Unidad 15: Protocolos y Servicios de Red de Nivel 2

Protocolo Ethernet

Un sistema Ethernet consiste de 3 elementos básicos que son:

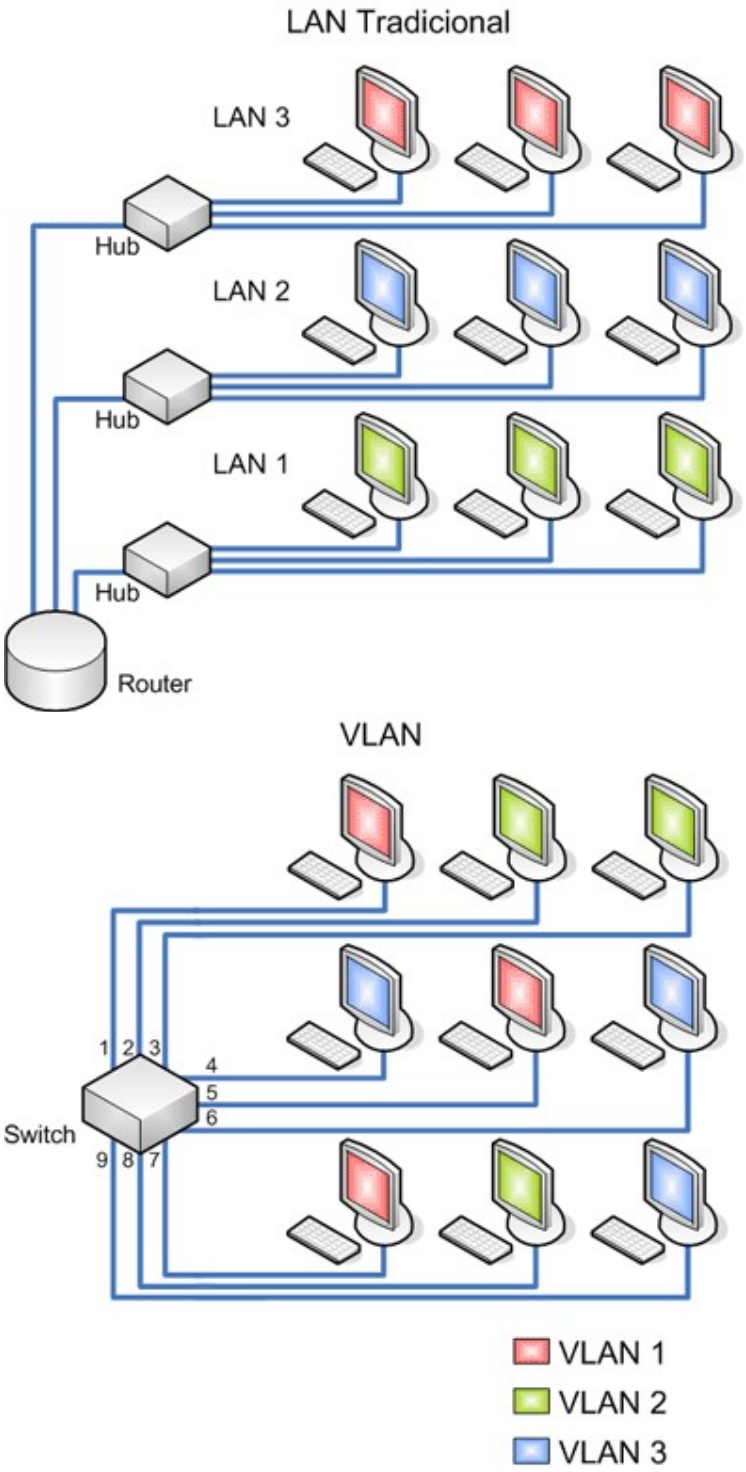
- El medio físico; utilizado para llevar las señales entre los dispositivos
- Un conjunto de reglas de control de acceso al medio, o protocolo, en cada interfaz Ethernet, que permite el acceso ordenado al canal Ethernet compartido.
- Un marco (trama) Ethernet, que consiste en un conjunto estandarizado de bits utilizado para llevar datos a través del sistema.

Funcionamiento de Ethernet

El protocolo de acceso al medio CSMA/CD, y el marco Ethernet son idénticos para todas las variantes de Ethernet, sin importar la velocidad de transmisión, sin embargo, cada dispositivo equipado con una interfaz Ethernet, también conocido como estación, opera de manera independiente de todas las demás estaciones en la red, no existe un controlador central. Todas las estaciones unidas al Ethernet son conectadas a un sistema de señalamiento compartido, también conocido como medio compartido que puede ser un cable, aire o una Fibra Óptica.
Las señales Ethernet son transmitidas de manera serial, una trama a la vez, sobre el canal, a todas las estaciones conectadas. Para enviar datos, una estación escucha el canal y cuando está sin transmisión, la estación transmite sus datos en la forma de un marco Ethernet o paquete.
Después de la transmisión de cada paquete, todas las estaciones en la red entran nuevamente en una contienda por la siguiente oportunidad de transmisión, lo cual asegura que el acceso al canal es equitativo, y ninguna estación puede asegurar el medio a otras estaciones. El acceso al canal compartido es determinado por el mecanismo de control de acceso al medio, integrado en la interfaz Ethernet de cada estación. El mecanismo de acceso al medio está basado en un sistema llamado Acceso Múltiple por Sensado de Portadora con Detección de Colisión (Carrier Sense Multiple Access with Collision Detect, CSMA/CD).
Las ventajas del protocolo Ethernet residen fundamentalmente en la simplicidad de su implementación y la velocidad que se puede lograr mejorando el control de las colisiones en redes pequeñas. Las desventajas justamente tienen que ver con el aumento logarítmico de las colisiones cuando el número de estaciones aumenta. Para solucionar esta desventaja, la primera y más sencilla solución es la implementación de Switches que separa los Dominios de Colisión y la segunda y un poco más sofisticada es la separación en Dominios de Broadcast con las Virtual LANS (VLAN).

