**REDUNDANCIA DE GATEWAY**

Nuestras redes requieren un nivel de disponibilidad cada vez más elevado, y en lo posible descartar completamente la posibilidad de interrupciones de servicio. Es por esto que la redundancia es una herramienta recurrente. Redundancia en el suministro de energía, redundancia en capa 2, redundancia en capa 3, redundancia en el gateway.

Protocolos de administración dinámica del Gateway

**HSRP - HOT STANDBY ROUTER PROTOCOL**

Protocolo propietario de Cisco

Utiliza una IP virtual y define automáticamente una MAC virtual para el clúster.

Entre los routers asociados al router virtual define un router activo y otro de backup.

No realiza balanceo de tráfico, solo un gateway permanece activo mientras los demás están es espera.

La alta disponibilidad en HSRP se logra compartiendo una misma dirección IP virtual entre dos o más Router. En la configuración del protocolo HSRP tenemos dos tipos de Router: el Router Activo y el Router Pasivo. El Router Activo es aquel que atiende permanentemente las peticiones que se realizan a la dirección IP Virtual. En caso que el Router Activo falle, entonces el Router Pasivo adquiere el rol del Router Activo y comienza atender las peticiones enviadas a la dirección IP Virtual.

En términos prácticos, el objetivo de HSRP es permitir que nuestros paquetes IP sigan encaminándose a través de la red WAN aun cuando el Default Gateway haya sufrido una avería, sea de hardware o software,

El procedimiento para configurar HSRP en Cisco IOS es el siguiente:

Entra al modo de configuración Global

RouterA#configure terminal

Entra a la interface f0/0

RouterA(config)#interface f0/0

Configuración de dirección IP a la interface física

RouterA(config-if)#ip address 10.0.0.1

Configuración de dirección IP virtual

RouterA(config-if)#standby 1 ip 10.0.0.3

Configuración de la prioridad en HSRP

RouterA(config-if)#standby 1 priority 200

Entra a la interface f0/0

RouterB#configure terminal

Entra a la interface f0/0

RouterB(config)#interface f0/0

Configuración de dirección IP a la interface física

RouterB(config-if)#ip address 10.0.0.2

Configuración de dirección IP virtual

RouterB(config-if)#standby 1 ip 10.0.0.3

Para imprimir en pantalla el status de HSRP ejecutamos el siguiente comando:

RouterA#show standby

Ethernet0 – Group 1

Local state is Standby, priority 100

Hellotime 3 sec, holdtime 10 sec

Next hello sent in 0.776

Virtual IP address is 10.0.0.3 configured

Active router is local

Standby router is 10.0.0.2, priority 200 expires in 9.568

1 state changes, last state change 00:00:22

RouterB#show standby

Ethernet0 – Group 1

Local state is Standby, priority 100

Hellotime 3 sec, holdtime 10 sec

Next hello sent in 0.776

Virtual IP address is 10.0.0.3 configured

Standby router is local

Active router is 10.0.0.1, priority 100 expires in 9.568

1 state changes, last state change 00:00:22

La prioridad por defecto en HSRP es 100. Si ambos Router tienen la misma prioridad, aquel que suba primero será el Router Activo. Si queremos influir en la toma de decisión sobre quién será el Router Activo utilizamos el comando standby 1 priority.

Así de sencillo es la configuración HSRP en un Cisco Router.

**GLBP - GATEWAY LOAD BALANCING PROTOCOL**

Protocolo propietario de Cisco.

Utiliza una única IP virtual y múltiples direcciones MAC virtuales (una por cada dispositivo que integra el clúster).

Sólo un dispositivo actúa como máster y responde las solicitudes ARP, pero todos permanecen activos y reenvían el tráfico que está dirigido a la dirección MAC virtual que les ha sido asignada.

