Universidad Nacional Autónoma de México
Facultad de Contaduría y Administración
Sistema Universidad Abierta y Educación a Distancia

Licenciatura en Informática

Telecomunicaciones II (Redes Globales)

Apunte electrónico

SUAyED

COLABORADORES

DIRECTOR DE LA FCA
Dr. Juan Alberto Adam Siade

SECRETARIO GENERAL
L.C. y E.F. Leonel Sebastián Chavarría

– – – –

COORDINACIÓN GENERAL
Mtra. Gabriela Montero Montiel
Jefe de la División SUAyED-FCA-UNAM

COORDINACIÓN ACADÉMICA
Mtro. Francisco Hernández Mendoza
FCA-UNAM

– – – –

AUTOR
Ing. Angie Aguilar Domínguez

DISEÑO INSTRUCCIONAL
Mtro. Joel Guzmán Mosqueda

CORRECCIÓN DE ESTILO
Mtro. Carlos Rodolfo Rodríguez de Alba

DISEÑO DE PORTADAS
L.CG. Ricardo Alberto Báez Caballero
Mtra. Marlene Olga Ramírez Chavero
L.DP. Ethel Alejandra Butrón Gutiérrez

DISEÑO EDITORIAL
Mtra. Marlene Olga Ramírez Chavero

OBJETIVO GENERAL

Al finalizar el curso, el alumno conocerá los modelos operacionales de las redes globales, los mecanismos que permiten garantizar la seguridad de los datos y administrar los diversos componentes de las redes globales.

TEMARIO OFICIAL
(64 horas)

	Horas
1. Interoperabilidad en redes	16
2. Integridad	14
3. Seguridad	16
4. Redes inalámbricas	18
Total	**64**

INTRODUCCIÓN A LA ASIGNATURA

Actualmente, las telecomunicaciones tienen un vasto uso: radio, televisión, internet. Para el caso de internet, la tendencia se encamina hacia las tecnologías con mayor movilidad y portabilidad en los dispositivos, así como en diseños y conexiones que soporten cada vez mayor cantidad de usuarios interconectados enviando y recibiendo información.

El punto anterior representa un gran reto para el diseño, aplicación, mantenimiento y seguridad de las redes de telecomunicaciones que deben establecerse para cubrir los requerimientos de interconexión y operabilidad.

En el presente texto se encuentran desarrollados temas importantes y actuales en materia de telecomunicaciones: interoperabilidad en redes, integridad, seguridad y redes inalámbricas.

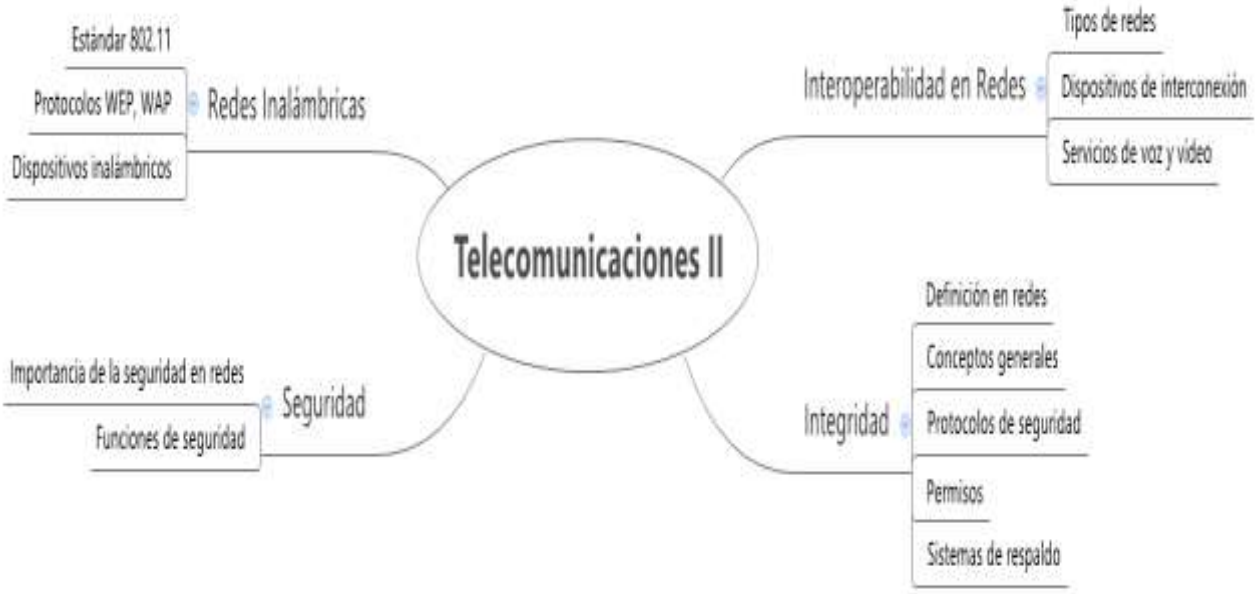
En la interoperabilidad de redes se tocan puntos como los tipos de redes existentes hoy, dispositivos de interconexión y servicios de voz y vídeo, los cuales se emplean de forma masiva.

Es importante destacar que hay 2 aspectos que van de la mano en este tema: la integridad y seguridad de las comunicaciones que se establecen, pues debe garantizarse el adecuado manejo del flujo de información, por medio de técnicas y métodos que mantengan tales aspectos al día.

En este punto, el mantener privada una comunicación, así como garantizar su apropiado funcionamiento no son aspectos triviales, por lo que se abordan ambos temas buscando proporcionar herramientas útiles para su implementación.

Finalmente, en el tema de redes inalámbricas, se proporciona información útil del estándar 802.11 de la IEEE, que permite entender el funcionamiento de las comunicaciones mediante dispositivos móviles, redes inalámbricas y las tecnologías empleadas para su ejecución. Esto es importante, ya que el uso de redes inalámbricas se encuentra cada vez más extendido y ha cobrado especial relevancia en los últimos años.

ESTRUCTURA CONCEPTUAL



Unidad 1

Interoperabilidad en redes

OBJETIVO PARTICULAR

El alumno conocerá las funciones y características de los diferentes equipos, estándares de red y protocolos de comunicación para proponer soluciones de interoperabilidad y comunicación entre redes de diferente tipo, y con el fin de proporcionar los servicios de voz, video y datos.

TEMARIO DETALLADO
(16 horas)

1. Interoperabilidad en redes

- 1.1. Interconexión
  - 1.1.1. Redes LAN
  - 1.1.2. Redes MAN
  - 1.1.3. Redes WAN
  - 1.1.4. Conexiones remotas
- 1.2. Dispositivos de interconexión
  - 1.2.1. Ruteadores
    - 1.2.1.1. Métodos de ruteo
      - 1.2.1.1.1. Por saltos mínimos
      - 1.2.1.1.2. Por tipo de servicio
      - 1.2.1.1.3. Ruteo directo
      - 1.2.1.1.4. Ruteo indirecto

1.2.1.2. Protocolos
1.2.1.2.1. RIP
1.2.1.2.2. IGRP/EIGRP
1.2.1.2.3. OSPF
1.2.1.2.4. BGP
1.2.2. Protocolos ruteables
1.2.2.1. IP
1.2.2.2. IPX
1.2.2.3. Apple Tablet (Talk)
1.2.3. Bridges
1.2.4. Switches
1.2.4.1. Características
1.2.4.2. Modos de operación
1.2.4.3. VLAN
1.3. Servicios de voz y video.

INTRODUCCIÓN

Dentro del mundo de las redes existe un gran desarrollo tecnológico. Esto permite que cada día puedan ofrecerse servicios más sofisticados a los usuarios. Hace unos años era muy costoso producir una videoconferencia en tiempo real, ahora ya es posible usar este recurso desde cualquier computadora con acceso a internet. Esto ha sido asequible gracias a que las redes han evolucionado, sus capacidades han aumentado y los dispositivos ahora tienen mayor capacidad de cómputo.

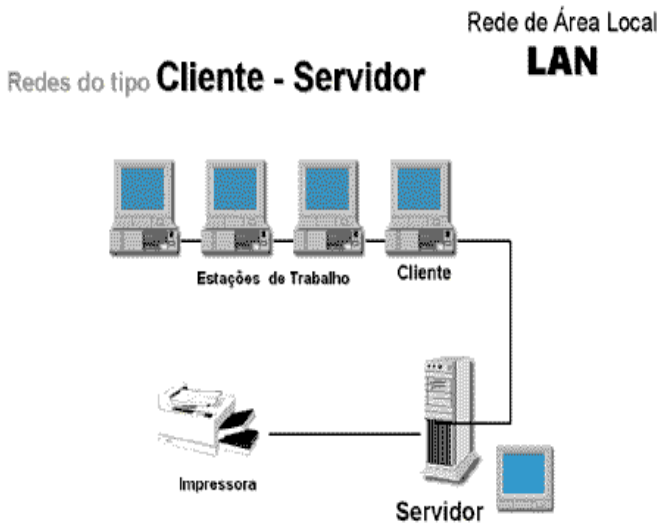
Las tecnologías empleadas en una red son fundamentales para su funcionamiento. Se han desarrollado para que la información pueda ser comunicada de un lugar a otro de manera segura, confiable y de tal modo que satisfaga las necesidades de los usuarios, las cuales van aumentando al mismo tiempo que las aplicaciones. No es lo mismo un usuario que enviaba un correo electrónico, que un usuario que carga videos a YouTube. La tecnología de aquellos tiempos no lo soportaba. El desarrollo de las tecnologías de red permite servicios nuevos que los clientes pueden disfrutar, como el uso de telefonía IP compatible con la telefonía tradicional, haciendo que las empresas sean más flexibles. El desarrollo de la tecnología permite que un usuario común ponga su estación de radio o su canal de televisión en internet sin necesidad de depender de un medio tradicional de información.

Este crecimiento también tiene sus riesgos. En un mundo donde ahora se comparte toda la información por medio de redes sociales, es fácil que personas no autorizadas accedan a información ajena.

1.1. Interconexión

1.1.1. Redes LAN

Se les llama redes LAN (del inglés Local Access Network) a las redes que cubren un área geográfica pequeña. Puede ser desde una red casera, una red en una oficina, en una escuela, etc. Una red LAN también está definida por las tecnologías de transporte que utiliza.



Ejemplo de red LAN

Fuente: http://bit.ly/1pEtyfV

En la actualidad, una red de área local se basa en Ethernet como tecnología estándar. La velocidad de la red puede ir desde 10 Mbps hasta 10 Gbps, dependiendo de las necesidades y el presupuesto asignado, dado que entre más velocidad, el costo se incrementa.

Otra característica de una red LAN es la forma como se encuentra interconectada. Las redes de área local generalmente utilizan una topología física de estrella. Se le nombra de esta manera cuando los dispositivos de red se conectan a un equipo de interconexión central, como un *switch* o concentrador.

En caso de que la red LAN sea inalámbrica, los dispositivos que se encuentran en red se conectan a un Punto de Acceso (del inglés, Access Point), enrutador inalámbrico o estación base. Existe un estándar para las redes LAN inalámbricas, llamado IEEE 802.11, aunque se le conoce popularmente como Wifi

1.1.2. Redes MAN

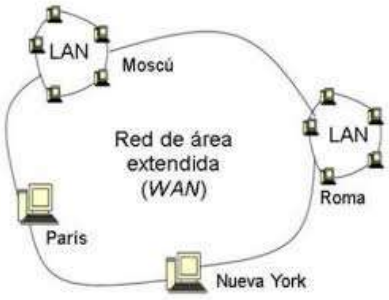
Las Redes de Área Metropolitana (*Metropolitan Area Network*, por sus siglas en inglés) son redes que cubren una extensión geográfica de mayor tamaño que una red LAN. Es decir, un grupo de redes locales que se unen dentro de una misma ciudad mediante un medio de interconexión, ya sea físico o inalámbrico.

Las tecnologías utilizadas para este tipo de redes generalmente se conocen como enlaces dedicados. Se trata de enlaces digitales que permiten la interconexión a grandes distancias, alcanzando anchos de banda de hasta 155 Mbps. Dichos enlaces digitales son los tipos de enlaces más comerciales, aunque ya comienzan a aparecer opciones para también utilizar tecnologías como Ethernet sobre fibra óptica y alcanzar velocidades de hasta 100 Mbps o 1 Gbps, pero su costo continúa siendo elevado.

Este tipo de redes requiere de una mayor inversión en tecnología y, en su caso, se puede necesitar la contratación de un Proveedor de Servicios de internet (ISP, por sus siglas en inglés).

1.1.3. Redes WAN

Las redes de área amplia o redes WAN (*Wide Area Network*, por sus siglas en inglés) son redes que están interconectadas de una ciudad a otra o incluso con otros países.



Ejemplo de red WAN

Fuente: http://bit.ly/VAFvwi

Las tecnologías son las mismas que en una red MAN, incluso con las mismas velocidades, pero a distancias mayores. También se contratan servicios de un ISP (*internet Service Provider*), ya que sería muy costoso contar con infraestructura propia para cubrir grandes regiones de un país. El ISP es una empresa que cuenta con esa infraestructura y que brinda esos servicios. En México, los principales ISP son Telmex, Axtel, Alestra, Metrored.

1.1.4. Conexiones remotas

Las conexiones remotas son de gran utilidad para los administradores de red. Les permite manipular una aplicación o un dispositivo de red sin estar físicamente presentes en el lugar donde se encuentra dicha aplicación o dispositivo. Un ejemplo muy claro surge cuando se presenta un incidente dentro de la red en un día no laborable, se trata de un momento en el cual el administrador de red no se encuentra en el lugar del problema, pero con una conexión remota desde su casa es posible que corrija el problema sin necesidad de perder el tiempo en desplazarse hasta el lugar de los hechos. El tipo de conexión remota a utilizar dependerá del tipo de aplicación que se maneje, incluso del sistema operativo con que la aplicación funcione. Los Centros de Operación de Red (NOC, por sus siglas en inglés) son áreas de trabajo especializadas en vigilar los incidentes de red y dar respuesta para corregir algún problema. El personal especializado de estos centros cuenta con herramientas para conectarse a los dispositivos de red de manera remota y responder a problemas urgentes. Las conexiones remotas también permiten gestionar, desde un punto central, toda una infraestructura tecnológica que se encuentra en diferentes puntos geográficos.

1.2. Dispositivos de interconexión

Durante el proceso de comunicación en una red de cómputo, los equipos de interconexión juegan un papel muy importante. Dichos equipos son los elementos de la red que permiten que los usuarios finales puedan comunicarse con otros en la misma red o fuera de ella.

Cuando un usuario final desea conectarse a un sitio en internet, es necesario que la información pase por diferentes dispositivos de interconexión que cumplan con una función específica dentro de todo el proceso de comunicación.

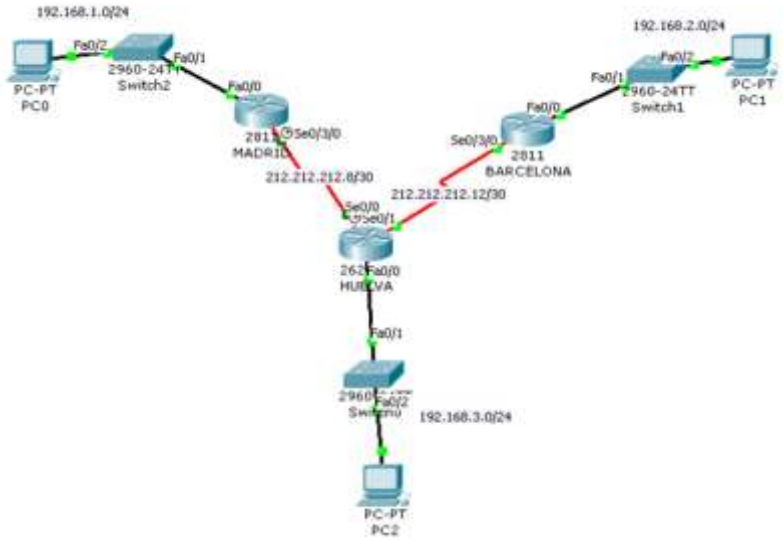
1.2.1. Ruteadores

Como ya se había indicado, los ruteadores son dispositivos que deciden la mejor ruta para transitar de un origen a un destino. Sus decisiones están basadas en direcciones IP, mediante una tabla de ruteo que mantienen por *software*, y en algoritmos de ruteo.

1.2.1.1. Métodos de ruteo

1.2.1.1.1. Por saltos mínimos

Un mecanismo que utilizan los ruteadores para encontrar el mejor camino o ruta para llegar a un destino, es el número de saltos que un paquete dará. Debido a que puede haber múltiples caminos para llegar a un destino, es necesario elegir cuál es el mejor. Un salto corresponde a un ruteador por el cual es procesado un paquete. Cabe mencionar que este método es el más simple y se utiliza para redes poco complejas.



Ejemplo de ruteo por saltos mínimos

Fuente: http://redeslocales-estella.blogspot.mx/2011/02/tablas-de-enrutamiento.html

1.2.1.1.2. Por tipos de servicio

En el protocolo IP es posible etiquetar campos para aplicaciones que requieran de un trato especial, esto es conocido como *Type of Service* (ToS). Éste es utilizado para darle prioridad a aplicaciones sensibles, como audio y video que, por sus características, son un tipo de tráfico que deja de funcionar si hay retransmisiones de por medio.

