TEMA 1

1. Beneficios de una red jerárquica en una lan conmutada (tabla).

Beneficios de una red jerárquica

Escalabilidad
- Las redes jerárquicas pueden expandirse con facilidad

Redundancia
- La redundancia a nivel del núcleo y de la distribución asegura la disponibilidad de la ruta

Rendimiento
- El agregado del enlace entre los niveles y los switches del núcleo de alto rendimiento y del nivel de distribución permite casi la velocidad del cable en toda la red

Seguridad
- La seguridad del puerto en el nivel de acceso y las políticas en el nivel de la distribución hacen que la red sea más segura

Facilidad de administración
- La consistencia entre los switches en cada nivel hace que la administración sea más simple

Facilidad de mantenimiento
- La modularidad del diseño jerárquico permite que la red escale sin volverse demasiado complicada

2. Define los términos (diámetro de la red, ancho de banda agregada y enlace redundante).

Diámetro de la red: es el número de dispositivos que un paquete debe cruzar antes de alcanzar su destino.

Agregado de ancho de banda: para cada capa del modelo de redes jerárquicas según unos requisitos específicos de ancho de banda. Se pueden agregar enlaces entre switches específicos, lo que recibe el nombre de agregado de enlaces. El agregado de enlaces logra un rendimiento superior entre los switches.

Redundancia

La redundancia es la duplicación de dispositivos, servicios o conexiones de modo que si falla, los dispositivos, servicios o conexiones puedan seguir trabajando en caso de que falle

3.Funcionalidad Poe y MDIx.

Funcionalidad de PoE (Power over Ethernet):

(PoE) permite que el switch suministre energía a un dispositivo por el cableado de Ethernet existente. Es más flexible al poder instalar dispositivos donde tenga conexiones Ethernet. Suele utilizarse en teléfonos ip y puntos de aceso.

MDIX (Interfaz cruzada dependiente del medio): es un puerto Ethernet que permite a estaciones de red (PC o workstations) conectar entre ellas usando un cable de red cruzado.

4.Caracteristicas de los Switch de la capa de acceso.

- Facilitan la conexión de los dispositivos de nodo final a la red.
- La seguridad de puerto permite que el switch decida cuántos y qué dispositivos específicos se permiten conectar al switch. La seguridad de puerto se aplica en la capa de acceso.
- La velocidad de puerto que se debe elegir entre los puertos de switch Fast Ethernet (100Mb/s) y Gigabit Ethernet (1000Mb/s).
- POE.
- El agregado de enlaces permite que el switch utilice enlaces múltiples simultáneamente.
- La velocidad interna de reenvío.
- Necesitan admitir QoS para mantener la prioridad del tráfico para una red convergente que admite tráfico de datos, voz y video.

5. Características de los Switches de la capa de distribución.

- Recopilan los datos de todos los switches de capa de acceso y los envían a los switches de capa núcleo.
- Proporcionan funciones de enrutamiento entre las VLAN para que una VLAN pueda comunicarse con otra en la red.
- Reducen la necesidad de que los switches núcleo realicen la tarea, debido a que el núcleo está ocupado con el tráfico. Debido a que el enrutamiento entre las VLAN se realiza en la capa de distribución, los switches en esta capa necesitan admitir las funciones de la Capa 3.
- Políticas de seguridad: Se utilizan listas de acceso para controlar cómo fluye el tráfico a través de la red. Una Lista de control de acceso (ACL, Access Control List) permite que el switch impida ciertos tipos de tráfico y autorice otros. Las ACL también permiten controlar qué dispositivos de red pueden comunicarse en la misma.
- Calidad de servicio: necesitan admitir QoS para mantener la prioridad del tráfico que proviene de los switches de capa de acceso que implementaron QoS. Así se garantiza un ancho de banda adecuado para las comunicaciones de audio y video.
- Admitir redundancia para una disponibilidad adecuada.
- Necesitan admitir el agregado de enlaces para asegurar el ancho de banda y el tráfico que proviene de los switches de la capa de acceso.

6. Características de los Switch de la capa de núcleo.

- Requiere switches que pueden manejar tasas muy altas de reenvío.
- Agregado de enlaces para asegurar el ancho de banda adecuado que ingresa al núcleo proveniente de los switches de capa de distribución.
- Redundancia más veloz.
- QoS es una parte importante de los servicios prestados por los switches de capa núcleo. Por ejemplo, los prestadores de servicios.

TEMA 2

7. Funcionalidad de CSMA/CD.

El conjunto de normas que utiliza Ethernet se basa en la tecnología de acceso múltiple por detección de portadora y detección de colisiones (CSMA/CD) IEEE y determinan cuál es la estación que puede tener acceso a la red.

-Detección de portadora

Detección de portadora: en el método de acceso CSMA/CD, todos los dispositivos de red que tienen mensajes para enviar deben escuchar antes de transmitir.

-Acceso múltiple

Acceso múltiple: dos dispositivos comienzan a transmitir señales. Cuando se encuentran los mensajes se produce una colisión pero la mezcla de señales continúa propagándose en el medio.

-Detección de colisiones

Cuando un dispositivo está en el modo de escucha, puede detectar cuando se produce una colisión en la red.

Todos los dispositivos que estén transmitiendo en ese momento lo seguirán haciendo para garantizar que todos los dispositivos en la red puedan detectar la colisión.

-Señal de congestión y postergación aleatoria

Cuando se detecta una colisión, los dispositivos de transmisión envían una señal de congestionamiento. La señal de congestionamiento avisa a los demás dispositivos acerca de la colisión para que éstos invoquen un algoritmo de postergación para que todos los dispositivos detengan su transmisión.