El reenvío de tráfico es realizado por cada uno de los routers del clúster de acuerdo a la dirección MAC virtual a la cual es enviado el tráfico por la terminal

**Descripción de GLBP**

Con el fin de mejorar las capacidades del Protocolo de enrutador Hot Standby (HSRP), Cisco desarrolló GLBP. GLBP proporciona un equilibrio automático de la carga de la puerta de enlace del primer salto, que permite un uso más eficiente de los recursos y reduce los costos administrativos. Es una extensión de HSRP y especifica un protocolo que asigna dinámicamente la responsabilidad de una dirección IP virtual y distribuye múltiples direcciones MAC virtuales a los miembros de un grupo GLBP.

En las redes del campus, las interfaces VLAN de Capa 3 actúan como la puerta de enlace para los hosts. Estas interfaces VLAN de Capa 3 de diferentes conmutadores se equilibran con la carga utilizando GLBP. Las interfaces de capa 3 de varios conmutadores forman un grupo GLBP. Cada grupo contiene una dirección IP virtual única.

Supervisor 720 puede tener un máximo de 1024 grupos de GLBP (números de grupo 0 a 1023). Supervisor 2 admite solo un grupo de GLBP. Un grupo de GLBP puede tener un máximo de 4 miembros. Esto significa que GLBP puede cargar hasta 4 puertas de enlace.

Los miembros de GLBP tienen dos roles:

Puerta de enlace virtual: asigna direcciones MAC virtuales a los miembros.

Reenviador virtual: reenvía datos para el tráfico destinado a la dirección MAC virtual

**Puerta de enlace virtual**

Un miembro de un grupo puede estar en cualquiera de estos estados: activo, en espera o escuchando. Los miembros de un grupo GLBP eligen que una puerta de enlace sea la puerta de enlace virtual activa (AVG) para ese grupo. También elige a un miembro como Standby Virtual Gateway (SVG). Si hay más de dos miembros, entonces los miembros que permanecen están en el estado de escucha.

Si un AVG falla, el SVG asume la responsabilidad de la dirección IP virtual. Luego se elige un nuevo SVG de las puertas de enlace en el estado de escucha. Si el AVG fallido o el nuevo miembro con un número de prioridad más alto se conecta, no se anulará de forma predeterminada. Puede configurar los interruptores para que pueda adelantarse.

La función de la AVG es que asigna una dirección MAC virtual a cada miembro del grupo GLBP. Recuerde que en HSRP solo hay una dirección MAC virtual para la dirección IP virtual. Sin embargo, en GLBP a cada miembro se le asigna una dirección MAC virtual. AVG se encarga de la asignación de la dirección MAC virtual.

Nota: como GLBP admite un máximo de 4 miembros para un grupo, AVG puede asignar solo un máximo de 4 direcciones MAC.

**Reenviador Virtual**

AVG asigna direcciones MAC virtuales a cada miembro en secuencia. El miembro se llama Primary Virtual Forwarder (PVF) o Active Virtual Forwarder (AVF) si la dirección MAC es asignada directamente por AVG. El mismo miembro es el reenviador virtual secundario (SVF) para las direcciones MAC asignadas a otros miembros. PVF está en estado activo y SVF está en estado de escucha.

En resumen, para un grupo GLBP de 4 miembros, cada miembro es PVF para una dirección MAC y SVF para otras tres direcciones MAC.

Si el PVF para una dirección MAC virtual falla, cualquiera de los SVF asume la responsabilidad de esa dirección MAC virtual. En este momento, ese miembro es PVF para 2 direcciones MAC virtuales (una asignada por AVG y la otra toma el control del miembro fallido). El esquema preventivo del reenviador virtual está habilitado de forma predeterminada. Recuerde que el esquema preventivo para la puerta de enlace virtual no está habilitado de forma predeterminada, pero el esquema preventivo para el Reenviador virtual está habilitado de forma predeterminada.

Para eliminar un AVF correctamente, use el comando de redireccionar temporizadores en los otros AVF para que cuando se elimine el AVF actual, el AVF secundario tome el control sin causar ninguna pérdida de paquetes en el enlace.

De manera predeterminada, GLBP usa temporizadores incorporados para detectar la presencia de un AVF basado en el cual continúa proporcionando el MAC virtual alineado con el AVF. Cuando el AVF se apaga, el proceso de GLBP espera un tiempo específico después del cual declara que el AVF ya no está disponible. Luego comienza a propagar el mismo MAC virtual que lo enlaza con otros AVF disponibles. El valor predeterminado para este temporizador es de 300 segundos. Esto se puede reducir para aprovechar mejor la situación y hacer un cambio rápido.