Virtual LANS (VLANs)

Una red de área local (LAN) está definida como una red de computadoras dentro de un área geográficamente acotada como puede ser una empresa o una corporación. Uno de los problemas que nos encontramos estando todas las estaciones de trabajo en un mismo dominio de colisión es que el ancho de banda de la misma no es aprovechado correctamente. La solución a este problema es la división de la LAN en segmentos físicos los cuales fueran independientes entre si, dando como desventaja la imposibilidad de comunicación entre las LANs para algunos de los usuarios de la misma.
El mejor aprovechamiento del ancho de banda disponible dentro de la corporación ha llevado a la creación y crecimiento de las VLANs.
Una VLAN se encuentra conformada por un conjunto de dispositivos de red interconectados (hubs, bridges, switches o estaciones de trabajo) la definimos como como una subred definida por software y es considerada como un dominio de Broadcast que pueden estar en el mismo medio físico o bien puede estar sus integrantes ubicados en distintos sectores de la corporación.



La tecnología de las VLANs se basa en el empleo de Switches, en lugar de hubs, de tal manera que esto permite un control más inteligente del tráfico de la red, ya que este dispositivo trabaja a nivel de la capa 2 del modelo OSI y es capaz de aislar el tráfico, para que de esta manera la eficiencia de la red entera se incremente. Por otro lado, al distribuir a los usuarios de un mismo grupo lógico a través de diferentes segmentos, se logra el incremento del ancho de banda en dicho grupo de usuarios.

Segmentación

Con los switches se crean pequeños dominios, llamados segmentos, conectando un pequeño hub de grupo de trabajo a un puerto de switch o bien se aplica microsegmentación la cual se realiza conectando cada estación de

trabajo y cada servidor directamente a puertos de switch teniendo una conexión dedicada dentro de la red, con lo que se consigue aumentar considerablemente el ancho de banda a disposición de cada usuario.

Una de las ventajas que se pueden notar en las VLAN es la reducción en el tráfico de la red ya que solo se transmiten los paquetes a los dispositivos que estén incluidos dentro del dominio de cada VLAN, una mejor utilización del ancho de banda y confidencialidad respecto a personas ajenas a la VLAN, alta performance, reducción de latencia, facilidad para armar grupos de trabajo.

Tipos de VLAN

VLAN Estáticas

Los puertos del switch están ya preasignados a las estaciones de trabajo.

Por puerto

Se configura por una cantidad "n" de puertos en el cual podemos indicar que puertos pertenecen a cada VLAN. Para la Figura 1 tendríamos en el Switch 9 puertos de los cuales el 1,5 y 7 pertenecen a la VLAN 1; el 2, 3 y 8 a la VLAN 2 y los puertos 4, 6 y 9 a la VLAN 3 como la tabla lo indica (Figura 2).

Puerto	VLAN
1	1
2	2
3	2
4	3
5	1
6	3
7	1
8	2
9	3

Figura 2

Ventajas:

- Facilidad de movimientos y cambios.
- Microsegmentación y reducción del dominio de Broadcast.
- Multiprotocolo: La definición de la VLAN es independiente del o los protocolos utilizados, no existen limitaciones en cuanto a los protocolos utilizados, incluso permitiendo el uso de protocolos dinámicos.

Desventajas:

- Administración: Un movimiento en las estaciones de trabajo hace necesaria la reconfiguración del puerto del switch al que está conectado el usuario. Esto se puede facilitar combinando con mecanismos de LAN Dinámicas.

Por dirección MAC

Los miembros de la VLAN están especificados en una tabla por su dirección MAC (Figura 3).

MAC	VLAN
12.15.89.bb.1d.aa	1
12.15.89.bb.1d.aa	2
aa.15.89.b2.15.aa	2
1d.15.89.6b.6d.ca	2
12.aa.cc.bb.1d.aa	1

Figura 3

Ventajas:

- Facilidad de movimientos: No es necesario en caso de que una terminal de trabajo cambie de lugar la reconfiguración del switch.
- Multiprotocolo.
- Se pueden tener miembros en múltiples VLANs.

Desventajas:

- Problemas de rendimiento y control de Broadcast: el tráfico de paquetes de tipo Multicast y Broadcast se propagan por todas las VLANs.
- Complejidad en la administración: En un principio todos los usuarios se deben configurar de forma manual las direcciones MAC de cada una de las estaciones de trabajo. También se puede emplear soluciones de DVLAN.

Por protocolo

Asigna a un protocolo una VLAN. El switch se encarga de dependiendo el protocolo por el cual venga la trama derivarlo a la VLAN correspondiente (Figura 4).

Protocolo	VLAN
IP	1
IPX	2
IPX	2
IPX	2
IP	1

Figura 4

Ventajas:

- Segmentación por protocolo.
- Asignación dinámica.

