Universidad Continental

Guía de Trabajo

Redes de Computadoras

Guía de Trabajo
Redes de Computadoras

Primera edición digital
Huancayo, 2022

Av. San Carlos 1795, Huancayo-Perú
Teléfono: (51 64) 481-430 anexo 7361
Correo electrónico: recursosucvirtual@continental.edu.pe
http://www.continental.edu.pe/

Cuidado de edición
Fondo Editorial

Diseño y diagramación
Fondo Editorial

Contenido

Presentación

¡Bienvenido al primer curso: Redes de Computadoras! Este es el primero de los tres cursos que están alineados con el examen de certificación CCNA. Este curso contiene diecisiete capítulos.

En Redes de Computadoras obtendrá una comprensión básica de la forma en que operan las redes. Aprenderá acerca de los componentes de red y sus funciones. Además, cómo se estructura una red y las arquitecturas utilizadas para crear redes, incluido Internet.

Pero en esta asignatura Redes de Computadoras se trata de algo más que de aprender conceptos de redes. Al final de este curso, podrá crear redes de área local (LAN), desarrollar configuraciones básicas en enrutadores y conmutadores e implementar el protocolo de internet (IP).

Se recomienda leer bastante todos los conceptos que se les ofrece a través del material que está en la Academia de Cisco Netacad (www.netacad.com), así como la resolución de sus evaluaciones por cada tema. También se les recomienda resolver todas las prácticas haciendo uso del *software* simulador de redes *packet tracer*.

Primera Unidad

Semana 1

Configuración inicial en la red

Sección: ..... Fecha: ...../...../2022 Duración: 240 min.
Docente: ..... Unidad: 1
Apellidos y nombres: .....

Instrucciones

A continuación, de manera colaborativa, configure parámetros básicos de red con las siguientes instrucciones.

I. Objetivo

El estudiante será capaz de realizar una práctica colaborativa de laboratorio con el *software* de simulación *packet tracer*, equipos reales y equipos virtuales, en donde se va a configurar de manera básica una red pequeña para poder tener acceso a los recursos de manera remota.

II. Descripción de la actividad a realizar (práctica)

En esta actividad, se va a aprender a usar de manera introductoria al *software* de simulación *packet tracer*, equipos reales y equipos virtuales, en donde se va a configurar de manera básica una red pequeña para poder tener acceso a los recursos de manera remota.

III. Procedimientos

Parte 1: Introducción a *packet tracer*

- Explorar las partes del *software*.
- Hacer conexiones entre PC con UTP cruzado.
- Realizar conexiones con *switches* y equipos finales con cable UTP directo.
- Configurar direccionamiento IPv4 y hacer pruebas de conectividad.

Parte 2: Configuración de red en equipos de reales

- Verificar y configurar el direccionamiento IPv4 de Windows.
- Realizar pruebas de conectividad con el comando *Ping*.
- Configurar el *firewall* de Windows.

Parte 3: Configuración de red en equipos de reales

- Configurar máquinas virtuales como Windows XP, 7, 8 y 10.
- Verificar y configurar el direccionamiento IPv4 de Windows.
- Realizar pruebas de conectividad con el comando Ping.
- Configurar el *firewall* de Windows.

Parte 4: Configuración de red en equipos de reales

- Compartir recursos en máquinas virtuales.
- Configurar permisos NTFS en los recursos compartidos.
- Compartir recursos en máquinas reales.
- Configurar permisos NTFS en los recursos compartidos.

Semana 2

Navegación de IOS

Sección: ..... Fecha: ...../...../2022 Duración: 30 min.
Docente: ..... Unidad: 1
Apellidos y nombres: .....

Instrucciones

A continuación, de manera colaborativa, configure parámetros básicos de red con las siguientes instrucciones.

I. Objetivo

El estudiante será capaz de practicar las habilidades necesarias para navegar dentro de Cisco IOS, como los distintos modos de acceso de usuario, diversos modos de configuración y comandos comunes que utiliza habitualmente. También practicará el acceso a la ayuda contextual mediante la configuración del comando *clock*.

II. Descripción de la actividad a realizar (práctica)

En esta actividad se va a aprender a usar de manera básica Cisco IOS los distintos modos de acceso de usuario, diversos modos de configuración y comandos comunes que utiliza habitualmente. También practicará el acceso a la ayuda contextual mediante la configuración del comando *clock*.

III. Procedimientos

Parte 1: Establecimiento de conexiones básicas, acceso a la CLI y exploración de ayuda

En la parte 1 de esta actividad, conectar una PC a un switch mediante una conexión de consola e investigar los diferentes modos de comando y características de ayuda.

Paso 1: Conecte la PC1 a S1 mediante un cable de consola.

a. Haga clic en el ícono **Conexiones**, similar a un rayo, en la esquina inferior izquierda de la ventana de *Packet Tracer*.
b. Haga clic en el cable de consola celeste para seleccionarlo. El puntero del mouse cambia a lo que parece ser un conector con un cable que cuelga de él.
c. Haga clic en PC1. Aparece una ventana que muestra una opción para una conexión RS-232.
d. Arrastre el otro extremo de la conexión de consola al *switch* S1 y haga clic en el *switch* para acceder a la lista de conexiones.
e. Seleccione el puerto de consola para completar la conexión.

Paso 2: Establezca una sesión de terminal con el S1.

a. Haga clic en PC1 y luego en la ficha Escritorio.
b. Haga clic en el ícono de la aplicación Terminal. Verifique que los parámetros predeterminados de la configuración de puertos sean correctos.
   ¿Cuál es el parámetro de bits por segundo?

   _____

c. Haga clic en Aceptar.
d. La pantalla que aparece puede mostrar varios mensajes. En alguna parte de la pantalla tiene que haber un mensaje que diga *Press RETURN to get started!* (Presione REGRESAR para comenzar). Pulse INTRO.
   ¿Cuál es la petición de entrada que aparece en la pantalla?

   _____

Paso 3: Examine la ayuda de IOS.

a. El IOS puede proporcionar ayuda para los comandos según el nivel al que se accede. La petición de entrada que se muestra actualmente se denomina Modo EXEC del usuario y el dispositivo está esperando un comando. La forma más básica de solicitar ayuda es escribir un signo

de interrogación (?) en la petición de entrada para mostrar una lista de comandos.

S1> **?**
¿Qué comando comienza con la letra "C"?

_____

b. En la petición de entrada, escriba **t**, seguido de un signo de interrogación (**?**).
S1> **t?**
¿Qué comandos se muestran?

_____

c. En la petición de entrada, escriba **te**, seguido de un signo de interrogación (**?**).
S1> **te?**
¿Qué comandos se muestran?

_____

Este tipo de ayuda se conoce como Ayuda **contextual**. Proporciona más información a medida que se expanden los comandos.

Parte 2: Exploración de los modos EXEC.

En la parte 2 de esta actividad, debe cambiar al modo EXEC privilegiado y emitir comandos adicionales.

Paso 1: Ingrese al modo EXEC privilegiado.

a. En la petición de entrada, escriba el signo de interrogación (**?**).
S1> **?**
¿Qué información de la que se muestra describe el comando ***enable***?

