TECNOLOGÍAS PARA REDES LAN INALÁMBRICAS

Ing. Maria Andrea Mora.
Universidad Rafael Belloso Chacín. Venezuela

RESUMEN

Una red inalámbrica presta esencialmente el mismo servicio que una red cableada tradicional. Sin embargo, la carencia de un cableado hace a la red mucho más flexible: la re-localización de un nodo es inmediata, a diferencia del trabajo que implica mover un nodo en una red convencional. Una red inalámbrica también es una ventaja cuando la disposición física del edificio haga imposible la instalación del cableado. Las redes inalámbricas son particularmente apropiadas para la utilización de computadores portátiles o dispositivos de telemetría, lo cual permite movilidad sin sacrificar las ventajas de estar conectado a una red. La excitante tecnología para redes LAN inalámbricas está naciendo como solución para implementaciones empresariales, públicas y domésticas. Para admitir estas implementaciones, se deben satisfacer varios desafíos. Las redes LAN inalámbricas se construyen utilizando dos topologías básicas. La topología de infraestructura, el cual el punto de acceso coordina la transmisión y recepción de múltiples dispositivos inalámbricos y una topología ad hoc, en el cual cada dispositivo se comunica directamente con los demás dispositivos de la red. Algunos retos surgen de las diferencias entre las redes LAN con cable y las redes LAN inalámbricas, entre los cuales se encuentran: los retos de seguridad, para usuarios móviles, de configuración, entre otros.

Palabras clave: red inalámbrica, red cableada, tecnología, topología.

ABSTRACT

A quick radio network essentially the same service that a twisted network traditional. Nevertheless, the deficiency of a wiring does to the much more flexible network: the re-location of a node is immediate, unlike the work that implies to move a node in a conventional network. A radio network also is an advantage when the physical disposition of the building makes the installation impossible of the wiring. The radio networks are particularly appropriate for the use of portable computers or devices of telemetry, which allows mobility without sacrificing the advantages to be connected to a network. The exciting technology for wireless networks LAN is being born like solution for enterprise, public and domestic implementations. In order to admit these implementations, several challenges are due to satisfy. Wireless networks LAN are constructed using two basic topologies. The infrastructure topology,

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 3 Edición No 1 – Año 2005

which the joining point coordinates the transmission and reception of multiple wireless devices and a topology ad hoc, in which each device communicates directly with the other devices of the network. Some challenges arise from the differences between networks LAN with cable and the wireless networks LAN, between which they are: the security challenges, movable users, configuration among others.

Key words: radio network, twisted network, technology, topology.

INTRODUCCIÓN

La disponibilidad de conexiones y redes LAN inalámbricas puede ampliar la libertad de los usuarios de la red a la hora de resolver varios problemas asociados a las redes con cableado fijo y, en algunos casos, incluso reducir los gastos de implementación de las redes.

Sin embargo, a pesar de esta libertad, las redes LAN inalámbricas traen consigo un nuevo conjunto de desafíos. Actualmente, existen varias soluciones de redes LAN inalámbricas, con distintos niveles de estandarización e interoperabilidad. Dos soluciones que hoy por hoy lideran el sector son HomeRF y Wi-Fi™ (IEEE 802.11b).

De estas dos, las tecnologías 802.11 disponen de una mayor aceptación en el mercado y están destinadas a solucionar las necesidades de las redes LAN inalámbricas para zonas activas empresariales, domésticas y públicas. La alianza Wireless Ethernet Compatibility Alliance trabaja para proporcionar certificados de compatibilidad con los estándares 802.11, lo que ayuda a garantizar la interoperabilidad entre los distintos fabricantes.

El amplio interés del sector para que exista interoperabilidad y compatibilidad entre los sistemas operativos ha permitido resolver algunas de las cuestiones relacionadas con la implementación de las redes LAN inalámbricas. Con todo, las redes LAN inalámbricas exponen nuevos retos en lo que respecta a la seguridad, la movilidad y la configuración. Durante el desarrollo del siguiente artículo, describen estos retos y se presentan algunas de las posibles soluciones de compatibilidad con una configuración rápida, seguridad 802.1x y otras innovaciones.

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

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 3 Edición No 1 – Año 2005

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

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 3 Edición No 1 – Año 2005

experiencia con varias aplicaciones o servicios a través de PC o dispositivos móviles. Además, los avances en curso de estos estándares inalámbricos continúa aumentando el ancho de banda, con velocidades de 22 MB.