8.Unicast, multicast y broadcast.

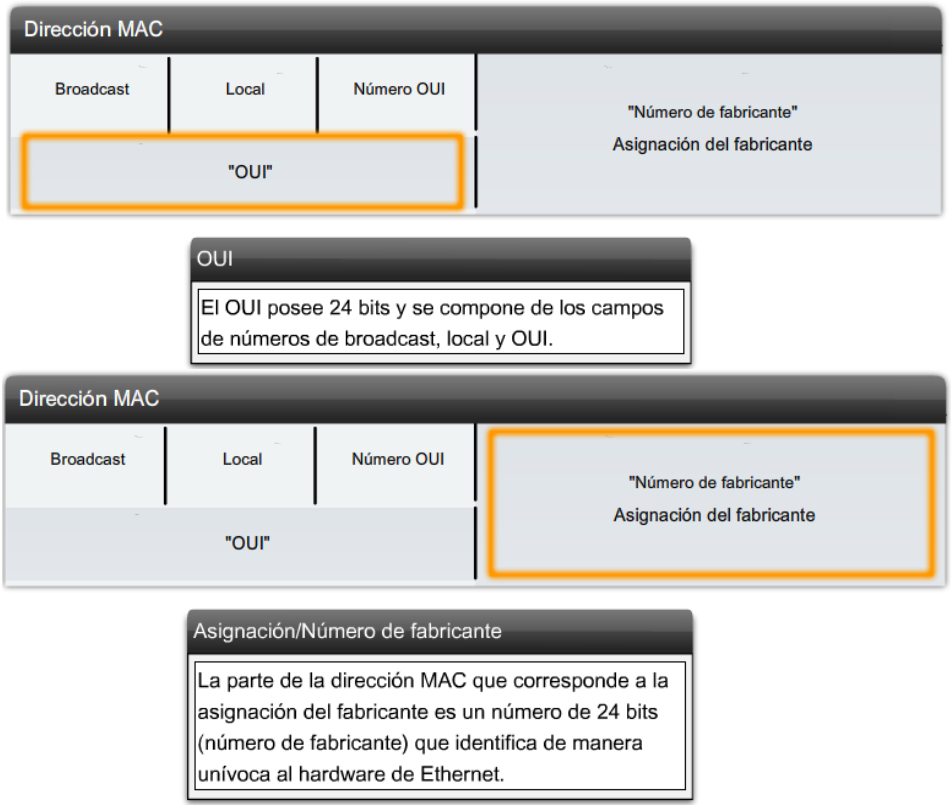
Unicast: Comunicación en la que un host envía una trama a un destino específico. Algunos ejemplos de protocolos que usan transmisiones unicast son: HTTP, FTP y Telnet.

Multicast: Comunicación en la que se envía una trama a un grupo específico de dispositivos o clientes. Un ejemplo de transmisión multicast son las transmisiones de voz y video relacionadas con las reuniones de negocios en conferencia basadas en la red.

Broadcast: Comunicación en la que se envía una trama desde una dirección hacia todas las demás direcciones. En este caso, existe sólo un emisor pero se envía la información a todos los receptores conectados. Un ejemplo de transmisión broadcast es la consulta ARP

9. Dirección Mac y ejemplos.

Una dirección Ethernet MAC es un valor binario de 48 bits que se compone de dos partes y se expresa como 12 dígitos hexadecimales. Por ejemplo: 00-05-9A-3C-78-00

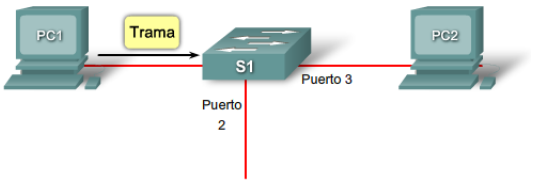


10.Half duplex y full duplex.

Half Duplex: La comunicación half-duplex se basa en una circulación de datos en un sentido en el que el envío y la recepción de datos no se producen al mismo tiempo.
La comunicación half-duplex implementa el CSMA/CD con el objeto de reducir las posibilidades de que se produzcan colisiones y detectarlas en caso de que se presenten. Presentan problemas de funcionamiento debido a la constante espera, ya que la circulación de datos se realiza en un sentido a la vez

Full duplex: En las comunicaciones full-duplex el flujo de datos es bidireccional, por lo tanto la información puede enviarse y recibirse al mismo tiempo. Mejora el rendimiento, dado que reduce el tiempo de espera entre las transmisiones. Actualmente, la mayoría de las tarjetas NIC Ethernet proporciona full-duplex. El circuito de detección de colisiones se encuentra desactivado dado que las tramas no pueden colisionar. Cada conexión full-duplex utiliza un solo puerto. Las conexiones full-duplex requieren un switch que admita esta modalidad.

11.Funcionamiento de una tabla MAC en un switch. Comandos.



Los switches emplean direcciones MAC para dirigir las comunicaciones de red a través de su estructura al puerto correspondiente hasta el nodo de destino.

A continuación se describe este proceso:

Paso 1. El switch recibe una trama de broadcast de la PC 1 en el Puerto 1.

Paso 2. El switch ingresa la dirección MAC de origen y el puerto del switch que recibió la trama en la tabla de direcciones.

Paso 3. Dado que la dirección de destino es broadcast, el switch genera flooding en todos los puertos enviando la trama, excepto el puerto que la recibió.

