[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:

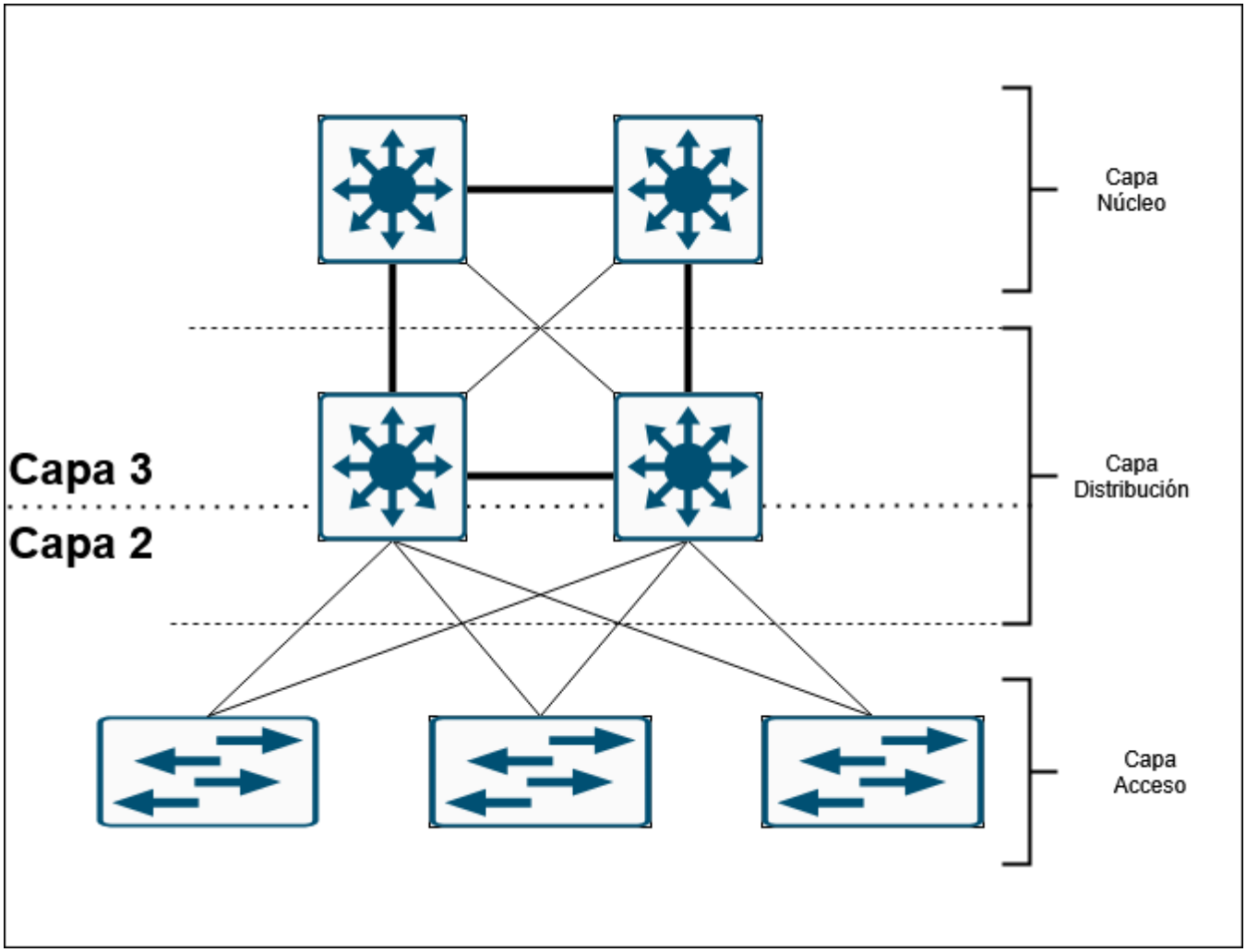
- Capas especializadas en funciones concretas
- Se basa en la estructura jerárquica de la organización
- Facilita la selección de dispositivos, configuración y mantenimienot
- Sirve tanto para WAN como para LAN

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:

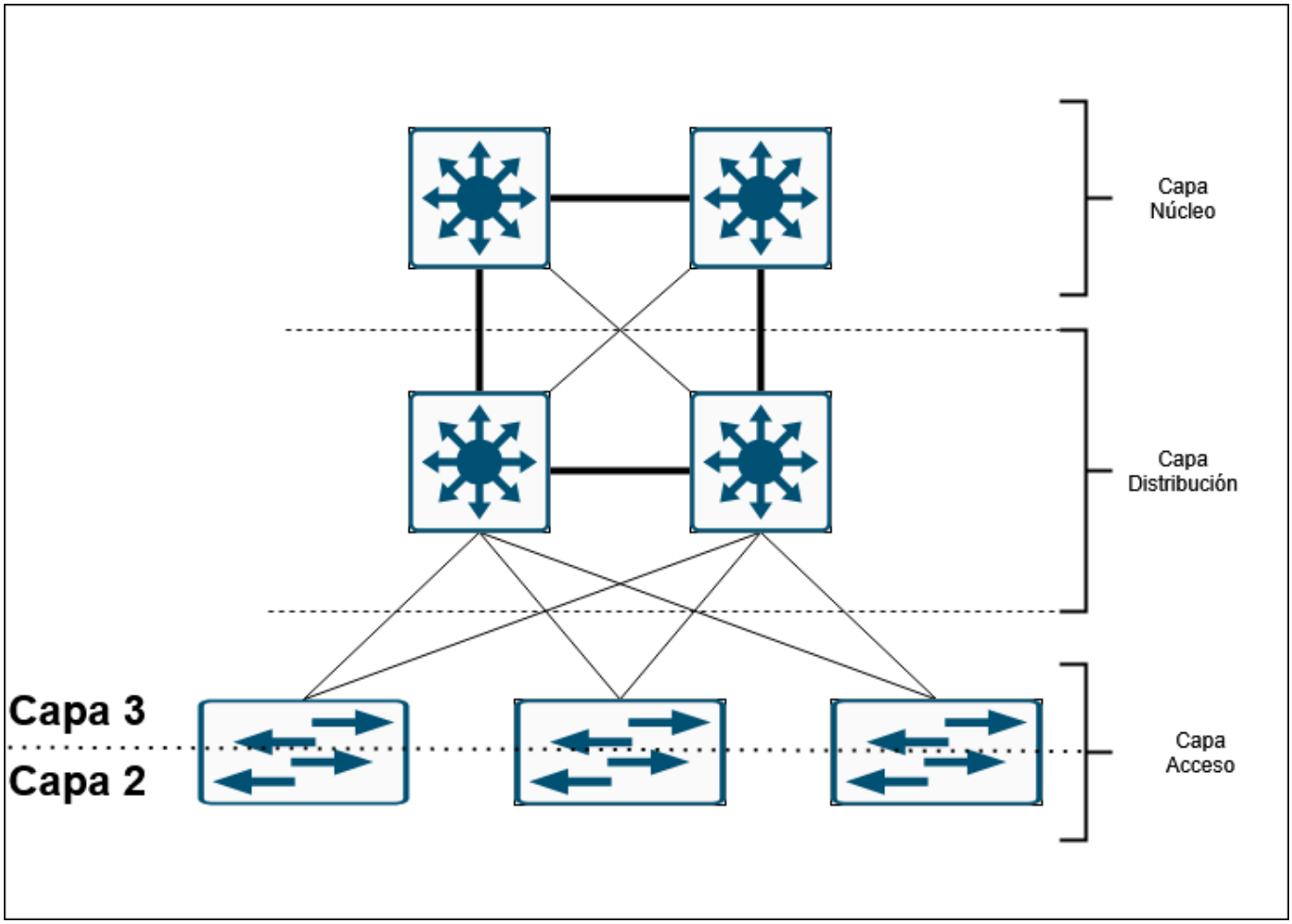
- Alta velocidad
- Baja latencia
- Alta disponibilidad y tolerancia a fallos
- Se debe evitar la manipulación de paquetes
- Diámetro limitado y consistente
- Aplicación de QoS

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

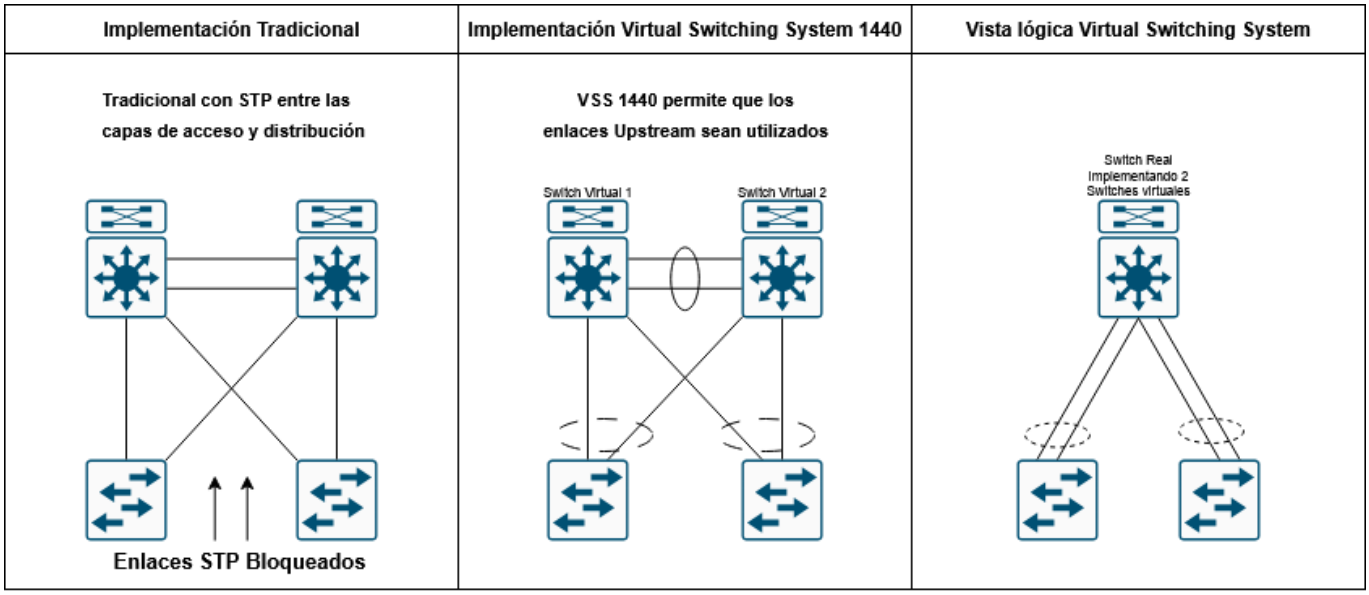
1.1.3 Modelo jerárquico usando capa 3 hasta capa de acceso.