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

COMPARACIÓN DE LAS TECNOLOGÍAS DE LAS REDES LAN INALÁMBRICAS

Actualmente, destaca la implementación de dos soluciones LAN inalámbricas. Se trata de los estándares IEEE 802.11, principalmente 802.11b, y la solución propuesta por el grupo de trabajo HomeRF. Ambas soluciones no son interoperables entre sí ni con otras soluciones de redes LAN inalámbricas. Mientras que HomeRF está diseñado exclusivamente para el entorno doméstico, 802.11b se está implementando en hogares, en la pequeña y mediana empresa, en grandes organizaciones y en un número cada vez mayor de zonas activas de redes inalámbricas públicas. Algunos de los principales distribuidores de portátiles los equipa o tiene previsto equiparlos con tarjetas NIC 802.11b internas.

A continuación se ofrece una comparación de las dos soluciones:

	IEEE 802.11b	**HomeRF**
Principales fabricantes que lo han admitido	Cisco, Lucent, 3Com WECA	Apple, Compaq, HomeRF Working Group
Estado	Se incluye	Se incluye (baja velocidad)
Extensión	50-300 pies (15,24-91,44 cm)	150 pies (45,72 cm)
Velocidad	11 Mbps	1, 2, 10 Mbps
Aplicación	Hogares, oficinas pequeñas, campus, empresas	Hogar
Costo	75-150 dólares por tarjeta	85-129 dólares
Seguridad	WEP/802.1x	NWID/cifrado
Distribuidores	Más de 75	Menos de 30
Puntos de acceso públicos	Más de 350	Ninguno
Cuota de mercado de las tarjetas NIC inalámbricas	72%	21%

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 3 Edición No 1 – Año 2005

TOPOLOGÍAS DE REDES LAN INALÁMBRICAS

Las redes LAN inalámbricas se construyen utilizando dos topologías básicas. Para estas topologías se utilizan distintos términos, como administradas y no administradas, alojadas y par a par, e infraestructura y "ad hoc". Estos términos están relacionados, esencialmente, con las mismas distinciones básicas de topología.

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. 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.

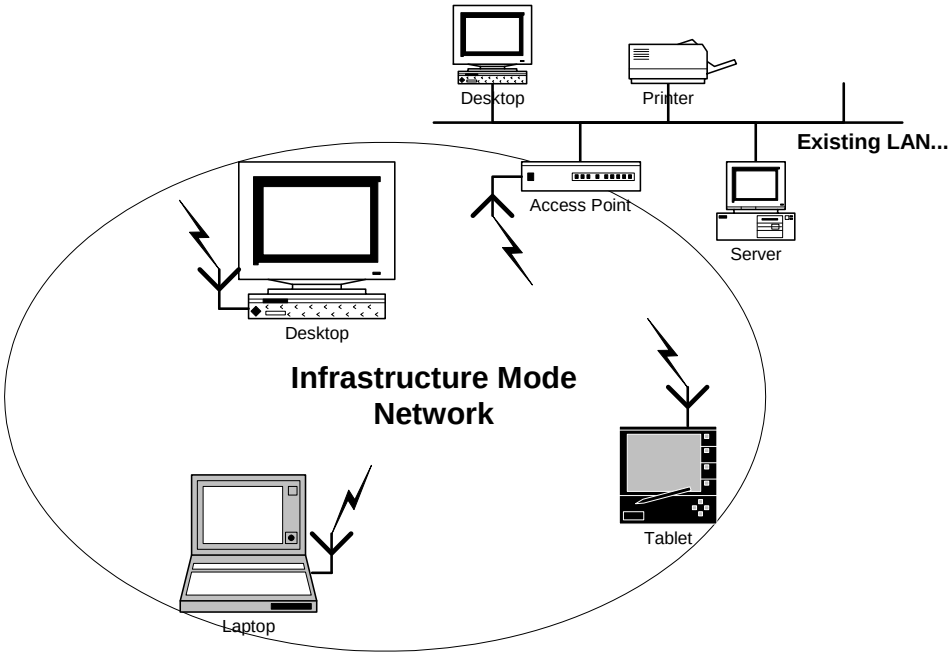


Figura 1. Red de la modalidad de infraestructura

En una topología ad hoc, los propios dispositivos inalámbricos crean la red LAN y no existe ningún controlador central ni puntos de acceso. Cada

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 3 Edición No 1 – Año 2005

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.

