REDES DE AREA LOCAL

LAN's Conmutadas y VLAN's

REDES LAN’s

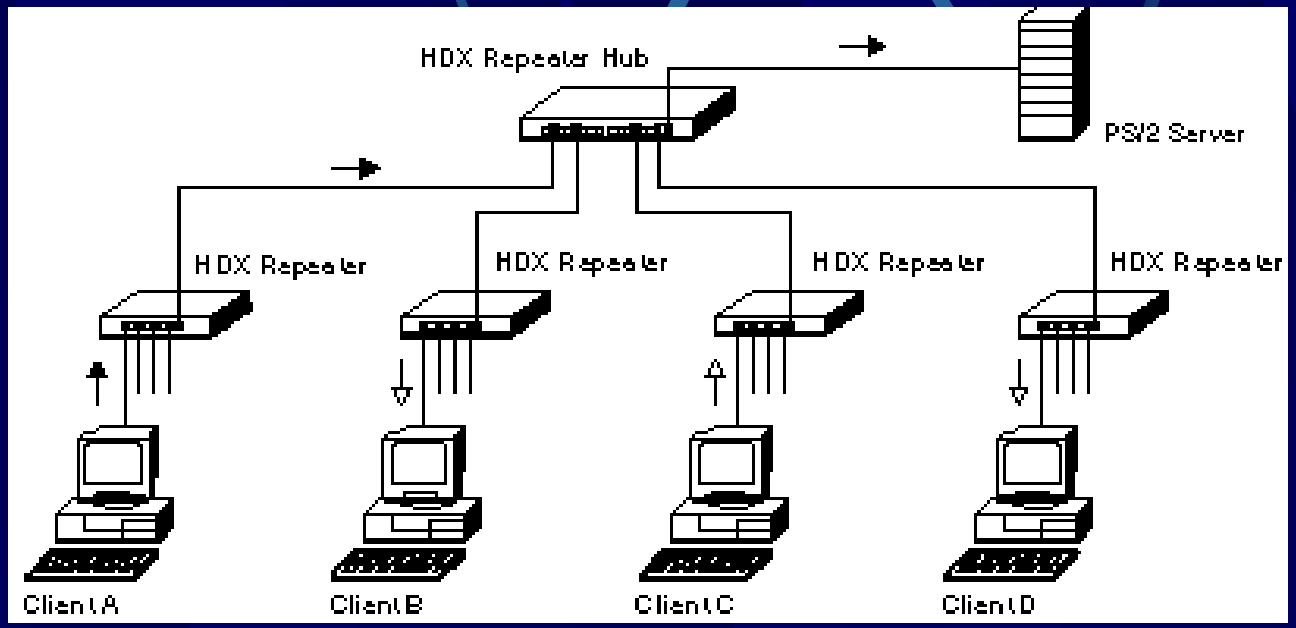
- Redes LAN Conmutadas
- VLAN´s.
- Discusión de Casos

LAN’s CONMUTADAS: TEMARIO

- Revisión de conceptos y motivación.
- Concepto de una red conmutada.
- Función básica de un switch (conmutador): filtrado de tráfico.
- Revisión del concepto de puente y filtrado de tráfico
- Redundancia. Algoritmo de Arbol de Extensión (Spanning Tree Protocol)
- Arquitectura de Switchs (conmutadores): Modo de trabajo
- Agrupación de Tráfico (trunking)

REVISION DE CONCEPTOS: LAN's compartidas

Las Redes de Area Local convencionales, usualmente se basan en tecnología en ethernet y se disponen Hub's (concentradores) para materializar la estrella:



REVISION DE CONCEPTOS: LAN’s compartidas

En este tipo de redes se compite por el acceso al medio y el ancho de banda se comparte entre todos los equipos del segmento.

- El *Dominio de Colisión* o segmento es único, ya que se extiende a todos los puestos de la red.
- El *Dominio de Difusión (Broadcast)* también es único.

REVISION DE CONCEPTOS: LAN’s compartidas

Suelen aparecer dos tipos de problemas:

- Incremento de las colisiones
- Cuellos de botella en el acceso a servidores

REVISION DE CONCEPTOS: LAN’s compartidas

Además se tornan difíciles para administrar.

No es sencillo aislar Sistemas Operativos heterogéneos.

Pueden aparecer problemas de seguridad.

LAN's CONMUTADAS

Qué soluciones posibles se pueden plantear para mejorar este problema?

- Segmentar o subdividir las redes, de manera física o de manera lógica.
- Filtrar tráfico: disponiendo puentes (bridges) o Switchs (conmutadores).
- Debemos cuidar el acceso a los servidores en cualquiera de las soluciones posibles.
- No olvidemos revisar el cableado existente.

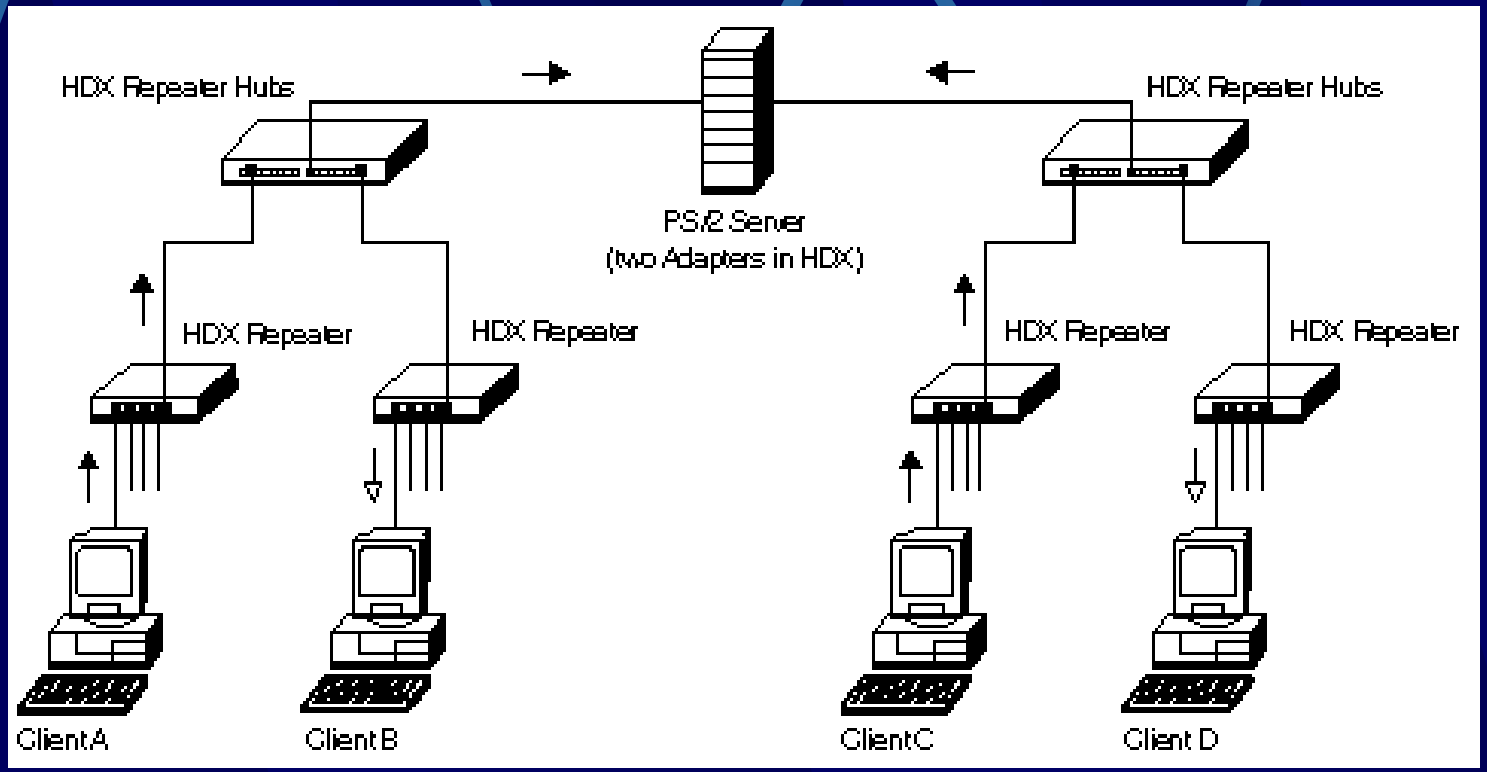
Segmentado físico y lógico de LAN´s

Como segmentamos las redes?

- Segmentado físico
- Segmentado lógico

LAN's: Segmentado físico

Se puede hacer de dos formas totalmente distintas: dividiendo directamente los segmentos, perdiendo así conectividad, en lo que se denomina un segmentado físico.



LAN’s: Segmentado lógico mediante routers

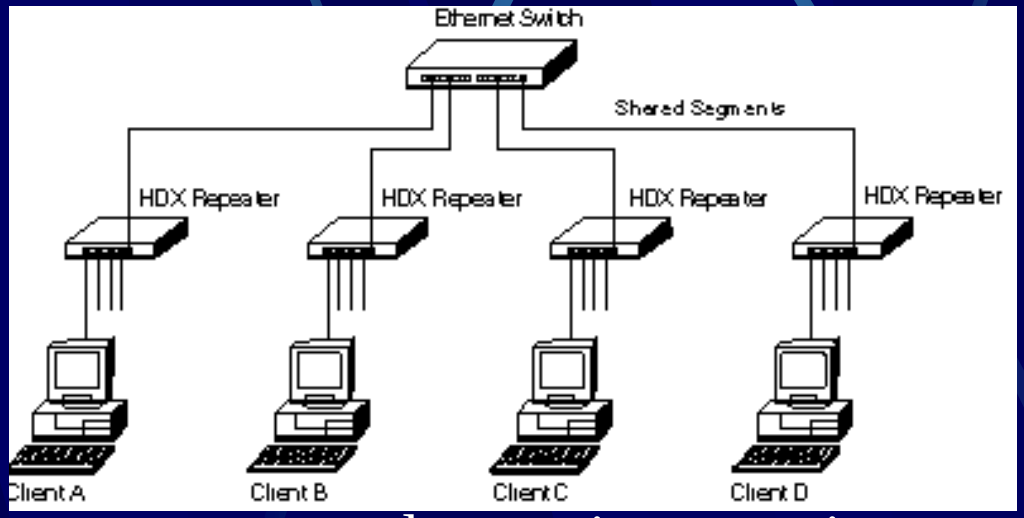
• Otra opción es disponer equipos que segmenten o aíslen los dominios de colisión y de difusión.

• En estos casos los routers pueden ser adecuados. Con un PC de bajo costo, dos placas de red y S.O. Linux se pueden materializar este tipo de routers de bajo costo.

• Inconvenientes: posible lentitud en la red, dificultad en el acceso a los servidores.

LAN's: Segmentado lógico mediante Switchs (conmutadores):

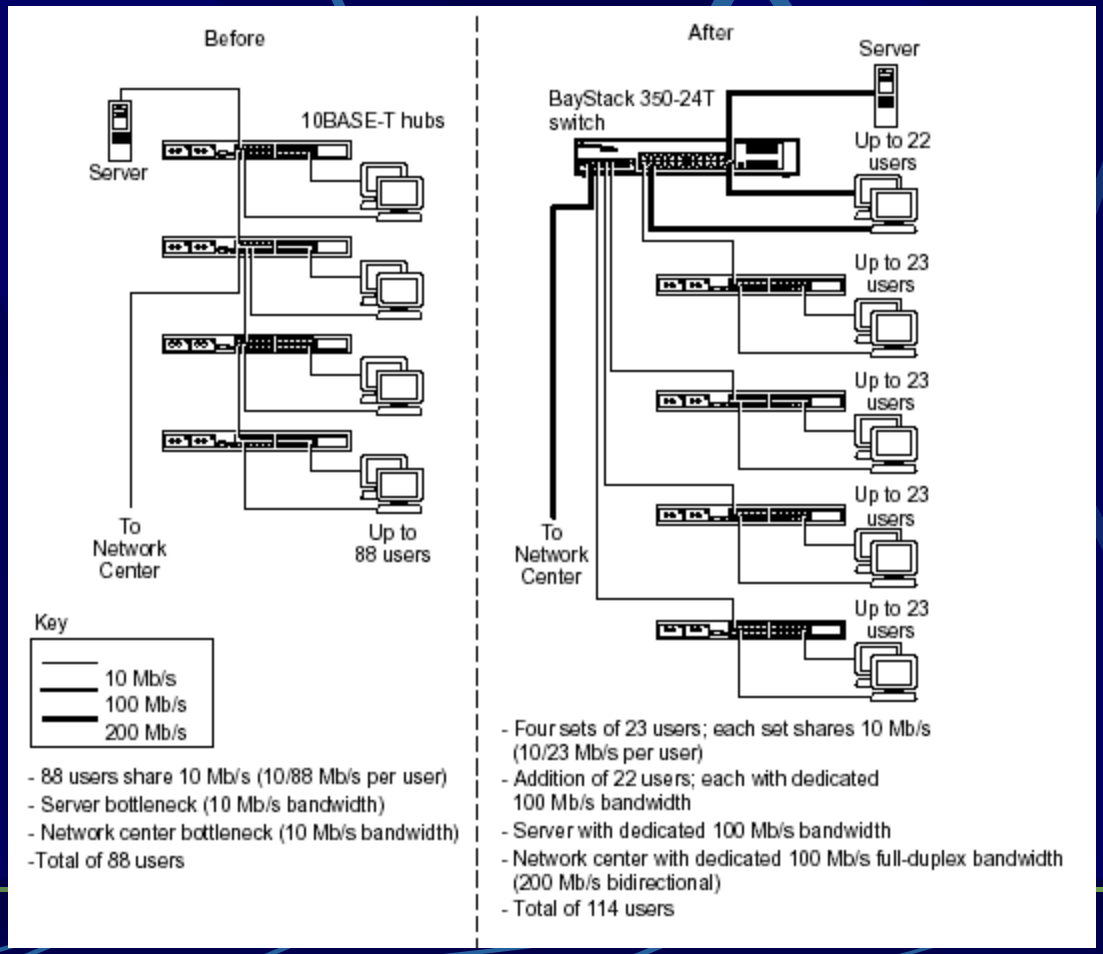
Una alternativa importante es reemplazar los hubs por Switchs (conmutadores). De esta manera se filtra buena parte del tráfico de la red y se pueden lograr aumentos en el rendimiento de la misma.



Sin embargo permanecen algunos inconvenientes: el dominio de difusión es único.

Ejemplo de LAN conmutada

Evolución de una red compartida a red conmutada.



LAN's CONMUTADAS: Switchs (conmutadores):

Qué es un switch (conmutador)?

Esencialmente es un equipo que funciona como un bridge (puente), pero que agrega otras prestaciones.

En general un switch (conmutador)permite:

• Controlar y disminuir el número de colisiones, subdiviendo los segmentos.

•**En particular con un switch (conmutador) se puede:**

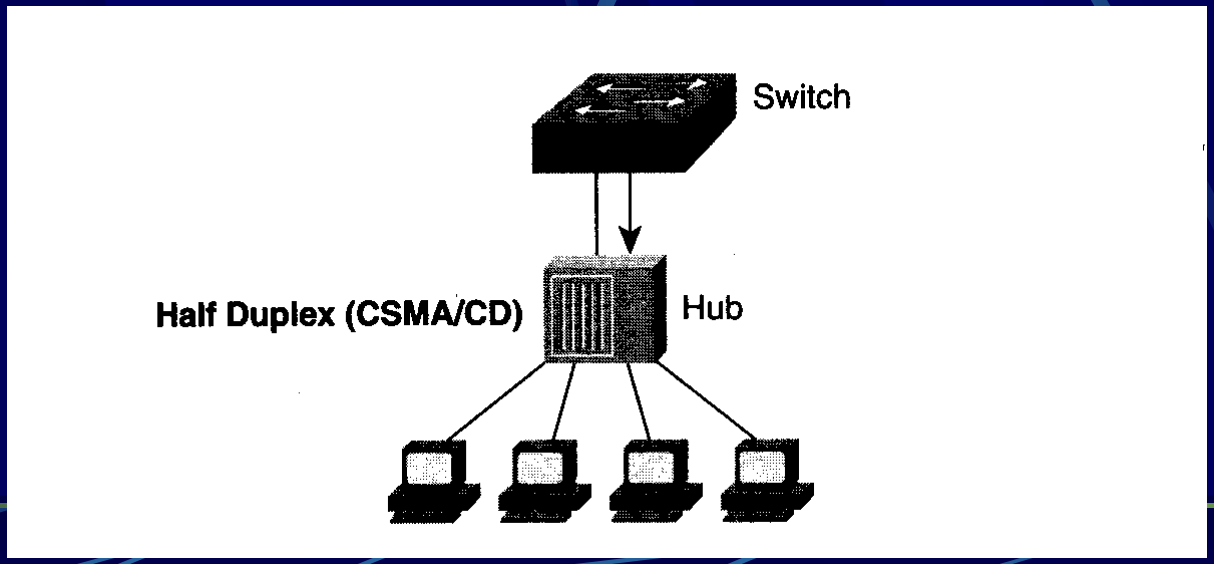
• Administrar el ancho de banda, garantizando un mejor acceso a servidores u otros Switchs (conmutadores): mediante la agrupación de conexiones (aggregation link).

• Permiten aislar tráfico de difusión mediante las llamadas redes virtuales o VLAN's.

Modos de Transmisión de un Switch (conmutador)

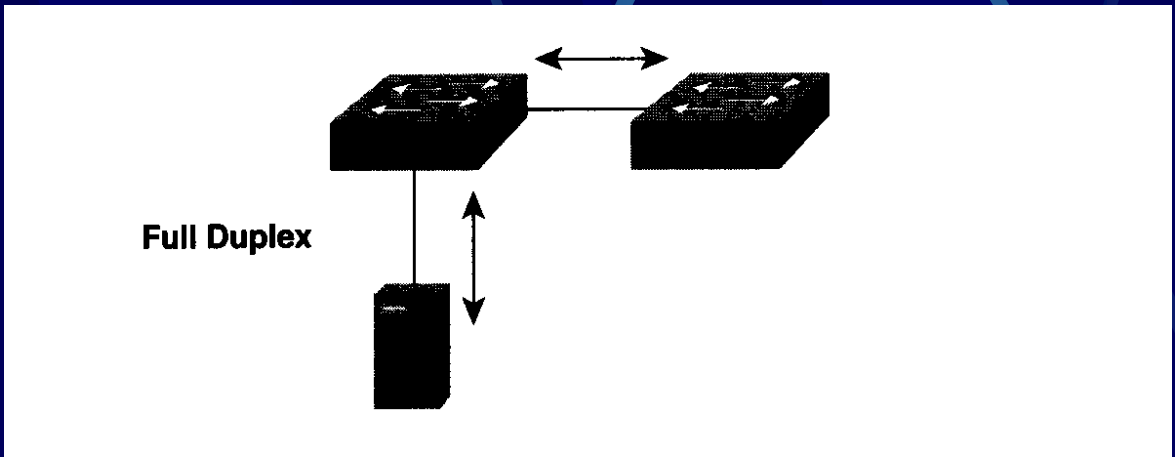
Los puertos de un switch (conmutador) pueden funcionar en modo Half Duplex o Full Duplex, según el equipo o estación que este conectado al mismo.