Ejemplo de ruteo por tipos de servicio

Fuente: http://www.icono-computadoras-pc.com/diagramas-de-redes-de-computadoras.html

1.2.1.1.3. Ruteo directo

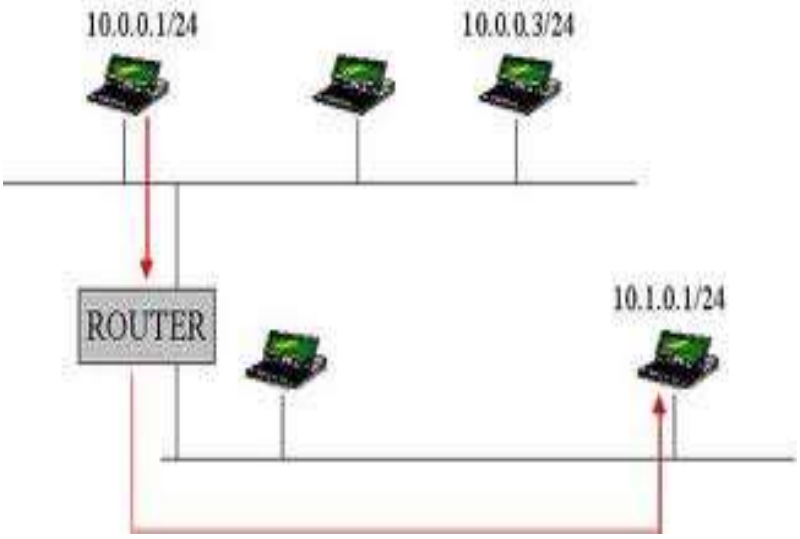
Este tipo de ruteo se hace dentro de una misma red local sin necesidad de un ruteador o puerta de enlace. Todo el proceso se realiza mediante el protocolo ARP, que se encarga de relacionar las direcciones físicas (MAC) a las direcciones lógicas IP, para encontrar la computadora destino.

Ejemplo de ruteo directo

Fuente: http://bit.ly/1nXuhbs

1.2.1.1.4. Ruteo indirecto

A diferencia del ruteo directo, aquí se utiliza un ruteador para decidir a qué *host* debe enviarse el paquete de información. Este tipo de ruteo se utiliza para comunicaciones entre redes que están separadas física y/o geográficamente, o para redes que están separadas lógicamente.



Ejemplo de ruteo indirecto

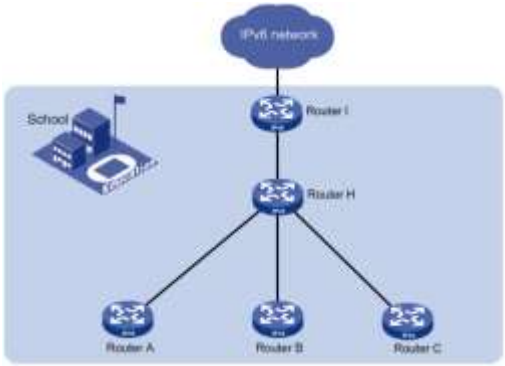
Fuente: http://tinyurl.com/le25oqu

1.2.1.2. Protocolos

Los protocolos de ruteo son procedimientos que cada ruteador utiliza para intercambiar información útil y alcanzar un destino. Se utilizan cuando las redes son grandes y complejas y requieren de decisiones automatizadas; también, cuando la cantidad de destinos dentro de una o varias redes es tan grande que se vuelve inmanejable para un administrador de red que pretendiera hacer manualmente tal programación de destinos.

1.2.1.2.1. RIP

El *Routing Information Protocol* es un protocolo de ruteo que emplea el número de saltos para decidir la mejor ruta para un destino. El protocolo permite que el ruteador haga el intercambio de mensajes de control con los ruteadores vecinos, para saber qué redes y a cuántos saltos de distancia se encuentran otras redes. Esta información permitirá a un ruteador establecer la cantidad de saltos para llegar a una red en particular y de esa manera tomar sus decisiones.



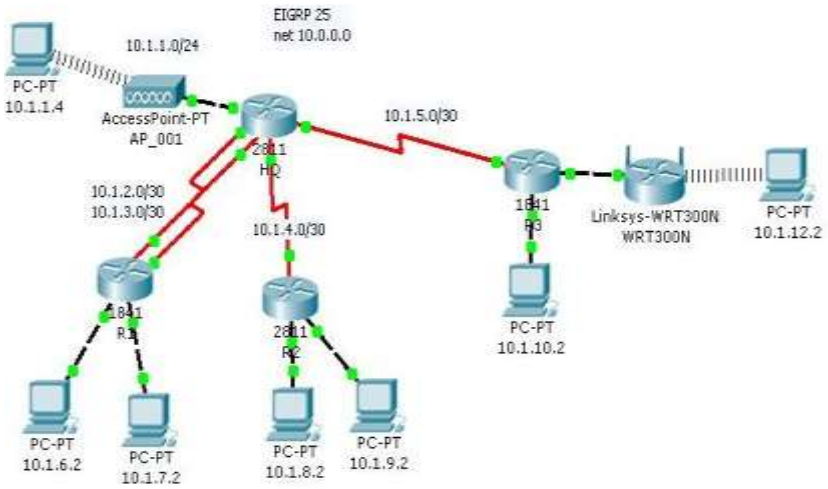
Ejemplo de uso del protocolo RIP

Fuente: http://bit.ly/1mO2LRm

Un problema que presentó la primera versión del protocolo RIPv1 es que no podía manejar subredes, cuestión que ya se arregló en la versión 2 con el soporte de VLSM. La característica de VLSM (*Variable Lenght Subnet Mask*) radica en que permite que dentro de una red se tenga una dirección IP con una máscara de subred diferente. Una desventaja de este protocolo es que no permite la creación de jerarquías, por lo que la propagación de las rutas se hará a todo lo largo de la red que se use. Cuando existe un problema en la red, es un protocolo con una convergencia lenta.

1.2.1.2.2. IGRP/EIGRP

IGRP nació con la idea de competir contra RIP y sus deficiencias. RIP solamente contaba con la métrica de los saltos para decidir la mejor ruta, por lo que IGRP introdujo métricas como el ancho de banda, el retardo, la carga entre otras para tomar esas decisiones. Las actualizaciones se realizan cada 90 segundos para que toda la red de ruteadores se entere de los cambios en la topología. Este protocolo no es estándar, sino propietario de la marca *Cisco*. Es un protocolo que tampoco identifica subredes, por lo que ya ha quedado obsoleto. Su lugar fue ocupado por EIGRP, que hace lo mismo que IGRP, pero añadiendo las funciones de reconocer las máscaras de subred.



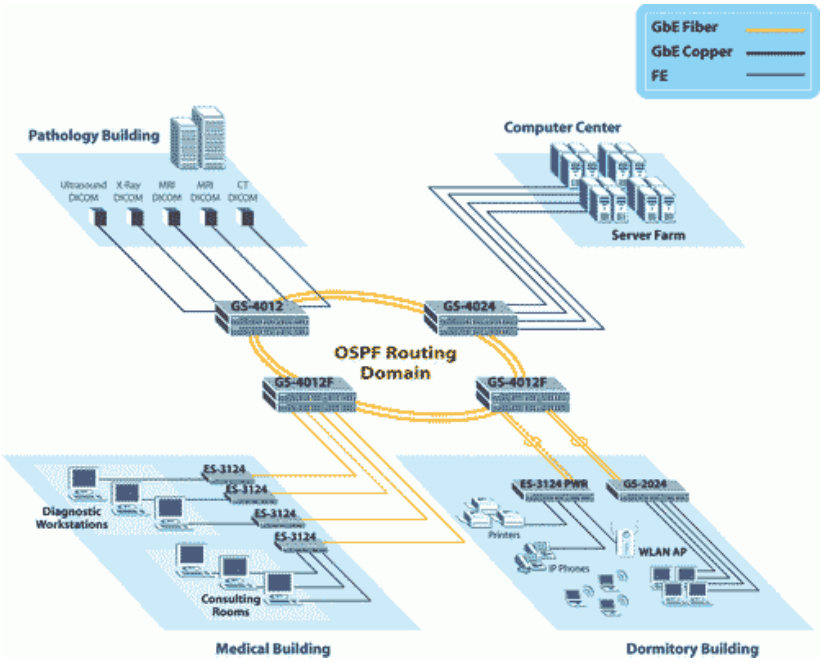
Ejemplo de IGRP/EIGRP

Fuente: http://bit.ly/1lsYeP3

1.2.1.2.3. OSPF

El *Open Shortest Path First* (*OSPF*) es un protocolo de ruteo estándar jerárquico, ya que permite la creación de áreas de ruteo para un mejor desempeño en entornos grandes. A diferencia de los dos protocolos anteriores que se basan en la información que el ruteador vecino les proporciona, este protocolo utiliza un algoritmo diferente que calcula la mejor ruta, llamado *link-state*.

En este protocolo cada ruteador conoce la topología y estructura de la red entera, así como el mejor camino para su destino. Esto hace más eficiente la red, ya que no es necesario enviar actualizaciones periódicas para converger y encontrar una ruta alterna, sino que en el mismo instante de una falla, el algoritmo actúa y recalcula nuevamente las rutas para un destino.

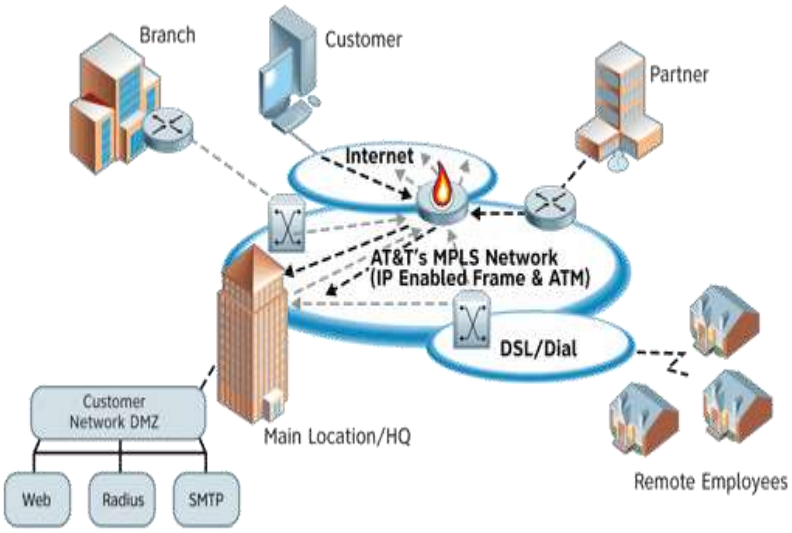


Ejemplo de OSFP

Fuente: http://bit.ly/1vp5G3z

1.2.1.2.4. BGP

El protocolo *Border Gateway Protocol (BGP)* se utiliza para conocer las redes de otros sistemas autónomos (SA). Un SA es un conjunto de redes administrado por una misma entidad, y para conocer redes más allá del entorno en el que se está, es necesario un protocolo de este tipo. En internet, este es el protocolo estándar para intercambio de redes entre todas las redes del mundo. Cuando se trata de una red grande, como una universidad o una empresa con miles de equipos de cómputo, siempre es recomendable contar con un sistema autónomo para su mejor gestión.



Ejemplo de BGP

Fuente: http://bit.ly/1m3hqr4

1.2.2. Protocolos ruteables

Los protocolos ruteables son aquellos protocolos que manejan su propio direccionamiento y que permiten ser transportados dentro de un protocolo de ruteo. Un protocolo ruteable no es capaz de llevar información de tablas de ruteo, como sí lo hace un protocolo de ruteo. Los protocolos ruteables se usan para asignar direccionamiento a los dispositivos de red.

1.2.2.1. IP

El *Internet Protocol* es la parte de la pila de protocolos TCP/IP que son la base para que internet funcione. Este protocolo está definido en el RFC 791 y realiza operaciones que define la capa 3 del modelo OSI. Actualmente se utiliza la versión 4, mas se está impulsando la utilización de la versión 6, que amplía el rango de direcciones disponibles. IP es un protocolo de la capa de red y se encarga de dos aspectos fundamentales de internet: el direccionamiento y el ruteo de redes de datos.

En cuanto al direccionamiento, se debe saber que cada computadora en internet necesita una dirección IP para que pueda ser identificada por quienes tratan de enviarle un paquete de datos de información. El ruteador se encargará de llevar ese paquete a su destino.

1.2.2.2. IPX

El *Internetwork Packet Exchange* también opera en la capa 3 del modelo OSI, realizando las mismas funciones de IP. La diferencia es que IPX ya quedó obsoleto, porque IP es el estándar en la industria del internet. Fue creado por Novell para interconectar dispositivos de cómputo dentro de una red local.

1.2.2.3. Apple tablet (Talk)

Apple también desarrolló un protocolo para la comunicación entre redes, pero, de la misma forma que IPX, ya ha quedado obsoleto y dándole el paso a IP. El direccionamiento es de 4 *bytes*, parecido a IPX, utilizando dos para la dirección, un *byte* para el número de nodo y el último como un número de *socket* para identificar los servicios.

1.2.3. Bridges

Los también conocidos *bridges* son dispositivos que permiten la interconexión de dos segmentos de red de similar o de diferente tecnología. Estos dispositivos introducen el término de “segmentación”, que no es más que limitar el dominio de colisiones, es decir, el espacio en que los paquetes pueden colisionar, porque están intentando hacer uso del medio de transmisión.

Estos son un poco más “inteligentes” que los concentradores, porque contienen un poco el tráfico y no lo retransmiten de manera indiscriminada. Al operar en la capa 2 del modelo OSI, ya cuentan con un *software* interno que permite separar segmentos de red según ciertas direcciones físicas o MAC. Paquetes que van dentro del mismo segmento son analizados y reenviados, pero paquetes que van

de un segmento a otro son filtrados, incluidos los que traen alguna malformación o alteración de origen.

El problema con los puentes nuevamente es la cantidad de dispositivos. Cuando esta cantidad aumenta, la red se vuelve susceptible a los llamados *loops*, debido a que la integridad de sus tablas de información está duplicada. Un *loop* es un fenómeno en el cual los paquetes de datos circulan por la Red de un lado a otro, sin encontrar su destino, lo que provoca irregularidades en la misma.

1.2.4. Switches

1.2.4.1. Características

Un *switch* se puede definir como un dispositivo de red que recibe paquetes por un puerto y los reenvía por otro de sus puertos. Cuando un equipo envía una trama, al llegar al *switch* éste verificará su tabla de direcciones MAC, y si se encuentra la dirección MAC destino es enviado sólo y únicamente al puerto asociado (en la tabla); si no lo conoce, envía a todos los puertos, menos al del emisor (*broadcast*).

Generalmente, resuelve problemas de rendimiento, de congestión y puede agregar mayor ancho de banda; acelera la salida de tramas y reduce tiempo de espera. Opera generalmente en la capa 2 del modelo OSI; asimismo, reenvía las tramas con base en la dirección MAC.

1.2.4.2. Modos de operación

Por la forma en que conmutan los paquetes, hay *switches* del tipo *Store-and-forward*, *cut-through y FragmentFree*. El primero se caracteriza por tomar las decisiones una vez que recibió el paquete completo. El segundo decide a dónde enviar la trama después de recibir los primeros 6 bytes de la trama (dirección MAC destino). El tercer tipo se caracteriza por tomar los primeros 64 *bytes* antes de enviar las tramas.

1.2.4.3. VLAN

A cada red LAN lógica se le conoce como VLAN (Virtual Local Access Network), ya que es un agrupamiento lógico de computadoras personales, independientemente de su ubicación física dentro de la LAN. Permite extender la red LAN geográficamente. Cada VLAN es un dominio de broadcast diferente, que permite ahorros significativos en la adquisición de switches de red; además, se puede definir por puerto, por protocolo o por dirección MAC, para agrupar los equipos de cómputo

A cada red LAN lógica se le conoce como VLAN (*Virtual Local Access Network*), ya que es un agrupamiento lógico de computadoras personales, independientemente de su ubicación física dentro de la LAN. Permite extender la red LAN geográficamente. Cada VLAN es un dominio de *broadcast* diferente, que permite ahorros significativos en la adquisición de *switches* de red; además, se puede definir por puerto, por protocolo o por dirección MAC, para agrupar los equipos de cómputo.

El contar con VLAN obedece a las necesidades de la empresa, puesto que a veces la distribución del equipo de red no coincide con la estructura de la organización.

1.3. Servicios de voz y video

Los servicios de voz y video se vuelven cada día más comunes. Actualmente, las principales empresas telefónicas ofrecen servicios sin necesidad de un teléfono tradicional, sino mediante una conexión a internet. Empresas como Skype, a lo largo del mundo, ofrecen tarifas competitivas para las llamadas internacionales mediante una conexión a internet. Con el crecimiento de los teléfonos celulares conectados a internet, los servicios de telefonía encuentran un nicho de negocios muy importante en esas plataformas.

Ejemplo de un servicio de voz y video, mediante *Skype*

Fuente: http://dreamstechnology.es/internet/televisores-sony-y-vizio-contaran-con-servicio-skype/

La tecnología llamada Voz sobre IP (VoIP) brinda las bondades del servicio telefónico utilizando una red de datos ya existente. Los mismos fabricantes de

tecnología han empujado este cambio al dejar el desarrollo de los conmutadores tradicionales y enfocarse a los que puedan conectarse a la Red. Una organización que tiene oficinas alrededor del mundo, deja de gastar dinero en llamadas de larga distancia, porque ahora utiliza su red de datos para comunicarse. Pero este tipo de servicios demanda ciertas características en una red. Una de estas características es el retardo en las comunicaciones. Una llamada de voz no permite retardos, porque la llamada se ve interrumpida y eso resta calidad a un servicio. Por ello, durante el diseño de una red de datos pensada con servicios de voz, se deben tener en cuenta tales requerimientos.