Desventajas

- Problemas de rendimiento y control de Broadcast: Por las búsquedas en tablas de pertenencia se pierde rendimiento en la VLAN.
- No soporta protocolos de nivel 2 ni dinámicos.

Por direcciones IP

Está basado en el encabezado de la capa 3 del modelo OSI. Las direcciones IP a los servidores de VLAN configurados. No actúa como router sino para hacer un mapeo de que direcciones IP están autorizadas a entrar en la red VLAN. No realiza otros procesos con la dirección IP.

Ventajas:

- Facilidad en los cambios de estaciones de trabajo: Cada estación de trabajo al tener asignada una dirección IP en forma estática no es necesario reconfigurar el switch.

Desventajas:

- El tamaño de los paquetes enviados es menor que en el caso de utilizar direcciones MAC.
- Perdida de tiempo en la lectura de las tablas.
- Complejidad en la administración: En un principio todos los usuarios se deben configurar de forma manual las direcciones MAC de cada una de las estaciones de trabajo.

Por nombre de usuario

Se basan en la autenticación del usuario y no por las direcciones MAC de los dispositivos.

Ventajas:

- Facilidad de movimiento de los integrantes de la VLAN.
- Multiprotocolo.

Desventajas:

- En corporaciones muy dinámicas la administración de las tablas de usuarios.

VLAN Dinámicas (DVLAN)

Las VLAN dinámicas son puertos del switch que automáticamente determinan a que VLAN pertenece cada puesto de trabajo. El funcionamiento de estas VLANs se basa en las direcciones MAC, direcciones lógicas o protocolos utilizados. Cuando un puesto de trabajo pide autorización para conectarse a la VLAN el switch chequea la dirección MAC ingresada previamente por el administrador en la base de datos de las mismas y automáticamente se configura el puerto al cual corresponde por la configuración de la VLAN. El mayor beneficio de las DVLAN es el menor trabajo de administración dentro del armario de comunicaciones cuando se cambian de lugar las estaciones de trabajo o se agregan y también notificación centralizada cuando un usuario desconocido pretende ingresar en la red.

Spanning Tree Protocol

(Spanning Tree Protocol) es un protocolo de red de nivel 2 de la capa OSI. Su función es la de gestionar la presencia de bucles en topologías de red debido a la existencia de enlaces redundantes (necesarios en muchos casos para garantizar la disponibilidad de las conexiones). El protocolo permite a los dispositivos de interconexión activar o desactivar automáticamente los enlaces de conexión, de forma que se garantice que la topología está libre de bucles. STP es transparente a las estaciones de usuario. Trabaja a nivel de los switches de interconexión.

Los bucles infinitos ocurren cuando hay rutas alternativas hacia una misma máquina o segmento de red destino. Estas rutas alternativas son necesarias para proporcionar redundancia, ofreciendo una mayor fiabilidad. Si existen varios enlaces, en el caso que uno falle, otro enlace puede seguir soportando el tráfico de la red. Los problemas aparecen cuando utilizamos dispositivos de interconexión de nivel de enlace, como un puente de red o un conmutador de paquetes.

Cuando hay bucles en la topología de red, los dispositivos de interconexión de nivel de enlace reenvían indefinidamente las tramas Broadcast, al no existir ningún campo TTL (Time To Live, *Tiempo de Vida*) en la Capa 2, al contrario que en la Capa 3. Se consume entonces una gran cantidad de ancho de banda, y en muchos casos la red queda inutilizada. Un router, por el contrario, sí podría evitar este tipo de reenvíos indefinidos. La solución consiste en permitir la existencia de enlaces físicos redundantes, pero creando una topología lógica libre de bucles. STP permite solamente una trayectoria activa a la vez entre dos dispositivos de la red (esto previene los bucles) pero mantiene los caminos redundantes como reserva, para activarlos en caso de que el camino inicial falle.

Si la configuración de STP cambia, o si un segmento en la red redundante llega a ser inalcanzable, el algoritmo reconfigura los enlaces y restablece la conectividad, activando uno de los enlaces de reserva.

Existen múltiples variantes del *Spaning Tree Protocol*, debido principalmente al tiempo que tarda el algoritmo utilizado en converger. Una de estas variantes es el Rapid Spanning Tree Protocol

El árbol de expansión (Spanning tree) permanece vigente hasta que ocurre un cambio en la topología, situación que el protocolo es capaz de detectar de forma automática. El máximo tiempo de duración del árbol de expansión es de cinco minutos. Cuando ocurre uno de estos cambios, el puente raíz actual redefine la topología del árbol de expansión o se elige un nuevo puente raíz.

Funcionamiento del protocolo STP

Cada switch es asignado a un grupo de identificadores (IDs), uno para el propio switch y otro para cada puerto en el switch. El identificador de switch, llamado el 'bridge ID', tiene 8 bytes de largo y contiene 2 bytes de prioridad acompañada con la dirección MAC, la cual tiene otros 6 bytes. Cada identificador de puerto tiene una longitud de 16 bits divididas en dos partes: 6 bits prioritarios y diez para el número de puerto.

Un coste de ruta es dado para cada puerto (path cost). Dicho coste es normalmente basado un procedimiento ya establecido la cual es parte del protocolo 801.2d. Según la especificación original, el coste es mil (1000) Mbps dividido por el ancho de banda del segmento conectado al puerto. Dependiendo de este ancho de banda, los costes pueden variar ligeramente, lo cual hace spanning-tree un sistema totalmente automatizado.

