MODELO OSI CAPA 2

1 OBJETIVO

En la clase de hoy veremos cuales son los límites impuestos por la capa 1 del modelo OSI y como los soluciona la capa 2. Las soluciones que aporta esta capa son muchas y variadas, estas van desde la identificación de los nodos (aportando eficiencia al despacho de los paquetes y confidencialidad de la información que circula por la red), control de acceso al medio, calidad del servicio (elementos en la red que deciden la prioridad de la información que transita por la misma), división de segmentos de una red y aumento del ancho de banda.

También es objetivo de la clase conocer la función y funcionalidades de BRIDGES Y SWITCHES ya que estos elementos pueden aportar alguna o todas de las características mencionadas más arriba.

2 CAPA DE ENLACES DE DATOS

Esta capa es la que permite la transmisión física a través del medio. Para poder realizar esta tarea, una de las cosas que debe conocer es el tipo de medio y su velocidad de trabajo para poder manejarlo, sea RG58, UTP o Fibra Óptica y la velocidad de transmisión. Por ejemplo podemos encontrar tres velocidades, 10 Mb/s, 100Mb/s y 1000Mb/s, esto significa que se deberá acondicionar el flujo de señales a cada una de las circunstancia.

Otra tarea que tiene es la implementar la forma en que dialogarán los integrantes de la red, esta se lleva a cabo utilizando un ***Protocolo de Comunicación*** que podemos definirlo como un conjunto de reglas para entablar y mantener una comunicación. Dicho protocolo esta definido en una tecnología de red llamada Ethernet, la cual desarrollaremos a continuación.

3 TECNOLOGÍA ETHERNET

La red Ethernet es la tecnología de red de área local (LAN) más ampliamente usada. La versión original de Ethernet más popular soporta transferencias a 10 Mega bits por segundo. Las versiones nuevas llamadas ***Fast Ethernet*** (Ethernet rápida) y ***Gigabit Ethernet***, soportan transferencias a 100 Mega bits y 1000 Mega bits (1 Gigabit por segundo) respectivamente.

Una red Ethernet puede usar cable coaxial, cable de pares retorcidos (UTP) o fibra óptica. Las configuraciones de cableado que utiliza son la de Bus y Estrella, siendo esta última la más popular en la actualidad como hemos visto. Todos los dispositivos que participan de una red Ethernet, se dice que compiten por acceder a la red, utilizando un protocolo llamado ***CSMA/CD*** (Carrier Sense Multiple Access with Collision Detection - Sensado de Portadora de Múltiple Acceso con Detección de Colisiones).

3.1 LA HISTORIA DE ETHERNET

El primer sistema experimental Ethernet, fue desarrollado a los principios de los '70 por Bob Metcalfe y David Boggs del Centro de Investigaciones de Palo Alto de Xerox.

En 1979, Digital Equipment Corporation (DEC), Intel y Xerox se juntaron con el propósito de estandarizar el sistema Ethernet, para que cualquier compañía lo pudiese utilizar. En septiembre de 1980 las tres compañías lanzaron la versión 1.0 de la primera especificación Ethernet, llamada ***Ethernet Blue Book*** (Ethernet Libro Azul) o estándar ***DIX*** (por las iniciales de las tres compañías). Habían definido el sistema ***Thick Ethernet*** (Ethernet grueso), basado en 10 Mega bits por segundo de velocidad de comunicación y el protocolo CSMA/CD. Fue conocido con ese nombre por el cable coaxial usado para interconectar a los dispositivos (RG211) que era bastante grueso.

En 1983, el Instituto de Ingenieros Eléctricos y Electricistas (IEEE), que es un organismo que establece estándares industriales, lanzó el primer estándar para la tecnología Ethernet. Fue desarrollada por el grupo de trabajo del comité ***IEEE 802***. El título formal del estándar fue ***IEEE 802.3 Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specification*** (especificación de capa física y método de acceso). El grupo de trabajó realizando algunas modificaciones sobre el formato de las transmisiones, pero permitiendo que el formato anterior sea reconocido y compatible.

En 1985, el estándar ***IEEE 802.3a*** definió una segunda versión de Ethernet, conocida como ***Thin Ethernet*** (Ethernet Delgada), ***Cheappernet*** (red más barata) o ***10Base-2***, que usaba un cable más delgado y más barato que el de la especificación original: el RG58.

En 1987 fueron lanzados dos estándares. Uno fue el ***IEEE 802.3d*** que definió el enlace entre repetidores por fibra óptica ***FOIRL*** (Fiber Optic Inter Repeater Link) que permitió extender el alcance entre repetidores a 10 Mega bits por segundo, hasta 1 Kilómetro (un repetidor, es un dispositivo electrónico que nos permite enlazar segmentos de red para extender su alcance, y se estudiarán en una clase posterior).

El otro fue el ***IEEE 802.3e*** definiendo un estándar Ethernet en cable de pares retorcidos a 1 Megabit por segundo. Este estándar nunca fue ampliamente usado.

En 1990 se ha desarrollado el mayor avance en la tecnología Ethernet, cuando se introdujo la especificación del estándar ***IEEE802.3i 10Base-T***. Permitió operar a 10 Megabits por segundo sobre un cable de pares retorcidos categoría 3 sin blindaje UTP (Unshielded Twisted Pair - Par Retorcido sin blindar). Como había una amplia base de cableado de este tipo para telefonía, existente en los edificios, esto creó una gran demanda de tecnología 10Base-T. Esta especificación facilitó las tareas de expansión, reparación y mantenimiento de las redes Ethernet.

En 1993 fue lanzado el estándar ***IEEE 802.3j*** para ***10Base-F*** (FP, FB y FL), el cual permitió enlaces sobre distancias más largas (2Km) vía dos cables de fibra óptica. Este estándar actualizó y expandió el anterior estándar ***FOIRL***.

En 1995 el IEEE mejoró el desempeño de las redes Ethernet en un factor de 10, cuando lanza-ron el estándar 802.3u 100Base-T. Esta versión de Ethernet es la más conocida como "Ethernet Rápida" (*Fast Ethernet*). Soporta tres tipos de medios:

- **100Base-TX** opera sobre dos pares de cables UTP Categoría 5 o superior.
- **100Base-T4** (o 100Base-VG - Voice Grade - Grado Voz) opera sobre cuatro pares de cable UTP categoría 3 o superior.
- **100Base-FX** opera sobre dos cables de Fibra Óptica en multimodo.

En 1997 el estándar ***IEEE 802.3x*** definió la operación ***Ethernet Full Dúplex***. La operación Full Dúplex sobrepasa el protocolo CSMA/CD para permitir a dos estaciones comunicarse a través de un enlace punto a punto en forma bidireccional simultánea. Efectivamente dobla la velocidad de transferencia, ya que las estaciones pueden transmitir simultáneamente en dos canales separados. El protocolo Full Dúplex es aplicable a 10, 100 y más Megabits por segundo. También en 1997 se lanzó el estándar **802.3** y ***100Base-T2*** para operar a 100 Megabits sobre dos pares de cable balanceado UTP categoría 3.

