# 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

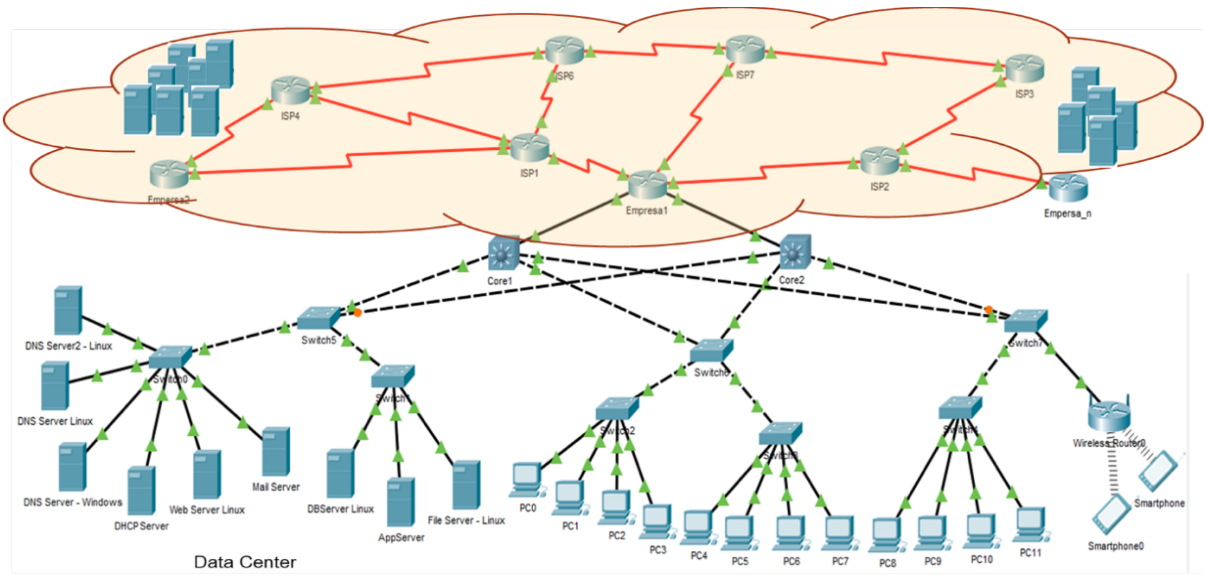
## Herramientas a utilizar

- 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 inalámbricos 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:

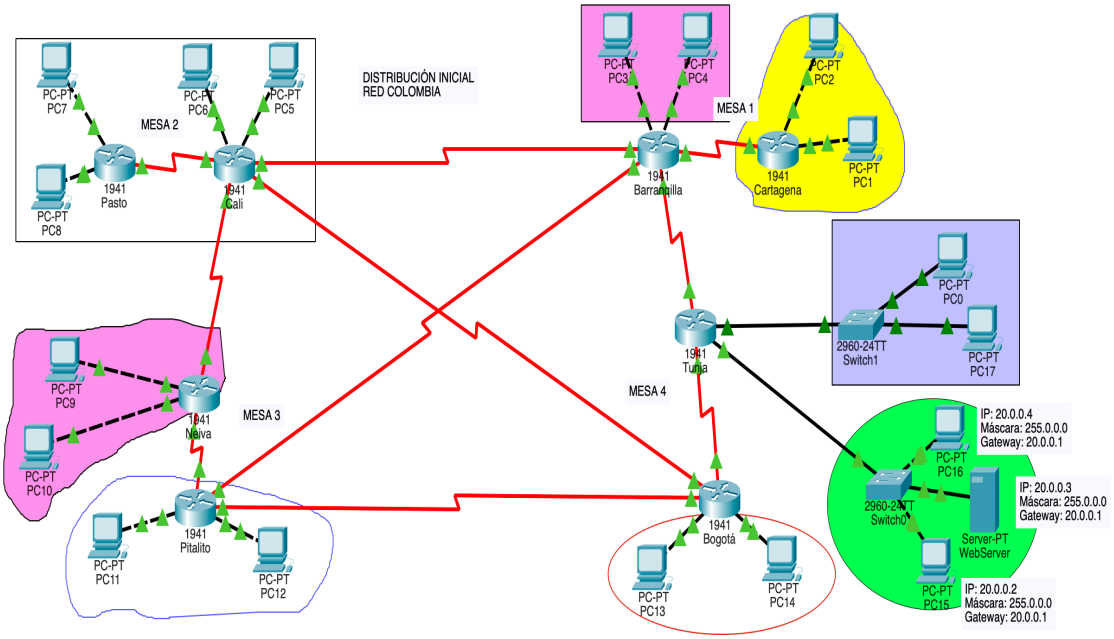


# Experimentos

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 disponible en la plataforma de Cisco?
  2. A través de la plataforma de Cisco inscribase en el curso Getting Started with Cisco Packet tracer y Exploring Networking with Cisco Packet tracer (https://www.netacad.com/courses/packet-tracer/introduction-packet-tracer). Realicen un video que resumen los cursos. Máximo 5 min.
- Usando Packet Tracer cada estudiante debe hacer el diagrama de red que se presenta en la página siguiente.
  Nota:
  - No tenga en cuenta los colores de los puntos/rectángulos que aparecen en los enlaces (los enlaces son las líneas de conexión entre dispositivos. Más adelante serán importantes los colores de dichos enlaces, 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?
    - Los cables de color rojo corresponden a cables seriales – Conexiones típicamente WAN).
    - Configure los equipos PC0, PC17 y WebServer con las IP indicadas.




**Nota**: Cada estudiante debe construir y entregar el archivo de packet tracer con la red.

## 2. Siguiendo mensajes con Packet tracer

- Haga ping desde el PC15 o PC16 al servidor Webserver desde el modo simulación de packet tracer
- Ahora, revise los PDUs por capas (Todavía no hemos visto el significado de lo que cada uno tiene, pero observen 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 traffic[1].**

- 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 PC15 or PC16. Choose the Desktop tab. Open the Command Prompt. Enter the command ping IP_WebServer). 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 red[2]. La utilizaremos dentro del curso para observar, en tiempo real, los datos que pasan por la red y la manera de operación de los diferentes protocolos que estudiaremos. Por tal razón

- Instale (si está en casa) y ejecute Wireshark en el computador en el que está trabajando
- Revise videos y documentación sobre la operación de Wireshark. ¿Qué es Wireshark?
- ¿Qué significa que la tarjeta queda en modo promiscuo?
- Haga un video en donde especifique las partes de la interface que lo compone, ¿Cómo generar filtros?, ¿Para qué se usan?. De unos ejemplos. El video debe ser de 5 minutos aproximadamente.
- Realice una consulta web al link k http://laboratorio.is.escuelaing.edu.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 que cada capa hace, revise la información que se puede ver en diferentes áreas de la pantalla de Wireshark y presente capturas del mismo (Para facilitar el análisis, filtre y encuentre un paquete capturado que contenga la palabra GET).
- En el caso de grupos de 3 estudiantes, consulte otros 2 recursos web y muestre la operación. Verifique si el comportamiento es similar en las 3 consultas.
- Presente su respuesta con un video de máximo 5 min

[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/

## 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 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.

# 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 su gestión.

## 1. Shell programming- Unix

Usando una máquina virtual de Linux Slackware, FreeBSD y Centos, según número de personas en el grupo, desarrolle las siguientes aplicaciones (recuerde documentar su código).

### Comando ls

- Realice un Shell que liste los archivos en un directorio, inclusive los ocultos, dado y permita
  - Ordenarlo por las diferentes opciones e indicar la cantidad por grupos:
    - Más reciente (debe decir cuántos archivos son de la misma fecha)
    - Más antiguo (debe decir cuántos archivos son de la misma fecha)
    - Tamaño de mayor a menor (debe decir cuántos archivos son del mismo tamaño)
    - Tamaño de menor a mayor (debe decir cuántos archivos son del mismo tamaño)
    - Tipo de archivo (Archivo/directorio) (debe decir cuántos archivos son del mismo tipo)
  - Que tenga las siguientes condiciones (dar la opción de sólo en el directorio indicado o en el directorio indicado y sus subdirectorios)
    - Inicie con una cadena dada
    - Termine con una cadena dada
    - Contenga una cadena dada

  Después de pedir el directorio a revisar, cree un menú con las opciones anteriores (se debe quedar en el menú hasta que el usuario indique que quiere salir). Debe limpiar pantalla antes de mostrar el resultado y si es muy extenso el resultado, debe paginar.

