[Redes Seguras] TurboResumenExpress.txt

[TEMA 1] Diseño de Redes Seguras

Hay 2 modelos de diseño de red básicos, Modelo jerárquico y el de arquitectura de red corporativa Cisco.

1.1 Arquitecturas de Red Corporativa. Modelo Jerárquico

Divide la red en varias capas:

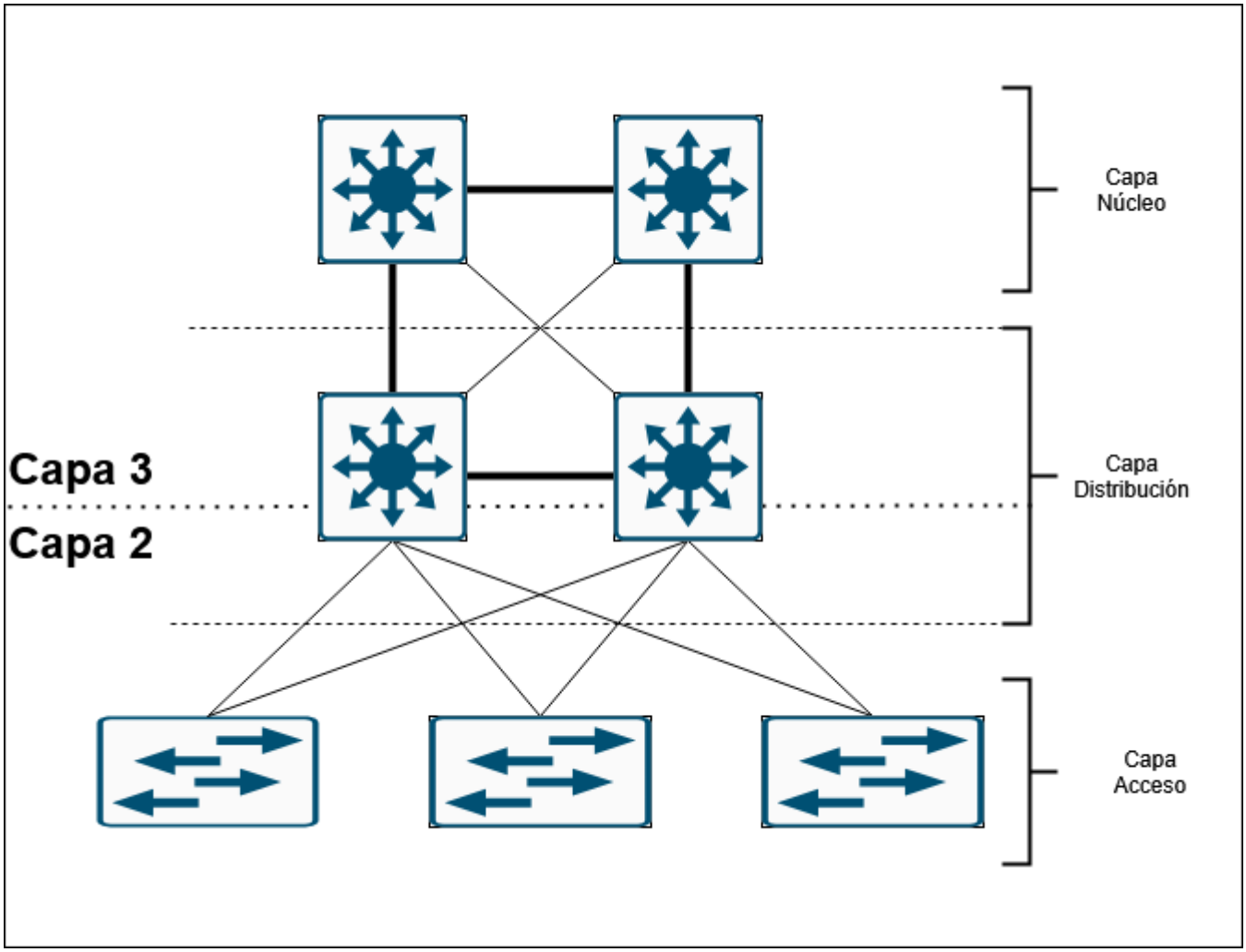
- Capas especializadas en funciones concretas
- Se basa en la estructura jerárquica de la organización
- Facilita la selección de dispositivos, configuración y mantenimienot
- Sirve tanto para WAN como para LAN

1.1.1 Ventajas del modelo Jerárquico

- **Fácil de comprender**, cada elemento implementa una serie de funciones limitadas. La monitorización y los sistemas de gestión pueden ser estructurados por capas.
- **Permite el crecimiento modular**, se maximiza la escalabilidad reutilizando bloques de diseño.
- Mejora la capacidad para **ubicar posibles fallos** en la red.
- **Ahorro de costes** si se aplica bien.

