Trabajo Practico Nº1

Netkit: STP, Port Bonding, y VLAN

Juliana Consolati,
Franco Gozzerino y Matías Uberti

June 8, 2019

Introduccion:

En este trabajo práctico se analizaran tres tipos de protocolos de conexiones: Port Bonding, Vlan y Stp. Se los arribará con el uso del software Netkit simulandos en distintos tipos de laboratorios para, de esta manera comprender como funcionan experimentando con estos.

Para comprender mejor estos conceptos primero debemos definir lo que seria un bridge/switch, que en este cso los utilizaremos para conectar nuestras interfaces.

- El bridge en si, permite unir dos conecciones haciendo la transferencia de datos de una red hacia otra con base en la dirección física de destino de cada paquete.
- Un switch sin embargo es un dispositivo de interconexión, sin límite exeptuando por la cantidad de puertos fisicos, utilizado para conectar equipos en red formando lo que se conoce como una red de área local (LAN) y cuyas especificaciones técnicas siguen el estándar conocido como Ethernet

Definiciones:

STP

Spanning Tree Protocol (STP) es un protocolo de capa 2 que se ejecuta en bridges y switches. La especificación para STP es IEEE 802.1D. El propósito principal de STP es garantizar que no se creen loops cuando haya ciclos en la red. Los loops son fatales para una red. Por este motivo se decidio implementarlo en un cuclo de switches.

Con STP, la clave es elegir para todos los switches en la red un root bridge que se convierta en el centro de la red. Las demás decisiones sobre la red, como qué puerto se debe bloquear y qué puerto se debe colocar en el modo de reenvío, se toman desde la perspectiva de este root bridge. Un entorno conmutado, que es diferente a un entorno de bridge, es más probable que trate varias VLAN. Cuando se implementa un root bridge en una red de switching, usualmente se refiere al root bridge como el switch root. Cada VLAN debe tener su propio root bridge porque cada VLAN es un dominio de broadcast separado. Todas las roots de las diferente VLAN pueden residir en un un solo switch o en varios switches.

Todos los switches intercambian información para su uso en la selección del switch root y para la configuración subsiguiente de la red. Las unidades de datos de protocolo de bridge (BPDU) llevan esta información. Cada switch compara los parámetros en la BPDU que el switch envía a un vecino con los parámetros en la BPDU que el switch recibe del vecino.

VLAN

Las VLAN (redes de área local virtuales) pueden considerarse como dominios de difusión lógica. Una VLAN divide los grupos de usuarios de la red de una red física real en segmentos de redes lógicas. Es un método para crear redes lógicas independientes dentro de una misma red física Varias VLAN pueden coexistir en un único conmutador físico (Switch en nuestro caso) o en una única red física. Son útiles para reducir el dominio de difusión y ayudan en la administración de la red, separando segmentos lógicos de una red de área local.

Esta implementación proporciona soporte al estándar de identificación IEEE 802.1Q VLAN con la posibilidad de permitir que en los adaptadores Ethernet se ejecuten varios ID de VLAN. Cada ID de VLAN está asociado a las capas superiores (IP, etc) con una

interfaz de Ethernet independiente y crea instancias lógicas del adaptador Ethernet para cada VLAN, por ejemplo, ent1, ent2 y así sucesivamente.

Se han definido diversos **tipos de VLAN**, según criterios de conmutación y el nivel en el que se lleve a cabo. Así, la VLAN de nivel 1 define una red virtual según los puertos de conexión del switch. La VLAN de nivel 2 (basada en la dirección MAC) define una red virtual según las direcciones MAC de las estaciones. Este tipo de VLAN es más flexible que la VLAN de primer nivel, ya que la red es independiente de la ubicación de la estación.

Además de las anteriores, existe la VLAN de nivel 3, que incluye diferentes tipos. La VLAN basada en la dirección de red conecta subredes según la dirección IP de origen de los datagramas (o paquete de datos). Este tipo de solución brinda gran flexibilidad, en la medida en que la configuración de los conmutadores cambia automáticamente cuando se mueve una estación. En contrapartida, puede haber una ligera disminución del rendimiento, ya que la información contenida en los paquetes debe analizarse detenidamente. La VLAN basada en protocolo permite crear una red virtual por tipo de protocolo (por ejemplo, TCP/IP, IPX, etc). Por lo tanto, se pueden agrupar todos los equipos que utilizan el mismo protocolo en la misma red.

La VLAN permite definir una nueva red por encima de la red física y, por lo tanto, ofrece diversas ventajas: una mayor flexibilidad en la administración y en los cambios de la red, ya que la arquitectura puede cambiarse usando los parámetros de los conmutadores; un aumento de la seguridad, puesto que la información se encapsula en un nivel adicional y puede ser analizada; una disminución en la transmisión de tráfico en la red.

