Carlos González Perez



Redes Datos CISCO

1. ***Diagnosticar errores en una interfaz***

La mayoría de los switches tienen alguna forma de rastrear los paquetes y los errores que se producen en un puerto o interfaz

Excesivos errores en algunos contadores suelen indicar un problema.

Cuando se opera en half-duplex, algunos errores de enlace de datos incrementando en Frame Check Sequence (FCS), alineación, runts, y los contadores de colisión son normales. En general, una relación de los errores uno por ciento del tráfico total es aceptable para las conexiones half-duplex. Si la relación de errores de paquetes de entrada es mayor que dos o tres por ciento, la degradación del rendimiento puede ser notable.

Cuando se opera en  full-duplex, errores de FCS, CRC, alineación, y los contadores runt deben ser mínimos. Si el enlace funciona a full-duplex, el contador de colisiones no estará activo. Si hay incremento de FCS, CRC, alineación, o contadores runt, se debe comprobar si hay un desajuste de duplex (duplex mistmatch)  o velocidad.

Se debe asegurar que ambos equipos enlazados estén configurados de la misma forma.

Tipos de contadores:

* Errores de CRC: indican que la suma de la comprobación de redundancia cíclica generada por el dispositivo de LAN de origen no coincide con la suma de comprobación calculada a partir de los datos recibidos. En una LAN, esto suele indicar ruido o problemas de transmisión en la interfaz LAN o el bus LAN sí mismo. Un alto número de CRC es generalmente el resultado de colisiones o bien un problema físico en donde es requerido un remplazo.
* Giants: se definen como cualquier trama sobre el tamaño máximo de una trama de Ethernet (mayor que 1518 bytes) y que tiene una mala FCS.
* FCS (Frame Check Sequence): es un conjunto de bits adjuntos al final de la trama Ethernet utilizado para verificar la integridad de la información recibida mediante una "secuencia" de verificación de trama incorrecta, también conocido como CRC o checksum.
* Runts: son los paquetes Ethernet que son menos de 64 bytes y puede ser causados por las colisiones excesivas.

Pueden ser causados por un desajuste duplex y problemas físicos, como un mal cable, puerto o NIC en el dispositivo conectado.

* Errores de alineación (Alignment): son un recuento del número de tramas recibidas que no terminan con un número par de octetos y tienen una mala comprobación de redundancia cíclica (CRC).

Generalmente son el resultado de un desajuste duplex o un problema físico (como el cableado, un puerto malo, o NIC malo). Cuando el cable se conecta por primera vez al puerto, algunos de estos errores pueden ocurrir. Además, si hay un HUB conectado al puerto, las colisiones entre los otros dispositivos y el HUB pueden causar estos errores.

Ejemplo de una interfaz con problemas.

30295 runts, 7 giants, 0 throttles

0 parity

35143 input errors, 436 CRC, 0 frame, 0 overrun, 0 ignored, 4405 abort

Ejemplo de algunos comandos a usar:

-show interfaces fastEthernet 6/1

-show interfaces fast 6/1 status

-sh interfaces fastEthernet 6/1 counters errors

1. **Listado comandos para extraer información**

* Show Interfaces

Despliega las estadísticas completas de todas las interfaces del router:

Router# show interfaces

* Show interface serial

Despliega la información de esta interfaz serial:

Router# show interface serial 0/0/0

* Show ip interface brief

Despliega un resumen de todas las interfaces incluyendo el estado y la dirección IP

Router# show ip interface brief

* Show controllers nombre\_interfaz

Despliega las estadísticas del hardware de una interfaz (información de si el cable es DTE o DCE):

Router# show controllers nombre\_interfaz

* Show clock

Despliega la hora del router:

Router# show clock

* Show history

Despliega el historial de comandos utilizados:

Router# show history

* Show flash

Despliega información acerca de la memoria flash y los archivos IOS que se encuentran almacenados en ella:

Router# show flash

* Show version

Despliega la información acerca del router y de la imagen de IOS que esté corriendo en la memoria RAM, también muestra el valor del registro de configuración del router:

Router# show version

* Show arp

Despliega la tabla ARP del router:

Router# show arp

* Show protocols

Despliega los protocolos de capa 3 configurados:

Router# show protocols

* Show startup-config

Despliega la configuración grabada en la NVRAM:

Router# show startup-config

* Show running-config

Despliega la configuración que se encuentra actualmente corriendo en la memoria RAM:

Router# show running-config

* Show hosts

Despliega la lista en caché de los nombres de host y sus direcciones:

Router# show hosts

* Show users

Despliega todos los usuarios conectados al router:

Router# show users

* Show ip route

Despliega la tabla de enrutamiento del router:

Router# show ip route

La tabla de enrutamiento es la lista de todas las redes que el dispositivo puede alcanzar, su métrica, y la forma en que accede a ellas.

* Show ip route summary

Despliega el resumen de la tabla de enrutamiento del router:

Router# show ip route summary

* Show ip traffic

Despliega las estadísticas del tráfico IP en el router:

Router# show ip traffic

* Show access-list

Despliega las listas de acceso configuradas y el número de hits que cada línea ha recibido, de este modo podemos hacer un mejor debug de cualquier problema con las listas de acceso:

Router# show access-list

* Show cdp neighbors

Despliega un reporte de todos los dispositivos Cisco al que estamos conectados:

Router# show cdp neighbors

* Show cdp neightbors detail

Despliega un reporte detallado de todos los dispositivos Cisco al que estamos conectados:

Router# show cdp neighbors detail

* Show inventory

Despliega el inventario de tarjetas:

Router# show inventory

* Show processes

Despliega los procesos activos:

Router# show processes

* Show sessions

Despliega las conexiones Telnet establecidas en el router:

Router# show sessions

* Show memory

Despliega las estadísticas de memoria del router:

Router# show memory

* Show tech-support

Despliega la información completa del sistema:

Router# show tech-support

* Show ip rip database

Despliega la información del protocolo de rute RIP:

Router# show ip rip database

* Show ip eigrp topology

Despliega las rutas aprendidas con el protocolo eigrp:

Router# show ip eigrp topology

* Show vlan

Despliega la lista de vlans existentes en el switch:

Switch# show vlan

* Show vlan-membership

Despliega la lista de vlans y las interfaces asignadas a cada vlan:

Switch# show vlan-membership

* Show mac-address-table

Despliega la información de la tabla de direcciones mac:

Switch# show mac-address-table

* show spanning-tree

Despliega la información del protocolo spannig-tree:

Switch# show spanning-tree

* Show boot

Muestra el archivo de boot:

Switch# show boot

1. **Recuperacion de contraseña switch Catalyst**

* Conectar el cable de consola (cable azul) al puerto de consola del switch.
* Por medio de un emulador de terminal (Hyperterminal) verificar que la contraseña conocida no permita el acceso a la configuración.
* Apagar el switch.
* Encender el switch y dejar presionado el botón “Mode”.
* Soltar el botón cuando el puerto 1x se apague.
* En el emulador de terminal deberá aparecer:

*The system has been interrupted prior to initializing the flash file system to finish*

*loading the operating system software:*

*flash\_init*

*load\_helper*

*boot*

*switch:*

*Teclear el comando “flash\_init”*

*switch: flash\_init*

*Initializing Flash...*

*flashfs[0]: 143 files, 4 directories*

*flashfs[0]: 0 orphaned files, 0 orphaned directories*

*flashfs[0]: Total bytes: 3612672*

*flashfs[0]: Bytes used: 2729472*

*flashfs[0]: Bytes available: 883200*

*flashfs[0]: flashfs fsck took 86 seconds*

*....done Initializing Flash.*

*Boot Sector Filesystem (bs:) installed, fsid: 3*

*Parameter Block Filesystem (pb:) installed, fsid: 4*

*switch:*

* Después teclear “load\_helper”

*switch: load\_helper*

* Ahora ejecutar “dir flash:”

*switch: dir flash:*

*Directory of flash:/*

*-rwx 1803357 <date> c29xx.xxx.x.x.x.x.bin*

*-rwx 1131 <date> config.text*

*-rwx 109 <date> info*

*-rwx 389 <date> env\_vars*

*drwx 640 <date> html*

*-rwx 109 <date> info.ver*

*403968 bytes available (3208704 bytes used)*

*switch:*

* Teclear “flash:config.text flash:config.old” para renombrar el archivo de configuración.

*switch: rename flash:config.text flash:config.old*

* A continuación ejecutar el comando “boot”.

*switch: boot*

*Loading”flash:c3500xl-c3h2s-mz.120-5.WC7.bin”*

*File “flash:c3500xx-xxxxx-mz.xxx-x.xxx.bin” uncompressed and installed, entry* point: 0×3000 executing…

* Aparecerá la pregunta “si queremos empezar con la configuración inicial” teclear “n”

*--- System Configuration Dialog ---*

*At any point you may enter a question mark '?' for help.*

*Use ctrl-c to abort configuration dialog at any prompt.*

*Default settings are in square brackets '[]'.*

*Continue with configuration dialog? [yes/no]: n*

* Presionar Enter

*Press RETURN to get started.*

*Switch>*

* Ahora escribir el comando “enable”

*Switch>enable*

*Switch#*

* Para renombrar la configuración con su nombre original usaremos el comando:

*rename flash:config.old flash:config.text*

*Switch#rename flash:config.old flash:config.text*

*Destination filename [config.text]*

* Presionar “Enter”.