Cada switch comienza un proceso de descubrimiento para elegir los mejores caminos de red que debería usar para cada segmento. Esta información es compartida por todos los switches por medio de unas tramas especiales llamadas BPDUs (bridge protocol data units). Las partes de una BPDU es:

- El identificador root del bridge (BID) del propio bridge.
- El coste de ruta del root bridge, que determina lo lejos que está el root bridge.
- El identificador de puerto, que es el puerto del switch de donde el BPDU fue enviado.

Todos los switches están constantemente enviando BPDUs entre ellos, intentando determinar el camino más óptimo entre varios segmentos. Cuando un switch recibe un BPDU (de otro switch) que es mejor que el que está difundiendo desde el mismo segmento, parará de difundir sus BPDUs desde ese segmento. En lugar de eso, almacenará el BPDU del otro switch como referencia y para extenderlo a segmentos inferiores, es decir, los que están muy alejados desde el root bridge.

Un bridge root es elegido basado en el resultado del proceso BPDU entre switches. Inicialmente, todos los switches se consideran ellos mismos como roots. Cuando un switch arranca en una red, envía una BPDU con su propio identificador como si fuera root. Cuando los otros switches reciben el BPDU, comparan le identificador del bridge con el que tienen almacenado como el root bridge.

Si el nuevo identificador de root tiene un valor más bajo, sustituyen al que tienen almacenado en memoria. Pero si el que tienen ya guardado es menor, un BPDU es enviado al nuevo switch con el identificador del actual root bridge. El nuevo switch entiende que no puede ser el root bridge y reemplaza el ID de root que tiene con el que le han enviado. El resultado es que el switch con el BID más bajo, es elegido por todos los demás switches como root.

Basándose en la localización del root bridge, los otros switches determinan cuales de sus puertos tienen el menor coste al root bridge elegido. Estos puertos se llaman root ports, y cada switch (aparte del propio root bridge) deben tener uno.

Los switches determinan quienes tienen los puertos designados. Un puerto designado es la conexión usada para enviar y recibir paquetes en un segmento específico. Teniendo solo un puerto designado por segmento, todos los problemas de bucles están solucionados.

Los puertos designados son elegidos basados en la ruta de menor coste al root bridge para un segmento. Al tener el root bridge un coste de ruta de valor cero, cualquier puerto conectado a segmentos se convertirá en puerto designado. Si uno o más puertos tienen el mismo coste de ruta, entonces el switch con menor BID será elegido.

Una vez que ha sido elegido el puerto designado para un segmento de red, cualquier otro puerto que conecta con ese segmento se convierte en puerto no-designado. Bloquean y previenen tráfico de red de que pueda tomar ese camino, por lo que solo puede circular por los puertos asignados.

Cada switch tiene una tabla de BPDUs que está continuamente actualizándose. La red está configurada como una red spanning-tree teniendo un switch como la cabecera y todos los demás switches como extensiones que cuelgan de el. Cada switch comunica con el root bridge a través de sus puertos root, y con cada segmento por medio de los puertos designados. Con esto se consigue que la red esté libre de bucles.

En el caso de que el root bridge comience a fallar o tenga problemas de red, el protocolo de spanning-tree permite que todos los demás switches reconfiguren la red con otro switch que tome el relevo. Todo este proceso proporciona la posibilidad de tener una red compleja con una buena tolerancia a fallos y fácil de mantener.

Trunking

El **trunking** es una función para conectar dos switches, routers o servidores, del mismo modelo o no, mediante 2 cables en paralelo en modo Full-Duplex. Así se consigue un ancho de banda del doble para la comunicación entre los equipos. Esto permite evitar cuellos de botella en la conexión de varios segmentos y servidores. El protocolo es 802.1ad

Port Mirroring

El **puerto espejo** o **port mirroring** es utilizado con un switch de red para enviar copias de paquetes de red vistos en un puerto del switch (o una VLAN entera) a una conexión de red monitoreada en otro puerto del

switch. Esto es comunmente utilizado para aplicaciones de red que requieren monitorear el tráfico de la red, tal como una intrución-detección al sistema.

Sistemas de validación con protocolo 802.1x

La **IEEE 802.1X** es una norma del IEEE para el control de acceso a red basada en puertos. Es parte del grupo de protocolos IEEE 802 (IEEE 802.1). Permite la autenticación de dispositivos conectados a un puerto LAN, estableciendo una conexión punto a punto o previniendo el acceso por ese puerto si la autenticación falla. Es utilizado en algunos puntos de acceso inalámbricos cerrados y se basa en el protocolo de autenticación extensible (EAP– RFC 3748).

802.1X está disponible en ciertos switches y puede configurarse para autenticar nodos que están equipados con software *suplicante*. Esto elimina el acceso no autorizado a la red al nivel de la capa de enlace de datos.

Algunos proveedores están implementando 802.1X en puntos de acceso inalámbricos que pueden utilizarse en ciertas situaciones en las cuales el punto de acceso necesita operarse como un punto de acceso cerrado, corrigiendo deficiencias de seguridad de WEP. Esta autenticación es realizada normalmente por un tercero, tal como un servidor de RADIUS. Esto permite la autenticación sólo del cliente o, más apropiadamente, una autenticación mutua fuerte utilizando protocolos como EAP-TLS.