1.1.2 Las capas del modelo jerárquico

El modelo jerárquico cuenta con 3 capas: **núcleo** (Transporte a la mayor velocidad posible), **distribución** (Conectividad basada en directivas) y **acceso** (Acceso a la red a los usuarios finales)



1.1.2.1 Capa de Acceso

Proporciona conexión a los usuarios del segmento local de la red con las siguientes funciones:

- Conmutación en capa 2
- Alta disponibilidad
- Seguridad de puerto
- Limitación del trafico de broadcast
- QoS: clasificación, etiquetado y establecimiento de límites de confianza
- Limitación del ratio de transferencia
- Inspección ARP
- Lista de control de acceso virtual
- POE
- Spanning Tree
- VLANs
- Network Access Control (NAC)

1.2.2.2 Capa de distribución

Centraliza la conectividad de red de un edificio. Sirve como punto de aislamiento entre las capas de acceso y distribución. Punto clave de las redes seguras. Tiene las siguientes funciones:

- Conectividad basada en políticas: Define la conectividad entre grupos de dispositivos. Se aplican reglas que definen los flujos de tráfico permitidos.
- Se pueden implementar mediante ACLs
- Se pueden filtrar actualizaciones de enrutamiento, ser punto de transición entre enrutamientoe stático y dinámico.
- Redundancia y balanceo de carga
- Agragación de conexiones de planta o de enlaces.
- Apliación de Q0S
- Agregación de direcciones
- Definición de dominios de broadcast
- Enrutamiento entre VLANs
- Frontera entre protocolos de enrutamiento estático y dinámico.

1.2.2.3 Capa de Núcleo

Parte central de la red que se encarga de conmutar paquetes de datos a alta velocidad. Tiene las siguientes características:

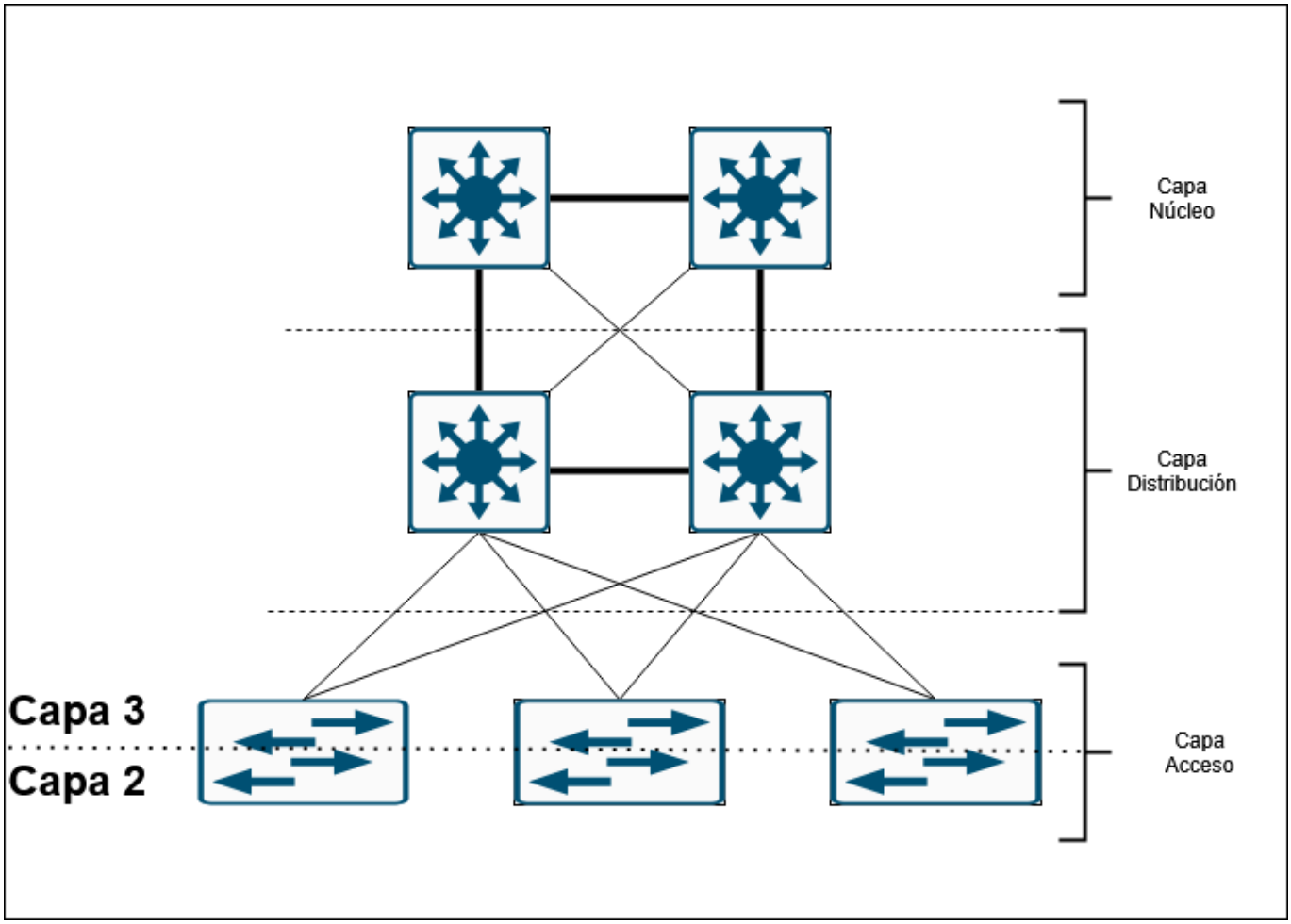
- Alta velocidad
- Baja latencia
- Alta disponibilidad y tolerancia a fallos
- Se debe evitar la manipulación de paquetes
- Diámetro limitado y consistente
- Aplicación de QoS