Port bonding

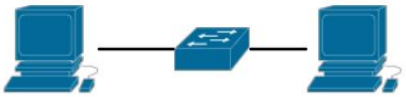
Es un protocolo que permite agrupar varias conexiones ethernet en una sola. Si tenemos un NAS o un ordenador con dos o más interfaces de red (conexiones ethernet) podemos fusionarlas de tal manera que tengamos una sola y que el resultado sea la suma de ambas.

En si, es una técnica que permite agregar varios interfaces de red físicos en uno único virtual. A cada interfaz físico se le denominará esclavo (slave). Con esto podemos realizar un balanceo de carga entre las dos interfaces y conseguir un ancho de banda final igual a la suma de los anchos de banda de cada esclavo. Además de una ventaja adicional inmediata: redundancia de la conexión, lo que implica que si tenemos varios enlaces físicos a la red, perder alguno de ellos supondría una degradación de servicio pero no la pérdida completa de conexión.

En las redes informáticas, el término agregación de enlaces se aplica a varios métodos de combinación (agregación) de múltiples conexiones de red en paralelo con el fin de aumentar el rendimiento más allá de lo que una sola conexión podría soportar, y para proporcionar redundancia en caso de que uno de los enlaces falle.

Procedimiento :

Bridge/Switch:

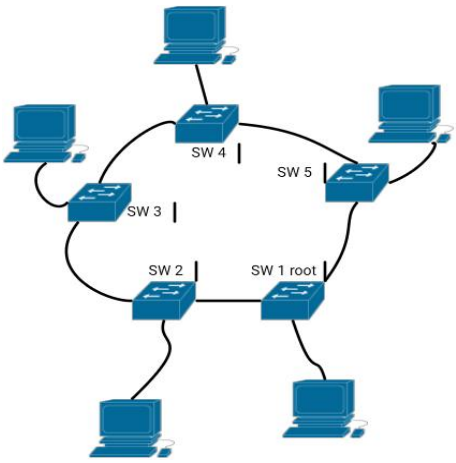


Para el laboratorio de Swtich creamos 3 "PCs" y las conectamos entre si, la cual una de ellas sera nuestro Switch. Para lograr esto, en la pc del medio pondremos los siguientes comandos. De esta manera la configuramos como un bridge virtual, haciendo la transferencia de datos entre la PC1 y la PC2:

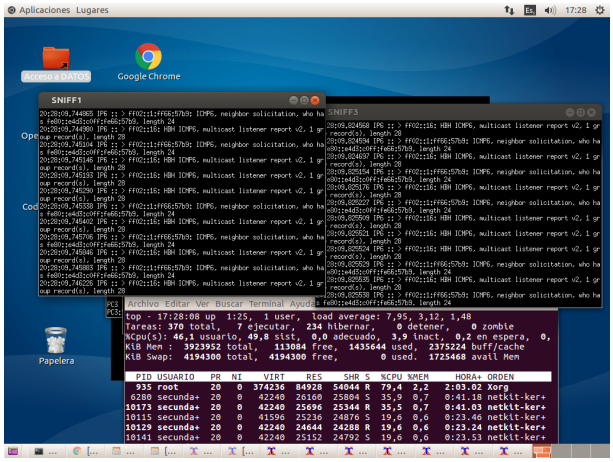
1. `brctl addbr br0`
2. `brctl addif br0 eth0`
3. `brctl addif br0 eth1`
4. `ifconfig br0 up`
5. `ifconfig eth0 up`
6. `ifconfig eth1 up` Una vez hecho esto la PC del medio se convertira en Bridge.

STP:

