED_HTTP
    virtual 10.0.0.2 tcp www
    serverfarm RESTRICTED
    idle 120
    delay 5
    inservice
    end
```

<http://www.cisco.com/en/US/docs/ios/ios/slbc/configuration/15.2/slbc-conf-examples.html>

Redundancia

En sistemas de servidores – Server Load Balancing

Ejemplo de configuración - Cliente Restringido

```
ip slb vserver RESTRICTED_HTTP
no inservice
client 10.4.4.0 255.255.255.0 restringe los clientes que pueden consultar al servidor
inservice
end
```



Ejemplo de configuración - Probe

```
ip slb probe PROBE2 http
request method POST url /probe.cgi?all
header HeaderName HeaderValue
```

definir el probe
definir el método de prueba
definir el encabezado http

<http://www.cisco.com/en/US/docs/ios/ios/slbtm/configuration/15.2/slbtm-conf-examples.html>

Redundancia

En sistemas de servidores – Server Load Balancing

Configuración completa

```

ip slb probe PROBE2 http
request method POST url /probe.cgi?all
header HeaderName HeaderValue
!
ip slb serverfarm PUBLIC
nat server
real 10.1.1.1
reassign 4
faildetect numconns 16
retry 120
inservice
real 10.1.1.2
reassign 4
faildetect numconns 16
retry 120
inservice
probe PROBE2

ip slb serverfarm RESTRICTED
predictor leastconns
bindid 309
real 10.1.1.1
weight 32
maxconns 1000
reassign 4
faildetect numconns 16
retry 120
inservice
real 10.1.1.20
reassign 4
faildetect numconns 16
retry 120
inservice
real 10.1.1.21
reassign 4
faildetect numconns 16
retry 120
inservice

ip slb vserver PUBLIC_HTTP
virtual 10.0.0.1 tcp www
serverfarm PUBLIC
!
ip slb vserver RESTRICTED_HTTP
virtual 10.0.0.2 tcp www
serverfarm RESTRICTED
no advertise
sticky 60 group 1
idle 120
delay 5
client 10.4.4.0 255.255.255.0
synguard 3600000
inservice

```

<http://www.cisco.com/en/US/docs/ios/ios/slbtm/configuration/15.2/slbtm-conf-examples.html>

Cuestionario

- 1- Cuál es la finalidad de HSRP y qué se configura en los routers y en los hosts?
- 2- Cómo se puede lograr en HSRP el relevo del router activo cuando cae una interfaz de salida del tráfico?
- 3- Cómo puede hacerse balance de carga con HSRP?
- 4- Qué diferencias presenta VRRP respecto de HSRP?
- 5- Qué variantes incorpora GLBP respecto de HSRP?
- 6- Qué es una ruta flotante y cómo se emplea en el caso de respaldar Frame Relay con RDSI?
- 7- En qué consiste IP SLA, qué mediciones puede efectuar, y cuál es su utilidad?
- 8- Qué diferencia hay entre protección y restauración de un LSP?
- 9- Qué diferencia hay entre una recuperación local y una global?
- 10- Qué alternativas de redundancia se prevén en MPLS?
- 11- Cómo se emplean las etiquetas en la redundancia “link protection” de MPLS?
- 12- Qué alternativas de enrutamiento se tienen para el tráfico saliente de un sistema autónomo?
- 13- Cómo puede encaminarse selectivamente el tráfico entrante según el destino, conservando la posibilidad de redundancia?
- 14- Cómo puede hacerse balance de carga para el tráfico saliente de un sistema autónomo?
- 15- Cómo se implementa redundancia mediante round robin de DNS, y cuáles son sus limitaciones?
- 16- En qué consiste el empleo de “anycast” para redundancia de servidores, y en qué casos no puede emplearse y por qué?
- 17- En qué consiste la funcionalidad de “Server Load Balancing”? Qué algoritmos y funciones soporta?

Investigación

En qué consisten las técnicas de “cluster” de servidores?

Análisis y discusión

Las técnicas de redundancia de red y de servidores, son excluyentes? Sustituye una a la otra? Argumentar.