

Resolución de Problemas de Switching

[Introducción a la Resolución de Problemas de Capa 2](#)

[Metodología para la Resolución de Problemas](#)

[Data Plane vs. Control Plane](#)

[El Data Plane en la Capa 2](#)

[Principales Comandos para la Resolución de Problemas de Capa 2](#)

Introducción a la Resolución de Problemas de Capa 2

La resolución de problemas en el Curso CCNA, debe orientarse al uso de una serie de pasos metodológicos, que parten del CONOCIMIENTO de la TECNOLOGIA, del patrón de tráfico y del comportamiento de los equipos según una configuración dada.

Este capítulo no es evaluado en sí, como un objetivo específico durante el examen de certificación CCNA, pero el entender y dominar este capítulo, te ayudará a ganar tiempo en responder preguntas específicas que tengan contenido de análisis en el tráfico de la red.

Los problemas, suelen resolverse de una mejor manera, cuando aplicamos una Metodología, tanto para atacar el problema directamente, como cuando analizamos el problema para obtener información que nos ayude a determinar las posibles causas del problema de conectividad.

Muchos de los problemas o actividades de resolución de problemas en una internetwork, tienen que ver con la conectividad a nivel de Capa 3. Sin embargo, este no es el único tipo de problemas que podemos afrontar en una internetwork.

Como Administrador de Rede de Internet y como especialista Cisco System, deberás, no solo tener un Metodología para comenzar a resolver problemas, también deberás tener conocimiento de la terminología utilizada en la internetwork para determinar el flujo de paquetes en la red, así como la manera como se transmiten estos paquetes en la red.

Tres grandes términos que deberás conocer y dominar en esta etapa de formación, son **MANAGEMENT PLANE, DATA PLANE y CONTROL PLANE**.

En la siguiente sección, hablaremos sobre estos términos y su implicación en la resolución de problemas. No debemos olvidar, los principales comandos que dan vida a la recolección de información y depuración de nuestro sistema, como lo son los comandos show y debug.

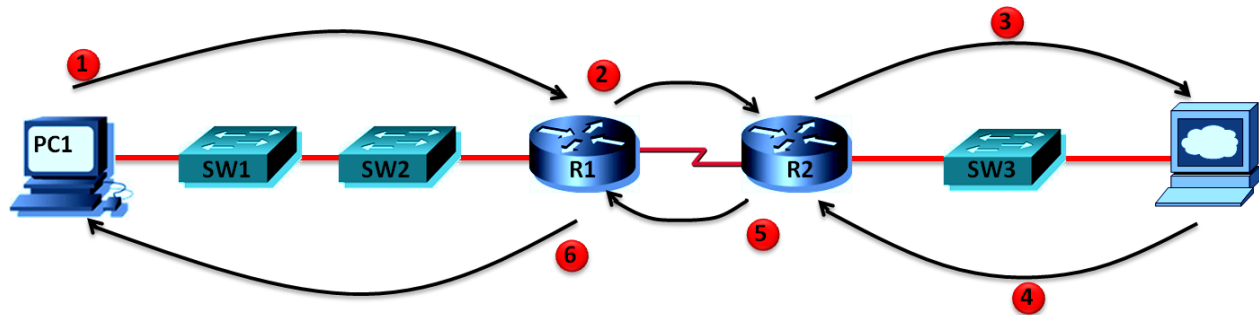


Figura.- Capa 3 problema de aislamiento

Metodología para la Resolución de Problemas

La MODULARIDAD, es el aspecto importante al momento de diseñar y configurar una red, sea esta pequeña, mediana o grande.

En el mismo orden de ideas, la MODULARIDAD, representa un aspecto importantísimo en la resolución de problemas, porque permite, identificar segmentos de nuestra red, como escenarios independientes de conectividad y no como un todo confuso e irreparable.

La MODULARIDAD, nos brinda segmentación y la segmentación, nos brinda a su vez, la posibilidad de identificar el ORIGEN y DESTINO de nuestro tráfico a través de la red, pudiendo en muchos casos ser PREDECIBLE y DETERMINISTICO.

Mientras más DETERMINISTICO y PREDECIBLE, sea nuestro tráfico, más fácil será reparar nuestra red. Ahora como sabemos esta facilidad viene gracias a la posibilidad y capacidad de haber diseñado y configurado nuestra red en módulos.

Al contar y aprender a dividir, física y lógicamente nuestra red, estaremos un paso adelante en la resolución de problemas, porque en la IDENTIFICACION del tráfico ORIGEN y DESTINO, esta la base de toda resolución de problemas en una internetwork.

