UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CONTADURÍA Y ADMINISTRACIÓN

AUTOR: CARLOS ALBERTO VICENTE ALTAMIRANO

TELECOMUNICACIONES II		Clave: 1567
Plan: 2005		Créditos: 8
Licenciatura: Informática		Semestre: 5°
Área: Informática (Redes y Telecomunicaciones)		Asesoría: 4 h
Requisitos: Ninguno		Por semana: 4 h
Tipo de asignatura:	Obligatoria (X)	Optativa ( )

Objetivo general de la asignatura

Al finalizar el curso, el alumno conocerá los tipos de diseño y formas de operación de redes globales de gran tamaño así como los métodos que permiten garantizar la seguridad e integridad de los datos que viajan en éstas.

Temario oficial (64 horas sugeridas)

1. Interconectividad 16 h
2. Interoperabilidad en redes 14 h
3. Integridad 16 h
4. Seguridad 18 h

Introducción

Hablar de Internet en estos días es algo cotidiano. Es algo que casi todas las personas saben de qué se trata. Muchas empresas han entendido que es un medio por el cual pueden llegar a muchos clientes, lo mismo las personas comunes han entendido que se pueden comunicar con amigos y familiares a kilómetros de distancia con tan solo un clic.

Esta comunicación inmediata está apoyada por infraestructura tecnológica que permite el envío masivo de información a través de grandes distancias. Estos dispositivos de red son manejados por las grandes corporaciones tecnológicas, por universidades grandes. En una escala más pequeña cada empresa cuenta con su propia infraestructura y con personal capacitado para manejarla.

Con este material se podrán conocer los elementos que conforman esa infraestructura, las diferentes clases de equipos que existen, así como sus funciones en cada aspecto de una red de datos.

TEMA 1. INTERCONECTIVIDAD

Objetivo particular

El alumno reconocerá los dispositivos de interconexión en una red y su evolución a lo largo de la historia de las redes de cómputo.

Temario detallado

1.1 NIC (tarjeta de red)
1.2 Tranceiver
1.3 Repetidor
1.4 Concentrador
1.5 Puente
1.6 Gateway
1.7 Ruteador
1.8 Switch
1.9 Híbridos

Introducción

Durante el proceso de comunicación en una red de cómputo, los equipos de interconexión juegan un papel muy importante. Son los elementos de la red que permiten que los usuarios finales puedan tener acceso a los recursos de su interés.

Cuando un usuario final desea conectarse a un sitio en Internet es necesario que la información pase por diferentes dispositivos de interconexión que cumplen con una función específica dentro de todo el proceso de comunicación. De estos dispositivos, de sus características principales y de sus funciones se hablará a continuación.

1.1 NIC (tarjeta de red)

La tarjeta de red es un dispositivo que generalmente viene incluida en los equipos terminales de uso personal. Se utiliza para interconectar un equipo de escritorio, laptop, netbook a la red local o la red de Internet a través de un medio físico o inalámbrico. Las velocidades han ido evolucionando y ya hay tarjetas de red que alcanzan 1 Gb/s. Pero no siempre fue así, las primeras tarjetas de red solamente alcanzaban velocidades de 2.94 Mbs utilizando cable coaxial y teniendo Ethernet como tecnología de transporte, la cual sigue usándose en la actualidad.

Es interesante que las primeras tarjetas de red vinieran de la mano con la tecnología Ethernet, actual estándar de interconexión entre dispositivos, después surgieron otras tecnologías como token ring o fddi que alcanzaban velocidades de 4 y 16 Mbps pero la popularidad de Ethernet hizo que aquellas cayeran en desuso.

Para que una tarjeta de red funcione correctamente en un sistema operativo es necesario que se tenga un programa controlador también conocido como *driver* el cual permite que la computadora interactúe adecuadamente con la tarjeta de red. Es común que los sistemas operativos ya tengan incorporados un número muy grande de controladores debido a la amplia gama de tarjetas de red que existe en el mercado.

Actualmente existen marca líderes en la fabricación de tarjetas de red como: 3Com, Intel y Broadcom quienes desarrollan controladores para los más populares sistemas operativos incluyendo los llamados *open source*, que son sistemas operativos basados en código libre y se han ido popularizando cada vez más como Fedora, Debian, Ubuntu entre otros. La actualización de las tarjetas de red ha ido de la mano del desarrollo y evolución del estándar Ethernet, ya que ha pasado de utilizar cable coaxial a cable UTP, incluso se puede llegar ver tarjetas de red con conectores en fibra óptica, las cuales no son muy comunes por su costo.

Una tarjeta de red dañada puede provocar serios problemas en una red local ya que puede llenar de errores el medio de transmisión, lo cual repercute en el desempeño del mismo. Para poder detectar este tipo de anomalías es necesario contar con un analizador de protocolos que permita ver el tráfico que circula por la red.

Basándose en el modelo de referencia OSI, las tarjetas de red trabajan en la capa física y en la capa de enlace de datos. Mediante el controlador instalado en el sistema operativo es posible realizar algunas tareas de diagnóstico que permiten determinar puntos de falla.

1.2 Transceiver

El *transceiver* es un dispositivo que a diferencia de la tarjeta de red no va insertado en una computadora personal ni en otro dispositivo de red sino que es un dispositivo *standalone,* es decir, que funciona de manera autónoma y su función es permitir el cambio de un medio de transmisión a otro. Son conocidos como convertidores de medio o *media converters* en inglés.

Es común que una red tenga que usar este tipo de dispositivos para poder adaptar otros dispositivos a la red local. Por ejemplo, una red que cuenta con conexiones en fibra óptica necesitará un *transceiver* para interconectar una antena inalámbrica que solamente puede ser conectada mediante cable UTP.

Los problemas más comunes en estos dispositivos son los bloqueos que experimentan ante sobrecargas de calor o frente intensas ráfagas de tráfico. Al tener poca capacidad de procesamiento son muy propensos a este tipo de problemas. Para minimizar un poco este riesgo existen *transceivers* que soportan los llamados *jumbo-frames* o paquetes de datos muy grandes que algunas aplicaciones requieren. El estándar Ethernet especifica un tamaño de 1500 bytes,

los jumbo-frames pueden alcanzar longitudes de hasta 9000 bytes.