*Switch#*

* Copiar la configuración a la memoria con el comando

*copy flash:config.text system:running-config*

*Switch#copy flash:config.text system:running-config*

*Destination filename [running-config]?*

* Presionar “Enter”.

*1131 bytes copied in 0.760 secs*

*Nombre-del-switch#*

* En este paso es importante notar que reaparece la configuración que se encontraba en el switch. Ahora solo nos resta reconfigurar las claves de acceso. Configurar “enable secret” y “enable password”.

*Nombre-del-switch# conf t*

*Nombre-del-switch(config)#enable secret <new\_secret\_password>*

*Nombre-del-switch(config)#enable password <new\_enable\_password>*

* Configurar las claves de acceso vía telnet:

*Nombre-del-switch(config)#line vty 0 15*

*Nombre-del-switch(config-line)#password <new\_vty\_password>*

*Nombre-del-switch(config-line)#login*

* Configurar las claves para el acceso vía consola:

*Nombre-del-switch(config-line)#line con 0*

*Nombre-del-switch(config-line)#password <new\_console\_password>*

* Por último guardar los cambios en la configuración:

*Nombre-del-switch #write memory*

*Building configuration...*

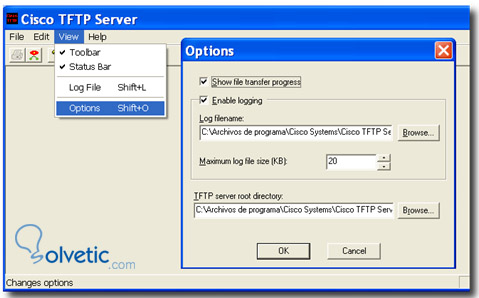
*[OK]*

*Nombre-del-switch #*

1. **Backup configuracion de router:**

* En primer lugar, debemos instalar un servidor Tftp en algún equipo de nuestra red local.

Todos los archivos transferidos por medio del servidor Tftp serán almacenados en la ruta: “Archivos de programa\Cisco Systems\Cisco TFTP Server” , si deseamos cambiar la ruta debemos entrar al menú “View” , “Options” y modificar la opción “Tftp server root directory”.



*Respaldo configuración*

* Para respaldar la configuración actual del “Router1”, debemos iniciar sesión en modo privilegiado en el “Router1”.

*Router1> enable*

*Router1#*

* Ejecutar el comando “copy running-config tftp:”

*Router1#copy running-config tftp*:

* Introducir la dirección IP del equipo donde se encuentra instalado el TFTP Server. En nuestro ejemplo corresponde la dirección Ip 192.168.10.4

Address or name of remote host : 192.168.10.4

* Introducir el nombre del archivo donde se guardará la configuración del “Router1”. En nuestro ejemplo decidimos llamarlo “backup\_router1\_confg”.

*Destination filename [router1-confg]? backup\_router1\_confg*

*!!*

*1030 bytes copied in 2.487 secs (394 bytes/sec)*

*Router1#*

* Por último verifica en la ruta “Archivos de programa\Cisco Systems\Cisco TFTP Server” del servidor Tftp la creación del archivo “backup\_router1\_confg”.

*Restaurar configuración*

* Para restaurar la configuración del “Router1”, debemos iniciar sesión en modo privilegiado en el “Router1”.

*Router1> enable*

*Router1#*

* Ejecutar el comando “copy tftp: running-config”. Este comando copiará el archivo desde el servidor Tftp hacia la memoria del router.

*Router1#copy tftp: running-config*

* Introducir la dirección IP del equipo donde se encuentra instalado el TFTP Server. En nuestro ejemplo corresponde la dirección Ip 192.168.10.4

Address or name of remote host: 192.168.10.4

* Introducir el nombre del archivo donde se encuentra respaldada la configuración del “Router1”. En nuestro ejemplo el nombre del archivo es “backup\_router1\_confg”.

*Source filename []?backup\_router1\_confg*

* El nombre destino será “running-config” ya que deseamos sobrescribir la configuración actual.

*Destination filename [running-config]?*

*Accessing tftp:// 192.168.10.4/ backup\_router1\_confg...*

*Loading backup\_router1\_confg from 192.168.10.4 (via FastEthernet0/0): !*

*[OK - 1030 bytes]*

*1030 bytes copied in 9.613 secs (106 bytes/sec)*

*Router1#*

*Errores comunes*

* Para una exitosa transferencia de archivos se recomienda mantener abierto el servidor Tftp.
* Es común que el router no pueda comunicarse con el servidor Tftp debido a que algún cortafuegos bloqueé la comunicación entre el router y el equipo donde se encuentra el servidor Tftp.
* El puerto de comunicación utilizado para la transferencia de archivos vía Tftp es el 69 udp.

1. **Troubleshooting de Switches Cisco**

*COMANDOS GENERALES*

* show mac address-table

Nos permite observar las direcciones MAC aprendidas por el switch. Nos indica a que vlan pertenece, así como en que puerto ve la MAC. Esto nos permite verificar que la VLAN de los equipos es correcta.

* show vlan

Muestra una relación de todas las VLAN’s creadas en el switch y a que puerto pertenecen.

* show interfaces trunk

Muestra el estado de los puertos configurados como trunk’s.

* clear mac address-table dynamic

Limpia la tabla de direcciones MAC aprendidas por el switch. Si una dirección no es aprendida de nuevo puede indicar que hay un problema con el dispositivo que contiene dicha MAC.

* show interfaces switchport

Muestra un listado de los puertos del switch, incluyendo la VLAN e información de configuración del trunk.

* traceroute mac [dirección\_MAC\_origen] [dirección\_MAC\_destino]

Usa CDP para crear una lista de switches por los que tiene que pasar un paquete dirigido de la MAC origen al destino. Nos permite ver si hay algún punto de fallo en el camino si dos equipos no logran comunicarse.

*SPANNING-TREE*

Si STP falla se pueden producir bucles a nivel 2, que tirarán fácilmente la red (el concepto de la corrupción de direcciones en la tabla MAC y el de broadcast storms).

* show spanning-tree vlan [ID\_VLAN]

Nos indica el ID del switch que hace de Root, que dirección tiene, que Priority presenta y los temporizadores del Hello. También obtenemos nuestro ID del puerto que actúa de Bridge en nuestro switch, con sus costes.

Normalmente el admin del sitio quiere que el root switch sea el mejor posicionado de todos, para mejorar el rendimiento (y como buenas prácticas), así que el switch elegido tendría que reducir su prioridad para ser declarado root bridge. En el diagnóstico de STP, lo fundamental es obtener [quien es el root bridge] y [que función cumplen los puertos de todos los switches].

* show spanning-tree summary

Un resumen rápido de cómo funciona el STP en el switch: en qué modo está (PVST, etc.), configuraciones variadas (etherchannel, BPDU guard, Portfast por defecto, etc.), así como el estado de la vlan (Blocking, Listening, Learning o Forwarding).

* show spanning-tree interface [interfaz] detail

Este comando nos muestra información detallada del puerto seleccionado, en concreto, lo que muestra en sus BPDU. También tiene contadores de BPDU para ver cuantos han sido enviados y recibidos.

*STP + Etherchannel*

Cuando hay varios puertos funcionando con Etherchannel (para crear un solo enlace virtual conectando varios puertos entre dos switches) se tiene que tener en cuenta las siguientes normas:

* La configuración de todos los puertos que crean el Etherchannel en los dos switches tiene que ser idéntica: velocidad, duplex, modo trunk, VLAN nativa, etc.
* La configuración Etherchannel de los dos switches tiene que ser idéntica. Por ejemplo, el protocolo a elegir {Link Aggregation Control Protocol (LACP) o Port Aggregation Protocol (PAgP)} tiene que ser el mismo.
* El algoritmo de distribución tiene que ser el mismo. Este algoritmo de hash sirve para distribuir la carga entre los enlaces de forma correcta.

1. **Configuracion de puerto de switch**

*Ethernet (10 Mbps, IEEE 802.3)*

* Para evitar el problema de medio compartido y por lo tanto half-duplex Ethernet Switching dedica un ancho de banda de 10 Mbps dedicado por cada uno de los puertos del switch. Con esto se consigue que el número de usuarios conectados a un segmente Ethernet se reduzca y por tanto es menos probable que haya colisiones y que el dominio de colisión se reduzca de tamaño.

*FastEthernet (100 Mbps, IEEE 802.3u)*

* La velocidad del enlace se determina vía una señalización eléctrica para que cada extremo del enlace pueda determinar qué velocidad está intentando usar el otro extremo. Si ambos extremos están configurados para auto negociación, se usará la velocidad más alta posible para ambos extremos.
* El duplex de un enlace se negocia a través de intercambio de información. Si la auto negociación del duplex falla, el puerto de switch se pone en su configuración por defecto: half-duplex.
* Cisco recomienda configurar la velocidad (speed) y duplex en ambos extremos para asegurar que alguno de los extremos cambie su configuración y pueda causar que el enlace se caiga (corte).

