Servicios de Red

• DHCP

DHCP significa protocolo de configuración de host dinamico. Es un protocolo que permite que un equipo conectado a una red pueda obtener su configuración (configuración de red) en forma dinámica. Sólo tiene que especificarle al equipo, mediante DHCP, que encuentre una dirección IP de manera independiente. El objetivo es simplificar la administración de la red.

El protocolo DHCP sirve principalmente para distribuir direcciones IP en una red, pero se diseñó como complemento del protocolo BOOTP (Protocolo Bootstrap) que se utiliza cuando se instala un equipo a través de una red (BOOTP se usa junto con un servidor TFTP donde el cliente encontrará los archivos que se cargarán y copiarán en el disco duro). Un servidor DHCP puede devolver parametros BOOTP o la configuración especifica a un determinado host

• DNS

Domain Name System (Sistema de nombres de dominio) es un sistema de nomenglatura jerárquico para computadoras, servicios o cualquier recurso conectado a internet o a una red privada. Este sistema asosia información variada con nombres de dominio asignados a cada uno de los participantes. Su función más importante, es traducir (resolver) nombres intangibles para las personas en identificadores binarios asosiados con los equipos conectados a la red, esto con el proposito de poder localizar y direccionar estos equipos mondialmente.

El servidor DNS utiliza una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet. Aunque como base de datos el DNS es capaz de

asociar diferentes tipos de información a cada nombre, los usos mas comunes son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico de cada dominio.

La asignación de nombres a direcciones IP es la función mas conocida de los protocolos DNS. Por ejemplo, si la dirección IP del sitio FTP de prox.mx es 200.64.128.4, la mayoría de la gente llega a este equipo especificando ftp.prox.mx y no la dirección IP. Ademas de ser facil de recordar el nombre es mas fiable. La dirección numérica podría cambiar por muchas razones, sin que tenga que cambiar de nombre.

Inicialmente, el DNS nació de la necesidad de recordar fácilmente los nombres de todos los servidores conectados a internet. En un inicio, SRI (ahora SRI International) alojaba un archivo llamado HOSTS que contenía todos los nombres de dominio conocidos. El crecimiento explosivo de la red causó que el sistema de nombres centralizado en el archivo de hosts no era practico y en 1983, Paul V. Mockapetris publico RFC 882 y RFC 883 definiendo lo que hoy en día ha evolucionado hacia el DNS moderno.

- **SSH**

SSH secure Shell (intérprete de órdenes segura) es el nombre del protocolo que sirve para acceder a máquinas remotas a través de una red. Permite manejar por completo el equipo mediante un intérprete de comandos, también puede redirigir el tráfico de X para poder ejecutar programas gráficos si se tiene un servidor X corriendo. Además de la conexión a otros dispositivos, SSH permite copiar datos de forma segura (Tanto archivos sueltos como simulaciones de sesiones FTP cifradas), gestionar claves RSA para

no escribir claves al conectar a los dispositivos y pasar los datos de cualquier otra aplicación por un canal seguro utilizando el protocolo de SSH

• FTP y TFTP

- TFTP, Trivial File Transfer Protocol (Protocolo de transferencia de archivos trivial) es un protocolo de transferencia simple semejante a FTP que a menudo se utiliza para transferir archivos pequeños entre computadoras en una red, como cuando un terminal o un cliente ligero arranca desde un servidor de red.
Algunas características de TFTP:
  - Utiliza UDP (Puerto 69) como protocolo de transporte
  - No puede listar el contenido de los directorios
  - No existen mecanismos de autenticación o cifrado
  - Se utiliza para leer y escribir archivos de un servidor remoto.
  - Soporta tres modos diferentes de transferencia, "netascii", "octet" y "mail", de los cuales los dos primeros corresponden a los modos "ascii" e "imagen" del protocolo FTP.

- FTP File transfer protocol (Protocolo de transferencia de archivos) es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP (Transmission Control Protocol), basado en la arquitectura cliente-servidor. Desde un equipo cliente se puede conectar a un servidor para descargar archivos desde él o para enviarle archivos, independientemente del sistema operativo utilizado en cada equipo.

El servicio FTP es ofrecido por la capa de aplicación del modelo de capas de red TCP/IP al usuario, utilizando normalmente el puerto de red 20 y el 21. Un problema básico de FTP es que está pensado para ofrecer la máxima velocidad en la conexión pero, no la máxima seguridad, ya que todo el

intercambio de información, desde el login y password del usuario en el servidor hasta la transferencia de cualquier archivo, se realiza en texto plano sin ningún tipo de cifrado, con lo que un posible atacante puede capturar este tráfico, acceder al servidor y/o apropiarse de los archivos transferidos. Para solucionar ese problema aplicaciones como scp y sftp son de gran utilidad incluido SSH que permite transferir archivos cifrando todo el tráfico.