_____

b. Escriba **en** y presione la tecla **Tabulación**.
S1> **en<Tab>**
¿Qué se muestra después de presionar la tecla **Tabulación**?

_____

Esto se denomina completar un comando o completar la tabulación. Cuando se escribe parte de un comando, la tecla **Tabulación** se puede utilizar para completar el comando parcial. Si los caracteres que se escriben son suficientes para formar un comando único, como en el caso del comando **enable**, se muestra la parte restante.

¿Qué ocurriría si escribiera te<Tab> en la petición de entrada?

c. Introduzca el comando **enable** y presione INTRO. ¿Cómo cambia la petición de entrada?

d. Cuando se le solicite, escriba el signo de interrogación (**?**).

S1# **?**

Antes había un comando que comenzaba con la letra "C" en el modo EXEC del usuario.

¿Cuántos comandos se muestran ahora que está activo el modo EXEC privilegiado? (**Ayuda**: puede escribir c? para que aparezcan solo los comandos que comienzan con la letra "C")

Paso 2: Ingrese en el modo de configuración global.

a. Cuando se encuentra en el modo EXEC privilegiado, uno de los comandos que comienza con la letra "C" es **configure**. Escribe el comando completo o una parte suficiente

como para que sea único. Presione la tecla <**Tabulación**> para emitir el comando y presione la tecla INTRO.
S1# **configure**
¿Cuál es el mensaje que se muestra?

_____

b. Presione Intro para aceptar el parámetro predeterminado que se encuentra entre corchetes [**terminal**].
¿Cómo cambia la petición de entrada?

_____

c. Esto se denomina "modo de configuración global". Este modo se analizará en más detalle en las próximas actividades y prácticas de laboratorio. Por el momento, escriba **end**, **exit** o **Ctrl-Z** para volver al modo EXEC privilegiado.
S1(config)# **exit**
S1#

Parte 3: Configuración del reloj

Paso 1: Utilice el comando clock.

a. Utilice el comando **clock** para explorar en más detalle la ayuda y la sintaxis de comandos. Escriba **show clock** en la petición de entrada de EXEC privilegiado.
S1# **show clock**
¿Qué información aparece en pantalla? ¿Cuál es el año que se muestra?

_____

b. Utilice la ayuda contextual y el comando **clock** para establecer la hora del switch en la hora actual. Introduzca el comando **clock** y presione la tecla Intro.

S1# **clock<ENTER>**

¿Qué información aparece en pantalla?

_____

c. El mensaje "% Incomplete command" se regresa a IOS. Esto significa que el comando **clock** necesita más parámetros. Cuando se necesita más información, se puede proporcionar ayuda escribiendo un espacio después del comando y el signo de interrogación (?).
S1# **clock ?**
¿Qué información aparece en pantalla?

_____

d. Configure el reloj con el comando **clock set**. Proceda por el comando un paso a la vez.
S1# **clock set ?**
¿Qué información se solicita?

_____

¿Qué información se habría mostrado si solo se hubiera ingresado el comando **clock set** y no se hubiera solicitado ayuda con el signo de interrogación?

_____

e. En función de la información solicitada por la emisión del comando **clock set ?**, introduzca las 3:00 p. m. como hora utilizando el formato de 24 horas, esto será 15:00:00. Revise si se necesitan otros parámetros.
S1# **clock set 15:00:00 ?**
El resultado devuelve la solicitud de más información:
<1-31> Day of the month
MONTH Month of the year

f. Intente establecer la fecha en 01/31/2035 con el formato solicitado. Es posible que para completar el proceso deba solicitar más ayuda mediante la ayuda contextual. Cuando termine, emita el comando **show clock** para mostrar la configuración del reloj. El resultado del comando debe mostrar lo siguiente:
S1# **show clock**
*15:0:4.869 UTC Tue Jan 31 2035

g. Si no pudo lograrlo, pruebe con el siguiente comando para obtener el resultado anterior:
S1# **clock set 15:00:00 31 Jan 2035**

Paso 2: Explore los mensajes adicionales del comando.

a. El IOS proporciona diversos resultados para los comandos incorrectos o incompletos. Continúe utilizando el comando **clock** para explorar los mensajes adicionales con los que se puede encontrar mientras aprende a utilizar el IOS.

b. Emita el siguiente comando y registre los mensajes:
S1# **cl**
¿Qué información se devolvió?

_____

S1# **clock**
¿Qué información se devolvió?

_____

S1# **clock set 25:00:00**
¿Qué información se devolvió?

_____

S1# **clock set 15:00:00 32**
¿Qué información se devolvió?

_____

Semana 3

Comandos básicos IOS

Sección: ..... Fecha: ...../...../2022 Duración: 120 min.
Docente: ..... Unidad: 1
Apellidos y nombres: .....

Instrucciones

A continuación, de manera colaborativa, configure parámetros básicos de red con las siguientes instrucciones.

I. Objetivo

El estudiante será capaz de armar una red simple mediante cableado LAN Ethernet y accederá al *switch* y *router* de Cisco utilizando los métodos de acceso de consola y remoto. Configurará los parámetros básicos y la asignación de direcciones IP y demostrará el uso de una dirección IP de administración para la administración remota de *switches* y *router*. La topología consta de un *switches*, *routers* y host que solo usa puertos Ethernet y de consola.

II. Descripción de la actividad a realizar (práctica)

En esta actividad se va a realizar el armado de una red simple mediante cableado LAN Ethernet y accederá al *switch* y *router* de Cisco utilizando los métodos de acceso de consola y remoto. Configurará los parámetros básicos y la asignación de direcciones IP y demostrará el uso de una dirección IP de administración para la administración remota de *switches* y *router*. La topología consta de un *switches*, *routers* y host que solo usa puertos Ethernet y de consola.

III. Procedimientos

a) Realice las conexiones tal como se muestra en el esquema compartido por el docente.

b) Nombre del *switch* o *router*.

c) Contraseña "cisco" para las líneas VTY y consola.

d) Cifre todas las contraseñas.

e) Crear un mensaje de advertencia.

f) Configure las IP a las interfaces que correspondan, según el modelo que se le brindó.

g) Guarde las configuraciones.

h) Desde cualquier computadora que ha sido configurada, debe de poder hacer ping al *switch* y *al router*, así como telnet.

i) Una vez terminado todo y verificado por el docente, borre toda la configuración con los comandos:

- Router# erase startup-config
- Router# reload

Si te pide guardar los cambios, presiona la tecla "N" para no guardar los cambios.

- Switch# erase startup-config
- Switch# delete vlan.dat
- Switch# reload

Si le piden guardar los cambios, presione la tecla "N" para no guardar los cambios.

Semana 4

Usando *wireshark* y análisis de datos

Sección: ..... Fecha: ...../...../2022 Duración: 60 min.
Docente: ..... Unidad: 1
Apellidos y nombres: .....

Instrucciones

A continuación, de manera colaborativa, configure parámetros básicos de red con las siguientes instrucciones.

I. Objetivo

El estudiante será capaz de capturar y analizar datos ICMP locales y remotos en Wireshark.

II. Descripción de la actividad a realizar (práctica)

En esta actividad, haciendo uso de equipos reales, se va a realizar la captura y analizar datos ICMP locales y remotos en Wireshark.

