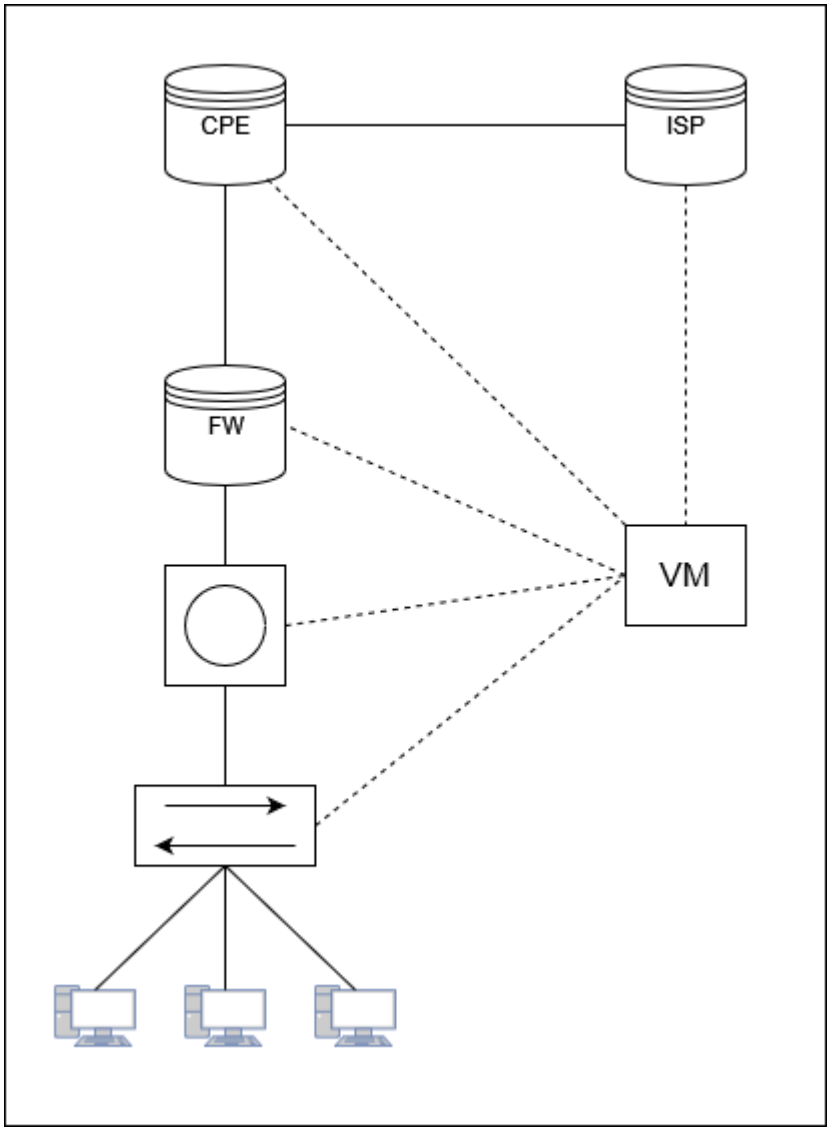
Fortificación de los Dispositivos de Red