En 1998 el IEEE otra vez mejoró el desempeño de Ethernet en un factor de 10, cuando lanzó el estándar ***IEEE 802.3z 1000Base-X***. Esta versión es la más conocida como "Gigabit Ether-net". Tres tipos de medios están soportados:

- **1000Base-SX** que opera con un láser de 850nm sobre fibra en multimodo.
- **1000Base-LX** que opera con un láser de 1300nm sobre fibra en mono y multimodo.
- **1000Base-CX** que opera sobre cobre en par retorcido blindado "twin axial".

También fue lanzado en 1998 el estándar ***IEEE 802.3ac*** que define extensiones para soportar VLAN (LAN Virtuales).

En 1999 el estándar ***802.3ab 1000Base-T*** definió la operación a 1 Gigabit por segundo sobre los cuatro pares del cable UTP en Categoría 5 o superior.

3.2 ETHERNET HALF DUPLEX: PROTOCOLO CSMA/CD

El protocolo de acceso al medio CSMA/CD (***C***arrier ***S***ense ***M***ultiple ***A***ccess with ***C***ollision ***D***etection - *Sensado de Portadora de Múltiple Acceso con Detección de Colisiones*) es la forma tradicional de acceso de ***Ethernet Half Duplex*** (Half Duplex es el modo de usar al medio de comunicación, por el cual sólo una transmisión a la vez puede estar en curso).

Con CSMA/CD, dos o más estaciones comparten un medio común de comunicación. Para transmitir un ***"Frame"*** *<freim>* (Trama: paquete de datos con un formato estandarizado), una estación debe esperar por un lapso de descanso del medio, donde ninguna estación transmita información. Luego comienza la transmisión del frame, el cual es "escuchado" por todas las estaciones conectadas. Si alguna estación trata de enviar datos al mismo tiempo, una "***colisión***" ocurre. Las estaciones que colisionaron, deben permanecer en silencio por un tiempo establecido al azar, antes de reinten-

tar la operación fallida. Este procedimiento es repetido hasta que el frame es eventualmente transmitido exitosamente.

Las reglas básicas para transmitir un frame son las siguientes:

1) La red es examinada por la presencia de una "portadora", o presencia de una transmisión en curso. Este proceso se lo conoce como "sensado de portadora".
2) Si una portadora es detectada, luego la transmisión es diferida. La estación continuará examinando la red hasta que cese la portadora.
3) Si una portadora activa no es detectada y el período de silencio es mayor o igual a la brecha existente entre frames transmitidos, luego la estación comenzará a transmitir inmediatamente.
4) Mientras está transmitiendo la información, examina al mismo tiempo la información que sale al medio, en busca de una colisión.
5) Si una colisión es detectada, la estación detiene la transmisión inmediatamente y envía una secuencia de 32 bits (***jam sequence*** - secuencia de bloqueo) para asegurar que la colisión sea detectada por la o las otras estaciones.
6) Luego de la secuencia de bloqueo, las estaciones participantes de la colisión, deberán esperar un tiempo tomado al azar antes de reintentar la operación. La probabilidad de repetir la colisión es reducida, debido a la espera impuesta al azar.
7) Si la colisión se repite, luego la transmisión será repetida, pero duplicando los tiempos de espera que se tomaron inicialmente, para reducir aún más la posibilidad de una nueva colisión.
8) Este proceso se repite hasta que una estación logre transmitir exitosamente un frame sin colisión.

3.3 EL TIEMPO DE RANURA (SLOT TIME)

El "slot time" es un parámetro clave para la operación de Ethernet Half Duplex. Está definido como el tiempo empleado para transmitir 512 bits en una red de 10 y de 100 Megabits por segundo, y de 4096 bits para Gigabit Ethernet.

Para asegurar que cada estación transmisora detecte confiablemente las colisiones, el mínimo tiempo de transmisión para un frame completo debe ser al menos de un "slot time", y que el tiempo requerido para que las colisiones se propaguen a todas las estaciones en la red debe ser menor a un "slot time".

Las señales transmitidas por las estaciones Ethernet encuentran retardos a medida que viajan a través de la red. Estos retardos se deben a las demoras que sufren las señales en su viaje por el cable de la red y de los retardos lógicos encontrados cuando la señal debe pasar por componentes electrónicos, como placas de red (NICs) y repetidores.

Cuanto haya segmentos más largos y mayor cantidad de repetidores entre las estaciones, tanto más se incrementará el ***tiempo de propagación*** desde una punta hasta la otra de la red.

Para que una estación pueda detectar que su transmisión ha encontrado una colisión, su señal debe propagarse a través de la red con la velocidad suficiente como para llegar hasta la otra estación que transmite, y regresar hasta origen antes de haber finalizado la transmisión del frame.

Si el tiempo de propagación de la red es superior al slot time, alguna estación podría completar la transmisión del frame sin enterarse que ha colisionado. Este fenómeno se conoce como "colisión tardía" y se considera una falla, ya que es el software de aplicación quien debe ahora hacerse cargo del problema de la retransmisión.

El slot time para Gigabit Ethernet ha tenido que incrementarse a 4096 bits, ya que un slot time de 512 bits a un Gigabit por segundo, limitaría la longitud máxima de los segmentos a 20 metros como máximo, que por otro lado sería impracticable. Con la corrección del slot time y el acotado de repetidores a sólo uno, una longitud de 200 metros puede ser soportada por Gigabit Ethernet.

3.4 ETHERNET FULL DUPLEX

El estándar IEEE 802.3x definió un segundo modo operativo para Ethernet, llamado "Full Duplex". A diferencia del protocolo CSMA/CD que describe el modo en que dos estaciones pueden transmitir información entre sí, de a una a la vez, nunca simultáneamente, full duplex permite establecer comunicaciones bidireccionales simultáneas, sobre una línea de comunicación punto a punto.

Sólo es posible implementar sobre enlaces que provean caminos independientes para la transmisión y la recepción.

Los medios físicos que permiten operación Full Duplex, serán aquellos que permitan transportar transmisión y recepción simultánea, como **10Base-T, 10Base-FL, 100Base-TX, 100Base-FX, 1000Base-CX, 1000Base-SX, 1000Base-LS y 1000BaseT**.

Los que **NO** soportan full duplex son: **10Base5, 10Base2, 10Base-FP, 10Base-FB y 100Base-T4**.

La operación full duplex está restringida a los enlaces punto a punto. Debido a que no hay contención para compartir el medio de transmisión (es exclusivo), el protocolo CSMA/CD es innecesario, pues las colisiones nunca ocurren. Ambas estaciones deben ser hábiles y deben estar configuradas para manejar transmisiones en full duplex.

Las ventajas de este modo de transmisión, son las siguientes:

- La velocidad efectiva del enlace se duplica, ya que se permiten transmisiones y recepciones simultáneas.
- La eficiencia del enlace está mejorada por la eliminación de las colisiones potenciales.
- Al no haber colisiones, se pueden aumentar las longitudes de los segmentos, ya que no tiene efecto el "slot time" estudiado anteriormente. Por ejemplo en el caso de 100Base-FX en half duplex se encuentra limitado a 412 metros de longitud, pero se pueden alcanzar longitudes de segmento de hasta 2Km en full duplex.

4 FORMATO DE LOS DATOS TRANSPORTADOS (FRAMES)

Sabemos que una máquina conectada en red, intercambia información con otras máquinas a través del medio de comunicación (cables, radio, fibras ópticas, etc.).