Paso 4. El dispositivo de destino responde al broadcast con una trama de unicast dirigida a la PC 1.

Paso 5. El switch ingresa la dirección MAC de origen de la PC2 y el número de puerto del switch que recibió la trama en la tabla de direcciones. La dirección de destino de la trama y el puerto relacionado a ella se encuentran en la tabla de direcciones MAC.

Paso 6. Ahora el switch puede enviar tramas entre los dispositivos de origen y de destino sin saturar el tráfico, ya que cuenta con entradas en la tabla de direcciones que identifican a los puertos asociados.

12. Dominio de colisión y dominios de broadcast. (Practica).2.1.2.1 y 2.1.2.2
13. Latencia de la red y control de la misma.

La latencia es el tiempo que tarda una trama o a un paquete hacer el recorrido desde la estación origen hasta su destino final. Consiste:

-En primer lugar, el tiempo que toma la NIC origen en colocar pulsos de voltaje en el cable y el tiempo que tarda la NIC destino en interpretar estos pulsos.

-En segundo lugar, el retardo de propagación real, ya que la señal tarda un tiempo en recorrer el cable
En tercer lugar, la latencia aumenta según los dispositivos de red que se encuentren en la ruta entre dos dispositivos.

Control de latencia:

Se necesita tener en cuenta la latencia originada por cada dispositivo de la red. Por ejemplo si un switch da soporte a 10 puertos, trabajando cada puerto a 100 MB/s, el switch necesitara admitir 2000 MB/s para mantener la velocidad del cable a su perfecto funcionamiento.

Los dispositivos de la capa OSI más altas pueden aumentar la latencia de la red, por ejemplo si un dispositivo de capa 3 lo sometemos a realizar una tarea profunda de la trama de un dispositivo de capa 2, el tiempo de procesamiento será mayor, aumentando así la latencia

14. Método de reenvió de tramas de red.

Conmutación por almacenamiento y envío

Cuando el switch recibe la trama la almacena hasta recibir la trama en su totalidad. Durante el proceso de almacenamiento, el switch analiza la trama para buscar información acerca de su destino. En este proceso, el switch también lleva a cabo una verificación de errores utilizando la porción del tráiler de comprobación de redundancia cíclica (CRC, Cyclic Redundancy Check) de la trama de Ethernet.

Después de confirmar la integridad de la trama, ésta se envía desde el puerto correspondiente hasta su destino. Cuando se detecta un error en la trama, el switch la descarta.

Conmutación por método de corte

En este tipo de conmutación, el switch actúa sobre los datos cuando apenar los a recibido, incluso si la transmisión aún no se ha completado. El switch recopila sólo la información suficiente como para leer la dirección MAC de destino saber a qué puerto debe reenviar los datos.
El switch busca la dirección MAC de destino en su tabla de conmutación, determina el puerto de la interfaz de salida y reenvía la trama a su destino mediante el puerto de switch designado., la conmutación por método de corte es más rápida ya que no tiene que comprobar la trama ni esperar la totalidad de ella . Puede reenvía tramas dañadas por no comprobarlo

Presenta dos variantes:

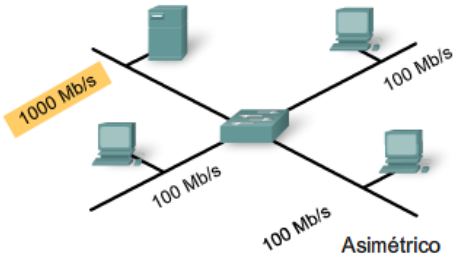
- Conmutación por envío rápido: reenvía el paquete inmediatamente después de leer la dirección de destino.

- Conmutación libre de fragmentos: el switch almacena los primeros 64 bytes de la trama antes de reenviarla.

15. Conmutación asimétrica y simétrica de un switch.

Asimétrica

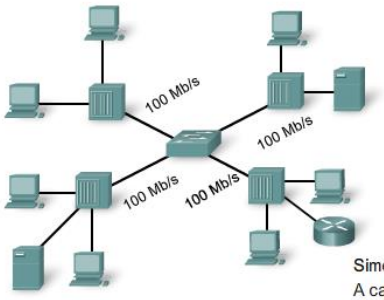
La conmutación asimétrica permite un mayor ancho de banda dedicado al puerto de conmutación del servidor para evitar que se produzca un cuello de botella. Esto brinda una mejor calidad en el flujo de tráfico, donde varios clientes se comunican con un servidor al mismo tiempo. Se requieren buffers de memoria en un switch asimétrico. Para que el switch coincida con las distintas velocidades de datos en los distintos puertos, se almacenan tramas enteras en los búferes de memoria y se envían al puerto una después de la otra según se requiera.



Asimétrico
Se asigna más ancho de banda al puerto conectado al servidor.

Simétrica

En un switch simétrico, todos los puertos cuentan con el mismo ancho de banda. La conmutación simétrica se ve optimizada por una distribuir el tráfico de manera uniforme.
El administrador de red evalúa la cantidad de ancho de banda que se necesita para las conexiones adaptadas a las necesidades.



Simétrico
A cada puerto del switch se le asigna el mismo ancho de banda.

16. Tipo de búfer de memoria de un switch.

Los buffer de memoria se utilizan para almacenar tramas antes de enviarlas. Existen:

Búfer de memoria basada en puerto: Las tramas se almacenan en una lista que están conectadas a puertos de entrada específicos.
Una trama se transmite al puerto de salida una vez que las tramas que están delante se han trasmitido. Una trama puede retardar todas las tramas almacenadas en la memoria debido al tráfico del destino.