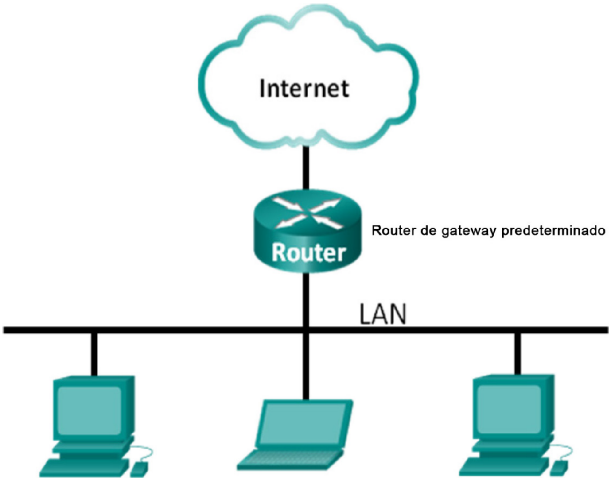
III. Procedimientos

Parte 1: Captura y análisis de datos ICMP locales en Wireshark

En la parte 1 de esta práctica de laboratorio, hará *ping* a otra PC en la LAN y capturará solicitudes y respuestas ICMP en Wireshark. También verá dentro de las tramas capturadas para obtener información específica. Este análisis debe ayudar a aclarar de qué manera se utilizan los encabezados de paquetes para transmitir datos al destino.

Ver Figura 1 en la siguiente página.

Figura 1. Topología de enrutamiento



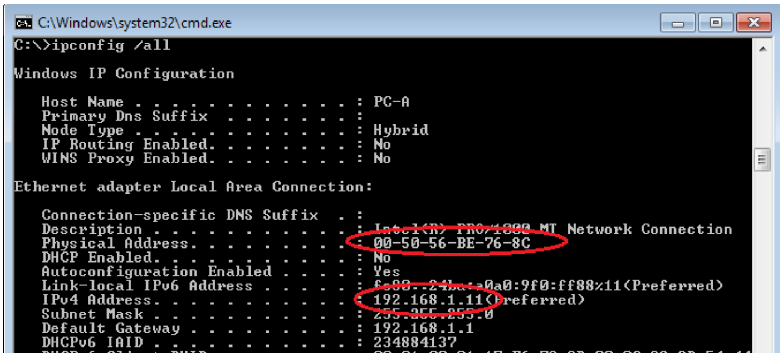
Paso 1: Recupere las direcciones de interfaz de la PC

Para esta práctica de laboratorio, deberá recuperar la dirección IP de la PC y la dirección física de la tarjeta de interfaz de red (NIC), que también se conoce como "dirección MAC".

a. Abra una ventana de comandos, escriba **ipconfig /all** y luego presione Intro.

b. Observe la dirección IP y la dirección MAC (física) de la interfaz de la PC.

Figura 2. Topología de enrutamiento



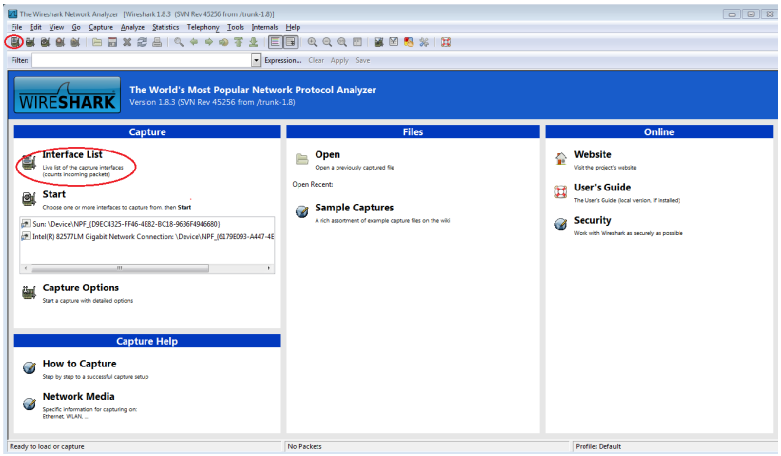
c. Solicite a un miembro del equipo la dirección IP de su PC y proporciónele la suya. En esta instancia, no proporcione su dirección MAC.

Paso 2: Inicie Wireshark y comience a capturar datos

a. En la PC, haga clic en el botón **Inicio** de Windows para ver Wireshark como uno de los programas en el menú emergente. Haga doble clic en **Wireshark**.

b. Luego de que se inicia Wireshark, haga clic en **Interface List** (Lista de interfaces).

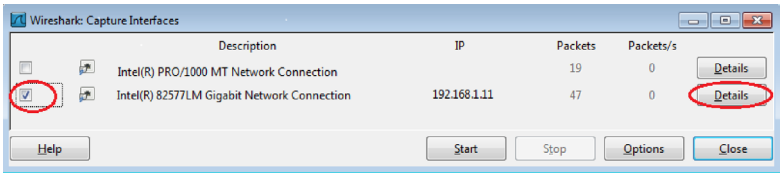
Figura 3. Topología de enrutamiento



Nota: Al hacer clic en el ícono de la primera interfaz de la fila de íconos, también se abre la Lista de interfaces.

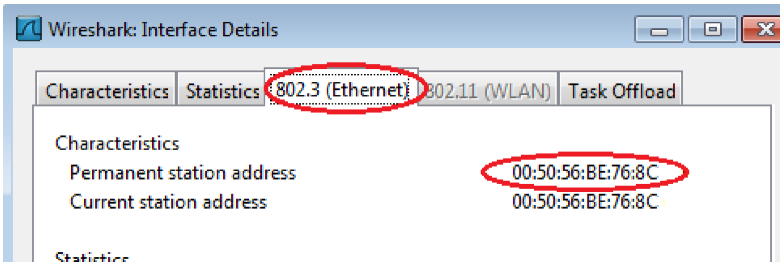
c. En la ventana Wireshark: Capture Interfaces (Wireshark: capturar interfaces), haga clic en la casilla de verificación junto a la interfaz conectada a la LAN.

Figura 4. Wireshark: capturar interfaces



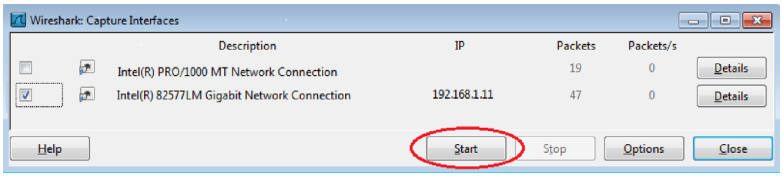
Nota: si se indican varias interfaces, y no está seguro de cuál activar, haga clic en el botón Details (Detalles) y, a continuación, haga clic en la ficha 802.3 (Ethernet). Verifique que la dirección MAC coincida con lo que observó en el paso 1b. Después de verificar la interfaz correcta, cierre la ventana **Detalles de la interfaz**.