Supongamos entonces que desde una máquina deseamos transferir un archivo cuyo tamaño es de diez megabytes a otra. Si la máquina transmitiera dichos datos de forma continua por el medio de comunicación, ninguna otra computadora conectada a la misma red podría transferir datos, porque el medio se encuentra ocupado.

Esto se soluciona ***fragmentando*** los datos a transmitir en "paquetes" a una longitud limitada, de modo que completado el envío de un fragmento, el medio quede disponible para que otras máquinas tengan oportunidad de transmitir.

Por otro lado es evidente que el fragmento cuando se transmite por el medio, ***todas*** las computadoras conectadas reciben esa misma información. Para poder hacer llegar un fragmento a una computadora específica en la red se deberá implementar una forma de direccionamiento.

La solución es colocar al fragmento una dirección **destino** y una dirección **origen**, en forma análoga al envío de una carta, donde colocamos al frente el **destinatario** y al dorso el **remitente**.

Los datos de las direcciones, ***no forman parte de los datos originales***, sino que ***son agregados***. Siguiendo con el ejemplo de la correspondencia, los datos del destinatario y del remitente, se escriben ***en el sobre*** y ***no en la carta*** propiamente dicha.

Cada máquina entonces, antes de transmitir los datos por el medio de comunicación, *"ensobra"* los datos, escribe la dirección del destinatario y del remitente **en el sobre** para luego comenzar la transmisión. Luego de esta reforma todas las máquinas recibirán el mismo fragmento, pero ahora las que los que lo reciban constatarán la dirección de destino, descartándolo si no le pertenece y tomándolo si le corresponde para procesarlo.

El sobre que transporta a los datos, se lo conoce como *Trama* (o Frame, en inglés).

Varios niveles (o capas) de ensobrados hacen falta, para establecer una comunicación confiable y efectiva entre dos máquinas.

A estos distintos niveles de ensobrado también se lo denomina ***encapsulamiento*** y son los servicios que presta una capa superior a una inferior.

Para transportar los datos por ***un segmento*** de la red entre dos máquinas que se encuentren interconectadas *por el mismo cable*, el ensobrado corresponde a la capa de enlace de datos

(data link). Para el caso de una red Ethernet, las normas son:

ETHERNET_802.3 **ETHERNET_802.2**

ETHERNET_II **ETHERNET_SNAP**

Los frames 802.3 y 802.2 son los que emplea Novell Netware. El 802.3 es utilizado en las versiones 3.11 y anteriores y el 802.2 (la versión mas moderna) en las versiones 3.12 y posteriores.

El frame ETHERNET_II es empleado principalmente por TCP/IP; y el SNAP (**S**ub **N**etwork **A**ccess **P**rotocol) que es un standard posible de emplear en Novell, TCP/IP, OSI, etc.

A continuación detallaremos el formato del Frame ETHERNET_II utilizado en TCP/IP

Frame ETHERNET_II

64 bits	48 bits	48 bits	16 bits	desde 368 hasta 12000 bits	32 bits
Preámbulo (sincronismo)	Dirección destino	Dirección origen	Tipo de frame	Datos transportados (desde 46 hasta 1500 bytes)	CRC

Como podemos observar en la figura superior hay dos campos de cuarenta y ocho bits (compuesto por seis grupos de seis bytes cada uno), estos contienen la **dirección física de la *placa* origen** y la **dirección física de la *placa* destino** de las cuales ya estuvimos hablando.

Esta dirección física está presente en todas las placas de red y es grabado en fábrica dentro de en una memoria ROM, estando compuesto por un número de 48 bits. Esta dirección física también se la conoce con el nombre de ***MAC Address*** (Media Access Control Address – Dirección de Control de Acceso al Medio). El organismo IEEE es el encargado de regular la asignación de rangos numéricos a cada fabricante, evitando de esta forma la superposición de una misma serie numérica en cualquier producto.

Las direcciones físicas de las placas de red son números de 48 bits compuestos por seis grupos de 8 bits cada uno, que a su vez se expresan en dos dígitos hexadecimales separados por dos puntos. Un ejemplo de una dirección de placa podría ser: ***00: 08: 00: 12: F5: EC***.

Este número es el que emplea la placa de red, para saber si debe procesar el frame recibido o no. Si una placa recibe un frame cuyo campo de "dirección destino" trae grabado ***el mismo número*** que el que está grabado en la placa, lo procesa; si no, lo ignora.

Si el sistema desea responder a la máquina que envió los datos, toma la "dirección origen" (dirección del remitente) para enviar la respuesta.

El campo "Preámbulo" de sesenta y cuatro bits, es utilizado para sincronizar las transmisiones entre placas que intervienen en la transmisión, en el campo "Tipo de frame" se envía información acerca de qué tipo de datos son los transportados.

El campo identificado como "CRC" (***C**yclic **R**edundant **C**ontrol - **C**ontrol **R**edundante **C**íclico)*, es un sistema que se implementa para el control de errores, para asegurar la integridad de la información que se encuentra dentro del campo llamado "Datos transportados".

4.1 BROADCAST ADDRESS:

Como hemos visto, para poder transmitir un frame a otra máquina, hay que conocer de antemano la dirección física de la placa destino.

También cada máquina debería entonces tener grabado en algún lado, una tabla con el listado de las direcciones de las placas de todas las otras máquinas que componen la red.

Configurar estas tablas en todas las máquinas manualmente, sería una tarea tediosa y engorrosa. Además, si por algún inconveniente técnico hay que reemplazar una placa de red en alguna máquina, habría que actualizar los datos de las tablas en ***todas*** las máquinas, para que ahora sepan que si desean enviarle datos, deben hacerlo a la nueva dirección de la placa.

Para evitar esta situación, existe un canal de comunicación comunitario conocido como “Broadcast”o difusión. Esto es simplemente un frame que se arma con una dirección especial, el cual se envía a todos los integrantes de la red y estos se encuentran obligados a recibir. La dirección de la que hablamos esta expresada con el número hexadecimal y es ***FF: FF: FF: FF: FF: FF***.

5 EXTENSIONES TOPOLÓGICAS

Cuando definimos las topologías, conocimos sus limitaciones con respecto a la longitud máxima del cable de cada segmento tanto en redes cables RG58 como UTP, estas son producto de las características eléctricas y la forma de transmitir los datos. Por este motivo es que se deberán tener en cuenta estos factores al momento de extender la longitud o agregar máquinas.

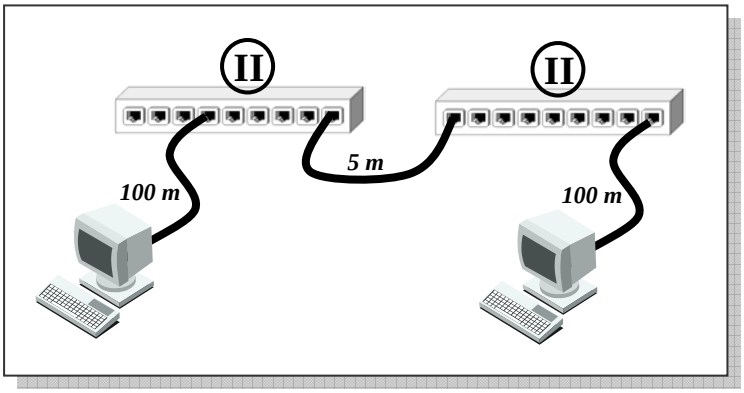
Este desafío de incrementar la cantidad de máquinas en una red mas allá de lo establecido, comienza con las redes Ethernet de topología BUS que trabajan a 10Mbps y hasta hace poco tiempo con las de tipo estrella también a 10 Mbps.

