Apuntes

de

Redes de Ordenadores

Tema 5

Switched LAN

Uploaded by

IngTeleco

http://ingteleco.iespana.es
ingtelecoweb@hotmail.com

La dirección URL puede sufrir modificaciones en el futuro. Si no funciona contacta por email

5.- PUENTES Y CONMUTADORES

5.1.- PUENTES (BRIDGES)

Los puentes son dispositivos que habitualmente se incorporan a una red, bien para poder extenderla más allá de los límites de las especificaciones 802 (limitaciones de distancia o número de nodos) o para mejorar las características de la misma, rendimiento, fiabilidad o seguridad, mediante su segmentación.

Son dispositivos que operan en el nivel de enlace de datos interconectando dos (o más) redes del mismo tipo (802.3, 802.5 , ...) y permitiendo la comunicación entre ellas. Para ello, analizan todas las tramas que reciben para bien filtrar o reencaminarlas de acuerdo con sus direcciones MAC de origen y destino.

La actividad de estandarización de los puentes ha sido llevada a cabo por el grupo 802.1, recogida en los estándares 802.1D y 802.1G (puentes remotos), además de 802.1t (correcciones técnicas y editoriales) y 802.1w (reconfiguración rápida), así como otros relacionados y que analizaremos más adelante en este capítulo 802.1Q, 802.1u y 802.v.

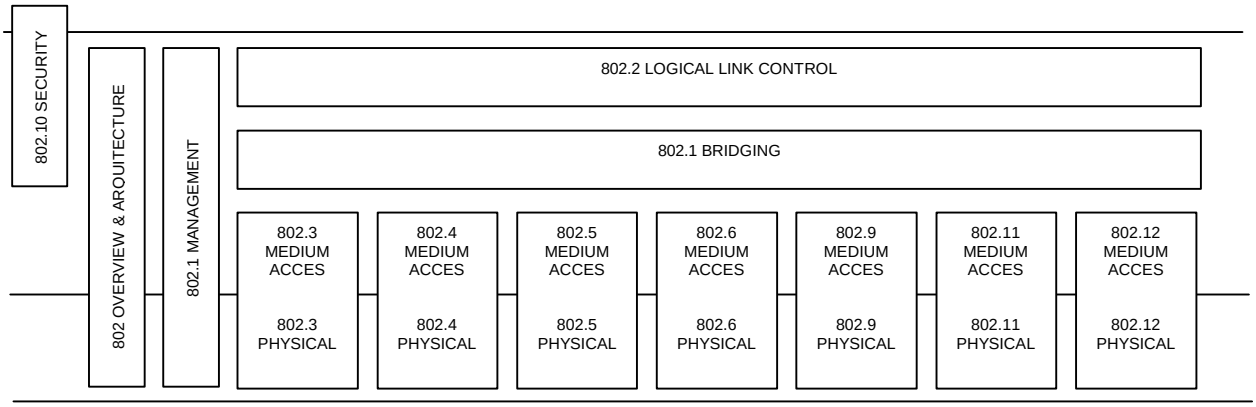

Figura 5.1

En el caso de las redes basadas en colisiones como Ethernet, los puentes dividen la red en dominios de colisión independientes. Esto supone que podrán existir varias estaciones transmitiendo simultáneamente en la red, siempre que se encuentren en segmentos que pertenezcan a diferentes dominios de colisión. De este modo se consigue mejorar el rendimiento de la red, puesto que el ancho de banda estará disponible para cada uno de los dominios de colisión de manera independiente. Además, como sólo una parte del tráfico es encaminada entre segmentos (aquel cuyas estaciones de origen y destino se encuentran en lados distintos del puente), por un lado el tráfico de cada uno de los segmentos será inferior al tráfico global de la red lo que beneficiará al rendimiento, pero también a la seguridad, puesto que los errores de red quedarán confinados a un segmento y no se propagarán por la red.

El modo de operar de los puentes se basa en la inspección de la dirección de destino MAC de todas las tramas que recibe. El puente decide si reenviar o filtrar una trama basándose en la localización de la estación de destino con respecto al emisor de la misma. Aprenden de manera dinámica la localización de los dispositivos, registrando la dirección de origen de cada trama que reciben en la Tabla de Direcciones de Origen (SAT), de este modo saben en todo momento qué estaciones se encuentran conectadas en los segmentos de cada uno de sus puertos. Cuando reciba una trama, buscará en sus tablas SAT en qué puerto se encuentra la estación que corresponde a la dirección de destino de la trama y reencaminará esta hacia el puerto de destino correspondiente a menos que el puerto de recepción de la trama coincida con el puerto en el que se encuentra la estación de destino (se entiende que en este caso la estación de destino ya habrá recibido dicha trama). Es posible agregar filtros basados en cualquiera de los campos de la cabecera del subnivel MAC de modo que el encaminamiento no se lleve a cabo para determinados destinos, orígenes, ... en cuyo caso las tramas serán filtradas y no reenviadas. Pero dado que en la cabecera también se incluye información relativa al nivel superior, también pueden aplicarse filtros relacionados con éste. De de este modo puede mejorarse la seguridad de la red impidiendo el tráfico desde/hacia determinadas estaciones o protocolos. Además, los filtros pueden resultar muy útiles para eliminar tramas broadcast o multicast innecesarias.

Algunas situaciones en las que puede ser conveniente utilizar puentes son las siguientes:

- Interoperabilidad: Se dispone de redes basadas en medios físicos diferentes. Por ejemplo en una empresa puede disponerse de una red Token Ring en unos edificios y Ethernet en otros.

- Distancia: Se necesita cubrir una distancia mayor que la que puede cubrirse con una red local (por ejemplo más de 4 Km en Ethernet a 10 Mb/s).

- Número de ordenadores: Se quiere conectar más equipos que los que se permiten en una red local (más de 1024 en Ethernet, o mas de 72-250 en Token Ring).

- Tráfico: Si existe una elevada cantidad de tráfico, principalmente de carácter local, se puede reducir éste dividiendo la red en varias mediante puentes. Por ejemplo si en una empresa cada departamento tiene su propio servidor mucho de su tráfico será local.

- Fiabilidad: Si se quiere evitar que un problema en un ordenador pueda colapsar toda la red (por ejemplo en Ethernet una tarjeta o transceiver averiado puede inutilizar toda la red). Si se divide la red por zonas el problema afectará a menos equipos.

- Seguridad: En una red local cualquier ordenador funcionando en modo promiscuo puede ver todas las tramas. La división en varias redes evita en cierta medida que los paquetes puedan ser vistos fuera de la red.

5.1.1.- Clasificación

Los puentes pueden clasificarse en algunas de las siguientes categorías:

- Puentes transparentes o con encaminamiento desde el origen
- Puentes traductores
- Puentes locales o remotos

Puentes transparentes

Los puentes transparentes son aquellos cuya presencia y operación resulta transparente a los nodos de la red y son utilizados principalmente en redes Ethernet; son equipos que no necesitan ningún tipo de configuración previa, actuando como dispositivos 'plug and play'.

Veamos como funciona un puente transparente. Supongamos un puente que une dos redes, LAN1 y LAN2. El puente tendrá dos interfaces físicas, cada una conectándole con cada una de las dos LANs. Al encender el puente éste empieza reenviando todas las tramas que recibe por LAN1 a LAN2, y viceversa. En todo momento el puente actúa en modo promiscuo, es decir, capturando todas las tramas que se envían por cada una de las redes a las que está conectado, independientemente de cual sea la dirección de destino.

Además de reenviar las tramas de forma indiscriminada, el puente va silenciosamente extrayendo de cada una la dirección de origen y la dirección de destino; la de origen la anota en una tabla (SAT Source Address Table) correspondiente a la LAN por la que ha llegado la trama, y la de destino la busca en la misma tabla. Supongamos que el puente recibe por la interfaz LAN1 una trama que lleva la dirección de origen A y la dirección de destino B. Primeramente el puente actualizará su tabla de direcciones de LAN1 añadiendo A (si es que no lo estaba ya); después buscará en su tabla si en la columna LAN1 aparece B; si es así sencillamente descartará la trama, ya que sabe que A y B están ambas en LAN1 y no hay ninguna necesidad de reenviar esa trama. Por el contrario, si B no aparece en la tabla de LAN1 el puente reenviará la trama a LAN2. Es posible que B esté en LAN1 y el puente no le tenga aún 'fichado' (porque B no haya enviado aún ninguna trama), pero ante la duda el puente se 'cura en salud' y reenvía la trama por la otra interfaz. Esta estrategia de tirar por elevación enviando la información en caso de duda se denomina inundación (flooding)

El mecanismo utilizado por los puentes para averiguar que ordenadores tienen conectados en cada una de sus redes tiene algunas consecuencias que merece la pena destacar:

- Un ordenador 'tímido', es decir, que no emita ninguna trama, no puede ser localizado, por lo que los puentes enviarán por todas sus interfaces las tramas dirigidas a dicho ordenador. Sin embargo no es probable que un ordenador que recibe tráfico permanezca callado durante mucho tiempo (o de lo contrario pronto dejará de recibirlo, ya que la mayoría de los protocolos requieren alguna contestación, al menos de vez en cuando).

- Las tramas enviadas a direcciones multicast o broadcast (las que tienen a 1 el primer bit) siempre son retransmitidas por los puentes por todas sus interfaces, ya que en principio puede haber destinatarios en cualquier parte (los puentes no almacenan direcciones multicast en sus tablas).

A fin de adaptarse a cambios en la red (por ejemplo un ordenador es desenchufado físicamente de LAN1 y enchufado en LAN2), las entradas en las tablas de direcciones son eliminadas cuando han pasado varios minutos sin que la dirección correspondiente haya enviado ninguna trama.

Existen puentes multipuerta, es decir, con múltiples interfaces, que permiten interconectar varias LANs en una misma caja. El algoritmo en estos casos es similar, salvo que se mantiene una tabla de direcciones para cada interfaz. Las tablas se van llenando con las direcciones 'escuchadas' en cada interfaz; cuando se recibe una trama en cualquiera de las interfaces se busca la dirección de destino en la columna de dicha interfaz; si el destinatario se encuentra allí la trama simplemente se descarta, si no se busca en las columnas correspondientes a las demás interfaces; si se encuentra en alguna columna se manda a la interfaz correspondiente. Por último, si no se encuentra en ninguna de las tablas se envía a todas las interfaces excepto aquella por la que llegó (inundación).

Los puentes han de mantener una tabla de direcciones para cada una de sus puertas; la cantidad de memoria destinada a dichas tablas es limitada, y en redes grandes puede llegar a agotarse. Los fabricantes suelen especificar el número máximo de direcciones MAC que sus puentes son capaces de soportar. Algunos equipos se bloquean sin más explicaciones cuando se les llena la tabla de direcciones MAC.

Puentes con encaminamiento desde el origen

El algoritmo source-route bridging (SRB) fue desarrollado por IBM y propuesto al comité IEEE 802.5 para su uso en los puentes entre LANs.

Con posterioridad a su propuesta inicial, IBM ha ofrecido un nuevo estándar al comité IEEE 802: la solución source-route transparent (SRT) bridging. SRT elimina los SRB puros por completo, proponiendo que los dos tipos de puentos LAN sean los puentes transparentes y los SRT. Aunque los puentes SRT consiguieron un cierto apoyo, el retroceso experimentado por las redes Token Ring ha condicionado notablemente su expansión.

Los puentes SRB reciben este nombre porque suponen que todas las tramas que circulan entre diferentes LAN contienen la información completa de la ruta hasta el destino, registrada por la estación emisora. Los puentes SRB almacenan y reenvían las tramas tal y como se indica en la ruta contenida en el campo correspondiente de la cabecera.

Consideremos la situación reflejada por la figura, y supongamos que el nodo X quiere enviar una trama al nodo Y. Inicialmente el nodo X no tiene forma de saber si el nodo Y reside en su misma LAN o en otra distinta. Para determinarlo, X envía una trama de prueba, que en caso de volver al nodo X sin una indicación positiva de haber visitado al nodo Y hará que suponga que Y se encuentra en un segmento remoto.

Para determinar la localización exacta del nodo Y, X envía una trama de exploración. Cada puente que recibe dicha trama copia la misma en todos sus puertos, añadiendo el identificador del puente y de la LAN a la que lo envía (de este modo se registra la información de la ruta a medida que esta trama viaja por la red). Cuando estas tramas llegue al nodo Y, éste responderá a cada individualmente, utilizando la información de ruta acumulada. Una vez recibidas todas las tramas de respuesta, el nodo X elige el mejor camino de acuerdo a algún criterio predeterminado, que no figura indicado en la especificación IEEE 802.5. Este criterio podría ser elegir la primera respuesta recibida, o la respuesta con menor número de saltos o con el mayor tamaño de trama posible, o combinaciones de las anteriores.