Figura 5. Wireshark: detalle de interfaces



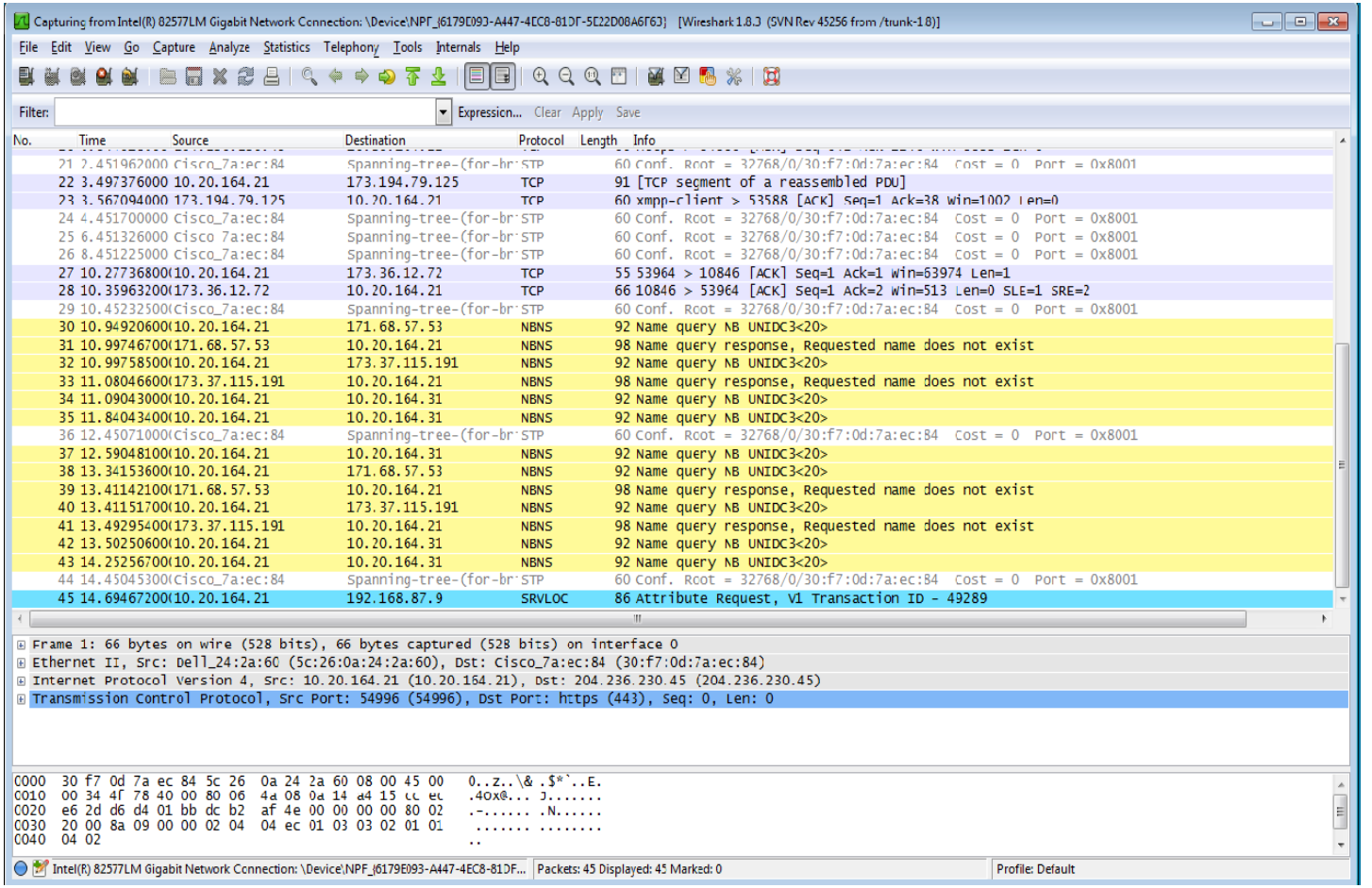
d. Después de activar la interfaz correcta, haga clic en Start (Comenzar) para iniciar con la captura de datos.

Figura 6. Wireshark: captura de interfaces



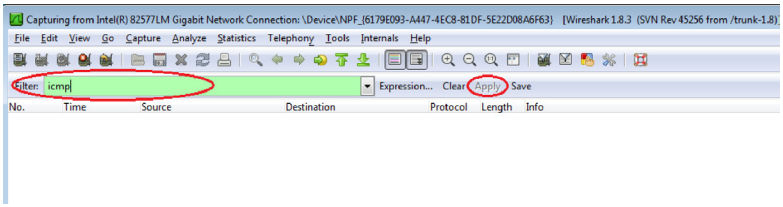
La información comienza a desplazar hacia abajo la sección superior de Wireshark. Las líneas de datos aparecen en diferentes colores según el protocolo. Ver Figura 7 en la siguiente página.

Figura 7. Topología de enrutamiento: líneas de datos



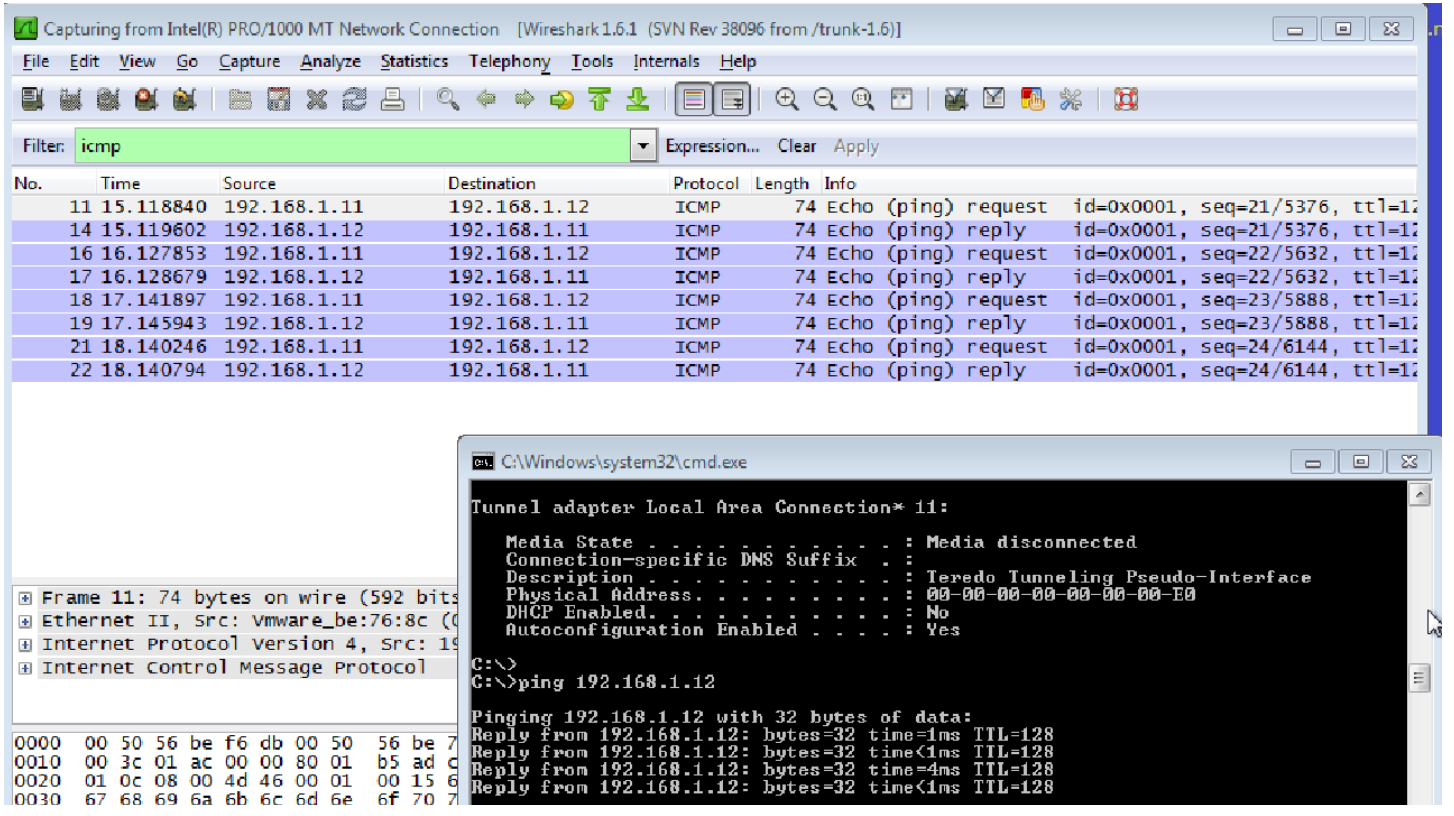
Es posible desplazarse muy rápidamente por esta información según la comunicación que tiene lugar entre la PC y la LAN. Se puede aplicar un filtro para facilitar la vista y el trabajo con los datos que captura Wireshark. Para esta práctica de laboratorio, solo nos interesa mostrar las PDU de ICMP (ping). Escriba **icmp** (Figura 8) en el cuadro Filtro que se encuentra en la parte superior de Wireshark y presione Intro o haga clic en el botón **Apply** (Aplicar) para ver solamente PDU de ICMP (ping).