*GigabitEthernet (1.000 Mbps o 1Gbps, IEEE 802.3z)*

* La ventaja de GigabitEther es que a pesar de que la Capa 1 se ha modificado para incrementar la velocidad de transmisión, todo el resto es compatible con los anteriores Ethernet.
* El duplex de los puertos GigabitEthernet está siempre activado en los switches Cisco, por lo que la auto negociación del duplex no es posible.

*GigabitEthernet (10.000 Mbps o 10Gbps, IEEE 802.3ae)*

* Ethernet escala de la siguiente forma, 10 Mbps, 100 Mbps, 1.000 Mbps y ahora 10.000 Mbps. Las características de Ethernet Capa 2 se mantienen operando SOLO a full duplex, lo que si difiere es la Capa Física (PHY) que pueden ser:
  + LAN PHY: interconecta switches en una red de campus y predomina en la capa del núcleo (core layer).
  + WAN PHY: se encuentran en redes de área metropolitana (MAN = metropolitan-area networks) y sus interfaces son synchronous optical network (SONET) o synchronous digital hierarchy (SDH).
* Cisco Catalyst switches soportan 10-Gigabit Ethernet PMDs en la forma de XENPAK, X2 y SFP+ transceivers. Generalmente, el formato X2 es más pequeño que el de XENPAK y el SFP+ es incluso más pequeño permitiendo más densidad de puertos en un módulo de un switch.

Aunque por lo general se suele decir puerto de switch en IOS de Cisco se denominan "interfaces". Para elegir un puerto a configurar se usa el comando en modo de configuración global:

*Switch(config)# interface type module/number*

* Tipo de puerto:
* Fastethernet
* Gigabitethernet
* Tengigabitethernet
* vlan,
* módulo: slot donde está localizado, lo que no soporten módulos ni slots se usa el módulo 0 (cero) y por último se indica el número de puerto (number) dentro del módulo. En algunos modelos puede haber chasis o stacks en cuyo caso sería stack/module/number.

Para seleccionar varios puertos y configurarlos a la vez y no tener que estar entrando puerto por puerto podemos usar este comando si son puertos no contiguos:

*Switch(config)# interface range type module/number [, type module/number ...]*

Comando si son puertos contiguos:

*Switch(config)# interface range type module/firstnumber – lastnumber*

También podemos definir una macro que contenga un listado de puertos, rangos o ambos, para ello debemos seguir estos pasos:

* definir el nombre de la macro y especificar el listado de puertos y/o rangos de puertos como se necesite

*Switch(config)# define interface-range macro-name type module/number [, type module/ number ...] [type module/first-number – last-number] [...]*

* invocar la macro que se ha definido justo antes de aplicar los comandos comunes.

*Switch(config)# interface range macro macro-name*

*NOTA: es muy importante que tanto las comas (,) como los guiones (-) tengan un espacio delante y detrás en el comando interface rango anterior.*

*Identificando puertos*

Se puede añadir una descripción o comentario a cada puerto que nos ayude a identificar lo que hay en ese puerto.

*Switch (config-if) # description description-string*

Quitar el comentario:

*Switch(config-if)# no description*

*Velocidad del puerto*

Se puede especificar una velocidad concreta a un puerto (siempre que esté soportada) o dejarlo en auto negociación (auto) que es como está por defecto, menos los puertos GBIC que están a 1000.

*Switch(config-if)# speed {10 | 100 | 1000 | auto}*

*El modo duplex del puerto*

Se puede especificar el modo del puerto (duplex mode) que puede ser half-duplex, full-duplex o auto negociado, que está por defecto y solo está permitido en UTP Fast y Giga Ethernet. En auto negociación primero se intenta negociar a full-duplex y si falla se queda en half-duplex. El proceso de negociación de repita cada vez que el enlace (link) cambia de estado. Es importante configurar ambos extremos de idéntica forma para evitar problemas de discordancias y por lo tanto half-duplex.

*Switch(config-if)# duplex {auto | full | half}*

*Detectando condiciones de error*

Por defecto, un switch Catalyst detecta una condición de error en cada puerto por cada posible causa. Si se detecta una condición de error, el puerto se pone en modo errdisable y se deshabilita. Se puede configurar este comportamiento para que solo ciertas condiciones se apliquen en el modo errdisable del puerto en caso de error.

Para configurar que condiciones deshabilitan el puerto se usa este comando:

*Switch (config)# [no] errdisable detect cause [all | cause-name]*

Se puede repetir el comando por cada uno de las siguientes causas:

* all—Detecta todas las posibles causas.
* arp-inspection—Detecta errores con la inspección ARP dinámica.
* bpduguard—Detecta cuando se recibe una unidad de datos de protocolo de puente de árbol de expansión (BPDU) en un puerto configurado para STP.
* PortFastchannel-misconfig—Detecta un error con un paquete EtherChannel.
* dhcp-rate-limit—Detecta un error con el snooping de DHCP.
* dtp-flap— Detecta cuándo la encapsulación de enlaces está cambiando de un tipo a otro.
* gbic-invalid—Detecta la presencia de un módulo GBIC o SFP no válido.
* ilpower—Detecta un error con la oferta de potencia en línea.
* link-flap—Detecta cuando el estado del enlace de puerto está "flapeando" entre los estados ascendente y descendente.
* loopback—Detecta cuando una interfaz entra en bucle.
* pagp-flap—Detecta cuando los puertos de un paquete EtherChannel ya no tienen configuraciones coherentes.
* psecure-violation—Detecta las condiciones que activan la seguridad del puerto configurada en un Puerto.
* rootguard—Detecta las condiciones que activan la seguridad del puerto configurada en un puerto.
* security-violation—Detecta errores relacionados con la seguridad del Puerto
* storm-control—Detecta cuando se ha sobrepasado un límite de control en un Puerto.
* udld—Detecta cuándo se ve que un enlace es unidireccional.
* unicast-flood—Detecta las condiciones que desencadenan el bloqueo de inundación unicast en un puerto.
* vmps—Detecta errores al asignar un puerto a una VLAN dinámica a través del servidor de directivas de pertenencia VLAN (VMPS).

*Recuperar automáticamente desde condiciones de error*

Por defecto cuando un puerto se pone en modo errdisable debe ser habilitado de nuevo manualmente. Esto se hace bajando (shutdown) y levantando (no shutdown) el puerto concreto. Antes de proceder a habilitar el puerto se debe comprobar la causa del error para que no se vuelva a deshabilitar de nuevo.

También se puede configurar el switch para que habilite automáticamente el puerto deshabilitado, si es más importante que el puerto esté levantado. Para ello se debe especificar que causas se permiten que se habilite el puerto automáticamente con el comando (ver las cusas más arriba):

*Switch(config)# errdisable recovery cause [all | cause-name]*

Por defecto desde que el puerto es deshabilitado hasta que se habilita automáticamente pasan 300 segundos (5 minutos). Este valor se puede cambiar con el comando (de 30 a 86400 segundos = 24 horas):

*Switch(config)# errdisable recovery interval seconds*

*Resolviendo conectividad de un puerto*

Para resolver un problema de conectividad podemos usar el comando "show interfaces" que muestra una completa información sobre el puerto del switch.

La primera línea nos muestra el estado, indicando en la primera parte el estado del enlace físico (data link layer) que si está Down indica que está físicamente desconectado o no detecta enlace y la segunda parte nos indica el estado del protocolo (line protocol) es decir el estado de la Capa 2, si está en errdisable es que se ha detectado una condición de error y automáticamente se ha deshabilitado el puerto.

Una forma rápida de ver los estados de TODOS los puertos podemos usar el comando "show interface status". Y para ver TODOS los puertos que están en errdisable podemos usar este comando "show interface status err-disabled".

Otro posible problema puede surgir si un usuario detecta un tiempo de respuesta lento o bajo ancho de banda cuyo problema puede ser causado a una discordancia en la velocidad y/o el duplex entre el puerto del switch y el servidor. Esto es bastante común cuando un extremo está puesto que auto negocie y el otro no. Para ello observaremos que no haya ningún valor de error mayor de cero y también que no esté a half-duplex.

**Configuracion protocolo HSRP**

Hot Standby Router Protocol (HSRP) fue desarrollado por Cisco y se utiliza para proporcionar redundancia en la capa 3 (Layer 3) del Modelo OSI y principalmente en el Gateway.

Este protocolo se implementa en la capa de distribución (haciendo referencia al modelo Core/Distrubution/Access). HSRP utiliza una dirección IP y una dirección MAC virtual dónde un Gateway Backup asume el control en al momento de ocurrir una falla.

HSRP utiliza un router en modo Active y otro en modo Standby. La dirección IP virtual está configurado tanto el router Active como en el Standby dónde solamente existe una dirección IP y MAC por grupo (Active/Standby).

*HSRP Timers*

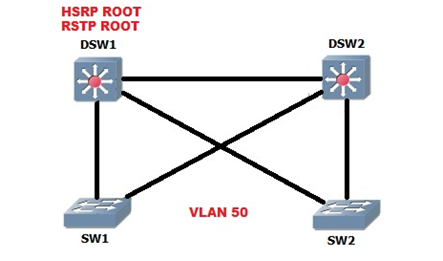
HSRP envía “*hello packets*” vía la dirección multicast 224.0.0.2 y por defecto lo envía cada 3 segundos y el tiempo por default para declarar un router inaccesible son 10 segundos, ambos tiempos pueden ser ajustados hasta milisegundos para obtener un mejor rendimiento en el failover. Si el router que se encuentra en modo Standby deja de recibir mensajes “*hello*” desde el router activo, entonces éste asume el control de la topología. HSRP requiere conectividad de capa 2 (Layer 2) entre los routers.