Después de seleccionar una ruta, ésta se insertará en las tramas destinadas al nodo Y en forma de un campo de información de encaminamiento (*routing information field* RIF), para ello se almacenará en una memoria caché para no tener que repetir el procedimiento de búsqueda cada vez que se desee enviar una trama al mismo destino. El campo RIF sólo se incluye en las tramas destinadas a otras LAN y no en aquellas destinadas a estaciones que se encuentran en el mismo segmento de la estación emisora. Con el fin de indicar la presencia de información de encaminamiento en la cabecera, se utiliza el bit más significativo de la dirección de origen, denominado *routing information indicator* bit (RII) que se pone a 1.

El campo RIF de las tramas 802.5 está compuesto de dos campos, tal como se indica en la figura 5.2: el campo de control de encaminamiento y el descriptor(es) de ruta.

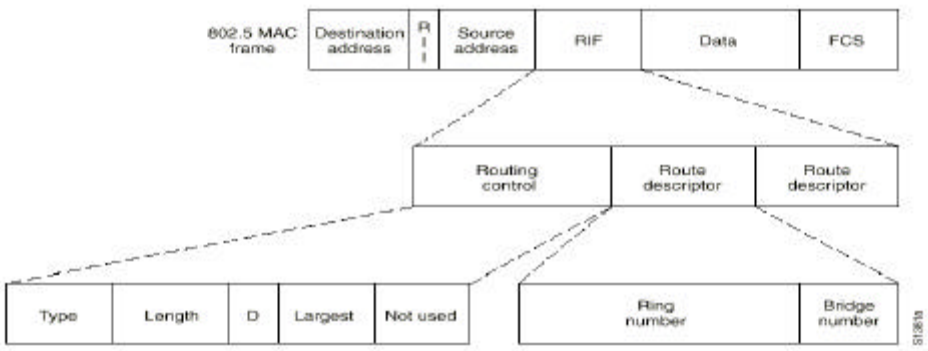

Figura 5.2

El campo de control de encaminamiento (Routing Control) contiene la siguiente información:

- *Tipo*: indica uno de los tres tipos de posibles de control de encaminamiento
    - Encaminado específicamente. Se utiliza cuando el nodo emisor proporciona la ruta en la cabecera RIF. Los puentes utilizan los campos de la descripción de ruta para reencaminar la trama.
    - Exploración de todos los caminos. Utilizado para encontrar un nodo remoto. La ruta se recoge a medida que la trama viaja por la red. Los puentes añadern a la trama su número de puente y el número de anillo al que envían la trama de prueba. (El primer puente añade también el número del primer anillo) El destino de la trama recibirá tantas copias de la misma como rutas existan hasta él .
    - Exploración del Arbol de expansión (Spanning-tree). Utilizado para encontrar un nodo remoto. Sólo los puentes del árbol de expansión (spanning tree) reenvían la trama, añadiendo su número de puente y el número de anillo cuando reenvían la trama. La exploración sobre el árbol de expansión reduce el número de tramas enviadas durante el proceso de búsqueda.

- *Longitud:* Indica la longitud total en bytes del campo RIF. Su valor puede oscilar entre from 2 y 30 bytes.

- *Bit D:* Indica y controla la dirección (avance o retroceso) en que la trama atraviesa el puente. El bit D afecta si los puentes leen las combinaciones número de anillo / número de puente de los designadores de ruta desde la derecha a la izquierda (avance) o de izquierda a derecha (retroceso).

- *Trama más grande:* Indica el tramaño de trama más grande que puede ser gestionado en la ruta indicada. El emisor fija inicialmente el tamaño máximo de trama, pero los puentes pueden reducir dicho valor si no soportan tramas tan grandes.

Cada campo descriptor de ruta consta de dos subcampos:

- *Número de anillo* (12 bits)
- *Número de puente* (4 bits)

Los puentes añaden a la trama su número de puente y el número de anillo al que la reenvían en el proceso de búsqueda de la ruta hacia un destino. Las rutas son secuencias alternadas de números de anillo y puentes comenzando y terminado por el identificador de un anillo. La espcificación de IEEE fija en 14 el número máximo de campos descriptores de ruta (un máximo de 13 puentes o saltos).

Los puentes con encaminamiento desde el origen intentan resolver en el nivel de enlace tareas que corresponden claramente al nivel de red. Algunos expertos opinan que esto es un atraso, y que las decisiones sobre encaminamiento de tráfico deben hacerse en el nivel de red, que es el que tiene la información y los algoritmos adecuados para resolver este tipo de problemas.

Puentes traductores

La mayoría de los puentes operan entre redes homogéneas (que utilizan el mismo protocolo MAC), pero otros pueden traducir entre diferentes procotolos de nivel MAC (por ejemplo, 802.3 y 802.5). El mecanismo básico de traducción es el mostrado en la figura; en ella el nodo A (802.3) envía una trama encapsulada en una trama 802.3 hasta un puente, en éste la trama es despojadade su cabecera en el subnivel MAC y pasada al subnivel LLC para su procesamiento. Después de esto, la información se pasa al subnivel MAC 802.5 que lo encapsula en una trama con cabecera 802.5 para transmitirla por una red 802.5 hasta el nodo B.

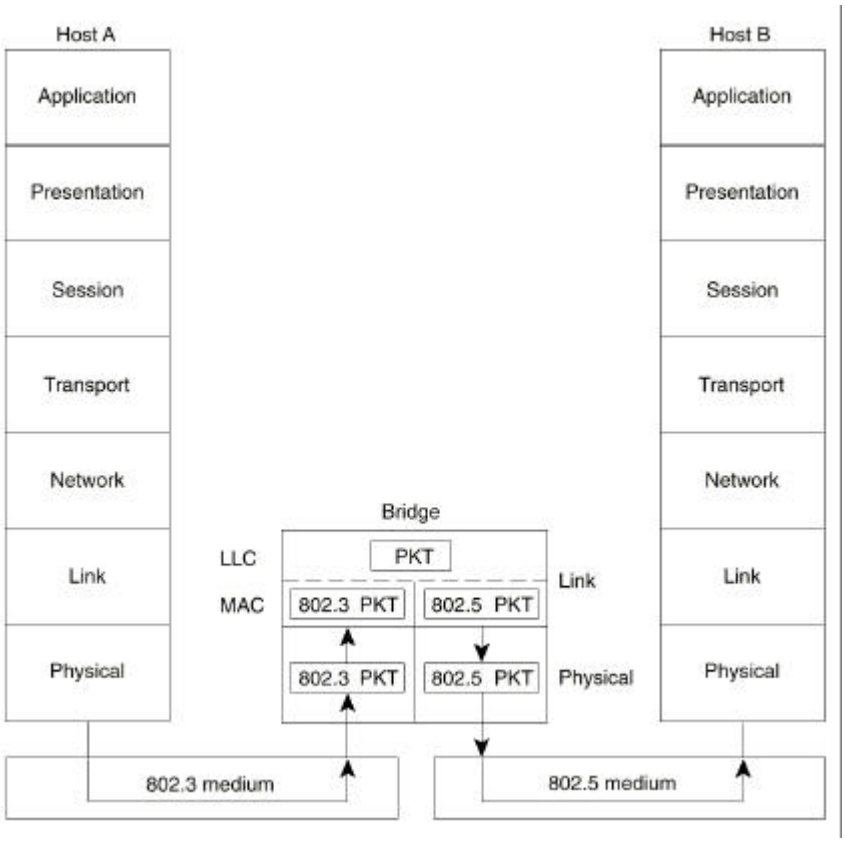

Figura 5.3

La traducción de un puente entre redes de diferentes tipos nunca resultará perfecta porque existen numerosos inconvenientes.

- La ordenación de bits es incompatible: Aunque las direcciones MAC en ambos casos tienen 48 bits de lontitud, la representación interna de éstas es diferente. Token Ring considera el primer bit de la misma el más significativo de un byte; Ethernet, sin embargo, considera el primer bit encontrado el menos significativo del byte.
- Direcciones MAC embebidas—En algunos casos, las direcciones MAC son transportadas realmente en el campo de datos de la trama (el protocolo ARP, por ejemplo). La conversión de estas direcciones, que pueden estar presentes o no es dificil porque debería considerarse en cada caso.
- Tamaños máximos de trama (MTU) sincompatibles: Token Ring y Ethernet soportan diferentes tamaños máximos de trama diferentes. La MTU en Ethernet es de 1500 bytes, mientras que en Token Ring el valor es muy superior. Dado que los puentes no son capaces de fragmentar y reensamblar paquetes, aquellos que excedan del MTU de una red serán descartados.
- Manejo de bits indicadores del estado de la trama: Las tramas Token Ring incluyen tres bits de estado de trama: A, C, y E. Dado que Ethernet no soporta estos bits, el modo en que éstos se traten dependerá del fabricante del puente.
- Manejode las funciones exclusivas de Token Ring: Algunas funciones Token Ring no tienen equivalente en Ethernet. Ethernet, por ejemplo, carece de mecanismo de prioridad; otros bits que deben ser eliminados cuando se covierte una trama Token Ring frame en una trama Ethernet son los bits de token, el de monitor, y los de reserva.
- Manejo de la trama de exploración: Los puentes transparentes no son capaces de colaborar en el proceso de descubrimiento de rutas SRB.
- Manejo del campo información de encaminamiento (RIF): Los puentes transparentes no tienen un equivalente al campo RIF ni a la función de encaminamiento.
- Incompatibilidad de los algoritmos de árbol de expansión (spanning-tree).

No existe una estandarización real del modo en que debe producirse la comunicación entre dos tipos de medio, por lo cual, existen diversos métodos para su implementación en puentes traductores.

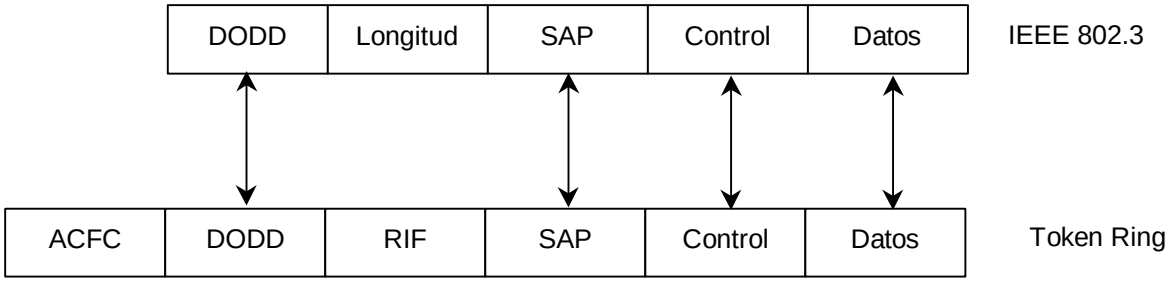

Figura 5.4

En la figura 5.4 se muestra la conversión de tramas entre IEEE 802.3 y Token Ring. Los campos dirección de origen y destino (DODD), el punto de acceso al servicio (SAP), y el campo de datos se trasladan a los campos correspondientes de la trama de destino, el resto de los campos son eliminados.

En la figura 5.5 se muestra otro ejemplo con la conversión entre una trama Ethernet II y una trama SNAP de Token Ring

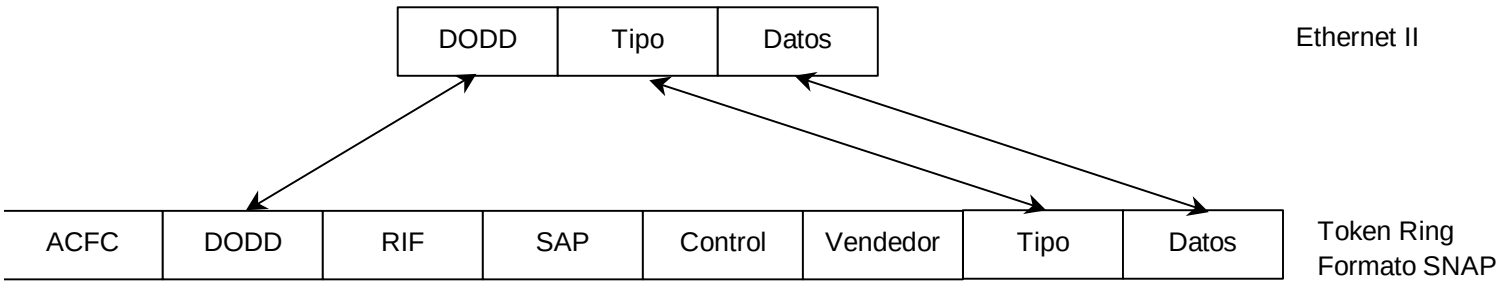

Figura 5.5

Puentes remotos

En ocasiones se tiene necesidad de conectar entre sí dos redes locales remotas como si fueran la misma LAN. Para esto se usa un tipo de puentes denominados puentes remotos. El mecanismo básico de funcionamiento es el mismo que hemos visto para los puentes locales, salvo que el puente está constituido por dos 'medios puentes' interconectados por una línea dedicada cuya velocidad típicamente suele estar entre 64 Kb/s y 2,048 Mb/s. También se pueden unir los puentes remotos por redes X.25, Frame Relay o incluso radioenlaces.