Lo mismo pasa con el video. Las videoconferencias también son aplicaciones que no permiten los retardos, porque, como en una llamada que se entrecorta, es muy incómodo estar viendo un video con demasiados cortes en su reproducción. Y cuando se trata de un evento en vivo (*live streaming*), la necesidad de una transmisión sin interrupciones es mayor. La utilización del video ya no se limita al ambiente académico; sitios como YouTube o Vimeo han popularizado este servicio. Ahora cualquier persona puede abrir un canal de video y subir sus grabaciones caseras; sin embargo, esta realidad demanda una tecnología actualizada y medios de transmisión con mayor velocidad.

RESUMEN

La revisión de esta segunda unidad contempló la clasificación de las redes en LAN, MAN y WAN, y sus particularidades. Es importante notar que cada uno de estos tipos de redes cumple distintos objetivos dentro de las organizaciones donde se implementan. Se recomienda estar informado acerca de cada una de ellas para poder entender su funcionamiento, así como sus debilidades y fortalezas.

También se mencionaron los mecanismos de ruteo existentes, así como la forma en que cada uno de ellos opera. Esto tiene la finalidad de entender el funcionamiento interno de una red de equipos de cómputo (computadoras, servidores, impresoras y cualquier otro dispositivo conectado en red).

Para lograr el objetivo de identificar los tipos de redes, se expusieron conceptos básicos, que familiarizaron al alumno con este propósito, entre ellos el concepto de VLAN, protocolos, voz y video; asimismo, se mencionó cada dispositivo de interconexión, señalando las funciones importantes para las redes, como el *switch* y el *router*.

BIBLIOGRAFÍA

SUGERIDA

Autor	Capítulo	Páginas
Tannenbaum, A.	5	14-25
		431-464

Tanenbaum, A. (2002). *Computer Networks* (4th edition). New Jersey: Prentice Hall. Disponible en: http://books.google.com/books?id=WWD-4oF9hjEC&printsec=frontcover&dq=redes+de+computadoras&hl=es&ei=YG3yTa_OBYO5twetzozuAg&sa=X&oi=book_result&ct=result&resnum=1&ved=0CC0Q6AEwAA#v=onepage&q&f=false

Unidad 2

Integridad

OBJETIVO PARTICULAR

El alumno conocerá y aplicará los protocolos y mecanismos que permiten proteger la integridad de la información frente a la alteración, pérdida o destrucción durante la transmisión emisor-receptor y entre redes de diferente tipo.

TEMARIO DETALLADO
(14 horas)

2. Integridad

- 2.1. Definición en redes
- 2.2. Conceptos generales
  - 2.2.1. Protección
  - 2.2.2. Interrupción
  - 2.2.3. Intercepción
  - 2.2.4. Modificación
  - 2.2.5. Fabricación
  - 2.2.6. Control de acceso
  - 2.2.7. Disponibilidad
- 2.3. Protocolos de seguridad
- 2.4. Permisos
- 2.5. Sistemas de respaldo

INTRODUCCIÓN

La información siempre ha estado expuesta a ser modificada, robada o destruida. Con el avance de la tecnología computacional, se han realizado mejoras en el manejo de la información y de su seguridad. Actualmente es posible emplear protocolos y algoritmos de cifrado potentes que brindan altos niveles de seguridad. Estos avances se presentan no sólo en cuestiones de integridad; sino también en las de confidencialidad, autenticidad y disponibilidad. Es necesario contar con políticas que definan claramente el propósito y la forma de mantener la integridad de la información. Este proceso no siempre implica una transición sencilla para las personas involucradas, es por ello que de la mano de las implicaciones tecnológicas, que permiten aumentar la seguridad de la información en dispositivos o redes, es necesario contar con una campaña de amplia difusión de seguridad en el área de TI.

2.1. Definición de redes

En particular, la integridad de la información es importante cuando se necesita que los recursos no sufran modificaciones por parte de agentes que no tienen la autorización para hacerlo. En una red de cómputo, la integridad debe mantenerse sobre los dispositivos de red, porque si sufrieren alguna alteración en sus configuraciones, la red dejaría de funcionar adecuadamente. También se debe cuidar la integridad del tipo de tráfico que circula por la red, porque un tráfico anómalo puede dejar sin servicio a los usuarios, y es señal de un ataque informático.

2.2. Conceptos generales

2.2.1. Protección

La protección es el conjunto de políticas y herramientas utilizadas para prevenir ataques a la integridad de un sistema de información. Cada organización necesita contar con una estrategia de seguridad para protegerse de las amenazas existentes en internet. Esta estrategia debe incluir políticas específicas de seguridad, en aspectos de confidencialidad, autenticación e integridad. Una alternativa es el uso de herramientas adecuadas para llevar a cabo los objetivos de seguridad. El cifrado de la información ayuda también en la tarea de proteger la información. Dicho cifrado de información consiste transformar la información, de manera que un lector casual o malintencionado no pueda entender lo que está leyendo.

Seguridad informática

Fuente: http://seguridadinformatica-ezequielgarcia.blogspot.mx/2012/08/para-que-sirve-la-seguridad-informatica.html

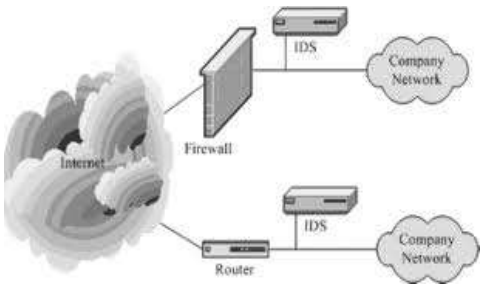
La capacidad de las computadoras actuales facilita las tareas de cifrado, pero también las del descifrado. La información es susceptible de amenazas con el potencial suficiente para causar pérdidas o daños a sistemas de información de cualesquier tipos: sea un sistema personal, una base de datos o una red de cómputo. Cuatro tipos de amenazas son las principales que atentan contra un sistema de información y que se describen en seguida.

2.2.2. Interrupción

Se presenta cuando un sistema de información se hace no disponible o inutilizable mediante acciones maliciosas. Esta es una de las amenazas más visibles, porque sus efectos son notables. Un ejemplo se presenta con los sitios que reciben ataques de negación de servicio haciéndolos inutilizables. Tanto empresas como oficinas de gobierno son el blanco de este tipo de ataques, en algunos casos por venganza y en otros como protesta.

Los equipos de red como *switches* y ruteadores también padecen este tipo de amenazas. Un ataque dirigido a un servidor afectará el dispositivo al que se conecta, por lo que el daño se puede extender a toda una red local y no solamente al servidor al que va dirigido. Un ataque puede bloquear un dispositivo dejándolo inutilizable para el resto de los equipos de cómputo que interconecta.

Una buena práctica de seguridad es contar con tecnología de detección de intrusos que limite ataques de negación de servicio. Un sistema detector de intrusos o IDS (*Intrusion Detection System*) se encuentra siempre observando el tráfico de la red, y según ciertas reglas detecta comportamientos fuera de lo normal y los reporta como posibles ataques.



Uso de IDS

Fuente: http://www.insecure.in/ids.asp

2.2.3. Intercepción

Se presenta cuando un agente no autorizado logra obtener acceso a recursos del sistema de información sin necesariamente poder manipularlos. Un ejemplo es la intervención de un canal de comunicación. Cuando alguien escucha una conversación telefónica o por internet, el servicio sigue funcionando, no se interrumpe, pero se está teniendo acceso a información privada por parte de un elemento (equipo o persona) no deseada. A este tipo de ataque se le conoce como *Man in the Middle*.

Generalmente un equipo de interconexión no es capaz de detectar amenazas de este tipo, por eso se usa tecnología especializada para la detección de intrusos. Por lo regular, se emplean mecanismos de cifrado para prevenir una posible intercepción de datos.

Una buena práctica de seguridad, es utilizar cifrado en las conexiones remotas a los dispositivos de red, para evitar que mediante un analizador de protocolos capturen contraseñas o cualquier otra información sensible que viaja por el canal de comunicación.

2.2.4. Modificación

En algunas situaciones, se puede llegar a presentar modificación de la información cuando un agente no autorizado logra acceder a recursos del sistema de información y puede manipularlos.

Un ejemplo es cuando se altera un programa para que otorgue resultados diferentes, como al hacer una transferencia vía banca electrónica, donde el sistema informático del banco acumula cualquier movimiento hacia una cuenta fraudulenta.

Esto solamente se puede lograr si el sistema original fue modificado para enviar depósitos a la cuenta de otra persona.

Ataque Man in the middle

Fuente: http://www.designbrooklyn.com/images/mimt2.jpg

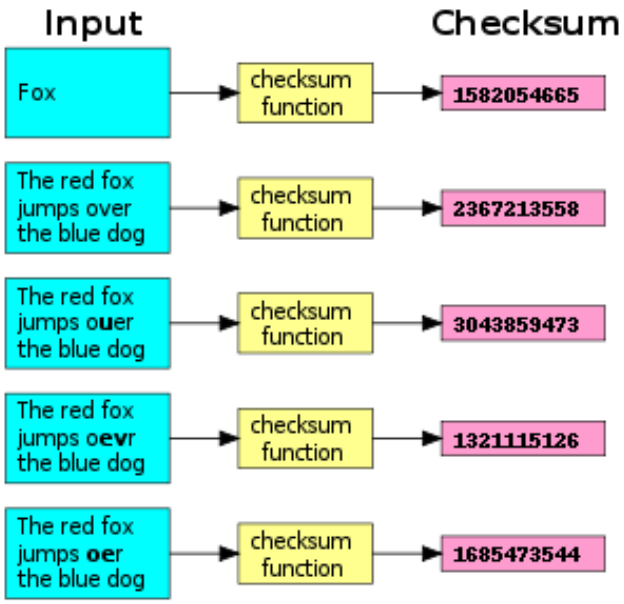
Un sistema que vigile la integridad de un sistema verificará cualquier cambio en los elementos que lo conforman. Cuando se trata de un equipo de interconexión de tipo ruteador o, bien, un servicio de internet, se debe cuidar que sus configuraciones no sean modificadas para que no afecte la forma como la red opera.

Puede suceder que por error o maliciosamente se especifique una dirección IP diferente al equipo, lo cual provocaría que un segmento de red se quede sin poder comunicarse con el resto de los segmentos de red.

Por todo lo anterior, en la transmisión y recepción de información entre 2 equipos de computadoras, es necesario llevar a cabo verificaciones en el destinatario, lo que permitirá identificar la posible modificación de los paquetes de información que se intercambian entre ambos equipos.

Para ello, se emplean algunos algoritmos de verificación, por ejemplo, en los protocolos TCP y UDP se realiza una suma de verificación, conocida como *checksum*, en los paquetes de datos para verificar que no están corruptos o que no

han sido modificados. En el siguiente esquema puede verse la aplicación de la suma de verificación, la cual permite identificar si hubo algún cambio en el mensaje original.



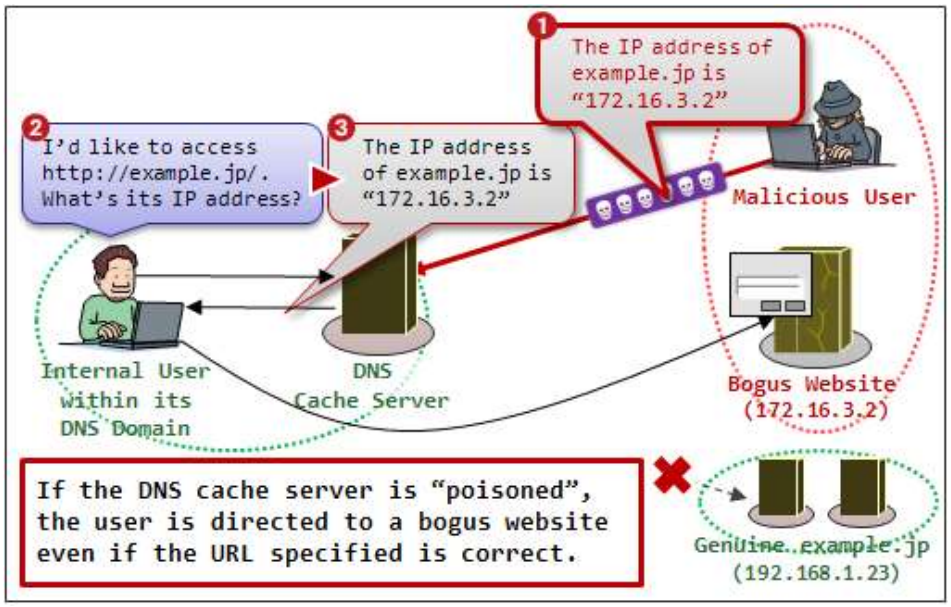
Suma de verificación para una frase

Fuente: https://en.wikipedia.org/wiki/Checksum

2.2.5. Fabricación

Se presenta cuando un agente no autorizado crea información falsa dentro del sistema de información. Un ejemplo de esto consiste en agregar registros en una base de datos.

Existe un tipo de ataque llamado *DNS cache poisoning*, que de manera maliciosa provee datos a un DNS. Este servidor se encarga de convertir nombres de dominio al lenguaje IP utilizado en internet, lo que podría provocar que todas las peticiones que se hicieran a internet realmente fueran a un servidor con propósitos maliciosos.



Ejemplo de DNS cache poisoning

Fuente: http://www.ipa.go.jp/files/000013084.png

Además de la integridad, hay otras características que un sistema de información debe considerar, como el control de acceso, la disponibilidad y la confidencialidad.

2.2.6. Control de acceso

Se refiere a las tareas o mecanismos que se utilizan para mantener el control sobre las conexiones entrantes a una red. Las restricciones sobre estas conexiones dependerán del grado de riesgo y de la privacidad que requiere la información. Un servicio público de una página web no requiere la misma política de control de acceso que una red privada o intranet. El control de acceso incluye a los mecanismos de autenticación y de autorización de cualquier entidad que requiera ingresar a la red.

Autenticación

Esta tarea se utiliza para garantizar que los participantes en una comunicación tengan en realidad la identidad válida para realizar sus actividades. Se puede autenticar usuarios, computadoras y aplicaciones. Para autenticar usuarios, generalmente se utiliza un nombre de usuario y una contraseña; para autenticar computadoras se utilizan direcciones IP o direcciones MAC; y para autenticar aplicaciones se utilizan puertos de la familia de protocolos TCP/IP.

Un escenario típico es el proceso de identificar a un usuario que quiere ingresar a revisar su correo electrónico. Antes de proceder a leer, borrar o enviar correos electrónicos, el sistema le pide que se identifique con su nombre de usuario y contraseña; si estas credenciales son correctas, el sistema le da paso, porque confía en que es la persona que dice ser.

Autenticación de usuarios

Fuente:

http://www.cert.uy/wps/wcm/connect/b032b3004fb7ad9a8d85eddeba2def97/Sin+t%C3%ADtulo.png?MOD=AJPERES&CACHEID=b032b3004fb7ad9a8d85eddeba2def97

Si una persona se apodera de esas credenciales puede hacer mal uso de ellas. Una de las recomendaciones para evitar que una persona maliciosa se apodere de ellas, es la utilización de contraseñas fuertes que tienen la característica de no ser palabras o frases de uso común; también se recomienda el uso de caracteres numéricos y alfanuméricos, así como de algún carácter especial. Una última recomendación es el cambio de la contraseña cada determinado tiempo, dependiendo de la importancia de la información.

Autorización

Una vez que el usuario ha sido autenticado, existen otras políticas que definen las tareas que tiene permitido hacer, a esto se le conoce como políticas de autorización. No es lo mismo que un gerente de banco entre al sistema de nómina a que lo haga un cajero que, por motivos de seguridad, necesita menos privilegios en la información.

En una red se pueden restringir las aplicaciones que cada usuario puede utilizar. Es común que una empresa limite el uso de ciertas aplicaciones de mensajería para mejorar la productividad de sus trabajadores. Es una práctica recurrente que se

limite el acceso a ciertas páginas en internet, dependiendo del nivel de autorización de cada usuario.

Distintos privilegios para usuarios

Fuente: https://encrypted-tbn3.gstatic.com/images?q=tbn:ANd9GcQX_9CgdqmLZ05wRHG6Njo-N8pi9a2iFQI9xbVTD7Zgc6x5dmXGNg

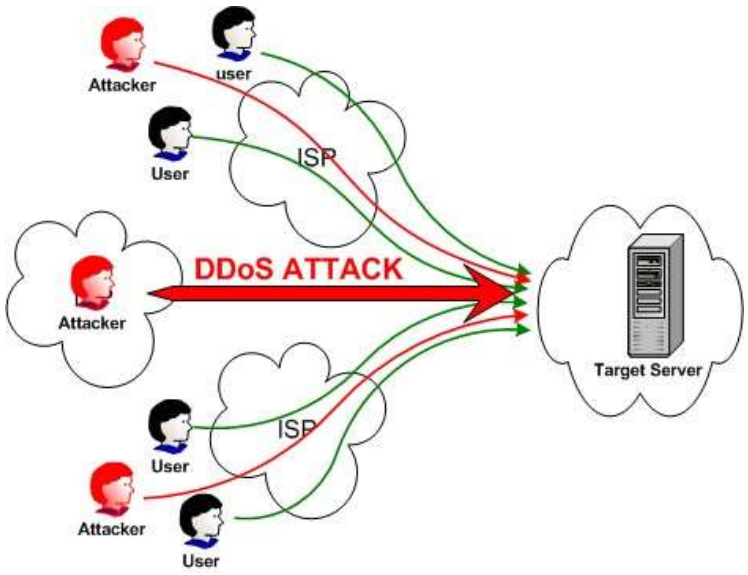
2.2.7. Disponibilidad

Un sistema se encuentra disponible cuando se le demanda algún servicio y responde sin importar la hora, el lugar geográfico, el día o la cantidad de demanda que exista cuando se le está requiriendo. Cuando sucede lo contrario, entonces la disponibilidad del sistema se pierde. Es importante recordar que la disponibilidad de un sistema (red, impresora, sitio web, etc.) está determinado por las reglas del negocio.

