Laboratorio de Diseño de Redes de Capa 2

Introducción

El propósito de estos ejercicios es construir una red de capa dos (con conmutadores), utilizando los conceptos que han explicado durante el taller. Los participantes van a construir una topología de estrella, agregación, redes virtuales (VLANs), Protocolo de detección de bucles, y ver como todo funciona al mismo tiempo.

Vamos a tener cinco (5) grupos de estudiantes, con cuatro (4) conmutadores por grupo. La distribución del espacio de direcciones de IP para las redes capa dos de los edificios, es como sigue:

* Grupo 1: 10.10.64.0/24
* Grupo 2: 10.20.64.0/24
* Grupo 3: 10.30.64.0/24
* Grupo 4: 10.40.64.0/24
* Grupo 5: 10.50.64.0/24

Tipos de Conmutadores a ser utilizados en el laboratorio

Cisco 3725 con modulo de 16 Port 10BaseT/100BaseTX EtherSwitch (NM-16ESW)

Nota: Este modelo es realmente un enrutador, pero el módulo de 16 puertos tiene la capacidad de un conmutador básico, y vamos a utilizarlo como tal. Lamentable, Dynamips no soporta la emulación de los conmutadores Cisco Catalyst.

Instrucciones de Acceso al Laboratorio

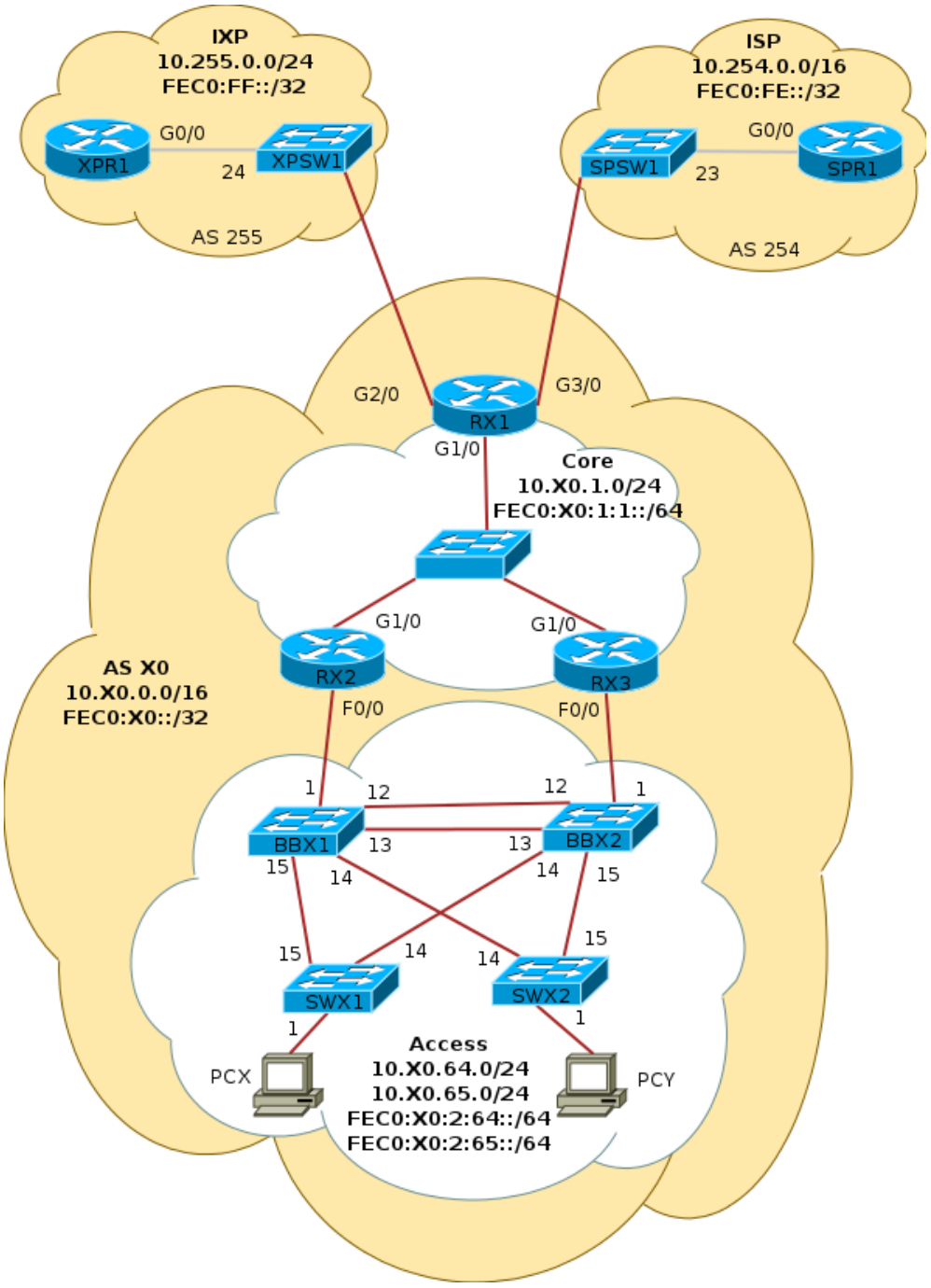
Ver el archivo llamado [lab-access-dynamips]