Introducción

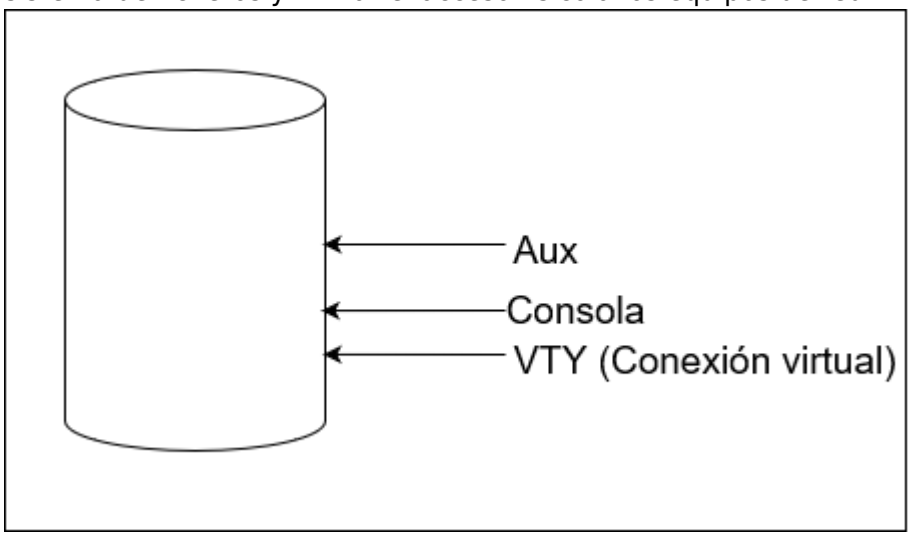
Los dispositivos de red son un elemento que debemos proteger desde diferentes punto de vista ya que están expuestos a nivel de perímetro. Tenemos 3 planos:

- Tráfico de usuario (Plano de datos)
- STP, OSPF, HSRP... (Plano de control)
- Plano de Gestión

Cada uno de estos planos necesita requerimientos de protección distintos. Existen interdependencias a la hora de proteger o configurar los diferentes mecanismos de seguridad de cada plano.

Seguridad en el Plano de Gestión

El objetivo es permitir el acceso solo a los usuarios autenticados, controlar que pueden hacer en función a sus privilegios, cifrar las comunicaciones de gestión remota (SSHv2, SSL/TLS), proteger el sistema de ficheros y limitar el acceso físico a los equipos de red.



Se puede usar protección por contraseña de línea (Menos seguro), protección con usuarios locales y otra es la utilización de AAA new Model. Lo mejor es usar una lista de métodos de autenticación:

1. AAA Server
2. BBDD de Usuarios Locales

También se debe proteger la sincronización horaria ya que si se desincroniza pueden fallar los certificados digitales al fallar la fecha. Telnet debe ser deshabilitado y el uso de SSH y TLS 1.2 es mandatorio. Se debe monitorizar de forma segura con SNMP ya sea versión 2 o 3. Buenas prácticas:

- Reestablecer contraseña tras contraseñas fallidas
- Bloquear cuentas temporalmente si se ponen contraseñas mal
- Forzar contraseñas de longitud mínima
- Definir niveles de privilegio
- Desplegar servicios AAA para autenticación
- Deshabilitar servicios no necesarios, disminuyendo así la superficie de ataque
- Utilizar infraestructuras diferenciadas para gestionar dispositivos.

El plano de gestión está enlazado a la administración de dispositivos.

1. Consola (Line Console 0): se usa para administrar el router cuando viene de fábrica o cuando se produce una catástrofe total. Lo malo es que conectarse por vía consola suele ser incómodo.
2. Acceso remoto (Line VTY 0-15): puede ser por telnet (no seguro) y SSH v2 (Seguro)
3. Protocolo SNMP: Permite monitorizar y configurar los dispositivos, aunque en general se usa para monitorización.