Cuando una red de cómputo es lenta o se satura, entonces su disponibilidad está en riesgo. Esto puede presentarse por una demanda superior a la esperada o también por ataques contra la disponibilidad de la red o algún sistema dentro de la misma. En el caso de un virus de alto impacto, éste puede dañar la disponibilidad de una red, dado que su rápida propagación afecta el rendimiento de la misma, llegando a saturarla. Un ejemplo es el famoso gusano informático llamado *Code*

Red, que en tan solo dos días ya se había propagado a 350,000 computadoras personales.

También existen distintos tipos de ataques que impactan en la disponibilidad de una red, uno de ellos es conocido como DoS (*Denial of Service*), el cual satura las peticiones a un recurso determinado impidiendo su funcionamiento normal.



Ataque DoS

Fuente: https://tigr.net/wp-content/uploads/2014/07/DDoS1.jpg

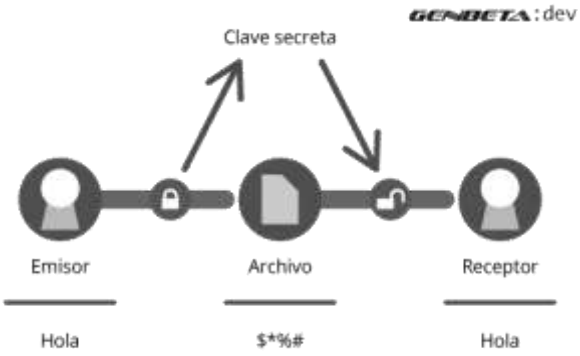
En estos casos, una posible solución consiste en monitorizar frecuentemente las peticiones recibidas, lo que permitirá cortar las conexiones identificadas como provenientes de un rango de direcciones IP que están realizando la saturación.

2.3. Protocolos de seguridad

Un protocolo se define como una serie de pasos utilizados con el fin de resolver un problema, en este caso un problema de seguridad. Un protocolo de seguridad es una forma de implementar servicios de seguridad a sistemas, redes y computadoras personales. Además, involucra una o más partes que se ponen de acuerdo para seguir ciertas reglas.

Cuando se compra un producto en un centro comercial, la persona que compra se pone de acuerdo con esa tienda para adquirir cierta mercancía. Ella se ajusta a sus reglas, se pone de acuerdo con el pago, si es en efectivo o si acepta tarjeta de crédito. Una vez que la tienda recibe el pago, entrega lo que se compró. Todo este proceso es un protocolo que se debe seguir para la compra de productos.

En seguridad, un protocolo acude a la criptografía para que la información legible sea transformada por medio de un elemento conocido como llave, de modo que sólo el que la posea pueda tener acceso a la información. En el medio ambiente de redes es necesario utilizar protocolos, porque se intercambia información entre una computadora y otra. Es menester que estos intercambios sean acompañados de criptografía para brindar seguridad informática.



Cifrado de datos.

Fuente: https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcSml95A-6s2ZBXcqocTk9u7-PDXX9nmWlTBiOSAPjIcG8pcjfqXTQ

En un comienzo, los algoritmos empleados para cifrar eran muy sencillos: una sustitución de letras y números, un corrimiento de letras, etc., pero con el avance del procesamiento por computadora, actualmente se emplean algoritmos matemáticos que buscan ser robustos y proteger la información que están cifrando.

Para Tanenbaum:

> Hasta la llegada de las computadoras, una de las principales restricciones de la criptografía había sido la capacidad del empleado encargado de la codificación para realizar las transformaciones necesarias, con frecuencia en un campo de batalla con poco equipo. Una restricción adicional ha sido la dificultad de cambiar rápidamente de un método de criptografía a otro, debido a que esto implica volver a capacitar a una gran cantidad de personas (2003: 725).

Hoy se emplean 2 tipos de algoritmos:

- Algoritmos de clave simétrica. Utilizan la misma clave para cifrar y para descifrar.
- Algoritmos de clave asimétrica. Utilizan una clave para cifrar y otra para descifrar.

2.4. Permisos

Los mecanismos de autorización indican qué privilegios tiene un usuario una vez que ha ingresado a un sistema por medio de sus correctas credenciales. Los permisos permiten brindar privilegios a usuarios, aplicaciones y computadoras.

Por ejemplo, para el caso de los permisos en un sistema operativo: un usuario común, con pocos privilegios, no podrá realizar tareas de administración en una computadora, no podrá instalar o desinstalar programas. En cambio, un usuario con permisos de administrador sí podrá hacerlo.

Para asignar privilegios, se puede emplear una matriz de privilegios en la que se colocan, por un lado, los privilegios con los que se cuenta y, por otro, los usuarios del sistema.

	Monitor	Operator	Maintainer	Deployer	Auditor	Administrator	SuperUser
Read Config and State	X	X	X	X	X	X	X
Read Sensitive Data [2]					X	X	X
Modify Sensitive Data [2]						X	X
Read/Modify Audit Log					X		X
Modify Runtime State		X	X	X[1]		X	X
Modify Persistent Config			X	X[1]		X	X
Read/Modify Access Control						X	X

Matriz de privilegios

Fuente: http://www.dmartin.es/wp-content/uploads/2014/07/rbac_table.png

Por otro lado, dependiendo del sistema, también se pueden tener Listas de Control de Acceso (ACL, por sus siglas en inglés), las cuales proporcionan privilegios sobre el tráfico que puede presentarse en la red sobre dispositivos como *routers* o conmutadores, cuyo funcionamiento permite o niega el tráfico de red de acuerdo a una regla o condición establecida.

Siempre es recomendable operar bajo el principio del privilegio menor: otorgar los mínimos privilegios necesarios para que los usuarios u otros sistemas realicen las tareas asignadas sin verse impedidos.

La asignación de privilegios debe realizarse con base en los roles y privilegios establecidos por las reglas del negocio.

2.5. Sistemas de respaldo

Es una buena práctica realizar el respaldo de la información, porque siempre es susceptible a las amenazas informáticas, a las amenazas naturales y a los errores humanos que pueden dañarla.

Los respaldos de información tienen como objetivo la restauración de archivos individuales que sufren algún daño o pérdida y la restauración de sistemas completos. El disco duro de una computadora puede fallar en cualquier momento o un archivo puede ser borrado accidentalmente en cualquier área de trabajo. Por lo tanto, es necesario contar con un sistema de respaldo diario, semanal o mensual, dependiendo de la importancia de la información.

En el ámbito informático los respaldos más comunes se realizan sobre: información crítica, configuraciones de servidores, algunas bitácoras de alguna aplicación,

usuarios y privilegios asignados. Adicionalmente, las reglas del negocio determinarán qué otra información deberá respaldarse.

Para realizar los respaldos, es necesario establecer una estrategia, ya que es necesario responder a los siguientes puntos:

- ¿Qué se quiere respaldar? No se puede respaldar toda la información, sólo aquella que sea considerada crítica o que permita recuperar en caso de pérdida aspectos como: funcionalidad, usuarios y privilegios, información crítica.
- ¿Cada cuánto se debe realizar? Algunos respaldos deberán realizarse con mayor frecuencia que otros, dependiendo de la ventana de tiempo en que la información se modifica.
- ¿Dónde se va a almacenar? No tiene mucho sentido generar un respaldo para que se quede en el mismo servidor, deberá considerarse infraestructura adicional para resguardar los respaldos de forma segura.
- ¿Qué tipo de respaldo se va a generar? Actualmente existen respaldos totales (información completa) o bien respaldos diferenciales o incrementales (últimas modificaciones a la información), por lo que esto también debe considerarse.
- ¿Se deberá probar el respaldo generado? Un error muy frecuente consiste en generar los respaldos, pero no probar su correcto funcionamiento. Es necesario probar la recuperación de la información almacenada.

Los puntos anteriores deberán ser determinados por las reglas del negocio, pero también acorde a los recursos con los que se cuenta para realizar los respaldos.

RESUMEN

Conforme a lo revisado es menester señalar la importancia, en gran medida, de un sistema de seguridad en las redes de telecomunicación.

Los sistemas de seguridad contemplan políticas y herramientas utilizadas para prevenir ataques a la integridad de un sistema de información, por lo que es recomendable protegerse con los requerimientos mínimos para la detección de sistemas intrusos en el equipo de trabajo.

También se habló y se especificó la importancia de un respaldo de la información almacenada en nuestros equipos. La práctica del respaldo de la información siempre debe estar presente en el trabajo diario, ya que siempre es susceptible a las amenazas informáticas, a las amenazas naturales y a los errores humanos que pueden dañar la información.

En conclusión, es de suma importancia valorar los protocolos de seguridad en nuestras áreas de trabajo, con la finalidad de resolver un problema, en este caso, el de seguridad. Un protocolo de seguridad es una forma de aplicar servicios de seguridad a sistemas, redes y computadoras personales.

BIBLIOGRAFÍA

SUGERIDA

Autor	Capítulo	Páginas
Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social, y al Comité de las Regiones de Seguridad	Seguridad de las redes y de la información: Propuesta para un enfoque político europeo.	1-12

Barrett, Daniel J. y otros (2003). *Linux security cookbook*. California: O'Reilly Media, Sebastopol.

SSI, UNAM-CERT. *Seguridad de la información*. México: UNAM. Disponible en: http://www.seguridad.unam.mx

Unidad 3

Seguridad

OBJETIVO PARTICULAR

El alumno estudiará los algoritmos de la criptografía simétrica y asimétrica, que le permitirán configurar diversas herramientas para aplicar los servicios de la seguridad informática a las redes de datos.

TEMARIO DETALLADO
(16 horas)

3. Seguridad

- 3.1. Importancia de la seguridad en redes
- 3.2. Funciones de seguridad
  - 3.2.1. Análisis de riesgo
  - 3.2.2. Servicios de seguridad
    - 3.2.2.1. Autenticación de las comunicaciones
    - 3.2.2.2. Autenticación de los datos
    - 3.2.2.3. Control de acceso
    - 3.2.2.4. Garantía de la privacidad de los datos
    - 3.2.2.5. Análisis de flujo de tráfico
    - 3.2.2.6. Garantía de la integridad de los datos
    - 3.2.2.7. Reconocimiento del receptor y/o transmisor

INTRODUCCIÓN

La seguridad en redes es un elemento desconocido por gran parte del personal de una organización. Generalmente se le reconoce, pero en la práctica no se le otorga la importancia debida. Tal vez una de las razones de este acontecer sea la inversión que debe realizarse en análisis e infraestructura para su adecuada aplicación. El reto es dar a conocer la importancia de la seguridad en redes, el impacto que tienen los ataques informáticos en la economía y prestigio de la organización.

Existen diversos ataques que afectan la red dentro de las organizaciones. Entre ellos, uno de los más comunes contra algunas de las entidades financieras más importantes del mundo, consiste en realizar una inundación de peticiones para que su sitio web pierda disponibilidad, dejando en evidencia ante el mundo que cualquier sitio tiene algún grado de vulnerabilidad.

La seguridad en redes es una necesidad que las organizaciones deben tener muy presente. Al presente, es cada vez más común que una empresa cuente con tecnología para evitar intrusiones, o que solicite un análisis de riesgos para medir su nivel de seguridad. Hay nuevos retos, nuevas formas de atacar redes, y es necesario estar preparados para responder ante nuevas amenazas. Existen corporaciones que diariamente se dedican a romper la seguridad de una empresa, cobrando grandes cantidades de dinero.

Por lo anterior, la seguridad en redes se convierte en un tema importante para mantener la seguridad de la información.

3.1. Importancia de la seguridad en redes

Así como la información tiene un valor específico para cada organización que la utiliza para tomar decisiones, la seguridad informática aplicada a redes de cómputo también es importante, pues minimiza el riesgo existente de que dicha información sea comprometida o puesta en peligro, estableciendo los mecanismos adecuados y necesarios para cada caso.

La seguridad en redes es una disciplina que requiere de constante actualización. Por ejemplo, una aplicación antivirus hará bien su tarea al revisar los correos electrónicos de una empresa, mientras mantenga actualizada su base de datos. En caso de detener las actualizaciones del programa antivirus, se exponen distintos recursos, entre ellos, uno de los más valiosos: la red.

Puede pensarse en un *firewall*, como un dispositivo que controla los accesos a la red manteniéndola aislada de algunas amenazas en internet. Este dispositivo se maneja con base en reglas definidas por un administrador, las cuales requieren modificarse eventualmente cuando una aplicación nueva se integra; si no hay personal calificado para esta tarea, entonces esa aplicación puede quedar expuesta a un ataque.

La seguridad en redes no es tarea que se realice una sola vez, es un proceso constante de análisis e implementación ya que, lamentablemente, día con día aparecen nuevas amenazas, técnicas de ataque y vulnerabilidades en los sistemas. No se puede correr el riesgo de pensar que nadie se fijará en la red o que no exista algún recurso para vulnerarla y, por lo tanto, que no se necesite de seguridad informática.

El punto anterior es independiente de si la empresa es grande como una transnacional o bien pequeña como una PyME, se puede pensar erróneamente que como la empresa es pequeña, no es un objetivo de ataques informáticos; pero la mala noticia es que sí puede ser usada como origen de un ataque hacia empresas más grandes.

También es necesario considerar que pueden existir ataques dirigidos desde la propia organización hacia su misma infraestructura.

3.2. Funciones de la seguridad

La seguridad dentro de las organizaciones es un tema importante, pues muchas de las pérdidas de información se dan por fallos o debilidad en la seguridad de los sistemas y redes involucrados en el tratamiento de la información.

El tema de la seguridad es complejo, sin embargo, un punto importante que debe ejecutarse para comenzar a aplicar, mejorar o actualizar la seguridad dentro de la organización consiste en analizar los riesgos.

Tal análisis permitirá determinar los puntos más importantes sobre los cuales se deben enfocar los esfuerzos para mantener seguros los activos de la organización.

3.2.1. Análisis de riesgo

El primer paso para determinar el nivel de seguridad que se requiere, es la realización de un análisis de riesgos en la infraestructura informática y de red. El análisis de riesgos emplea una metodología para examinar aspectos organizacionales y tecnológicos de una empresa, y determinar sus necesidades en cuanto a seguridad de la información.

Un riesgo es la posibilidad de que un sistema sufra daño o pérdida. Lo que se logra con un análisis de riesgos es identificarlos, analizarlos para saber dónde se originan y tomar las medidas necesarias para mitigarlos. Conviene aclarar que no existe sistema seguro al cien por ciento, pues siempre hay errores humanos.

Un análisis de riesgos se compone básicamente de tres fases:

1. Elaboración de perfiles de activos y amenazas. En esta etapa se identifican los activos de la organización; es decir, la información, los sistemas, los procesos, el *software*, el *hardware* y el personal (este último no como un activo, sino como capital humano que interactúa con los activos). Se identifican las áreas problemáticas en cada activo.

Por ejemplo, en un análisis se podría encontrar que hay fuentes de amenazas internas referidas a personal poco confiable, o localizar defectos en un sistema o en un equipo de *hardware*.

El encontrar estas áreas problemáticas permite identificar cuáles serían las complicaciones que pudieren presentarse, es decir, los riesgos que se corren con estos problemas. Si el personal no es confiable, hay riesgo de que cierta información confidencial sea revelada o modificada. Si se encuentran deficiencias en *hardware* o *software*, puede ser una fuente de pérdida o exposición accidental de información.

En esta fase, también se identifican los aspectos de seguridad que se deben proteger: confidencialidad, integridad y disponibilidad de los datos.

2. Identificación de vulnerabilidades. En la fase anterior se identificaron los activos y las amenazas potenciales. En ésta se detecta qué tan vulnerable es el sistema o la red a esas amenazas; se focalizan recursos para encontrar errores de diseño, problemas de aplicación, configuraciones defectuosas en toda la red, usando herramientas de evaluación de vulnerabilidades (manuales o automatizadas), como un escáner de infraestructura o un escáner de sistema operativo y servicios que se ejecutan.

Esta evaluación dará como resultado un informe preliminar donde se agrupen los resultados obtenidos de la evaluación, y brindará un resumen con el nivel de severidad de cada vulnerabilidad, así como una descripción de cada uno de esos

niveles. Además, proporciona una relación entre los componentes evaluados y su nivel de severidad asociado.

En esta fase se puede encontrar, por ejemplo, una vulnerabilidad en el puerto 80 (el cual brinda servicios web), o se puede encontrar que el servidor de correo electrónico de la empresa cuenta con las actualizaciones debidas y no tiene alguna vulnerabilidad conocida. Esta tarea debe realizarse constantemente, porque conforme avanza la tecnología y las técnicas de intrusión, pueden aparecer vulnerabilidades nuevas que antes no se detectaban.

La información recabada en esta fase brinda la base para tomar las medidas correctivas necesarias para que el riesgo de seguridad disminuya.

3. Estrategias de protección. Una estrategia de protección define las iniciativas que una organización debe implementar para mantener la seguridad interna. Para ello, se necesita la información obtenida del análisis de riesgos, y así poder generar planes de reducción de amenazas.

Por ejemplo, si el informe indica que un servidor que aloja páginas web se encuentra en estado vulnerable, una de las acciones correctivas será actualizar la aplicación del servicio, subsanando la parte vulnerable.