### Comandos de búsqueda o visualización de archivos

- Realice un Shell que desde la línea de comando (dando los parámetros indicados) permita
  - Buscar un archivo/parte de un archivo dado una ruta y un nombre/parte de un nombre de un archivo. La salida será las ubicaciones y nombres de los archivos y al final, la cantidad de veces que se encontró el archivo

    ```
    Buscar_archivo path nom_arch|parte_nom_arch
    ```
  - Busque una palabra/parte de una palabra en un archivo dado. La salida será la palabra encontrada y las líneas en las que la encontró y al final, la cantidad de veces que se repitió.

    ```
    Buscar_palabra nom_archivo palabra|parte_palabra
    ```

- Busque un archivo/parte de un archivo en una ruta dada y cuando lo encuentre, busque una palabra/parte de una palabra. La salida será, por cada archivo encontrado, la línea en donde se encontró la palabra y al final, la cantidad de veces que se repitió.

  ```
  Buscar_palabra_arch path nom_arch|parte_nom_arch palabra|parte_palabra
  ```

- Usando un menú
  - Cuente la cantidad de líneas de un archivo.
  - Muestre las primeras *n* líneas de un archivo dado.
  - Muestre las últimas *n* líneas de un archivo dado.

### Revisión de log

Escriba un programa Shell que:

- ¿Qué son los logs?
- ¿Qué tipo de logs encuentra en los sistemas operativos que instaló?
- ¿Qué es syslog? ¿En qué consiste este estándar?, ¿los logs que encontró en los sistemas operativos siguen este estándar?
- Limpie la pantalla
- Permita, con un menú, hacer una de las siguientes actividades
  - Muestre las últimas *n* líneas de 3 archivo de log que contiene los datos de la actividad general del sistema. *n* es dado por el usuario.
  - Muestre, de esas *n* líneas de los mismo archivo, las que contengan una palabra particular. *n* es dado por el usuario.

### 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

```
newgroup nombre_grupo ID_grupo

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

Para el caso de grupos de 3 estudiantes, realizar los mismos ejercicios para Windows Server usando PowerShell

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

## 2. Editor VI en Linux/Unix

- 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.

Vamos a revisar como es la escritura sobre el editor Vi. Este editor es muy util y es muy importante en sistemas operativos tipo UNIX, en algunos casos es posible utilizar otros editores como PICO o NANO pero en algunas ocasiones no es posible utilizar estos editores mientras que VI siempre está presente y funcional en estos ambientes.

El editor VI es muy potente, la cantidad de comando que tiene y las multiples funcionalidades con las que cuenta, lo hace un excelente editor. La dificultad con el editor es entender que trabaja en dos modos, el modo comando y el modo edición. Para entrar al modo comando se presiona la tecla ESC y a partir de allí, todas las teclas que se presionen se entenderan como un comando. Para entrar al modo edición, estando en el modo comando, se puede hacer de varias manera, ej.: i, a, A, o.

- Grabe el trabajo realizado sin salir del editor
- Cambie las letras 'a' del primer párrafo por el símbolo -
- Cambie las palabras "al" en todo el texto por los símbolos ##
- ¿Qué comando se puede usar para borrar una palabra en VI?
- Borre la última 4 línea del documento con un solo comando.
- 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 `editor` 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

En el caso de grupos de tres estudiantes, realice el mismo ejercicio en Centos . Es igual?, si encontró diferencias, indíquelas.

## 3. Generación de máquinas

Para el trabajo del semestre se necesitarán 2 máquinas virtuales de cada sistema operativo instalado excepto Windows Server sin GUI y Android. Genere las nuevas máquinas y pruebe que puedan verse entre ellas y hacia internet.

## 4. Compartir archivos

Uno de los servicios claves en un ambiente empresarial son los file system compartidos, en donde las personas de la empresa pueden guardar archivos y compartirlos con un grupo de trabajo. La tarea en esta ocasión consiste en configurar un servidor de archivos en Linux Slackware usando SMB/SAMBA, de tal manera que se permita compartir archivos entre los tres sistemas operativos (Linux Slackware, FreeBSD y Windows. Adicionalmente, Centos --> En los grupos de 3).