Ambas topologías plantean los mismos inconvenientes al compartir la misma tecnología y por lo tanto comparten las mismas soluciones, pero debemos tener en cuenta que estas redes a 10 Mbps en la actualidad ya no se implementan debido a su baja velocidad, pero si se les brinda mantenimiento.

El desarrollo de este tema sería bastante extenso y anacrónico, sin embargo para aquellos que se encuentren interesados en este con fines de mantenimiento o el crecimiento de sus conocimientos (lo que recomendamos fuertemente para una mejor comprensión de los próximos puntos), es que ponemos a disposición el desarrollo completo de este tema como material complementario.

5.1 LIMITACIONES DE EXPANSIÓN EN FAST ETHERNET

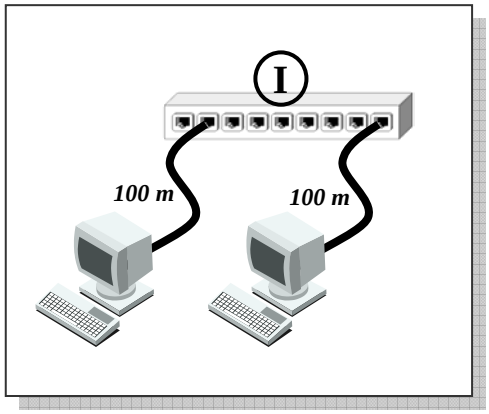
En la topología 100BaseTX se tienen los parámetros de tiempo más ajustados. El hecho de que las transmisiones sean diez veces más rápidas que Ethernet 10BaseT, hace que el tiempo límite para detectar una colisión sea inferior. Esto limitará la longitud del cable que deberá utilizar y la cantidad de hubs (repetidores) permitidos entre enlaces.



El estándar Fast Ethernet define dos tipos de repetidores: Clase I y Clase II. El estándar requiere que los repetidores Fast Ethernet estén rotulados con los números romanos I y II centrados en un círculo para identificarlos.

Los repetidores Clase I tienen permitidos introducir demoras más grandes en los enlaces y permitir operar con traducción de señales entre los puertos. Esta traducción permite enlazar segmentos 100BaseTX con 100BaseFX o 100BaseT4.

Los repetidores Clase II son más rápidos (deben producir demoras inferiores) y no traducen señales



entre los puertos. Con estos repetidores no se pueden mezclar segmentos de distintas normas.

Si utilizamos un repetidor **Clase I**, no se permiten las conexiones en cascada. La longitud de cada segmento será de 100 metros como máximo. Ello implica que la distancia máxima entre dos nodos es de 200 metros, atravesando un repetidor. Si utilizamos un repetidor **Clase II**, sólo se puede armar una cascada entre **dos** unidades, con un segmento desierto de **cinco** metros de largo como máximo. La longitud de cada segmento poblado será de 100 metros como máximo. Esto indica que la distancia entre cualquier par de nodos debe ser de 205 metros máximo, atravesando dos repetidores.

Como vemos estamos muy limitados para extender la red Fast Ethernet. Como alternativa adicional, si los hubs lo permiten, está la posibilidad de apilarlos.

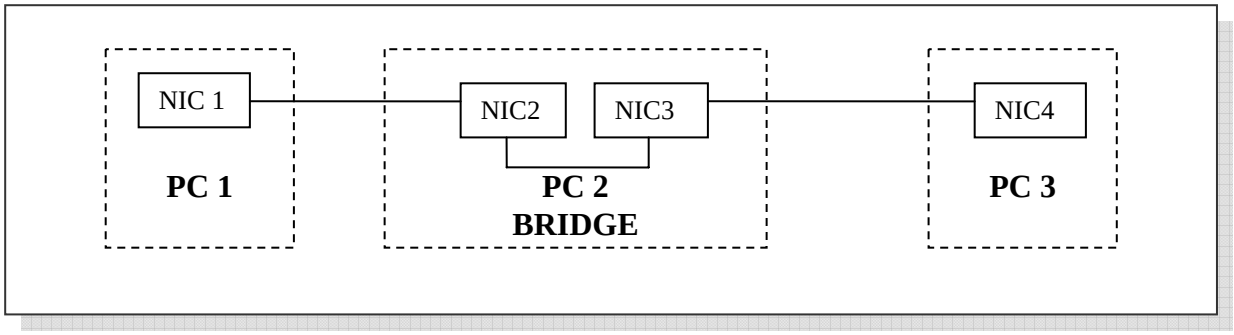
6 DISPOSITIVOS DE CAPA 2

6.1 BRIDGE

Los Bridge tienen la característica de poseer sólo dos bocas de conexión y utiliza las direcciones MAC de las placas de red, para saber a quien debe enviar un frame o de quien lo esta recibiendo.

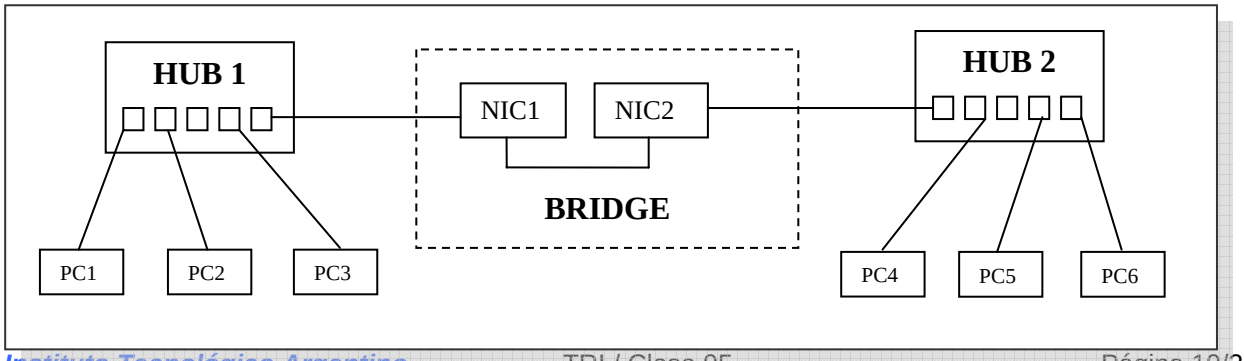
En la próxima figura podemos observar un esquema simplificado de un Bridge realizado a partir de una PC con dos placas de red y una tabla que guardará las direcciones MAC de las máquinas que se conecten a través de esta NIC.

La forma en la cual funciona es muy simple, el Bridge escucha todos los datos que circulan por la red y toma nota de la dirección origen que se encuentra en el frame, de esta forma sabe quien está conectado en una de sus bocas.



El ejemplo nuestro es básico, ya que si la PC 1 quisiera comunicarse con la PC 3, la PC2 que tiene la tabla de direcciones sólo tendría que fijarse en la misma si tiene la dirección MAC de destino que recibió en el frame enviado por la PC 1.