Sin embargo, esta etapa resulta más compleja, dado que, siguiendo con el ejemplo, para proteger una página web visible en internet, es necesario contar con estrategias para cada uno de los elementos involucrados en su funcionamiento. Esto implica pensar en protección de la red (interna y externa que enlaza con

internet), el servidor o servidores en los que se aloja el sitio, el personal involucrado en la implementación y mantenimiento de la página *web*, entre otros aspectos.

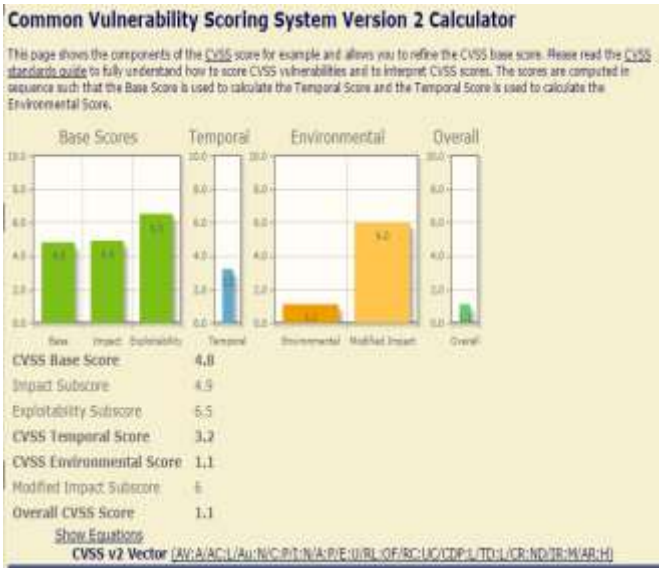
Es importante apuntar que sí existen implicaciones económicas y de prestigio al presentarse una intrusión en la red de la organización.

El impacto de una intrusión es un aspecto que deberá considerarse al realizar el análisis de riesgos sobre los activos de la organización. La pérdida de información es uno de los factores que hay que tener muy presentes, ya que las implicaciones económicas que acarrea pueden ser graves.

Sin embargo, no hay que dejar de lado el prestigio de la empresa, el cual se ve afectado seriamente, sobre todo en la credibilidad y confianza de sus clientes (si es que la organización se dedica a vender algún bien o prestar algún servicio).

Por ejemplo, es común leer en las noticias que cierta empresa ha sido vulnerada y se pudo extraer información de su cartera de clientes, o que la infraestructura tecnológica de determinada organización ha sido empleada como plataforma para atacar a otra.

En cuanto al *software* y *hardware,* existe una base de datos en línea en la que se publican periódicamente las vulnerabilidades existentes. La liga es: https://nvd.nist.gov/home.cfm. Adicionalmente, se cuenta con una calculadora que pondera el impacto que una vulnerabilidad tiene sobre la disponibilidad, confidencialidad e integridad de un activo. La liga es: http://nvd.nist.gov/cvss.cfm?calculator&version=2.



Calculadora de impacto de vulnerabilidades

3.2.2. Servicios de seguridad

Los servicios de seguridad en redes permiten monitorizar el tráfico en la red y los dispositivos de la organización. Estos servicios pueden ser contratados con una empresa dedicada a esta tarea o, bien, se puede implementar dentro de la organización.

El objetivo principal es encontrar una actividad que no se considere "normal" dentro de la operación cotidiana de la red, esto permitirá evitar o mitigar ataques (tanto internos como externos) hacia un equipo o equipos, segmento de red o la red completa.

El objetivo primordial del uso de servicios de seguridad de una red es proteger los activos de información de la organización y mantener en todo momento su confidencialidad, disponibilidad e integridad.

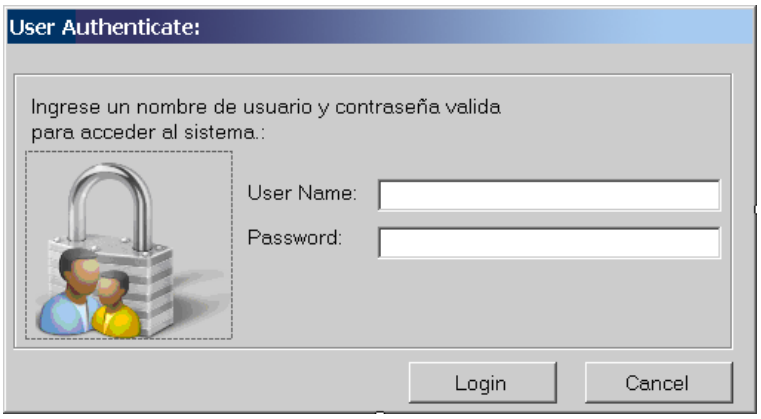
3.2.2.1. Autenticación de las comunicaciones

La autenticación sirve para garantizar que los participantes de la comunicación establecida dentro de los dispositivos y la red de la organización cuentan realmente con una identidad válida.

Por ejemplo, cuando en un sistema se ingresa nombre de usuario y contraseña, la computadora no tiene la capacidad de validar quién es por el aspecto físico, sino que comprueba que los datos ingresados coincidan con los guardados en una base de datos y que correspondan a la persona en cuestión, autenticando la validez de la información ingresada.

También se pueden autenticar las transacciones realizadas mediante una red de cómputo. Casos como el envío de información de inventarios entre una sucursal y su oficina central o el acceso remoto a un servidor de la empresa, requieren de autenticar las comunicaciones. Si no se realiza, se corre el riesgo de que cualquier usuario, en cualquier parte de internet o de la misma organización, pueda obtener o intentar obtener acceso a un servidor principal sin que nada se lo impida.

La autenticación más básica se puede realizar mediante la verificación de nombre de usuario y contraseña. Este mecanismo es el más utilizado actualmente, pero presenta debilidades cuando se usan contraseñas escritas con palabras comunes y fáciles de adivinar, o cuando se utilizan medios que están a la vista de cualquier intruso en internet.



Autenticación mediante usuario y contraseña

Fuente: http://msdn.microsoft.com/es-es/library/bb972283.aspx

Existen mecanismos más robustos de autenticación que se basan en criptografía asimétrica. Este tipo de criptografía utiliza una llave pública y una llave privada. Quien desea enviar información a un participante, la cifra utilizando la llave pública. El receptor es el único que puede descifrarla, empleando su llave privada. Este tipo de sistema se basa en la construcción de funciones matemáticas, cuyo inverso sea computacionalmente imposible de calcular. RSA es de los estándares más conocidos en criptografía asimétrica.

Cuando dos entidades de una red de cómputo se autentican usando llave pública, solamente los que compartan esta llave podrán participar en el proceso de autenticación para realizar sus tareas. Por ejemplo, *Secure Shell* es una aplicación utilizada para conexiones remotas seguras y ofrece la posibilidad de autenticación remota mediante llave pública.

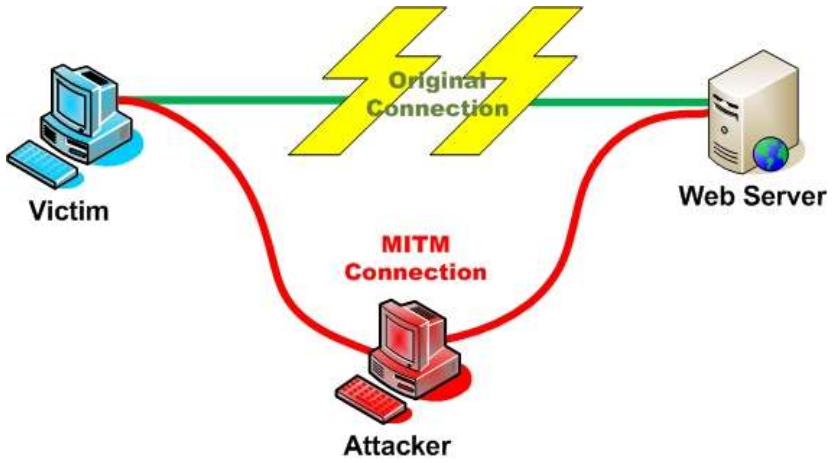
3.2.2.2. Autenticación de los datos

Los datos que se intercambian en la red entre los equipos deben ser correctamente verificados: el origen del que proceden, en contenido que se envía no debe ser modificado y el destinatario debe ser el indicado. Este aspecto es importante, ya que permite corroborar el origen de los datos que se están recibiendo, así como las

posibles modificaciones e intercepciones de los datos en su camino hacia el destino final.

Este punto es importante, ya que la información puede ser modificada en el tránsito hacia el destinatario o, bien, llegar a un destino diferente al original. Lo anterior puede tener un impacto fuerte en la confidencialidad de la información, sobre todo si ésta se considera un activo crítico.

Uno de los ataques más comunes dentro de las redes de computadoras es el que se conoce como *Man in the Middle*.



Ataque *Man in the Middle*.

Fuente: https://www.owasp.org/index.php/Man-in-the-middle_attack

Por lo anterior, es necesario contar con algún mecanismo que permita mantener la integridad de los datos enviados mediante una red. El primer paso consiste en cifrar el canal de comunicación entre origen y destino. Esto se puede realizar mediante un cifrado asimétrico (para mayor robustez). Lo que permitirá disminuir la modificación de los datos que se envían durante su tránsito del origen al destino.

Es importante notar que los datos se encuentran en claro antes de ser enviados y se cifran sólo durante su tránsito en el canal de comunicación para ser descifrados

finalmente al llegar a su destino (donde vuelven a estar en claro). Para complementar, se puede considerar el empleo de *IPsec.*

Al respecto, Tanenbaum menciona que:

> El diseño IPsec completo es una estructura para servicios, algoritmos y granularidades múltiples. La razón para los servicios múltiples es que no todas las personas quieren pagar el precio por tener todos los servicios todo el tiempo, por lo que los servicios están disponibles a la carta. Los servicios principales son confidencialidad, integridad de datos y protección contra ataques de repetición (un intruso repite una conversación). Todos estos se basan en criptografía simétrica debido a que el alto rendimiento es crucial (2003: 772-773).

El uso que se puede dar a IPsec consiste en que agrega datos de autenticación al paquete enviado por la red (mediante el protocolo TCP/IP). Esto permite que al llegar al destino se pueda verificar si la información fue o no modificada en el camino.

Posteriormente, es necesario revisar los datos en el destino, lo que generalmente se realiza en la capa de aplicación. Para esto, es necesario contar con la descripción de los datos que se espera recibir.

Por ejemplo, si se espera información tal como nombre de usuario, correo electrónico, contraseña y dirección IP., los datos deben ser recibidos y verificados para que continúen fluyendo en el proceso del que forman parte.

En caso de que los datos recibidos no cumplan con las características y especificaciones indicadas, es necesario considerar una serie de medidas que deben tomarse para corregir y verificar qué sucedió.

Las causas pueden ser diversas: fallo en el establecimiento de las comunicaciones, error al enviar los datos por parte del origen, modificación en el canal de comunicación, modificación al recibir los datos. Estas medidas deben tomarse con base en el análisis de riesgos previos y las soluciones propuestas en la tercera etapa.

3.2.2.3. Control de acceso

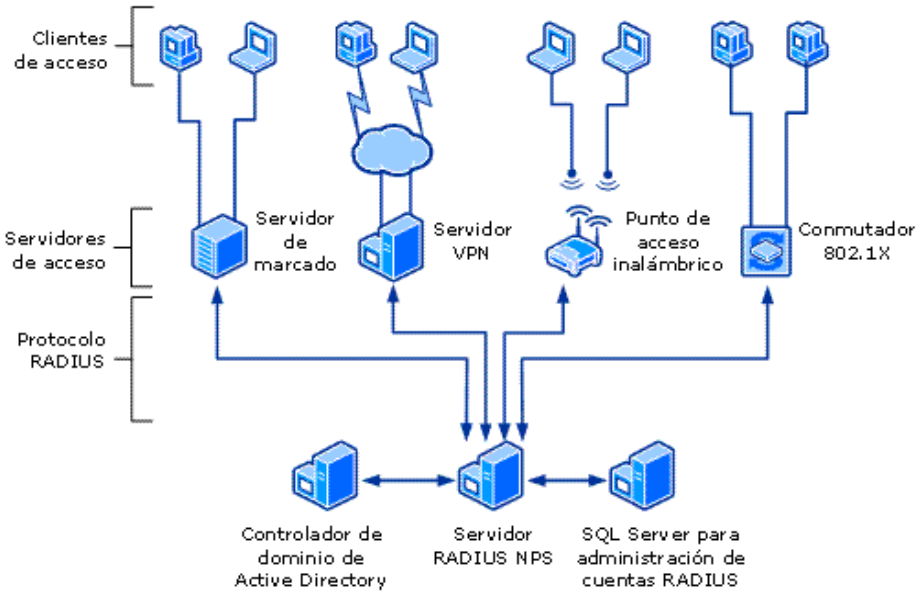
Además de autenticar a los usuarios y las conexiones que se establecen, es necesario controlar los accesos en nivel de red y para cada usuario, de modo que cada uno pueda tener los servicios y recursos disponibles según su identidad.

Para implementar el control de accesos, es necesario realizar primero un ejercicio teórico en el que debe responderse a las preguntas:

- ¿Quiénes son los usuarios?
- ¿Cuáles son las actividades, conexiones, que se deben realizar?
- ¿Cuáles son los equipos, aplicaciones, recursos a los que tendrán acceso?

Por ejemplo, cuando se visita el portal de un banco y se ingresan las credenciales, se espera ver únicamente la información de esa cuenta y que nadie más pueda tener acceso a ella. Igualmente, un alumno accede a su historial académico únicamente y según recursos que sean compartidos entre otros miembros de su grupo; no es posible ver calificaciones de otros alumnos, porque el sistema controla los recursos asignados a cada perfil autenticado.

RADIUS (del inglés *Remote Authentication Dial-In User Service*) es un sistema que permite autenticar usuarios, pero además aprueba crear perfiles de usuario para asignarles permisos y roles una vez que han sido autenticados. Es muy utilizado para redes inalámbricas grandes, donde puede haber varios roles. En una universidad hay perfiles de estudiante, investigador o administrativo, con permisos y privilegios distintos para cada uno.



Ejemplo de uso de RADIUS

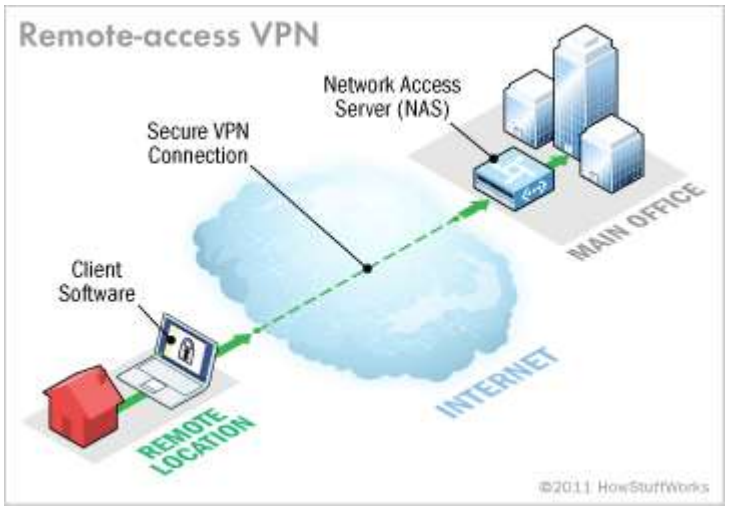
Fuente: http://technet.microsoft.com/es-es/library/cc755248.aspx

Los servicios son recursos de red cuyo acceso será susceptible de ser controlado. Volviendo al ejemplo de una red universitaria, un alumno puede tener derecho a ver videos con un ancho de banda limitado, pero un investigador tendrá asignado un ancho de banda mayor; de la misma forma como un administrativo puede tener permisos de hacer llamadas telefónicas por internet. Es cuestión solamente de definir esos privilegios en el sistema de control de acceso de la organización.

Esto permitirá tener un panorama claro de cuáles son los accesos que se requieren y con qué finalidad, así como identificar a quién los usará.

Otra forma de controlar los accesos después del proceso de autenticación, es la dirección IP de origen. Existen servicios que solamente pueden ser consultados desde determinada red, impidiendo su acceso desde cualquier red casera o café internet. Las *Virtual Private Networks* (*VPN*) o Redes Privadas Virtuales, permiten accesos a redes privadas desde redes públicas.

Por ejemplo, se emplea conexión a red VPN para poder acceder a una biblioteca digital desde la comodidad de los hogares, porque una VPN los hace parte de la red universitaria desde la cual es posible ingresar a ese sitio.



Funcionamiento de VPN

Fuente: http://computer.howstuffworks.com/vpn3.htm

3.2.2.4. Garantía de la privacidad de los datos

Lo único que garantiza la privacidad de los datos es la criptografía. Junto con esta, las recomendaciones básicas de seguridad permitirán mantener la confidencialidad de la información.

La criptografía se basa en funciones matemáticas para cifrar y descifrar un mensaje. El cifrado es el proceso de transformar un mensaje para ocultar su contenido. Al proceso de regresar un mensaje cifrado a texto en claro se le conoce como *descifrado*.

La seguridad del cifrado debe basarse en la seguridad del algoritmo y de la llave. El algoritmo y los detalles de implementación son públicamente conocidos y basados en estándares. La criptografía moderna se usa en la selección de llaves de un gran espacio, para alimentar un algoritmo que se encargará de cifrar un texto o mensaje en claro. La llave es un acuerdo previo de un secreto, que solamente conocen los participantes y se comparte para alimentar el algoritmo. Si la llave se compromete, la seguridad ya no se garantiza.