El protocolo spanning tree también se utiliza en puentes remotos. Topológicamente un puente remoto el enlace punto a punto se debe considerar como una LAN con un puente en cada extremo.

No hay un estándar en puentes remotos, lo que hace que generalmente la interoperabilidad solo sea posible entre equipos del mismo fabricante. Las tramas LAN se encapsulan normalmente en tramas HDLC, pero el sistema utilizado puede variar de un fabricante a otro.

Dado que generalmente los puentes remotos se conectan mediante líneas de menor velocidad que las redes a las que enlazan, es frecuente que dicha conexión sea el factor limitante de las prestaciones de la red (aun cuando el algoritmo propio de los puentes evita que el tráfico local cruce al otro lado). Esto es especialmente crítico cuando se utilizan líneas de baja velocidad (por ejemplo 64 Kb/s) y mas aun cuando se trata de puentes transparentes y el tráfico broadcast y/o multicast es importante (recordemos que este tipo de tráfico siempre atraviesa los puentes transparentes). Los puentes remotos no pueden mejorar la velocidad de los enlaces WAN, pero pueden compensar las diferencias de velocidad mediante una capacidad de almacenamiento (buffering) suficiente. Si un

dispositivo LAN capaz de una velocidad de transmisión de 3 Mbps quiero comunicarse con otro dispositivo en una LAN remota, el puente local debe regular el flujo de datos de 3 Mbps para no saturar el enlace de 64 kbps, para ello almacena los datos recibidos en un buffer y los envía por el enlace serie a la velocidad que este puede soportar. Este almacenamiento sólo puede llevarse a cabo en ráfagas cortas que no sobrepasen la capacidad de almacenamiento del buffer.

5.2.- ARBOL DE EXPANSIÓN (SPANNING TREE)

En algunas situaciones es interesante unir dos LANs con más de un puente, normalmente por razones de fiabilidad o redundancia. Sin la existencia de un protocolo puente-puente, los algoritmos de los puentes tranparentes fallarían cuando existen varios caminos alternativos, constituidos por puentes y redes LAN, entre dos redes LAN cualquiera de un conjunto de LAN interconectadas.

En la figura 5.6 puede verse una situación en la cual existen dos caminos alternativos entre las redes 1 y 2 que originan un bucle.

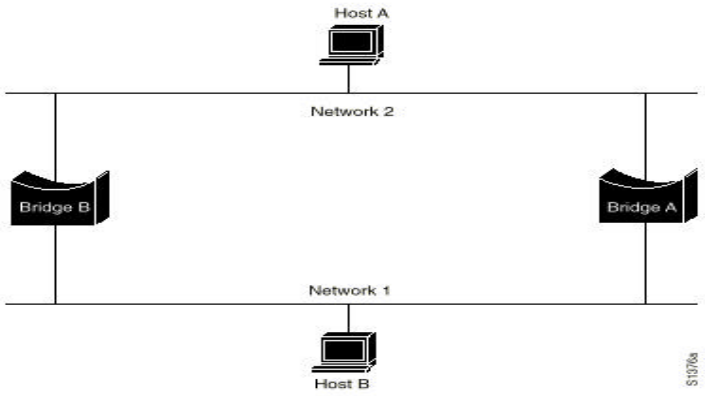

Figura 5.6

Supongamos que el nodo A envía una trama al nodo B. Los dos puentes, A y B conectados a la red 2 recibirán la trama correctamente, registrando la dirección del nodo A perteneciente a la red 2 y, suponiendo que disponen en su tabla SAT de la dirección de B encaminarán dicha trama por el segmento de la red 1. El nodo B recibirá dos veces la misma trama, pero además, los puentes A y B recibirán la trama procedente del nodo A a través del interfaz conectado a la red 1, lo que hará que cambien la entrada correspondiente de la tabla SAT para indicar que el nodo A se encuentra ahora en la red 1. Cuando el nodo B envíe un mensaje al nodo A, como respuesta a la trama recibida, ninguno de los puentes encaminaría dicha trama, puesto que en su opinión el nodo A se encuentra en la misma red que el nodo B. En esta situación, el nodo B se vería imposibilitado de enviar ningún mensaje al nodo A.. Pero es que además de estos problemas básicos de conectividad, si los puentes A y B no conocieran la ubicación del nodo B difundirían la trama recibida por la red 1 hacia la red 2, ya así sucesivamente, provocando que las tramas entren en un bucle infinito, y si en vez de ser puentes con solo 2 segmentos fueran multisegmento provocarían problema de tráfico en la red.

Una topología con bucles puede resultar muy útil porque permite preparar caminos alternativos ante potenciales fallos de la red, aumentando la tolerancia de la red a los fallos mediante el incremento de la flexibilidad topológica. Por lo tanto, y con el fin de aprovechar esta ventaja resulta preciso idear algún mecanismo que obvie los inconvenientes anteriores, permitendo a los puentes comunicarse entre sí, intercambiando información sobre la topología de las conexiones existentes; una vez averiguada dicha topología los puentes desactivarán las conexiones redundantes para garantizar que haya un único camino (directo o indirecto) uniendo todas las redes, de forma que se evite la creación de bucles. Las conexiones que lógicament se pongan fuera de servicio quedarán listas para entrar en funcionamiento si las conexiones activas fallan por algún motivo. El algoritmo se repite cada cierto tiempo, por lo que si alguno de los enlaces queda fuera de funcionamiento por algún motivo (por ejemplo una avería) en la siguiente ronda se habilitará algún camino alternativo que lo sustituya. El protocolo que permite esto se conoce como Spanning Tree Protocol (STP) y también como Spanning Tree Learning Bridge Protocol, y forma parte de la especificación IEEE 802.1D.

El algoritmo del arbol de expansión o “spanning-tree algorithm” (STA) fue desarrollado por Digital Equipment Corporation y fuer revisado posteriormente por el comité IEEE 802 que lo publicó más tarde como la especificación 802.1d (aunque ambos algorimnos no sean compatibles).

El STA crea un subconjunto de la topología de la red libre de bucles poniendo en estado “standby” aquellos puertos de los puentes que, si estuvieran activos, crearían bucles. El bloqueo de los puertos puede ser activado en caso de que uno de los enlaces principales falle, proporcionando un camino alternativo en la red. El STA utiliza una conclusión de la teoría de grafos como base para construir un subconjunto libre de bucles. La teoría de grafos afirma lo siguiente: “Para cualquier grafo conectado constituido por nodos y enlaces entre pares de nodos, existe un arbol de expansión de enlaces que mantiene la conectividad del grafo sin contener bucles”.

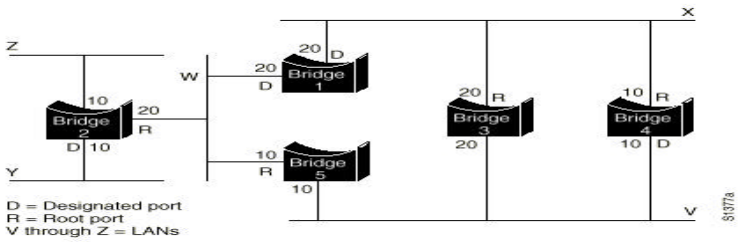

Figura 5.7

La figura 5-7 ilustra el modo en que el STA elimina los bucles.

A cada puente se le asigna un identificador único (BID) de 8 bytes, generalmente constituido por una prioridad (2 bytes) y una de las dirección MAC del puente (6 bytes) y a cada puerto se le asigna un identificador único, dentro de cada puente, de 16 bits con 6 bits de prioridad y 10 bits de número de puerto.

Además, a cada puerto se le asocia un coste, generalmente basado en la guía indicada en el estándar 802.1d. De acuerdo con la especificación original, el coste es 1000 Mbps dividido entre la velocidad de transmisión del segmento. Sin embargo, y para compensar la velocidad creciente de las redes más allá del Gbps se ha modificado el coste estándar, asignando los siguientes valores

Velocidad	Coste STA
4 Mbps	250
10 Mbps	100
16 Mbps	62
45 Mbps	39
100 Mbps	19
155 Mbps	14
622 Mbps	6
1 Gbps	4
10 Gbps	2

Tabla 5.1

En cualquier caso el coste puede ser un valor arbitrario elegido por el administrador de la red en función de los objetivos que persiga.

La primera actividad del protocolo de árbol de expansión es seleccionar un *puente raíz,* que es aquel con el identificador más pequeño. En la figura 5.x es el puente 1. A continuación, se determina el puerto raíz de todos los puentes, que es aquel a través del cual puede alcanzarse el puente raíz siguiendo un camino con menor coste agregado, lo que se denomina *coste del camino raíz*.

Finalmente, se determinan los *puentes designados* y sus *puertos designados*. Un puente designado es aquel puente de cada segmento o LAN que proporciona el camino raíz mínimo y resulta ser el único puente con permiso para encaminar tramas hacia y desde la LAN para la cual es designado. El puerto designado de una LAN es el puerto que conecta ésta con el puente designado.

En algunos casos, dos o más puentes pueden tener el mismo coste, por ejemplo en la figura 5.x los puentes 4 y 5 pueden alcanzar el puente 1, el puente raíz, con un coste de 10. En este caso, los identificadores de puente se utilizan de nuevo para determinar en este caso los puentes designados; de modo que en el ejemplo de nuestra figura el puerto de la LAN V del puente 4 sería elegido en lugar del correspondiente al puente 5.

Siguiendo este proceso son eliminados todos los puentes, menos uno, directamente conectados a cada LAN, eliminando así todoslos bucles entre dos LAN. STA también elimina bucles que involucren más de dos LAN, preservando sin embargo la conectividad. La figura 5.x muestra el resultado de aplicar STA al ejemplo anterior.

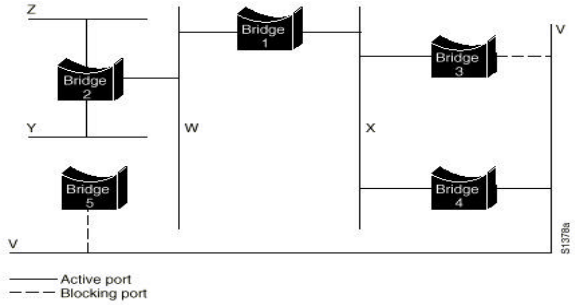

Figura 5.8

El cálculo del árbol de expansión se lleva a cabo cada vez que se conecta un puente y cuando se detecta un cambio en la topología. Su aplicación precisa de comunicación entre los puentes que participan en el proceso, que se lleva a cabo mediante el intercambio de mensajes de configuración, llamados BPDU (*bridge protocol data units*).

Los mensajes de configuración contienen información que identifica el puente que es considerado el raíz (root identifier) y la distancia desde el nodo emisor al nodo raíz (root path cost). Los mensajes de configuración contienen también los identificadores de puento y puerdo del nodo emisor así como la antigüedad de la información contenida en el mensaje de configuración y la antigüedad máxima de validez fijada por el puente raíz para la información topológica.

Los puentes intercambian mensajes de configuración a intervalos regulares (generalmente cada uno o cuatro segundos). Si un puente falla, causando un cambio en la topología, los puentes vecinos detectarán la falta de mensajes de configuración e iniciaran un nuevo cálculo del árbol de expansión. Todas las decisiones topológicas de los puentes transparentes se toman localmente. Los mensajes de configuración se intercambian entre nodos vecinos y no existe ninguna autoridad central sobre topología de la red y la administración.

La figura 5.9 muestra el formato de una BPDU de acuerdo con el estándar IEEE 802.1d

2	1	1	1	8	4	8	2	2	2	2	2
Identificador de Protocolo	Versión	Tipo de Mensaje	Flags	Id Raíz	Coste del camino ráiz	Id Puente	Id Puerto	Antigüedad del mensaje	Antigüedad máxima	Tiempo de Hello	Demora en reenvío

Figura 5.9

Las notificaciones de cambio topológico sólo contienen los primeros 4 bytes y sirven para que un puente notifique a otros que se ha producido un cambio topológico para que éstos inicien también el cálculo del nuevo árbol de expansión.

No es posible con Spanning Tree tener varias conexiones activas al mismo tiempo, lo cual permitiría repartir el tráfico entre varios puentes, mejorando así el rendimiento de la conexión (como se hace por ejemplo en etherchannel).

El protocolo spanning tree es algo opcional, por lo que no siempre está presente en los puentes. Al construir una topología basta con que uno de los puentes que forman el bucle incorpore el spanning tree para que el puente rompa el bucle y la red funcione correctamente.