Búfer de memoria compartida: Deposita todas las tramas en un búfer de memoria común que comparten todos los puertos del switch. A las tramas en el búfer se le asigna un puerto de destino. Esto permite la recepción del paquete por un puerto y la transmisión por otro puerto, sin tener que colocarlo en otra cola.

17. Diferencias entre un switch de capa 2, switch de capa 3 y un router. (no lo tengo)

Los switches de Capa 3 pueden enviar paquetes entre distintos segmentos de una LAN de modo similar que los routers dedicados.

Los routers proporcionan servicios adicionales de Capa 3 que los switches de Capa 3 no pueden realizar. Los routers también pueden llevar a cabo tareas de reenvío de paquetes que no realizan los switches de Capa 3, como establecer conexiones de acceso remoto con dispositivos y redes remotas. Los switches de Capa 3 ofrecen funciones básicas de enrutamiento en una LAN y reducen la necesidad de utilizar routers dedicados.

TEMA 3

18. Definición de VLAN. Beneficios de una VLAN y tipos de VLAN.

Una vlan permite crear grupos de dispositivos conectados a la red de manera lógico que actúan como si tuvieran su propia red independiente, incluso comparten la misma infraestructura. Se les puede asignar un nombre a cada vlan

Una vlan es una subred ip separada. Las vlan permiten que redes ip y subredes existan en la misma red.

Los principales beneficios de utilizar las VLAN son los siguientes:

- Seguridad: Los grupos se separan para que no se vean
- Reducción de costos: Ahorro en equipo
- Mejor rendimiento: Reduce el trafico innecesario en la red y potencia el rendimiento.
- Mitigación de la tormenta de broadcast: reduce la cantidad de dispositivos que participan en un broadcast.
- Mayor eficiencia del personal de TI: facilitan el trabajo al tener a usuarios con requerimientos similares.
- Administración de aplicación o de proyectos más simples: Es más fácil trabajar de manera separadas con vlan

Tipos de Vlan:

VLAN de datos: Una VLAN de datos es una VLAN configurada para enviar sólo tráfico de datos generado por el usuario. (la voz no cuenta)

VLAN predeterminada: Todos los puertos de switch pertenecen a una vlan predeterminada. Pertenecen al mimo dominio de broadcast. No se puede eliminar

VLAN nativa: Se asigna una VLAN nativa a un puerto troncal 802.1Q. Un puerto de enlace troncal 802.1 Q admite el tráfico que llega de muchas VLAN (tráfico etiquetado) como también el tráfico que no llega de una VLAN (tráfico no etiquetado).

VLAN de administración: Una VLAN de administración es cualquier VLAN que se configura para acceder a las capacidades administrativas de un switch.

19. Que es un enlace troncal y que resuelve.

Un enlace troncal es un enlace punto a punto entre dos dispositivos de red que lleva más de una VLAN. Un enlace troncal de VLAN le permite extender las VLAN a través de toda una red. Cicso admite IEEE 802.1Q para la coordinación de enlaces troncales en interfaces Fast Ethernet y Gigabit Ethernet. Aprenderá más adelante en esta sección acerca de 802.1Q.

Un enlace troncal de VLAN no pertenece a una VLAN específica, sino que es un conducto para las VLAN entre switches y routers.

El problema que resuelve un enlace troncal es que no necesitas un cable por cada subred, con un cable englobas todas las subredes de manera virtual.

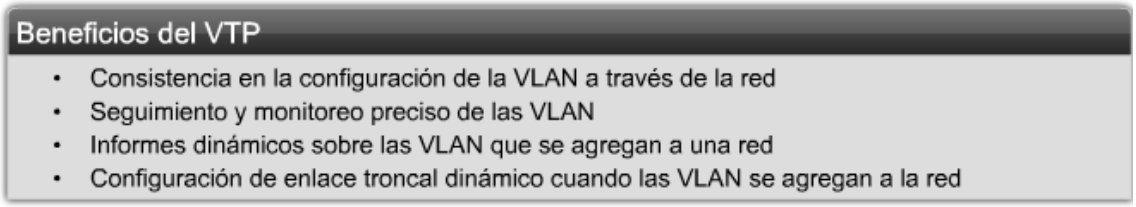
20. Protocolo 802.1Q.

Aunque se puede configurar un switch de Cisco para admitir dos tipos de puertos de enlace troncal, IEEE 802.1Q e ISL, en la actualidad sólo se usa el 802.1Q.
Un puerto de enlace troncal IEEE 802.1Q admite tráfico simultáneo etiquetado y sin etiquetar. A un puerto de enlace troncal 802.1Q se le asigna un PVID predeterminado y todo el tráfico sin etiquetar se transporta en el PVID predeterminado del puerto. El resto del tráfico se envía con una etiqueta de VLAN.

TEMA 4

21. Concepto de VTP. Beneficios del VTP.

El VTP permite a un administrador de red configurar un switch de modo que propagará las configuraciones de la VLAN hacia los otros switches en la red. El switch se puede configurar en la función de servidor del VTP o de cliente del VTP.



