Investigación 01

9941 19 824 – Julio Cesar de la Cruz Ovando
jdelacruzo@miumg.edu.gt
Redes I
Ingeniería en Sistemas
Universidad Mariano Gálvez de Guatemala, Sede Portales

Introducción

En la siguiente investigación veremos temas introductorios necesarios para comprender el curso de Redes I, dentro de estos temas veremos los diferentes protocolos de Red existentes en la actualidad, así como las vulnerabilidades que estos puedan poseer y los puertos necesarios para su funcionamiento.

Protocolos de Red

Historia y origen de las redes

La ARPA (Advanced Research Projects Agency) en el año 1965 patrocino un programa que trataba de analizar las redes de comunicación usando computadoras. Mediante este programa, la máquina TX-2 en el laboratorio Licoln del MIT y la AN/FSQ-32 del System Development Corporation de Santa Mónica en California, se enlazaron directamente mediante una línea delicada de 1200 bits por segundo.

En 1967 La ARPA convoca una reunión en Ann Arbor (Michigan), donde se discuten por primera vez aspectos sobre la futura ARPANET. En 1968 la ARPA no espera más y llama a empresas y universidades para que propusieran diseños, con el objetivo de construir la futura red. La universidad de California gana la propuesta para el diseño del centro de gestión de red y la empresa BBN (Bolt Beraneck and Newman Inc.) El concurso de adjudicación para el desarrollo de la tecnología de conmutación de paquetes mediante la implementación de la Interfaz Message Processors (IMP).

En 1969 se construye la primera red de computadoras de la historia. Denominada ARPANET, estaba compuesta por cuatro nodos situados en UCLA (Universidad de California en los Angeles), SRI (Stanford Research Institute), UCBS (Universidad de California de Santa Bárbara, Los Angeles) y la Universidad de UTA. En 1970 la ARPANET comienza a utilizar para sus comunicaciones un protocolo Host-to-post. Este protocolo se denominaba NCP y es el predecesor del actual TCP/IP que se utiliza en toda la Internet. En ese mismo año, Norman Abramson desarrolla la ALOHANET que era la primera red de conmutación de paquetes vía radio y se uniría a la ARPANET en 1972.

En 1973 se produce la primera conexión internacional de la ARPANET. Dicha conexión se realiza con el colegio universitario de Londres (Inglaterra) En ese mismo año Bob Metcalfe expone sus primeras ideas para la implementación del protocolo Ethernet que es uno de los protocolos más importantes que se utiliza en las redes locales. A mediados de ese año se edita el RFC454 con especificaciones para la transferencia de archivos, a la vez que la universidad de Stanford comienza a emitir noticias a través de la ARPANET de manera permanente. En ese momento la ARPANET contaba ya con 2000 usuarios y el 75% de su tráfico lo generaba el intercambio de correo electrónico.

En 1974 Cerf y Kahn publican su artículo, un protocolo para interconexión de redes de paquetes, que especificaba con detalle el diseño del protocolo de control de transmisión (TCP). En 1975 Se prueban los primeros enlaces vía satélite cruzando dos océanos (desde Hawái a Inglaterra) con las primeras pruebas de TCP de la mano de Stanford, UCLA y UCL. En ese mismo año se distribuyen las primeras versiones del programa UUCP (Unís-to-Unix CoPy) del sistema operativo UNIX por parte de AT&T. En 1980 se crean redes particulares como la CSNET que proporciona servicios de red a científicos sin acceso a la ARPANET.

En 1982 la DCA y la ARPA nombran a TCP e IP como el conjunto de protocolos TCP/IP de comunicación a través de la ARPANET. En 1985 se establecen responsabilidades para el control de los nombres de dominio y así el ISI (Información Sciences Institute) asume la responsabilidad de ser la raíz para la resolución de los nombres de dominio. El 15 de marzo se produce el primer registro de nombre de dominio (symbolics.com) a los que seguirían cmu.edu, purdue.edu, rice.edu, ucla.edu y .uk

Protocolos

Un protocolo es un método estándar que permite la comunicación entre procesos y un conjunto de reglas y procedimientos que deben respetarse para el envío y la recepción de datos a través de una red.

