

Implementación de red de datos

INFORME DE DESARROLLO

LITIUM S.A.

Sede San Salvador de Jujuy

Micaela Brizuela

Frank Matías Flores Rea

Ulises Alejandro Larrabe

26/10/2024

TABLA DE CONTENIDOS

1. Introducción.....	3
1.1 Marco teórico.....	3
2. Diseño de las capas.....	3
2.1 Servicios.....	3
2.2 Protocolos.....	3
2.3 Seguridad.....	4
3. Configuración dinámica de host DHCP.....	4
4. Descripción de servicios de capa de aplicación implementados.....	5
4.1 Resolución de nombres DNS.....	5
4.2 World wide web (www).....	6
4.3 Correo.....	7
5. Emulación.....	8
5.1 Diseño del esquema:.....	8
6. Conclusiones.....	9
7. Dificultades encontradas.....	9
8. Dispositivos con IP estática.....	10

1. INTRODUCCIÓN

El presente proyecto tiene como objetivo diseñar e implementar una red para una sede ubicada en San Salvador De Jujuy de la empresa Litium S.A. Esta sede tiene dos pisos.

En el primero, se encuentra el Departamento Comercial, Operaciones mineras y el Departamento de Logística y Transporte. En el segundo Piso se encuentra el Departamento de Administración y el Cuarto de servidores.

1.1 MARCO TEÓRICO

En este informe se detallan conceptos vistos en clase como la pila de protocolos TCP/IP (como es el caso de los protocolos HTTP, POP3 y TCP), servicios de capa de aplicación (multiplexación, envío de correo, resolución de hosts), concepto de diseño de red (switches, hosts, concepto de Intranet), y el uso de cisco Packet Tracer.

2. DISEÑO DE LAS CAPAS

2.1 SERVICIOS

Se implementan servicios de capas tales como la asignación de IP dinámicas, la multiplexación de datos, el control de flujo, la visualización de contenido web, entrada y salida de correo, y la resolución de nombres de dominios, entre otros.

2.2 PROTOCOLOS

Dentro de los protocolos que se utilizan para el trabajo, podemos encontrar:

- Protocolo UDP: Es un protocolo no orientado a conexión, lo que significa que no se puede garantizar que los datos se envíen correctamente. Es utilizado especialmente para enviar las consultas (también llamadas queries) de DNS, como también para escuchar y responder las consultas del servidor DHCP.
- Protocolo TCP: Es un protocolo orientado a conexión, lo que significa que se garantiza la entrega de paquetes mediante un establecimiento de conexión previa. Además de también garantizar el orden correcto y la corrección de errores, permitiendo reenviar segmentos que se perdieron en el camino. Es utilizado en el servicio DNS para la comunicación entre servidores primarios y secundarios, y en HTTP y HTTPS para tener una entrega fiable de datos.
- Protocolo SMTP: El protocolo SMTP (Simple Mail Transfer Protocol) se encarga de enviar los mails al destinatario. Es un protocolo basado en el concepto de push (empuje). Toma un mensaje y se conecta con un servidor remoto para transferirlo.
- Protocolo IMAP: El protocolo IMAP (Internet Message Access Protocol) se encarga de la visualización de los mails para los usuarios. La idea en que se basa IMAP es que

el servidor de correo electrónico mantenga un depósito central al que el usuario puede acceder desde cualquier máquina.

- Protocolo POP3: Este protocolo es una versión anterior al protocolo IMAP. Por lo general, el correo se descarga de manera local para ser visualizado en un agente de usuario, en vez de permanecer en el servidor de correo. Lo que significa que si la computadora se descompone, cabe la probabilidad de perder todo el correo electrónico almacenado allí de manera permanente.
- Protocolo HTTP/HTTPS: Utilizado para transferir archivos del formato HTML y su versión de transferencia de datos cifrados.
- Protocolo DNS: Utilizados en la traducción de nombres de hosts (usados por humanos) y direcciones IP (usados por computadoras).
- Protocolo DHCP: Utilizados en la red para asignar una dirección a IP a cualquier dispositivo de red que necesite comunicarse en la red con una IP.