Radius

RADIUS (acrónimo en inglés de ***R**emote **A**uthentication **D**ial-**I**n **U**ser **S**erver*). Es un protocolo de autenticación y autorización (AAA) para aplicaciones de acceso a la red o movilidad IP. Utiliza el puerto 1812 UDP para establecer sus conexiones.

Cuando se realiza la conexión con un ISP mediante módem, DSL, cable módem, Ethernet o WiFi, se envía una información que generalmente es un nombre de usuario y una contraseña. Esta información se transfiere a un dispositivo Network Access Server (NAS) sobre el protocolo PPP, quien redirige la petición a un servidor RADIUS sobre el protocolo RADIUS. El servidor RADIUS comprueba que la información es correcta utilizando esquemas de autenticación como PAP, CHAP o EAP. Si es aceptado, el servidor autorizará el acceso al sistema del ISP y le asigna los recursos de red como una dirección IP, y otros parámetros como L2TP, etc.

Una de las características más importantes del protocolo RADIUS es su capacidad de manejar sesiones, notificando cuando comienza y termina una conexión, así que al usuario se le podrá determinar su consumo y facturar en consecuencia; los datos se pueden utilizar con propósitos estadísticos.

Los servidores Proxy RADIUS se utilizan para una administración centralizada y pueden reescribir paquetes RADIUS al vuelo (por razones de seguridad, o hacer conversiones entre dialectos de diferentes fabricantes)....

RADIUS es extensible; la mayoría de fabricantes de software y hardware RADIUS implementan sus propios dialectos.

Protocolos de LAN inalámbricas

Descripción general de las redes LAN inalámbricas

Las redes LAN inalámbricas de alta velocidad ofrecen las ventajas de la conectividad de red sin las limitaciones que supone estar atado a una ubicación o por cables. Existen numerosos escenarios en los que este hecho puede ser de interés; entre ellos, se pueden citar los siguientes.

Las conexiones inalámbricas pueden ampliar o sustituir una infraestructura con cables cuando es costoso o está prohibido tender cables. Las instalaciones temporales son un ejemplo de una situación en la que la red inalámbrica tiene sentido o incluso es necesaria. Algunos tipos de construcciones o algunas normativas de construcción pueden prohibir el uso de cableado, lo que convierte a las redes inalámbricas en una importante alternativa.

Y, por supuesto, el fenómeno asociado al término "inalámbrico", es decir, no tener que instalar más cables además de los de la red de telefonía y la red de alimentación eléctrica, ha pasado a ser el principal catalizador para las redes domésticas y la experiencia de conexión desde el hogar.

Los usuarios móviles, cuyo número crece día a día, son indudables candidatos a las redes LAN inalámbricas. El acceso portátil a las redes inalámbricas se realiza a través de equipos portátiles y NIC inalámbricas. Esto permite al usuario viajar a distintos lugares (salas de reunión, vestíbulos, salas de espera, cafeterías, aulas, etc.) sin perder el acceso a los datos de la red. Sin el acceso inalámbrico, el usuario tendría que llevar consigo pesados cables y disponer de conexiones de red.

Más allá del campo empresarial, el acceso a Internet e incluso a sitios corporativos podría estar disponible a través de zonas activas de redes inalámbricas públicas. Los aeropuertos, los restaurantes, las estaciones de tren y otras áreas comunes de las ciudades se pueden dotar del equipo necesario para ofrecer este servicio. Cuando un trabajador que está de viaje llega a su destino, quizás una reunión con un cliente en su oficina, se puede proporcionar acceso limitado al usuario a través de la red inalámbrica local. La red reconoce al usuario de la otra organización y crea una conexión que, a pesar de estar aislada de la red local de la empresa, proporciona acceso a Internet al visitante.

En todos estos escenarios, vale la pena destacar que las redes LAN inalámbricas actuales basadas en estándares funcionan a alta velocidad, la misma velocidad que se consideraba vanguardista para las redes con cable hace tan solo unos años. El acceso del usuario normalmente supera los 11 MB por segundo, de 30 a 100 veces más rápido que las tecnologías de acceso telefónico o de las redes WAN inalámbricas estándar. Este ancho de banda es sin duda adecuado para que el usuario obtenga una gran experiencia con varias aplicaciones o servicios a través de PC o dispositivos móviles. Además, el avance en curso de estos estándares inalámbricos continúa aumentando el ancho de banda, con velocidades de 300 MBps.

Muchos proveedores de infraestructura están dotando de cable zonas públicas de todo el mundo. En los próximos 12 meses, la mayoría de los aeropuertos, centros de conferencias y muchos hoteles proporcionarán acceso de 802.11b a sus visitantes.

Protocolos Ethernet para LAN inalámbrica

Para mejorar el acceso a las LAN inalámbricas, se suele utilizar una modificación del protocolo CSMA/CD llamado CSMA/CA o CSMA/CAW, (**C**arrier **S**ense **M**ultiple **A**ccess **C**ollision **A**voidance for **W**ireless) donde la diferencia fundamental con el CSMA/CD es que el emisor estimule al receptor a enviar una trama corta que será detectada por las estaciones cercanas, evitando así transmitir durante la siguiente trama de datos.

Como A envíará una trama a B

– A envía una trama RTS a B

• RTS: Ready to Send
• Es una trama corta que contiene la longitud de la trama de datos a enviar.