Dentro de los protocolos actuales o existentes hoy en día tenemos:

TCP (Transmission-Control-Protocol)

El Protocolo de Control de Transmisión es uno de los protocolos fundamentales en Internet. Fue creado entre los años 1973-1974 por Vint Cerf y Robert Kahn. Este es uno de los principales protocolos de la capa de transporte del modelo TCP/IP. En el nivel de aplicación, posibilita la administración de datos que vienen del nivel más bajo del modelo, o van hacia él, (es decir, el protocolo IP). Cuando se proporcionan los datos al protocolo IP, los agrupa en datagramas IP, fijando el campo del protocolo en 6 (para que sepa con anticipación que el protocolo es TCP). Como es un protocolo orientado a conexión permite que dos máquinas que están comunicadas controlen el estado de la transmisión. Las principales características del protocolo TCP son las siguientes: Da soporte a muchas de las aplicaciones más populares de Internet, incluidas HTTP, SMTP, SSH y FTP. Permite colocar los datagramas nuevamente en orden cuando vienen del protocolo IP.

IP (Internet Protocol)

El Protocolo de Internet es un protocolo no orientado a conexión usado tanto por el origen como por el destino para la comunicación de datos a través de una red de paquetes conmutados.

El Protocolo de Internet provee un servicio de datagramas no fiable, IP no provee ningún mecanismo para determinar si un paquete alcanza o no su destino y únicamente proporciona seguridad de sus cabeceras y no de los datos transmitidos. Por ejemplo, al no garantizar nada sobre la recepción del paquete, éste podría llegar dañado, en otro orden con respecto a otros paquetes, duplicado o simplemente no llegar. Si se necesita fiabilidad, ésta es proporcionada por los protocolos de la capa de transporte, como TCP. Las direcciones IP son direcciones numéricas compuestas por cuatro números enteros (4bytes) entre 0 y 255, y escritos en el formato xxx.xxx.xxx.xxx. Por ejemplo, 194.153.205.26es una dirección IP en formato técnico.

El IP es el elemento común en la Internet de hoy. Poco a poco Internet está agotando las direcciones disponibles por lo que se utilizan direcciones de fuente y destino de 128bits (lo cual asigna a cada milímetro cuadrado de la superficie de la Tierra la colosal cifra de 670.000 millones de direcciones IP).

HTTP (HyperText Transfer Protocol)

(Protocolo de transferencia de hipertexto) es el protocolo más utilizado en Internet. Es el protocolo usado en cada transacción de la Web (WWW). El propósito del protocolo HTTP es permitir la transferencia de archivos (principalmente, en formato HTML) entre un navegador (el cliente) y un servidor web (denominado, entre otros, http en equipos UNIX).HTTP define la sintaxis y la semántica que utilizan los elementos software de la arquitectura web (clientes, servidores, proxies) para comunicarse. Es un protocolo orientado a transacciones y sigue el esquema petición-respuesta entre un cliente y un servidor. Al cliente que efectúa la petición (un navegador o un spider) se lo conoce como "user agent" (agente del usuario). A la información transmitida se la llama recurso y se la identifica mediante una cadena de caracteres denominada dirección URL. Los recursos pueden ser archivos, el resultado de la ejecución de un programa, una consulta a una base de datos, la traducción automática de un documento, etc.

ARP (Address Resolution Protocol)

El ARP (Protocolo de resolución de direcciones) es un protocolo de nivel de red responsable de encontrar la dirección hardware (Ethernet MAC) que corresponde a una determinada dirección IP. Para ello se envía un paquete (ARP request) a la dirección de difusión de la red que contiene la dirección IP por la que se pregunta, y se espera a que esa máquina (u otra) responda (ARP reply) con la dirección Ethernet que le corresponde. Cada máquina mantiene una caché con las direcciones traducidas para reducir el retardo y la carga. ARP permite a la dirección de Internet ser independiente de la dirección Ethernet, pero esto sólo funciona si todas las máquinas lo soportan. En Ethernet, la capa de enlace trabaja con direcciones físicas

