EXAMEN FINAL SEGURIDAD EN REDES LAN

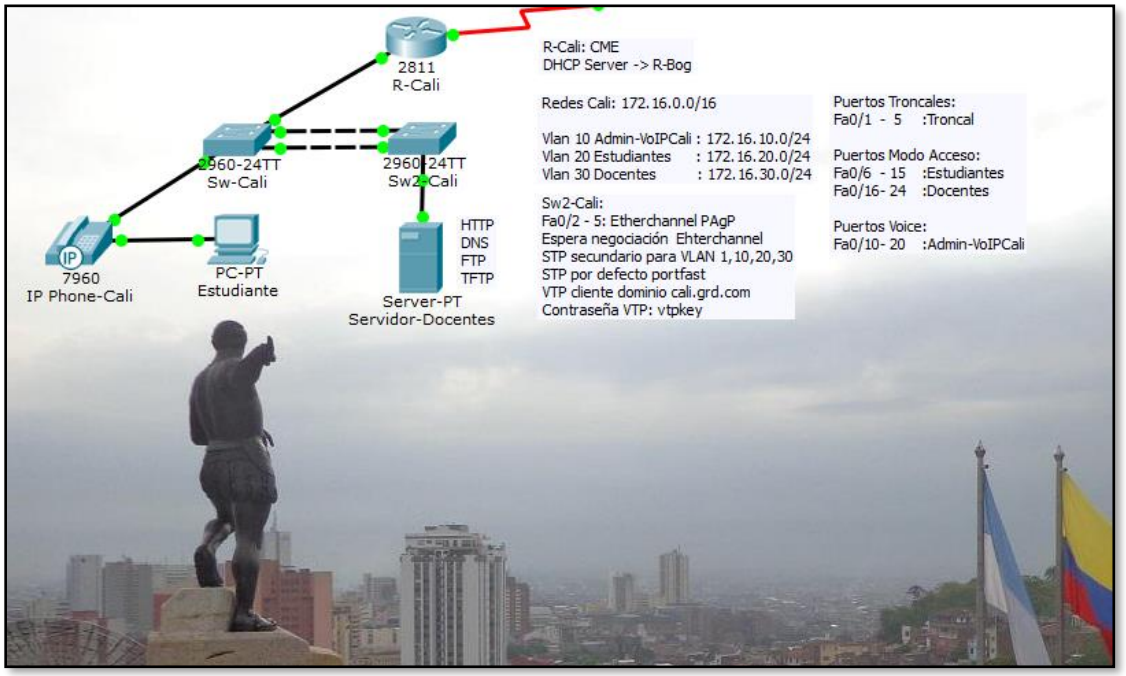
Usted ha sido recomendado para realizar una actualización en la red de una empresa que tiene sedes a nivel Nacional, la actualización se enfocará en 2 objetivos principales, el primero es asegurar todos los puntos en los que encuentre falencias de Seguridad, y el segundo asegurar la alta disponibilidad de la red, implementando algunas mejoras que ayuden a tener un desempeño óptimo de la red.

Después de realizar un relevamiento de Sitio se han descubierto varias falencias en la topología que no solo afectan la seguridad de los datos, sino que también no sacan el mayor desempeño a algunas características de los dispositivos que tiene la compañía, y que con una buena configuración podría asegurar una mayor disponibilidad de la red como tal.

La planificación tomada después del análisis de la compañía, sugiere iniciar a aplicar las mejoras inicialmente en el entorno LAN. Por ende se iniciará a realizar los cambios en mejora de la red en los Switchs de la compañía y finalmente se trabajará en los Routers.

CAMBIOS GENERALES A REALIZAR EN LOS DISPOSITIVOS:

1. CONFIGURACIÓN RED PRINCIPAL CALI:



Dispositivo	Hostname	Mejoras Generales
Router 2811	R-Cali	HSRP, DHCP Relay, NTP, Syslog
Switch 2960	Sw-Cali	RSTP, Portfast, VTP, Etherchannel
Switch 2960	Sw2-Cali	RSTP, Portfast, VTP, Etherchannel

Diseñado por: Gustavo Rodríguez Salinas
Instructor Regional Valle
CCNA, CCAI, CCNP

En la imagen anterior puede visualizar algunos datos importantes para realizar las mejoras de configuraciones solicitadas, información tanto de STP, Etherchannel, VTP, entre otras, se recomienda que se familiarice inicialmente con estos datos, en especial como está diseñado el direccionamiento interno de la LAN de Cali y sus 3 VLAN principales. Una vez tenga lo anterior claro de inicio con la configuración de esta Ciudad, iniciando con los Switchs, y finalmente pasando a realizar las mejoras necesarias en el Router.