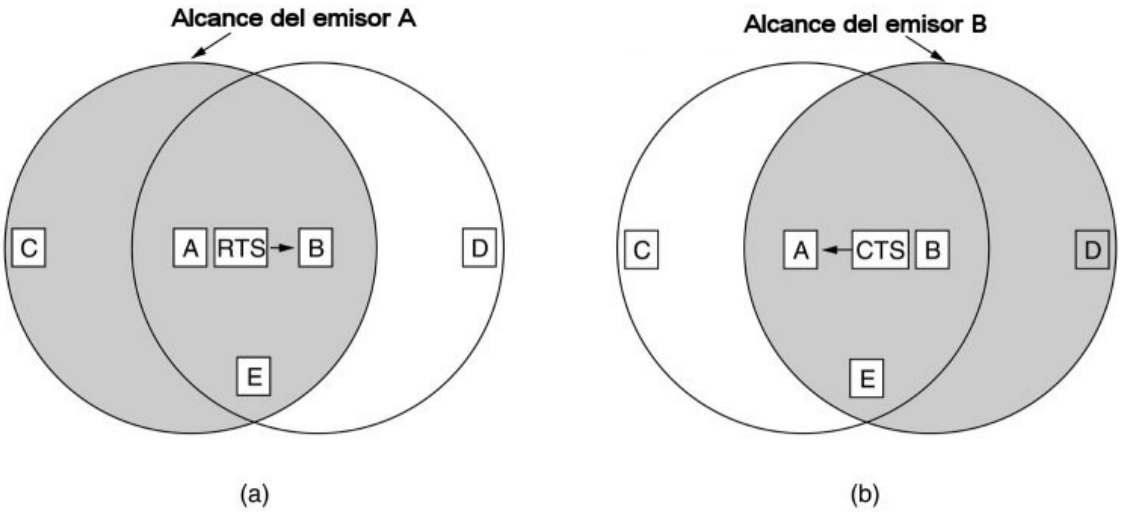
– B contesta con un trama CTS

• CTS: Clear To Send
• También contiene la longitud de los datos

– A recibe la trama CTS y comienza a transmitir

• Las estaciones que escuchan el RTS (cerca de A) permanecen en silencio para que A reciba el CTS
• Las estaciones que escuchan el CTS (cerca de B) permanecen en silencio durante la siguiente transmisión de datos.

– La longitud la obtiene de la trama CTS



Topologías de redes LAN inalámbricas

Las redes LAN inalámbricas se construyen utilizando dos topologías básicas. En este documento se utilizarán los términos "infraestructura" y "ad hoc".

Una topología de infraestructura es aquella que extiende una red LAN con cable existente para incorporar dispositivos inalámbricos mediante una estación base, denominada punto de acceso AP (Access point). El punto de acceso une la red LAN inalámbrica y la red LAN con cable y sirve de controlador central de la red LAN inalámbrica. El punto de acceso coordina la transmisión y recepción de múltiples dispositivos inalámbricos dentro de una extensión específica; la extensión y el número de dispositivos dependen del estándar de conexión inalámbrica que se utilice y del producto. En la modalidad de infraestructura, puede haber varios puntos de acceso para dar cobertura a una zona grande o un único punto de acceso para una zona pequeña, ya sea un hogar o un edificio pequeño.

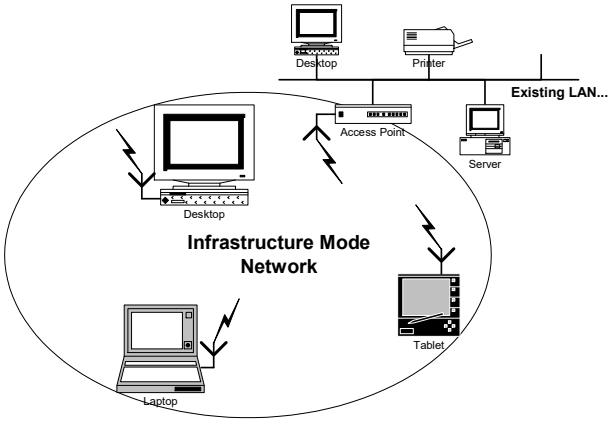


Figura 1. Red de la modalidad de infraestructura

En una topología ad hoc, los propios dispositivos inalámbricos crean la red LAN y no existe ningún controlador central ni puntos de acceso. Cada dispositivo se comunica directamente con los demás dispositivos de la red, en lugar de pasar por un controlador central. Esta topología es práctica en lugares en los que pueden reunirse pequeños grupos de equipos que no necesitan acceso a otra red. Ejemplos de entornos en los que podrían utilizarse redes inalámbricas ad hoc serían un domicilio sin red con cable o una sala de conferencias donde los equipos se reúnen con regularidad para intercambiar ideas.