22. Componentes de VTP.

Componentes del VTP

- Dominio del VTP: consiste en uno o más switches interconectados.
- Publicaciones del VTP: el VTP usa una jerarquía de publicaciones para distribuir y sincronizar las configuraciones de la VLAN a través de la red.
- Modos del VTP: un switch se puede configurar en uno de tres modos: servidor, cliente o transparente.
- Servidor del VTP: los servidores del VTP publican la información VLAN del dominio del VTP a otros switches habilitados por el VTP en el mismo dominio del VTP. Los servidores del VTP guardan la información de la VLAN para el dominio en la NVRAM. El servidor es donde la VLAN puede ser creada, eliminada o redenominada para el dominio.
- Cliente del VTP: los clientes VTP funcionan de la misma manera que los servidores VTP pero no pueden crear, cambiar ni eliminar las VLAN en un cliente VTP. Un cliente del VTP sólo guarda la información de la VLAN para el dominio completo mientras el switch está activado. Un reinicio del switch borra la información de la VLAN. Debe configurar el modo de cliente VTP en un switch.
- VTP transparente: los switches transparentes envían publicaciones del VTP a los clientes VTP y servidores VTP. Los switches transparentes no participan en el VTP. Las VLAN que se crean, redenominan o se eliminan en los switches transparentes son locales a ese switch solamente.
- Depuración del VTP: la depuración del VTP aumenta el ancho de banda disponible para la red mediante la restricción del tráfico saturado a esos enlaces troncales que el tráfico debe utilizar para alcanzar los dispositivos de destino.

TEMA 5

23. ¿Que es STP?.¿Que algoritmo utiliza?

Protocolo que utiliza el algoritmo snanning-tree, para permitir que un puente rompa de forma dinámica los bucles que se producen en una topología de red. Los puertos intercambia BPDU para detectar bucles y eliminarlos apagando la interfaz

24. ¿Qué es una tormenta de Broadcast?. ¿Qué es una trama de unicast duplicada?. Como se produce un bucle en el armario de cableado.

<u>Tormentas de broadcast</u>

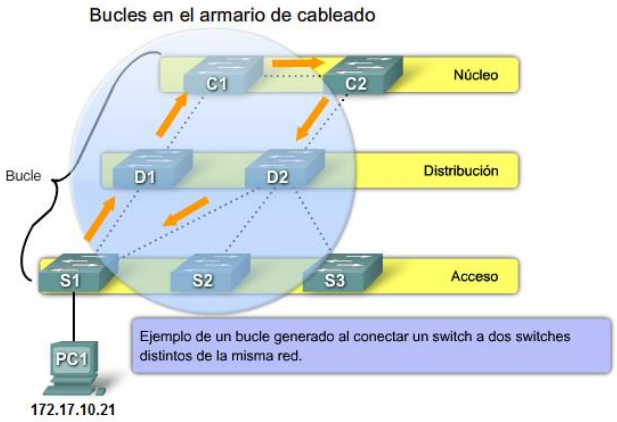
Una tormenta de broadcast se produce cuando existen tantas tramas de broadcast atrapadas en un bucle de Capa 2, que se consume todo el ancho de banda disponible.

<u>Tramas de unicast duplicadas</u>

Las tramas de unicast enviadas a una red con bucles, pueden que no contenga la dirección de destino y envie un broadcast generar tramas duplicadas.

Bucles en el armario de cableado

Conexiones duplicadas accidentalmente dentro de los armarios de cableado consecuencia de etiquetadas erróneas del cable



25. Describe el funcionamiento del algorimo STP.

STP utiliza el algoritmo de spanning tree (STA) para determinar los puertos de switch de la red que deben configurarse para el bloqueo a fin de evitar que se generen bucles. El STA designa un único switch como puente raíz y lo utiliza como punto de referencia para todos los cálculos de rutas.
Después de determinar el puente raíz, el STA calcula la ruta más corta hacia el mismo. Todos los switches utilizan el STA para determinar los puertos que deben bloquearse. Mientras el STA determina las mejores rutas hacia el puente raíz para todos los destinos del dominio de broadcast, se evita que todo el tráfico sea enviado a través de la red.

26.Describe la utilización de BPDU y BID en STP. ¿Para qué se utiliza?. Temporizadores de BPDOU. (mirar despacio porque no esta completo)

La trama de BPDU contiene 12 campos distintos que se utilizan para transmitir información de prioridad y de ruta que STP necesita para determinar el puente raíz y las rutas al mismo.

- Los primeros cuatro campos identifican el protocolo, la versión, el tipo de mensaje y los señaladores de estado.
- Los cuatro campos siguientes se utilizan para identificar el puente raíz y el costo de la ruta hacia éste.
- Los últimos cuatro campos son todos campos temporizadores que determinan la frecuencia en que se envían los mensajes de BPDU
-

Campos BID

El ID de puente (BID) se utiliza para determinar el puente raíz de una red

Temporizadores de BPDU

Tiempo de saludo	El tiempo de saludo es el tiempo que transcurre cada vez que una trama de BPDU es enviada a un puerto. Este valor está predeterminado en 2 segundos pero puede ajustarse al intervalo de 1 a 10 segundos.
Retardo de envío	El retardo de envío es el tiempo que transcurre en los estados de escuchar y aprender. Este valor es igual a 15 segundos de manera predeterminada para cada estado pero puede ajustarse al intervalo de 4 a 30 segundos.
Antigüedad máxima	El temporizador de antigüedad máxima controla la cantidad máxima de tiempo en que un puerto de switch guarda información de la configuración de la BPDU. Este valor está predeterminado en 20 segundos pero puede ajustarse al intervalo de 6 a 40 segundos.