Red Jerárquica y Redundante

Nuestro segmento de red en el edificio está compuesta por dos conmutadores dorsales redundantes y dos conmutadores de acceso. Los conmutadores dorsales se conectan al núcleo de capa tres y sirven como punto de agregación para los conmutadores de acceso. Los conmutadores de acceso sirven a los usuarios finales. Cada conmutador de acceso tiene una conexión a cada conmutador dorsal,

de forma tal que si uno de los conmutadores dorsales falla, el conmutador de acceso tendrá una alternativa de conexión.

Topología del Laboratorio



== 1ra PARTE ==

Configuración Básica del Conmutador

Para cada conmutador realice la instrucciones siguientes:

1. Asigne un nombre al conmutador

~~~~~~
```
enable
config terminal
hostname <NOMBRE>
```
~~~~~~

2. Configure la Autentificación

~~~~~~
```
aaa new-model
aaa authentication login default local
aaa authentication enable default enable
username nsrc secret nsrc
enable secret nsrc
service password-encryption
line vty 0 4
 transport preferred none
line console 0
 transport preferred none
```
~~~~~~

3. Configure el respaldo de reporte de actividades

~~~~~~
```
no logging console
logging buffered 8192 debugging
```
~~~~~~

4. Deshabilite la resolución de DNS

~~~~~~
```
no ip domain-lookup
```
~~~~~~

5. Salga del modo de configuración y guarde la configuración:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
end
write memory
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

Configuración de la Dirección de IP

1. Asigne una dirección de IP para cada conmutador siguiendo el ejemplo de más abajo:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
int vlan 1
 ip address 10.X0.64.Y 255.255.255.0
 no shut
end
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

Remplace la “X” con el octeto que corresponde a su grupo, en la lista de prefijos de IP, y remplace la “Y” como sigue:

    BBX1: 10.X0.64.4
    BBX2: 10.X0.64.5
    SWX1: 10.X0.64.6
    SWX2: 10.X0.64.7

Verifique la conectividad haciendo un ping a cada conmutador. No continúe hasta que todos los conmutadores se puedan ver en ambas direcciones.

CONSEJO: Si el ping falla, pero la configuración se ve bien, trate de hacer lo siguiente:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
int vlan 1
 shutdown
 no shutdown
end
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

(esto no es necesario o normal, pero es posible que sea un problema con el sistema operativo)

Protocolo de Detección de Bucles - Spanning Tree Protocol (STP)

STP Status

Ejecute los siguientes comando y preste mucha atención a la salida:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
show spanning-tree brief
show spanning-tree blockedports
show spanning-tree
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

a. Cuál es la prioridad de cada conmutador?

b. Cuál conmutador es el raíz? Por qué?

c. Cuales puertos están bloqueados? Por qué?

Configuración de STP

1. Configure las prioridades de STP explícitamente para cada conmutador, de acuerdo con el plan en el apéndice A.

Por ejemplo, en BB11:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
BB11(config)#spanning-tree vlan 1 priority 12288
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

2. Verifique:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
show spannning-tree brief
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

Por que es importante el asignar prioridades explícitamente?

Deshabilite STP

Ahora vamos a deshabilitar SPT para ver que efecto tiene.

CUIDADO : Deshabilitar STP en este laboratorio causará que dynamips incremente la carga del CPU de la máquina virtual. Por esta razón, no podemos tener a todos los grupos deshabilitando

STP al mismo tiempo. Vamos a tomar turnos de cisco (5) –a diez (10) minutos por grupo.

COMUNIQUESE CON EL INSTRUCTOR ANTES DE DESHABILITAR EL STP!!!

Cuando el instructor le comunique que está bien, ejecute el siguiente comando en cada conmutador:

~~~~~~
no spanning-tree vlan 1
~~~~~~

Pueden los conmutadores verse de manera confiable? Por qué?