Para agregar un poco de complejidad a este ejemplo colocaremos un HUB con máquinas en cada una de las bocas nuestro Bridge, si analizamos ahora este esquema veremos que a cambiado sustancialmente la forma en la cual se comportará.



Las PC que se encuentran conectadas al HUB1, si quisieran comunicarse entre si no se necesitará el servicio del Bridge, y lo mismo sucede con las máquinas que están conectadas al HUB2.

Teniendo estos datos analizaremos que sucedería si la PC1 quiere comunicarse con la PC6 sabiendo que la tabla de direcciones del Bridge no tiene registrada la perteneciente a la PC6

- Para solucionar este problema nuestro Bridge arma un frame especial con una dirección de destino ***FF : FF : FF : FF : FF : FF*** llamado ***Flowding*** (*Inundación)* que se envía a todas las PC menos a la que originó el pedido, el resultado es que todas las PC conectadas al HUB2 están obligadas a recibir este frame.
- Como resultado de esta acción todas las PC que están conectadas al HUB2 y que están escuchando, tendrán que armar un frame de respuesta en el cual figura la dirección MAC propia. Aquí en esta paso debemos recordar que el HUB1 no escucha nada de lo que sucede ya que este es atendido por la NIC1 con su correspondiente tabla.
- Este envío masivo tiene como destinatario la NIC2 del Bridge que incorporará a su tabla las nuevas direcciones MAC que se encuentran en el HUB 2.
- Finalmente el Bridge ya pude contar con la dirección MAC de la PC6 en la tabla y puede enviar el frame a través de su NIC2

De esta forma es como tiene conocimiento de las direcciones MAC un Bridge para luego canalizar el envío de frames a las máquinas el HUB2.

Otro punto a tener en cuenta es que a raíz de forma en que funciona, la red se divide en dos grupos ubicados a ambos lados del Bridge y se elimina la puja por tener acceso al medio entere estos grupos.

Si analizamos que sucede cuando la PC1 quiere comunicarse con la PC3 podemos deducir que no será necesaria una consulta mediante un Flowding ya que todas las PC se encuentran conectadas al mismo HUB y la NIC1 del Bridge posee las direcciones MAC de todas ellas. De esta forma ver que las comunicaciones entabladas por las PC conectadas al HUB1 no se propagarán al HUB2, por lo tanto los PC conectadas a este último con tendrán que competir por el acceso al medio con las PC de HUB1.

Por este motivo es que se dice que los Bridge dividen dominios de colisión.

Otra característica del Bridge es que al trabajar en la capa 2, sólo puede enlazar dos redes que posean la misma tecnología, por ejemplo dos Ethernet y no una red Token Ring con una Ethernet.

Uno de los motivos es que el frame utilizado por Token Ring (IEEE 802.5) tiene dos versiones, uno con direcciones MAC 48 bits y otro de 16 bits 16 Bits, siendo esta último un escollo imposible de sortear.

6.2 SWITCH

El Switch trabaja con el mismo principio de funcionamiento y podríamos considerar a cada una de sus bocas como una placa de red (igual a nuestro Bridge), o dicho de otra forma es un Bridge con múltiples bocas y que cada una de ellas se las considera como un dominio de colisión en si mismo.

Si recordamos el principio de funcionamiento, podemos llegar fácilmente a la conclusión de que es posible mantener dos comunicaciones en forma simultánea, y sin que exista la puja por el acceso al medio.

Esto nos lleva a dos nuevos resultados:

- El primero es que este método le permite a la red transportar una mayor cantidad de datos en el mismo tiempo ya que no se tiene que compartir el medio físico si conectaron dos PC directamente a las bocas del Switch.
- El segundo es un emergente del anterior ya que bajo estas condiciones se pueden efectuar una transmisión de datos entre dos estaciones en forma simultánea, también conocida con el nombre Full Duplex.

Como podemos apreciar estas características sobresalientes le permiten a los switch tomar una red de grandes proporciones y dividirla en pequeños segmentos aumentando el ancho de banda disponible al máximo teórico y evitando las colisiones. Finalmente podemos decir que con esta tecnología nos permite extender una red sin temer al problema de las limitaciones impuestas por Ethernet.

7 FUNCIONES ESPECIALES EN LOS SWITCH

Cuando se crearon los Switch no sólo se pensó en mejorar el rendimiento de la red eliminando al único dominio de colisión, ya que este debería trabajar en entornos empresariales se pensó que también se lo debería dotar de sistemas de conexiones redundantes para asegurar el flujo constante de datos en puntos críticos de la red.

En la misma tónica ya sea desde el comienzo y a lo largo del tiempo se le incorporaron funciones como, forma de despachar de tráfico, controlar las conexiones redundantes para evitar lazos cerrados, permitir segmentar aún más la red a través de la tecnología VLAN (Virtual LAN – LAN Virtual), controlar la forma en que se entrega la información en base a una política conocida QoS (Quality of Service – Calidad de Servicio). Finalmente debemos decir que a todas estas características se le agrega un indispensable que es la de administración.

A continuación realizaremos una reseña de las tecnologías involucradas en estas funcionalidades.

7.1 DESPACHO DE TRÁFICO

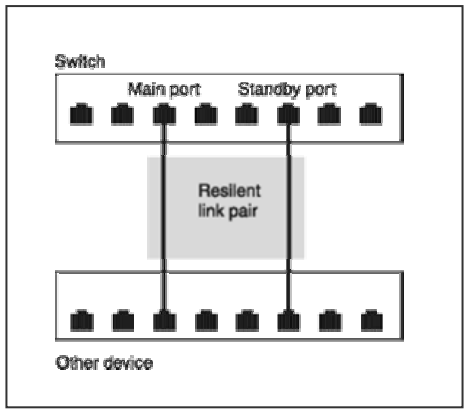
Esta es un funcionalidad que depende del entorno de trabajo, teniendo en cuenta la urgencia de entrega de los datos, esto es debido a que en algunas redes se podrían llegar a privilegiar la inmediatez de la información, con esto en mente es que existen dos tipos de manejo de entrega:

- ***Cut Trough***: es la tecnología que permite implementar entregar de la información antes que finalice su ingreso. Es significa que los datos transportados de esta forma tendrán un baja latencia (Variaciones del tiempo que se encuentra entre cada frame entregado). Como toda tecnología posee ventajas y desventajas, por ejemplo esta forma de trabajar tiene el inconveniente que para enviar rápidamente los datos omite la verificación de integridad de estos trayendo como resultado el envío de información corrupta haciendo que se tenga que volver a retransmitir y por consiguiente una demora no deseada.
- ***Store and Forward***: a diferencia de la tecnología anterior, esta sí verifica la integridad de la información, para lograr esto incorpora una memoria de entrada para almacenar temporalmente el frame y realizar la verificación. La ventaja de este sistema es que no se enviarán frames corruptos, ya que los mismos son descartados en el proceso, finalmente se puede adelantar que esto nos permitiría de forma adicional controlar tráfico mediante el almacenamiento temporal. La desventaja es que la latencia se vería incrementada a raíz del tiempo que se tarda en almacenar el frame y su posterior verificación.

Como hemos visto estas dos tecnologías se tendrán que utilizar en base a los requerimientos de tráfico de la red, como dato interesante podemos decir que estas características se las encuentran disponibles en todas las marcas fabricantes y algunos suelen cambiar de forma automática el modo de funcionamiento.