Recordemos que en el modo half duplex se compite por el acceso al medio y pueden ocurrir colisiones.



Modos de Transmisión de un switch (conmutador):Full Duplex

El modo full duplex se implementa cuando solo hay dos dispositivos conectados y el enlace trabaja en modo punto a punto



Modo de Transmisión Full Duplex: Posibilidades

Esta posibilidad (enlace punto a punto) brinda gran flexibilidad para diseñar redes.

Puede conectarse de ese modo una estación, un servidor u otro switch.

Para tomar ventaja de esta característica la placa de red de la estación o equipo conectado al switch debe funcionar en modo FDX. En este caso desaparecen las colisiones y no es necesario emplear CSMA/CD.

Sin embargo, si la otra placa no habla FDX se produce un dominio de colisión!!!

Modo de Transmisión Full Duplex: Ventajas

Una ventaja de evitar el modo CSMA/CD es que se pueden extender los límites al diámetro de la red debido a que ya no se deben detectar colisiones.

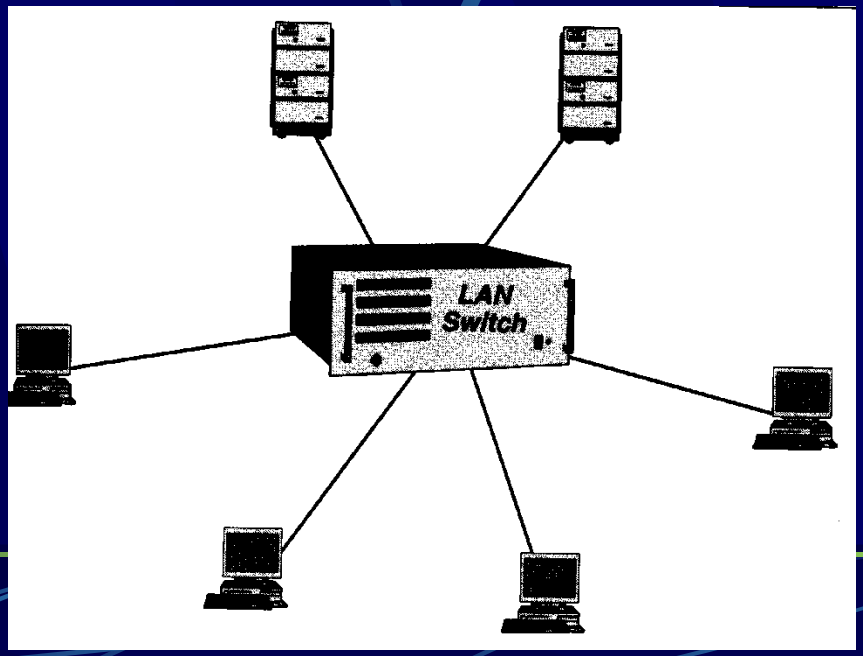
Por ejemplo en F.O., bajo las normas 10Base FL o bien 100 Base FX, se puede pasar de 400 m (HDX) a 2 km en modo FDX.

Modos de Transmisión Full Duplex: Ejemplos

Esta posibilidad (enlace punto a punto) brinda gran flexibilidad para diseñar redes.

Puede conectarse de ese modo una estación, un servidor u otro switch. A este tipo de disposición se la llama *microsegmentación.*

Se denomina microsegmentación al segmento constituido por la boca del switch y una estación u otro tipo de equipo



Modos de Transmisión de un switch (conmutador):Full Duplex

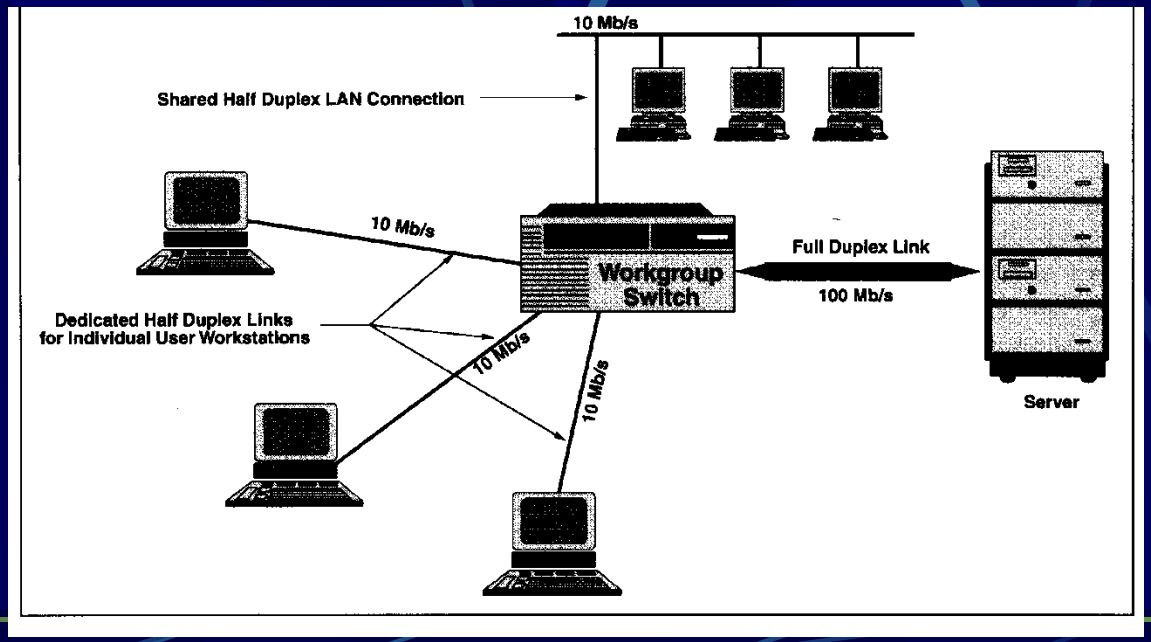
Es importante destacar que al haber solo dos equipos en los extremos el enlace ahora es dedicado, trabaja en forma de punto a punto.

Notemos que estamos aplicando en la LAN una idea, el enlace punto a punto, y un equipo, el conmutador, típicos de las redes WAN.

Modos de Transmisión Full Duplex

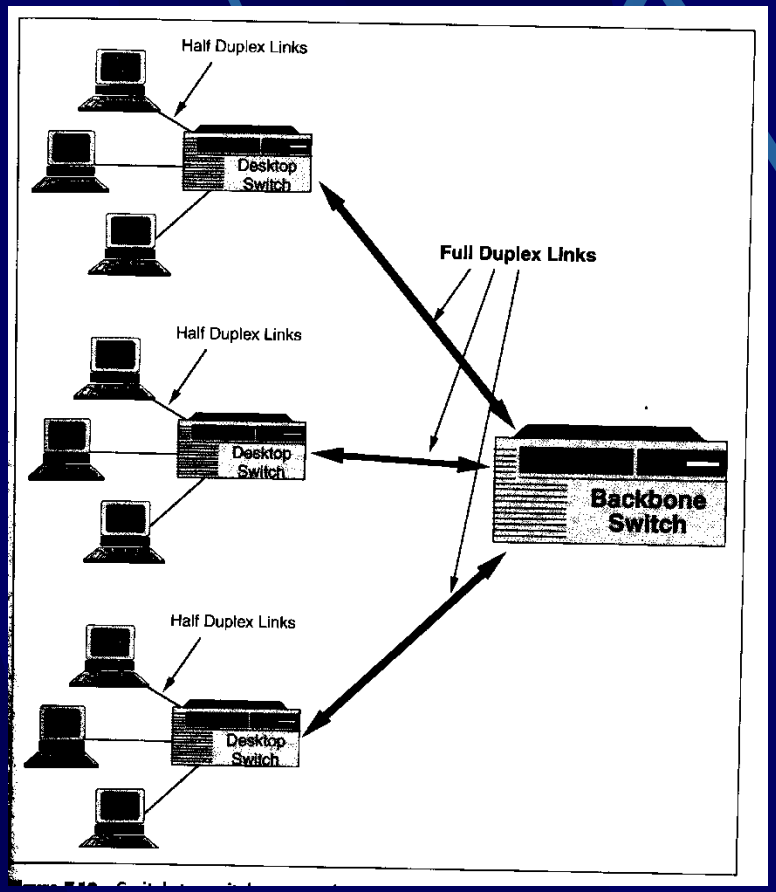
El modo full duplex se puede utilizar para garantizar ancho de banda en el acceso a servidores, enlaces entre switchs y acceso a estaciones críticas (power users)

Ejemplos:



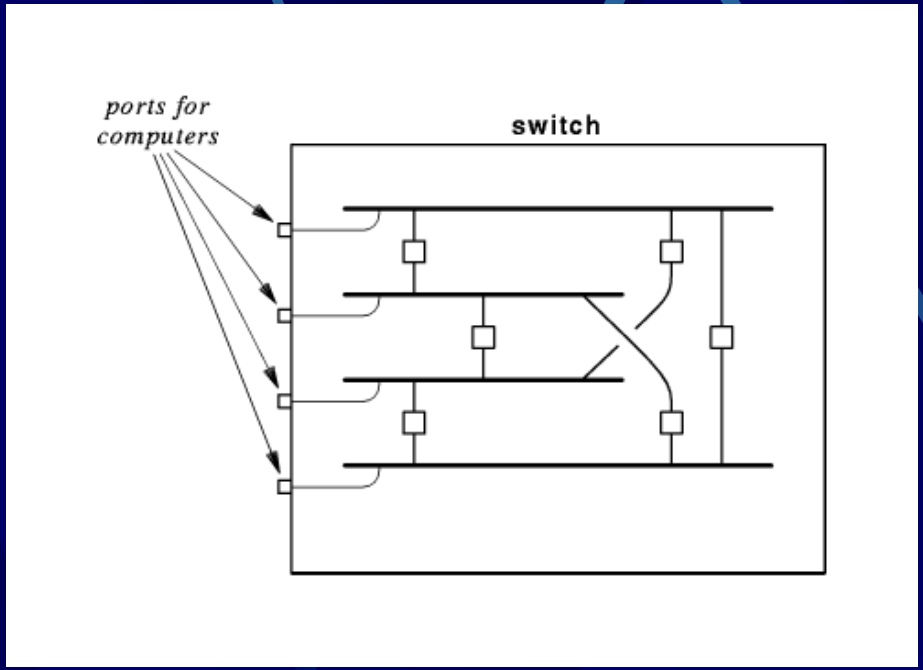
Modos de Transmisión Full Duplex: Ejemplos

Otra situación en donde se debe utilizar full duplex es en la conexión (backbones) entre Switchs (conmutadores):



LAN's CONMUTADAS: switchs (conmutadores):

Además de filtrar tráfico, función esencial de un bridge, un switch (conmutador) permite realizar transmisiones en paralelo:



Se materializan circuitos virtuales de alta velocidad y muy corta duración.

Switchs (conmutadores): Filtrado de tráfico

Un switch (conmutador) es como un Bridge, su función esencial es el filtrado de tráfico.

Esta tarea la realiza analizando los marcos de hardware, por eso se dice que un switch (conmutador) es un equipo de capa 2.

Para llevar a cabo el filtrado de tráfico un switch (conmutador) debe realizar una serie de tareas básicas.

Switchs (conmutadores): Tareas básicas del Filtrado de tráfico

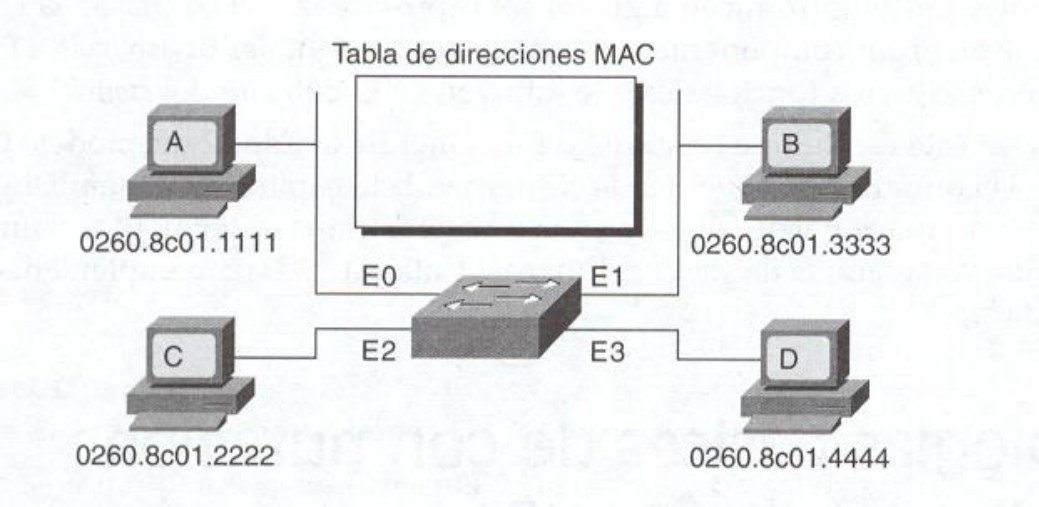
- Aprender direcciones de los dispositivos conectados a cada uno de sus puertos. Recordemos que en un puerto de un switch (conmutador) pueden conectarse una estación, un hub, o bien otro conmutador.
- Rechazar los marcos que tienen como destino el propio puerto (es decir aquellos que comparten un mismo dominio de difusión)
- Controlar la integridad de los marcos recibidos.

Switchs (conmutadores): Tareas básicas del Filtrado de tráfico

- Si el marco es correcto y no posee como destino una estación asociada a ese puerto, reenvía la trama.
- Para ello localizar el puerto de destino en la Base de Datos y enviar la trama solo a ese puerto

Switchs (conmutadores): Aprendizaje de direcciones

Al encender un switch la tabla de direcciones esta vacía



No se pueden tomar decisiones !!!

El switch debe retransmitir la trama entrante a todos los puertos, mecanismo conocido como inundación

Switchs (conmutadores): Aprendizaje de direcciones

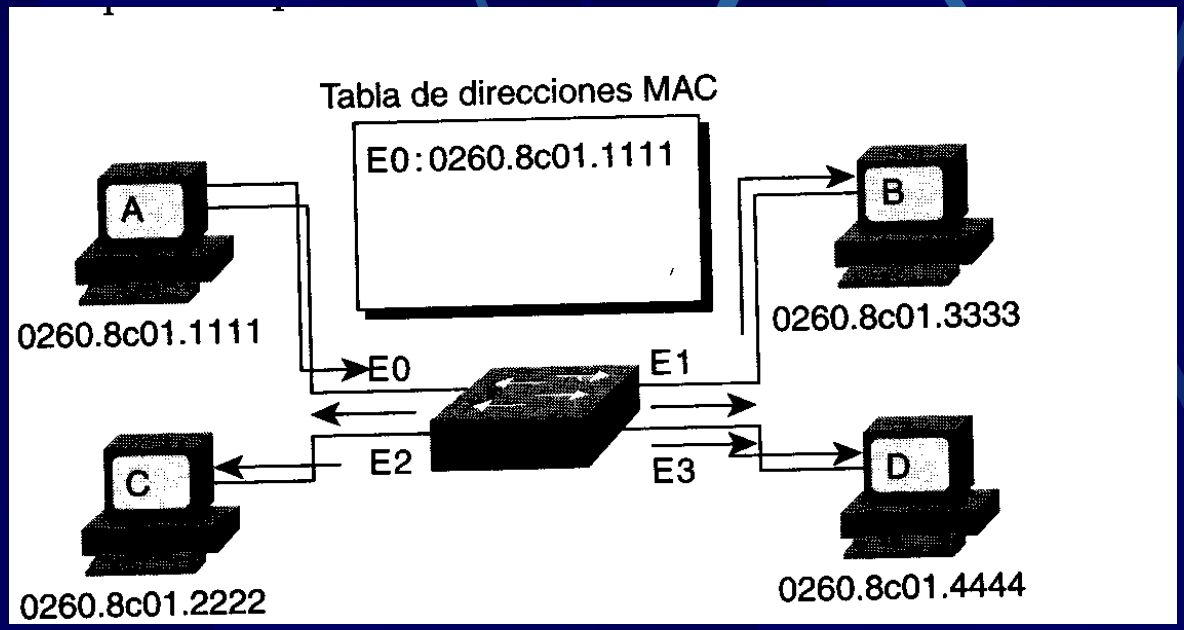
Inundar es costoso en términos de ancho de banda

Deben implementar buffers de memoria para que puedan recibir y transmitir tramas de manera independiente para cada puerto o segmento

Switchs (conmutadores): Aprendizaje de direcciones

Cómo aprende una dirección un switch?

