

Laboratorio No. 2 - Alistamiento S.O, Shell y Software de apoyo en redes

Objetivo

- Continuar la instalación de sistemas operativos base.
- Conocer el modo de operación de herramientas de redes.
- Conocer sobre administración de sistemas operativos usando programas en Shell

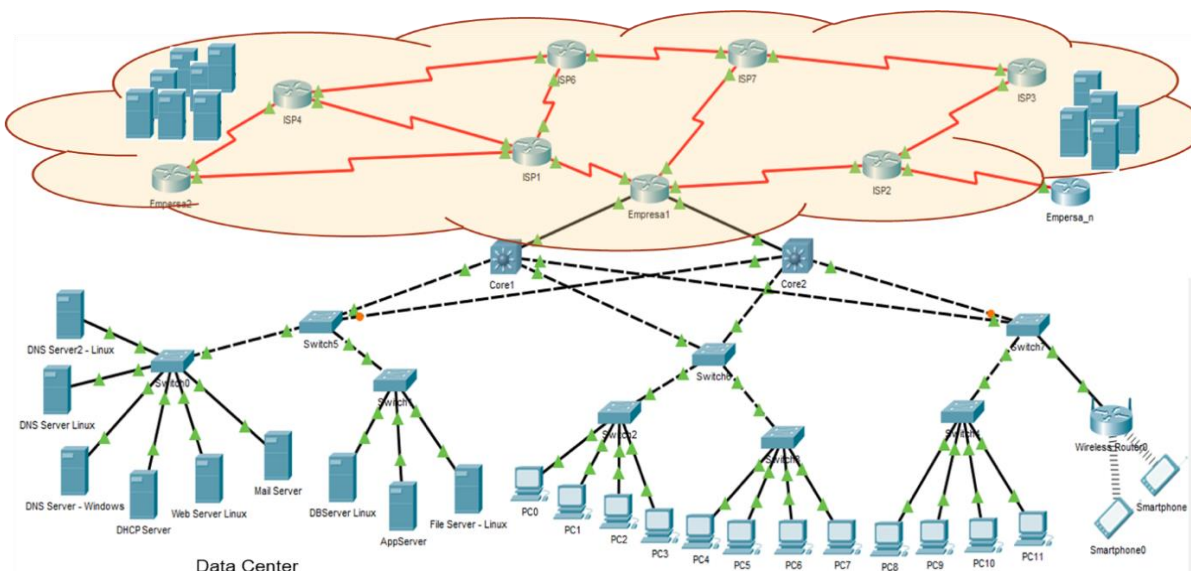
Herramientas a utilizar

- Computadores Laboratorio de Informática
- Acceso a Internet
- Software de virtualización
- Imágenes de Sistemas Operativos
- Packet tracer
- Wireshark

Introducción

Como ya hemos hablado, una empresa normalmente cuenta con varios servicios de infraestructura TI. En ella se encuentran estaciones de usuario alámbricas e inalámbricas y servidores (físicos y virtualizados), todos estos conectados a través de switches (capa 2 y 3), equipos inalámbricos y routers que lo conectan a Internet. También es común contar con infraestructuras en la nube desde donde se provisionan recursos según las necesidades de la organización. Dentro de los servidores se pueden encontrar servicios web, DNS, correo, base de datos, almacenamiento y aplicaciones, entre otros.

A continuación se presenta una posible configuración:



Experimentos

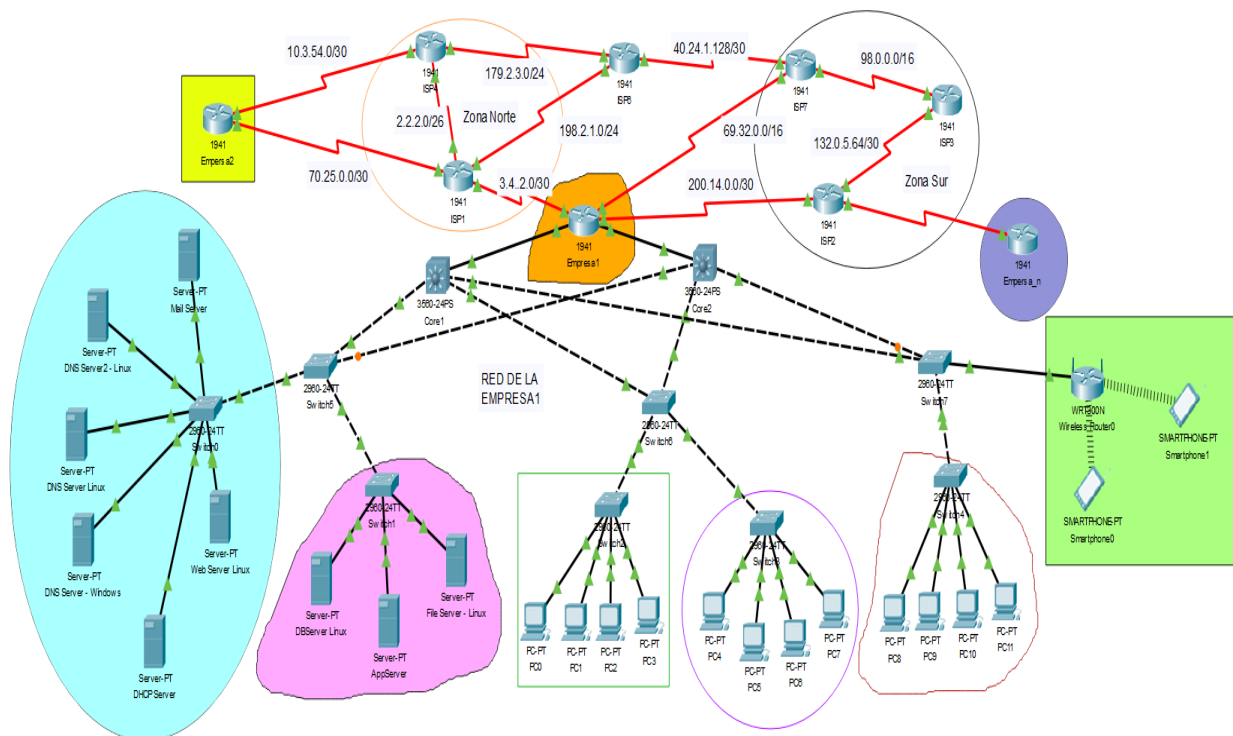
Para construir una infraestructura tecnológica como la presentada en el dibujo anterior, se debe contar con computadores y servidores, los cuales tienen instalado un sistema operativo, también es importante conocer la operación de los mismos desde el punto de vista del administrador del sistema, así como apoyar procesos de automatización. A continuación, se plantean diferentes actividades enfocadas a conocer dicha estructura.

1. Conociendo Packet Tracer

- Responda las siguientes preguntas
 1. ¿Qué versión de Packet Tracer se encuentra instalada en el Lab?,
 2. A través de la plataforma de Cisco inscribise en el curso Introduction to Packet Tracer v1.1. muestre con un video hecho por el grupo un resumen del curso. Máximo 5 min.
 3. Realice la evaluación del curso y tome un pantallazo del resultado de la evaluación
- Usando Packet Tracer haga el diagrama de red que se presenta en la página siguiente.

Nota:

- No tenga en cuenta los colores de los puntos que aparecen en los enlaces (los enlaces son las líneas de conexión entre dispositivos. Más adelante serán importantes los colores de dichos puntos, pero en su momento los revisaremos).
- Las conexiones o enlaces que se presentan en el diagrama son:
 - Las de color negro corresponden a cables Ethernet (Ethernet, FastEthernet o GigaEthernet).
 - ¿Qué significan las conexiones negras continuas?
 - ¿Qué significan las conexiones negras discontinuas?
 - Las de color rojo son seriales (Conexiones típicamente WAN). Al dibujarlas en packet tracer aparecerán un poco diferente respecto al dibujo.



2. Siguiendo mensajes con Packet tracer

- Seleccione dos servidores ubicados en el ovalo azul agua marina (izquierda-abajo en el dibujo). Póngales la siguiente configuración
 - Servidor 1
 - IP 44.87.10.100
 - Máscara: 255.255.255.0
 - Servidor 2
 - IP 44.87.10.231
 - Máscara 255.255.255.0
- Entre en el modo simulación con que cuenta Packet Tracer y revise los PDUs por capas (Todavía no hemos visto el significado de lo que cada uno tiene, pero vea que existen y que cada capa adiciona información a los datos de usuario). Para esto use la siguiente información como guía

Run the simulation and capture the traffic¹.