1.3 Repetidor

El repetidor es un dispositivo que opera en la capa física del modelo OSI y tiene la funcionalidad de extender la longitud de una red mediante la repetición de la señal. Como se sabe, el estándar Ethernet especifica la distancia máxima para que una señal no presente degradación, si se requiere interconectar dispositivos a una distancia mayor entonces es necesario un repetidor o *extender.* Por ejemplo, la tecnología FasEthernet especifica cien metros cuando se utiliza cable de cobre (UTP) y hasta 412 metros si se utiliza fibra óptica.

El problema con los repetidores es que si la señal de origen presenta ruido, este dispositivo también amplifica la señal con ruido, no siendo capaz de detenerlo.

Se recomienda utilizar los repetidores únicamente para extender el medio físico pero no para extender lógicamente una red porque al mismo tiempo se extiende el dominio de colisiones. Es decir, un repetidor traerá menos problemas si se coloca en un enlace que es interconectado por dos ruteadores en los extremos y el repetidor únicamente se utilizó por razones de distancia. El estándar IEEE 802.3 especifica un máximo de cuatro repetidores en una red local.

1.4 Concentrador

El concentrador es un repetidor multipuertos, es decir que regenera la señal de un puerto a otro indiscriminadamente. Por lo tanto también es un dispositivo que trabaja en la capa 1 del modelo OSI. Los concentradores fueron el inicio de lo que hoy se conoce como *switches* ya que era importante poder agrupar un conjunto de computadoras personales en una misma área geográfica, como una oficina.

El estándar Ethernet se comporta como un medio compartido, esto es, que un paquete transmitido por una terminal es conocido por todos los que están en la red. Este tipo de medios es propenso a *broadcast* y a *colisiones.* Con un concentrador este comportamiento se multiplica porque son muchas computadoras intentando hacer uso del medio de transmisión. Si se aumenta el número de concentradores en una misma red el problema se multiplica y la red se vuelve lenta.

1.5 Puente

El también conocido como *bridge* 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 con base en direcciones físicas o MAC. Paquetes que van dentro del mismo segmento son analizados y son 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 crece la red se vuelve susceptible a los llamados “loops” debido a que la integridad de sus tablas de información tiene información duplicada. Un *loop* es un fenómeno en el que los paquetes de datos circulan por la red de un lado a otro sin encontrar su destino, lo que provoca irregularidades en la red.

Para controlar estos comportamientos se definió un estándar llamado *Spanning Tree* (IEEE 802.1d) que consiste en bloquear los enlaces redundantes mientras un enlace se encuentra activo para comunicarse con los demás dispositivos.

1.6 Gateway

El gateway es un nombre genérico que se le aplica a aquellos dispositivos que son capaces de hacer interoperar redes basadas en protocolos y tecnologías de acceso diferentes. Actualmente el estándar de interconexión es Ethernet usando TCP/IP. Pero para enlaces de tipo WAN se utiliza otro tipo de tecnologías como HDLC o PPP, para ello se requiere de equipos especiales que hagan convivir ambas tecnologías. Hace unos años, además de redes TCP/IP existían protocolos como IPX o AppleTalk y era mediante un gateway que se podía hacer que interactuaran.

Ahora los dispositivos que tienen estas capacidades son los switches y los ruteadores.

1.7 Ruteador

Es un dispositivo que opera en la capa tres del modelo OSI, que al igual que un *bridge* es capaz de segmentar dominios de colisiones y adicionalmente separar dominios de *broadcast*. Este dispositivo crea una tabla de rutas origen y destino para poder mover los paquetes de información. Cada puerto de un ruteador es un segmento de colisiones y *broadcast* separados de los demás, cada puerto es una red diferente a los demás con su propio direccionamiento y sus propias reglas de uso.

El ruteador es un equipo más complejo que requiere de software más complejo ya que es capaz de crear tablas de ruteo estáticas y dinámicas mediante la operación de protocolos de ruteo. Los ruteadores de dimensiones pequeñas tienen pocos

puertos, generalmente tienen uno o dos puertos LAN para la red local y uno o dos puertos seriales para la red WAN. Ruteadores de mayor capacidad se componen de módulos donde pueden convivir puertos de interconexión de diferentes tecnologías.

Un ruteador necesita ser configurado por un administrador de red. Su configuración más básica es definir el segmento de red a la cual van a pertenecer todas las computadoras que formarán parte de esa red, esto es necesario para que la red en su conjunto pueda tener comunicación con otras redes.

Los ruteadores son de diferentes capacidades, los hay con interfaces o puertos fijos que vienen con un número de puertos predefinidos y estos no pueden ser escalables. Los hay modulares los cuales se pueden escalar al gusto del administrador usando tarjetas que van insertadas en los módulos.

Actualmente los ruteadores son dispositivos muy importantes en la infraestructura de una red, son elementos que son vigilados continuamente por un grupo de expertos cuando se trata de redes grandes debido a que si uno falla una buena parte de la red está en riesgo de no funcionar. De los ruteadores depende, en buena medida, la funcionalidad de una red y por eso su importancia.

1.8 Switch

El switch es un dispositivo con las mismas funciones que un *bridge* pero con múltiples puertos aunque los *switches* hoy en día únicamente funcionan con una sola tecnología como Ethernet. Al igual que un concentrador sirve para poder agrupar en un mismo equipo a muchas estaciones de trabajo que conforman una misma red pero con la diferencia de que no retransmite la señal indiscriminadamente como los concentradores. Esto es muy importante porque se previenen las colisiones y la eficiencia de la red aumenta considerablemente.

Cada puerto de switch es capaz de contener las colisiones en sí mismo aunque sigue propagando el *broadcast* ya que todos los puertos forman parte de la misma red lógica Diferente de un ruteador que es un dispositivo que sí contiene el *broadcast* ya que cada uno de sus puertos pertenece a redes lógicas diferentes.

