UD 3.- Administración e configuración de conmutadores

Sumario

As redes locais e redes de área extensa funcionan gracias aos **dispositivos de interconexión de redes**, que organizan as súas conexións e fan que a comunicación sexa posible.

Un dos dispositivos máis empregados nas redes locais son os **conmutadores** ou **switches**. Os conmutadores levan unha configuración de fábrica que lles permite funcionar correctamente nas redes nas que van traballar: son equipos que non requiren de ningunha configuración especial para funcionar correctamente. A pesar diso, se queremos realizar unha configuración avanzada relacionada cunha topoloxía máis complexa, temos que modificar os seus parámetros de funcionamento. Na imaxe vemos un switch situado nun armario rack.

3.1. Nivel de enlace

Un conmutador ou switch, en xeral, traballará no **nivel de enlace** da arquitectura de rede: traballará coas **direccións MAC**. Deste xeito, examinan as mensaxes que reciben e consultan as direccións MAC de orixe e destino. A partir desta información, os conmutadores poden saber en que portos están conectados os equipos e cara onde enviar os paquetes recibidos, empregando a táboa na que gardan a topoloxía da rede: unha correspondencia porto-dirección MAC.

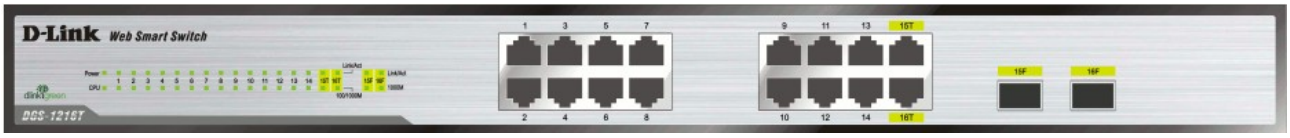
Os equipos que están conectados por un switch (sen VLAN's creadas) forman o que se coñece como **dominio de difusión.**

Dominio de difusión: conxunto de equipos que reciben as mesmas mensaxes broadcast, formando unha rede IP.

Moitos protocolos empregan mensaxes broadcast, entre os que podemos destacar o protocolo **ARP**, e o **DHCP** (***bootp***), como xa foi visto en temas anteriores.
Para reducir o tráfico broadcast, as organizacións dividen as súa rede en varias subredes, normalmente asignadas ás distintas funcións que realizan os seus traballadores. Unha empresa de certo tamaño, por exemplo, pode ter un dominio de difusión para cada departamento: un para o departamento de ventas, outro para o de recursos humanos, etc.

3.2. Funcionamento básico dun switch

Os switches son dispositivos que permiten a interconexión mediante cables (normalmente UTP) de hosts e equipos intermedios. Para iso emprega portos numerados nos que se conectan estes cables.



Vista frontal do switch D-Link DGS 1216T, con 16 portos para RJ45 e 2 portos para fibra óptica

Cando un conmutador recibe unha trama a través dun dos seus portos, realiza as seguintes tarefas:

- Comproba se a trama chegou con erros. Se é así, descártaa ou inicia o procedemento correspondente.
- Le da trama as direccións MAC de orixe e destino da trama.
- Coñecida a MAC de orixe da trama, comproba se existe na súa táboa de direccionamento MAC a entrada que asocia a MAC do dispositivo remitente co porto polo que foi recibida a trama. Se esta asociación non existe, almacena na táboa un rexistro novo MAC-Porto.
- Reenvía a trama polo porto que corresponda:
    - Se a dirección MAC de destino é unha dirección de broadcast, reenviará a trama polo resto de portos.
    - Se a dirección MAC de destino é unha dirección multicast, o resultado dependerá do conmutador. Algúns poden configurarse para reenviar a trama por determinados portos e outros, en cambio, reenviarana polo resto de portos coma se se tratara dunha trama de broadcast.
    - Se a dirección MAC de destino se corresponde cunha dirección unicast, o conmutador

comprobará se hai algunha entrada na táboa de direccionamento MAC para a dirección MAC de destino. Se é así, reenviará a trama polo porto que corresponda segundo indique a táboa e se, pola contra, aínda non existe unha entrada para este destinatario, reenviará a trama por todos os portos (agás aquel por onde chegou a trama). Cando o dispositivo destinatario responda á trama, se o fai, o conmutador poderá aprender en que porto está conectado dito dispositivo.