Para configurar el tiempo entre los paquetes de saludo enviados por la puerta de enlace GLBP y el momento en que la información de la puerta de enlace virtual y del reenviador virtual se considera válida, use el comando de tiempo de espera de glbp group [ msec ] hellotime [ msec ] en el modo de configuración de la interfaz.

**Limitación**

Cisco Non-Stop Forwarding (NSF) con cambio de estado (SSO) tiene una restricción con GLBP. El SSO no es compatible con GLBP, lo que significa que la información del estado de GLBP no se mantiene entre el motor supervisor activo y en espera durante el funcionamiento normal. GLBP y SSO pueden coexistir, pero ambas características funcionan de forma independiente. El tráfico que se basa en GLBP puede cambiar al modo de espera de GLBP en caso de un cambio de supervisor.

**Beneficios de GLBP**

Compartiendo carga

Puede configurar GLBP de tal manera que el tráfico de los clientes de LAN pueda ser compartido por múltiples enrutadores, compartiendo así la carga de tráfico de manera más equitativa entre los enrutadores disponibles.

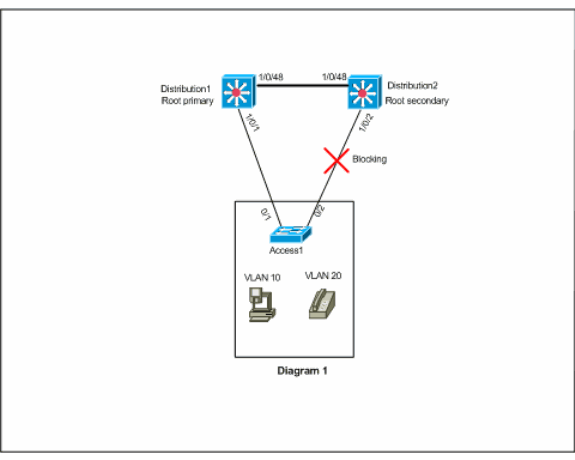
Enrutadores virtuales múltiples GLBP admite hasta 1024 enrutadores virtuales (grupos GLBP) en cada interfaz física de un enrutador, y hasta 4 reenviadores virtuales por grupo.

**Derecho preferente de compra**

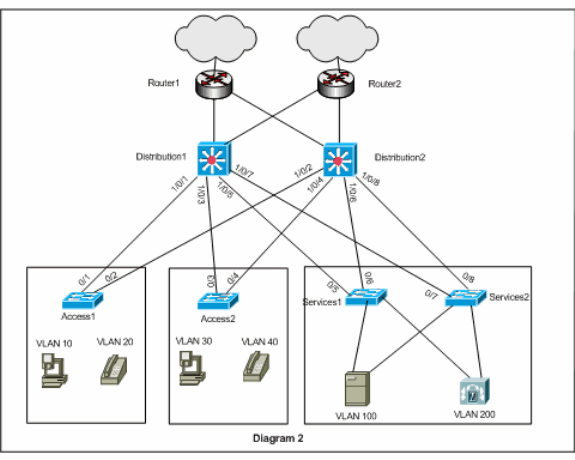
El esquema de redundancia de GLBP le permite anticiparse a una pasarela virtual activa con una pasarela virtual de respaldo de mayor prioridad que está disponible. La preferencia de reenviador funciona de una manera similar, excepto que la preferencia de reenvío utiliza la ponderación en lugar de la prioridad y está habilitada de forma predeterminada.