Un switch cuenta con una tabla que relaciona direcciones IP con direcciones MAC para determinar a qué puerto del switch debe enviar la información, de esta manera evita que todos los dispositivos reciban la información reduciendo considerablemente el *broadcast* como sucedía en los concentradores. Por esto se le considera un dispositivo que opera en la capa 2 del modelo OSI.

Los *switches* tienen la característica llamada *full-duplex* que permite el envío y recepción de toda su capacidad de transmisión sin que se produzcan colisiones. Esto también va de la mano del volumen de información que el dispositivo tiene la capacidad de transmitir, a esta característica se le conoce como *throughput*.

Los *switches* han ido evolucionando en los servicios que ofrecen. Actualmente existen modelos que hasta pueden realizar funciones de capa 3 como un ruteador, es decir, soportan capacidades de ruteo de protocolos.

1.9 Híbridos

Actualmente existen dispositivos que pueden combinar las funciones de diferentes dispositivos. Se puede encontrar un switch con funciones de ruteo, un ruteador con módulos de switch entre otros. Por ejemplo, un ruteador actualmente posee la capacidad de realizar también funciones de firewall, de concentrador de VPN entre otros. Va a depender del diseño de la red para determinar si es mejor un solo dispositivo que realice todas las funciones con el riesgo de tener un solo punto de falla o distribuir las funciones entre diferentes dispositivos lo cual impacta en el costo de la red.

Bibliografía del tema 1

Doherty, J. & Anderson, N. (2007*). Cisco Networking Simplified*, 2nd ed., Indianápolis, Indiana, Cisco Press.

Nader, F. Mir. (2006). *Computer and Communication Networks*. Upper Saddle River, NJ, Prentice Hall

Actividades de aprendizaje

A.1.1 Selecciona equipo de interconexión

El alumno accederá al sitio web http://www.cisco.com/en/US/products/index.html y deberá realizar lo siguiente:

a) Elige un switch que cumpla con las siguientes características:

- Capacidad para 48 Puertos LAN FastEthernet
- Capacidad para 2 interfaces GigabitEthernet
- Capacidad de ruteo ospf
- Capacidad de crear VLAN

b) Para finalizar deberás entregar los datos del switch elegido, así como la URL donde se encuentra la información del dispositivo.

A.1.2 Lectura de artículo

a) El alumno leerá el siguiente artículo http://www.cisco.com/web/ES/solutions/smb/products/routers_switches/routing_switching_primer.html

b) Deberás entregar un resumen con las diferencias entre un switch y un ruteador.

A.1.3 Descripción de equipo de ruteo

El alumno leerá las siguientes características de un equipo de ruteo:
http://www.juniper.net/us/en/products-services/routing/m-series/m320/

Entregarás un reporte con todas las características del dispositivo de acuerdo con los siguientes puntos.

1. Indicar el *Throguput* del dispositivo en Full-duplex
2. Indicar la cantidad de Módulos y submódulos (PIC) que soporta
3. Listar todos los tipos de interfaces que soportan en los módulos
4. Indicar el modelo del ruteador.
5. Indicar los protocolos de ruteo que soporta
6. Menciona dos características de seguridad que soporta.

Cuestionario de autoevaluación

1. ¿Para qué se utiliza una tarjeta de red?
2. ¿Cuál es la diferencia entre una tarjeta de red y un *transceiver*?
3. ¿Para qué se utiliza un *transceiver*?
4. ¿En qué capa del modelo OSI opera un repetidor?
5. ¿Cuál es el problema con los repetidores?
6. ¿Qué función tiene un *bridge*?
7. ¿En qué se basa un ruteador para mover los paquetes de información?
8. ¿Qué problemas importantes previene un *switch*?
9. ¿Por qué son importantes los ruteadores?
10. ¿Qué tecnología se ocupa para evitar “*loops*”?

Examen de autoevaluación

Selecciona la respuesta correcta

I. Lee cada enunciado y elige la letra F si el enunciado es falso y una V si el enunciado es verdadero.

1.	La tarjeta de Red es un dispositivo que generalmente viene incluida en los equipos terminales de uso personal.	V	F
2.	Una red que cuenta con conexiones en fibra óptica necesitará un *transceiver* para interconectar una antena inalámbrica que solamente puede ser conectada mediante cable UTP.	V	F
3.	Un concentrador regenera la señal indiscriminadamente	V	F
4.	Cuando se usa concentradores el *broadcast* y las colisiones disminuyen.	V	F
5.	Los *bridge* son dispositivos que impide la interconexión de dos segmentos de red de similar o de diferente tecnología.	V	F

II. Elige la opción que conteste correctamente cada enunciado.

1. Este dispositivo sirve extender la longitud de la red.
    a) Ruteador
    b) Switch
    c) Repetidor
    d) Bridge

2. Dispositivo que disminuye las colisiones
    a) Ruteador
    b) Switch
    c) Repetidor
    d) Bridge

3. Dispositivo que opera en la capa 3 del modelo OSI

a) Ruteador

b) Switch

c) Repetidor

d) Bridge

4. Dispositivo que genera tablas estáticas o dinámicas para tomar decisiones.

a) Ruteador

b) Switch

c) Repetidor

d) Bridge

5. Dispositivo que cuenta con una tabla de direcciones IP con direcciones MAC

a) Tarjeta de red

b) Switch

c) Repetidor

d) Concentrador

TEMA 2. INTEROPERABILIDAD EN REDES

Objetivo particular

El alumno identificará los tipos de redes existentes, los dispositivos que las conforman, así como las diferentes tecnologías que existen para su funcionamiento.