Figura 8. Topología de enrutamiento: Captura



e. Este filtro hace que desaparezcan todos los datos de la ventana superior, pero se sigue capturando el tráfico en la interfaz. Abra la ventana del símbolo del sistema que abrió antes y haga ping a la dirección IP que recibió del miembro del equipo. Comenzará a ver que aparecen datos en la ventana superior de Wireshark nuevamente. Ver Figura 9 en la siguiente página.

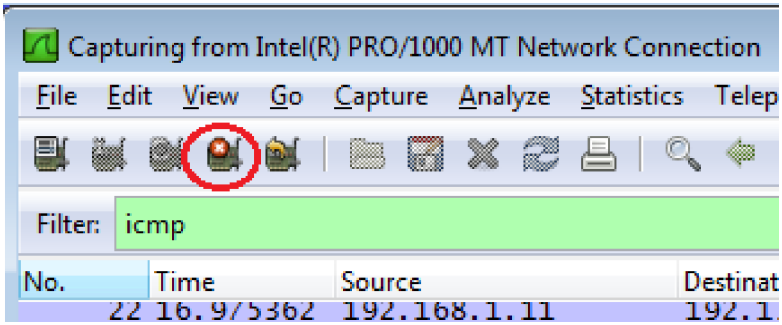
Figura 9. Topología de enrutamiento



Nota: Si la PC del miembro del equipo no responde a sus pings, es posible que se deba a que el firewall de la PC está bloqueando estas solicitudes. Consulte Appendix A: Allowing ICMP Traffic Through a Firewall para obtener información sobre cómo permitir el tráfico ICMP a través del firewall con Windows 7.

f. Detenga la captura de datos haciendo clic en el ícono Stop Capture (Detener captura).

Figura 10. Topología de enrutamiento



Paso 3: Examine los datos capturados

En el paso 3, examine los datos que se generaron mediante las solicitudes de ping de la PC del miembro del equipo. Los datos de Wireshark se muestran en tres secciones:

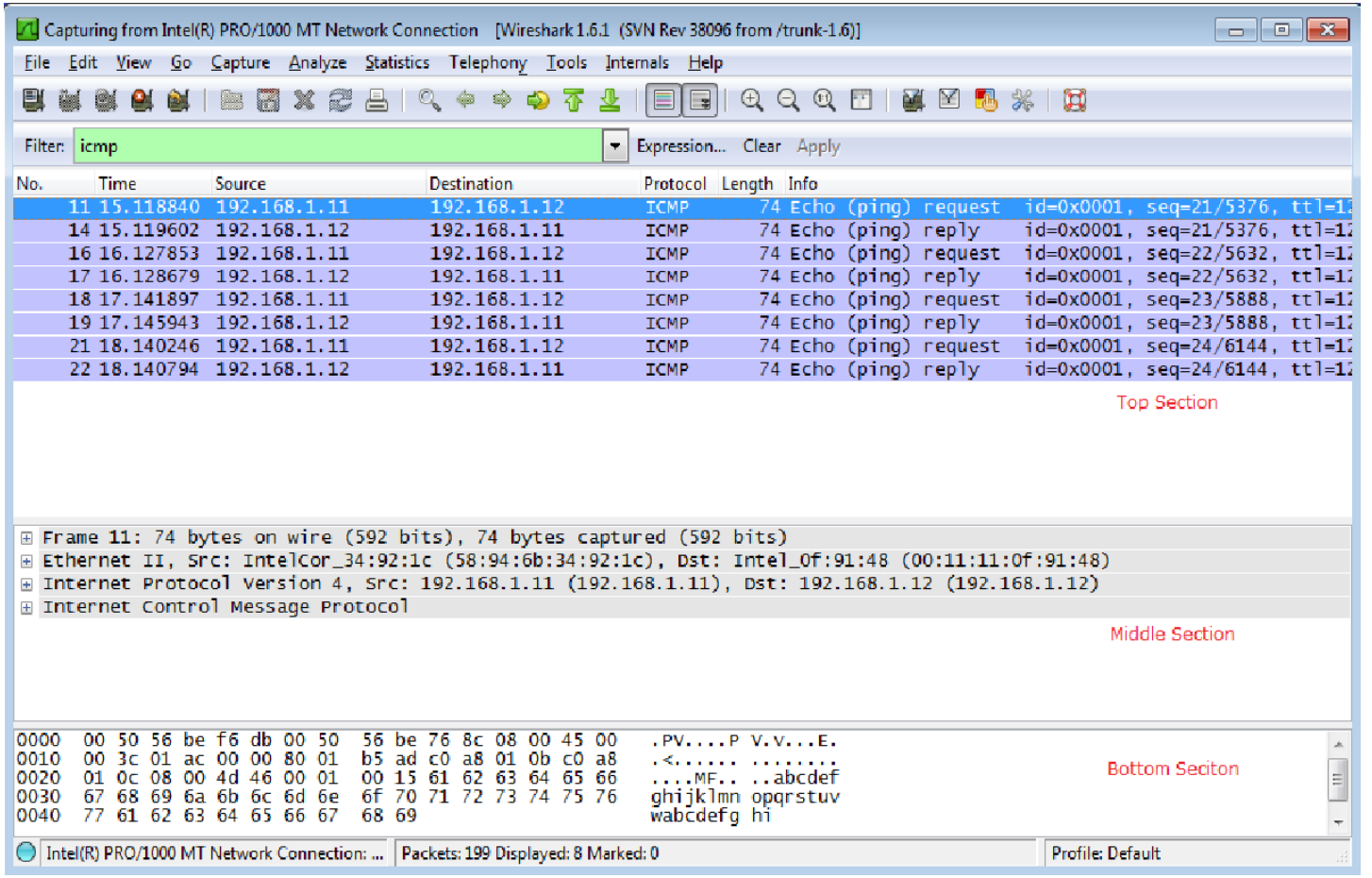
1) La sección superior muestra la lista de tramas de PDU capturadas con un resumen de la información de paquetes IP enumerada.