Supongamos que el puesto A con dirección 0260.8c01.1111, quiere hablar con el puesto C, con dirección 0260.8c01.2222



Switchs (conmutadores): Aprendizaje de direcciones

Paso 1: La trama se recibe en el puerto E0 y se almacena en memoria temporal

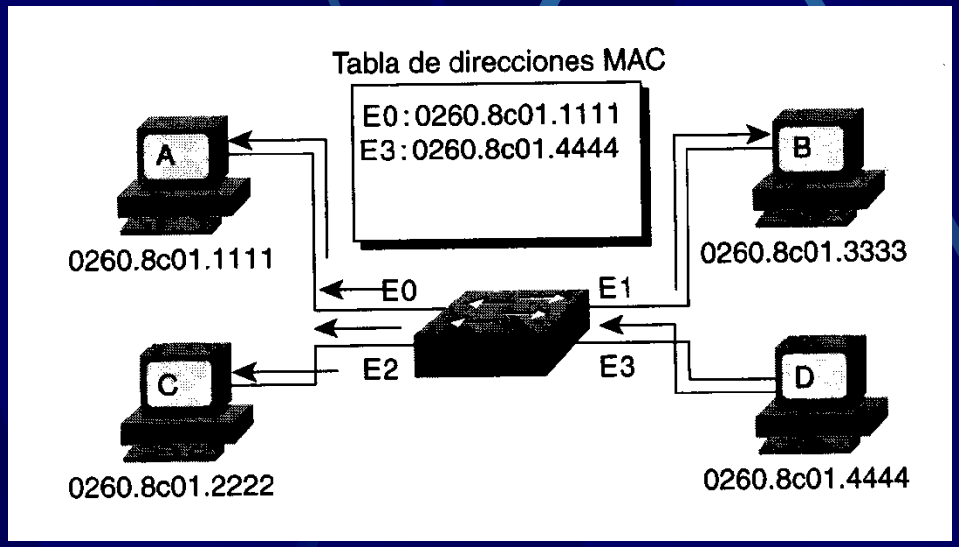
Paso 2: El switch no conoce la interfaz del puerto de destino e inunda toda la trama.

Paso 3: Mientras inunda la trama aprende la dirección MAC de E0 y la asigna a la base de datos

Paso 4: La dirección pasa a memoria cache y se la descarta si no se la actualiza en un intervalo de tiempo dado.

Switchs (conmutadores): Aprendizaje de direcciones

El proceso de aprendizaje continua a medida que aparece tráfico: El puesto D con dirección 0260.8c01.3333 envía una trama al puesto C con dirección 0260.8c01.2222



Switchs (conmutadores): Aprendizaje de direcciones

Qué tareas hace el switch en este caso?

Paso 1: La dirección de origen 0260.8c01.4444 se añade a la tabla de direcciones MAC

Paso 2: Se compara la dirección de destino (Puerto C) con las entradas en la tabla.

Paso 3: Si no existe asignación para este puerto se deben inundar todos los puertos con la trama (Broadcast), excepto el puerto por donde entró la trama

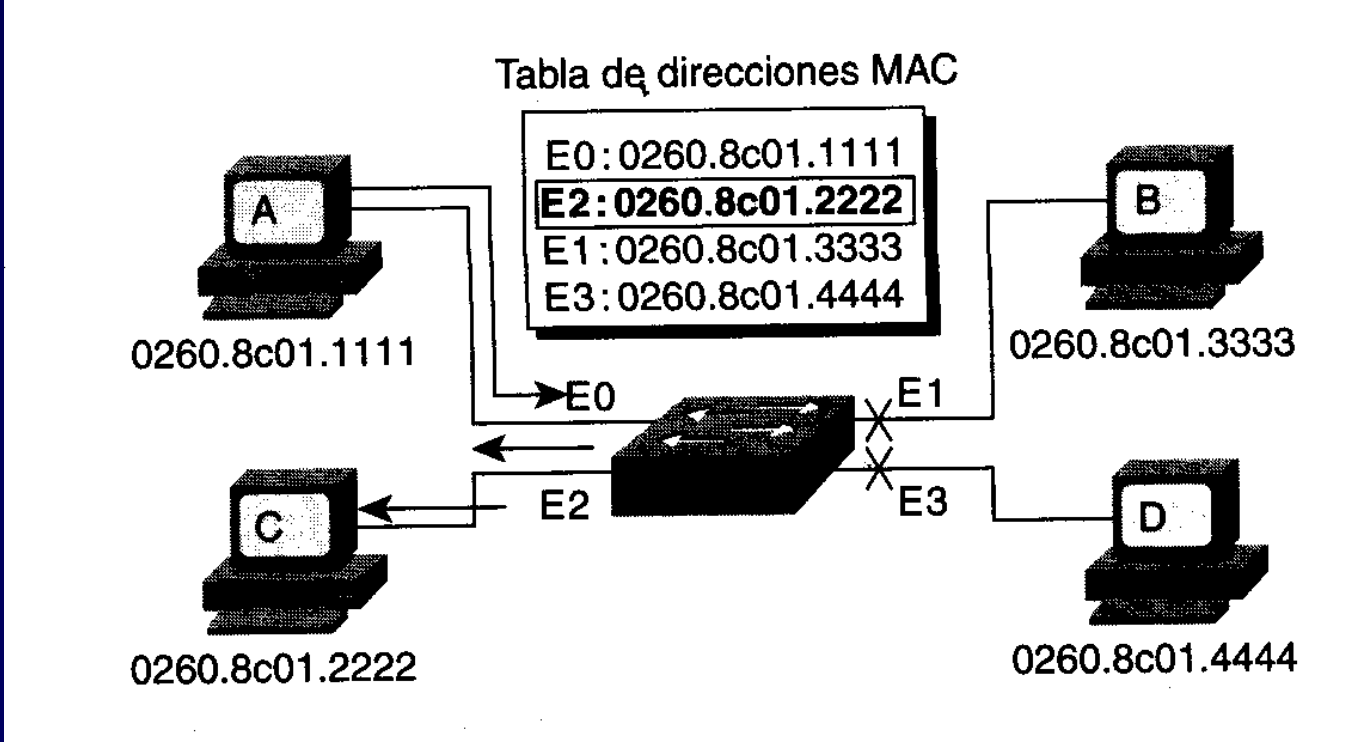
Paso 4: Cuando el puesto C envía la trama de vuelta al puesto A. El switch aprende también la dirección Mac del puesto C en la interfase E2.

Paso 5: se completa la tabla y se actualiza periódicamente

Switchs (conmutadores): Transmisión

Una trama, conocidos el puerto de origen y destino, solo se transmite al puerto de destino y no a los demás

Trama desde A hacia C



Switchs (conmutadores): Filtrado de Tramas

Para cumplir con el objetivo anterior, el switch realiza las siguientes operaciones:

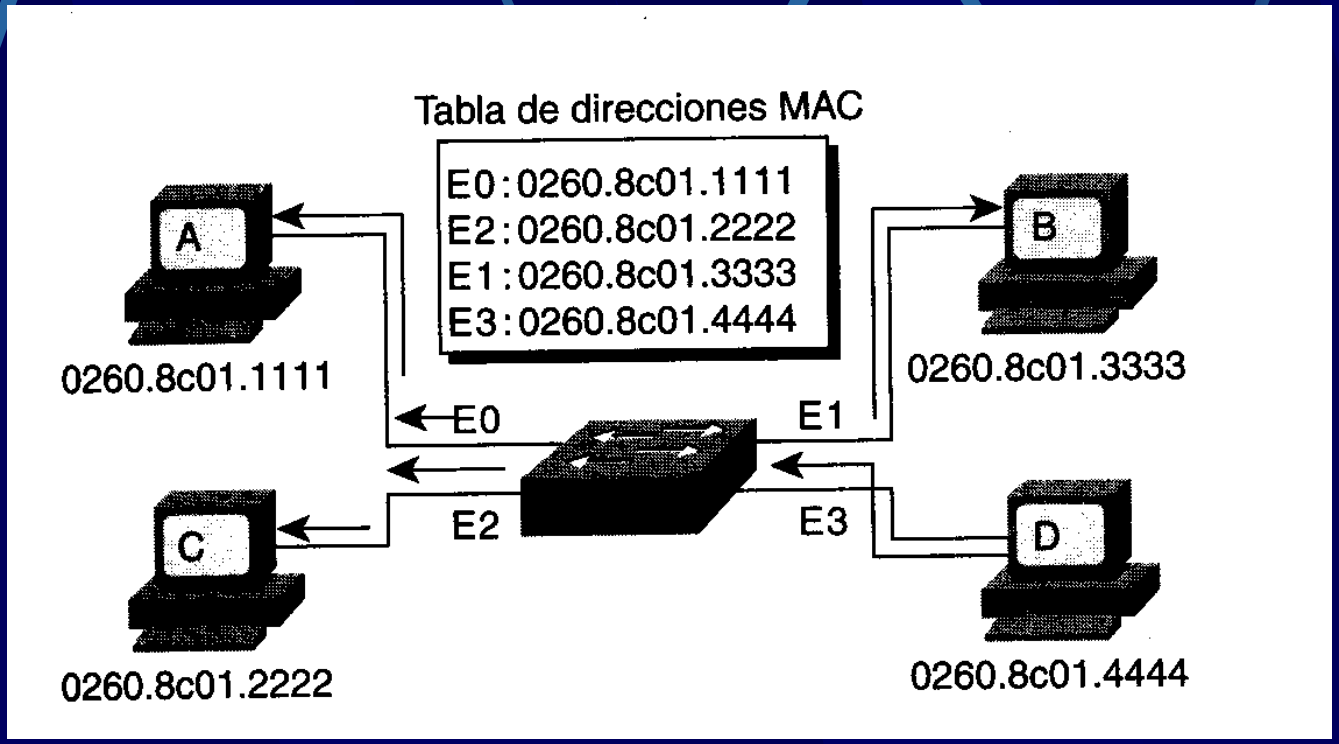
Paso 1: Se compara la dirección MAC de destino 0260.8c01.2222, con las entradas en la tabla.

Paso 2: Cuando el switch la encuentra solo la envía el puerto correspondiente, en este caso E2.

Paso 3: el switch no retransmite la trama ni a E1 ni a E3, operación conocida como Filtrado de Tramas.

Switchs (conmutadores): Difusión

Si el puerto D envía una trama de difusión o multidifusión, el switch la reenvía a todos los puertos menos al que la origina.



LAN’s CONMUTADAS: Electrónica de un Conmutador

Además de filtrar las tramas, tarea esencial, los switchs son capaces de mantener más de una conexión a la vez.

Habíamos dicho: circuitos virtuales de muy alta velocidad y de muy corta duración!!

Desde el punto de vista de la Ing. de Sistemas o Ingeniería de Redes sería suficiente pensarlos como una especie de caja negra de alta capacidad.

Sin embargo conviene revisar su electrónica y modo de funcionamiento para conocer los parámetros a exigir para una eventual compra.

LAN’s CONMUTADAS: Electrónica de un Conmutador

Un switch (conmutador) descansa en los siguientes elementos fundamentales:

- Puertos
- Plano posterior o backplane: permite la conexión de los puertos materializando los circuitos virtuales
- CPU

LAN’s CONMUTADAS: Puertos de un Conmutador

Los puertos de un switch (conmutador) moderno son RJ-45, que operan en modo autosense a 10/100 Mbits y pueden funcionar en modos half-duplex o full-duplex.

Cada vez es más común encontrar equipos que trabajan a Gigabit (1000 Mbits/s)

Cada puerto, a lo sumo cada dos puertos, existe un chip especial, llamado ASIC que realiza las funciones esenciales que hemos visto en las filminas anteriores.

LAN’s CONMUTADAS: Chips ASIC

Los chips ASIC (Application Specific Integrated Circuits) se diseñan especialmente para cumplir determinadas funciones a nivel de hardware que evitan recurrir al software y a la CPU del equipo.

Estos chips son prácticamente imposibles de actualizar y son, en gran medida, responsables de la obsolecencia del equipo.

Estos chips poseen distintas formas de trabajo para analizar y reenviar los marcos entrantes.

Switchs (conmutadores):Modos de reenvío de marcos

Existen tres modos tradicionales de trabajo:

- Almacenamiento y Reenvío (Store and forward)
- Modo de corte (Cut-Through)
- Libre de Fragmentos (Fragment free)

En general cada switch (conmutador) utiliza uno de ellos por defecto, pero puede cambiarlo en la práctica o alterarse por software

Switchs (conmutadores): Modos de reenvío de marcos

Los switchs (conmutadores) más económicos trabajan con el modo Store & Forward (Almacenamiento y reenvío).

Los switchs (conmutadores) más avanzados o más costosos utilizan los otros dos modos.

En general cada switch (conmutador) utiliza uno de ellos por defecto, pero puede cambiarlo en la práctica o alterarse mediante el Sistema Operativo.

Switchs (conmutadores): Concepto de Latencia

Asociado al modo de reenvío de las tramas está el concepto de latencia.

Se define la *latencia* como el retraso ocasionado por un dispositivo en la red. En general se mide como el tiempo transcurrido entre la entrada y la salida del primer bit. El modo de guardar y reenviar lo mide de forma distinta.

Switchs (conmutadores): Modos de reenvío de marcos

Almacenamiento y Reenvío (Store and fordward)

Cuando el switch opera en este modo debe almacenar toda la trama antes de reenviarla.

Se siguen los siguientes pasos:

- Se leen las direcciones de origen y destino
- Se aplica el control de redundancia cíclica (CRC)
- Se aplican los filtros apropiados
- Si corresponde se retransmite la trama

La latencia se mide en este caso como el tiempo transcurrido entre la llegada del último bit y la salida del primero.

Switchs (conmutadores): Modos de reenvío de marcos

- Modo de corte (Cut-Through)

En este modo de trabajo el switch lee la cabecera del marco y comienza a retransmitir. Incluso en algunos casos solo lee la dirección de destino.

El retraso es mínimo y además es constante (tiempo para leer la cabecera).

Sin embargo, como no controla la integridad de los marcos, puede reenviar marcos inválidos con las consecuentes pérdidas de tiempo.

Si el switch detecta muchos errores puede cambiar al modo de almacenar y reenviar.

Switchs (conmutadores): Modos de reenvío de marcos

- Sin Fragmentos (Fragment free)

En este modo de trabajo el switch lee los primeros 64 bytes antes de retransmitir la trama.

Usualmente las colisiones afectan a los primeros 64 bytes, con lo cual la información contenida en los mismos es suficiente para decidir la validez del marco.

Electrónica de un Switch (conmutador):Backplane

El plano posterior o backplane, también llamado switching fabric es el elemento en el cual se materializan los circuitos que permiten enviar los marcos de hardware de un puerto a otro.

Existen diferentes tecnologías:

Memoria compartida

Bus compartido

Matriz de conmutación

Backplane de un switch (conmutador):Memoria compartida

Como su nombre lo indica es un área de memoria compartida por todos los puertos, en la que se almacenan los marcos recibidos.

Una tabla asocia los marcos con los puertos de destino. La demora o latencia que introduce el switch esta asociada a los tiempos de lectura y escritura de dicha memoria.

Es la tecnología menos costosa pero suele tener limitaciones de ancho de banda.

Backplane de un switch (conmutador): Bus compartido

En este caso existe un bus compartido por todos los puertos que se utiliza para comunicar a los diferentes puertos entre si.

El bus debe accederse de a una vez para enviar los diferentes mensajes, con lo cual debe arbitrarse su empleo. De alguna manera es semejante a CSMA/CD.

Esta tecnología es buena para multicast o broadcast.

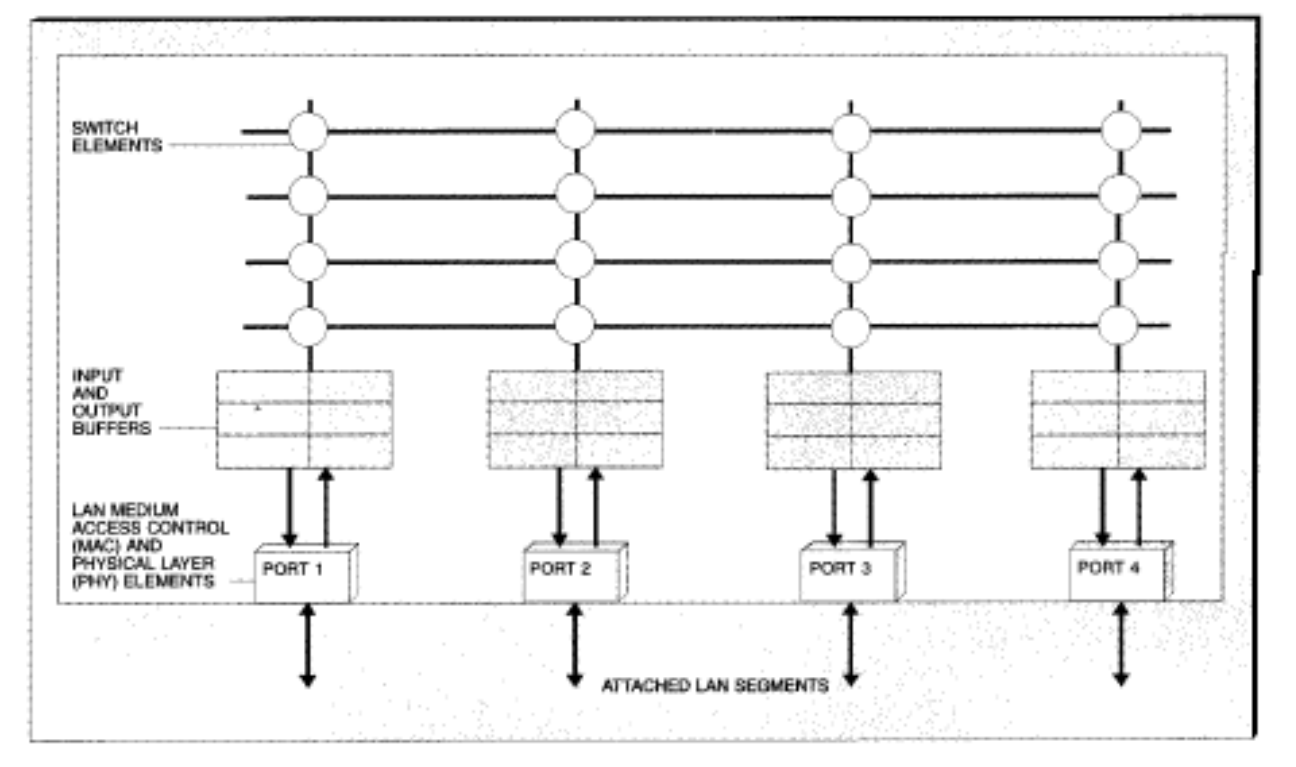
Backplane de un Switch (conmutador): Matriz de conmutación

Se disponen dos planos ortogonales que permiten unir los diferentes puertos mediante una matriz de Switchs (conmutadores): electrónicos que permiten establecer por períodos de tiempo muy cortos los circuitos necesarios para transmitir los distintos marcos de hardware.

Existen dos inconvenientes: el tráfico de multicast y los cuellos de botella cuando se carga demasiado tráfico a un solo puerto de destino

Poseen gran ancho de banda.

Backplane de un switch (conmutador):Matriz de conmutación



Backplane de un Switch (conmutador):Matriz de conmutación

Existen arquitecturas del tipo blocking y non-blocking.