Este protocolo tiene varias limitaciones. Se necesita mucho tiempo de administración para mantener las tablas importantes en los servidores. Esto se ve reflejado aún más en las grandes redes, lo que plantea problemas de recursos humanos, necesarios para el mantenimiento de las tablas de búsqueda y de capacidad por parte del hardware que aloja la parte del servidor del protocolo RARP. Efectivamente, este protocolo permite que varios servidores respondan a solicitudes, pero no prevé mecanismos que garanticen que todos los servidores puedan responder, ni que respondan en forma idéntica. Por lo que, en este tipo de arquitectura, no podemos confiar en que un servidor RARP sepa si una dirección MAC se puede conectar con una dirección IP, porque otros servidores ARP pueden tener una respuesta diferente.

FTP (File Transfer Protocol)

El protocolo FTP (Protocolo de transferencia de archivos) es, como su nombre lo indica, un protocolo para transferir archivos. La implementación del FTP se remonta a 1971 cuando se desarrolló un sistema de transferencia de archivos entre equipos del Instituto Tecnológico de Massachusetts. Este protocolo define la manera en que los datos deben ser transferidos a través de una red TCP/IP. El objetivo del protocolo FTP es:

- Permitir que equipos remotos puedan compartir archivos.
- Permitir la independencia entre los sistemas de archivo del equipo del cliente y del equipo del servidor.
- Permitir una transferencia de datos eficaz.

SMTP (Simple Mail Transfer Protocol)

SMTP (Protocolo simple de transferencia de correo) es un protocolo de la capa de aplicación. Es un protocolo de red basado en texto utilizado para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos. SMTP se basa en el modelo cliente-servidor, donde un cliente envía un mensaje a uno o varios receptores. La comunicación entre el cliente y el servidor consiste enteramente en líneas de texto compuestas por caracteres ASCII. El tamaño máximo permitido para estas líneas es de 1000 caracteres. Las respuestas del servidor constan de un código numérico de tres dígitos, seguido de un texto explicativo. El número va dirigido a un procesado automático de la respuesta por autómata, mientras que el texto permite que un humano interprete la respuesta. En todas las órdenes, réplicas o datos son líneas de texto, delimitadas por el carácter <CRLF>. Todas las réplicas tienen un código numérico al comienzo de la línea.

POP (Post Office Protocol)

Se utiliza el Post Office Protocol en clientes locales de correo para obtener los mensajes de correo electrónico almacenados en un servidor remoto. La mayoría de los suscriptores de los proveedores de Internet acceden a sus correos a través de POP3.POP3 está diseñado para recibir correo, no para enviarlo; les permite a los usuarios con conexiones intermitentes o muy lentas (conexiones por módem), descargar su correo electrónico mientras tienen conexión y revisarlo posteriormente incluso estando desconectados. Cabe mencionar que la mayoría de los clientes de correo incluyen la opción de dejar los mensajes en el servidor, de manera tal que, un cliente que utilice POP3 se conecta, obtiene todos los mensajes, los almacena en la computadora del usuario como mensajes nuevos, los elimina del servidor y finalmente se desconecta.

El protocolo IMAP permite los modos de operación conectado y desconectado. Los clientes de correo electrónico que utilizan IMAP dejan por lo general los mensajes en el servidor hasta que el usuario los elimina directamente. Esto y otros factores hacen que la operación de IMAP permita a múltiples clientes acceder al mismo buzón de correo. La mayoría de los clientes de correo electrónico soportan POP3 o IMAP; sin embargo, solo unos cuantos proveedores de internet ofrecen IMAP como valor agregado de sus servicios. Al igual que otros viejos protocolos de internet, POP3 utilizaba un mecanismo de firmado sin cifrado. La transmisión de contraseñas de POP3 en texto plano aún se da. En la actualidad POP3 cuenta con diversos métodos de autenticación que ofrecen una diversa gama de niveles de protección contra los accesos ilegales al buzón de correo de los usuarios. Uno de estos es APOP, el cual utiliza funciones MD5 para evitar los ataques de contraseñas