7.2 SPANNING TREE IEEE 802.1D

Anteriormente hablamos de conexiones redundantes para garantizar el flujo de datos, la tecnología empleada se llama Resilient Link y trabaja en la capa 1 del modelo OSI configurando a una boca del Switch como Standby (en espera) de otro.



Como podemos ver en la figura es muy sencillo realizar dos conexiones físicas creando un viculo de respaldo, pero su implementación requiere del cumplimiento de la norma IEEE802.1D que especifica los fundamentos del Bridge y el Spanning Tree Protocol. Este protocolo es el encargado de asegurarse que no se creen lazos redundantes permanentes en la red que podrían ocasionar que un frame quede permanentemente dando vueltas. La segunda función que tiene es el reconocer a los vínculos, uno como root (raíz) el cual se en encarga del transporte y el segundo se

encuentra en estado de stand by (en espera) listo para entrar en acción cuando detecte una falla del root.

Para lograr esto el protocolo utiliza un frame especial llamado BPDUs (Bridge Protocol Data Units) este es frame especial para que los distintos switch de la red se intercambien entre ellos información referida a los links existentes y su estado, asegurándose que solamente este uno sólo de ellos activo evitando los lazos cerrados.

Esto también provee de información actualizada y permanente de la configuración de red, ya que tiene la capacidad de monitorear todos los links que se implementen con posterioridad a la configuración inicial.

Este protocolo se encuentra definido en la norma IEEE 802.2Q en el cual el tiempo estimado para recuperarse de un fallo de link es variable pero se estima que puede demorarse unos 30 segundos, debido a esto es que se desarrolló otra versión mas rápida de este protocolo que puede realizar la misma tarea en aproximadamente en 5 segundos lo que permitirá un tiempo mínimo de falta de datos en la red, a este nuevo protocolo la IEEE lo denominó 802.1W y se lo conoce como RSTP (Rapid SPT – STP Rápido).

7.3 VLAN

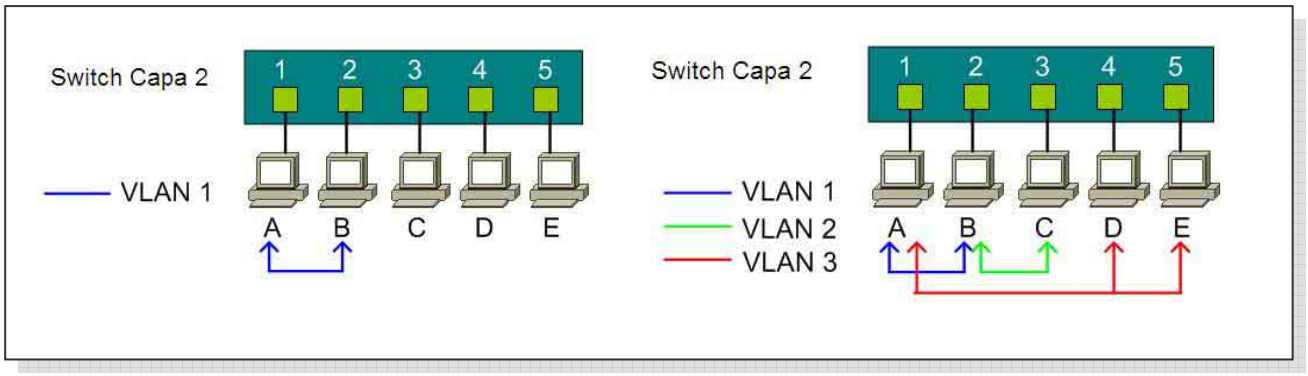
Las VLAN Virtual (LAN – LAN Virtual) permiten utilizar los medios físicos disponibles de una red realizadas con un switch y transformarla en varias redes independientes a nivel de la capa 2, dicho de otra forma podemos particionar nuestro switch en un conjunto de switch virtuales.

La creación de una VLAN es un proceso que es realizado por el administrador y se trata de seleccionar un grupo de bocas para que trabajen en forma independiente y sean reconocidos por un identificador único dentro del switch, esto significa que cada VLAN mantendrá su propia tabla direcciones MAC.

Las ventajas que ofrece el uso de VLAN las podemos enumerar en:

- El primer objetivo de esta tecnología es limitar los dominios de broadcast a nivel de la capa 3 del modelo OSI. El broadcast es una difusión masiva (a todos los integrantes de una red) de una dirección especial IP que veremos mas adelante y que todos los integrantes de un red están obligados a contestar. Esto provoca en la red una sobrecarga de tráfico que disminuye su rendimiento.
- El segundo es la facilidad de administración en grupos virtuales, se lo denomina así ya que es posible agrupar a los usuarios en grupos sin importar su ubicación geográfica simplificando la cantidad configuraciones necesarias en la red.
- Aumento de la seguridad en la red ya que los usuarios que los integrantes de la red que no pertenezcan a la VLAN no tendrán acceso a la misma.

Un ejemplo gráfico de una VLAN puede ser la siguiente figura donde podemos observar como podemos crear dos VLANs mas en una red compuesta por un solo switch.



Para poder crear una VLAN se dependerá del software provisto por el fabricante del switch, pero el procedimiento desde el punto de vista conceptual será muy similar en todos las marcas.

En el primer ejemplo podemos ver como se han asociado a las bocas 1 y 2 del switch a una VLAN que llamamos 1 donde se conectan las PC A y B, con este mismo procedimiento podemos llegar a otras VLAN como en el segundo ejemplo en el cual hemos creado 3 VLANs asociando libremente cualquiera de las bocas a estas.

En la vida real este proceso requiere que se ingrese al switch para poder configurarlo de acuerdo a nuestras necesidades, los procesos que se deben llevar acabo son muy similares a los descriptos anteriormente y sólo dependerá del tipo de herramienta administrativa que utilicemos, si se utiliza una interfaz gráfica (vía Web) o línea de comandos a través de la emulación de terminal con Telnet. Esto quiere decir que no será un impedimento o una complicación si accedemos a una interfaz gráfica, una línea de comando, o cualquiera sea el fabricante del producto; si tenemos bien claro cual es el procedimiento.