Mire los contadores de los puertos de interconexión entre los conmutadores.

~~~~~~
show interfaces stats
show process cpu
~~~~~~

Que está pasando con los contadores de las interfaces entre conmutadores? Por qué cree que está pasando esto?

Rápidamente habilite STP en todos los conmutadores:

~~~~~~
spanning-tree vlan 1
~~~~~~

Simule un fallo de uno de los conmutadores dorsales

1. Desconecte BBX1 del resto de la red:

~~~~~~
interface range fastEthernet 1/12 - 15
 shutdown
~~~~~~

Mientras está desconectado del resto, verifique el estatus de STP en los demás conmutadores.

a. Quién es el conmutador raíz ahora?

b. Verifique el papel de los puertos y el estatus. Verifique la conectividad con ping.

2. Reconecte BBX1:

~~~~~~
interface range fastEthernet 1/12 - 15
 no shutdown
~~~~~~

Que le pasó a STP ahora que el conmutador está en línea?

== 2da PARTE ==

VLANs

Ahora vamos segmentar la red para separar el tráfico de los usuarios del tráfico de voz sobre IP (VoIP) y del tráfico de administración de los dispositivos. Cada uno de estos segmentos serán un subred diferente e independiente.

Configure los conmutadores con las VLANs de DATA, VOIP y MGMT.

El protocolo VTP (VLAN Trunking Protocol) es una tecnología propietaria de Cisco Systems que permite el aprovisionamiento dinámico de VLANs. VTP no será utilizado para este taller.

1. Configure VTP en modo transparente para deshabilitarlo:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
vtp mode transparent
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

2. Crear las nuevas VLANs en la base de datos de VLANs y asígneles un nombre que lo ayude a identificarlas:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
vlan 64
 name DATA
vlan 65
 name VOIP
vlan 255
 name MGMT
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

3. Mueva la dirección de IP en VLAN 1 a la vlan MGMT (note que la nueva subred usa el octeto 255):

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
interface vlan 1
 no ip address
interface vlan 255
 ip address 10.X0.255.Y 255.255.255.0
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

Verifique la conectividad entre los conmutadores. Puede hacerle ping a todos? Que falta?

4. Configure los puertos de enlace entre los conmutadores como troncales. Haga lo siguiente para cada puerto que necesite marcar las tramas de VLANs:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
interface FastEthernet1/14
 switchport mode trunk
 switchport trunk encapsulation dot1q
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

Nota: Revise la figura 1 para ver que puertos necesitan ser modificados. BBX1 y BBX2 están conectados a enrutadores en el puerto FastEthernet1.1. Este puerto debe ser configurado como una troncal también.

Trate de hacer ping entre los conmutadores de nuevo. Si no está funcionando como debe ser, debería funcionar.

5. Designe cinco (5) puertos de acceso para las VLANs DATA y VOIP:

En los conmutadores SWX1 and SWX2 solamente:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
interface range Fast1/1 - 5
 switchport mode access
 switchport access vlan 64
!
interface range Fast1/6 - 10
 switchport mode access
 switchport access vlan 65
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

Verifique que puertos ahora son miembros o troncos para cada VLAN:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
show vlan-switch id <VLAN ID>
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

Imagine que tenemos computadoras conectadas a la VLAN de DATA. Usted cree que podrían hacerle un ping al conmutador? Explique su respuesta.

Verifique el estatus del Spanning Tree:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
show spanning-tree brief
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

Preste atención a la raíz y la prioridad del conmutador para cada VLAN (1,64,65,255). Son el mismo?

Nota: Esta configuración se llama Spanning Tree por VLAN (PVST). En esta configuración, los conmutadores crean cuatro (4) arboles diferentes, cada uno con sus propios parámetros, estatus, computaciones, etc. Imagine que usted tenga cientos de VLANs. Obviamente, PVST no es ideal en este caso. Existen mejores modelos, como el Spanning Tree Multiple (MST), que permiten que el administrador cree un número deseado de arboles, y se pueden asignar grupos de VLANs a cada árbol. Desafortunadamente, el conmutador que estamos usando en este taller no soporta MST.

Balanceado de las cargas de las VLANs usando PVST

Los dos conmutadores dorsales están conectados a un enrutador de núcleo (que no se muestra en algunas figuras).

Suponga que usted quisiera balancear el tráfico de todas las VLANs cuando el tráfico va hacia los enrutadores. Que tendríamos que hacer para lograr esto?