*Estados HSRP*

HSRP consta de 5 estados de operación:

* Initial: Aquí aún NO está trabajando HSRP, éste estado es cuando la interface acaba de subir.
* Listen: Escucha los “Hellos Messages”, conoce la IP virtual.
* Speak: Envía Hellos Messages y participa en la elección de los routers (Active/Passive).
* Standby: Es candidato para el próximo active router
* Active: Es el encargado de enviar paquetes hacia la IP virtual.

Veamos la topología que vamos a utilizar en esta configuración:



*HSRP-1*

Vamos a configurar HSRP para la VLAN 50. Teniendo en cuenta que se debe configurar por cada VLAN que necesitemos la redundancia, un grupo HSRP es necesario que sea definido en el SVI (Switch Virutal Interface) para la VLAN 50.

En primer lugar, debemos tener presente que la VLAN 50 debe existir primero en los switch antes de hacer la configuración. Sólo puede existir un router Active y otro Standby por grupo de HSRP, dónde el Standby sólo funcionaría sí el Active falla. Es muy importante, pero recuerden siempre esto: “El router Active debe ser el ROOT de Spanning-Tree en la topología. Esto es importante para evitar loops en la red. En ésta topología, el DSW1 será el Active Router, dónde el SW1 y SW2 deberían enviar tráfico directamente hacia el DSW1.

1. Configuración:

*DSW1(config)#interface vlan50*

*DSW1(config-if)#ipaddress 10.10.50.2 255.255.255.0*

*DSW1(config-if)#standby 1 ip 10.10.50.1*

*DSW1(config-if)#end*

La dirección 10.10.50.1 es la Virtual IP. HSRP utiliza también una MAC address virtual utilizando éste formato: 0000.0C07.ACXX (XX es el número del grupo expresado en hexadecimal). La dirección IP y dirección MAC virtual son empleadas por el Standby router en caso que el Active falle. En nuestro caso particular, la dirección MAC virtual se vería de la siguiente manera: 0000.0C07.AC01,

1. Prioridad

Necesitamos que DSW1 sea siempre el router Activo. Para esto debemos configurar la prioridad de DSW1 y DSW2, dónde debemos tener en cuenta 2 parámetros: prioridad y preemption, los cuáles veremos más tarde.

La prioridad por defecto de HSRP es 100. Para poder lograr esto, debemos modificar la prioridad de DSW1 y llevarla a 150.

*DSW1(config-if)#standby 1 priority 150*

1. Preempt

Un router HSRP nunca intentara convertirse en Active cuando es introducido en una topología existente, incluso teniendo la prioridad más alta. Necesitamos que DSW1 sea siempre el router Active. Para poder lograr esto debemos configurar preempt. Esto permitirá que el router con la prioridad más alta inicie el proceso para convertirse en el router Active; sí éste tiene la prioridad más alta, pero si ambas prioridades son iguales, entonces, el router con la dirección IP más alta ganará la elección.

*DSW1(config-if)#standby 1 preempt*

Si DSW1 falla y procede de nuevo a ser operativo, necesitamos asegurar que vuelva a ser el Active, porque en el caso que falle DSW2, éste tomaría el control de la topología, pero cuando regrese DSW1, por esta opción, vuelve a ser el Active y DSW2 Standby.

1. Modificacion de “*timers”*

Necesitamos disponer de rápida convergencia para que el usuario no se dé cuenta de cambios en la topología. Por ésta razón, vamos a modificar los “*hellos messages*” a 200 milisegundos y el *deadtimer* 600 milisegundos.

yency-2

* Configuración en DSW1:

*DSW1(config-if)#standby 1 timersmsec 200 msec 600*

* Configuración en DSW2:

*DSW2(config)#interface vlan50*

*DSW2(config-if)#ipaddress 10.10.50.3 255.255.255.0*

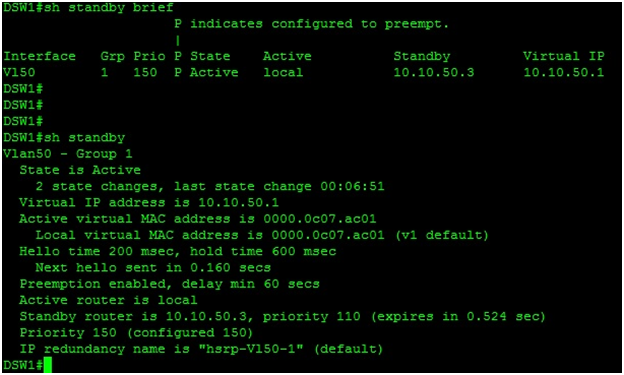
*DSW2(config-if)#standby 1 ip 10.10.50.1*

*DSW2(config-if)#standbytimersmsec 200 msec 600*

*DSW2(config-if)#standby 1 priority 110*

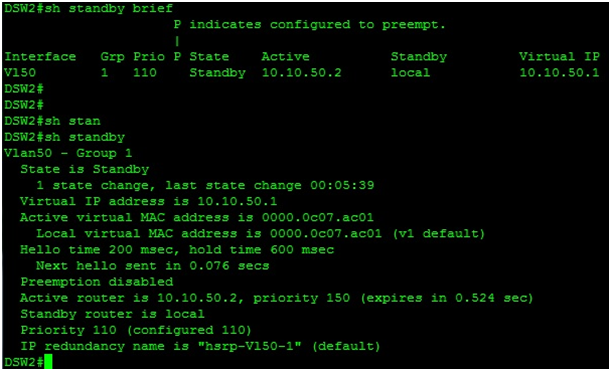
*DSW2(config-if)#end*

Como vemos en la configuración de DSW2, la prioridad está en 110. Para garantizar que en la topología siempre el Active Router sea DSW1, un tercer Router puede ser añadido dónde tendría la prioridad en 100. Por esta razón, es recomendable configurar la prioridad del Standby más alta que un tercer Router.



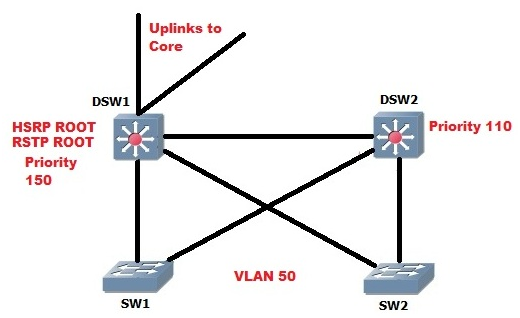
Como podemos visualizar el DSW1, la prioridad es 150 y ésta configurado preempt (P). Si vemos en la columna Active, dice Local, ésto quiere decir que es el router Active en la topoligía y el Standby tiene la dirección 10.10.50.3

Veamos la configuracion de DSW2:



Podemos verificar que su prioridad es 110. Su estado (state) es “Standby”. En la columna de Active tenemos la dirección 10.10.50.2, el cual es DSW1.

*Interface Tracking*



Ya hemos implementado HSRP, pero ahora vamos a ver cómo manejamos algunas fallas de conectividad en caso que DSW1 falle por completo, y hacer algunas pruebas para que DSW2 tome el control de la topología, principalmente, logrando que el Uplink de DSW1 falle.

La opción de “Interface Tracking” se utiliza en el caso de que unos de los Uplinks falle, y estos son determinados por el estatus del line protocol status. DSW1 deberá reducir en 50 su prioridad para que DSW2 tome el control y sea el Active Router.

*Importancia de su uso:*

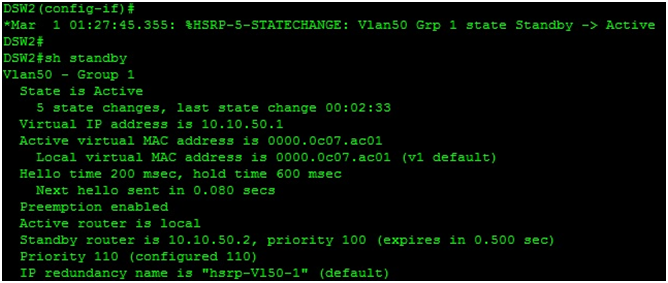
Si los nodos (hosts) de SW1 están enviando su tráfico a través de DSW1 por ser el Active Router, pero ocurre un problema con el uplink de DSW1 que lo conecta con el CoreLayer, pero los host que están en SW1 y SW2 no saben que pasa, no tendrán conectividad y se podría generar un loop en la red. Entonces, configuramos “Interface Tracking” en la interface F0/24 (uplink DSW1) con un decremento de 50. ¿Por qué 50? Si le reducimos 50 a la prioridad de DSW1 (150), ésta quedaría en 100 y la prioridad de DSW2 es 110. En éste caso es electo el Active Router y el tráfico es enviado a través de él.

*DSW1(config-if)#standby 1 track fa0/24 50*

Es necesario configurar preempt en DSW2 para cuando DSW1 tenga su prioridad en 100, DSW2 sea el Active.