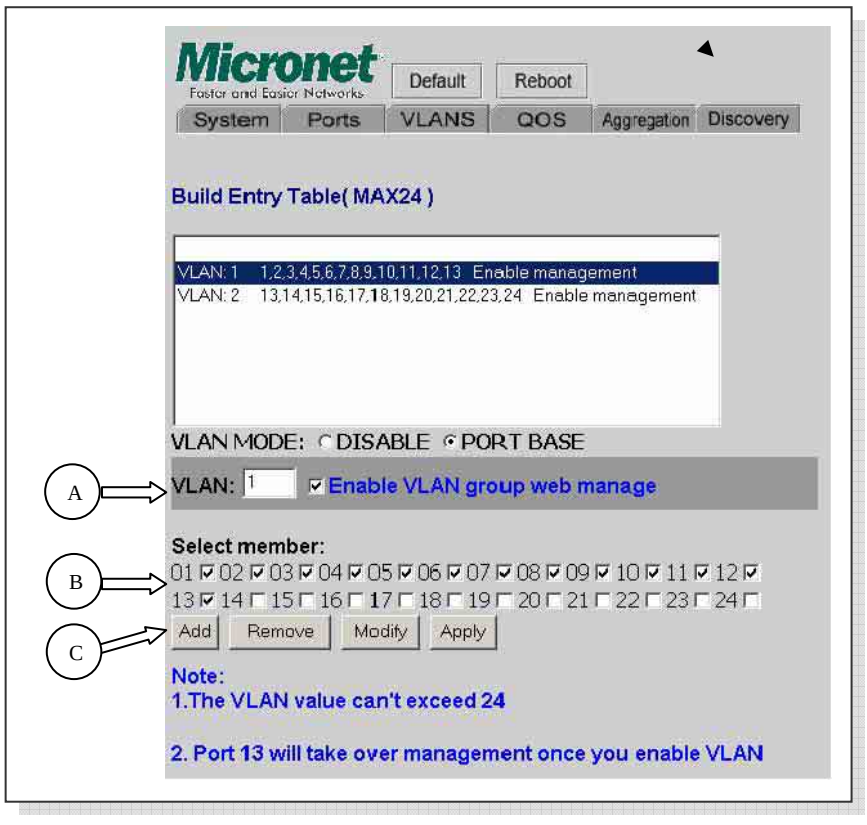
Un ejemplo de esto es la próxima imagen de una ventana que pertenece a un switch administrado vía Web al cual hemos ingresado mediante la dirección IP predeterminada por el fabricante, luego de esto se abre normalmente una ventana que solicita el nombre de usuario y contraseña del administrador a cargo, si los datos son los correctos podremos ver la ventana principal y desde esta seleccionaremos la solapa que lleva el nombre de VLANs.

Como podemos observar la disposición de los controles y sus denominaciones hacen parecer la creación de VLANs una tarea sencilla e intuitiva si recordamos los pasos el procedimiento

Sobre el lado izquierdo se han ordenado alfabéticamente los pasos que deberíamos seguir para armar 2 VLANs:

- A: definir la identificación de la VLAN (1), en este caso se le puede asignar cualquier número ya que es meramente descriptivo.
- B: seleccionar las bocas que desee hacer pertenecer a la VLAN, esto se logra simplemente colocando un tilde en el recuadro perteneciente a la boca, en nuestro caso las bocas 1 a la 12.
- C: finalmente solo resta aplicar los cambios realizados a la configuración y verificar que los puestos de trabajo conectados a los puertos definidos tengan comunicación entre ellos.

.



El siguiente paso consiste en repetir este procedimiento repitiendo los pasos A, B, y C cambiando las bocas que se seleccionaran en el paso B (bocas 13 a la 24). De esta forma hemos obtenido dos VLANs dentro de un mismo swicth, proceso al cual se lo conoce como particionado de VLAN.

Este es solo un ejemplo sobre un tipo de hardware específico pero debemos decir que el límite de VLAN que se pueden llegar a crear está dado por la cantidad de bocas disponibles en el switch, en el caso anterior esto es 24 VLAN.

7.4 STP (SANNING TREE PROTOCOL)

STP abreviación de Spanning Tree Protocol - Protocolo de Expansión en Árbol: no siempre se lo traduce de esta forma y solo se lo define como un protocolo que se utiliza en redes conmutadas para administrar todos los enlaces físicos en la red.

Cuando se trabaja en redes conmutadas con una extensión considerable se puede llegar crear conexiones redundantes de dos formas:

- La primera es por error, ya que se podría realizar una conexión no deseada provocando un lazo en donde los frames pueden ser duplicados permanentemente creando una baja en el rendimiento de la red.
- La segunda forma de crear enlaces de forma explicita para crear redundancia en casos de fallo de algún vínculo.

Los objetivos de STP es administrar las conexiones redundantes en la red haciendo que una sola este funcional y de esta forma evitar los lazos. En caso de fallo SPT analiza la red y habilita la conexión redundante hasta que se recupere la caída.

Este estándar se encuentra definido dentro de la norma IEEE 802.1D del año 1993, y se calcula que la demora que tiene en reestablecer el servicio es de aproximadamente 30 segundos, en la actualidad se utiliza una variante de este protocolo conocido como IEEE 802.1W conocido como RSPT (Rapid STP) que demora tan solo 5 segundos en reponer el servicio.

7.5 LINK AGGREGATION

Link Aggregatión o Agregado de Conexiones es un método

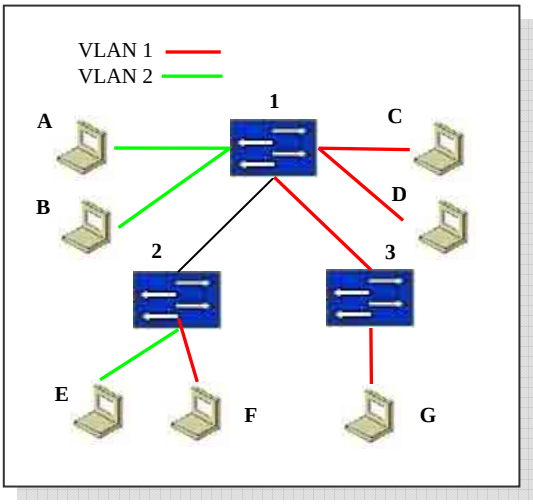
que se utiliza para agrupar varias bocas del switch y hacer que se comporten como una sola unidad.

Esto hace que este nuevo enlace se comporte como uno de mayor velocidad y proporcional a la cantidad de conexiones agrupadas.

Un ejemplo de su utilización es aplicarlo a interconexión entre Switch logrando así que se puedan agregar mas puestos de trabajo sin que se degrade el rendimiento.

7.6 VLAN IEE802.1Q

Hasta ahora hemos tratado las VLANs dentro del entorno en mismo switch, pero que sucede en grandes redes donde los switch pueden alcanzar una cantidad importante y adoptan una configuración llamada ***tree*** o árbol debido a su conexionado, tal como se ve en la siguiente figura.



Ya sabemos que las VLANs segmentan al switch y se puede hacer que dos grupos de trabajo queden separados por seguridad o por razones de rendimiento de la red.

Bajo estas circunstancias partamos de la siguiente configuración, nuestra red esta formada por el switch “1” que tiene la VLAN 1 con los puestos A y B, y la VLAN 2 con los puestos C y D.

Ahora analicemos que sucedería si quisiéramos extender nuestra red agregando al switch 2 haciendo que el puesto E pertenezca a la VLAN 1 y el puesto F lo haga a la VLAN 2.

De acuerdo a la nueva configuración y el conocimiento sobre las VLANs, el puesto A no podría alcanzar al E ya que este último no se encuentra conectado físicamente a una boca del switch 2, y este no está asociado a la VLAN 1.

Esto significa que las VLANs están confinadas a la estructura del switch.

Para solucionar este problema es que dentro de la IEEE 802.1Q también se define la forma de cómo hacerlo, para ello implementa un sistema de identificación de las VLAN mediante un sistema de marcado del frame ethernet con un sub encabezado.

El proceso de marcado es llamado ***Tagging*** (marcado), y lo detallamos a continuación la próxima figura detallando la función de cada recetor.