1.1.2 Implementación tradicional del modelo jerárquico

- Enlaces a Capa 3 entre distribución y núcleo
- Enlaces a Capa 2 ntre distribución y acceso
- Frontera entre capas 2 y en en la capa de Distribución
    - Las Vlan se extienden entre capa de acceso y distribución
    - En la capa de distribución se lleva a cabo el enrutamiento entre Vlans y el núcleo
- Desventaja: Se necesita Spanning Tree para permitir un diseño con enlaces rendundantes en Capa 23.
    - Si hay una sola VLAN, stp provoca que no se pueda balancear la carga
    - Se puede solucionar con Per VLAN STP o Multiple STP

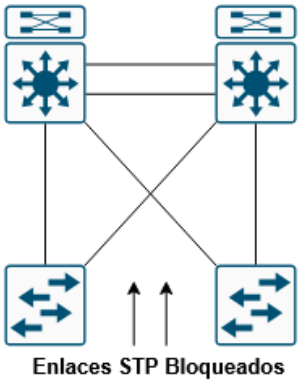
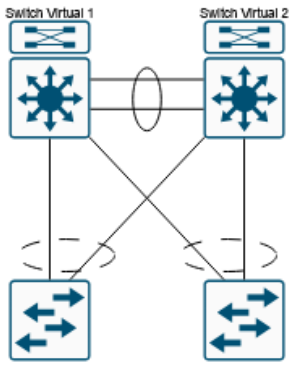
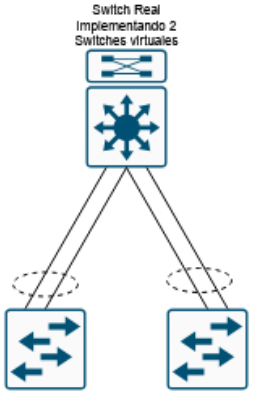
1.1.3 Modelo jerárquico usando capa 3 hasta capa de acceso.

Evita que sea necesario usar STP, permitiendo el balanceo de carga desde la capa de acceso El problema es que es más carlo y las VLAN deben permanecer de forma local en cada switch de la capa de acceso.



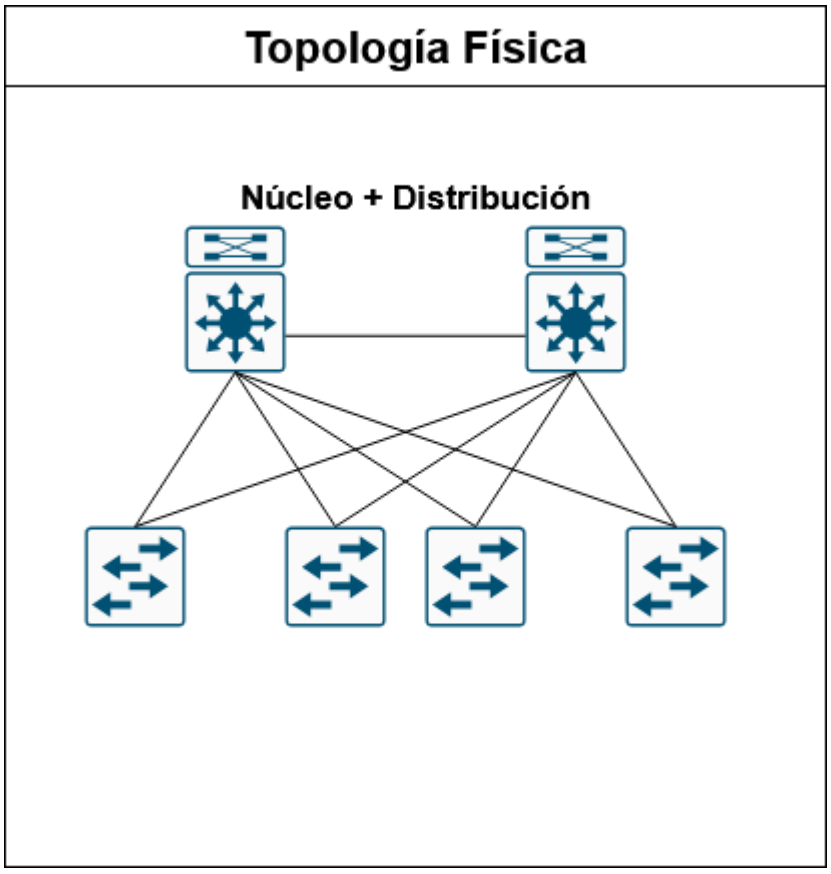
1.1.4 Implementación del modelo jerárquico usando Virtual Switches

Se evita el uso de STP y HSRP, permitiendo el balanceo de carga desde acceso. El proiblema es que es más caro realizar la instalación y la tecnología no es interoperable.