- In the far lower right of the PT interface is the toggle between Realtime and Simulation mode. Click on Simulation mode.
- Click in the Edit filters button and select only ICMP.
- Click in PCA. Choose the Desktop tab. Open the Command Prompt. Enter the command ping IP_PCB). Pressing the Enter key will initiate four ICMP echo requests. Minimize the PC configuration window. Two packets appear in the Event List, the first ICMP echo request and an ARP request needed to resolve the IP address of the server to its hardware MAC address.
- Click the Auto Capture / Play button to run the simulation and capture events. Click OK when the "No More Events" message is reached.

- Revise el contenido de los paquetes capturados. Vea cómo se van construyendo los PDU de cada capa

En la red real

Realice las siguientes pruebas usando la herramienta Wireshark.

1. Usando Wireshark

Wireshark es una herramienta multiplataforma utilizada para realizar análisis sobre paquetes de red². La utilizaremos dentro del curso para observar, en tiempo real, lo datos que pasan por la red y la manera de operación de los diferentes protocolos que estudiaremos. Por tal razón

- Ejecute Wireshark en el computador en el que está trabajando
- Revise los siguientes videos o use de apoyo los laboratorios 3.4.1.1 y 3.4.1.2 del curso Introduction to network del material para preparación para la certificación CCNA.
 - Wireshark Tutorial for Beginners.
<https://www.youtube.com/watch?v=TkCSr30UojM>.
 - Wireshark Tutorial for Beginners 2017 - Overview of the environment.
<https://www.youtube.com/watch?v=6LGw31TsP6E>.
 - Wireshark demo (simple http).
<https://www.youtube.com/watch?v=PYoXowOCppc>.

¹ Basado en 2.6.2: Using Packet Tracer to View Protocol Data Units. CCNA1

² <https://www.welivesecurity.com/la-es/2013/01/28/uso-filtros-wireshark-para-detectar-actividad-maliciosa/>

- ¿Qué es Wireshark?
- ¿Cómo generar filtros?, ¿Para qué se usan?. De unos ejemplos
- Realice una consulta web al link <http://www.ideam.gov.co/> y capture el tráfico generado (para eso, ingrese al browser, inicie la captura con Wireshark y visite a la página indicada, termine la captura). Finalmente, pare la captura.
- Analice los datos encontrados en uno de los paquetes capturados. Mire el encapsulamiento y presente capturas del mismo (Use el paquete que contiene una de las solicitudes GET que se realizan).

2. Tarjetas de red

Conozca las tarjetas de red de varios dispositivos. Para esto, busque la información de las tarjetas de red de los computadores de la Escuela asignados a su grupo de laboratorio y de al menos 3 equipos diferentes (computadores, portátiles celulares, tablets, consolas de juegos, etc.) de cada miembro de su equipo de trabajo.

Incluya información como Proveedor, modelo, velocidad, MAC Address, IPv4 Address, IPv6 Address, cantidad de bytes transmitidos y recibidos. En el caso de tarjetas inalámbricas Velocidad de conexión, SSID

Ahora, revise la misma información para 2 de sus máquinas virtuales y compare la información obtenida con la información de las máquinas anfitrionas.

Nota: Puede usar como guía el laboratorio 4.2.4.5 del curso Introduction to network del material para preparación para la certificación CCNA.

Software Base

De la infraestructura también se requiere contar con programas que apoyen la administración de diferentes actividades del sistema operativo. Vamos a realizar actividades que les ayuden a entender un poco el sistema operativo y la gestión de usuarios.

1. Shell programming- Unix

Usando una máquina virtual de Linux Slackware y una de FreeBSD y desarrolle las siguientes aplicaciones (recuerde documentar su código).

Comandos LS y PWD

- Use el comando pwd, ¿qué obtiene?
- Use el comando ls, ¿qué obtiene?
- ¿Cómo puede utilizar el comando ls para obtener información adicional como por ejemplo fecha y permisos?
- ¿Cómo puede utilizar el comando ls para listar los archivos ocultos de un directorio?
- ¿Cómo puede utilizar el comando ls para listar los archivos ordenados por fecha de modificación?
- ¿Cómo mostrar el contenido de un directorio en donde uno no se encuentra ubicado usando el comando ls?
- Cuando un directorio contiene muchos archivos, ¿cómo hacer para mostrarlo por páginas? (use la ruta /etc)
- ¿Cómo listar los archivos que comienzan con la letra m?
- ¿Qué otros ordenamientos se pueden realizar?
- ¿Qué es una expresión regular? y ¿en dónde se puede usar dentro del Shell?