5.3.- LAN Conmutadas

De forma genérica, podemos describir un conmutador LAN como un dispositivo de red que acepta paquetes entrantes y los retiene en un almacenaje temporal, antes de enviarlos a sus direcciones de destino.

Los conmutadores son similares a los puentes transparentes en funciones tales como el aprendizaje de la topología, el encaminamiento de tramas y el filtrado, pero proporcionan mayor densidad de puertos que un puente a un coste muy inferior del de los puentes tradicionales. Sin embargo, también incorporan nuevas funcionalidades tales como comunicaciones dedicadas entre dispoitivos, conversaciones múltiples simultáneas, comunicación full-dúplex y adaptación de l velocidad del medio. Podemos sin embargo decir que la función básica de un conmutador LAN es dividir un “dominio de broadcast” en “dominios de colisión”

Por esta razón, los conmutadores LAN están permitiendo diseños de red con menos dispositivos por segmento, incrementando de este modo el ancho de banda del que dispone cada usuario; esta tendencia de reducir el número de usuarios por segmento se conoce como microsegmentación, que llega hasta la creación de segmentos dedicados, un dispositivo por segmento en las redes totalmente conmutadas. En este caso, cada dispositivo puede aprovechar toda la capacidad de transmisión el medio sin contienda con otros dispositivos, desapareciendo por tanto las colisiones y sus consecuencias.

Los conmutadores LAN aparecieron por primera vez a mediados de los 90 en las capas de fibra óptica o FDDI de las LAN. Desde entonces, su adopción se ha extendido a otros medios físicos, incluyendo las redes Ethernet más comunes con cableado de cobre. Aunque los conmutadores LAN llevan presentes más de una década, no ha sido hasta los últimos tres años cuando la tecnología ha aumentado su predominio y las tasas de adopción han crecido de forma masiva. Se trata de una tecnología que actualmente sustenta la creación de redes en las empresas, y se asienta en el núcleo y en la red troncal de numerosas infraestructuras, si bien es cada vez es más común también el despliegue de conmutadores en la periferia de las LANs.

El ascenso del conmutador ha coincidido también con la necesidad de segmentar las LAN para mejorar el uso del ancho de banda disponible y evitar problemas de congestión en la red, algo necesario con el aumento del tráfico en las LAN.

De hecho, la producción de conmutadores LAN está empezando a hacer decrecer la demanda de hubs, muy elevada hasta ahora. Las cifras que recoge IDC indican que, para el año 2004, los puertos vendidos de conmutadores LAN de todos los tipos alcanzarán los 231 millones de unidades, mientras que los puertos para hubs disminuirán hasta 31 millones de unidades, lo que supone menos del 50 por ciento de las ventas registradas en 1999. Las razones principales para esta reducción del mercado de hubs son el menor precio de los conmutadores LAN y sus mayores niveles de funcionalidad, así como el aumento en la demanda de ancho de banda gestionable.

Inicialmente los conmutadores sólo trabajaban en la Capa 2 del modelo OSI, mientras que la Capa 3 se gestionaba mediante routers. Sin embargo, los conmutadores han sufrido una importante evolución, de modo que los conmutadores de última generación pueden trabajar también con las capas situadas por encima de la Capa 2, pues han sido diseñados con el tipo de “inteligencia” integrada que hasta ahora era patrimonio de los routers (lo que también ha introducido una notable confusión en las diferencias entre routers y conmutadores). Este desarrollo se conoce como conmutación multicapa (MLS) y constituye la gran evolución actual de la tecnología LAN.

La propuesta de valor de MLS se centra en la mejora del rendimiento y control, y entre sus ventajas concretas podemos destacar:

- La mejora de las arquitecturas.
- Las empresas en rápido crecimiento pueden ampliar su capacidad de red con mayor facilidad.
- Se escalan las soluciones hasta para millones de paquetes por segundo tanto en Capa 2 como en Capa 3.
- Hace llegar la conmutación y enrutamiento de alta velocidad y sin bloqueos a todos los puertos, y por tanto a todas las interfaces y protocolos de red.

La diferencia que distingue a los dispositivos de MLS, frente a los dispositivos exclusivamente de Capa 2, es que cubren las funciones tanto de los conmutadores de Capa 2 como de los routers de Capa 3, estando dotados al mismo tiempo de las características inteligentes adecuadas para cubrir también la capa de aplicación. La capacidad de conmutación de Capa 3 es esencial para sacarle el máximo partido a Gigabit Ethernet, al anterior Fast Ethernet que funciona a 100 Mbits/s. y a la introducción de nuevos sistemas operativos (tales como Windows 2000). Las capas se refieren al modelo de red OSI y a su especificación básica de siete niveles.

Con la conmutación de Capa 4, se pueden lograr aún más ventajas al resolver los problemas de conexión en red, especialmente a nivel de arquitectura. Permite clasificar las aplicaciones y propagar dichas clasificaciones por toda la red. Se pueden integrar los atributos de las políticas de gestión en el propio tejido de conmutación, haciendo innecesarios los servidores dedicados a gestión de políticas. Permiten fijar los niveles de prioridad del tráfico, así como el equilibrio de carga en los servidores. Y todas estas funciones van integradas en cada conmutador de Capa 4, con lo que se dispone también de opciones de seguridad y de flexibilidad en el despliegue. Entre éstas se incluyen redes troncales, LANs virtuales y la asignación dinámica de recursos de intranet. Tales redes internas basadas en Web son cruciales para las comunicaciones de la empresa y para compartir la información, y a menudo es necesario ampliarlas o reconducirlas para dar respuesta a cambios en las necesidades. Los conmutadores de Capa 4 soportan también la creación de una sofisticada clase de gestión y de calidad de los niveles de servicio de gestión.

5.3.1.- Tecnologías de conmutación

Originalmente un conmutador LAN no era sino un puente multipuerto, que operaba en la Capa 2 del modelo OSI tal y como hemos visto en los apartados anteriores reenviando las tramas por el puerto adecuado en función de su dirección MAC de destino.

Los conmutadores LAN emplean uno de los siguientes métodos para el encaminamiento del tráfico:

Cut-Through

Los conmutadores leen la dirección MAC tan pronto como les es posible (en cuanto han recibido los bytes suficientes de la cabecera MAC) y depués de almacenar los 6 bytes de la dirección, toman la decisión de encaminamiento y comienzan la retransmisión de la trama hacia el nodo de destino mientras se sigue recibiendo el resto de la trama.

Esta técnica se caracteriza por una muy baja latencia, que puede ser de sólo un 5% de la que genera la siguiente.

Algunos conmutadores almacenan los primeros 64 bytes con el fin de asegurarse de que no se produce una colisión y de este modo no introducir tramas fruto de una colisión en el segmento de destino. Esta técnica se conoce como Fragment free y permite eliminar una buena parte de las tramas erróneas.

Store and Forward

- El conmutador almacenará la trama completa en el buffer y analizará la validez de la misma antes de reenviarla. Si una trama contiene errores o tiene una longitud menor de 64 bytes será descartada, en caso contrario, el switch analizará la dirección de destino, tomará la decisión de encaminamiento y retransmitirá la trama por el puerto oportuno.

Muchos conmutadores combinan ambas técnicas, utilizando Cut-through hasta que se detecta cierto nivel de errores, cambiando entonces a una técnica Store and Forward. Cuando la tasa de errores vuelve a bajar por debajo del umbral marcado, se retoma la primera de las tácnicas para mejorar el rendimiento. Son muy pocos los conmutadores que operan exclusivamente con la técnica Cut-through puesto que no proporciona ninguna corrección de errores, perdiendo uno de los valores añadidos de los conmutadores que es el aumento de fiabilidad de la red.

En algunos casos la técnica de Store and Forward es necesaria, como por ejemplo en los conmutadores asimétricos, donde la velocidad de recepción puede ser mayor que la de emisión, o cuando el puerto de salida está ocupado.

Los conmutadores LAN varían en su diseño físico. En la actualidad hay tres configuraciones muy utilizadas en cuanto al modo de realizar la conmutación.

Memoria compartida

Se almacenan todas las tramas recibidas en un buffer común compartido por todos los puertos para a continuación enviarlas por el puerto adecuado a su dirección de destino.

Matriz

Este tipo de conmutador tiene una matriz interna que interconecta los puertos de entrada y salida entre sí. Cuando se detecta un paquete en un puerto de entrada, se compara la dirección MAC con la tabla SAT para averiguar el puerto de salida apropiado. El conmutador realiza una conexión en la matriz donde se intersectan estos dos puertos.

Arquitectura de bus

En lugar de una matriz, se comparte un bus común de transmisión entre todos los puertos mediante una técnica TDMA. En este caso, el conmutador dispondrá de un buffer dedicado a cada puerto, así como un ASIC para controlar el acceso al bus interno.

Mientras las tramas son procesadas en el conmutador, éste las mantiene almacenadas en buffers. Si el segmento de destino está ocupado, el conmutador mantendrá la trama en el buffer a la espera de poder darle salida. El desbordamiento de los buffer representan un grave problema, por lo que el análisis de su tamaño y la estrategia de uso es un aspecto muy importante en el diseño del conmutador. En cuanto a la ubicación de los buffers existen varias alternativas.

Buffer en la entrada.

Se dispone de un buffer en cada puerto de entrada para almacenar las tramas recibidas mientras se toma una decisión de encaminamiento. La retransmisión de la misma se produce cuando el puerto de salida esté libre. En este caso se puede producir un bloqueo “head-of-line” en caso de que el puerto de salida correspondiente a una trama esté congestionado y ésta interrumpa la emisión de otras tramas recibidas posteriormente y cuyos puertos de salida sí esten libres.

Buffer en la salida

Se dispone de un buffer en cada puerto de salida, donde se coloca la trama tan pronto como se ha identificado el puerto de salida. Tiene el incoveniente de que no pueden producirse varias escrituras simultáneas sobre el mismo buffer, por lo que el acceso es denegado a un puerto de entrada si se está enviando tráfico a dicho destino desde otro puerto de entrada.

Buffer en el camino

Hay un buffer tanto en el puerto de entrada como en el de salida, con lo que se evitan los bloqueos mencionados anteriormente.

Si consideramos las especificaciones de un comutador y sumamos la velocidad teórica de todos los puertos tendremos el rendimiento teórico del conmutador. Si el bus del dispositivo, o sus componentes no pueden manejar el total teórico de todos los puertos el conmutador opera con bloqueo (blocking switch). Existe un debate sobre la conveniencia de que todos los conmutadores operaran sin bloqueo, pero en este momento y por los costes añadidos que esto supone sólo los conmutadores de backbone trabajan actualmente sin bloqueo. Para la mayoría de las aplicaciones es aceptable un conmutador con bloqueo con un nivel de rendimiento razonable, puesto que el grado de utilización de la red será relativamente bajo.

5.3.2.- Tipos de conmutación LAN

Más allá de las funciones básicas de los conmutadores LAN, se han ido añadiendo capacidades adicionales que incrementan la propuesta de valor del conmutador. Los conmutadores LAN tienen ya un considerable impacto en el negocio de hubs y comienzan a penetrar en áreas que hasta ahora eran patrimonio de los routers. Los desarrollos futuros supondrán niveles aún mayores de funcionalidad en la conmutación. Así han surgido productos de conmutación que trabajan en las capas 3 y superiores del OSI. Los routers disponen aún de ventajas frente a los conmutadores en campos tales como el manejo de varios protocolos y la conectividad en WAN. Estos son los tipos de conmutadores de LAN disponibles hoy en día para distintas capas del OSI, basados en definiciones propuestas por IDC:

- Conmutadores de Capa 2: Este hardware opera en la capa del enlace de datos de los modelos OSI e interacciona con la capa física de una red, donde se manejan tareas tales como la inserción y extracción de datos de dicha red. Los conmutadores de Capa 2 se instalan tanto en segmentos de la red como en el extremo de una LAN, y son aún predominantes. Seguirán reteniendo su valor durante un tiempo considerable.

- Conmutadores de Capa 3: Se trata de dispositivos capaces de enrutar paquetes a la velocidad del cable, empleando la capa de red. El rendimiento de estos conmutadores supera al de los routers, logrando cifras de millones de paquetes por segundo frente a las tasas de miles de paquetes por segundo que logran los routers basados en software; este rendimiento es alcanzable gracias a que la “inteligencia” del conmutador está incorporada en el hardware del mismo. La incorporación de características adicionales tales como la conectividad en WAN y el manejo de varios protocolos ayudará a que los proveedores de este tipo de dispositivos puedan comparar favorablemente sus productos con los routers, tanto a nivel de empresa como de proveedor de servicios. Estos dispositivos pueden trabajar con una técnica “Packet by Packet“ (PPL3), analizando cada paquete reenviado o bien “Cut-trough” (CTL3) si analizan el primer paquete de una serie, establecen una conexión y a partir de este momento realizan la conmutación a nivel 2, consiguiendo todavía un mejor rendimiento. Hacen uso de protocolos de red (RIP y OSPF) para para procesar rutas externas al conmutador.