2) La sección media indica información de la PDU para la trama seleccionada en la parte superior de la pantalla y separa una trama de PDU capturada por las capas de protocolo.

3) La sección inferior muestra los datos sin procesar de cada capa. Los datos sin procesar se muestran en formatos hexadecimal y decimal.

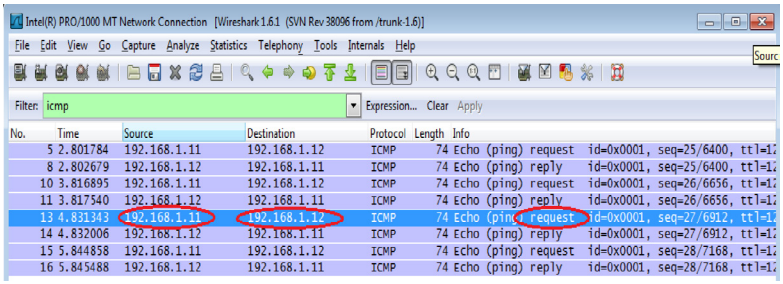
Ver Figura 11 en la siguiente página.

Figura 11. Topología de enrutamiento: datos de Wireshark



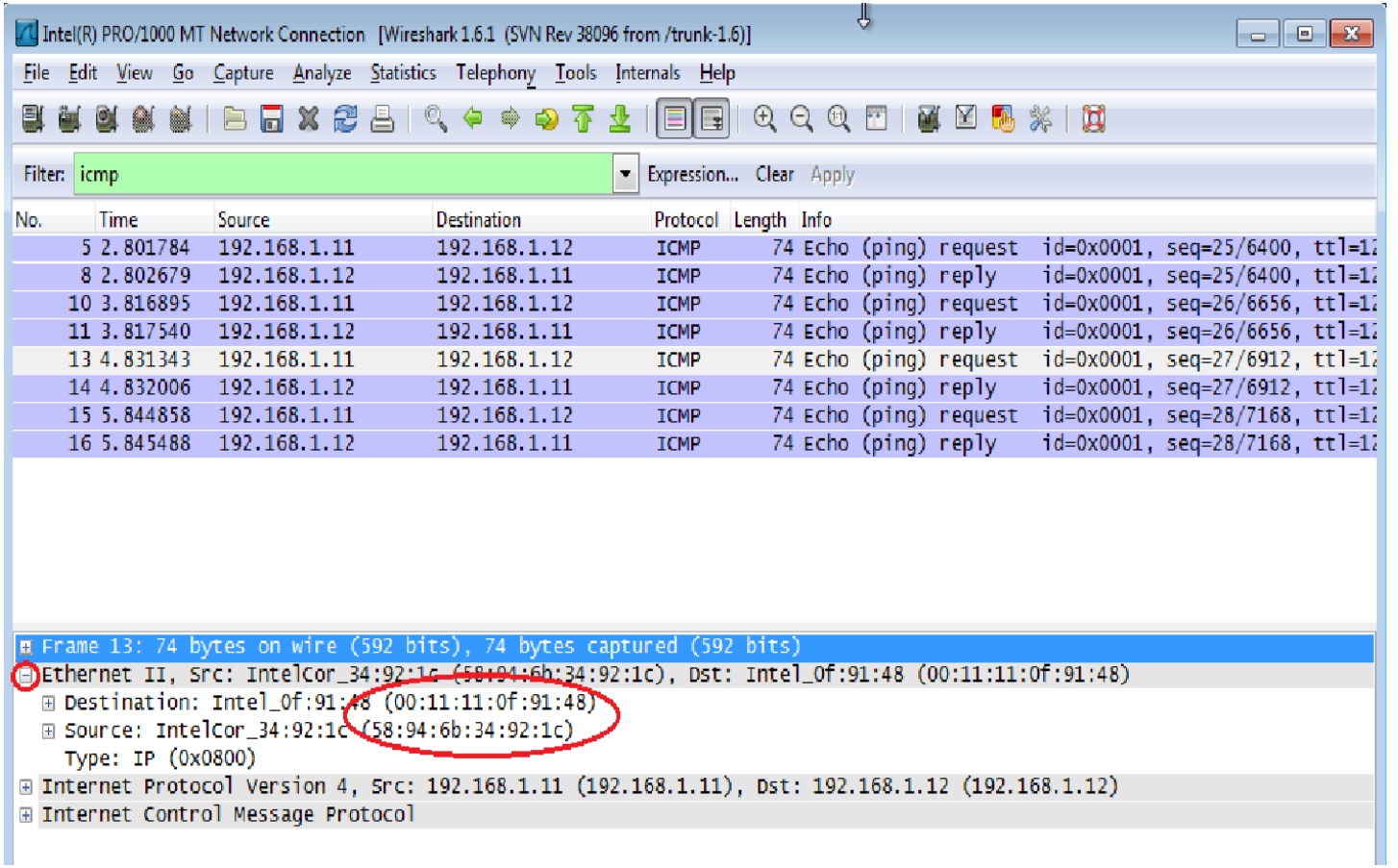
a. Haga clic en las primeras tramas de PDU de la solicitud de ICMP en la sección superior de Wireshark. Observe que la columna Origen contiene la dirección IP de su PC y la columna Destino contiene la dirección IP de la PC del compañero de equipo a la que hizo ping.

Figura 12. Topología de enrutamiento



Con esta trama de PDU aún seleccionada en la sección superior, navegue hasta la sección media. Haga clic en el signo más que está a la izquierda de la fila de Ethernet II para ver las direcciones MAC de origen y destino. Ver Figura 13 en la siguiente página.

Figura 13. Topología de enrutamiento: direcciones MAC de origen y destino



¿La dirección MAC de origen coincide con la interfaz de su PC?

¿La dirección MAC de destino en Wireshark coincide con la dirección MAC del compañero de equipo?

¿De qué manera su PC obtiene la dirección MAC de la PC a la que hizo ping?

Nota: En el ejemplo anterior de una solicitud de ICMP capturada, los datos ICMP se encapsulan dentro de una PDU del paquete IPv4 (encabezado de Ipv4), que luego se encapsula en una PDU de trama de Ethernet II (encabezado de Ethernet II) para la transmisión en la LAN.

Segunda Unidad

Semana 5

Armado de cable UTP

Sección: ..... Fecha: ...../...../2022 Duración: 270 min.
Docente: ..... Unidad: 2
Apellidos y nombres: .....

Instrucciones

A continuación, de manera colaborativa, prepare los cables UTP siguiendo las instrucciones del docente.