**Autenticación**

Puede usar un esquema de autenticación de contraseña de texto simple entre los miembros del grupo GLBP para detectar errores de configuración. Un enrutador dentro de un grupo GLBP con una cadena de autenticación diferente a la de otros enrutadores será ignorado por otros miembros del grupo



|  |
| --- |
| Distribution1 |
| Distribution1(config)#interface vlan 10  Distribution1(config-if)#ip address 172.18.10.2 255.255.255.0  Distribution1(config-if)#glbp 10 priority 110  Distribution1(config-if)#glbp 10 preempt  Distribution1(config-if)#glbp 10 authentication md5 key-string s!a863  Distribution1(config-if)#glbp 10 ip 172.18.10.1  Distribution1(config-if)#exit  Distribution1(config)#interface vlan 20  Distribution1(config-if)#ip address 172.18.20.2 255.255.255.0  Distribution1(config-if)#glbp 20 priority 110  Distribution1(config-if)#glbp 20 preempt  Distribution1(config-if)#glbp 20 authentication md5 key-string s!a863  Distribution1(config-if)#glbp 20 ip 172.18.20.1  Distribution1(config-if)#exit  Distribution1(config)#interface vlan 30  Distribution1(config-if)#ip address 172.18.30.2 255.255.255.0  Distribution1(config-if)#glbp 30 priority 110  Distribution1(config-if)#glbp 30 preempt  Distribution1(config-if)#glbp 30 authentication md5 key-string s!a863  Distribution1(config-if)#glbp 30 ip 172.18.30.1  Distribution1(config-if)#exit  Distribution1(config)#interface vlan 40  Distribution1(config-if)#ip address 172.18.40.2 255.255.255.0  Distribution1(config-if)#glbp 40 priority 110  Distribution1(config-if)#glbp 40 preempt  Distribution1(config-if)#glbp 40 authentication md5 key-string s!a863  Distribution1(config-if)#glbp 40 ip 172.18.40.1  Distribution1(config-if)#exit  Distribution1(config)#interface vlan 100  Distribution1(config-if)#ip address 172.18.100.2 255.255.255.0  Distribution1(config-if)#glbp 100 priority 110  Distribution1(config-if)#glbp 100 preempt  Distribution1(config-if)#glbp 100 authentication md5 key-string s!a863  Distribution1(config-if)#glbp 100 ip 172.18.100.1  Distribution1(config-if)#exit  Distribution1(config)#interface vlan 200  Distribution1(config-if)#ip address 172.18.200.2 255.255.255.0  Distribution1(config-if)#glbp 200 priority 110  Distribution1(config-if)#glbp 200 preempt  Distribution1(config-if)#glbp 200 authentication md5 key-string s!a863  Distribution1(config-if)#glbp 200 ip 172.18.200.1  Distribution1(config-if)#exit |



|  |
| --- |
| Distribution2 |
| Distribution2(config)#interface vlan 10  Distribution2(config-if)#ip address 172.18.10.3 255.255.255.0  Distribution2(config-if)#glbp 10 authentication md5 key-string s!a863  Distribution2(config-if)#glbp 10 ip 172.18.10.1  Distribution2(config-if)#exit  Distribution2(config)#interface vlan 20  Distribution2(config-if)#ip address 172.18.20.3 255.255.255.0  Distribution2(config-if)#glbp 20 authentication md5 key-string s!a863  Distribution2(config-if)#glbp 20 ip 172.18.20.1  Distribution2(config-if)#exit  Distribution2(config)#interface vlan 30  Distribution2(config-if)#ip address 172.18.30.3 255.255.255.0  Distribution2(config-if)#glbp 30 authentication md5 key-string s!a863  Distribution2(config-if)#glbp 30 ip 172.18.30.1  Distribution2(config-if)#exit  Distribution2(config)#interface vlan 40  Distribution2(config-if)#ip address 172.18.40.3 255.255.255.0  Distribution2(config-if)#glbp 40 authentication md5 key-string s!a863  Distribution2(config-if)#glbp 40 ip 172.18.40.1  Distribution2(config-if)#exit  Distribution2(config)#interface vlan 100  Distribution2(config-if)#ip address 172.18.100.3 255.255.255.0  Distribution2(config-if)#glbp 100 authentication md5 key-string s!a863  Distribution2(config-if)#glbp 100 ip 172.18.100.1  Distribution2(config-if)#exit  Distribution2(config)#interface vlan 200  Distribution2(config-if)#ip address 172.18.200.3 255.255.255.0  Distribution2(config-if)#glbp 200 authentication md5 key-string s!a863  Distribution2(config-if)#glbp 200 ip 172.18.200.1  Distribution2(config-if)#exit |

**SEGURIDAD DE PUERTO EN SWITCHES CISCO**

Con el objetivo de incrementar la seguridad en una red LAN es posible implementar seguridad de puertos en los switches de capa de acceso, de manera de permitir que a cada puerto se conecte sólo la estación autorizada. Para ello Cisco provee port security, un mecanismo bastante potente y sencillo que resumiré a continuación.