- Conmutadores de Capa 4: En este nivel, los conmutadores son capaces de distinguir entre paquetes para distintos tipos de aplicaciones. Los gestores de la red pueden centrarse en proporcionar un servicio óptimo a grupos prioritarios de usuarios, clasificar los tipos de tráfico de aplicaciones y habilitar el número máximo de servidores incluyendo su equilibrio de carga. Además, estos conmutadores permiten establecer las condiciones de clase de servicio y de calidad de servicio para todo tipo de redes, incluyendo redes convergentes basadas en telefonía LAN. Los conmutadores de Capa 4 soportan también estándares avanzados de red, tales como el protocolo de configuración dinámica de hosts (DHCP), que facilita los parámetros de configuración automática en toda una red. Los conmutadores de Capa 4 tienen también un valor incalculable para soportar difusiones multicast en una red.

- Conmutadores Inteligentes de Contenido (Capas 5-7): La identificación y conmutación de contenidos provenientes de la Web y de Internet son los cometidos principales de los conmutadores diseñados para las capas cinco a siete del OSI. Dichos dispositivos han de filtrar el tráfico basándose en diversos criterios, tales como cabeceras de las solicitudes HTTP, cookies y URLs. En estos niveles de conmutación se facilita la QoS, pues se puede explotar la información de la Capa 4 para averiguar dónde hay que realizar ajustes de asignación de ancho de banda.

5.3.3.- Arquitecturas de conmutación LAN

En otro de los frentes abiertos por la conmutación LAN, IDC advierte que está comenzando la adopción de Gigabit Ethernet en entornos empresariales donde tiene lugar la consolidación de servidores. Tal y como ocurrió cuando se introdujo la velocidad de 100 Mbits/s., o Fast Ethernet, se prevé que el despliegue inicial de Gigabit Ethernet sea principalmente para conexiones de conmutador a conmutador y de servidor a conmutador. De forma simultánea a la adopción de Gigabit Ethernet, los conmutadores LAN llegarán a ser predominantes en la estructura troncal de las redes. Estos dispositivos serán capaces de conmutar varias conexiones Fast Ethernet y se podrán conectar a diversos enlaces ascendentes Gigabit, con lo que dotarán de mayor flexibilidad y rendimiento a la red. Los conmutadores de Capa 2 se desplegarán en la periferia de la infraestructura LAN.

A medida que Gigabit Ethernet se extienda más allá de la red troncal, las previsiones apuntan a que se introducirá primero a aquellos usuarios cuyo funcionamiento es crítico, mientras que el resto de la base de usuarios migrarán a velocidades de gigabits únicamente cuando 10 Gigabit Ethernet esté disponible de forma generalizada. Sin embargo, puede que esto no ocurra hasta dentro de varios años, pues Gigabit Ethernet proporcionará una capacidad de red más que suficiente para servir los requisitos empresariales que cabe prever. Por lo tanto, es importante no descartar aquellas actualizaciones de las redes Ethernet desplegadas que fuesen necesarias, basándose en las futuras promesas. Y la opción de Gigabit Ethernet debería proporcionar un ancho de banda más que suficiente, sin duda al menos para pequeñas empresas. El siguiente capítulo analiza con más detalle la implementación de una arquitectura de LAN conmutada.

Las empresas buscan soluciones de red escalables que impliquen unos costes estructurales de gestión no muy elevados en términos de ancho de banda, y que ofrezcan asimismo unas buenas características de seguridad y de eficacia/coste que pueda materializarse con rapidez. La evolución hacia una red tal de gran capacidad implica grandes costes y, al menos en un principio, interrupciones de funcionamiento a gran escala. Todo ello se debe a que es necesario remodelar completamente la infraestructura; concretamente, el cableado. Es importante destacar que cuando se presenta una nueva versión de Ethernet, primero se despliega en el medio físico de la fibra óptica. Por tanto, a menos que contemple entre sus planes de desarrollo la introducción de un avanzado cableado de fibra, el salto a 10 Gigabit Ethernet será aún más costoso y complejo.

La conmutación LAN avanzada ofrece una serie de ventajas a los proveedores de servicios. Entre tales ventajas, cabe destacar la obtención de mejores técnicas de balanceo de carga para gestionar granjas de servidores e infraestructuras de servidores con un alcance global. Tales organizaciones serán capaces de aplicar los conmutadores de más alto nivel para establecer prioridades de tráfico, ofrecer QoS y permitir el soporte de servicio de extremo a extremo.

5.3.4.- Implementación de una Arquitectura LAN Conmutada

La conmutación ofrece enormes ventajas a las empresas que operan con LANs Ethernet pero el diseño e implementación de la red influirá considerablemente en la consecución de lo que se promete. Todo ello ha de ir unido a una práctica completa de gestión de la red, tratada en el capítulo cuatro. En este apartado analizaremos los principios y componentes de una infraestructura LAN conmutada.

El diseño de una arquitectura LAN depende de dos principios.

- Proporcionar redes que sean rápidas y fáciles de administrar, así como altamente fiables y escalables sin que ello suponga un sacrificio del control. Esto implica el uso combinado de tecnología de conmutación altamente funcional en Capa 2, Capa 3 y Capa 4 del Modelo de Referencia OSI, además del uso de herramientas de gestión de la red. El objetivo consiste en ayudar a las organizaciones usuarias a superar los actuales retos de las redes y a preparar la infraestructura de red para las mejoras en el futuro. Ejemplos de tales ayudas son el desarrollo de una red convergente y añadir aplicaciones multimedia y multicast.
- Ofrecer el máximo nivel de servicio posible para un mínimo coste total. Esta propuesta se basa en la necesidad de reducir la complejidad al mínimo y aumentar el valor a largo plazo de la red.

Es fácil demostrar que existen cuatro necesidades fundamentales que sustentan el establecimiento de una infraestructura de LAN. Dichas necesidades son: capacidad, operación continua, control y coste de propiedad. La naturaleza de la arquitectura de la LAN conmutada ha de adaptarse a las necesidades concretas de cada empresa.

Podemos dividir la LAN Ethernet típica en tres niveles. El nivel más externo enlaza los distintos pisos y armarios de cableado, y se trata en realidad de la estructura troncal de la red. En la actualidad, este nivel se basa a menudo en Gigabit Ethernet, al igual que el centro de datos o núcleo. En el nivel intermedio están los armarios de cableado que hoy en día llevan Ethernet y Fast Ethernet a los ordenadores de sobremesa. Finalmente, en el corazón de la red está el último nivel, denominado núcleo de datos. La granja de servidores se ubica también en el corazón de la red. Una de las características fundamentales del centro de datos ha de ser la flexibilidad, basada en conmutadores alojados en un chasis, o apilados juntos.

Si trazamos las correspondencias con las cuatro necesidades fundamentales anteriormente descritas, el modelo de LAN de tres niveles muestra la necesidad de afrontar las siguientes cuestiones clave:

Capacidad:
- Armario de Cableado: precio/rendimiento y alta densidad
- Centro de Datos: flexibilidad en ancho de banda
- Red troncal: capacidad masiva

Operación continua
- Armario de Cableado: necesidad de flexibilidad
- Centro de Datos: total redundancia
- Red troncal: ultra-fiabilidad

Control
- Armario de Cableado: Una estructura sencilla y lógica. Tarjetas inteligentes de red. Soporte para aplicaciones vanzadas y prioridades de tráfico. Bajos costes estructurales de administración.
- Centro de Datos: Complejidad minimizada.Configuración más fácil. Soporte para aplicaciones vanzadas, seguridad y prioridad de tráfico. Bajos costes estructurales de administración.
- Red troncal: Estructura lógica para minimizar la complejidad. Configuración más sencilla. Soporte para aplicaciones avanzadas, seguridad y prioridad de tráfico.

Coste de Propiedad
- Armario de Cableado: Ethernet Escalable y Fast Ethernet, soporte para estándares.
- Centro de Datos: Interoperabilidad, escalabilidad flexible, soporte para estándares.
- Red troncal: Interoperabilidad, escalabilidad flexible, soporte para estándares.

El coste de propiedad es un aspecto de tal importancia para las organizaciones que conviene hacer algunas indicaciones al respecto. En primer lugar, el objetivo ha de ser la transición desde una administración compleja hasta una administración nula. El siguiente paso es otra transición, desde una disponibilidad del 90 por ciento hasta un 99,99 por ciento. Además de los objetivos relativos al coste de propiedad, la red ha de prepararse para nuevas aplicaciones de dos formas. La primera consiste en la transición desde el paradigma del almacenamiento y reenvío, asociado a las transferencias de archivos, hasta la inclusión de flujos de tráfico en tiempo real tales como voz y vídeo. La segunda es el abandono de la gestión puramente centrada en dispositivos, a favor de un enfoque integrado basado en la gestión de políticas.

5.3.5.- Aplicación de conmutadores y alta disponibilidad

Sin entrar en demasiados detalles acerca del tipo de producto y configuración, la elección de un conmutador depende de la parte de la red donde sea necesario dicho dispositivo. Un buen consejo podría ser instalar conmutadores de Capa 2 en el armario de cableado, enlazados con el centro de datos mediante conexiones flexibles. Una combinación de conmutadores de enrutamiento en Capa 2 y Capa 3, de altas prestaciones, es una buena elección para el centro de datos. Los servidores críticos para el negocio se pueden colocar tras conmutadores ultrarrápidos a velocidad de cable, en Capa 3 y Capa 4. El nivel de interconexión exige conmutadores de alta capacidad que funcionen a velocidad de cable. Los conmutadores a velocidad de cable manejan los paquetes a mayor velocidad

porque el tráfico pasa por unos circuitos integrados específicos para la aplicación (ASICs). Se trata de chips especializados que ofrecen unas velocidades de transferencia mucho mayores que los dispositivos de red basados únicamente en software, como es el caso de numerosos routers. A medida que sigue creciendo la carga que soportan las redes, junto con la demanda de ancho de banda, es necesario diferenciar el tráfico con más precisión y entregarlo con más rapidez. Esto es especialmente cierto en aquellas redes que soporten operaciones de e-commerce, pero también puede aplicarse sin duda a todas las transmisiones de carácter crítico para el negocio.

Evidentemente, una alta disponibilidad es un objetivo importante para cualquier organización que trabaje en red, y depende de tres factores: los dispositivos individuales, la tipología de la red y la planta de cable. Y cualquier estrategia de disponibilidad de tiempo tiene que incluir también la formación del personal, existencias de repuestos y soporte técnico de terceros.

Aunque una alta disponibilidad es algo claramente crucial para cualquier parte de la red, garantizar un tiempo máximo de disponibilidad en el núcleo y en la red troncal es esencial. Los fallos temporales en un armario de cableado tendrán un impacto evidente sobre los usuarios, pero si los afectados son el núcleo o la red troncal, las repercusiones alcanzarán a toda la organización. A pesar de todo, el objetivo real ha de ser una estrategia de disponibilidad de extremo a extremo que cubra la totalidad de la red. Una inversión incremental en ancho de banda adicional y en conmutadores en la periferia de la red ayudará a lograr este propósito.

La alta disponibilidad depende también de la configuración y características de los dispositivos de una red. Tanto los conmutadores modulares, basados en chasis, como las configuraciones apilables presentan ventajas en este sentido, mientras que los conmutadores individuales deberían proporcionar flexibilidad adicional. Las características de conmutación inteligente, tales como la capacidad de emprender acciones para evitar que los fallos interrumpan las operaciones y disminuyan el nivel de tráfico de la red, también deben tenerse en cuenta a la hora de escoger.

Otro aspecto clave a evaluar es la inclusión de sistemas de alimentación ininterrumpida, en caso de que se produzcan cortes de la electricidad.

5.3.6.- Redes convergentes

En lo referente a las arquitecturas de LAN, uno de los desarrollos más interesantes y de mayores exigencias es la red convergente, donde la voz, los datos e incluso el vídeo se transmiten por una misma infraestructura Ethernet. La combinación de la voz con la transferencia de archivos y el tráfico de correo electrónico, es decir, con los usos típicos de una LAN en el pasado, obliga a establecer nuevos niveles de prioridad.

Hay que dar mayores niveles de prioridad a la voz y al vídeo, sin que apenas exista latencia o factor de redundancia. Después de todo, si se pierde o retrasa la entrega de incluso unos pocos paquetes de una comunicación de voz o de vídeo, el resultado es inaceptable. El simple recurso de dotar a la LAN con mayores niveles de ancho de banda y añadir conmutadores adicionales es únicamente un primer paso. Por ello, el siguiente capítulo analiza la cuestión fundamental de gestionar la red para obtener niveles de servicio mayores y sostenidos, así como de ayudar a garantizar que se logre la rentabilidad de la inversión.

