Práctica de diseño de redes nivel 2

Introducción

El propósito de esta práctica es construir redes de nivel 2 (conmutadas) utilizando los conceptos explicados en las presentaciones sobre diseño. Los estudiantes podrán observar cómo se combinan la topología en estrella, la agregación de tráfico, las VLANs, el protocolo Spanning Tree, la agregación de puertos y algunas funcionalidades de seguridad en los switches.

Los ejercicios incluirán:

1. Configuración básica de un switch
2. Configuración de Spanning Tree
3. Configuración redundante
4. Configuración de protección del plano de control
5. Agregación de puertos
6. Configuración de MST
7. DHCP Snooping

Habrá 5 grupos de 4 a 6 estudiantes, con 4 switches por grupo. La distribución del espacio IP para las redes nivel 2 será 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

Tipo de switches utilizados en el laboratorio

- Hewlett Packard Procurve Switch 2824 (J4903A)

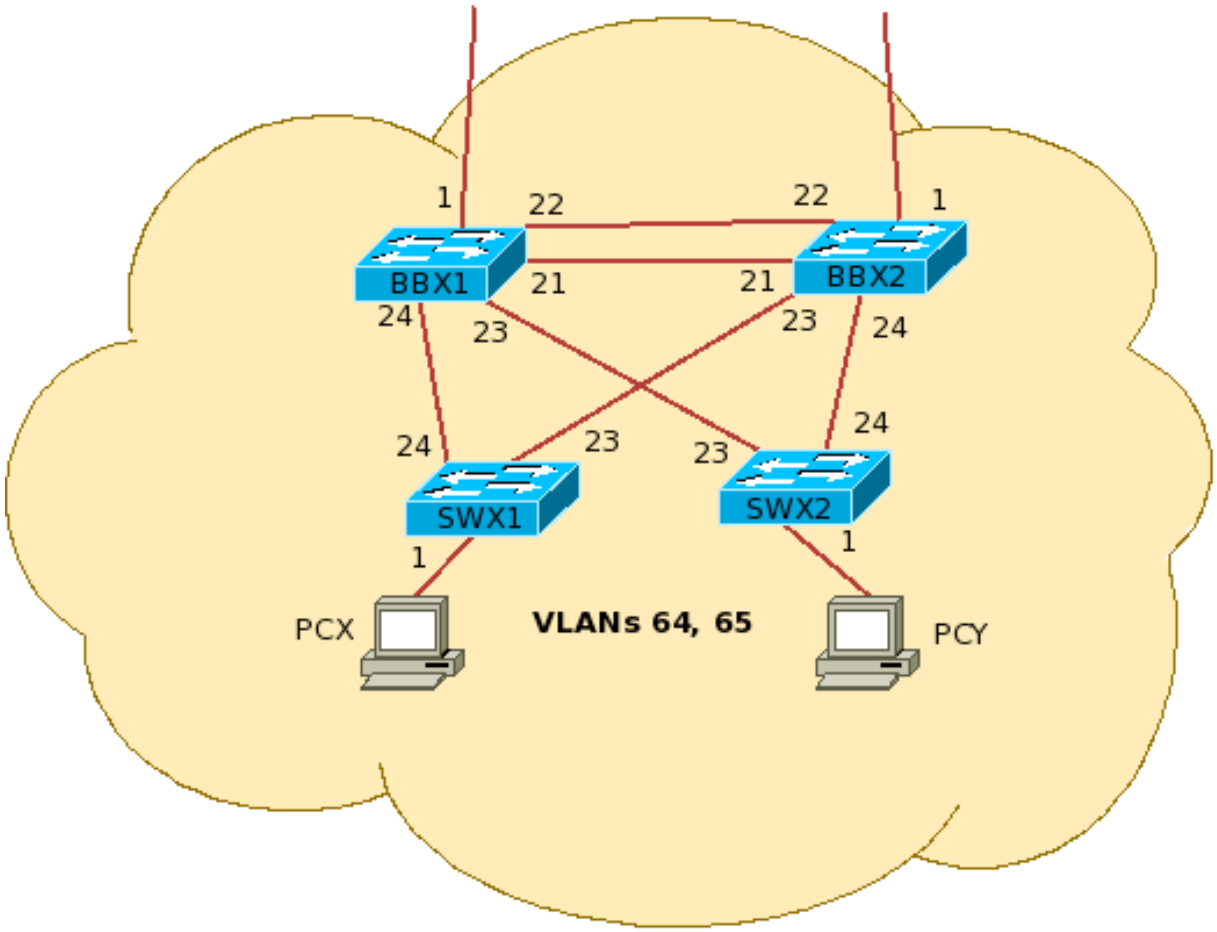
Instrucciones para el acceso remoto

Refiérase al documento llamado *instrucciones-acceso-nsrc-lab.txt*

Breve introducción a la configuración de switches

Vea el Apéndice A

Topología física de nivel 2



Información de diseño de Spanning Tree

Tabla de prioridades

Multiplicador	Prioridad	Descripción	Notas
0	0	Nodo núcleo (core)	Los routers de core no participan en STP. Reservado por si ocurre en un futuro.
1	4096	Nodo núcleo redundante	Los routers de core no participan en STP. Reservado por si ocurre en un futuro.
2	8192		Reservado
3	12288	Dorsal de edificio	
4	16384	Dorsal de edificio redundante	
5	20480	Dorsal secundario	Para complejos de edificios, en que uno o más dorsales secundarios se conectan al dorsal principal
6	24576	Switches de acceso	Prioridad para switches de usuario final (acceso)
7	28672	Switches de acceso	Utilizado por switches de acceso que están conectados en cascada a otro switch de acceso
8	32768	Por defecto	Ningún dispositivo debería tener configurada ésta.

Ejercicios

1. La primera meta es construir una red de switches jerárquica, por lo que utilizaremos un switch para agregación de tráfico (dorsal), y conectaremos dos switches de acceso a éste. Siga estas instrucciones para configurar cada switch:

    a. La configuración inicial para los switches dorsales y de acceso aparece en el **Apéndice B**. Fíjese en las líneas con direcciones IP y sustituya la "X" con el octeto correspondiente del prefijo de su grupo. No se olvide de:
        - Asignar una dirección diferente a cada switch:
            1. Dorsal: 10.X0.64.4
            2. Switch de acceso 1: 10.X0.64.6
            3. Switch de acceso 2: 10.X0.64.7
        - Asignar a cada switch su nombre correspondiente de acuerdo al diagrama
    b. Conéctese a las estaciones de trabajo y verifique sus direcciones IP
        - Estación 1: 10.X0.64.20 conectada al switch11
    c. Verifique la conectividad haciendo "ping" a cada estación y cada switch.

2. En el segundo switch dorsal, todos los enlaces a otros switches están desactivados a propósito. Qué pasa si se activan esos puertos?
    a. Conéctese al switch dorsal secundario y active los puertos 21-24

    ```
    # switch(config)# interface 21-24 enable
    ```

    b. Observe los contadores de tráfico en los puertos de enlaces entre switches. Qué puede observar acerca de los contadores de broadcast/multicast?

    ```
    # show interfaces [port]
    ```

    c. Puede hacer "ping" entre switches de manera consistente? Por qué?
    d. Desactive los puertos otra vez

    ```
    # switch(config)# interface 21-24 disable
    ```

3. Ahora configuraremos el protocolo **Spanning Tree**.
    a. Utilice las configuraciones en el **Apéndice C** and aplíquelas a *BBX1*, *SWX1* y *SWX2*
    b. Cuál es la principal diferencia entre las configuraciones de los switches dorsales y los switches de acceso?
    c. Verifique los roles y estados de los puertos:

    ```
    # show spanning-tree config
    # show spanning-tree
    # show spanning-tree [port] detail
    ```

    Cuál es el switch raíz?
    Cuáles puertos están pasando tráfico (forwarding) y cuáles están bloqueados?

d. Vuelva a activar los puertos en el dorsal secundario. Cómo han cambiado las cosas desde la últiva vez?