Internet es una red pública en la cual todo mundo está conectado. Para garantizar la privacidad de los datos en una transacción que es pública, se necesitan elementos criptográficos.

Por ejemplo, una red de tipo VPN debe soportar cifrado de datos para que realmente sea segura. La conexión remota a uno de nuestros servidores debe ser mediante canales seguros, para garantizar que nadie vea las contraseñas y la información que se encuentra en tránsito.

Uno de los principales problemas consisten en que las aplicaciones, conexiones de red, bases de datos, sitios web, entre otros, no fueron diseñados pensando en la seguridad de la información. Esto impacta en la privacidad, disponibilidad e integridad de los datos que se manipulan.

Por ejemplo, es posible robar sesiones de redes sociales, como *Facebook o Twitter*, en redes inalámbricas, debido a que no se asegura el cifrado de las comunicaciones. Basta con ir a una plaza comercial con servicio inalámbrico público, ejecutar un programa y comenzar a robar sesiones sin necesidad de conocimientos amplios en técnicas de intrusión.

Si se tiene información confidencial en una computadora personal, existen programas para cifrar el contenido de programas. Pero hay que recordar que siempre se debe tener cuidado con las contraseñas utilizadas para cifrar la información, esas llaves son el acceso a los recursos.

3.2.2.5. Análisis del flujo de tráfico

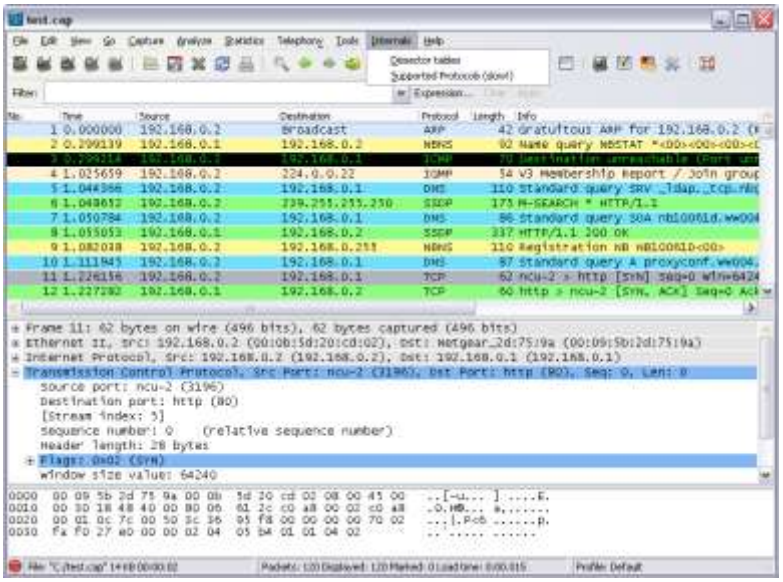
El análisis de flujo de tráfico consiste en estudiar los patrones de los paquetes, aunque éstos se encuentren cifrados.

Analizar el flujo de tráfico de una red es muy importante. Es la única forma de evaluar lo que circula por una red y determinar si es potencialmente dañino o no. Sirve también para evaluar la confidencialidad de la información. Se puede detectar si una de las aplicaciones está enviando la información como texto claro y no lo está cifrando.

Las herramientas que permiten estas tareas son conocidas como analizadores de protocolos o *sniffers*, y son de gran ayuda para un encargado de la red y su seguridad. Pero estas herramientas también pueden ser utilizadas para tener acceso a un sistema con el fin de dañarlo o usarlo para dañar a terceros. Son herramientas muy útiles para auditar la confidencialidad de la información.

Los *sniffers* permiten la inspección profunda de cientos de protocolos. Los protocolos basados en TCP/IP están compuestos por campos de control y campos de información. Si una conversación en la red no va cifrada, es posible llegar a ver cierta información que pueda atentar contra datos confidenciales. Existen tanto los comerciales como los de distribución libre.

Uno de los más populares se llama *Wireshark* y está disponible en http://www.wireshark.org.



Pantalla de Wireshark

Fuente: https://www.wireshark.org/docs/wsug_html/

Para poder interpretar la información de un analizador de protocolos, es necesario un conocimiento amplio en cada protocolo de red, su funcionamiento y sus campos.

3.2.2.6. Garantía de la integridad de los datos

Una vez tomadas todas las medidas de seguridad pertinentes, existen herramientas para verificar periódicamente la integridad de la información. Para garantizar integridad, también la criptografía juega un papel muy importante. Las funciones *hash* son funciones unidireccionales, porque pueden calcularse en un sentido, pero no en su modo inverso.

Estas funciones aceptan entradas grandes y entregan salidas de longitud fijas y pequeñas. No es posible que dos entradas resulten en el mismo valor. Este tipo de funciones son las más comunes para verificar la integridad de los datos, ya que cada valor es considerado como una huella digital. De esta manera se puede producir un identificador único para cualquier documento digital. Entre los algoritmos más utilizados están MD5 y SHA.

Por ejemplo, cuando se descarga software de internet, generalmente se pide verificar la integridad de ese programa mediante una función hash. Los proveedores publican una firma digital del programa, la cual se compara con la firma que arroja la ejecución de la función hash en el programa descargado. Si los resultados son iguales, entonces ese programa no ha sido modificado, por lo tanto, está íntegro.

Ha ocurrido que sitios *web* han sido comprometidos y alterados los programas que ofrecen para descarga. Si no se verifica la integridad, se corre el riesgo de estar instalando un programa corrupto o alterado por un tercero malicioso.

Este mismo principio se puede aplicar a los datos almacenados en algún dispositivo, ya que puede cifrarse no sólo la comunicación en red; sino que también un disco

duro completo o una partición, o bien, un dispositivo portátil externo (memoria USB, por ejemplo). La información almacenada estará protegida y sólo quién tenga la llave tendrá acceso a recuperar lo que se encuentra cifrado.

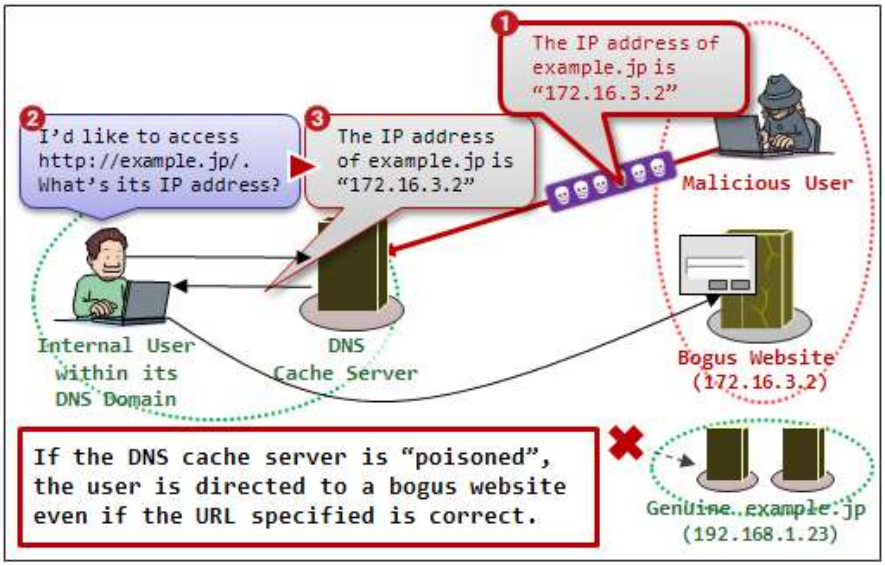
3.2.2.7. Reconocimiento del receptor y/o transmisor

El reconocimiento entre receptor y transmisor se realiza mediante la autenticación de algún parámetro de identidad.

Los parámetros más utilizados son la dirección IP origen y destino, la dirección física MAC o, como ya se ha visto, algún protocolo que implemente criptografía de llave pública. Este reconocimiento es importante para asegurarse de que se está estableciendo comunicación con quien se desea y que no se está iniciando una conversación con una entidad suplantadora.

Existen mecanismos de intrusión que interceptan las comunicaciones o que suplantan identidades y hacen creer que son los destinatarios válidos. Esto puede provocar enviar información confidencial a una entidad no autorizada. La información se compromete si no se tiene este reconocimiento.

Uno de los ataques que pueden llegar a presentarse es el que se conoce como DNS Caché Poisoning, en el cual se modifica temporalmente la forma de resolver los nombres (nombre de dominio-dirección IP) de los servidores o servicios destino, cambiando por algún otro que puede ser malicioso.



DNS Caché Poisoning

Fuente: http://www.ipa.go.jp/security/english/vuln/200809_DNS_en.html

RESUMEN

En esta unidad se señaló la importancia de aplicar servicios de seguridad en una red y los servicios de seguridad más trascendentes; se observó que en ciertas empresas o instituciones, aunque se les reconozca, no se les otorga la significación debida.

Se resaltó la importancia de la seguridad en redes, el impacto que tienen los ataques informáticos en la economía y prestigio de la organización.

Por ello, se hizo hincapié en la relevancia de un análisis de riesgos, señalando sus ventajas y sus características.

Punto a destacar fueron los servicios de seguridad en cuanto a autenticación, integridad y control de acceso.

Por lo anterior, el tema de seguridad en redes es sumamente importante para mantener la seguridad de la información dentro de la organización.

BIBLIOGRAFÍA

SUGERIDA

Autor	Capítulo	Páginas
Tanenbaum, Andrew S.	8	721
Herzog, Pete	Sección A, B y C	33-66.
Stoneburner, Gary	3	8-26

Tanenbaum, Andrew S. (2003). *Redes de computadoras* (4ª. Ed.). México: Pearson Educación, 912 pp.

Herzog, Pete (2000). *Manual de la metodología abierta de testeo de seguridad*, ISECOM-Instituto para la Seguridad y las *Metodologías* Abiertas, OSSTMM 2.1., pp. 33-66. Disponible en: http://isecom.securenetltd.com/OSSTMM.es.2.1.pdf

Stoneburner, Gary, et al. (2002). *Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology*, pp. 8-26. Disponible en: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

Unidad 4

Redes inalámbricas

OBJETIVO PARTICULAR

El alumno conocerá las principales tecnologías de redes *wireless*, hardware, estándares, aplicaciones y protocolos de seguridad para aplicar soluciones de comunicación inalámbrica acordes a necesidades específicas.

TEMARIO DETALLADO
(18 horas)

4. Redes inalámbricas

- 4.1. Estándar 802.11
- 4.2. Protocolos WEP, WAP
- 4.3. Dispositivos inalámbricos

INTRODUCCIÓN

El diseño, aplicación y uso de comunicación inalámbrica digital es una tecnología que está creciendo a grandes pasos. El número de usuarios con dispositivos que pueden conectarse de manera inalámbrica crece cada día, por lo que las tecnologías empleadas para su ejecución deben ir acordes a las necesidades de interconexión que se tengan.

La aplicación de una infraestructura de redes inalámbricas se enfrenta a retos que las redes cableadas no presentan; por ejemplo, la colocación estratégica de los puntos de acceso, la intensidad de la señal para que cubra satisfactoriamente el área requerida, el protocolo mediante el cual se emplea la comunicación y el cifrado que utiliza la seguridad, etc.

Parte de la importancia que tienen hoy radica en el ahorro que representan, ya que este tipo de suministro elimina la adquisición de cableado y conexiones físicas entre los nodos de la red.

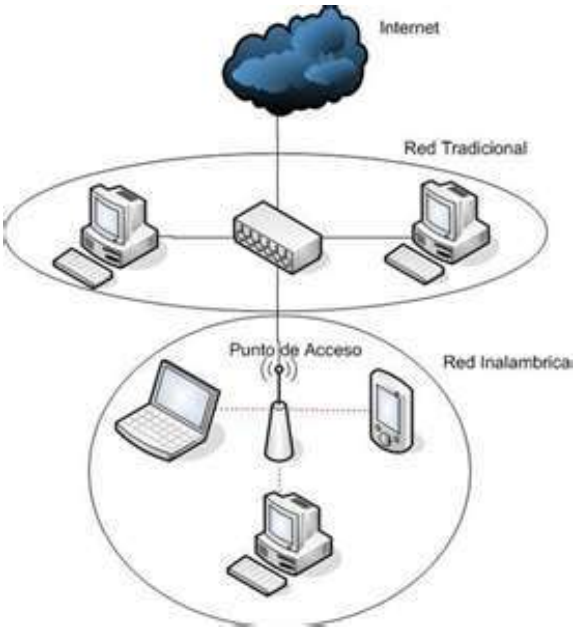
Actualmente existen diversas soluciones que propician adoptar esta tecnología, por lo que es necesario un análisis que determine cuál de ellas es conveniente usar de acuerdo a las necesidades de los usuarios.

4.1. Estándar 802.11

Con el surgimiento de las computadoras portátiles también surge la necesidad de conectarse en cualquier punto de manera inalámbrica, en lugar de estar buscando un punto de conexión para el cable de red.

Los primeros intentos consistieron en interconectar varias computadoras en una LAN, con una marca específica de dispositivos (transmisores y receptores) para realizarlo. Esto representó un problema, dado que al intentar conectar ese mismo equipo en otra red LAN, el dispositivo de interconexión no funcionaba.

A partir de lo anterior, surgió la necesidad de estandarizar las redes LAN inalámbricas.



Ejemplo de punto de acceso para una red inalámbrica
Fuente: http://euri-yuri.blogspot.mx/

El estándar 802.11 perteneciente a la IEEE (*Institute of Electrical and Electronics Engineer*) establece las normas de funcionamiento para redes LAN inalámbricas. Este estándar es empleado por la mayoría de los sistemas; es popularmente conocido como Wi-Fi.

El estándar 802.11 es compatible con Ethernet sobre la capa de enlace de datos, ya que cuando este estándar comenzó a emplearse, Ethernet era la tecnología dominante para el enlace de redes.

En las primeras versiones del estándar, la velocidad de enlace de la red LAN estaba ajustada para 1 y 2 Mbps, sin embargo, estas velocidades pronto se vieron rebasadas por la demanda de rapidez en la comunicación, por lo que hubo que realizar mejoras.

Según Tanenbaum:

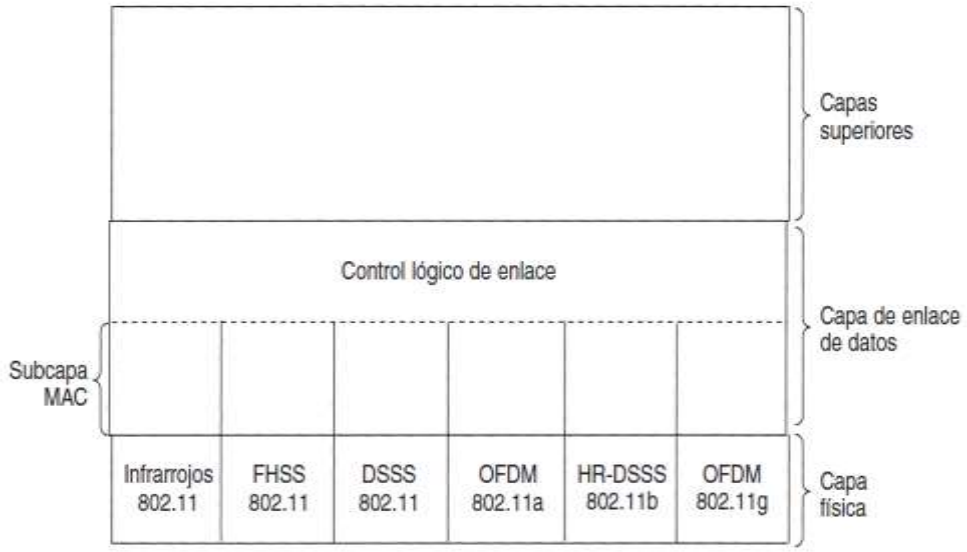
El estándar 802.11a utiliza una banda de frecuencia más ancha y se ejecuta a velocidades de hasta 54 Mbps. El estándar 802.11b utiliza la misma banda de frecuencia que el 802.11, pero se vale de una técnica de modulación diferente para alcanzar 11 Mbps (2003: 70).

Una vez presente el estándar, el uso de redes LAN inalámbricas se ha vuelto muy popular y su uso se encuentra extendido, por lo que se usa para proporcionar cobertura en escuelas, hospitales, edificios de oficinas, aeropuertos y otros lugares públicos.

Pila de protocolos 802.11

La pila de protocolos 802.11 comprende también la tecnología Ethernet, ya que comparten ciertas similitudes en su estructura. La capa física corresponde muy bien

con la capa física OSI; pero la capa de enlace de datos de todos los protocolos 802 se divide en dos o más subcapas.



Pila de protocolos 802.11
Fuente: Tanenbaum, 2003: 293

El estándar especifica 3 formas de transmisión que están permitidas en la capa física: el método de infrarrojos emplea la misma tecnología que emplean los controles remotos; los otros dos métodos emplean el radio de corto alcance (FHSS y DSSS). OFDM y HR-DSSS son similares, pero ocupan anchos de banda más altos; posteriormente se introdujo otra variante de OFDM, pero en otra frecuencia.

Capa física del estándar 802.11

Cada una de las 5 formas de transmisión es diferente en la tecnología que emplea, así como en la velocidad que alcanza. A continuación se presenta brevemente cada uno de los elementos de la capa física con la cual opera el estándar. Ver tabla 1.