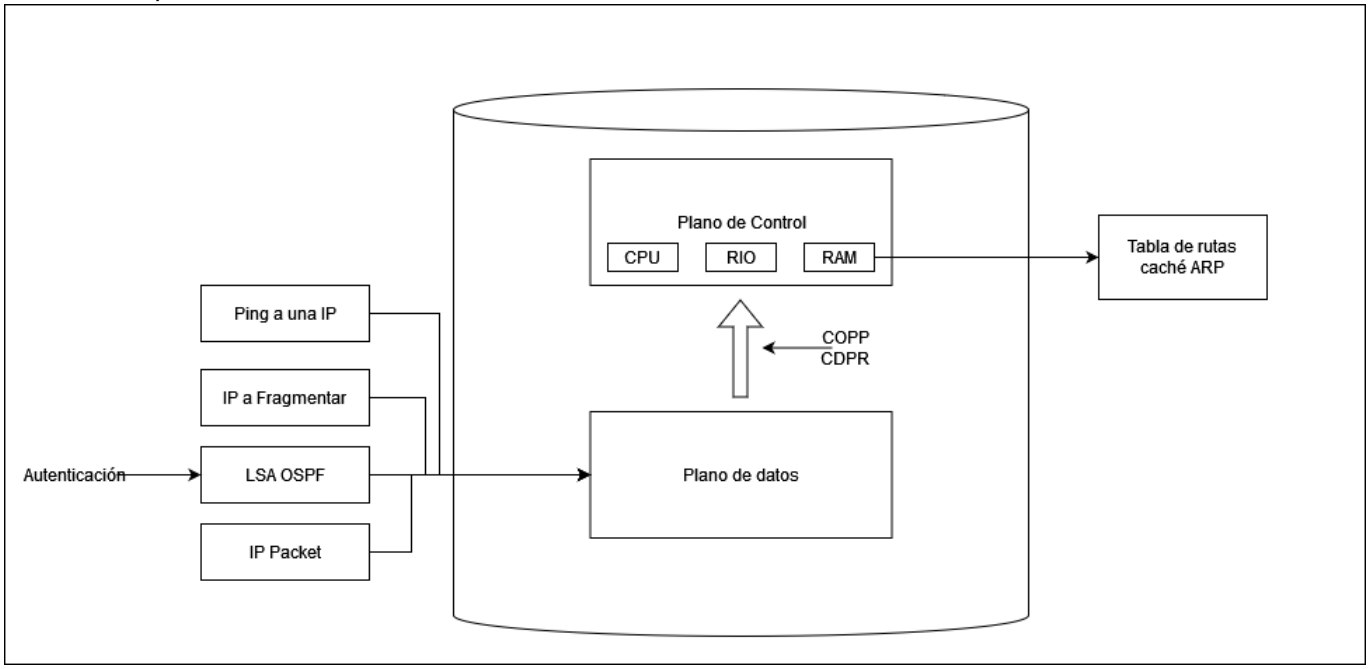
Para asegurar estos puntos de acceso a la gestión se recomienda establecer métodos de autenticación:

1. Contraseña de línea: Contraseña especificada durante la configuración inicial, método muy poco seguro. Comandos clave: “login” y “password”
2. Configuración de usuarios locales: cuando se añaden usuarios locales la contraseña de línea

queda desactivada. Comandos clave: “login local” y “username () password”

3. Autenticación AAA: Permite definir métodos alternativos de autenticación, por ejemplo, la utilización de usuarios que se encuentren en un servidor externo. También se pueden usar métodos de autenticación de backup, de forma que puedes dejar un segundo método de autenticación en caso de que falle el servidor externo. AAA permite también autorizar, asignando niveles de privilegio a los usuarios, limitando que usuarios pueden configurar el router.

Los equipos de cisco tienen 16 niveles de privilegios, cuando uno hace login entra en nivel 1 y en cuanto se hace “enable” se pasa a nivel 15. Lo malo de este sistema es que si alguien tiene nivel 15 puede acceder a todos los comandos de los otros niveles, lo que hace que no sea posible crear usuarios especializados con acceso solo a ciertos comandos.



Buenas prácticas

- Configurar mecanismos de autenticación de protocolos de enrutamiento
- Implementación de técnicas que limiten los paquetes que deben ser procesados por la cpu con CoPP y CPPr:
  - CoPP: Control Plane Policing: Filtros para cualquier tráfico dedicado a las IPs del router. Se puede aplicar al tráfico de gestión. Evita ataques basados en el envío masivo de datos.
  - CPPr: Control Plane Protection: Permite llevar a cabo un proceso de filtrado más detallado. Consideran 3 interfaces distintas en función al tipo de tráfico que debe manejar.
    - Host subiterface: maneja el tráfico hacia una interfaz física o lógica del router
    - Transit subiterface: Gestiona el tráfico del data plane que necesita la intervención de la CPU antes de enviarlo
    - CEF-Exception subinterface: relacionado con el tráfico que procesa el DEF que produce situaciones excepcionales