Principales puertos TCP que usan muchos protocolos de la capa de aplicación y también aplicaciones:

- **Puerto 21**: El puerto 21 por norma general se usa para las conexiones a servidores FTP en su canal de control, siempre que no hayamos cambiado el puerto de escucha de nuestro servidor FTP o FTPES.
- **Puerto 22**: Por normal general este puerto se usa para conexiones seguras SSH y SFTP, siempre que no hayamos cambiado el puerto de escucha de nuestro servidor SSH.
- **Puerto 23**: Telnet, sirve para establecer conexión remotamente con otro equipo por la línea de comandos y controlarlo. Es un protocolo no seguro ya que la autenticación y todo el tráfico de datos se envía sin cifrar.
- **Puerto 25**: El puerto 25 es usado por el protocolo SMTP para él envió de correos electrónicos, también el mismo protocolo puede usar los puertos 26 y 2525.
- **Puerto 53**: Es usado por el servicio de DNS, Domain Name System.
- **Puerto 80**: Este puerto es el que se usa para la navegación web de forma no segura HTTP.
- **Puerto 101**: Este puerto es usado por el servicio Hostname y sirve para identificar el nombre de los equipos.
- **Puerto 110**: Este puerto lo usan los gestores de correo electrónico para establecer conexión con el protocolo POP3.
- **Puerto 143**: El puerto 143 lo usa el protocolo IMAP que es también usado por los gestores de correo electrónico.
- **Puerto 443**: Este puerto es también para la navegación web, pero en este caso usa el protocolo HTTPS que es seguro y utiliza el protocolo TLS por debajo.
- **Puerto 445**: Este puerto es compartido por varios servicios, entre el más importante es el Active Directory.
- **Puerto 587**: Este puerto lo usa el protocolo SMTP SSL y, al igual que el puerto anterior sirve para el envío de correos electrónicos, pero en este caso de forma segura.
- **Puerto 591**: Es usado por Filemaker en alternativa al puerto 80 HTTP.
- **Puerto 853**: Es utilizado por DNS over TLS.
- **Puerto 990**: Si utilizamos FTPS (FTP Implícito) utilizaremos el puerto por defecto 990, aunque se puede cambiar.
- **Puerto 993**: El puerto 993 lo usa el protocolo IMAP SSL que es también usado por los gestores de correo electrónico para establecer la conexión de forma segura.
- **Puerto 995**: Al igual que el anterior puerto, sirve para que los gestores de correo electrónico establezcan conexión segura con el protocolo POP3 SSL.
- **Puerto 1194**: Este puerto está tanto en TCP como en UDP, es utilizado por el popular protocolo OpenVPN para las redes privadas virtuales.
- **Puerto 1723**: Es usado por el protocolo de VPN PPTP.

- **Puerto 1812**: se utiliza tanto con TCP como con UDP, y sirve para autenticar clientes en un servidor RADIUS.
- **Puerto 1813**: se utiliza tanto con TCP como con UDP, y sirve para el accounting en un servidor RADIUS.
- **Puerto 2049**: es utilizado por el protocolo NFS para el intercambio de ficheros en red local o en Internet.
- **Puertos 2082 y 2083**: es utilizado por el popular CMS cPanel para la gestión de servidores y servicios, dependiendo de si se usa HTTP o HTTPS, se utiliza uno u otro.
- **Puerto 3074**: Lo usa el servicio online de videojuegos de Microsoft Xbox Live.
- **Puerto 3306**: Puerto usado por las bases de datos MySQL.
- **Puerto 3389**: Es el puerto que usa el escritorio remoto de Windows, muy recomendable cambiarlo.
- **Puerto 4662 TCP y 4672 UDP**: Estos puertos los usa el mítico programa eMule, que es un programa para descargar todo tipo de archivos.
- **Puerto 4899**: Este puerto lo usa Radmin, que es un programa para controlar remotamente equipos.
- **Puerto 5000**: es el puerto de control del popular protocolo UPnP, y que, por defecto, siempre deberíamos desactivarlo en el router para no tener ningún problema de seguridad.
- **Puertos 5400, 5500, 5600, 5700, 5800 y 5900**: Son usados por el programa VNC, que también sirve para controlar equipos remotamente.
- **Puertos 6881 y 6969**: Son usados por el programa BitTorrent, que sirve para e intercambio de ficheros.
- **Puerto 8080**: es el puerto alternativo al puerto 80 TCP para servidores web, normalmente se utiliza este puerto en pruebas.
- **Puertos 51400**: Es el puerto utilizado de manera predeterminada por el programa Transmission para descargar archivos a través de la red BitTorrent.
- **Puerto 25565**: Puerto usado por el famoso videojuego Minecraft.