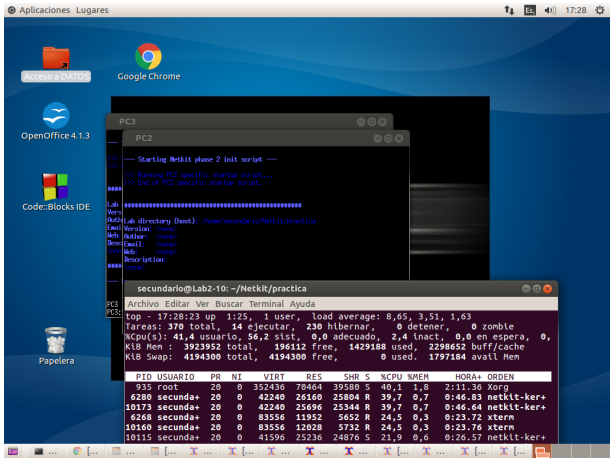
Para los laboratorios STP creamos una serie de switches en loop para poder analizarlos y usar el comando `top` en la consola de Linux para ir viendo el consumo de CPU y memoria que realizaba la red cuando hacia un *ping* desde una computadora a otra pasando por el ciclo de conmutadores. Para esto pusimos 5 switches en anillo (circulo), y cinco computadoras y a cada una le asignamos una IP diferente con el comando ifconfig eth0 seguido de su respctiva IP. Y a cada switch lo configuramos añadindo bridges para poder interconectarse entre si y con las otras computadoras. Ademas este protocolo requiere un switch *root* que se convierta en el centro de la red(en el caso de no especificar cual sea, se elige 1 que este lo mas cerca posible de todos). Las demás decisiones sobre la red, como qué puerto se debe bloquear y qué puerto se debe colocar en el modo de reenvío, se toman desde la perspectiva de este root bridge.



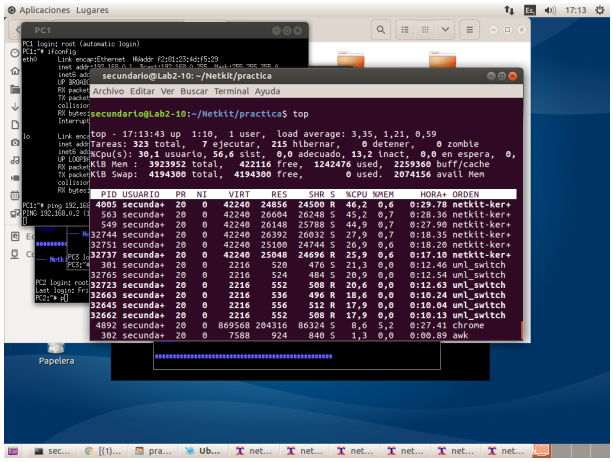
Cuando haciamos esto sin utilizar el protocolo STP al ejecutar el comando top nos mostraba esto:



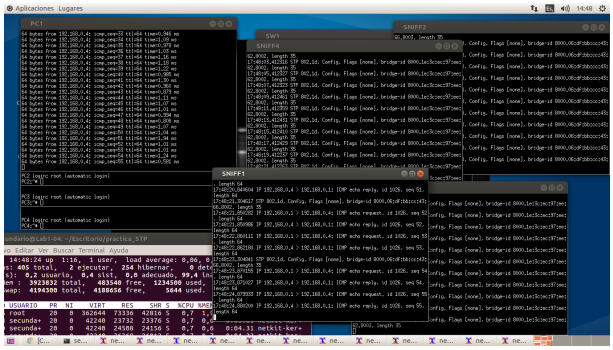
Un dato curioso es que cuando minimizabamos los sniffers el consumo del CPU disminuía notoriamente:



Y por ultimo cuando activamos el protocolo STP en los switches ya el uso del CPU disminuía a un consmo normal y practicamente nulo:



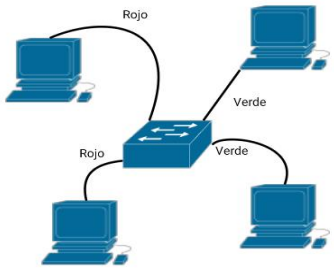
Para hacer esto deberemos usar el comando `brctl stp br0 on` Lo que hace esto es encender el protocolo STP.



Luego, si queremos establecer el root manualmente deberemos usar el comando `brctl setbridgeprio br0` en el switch que deseemos.

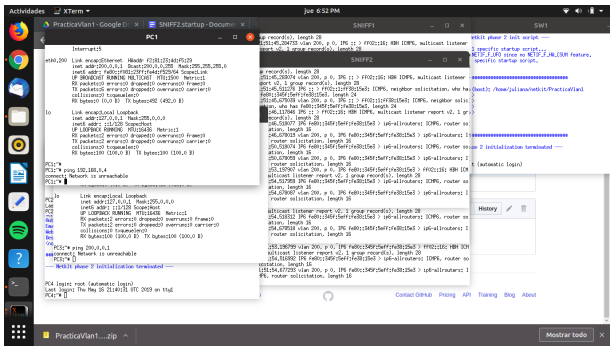
VLAN

Para experimentar con este protocolo lo que hicimos fue, conectar cuatro PCs a un solo switch y hacer que dos de estas pertenezcan a un "color" y las otras dos a otro. Para asignar el color utilizamos el comando `vconfig` y un número, lo que llamamos de manera coloquial el color. Luego para configurara el puerto (eth) lo que debemos hacer es usar el comando `ifconfig eth0.100 100.0.0.1/24 up` a cada PC, donde 100 seria la identificacion de una red lógica. Teniendo en cuenta cómo se configura podemos observar que un puerto puede pertenecer a varias VLAN.