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.



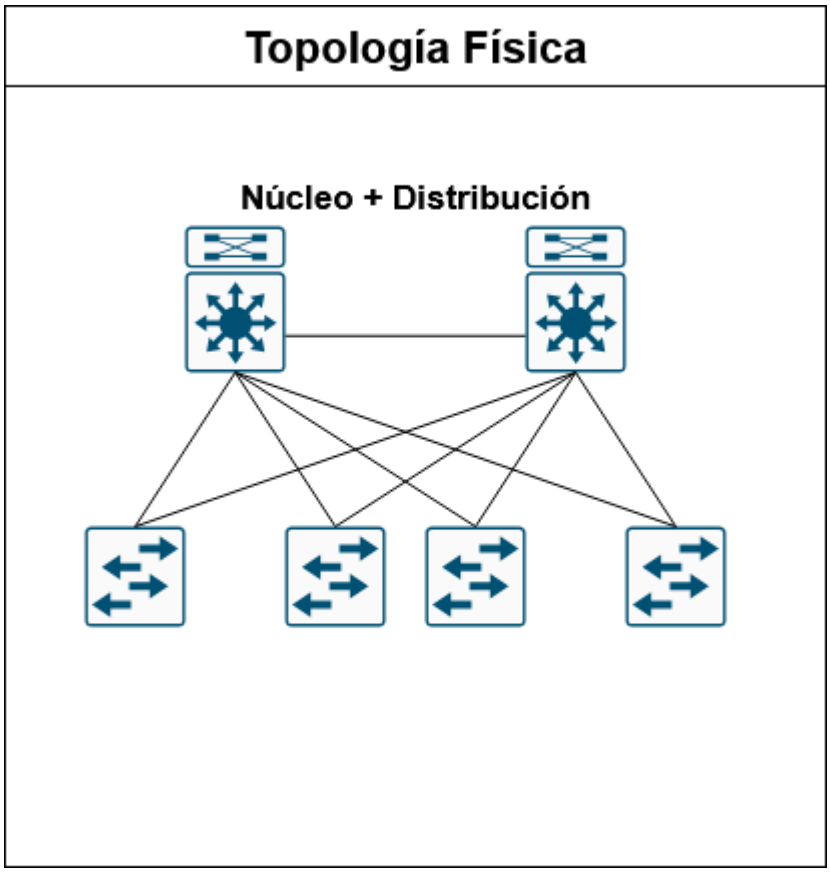
1.1.4 Implementación del modelo jerárquico usando Virtual Switches

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.

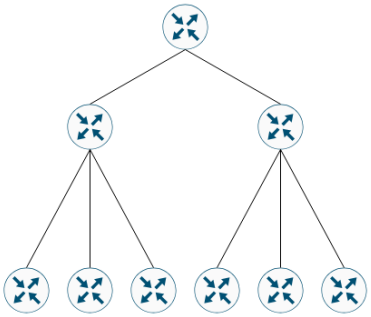
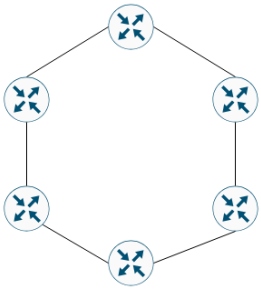
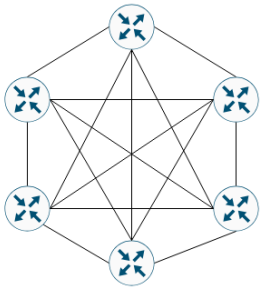


1.1.5 Implementación del modelo jerárquico con Núcleo Colapsado

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

2.2.1 Protección del plano de control

From:
https://knoppia.net/ - **Knoppia**

Permanent link:
https://knoppia.net/doku.php?id=redes:turboresumenexpress&rev=1752099578

Last update: **2025/07/09 22:19**