27. Describe los terminos:

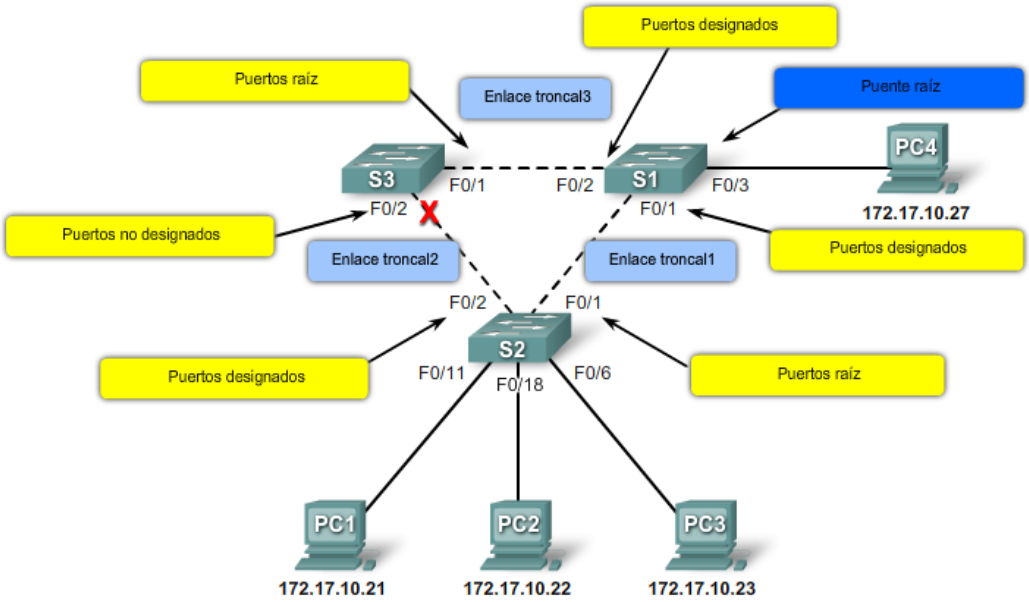
puente raíz describe la forma en que los puertos de switch se configuran para funciones específicas para evitar la posibilidad de bucles en la red y suministra medios en caso de fallas de la red.

Puertos raíz: los puertos de switch más cercanos al puente raíz.

Puertos designados: todos los puertos que no son raíz y que aún pueden enviar tráfico a la red.

Puertos no designados: todos los puertos configurados en estado de bloqueo para evitar los bucles.

Funciones de los puertos



28. Estado de los puertos del Switch en STP. Pasos de convergencia de STP.

Estados de los puertos

- Bloquear: el puerto es un puerto no designado y no participa en el envío de tramas.

- Escuchar: recibe tramas de BPDU y transmite sus propias tramas de BPDU e informa a los switches adyacentes que éste se preparado
- Aprender: el puerto se prepara para participar en el envío de tramas y comienza a llenar la tabla de direcciones MAC.
- Reenviar: envía tramas y envía y recibe tramas de BPDU.
- Deshabilitado: el puerto de la Capa 2 no participa en el spanning tree y no envía tramas..

<u>Pasos de convergencia de STP</u>

Paso 1. Elegir un puente raíz

Paso 2. Elegir los puertos raíz

Paso 3. Elegir los puertos designados y no designados

29. Tecnologia Portfast de CISCO. Variantes de Cisco y STP.

Cuando un switch de puerto configurado con PortFast se establece como puerto de acceso, sufre una transición del estado de bloqueo al de enviar de manera inmediata, saltando los pasos de escuchar y aprender. Puede utilizarse PortFast en puertos de acceso, conectados a una única estación de trabajo o servidor, para permitir que dichos dispositivos se conecten a la red de manera inmediata sin esperar la convergencia de spanning tree.

Variantes: PVST, PVST + , PVST + rápido, RSTP y MSTP

TEMA 6

30 ¿Que es el enrutamiento entre VLAN?.

Es un proceso para reenviar el tráfico de la red desde una VLAN a otra mediante un router. Las VLAN están asociadas a subredes IP únicas en la red. Los dispositivos en dichas VLAN envían el tráfico a través del router hasta llegar a otras VLAN.

31. Enrutamiento entre VLAN tradicional.

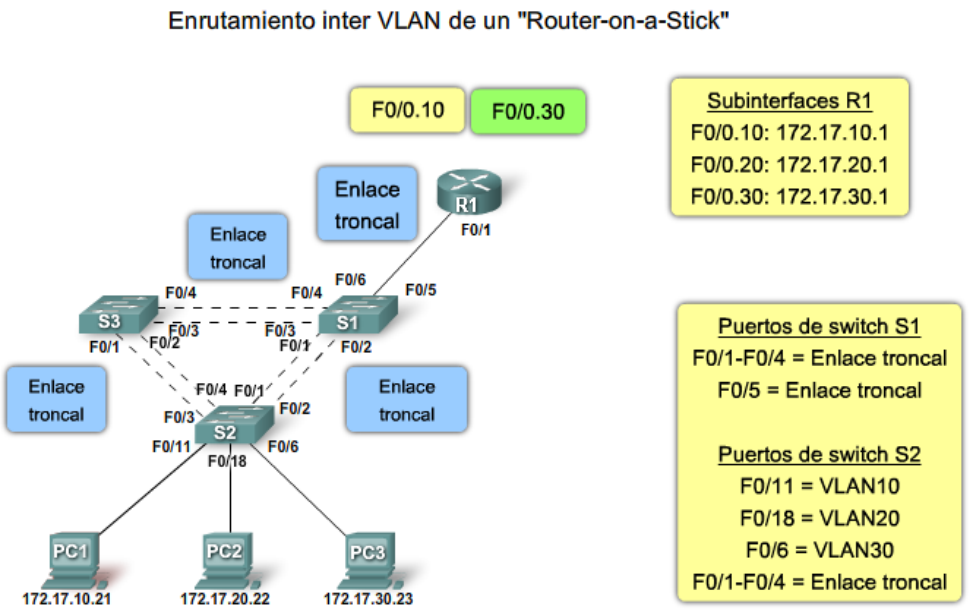
El enrutamiento de la LAN utiliza routers con interfaces físicas múltiples (varios cables). Es necesario conectar cada interfaz a una red separada (vlan).