Temario detallado

2.1 Interconexión
- 2.1.1 Redes LAN
- 2.1.2 Redes MAN
- 2.1.3 Redes WAN
- 2.1.4 Conexiones Remotas

2.2 Dispositivos de Interconexión
- 2.2.1 Ruteadores
  - 2.2.1.1 Métodos de Ruteo
    - 2.2.1.1.1 Por saltos mínimos
    - 2.2.1.1.2 Por tipo de servicio
    - 2.2.1.1.3 Ruteo Directo
    - 2.2.1.1.4 Ruteo Indirecto
  - 2.2.1.2 Protocolos
    - 2.2.1.2.1 RIP
    - 2.2.1.2.2 IGRP/EIGRP
    - 2.2.1.2.3 OSPF
    - 2.2.1.2.4 BGP
- 2.2.2. Protocolos Ruteables
  - 2.2.2.1 IP
  - 2.2.2.2 IPX
  - 2.2.2.3 AppleTalk

Introducción

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

Las tecnologías que se emplean en una red son fundamentales para su funcionamiento. Se ha desarrollado para que la información pueda ser comunicada de un lugar a otro de manera segura, confiable y de tal manera 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 aquéllos tiempos no lo soportaría. 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 posible que personas no autorizadas tengan acceso a información que no deberían.

2.1 Interconexión

2.1.1 Redes LAN

Se les llama redes LAN 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.

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 ya que entre más velocidad el costo incrementa.

Otra característica de una red LAN es la forma en que 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.

2.1.2 Redes MAN

Las Redes de Área Metropolitana 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 a través de 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 155Mbps. 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 ó 1 Gbps pero su costo sigue siendo elevado.

Este tipo de redes requieren de una mayor inversión en tecnología y en su caso se puede necesitar la contratación de un Proveedor de Servicios de Internet (ISP).

2.1.3 Redes WAN

Las redes de área amplia o redes WAN son redes que están interconectadas de una ciudad a otra o incluso con otros países. 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 saldría 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.

2.1.4 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 presente 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 que 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) son áreas de trabajo

especializados en vigilar los incidentes de red y dar respuesta para corregir algún problema. El personal especializado de estos centros cuentan con herramientas para poder conectarse a los dispositivos de red de manera remota para 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.

2.2 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 usuarios 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 cumplen con una función específica dentro de todo el proceso de comunicación.

2.2.1 Ruteadores

Como ya se había indicado los ruteadores son dispositivos que deciden la mejor ruta para llegar 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.

2.2.1.1 Métodos de ruteo

2.2.1.1.1 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.

2.2.1.1.2 Por tipo 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 es un tipo de tráfico que deja de funcionar si hay retransmisiones de por medio.

2.2.1.1.3 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.

2.2.1.1.4 Ruteo Indirecto

A diferencia del ruteo directo aquí se utiliza de 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.

2.2.1.2 Protocolos

Los protocolos de ruteo son procedimientos que cada ruteador utiliza para intercambiar información útil para alcanzar a un destino. Se utilizan cuando las redes son grandes y complejas y requieren de decisiones automatizadas. Se

utilizan cuando la cantidad de destinos dentro de una o varias redes es tan grande que se vuelve inmanejable para un administrador de red que haría manualmente esa programación de destinos.

2.2.1.1.1 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.

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.

2.2.1.1.2 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 introduce 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.

2.2.1.1.3 OSFP

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 y conoce perfectamente 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.

2.2.1.1.4 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, una empresa con miles de equipos de cómputo, siempre es recomendable contar con un sistema autónomo para una mejor gestión.

2.2.2 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.

2.2.2.1 IP

El *Internet Protocol* es el 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 pero 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 traten de enviarle un paquete de datos de información. El ruteador se encargará de llevar ese paquete a su destino.

2.2.2.2 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.

2.2.2.3 AppleTalk

Apple también desarrolló un protocolo para la comunicación entre redes pero de la misma forma que IPX ya ha quedado obsoleto 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.

2.2.3. 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 son 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 crece, la red se vuelve susceptible a los llamados "loops" debido a que la integridad de sus tablas de información tiene información duplicada. Un *loop* es un fenómeno en el que los paquetes de datos circulan por la Red de un lado a otro sin encontrar su destino lo que provoca irregularidades en la Red.

2.2.4 Switches

2.2.4.1. 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*, este verificará su tabla de direcciones MAC y si se encuentra la dirección MAC destino es enviado solo y únicamente al puerto asociado (en la tabla), si no lo conoce envía a todos los puertos, menos al del emisor (broadcast).

Resuelve problemas de rendimiento, de congestión y puede agregar mayor ancho de banda. Acelera la salida de tramas. Reduce tiempo de espera. Opera generalmente en la capa 2 del modelo OSI. Reenvía las tramas con base en la dirección MAC.

2.2.4.2 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.

2.2.4.3. Virtual LAN (VLAN)

Una red virtual o VLAN 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.

2.3. Servicios de Voz y Video

Los servicios de voz y video se vuelven cada día más comunes. Hoy en día las principales empresas telefónicas ofrecen servicios telefónicos 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 a través de una conexión a Internet. Con el crecimiento de los teléfonos celulares conectados a Internet, los servicios de telefonía encuentran un nicho de negocio muy importante en esas plataformas.

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 por unos que se puedan conectar 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 vería interrumpida y eso resta calidad a un servicio. Por ello, durante el diseño de una red de datos pensada con servicios de voz se debe tener en cuenta tales requerimientos.

Lo mismo pasa con el video, no es muy cómodo estar viendo un video que se esté cortando a cada rato. Las videoconferencias también son aplicaciones que no permiten los retardos porque de la misma forma que 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.

Bibliografía del tema 2

Brent, Stewart (2010*). CCNP TSHOOT 642-832 Quick Reference*. Indianápolis, Cisco Press

Davidson, J. (2006*). Voice over IP Fundamentals*, Second Edition. Indianápolis, Cisco Press

Stevens, R. (1993). *TCP/IP Illustrated*, Volume 1: The Protocols. Upper Saddle River, NJ, Addison-Wesley Professional

Tanenbaum, A. (2002). *Computer Networks*, Fourth Edition. Upper Saddle River, NJ, Prentice Hall

Actividades de aprendizaje

A.2.1 Resumen de Protocolo de ruteo

Lee las páginas 3 y 4 del RFC 4274 ubicado en el siguiente enlace http://www.rfc-archive.org/getrfc.php?rfc=4274&tag=BGP-4-Protocol-Analysis y responde lo siguiente:

1. ¿Qué tipo de algoritmo usa BGP?