La metodología que vamos a utilizar, para este capítulo, se enmarca dentro de 3 grandes pasos, los cuales se detallan a continuación:

- 1. ANALISIS Y PREDICCIÓN DEL FUNCIONAMIENTO DE LA RED Y EL FLUJO DE TRÁFICO**
- 2. AISLAMIENTO DEL PROBLEMA**
- 3. ANALISIS DE LA RAZA DEL PROBLEMA**

MANAGEMENT PLANE vs DATA PLANE vs CONTROL PLANE:

Cuando intentamos resolver el problema de nuestra red, desde la perspectiva del Análisis y Predicción del Problema de la red, debemos comenzar con estos dos grandes e importantes conceptos en mente:

Data Plane: El Data Plane, hace referencia al seguimiento de la trama desde el origen hasta el destino, tomando en cuenta el funcionamiento normal de cada equipo. Por ejemplo, los Broadcast generados por los Switches cuando no conocen la Dirección MAC destino, o el mecanismo de encapsulamiento, que realiza el Router para poder cumplir su tarea de enrutamiento. Todas estas son tareas, que ejecuta cada equipo y nos permiten definir como un paquete se comportaría en una internetwork, aun cuando no tenemos conocimiento de algún protocolo configurado en el equipo o mecanismo de **CONTROL PLANE**.

Control Plane: El Control Plane, hace referencia al manejo de uno o varios paquetes en la internetwork y obedece a Protocolos configurables, que ejecutan una actividad en particular, como, por ejemplo, los Protocolos de Enrutamiento. Un protocolo de enrutamiento está a cargo de tomar decisiones de la ruta a tomar por un Router y estas decisiones, tienen influencia en el envío de tramas y paquetes en la red.

Mientras que el Data Plane, hace énfasis en el trayecto o ruta específica que toma la trama en una topología de red, según el equipo que atraviesa, el Control Plane, hace su trabajo, garantizando, optimizando e influenciando la ruta a tomar para el reenvío del paquete en la Internetwork.

Management Plane: El Management Plane, hace referencia a la capacidad que tienen los equipos o interfaces que tienen los dispositivos de red para poder ser gestionados o administrados. Ejemplos de Management Plane son: La Consola para acceder vía CLI, Telnet, SSH, HTTP, API.

El Data Plane en la Capa 2

Existen 4 grandes pasos, que nos ayudaran a resolver problemas a nivel de Capa 2 y ellos son, los siguientes:

DIAGRAMAR LA RED CON CDP:

CDP o Cisco Discovery Protocol, es un protocolo propietario de Cisco, a nivel de Capa 2. Es muy útil para diagramar la red, cuando no tenemos conocimiento de la Topología y es requerido por los Teléfonos IP de Cisco, para su normal funcionamiento.

Sin embargo, CDP no es el protocolo robusto que uno desea. Por esa razón, Cisco, recomienda utilizarlo, solo en aquellas interfaces que lo requieran y desactivarlo en las otras.

Si no se necesita, entonces desactivarlo completo. En resumen, CDP, es un excelente protocolo que nos ayuda a obtener información detallada de nuestros vecinos directamente conectados, permitiéndonos así crear un diagrama de la red en cuestión de minutos.

Show cdp	* Información de configuración de cdp (60", 180", holdtime, CDPv2)
Show cdp neighbors	* Muestra una lista de los vecinos, nombre, interfaz local, tipo, plataforma y el Port ID
Show cdp neighbord detail	* IP, Interfaz local y remota, IOS version, modo duplex Int, plataforma.
Show cdp entry (nombre dispositivo vecino)	* Es como el detail pero de un solo equipo

AISLAR PROBLEMAS DE INTERFACES:

Los problemas de interfaces vienen dados por problemas de Capa Física o en su defecto problemas de Dúplex. Para identificar problemas de Capa 1, se deberán ver los cables y las conexiones, así como los pares identificados en los estándares 568-A/B. Igualmente, un problema de conexión puede identificarse a nivel del estatus de la interfaz, un desacople de DUPLEX, así como una falta de entendimiento en la velocidad de utilizar, sea Ethernet, FastEthernet, GigaEthernet o 10GigaEthernet.

Un ejemplo clásico de problemas de interfaces, es configurar una Interfaz GigaEthernet, para que funcione, manualmente, como una interfaz HALF-DUPLEX y a 10 Mbps, conectada a otra interfaz GigaEthernet, funcionando a velocidad y mecanismo de dúplex normal. Como sabemos, las redes Ethernet trabajan con CSMA/CD, en un modo Half-Duplex, enviando y recibiendo en tiempos separados, mientras que las conexiones Gigaethernet, no utilizan CSMA/CD porque envía y reciben al mismo tiempo.