En una red que utiliza varias VLAN dividir el tráfico de la red, el enrutamiento se realiza mediante varios cables a diferentes puertos del switch. Se asignan VLAN estáticas a cada interfaz del puerto.

32.Enrutamiento entre VLAN "Router-on-a-stick".

"Router-on-a-stick" es un tipo de configuración de router en la cual una interfaz enruta el tráfico entre múltiples VLAN en una red (es como si fueran todas las vlan por un mismo cable virtual).

La interfaz del router se configura para funcionar como enlace troncal y está conectada a un puerto del switch configurado en modo de enlace troncal. El router realiza el enrutamiento entre VLAN al aceptar el tráfico que viene etiquetado de la VLAN de la interfaz troncal del switch vecino y enrutar en forma interna entre las VLAN, mediante subinterfaces. El router luego reenvía el tráfico enrutado de la VLAN etiquetada para la VLAN de destino por la misma interfaz física.



TEMA 7

33. Tecnologías inalámbricas.

	PAN	LAN	MAN	WAN
Estándares	Bluetooth 802.15.3	802.11	802.11 802.16 802.20	GSM, CDMA, Satélite
Velocidad	< 1 Mbps	de 11 a 54 Mbps	10-100+ Mbps	10 Kbps-2 Mbps
Intervalo	Cortocircuito	Medio	Medio-Largo	Largo
Aplicaciones	Punto a punto Dispositivo a dispositivo	Redes de empresas	Acceso de última milla	Datos móviles Dispositivos

34. Comparación entre una WLAN y una VLAN.

Característica	LAN inalámbrica 802.11	Redes LAN Ethernet 802.3
Capa física	Radiofrecuencia (RF)	Cable
Acceso de medios	Prevención de colisión	Detección de colisiones
Disponibilidad	Cualquiera con una radio NIC en el rango de un punto de acceso	Se requiere conexión por cable
Interferencia en la señal	Sí	Irrelevante
Regulación	Regulación adicional a cargo de las autoridades locales	El estándar IEEE dictamina

35. Estándares de LAN inalámbricas. ¿Que es la certificación WI-FI?.

Estándares de LAN inalámbricas

	802.11a	802.11b	802.11g		802.11n
Banda	5,7 GHz	2,4 GHz	2,4 GHz		No confirmado Posiblemente bandas 2,4 y 5 GHz
Canales*	Hasta 23	3	3		
Modulación	OFDM	DSSS	DSSS	OFDM	MIMO-OFDM
Velocidad de los datos	Hasta 54 Mbps	Hasta 11 Mbps	Hasta 11 Mbps	Hasta 54 Mbps	Se especula que será 248 Mbps para dos streams MIMO
Pros	~150 pies o 35 metros	~150 pies o 35 metros	~150 pies o 35 metros		~230 pies o 70 metros
Contras	Octubre de 1999	Octubre de 1999	Junio de 2003		Esperado para el 2008
Pros	Rápido, menos susceptible a interferencias	Bajo costo, buen alcance	Rápido, buen alcance, difícil de obstruir		Buenas velocidades de transferencia de datos, alcance mejorado
Contras	Costo superior, menor alcance	Lenta, susceptible a interferencias	Susceptible a interferencias desde aplicaciones que operan en la banda de 2,4 GHz		

La Wi-Fi Alliance es una asociación de proveedores cuyo objetivo es mejorar la interoperabilidad de productos que están basados en el estándar 802.11, y certifica proveedores en conformidad con las normas de la industria. La certificación incluye las tres tecnologías RF IEEE 802.11, y los estándares de seguridad WPA y WPA2 basados en IEEE 802.11i.

36. Componentes de infraestructura inalámbricas.

-Los nic capturadores de señales inalambricas que permiten a un dispositivo utilizar una red.
-Un punto de acceso conecta a los clientes (o estaciones) inalámbricos a la LAN cableada. Convierte los paquetes de datos TCP/IP desde su formato de encapsulación en el aire 802.11 al formato de trama de Ethernet 802.3 en la red Ethernet conectada por cable.
-Los routers inalámbricos cumplen el rol de punto de acceso, switch Ethernet y router.

37. Describe el funcionamiento de CASMA/CA. (mirar)

Los puntos de acceso supervisan una función de coordinación distribuida (DCF) llamada acceso múltiple por detección de portadora con prevención de colisiones (CSMA/CA). Esto simplemente significa que los dispositivos en una WLAN deben detectar la energía del medio y esperar hasta que éste se libere antes de enviar. Si un punto de acceso recibe información desde la estación de un cliente, le envía un acuse de recibo para confirmar que se recibió la información. Este acuse de recibo evita que el cliente suponga que se produjo una colisión e impide la retransmisión de información por parte del cliente.

38. Describe los terminos Beacon, Ad-hoc, BSS y ESS.

Redes Ad hoc

Las redes inalámbricas pueden que operan sin punto de acceso. Los clientes que utilizan el modo ad hoc configuran sus parámetros entre ellas.