2. ¿Cómo funciona el intercambio de información en BGP?

3. ¿Cuáles son los 6 estados en los que BGP puede encontrarse?

A.2.2 Encabezado del protocolo BGP

Realiza la lectura de las páginas 11 y 12 del RFC 4271 disponible en: http://www.rfc-archive.org/getrfc.php?rfc=4271&tag=A-Border-Gateway-Protocol-4-(BGP-4) y responde lo siguiente:

1. ¿Cuáles son los cuatro tipos de mensaje que define BGP?

2. ¿Cuál es el primer mensaje enviado por un ruteador después de que la conexión TCP ha sido establecida?

3. Escribe cuáles son los campos del mensaje OPEN y para qué sirven.

A.2.3 Reporte de una red LAN

Visita una oficina, escuela o establecimiento donde tengan una red LAN e identifica lo siguiente:

- Marca y modelo del dispositivo de interconexión central.
- Número de computadoras conectadas al dispositivo.
- Marca y modelo del dispositivo que brinda acceso a Internet

Cuestionario de autoevaluación

1. ¿Qué es una red LAN?
2. ¿Qué es una red MAN?
3. ¿Qué es una red WAN?
4. ¿En qué consiste el método de ruteo por saltos mínimos?
5. ¿Qué es el ruteado directo?
6. ¿Qué es un protocolo de ruteo?
7. ¿Qué mecanismo emplea RIP para determinar la mejor ruta?
8. ¿De qué se encarga el protocolo IP?
9. ¿Qué es un switch?
10. ¿Qué es una VLAN?

Examen de autoevaluación

I- Lee con cuidado cada enunciado y elije si es verdadero o falso.

1.	Una red LAN puede tener una velocidad de 1 Gbps	V	F
2.	Una red WAN permite conexiones entre redes ubicadas en diferentes ciudades	V	F
3.	La tecnología llamada Voz sobre IP (VoIP) brinda las bondades del servicio telefónico utilizando una red de datos ya existente:	V	F
4.	El protocolo IP está definido en el RFC 791	V	F

II. Lee cada enunciado y elige la opción correcta.

1. Un ruteador es un dispositivo que:
    a) conmuta paquetes
    b) decide la mejor ruta
    c) repite la señal

2. Qué operación realiza un *switch* cuando no conoce la dirección destino:
    a) entrega el paquete
    b) tira el paquete
    c) envía un *broadcast*

3. En qué consiste un *broadcast*:
    a) Enviar información a todos los puertos
    b) Enviar paquete a un puerto
    c) No enviar ninguna información

4. Son protocolos de ruteo:
    a) IP, IPX
    b) OSPF, BGP
    c) RIP, IP

5. Son protocolos ruteables:
    a) IP, IPX, OSPF
    b) IP, TCP, BGP
    c) IP, IPX

6. Tipo de ruteo donde el ruteador toma las decisiones:
    a) Directo
    b) Indirecto
    c) Ambos

TEMA 3. INTEGRIDAD

Objetivo particular

El alumno reconocerá la importancia de la integridad de la información, así como las definiciones que envuelven un proceso de seguridad de la información.

Temario detallado

3.1. Definición en redes
3.2. Conceptos Generales
    3.2.1. Protección
    3.2.2. Interrupción
    3.2.3. Modificación
    3.2.4. Fabricación
    3.2.5. Control de acceso
    3.2.6. Disponibilidad
3.3. Protocolos de seguridad
3.4. Permisos
3.5. Sistemas de respaldo

Introducción

La información siempre ha estado expuesta a ser falsificada, robada o destruida. Con el avance de la tecnología computacional se han realizado mejoras en el manejo de la información para su mayor seguridad. Ya es posible usar protocolos y algoritmos de cifrado potentes que permiten mantener altos niveles de seguridad. Estos avances no solamente en cuestiones de integridad sino también en los de confidencialidad, autenticidad y disponibilidad. También se necesita de políticas que definan claramente el propósito y la forma de mantener la integridad de la información. Este proceso suele traer incomodidades al usuario final porque

implica un cambio en sus costumbres de trabajo, por eso es necesario contar con campañas enfocadas a hacer conciencia de la seguridad de la información.

3.1 Definición en 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 sufren 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 también puede dejar sin servicio a los usuarios. Eso sería una señal de un ataque informático.

3.2 Conceptos Generales

3.2.1 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 la red de 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. También el cifrado de la información puede ayudar en la tarea de proteger la información. Dicho cifrado de información consiste en realizar una transformación a la información de manera que un lector casual o malintencionado no pueda entender lo que está leyendo.

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 un sistema de información de

cualquier tipo; ya 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 son las siguientes:

3.2.2 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 servicios DoS haciéndolos inutilizables. Tanto empresas como oficinas de gobiernos son el blanco de este tipo de ataques, en algunos casos por venganza y otros casos 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 servicios. Un sistema detector de intrusos o IDS (*Intrusion Detection System*) se encuentra siempre observando el tráfico de la red y conforme reglas detecta comportamientos fuera de lo normal y los reporta como posibles ataques.

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.

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 las contraseñas.

3.2.3 Modificación

Se presenta cuando un agente no autorizado logra obtener acceso a recursos del sistema de información y con la capacidad de manipular la información. Un ejemplo es cuando se altera un programa para que otorgue resultados diferentes. Como, al hacer una transferencia vía banca electrónica el sistema informático del banco acumula cualquier movimiento hacia una cuenta fraudulenta. Eso solamente se puede lograr si el sistema original fue modificado para enviar depósitos a una cuenta de otra persona.

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 tiene que cuidar que sus configuraciones no sean modificadas para que no afecte la forma en la que la red opera. Puede suceder que por error o maliciosamente se especifique una dirección IP diferente al equipo, esto provocaría que un segmento de red se quede sin poder comunicarse al resto de los segmentos de red.

