Administración Out-of-Band

Guillermo Pérez Trabado *©2016-2022*

Diseño de Infraestructuras de Redes

Depto. de Arquitectura de Computadores - Universidad de Málaga

Introducción

Un problema a resolver en el diseño de la red es cómo administrar los equipos activos de la propia red (switches, routers y firewalls). Tenemos el problema de que los equipos de la red se encuentran distribuidos por todos los sites de la empresa, por lo que la administración mediante conectando una consola física a cada equipo mediante un puerto serie RS-232 no es posible ya que tendríamos que desplazarnos a veces miles de kilómetros hasta otras sucursales. Este tipo de consola solo se usa cuando se instala por primera vez el equipo. Una vez configurado necesitamos administrarlos remotamente para no tener que desplazarnos.

Una de las grandes preocupaciones de todo administrador de redes es mantener seguro el acceso remoto para evitar que un intruso pueda usar una vulnerabilidad para tomar el control de los propios equipos de red. Hay que tener en cuenta que la seguridad de nuestro diseño basado en VLANs está basada en una configuración software. Se trata de una **infraestructura definida por software**. Si un intruso toma el control de los equipos de red, todas las medidas de seguridad son derrotadas inmediatamente.

Administración in-band

Una de las formas de administración remota es usar la propia red de datos para controlar remotamente los equipos de red. Como cada equipo de red tiene un sistema operativo, basta que el sistema tenga un interfaz lógico conectado a las colas de paquetes que atraviesan por el equipo. Dicho interfaz tiene una dirección IP asignada. Cuando un paquete recibido por el equipo va dirigido a dicha IP, el paquete es pasado al interfaz local y retirado de las colas de *forwarding***.** El sistema puede ofrecer servicios de administración basados en protocolos de la familia TCP/IP tales como SSH, TELNET, http, https o SNMP.

Se denomina **administración in-band** al hecho de usar la misma red de datos como red de administración. El concepto ya existía en los antiguos equipos analógicos de transmisión de datos donde se usaba la misma **banda analógica** del espectro de frecuencia usada por las señales de datos para las señales de control.

El problema de éste tipo de administración es que es muy peligrosa porque cualquier vulnerabilidad conocida (empezando por un password débil o robado) da acceso al equipo a cualquier intruso cuyo tráfico pueda alcanzar el equipo. La única forma de reforzar la seguridad es usar ACLs que restrinjan el acceso a los servicios de administración del equipo solamente desde ciertas direcciones IP.

Administración out-of-band

El término **out-of-band** es igual de antiguo y es la solución al problema de la seguridad. Se trata de usar otro canal de comunicación separado de los datos para el control. Esto implica

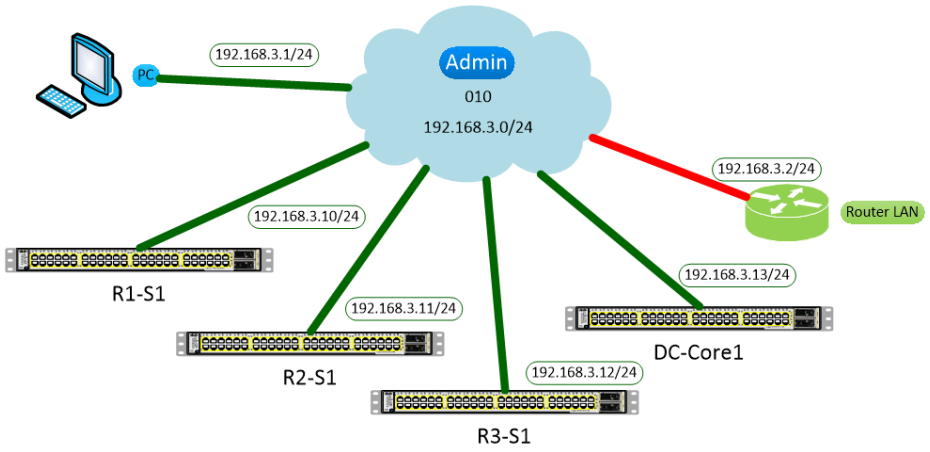
añadir una red de control independiente de la red de datos, y eso resulta muy caro ya que requiere duplicar los medios de transmisión (cables y fibra) e incluso tener equipos de comunicación solo para la red de control. Además, los equipos de la red requieren tener un interfaz físico para ser conectados a la red de control.