Las primeras permiten tráfico en paralelo y no impiden transmisiones simultáneas: ej crossbar y banyan

Si el switch (conmutador)admite algún tipo de colisión interna entonces pertenece al segundo caso. Ej; bus compartido.

Switch (conmutador): Funciones de la CPU

Además de los puertos (y los correspondientes chips ASIC) y el backplane que permite la interconexión de los mismos, el tercer elemento importante del hardware es la CPU.

La CPU es la encargada del arranque del equipo y de administrar tareas centralizadas que involucran a todos los puertos.

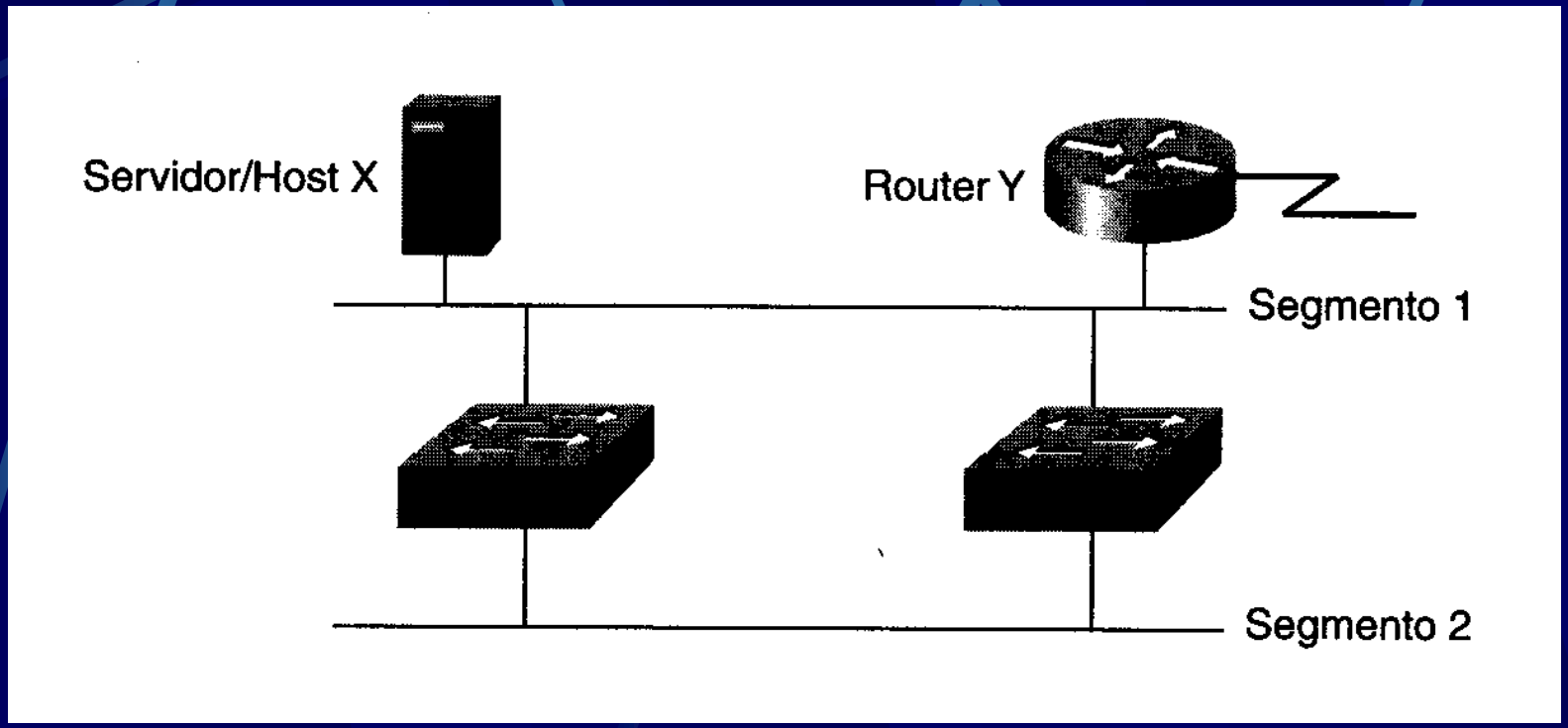
Entre otras tareas pueden citarse la administración vía SNMP, el algoritmo de spanning tree, etc.

Switchs (conmutadores): Funciones avanzadas

- Redundancia y bloqueo de bucles: Algoritmo de árbol de extensión.
- Agrupación de tráfico
- VLAN’s

Switchs (conmutadores): Enlaces redundantes

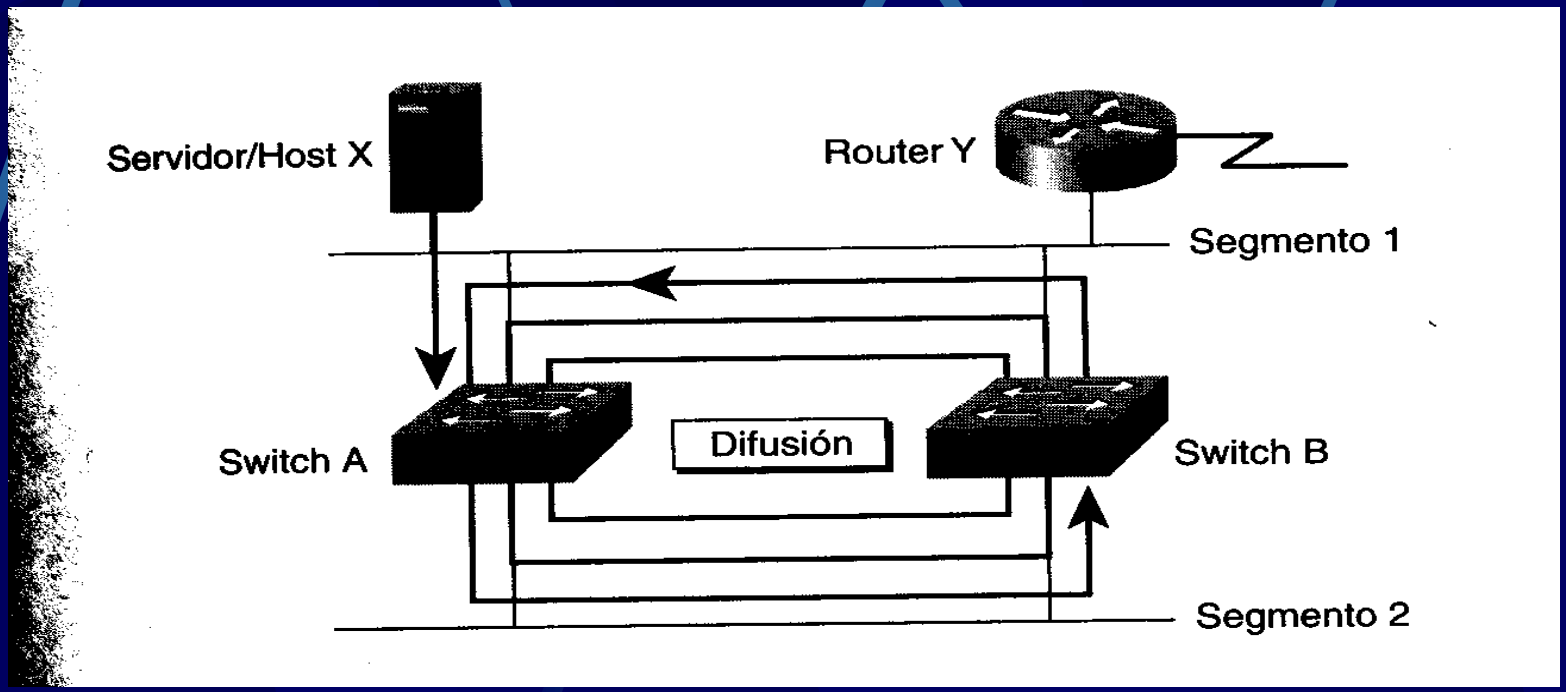
En muchas instalaciones críticas se disponen enlaces redundantes con el fin de prevenir salidas de servicio



Se originan bucles en la red, los cuales no se pueden permitir, ya que originan las *tormentas de difusión*

Switchs (conmutadores): Tormentas de Difusión

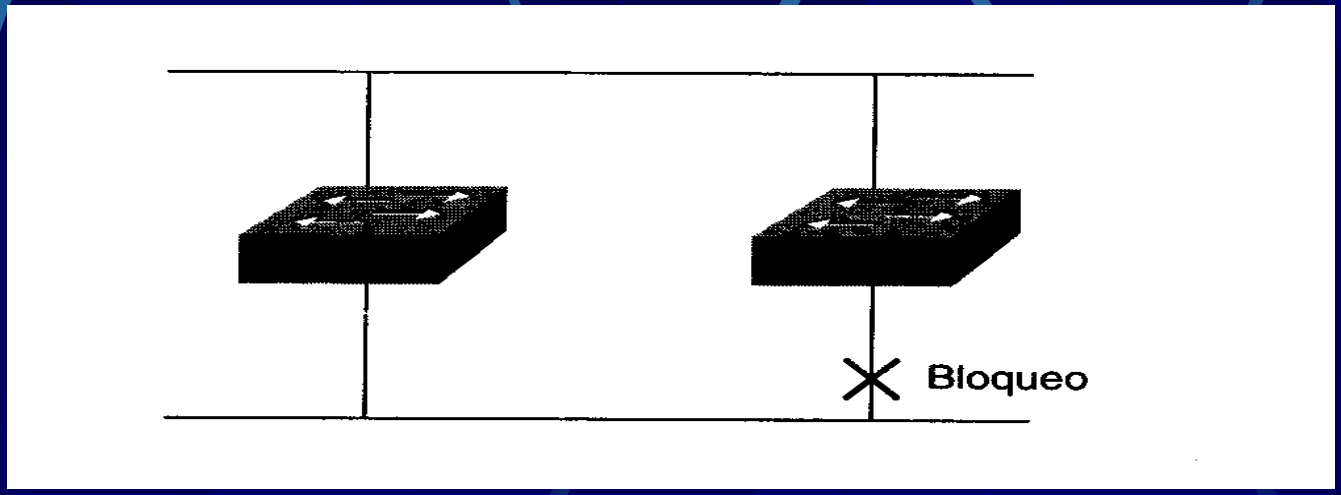
Las tormentas de difusión se originan en la realimentación de este tipo de tráfico, que provoca una transmisión sin límite



Se corrige mediante el algoritmo de Spanning Tree (Arbol de Extensión)

Switchs (conmutadores): Spanning Tree (Arbol de extensión)

Para impedir las tormentas de difusión se bloquean los enlaces redundantes. El mecanismo para dicho bloqueo se conoce como árbol de extensión (spanning tree)



Para ello el sistema escoge automáticamente a uno de los Switchs (conmutadores): como root y bloquea los enlaces redundantes a dicho equipo.

Spanning Tree Protocol (STP)

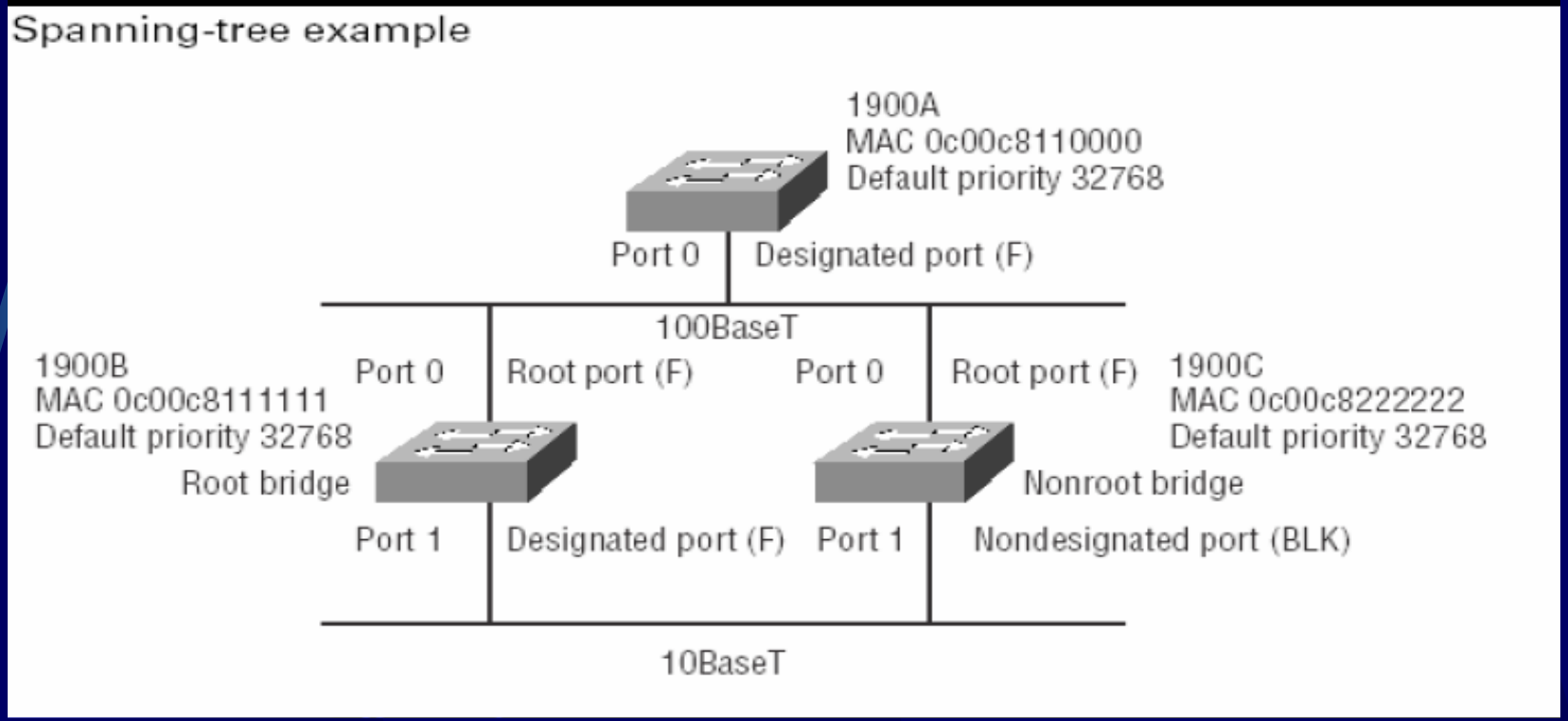
- Creado por DEC (Digital Equipment Corporation)
- Estandarizado por IEEE
  - 802.1d
- Meta: Apagar puertos redundantes y formar un árbol jerárquico
- Intercambio de información usando tramas multicast (Ethernet)

Spanning Tree Protocol (STP)

- Seleccionar un switch raíz
  - El que tenga el menor ID
  - ID = Prioridad (conf) + MAC del dispositivo
  - Sus puertos son ‘puertos designados’
- Seleccionar ‘puertos raíz’ en los demás switches
  - El que tenga el menor ‘costo’
    - Mayor velocidad, menor costo
- Bloquear los puertos no-designados

Spanning Tree Protocol (STP)

Ejemplo de STP



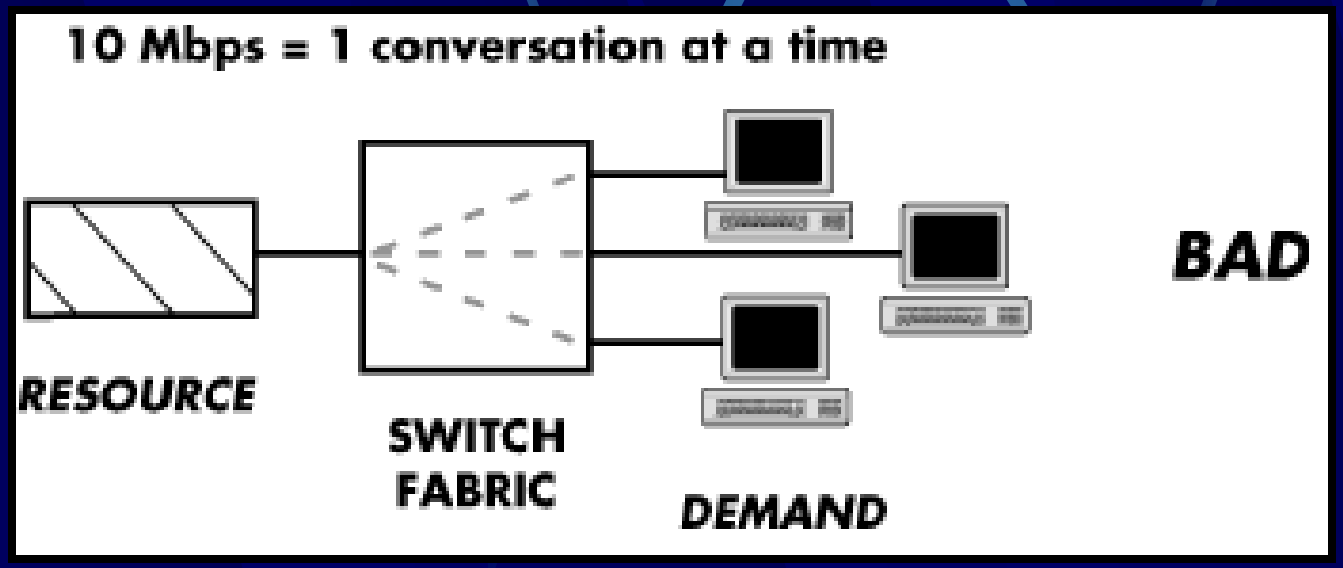
Spanning Tree Protocol (STP)

Estados de puertos en STP

- Bloqueado (Blocked)
  - Al iniciar el switch
- Escuchando (Listening)
  - Esperando mensajes STP para asegurarse de que no hay bucles
- Aprendiendo (Learning)
  - Recibiendo tramas y guardando direcciones MAC en la tabla
- Reenviando (Forwarding)

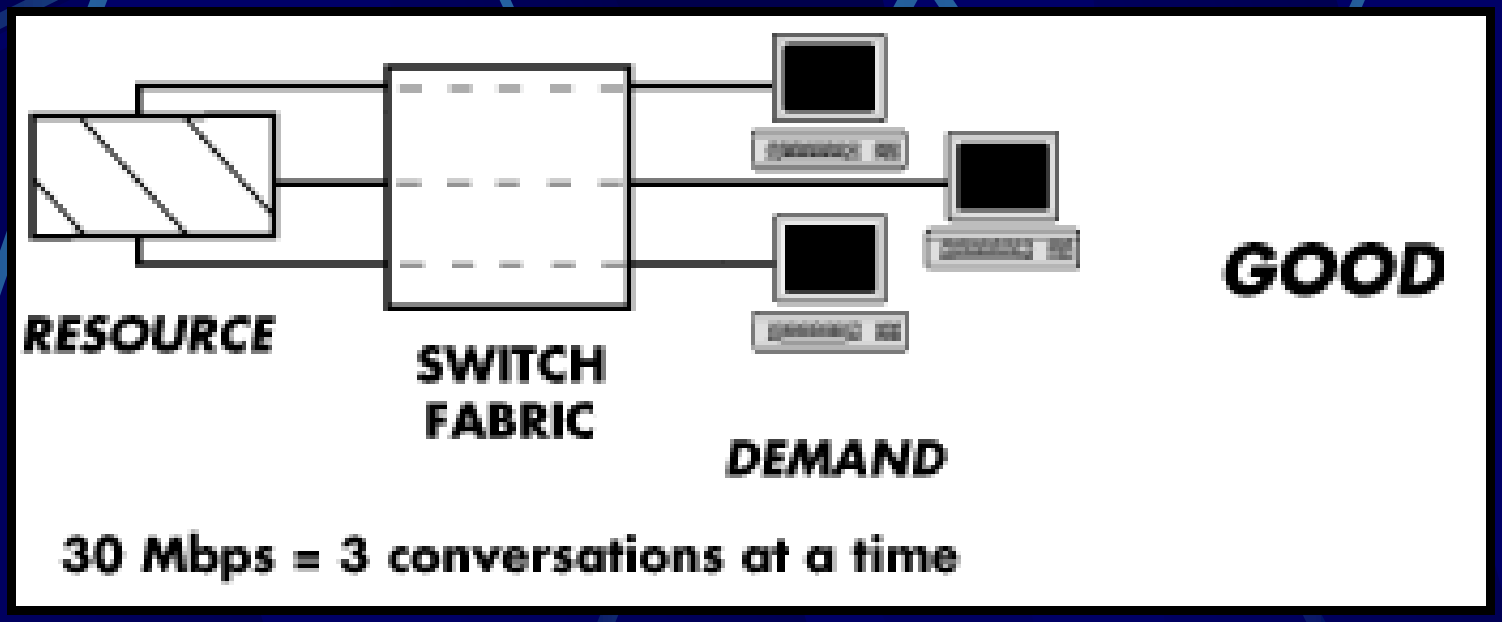
Switchs (conmutadores): Agrupación de tráfico

En ciertas ocasiones se producen cuellos de botella en el acceso a ciertos equipos críticos como servidores, estaciones de altas prestaciones, equipos de interconexión, etc.