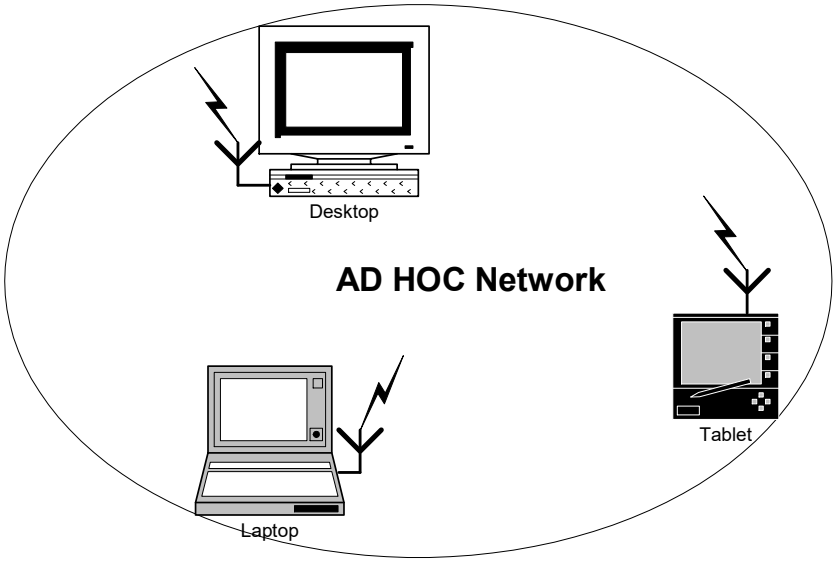


Figura 2. Red ad hoc

Por ejemplo, cuando se combinan con la nueva generación de software y soluciones par a par inteligentes actuales, estas redes inalámbricas ad hoc pueden permitir a los usuarios móviles colaborar, participar en juegos de equipo, transferir archivos o comunicarse de algún otro modo mediante sus PC o dispositivos inteligentes sin cables.

Descripción general del funcionamiento de la modalidad de infraestructura

El portátil o dispositivo inteligente, denominado "estación" en el ámbito de las redes LAN inalámbricas, primero debe identificar los puntos de acceso y las redes disponibles. Este proceso se lleva a cabo mediante el control de las tramas de señalización procedentes de los puntos de acceso que se anuncian a sí mismos o mediante el sondeo activo de una red específica con tramas de sondeo.

La estación elige una red entre las que están disponibles e inicia un proceso de autenticación con el punto de acceso. Una vez que el punto de acceso y la estación se han verificado mutuamente, comienza el proceso de asociación.

La asociación permite que el punto de acceso y la estación intercambien información y datos de capacidad. El punto de acceso puede utilizar esta información y compartirla con otros puntos de acceso de la red para diseminar la información de la ubicación actual de la estación en la red. La estación sólo puede transmitir o recibir tramas en la red después de que haya finalizado la asociación.

En la modalidad de infraestructura, todo el tráfico de red procedente de las estaciones inalámbricas pasa por un punto de acceso para poder llegar a su destino en la red LAN con cable o inalámbrica.

El acceso a la red se administra mediante un protocolo que detecta las portadoras y evita las colisiones. Las estaciones se mantienen a la escucha de las transmisiones de datos durante un período de tiempo especificado antes de intentar transmitir (ésta es la parte del protocolo que detecta las portadoras). Antes de transmitir, la estación debe esperar durante un período de tiempo específico después de que la red está despejada. Esta demora, junto con la transmisión por parte de la estación receptora de una confirmación de recepción correcta, representan la parte del protocolo que evita las colisiones. Observe que, en la modalidad de infraestructura, el emisor o el receptor es siempre el punto de acceso.

Dado que es posible que algunas estaciones no se escuchen mutuamente, aunque ambas estén dentro del alcance del punto de acceso, se toman medidas especiales para evitar las colisiones. Entre ellas, se incluye una clase de intercambio de reserva que puede tener lugar antes de transmitir un paquete mediante un intercambio de tramas "petición para emitir" y "listo para emitir", y un vector de asignación de red que se mantiene en cada estación de la red. Incluso aunque una estación no pueda oír la transmisión de la otra estación, oirá la transmisión de "listo para emitir" desde el punto de acceso y puede evitar transmitir durante ese intervalo.

El proceso de movilidad de un punto de acceso a otro no está completamente definido en el estándar. Sin embargo, la señalización y el sondeo que se utilizan para buscar puntos de acceso y un proceso de

reasociación que permite a la estación asociarse a un punto de acceso diferente, junto con protocolos específicos de otros fabricantes entre puntos de acceso, proporcionan una transición fluida.

La sincronización entre las estaciones de la red se controla mediante las tramas de señalización periódicas enviadas por el punto de acceso. Estas tramas contienen el valor de reloj del punto de acceso en el momento de la transmisión, por lo que sirve para comprobar la evolución en la estación receptora. La sincronización es necesaria por varias razones relacionadas con los protocolos y esquemas de modulación de las conexiones inalámbricas.

Descripción general del funcionamiento de la modalidad ad hoc

Después de explicar el funcionamiento básico de la modalidad de infraestructura, del modo ad hoc se puede decir que no tiene punto de acceso. En esta red sólo hay dispositivos inalámbricos presentes. Muchas de las operaciones que controlaba el punto de acceso, como la señalización y la sincronización, son controladas por una estación. La red ad hoc no disfruta todavía de algunos avances como retransmitir tramas entre dos estaciones que no se oyen mutuamente.

Retos actuales de las redes LAN inalámbricas

Cuando un medio de red nuevo se introduce en un nuevo entorno siempre surgen nuevos retos. Esto es cierto también en el caso de las redes LAN inalámbricas. Algunos retos surgen de las diferencias entre las redes LAN con cable y las redes LAN inalámbricas. Por ejemplo, existe una medida de seguridad inherente en las redes con cable, ya que la red de cables contiene los datos. Las redes inalámbricas presentan nuevos desafíos, debido a que los datos viajan por el aire, por ondas de radio.

Otros retos se deben a las posibilidades únicas de las redes inalámbricas. Con la libertad de movimiento que se obtiene al eliminar las ataduras (cables), los usuarios pueden desplazarse de sala en sala, de edificio en edificio, de ciudad en ciudad, etc., con las expectativas de una conectividad ininterrumpida en todo momento.