Seguridad en el Plano de Datos

Recomendaciones:

- Implementación de ACLs para filtrar tráfico directamente
    - Se debe permitir solo tráfico autorizado en la política de seguridad
    - Se previene el IP Spoofing
- Funcionalidades de firewall
    - CBAC: Context Based Access Control
    - ZBF: Zone Based Firewall
- IPS: implementación software
- TCP intercept
    - Evita ataques SYN-FLOOD
- Unicast Reverse Path Forwarding
    - Compruea la dirección IP de origen de los paquetes.

Protección del plano de gestión

Protección de la infraestructura de red para evitar el acceso no autorizado y otras cosas.

1. Seguir política de seguridad de acceso al router establecida
2. Proteger acceso físico
    - Colocar los dispositivos de red en una habitación cerrada accesible solo para personal autorizado
    - Instalar UPS
    - Disponer de dispositivos y piezas de recambio.
3. Usar contraseñas fuertes
    - Complejidad mínima de 10 caracteres con comando “security password min-length 10”
    - Cifrar las claves usando secret en lugar de password. En su defecto usar el comando “service password encryption” para un cifrado débil.
    - Usar mecanismo de gestión de identidades centralizado AAA
4. Control de acceso al router
    - Puerto de consola y auxiliar
    - Lineas VTY: Acceso por SSH + filtrado ACLs
5. Acceso seguro a la gestión: Implementación de AAA
6. Uso de protocolos de gestión seguros como SSHv2, HTTPS o SNMPv3
    - Reforzar la seguridad con VPNs
7. Reforzar la seguridad con conexiones virtuales
8. Implementación de sistema de logging → telemetría de tráfico → detectar actividad inusual o fallos. Comando “service timestamps log datetime”
9. Configurar copias de seguridad periódicas de las configuraciones y del sistema operativo
10. Desactivar servicios no necesarios.

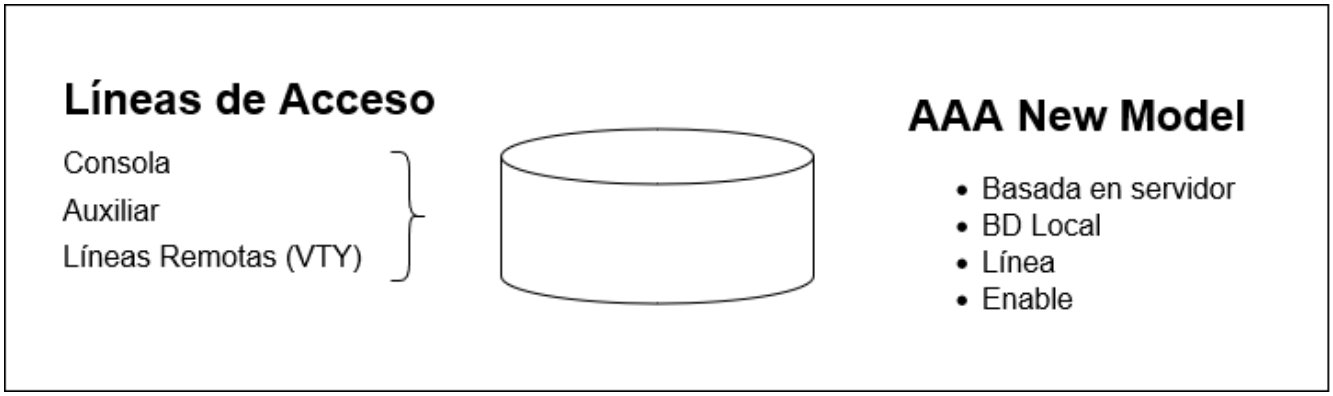
Política de seguridad en el Router

La política de seguridad de un router debe permitir contestar a las siguientes cuestiones:

- Como se hace el cifrado de contraseñas y cual es su complejidad
- Como se configura la seguridad de los protocolos de enrutamiento
- Como se implementa el mantenimiento de las configuraciones
- Como gestionan los cambios: documentación de los cambios y actualizaciones
- Actualizaciones de seguridad: Seguimiento de las últimas vulnerabilidades.