2.3 SEGURIDAD

Para garantizar la seguridad de los datos en la red de Litium SA, se ha implementado un firewall encargado de manejar los accesos de la intranet del sistema administrativo. El firewall funciona como una barrera que permite el acceso únicamente a usuarios autorizados y deniega el acceso de cualquier conexión que no provenga de la red del Departamento Administrativo. Además, en este servidor se configuró el acceso solo a través de conexiones seguras mediante el uso del protocolo HTTPS que se establecen a través del puerto 443.

Para el resto de los servidores, se bloquearon los puertos de los servicios no utilizados como práctica estándar de seguridad informática.

Para el establecimiento de conexiones inalámbricas, se utilizaron conexiones seguras WPA-PSK con encriptación AES en los puntos de acceso (AP) ubicados en cada piso de la sede. La conexión WPA-PSK con cifrado AES utiliza los protocolos seguros llamados EAP y TKIP para redes Wi-fi que piden una clave única a cada usuario que debe ser encriptada para no ser robada por ataques externos.

3. CONFIGURACIÓN DINÁMICA DE HOSTS DHCP.

DHCP (Dynamic Host Configuration Protocol) es un protocolo de red que permite a los nodos de una red IP obtener sus parámetros de configuración automáticamente. Este protocolo sirve para ahorrar una cantidad considerable de tiempo para los administradores de red, que al no tener que configurar IPs estáticas a cada dispositivo que pueda ser agregada con DHCP, se puede evitar el tener IPs duplicadas. Se utiliza el modelo cliente-servidor, utilizando el protocolo de capa 4 UDP en el puerto 68, respondiendo a las peticiones en el puerto 67.

Además, este protocolo cuenta con 3 métodos de asignación de direcciones IP:

- Asignación manual o estática: Asigna una dirección IP fija a una máquina determinada. Se hace manualmente o por MAC Address.
- Asignación automática: Asigna una dirección IP de forma permanente a una máquina cliente la primera vez que hace la solicitud al servidor DHCP.
- Asignación dinámica: Se determina un rango de direcciones IP y cada computadora está configurada para solicitar su dirección IP al servidor. El procedimiento usa un concepto de un intervalo de tiempo controlable.

En el trabajo lo configuramos para poner IPs automáticas a partir de la IP 192.168.145.81, con un tamaño máximo de hasta 45 dispositivos conectados al mismo tiempo. Nos decidimos en implementar este rango porque la próxima IP disponible, luego de haber asignado todas las IPs estáticas, es la 192.168.145.81, y la última IP disponible para hosts que se obtiene de la subred con la máscara 255.255.255.192 es 192.168.145.126, ya que la IP 192.168.145.127 está reservada para broadcast.

4. DESCRIPCIÓN DE SERVICIOS DE CAPA DE APLICACIÓN IMPLEMENTADOS.

4.1 RESOLUCIÓN DE NOMBRES DNS

DNS (Domain Name System) es una base de datos distribuida que permite realizar una relación entre nombres de máquinas y direcciones IP. En otras palabras, es un sistema utilizado en Internet cuya función principal es traducir nombres de dominios de red en direcciones IP. Esto es útil porque al asignar a cada máquina (u host) una IP y un nombre, un usuario que quiere acceder a otros hosts, no debe memorizar múltiples cadenas de números, sino conocer sus nombres de dominio.

Algunas de las características del DNS son:

- Se basa en servidores de nombres distribuidos geográficamente.
- Utiliza el puerto 53.
- Los protocolos de transporte que utiliza son UDP (para realizar la consultas o queries DNS) y TCP (para la comunicación entre servidores primarios y secundarios).
- Hay uno o varios servidores DNS secundarios (o backups) independientes del primario, que obtienen la información de la base de datos a partir del primario (información que normalmente se actualiza cada 3 horas).

A su vez, DNS presenta una serie de registros especiales:

- Registros SOA (Start Of Authority): proporciona el nombre de la fuente primaria de información sobre la zona del servidor de nombres, la dirección de correo electrónico de su administrador, un número de serie único, varias banderas y temporizadores.