Conjunto de servicios básicos (BSS)

Los puntos de acceso proporcionan una infraestructura que agrega servicios y mejora el alcance para los clientes. Un punto de acceso simple en modo infraestructura administra los parámetros inalámbricos y la topología es simplemente un BSS.

Conjuntos de servicios extendidos

Cuando un BSS simple no proporciona la suficiente cobertura RF, se pueden unir uno o más a través de un sistema de distribución simple hacia un conjunto de servicios extendidos (ESS).

Beacons - Tramas que utiliza la red WLAN para comunicar su presencia.

40. Descripción general de la configuración del punto de acceso inalámbrico. Parámetros configurables en los puntos finales inalámbricos.

- Paso 1: Verificar el funcionamiento local por cable de DHCP y el acceso a Internet
- Paso 2: Instalar el punto de acceso
- Paso 3: Configurar el punto de acceso SSID (sin seguridad todavía)
- Paso 4: Instalar un cliente inalámbrico (sin seguridad todavía)
- Paso 5: Verificar el funcionamiento de la red inalámbrica
- Paso 6: Configurar la seguridad inalámbrica WPA2 con PSK
- Paso 7: Verificar el funcionamiento de la red inalámbrica

Configuraciones inalámbricas básicas

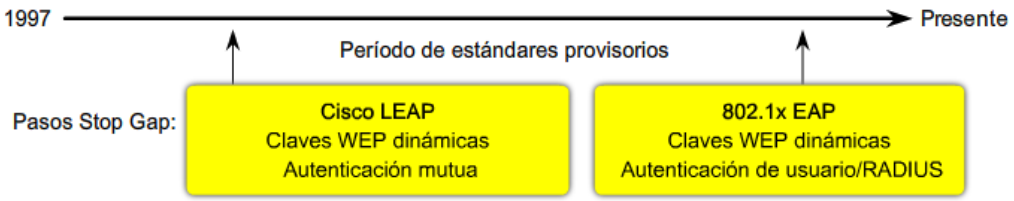
- Network Mode
- Network Name (SSID)
- SSID Broadcast
- Radio Band
- Wide Channel
- Standard Channel

39. Tipos de autenticación en el estándar 802.11. Mecanismos de encriptación en el estándar 802.11.

Descripción general del protocolo inalámbrico

Pasos principales para proteger una WLAN

Acceso abierto	Encriptación de primera generación	Provisoria	Presente
SSID	WEP	WPA	802.11i/WPA2
• Sin encriptación • Autenticación básica • Manejo no seguro	• Sin autenticación fuerte • Claves estáticas, frágiles • No escalable	• Estandarizada • Encriptación mejorada • Autenticación fuerte, basada en el usuario (por ejemplo, LEAP, PEAP, EAP-FAST)	• Encriptación AES • Autenticación: 802.1X • Administración de clave dinámica • WPA2 es la implementación Wi-Fi Alliance de 802.11i



Encriptación: Hay dos mecanismos de encriptación a nivel empresa especificados por el 802.11i certificados como WPA y WPA2 por la Wi-Fi Alliance: Protocolo de integridad de clave temporal (TKIP) y Estándar de encriptación avanzada (AES).

Cuando configura los puntos de acceso Linksys o los routers inalámbricos, puede que no vea el WPA o el WPA2. En lugar de eso, podrá ver algo llamado clave precompartida (PSK). Algunos de los distintos tipos de PSK son:

- PSK o PSK2 con TKIP es el mismo que WPA
- PSK o PSK2 con AES es el mismo que WPA2
- PSK2, sin un método de encriptación especificado, es el mismo que WPA2

PRACTICA

Tradicional

enable
conf t
interface fa0/3
switchport mode access
switchport access vlan 20
end

conf t
interface fa0/4
switchport mode access
switchport access vlan 30
end

copy run startup

Vtp

enable
show vtp status (ver el estado del vtp)
conf t
vtp domain PAR (poner el nombre del dominio)
vtp version 2 (poner el numero de versión)
vtp password asir (poner la contraseña)
vtp mode trnasparent(poner el vtp en modo cliente, trnasparente o servidor)

poner los enlaces troncales
crear las vlan (solo en el servidor)

enable
conf t
vtp domain PAR
vtp version 2
vtp password asir
vtp mode client
exit
copy run startup

conf t

interface fa0/1
switchport mode trunk
end
copy run startup

enable
conf t
vlan 10
name Estudiantes
end
copy run startup

Router on a stick

(router)
conf t
interface fa0/1.10 (crear subinterfaces virtuales en el puerto conectado y se suele poner el de la vlan)

encapsulation dot1q 10 (encapsularlo segun el protocolo y ponerle el numero de la vlan)
ip address 192.168.50.254 255.255.255.0 (la dirección de la puerta de enlace de la subinterfaz que queremos poner. La 192.168.50.0 sera la direccion de la sured)
interface f0/1.30
encapsulation dot1q 30
ip address 192.168.60.254 255.255.255.0

interface fa0/1 (dar de baja la subinterfaz)
no shutdown ( )

Vlan

configuración ip en el switch

conf t
interface vlan 99
ip address 172.17.99.11 255.255.0.0
no shutdown
end

Asignar a una interfaz una vlan

conf t
interface fast ethernet 0/18
switchport mode access
switchport acces vlan 99
end

---
crear vlan

enable
conf t
vlan 40
name ASIR
end
copy run startup

show vlan (vemos vlan creadas)

Troncal

conf t
interface fa0/5
switchport mode trunk
switchport trunk native vlan 1
end

Commandos sw
Dominio collision y dominio broadcast