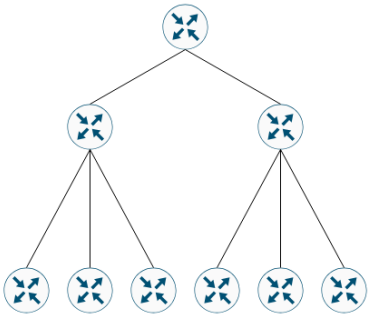
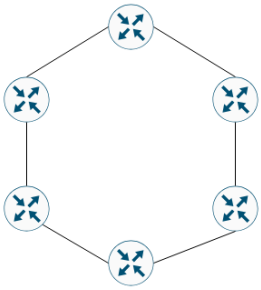
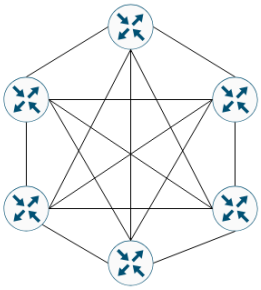
Implementación Tradicional	Implementación Virtual Switching System 1440	Vista lógica Virtual Switching System
Tradicional con STP entre las capas de acceso y distribución 	VSS 1440 permite que los enlaces Upstream sean utilizados 	

1.1.5 Implementación del modelo jerárquico con Núcleo Colapsado

Se combinan las capas de distribución y núcleo en los mismos dispositivos de red físicos. Se recomienda para organizaciones que solo ocupen un edificio. Se incluyen dos dispositivos de capa de distribución para redundancia, aunque se puede implementar usando un solo switch en caso de tener bajo presupuesto.



1.1.6 Modelo jerárquico en WAN

Estrella extendida Hub & Spoke	Anillo	Malla completa
		
Características • Escalabilidad • Convergencia rápida • Facilita políticas de seguridad Permite mayor escalabilidad y facilita la gestión	**Características** • Recomendada para redes de transporte Cuantos nodos se añadan, mayor será la latencia.	**Características** • Tolerancia a fallos • Alta disponibilidad • CPDs sincronizados Requiere conexión de red a todos los demás dispositivos

1.2 Aproximaciones de Seguridad permietral

Consiste en la restricción de acceso entre las diferentes partes de la red, agrupando lógicamente dispositivos con las mismas políticas y requisitos de seguridad, faciltiando así la aplicación de pplíticas de seguridad. Hay varios tipos de zonas básicas:

- **Zona pública**: Zona externa que no está bajo el control de la organización
  - Se suele corresponder con internet
- **DMZ**: Zona que alberga los servicios públicos de la roganización, pueden ser accedidos desde la zona pública. Contiene servicios como proxys de correo, proxys web, proxys inversos y los servicios de acceso remoto
  - Componentes que se ubican en la frontera con internet
- **Zona privada**: Zona interna que contiene los servicios de datos críticos de la organización
  - Resto de la organización seccionada en varias zonas restringidas:
    - Zona de gestión: Acceso a la administración de la infraestructura, intranet del datacenter.
    - Zona de operaciones: Servicios para los usuarios internos.

Además de realizar la división en zonas es necesario usar configuraciones y tecnologías de seguridad como:

- **Acceso seguro a la red**: Controlar y proteger los dispositivos finales de los usuarios de la organización.
- **VPN**: Facilita la conexión a la sede principal de la organización a través de internet.
- **Protección de la infraestructura**: Limitar el acceso a usuarios y dispositivos autorizados.
- **Gestión de red y Seguridad**: Deben tulizarse herramientas que permitan la adminsitración tanto de la red como de la seguridad de esta

[TEMA 2] Fortificación de los dispositivos de red

2.1 Seguridad en los planos

Un dispositivo de red tiene 3 planos funcionales:

- Pano de gestión: Tráfico envido y recibido para la administración del dispositivo (Telnet, SSH…)
- Plano de control: Está relacionado con la toma de decisiones de envío (Protocolos de routing, spanning tree, HSRP, VRRP…)
- Plano de datos: Envío de datos de usuario, implantación de políticas de seguridad de tráfico de usuario.