1. Configure BBX1 como la raíz para las VLANs 64 y 65; y configure BBX2 como el conmutador raíz para la VLAN 255. Además configure cara conmutador como la raíz secundaria para las otras VLANs:

En BBX1:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
spanning-tree vlan 64 priority 12288
spanning-tree vlan 65 priority 12288
spanning-tree vlan 255 priority 16384
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

En BBX2:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
spanning-tree vlan 64 priority 16384
spanning-tree vlan 65 priority 16384
spanning-tree vlan 255 priority 12288
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

En los conmutadores SWX1 and SWX2, las prioridades serán la misma para todas las VLANs:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
spanning-tree vlan 64 priority 24576
spanning-tree vlan 65 priority 24576
spanning-tree vlan 255 priority 24576
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

2. Verifique que el conmutador raíz es el adecuado para todas las VLANs:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
show spanning-tree brief
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

Configuraciones Adicionales de STP

PortFast

Portfast es una configuración que permite que los puertos de acceso comiencen a enviar/recibir tráfico tan pronto y sean conectados. En lugar de comenzar al principio de la jerarquía de estados (Bloqueado-Escuchando-Aprendiendo-Reenviando) de STP y que dura hasta treinta (30) segundos; Portfast comienza al final de la jerarquía. El puerto comienza en el estado de Reenvío, y si se detecta un bucle, STP ejecuta todas sus computaciones y bloquea los puertos que lo requieran.

Esta configuración debe ser aplicada solo a puertos que conectan a estaciones finales.

1. Configure los puertos de acceso para que utilicen portfast:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
interface range fast1/1 - 10
 spanning-tree portfast
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

BPDUGuard

Cuando usamos Portfast, los puertos de acceso todavía participan en l proceso de STP. Eso quiere decir que dispositivos conectados a esos puertos pueden enviar BPDUs y participar en (y por lo tanto, afectar el estado de) las computaciones del STP. Por ejemplo, si el dispositivo conectado al puerto de acceso está configurado con una prioridad de conmutador menor, ese dispositivo se convierte en el conmutador raíz y la topología del árbol se convierte en subóptima.

Otra configuración muy útil y que evita esta situación es el BPDUGuard. Cuando se recibe un BPDU en un puerto configurado con BPDUGuard y Portfast, el puerto es deshabilitado.

1. Habilitar BPDUGuard en todos los puertos que están configurados con Portfast:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
spanning-tree portfast bpduguard
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

Agrupación de Puertos

Digamos que ahora queremos aumentar el ancho de banda o introducir redundancia entre los conmutadores dorsales.

1. Configure un Port-Channel entre BBX1 y BBX2:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
interface port-channel 1
 description BBX1-BBX2 aggregate link
!
interface range fast1/12 - 13
 channel-group 1 mode on
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

2. Verifique el estatus:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
show interface port-channel 1
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

Que ancho de banda está disponible para el nuevo puerto agregado? Busque por la línea que dice BW … Kbit/sec

3. Deshabilite uno de los puertos en el canal agregado.

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
interface fast 1/12
 shutdown
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

Cual es el estatus del canal? Está arriba o abajo?

4. Habilítelo de nuevo:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
interface fast 1/12
 no shutdown
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

Nota: Existe un estandar para la creación de puertos agregados llamado protocolo de control de agregación de enlaces (LACP). Lamentablemente el dispositivo que estamos utilizando en el taller no soporta LACP. En el taller estamos utilizando un protocolo propietario de Cisco denominado Etherchannel. La mayoría de los conmutadores modernos tienen soporte para LACP, por lo tanto, recomendamos que se utilice LACP en lugar de protocolos propietarios.

Referencia

Apéndice A – Configuración de Spanning Tree

Refiérase a la tabla de prioridades, mas abajo, para determinar la prioridad de sus conmutadores basado en la función del dispositivo.

Prioridad	Descripción	Notas
0	Nodo de núcleo	
4096	Nodo Redundante de Núcleo	Dispositivos en el núcleo del campus
8192	Reservado	
12288	Agregación Primaria en Edificio	Dispositivos de agregación en el edificio
16384	Agregación Redundante en Edificio	
20480	Agregación Secundaria	Complejos de edificios
24576	Acceso	Prioridad normal para dispositivos de acceso en el edificio
28672	Segundo Nivel de Acceso	Dispositivo conectado en cascada. Esta configuración no es común y de ser posible, debe ser evitado
32768	Por Defecto	Dispositivos que no son nuestros utilizan esta prioridad