Tecnología	Características
Infrarrojo	• Velocidad de 1 y 2 Mbps. • Transmisión difusa (no requiere línea visual). • Emplea código de Gray. • La señal infrarroja no traspasa paredes, por lo que no es una opción muy popular.
Espectro Disperso con Salto de Frecuencia (FHSS)	• 79 canales con un ancho de banda de 1 MHz cada uno. • Emplea un generador de números pseudoaleatorios para producir la secuencia de frecuencias a saltar. • El tiempo de permanencia debe ser menor que 400 m/seg. • Emplea un ancho de banda bajo. • Permite establecer conexiones de un edificio a otro.
Espectro Disperso de Secuencia Directa (DSSS)	• Opera a 1 y 2 Mbps. • Emplea la secuencia de *Barker* para la transmisión de datos. • Fue empleado durante mucho tiempo en EUA por los equipos de comunicación inalámbrica.
Multiplexión por División de Frecuencias Ortogonales (OFDM)	• Puede enviar hasta 54 Mbps en banda ancha de 5 GHz. • Se utiliza en frecuencias diferentes: 52 en total (48 para datos y 4 para sincronización). • Mejora la inmunidad a la interferencia de bandas estrechas. • Posibilita el uso de bandas no contiguas. • Es compatible con el sistema europeo HiperLAN/2.

Espectro Disperso de Secuencia Directa de Alta Velocidad (HR-DSSS)	• Alcanza 11 Mbps en la banda de 2.4 GHz. • Utiliza modulación por desplazamiento de fase (para ser compatible con DSSS). • Utiliza códigos Walsh/Hadamard. • La tasa de datos se puede adaptar dinámicamente, para alcanzar la velocidad más óptima durante su operación.

Tabla 1. Capa física del estándar 802.11
Fuente: autoría propia.

Con base en la capa física del protocolo 802.11, cada una de sus variantes emplea alguna de las tecnologías mencionadas. A continuación se presentan las principales características de cada una de las variantes del protocolo 802.11.

Protocolo 802.11a

Esta versión del protocolo fue la primera en liberarse y cuenta con las siguientes características:

- Velocidad máxima de 54 Mbps.
- Opera en el espectro de 5 GHz.
- Menos saturado.
- No es compatible con las normas 802.11b y 802.11g.

Esta versión utiliza el mismo juego de protocolos base que el estándar original, también opera en la banda de 5 GHz y utiliza 52 subportadoras OFDM. Cuenta con 12 canales no solapados: 8 para red inalámbrica y 4 para conexiones punto a punto.

Protocolo 802.11b

- Velocidad máxima de 11 Mbps.
- Opera en el espectro de 2.4 GHz sin licencia.
- Se producen interferencias en el espectro de 2.4 GHz en el que opera, ya que hay gran cantidad de dispositivos que funcionan en la misma frecuencia, por ejemplo: hornos de microondas, teléfonos inalámbricos, entre otros.
- Popularmente conocido como Wi-Fi.
- Modulación DSSS (y compatibilidad con estos dispositivos del estándar 802.11a).

Protocolo 802.11g

- Velocidades de datos con distintos tipos de modulación: 6, 9, 12, 18, 24, 36, 48 y 54 Mbps; puede volver a 11 Mbps con DSSS y CCK, 5,5, 2 y 1.
- Multiplexión de división de frecuencia ortogonal (OFDM) con canales de subportadoras 52; es compatible con 802. 11b utilizando DSSS y CCK.
- Tres canales no superpuestos en la frecuencia de uso industrial, científico, médico (ISM) de la banda de 2,4 GHz.

Protocolo 802.11n

- Velocidades de datos con distintos tipos de modulación: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps.
- Multiplexión de división de frecuencia ortogonal (OFDM) de multiplexación utilizando múltiple entrada/múltiple salida (MIMO) y la unión de canales (CB).
- Tres canales no superpuestos en la banda de frecuencia (ISM) industrial, científica, médico a 2,4GHz.

- 12 no superpuestos canales de infraestructura de la información en 5 GHz frecuencia de banda con y sin CB.

Protocolo de la subcapa Mac 802.11

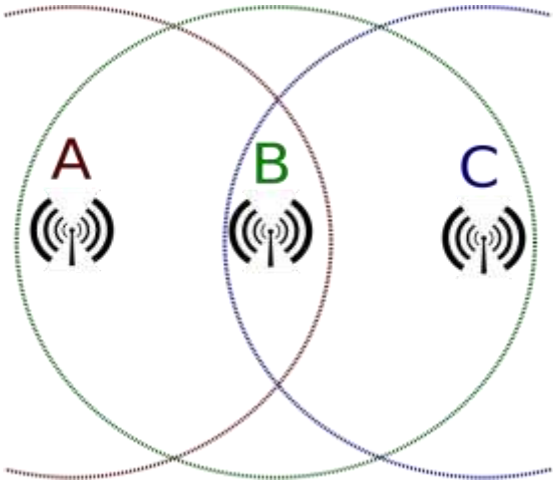
Esta subcapa se encarga de la asignación del canal, direccionamiento de unidades, de datos de protocolo (PDU), formato de tramas, revisión de error, fragmentación y reagrupación. El medio de transmisión puede funcionar en el *modo de contención*, por lo que todas las estaciones deberán competir por el acceso al canal por cada paquete transmitido. También se puede alternar entre el modo de contención (periodo de contención, CP) y el *periodo libre de contención* (CFP). Durante el periodo libre de contención, el uso del medio está controlado por un punto de acceso, por lo que se elimina la necesidad de que las estaciones compitan por el acceso.

Terminal oculta y terminal expuesta

Una diferencia importante entre una red LAN cableada y una inalámbrica, consiste en que, en general, una red WLAN no se puede considerar una topología completamente conectada entre los nodos. Existe un problema conocido como terminal oculta y terminal expuesta. No todas las estaciones están dentro del rango de otra, por lo que las transmisiones en curso en una parte de la celda pueden no ser recibidas en otra parte de la misma celda.

El problema de la terminal oculta puede ser ejemplificado en el esquema siguiente. En este ejemplo, la estación C está transmitiendo a la estación B; si A sondea el canal, no escuchará a nadie y falsamente concluirá que puede empezar a transmitir hacia B, ocasionando una colisión.

Por otro lado, existe el problema inverso, conocido como terminal expuesta; en este caso, B desea enviar hacia C; para poder aplicarlo, B escucha el canal y cuando quiere enviar hacia C, concluye que no puede, porque A está transmitiendo. En este caso, A está transmitiendo hacia otra terminal, por ejemplo D.



Estación oculta.

Fuente:

http://upload.wikimedia.org/wikipedia/commons/thumb/2/2b/Wifi_hidden_station_problem.svg/2000px-Wifi_hidden_station_problem.svg.png

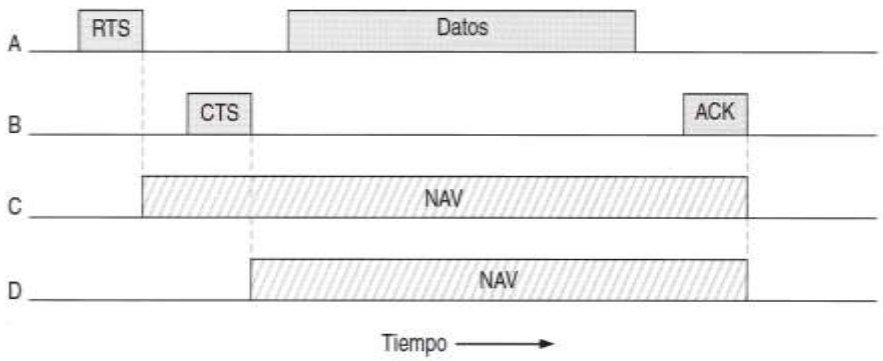
La mayoría de los radios son *half-duplex*, lo que significa que no pueden transmitir y escuchar al mismo tiempo en la misma frecuencia.

Para solucionar estos problemas, el estándar 802.11 soporta 2 modos de funcionamiento:

1. Función de Coordinación Distribuida (DCF, por sus siglas en inglés). No utiliza ningún tipo de control central (similar a Ethernet). Emplea un protocolo llamado CSMA/CA (CSMA con Evasión de Colisiones), el cual emplea dos métodos: la detección del canal físico y la del canal virtual.

En la detección del canal físico, cuando una estación desea transmitir, detecta el canal, si éste está inactivo, comienza a transmitir. No detecta el canal mientras transmite, pero emite tramas completas, las cuales pueden ser destruidas en el receptor debido a interferencia. Si un canal está ocupado, el emisor espera hasta que se encuentre inactivo para comenzar a transmitir. En caso de ocurrir una colisión, las estaciones involucradas esperan una ventana de tiempo aleatorio, y vuelven a intentarlo más tarde.

El otro modo de operación se basa en MACAW y utiliza la detección del canal virtual. Como puede verse en el siguiente esquema.



Detección del canal virtual.
Fuente: Tanenbaum, 203: 297

En este ejemplo, A desea enviar a B; C es una estación que está dentro del alcance de A. D es una estación dentro del alcance de B, pero no dentro de A. El protocolo comienza cuando A decide enviar datos a B; A inicia enviando una trama RTS a B (solicitud). B decide otorgarle permiso y regresa una trama CTS. Al recibir A el permiso, envía su trama y comienza un temporizador ACK. Al recibir correctamente los datos, B responde con otro ACK, con lo que termina el intercambio. Si el temporizador ACK de A termina antes de que el ACK regrese, todo el protocolo se ejecuta de nuevo.

Ahora desde el punto de vista de C y D, C está dentro del alcance de A, por lo que puede recibir la trama RTS; si pasa esto, se da cuenta de que se van a enviar datos, por lo que desiste de transmitir cualquier cosa hasta que el intercambio finalice. A partir de la información proporcionada en la solicitud RTS, C puede estimar cuánto tardará la secuencia (incluyendo el ACK final), por lo que se coloca así mismo como un canal virtual ocupado, indicado por NAV (Vector de Asignación de Red). En este caso, D, no escucha el RTS, pero sí el CTS, por lo que también se coloca en NAV.

Cabe destacar que las señales de tipo NAV no se transmiten, pero son recordatorios para mantenerse en silencio durante el tiempo que dura la transmisión.

Es importante recordar que, en contraste con las redes cableadas, las redes inalámbricas son ruidosas e inestables (hay muchos dispositivos que operan en la misma frecuencia); por ello, la probabilidad de que una trama llegue a su destino es menor conforme aumenta su longitud. Aproximadamente, una de cada nueve tramas se encuentra dañada, por lo que tendrá que ser retransmitida.

Para solucionar este problema, el estándar permite dividir las tramas en fragmentos, cada uno con su propia suma de verificación (*checksum*). Cada fragmento se numera de manera individual y su recepción se confirma empleando un protocolo de parada y espera (el emisor no puede transmitir el siguiente fragmento de la trama hasta que haya recibido la confirmación de recepción de fragmento anterior).

Una vez que se ha adquirido el canal mediante RTS y CTS, se pueden enviar múltiples fragmentos en una fila (ráfaga de fragmentos). La fragmentación incrementa la velocidad real de transporte. El tamaño del fragmento no lo proporciona el estándar, pero es un parámetro que cada celda y la estación base pueden ajustar.

El modo DCF permite enviar una ráfaga de fragmentos completa sin interferencia.

2. Función de Coordinación Puntual (PCF, por sus siglas en inglés). Utiliza la estación base para controlar la actividad en su celda; es decir, que en este mecanismo no hay control central de la celda, y la estación compite por tiempo aire como si fuera Ethernet.

En este caso, la estación base sondea a las demás estaciones y pregunta si hay tramas por enviar. Como el orden de transmisión se controla por completo por la estación base en este modo, no ocurren colisiones. Este mecanismo está diseñado por el estándar para sondeo; pero no la frecuencia o el orden, ni el hecho de que las demás estaciones necesiten un servicio igual.

El mecanismo básico consiste en la estación base difundiendo una trama guía (trama de *beacon*) de manera periódica, la cual contiene parámetros de sistema: secuencias de salto y tiempos de permanencia para FHSS, sincronización de reloj, etc. También invita a las nuevas estaciones al servicio de sondeo.

Una vez que una estación es sondeada a cierta tasa, se le garantiza cierta fracción de ancho de banda y se hace posible proporcionar garantías de calidad en el servicio.

La duración de la batería es un problema latente en los dispositivos inalámbricos móviles. Por lo anterior, el estándar 802.11 permite que una estación base pueda conducir una estación móvil al estado de hibernación hasta que la estación base o un usuario la saquen de ese estado. Sin embargo, entrar en hibernación significa que la estación base tiene la responsabilidad de almacenar el *búfer* de las tramas que vayan dirigidas a la estación móvil que está hibernando hasta que puedan ser colectadas.

PCF y DCF pueden coexistir en una celda ya que el estándar proporciona una forma de lograrlo: definiendo cuidadosamente el intervalo de tiempo entre tramas. Después de enviar una trama, se necesita cierto tiempo muerto antes de que cualquier estación pueda enviar una trama. Para ello, se definen 4 intervalos diferentes con un propósito específico:

1. SIFS (por sus siglas inglesas: Espaciado Corto Entre Tramas). Permite que las distintas partes de un diálogo transmitan. Incluye dejar que: el receptor envíe CTS para responder a una RTS, dejar que el receptor envíe un ACK para un fragmento o una trama con todos los datos y dejar que el emisor de una ráfaga de fragmentos transmita el siguiente fragmento sin tener que enviar una RTS nuevamente. Siempre hay una sola estación que debe responder después de un intervalo SIFS.

2. PIFS (Espaciado Entre Tramas PCF). Si la estación falla al utilizar su oportunidad de transmitir y transcurre una ventana de tiempo PIFS, la estación base podría enviar una trama *beacon* o una trama de sondeo. Esto permite tener una estación base que envía una trama de datos o una secuencia de fragmentos para terminar su trama sin que nadie interfiera, pero da a la estación base la oportunidad de tomar el canal cuando el emisor anterior haya terminado.

3. DIFS (Espaciado Entre Tramas DCF). Si la estación base no tiene nada que decir y transcurre un intervalo de tiempo DIFS, cualquier estación podría intentar usar el canal para enviar una nueva trama. Se aplican las reglas de contención normales y si ocurre una colisión, puede necesitarse el retroceso exponencial binario.

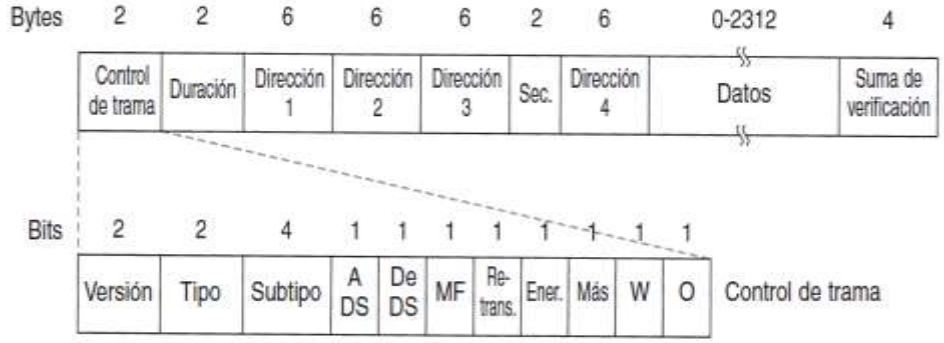
4. EIFS (Espaciado Entre Tramas Extendido). Sólo una estación que acaba de recibir una trama errónea o desconocida utiliza el último intervalo de tiempo, EIFS para reportar la trama errónea. Se da a este evento la menor prioridad porque puede suceder que el receptor no sepa lo que está pasando, entonces debe esperar un intervalo de tiempo extendido para evitar interferir en el dialogo que se lleva a cabo entre 2 estaciones.

Estructura de la trama

El estándar soporta 3 tipos diferentes de tramas: administración, control y datos:

- Administración. Usados para la asociación y disociación de la estación con el punto de acceso, temporización, sincronización, autenticación y des-autenticación.
- Control. Usados para el saludo inicial durante el periodo de contención, para confirmaciones positivas durante el periodo de contención y para terminar el periodo de libre contención.
- Datos. Usados para la transmisión de datos durante el periodo de contención y el periodo de libre contención. Pueden ser combinados con peticiones y confirmaciones durante el periodo de libre contención.

En el siguiente esquema puede verse el formato de la trama para el estándar 802.11.



Formato para la trama

Fuente: Tanenbaum, 2003: 300.

A continuación se menciona una breve descripción de cada uno de los campos contenidos en la trama que se envía:

1. Campo de control de trama contiene la siguiente información:
   - Versión. Permite operar 2 versiones del protocolo al mismo tiempo en la misma celda.
   - Tipo. Identifica la trama: si es de control, administración o datos.
   - Subtipo. Identifica el tipo de trama (RTS, CTS, etc.).
   - A DS. Indica si la trama va hacia el sistema de distribución (DS, por sus siglas en inglés).
   - De DS. Indica si la trama viene del sistema de distribución.
   - MF. Este *bit* indica que se realizarán más fragmentaciones.
   - Retransmisión. Este *bit* indica una retransmisión de la trama que ya había sido enviada.
   - Energía. Este *bit* es usado por la estación base (AP) para poner al receptor a hibernar o para reactivarlo.
   - Más. Este *bit* indica que el transmisor tiene tramas adicionales para el receptor.

- W. Este *bit* especifica que los datos han sido cifrados usando el algoritmo WEP.
- O. Este *bit* le dice al receptor que una secuencia de tramas con este *bit* activado debe ser procesado estrictamente en orden.