- **WWW: HTTP y HTTPS**

HTTP, Hypertext Transfer Protocol (Protocolo de transferencia de hipertexto) que es un protocolo de comunicación que hace posible la circulación de información a través de la World Wide Web (www). En HTTPS la letra "S" significa Secure si una pagina de internet inicia por "https://" quiere decir que podría no ser segura. HTTPS es una forma de dar seguridad a los datos.

- **NFS**

El Network File System (Sistema de archivos de red) es un protocolo de nivel de aplicación, según el Modelo OSI. Es utilizado para sistemas de archivos distribuido en un entorno de red de computadoras de área local. Posibilita que distintos sistemas conectados a una misma red accedan a ficheros remotos como si se trataran de locales. Originalmente fue desarrollado en 1984 por Sun Microsystems, con el objetivo de que sea independiente de la máquina, el sistema operativo y el protocolo de transporte, esto fue posible gracias a que está implementado sobre los protocolos XDR y ONC RPC. El protocolo NFS está incluido por defecto en los sistemas operativos UNIX y la mayoría de distribuciones Linux.

-DLAP

El protocolo ligero de acceso a directorios se utiliza para acceder a la información que está almacenada de forma centralizada en una red. Este protocolo se utiliza a nivel aplicación para acceder a los servicios de directorio remoto.

Cuando el cliente LDAP se conecta con el servidor, podrá realizar dos acciones básicas, bien consultar y obtener información del directorio o modificarla. Si un cliente quiere modificar la información del directorio tiene permisos de administrador o no. Entonces, la información y gestión de un directorio DLAP se podrá hacer de forma remota. El puerto de conexión para el protocolo DLAP es el TCP 389, aunque por supuesto, se podrá modificar por el usuario y establecerlo en el que desee si es así se lo indica al servidor.

- SMTP, POP, IMAP, SASL

- SMTP, Simple Mail Transfer Protocol (Protocolo para la transferencia simple de correo electrónico), es un protocolo de red utilizado para el intercambio de mensajes de correo electrónico entre compotadoras u otros dispositivos fue definido en el RFC 2821 y es un estándar oficial de internet.

El funcionamiento de este protocolo se da en línea, de manera que opera en los servicios de correo electrónico. Sin embargo, este protocolo posee algunas limitaciones en cuanto a la recepción de mensajes en el servidor de destino (cola de mensajes recibidos). Como alternativa a esta limitación se asocia normalmente a este protocolo con otros, como el POP o IMAP, otorgando a SMTP la tarea específica de enviar correo, y recibirlos empleando los otros protocolos antes mencionados.

- POP: En informática se utiliza el Post Office Protocol (Protocolo de oficina postal) en clientes locales de correo para obtener los mensajes de correo electrónico almacenados en un servidor remoto. Es un protocolo de nivel de aplicación en el modelo OSI.

POP3 está diseñado para recibir correo, no para enviarlo; le permite a los usuarios con conexiones intermitentes o muy lentas (como las 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.

- IMAP: Internet Message Access Protocol (Protocolo de acceso a mensajes de internet) es un protocolo de aplicación que permite el acceso a mensajes almacenados en un servidor de Internet. Mediante IMAP se puede tener acceso al correo electrónico desde cualquier equipo que tenga una conexión a internet. IMAP fue diseñado como una alternativo a POP por Mark Crispin en el año 1986. Fundamentalmente, los dos protocolos les permiten a los clientes de correo acceder a los mensajes almacenados en un servidor de correo.

- SASL: Simple Authentication and Security Layer (capa de seguridad y autenticación simple) es un Framework para autenticación y autorización en protocolo de Internet. Separa los mecanismos de autenticación de los protocolos de la aplicación permitiendo, en teoría, a cualquier protocolo de aplicación que use SASL usar cualquier mecanismo de autenticación

soportado por SASL. A pesar de que mediante SASL sólo se maneja la autenticación (y se requieren otros mecanismos como TIS, para cifrar el contenido que se transfiere), SASL proporciona medios para un uso negociado del mecanismo elegido. Las especificaciones originales de SASL fueron editadas por John Meyers en el RFC 2222. Este hecho fue obsoleto por el RFC 4422.

- Proxy

Un proxy es un equipo informático que hace de intermediario entre las conexiones de un cliente y un servidor de destino, filtrando todos los paquetes entre ambos. Siendo tú el cliente, esto quiere decir que el proxy recibe tus peticiones de acceder a una o otra página, y se encarga de transmitírselo al servidor web para que esta no sepa que los estáis haciendo tú.

De esta manera, cuando vayas a visitar una página web, en vez de establecer una conexión directa entre tu navegador y ella puedes dar un rodeo y enviar y recibir los datos a través de este proxy. La página que no se visite no conocerá la IP si no la del proxy y podrás hacerte pasar por un usuario de un país distinto.

Integrantes:

Domínguez Cruz Carlos Asahel
Mejía Camacho Edgar Daniel
Nolasco Amorador Eduardo
Rosales Bernal David