*DSW2(config-if)#standby 1 preempt*

Ahora vamos a remover el cable de la interface F0/24 de DSW1 para ver qué pasa:



**Configuracion VTP**

Para realizar la configuración de VTP, se debe configurar como troncales (trunk), las interfaces que conectan los switches entre sí, para esto debemos ingresar en el modo de configuración global *(****S1(config)#****),* utilizando el comando ***interface*** seguido de la interfaz correspondiente.

Ingresamos al modo de configuración de la interfaz (***S1(config-if)#****)* (***interface range*** si queremos configurar varias interfaces a la vez) y, más tarde, se ejecuta el comando “**switchport mode trunk**” para configurar el puerto como troncal.

Por motivos de seguridad, se debe configurar el resto de puertos como acceso, empleando el comando ***switchport mode access*** en el modo de configuración de interfaces:

*(****S1(config-if-range)#****)*

A continuación, debemos configurar el nombre del dominio VTP desde el modo de configuración global *(****S1(config)#****)* utilizando el comando **vtp domain** seguido del nombre del dominio,

Se asigna una contraseña al dominio con el comando “**vtp password**” seguido de la contraseña elegida; inmediatamente después, se debe especificar el modo en el que el switch funcionara mediante el comando ***vtp mode*** seguido del modo (**server, client, transparent**).

.

Tras haber configurado VTP, debemos anunciar las VLANs en el switch que está en modo servidor para que los que están en modo cliente puedan aprender las VLANs automáticamente.

Se logra por medio del comando ***vlan*** seguido del número de la VLAN (**1-1005**)

A continuación, en el modo de configuración de VLAN *(S1(****config-vlan)#****)* asignamos un nombre a la VLAN utilizando el comando ***name*** seguido del nombre que deseamos asignar a la VLAN.

Por último, debemos asignar las VLAN a los puertos, utilizando el comando ***interface*** o ***interface range*** seguido de la interfaz que deseamos asignar a una VLAN específica,

Posteriormente, ejecutamos el comando ***switchport access vlan*** seguido del número de la VLAN correspondiente.

**Configuración de puertos troncales y acceso**

* *Configuracion de las interfaces de S1*:

*S1(config)#interface range fastEthernet 0/1 – 2*

*S1(config-if-range)#switchport mode trunk*

*S1(config-if-range)#exit*

*S1(config)#interface range fastEthernet 0/3 – 24*

*S1(config-if-range)#switchport mode access*

* *Configuración de las interfaces de S2:*

*S2(config)#interface fastEthernet 0/1*

*S2(config-if)#switchport mode trunk*

*S2(config-if)#exit*

*S2(config)#interface range fastEthernet 0/2 – 24*

*S2(config-if-range)#switchport mode access*

* *Configuración de las interfaces de S3:*

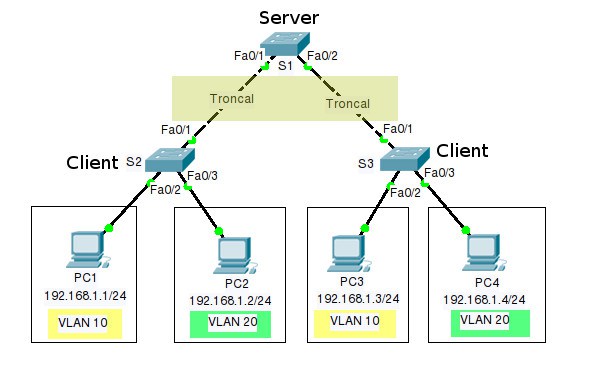
S3(config)#interface fastEthernet 0/1

S3(config-if)#switchport mode trunk

S3(config-if)#exit

S3(config)#interface range fastEthernet 0/2 – 24

S3(config-if-range)#switchport mode access



**Estado de la red:**

En este punto los switches están preparados para intercambiar información de las VLAN, pero debido a que no hemos configurado VTP ni las VLANs no se ha iniciado la transmisión de VLAN.

**Configuración de VTP**

* *Configuración del nombre, contraseña y modo del S1:*

*S1(config)#vtp domain Practica*

*S1(config)#vtp password seguro*

*S1(config)#vtp mode server*

* *Configuración del nombre, contraseña y modo del S2:*

*S2(config)#vtp domain Practica*

*S2(config)#vtp password seguro*

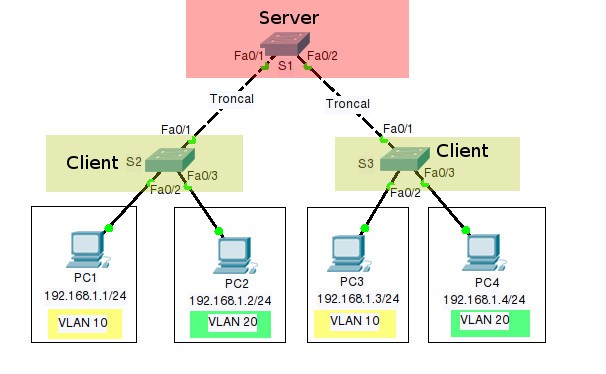
*S2(config)#vtp mode client*

* *Configuración del nombre, contraseña y modo del S3:*

*S3(config)#vtp domain Practica*

*S3(config)#vtp password seguro*

*S3(config)#vtp mode client*



**Estado de la red:**

En este punto, los switches están preparados para transmitir las VLAN configuradas en el switch server, pero como no tiene ninguna VLAN configurada no se está transmitiendo nada.

**Configuración de las VLAN en el switch server y verificación en todos los switches de las VLAN**

* ***VLANs en S1*:**

*S1#show vlan brief*

*1 default*

*S1#show vlan brief*

*1 default*

*1002 fddi-default*

*1003 token-ring-default*

*1004 fddinet-default*

*1005 trnet-default*

* **VLANs en S2**

*S1#show vlan brief*

*1 default*

*1002 fddi-default*

*1003 token-ring-default*

*1004 fddinet-default*

*1005 trnet-default*

* **VLANs en S3**

*S3#show vlan brief*

*1 default*

*1002 fddi-default*

*1003 token-ring-default*

*1004 fddinet-default*

*1005 trnet-default*

* **Configuración de la VLAN 10:**

*S1(config)#vlan 10*

*S1(config-vlan)#name Administracion*

* **Configuración de la VLAN 20**

*S1(config)#vlan 20*

*S1(config-vlan)#name Ventas*

* **VLANs en S1:**

*S1#show vlan brief*

*1 default*

*10 Administracion*

*20 Ventas*

*1002 fddi-default*

*1003 token-ring-default*

*1004 fddinet-default*

*1005 trnet-default*

* **VLANs en S2**

*S2#show vlan brief*

*1 default*

*10 Administracion*

*20 Ventas*

*1002 fddi-default*

*1003 token-ring-default*

*1004 fddinet-default*

*1005 trnet-default*

* **VLANs en S3**

S3#show vlan brief

1 default

10 Administracion

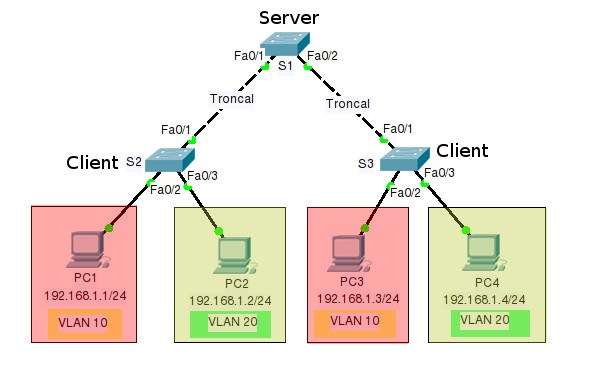
20 Ventas

1002 fddi-default

1003 token-ring-default

1004 fddinet-default

1005 trnet-default



**Estado de la red:**

En este punto, el switch server (S1) transmitió sus VLANs a los switches clientes (S2 y S3), actualmente las PC tienen comunicación entre si debido a que no han sido separadas en VLANs.

**Asignación de la los puertos a la VLAN 10**

* ***Configuracion del S2***

*S2(config)#interface fastEthernet 0/2*

*S2(config-if)#switchport access vlan 10*

*S2(config-if)#exit*

*S2(config)#interface fastEthernet 0/3*

*S2(config-if)#switchport access vlan 20*

* ***Configuracion del S3***

*S3(config)#interface fastEthernet 0/2*

*S3(config-if)#switchport access vlan 10*

*S3(config-if)#exit*

*S3(config)#interface fastEthernet 0/3*

*S3(config-if)#switchport access vlan 20*

**Estado del a red:**

En este punto, la red tiene comunicación a través de las VLAN: los equipos que se encuentran en una misma red y una misma VLAN ya tienen comunicación, por ejemplo las PC 1 y 3, tienen comunicación entre si debido a que están en la misma red (192.168.1.0/24) y en la misma VLAN (10), lo mismo pasa con las PC 2 y 4. Puede verificar la comunicación haciendo pruebas con ping.

**Configuracion ECMP en FortiGate:**

ECMP (Equal-Cost Multi-Path) es un protocolo utilizado por los equipos FortiGates para hacer distribución de tráfico hacia un mismo destino, utilizando diferentes rutas. Se puede agregar diversas rutas hacia una misma red destino, asignándoles a cada una la misma distancia y la misma prioridad.