El tráfico multimedia por la LAN es ya una cuestión clave que atañe a todas las organizaciones, y estará cada vez más relacionado con actividades de importancia crítica para el negocio de la empresa. Por ejemplo, el tráfico de voz que llega a un centro de atención al cliente y el tráfico relativo a e-business han de recibir prioridad sobre la navegación informal por la Web o cualquier otro uso de carácter no crítico de la red. Las redes convergentes son el objeto de una guía anterior de esta colección, denominada Soluciones de Telefonía en Red.

5.4.- LAN virtual (VLAN)

Las LAN virtuales (VLANs) se han convertido últimamente en un aspecto integral de las soluciones para las redes conmutadas, si bien el interés de los usuarios por ellas es todavía incipiente.

El rápido abaratamiento del coste por puerto de los conmutadores Ethernet, sobre todo, y Token Ring ha acelerado el proceso de creación de arquitecturas LAN completamente conmutadas, sustituyendo por conmutadores, no sólo de los routers locales y departamentales sino incluso de los hubs. Esta arquitectura resulta ideal para la implementación de VLAN, y es uno de los motivos de que el interés por esta solución vaya en aumento.

Los conmutadores dividen la red en segmentos más pequeños permitiendo un aumento del ancho de banda por segmento. Los routers, se especializaban en la contención de los broadcast, dividiendo las redes en dominios de broadcast, que a su vez se podían dividir en múltiples segmentos conmutados (diferentes dominios de colisión). Incialmente los segmentos podían contener 500 o más usuarios, pero progresivamente, al dividir la red en más y más segmentos el número de usuarios en cada uno se puede reducir incluso hasta una estación por segmento y anulando así los efectos de la colisión. Sin embargo, este proceso no reduce la necesidad de contener los mensajes de broadcast en un rango, que habitualmente, con el uso de routers es de 100 a 500 usuarios.

Las VLAN representan una solución alternativa a los routers para lo contención del broadcast, dado que las VLAN permiten a los conmutadores contener también el tráfico de broadcast. Con la instalación de conmutadores en conjunción con VLAN, cada segmento de red puede contener tan sólo un suaurio mientras que los dominios de broadcast pueden ser de hasta 1,000 o quizás incluso más. Además, si la implementación es adecuada, las VLAN pueden identificar los movimientos de un dispositivo a una nueva ubicación sin requerir una reconfiguración manual de la dirección IP.

Una VLAN es un grupo de dispositivos que funcionan como un solo segmento LAN (dominio de (broadcast). Estos dispositivos pueden encontrarse en segmentos físicos diferentes, e incluso en ubicaciones distantes, pese a lo cual se comunican como si pertenecieran al mismo. La creación de VLAN permite a usuarios situados en áreas distintas o conectados a puertos distintos pertener a una misma VLAN; los usuarios que han sido asignados a este grupo podrán enviar y recibir tráfico broadcast y multicast como si estuvieran todos conectados a un segmento común. Los conmutadores VLAN (VLAN aware switches) aislan el tráfico broadcast, multicast y de destino desconocido que reciben de los grupos VLAN, de modo que el tráfico de las estaciones de una VLAN queda confinado a ésta.

5.4.1.- Taxonomía de las VLAN

Dado que existen varios modos para definir la pertenencia a una VLAN, podemos dividir las VLAN en varios tipos generales:

- Asignación por puerto
- Asignación por dirección MAC
- Asignación por dirección de red (IP)
- Asignación por dirección multicast IP.
- Asignación por protocolo de nivel 4 o superior.

Asignación por puerto

La mayoría de las iplementacioens iniciales de VLAN definían la pertenencia mediante grupos de puertos (por ejemplo, los puertos 1, 2, 3, 7 y 8 de un conmutador constituían la VLAN A, mientras que los puertos 4, 5 y 6 constituían la VLAN B). Además, la mayorían de los conmutadores antiguos sólo soportaban la configuración de una VLAN sobre un solo conmutador.

La segunda generación de implementaciones soportaban VLANs que se expandían a múltiples conmutadores (por ejemplo, puertos 1 y 2 del conmutador #1 y puertos 4, 5, 6 y 7 del conmutador #2 constituían la VLAN A; mientras que los puertos 3, 4, 5, 6, 7 y 8 del conmutador #1 combinados con los puertos 1, 2, 3 y 8 del conmutador #2 constituyen la VLAN B). Esta situación se recoge en la Figura 5.11.

La agrupación de puertos es todavía el método más común para la definición de pertenencia a una VLAN, y la configruación resulta muy sencilla. Sin embargo, la definición de VLANs sólo por puerto no permite que varias VLANs incluyan el mismo segmento físico (o puerto de conmutador). Sin embargo, la principal limitación de la definición de VLANs por puerto es que el gestor de la red debe reconfigurar la VLAN cada vez que un usuario cambia de ubicación.

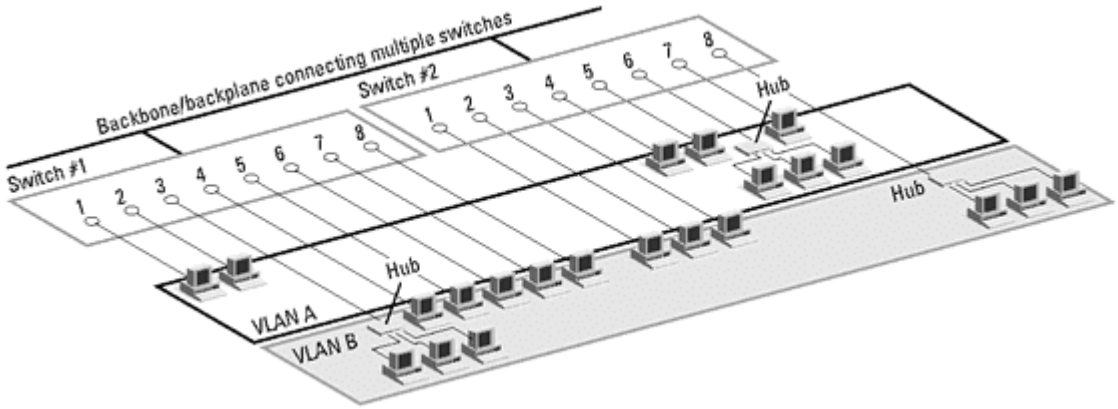

Figura 5.11 VLANs definidas por grupos de puertos

Asignación por dirección MAC

La definición de VLANs basándose en la dirección de nivel MAC presenta ventajas y desventajas. Dado que las direcciones MAC son asignadas en fábrica a las tarjetas interfaz de red (NIC) de las estaciones, estas VLANs permiten a los gestores de red mover las estaciones a ubicaciones diferentes, manteniendo éstos su pertenencia a una VLAN; por lo tanto, es posible pensar que la VLAN está definida en base a usuarios. Una de las desventajas de esta definición de VLANs es que todos los usuarios deben ser configurados en al menos una VLAN. Esto constituye un inconveniente importante en redes con miles de usuarios, a los que hay que asignar explícitamente a una VLAN, sin embargo, algunos fabricantes han mitigado esta tarea de configuración inicial mediente el uso de herramientas que crean VLANs basadas en el estado actual de la red, es decir, se crea una VLAN basada en dirección MAC para cada subred.

Las VLANs basadas en direcciones MAC que son implementadas en medios compartidos pueden experimentar graves problemas de degradación de rendimiento puesto que miembros de diferentes VLAN pueden coexistir sobre un mismo puerto. Además, el método de comunicar la información de pertenencia a una VLAN entre conmutadores también origina una degradación del rendimiento en implementaciones a gran escala.

Otra desventaja, aunque menor, de estas VLANs se origina en entornos que utilizan un número importante de ordenadores portátiles. El problema es que la "docking station" y el adaptador de red generalmente permancen fijos, mientras que el portátil se mueve por la red. Cuando el usuario se conecta desde una nueva ubicación, la pertenencia a la VLAN cambia, puesto que la dirección MAC no está asociada con el portátil, resultando imposible seguir la pista a la mismal, siendo necesario una configuración manual cada vez.

Asignación por información de la Capa 3

Las VLANs basadas en información de la Capa 3 tienen en cuenta el tipo de protocolo (si se soportan múltiples protocolos) o la dirección de la capa de red (por ejemplo direcciones de subre en redes TCP/IP) para determinar la pertenencia a una VLAN. Aunque estas VLANs se basan en información el nivel 2, esto no constituye una función de encaminamiento y no debería confundirse con el encaminamiento del nivel de red.

Incluso aunque el conmutador inspecciona la dirección IP para determinar la pertenencia a una VLAN, no se realiza ningún cálculo de ruta ni se emplean protocolos como RIP u OSPF, y las tramas que atraviesan el conmutador se encamian de acuerdo con la implementación del algoritmo Spanning Tree. Por lo tnato, desde el punto de vista de un conmutador que utiliza VLANs de nivel 3, la conectividad entre cualqueir VLAN dada es vista como una topología plana conmutada.

Se han hecho distinciones entre VLANs basadas en información de nivel 3 y encaminamiento, debería tenerse en cuenta que algunos vendedores están incorporando funciones de nivel 3 en sus conmutadores, habilitando funciones asociadas normalmente con el encaminamiento. Además, los conmutadores "layer 3 aware" o "multi-capa" tienen a menudo funciones de encaminamiento de paquetes incorporadas en su chip sets ASIC chip sets, mejorando notoriamente el rendimiento de los routers basados en CPU. Sin embargo, hay un punto clave que se mantiene: no importa donde esté situada un solución VLAN, el encaminamiento es necesario para proporcionar conectividad entre diferentes VLANs.

Son varias las ventajas de definir las VLANs en la capa 3. En primer lugar, permite realizar particiones por tipo de protocolo, lo que puede resultar atractivo a gestores de red con una estrategia VLAN basada en servicio o aplicación. En segundo lugar, los usuarios pueden moverse físicamente sin tener que reconfigurar cada dirección de la estación de trabajo. En terecer lugar, VLANs en la Capa 3 puede eliminar la necesidad de etiquetado de tramas para comunicar la pertenencia a un VLAN entre conmutadores, reduciendo, por lo tanto la sobrecarga en cada trama.

Una de las desventajas de definir VLANs en la capa 3 puede ser el rendimiento, dado que es preciso más tiempo para inspeccionar las direcciones de la capa 3 que las direcciones MAC. Por esta razón, los conmutadores que utilizan información de la capa 3 son generalmente algo más lentos que aquellos que sólo hacen uso de la información de la capa 2, aunque esto no resulta cierto en las implementaciones de todos los fabricantes.

Las VLAN definidas en la capa 3 son especialmente efectivas con TCP/IP, y algo menos con protocolos como IPX, DECnet, or AppleTalk, uqe no precisan configuración manual de las estaciones. Además, las VLANs definidas en la capa 3 tienen una dificultad particular en relación con protocolos no rutables como NetBIOS, ya que las estaciones que ejecutan estos protocolos no pueden ser diferenciadas y por o tnato no pueden ser definidas como parte de una VLAN de este tipo.

Asignación por Grupos Multicast IP

Los grupos multicast IP representan un enfoque diferente en la definición de VLAN, aunque el concepto fundamental de VLANs y dominios de difusión son aplicables. Cada estación de trabajo puede unirse a un grupo multicast respondiendo afirmativamente a una notificación broadcast que envía periódicamente un router conectado a su red señalando la existencia de dicho grupo. Todas las estaciones que se unen al grupo multicast IP pueden considerearse miembros de la misma LAN virtual. Sin embargo, sólo son miembros de este grupo durante un periodo de tiempo; esta naturalez dinámica de las VLANs definida de este modo permite un gran nivel de flexibilidad y sensibilidad a las aplicaciones. Además estas VLANs definidas por grupos multicast IP podrían expandierse inherentemente mediante routers y por lo tanto mediante conexiones WAN.

Asignación por información de la Capa 4 y superiores

En este caso las VLANs se definen basándose en aplicaciones, servicios o combinaciones de estas.
Puede utilizarse el tipo de protocolo de transporte o bien campos de la cabecera de transporte para realizar la definición de la pertenencia a un grupo (TCP o UDP, puertos de origen destino, ...). Esta definición permite al gestor de red dividir la red atendiendo específicamente a la aplicación o servicio, independientemente del usuario (estación final), proporcionando, por ejemplo servicios prioritarios a determinados servicios independientemente del usuario que haga uso de él. Desplazamientos sin reconfiguraciones. El inconveniente más importante de este tipo de VLAN es que la inspección de la cabecera para determinar la VLAN a la que pertenece un paquete es la más lenta de todas.