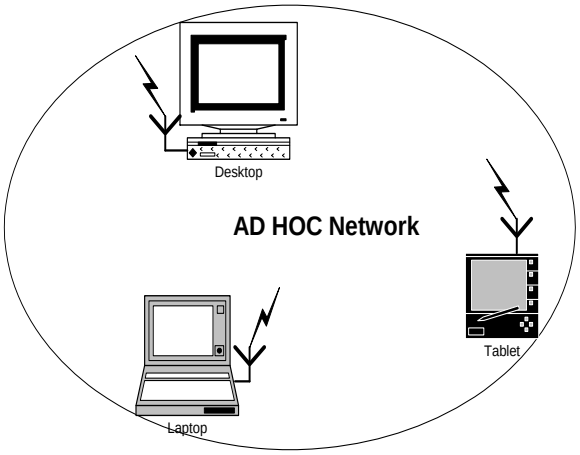


Figura 2. Red ad hoc

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.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 3 Edición No 1 – Año 2005

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 luego de haber 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, representa 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

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 3 Edición No 1 – Año 2005

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 reciente se introduce en un nuevo entorno siempre surgen desconocidos retos, esto se aplica 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 una persona no autorizada pueda 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.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 3 Edición No 1 – Año 2005

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

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.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 3 Edición No 1 – Año 2005

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.

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 de un conjunto de usuarios, 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.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 3 Edición No 1 – Año 2005

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.

RETOS DE CONFIGURACIÓN

Ahora que tenemos una conexión de red inalámbrica y la complejidad ha aumentado, posiblemente hay muchas más configuraciones que realizar. Por ejemplo, podría ser necesario configurar el SSID de la red a la que se va a realizar la conexión. También podría ser necesario configurar un conjunto de claves WEP de seguridad; posiblemente, varios conjuntos de claves si es necesario conectarse a varias redes. Podría ser necesario tener una configuración para el trabajo, donde la red funciona en modo de infraestructura, y otra configuración para el domicilio, donde funciona en modo ad hoc. Entonces, sería necesario elegir qué configuración se va a utilizar en función del lugar donde nos encontremos.

SOLUCIONES PARA LOS RETOS DE LAS REDES LAN INALÁMBRICAS

SEGURIDAD – 802.1X

Para ofrecer una mayor seguridad de la que proporciona WEP y definir IEEE 802.1X. 802.1X es un borrador de estándar para el control de acceso a redes basado en puerto que se utiliza para proporcionar acceso a red autenticado para las redes Ethernet. Este control de acceso a red basado en puerto utiliza las características físicas de la infraestructura LAN conmutada para autenticar los dispositivos conectados a un puerto LAN. Si el proceso de autenticación no se realiza correctamente, se puede impedir el acceso al puerto. Aunque este estándar se ha diseñado para redes Ethernet con cable, se puede aplicar a las redes LAN inalámbricas 802.11.

Concretamente, en el caso de las conexiones inalámbricas, el punto de acceso actúa como autenticador para el acceso a la red y utiliza un servidor del Servicio de usuario de acceso telefónico de autenticación remota (RADIUS) para autenticar las credenciales del cliente. La comunicación es posible a través de un “puerto no controlado” lógico o canal en el punto de acceso con el fin de validar las credenciales y obtener claves para obtener acceso a la red a través de un “puerto controlado” lógico. Las claves de que dispone el punto de acceso y el cliente como resultado de este intercambio permiten cifrar los datos del cliente y que el punto de acceso lo identifique.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 3 Edición No 1 – Año 2005

De este modo, se ha agregado un protocolo de administración de claves a la seguridad de 802.11.

De esta manera el estándar ha definido los siguientes pasos para describir el planteamiento genérico que se utilizaría para autenticar el equipo de un usuario de modo que obtenga acceso inalámbrico a la red.

- Sin una clave de autenticación válida, el punto de acceso prohíbe el paso de todo el flujo de tráfico. Cuando una estación inalámbrica entra en el alcance del punto de acceso, éste envía un reconocimiento a la estación.

- Cuando la estación recibe el reconocimiento, responde con su identidad. El punto de acceso reenvía la identidad de la estación a un servidor RADIUS que realiza los servicios de autenticación.

- Posteriormente, el servidor RADIUS solicita las credenciales de la estación, especificando el tipo de credenciales necesarias para confirmar su identidad. La estación envía sus credenciales al servidor RADIUS (a través del "puerto no controlado" del punto de acceso).

- El servidor RADIUS valida las credenciales de la estación (da por hecho su validez) y transmite una clave de autenticación al punto de acceso. La clave de autenticación se cifra de modo que sólo el punto de acceso pueda interpretarla.