1.1 **SWITCHS CALI:** (10 A 20 MINUTOS)

- ✓ Los 2 Switchs de Cali se observó una buena configuración en la parte de seguridad, ya que tienen configurado SSH, encriptación de contraseñas y seguridad de puertos. Además tiene configurado correctamente los puertos troncales y de modo acceso, al igual que la asignación correcta de los puertos a sus respectivas VLAN.

- ✓ Dentro de las configuraciones observamos que en los 2 Switchs se maneja STP, pero no se le está sacando el mejor desempeño a este, por lo tanto **se solicita que ambos Switchs** se configuren para trabajar con **RSTP**, se le habilite la característica de **Portfast** de manera predeterminada globalmente, y se defina a **Sw-Cali como Switch primario** para las VLAN 1**, 10, 20 y 30**, y el **Sw2-Cali se defina como secundario**.

- ✓ En lo relacionado con VTP se observa poca configuración, no tienen dominio definido, no se trabaja con la Versión 2, y no tiene contraseña de autenticación, por lo tanto configure la **versión 2 de VTP**, configure a **Sw-Cali como VTP server y Sw2-Cali como VTP cliente**, el dominio VTP a manejar será **cali.grd.com** y la contraseña de autenticación **vtpkey**.

- ✓ Se desea aprovechar al máximo los 2 enlaces que hay entre los 2 Switchs, pero al no tener agregación de enlaces, el protocolo STP está bloqueando uno de los 2 enlaces. De acuerdo a lo anterior se le solicita configurar con el **Protocolo Propietario de Cisco un enlace Etherchannel en ambos Switchs,** aunque de acuerdo al modo se puede asumir cual será, en la configuración deberá empezar seleccionando **el protocolo solicitado, configure el grupo 1 para los puertos Fa0/2 al Fa0/5, Sw-Cali será el que debe iniciar** el establecimiento del enlace y **Sw2-Cali el que estará a la espera.**

- ✓ Configure todos los puertos troncales **Fa0/1 y Po1** para que la **VLAN nativa sea la 10**, y que **solo permita el tráfico de las VLAN 1, 10, 20 y 30**. Finalmente **guarde la configuración** en ambos Switchs y compruebe con los **comandos de visualización y pruebas de conectividad** que toda la LAN Cali quedó funcionando correctamente, si requiere reiniciar algún Switch, realícelo de ser necesario.

1.2 **ROUTER CALI:** (10 A 15 MINUTOS)

- ✓ El Router de Cali al igual que los Switchs de Cali, tiene varias configuraciones correctamente, entre ellas se destacan SSH, Subinterfaces, y el CME principal de la compañía. En este se iniciará con la configuración de NTP y Syslog, y la habilitación de algunos servicios del Router.

- ✓ Inicie habilitando 2 Servicios fundamentales para la Seguridad y funcionamiento correcto de Syslog, estos **servicios son la encriptación de contraseñas** (este deberá realizarlo también en Bogotá) y el **servicio de marca de tiempo para los log** (Solo en Cali).

- ✓ Ahora configure al Servidor que se encuentra en la LAN Cali como Servidor NTP para R-Cali, este tiene la dirección IP **172.16.30.254**, utilice el mismo host para la configuración de Syslog. Una vez definido el **Servidor NTP y Syslog**, habilite en NTP **la actualización del calendario**, y en Syslog la **captura de cualquier tipo de registro** (debug), al igual que los **registros de información de usuarios**.