3.2.4 Fabricación

Se presenta cuando un agente no autorizado crea información falsa dentro del sistema de información. 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 fuesen a un servidor con propósitos maliciosos.

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

3.2.5 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 a 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 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 que es la persona que dice ser. 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 dichas credenciales (usuario y contraseña) 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 el usuario, 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.

3.2.6 Disponibilidad

Un sistema se encuentra disponible cuando se le demanda algún servicio y éste 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. Cuando una red de cómputo es lenta, o se satura entonces su disponibilidad está en riesgo. Esto puede darse por una demanda superior a la esperada o también por ataques contra la disponibilidad de la red o de algún sistema dentro de la red.

Un virus de alto impacto puede dañar la disponibilidad de una red ya que su rápida propagación afecta el rendimiento de la red 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.

3.3 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 en el pago, si es en efectivo o si acepta tarjeta de crédito. Una vez que la tienda recibe el pago, entregan lo que se compró. Todo este proceso es un protocolo que se debe seguir para la compra de productos.

En seguridad, un protocolo echa mano de la criptografía para que la información legible sea transformada por medio de un elemento conocido como llave. De modo que solamente el que posee dicha llave pueda tener acceso a la información. En un medio ambiente de red es necesario utilizar protocolos porque se intercambia información entre una computadora y otra. Es necesario que estos intercambios sean acompañados de criptografía para brindar seguridad a la información.

El algoritmo de cifrado 3DES utiliza una sola llave para descifrar el contenido de la información y hacerlo legible. Cuando se implementa por medio de un protocolo se necesita que ambas partes conozcan esa llave. Si no se conoce o si la llave es errónea el protocolo no puede completarse.

3.4 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.

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 programa. En cambio, un usuario con permisos de administrador sí podrá hacerlo.

3.5 Sistemas de respaldo

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

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.

Bibliografía del tema 3

Barrett; Daniel J., Richard E. Silverman; Robert G. Byrnes (2003). Linux *Security Cookbook*. Sebastopol, California, O'Reilly Media

SSI, UNAM-CERT, *Seguridad de la Información*. México, UNAM, disponible en línea: http://www.seguridad.unam.mx

Actividades de aprendizaje

A.3.1 Haz un reporte de media cuartilla explicando el funcionamiento de un *Intrusion Detection System* (IDS).

A.3.2 Los ataques para interrumpir la actividad en línea de sitios web es una realidad en las sociedades contemporáneas. Investiga un ataque masivo y organizado llamado 'Operación Tequila'. Debes entregar un texto en Word indicando de qué se trata este movimiento, a quiénes buscaba afectar y cuáles eran las razones principales.

A.3.3 Lee el siguiente artículo de la Comunidad Europea, *Seguridad de las redes y de la información: Propuesta para un enfoque político europea*. (2001), http://ec.europa.eu/information_society/eeurope/2002/news_library/pdf_files/netsec_es.pdf (consultado el 03/03/11)

Cuestionario de autoevaluación

1. En términos de seguridad de la información, ¿a qué ha estado expuesta siempre la información?
2. ¿Qué aspectos de la seguridad en cómputo deben mantenerse en una red?
3. ¿En qué consiste la protección de la información?
4. ¿Qué aspectos debería cumplir una estrategia de seguridad?
5. ¿En qué consiste la interrupción de la información?
6. ¿Qué es un IDS?
7. ¿En qué consiste la modificación de la información?

8. ¿En qué consiste la fabricación de información?
9. ¿En qué cosiste el control de acceso?
10. ¿A qué se refiere la disponibilidad?

Examen de autoevaluación

I. Lee cuidadosamente cada enunciado y elige si es verdadero (V) o falso (F).

1.	La información siempre ha estado expuesta a ser falsificada, robada o destruida.	V	F
2.	Hoy en día no es posible hacer uso de protocolos y algoritmos de cifrado fuertes que permiten mantener altos niveles de seguridad.	V	F
3.	La protección de la información se da cuando un agente no autorizado logra obtener acceso a recursos del sistema de información sin necesariamente poder manipularlos.	V	F
4.	El cifrado de la información puede ayudar en la tarea de proteger la información.	V	F
5	La intercepción se presenta cuando un agente no autorizado logra obtener acceso a recursos del sistema de información sin necesariamente poder manipularlos.	V	F

II. Lee cada oración y elige la opción que conteste correctamente a cada una.

1. Se presenta cuando un agente no autorizado crea información falsa dentro del sistema de información
    a) Modificación
    b) Fabricación
    c) Interrupción

2. En seguridad, un protocolo echa mano de la _____ para que la información legible sea transformada por medio de un elemento conocido como llave.
    a) Modificación
    b) Fabricación
    c) Criptografía

3. Cuando un sistema responde sin importar la hora, el lugar, el día, etc., a la demanda de algún servicio se dice que el sistema tiene

a) Disponibilidad
b) Seguridad
c) Autorización

4. Una vez que el usuario ha sido autenticado existen otras políticas que definen las tareas que tiene permitido hacer el usuario, dichas políticas son de:
    a) Restricción
    b) Autorización
    c) Autenticación

5. Serie de pasos utilizados con el fin de resolver un problema de seguridad:
    a) Buenas prácticas
    b) Recomendaciones
    c) Protocolo de seguridad

TEMA 4. SEGURIDAD

Objetivo particular

El alumno reconocerá la importancia de implementar servicios de seguridad en una red y también los servicios de seguridad más importantes.