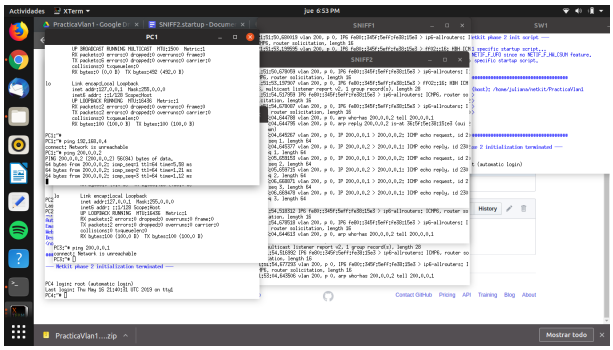


Le asignamos IPs a las VLAN: 200 a las PC1 y 2, y el numero 300 a las PCs 3 y 4. Entonces tratamos de realizar un ping de la

PC1 a la PC4, solo para asegurarnos de que si la VLAN funciona, deberia aparecer el mensaje *network is unreachable*, lo cual es lo que pasa:



Y luego transmitimos desde la PC1 a la PC2.



Ahora lo que hicimos fue, realmente, dividir el **dominio de broadcast** o sea hicimos la VLAN en el switch. En este lo que haremos sera crear 2 bridges de manera que, 2 PCs se conecten a un bridge (un "color") y los otros 2 se conecten al otro bridge(el otro "color").

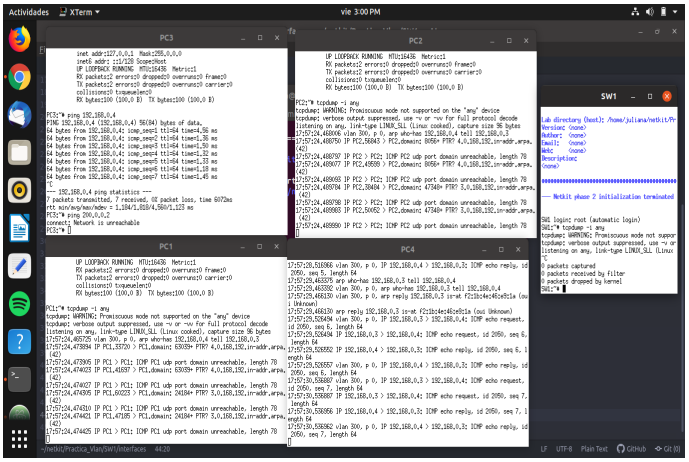
Otra forma de hacerlo seria: En el mismo nos vamos a */etc/network/interfaces* en donde modificamos el archivo y dentro de el a la sección iface añadir parámetro: `|vlan-raw-device`eth0— El nombre de la interfaz debe ser el nombre de la interfaz en bruto (el mismo que el especificado por vlan-raw-device), luego un punto, luego el ID de la VLAN, por ejemplo eth0.100. Puede ser "vlan" y luego el ID de la VLAN, por ejemplo vlan100. En cualquier caso, el ID de la VLAN está en el extremo, y este es el único lugar en el que está configurado.

Con el comando `|iface`eth0.100 inet static— le asignamos una direccion de IP estatica, dependiendo la VLAN, para cada puerto del switch, asi luego levantamos un bridge solo y despues, en nuestro caso levantamos otros dos (`auto br0.100` y `auto bro.200`) para cada VLAN.

Cabe destacar que este ultimo metodo no funciona en Netkit debido a que este no permite hacer —Vlan aware—, aunque cambiando el kernel del mismo es teoria es posible. Pero en un Switch real deberia funcionar perfectamente. El archivo final esta en el GitHub url: `https://github.com/julianaconsolati/Redes-Netkit/blob/master/Practica_Vlan/SW1.startup`

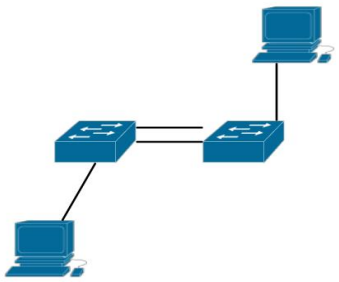
En la siguiente imagen se puede ver que luego de hacer todo esto, uso de *SNIFFS* a las PC1 PC2 Y PC4, trato de hacer un ping de la PC3 a la PC4, ademas de que lo reciben porque

ahora si estan en el mismo dominio de broadcast, los sniffers detectan esta comunicacion. Pero luego intento comunicar la PC3 con la PC2 no puedo hacerlo, aparece en pantalla `Network is unreachable` y lo importante es que como estan en diferentes dominios de broadcast, los sniffers no detectan que se quiso realizar ninguna comunicacion.