Autenticación, Autorización y Auditoría (AAA)

Una red corporativa debe estar diseñada para controlar quien se conecta (Autenticación) y que puede hacer cuando se conecta (Autorización). Nos centramos en el plano de gestión, que es la primera parte que se quiere fortificar. Los dispositivos de red suelen delegar parte del trabajo AAA a servidores externos.



Generalmente cuando uno se conecta al servidor se conecta en modo usuario en lugar de en modo usuario. Estos usuarios son de nivel 1. En los routers y switches hay 16 niveles de privilegios, pero solo se suelen usar los niveles 0, 1 y 15.

La auditoría nunca se puede llevar localmente, se suele usar un elemento externo que registre los sucesos que se están produciendo. Todo esto se hace utilizando un servidor externo. Cuando se usa el enfoque AAA New Model se suelen crear listas de métodos de autenticación, de forma que si falla el primer método de la lista, se puede usar el segundo método y en caso de que falle el segundo, el tercero y así hasta el último método de la lista. No se suelen usar ni contraseña de línea ni enable, generalmente se crean usuarios de rescate en el dispositivo para casos de emergencia. El método primario suele ser un Servidor AAA y el secundario una base de datos de usuarios.

- Local AAA: Una base de datos local
- Servidor AAA: se emplea un Server BD externo

Características de AAA basada en servidor

Radius permite que nuestro router se comunique con un servidor AAA. Este protocolo solo cifra la contraseña del usuario. No es demasiado seguro que digamos ya que usa un Hash MD5 y una clave secreta. Cuando se da de alta un servidor radius se debe decir la IP del servidor más una contraseña compartida y cuando en el servidor se de de alta el equipo, en el equipo debemos poner la IP del router y la misma contraseña compartida. Esta basado en UDP. Se pueden usar 2 pares de puertos distintos dependiendo de la versión.

Configuración de autenticación local AAA

1. Crear base de datos con “username <nombre> secret <contraseña>”
2. Habilitar AAA globalmente en el router con el comando “aaa new-model”
3. Definir lista de métodos de autenticación con el comando “aaa authentication login {default|list_name} metodo_1 metodo_2 …. metodo_n”

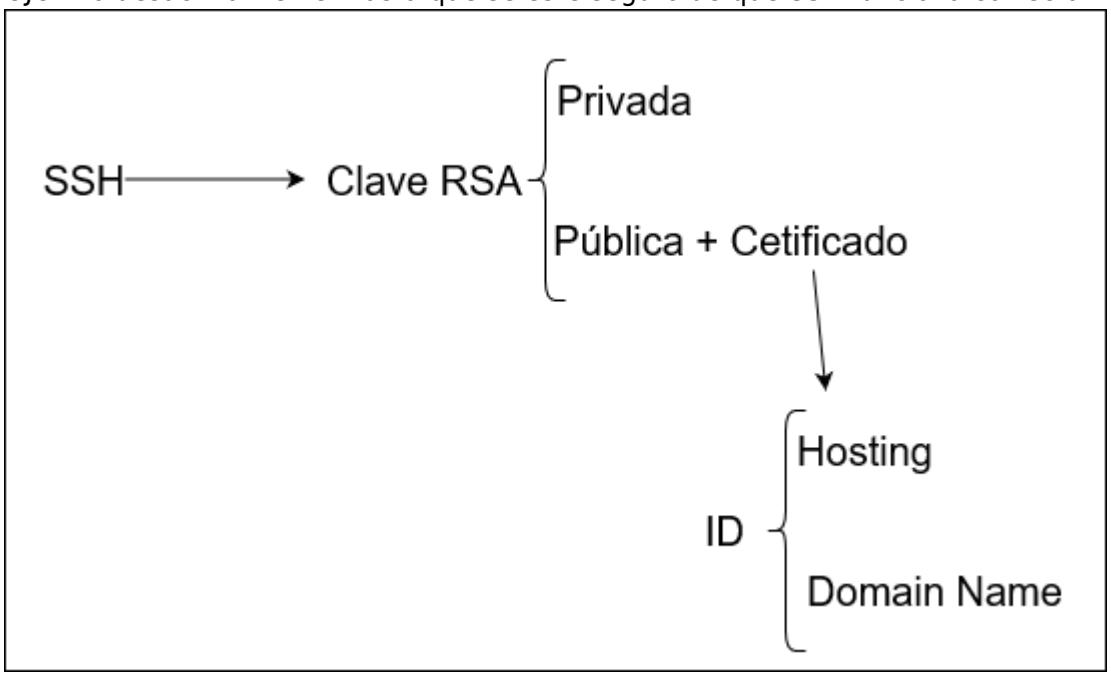
```
aaa authentication login TELNET-ACCESS group radius enable
```