Combinación de definiciones de VLAN

Debido al compromiso entre varios tipos de VLANs, muchos fabricantes incluyen múltiples métodos para definir VLANs, lo que permite a los gestores de red a configurar su VLAN para ajustarse lo mejor posible a su entorno de red. Por ejemplo, utilizando una combinación de métodos, una organización que utiliza IP y NETBIOS podría definir VLANs IP correspondiéndose a las subredes IP preexistentes (lo que le permitiría una migración suave), y definir después VLANs para las estaciones NetBIOS dividiéndolas por grupos de direcciones MAC.

5.4.2.- Automatización de la configuración VLAN

Otro aspecto central en el despliegue de una VLAN es el grado de automatización en su configuración, lo que está relacionado, hasta cierto punto, con el modo en que se definen las VLANs, pero sobre todo con la solución específica del fabricante. Hay tres niveles primarios de automatización en la configuración de una VLAN:
Manual. Con la configuración puramente manual, tanto la configuración inicial como los movimientos y cambios posteriores son controlados por el administrador de la red. Desde luego, este tipo de configuración permien un elevado nivel de control pero, sin embargo, en redes grandes, resulta inmanejable. Además elimina uno de los principales beneficios de las VLANs: eliminar el tiempo que le lleva al administrador los cambios y movimientos en la topología de la red.
Semiautomatizada. Esta configuración se refiere a la opción de automatizar, bien la configuración inicial o las reconfigurations siguientes (movimientos/cambios), o ambas. La automatización de la configuración inicial se consigue con un conjunto de herramientas que mapean las VLANs a las subredes existentes o algún otro criterio. Esta configuración también podría referirse a situaciones donde las VLANs son configuradas inicalmente de manera manual, y donde los movimientos posteriores se siguen automáticamente. La combianación de ambas técnicas sigue resultando semi-automatizada porque el gestor siempre tiene la opción de la configuración manual.
Completamente automatizada. La configuración automática de las VLAN supone que las estaciones se unen dinámicamente a las VLANs dependiendo de su aplicación, identificador de usuario, o algún otro criterio o política predefinida por el administrador.

5.4.3.- Comunicación de la información de pertenencia a una VLAN

Los conmutadores deben disponer de un modo para saber a qué VLAN pertenece el tráfico procedente de otros conmutadores, ya que de otro modo las VLANs quedarían limitadas al ámbito de un solo conmutador. En general, las VLANs de nivel 2 deben comunicar la pertenencia explícitamente, mientras que en el resto la pertenencia se comunica implícitamente en la dirección IP, el protocolo de transporte, la aplicación, ... En la actualidad se han implementado tres métodos para comunicación entre conmutadores de información de la VLAN: Mantenimiento de tablas mediante señalización, etiquetado de tramas y multiplexación por división del tiempo (TDM).

Mantenimiento de tablas mediante señalización

Cuando una estación difunde su primera trama, el conmutador resuelve la dirección MAC o el puerto de entrada con su pertenencia a la VLAN y la guarda en su memoria caché en tablas de direcciones.
Esta información es difundida constantamente a todos los demás conmutadores. A medida que la pertenencia a las VLAN cambia, estas tablas se actualizan manualmente por un administrador del sistema en la consola de gestión, A medida que la red se expande y se añaden más conmutadores, la señalización constante necesaria para actualizar las tablas de direcciones de cada conmutador puede originar una congestión en la red troncal. Por ello el método no resulta escalable.

Etiquetado de Tramas.

Se inserta una cabecera en cada trama en los tramos entre switches para identificar unívocamente a qué VLAN pertenece una determinada trama de nivel MAC. La solución de distintos fabricantes puede

diferir en el modo en que resuelven el problema de exceder ocasionalmente la longitud máxima de las tramas MAC cuando se insertan estas etiquetas. Estas cabeceras también sobrecargan el tráfico de la red.

TDM

El último método y menos utilizado es multiplexar en el tiempo, reservando canales para cada VLAN. Con este método se eliminan los problemas de sobrecarga inherentes a la señalización y etiquetado, pero también desperdicia ancho de banda debido a que los slots no utilizados por una VLAN no pueden ser aprovechados por otra.

5.4.4.- Estándares relacionados con VLANs

Dada la variedad de tipo de definiciones de VLAN y la variedad de modos en que los conmutadores se comunican la información relacionada con las VLAN, no resulta sorprendente que cada fabricante desarrollase su solución propietaria. El hecho es que la interoperabilidad entre soluciones VLAN no resulta completa en muchos casos. Como en otros ámbitos de las LAN, existe un estándar del comité 802 referido a las VLAN.

En 1995, Cisco Systems propuso el uso de IEEE 802.10, que se estableció originalmente para regular la seguridad de las LAN. Cisco intentó parovechar el formato de la cabecera de trama optional de 802.10 y reutilizarlo para el etiquetado de tramas VLAN en lugar de para transportar información de seguridad. Aunque esto resulte técnicamente posible, la mayoría de los miembros del comité 802 se opusieron al uso de un estandar para dos propósitos diferentes. Además , esta solución estaría basada en campos de tamaño variable, lo que haría más difícil la implementación de procesado de tramas basado en ASIC y por lo tanto más lenta y más cara.

En marzo de 1996, el Subcomité de Internetworking IEEE 802.1 completó la fase inicial de la investigación para el desarrollo de un estándar VLAN, y pasó las resoluciones concernientes a tres asuntos: el enfoque arquitectónico de las VLANs; un formato estándar para el etiquetado de tramas y la comunicación de pertenencia a VLAN entre xdispositivos multivendor, y una dirección futura para la estandarización de VLAN. El formato estandarizado para el etiquetado de tramas, conocido como 802.1Q, representa el hito principal en el desarrollo de las VLAN para ser implementadas entre equipos multivendor y la clave para el desarrollo que están experimentando las VLAN.

802.1Q define sólo VLAN de nivel 1 y de nivel 2 basadas en tipo de protocolo, el resto son soluciones propietarias.

El marco definido por 802.1Q para las VLAN se basa en un modelo a tres capas:

- Configuración
- Distribución de la información de configuración
- Conmutación

La configuración está relacionada con el modo en que se especifica por vez primera la configuración de una VLAN y la asignación de parámetros; la distribución está relacionada con el proceso de intercambio de información necesaria para saber a qué VLAN asignar cada trama recibida. Finalmente la conmutación está relacionada con los mecanismos de clasificación del trafico recibido según la VLAN a la que pertenecen, las decisiones acerca del encaminamiento o no del mismo, la elección del puerto (y formato) de salida y los procedimientos para añadir, modificar o retirar etiquetas de la cabecera de la trama.

5.4.5.- 802.1Q

Tramas

En el estándar se recoge la existencia de tres tipos de tramas:

- Tramas no etiquetadas
- Tramas etiquetadas con prioridad
- Tramas etiquetadas con VLAN

Las dos primeras no incluyen información de la VLAN a la que pertenece, por lo que su clasificación debe realizarse baándose en parámetros asociados al puerto por el que se recibió o extensiones propietarias (pe basándose en el contenido de la trama). Las últimas transportan una identificación explícita de la VLAN a la que pertenecen basándose en el VID incluido en la etiqueta de su cabecera que es insertado allí por un conmutador “VLAN aware” (el que es capaz de insertar y retirar etiquetas de la cabecera de una trama).

Formato de la etiqueta

La etiqueta de la cabecera contiene los siguientes componentes:

- Identificador del protocolo de etiqueta (TPID). Es un campo de dos octetos que contiene el valor Tipo Ethernet (81-00) que identifica la trama como etiquetada.
- Información de Control de la etiqueta (TCI). Es un campo de dos octetos que contiene la prioridad del usuario y los campos Identificador de Formato Canónico (CFI) e Identificador de VLAN (VID). La prioridad de usuario es un campo de tres bits interpretado como un número binario representando los niveles 0 a 7. El campo CFI es un solo bit que indica que todas la información de direcciones MAC que puede aparecer en el campo de datos está en formato canónico. Finalmente, el campo VID de doce bits identifica unívocamente la VLAN a la que pertenece la trama, estando serservados los valores 0 (la trama sólo contiene información de prioridad pero no de pertenencia a VLAN), 1 (valor del PVID por defecto cuando se usa clasificación por puerto) y FFF (reservado).
- El formato RIF embebido (E-RIF), cuando es requerido por el estado del campo CFI. Contiene un campo de control de ruta (RC) de dos octetos y una serie de descriptores de rutas de 0 o más octetos.

Operación

La operación de un conmutador 802.1Q tiene tres componentes principales:

- Conmutación y filtrado de tramas
- Mantenimiento de la información necesaria para las operaciones de conmutación y filtrado
- Gestión de lo anterior.

El conmutador conmuta tramas MAC entre segmentos conectados a sus puertos preservando el orden de recepción de las mismas. Las funciones que soporta esta conmutación deben ser:

- Recepción de tramas
- Descarte de las tramas recibidas con errores, aquellas cuyo tipo no sea datos de usuario, o aquellas cuyo tamaño exceda la MTU.
- Descarte de las tramas de acuerdo con la información de filtrado
- Selección de la clase de tráfico de acuerdo con la información de filtrado
- Encolado de las tramas de acuerdo con la clase de tráfico
- Descarte de tramas para asegurar que no se excede de un tiempo máximo de tránsito
- Selección de tramas encoladas para su transmisión
- Encaminamiento de tramas a otros puertos del conmutador

El conmutador filtra las tramas recibidas, es decir no encamina todas ellas hacia otros puertos. Las funciones que soporta el uso y mantenimiento de la información con este propósito es.

- Calculo y configuración de la topología LAN conmutada
- Configuración permanente de direcciones reservadas
- Configuración explícita de información de filtrado estático
- Aprendizaje automático de la información del filtrado dinámico para direcciones unicast a través de la observación de la dirección de origen de las tramas recibidas.
- Mantenimiento de la edad de la información de filtrado dinámica aprendida.
- Adición y eliminación automática de información de filtrado como consecuencia de los intercambios GMRP.

También clasifica las tramas en clases de tráfico para transmitir en primer lugar las tramas generadas por servicios sensibles al tiempo. La función que soporta el uso y mantenimiento de la información con este propósito es:

- Configuración explítica de información de clase de tráfico asociada con los puertos del conmutador.

El conmutador utiliza una serie de *reglas de ingreso* para clasificar las tramas de acuerdo con la VLAN a la que pertenecen, pueden filtrar tramas basándose en la ausencia de VID en la trama recibida, evitando la inyección de tramas no etiquetadas o etiquetadas con prioridad en un puerto en el que dichas tramas estén desabilitadas y pueden filtrar tramas basándose en el identificador de VLAN.

Para evitar la inyección de tramas no etiquetadas o etiquetadas con prioridad en un puerto en el que dichas tramas estén desabilitadas es posible configurar en cada puerto del conmutador el parámetro Tipo de Trama Aceptable, indicando si se admiten todo tipo de tramas o sólo tramas con etiqueta de VLAN (VID).

En una clasificación VLAN puerto, el VID asociado a cada trama no etiquetada, y en caso de ser admitidas éstas, se determina en función del puerto de recepción de la misma. El mecanismo precisa la asociación de un ID de VLAN, en este caso PVID (Port VLAN Identifier) con cada puerto del conmutador. El PVID de un puerto proporciona el VID a las tramas no etiquetadas que se reciben por el mismo.

El conmutador también puede filtrar tramas para evitar la inyección de tráfico para una VLAN en un puerto en el que dicha VLAN está deshabilitada, para lo cual puede configurarse asociado a cada puerto del conmutador el parámetro de Habilitación del Filtrado de Ingreso, que agregará a las reglas de ingreso la comprobación de que la pertenencia del puerto de la VLAN de la trama de entrada, descartando ésta en caso contrario.

Todas las tramas que no son descartadas como resultado de aplicar las reglas de ingreso pasan al proceso de envío y aprendizaje.

El proceso de envío filtra las tramas én base a la información contenida en la Base de Datos de Filtrado y el el estado de los puertos del conmutador (el puerto de salida está en modo envío, no coincide en el puerto de entrada y el tamaño de la trama no excede de la MTU). Las decisiones del filtrado se toman en base a la dirección MAC de destino de la trama, el VID asociado a la trama recibida y la información contenida en la Base de Datos de Filtrado para dicha dirección MAC y VID. Este proceso proporciona espacio de almacenamiento para las tramas en espera de ser transmitidas, preservando el orden de recepción para las tramas unicast con una prioridad de usuario para una combinación de direcciones de origen/destino. Se puede disponer de más de una cola por puerto, a las que las tramas se asignan en función de la prioridad de usuario que se utiliza para clasificar el tráfico. En los puertos que no soporten diferentes clases de tráfico, se asignará a todas las tramas la clase 0. Es posible que las tramas se eliminen de la cola sin ser transmitidas en el caso de que se exceda el tiempo de permanencia fijado para la misma o que el retraso de tránsito en el conmutador fijado para cada trama fuera a ser superado en el momento de transmisión de la misma.