Switchs (conmutadores): Agrupación de tráfico

En estos casos se debe resolver adecuadamente el acceso al recurso crítico:



Notemos que se ha hecho uso de la noción de paralelismo al disponer varios enlaces simultáneos

Switchs (conmutadores): Agrupación de tráfico

A este tipo de solución se le llama ***agrupación de tráfico,*** que en la literatura técnica del tema se conoce como link aggregation o incluso trunking o **IEEE 802.3ad**

La solución consiste, como se ha visto, en disponer dos o más enlaces en paralelo para conectar entre si a dos equipos críticos.

Este tipo de tráfico esta pautado por la norma IEEE 802.3ad

Cuando se establece un enlace de este tipo el switch automáticamente desbloquea la redundancia y desactiva el algoritmo de spanning tree para el trunk.

Switchs (conmutadores): Agrupación de tráfico

En que casos se puede utilizar esta solución?

- Conexiones switch to switch
- Conexiones switch a estación

Por estación se entiende en este caso a un servidor o a un equipo de interconexión de redes, etc.

Switchs (conmutadores) : Agrupación de tráfico

Características del trunking

- Incremento en la capacidad del enlace
- Adecuación de la capacidad incremental

Switchs (conmutadores): Agrupación de tráfico

- Incremento en la capacidad del enlace

Cuando se disponen varios enlaces en paralelo la capacidad del enlace resultante es la suma de todos los enlaces. Por ejemplo una agrupación de tres canales Fast Ethernet Full duplex, da como resultado 600 Mbits/seg. En cada dirección disponemos 300 Mbits/seg.

Switchs (conmutadores): Agrupación de tráfico

• Adecuación de la capacidad incremental

Cuando se dispone una actualización por hardware de un enlace crítico, el ancho de banda se dispone en módulos según la tecnología disponible:

10 Mbits; 100 Mbits; 1000 Mbits; etc.

La agrupación de tráfico permite graduar o adecuar el aumento del ancho de banda disponible a la necesidad de la transmisión en cuestión.

Switchs (conmutadores): Agrupación de tráfico

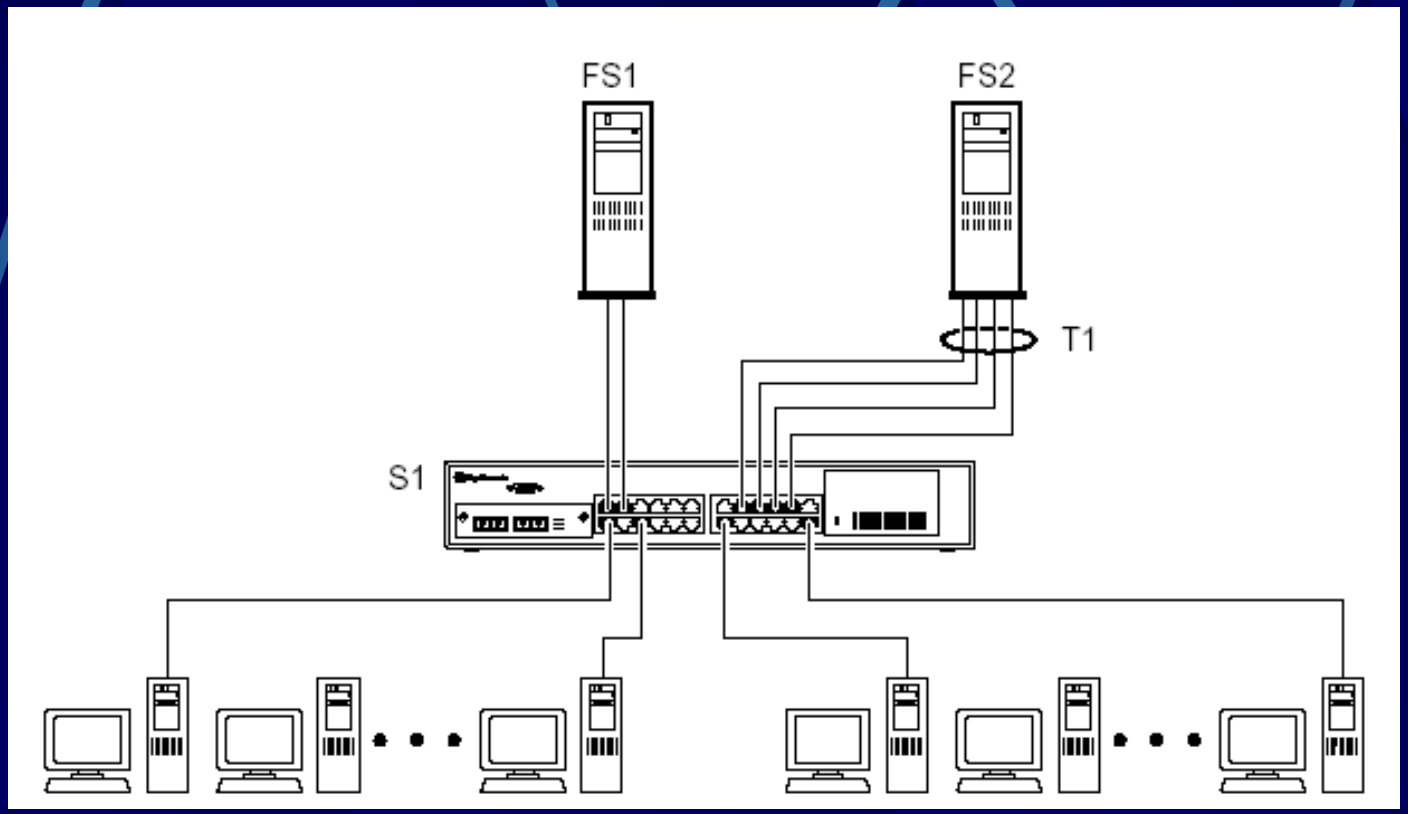
Robustez del agregado de tráfico

El agregado debe ser una característica del equipo, se debe poder administrar por software y ser tolerante a fallos.

Si uno de los enlaces individuales sale de servicio, el agrupado o trunking tiene que seguir funcionando, aunque con menor ancho de banda disponible.

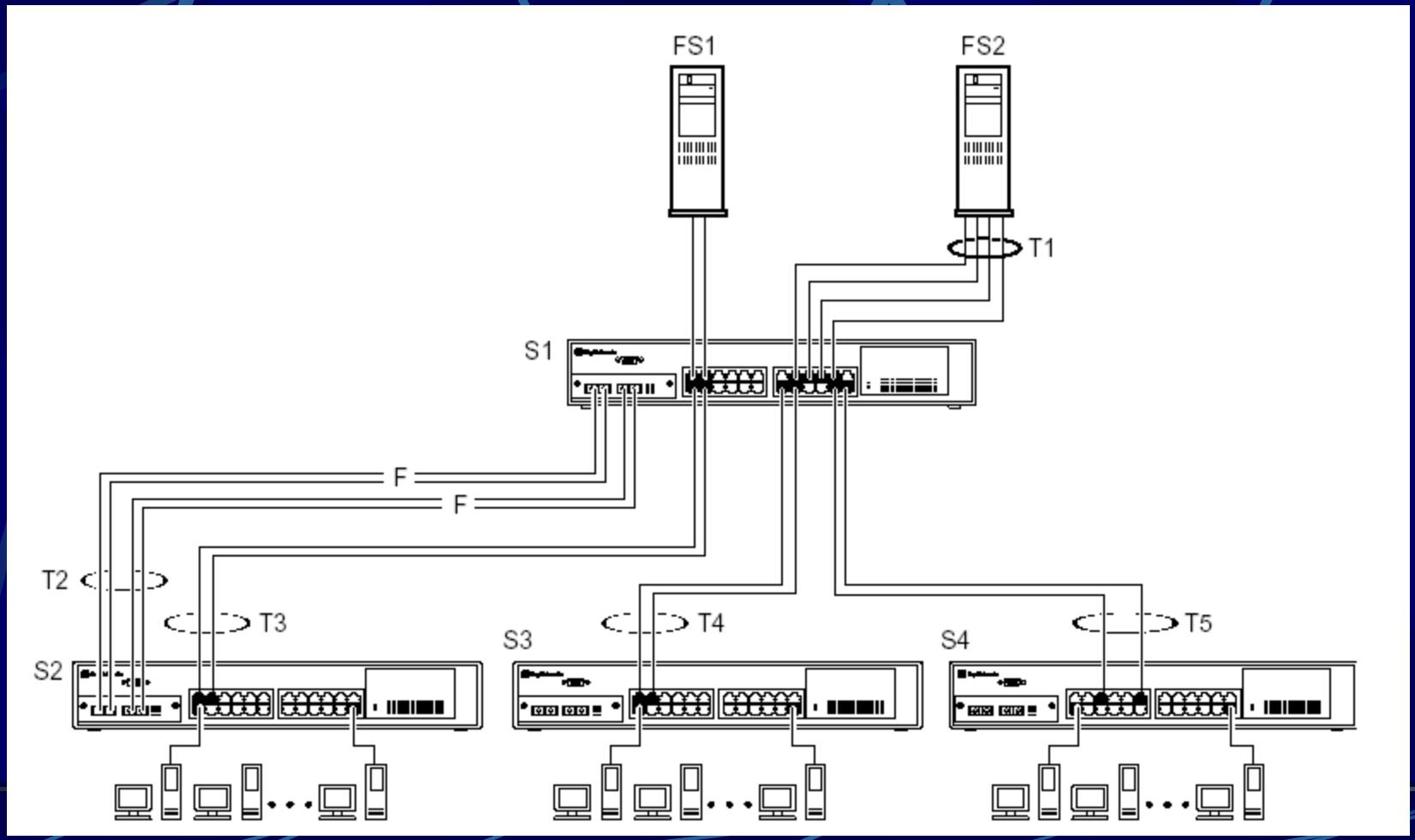
Switchs (conmutadores): Agrupación de tráfico

Aplicación: conexión con servidores, se utilizan placas especiales.



Switchs (conmutadores): Agrupación de tráfico

Aplicación: conexión con servidores, backbones



Switchs (conmutadores): Agrupación de tráfico

Aplicación: conexión con servidores, se utilizan placas especiales.

REDES LOCALES VIRTUALES (VLAN's)

REVISION DE CONCEPTOS

Hasta Ahora, recurrentemente, se han presentado ideas para mejorar el desempeño y el rendimiento de las redes de área local basadas en Ethernet.

Recordemos que existen dos problemas típicos:

- Disminuir los dominios de colisión
- Evitar los cuellos de botella

VLAN'S: Revisión de Conceptos

También se ha visto que las redes conmutadas y los Switchs (conmutadores) son herramientas eficientes para resolver los problemas planteados ya que:

- Disminuyen los dominios de colisión
- Facilitan el acceso a recursos críticos, como los servidores, ya que permiten disponer puertos de uplink o bien agrupación de enlaces (Link aggregation o port trunking)

VLAN'S: Revisión de Conceptos

Sin embargo permanece un problema...(Cuál es?)

EL DOMINIO DE DIFUSION ES UNICO !!!!

Los ruteadores permiten aislar los dominios de difusión, pero son equipos costosos, lentos y relativamente complejos de administrar...

Se recomienda leer el artículo *Switchs y ruteadores* para ver un resumen del tema...

VLAN’S: Introducción

Para mantener todas las ventajas citadas y resolver la dificultad asociada a los dominios de difusión, se hace uso de otra característica de los Switchs (conmutadores):

En ciertos casos los Switchs (conmutadores) pueden agrupar puertos y limitar los dominios de difusión.

Esta característica se conoce como Redes Locales Virtuales, en inglés Virtual LAN’s o VLAN’s.

VLAN'S: Temario

- Qué es una VLAN?
- Cómo funciona una VLAN?
- Cómo se comunican entre si las máquinas que pertenecen a diferentes VLAN's?
- Aplicaciones de las VLAN's
- Criterios para agrupar a las VLAN's
- Identificación de Marcos de hardware

VLAN'S: Definición

Una VLAN puede definirse como una agrupación lógica, artificial, de tráfico, que forma grupos de equipos que simulan el segmentado de una red, tanto para los dominios de colisión como para los dominios de difusión.

VLAN'S: Cómo funcionan?

Esencialmente una VLAN limita el dominio de difusión a un grupo de máquinas predefinidas.

Suele decirse que el dominio de difusión se limita a la VLAN, y para ello se filtran los mensajes de broadcast.

Notemos que ahora el switch (conmutador) no solo filtra mensajes de unicast, sino que también limita o filtra mensajes de broadcast.

Luego, a grandes rasgos, los efectos del switch (conmutador)sobre la red son parecidos a los de un router.

La gran diferencia es que las decisiones se basan en tráfico de capa 2 y no de capa 3.

VLAN’S: Se pueden comunicar las diferentes VLAN’s?

No, es totalmente imposible!!!

Recordemos que en las LAN las máquinas se comunican mediante direcciones de capa 2.

Que además se emplean, a través del protocolo ARP, mensajes de difusión para identificar estaciones desconocidas.

Luego no puedo, mediante mensajes de difusión, alcanzar a equipos ubicados en otras VLAN’s porque el domino de difusión es diferente y no leen los mensajes de broadcast de otras VLAN’s.

VLAN’S: Cómo se restablece la conectividad?

La interconexión de VLAN’s se restablece mediante el empleo de routers. No existe otra posibilidad.

En el mercado se ofrecen los denominados Switchs de capa 3 o layer 3 que agrupan las funciones de ruteador y switch (conmutador) en un mismo equipo.

VLAN’S: Aplicaciones

Además de heredar todas las características de las redes conmutadas y de resolver su problema más importante: dominio de difusión único, las VLAN’s toman ventaja de su propia naturaleza.

Recordemos que una VLAN’s es una agrupación lógica de tráfico.

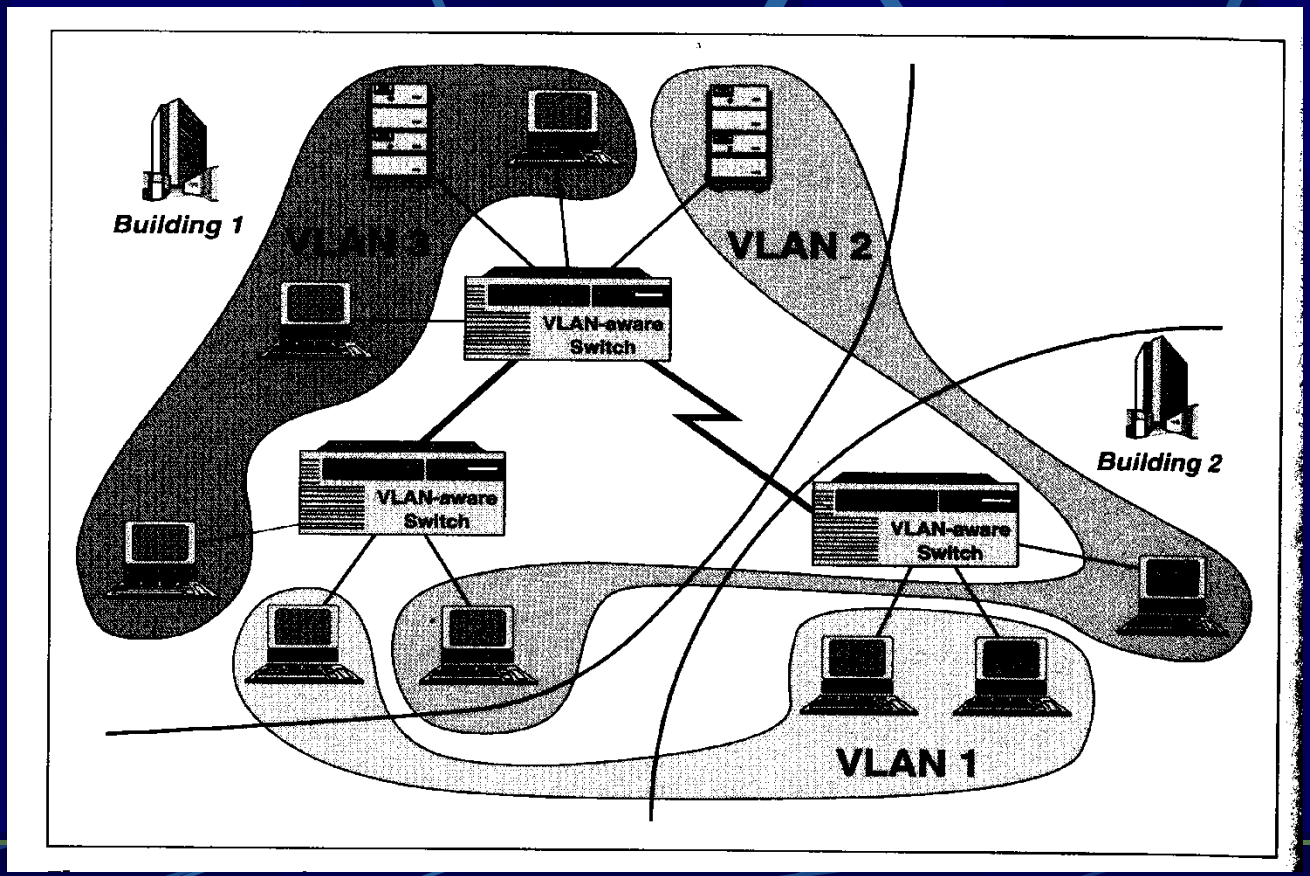
Para que podemos utilizar dicha característica?