En caso, de que se creen múltiples rutas hacia el mismo destino con la misma distancia pero diferente prioridad, entonces la ruta con menor prioridad será usada. Puede darse el caso que tenga la misma prioridad pero diferente distancia; en dicho caso, la de menor distancia será usada. En caso que sean múltiples rutas hacia el mismo destino pero con diferentes distancias y diferentes prioridades, entonces siempre será usada la ruta con menor distancia, ya que la distancia tiene preferencia sobre las prioridades.

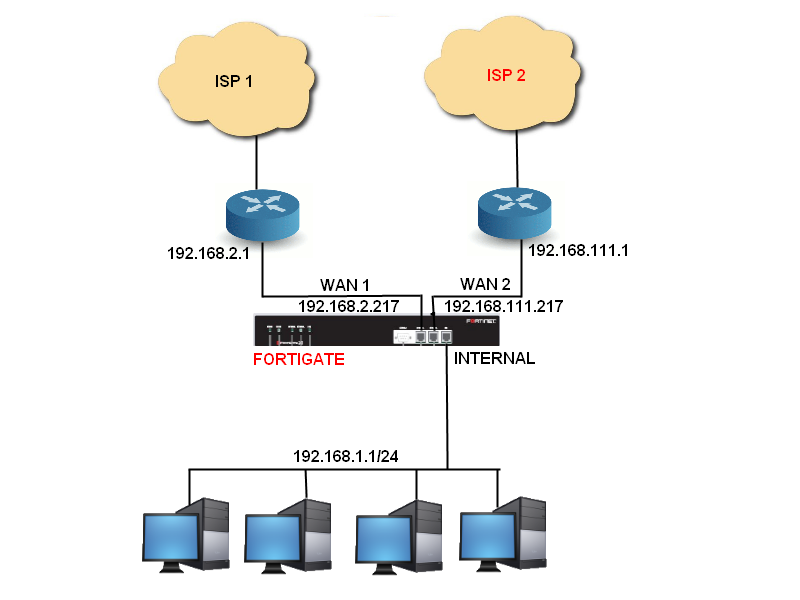
Este protocolo nos permite balancear las cargas de tráfico por diferentes enlaces, hacer redundancia de enlaces, ya que en caso de que uno falle, el sistema usará las rutas disponibles en el enlace que sí esté operando.

*Tipos de configuracion*:

* Source Based: conocida como *Basada en IP Fuente* (Source IP Based), permite al FortiGate balancear las sesiones entre las rutas ECMP basándose en la dirección IP fuente de las sesiones. Esta modalidad es la que trae el FortiGate configurada por defecto, por lo tanto no requiere mas configuración dentro de ECMP.
* Wieghted: conocida como *Basada en peso* (Weight-Based), El FortiGate distribuye la carga, basándose en el peso de las rutas ECMP, por lo tanto más tráfico será direccionado por la ruta de mayr peso. Donde será necesario hacer configuración del peso (Weight), para cada una de las rutas a través de la CLI
* Spill-Over: se conoce como *Basado en Uso* (Usage-Based), donde el FortiGate distribuirá el tráfico entre las rutas ECMP tomando como criterio el uso de la interface. Si se selecciona este método será necesario configurar los umbrales del Spillover en las interfaces involucradas en los enlaces para los cuales se hará el balanceo por ECMP. En este caso, el FortiGate enviará todas las sesiones del ECMP por la interface con menor número en el Spillover. Una vez alcance el valor configurado, pasará a enviar las sesiones por la siguiente Interface con menor número en Spill.

Cuando el ECMP selecciona una ruta para una sesión, se crea también un cache de rutas, para todas las sesiones con la misma IP de destino. Entonces, todas las nuevas sesiones hacia la misma IP de destino usaran la misma ruta hasta que dicha ruta se borre del cache. Estas rutas se borraran automáticamente luego de un periodo de tiempo en el que ya no se generen reciban peticiones de sesiones hacia la misma dirección IP de destino.

A continuación, se muestra un esquema donde tendremos un FortiGate con una LAN y dos interfaces recibiendo los enlaces de Internet, los cuales son independientes y con ellos haremos ECMP. Para este laboratorio, se ha empleado estamos un FortiGate FG310B-US, por lo tanto configuraremos el Port1 como *Internal,* el Port10 como *WAN1* y el Port9 como *WAN2*



1. Configuración vía GUI de ECMP: Source IP Based

Ambos enlaces de Internet poseen el mismo ancho de banda y el tráfico se dirige de forma repartida.

* *Configurando las Interfaces WAN*
* Para la configuración de las interfaces del FortiGate entramos en: *System-> Network-> Interface*, donde configuraremos las IPs para cada una de las Interfaces externas.

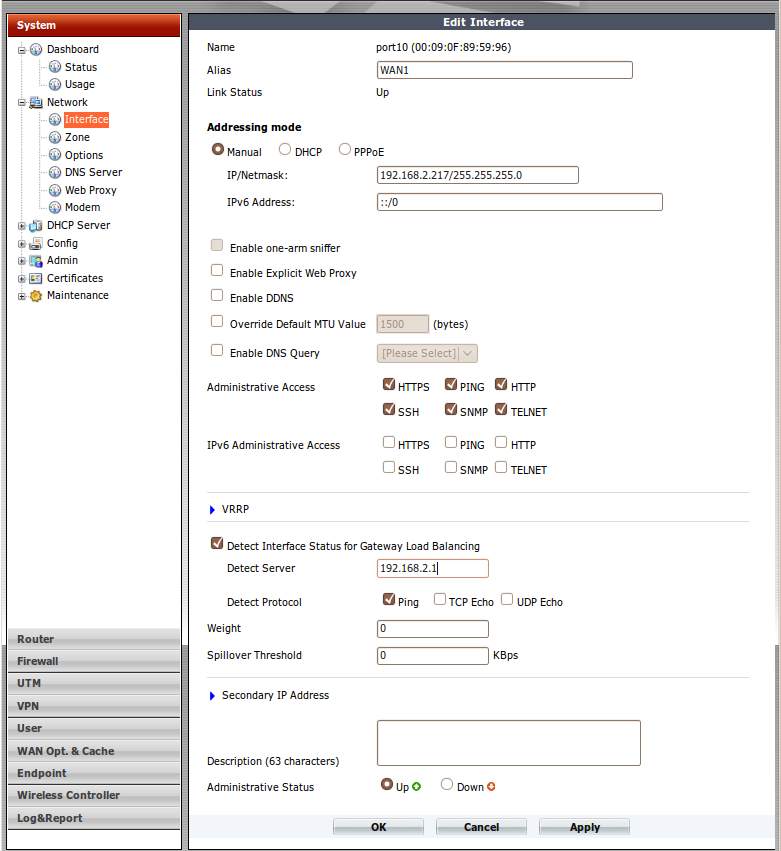


Ilustración 1. WAN1

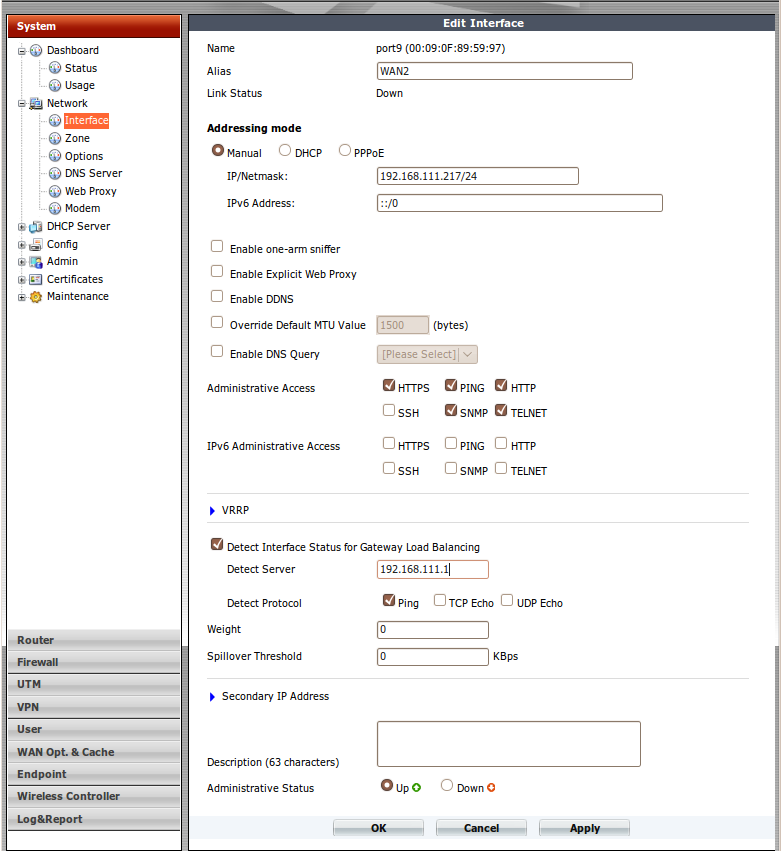


Ilustración 2. WAN2

* Configuración por CLI para las Interfaces:
* WAN1:

*config system interfaceedit “port10″*

*set vdom “root”*

*set ip 192.168.2.217*

*255.255.255.0*

*set allowaccess ping https*

*ssh snmp http telnet*

*set gwdetect enable*

*set detectserver*

*“192.168.2.1″*

*set type physical*

*set alias “WAN1″*

*end*

* WAN2:

*config system interfaceedit “port9″*

*set vdom “root”*

*set ip 192.168.111.217*

*255.255.255.0*

*set allowaccess ping https*

*snmp http telnet*

*set gwdetect enable*

*set detectserver*

*“192.168.111.1″*

*set type physical*

*set alias “WAN2″*

*end*

Tal como se muestra en las figuras anteriores, se habilitado la opción *Detect Interface Status for Gateway Load Balancing* lo que nos permite configurar un server que permitirá al FortiGate detectar cuando un enlace presente problemas de comunicación, de tal forma que si uno de los enlaces con los cuales estamos haciendo ECMP falla, el dispositivo enviará el tráfico por la otra interface, con lo cual, obtendremos del mismo modo redundancia a Fallas. Se recomienda colocar como Server una IP de un dispositivo remoto que sea confiable y que nunca falle.