Las redes siempre han tenido retos, pero éstos aumentan cuando se agrega complejidad, tal como sucede con las redes inalámbricas. Por ejemplo, a medida que la configuración de red continúa simplificándose, las redes inalámbricas incorporan características (en ocasiones para resolver otros retos) y métrica que se agrega a los parámetros de configuración.

Retos de seguridad

Una red con cable está dotada de una seguridad inherente en cuanto a que un posible ladrón de datos debe obtener acceso a la red a través de una conexión por cable, lo que normalmente significa el acceso físico a la red de cables. Sobre este acceso físico se pueden superponer otros mecanismos de seguridad.

Cuando la red ya no se sustenta con cables, la libertad que obtienen los usuarios también se hace extensiva al posible ladrón de datos. Ahora, la red puede estar disponible en vestíbulos, salas de espera inseguras, e incluso fuera del edificio. En un entorno doméstico, la red podría extenderse hasta los hogares vecinos si el dispositivo de red no adopta o no utiliza correctamente los mecanismos de seguridad.

Desde sus comienzos, 802.11 ha proporcionado algunos mecanismos de seguridad básicos para impedir que esta libertad mejorada sea una posible amenaza. Por ejemplo, los puntos de acceso (o conjuntos de puntos de acceso) 802.11 se pueden configurar con un identificador del conjunto de servicios (SSID). La tarjeta NIC también debe conocer este SSID para asociarlo al AP y así proceder a la transmisión y recepción de datos en la red. Esta seguridad, si se llegase a considerar como tal, es muy débil debido a estas razones:

- Todas las tarjetas NIC y todos los AP conocen perfectamente el SSID
- El SSID se envía por ondas de manera transparente (incluso es señalizado por el AP)
- La tarjeta NIC o el controlador pueden controlar localmente si se permite la asociación en caso de que el SSID no se conozca
- No se proporciona ningún tipo de cifrado a través de este esquema

Aunque este esquema puede plantear otros problemas, esto es suficiente para detener al intruso más despreocupado.

Las especificaciones 802.11 proporcionan seguridad adicional mediante el algoritmo WEP (Wired Equivalent Privacy). WEP proporciona a 802.11 servicios de autenticación y cifrado. El algoritmo WEP define el uso de una clave secreta de 40 bits para la autenticación y el cifrado, y muchas implementaciones de IEEE 802.11 también permiten claves secretas de 104 bits. Este algoritmo proporciona la mayor parte de la protección contra la escucha y atributos de seguridad física que son comparables a una red con cable.

Una limitación importante de este mecanismo de seguridad es que el estándar no define un protocolo de administración de claves para la distribución de las mismas. Esto supone que las claves secretas compartidas se entregan a la estación inalámbrica IEEE 802.11 a través de un canal seguro independiente del IEEE 802.11. El reto aumenta cuando están implicadas un gran número de estaciones, como es el caso de un campus corporativo.

Para proporcionar un mecanismo mejor para el control de acceso y la seguridad, es necesario incluir un protocolo de administración de claves en la especificación. Para hacer frente a este problema se creó específicamente el estándar 802.1x, que se describe más adelante en estas notas del producto.

Retos para los usuarios móviles

Cuando un usuario o una estación se desplaza de un punto de acceso a otro punto de acceso, se debe mantener una asociación entre la tarjeta NIC y un punto de acceso para poder mantener la conectividad de la red. Esto puede plantear un problema especialmente complicado si la red es grande y el usuario debe cruzar límites de subredes o dominios de control administrativo.

Si el usuario cruza un límite de subred, la dirección IP asignada originalmente a la estación puede dejar de ser adecuada para la nueva subred. Si la transición supone cruzar dominios administrativos, es posible que la estación ya no tenga permiso de acceso a la red en el nuevo dominio basándose en sus credenciales.

Más allá del simple desplazamiento dentro de un campus corporativo, otros escenarios de usuarios móviles son muy reales. Los aeropuertos y restaurantes agregan conectividad inalámbrica con Internet y las redes inalámbricas se convierten en soluciones de red populares para el hogar.

Ahora es más probable que el usuario pueda abandonar la oficina para reunirse con alguien de otra compañía que también disponga de una red inalámbrica compatible. De camino a esta reunión, el usuario necesita recuperar archivos desde la oficina principal y podría encontrarse en una estación de tren, un restaurante o un aeropuerto con acceso inalámbrico. Para este usuario sería de mucha utilidad poder autenticarse y utilizar esta conexión para obtener acceso a la red de la empresa. Cuando el usuario llegue a su destino, puede que no tenga permiso de acceso a la red local de la empresa que va a visitar. Sin embargo, sería fortuito que el usuario pudiera obtener acceso a Internet en este entorno extraño. Entonces, dicho acceso podría utilizarse para crear una conexión de red privada virtual con la red de su empresa. Después, el usuario podría irse a casa y desear conectarse a la red doméstica para descargar o imprimir archivos para trabajar esa tarde.

Ahora, el usuario se ha desplazado a una nueva red inalámbrica, que posiblemente incluso puede ser de la modalidad ad hoc.

Para este ejemplo, la movilidad es una situación que debe pensarse muy detenidamente. La configuración puede ser un problema para el usuario móvil, ya que las distintas configuraciones de red pueden suponer un reto si la estación inalámbrica del usuario no tiene capacidad para configurarse automáticamente.