4. Qué pasa a la red si el dorsal principal se cae? Ahora introduzcamos **redundancia**.
   a. Configure el switch dorsal secundario. Use la dirección 10.X0.64.5.
   b. Configure Spanning Tree con prioridad "4" en el dorsal secundario
   c. Verifique cuál es el switch raíz y explique por qué
   d. Verifique los roles y estatus de los puertos. Cuáles puertos están bloqueados?
   e. Reinicie el dorsal primario.
      1. Mientras reinicia, verifique el estatus de Spanning Tree. Cuál es el switch raíz? Verifique los roles y estatus de los puertos. Verifique la conectividad.
      2. Qué pasa con el estado del Spanning Tree cuando el dorsal primario vuelve a estar disponible?

5. Ahora queremos segregar el tráfico de usuarios del tráfico de voz y de gestión.
   a. Utilice las configuraciones en el **Apéndice D** para crear **VLANs de DATA, VOIP y MGMT**.
   b. Verifique la conectividad de los switches
   c. Desde las estaciones, intente hacer "ping" a los switches usando sus direcciones nuevas. Qué ha pasado?

6. Ahora queremos obtener más capacidad y redundancia entre los switches dorsales.
   a. Utilice el **Apéndice E** para configurar **Agregación de puertos (bundling)**.
   b. Verifique el estado de la nueva troncal (trunk):

```
# show lacp
```

   c. Qué capacidad de canal tiene ahora en la nueva troncal?
   d. Desactive uno de los puertos en el grupo. Qué pasa con la troncal?

7. Supongamos que fuera necesario balancear el tráfico desde/hacia las dos VLANs a través de los dos switches dorsales. Cómo podríamos lograr esto?
   a. **Configure MSTP** utilizando el **Apéndice F**.
   b. Verifique el estado de cada instancia MSTP. Fíjese en las diferencias entre los roles y estados de los puertos en cada instancia.

8. Si es posible, configure una estación de usuario como servidor DHCP. Utilizando otra estación, verifique si puede obtener una dirección IP. Qué pasa si sus usuarios hicieran esto sin su consentimiento?
   a. Utilice las instrucciones del **Apéndice G** para configurar **Prevención de servidores DHCP ilegítimos**.
      - Repita la prueba. Puede obtener una dirección IP ahora?

Appendix A - HP 28XX/410X Comandos relevantes

```
show config
show running-config [status]
show interfaces [brief] [config]
show system-information
show interfaces brief
show interfaces [port]
clear statistics [port]
show ip
show flash
show spanning-tree [detail]
show vlan <vlan-id>
show lacp
show cdp neighbors
show lldp info remote-device
copy tftp flash <TFTP_SERVER> <IMAGE_FILE> primary
configure
password manager user-name admin
end
write mem
reload
```

Appendix B – Configuración básica (HP2800)

```
hostname "switch"
time timezone -480
time daylight-time-rule Continental-US-and-Canada
lldp run
cdp run
ip icmp burst-normal 20
ip icmp reply-limit
ip ttl 6
vlan 1
   name "DEFAULT_VLAN"
   untagged 1-24
   ip address 10.X0.64.Y 255.255.255.0
   ip igmp
exit
no dhcp-relay
crypto key generate ssh rsa
ip ssh
ip ssh key-size 1024
ip ssh port default
interface all
   no lacp
exit
```

```
no telnet-server
```

Appendix C - Spanning Tree

```
spanning-tree
spanning-tree protocol-version RSTP
spanning-tree priority X*
write mem
reload
```

(*) Refiérase a la tabla de prioridades al comienzo de este documento para determinar las prioridades apropiadas para cada switch. Utilice el valor “multiplicador” aquí.