2.1.1 Seguridad en el plano de gestión

La seguridad en el plano de gestión tiene los siguientes objetivos:

- Permitir el acceso soloamente a los usuarios autenticados con contraseñas de línea, usuarios locales o AAA.
- Controlar que pueden hacer los usuarios en función de sus privilegios usando los niveles de privilegio y mecanismos AAA
- Proteger la sicronización horaria de los dispositivos
- Cifrar las cominicaciones de gestión remota con SSHv2 y/o SSL/TLS
- Monitorizar de forma segura con un syslog protegido y SNMPv2 o V3 en una red de gestión
- Proteger el sistema de ficehros
- Limitar el acceso físico a los dispositivos de red.

2.1.1.1 Buenas prácticas en la seguridad del plano de gestión

- Reforzar las directivas de contraseñas
- Definir grupos de usuarios usando el control de niveles de privilegios, roles y vistas.
- Desplegar Servicios AAA
- Porteger NTP
- Utilizar redes diferenciadas para gestión y restringir las IPs desde las que se pueden iniciar sesiones de gestión.
- Deshabilitar servicios no necesarios

2.1.2 Seguridad en el plano de control

- Limitar el daño que podría inflingir un atacante al enviar tráfico directamente a las IPs del dispositivo (Control Plane Policing y Control Pane Protection)
- Controlar la información relacionada con la toma de decisiones de envío

2.1.2.1 Buenas prácticas en la seguridad del plano de control

- Para proteger la CPU se debe enrutar usando mecanismos de cache como Cisco Express Forwardiong.
- Para proteger el camino de datos los paquetes relacionados con la toma de decisones de envío son recibidos o enviados por equipos de red.
- Deben configurarse mecanismos de autenticación en elos protocolos de enrutamiento
- Deben implementarse técnicas que limiten los paquetes que debe procesar la CPU
    - CoPP (Control Plane Policing): Filtros para cualquier tráfico destinado a las IPs del router. Evita ataques basados en el envío masivo de tráfico.
    - CPPr (Cpmtrol Plane Protection): Permite realizar una clasificación detallada del tráfico que se va a procesar en la CPU usando 3 subinterfaces
        - Host subinterface: Maneja el tráfico hacia una interfaz física o lógica del router
        - Transit subinterface: Gestiona tráfico del data plane que necesita la intervención de la CPU antes del envio
        - CEF-Exception Subinterface: Relacionado con el tráfico que procesa CEF

2.1.3 Seguridad en el plano de Datos

- Busca implementar políticas de seguriodad que definen flujos de tráfico de usuario que están permitidos o denegados por la organización

- Se usan Listas de Control de Acceso, VLANS, IPSs y firewalls.

2.1.3.1 Buenas prácticas en la seguridad del plano de datos

- Implementación de ACLs para filtrar tráfico directamente, solo se debe permitir el tráfico autorizado y prevenir el IP spoofing
- Funcionalidades de firewall: CBAC (Context based access control) y ZBF (Zone based firewall)
- Implementación de IPS: En los equipos de red con mecanismos basados en firma y equipos exclusivos dedicados
- TCP Intercept: Herramientas que permiten detectar el número de sesiones TCP malformadas. Evita ataques SYN-Flood
- Unicast Reeverse Path Forwarding: Comprueba la dirección IP de origen de los paquetes entrantes.
- Mecanismos de seguridad en capa 2 (Seguridad de puerto, DHCP snooping, Dynamic ARP Inspection, IP Source Guard)

2.2 Protección de los planos

2.2.1 Protección del plano de gestión

- Protección de la infraestructura de red para evitar el acceso no autorizado, un dispositivo de red comprometido pone en riesgo toda la red.
- Tareas que se deben realizar para proteger un dispositivo de red:
  - Seguir políticas de seguridad
  - Proteger el acceso de gestión
  - Utilizar SSH y ACLs para limitar el acceso al router
  - Realizar backups de configuraciones
  - Utilizar monitorización de red
  - Desactivar servicios no necesarios

Se puede realizar un cifrado de contraseñas mediante el uso del siguiente comando dentro del modo privilegiado:

```
enable secret <password>
```

2.2.1.1 Autenticación, Autorización y Auditoría (AAA) New-Model

- Una red corporativa debe estar diseñada para controlar quien se conecta y que hace una vez conectado, además de implementar un sistema de auditoría que permita hacer un seguimiento sobre que han hecho los usuarios en una línea de tiempo
- AAA new-Model es un framework basado en estos stándares para el control de acceso a gestiónde los dispositivos de red implementando mencanismos de autenticación, autorización y aditoría.
  - Incremeta la flexibilidad y el control de acceso a la configuración
  - Alta escalabilidad
  - Permite el uso de métodos de backup
  - Utiliza métodos de autenticación estandarizados

- Los usuarios deben autenticarse contra una BBDD, habiendo 2 opciones:
  - Local AAA: Hay una BBDD local,siendo esta la que se emplea para los roles del router. Las implementaciónes de AAA locales no son fáciles de escalar
  - AAA basado en servidor: Se emplea un server externo como RADIUS.
- RADIUS: Remote Dial In User Services
  - Permite cominicar el equipo de red y el servidor AAA
  - Solo cifra la clave de usuario con MD5 y una clave secreta, el resto de info se transmite en laro
  - Se utiliza en los ISP por que puede gestionar información detallada de facturación
  - Los servidores Proxy Emplean Radius por su escalabilidad

2.2.2 Protección del plano de control

Es crítica ya que afecta a los planos de gestión y datos. Los paquetes del plano de control so generados y recibidos por los propios dispositivos de red y permiten el funcionamiento de la propia ifnraestructura de red.