VLAN'S: Aplicaciones

- Flexibilidad en la comunicación de usuarios y formación de grupos.
- Incremento de la seguridad
- Facilita la movilidad de usuarios

VLAN'S: Flexibilidad en la formación de grupos

Una red de altas prestaciones en una empresa mediana o grande consiste en una agrupación de Switchs (conmutadores) que pueden estar en uno o más edificios:



VLAN'S: Aplicaciones

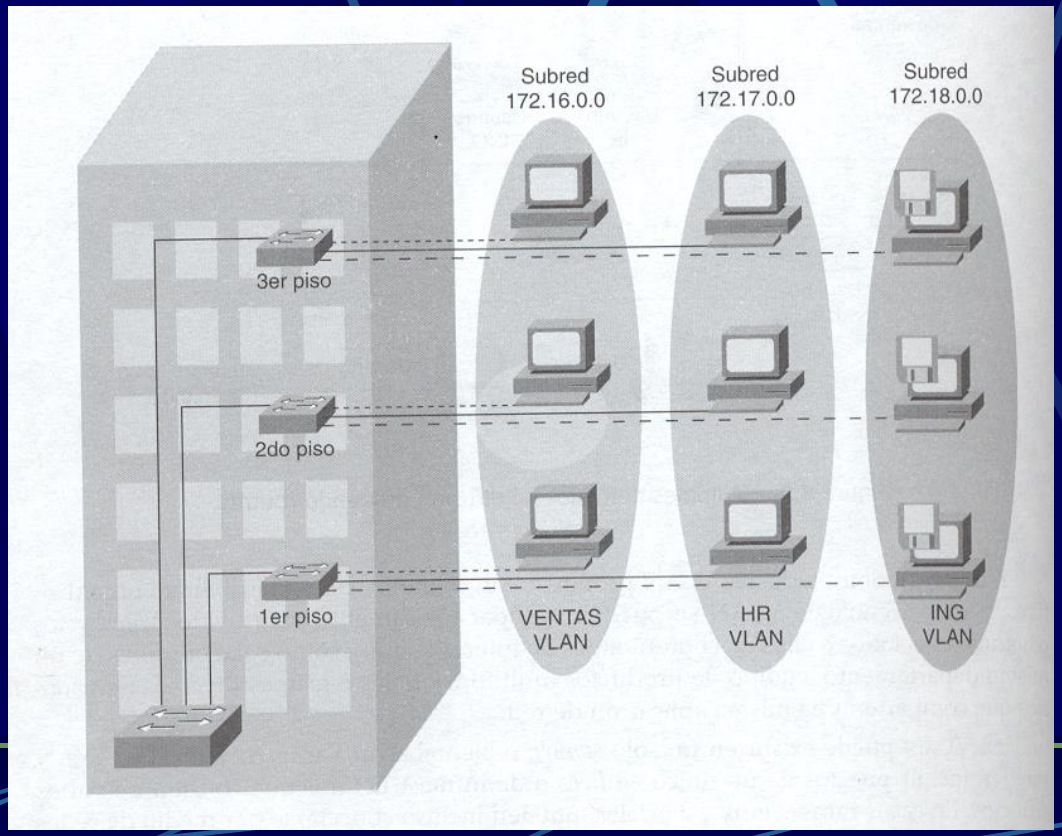
La flexibilidad en la agrupación de los usuarios viene dada por el hecho que una VLAN puede estar distribuida en varios Switchs (conmutadores): diferentes!!!

(Después veremos que debemos exigirle a los equipos para conseguir esta prestación!)

Luego no solo puedo disponer diferentes VLAN's en un mismo switch, sino que puedo extenderlas a diferentes equipos!!!

VLAN'S: Flexibilidad en la formación de grupos

Un ejemplo de esta facilidad consiste en formar VLAN's que agrupe a equipos de diferentes departamentos, como ventas, recursos humanos y/o ingeniería, los que generalmente se agrupan por piso.



VLAN'S: Aplicaciones

Supongamos que un integrante de Ventas debe desplazarse a Ingeniería para preparar una licitación.

En una red convencional dicha persona debería cambiar de subred o red para conseguir conectividad nuevamente, y muy posiblemente perdería conectividad con sus servidores y recursos habituales. Otra opción, no siempre sencilla, es rehacer conexiones en el patch pannel.

En este caso el administrador de red simplemente reconfigura el nuevo puerto de conexión del integrante a la VLAN de ventas y se soluciona el problema. Esta facilidad se la conoce como patchera por software.

VLAN'S: Seguridad

En una LAN compartida todos los equipos tienen el mismo privilegio para acceder a la red.

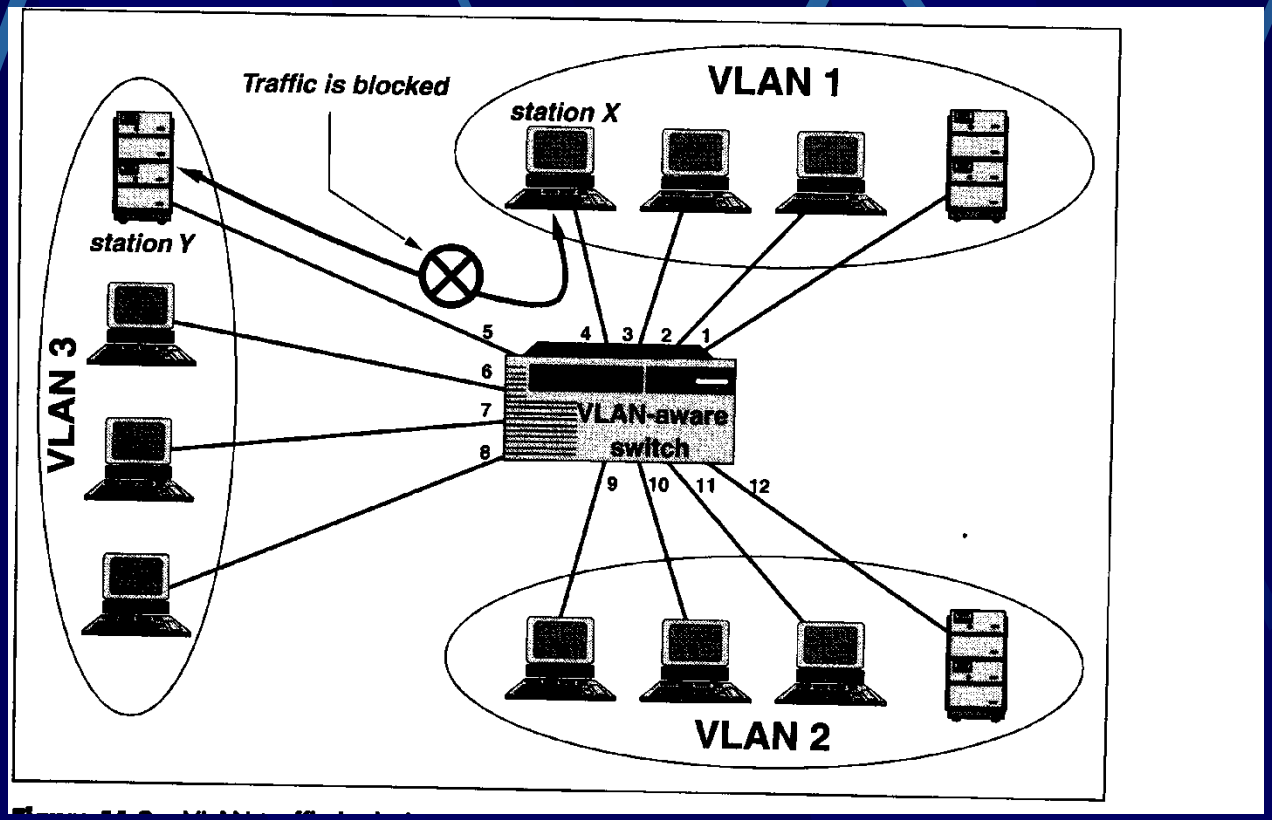
Luego cada equipo escucha, y puede capturar, el tráfico originado en cualquier otro puesto de la red. (Pensemos en un PC y un sniffer...)

Si conectamos a los usuarios, mediante una red conmutada, a una boca dedicada (microsegmentación), solo podrán escuchar tráfico de unicast dirigido a ellos, tráfico de unicast con destino desconocido y trafico de multicast/broadcast.

Los peligros se han limitado mucho...Sin embargo un switch convencional no filtra el tráfico de multicas/broadcast, con lo que se podrían intentar algunos ataques o invadir la red de tráfico..

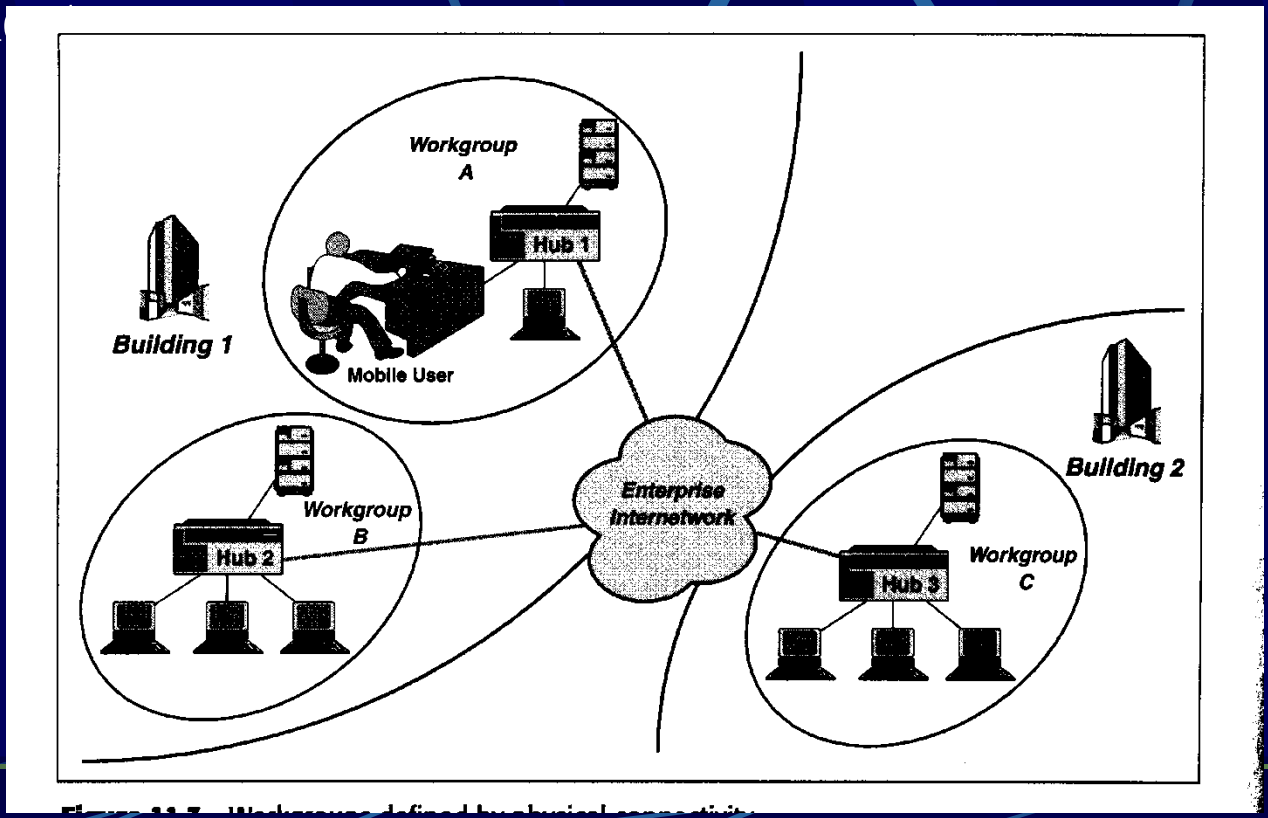
VLAN'S: Seguridad

Una VLAN además limita el tráfico de destino a los miembros de la misma, con lo cual se evitan muchos de los problemas citados:



VLAN'S: Movilidad de Usuarios

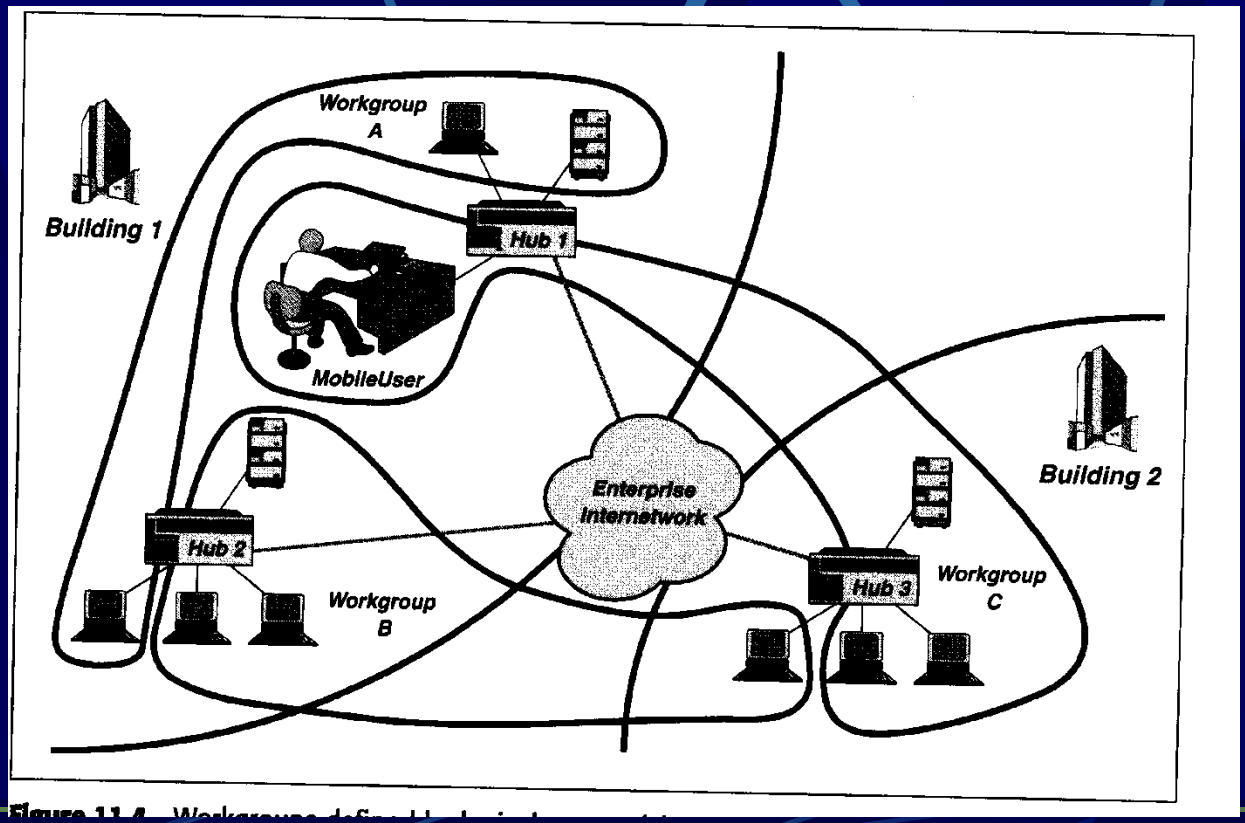
En una LAN tradicional, conformada por hubs o Switchs (conmutadores) tradicionales, la conectividad lógica queda definida por la conectividad física. Así un usuario conectado al Hub 1, puede acceder a los recursos disponibles para su red solam



VLAN'S: Movilidad de Usuarios

Ahora bien, si el usuario que se conecta al Hub 1 en realidad pertenece al grupo C y esta temporalmente en el grupo A, pierde el acceso a sus recursos.

Si la red esta armada en base a VLAN's, simplemente con asignar la nueva boca de conexión a la VLAN original se restablece la situación inicial.



VLAN'S: Algunos conceptos importantes

- Etiquetado de VLAN's (tagging)
- Reconocimiento de VLAN's
- Asociación de VLAN's
- Distribución de marcos de hardware

Para discutir estas ideas necesitamos presentar algunos conceptos básicos.

VLAN'S: Algunos conceptos importantes

Una VLAN es una agrupación lógica de:

- estaciones
- protocolos de red
- aplicaciones (por ejemplo: videoconferencias)

VLAN'S: Algunos conceptos importantes

Desde la perspectiva de dispositivos que reconocen VLAN's, son los marcos de hardware los que pertenecen a las VLAN's y no las estaciones, los protocolos, o las aplicaciones

Luego es necesario asociar de manera unívoca (1 a 1) los marcos de hardware a una VLAN !!!

VLAN'S: Asociación de marcos a VLAN's

La asociación de marcos se puede realizar de manera *implícita*, (ya sea mediante protocolos, subredes, aplicaciones, etc.), o bien de manera *explícita*, para lo cual se identifica o etiqueta el marco mediante una etiqueta adecuada (tag).