Appendix D – VLANs de Data, VOIP y Gestión

- **En los dorsales:**

```
vlan 1
   no ip address
   no ip igmp
exit
vlan 64
   name "DATA"
   tagged 1,21-24
   ip igmp
exit
vlan 65
   name "VOIP"
   tagged 1,21-24
   ip igmp
exit
vlan 255
   name "MGMT"
   tagged 1,21-24
   ip address 10.X0.255.Y 255.255.255.0
exit
```

- **En los switches de acceso:**

```
vlan 1
   no ip address
   no ip igmp
exit
vlan 64
   name "DATA"
   untagged 1-12
   tagged 23-24
   ip igmp
exit
```

```
vlan 65
   name "VOIP"
   untagged 13-20
   tagged 23-24
   ip igmp
exit
vlan 255
   name "MGMT"
   tagged 23-24
   ip address 10.X0.255.Y 255.255.255.0
exit
```

Appendix E - Port Bundling

- **En los dorsales solamente**:

```
interface 21-22 disable
trunk 21-22 Trk1 LACP
interface 21-22 enable
vlan 64 tagged Trk1
vlan 65 tagged Trk1
vlan 255 tagged Trk1
```

Appendix F - Multiple Spanning Tree (MSTP)

- En todos los switches:

```
spanning-tree protocol-version MSTP
write mem
reload
```

- En el dorsal principal:

```
spanning-tree config-name "mstp1"
spanning-tree config-revision 1
spanning-tree instance 1 vlan 64 65
spanning-tree instance 1 priority 3
spanning-tree instance 2 vlan 255
spanning-tree instance 2 priority 4
```

- En el dorsal secundario:

```
spanning-tree config-name "mstp1"
spanning-tree config-revision 1
spanning-tree instance 1 vlan 64 65
spanning-tree instance 1 priority 4
spanning-tree instance 2 vlan 255
spanning-tree instance 2 priority 3
```

- En los switches de acceso:

```
spanning-tree config-name "mstp1"
spanning-tree config-revision 1
spanning-tree instance 1 vlan 64 65
spanning-tree instance 1 priority 6
spanning-tree instance 2 vlan 255
spanning-tree instance 2 priority 6
```

Appendix G – Prevención de DHCP ilegítimo

```
dhcp-snooping
dhcp-snooping vlan 64
dhcp-snooping vlan 65
dhcp-snooping vlan 255
no dhcp-snooping option 82
no dhcp-snooping verify mac
dhcp-snooping option 82 untrusted-policy keep
interface <number> dhcp-snooping trust
```

Appendix H – Configuración AAA (Authentication, Authorization and Accounting)

```
no aaa authentication login privilege-mode
aaa authentication console login radius local
aaa authentication console enable local none
aaa authentication telnet login radius local
aaa authentication telnet enable local none
aaa authentication web login radius local
aaa authentication web enable local none
aaa authentication ssh login radius local
aaa authentication ssh enable local none
aaa accounting exec start-stop radius
aaa accounting commands stop-only radius
radius-server dead-time 5
radius-server timeout 3
radius-server retransmit 1
radius-server key verycomplexkey
radius-server host <a.b.c.d>
radius-server host <a.b.c.d>
```

Appendix I – Configuración de Gestión

```
timesync sntp
sntp server <a.b.c.d>
sntp server <a.b.c.d>
sntp unicast
ip icmp burst-normal 20
ip icmp reply-limit
```

```
ip ttl 6
snmp-server location "Edificio B, Salon 101"
snmp-server contact "network services, <noc@localdomain>"
snmp-server community "public" manager restricted
snmp-server host 10.X0.255.5 "public" Not-INFO
snmp-server enable traps authentication
ip authorized-managers 10.X0.255.0 255.255.255.0
no telnet-server
crypto key generate ssh rsa
ip ssh
ip ssh key-size 1024
ip ssh port default
```