[TEMA 3] Seguridad LAN en entornos ethernet

3.1 Buenas prácticas de protección básica

- A nivel de switches, hay un conjunto mínimo de configuraciones necesarias para tener un mínimo de seguridad, conocidas como buenas prácticas o Requisitos de seguridad.
- Contraseñas seguras, siempre se debe usar el comando “secret” en lugar de “password”.
- Se debe activar “Service password-encryption” para evitar que las contraseñas puedan ser obtenidas revisando la configuración
- Se deben etablecer banners de propósito legal y disuasivo con “banner motd” o “banner login”.
- Acceso seguro a la consola: seguridad física y lógica
- Acceso seguro a través de líneas VTY: USar SSHv2 en vez de telnet, aplicar ACLs y configuración de AAA new model.
- Deshabilitar HTTP o habilitar el servidor seguro con “ip http secure-server”
- Deshabilitar servicios no necesarios
- Usar SNMPv3 (Seguro). Se debe evitar el uso de funciones SNMP de escritura y también se deben usar ACLs a poder ser.
- Asegurar topología Spanning-Tree:
  - La introducción accidental de BPDUs puede bloquear un dispositivo o realizar una denegación de servicio
  - Es necesario identificar al puente raíz configurando la prioridad
  - Se debe activar root-guard para evitar que switches no autorizados se conviertan en raíz
  - Se debe utilizar BPDU guard para evitar que los host envíen BPDUs de forma maliciosa.
  - No se deben configurar BPDU guard y BPDU filter en el mismo puerto ya que se podrían provocar bucles.
- Reducir el uso de CDP/LLDP y de usarse se debe hacer bajo un estricto control
- Configurar sistema básico de logging (Syslog)

- Cisco IOS presenta un riesgo de seguridad al negociar automáticamente las capacidades de trunking ya que puede permitir la introducción de un puerto de enlace troncal no autorizado.
    - Se debe desactivar la negociación automática de trunking en los puertos de acceso y en los puertos troncales.
    - Se deben eliminar las VLAN no utilizadas de los enlaces troncales de forma manual.
- Configurar los puertos no utilizados
    - Colocar puertos no utilizados en una VLAN que no se propague en puertos trunking
    - Definirlos como puertos de acceso para deshabilitar automáticamente el trunking
- Enlaces troncales:
    - Sedeben configurar manualmente todas las acciones trunk y deshabilitar DTP
    - Se debe configurar una VLAN nativa que solamente esté operativa en los enlaces troncales

3.2 Vulnerabilidades mitigables en capa 2

- Análisis pasivo: recopilación de información sin inyección de tráfico
    - Se escucha el tráfico recibido en un puerto.
    - Es posible descubrir info sin hacer mucho ruido con arping, netdiscover y nmap.
- Análisis Activo: Se inyecta tráfico en nivel de capa 3, lo que puede provocar que sea detectado

3.3 Ataques típicos

3.3.1 Accesos no autorizados desde dispositivos falsos

- Conexión de un punto de acceso no autorizdo a la infraestructura de red. Esto sería una brecha de seguridad ya que se puede crear un punto de entrada detrás del firewall de la organización.
- Dispositivos de capa 2: Un posible atacante con acceso físico a la red podría coloca run switch con la intención de alterar el funcionamiento STP, provocar saltos de VLAN, snifar tráfico… Una posible solución es proteger el STP para que no acepte BPDUs falsas y fijar la ubicación del swtich raiz.

3.3.2 Mac flooding

- Consiste en sobrecargar la tabla CAM de forma que las tramas convencionales se envíen a todos los puertos en vez de enviarlo solo por el puerto conectado al dispositivo de destino.
- El objetivo de este ataque puede ser recibir todo el tráfico de red o realizar una denegación de servicios.
- Las tablas CAM tienen un tamaño bastante pequeño, por lo que hay un máximo de entradas que pueden almacenar, si un usuario introduce demasiadas mac invalidas en el switch, este no podrá aprender las direcciones MAC asignadas a los puertos correctos.
- El problema de esto es que el switch envía demasiado tráfico de forma ineficiente
- El intruso puede obtener info de tráfico que normalmente no recibiría.
- Como contramedida se recomienda configurar la Port Security, definiendo un número de MACs máximas que se pueden aprender por puerto, definiendo que direcciones MAC se permiten por puerto.