VLAN'S: Asociaciones implícitas

Un marco se puede asociar implícitamente mediante alguna de las siguientes reglas:

- Dirección Física
- Tipo de Protocolo
- Identificadores de red de capas altas (por ej. Subredes)
- Aplicaciones
- etc.

VLAN'S: Asociación explícita

El marco lleva consigo la identificación de la VLAN a la cual pertenece. Existen dos posibilidades:

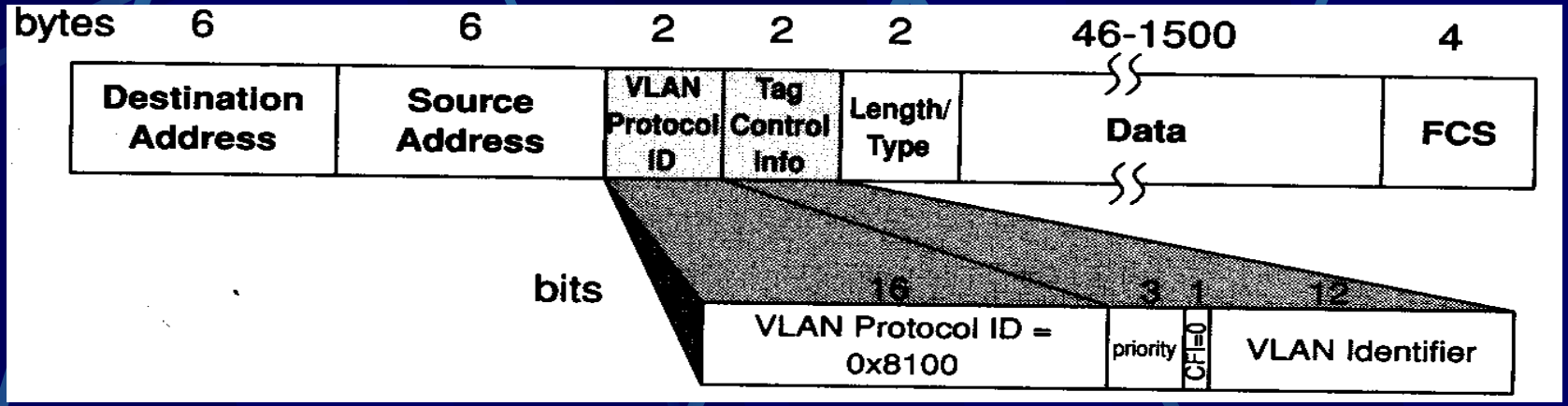
- IEEE 802.1Q

Standard al cual adhieren la mayoría de los fabricantes. Es relativamente nuevo ya que fue aprobado en diciembre de 1998.

Otra chance es el protocolo propietario de Cisco llamado ISL, que le agrega una cabecera propietaria al marco de capa 2. Los switchs de 3COM poseen un protocolo propietario llamado VTP.

VLAN'S: IEEE 802.1Q

Se agrega al marco un campo que permite identificar la VLAN a la cual esta asociado:



Pueden disponerse puertos que permitan el ingreso (egreso) de marcos etiquetados o no etiquetados.

El parámetro PVID nos permite asignar los marcos no etiquetados.

CFI: canonical format indicator

- **User Priority**- Defines user priority, giving eight (2^3) priority levels. ***IEEE 802.1P*** defines the operation for these 3 user priority bits.

- Se transformó en :

Priority code point (PCP): a 3-bit field which refers to the IEEE 802.1p class of service and maps to the frame priority level. Values in order of priority are: 0 (background), 1 por defecto, 2 (best effort), 3 (excellent effort), 4 (critical application), 5 (video), 6 (voz), 7 (network control). These values can be used to prioritize different classes of traffic (voice, video, data, etc.).

➢**CFI- Canonical Format Indicator** is always set to zero for Ethernet switches. **CFI** is used for compatibility reason between Ethernet type network and Token Ring type network. If a frame received at an Ethernet port has a **CFI** set to 1, then that frame should not be forwarded as it is to an untagged port..

Se transformó en:

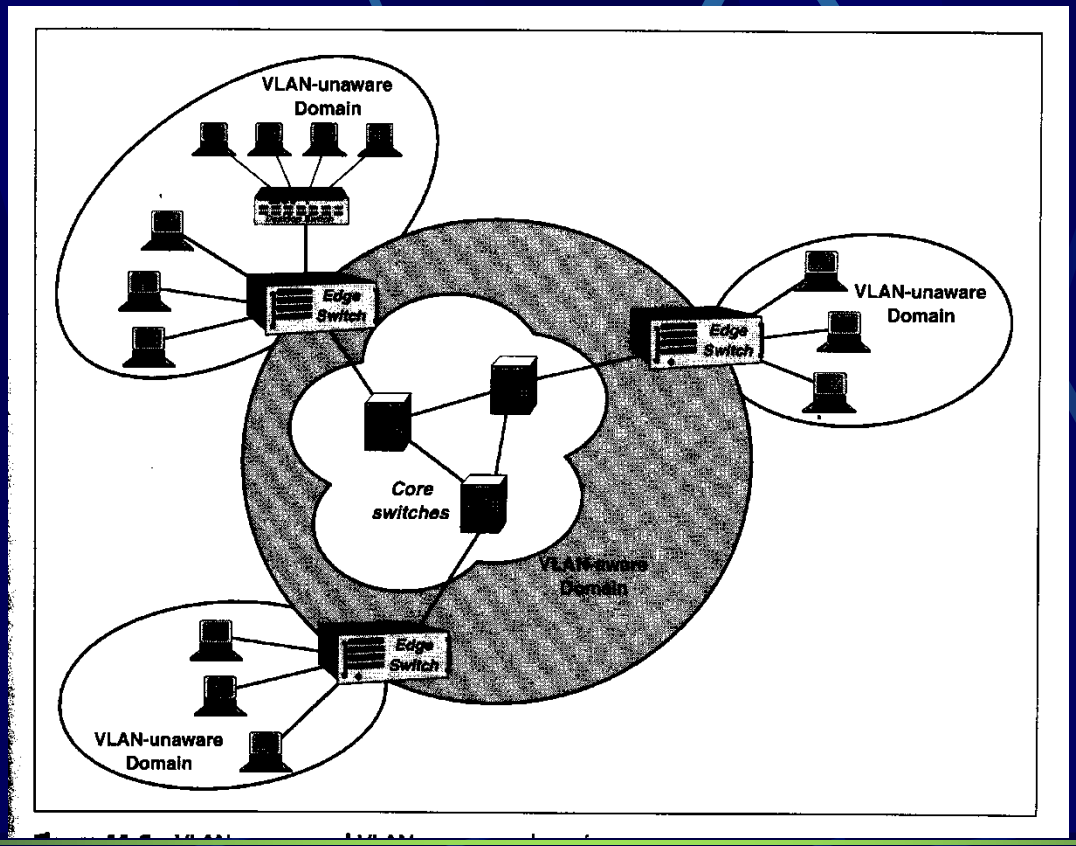
Drop eligible indicator (DEI): a 1-bit field. (formerly CFI[note 1][4]) May be used separately or in conjunction with PCP to indicate frames eligible to be dropped in the presence of congestion

➢**VID-** VLAN ID is the identification of the VLAN, which is basically used by the standard ***802.1Q***. It has 12 bits and allow the identification of 4096 (2^12) VLANs. Of the 4096 possible VIDs, a VID of 0 is used to identify priority frames and value 4095 (FFF) is reserved, so the maximum possible VLAN configurations are **4,094**.

- **Length/Type-** 2 bytes. This field indicates either the number of MAC-client data bytes that are contained in the data field of the frame, or the frame type ID if the frame is assembled using an optional **format**.
- **Data-** Is a sequence of nbytes (46=< n =<1500) of any value. The total frame minimum is 64bytes.
- **Frame check sequence (FCS)-** 4 bytes. This sequence contains a 32-bit cyclic redundancy check (CRC) value, which is created by the sending MAC and is recalculated by the receiving MAC to check for damaged frames.

VLAN'S: Compatibilización de marcos

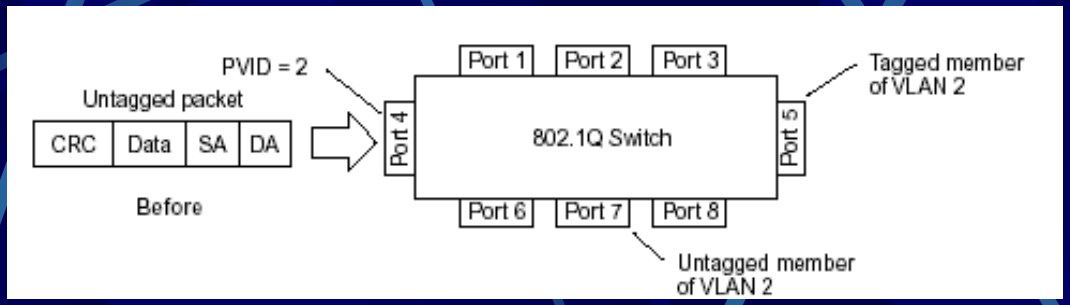
Los Switchs (conmutadores) deben tomar decisiones y ajustar marcos cuando reenvían y/o reciben tráfico de equipos que no soportan VLAN's.



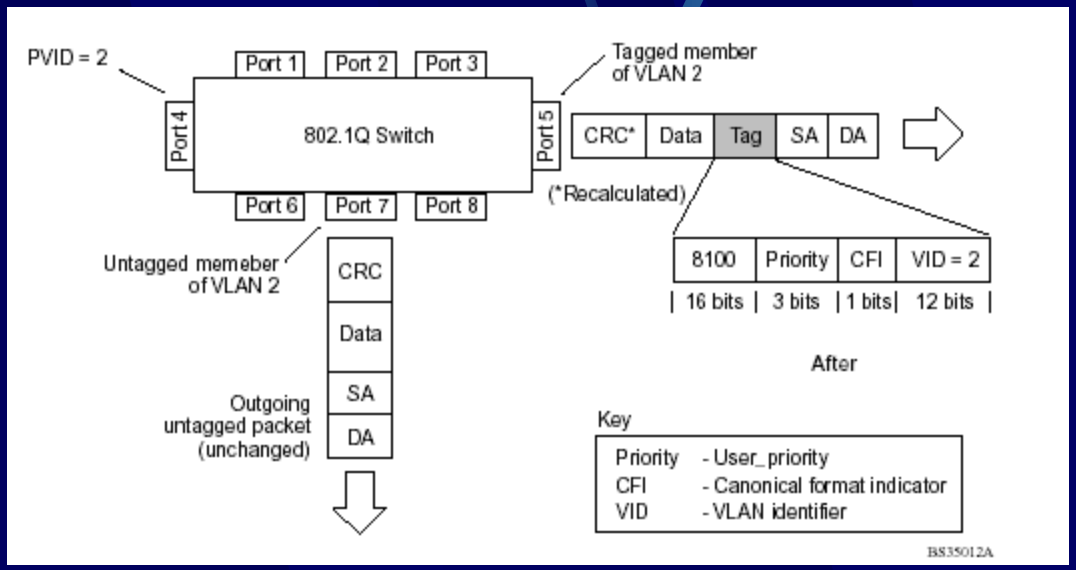
VLAN'S: IEEE 802.1Q

Reglas de ingreso y egreso de marcos no etiquetados

a)



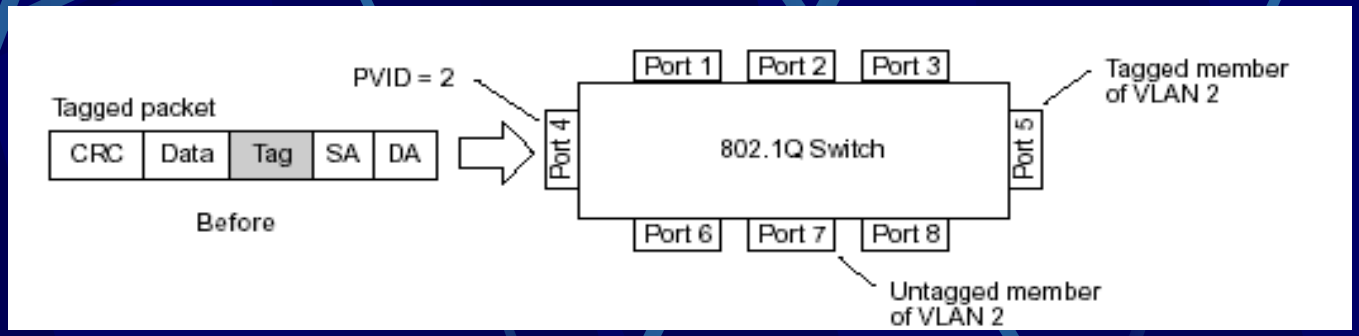
b)



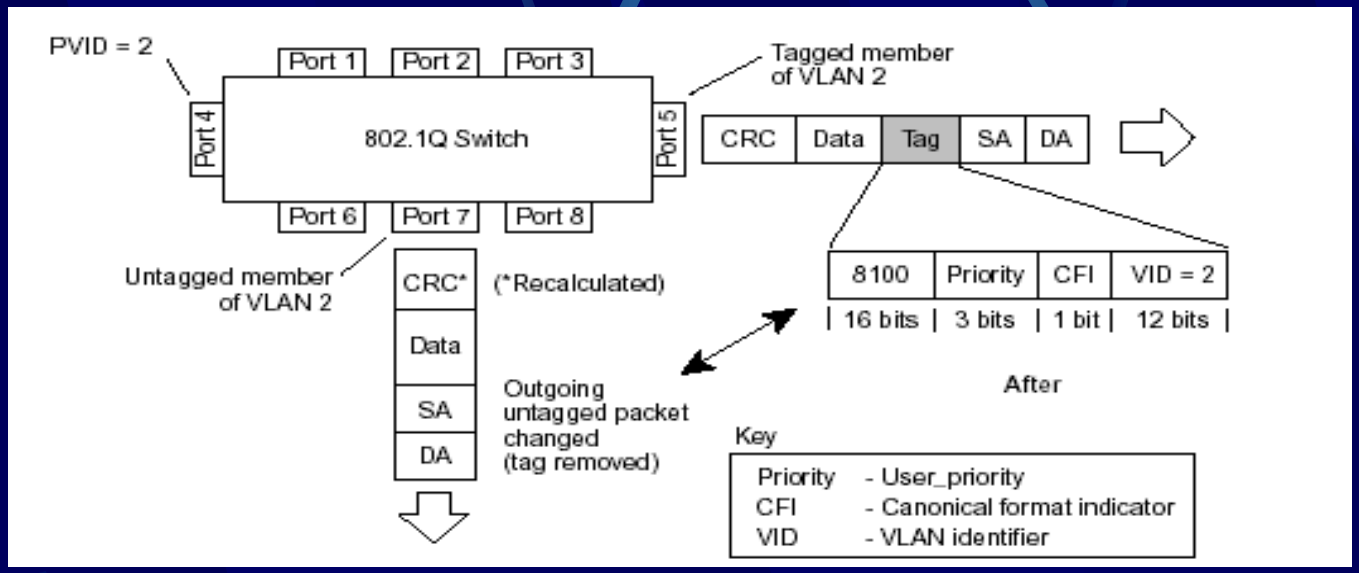
VLAN'S: IEEE 802.1Q

Reglas de ingreso y egreso de marcos etiquetados

a)

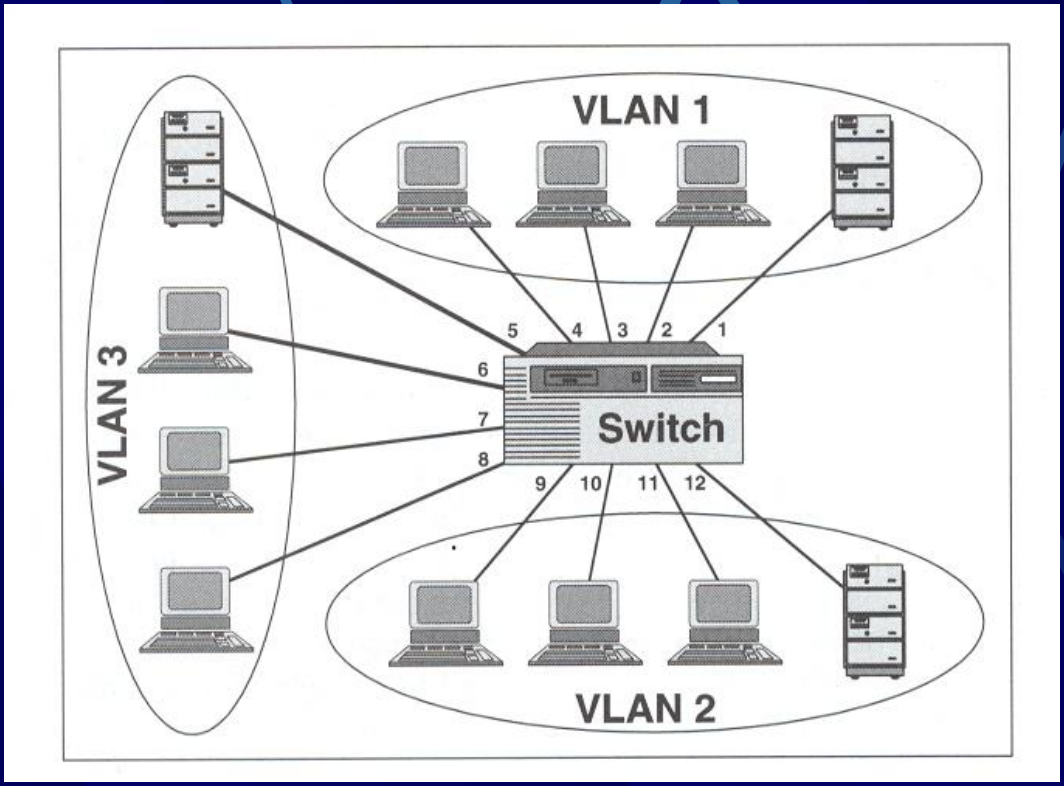


b)



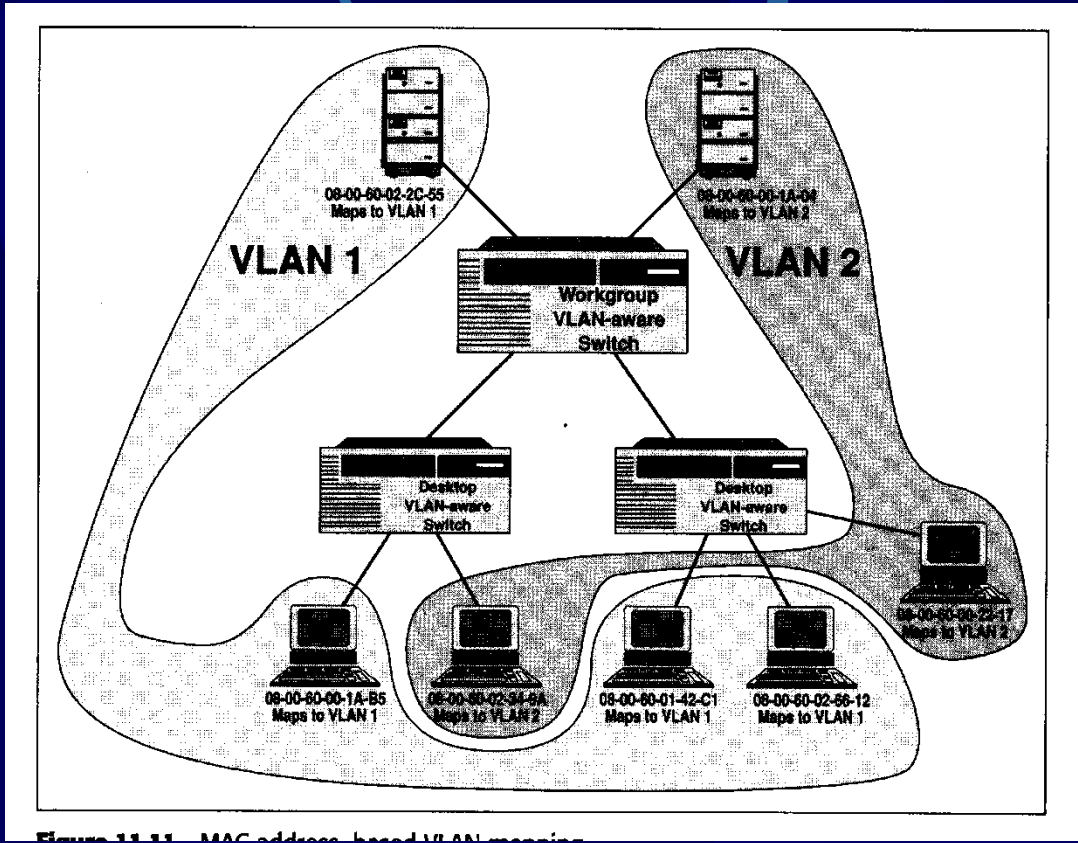
VLAN'S: Reglas de asociación

VLAN's por puerto: son las más comunes. Mucho trabajo de administración.