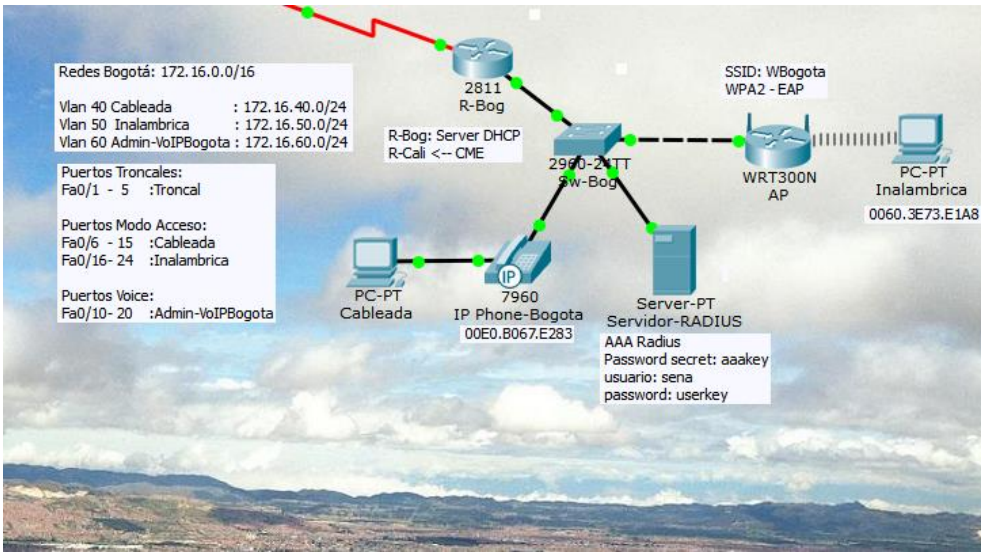
- ✓ Teniendo en cuenta que el Router de Bogotá empezará a manejar los Pool DHCP de toda la compañía de forma Centralizada se le ha solicitado **configurar en R-Cali el reenvío de peticiones DHCP** de todas las subinterfaces, a R-Bog, de las IP que maneja el R-Bog utilice la IP correspondiente a la VLAN Administrativa de Bogotá **(172.16.60.1).**

- ✓ Dentro de las proyecciones de la compañía y con el fin que asegurar una alta disponibilidad, está planificado la compra de un 2º Router en Cali, con el fin de tenerlo como equipo de respaldo, y poder utilizar de ahí en adelante una IP virtual como Gateway de cada una de las 3 VLAN principales. Es por lo anterior que **se les solicita configurar en cada subinterfaz de R-Cali la característica de HSRP**, esto con el fin que en un futuro al agregar el 2º Router, este ya quede listo para actuar como el Router principal.

- ✓ Para la configuración de HSRP tenga muy en cuenta las siguientes indicaciones. **Primero**: el **grupo HSRP tendrá el mismo número de la subinterfaz** que se esté configurando (10,20 o 30), y deberá tener como IP virtual una IP que pertenezca a la VLAN y que en el último octeto se maneje como estándar la IP .250. Ej: VLAN 10 -> 172.16.10**.250**. Segundo: Para cada subinterfaz, y en su grupo HSRP se deberá configurar la mayor prioridad posible y finalmente configurar igualmente el adelantamiento (preempt).

Diseñado por: Gustavo Rodríguez Salinas
Instructor Regional Valle
CCNA, CCAI, CCNP

2. CONFIGURACIÓN RED SUCURSAL BOGOTÁ



Dispositivo	Hostname	Mejoras Generales
Router 2811	R-Bog	AAA.
Switch 2960	Sw-Bog	SSH, Portsecurity, BPDUguard
WRT300N	AP	WPA2-EAP, Disable SSID Broadcast

En la imagen anterior puede visualizar algunos datos importantes para realizar las mejoras de configuraciones solicitadas, información principalmente de la red inalámbrica y AAA, entre otras, se recomienda que se familiarice inicialmente con estos datos, en especial como está diseñado el direccionamiento interno de la LAN de Bogotá y sus 3 VLAN principales. Una vez tenga lo anterior claro de inicio con la configuración de esta Ciudad, iniciando con el Router, luego el AP, y finalmente pasando a realizar las mejoras necesarias en el Switch.