1. Tras eso se aplican las listas de métodos a las interfaces:

```
username JR-ADMIN secret c0ntr4s3na
username ADMIN secret c0ntr4s3na
aaa new-model
aaa authentication login default_local
aaa authentication login TELNET-LOGIN local-case
line vty 0 4
login authentication TELNET-LOGIN
exit
```

Configuración SSH

OJO: No desactivar telnet hasta que se esté seguro de que SSH funciona correctamente.



comando a utilizar:

```
crypto key generate rsa general-keys modulus <modulus-size>
```

para verificar funcionamiento se usa:

```
show crypto key mypubkey rsa
```

dentro de vty al principio:

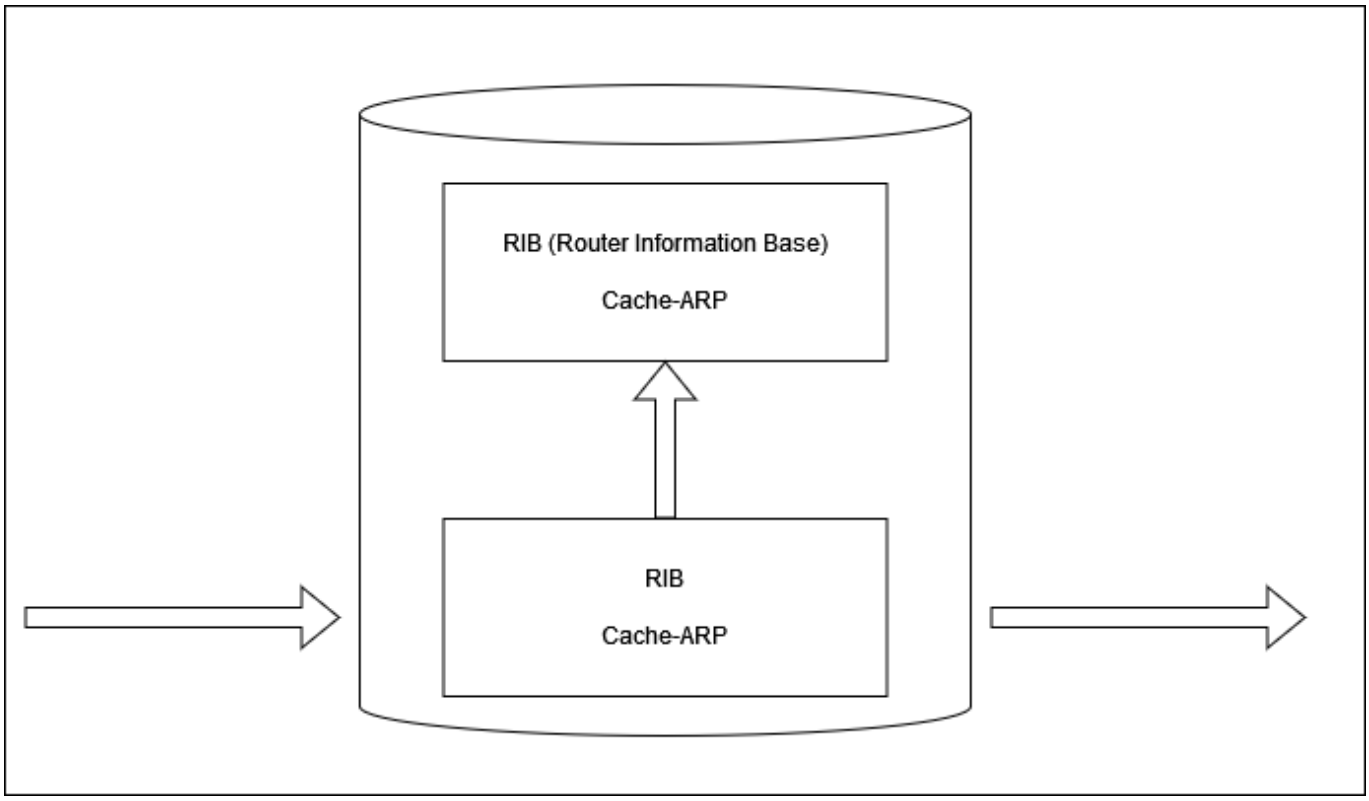
```
transport input all
```

una vez verificado el correcto funcionamiento de ssh:

```
trasnport input ssh
```

Proteger el acceso a la infraestructura usando ACLs

Se aplican en dirección entrante teanto en la interfaz que conecta la red corporativa con el exteriro y las interfaces que conectan con los usuarios internos. Establecemos mecanismos para controlar que pasa del plano de datos al plano de control. El plano de datos son los mecanismos que permiten enrutar datos.



Servicios de Backup y Restauración

Se usa para realizar copias de seguridad de IOS y de las configuraciones:

- TFTP: Envío y recepción de ficheros. Info enviada en texto plano
- Mecanismos de copia más seguros: Identificación
  - FTP, HTTP, o si es cifrado: SCP, HTTPS
  - Se pueden utilizar comandos de configuración auxiliares para establecer usuario y contraseña para utilizar con los diferentes protocolos como FTP o HTTP.

Este proceso puede ser automatizado con el comando archive:

```
Router(config)# archive
Router(config-archive)# path flash:/config-archive/$h-config-$t
Router(config-archive)#write-memory
Router(config-archive)#time-period 10080
```