Aunque algunas organizaciones con estándares de seguridad muy altos usan redes separadas de control, el precio es tan caro que la mayoría de las organizaciones optan por una solución mixta, que es usar una red de control **out-of-band virtual**. Evidentemente en el caso de Ethernet, se trata de usar una VLAN solo para el tráfico de administración de los equipos de red separada del resto de VLANs de datos. Esta solución es mucho más barata porque físicamente tan solo existe una red , pero a nivel lógico funcionan como redes independientes.

1. Configuración de una red de administración out-of-band

Resumidamente, en el esquema lógico la red de administración es una VLAN aislada que solo tiene conectados los equipos de red y algún terminal de los administradores. Como puede verse en la figura siguiente, la VLAN de administración se conecta a cada switch y también al router LAN, pero dichos equipos solo son terminales de la VLAN en este esquema.

Este último punto merece ser resaltado. Los equipos de red representados aquí son sistemas operativos cuyos servicios son contactados mediante la VLAN. En este esquema, los equipos de red no simbolizan conmutadores a los que está conectada la VLAN.



¿Cómo se implementa la conexión de todos los equipos de red sin que dichos equipos interconecten dicha VLAN con el resto de VLANs de la empresa?

Creación de la VLAN de administración

La VLAN de administración no se diferencia del resto en nada, excepto en los equipos que tienen acceso a la misma. Para crear la VLAN usa el switch máster de VTP y crea la nueva VLAN para que se propague a todos los switches de la empresa.

No olvides:

- Añadir la VLAN a tu tabla de VLANs y asignarle un ID de VLAN y un rango de direcciones IP suficiente para asignar direcciones a todos los equipos de red y a los PCs de los administradores de la red.
- Añadir la VLAN al esquema lógico de tu red. Recuerda que es una subred aislada del resto y que, aunque aparece conectada a los routers de la empresa, se entiende que

esta VLAN no tiene enrutamiento a través de ningún router. Por eso, el interfaz del router aparece en rojo.

- Añadir un PC de administración en las oficinas de los administradores del Data Center (las que están cerca del Data Center). El PC puede estar conectado a un switch del edificio o bien a un switch del Data Center. Pero evidentemente, en cualquier caso a un puerto asignado a la VLAN de administración. La dirección del PC se configurará de forma estática. Evidentemente no hay router ni DNS ya que esta VLAN está aislada.

Interfaz de administración en un switch

En el caso de los switches, la clave de cómo conectarse a la VLAN de administración está en la forma en que se crean los interfaces IP del sistema operativo. Para poder poner una dirección IP, primero hay que crear un interfaz. Como los interfaces físicos del switch son puertos del conmutador por los que pasan paquetes de varias VLANs, no tiene sentido poner una dirección IP en un puerto ya que afecta a varias subredes. Un interfaz IP se crea **asociado a una sola VLAN** concreta y funciona globalmente **para todos los puertos** del switch. Para definirlo basta crear un interfaz con el nombre **vlan<n>**. Una vez creado hay que configurar su IP igual que se hace en los interfaces de un router.

```
interface vlan10
 ip address 192.168.3.10 255.255.255.0
```

Si en el switch no se crea nada más que un solo interfaz IP, conectado a la VLAN de administración, su sistema operativo solo es capaz de recibir tráfico de dicha red y estará aislado del resto de VLANs. Además, hay que recordar que un switch no es capaz de hacer forwarding IP entre interfaces IP ya que no es un router. En el ejemplo anterior, el switch no es accesible nada más que desde la VLAN de administración.

Interfaz de administración en un router

En el caso de un router, podemos crear un subinterfaz para la VLAN de administración para que su servicio SSH sea accesible desde dicha VLAN. Sin embargo, esto crea un problema de seguridad inesperado. Ahora, el router hace *forwarding* entre la VLAN de administración y el resto de VLANs normales, por lo que todos los equipos de red son accesibles desde todas las VLANs, y con esto ponemos en peligro la seguridad de la VLAN de administración. Además, el servicio SSH del router también será accesible en la IP del router en cada VLAN, lo que representa otro riesgo adicional.