Modelo OSI

El modelo OSI (Open System Interconnection) organiza conceptualmente a las familias de protocolos de red en capas de red específicas. Este Sistema de Interconexión Abierto tiene por objetivo establecer un contexto en el cual basar las arquitecturas de comunicación entre diferentes sistemas. A continuación, listamos algunos de los protocolos de red más conocidos, según las capas del modelo OSI:

Protocolos de la capa 1 - Capa física

- USB: Universal Serial Bus
- Ethernet: Ethernet physical layer
- DSL: Digital subscriber line
- Etherloop: Combinación de Ethernet and DSL
- Infrared: Infrared radiation
- Frame Relay
- SDH: Jerarquía digital síncrona
- SONET: Red óptica sincronizada

Protocolos de la capa 2 - Enlace de datos

- DCAP: Protocolo de acceso del cliente de la conmutación de la transmisión de datos
- FDDI: Interfaz de distribución de datos en fibra
- HDLC: Control de enlace de datos de alto nivel
- LAPD: Protocolo de acceso de enlace para los canales
- PPP: Protocolo punto a punto
- STP (Spanning Tree Protocol): protocolo del árbol esparcido
- VTP VLAN: trunking virtual protocol para LAN virtual
- MPLS: Conmutación multiprotocolo de la etiqueta

Protocolos de la capa 3 - Red

- ARP: Protocolo de resolución de direcciones
- BGP: Protocolo de frontera de entrada
- ICMP: Protocolo de mensaje de control de Internet
- IPv4: Protocolo de internet versión 4
- IPv6: Protocolo de internet versión 6
- IPX: Red interna del intercambio del paquete
- OSPF: Abrir la trayectoria más corta primero
- RARP: Protocolo de resolución de direcciones inverso

Protocolos de la capa 4 - Transporte

- IL: Convertido originalmente como capa de transporte para 9P
- SPX: Intercambio ordenado del paquete
- SCTP: Protocolo de la transmisión del control de la corriente
- TCP: Protocolo del control de la transmisión
- UDP: Protocolo de datagramas de usuario
- iSCSI: Interfaz de sistema de computadora pequeña de Internet iSCSI
- DCCP: Protocolo de control de congestión de datagramas

Protocolos de la capa 5 - Sesión

- NFS: Red de sistema de archivos
- SMB: Bloque del mensaje del **servidor**
- RPC: Llamada a procedimiento remoto
- SDP: Protocolo directo de sockets
- SMB: Bloque de mensajes del servidor

- SMPP: Mensaje corto punto a punto

Protocolos de la capa 6- Presentación

- TLS: Seguridad de la capa de transporte
- SSL: Capa de conexión segura
- XDR: Extenal data representation
- MIME: Multipurpose Internet Mail Extensions

Protocolos de la capa 7 - Aplicación

- DHCP: Protocolo de configuración dinámica de host
- DNS: Domain Name System
- HTTP: Protocolo de transferencia de hipertexto
- HTTPS: Protocolo de transferencia de hipertexto seguro
- POP3: Protocolo de oficina de correo
- SMTP: protocolo de transferencia simple de correo
- Telnet: Protocolo de telecomunicaciones de red

Bibliografía

https://www.kionetworks.com/blog/data-center/protocolos-de-comunicaci%C3%B3n-de-redes

https://www.redeszone.net/tutoriales/internet/protocolos-basicos-redes/

https://sites.google.com/site/investigacionesitlm/home/historia-y-origen-de-las-redes