3.3. Tipos de switches

Segundo o método de conmutación das tramas podemos clasificar os switches:

- **Método de corte** (*Cut-Through*)
- **Almacenamento e Envío** (*Store-and-forward*)
- **Método de Corte Adaptativo** (*Adaptative Cut-Through*)

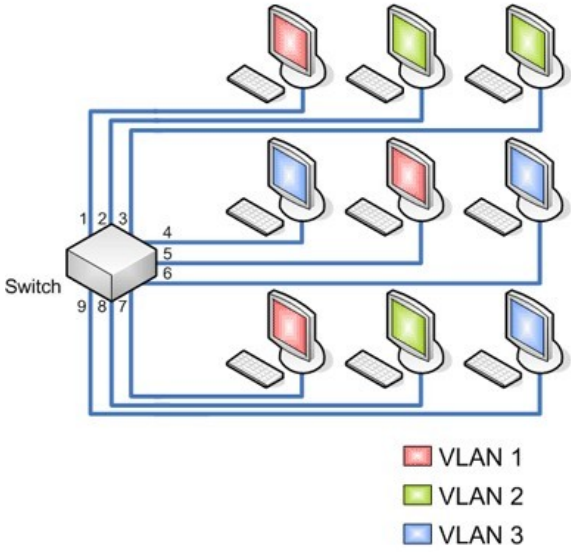
No **método de corte** o switch comeza a transmitir a trama en canto coñece a MAC destino (en canto le os primeiros 6 bytes da trama). **Non** se fai **comprobación de erros**: non hai pois detección de tramas corruptas causadas por colisións (tramas moi pequenas) nin erros de CRC. Canto maior sexa o número de colisións na rede, maior será o ancho de banda consumida no encamiñamento das tramas.
Unha mellora deste método é o método coñecido como **libre de fragmentos** (*fragment-free*), que espera a recibir os primeiros 64 bytes que inclúen todo o encabezamento da trama, evitando o reenvío das tramas corruptas causadas por colisións.
No método de **Almacenamento e Envío** o switch recibe toda a trama antes de facer o envío. Así pode facer a verificación de trama (erros do CRC) para asegurarse que a trama está libre de erros. Con este método a rede é máis confiable, pero o tempo empregado no procesamento das tramas engade un tempo de demora. Esta demora ou *delay* total é proporcional ao tamaño das tramas: canto maior é o tamaño máis tempo leva este proceso.
Finalmente, no **Método de Corte Adaptativo**, os switches son compatibles cos 2 métodos anteriores, e calquera pode ser elixido polo administrador da rede. O switch pode escoller entre os 2 métodos, segundo o número de tramas con erro que pasan polos portos. Se o número de tramas corruptas supera certo nivel, o conmutador pode cambiar do **Método de Corte** a **Almacenamento e Envío,** volvendo ao primeiro método cando a rede se normaliza.
O **Método de Corte** é máis recomendable en grupos pequenos de traballo, mentres que o control de erros (Almacenamento e Envío) será preciso en organizacións máis grandes.

3.4. VLAN's

Un **dominio de difusión** puro é aquel nos que as interfaces de rede dos equipos están conectados por un switch (ou varios), conformando unha rede IP ou LAN. Todos os equipos terán unha configuración

IP similar, variando só a dirección IP.

Unha VLAN (Virtual LAN) é un método que **permite crear redes lóxicas independentes** dentro dunha mesma rede física (a rede cableada). Cada VLAN terá un identificador numérico (VLAN ID) que permite que o switch saiba a que rede lóxica pertence cada equipo.