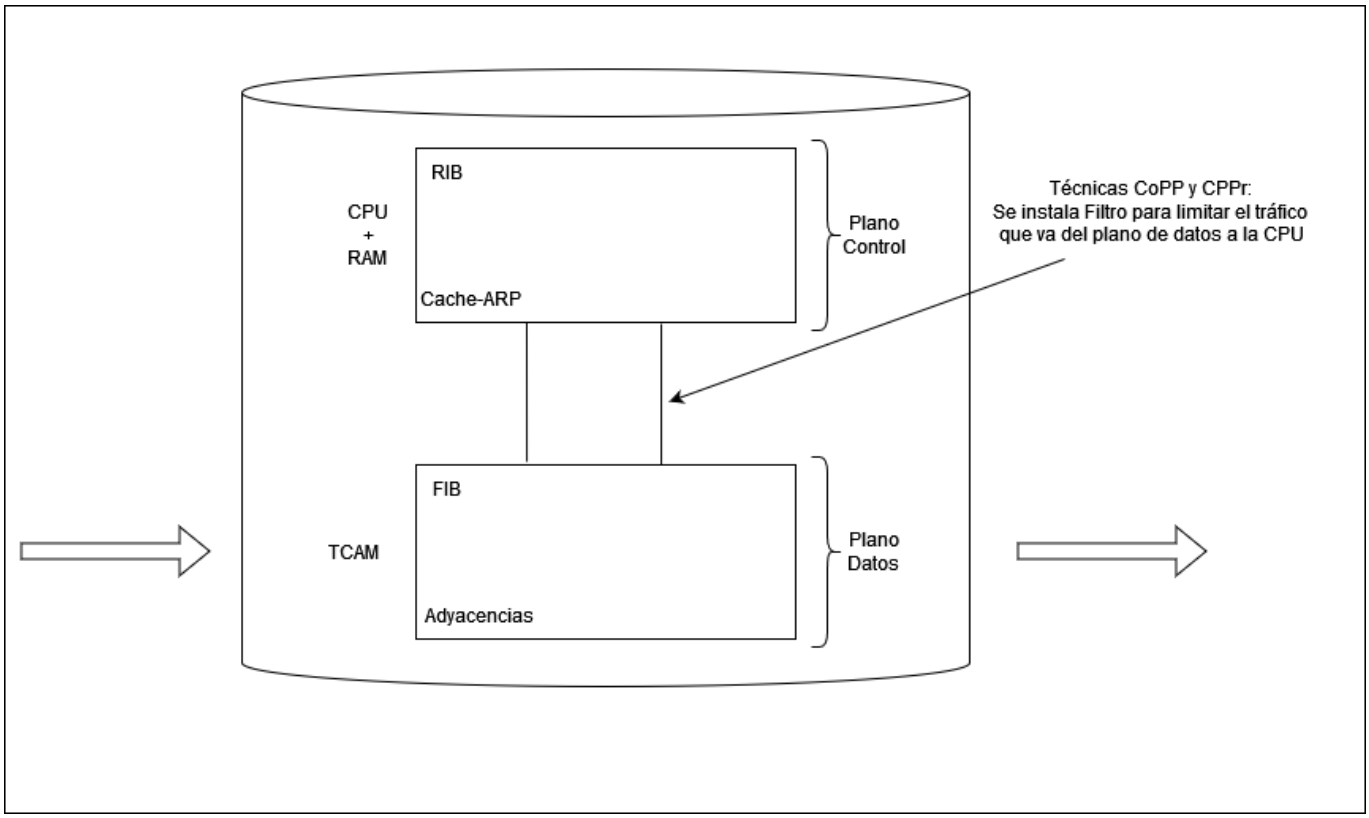
Para cargar una configuración nueva, se debe borrar la configuración que ya tiene cargada el equipo, reiniciando el equipo y luego procediendo a meter la nueva config.

Desactivación de servicios no usados

IOS ofrece muchos servicios, algunos de ellos pueden ser riesgos potenciales para la seguridad al estar obsoletos. Existen los siguientes riesgos de seguridad en los servicios activados por defecto:

- Resolución de nombres DNS: “no ip domain-lookup”
- CDP: “no cdp run /no cdp enable” → Cada cierto tiempo hace un broadcast con información sobre el equipo
- NTP: “ntp disable”
- Servidor BOOTP: “no ip bootp server” → El equipo se comporta como servicio DHCP
- DHCP: “no ip dhcp-server” → El equipo se comporta como servicio DHCP
- proxy ARP: “no ip proxy-arp” → Cuando se configura a un equipo como puerta de enlace su propia dirección IP, va a pedir la dirección IP final del equipo con el que se quiere conectar independientemente de la red, el problema de esto es que si el destinatario está en otra red nunca recibirá respuesta. Este servicio trata de resolver este problema.
- ip source routing: “no ip source-routing” → Facilita hacer ataques man in the middle.
- ip redirects: “no ip redirects”
- HTTP service: “no ip http server”

Protección del plano de control



Hay atacantes que intentan enviar muchas conexiones para saturar la CPU, para evitar esto se usan las siguientes técnicas:

- Control Plane Policing (CoPP): Permite identificar el tipo y ratio del tráfico que puede alcanzar el plano de control.
- Control Plane Protection (CPPr): Simula 3 interfaces distintas: una para tráfico de host, otra para tráfico de transito (Necesita ser procesado) y otro para excepciones de CEF. Es similar a CoPP

pero aplicando configuraciones a 3 interfaces distintas.