1. Configurando las rutas.

Se crean las rutas estáticas accediendo: *Router->Static->Static Route->Create New*.

Ambas rutas estáticas tendrán igual distancia y prioridad.

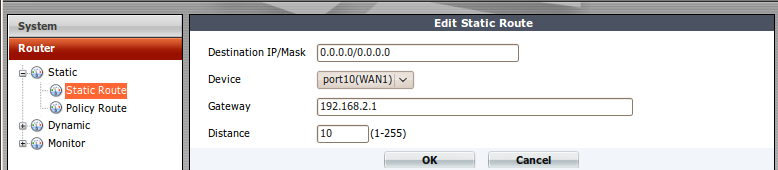


Ilustración 3. Trafico enrutado por WAN1

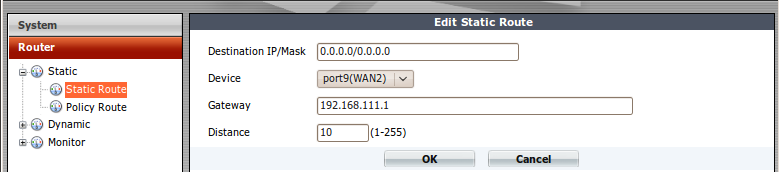


Ilustración 4. Trafico enrutado por WAN2

1. Configurando las rutas por la CLI:

* Ruta 1:

*config router staticedit 1*

*set device “port10″*

*set distance 10*

*set dst 0.0.0.0 0.0.0.0*

*set gateway 192.168.2.1*

*set priority 0*

*set weight 0*

*next*

*end*

* Ruta 2:

*config router staticedit 2*

*set device “port9″*

*set distance 10*

*set dst 0.0.0.0 0.0.0.0*

*set gateway 192.168.111.1*

*set priority 0*

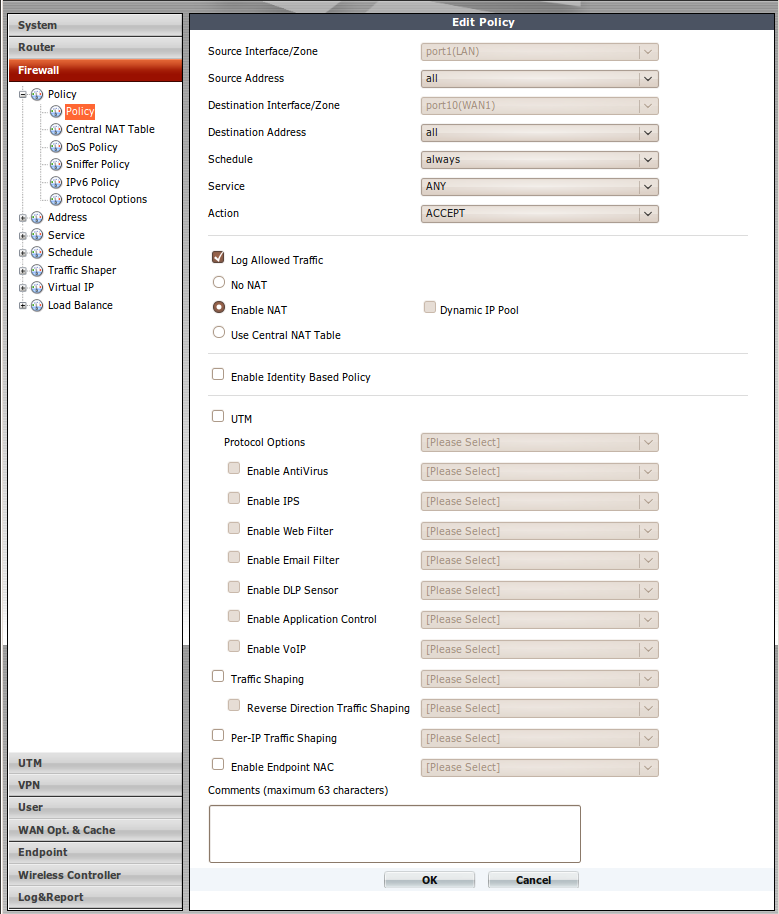
*set weight 0*

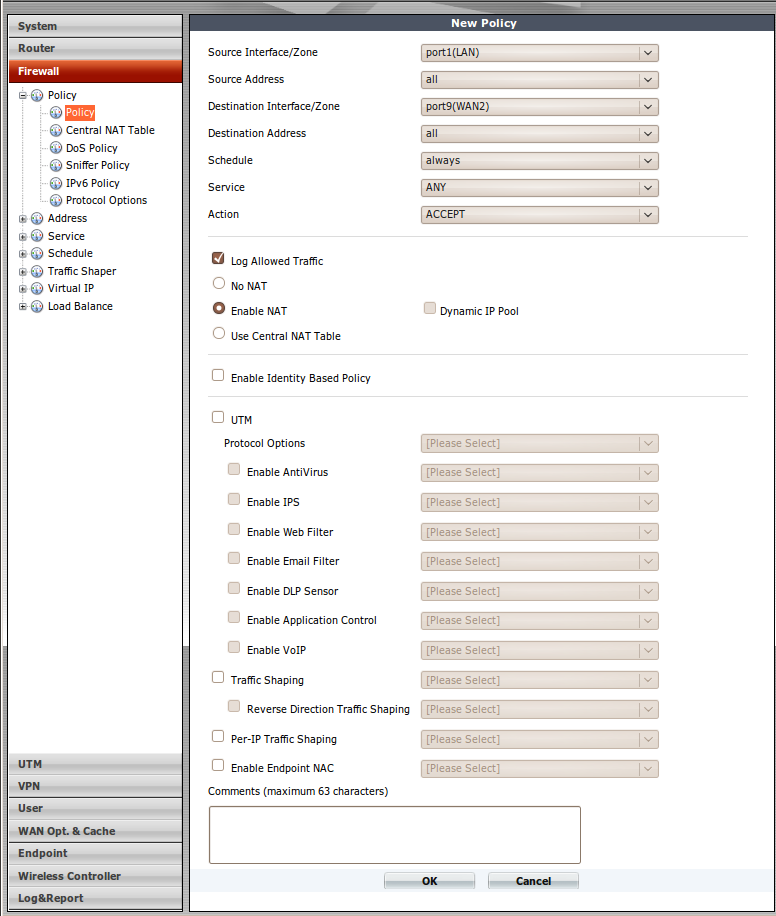
*next*

*end*

1. Creación de las Políticas de Firewall.

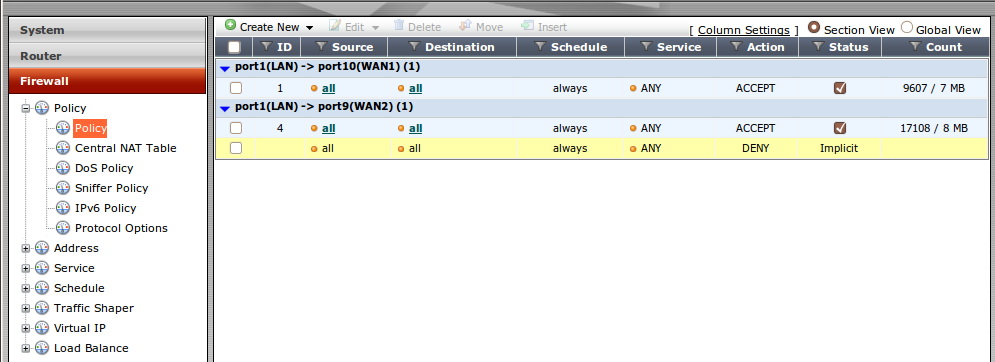
Ahora nos toca navegar en: *Firewall->Policy->Policy->Create New*, crear las políticas desde la LAN hacia la WAN1-WAN2 y permitir tráfico a través de ambos enlaces hacia el Internet.





Con estos pasos ya tenemos enlaces configurados con ECMP, redundantes entre sí.

Si revisamos las políticas, podremos ver que estamos pasando tráfico por ambas, y el criterio se basa en la IP fuente de usuario.