I. Objetivo

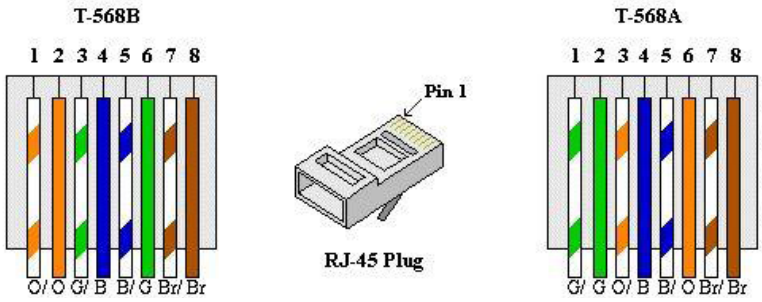
El estudiante será capaz de preparar y armar los cables UTP o pares trenzados para hacer conexiones LAN y poder armar una pequeña red, de tal manera que se tenga conectividad entre diferentes equipos.

II. Descripción de la actividad a realizar (práctica)

En esta actividad se va a realizar el armado cables UTP o pares trenzados para hacer conexiones LAN y poder armar una pequeña red, de tal manera que haya conectividad entre diferentes equipos.

III. Procedimientos

Figura 14. Topología de enrutamiento: armado cables UTP



Semana 6

Análisis de tramas Ethernet

Sección: ..... Fecha: ...../...../2022 Duración: 270 min.
Docente: ..... Unidad: 2
Apellidos y nombres: .....

Instrucciones

A continuación, de manera colaborativa, siga las siguientes instrucciones.

I. Objetivo

El estudiante será capaz revisará los campos que contiene una trama de Ethernet II. En la parte 2, utilizará Wireshark para capturar y analizar campos de encabezado de tramas de Ethernet II de tráfico local y remoto.

II. Descripción de la actividad a realizar (práctica)

En esta actividad se va a realizar la revisión de los campos que contienen una trama de Ethernet II. En la parte 2, utilizará Wireshark para capturar y analizar campos de encabezado de tramas de Ethernet II de tráfico local y remoto.

III. Procedimientos

Parte 1: Examinar los campos de encabezado de una trama de Ethernet II

En la parte 1, examinará los campos de encabezado y el contenido de una trama de Ethernet II. Se utilizará una captura de Wireshark para examinar el contenido de esos campos.

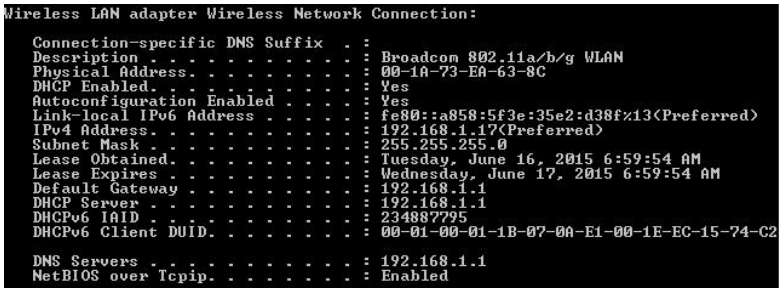
Paso 1: Revisar las descripciones y longitudes de los campos de encabezado de Ethernet II

Preámbulo	Dirección de destino	Dirección de origen	Tipo de trama	Datos	FCS
8 bytes	6 bytes	6 bytes	2 bytes	46 a 1500 bytes	4 bytes

Paso 2: Examinar la configuración de red de la PC

La dirección IP de este equipo host es 192.168.1.17, y el gateway predeterminado tiene la dirección IP 192.168.1.1.

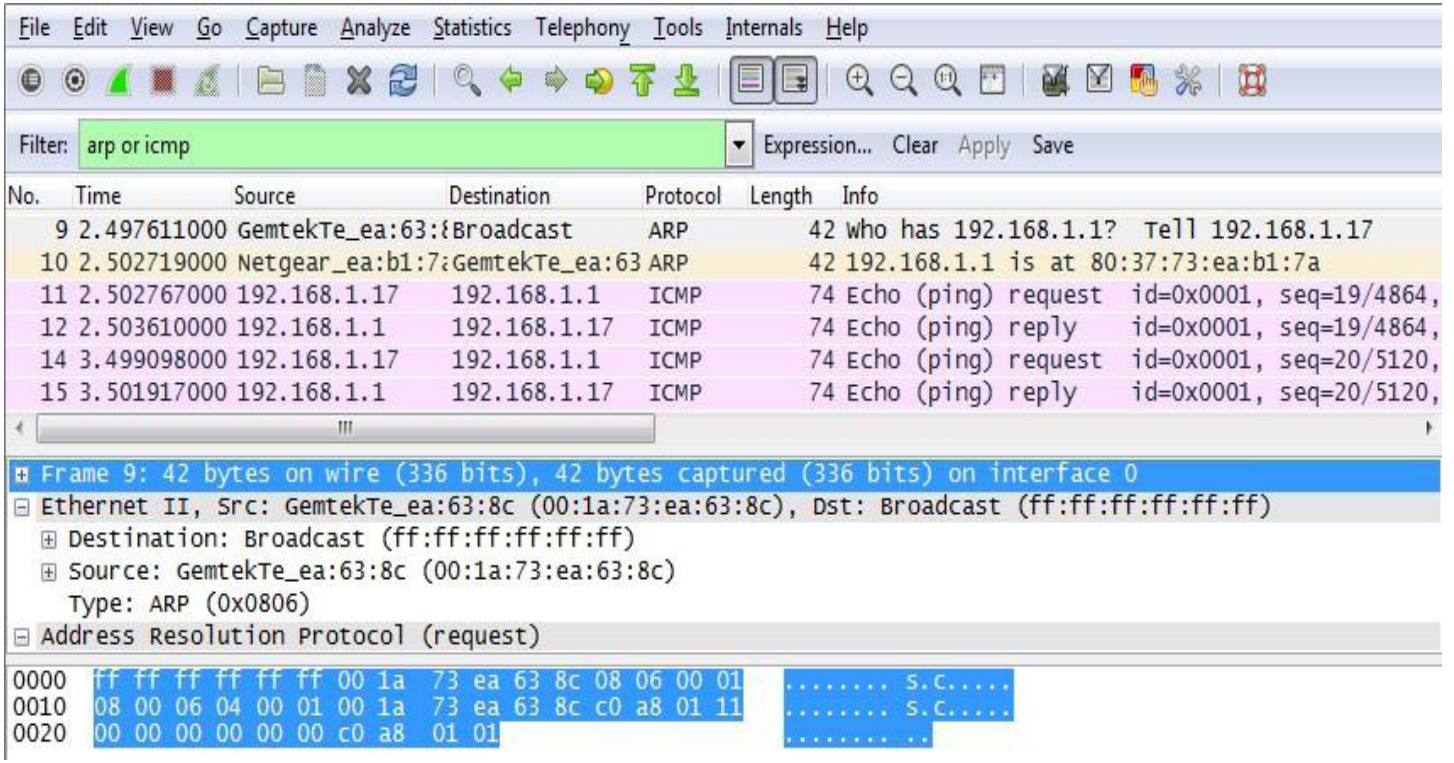
Figura 15. Configuración de red



Paso 3: Examinar las tramas de Ethernet en una captura de Wireshark

En la Figura 16 se muestran los paquetes generados por un ping que se hace de un equipo host a su *gateway* predeterminado. Se le aplicó un filtro a Wireshark para ver solamente el protocolo de resolución de direcciones (ARP) y el protocolo de mensajes de control de Internet (ICMP). La sesión comienza con una consulta ARP para obtener la dirección MAC del router del gateway seguida de cuatro solicitudes y respuestas de ping. Ver Figura 16 en la siguiente página.