- Host Origen: Host donde se mantiene el archivo

- Correo electrónico: Se refiere al responsable de la base de datos del DNS. La arroba (@) se sustituye por un punto (.), debido a que la arroba (@) representa el dominio raíz de la zona.
- Número de serie: La versión de ese archivo. Aumenta cada vez que el archivo cambia.
- Tiempo de actualización: Tiempo que espera un servidor de nombres secundario para ver si el archivo ha cambiado, y por lo tanto, pedir una transferencia de zona.
- Tiempo de reintento: Tiempo que espera un servidor de nombres secundario para iniciar una nueva transferencia de zona en el caso de que fallase este procedimiento.
- Tiempo de caducidad: Tiempo que el servidor de nombres secundario intentará descargar una zona. Cuando pase, se rechaza la información antigua.
- Tiempo de vida: Tiempo en el que el servidor de nombres mantiene la caché de cualquier registro del recurso de este archivo en base de datos.
- Registros NS: El registro NS (Name Server) contiene los servidores de nombre de ese dominio, lo que permite que otros servidores de nombre vean los nombres de su dominio.
- Registros A: Los registros de dirección A (Address) asocian nombres de host a direcciones IP dentro de una zona. Son los más numerosos dentro del archivo
- Registros CNAME: Estos registros son llamados también alias, si bien son conocidos como entradas de nombre canónico (CNAME, Canonical Name). Su uso más común es utilizar para apuntar a un único host más de un nombre.
- Registros MX: El registro MX es el registro de Intercambio de correo (Mail eXchange). Indica que host se encarga del procesamiento del correo electrónico de ese dominio.

En la emulación usamos tres DNS, uno para cada una de las zonas: root (DNS resolver), litium.com.ar y logistica.litium.com.ar. Las últimas dos tienen sus respectivos DNS primarios.

4.2 WORLD WIDE WEB (WWW)

Unos de los servicios implementados es el alojamiento de páginas web en los servidores dedicados, utilizamos los protocolos HTTP (HyperText transfer Protocol) y HTTPS (HyperText transfer Protocol Secure). Estos protocolos permiten la comunicación entre distintas máquinas basándose en el modelo cliente-servidor. El protocolo HTTP se utiliza principalmente para visualizar contenido sin mecanismos de seguridad y proporciona servicios a través del puerto 80. Por su parte, el HTTPS es una versión segura del protocolo HTTP que protege al usuario y mantiene la integridad de los datos a través de métodos de cifrado. Los servicios HTTPS se acceden mediante el puerto 443.

Para cumplir con los servicios solicitados, se requirieron 4 servidores web en la sede de San Salvador de Jujuy, en donde 3 servidores se encuentran ubicados en el cuarto de

servidores del 2º Piso y el servidor restante que es dedicado al Departamento de Logística y Transporte ubicado en el primer piso. Utilizamos el protocolo HTTP para la página principal de Litium S.A. (www.litium.com.ar), la página web del Departamento de Logística y Transporte (www.logistica.litium.com.ar) y además se configuró el protocolo HTTPS para el acceso a al sistema de gestión de logística (www.sistema.logistica.litium.com.ar) y por último para la Intranet del sistema administrativo (www.administracion.litium.com.ar).

4.3 CORREO

Los protocolos encargados de que los servidores de correo funcionen correctamente son SMTP(Simple Mail Transfer Protocol) y POP3(Post Office Protocol) o IMAP.

El protocolo SMTP es el que se encarga de la transferencia de los correos lleguen a destinatario, este protocolo se asegura de que el correo se traslade correctamente a través de la red y llegue al servidor de correo del destinatario

Mientras que los protocolos POP e IMAP son los encargados de la visualización de los mails de los usuarios. El POP3 permite que los clientes se puedan descargar sus correos directamente del servidor y tenerlos en sus máquinas, haciendo que estos se borren del servidor después de la descarga. En cambio, con el protocolo IMAP los correos se mantienen sincronizados en el servidor de correo, permitiendo que los correos se puedan visualizar en diferentes dispositivos.