Temario detallado

4.1 Importancia de la seguridad en redes

4.2 Funciones de seguridad

- 4.2.1 Análisis de riesgo
- 4.2.2 Servicios de seguridad
  - 4.2.2.1 Autenticación de las comunicaciones y los datos
  - 4.2.2.2 Control de acceso
  - 4.2.2.3 Garantía de la privacidad de los datos
  - 4.2.2.4 Análisis de flujo de tráfico
  - 4.2.2.5 Garantía de la integridad de los datos
  - 4.2.2.6 Reconocimiento del receptor y/o transmisor

Introducción

La seguridad en redes es una suerte de espécimen desconocido por los altos directivos de una organización. Generalmente se le reconoce pero en la práctica no se le otorga la importancia debida. Una de las razones por lo que esto sucede es, tal vez, que se tiene que invertir en análisis y en infraestructura. El reto es dar a conocer la importancia de la seguridad en redes, el impacto que tienen los ataques informáticos en la economía de la organización y en su prestigio. Recientemente se supo de un ataque a una de las entidades financieras más importantes del mundo, aunque solamente fue una inundación de peticiones para que su sitio web perdiera disponibilidad, dejando en evidencia ante el mundo que cualquier sitio tiene su grado de vulnerabilidad.

La seguridad en redes no es una opción, es una necesidad que las organizaciones cada día están comenzando a tomar en cuenta. Ya es 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. A diario, existen corporaciones de personas que se dedican a romper la seguridad de una empresa cobrando grandes cantidades de dinero. Términos como 'cyberterrorismo' o 'cyberguerra' comienzan a ser familiares.

Por todo esto, la seguridad en redes se convierte en un tema importante para la seguridad de la información.

4.1 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 que existe de que dicha información sea comprometida o puesta en riesgo, 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 que hará bien su tarea de revisar los correos electrónicos de una empresa mientras mantenga actualizada su base de datos de virus. Este simple ejemplo requiere de inversión por parte del usuario ya que cada marca de antivirus reconocida cobra un precio anual para tener el privilegio de las actualizaciones. Si se deja de actualizar el programa antivirus entonces se deja expuesta a esa red.

Ahora si se piensa 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. Estas reglas requieren modificarse eventualmente cuando una aplicación nueva se integra a la red; si no hay personal calificado para esta tarea entonces esa aplicación puede quedar expuesta a un ataque.

La seguridad en redes no es una tarea de una sola vez, es un proceso constante de análisis e implementación porque, lamentablemente, día con día aparecen amenazas, nuevas técnicas de ataque y vulnerabilidades en los sistemas. No se puede correr el riesgo de pensar que nadie se fijará en la red para vulnerarla y, por lo tanto, no se necesita de seguridad informática en ella. Generalmente una empresa pequeña no es un objetivo de ataques de informáticos pero la mala noticia es que sí puede ser usada como origen de un ataque hacia empresas más poderosas.

4.2 Funciones de Seguridad

4.2.1 Análisis de Riesgos

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 identificar esos riesgos, analizarlos para saber dónde se originan y tomar las medidas necesarias para mitigarlos. Conviene aclarar que no existe un sistema cien por ciento seguro, ya que siempre existirán errores humanos y de programación.

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, el personal. Se identifican las áreas problemáticas en cada activo. Por ejemplo, en un análisis se puede encontrar que hay fuentes de amenazas internas por medio de personal poco confiable. O se podrían localizar defectos en un sistema o en un equipo de hardware.

El encontrar estas áreas problemáticas conlleva a determinar cuáles serían los principales problemas que se podrían presentar, es decir, los riesgos que se corren con estos problemas. Si el personal no es confiable, se corre el riesgo de que cierta información confidencial sea revelada, o de que la información pueda ser modificada por ese tipo de personas. Si se encuentra deficiencias en hardware o software, ello puede ser una fuente de pérdida de información accidental debido a un mal funcionamiento.

En esta fase también se identifican los servicios de seguridad requeridos como confidencialidad, integridad y disponibilidad.

2. Identificación de vulnerabilidades

En la fase anterior se identificó a todos los activos y las amenazas potenciales. En esta fase lo que se hace es encontrar qué tan vulnerable es el sistema o la red a esas amenazas. En esta fase se focalizan recursos para encontrar errores de diseño, problemas de implementación, configuraciones defectuosas en toda la red, haciendo uso de herramientas de evaluación de vulnerabilidades como escáner de infraestructura y escáner de sistema operativo.

Esta evaluación dará como resultado un informe preliminar donde se agrupen los resultados obtenidos de la evaluación y brinda 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 que brinda servicios web. O se pude encontrar que el servidor de correo electrónico de la empresa cuenta con las actualizaciones debidas y no tiene ninguna 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. Si en el informe se arroja el estado vulnerable de un servidor web, la acción correctiva será actualizar la aplicación del servicio para que esa parte vulnerable sea corregida.

4.2.2 Servicios de Seguridad

4.2.2.1 Autenticación de las comunicaciones y los datos

La autenticación sirve para garantizar que los participantes en una comunicación en realidad tienen la identidad válida para realizar sus actividades. 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 corresponden 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 envío de información de inventarios entre una sucursal y su oficina central, como 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, pudiera 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 en palabras comunes y fáciles de adivinar. O cuando se utilizan medios que están a la vista de cualquier intruso en Internet. 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 sistemas se basan 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. *Secure shell* es una aplicación utilizada para conexiones remotas seguras y ofrece la posibilidad de autenticación remota mediante llave pública.

4.2.2.2 Control de Acceso

Además de autenticar a los usuarios y las conexiones, es necesario controlar los accesos a nivel de red y para cada usuario, de tal manera que cada usuario pueda tener los servicios y recursos disponibles según su identidad. Cuando se visita un

portal de banco e ingresa las credenciales se espera ver únicamente la información de esa cuenta y se espera que nadie más pueda tener acceso a ella. Igualmente, un alumno accede a su historial académico únicamente y a 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 es un sistema que permite autenticar usuarios pero además permite crear perfiles de usuario para asignarles permisos y roles una vez que ha sido autenticado. 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.

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 de 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.

Otra forma de controlar los accesos después del proceso de autenticación es la dirección IP de origen. Existen servicios de biblioteca digital 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. Permitirían acceder a una biblioteca digital desde la comodidad de los hogares porque una VPN los hace parte de la red universitaria desde donde sí es posible ingresar a ese sitio.