Las reglas de egresado determinan, para una VLAN a través de qué puertos pueden transmitirse las tramas (se pueden filtrar tramas cuando el VID corresponde a una VLAN cuyo tráfico no debe aparecer por un puerto) y en qué formato.

El proceso de aprendizaje que permite, por la observación de las direcciones de origen y los VIDs de las tramas clasificadas por las reglas de ingreso, actualizar la Base de Datos de Filtrado, condicionadamente al estado de los puertos. Este proceso puede deducir el puerto a través del cual pueden alcanzarse ciertas estaciones inspeccionando la dirección MAC de origen y el VID.

La Base de Datos de Filtrado contiene la información y soporta preguntas del proceso de encaminamiento sobre si debe encaminarse o no una trama con una dirección MAC y un VID. Mediante esta BD, el conmutador puede filtrar tramas para confinar el tráfico de una determinada VLAN en segmentos LAN que forman un camino desde el emisor del tráfico hasta los miembros de la VLAN. La información de la Base de Datos de Filtrado puede ser estática y dinámica (aprendida en la operación normal del conmutador).

La información estática puede ser de dos tipos: *entradas de filtrado estático* y *entradas de registro estático de VLANs*. Las primeras contienen información para direcciones MAC individuales y de grupo, permitiendo el control del envío de tramas a direcciones MAC particulares. Las segundas contienen toda la información estática relacionada con las VLANs, permitiendo controlar el envío de tramas para VID particulares y la inclusión o eliminación de las etiquetas en las cabeceras de las tramas.

La información dinámica está contenida en tres tipos de entradas. Las *entradas de filtrado dinámicas* se utilizan para especificar los puertos por los que se han aprendido determinadas direcciones MAC. Son creadas y actualizadas en el proceso de aprendizaje y pueden ser eliminadas de la BD cuando ha pasado determinado tiempo desde su inclusión en la misma. Las *entradas de registro de grupo* son creadas, actualizadas y eliminadas por el protocolo GMRP. Las entradas de registro dinámico de VLAN se utilizan para especificar los puertos por los cuales se ha registrado la pertenencia a una VLAN y son creados, mantenidos y eliminados por el protocolo GVRP.

5.4.6.- Beneficios de la implementación de VLAN

Reducción del coste de los movimientos y cambios

Es la razón más frecuente de la implementación de una VLAN en redes IP. Normalmente, cuando un usuario se mueve a una subred IP diferente, la dirección debe ser actualizada en la estación manualmente. Las VLANs eliminan esta tarea porque la pertenencia a una VLAN no está sujeta a la ubicación de una estación en la red, permitiendo a la estación desplazada retener su dirección IP original y la pertenencia a su subred.

Es una realidad que el fenómeno de las redes progresivamente más dinámicas requieren un trabajo cada vez mayor de los departamentos de IS. Sin embargo, no todas las implementacioens de VLAN reducirán estos costos. Las VLANs añaden otra capa de conectividad virtual que debe ser gestionada junto con la conectividad física. Es por ello que las organizaciones deben ser cuidadosas en la implantación de VLANs con el fin de no generar más trabajo de administración de la que por otro lado ahorra.

Grupos de trabajo virtuales

Uno de los objetivos más ambiciosos de las VLAN es el establecimiento de un modelo de grupos de trabajo virtuales. El concepto consiste en que una implementación global de VLAN en toda la red, los miembros del mismo departameno puede parecer que comparten la misma LAN, mantenendo la mayor parte del tráfico dentro del mismo dominio de broadcast VLAN. Un usuario podría desplazarse a una nueva ubicación física del mismo departamento sin ninguna reconfiguración. A la inversa, un usuario no necesitaría cambiar su ubicación física cuando cambia de departamento, sería sufuciente que el administrador de la red cambiara la VLAN a la que pertenece.

Desde la perspectiva de la gestión de la red, la naturaleza transitoria de los grupos de trabajo virtuales puede crecer hasta el punto de que la actualización de la configuración de las VLANs se convierta en un trabajo tan costoso como el mantenimiento de las tablas de encaminamiento de los routers.

El soporte de las VLAN se ajusta a la “regla 80/20", que supone que el 80% del tráfico es local al grupo de trabajo mientras que el 20% es remoto o externo al grupo. En teoría, configurando adecuadamente las VLANs para ajustarse a los grupos de trabajo, sólo el 20% del tráfico que es no local tendrá la necesidad de atravesar un router para salir del grupo, mejorando el rendimiento para el 80% del tráfico que se interior al grupo. Sin embargo, muchos creen que la aplicabilidad de la regla 80/20 no se cumple debido al despliegue de servidores y aplicaciones de red tales como el e-mail o Lotus Notes ® que utlizan los usuarios de la organización en base de igualdad.

Acceso a recursos locales de la red

El concepto de grupo virtual puede fallar con problemas tan simples como que los usuarios deben estar a veces próximos a ciertos recursos, tales como las impresoras. Cuando usuarios de un grupo comparten un dispositivo, por ejemplo la impresora, asignado a una VLAN diferente, pero físicamente próxima a ellos, su tráfico tendrá que alcanzar un router para pasar a la VLAN en que se encuentra la impresora. Este problema puede solucionarse haciendo a la impresora miembro de ambas VLANs, lo que requeriría que fuera posible solapar las VLANs.

Granjas de Servidores Centralizadas

Las granjas de servidores son servidores departamentales agrupados en un centro de datos, en el que puede proporcionarseles un backup consolidado, alimentación ininterrumpida y un entorno operativo apropiado. Este concepto genera problemas al modelo de grupos virtuales cuando las soluciones del fabricante no proporcionan la posibilidad de que un servidor pertenezca a más de una VLAN simultáneamente. Si no fuera posible el solapado de VLANs, el tráfico entre un servidor centralizado y los clientes que no pertenecen a la VLAN del servidor debe atravesar un router. Sin embargo, si el conmutador incorpora la función de encaminamiento y es capaz de encaminar paquetes entre VLAN a la velocidad del cable, no hay ventajas de rendimiento en el solape de VLAN sobre el encaminamiento entre VLANs para permitir el acceso universal a un servidor centralizado. Algunos fabricantes soportan el encaminamiento integrado en los conmutadores como alternativa al solapado de VLANs.

Reducción del encaminamiento para la contención del broadcast

Incluso los fabricantes más especializados en los routers han adoptado la filosofía de “conmuta cuando puedas y encamina cuando debas”. Aunque los conmutadores proporcionan una mejora sustancial de rendimiento sobre el encaminamiento de paquetes de nivel 3, los conmutadores no filtran normalmente el tráfico broadcast; en general, lo replican por todos sus puertos. Esto no sólo origina en las grandes redes LAN conmutadas que se inunden con mensajes de broadcast, sino que desperdicia ancho de banda de las WAN. Como resultado, los usuarios han forzado tradicionalmente la partición de sus redes con routers que actúan como contenedores de broadcast; en este caso, los conmutadores ismples no permiten a los usuarios desacerse de los routers.

Uno de los principales beneficios e las VLANs es que los conmutadores LAN que las soportan pueden ser utilizados para contener el tráfico broadcast reduciendo la necesidad de routers. El tráfico broadcast entre servidores y estaciones en una VLAN particular se replica sólo en aquellos puertos donde hay conectadas estaciones que pertenecen a dicha VLAN, creando de hecho el mismo tipo de contención a broadcast que proporcionan los router. Sólo los paquetes que son destinados a direcciones que no pertenecen a la VLAN necesitan utilizar un router para ser encaminados. Hay múltiples razones par utilizar las VLANs en la reducción de la necesidad de routers en la red:

Mayor rendimiento y menor latencia. A medida que se expande la red se necesitan más routers para dividirla en dominios de broadcast. A medida que aumenta el número de routers la latencia comienza a degradar el rendimiento de la red. Un elevado grado de latencia en la red es un problema, sobre todo para aplicaciones poco elásticas como el vídeo interactivo y aplicaciones multimedia. Los conmutadores pueden proporcionar la misma división de la red pero haciéndolo con latencias muy inferiores de las que originan los routers. Además, el rendimiento medido en paquetes encaminados por segundo de los conmutadores es de un orden superior al de los routers.

Sencillez de administración. Los routers precisan una configuración mucho más compleja que los conmutadores. La reducción del número de routers de la red ahorra tiempo en la gestión de la misma.

Coste. Los puertos de un router son más caros que los de un conmutador.

Encaminamiento entre VLANs.

Los conmutadores con soporte VLAN pueden utilizarse para establecer dominios de broadcast dentro de la red al modo en que lo hacen los routers, pero no pueden encaminar tráfico de una VLAN a otra. Los routers siguen siendo necesarios para encaminar el tráfico entre-VLAN. Un diseño óptimo de las VLANs de la red debe evitar en la medida de lo posible que haya tráfico atravesando routers, lo que reducirá la posibilidad de que éstos actúen como cuellos de botella de la red. Como resultado, el corolario “conmuta cuando puedas y encamina cuando debas” en un entorno VLAN se convierte en “el encaminamiento sólo es necesario para conectar VLANs”.

Conviene tener en cuenta, sin embargo, que en algunos casos el encaminamiento no será un cuello de botella puesto que dicha función está embebida en el conmutador troncal, permitiendo encaminamiento entre VLANs a alta velocidad.

VLANs sobre una WAN. Teóricamente las VLANs pueden extenderse a través de una VLAN, aunque no sea recomendable puesto que el tráfico broadcast de una LAN consumiría el ancho de banda de la WAN; sería más recomendable en este caso utilizar routers que confinan este tráfico. Sin embargo, ei el ancho de banda de la WAN es gratis (por ejemplo un empresa con fibra oscura ya desplegada), puede considerarse la opción de extender las VLANs.

Seguridad

La posibilidad de crear cortafuegos en las VLANs puede satisfacer unos requisitos de seguridad estrictos y reemplazar una gran parte de la funcionalidad de los routers en esta área. Esto es una realidad cuando las VLANs se implementa en una red completamente conmutada. El único tráfico broadcast presente en un segmento sería el generado o dirigido a un usuario, que de este modo no podría “escuchar” tráfico dirigido a otros usuarios.

VLANs y DHCP: soluciones solapadas

El protocolo DHCP (Dynamic Host Configuration Protocol), proporciona a los usuarios otra alternativa para la reducción del trabajo de administración de las direcciones IP de las estaciones. Desafortunadamente, DHCP puede entrar en conflicto con implementaciones VLAN, especialmetne cuando la definición de éstas se basa en direcciones IP.

En lugar de establecer dominios de broadcast independientes de la localización como se hace en las VLAN, DHCP asigna direcciones IP dinámicamente a las estaciones durante un período de tiempo. Cuando el servidor DHCP detecta una estación cuya dirección física no corresponde a su dirección IP asignada, simplemente le asigna una nueva dirección. De este modo DHCP permite move las estaciones de un subred a otra sin que el administrador deba configurar la dirección IP de la misma.

El elemento de DHCP que aproxima su funcionalidad a la de las VLAN es que el aministrador de red puede especificar un rango de direcciones IP disponibles para un determinado grupo de trabajo lógico.

Dado que DHCP es una solución puramente IP, no tiene utilidad en redes donde este protocolo no sea mayoritario, escenario en el que resulta más beneficioasa una solución VLAN. Sin embargo, en entornos pequeños (menos de 500 nodos) puramente TCP/IP DHCP puede ser una solución eficiente, e incluso en redes mayores, pero donde la necesidad de crear grupos lógicos independientes de la ubicación no sea importante, las VLANs pierden gran parte de su atractivo.

Sin embargo, hay un área en el que VLANs y DHCP no conmpiten: la reducción de la necesidad de routers en la red. Los servidores DHCP carecen de funcionalidad de encaminamiento y por lo tanto no pueden crear dominios de broadcast; por lo tanto allí donde este aspecto sea relevante las VLANs constituirán una solución mejor.

La coexistencia de DHCP y de VLANs de nivel 3 basadas en dirección IP es problemática. Cuando un usuario se desplace físicamente a una nueva subred, el servidor DHCP le asignará una nueva dirección IP; el administrador de la red debería actualizar las tablas VLAN del conmutador con esta nueva dirección, lo que eliminaría la ventaja de la utilización de VLAN. Por ello estas soluciones son excluyentes en la mayoría de los entornos de red.

Sin embargo, la implementación de VLANs definidas por dirección MAC junto con DHCP es una solución posible, aunque crearía una matriz redundante de grupos lógicos dificultando igualmente la tarea de administración.

Las VLANs basadas en puertos y DHCP pueden coexistir e incluso ser complementarios. Cuando un usuario se mueve de un puerto a otro cambia la pertenencia a una VLAN, DHCP, por otro lado reconfiguraría automáticamente su dirección IP sin intervención del administrador. Además, la VLAN proporcionará contención del tráfico broadcast, que se sumará a la automatización de cambios y movimientos.