VLAN1 vermella : 1, 5, 7

VLAN2 verde: 2, 3, 8

VLAN3 azul: 4, 6, 9

Cada VLAN **define un dominio de difusión**, diferenciando **LOXICAMENTE** - na configuración do switch - a que rede ou subrede pertence cada porto do switch. Neste exemplo os **3 dominios de difusión** están formados non por situación física, senón pola configuración do switch:

- VLAN1 vermella : 1, 5, 7
- VLAN2 verde: 2, 3, 8
- VLAN3 azul: 4, 6, 9

Así, os seus dominios de difusión da LAN están definidos **virtualmente** (non fisicamente) polo administrador da rede, de aí o nome de **VLAN**.

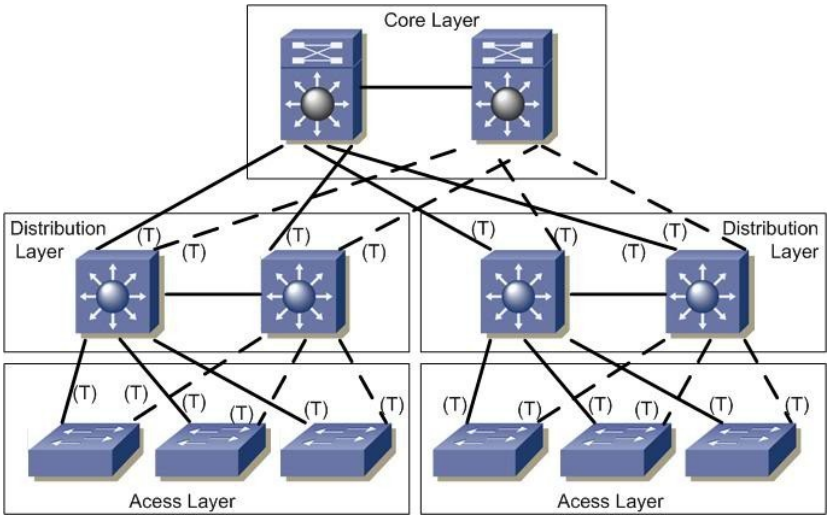
As **VLAN** veranse polo miúdo en temas posteriores

3.5. Portos espello (Port mirroring)

É unha función que teñen os switches para **copiar** todo o tráfico dun porto específico a outro porto. Esta función xeralmente emprégase para atrapar todo o tráfico dunha rede e poder analizalo (con ferramentas como wireshark por exemplo).
O porto espello nun sistema de switch Cisco xeralmente se refire a un analizador de portos do switch (Switched Port Analyzer: SPAN). Algunhas outras marcas usan outros nomes para isto, tal coma Roving Analysis Port (RAP) nos switches 3Com.

3.6. Protocolos de comunicación entre switches. Protocolo STP (*Spanning Tree Protocol*)

O protocolo de árbore de extensión **STP** (Spanning Tree Protocol) é un protocolo baseado en estándares que se usa **para evitar bucles** en switches anidados. Cando se comprobou a eficiencia dos switches para realizar a conmutación en grandes redes, iniciouse a súa incorporación de xeito copioso ata o punto de crear redes con switches anidados, formando unha estrutura de árbore xerárquico. Esta árbore ten rutas **redundantes** que son recomendadas para ofrecer máis confiabilidade e tolerancia a fallos, pero que poden xerar efectos non desexados como os bucles que producen tormentas de broadcast que rapidamente saturan a rede.