En el servidor de correo de Litium SA fue configurado con los Protocolos SMTP y POP3 para el envío, la recepción y la visualización de los correos. Todas las cuentas de correos se configuró siguiendo el formato usuario@litium.com.ar y se crearon varios usuarios distribuidos entre los siguientes departamentos de la sede de San Salvador de Jujuy para simular el funcionamiento:

- Departamento de Logística y Transporte: micaela@litium.com.ar
- Departamento Comercial: ulises@litium.com.ar
- Operaciones Mineras: matias@litium.com.ar

6. CONCLUSIONES

Mediante este trabajo pudimos poner a prueba todo lo que hemos aprendido en las últimas clases. Lo desafiante fue el haber tenido que configurar todos los servicios aprendidos en un solo trabajo, y se tuvo que tener en cuenta muchos aspectos. A su vez, tuvimos la oportunidad de indagar en búsqueda de información adicional para poder completar las consignas adecuadamente, como el uso de un firewall, el concepto de interredes y el cómo poder configurar conexiones inalámbricas. Gracias a este trabajo, cada integrante se pudo dar cuenta que temas ha asimilado y en cuáles tiene que reforzar el conocimiento.

7. DIFICULTADES ENCONTRADAS

Una de las dificultades encontradas fue al momento de probar la delegación de la zona DNS para mostrar la página web www.litium.com.ar. Ya que se había configurado la zona DNS del mismo, y se hizo la prueba conectando una PC a la red y solicitando dicha página. Sin embargo, la página no se mostraba, y se empezó a revisar cada dato puesto tanto en la delegación a la zona del DNS de la página, en el DNS de la zona "com.ar" como en el mismo DNS de la zona "litium.com.ar" y no se encontraron errores. Por lo tanto, se recurrió al modo simulación del emulador, aplicando el filtro para solo ver las solicitudes DNS, y así poder visualizar donde se perdía dicha solicitud. Luego de ver la simulación, nos percatamos que la solicitud DNS se perdía luego de llegar a la zona DNS del root server, y ahí nos dimos cuenta de que, si bien este DNS hacía la delegación al DNS "com.ar", la IP a la que apuntaba era distinta a la IP que tenía el DNS "com.ar". Una vez arreglado este error entre IPs, la página se mostró directamente en el PC.

8. DISPOSITIVOS CON IP ESTÁTICA

FQDN	FUNCIONES	IP	MÁSCARA	UBICACIÓN
Router Borde	Router Litium SA	192.168.145.65	255.255.255.192	2° Piso -Cuarto de Servidores
DNS Resolver	DNS Resolver	192.168.145.66	255.255.255.192	2° Piso -Cuarto de Servidores
dns1.litium.com.ar	DNS secundario Logística y Transporte	192.168.145.67	255.255.255.192	2° Piso -Cuarto de Servidores
www.litium.com.ar	Web Principal de Litium SA	192.168.145.68	255.255.255.192	2° Piso -Cuarto de Servidores
dns1.logistica.litium.com.ar	DNS Primario Logística y Transporte	192.168.145.69	255.255.255.192	1° Piso - Dep. de Logística y transporte
logistica.litium.com.ar	Web Logística y transporte	192.168.145.70	255.255.255.192	1° Piso - Dep. de Logística y transporte
dns2.logistica.litium.com.ar	DNS secundario Logística y Transporte	192.168.145.71	255.255.255.192	1° Piso - Dep. de Logística y transporte
correo.litium.com.ar	Servidor de correo	192.168.145.72	255.255.255.192	2° Piso-Cuarto de Servidores
www.sistema.logistica.litium.com.ar	Web acceso de gestión logística	192.168.145.73	255.255.255.192	2° Piso-Cuarto de Servidores
www.administracion.litium.com.ar	Web de sistema Administrativo	192.168.145.74	255.255.255.192	2° Piso -Cuarto de Servidores
dhcp.litium.com.ar	DHCP	192.168.145.75	255.255.255.192	2° Piso -Cuarto de Servidores
PC1 Departamento Administración	PC con Acceso a Intranet	192.168.145.76	255.255.255.192	2° Piso - Departamento Administración

PC2 Departamento Administración	PC con Acceso a Intranet	192.168.145.77	255.255.255.192	2° Piso - Departamento Administración
PC3 Departamento Administración	PC con Acceso a Intranet	192.168.145.78	255.255.255.192	2° Piso - Departamento Administración
PC4 Departamento Administración	PC con Acceso a Intranet	192.168.145.79	255.255.255.192	2° Piso - Departamento Administración
dns2.litium.com.ar	DNS Secundario litium.com.ar	192.168.145.80	255.255.255.192	2° Piso-Cuarto de Servidores