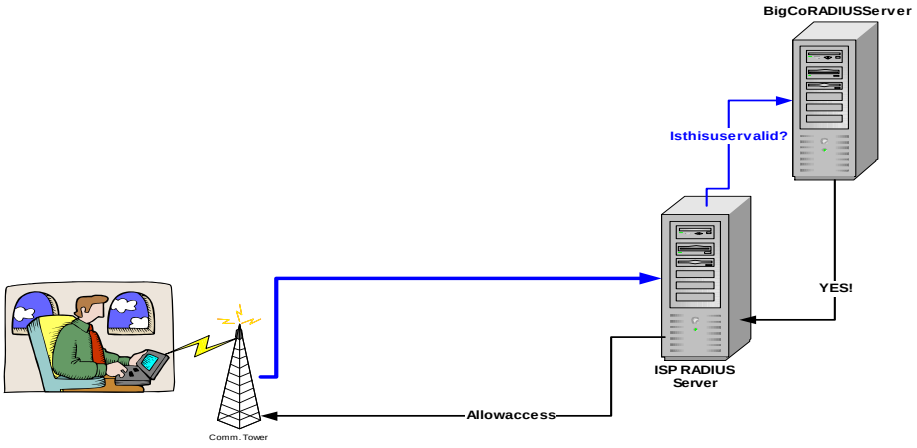
- El punto de acceso utiliza la clave de autenticación para transmitir de manera segura las claves correctas a la estación, incluida una clave de sesión de unidifusión para esa sesión y una clave de sesión global para las multidifusiones.

- Para mantener un nivel de seguridad, se puede pedir a la estación que vuelva a autenticarse periódicamente.

RADIUS SIMPLIFICA LA DIFICULTAD

Este planteamiento de 802.1x saca partido del uso extendido y creciente de RADIUS para la autenticación. Un servidor RADIUS puede realizar consultas en una base de datos de autenticación local si ello es adecuado para el escenario. La solicitud puede transmitirse a otro servidor para su validación. Cuando RADIUS decide que se puede autorizar el equipo en esta red, vuelve a enviar el mensaje al punto de acceso y éste permite que el tráfico de datos fluya hacia la misma.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 3 Edición No 1 – Año 2005



MOVILIDAD – MOVILIDAD FLUIDA

Esta característica se emplea para mejorar la experiencia de la movilidad inalámbrica mediante la detección de los desplazamientos a nuevos puntos de acceso; en el proceso, se exige una nueva autenticación para garantizar un acceso correcto a la red y se detectan los cambios de la subred IP de manera que se pueda utilizar una dirección adecuada para obtener un acceso óptimo a los recursos.

Pueden existir múltiples configuraciones de direcciones IP (direcciones asignadas por DHCP o estáticas) y la configuración correcta se selecciona automáticamente. La detección automática y la posibilidad de realizar una nueva configuración eliminan la necesidad de que IP móvil actúe como mediador y resuelven la mayoría de los problemas de los usuarios al desplazarse de una red a otra.

En los desplazamientos de un punto de acceso a otro, hay información de estado y de otro tipo sobre la estación que debe moverse con la estación. Entre otros datos, se incluye información sobre la ubicación de la estación para la entrega de mensajes y otros atributos de la asociación. En lugar de volver a crear esta información en cada transición, un punto de acceso puede transmitirla al nuevo punto de acceso. Los protocolos necesarios para transferir esta información no se definen en el estándar, pero varios distribuidores de redes LAN inalámbricas se han unido para desarrollar un protocolo de punto de interacceso (IAPP) con esta finalidad, lo que mejora todavía más la interoperabilidad entre los distintos distribuidores.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 3 Edición No 1 – Año 2005

CONFIGURACIÓN – CONFIGURACIÓN RÁPIDA DE LAS CONEXIONES INALÁMBRICAS

La automatización del proceso de configuración de la tarjeta NIC para su asociación a una red disponible. La NIC inalámbrica y su controlador NDIS deben hacer muy poco más que admitir unos cuantos identificadores de objetos (OID) NDIS nuevos que se utilizan para las consultas y configuraciones del comportamiento del dispositivo y del controlador.

Estas mejoras de configuración rápida están integradas con las mejoras de seguridad de modo que, si se produce un error en la autenticación, se encontrará otra red para intentar la asociación.

REFERENCIAS BIBLIOGRÁFICAS

Tanenbaum, A. (1997).Redes de Computadoras. (Era. ED.). México: Prentice Hall

http://standards.ieee.org/wireless/

http://www.idg.es/comunicaciones/wireless

http://www.intel.co.jp/es/home/trends/wireless

http://www.dlinkiberia.es/home.html

http://www.ing.ula.ve/~albornoz/digirad.html

http://www.iworld.com

http://www.computerworld.com

http://www.diarioinformatico.com

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 3 Edición No 1 – Año 2005