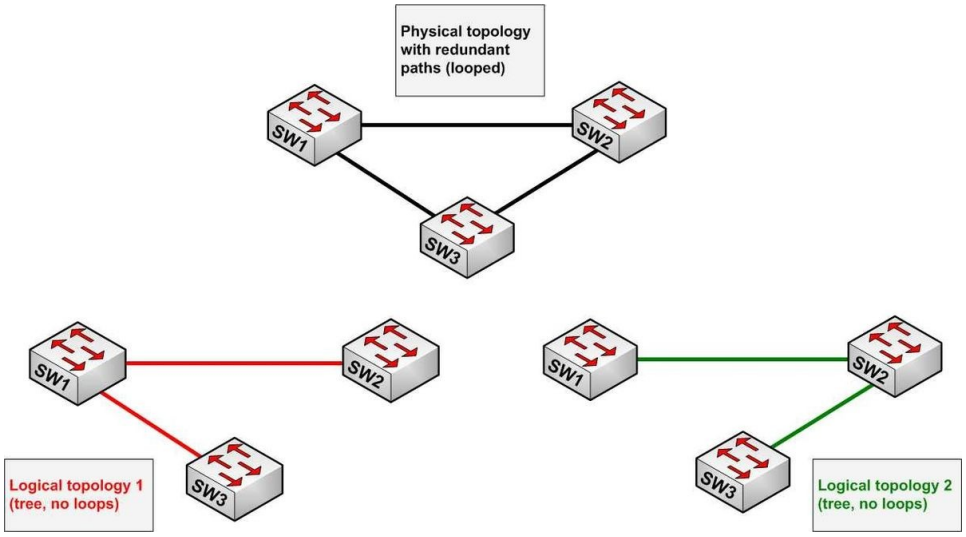
Cando existen bucles na topoloxía de rede, os dispositivos de interconexión de nivel de enlace de datos reenvían indefinidamente as tramas **broadcast** e **multicast**, creando así un **bucle infinito** que consume tanto o ancho de banda da rede coma CPU dos dispositivos de encamiñamento. Isto degrada o rendemento da rede en moi pouco tempo, podendo incluso chegar a quedar inutilizable. Ao non existir un campo TTL (tempo de vida) nas tramas de capa 2, estas quédanse atrapadas indefinidamente ata que un administrador de sistemas rompe o bucle.

Un router, pola contra, si podería evitar este tipo de reenvíos indefinidos. A solución consiste en permitir a existencia de enlaces físicos redundantes, pero creando unha topoloxía lóxica libre de bucles. STP calcula unha única ruta libre de bucles entre os dispositivos da rede pero mantendo os enlaces redundantes desactivados coma **reserva**, co fin de activalos en caso de fallo.

Se a configuración de STP cambia, ou se un segmento na rede redundante chega a ser inalcanzable, o algoritmo reconfigura os enlaces e restablece a conectividade, activando un dos enlaces de reserva. Se o protocolo falla, é posible que ambas conexións estean activas simultaneamente, o que podería dar lugar a un bucle de tráfico infinito na LAN.

A árbore de expansión (Spanning tree) permanece vixente ata que ocorre un cambio na topoloxía, situación que o protocolo é capaz de detectar de xeito automático. O máximo tempo de duración da árbore de expansión é de cinco minutos. Cando ocorre un destes cambios, o switch raíz actual redefine a topoloxía da árbore de expansión ou se elixe un novo switch raíz.

O algoritmo transforma unha rede física con topoloxía de malla, na que existen bucles, por unha rede lóxica en topoloxía de árbore (libre de bucles). Os switches comunícanse mediante mensaxes de configuración chamados Bridge Protocol Data Units (BPDU).



STP actúa contra os bucles, facendo que cada switch que opera con este protocolo envíe unha mensaxe denominada BPDU dende cada un dos seus portos para que os demais saiban da súa existencia. Despois, coa axuda do STA (Spanning Tree Algorithm), detéctanse cales son as rutas redundantes e son bloqueadas.

O resultado é a eliminación dos bucles mediante a creación dunha árbore xerárquica, pero en caso de ser necesitadas a rutas alternativas poden ser activadas.

Existen múltiples variantes do STP debido, principalmente, ao tempo que tarda en converxer o algoritmo utilizado. Unha destas variantes é o **Rapid Spanning Tree Protocol (RSTP)**, que hoxe en día substituíu o uso do STP orixinal.

Como extensión de RSTP, ademais temos **Multiple Spanning Tree Protocol (MSTP)**, que ten novas características.

NOTA: Na actualidade o protocolo STP está sendo substituído polo **SPB** (Shortest Path Bridging) especificado na norma **802.1aq** do IEEE. Este protocolo permite o envío de paquetes por **múltiples traxectos**: todos os camiños permanecen ACTIVOS pero o protocolo evita a creación de bucles. (ver https://es.wikipedia.org/wiki/IEEE_802.1aq)