4.2.2.3 Garantía de la privacidad de los datos

Lo único que garantiza la privacidad de los datos es la criptografía. Junta con ésta 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. Una 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. El gran problema de las flamantes aplicaciones es que no son creadas pensando en la seguridad de la información. Actualmente 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 que se utilizan para cifrar la información, esas llaves son el acceso a los recursos.

4.2.2.4 Análisis del flujo de tráfico

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 de usarlo para dañar a terceros.

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 puede atentar contra datos confidenciales. Los *sniffers* son herramientas muy buenas para auditar la confidencialidad de la información. 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.

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.

4.2.2.5 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.

Cuando se descarga software de Internet generalmente se pide verificar la integridad de ese programa mediante una función hash. Ellos 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 tanto es 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.

4.2.2.6 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 mediante 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.

Bibliografía del tema 4

Herzog, Pete. (2000). *Manual de la Metodología Abierta de Testeo de Seguridad*, ISECOM – Instituto para la Seguridad y las Metodologías Abiertas, OSSTMM 2.1, modificado el 23/08/03. Disponible en línea: http://isecom.securenetltd.com/OSSTMM.es.2.1.pdf

SSI, UNAM-CERT. (2011). *Seguridad de la Información*. Universidad Nacional Autónoma de México, disponible en línea: http://www.seguridad.unam.mx

Actividades de aprendizaje

A.4.1 Búsqueda de dispositivo de seguridad

Busca en el motor de búsqueda preferido o directamente del portal de un fabricante, tres modelos de un dispositivo de seguridad firewall de tres marcas y realiza un cuadro comparativo con los datos obtenidos.

A.4.2 Lectura de Artículo

Con el objetivo de profundizar más en el tema de seguridad, lee el artículo publicado en la siguiente dirección electrónica http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201103_sp.pdf y elabora un mapa conceptual.

A.4.3 Investigación

Investiga información de dos virus informáticos famosos: Code Red y Nimda y realiza un resumen que contenga el funcionamiento del virus, la velocidad de propagación, las medidas para contenerlo y la cantidad de computadoras afectadas.

Cuestionario de autoevaluación

1. Menciona una de las razones para no darle importancia a la seguridad informática.
2. ¿Cuál es la función de la seguridad informática?
3. ¿Qué es un firewall?
4. ¿Por qué la seguridad en redes debe ser un proceso?
5. ¿Cuál es el primer paso para determinar el nivel de seguridad que requerimos?
6. ¿A qué nos referimos con riesgo?
7. ¿Cuáles son las tres fases de un análisis de riesgos?
8. ¿En qué consiste el cifrado?
9. ¿Para qué sirve analizar el flujo de tráfico de una red?
10. ¿Para qué sirve la autenticación?

Examen de autoevaluación

I. Lee cuidadosamente cada oración y marca con una X la letra V si es verdadera o la F si es falsa

1.	La seguridad en redes es una disciplina que requiere de constante actualización.	V	F
2.	Cuando se deja de actualizar el programa antivirus no pasa nada	V	F
3.	Un riesgo es la posibilidad de que un sistema sufra daño o pérdida	V	F
4.	El primer paso para determinar el nivel de seguridad que se requiere es la realización de un análisis de riesgos	V	F
5	La Elaboración de perfiles de activos y amenazas es la fase donde se encuentra qué tan vulnerable es el sistema o la red a esas amenazas.	V	F

II. Lee cada pregunta y subraya la respuesta correcta

1. Dispositivo que controla los accesos a la red manteniéndola aislado de algunas amenazas en Internet:

a) VPN

b) Firewall

c) Switch

2. Metodología para determinar las necesidades de seguridad de la información en una empresa:

a) Análisis de riesgos

b) Riesgo

c) Control de acceso

3. Algoritmos más utilizados para la integridad de información:

a) MD5, SHA

b) IP, TCP

c) VPN, Firewall

4. Permiten la inspección profunda de cientos de protocolos.

a) Firewall

b) VPN

c) Sniffer

5. Lo único que garantiza la privacidad de los datos es

a) Criptografía

b) Buena suerte

c) Análisis de Riesgos

Bibliografía básica

(Los sitios electrónicos en línea funcionan al 17/03/11)

Barrett; Daniel J., Richard E. Silverman; Robert G. Byrnes (2003). *Linux Security Cookbook*. Sebastopol, California, O'Reilly Media

Brent, Stewart (2010*). CCNP TSHOOT 642-832 Quick Reference*. Indianápolis, Cisco Press.

Davidson, J. (2006*). Voice over IP Fundamentals*, Second Edition. Indianápolis, Cisco Press.

Doherty, J. & Anderson, N. (2007*). Cisco Networking Simplified*, Second Edition. Indianápolis, Cisco Press.

Herzog, Pete. (2000). *Manual de la Metodología Abierta de Testeo de Seguridad*, ISECOM – Instituto para la Seguridad y las Metodologías Abiertas, OSSTMM 2.1, modificado el 23/08/03. Disponible en línea: http://isecom.securenetltd.com/OSSTMM.es.2.1.pdf

Nader, F. (2006). *Computer and Communication Networks*. Upper Saddle River, NJ, Prentice Hall

Stevens, R. (1993). *TCP/IP Illustrated*, Volume 1: The Protocols. Upper Saddle River, NJ, Addison-Wesley Professional

Subdirección de Seguridad de la Información, CERT, DGTIC, (2011). *Seguridad de la Información*. México, UNAM, disponible en línea: http://www.seguridad.unam.mx

Tanenbaum, A. (2002). *Computer Networks*, 4ª ed., Upper Saddle River, NJ, Prentice Hall.

RESPUESTAS A LOS EXÁMENES DE AUTOEVALUACIÓN

TELECOMUNICACIONES II

	Tema 1		Tema 2		Tema 3		Tema 4	
1.	V	c	F	b	V	b	V	b
2.	V	b	V	c	F	c	F	a
3.	V	a	V	a	F	a	V	a
4.	F	a	V	b	V	b	V	c
5.	F	b		c	V	c	F	a
6.				b				