Comando ECHO

- ¿Cuál es el objetivo del comando ECHO?
- Variable PATH: ¿Para qué sirve la variable PATH?, use el comando ECHO para mostrar su contenido.
- ¿Cómo añadir datos al PATH?
- ¿Qué son las variables de ambiente?, de ejemplos de algunas de ellas

Ejecución automática de una secuencia de comandos, variables y condicionales

Escriba un programa Shell que:

- Limpie la pantalla
- Pida un nombre de archivo y una cadena
- Cuente la cantidad de líneas en donde se encuentra la cadena indicada
- Imprima el mensaje “El número de líneas del archivo xxxx que contienen la cadena yyy es:” y el número de líneas encontrados.

Escriba un programa Shell que:

- Limpie la pantalla
- Busque un archivo que termine con las letras indicadas por el usuario.
- Dentro de ese archivo busque una palabra dada por el usuario y cuente las repeticiones de dicha palabra.
- Muestre las rutas en donde se encuentra dicho archivo, las líneas en donde aparece la palabra buscada y al final el número de veces que se repite dicha palabra.
- La ejecución sería del estilo
\$ buscar_palabra.sh final_archivo palabra_buscada
Ejemplo \$ buscar_palabra.sh swd root

Revisión de log

Escriba un programa Shell que:

- Limpie la pantalla
- Permita, con un menú, hacer una de las siguientes actividades
 - Muestre las últimas 15 líneas del archivo messages
 - Muestre, de esas 15 líneas del archivo messages, las que contengan una palabra particular
 - Muestre de las últimas 15 líneas del archivo syslog el proceso de los eventos registrados (Solo debe mostrar el proceso de dichas líneas)

Creación de usuarios

Escriba un programa Shell que implemente el trabajo que hizo de creación de usuarios, grupos y permisos del laboratorio anterior. Debe solicitar en la línea de comandos toda la información requerida. Debe verse del estilo

```
newuser nombre grupo descripción directorio Shell permiso_usuario(en
número) permiso_grupo(en número) permiso_otros(en número)
newgroup nombre_grupo ID_grupo
```

Editor VI

- Utilice el editor VI para crear un archivo. Indique los comandos utilizados.
- Digite el siguiente texto y documente los comandos utilizados. Nota: debe quedar en cada línea del editor una línea del texto presentado, es decir, debe digitarse la tecla ENTER al final de cada fin de línea.

Este es un escrito que busca probar sus habilidades al escribir con el editor de texto VI. Este editor de texto es uno de los más antiguos editores de sistema operativos tipo Unix, Solarix y Linux.

Este editor puede parecer un poco difícil de manejar, ya que no funciona con los editores de texto modernos, pero al conocerlo más a fondo y entender su forma de operación, van a darse cuenta de las utilidades y gran funcionalidad con que cuenta.

Es importante entender los modos de operación y los comandos con que cuenta para aprovechar sus capacidades, así que es altamente recomendable que las estudien y practiquen para familiarizarse con este editor.

- Grabe el trabajo realizado sin salir del editor
- Cambie la letra 't' del primer párrafo por el símbolo +
- Cambie las palabras 'de' de todo el texto por los símbolos ##
- ¿Qué comando se puede usar para borrar una palabra en VI?
- Borre la última línea del documento.
- Deshaga el comando anterior.
- Pase a mayúscula la última línea del documento.
- Copie las últimas 2 líneas del segundo párrafo al final del archivo.
- Busque la palabra los dentro del texto
- Ubíquese en la línea 5 del texto usando un comando
- Haga un cuadro resumen con comandos de VI
- Grabe el trabajo y salga del editor
- Vuelva a entrar y borre las primeras 5 líneas
- Salga del archivo sin grabar

Power Shell

Para el grupo de tres estudiantes, En Windows, ¿qué es power Shell?, realice 5 programas en Power Shell similares a los que se hicieron en Linux y FreeBSD

NOTA: Muestre a su profesor la ejecución de sus programas.