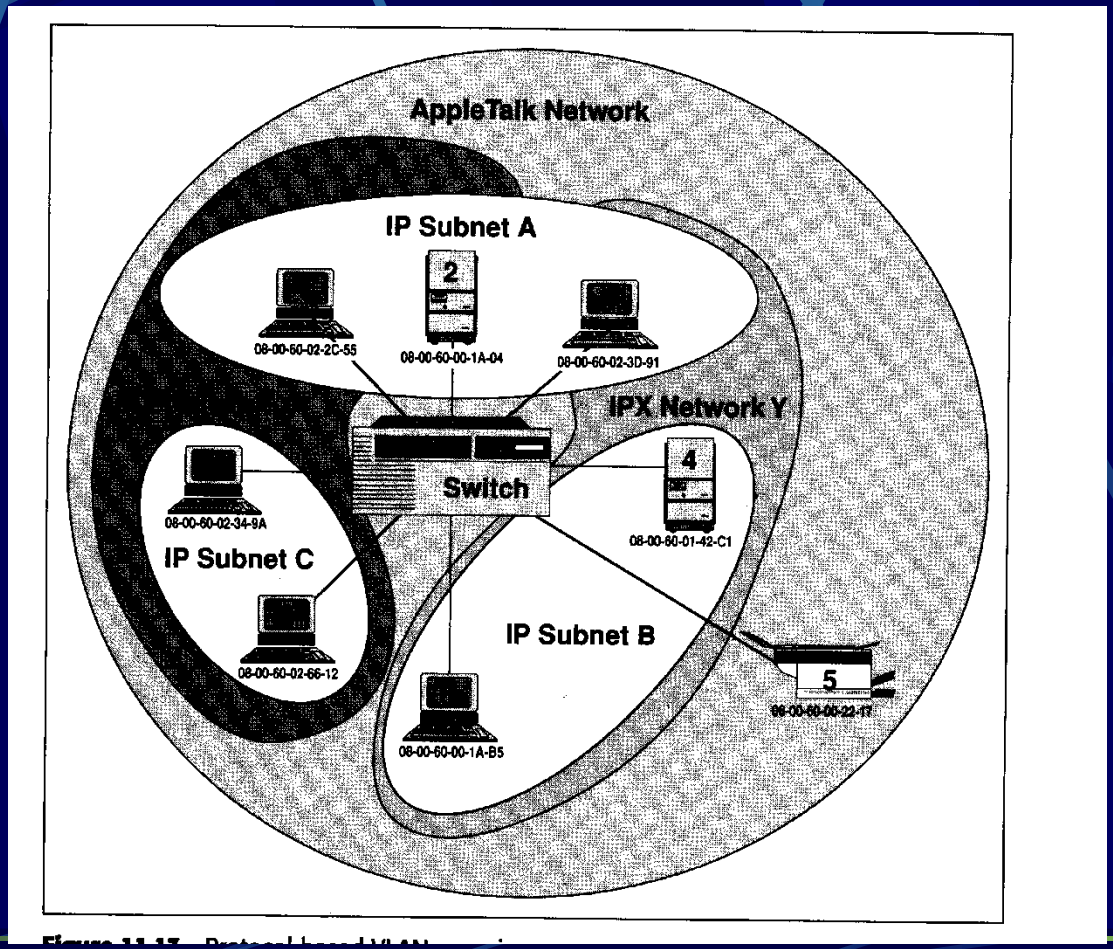
VLAN'S: Reglas de asociación

VLAN's por MAC



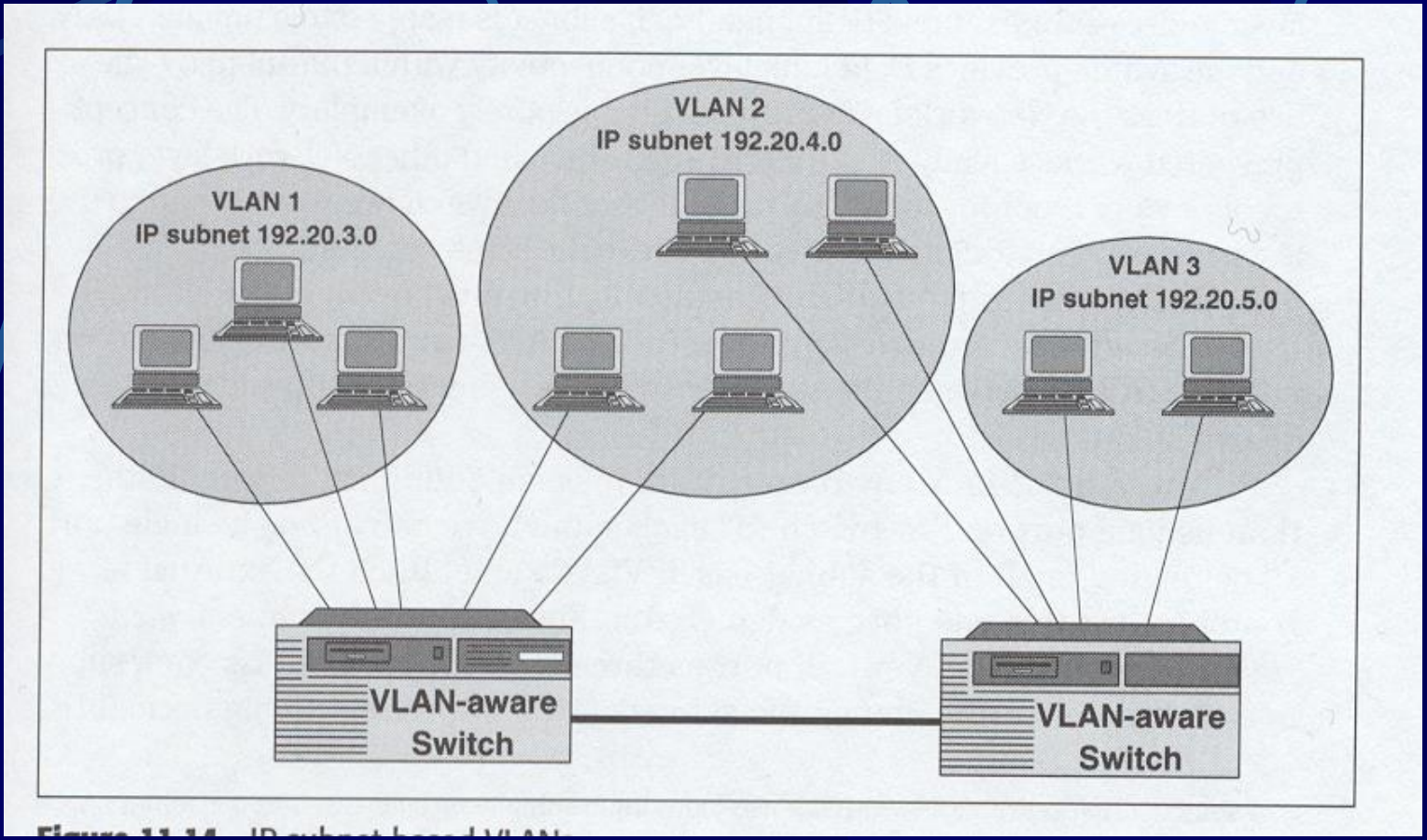
VLAN'S: Reglas de asociación

VLAN's por Protocolo



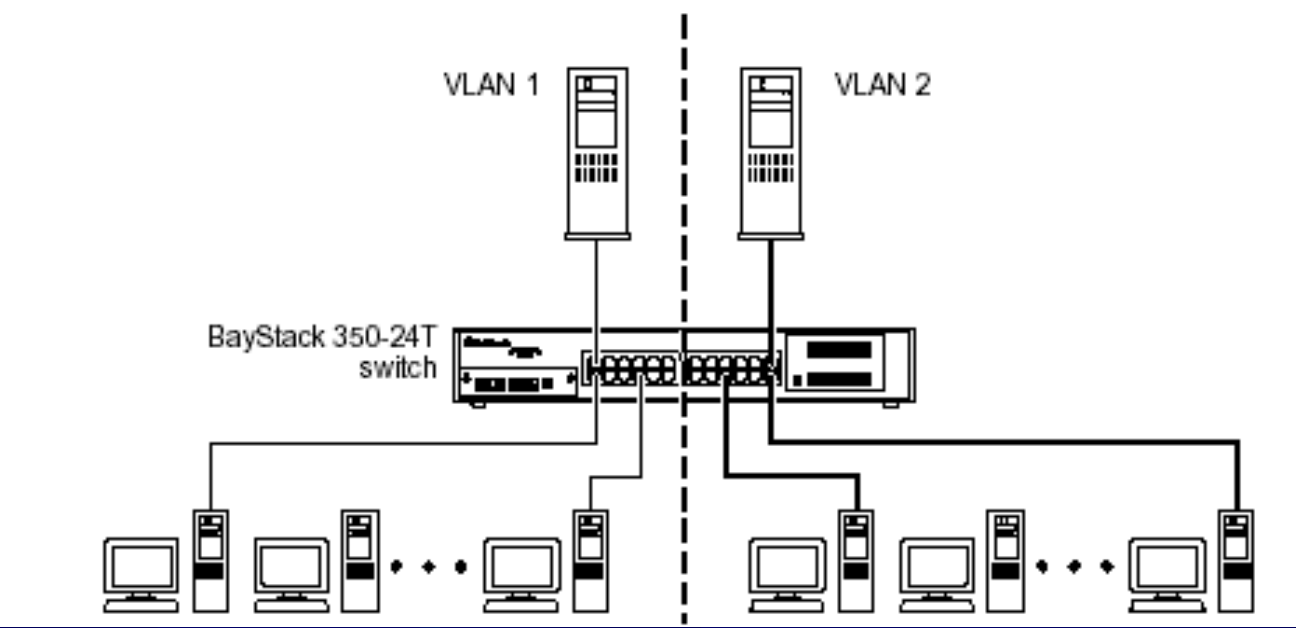
VLAN'S: Reglas de asociación

VLAN's por Subredes



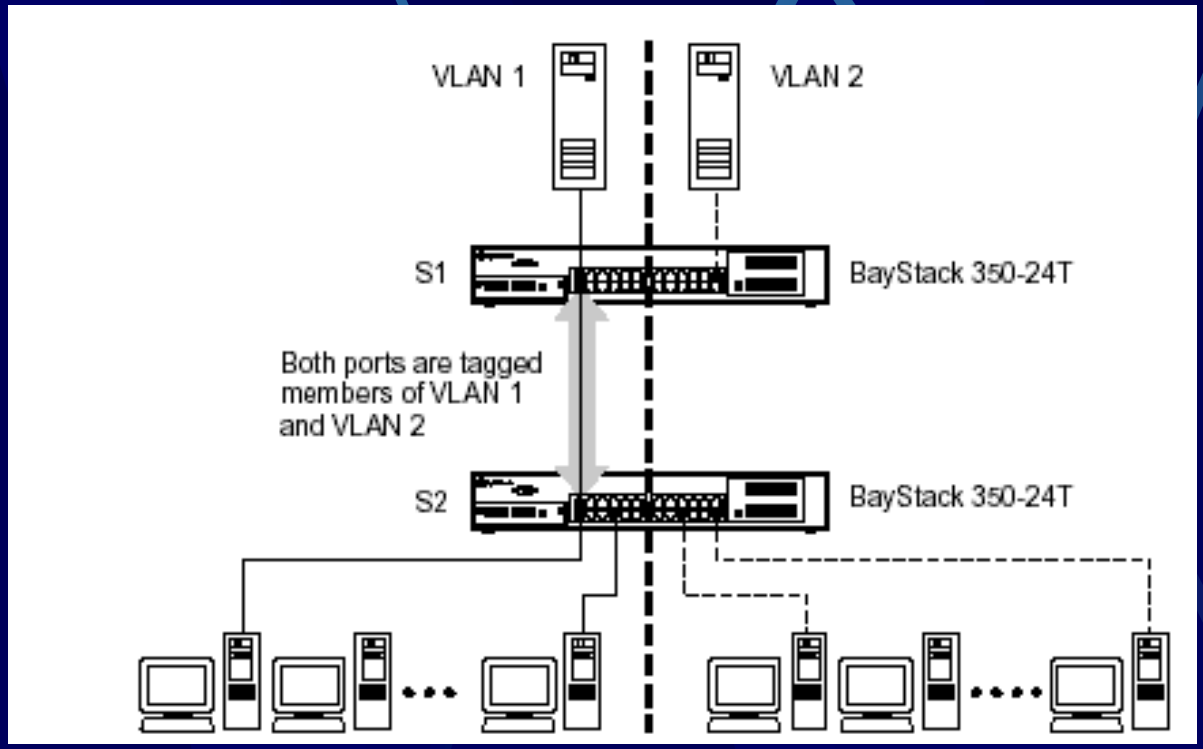
VLAN'S: Ejemplos

Vlan´s basadas en puertos



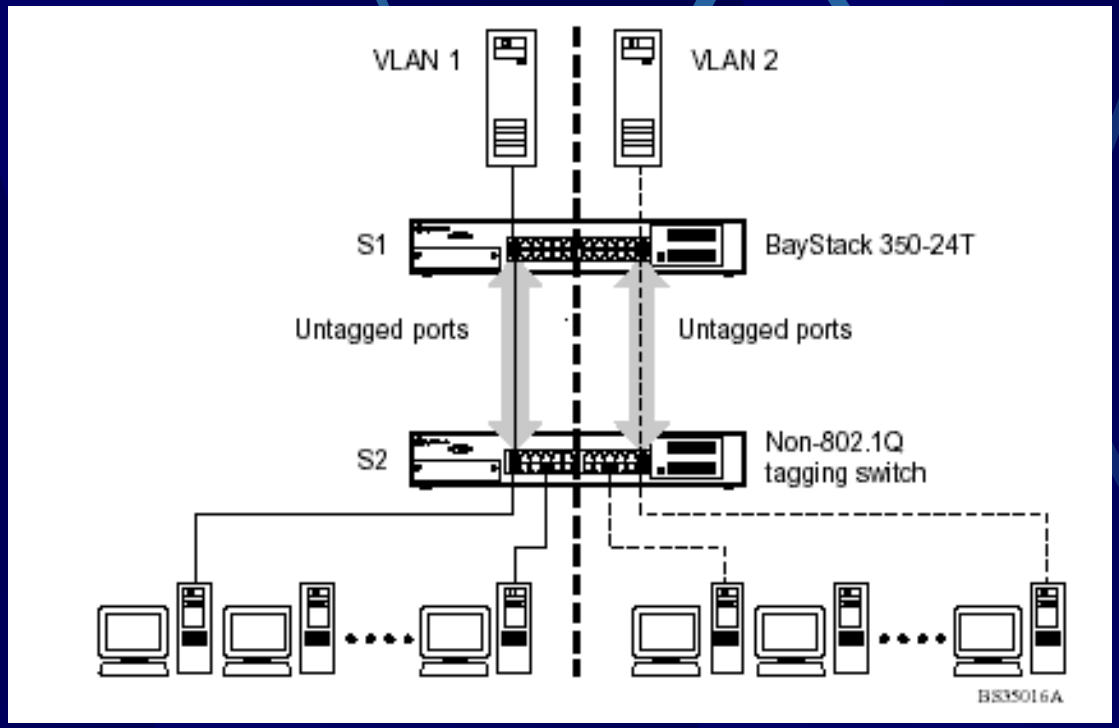
VLAN'S: Ejemplos

Vlan´s distribuidas en más de un conmutador. Uso de 802.1Q



VLAN'S: Ejemplos

Vlan´s distribuidas en más de un conmutador. Marcos no etiquetados



VLAN'S: Ejemplos

Empleo de múltiples VLAN´s por puerto para compartir recursos.