3.3.3 ARP Spoofing

- Una respuesta de ARP normalmente contiene la dirección MAC del propio equipo y una respuesta a una petición realizada por otro equipo que conoce su IP, pero no la MAC.
- Cuando se produce ARP Spoofing, un dispositivo atacante usa su dirección MAC para que aparezca como destino de una IP que no le pertenece, provocando que el dispositivo que va a enviar la info lo haga usando como MAC de destino la del atacante en vez de la de un dispositivo válido.
- Esto hace que todo el tráfico destinado a dicha IP vaya al equipo del atacante
- También se pueden usar mensajes “Gratuitous ARP” para envenenar caches ARP de los dospositivos del dominio broadcast.
- Otra forma de realizar el ataque es generando respuestas DHSCP como si el atacante fuera un servidor DHCP válido. Previamente el atacante agota las IP ofertadas por el server legítimo, generando peticiones falsas con direcciones MAC falsas.
- Si el atacante proporciona dirección IP y máscara, también puede proporcionar servidor DNS y pasarela por defecto, permitiendo realizar un ataque man in the middle.

3.3.4 Ataque de salto de VLAN: Switch Spoofing

Ataques que permiten que un sistema final envie o reciba paquetes de una vlan que no debería ser accesible para dicho equipo. Esto se puede hacer usando Switch Spooging o Double Tagging

3.3.4.1 Switch Spoofing

El atacante configura si sistema para realizar un enlace trunk mediante ISL o IEEE 802.1Q, utilizando Dynamic Trunk Protocol (DTP) que esta habiltiado por defecto en los equipos cisco. La configuración automática permite que después de recibir un paquete DTP generado por el atacante, el puerto se convierta en troncal y por lo tanto envíe y acepte tráfico desde y hacia cualquier VLAN, permitiendo al atacante acceso a los datos de todas las VLANs

3.3.4.2 Double Tagging

Una estación genera tramas con dos cabeceras 802.1Q con el fin de que el switch envíe tramas a una VLAN que en un principio no debería ser accesible al atacante. Para ello el atacante debe estar conectado a un puerto de acceso del switch, el switch tiene que tener un enlace troncal con 802.1Q y el enlace troncola tiene como VLAN nativa la misma VLAN que la del puerto de acceso al que está conectado el atacante.

3.3.4.3 Como evitar los ataque de salto de VLAN

- Se deben configurar todos los puertos no utilizados como puertos de acceso para que no puedan negociar un enlace troncal
- Se colcan todos los puertos no usandos en estado apagado y se asocian con una VLAN no operativa
- Cuando se configura un enlace troncal la VLAN nativa debe ser diferente a cualquier VLAN de

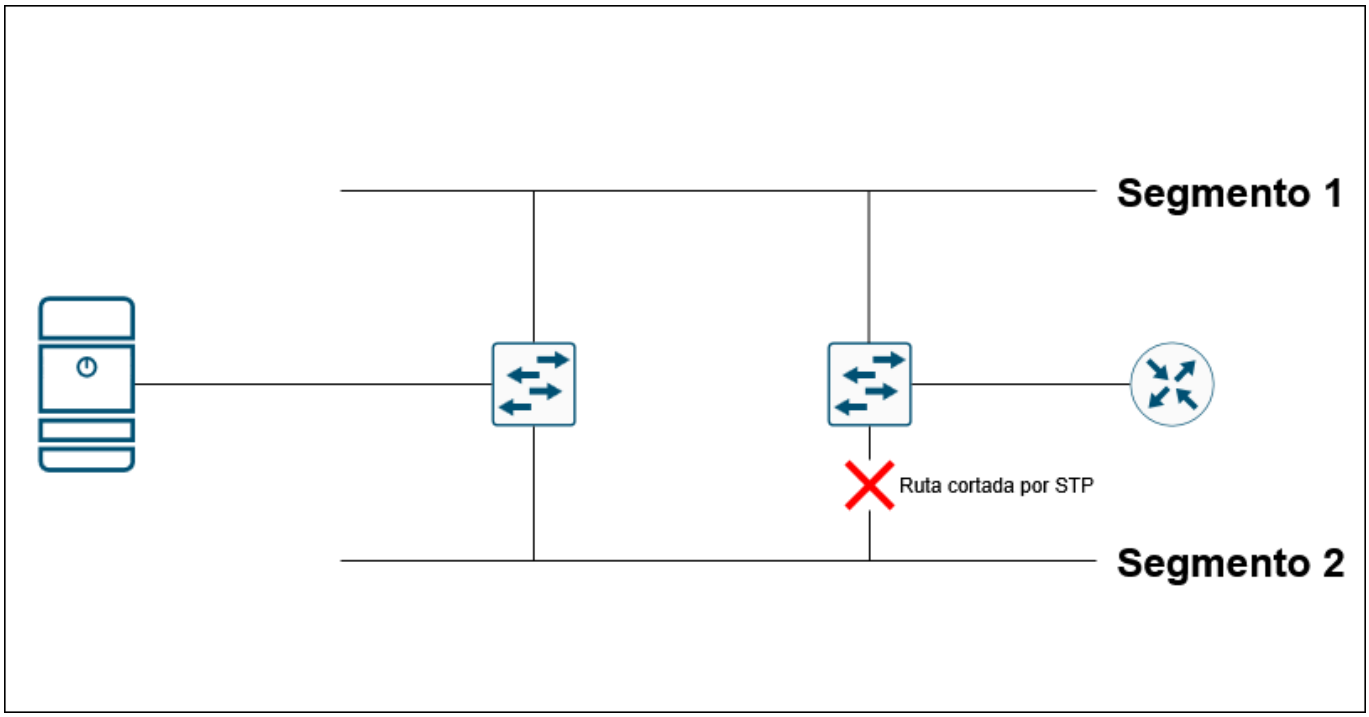
datos, se debe configurar el trunking de forma manual y se deben especificar el rango de VLANs soportadas en un enlace troncal, no permitiendo la VLAN nativa.