Dirección MAC segura estática

Se configura manualmente.

Se agrega a la tabla de direcciones MAC.

Se guarda en la running-config.

Se puede hacer permanente guardando la configuración.

SwA(config-if)# switchport port-security mac-address DIRECCION-MAC

Dirección MAC segura dinámica

Se aprende del tráfico que atraviesa la interfaz.

Se la guarda en la tabla de direcciones MAC.

Se pierde cuando se reinicia el equipo.

SwA(config-if)# switchport port-security

Dirección MAC segura sticky

Se la puede configurar de forma manual o dinámica.

Se la guarda en la tabla de direcciones MAC.

Se almacena en la running-config.

Se puede hacer permanente guardando la configuración.

SwA(config-if)# switchport port-security mac-address sticky [DIRECCION-MAC]

La principal ventaja de las direcciones sticky en contraposición con las dinámicas es que éstas últimas se agregan a la running-config. Así nos evitamos escribir un montón de direcciones MAC de manera estática pero aún podemos guardarlas en el archivo de configuración de manera que se mantengan inclusive si el switch se reinicia.

Dos aspectos importantes a tener en cuenta:

Si se habilitan las direcciones MAC sticky y ya había direcciones aprendidas de forma dinámica, éstas pasan a la running-config y todas las nuevas que se aprendan también se agregan allí.

Si se deshabilitan las direcciones MAC sticky todas las que hubiera pasan a ser dinámicas y se borran de la running-config. Además, todas las que se aprendan también serán dinámicas.

Acciones a tomar si se produce una violación

Es importante tener en cuenta que por violación se entiende uno de los siguientes dos casos:

Se alcanzó la cantidad máxima de direcciones MAC permitidas.

Una dirección MAC que se aprendió en un puerto se aprende por otro puerto diferente.

Los modos en los que se puede establecer un puerto para decidir qué acción tomar en el caso de una violación son, entonces:

Protect: una vez que se alcanzó el máximo de direcciones MAC en un puerto, todo el tráfico de orígenes desconocidos (es decir, de direcciones MAC que no sean válidas para ese puerto) es descartado. No obstante, se continúa enviando el tráfico legal normalmente. No se notifica al administrador de esta situación.

Restrict: el mismo comportamiento que el caso anterior pero con la diferencia que se envía un aviso al administrador mediante SNMP, se registra el evento en el syslog y se incrementa el contador de violaciones.

Shutdown: en este caso el puerto se da de baja dejándolo en estado err-disabled (deshabilitado por error). Además se envía un aviso al administrador mediante SNMP, se registra el evento en el syslog y se incrementa el contador de violaciones.

Shutdown VLAN: la única diferencia con el caso anterior es que se deshabilita la VLAN en ese puerto en lugar de dar de baja el puerto completo. Es particularmente atractivo para los puertos de trunk.

**Configuración**

Para configurar port-security es importante saber que la interfaz debe estar en modo access o en modo trunk. Port-security no puede habilitarse en una interfaz que esté en modo dinámico.

Habilitar port-security.

SwA(config-if)# switchport port-security

Indicar que sólo se permite una MAC por interfaz.

SwA(config-if)# switchport port-security maximum 1

Configurar el modo restrict para cuando ocurra una violación del puerto.

SwA(config-if)# switchport port-security violation restrict

Configurar el aprendizaje de direcciones MAC sticky.

SwA(config-if)# switchport port-security mac-address sticky

O bien especificar una MAC de forma estática.

SwA(config-if)# switchport port-security mac-address 5400.0000.0001

Chequear el estado de port-security.

SwA# show port-security