FRAME IEEE 802.1Q

7	1	6	6	2	2	2	42-1496	4
Preambule	SFD	DA	SA	TPID	TCI	Type Length	Data	CRC

3bits	1bit	12bits
User Priority	CFI	Bits of VLAN ID (VIDI) to identify possible VLANs

En la parte superior tenemos al frame ethernet al cual se le agrega la parte remarcada que consta de dos campos de 2 Bytes cada uno, que constan de:

- TPID: se lo conoce como Ether Type haciendo referencia al tipo de frame Ethernet, si es un frame IEEE 802.1Q / 802.1P.
- TCI (Tag Control Information - Marca de Control de Información) tiene una extensión de 2 Bytes que a su vez se encuentra dividido en tres partes:
  - Los primeros 3 bits pertenecen al User Priority (Prioridad de usuario) y se utilizan para determinar la forma en que se implementará el protocolo IEEE 802.1P que se encarga del manejo y priorización del tráfico en la red.
  - El próximo bit llamado CFI (Canonical Format Indicator – Indicador de Formato Oficial) y es utilizado para brindar compatibilidad con otra tecnología de switch, solo tiene dos valores posibles, cuando es 0 indica que es un Ethernet switch y si es un 1 es Token.
  - La última sección corresponde al identificador de la VLAN ID (VLAN Identification), esta dispone de 12 bits para determinar redes virtuales, con estos bits podemos crear un total de 4096 VLANs de las cuales sólo se pueden utilizar 4094 ya que la 0 y la 4096 están reservadas.

Como podemos apreciar esta última sección es la encargada de marcar con un número único a todos los frames que circulen a través de las bocas de los switch.

Para que este proceso (marcado de frame) se ponga en marcha es necesario que el administrador marque a la boca (por donde se pretende enviar los frames marcados) con la identificación de la VLAN deseada. De esta forma el frame podrá salir por esta boca seleccionada, llegara al siguiente switch y este lo desmarcara antes de entregarlo al puesto de trabajo.

Volviendo al escenario anterior, si deseamos que una misma boca pueda transportar frames de distintas VLANs, será necesario repetir el proceso de marcado de la boca nuevamente, pero esta vez con las identificaciones correspondientes a las otras VLANs.

7.7 CALIDAD DE SERVICIO

La Calidad de servicio ***QoS*** (Quality of Service) en redes IP puede implementarse en las capas de 2, 3 y 4 del modelo OSI y su misión es asegurar que en la red haya un ancho de banda específico y que los datos sean entregados con un mínimo retardo.

Para lograr este objetivo desde la capa 2 del modelo OSI disponemos de las VLANs + Tagging , recordemos que dentro del sub encabezado de tagging tenemos al sector TCI y los primeros 3 bits de este pertenecen al User Priority que se encarga de la priorización del trafico.

Los problemas resuelve son:

- Latencia: son la suma de todos los retardos que se acumulan antes de la entrega de un frame al destinatario.
- Retardos: demoras producidas por cables, dispositivos (Hub / Swich / NICs), tipo de envío (Store and Forward), procesamiento de la información (CRC, etc).
- Jitter (fluctuaciones): el una variación indeseable de los tiempos de retardo.

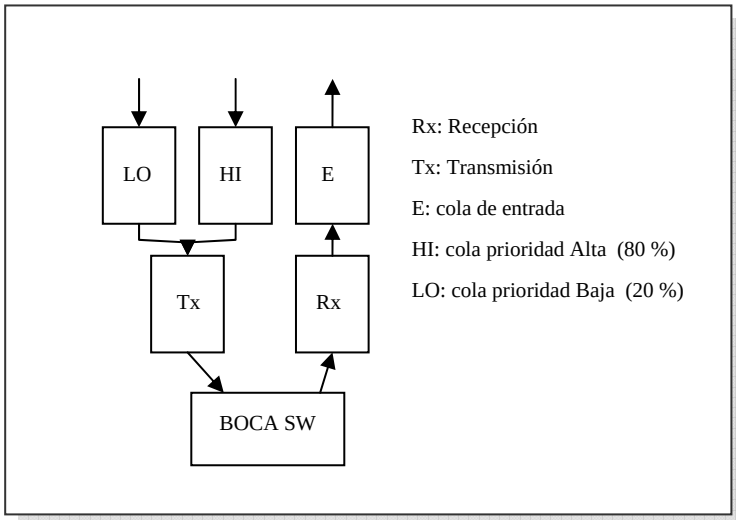
La calidad de servicio que se resuelve en capa 2 se la conoce con el nombre de ***CoS*** (Class of Service – Clase de Servicio) y esta definida en la norma IEEE 802.1P (incluida en la IEEE 802.1Q).

Para poder llevara acabo esta tarea requiere de hardware adicional llamado memoria Buffer o Cola Cache que significa lo mismo, estas memorias tienen la tarea de almacenar suficiente información (cantidad asignada previamente) para luego entregarla en forma regular y fluida, evitando así el efecto Jitter.

Las colas de cache existen en dos tipos, la de entrada y las de salida que normalmente son 2, una con prioridad baja y otra alta, ambas se encuentran en las entradas y salidas de todas las bocas que tiene el switch.

Esta configuración de colas cache es el ejemplo más simple y disponible en el mercado de los switch, esto significa que cada fabricante puede implementar variaciones sobre este tema para mejorar su producto, pero no la forma en la cual se controla.

En la próxima figura podemos ver un esquema simplificado de esta configuración de colas, donde la cola E de entrada se vacía de acuerdo a la Prioridad de Usuario (3 bits) que nos proporcionan 8 niveles posibles, desde 0 alta prioridad hasta 7 con baja prioridad.



Las colas de salida podemos ver que ya tienen asignados valores de 80 y 20 % respectivamente, esto significa que volcaran sus contenidos cuando el volumen de datos lleguen a los niveles establecidos, en este caso y a diferencia del anterior es el administrador quien define la prioridad de para salir en cada boca del switch.

Para finalizar podemos decir que todo lo visto es un poco de lo que se ofrece en el mercado, ya que algunos fabricantes desarrollan nuevas aplicaciones o mejoran las existentes haciendo combinaciones de productos líneas tope con la media a precios mas que razonables, permitiéndonos así crear mejores redes a costo razonable.

Estándares y Cumplimientos	
Nomenclatura IEEE	**Servicio**
802.1d	Bridging 1ª versión
802.1D	Bridging + Spanning Tree Protocol 2ª version
802.1p	Class of Service
802.1P	Traffic filtering,
802.1Q	VLAN Bridge
802.1w	Rapid Spanning Tree
802.1x	Port-based network access control
802.3	10T Ethernet
802.3ab	1000T
802.3ac	VLAN tag frame extension
802.3ad	Link Aggregation (static) Trunk
802.3u	100TX Ethernet
802.3x	Flow Control
802.3z	1000SX

NOTAS

CUESTIONARIO CAPITULO 05

1.- ¿Cuál es la unidad de información que se utiliza en la capa de enlace de datos?

2.- ¿Cuál es el objetivo del protocolo CSMA/CD?

3.- ¿Qué dispositivo me permite utilizar la comunicación Full Duplex? ¿Por que?

4.- ¿Qué funciones especiales puede nombrar de un Swich?

5.- ¿Para que sirve marcar un frame (Tagging)?