3.4 Fundamentos de Spannign Tree Protocol (STP)

La topología redundante ayuda a eliminar puntos únicos de fallo. Para evitar efectos indeseables en capa 2 se usa STP, que bloquea determinados puertos de forma lógica para crear un árbol lógico, mientras existe una estructura de grafo cíclico a nivel físico.

En topología redundante de capa 2 pueden ocurrir los siguientes problemas:

- Tormentas de broadcast: El tráfico de difusión circual de forma indefinida, enviándose a todos los Switches menos al de origen.
- Transmisión de tramas múltiples: Se pueden enviar múltiples copias de una trama a un dispositivo destino, lo que puede producir Unicast MAC Flooding cuando una trama cuya mac unicast de destino es conocida, se reenvíe a todos los puertos menos por el que entró.
- Inestabilidad de las tablas MAC: Es el resultado de recibir mútiples copias de las misma tabla por los mismos puertos



STP bloquea determinados puertos de forma lógica para crear un árbol:

- Utiliza conceptos como puente raíz, puertos raíz, puertos designados y puertos no designados para establecer rutas a través de la red.
- Obliga a determinados puertos a permanecer bloqueados para que no reenvíen o inunden tramas de datos.
- El objetivo es que solo haya un camino activo apra cada segmento de red
- Si hay un problema con la conectividad, STP reestablece la conectividad activando automáticamente una ruta inactiva.
- Se usa Bridge Data Protocl Unitds (BPDUs) para llevar a cabo estas operaciones

3.4.1 Estándares de Spanning Tree

- Versión original: estándar 802.1D, desarrollado para entornos de bridges, solo soporta LAN o VLAN.
- Common Spanning Tree (CST): Hay una instancia de spanning tree 802.1D para toda la red conmutada.
    - Un solo árbol STP
    - El tráfico de todas las VLANS fluye por los mismos enlaces y deca completamente inactivos otros. Soporta múltiples VLAN en un solo árblo
    - Convergencia de red lenta.
- Cisco PVST y PVST*: Mejora de STP patentada por Cisco que proporciona una instancia de Spanning-tree 802.1D independiente para cada VLAN configurada en la red, permitiendo mejoras como PortFast, BPDU GUard, BPDU Filter, Root Guard y Loop Guard, permitiendo múltiples árbloes STP y repartiendo el tráfico de las diferentes VLANS
- Multiple Spannign Tree (MST) o IEEE 802.1S: para reducir el número de instanacias que requiere STP, MST asigna múltiples VLANS con los mismso requisitos, en la misma instancia de spanning tree.
- Rapid STP (RSTP) o IEEE 802.1W: es una evolución de STP que proporciona una convergencia más rápida, pero solo tiene una instancia de STP.
- Cisco PVRST+: Mejora de RSTP, proporciona una isntancia independiente de 802.1W por VLAN.

3.4.2 Vulnerabilidades de STP

- Es un protocolo sin autenticación
- Los swtiches emiten y aceptan BPDUs por todos los puertos, por lo que un atacante podría:
    - Convertirse en switch raiz
    - Crear bucles
    - Rutas incosistente
    - Denegación de servicio totoal

3.5 Medidas de seguridad

3.5.1 Ataques de capa 2 y contramedidas

- MAC address Flooding: Se puede mitigar usando port security
- VLAN Hopping: Se puede mitigar realizando un control estricto de las configuraciones de troncales y de los puertos no usados.
- Ataques entre dispositivos de la misma VLAN: Private VLANS
- DHCP Starvation y DHCP Spoofing: Se puede solucionar aplicando DHCP Snooping
- Spanning Tree attack: Se mitiga configurando el switch raíz y un backup, así como habilitando root guard
- MAC Spoofing: Se implementa DHSC Snooping y Port Security
- ARP Spoofing: Se usa Dynamic ARP Inspection (DAI), DHCP Snooping y Port Security
- Manipulación de Cisco discovery protocol (CDP): Se desactiva CDP en todos los puertos que no lo necesiten
- Ataques a SSH y Telenet: Usar SSHv2 y usar telnet solo con VTY con ACLS activadas.