Además podremos monitorear las rutas, donde veremos que ambas tienen igual peso y prioridad en: *Router->Monitor->Routing Monitor*:

1. Configuración vía GUI de ECMP: Weight-Based

Para este método, solo se ha de cambiar el peso de las rutas y adicionalmente cambiar el método de ECMP via CLI.

* + *Cambiando el método de ECMP*

config system settingsset v4-ecmp-mode weight-based

end

* + Cambiando el Peso de las rutas. Este cambio lo podremos hacer via CLI.
  + Ruta 1:

*config router staticedit 1*

*set device “port10″*

*set distance 10*

*set dst 0.0.0.0 0.0.0.0*

*set gateway 192.168.2.1*

*set priority 0*

*set weight 10*

*next*

end

* + Ruta 2:

config router staticedit 2

set device “port9″

set distance 10

set dst 0.0.0.0 0.0.0.0

set gateway 192.168.111.1

set priority 0

set weight 20

next

end

Se trata de un escenario perfecto para el caso de tener enlaces de Internet con anchos de banda diferentes, por lo tanto, con esta configuración estamos forzando a que un tercio del tráfico pase a través del enlace conectado a la WAN1 y los otros dos tercios pasen a través del enlace conectado a la WAN2.

Podemos ahora monitorear las políticas de Firewall, tal como lo hicimos en la sección anterior para ver la distribución de tráfico que ha atravesado por cada una de ellas.

Asimismo, si monitoreamos las rutas vía CLI veremos que los pesos de las rutas hacia el mismo destino son diferentes.

*get router info routing-table*

*staticS\* 0.0.0.0/0 [10/0] via 192.168.111.1,*

*port9, [0/20]*

*[10/0] via 192.168.2.1, port10, [0/10]*

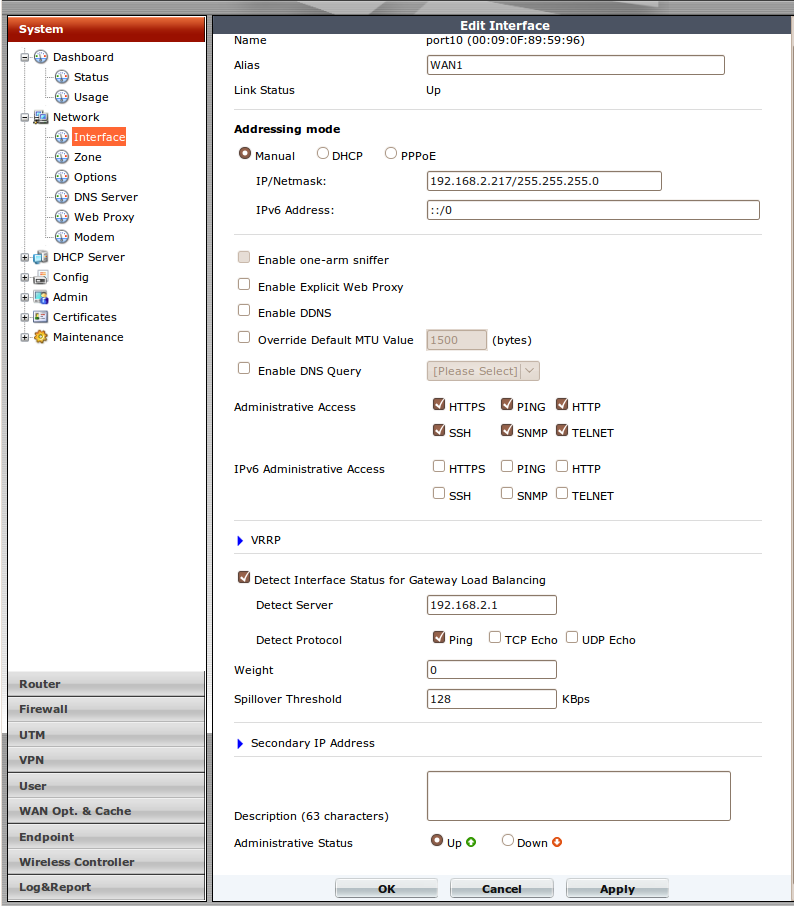
Por lo tanto, ECMP utilizará como primera ruta la de mayor peso. El parámetro del peso solo es utilizado en el momento de enviar la primera sesión hacia una Ip destino. Una vez se decide por qué camino enviar el tráfico, las nuevas sesiones que vayan hacia esa misma IP serán enviadas por esa misma ruta mientras dure la tabla de cache de sesiones.

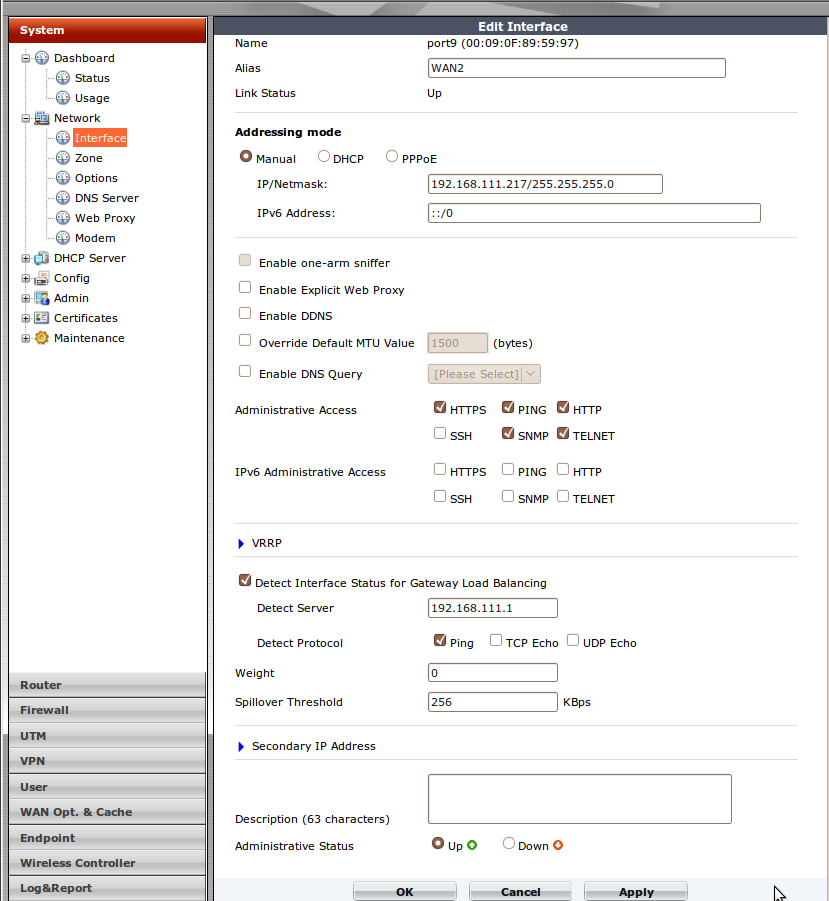
1. Configuración viá GUI de ECMP Basado en Uso (Spillover)

En la configuración de las interfaces, hemos configurado el parámetro de Spillover.

* Configurando el Umbral de Spillover en las Interfaces.

Navegando desde System->Network->Interface, donde configuraremos los umbrales de Spill para cada una de las Interfaces.



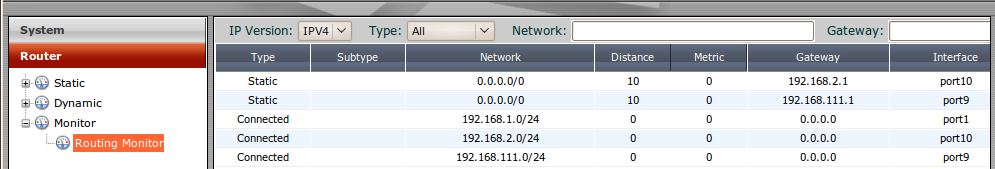


* Cambiando el método de ECMP.

*config system settingsset v4-ecmp-mode usage-based*

*end*

Si navegamos en Router->Monitor->Routing Monitor veremos que las rutas hacia el mismo destino (en este caso, las que apuntan a la red 0.0.0.0 0.0.0.0) son idénticas en cuanto a métrica y distancia.



Por lo tanto, el FortiGate enviará todas las sesiones a través de la ruta 1 por el gateway 192.168.2.1 y solo hasta que la interface port10 (WAN1) haya excedido el Umbral de Spillover de 128KBps pasará todas las nuevas sesiones a través de la siguiente ruta que sería por el gateway 192.168.111.1 y la interface Port9 (WAN2)

A través de la linea de comando (CLI), se puede determinar si una interface está excediendo el umbral de desbordamiento (Spillover Threshold), de la siguiente manera:

*diagnose netlink dstmac listdev=lo mac=00:00:00:00:00:00*

*rx\_tcp\_mss=0 tx\_tcp\_mss=0*

*overspill-threshold=0 bytes=0 over\_bps=0 sampler\_rate=0*

*dev=port10 mac=00:00:00:00:00:00 rx\_tcp\_mss=0 tx\_tcp\_mss=0*

*overspill-threshold=128000 bytes=1179 over\_bps=0 sampler\_rate=0*

*dev=port9 mac=00:00:00:00:00:00 rx\_tcp\_mss=0 tx\_tcp\_mss=0*

*overspill-threshold=256000 bytes=132 over\_bps=0 sampler\_rate=0*