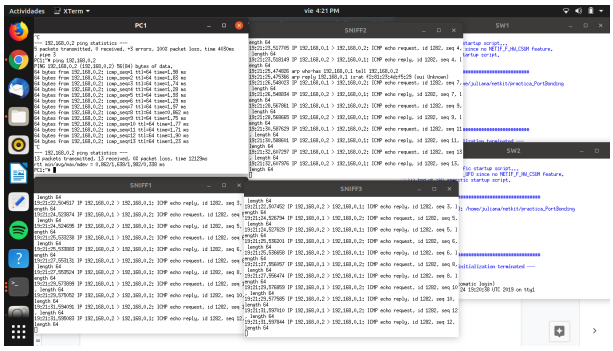
Port Bonding

Para experimentar el protocolo Port Bondig lo que hicimos fue conectar dos switches entre si con dos cables y luego activamos el protocolo con los comandos, estos lo que hacen es que los 2 cables actuen como uno solo, de manera que un aquete va por un cable y el paquete que le sigue va por el otro:

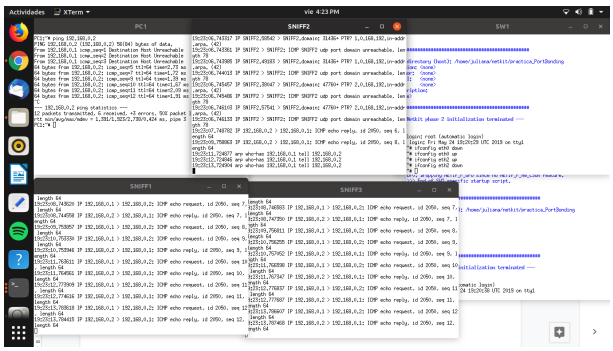


1. `modprobe bonding`
2. `echo balance-rr > /sys/class/net/bond0/bonding/mode`
3. `echo +eth0 > /sys/class/net/bond0/bonding/slaves`
4. `echo +eth1 > /sys/class/net/bond0/bonding/slaves`

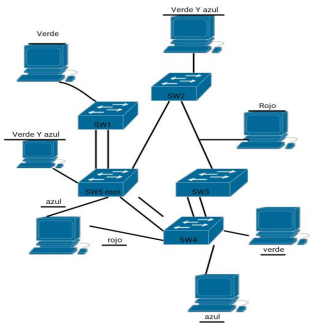
En la siguiente imagen estamos viendo la prueba que realizamos, haciendo un `ping` de la PC1 a la PC2. Y vemos como la informacion pasa por ambos cables y llega completa sin ningun error al receptor. Observando esto podemos deducir que un switch puede tener mas de un port bonding.



A su vez vimos lo que pasaba si bajabamos uno de los cables del Bonding, o sea dejabamos de transmitir por ahi, observamos que el paquete se manda solamente por el cable que queda, dejando la configuracion que hicimos en un principio del switch.



Experimento final



Con el conocimiento adquirido de las anteriores investigaciones, pruebas, e indagaciones. Pasamos a realizar un escenario de un laboratorio de 5 switches y 7 computadoras, aplicando los protocolos STP, VLAN, y Bonding.

Dividimos la red en tres VLANs y le asignamos las IPs 100, 200, y 300: (rojo, verde, azul respectivamente en el gráfico). Y lo interesante de este laboratorio es que dos switches, el SW4, y el SW5 (root) tienen dos port bondings.

Lo diseñamos de esta manera para que por ejemplo: cuando desee comunicarme con una PC dentro de una misma VLAN si o si pase por minimo dos Switchs, y corroborar que todo funcione.

De esta forma, comunicamos la PC3 con la PC6 que ambas comparten VLAN 100 (rojo), aunque la PC6 tambien pertenezca a la VLAN con IP 300, funciona, esto es porque solo nos interesa la VLAN que comparte con la computadora nro 3.

Con esto, corroboramos que andan los 3 protocolos, el STP porque no se hizo un ciclo infinito dentro de los switches en anillo que ubicamos, la VLAN porque se comunican correctamente las compuntadoras con un mismo dominio de broadcast, y el port bonding ya que los paquetes enviados pasan por switches los cuales aplican este protocolo y todos estos los recibe la PC receptora.