2. Duración. Avisa cuanto tiempo el paquete ocupara el canal y su confirmación (ACK), para que otras estaciones actualicen su NAV.
3. Dirección 1. Contiene cuatro direcciones (Dirección 1, Dirección 2, Dirección 3 y Dirección 4), de las cuales 2 son para la dirección del transmisor y el receptor deseado y las otras 2 para los AP fuente y destino para tráfico entre celdas.
4. Secuencia. Permite a los fragmentos ser numerados, de los 16 disponibles, 12 identifican la trama y 4 al fragmento.
5. Datos. Contiene los datos útiles, hasta 2312 *bytes*.
6. Suma de verificación. Revisión de redundancia cíclica de 32 bits (CRC) que se emplea para la detección de errores.

Los campos de administración cuentan con un formato parecido a los paquetes de datos, pero no tienen una dirección AP, ya que los paquetes de administración están restringidos a una celda. Los paquetes de control son más cortos, ya que sólo tienen 1 o 2 direcciones, no tienen campo de datos ni de secuencia. La información clave generalmente está en el campo de subtipo RTS, CTS o ACK.

Servicios

El estándar indica que cada red LAN inalámbrica que desee apegarse a él deberá proporcionar 9 servicios, los cuales se agrupan en categorías: 5 servicios de distribución y 4 servicios de estación.

Los servicios de distribución tienen que ver con la administración de conexión a la celda y la interacción que se da con las estaciones que están fuera de ella. Estos servicios son proporcionados por estaciones base.

Los servicios de estación tienen que ver sólo con lo que sucede dentro de la celda.

Los cinco servicios de distribución son proporcionados por las estaciones base y tienen relación con la movilidad de la estación y su entrada y salida de las celdas.

Los 9 servicios son los siguientes:

1. Asociación. Se emplea por las estaciones móviles para conectarse a las estaciones base (se usa cuando una estación se mueve dentro del alcance de radio de la estación base). Una vez que llega anuncia: tasas de datos soportadas (necesarias para el sondeo) y los requerimientos de administración de energía. La estación base puede aceptar/rechazar la estación móvil. Si se acepta, debe autenticarse.

2. Disociación. La estación o estación base puede romper la relación. Una estación puede estar en servicio antes de apagarse o de salir, pero la estación base también podría usarlo antes de su mantenimiento.

3. Reasociación. Permite cambiar una estación base mediante este servicio. Es útil para estaciones móviles que van de una celda a otra.

4. Distribución. Determina cómo colocar en ruta tramas enviadas a la estación base (puede ser directamente a través del aire o mediante red cableada).

5. Integración. Permite manejar la "traducción" del formato 802.11 a un formato de trama diferente para redes que no emplean el estándar.

Los 4 servicios restantes se llevan a cabo dentro de las celdas:

1. Autenticación. Una estación debe autenticarse antes de que pueda enviar datos. Una vez asociada la estación móvil, se envía una trama especial para verificar la clave secreta y la estación móvil prueba que la conoce mediante la codificación de la trama especial y regresándola a la estación base (en ningún momento se envía la contraseña). Si el resultado es correcto, la estación móvil formará parte de la celda. Es importante destacar que en este punto, en el estándar inicial la estación base no tiene que autenticarse ante la estación móvil, pero actualmente se busca reparar este defecto.

2. Desautenticación. Cuando una estación previamente autenticada abandona la red, es necesario que pase por el proceso de desauntenticarse, ya que después de esto es probable que no utilice la red.

3. Privacidad. Para mantener la confidencialidad a través del uso de la red LAN inalámbrica, es necesario codificar la información. Se debe manejar la codificación y la decodificación. El algoritmo empleado es RC4 (con una clave secreta de 40 o 104 *bits*).

4. Entrega de datos. Es importante recordar que 802.11 está basado en Ethernet, por lo que no se garantiza que la transmisión sea 100% confiable. Las capas superiores deben revisar y corregir los errores.

Es importante recordar que una celda en el estándar 802.11 tiene parámetros que pueden revisarse y ajustarse, por ejemplo: la codificación, intervalos de expiración de temporizador, tasas de datos, frecuencia de la trama de *beacon*, entre otros.

4.2. Protocolos WEP, WAP

Es importante proteger la seguridad de la información que se transmite mediante paquetes, los cuales se envían empleando redes LAN inalámbricas, ya que es uno de los aspectos más importantes dentro de las organizaciones.

Por lo anterior, el estándar 802.11 cuenta con algunos protocolos de seguridad que permiten establecer un canal de comunicación seguro entre los equipos que se encuentran conectados a la red inalámbrica.

Al habilitar seguridad dentro del estándar 802.11, cada estación cuenta con una clave secreta que comparte con la estación base y la forma en que se distribuyen las claves no está especificado por el estándar y sólo pueden ser precargadas por el fabricante.

Las claves pueden proporcionarse mediante una red cableada y la estación base o el equipo del usuario puede tomar una clave aleatoria y enviarla al otro mediante la red inalámbrica en un mensaje cifrado por medio del uso de la clave pública del

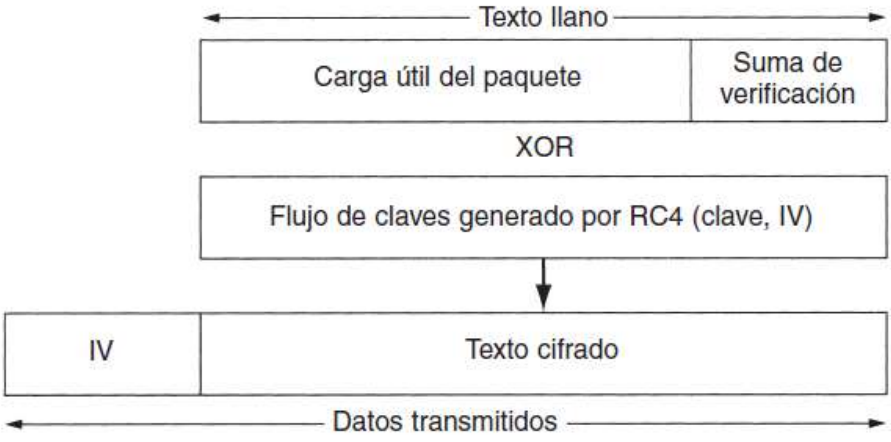
otro. Una vez establecidas, las claves, pueden permanecer estables por meses o años.

Protocolo WEP

Según Tanenbaum:

El estándar 802.11 establece un protocolo de seguridad en el nivel de capa de enlace de datos llamado WEP (Privacidad Inalámbrica Equivalente), diseñado para que la seguridad de una LAN inalámbrica sea tan buena como la de una LAN cableada. Puesto que lo predeterminado para las LAN alámbricas no es la seguridad, este objetivo es fácil de alcanzar, y WEP lo consigue (2003: 781).

El cifrado mediante el protocolo WEP emplea un cifrado en el flujo de datos mediante el algoritmo RC4. En WEP, el cifrado RC4 genera un flujo de claves a las cuales se aplica un XOR al texto en claro para obtener como resultado el texto cifrado.



Cifrado de paquetes mediante WEP

Fuente: Tanenbaum, 2003: 782.

El proceso detallado es el siguiente: primero, se realiza una suma de verificación de la carga útil mediante el uso de CRC-32 polinomial (Verificación de Redundancia Ciclica) y la suma de verificación se agrega a la carga útil para formar el texto plano para el algorítmo de cifrado. Posteriormente, al texto en claro se le aplica un XOR con un fragmento de flujo de claves de su mismo tamaño, lo que da como resultado el texto cifrado. El IV que se usó para iniciar el RC4 se envía junto con el texto cifrado. Cuando el paquete llega al destinatario, se extrae la carga útil, se genera el flujo de claves a partir de la clave secreta compartida y el IV que se acaba de recibir y finalmente, se aplica otro XOR para recuperar el texto en claro. Posteriormente, se puede revisar la suma de verificación para saber si el paquete ha sido modificado.

Es importante destacar que el protocolo WEP no fue diseñado por expertos en seguridad o criptografía, por lo que ha sido vulnerado. Por ejemplo, algunas de las *suites* existentes para auditoría de seguridad (dirigido a redes, servidores y aplicaciones) como *Kali* o *BackTrack*, cuentan con herramientas que permiten fácilmente encontrar la clave mediante la inyección de paquetes en la comunicación que se realiza entre 2 equipos de manera inalámbrica. Por lo anterior, ha sido necesario establecer mecanismos más robustos para implementar seguridad al nivel de la capa de enlace de datos.

A partir de lo anterior, el protocolo WEP sólo se recomienda para redes de tipo casero o bien para aplicaciones no críticas.

Protocolo WPA

WPA son las siglas de *Wi-Fi Protected Access* (Acceso Protegido a Wi-Fi). Este protocolo ha sido promovido por el WiFi Alliance y la IEEE y es una solución temporal que implementa la mayor parte del estándar 802.11i (el cual es un agregado al estándar original 802.11 como un apartado de seguridad) y que adicionalmente no requiere actualización de los equipos que están implementando el estándar 802.11.

Es importante destacar que WPA se propone como una medida emergente ante la ruptura del protocolo WEP.

WPA emplea el cifrado conocido como TKIP (*Temporal Key Integrity Protocol*), el cual proporciona soporte para los equipos WLAN al direccionar los flujos de datos originalmente empleados con el método de cifrado de WEP. WPA hace uso de WEP, pero cifra el *payload* de la capa 2 mediante TKIP y lleva a cabo la verificación de integridad del mensaje (MIC) en el paquete cifrado para asegurar que el mensaje no ha sido interceptado.

La llave de cifrado se intercambia inmediatamente después de que el dispositivo se ha conectado con la celda. Durante la fase de autenticación, el dispositivo cliente y la celda intercambian valores aleatorios que son empleados en combinación con una contraseña conocida por ambas partes para autenticarse mutuamente y generar llaves de cifrado en ambos puntos. Como sólo hay una contraseña que es usada en todos los dispositivos que se conectan a la celda, las claves que son generadas durante este procedimiento son únicas en cada conexión. Esto significa que los dispositivos no están capacitados para decodificar paquetes

que están destinados a otros dispositivos, a pesar de contar con la misma contraseña.

Hoy, no hay ataques conocidos que pueden romper la autenticación WPA, esto es gracias al cifrado en uso, pues la contraseña cuenta con la longitud suficiente y no puede ser rota con ataques de diccionario.

La siguiente versión del protocolo, conocido como WPA2 (Wireless Protected Access 2) implementa de manera completa el estándar 802.11i y es una versión más actualizada del protocolo, el cual cuenta con un algoritmo de autenticación y cifrado que conforma una mejora al estándar IEEE 802.11i ya que emplea AES (*Advanced Encryption Standard*) para cifrar el flujo de datos.

Muchos puntos de acceso pueden ser configurados para emplear ambos protocolos, tanto WPA como WPA2, o bien sólo WPA2. Para informar a los dispositivos, que desean conectarse a la celda, cuál método de autenticación y cifrado se deberá usar, un número de nuevos elementos informativos son agregados en las tramas *beacon*.

La única vulnerabilidad para el modo personal de WPA y WPA2 consiste en que todos los dispositivos utilizan la misma contraseña. Para redes caseras, esto es usualmente aceptable y también una solución práctica ya que sólo un número limitado de dispositivos y personas conocidas emplean la red.

Para entornos Wi-Fi en empresas, emplear una única contraseña es un riesgo de seguridad, ya que resulta mucho más difícil mantenerla segura. En estos casos, WPA y WPA2 cuentan con un modo empresarial que emplea un servidor de autenticación independiente que no está incluido en los puntos de acceso. Esto es necesario, ya que las compañías a menudo emplean diversos puntos de acceso a

la red inalámbrica, lo que necesita el almacenamiento de la información de autenticación en una ubicación centralizada.

Para autenticar a los dispositivos y ser capaz de negar el acceso a la red a un usuario, es necesario instalar certificados individuales en cada dispositivo. La parte pública del certificado también se almacena en el servidor de autenticación. Cuando un dispositivo se asocia a un punto de acceso, la autenticación se inicia por el punto de acceso como si estuviera en el modo normal. En lugar de verificar las credenciales por sí mismo como siempre, transparentemente reenvía las tramas de autenticación al servidor de autenticación en la red.

Existen diversos protocolos para este propósito y uno que se emplea para certificar WPA y WPA2 es EAP-TLS (*Extensible Authentication Protocol - Transport Layer Security*). El acceso completo a la red sólo se proporciona al dispositivo cliente cuando el servidor de autenticación autoriza hacerlo al punto de acceso y una vez que se han proporcionado las llaves para ejecutar el cifrado del tráfico de red.

A continuación se muestra una tabla resumen sobre las propiedades de cada uno de los protocolos antes mencionados:

	WEP	**WPA**	**802.11i/WPA2**
Método de autenticación	Llave previamente compartida	PSK o 802.1x	PSK o 802.1x
Cifrado	RC4	TKIP	AES
Integridad del mensaje	CRC-32	MIC	CCMP
Seguridad	Baja	Fuerte	Muy fuerte

Tabla 2. Comparativa entre protocolos.

Fuente: Switched Networks Companion Guide, Video Enhanced Edition.

4.3. Dispositivos inalámbricos

Para interconectar un dispositivo a una red LAN inalámbrica, es necesario que sea compatible con la norma 802.11. Para ello, existen una serie de características que deben reunirse.

Todos los tipos de redes dentro del estándar 802.11 tienen 2 componentes básicos:

- Un punto de acceso inalámbrico (usualmente es un *router*)
- Tarjetas de red inalámbricas.

Tarjeta de red inalámbrica

Network Interface Card (NIC). Es un periférico que permite interconectar 2 o más dispositivos y posibilita compartir recursos, en este caso, dentro de una red LAN inalámbrica.

Cada tarjeta de red cuenta con un número de identificación de 48 *bits* en formato hexadecimal, esta dirección es conocida como MAC (Control de Acceso al Medio). Las direcciones son asignadas por la IEEE, los tres primeros octetos identifican al proveedor y se conocen como número OUI (*Organizationally Unique Identifier*) que en conjunto con los otros 24 *bits* conforman la dirección MAC.
Las tarjetas se pueden adaptar a distintas normas del estándar 802.11; sin embargo, la tarjeta tipo RJ-45 cuenta con un uso extendido. La tarjeta varía con respecto a la velocidad de transmisión, las velocidades especificadas por los fabricantes son teóricas y tienen un rendimiento menor del indicado.

Punto de acceso

Un punto de acceso (*Access Point*) es un dispositivo del tamaño de una agenda que emplea uno o más puertos 8P8C (entrada para el cable con terminal RJ45) que se conecta a una red Ethernet 10BASE-T o, bien, si se desea, a una 10/100/1000.

Contiene un transmisor/receptor, cifrado y *software* para establecer la comunicación. El punto de acceso convierte señales convencionales de Ethernet en señales de Ethernet inalámbricas que son transmitidas en NIC inalámbricos en la red y realiza el mismo rol en sentido inverso para transferir señales provenientes de tarjetas de red inalámbricas a redes Ethernet convencionales.

En muchos casos, no se adquiere un punto de acceso como un elemento aislado, sino que se adquiere un *router* que también funciona como punto de acceso.

Los *routers* normalmente incluyen un *router*, *switch* y punto de acceso inalámbrico, pero muchos también pueden incluir un modem, cable/DSL y otras características.

Por defecto, los dispositivos Wi-Fi operan en un modo conocido como punto de acceso céntrico. Esto significa que los dispositivos del cliente sólo se comunican con el punto de acceso, incluso si quieren intercambiar datos con otro. Esto funciona bien para muchas aplicaciones, ya que la mayoría de los datos se intercambian entre un dispositivo inalámbrico y un servidor en internet.

Como cada vez se conecta una mayor cantidad de dispositivos en casa u oficina, esto se convierte en un problema, ya que los datos que se envían desde una TV o una computadora necesitan atravesar el aire 2 veces si ambos están conectados de forma inalámbrica. Entonces, el ancho de banda disponible se divide a la mitad, este modo no es ampliamente empleado en la práctica, ya que la mayoría de las redes caseras y de oficina requieren puntos de acceso para conectarse mediante redes locales hacia internet.

Para mejorar esta situación, cuando 2 dispositivos se comunican inalámbricamente con otro, el estándar 802.11e introduce el Protocolo de Enlace Directo (DLP, *Direct Link Protocol*) para patrocinar que se comuniquen directamente entre ellos. Una sesión DLP se inicia por los 2 dispositivos intercambiando tramas DLP mediante el punto de acceso a la red. Entonces, ambos dispositivos son capaces de emplear DLP y comenzar a comunicarse directamente una vez que la negociación DLP es exitosa. Sin embargo, en la práctica, actualmente muy pocos dispositivos soportan DLP.

RESUMEN

En esta unidad se consideró la aplicación de redes inalámbricas, así como las ventajas y desventajas que presentan. También se presentó el estándar 802.11, la capa física de operación y la familia de protocolos y métodos empleados que operan con él. Es importante notar que cada uno de ellos cuenta con un uso distinto; sin embargo, el más popular es el conocido como Wi-Fi. Adicionalmente, se revisaron los servicios empleados para la ejecución del estándar.

También se revisó el estándar existente para la implementación de redes LAN inalámbricas, así como los principales métodos de cifrado existentes hoy para proteger el tráfico en este tipo de redes.

Finalmente, se proporcionó información sobre los dispositivos físicos que se emplean para la culminación de redes LAN inalámbricas.

BIBLIOGRAFÍA

SUGERIDA

Autor	Capítulo	Páginas
Tanenbaum	4	292-302
Tanenbaum	8	781-783

Tanenbaum, Andrew (2003). *Redes de computadoras* (4ª. Ed.). México: Pearson Educación, 912 pp.

Facultad de Contaduría y Administración
Sistema Universidad Abierta y Educación a Distancia