Para añadir un router de forma segura a la VLAN de administración debemos:

- Añadir ACLs al **interfaz de administración** que prohíban hacer forwarding entre dicha subred y el resto de subredes. Por ejemplo, si el router tiene como IP 192.168.3.2, y los PCs de administración tienen las direcciones 192.168.3.[16-31], añadimos reglas para permitir tan solo esos accesos al puerto 22 del router:

```
ip access-list extended admin-in
 permit tcp 192.168.3.16 0.0.0.7 host 192.168.3.2 eq 22
ip access-list extended admin-out
 permit tcp host 192.168.3.2 eq 22 192.168.3.16 0.0.0.7
established

interface FastEthernet0/0.10
 encapsulation dot1Q 10
```

```
 ip address 192.168.3.2 255.255.255.0
 ip access-group admin-in in
 ip access-group admin-out out
```

Para añadir el servicio SSH a un router de forma segura sin que se pueda acceder desde el resto de VLANS debemos:

- Añadir una ACL al **servicio SSH** para que solo se pueda acceder al puerto 22 desde la subred de administración. Presta atención al hecho de que esta ACL se instala en el servicio para que no puedan conectar clientes de otros interfaces, y no en el interfaz de la subred de administración que contiene una ACL para evitar el forwarding.

```
ip access-list extended ssh-in
 permit tcp 192.168.3.0 0.0.0.255 any eq 22

line vty 0 4
 access-class ssh-in in
 login local
 transport input ssh
```

Si no se añaden las ACLs anteriores, el router enrutará la VLAN de administración hacia el resto de VLANs de la empresa exponiendo todos los switches a posibles ataques. Igualmente, el servicio SSH del router también será accesible a cualquier cliente de la empresa.

2. Habilitando el acceso SSH en los elementos de red

Todos los equipos Cisco traen deshabilitado por defecto el acceso SSH. En las siguientes secciones vemos los pasos para habilitar el servicio y configurar las contraseñas para acceder con el usuario **admin**. Por cierto. Para habilitar la entrada por SSH, es obligatorio poner un password para cambiar del modo inicial al modo **enable**.

Una vez configurado el interfaz de la VLAN de administración como se explica en la sección anterior pasamos a configurar las contraseñas. Primero ponemos una contraseña para el modo **enable**. En este caso será **cisco** para que sea claramente distinta a la contraseña de acceso mediante SSH.

```
switch(config)# enable secret cisco
```

A continuación ponemos la contraseña para la consola serie del switch y habilitamos el **login** para que nos pida la contraseña de ahora en adelante:

```
switch(config)# line vty 0 15
switch(config-line)# password cisco
switch(config-line)# login
```

El siguiente comando pide al sistema operativo que encripte los passwords de forma que no se vean en la configuración de texto:

```
switch(config)# service password-encryption
```

Para poder habilitar el servicio SSH, el switch debe tener un hostname y un nombre de dominio:

```
switch(config)# hostname R1-S1
R1-S1(config)# ip domain-name acme.com
```

El siguiente paso es generar las claves RSA del servicio SSH. Cuando pregunta el tamaño de la clave, vamos a elegir 1024 bits:

```
R1-S1(config)# crypto key generate rsa
The name for the keys will be: R1-S1.acme.com
Choose the size of the key modulus in the range of 360 to 2048
for your
  General Purpose Keys. Choosing a key modulus greater than 512
may take
  a few minutes.

How many bits in the modulus [512]: 1024
%  Generating  1024  bit  RSA  keys,  keys  will  be  non-
exportable...[OK]
```

Creamos un usuario **admin** con su password **vc0910$$**:

```
R1-S1(config)# username admin secret vc0910$$
```

Y ahora ya estamos listos para habilitar el servicio SSH:

```
R1-S1(config)# line vty 0 15
R1-S1(config-line)# transport input telnet ssh
R1-S1(config-line)# login local
```

No olvides salvar la configuración en NVRAM.

Una vez configurado, añade un PC a la VLAN de administración conectándolo a un switch del data-center. Configura la IP del PC de administración de forma estática y desde **su consola de comandos** usa el comando ssh para conectarte al equipo configurado. Recuerda que el password de acceso es **vc0910$$** y que el de **enable** es **cisco**. Por ejemplo:

```
PC>ssh -l admin 192.168.3.10
Open
Password:

This is the core switch.

P-Core1>ena
Password:
P-Core1#
```

La configuración de contraseñas y de acceso por SSH es idéntica tanto en switches como routers.