Esto genera un exceso de tráfico en la red, que no va a ser demodulado por la interfaz en modo Ethernet, por el simple hecho de estar trabajando en mecanismos de comunicación diferentes.

Line status	Protocol Status	Interface Status	Typical Root Cause
Admin Down	DOWN	DISABLE	Shutdown cmd
DOWN	DOWN	NOT-CONNECT	Cable malo, cortado, pines errados o el otro lado esta shutdown.
UP	DOWN	NOT-CONNECT	Cable correcto pero con problemas de capa 2.
DOWN	DOWN (ERR-DISABLE)	ERR-DISABLE	Port-security ha deshabilitado la interfaz(port shutdown
UP	UP	CONNECT	La interfaz está trabajando

IDENTIFICACIÓN DEL TRAFICO EN LA INTERFAZ:

Si estamos utilizando Port Security o algún mecanismo de filtrado de tramas, será necesario, activar o desactivar estos mecanismos para lograr encontrar la solución al problema de conectividad.

PROBLEMAS COMUNES CAPA 1		
Ruido excesivo	Muchos errores de entrada	EMI, cable malo, error de PIN, mala categoría
Colisiones	Mas de 0.1% de tramas enviadas	Duplex mismatch, jabber, Dos, attack
Colisiones tardías	Incremento del contador tardío de colisiones	Dominio de colisiones, Duplex Mismatch

IDENTIFICAR VLAN Y TRONCALES:

Las VLAN de acceso, deberán ser configuradas correctamente en los puertos de acceso.

En el mismo orden de ideas, los enlaces troncales, deberán estar configurados correctamente, permitiendo el tráfico correcto de la internetwork.

Para las troncales, que trabajan con 802.1q, debemos recordar que la VLAN NATIVA, no lleva ninguna etiqueta, por lo que, si se requiere cambiar el valor de la VLAN NATIVA en un puerto troncal, también deberá hacerse en cada puerto troncal, por donde pasará el tráfico de esta vlan.

Modo	ACCESS	DYNAMIC AUTO	TRUNK	DYNAMIC DESIRABLE
ACCESS	ACCESS	ACCESS	ACCESS	ACCESS
DYNAMIC AUTO	ACCESS	ACCESS	Trunk	Trunk
TRUNK	ACCESS	Trunk	Trunk	Trunk
DYNAMIC DESIRABLE	ACCESS	Trunk	Trunk	Trunk

Opción de Comando	Descripción
ACCESS	No permite el TRUNK en la interfaz. Hace que el puerto siempre funcione como puerto de acceso.
TRUNK	Permite el TRUNK en la interfaz. Hace que el puerto siempre funcione como puerto TRUNK.
DYNAMIC DESIRABLE	Modo DTP . Permite el TRUNK en la interfaz. Hace que el puerto busque siempre funcionar como puerto TRUNK.
DYNAMIC AUTO	Modo DTP . Permite el TRUNK en la interfaz. Hace que el puerto espere siempre mensajes de negociacion de Trunk.

Principales Comandos para la Resolución de Problemas de Capa 2

COMANDO	DESCRIPCION
SW(config)# cdp run	Activa el CDP de forma global.
SW(config)# no cdp run	Desactiva el CDP de forma global.
SW(config-if)# cdp enable	Activa el CDP en la interfaz.
SW(config-if)# no cdp enable	Deactiva el CDP en la interfaz.
Sw(config)# show cdp neighbors detail	Muestra información detallada del vecino CDP.
Sw(config)# show cdp neighbors	Muestra una lista detallada de los vecinos CDP.
Sw(config)# show interfaces [type] status	Muestra los estados de conexión de las interfaces.
Sw(config)# show interfaces [type] description	Muestra la descripción de la interfaz.
Sw(config)# show port-security interface [type]	Muestra el estado de port/security en una interfaz
Sw(config)# show vlan brief	Muestra la base de datos de vlan resumida y la asignación de puerto a vlan.
Sw(config)# show interfaces [type] switchport	Muestra el modo operacional de la interfaz.
Sw(config)# show mac-address-table dynamic	Muestra las direcciones MAC aprendidas por el switch y asociadas a las interfaces que han sido aprendidas dinámicamente.
Sw(config)# show interfaces trunk	Muestra las interfaces en modo trunk, las VLAN activas en el dominio y las VLAN en modo trunk.

The House of Routing
<https://cursos.thehouseofrouting.com>