2.1 ROUTER BOGOTÁ: (5 A 10 MINUTOS)

- ✓ Finalmente en el Router de Bogotá, y con el fin de aprovechar el Servidor Radius de esta Ciudad se recomendo que el Router de Bogotá realizara su autenticación por medio de AAA, para esto habilite AAA y configure correctamente tanto la IP del Servidor Radius **172.16.50.254** como la clave secreta **aaakey**, cree la configuración de autenticación llamada **SEGURIDAD** en donde como primera alternativa se busque al Servidor Radius y como segunda la base de datos de usuarios local del router, finalmente asocie el nuevo tipo de autenticación a las lineas tanto de Consola como VTY del Router. Pruebe conectividad con el Servidor y salga de todos los modos para comprobar de nuevo el tipo de autenticación de usuarios. No olvide habilitar el **servicio de encriptación de contraseñas**.

2.2 AP Y PC INÁLAMBRICO: (10 A 15 MINUTOS)

- ✓ Se encuentra en el AP y en la red inalámbrica en general una brecha enorme de inseguridad, ya que manejan esta red con autenticación Abierta, se solicita configurar autenticación **EAP** con cifrado **WPA2**, se debe tener en cuenta que el Servidor Radius cuenta con la IP **172.16.50.254**, y ya se encuentra configurado correctamente con la clave secreta **aaakey**.

Diseñado por: Gustavo Rodríguez Salinas
Instructor Regional Valle
CCNA, CCAI, CCNP

- ✓ Una vez configurado el AP, ingrese al PC Inalámbrico y conéctelo a la red inalámbrica con el usuario **sena**, y la contraseña **userkey,** espere un tiempo prudente para que se realice la conexión, puede ir adelantando otro punto mientras esto ocurre. Tenga en cuenta que este mismo usuario se utilizara más adelante para la autenticación desde el Router de Bogotá. Una vez conectado el PC a la red inalámbrica, vaya al Linksys y **deshabilite la difusión del SSID**.

2.3 **SW-BOG:** (10 A 15 MINUTOS)

- ✓ De todos los dispositivos se encuentra que este Switch es el que tiene más falencias de seguridad, es por esto que inicialmente se solicita que se configure SSH, para esto tenga en cuenta que el dominio en el cual se está trabajando en esta ciudad es **bogota.grd.com**, se requiere que se utilice una clave rsa de longitud 1024, habilite la versión más segura de SSH, y configure el usuario **Sw-Bog** con contraseña cifrada **sena**. Asegure que de aquí en adelante solo se pueda acceder de forma remota por SSH con el usuario creado. Configure que cada vez que se inicie por consola también solo se pueda acceder con el usuario previamente creado
  .
- ✓ Otro inconveniente que se ve muy común en la red es que se conectan Switchs adicionales sin la autorización del Administrador de la Red, generando tráfico no autorizado adicional, por medio de un sniffer (husmeador de red) se logró detectar que en la oficina a donde llegan los puertos **Fa0/6 hasta el Fa0/12** es que se viene presentando la problemática de conexión de **Switchs no Autorizados**, se solicita que en esto puertos se **habilite la vigilancia de BPDU**.

- ✓ Finalmente, en el Sw-Bog **configure seguridad en el último puerto FastEthernet**, que es en el cual se conecta el Servidor Radius, se solicita habilitar la seguridad de puertos, y permitir **máximo 2 MAC** por ese puerto, esto teniendo en cuenta que si hay una posible falla, al realizar un cambio rápido de Servidor este 2º no se vea bloqueado. También se solicita que todo el aprendizaje que se realice de las **MAC confiables se realice de forma automatizada**, y que en el caso de haber una **violación del puerto este inmediatamente se apague**. Genere tráfico desde el Servidor Radius a su Gateway para que el Switch capture su MAC y la guarde automáticamente como confiable. Si la VPN y NAT ya están configurados puede hacer pruebas a www.cali.grd.com y www.google.com.

Una vez finalizado todo compruebe mediante los comandos **show y ping** el correcto funcionamiento de todo, ingrese desde el PC inalámbrico y el PC de Cali a www.cali.grd.com y www.google.com, y realice llamadas del Teléfono IP de Cali a Bogotá. **Tiempo Total:** 45 min, **Máximo:** 1 horas 15 min.

Cualquier duda consúltela con el instructor a cargo de la prueba.

Diseñado por: Gustavo Rodríguez Salinas
Instructor Regional Valle
CCNA, CCAI, CCNP