Figura 16. Tramas de Ethernet



Paso 4: Examinar el contenido del encabezado de Ethernet II de una solicitud de ARP

En la siguiente tabla, se toma la primera trama de la captura de Wireshark y se muestran los datos de los campos de encabezado de Ethernet II.

Campo	Valor	Descripción
Preámbulo	No se muestra en la captura.	Este campo contiene bits de sincronización, procesados por el hardware de la NIC.
Dirección de destino	Broadcast (ff:ff:ff:ff:ff:ff) (Difusión [ff:ff:ff:ff:ff:ff])	Direcciones de capa 2 para la trama. Cada dirección tiene una longitud de 48 bits, o 6 octetos, expresada como 12 dígitos hexadecimales (0-9, A-F). Un formato común es 12:34:56:78:9A:BC. Los primeros seis números hexadecimales indican el fabricante de la tarjeta de interfaz de red (NIC), y los últimos seis números son el número de serie de la NIC. La dirección de destino puede ser de difusión, que contiene todos números uno, o de unidifusión. La dirección de origen siempre es de unidifusión.
Dirección de origen	GemtekTe_ea:63:8c (00:1a:73:ea:63:8c)	
Tipo de trama	0x0806	Para las tramas de Ethernet II, este campo contiene un valor hexadecimal que se utiliza para indicar el tipo de protocolo de capa superior del campo de datos. Ethernet II admite varios protocolos de capa superior. Dos tipos comunes de trama son los siguientes: Valor Descripción 0x0800 Protocolo IPv4 0x0806 Protocolo de resolución de direcciones (ARP)
Datos	ARP	Contiene el protocolo de nivel superior encapsulado. El campo de datos tiene entre 46 y 1500 bytes.

continúa...

... viene

FCS	No se muestra en la captura.	Secuencia de verificación de trama, utilizada por la NIC para identificar errores durante la transmisión. El equipo emisor calcula el valor abarcando las direcciones de trama, campo de datos y tipo. El receptor lo verifica.

¿Qué característica significativa tiene el contenido del campo de dirección de destino?

¿Por qué envía la PC un ARP de difusión antes de enviar la primera solicitud de ping?

¿Cuál es la dirección MAC del origen en la primera trama?

¿Cuál es el identificador de proveedor (OUI) de la NIC del origen?

¿Qué porción de la dirección MAC corresponde al OUI?

¿Cuál es el número de serie de la NIC del origen?

Parte 2: Utilizar Wireshark para capturar y analizar tramas de Ethernet

En la parte 2, utilizará Wireshark para capturar tramas de Ethernet locales y remotas. Luego, examinará la información que contienen los campos de encabezado de las tramas.

Paso 1: Determinar la dirección IP del gateway predeterminado de la PC

Abra una ventana del símbolo del sistema y emita el comando ipconfig.

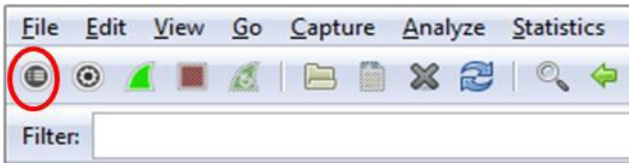
¿Cuál es la dirección IP del gateway predeterminado de la PC?

Paso 2: Comenzar a capturar el tráfico de la NIC de la PC

a. Abra Wireshark.

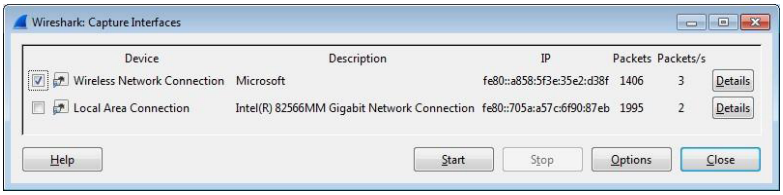
b. En la barra de herramientas Network Analyzer (Analizador de red) de Wireshark, haga clic en el ícono Lista de interfaces.

Figura 17. Ícono Lista de interfaces



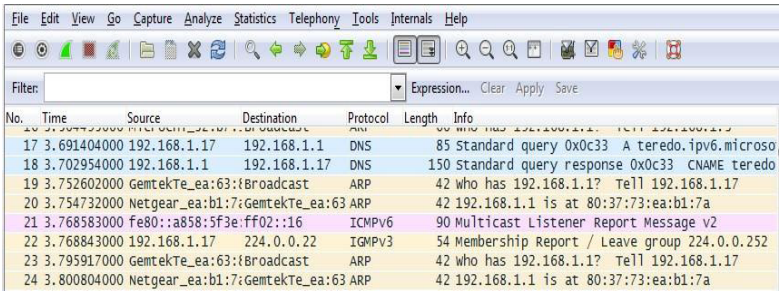
c. En la ventana Capture Interfaces (Capturar interfaces) de Wireshark (figura 18), haga clic en la casilla de verificación adecuada para seleccionar la interfaz en la cual comenzar la captura de tráfico. A continuación, haga clic en Start (Iniciar). Si no está seguro de qué interfaz revisar, haga clic en Details (Detalles) para obtener más información sobre cada interfaz de la lista.

Figura 18. Topología de enrutamiento: captura de interfaces



d. Observe el tráfico que aparece en la ventana Packet List (Lista de paquetes:

Figura 19. Ventana Packet List (lista de paquetes)

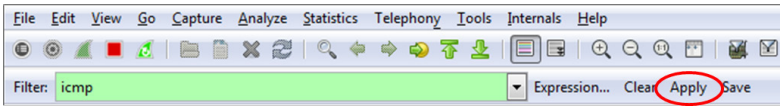


Paso 3: Filtrar Wireshark para que solamente se muestre el tráfico ICMP

Puede usar el filtro de Wireshark para bloquear la visibilidad del tráfico no deseado. El filtro no bloquea la captura de datos no deseados, sino lo que se muestra en pantalla. Por el momento, solo se debe visualizar el tráfico ICMP.

En el cuadro Filter (Filtro) de Wireshark, escriba icmp. Si escribió el filtro correctamente, el cuadro debe volverse de color verde. Si el cuadro está de color verde, haga clic en Apply (Aplicar) para que se aplique el filtro.

Figura 20. Cuadro Filter (Filtro) de Wireshark



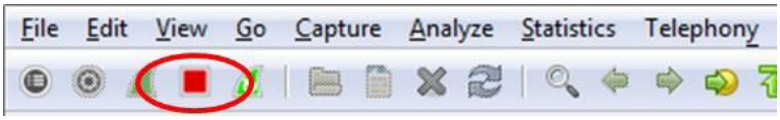
Paso 4: En la ventana del símbolo del sistema, hacer un ping al *gateway* predeterminado de la PC

En la ventana del símbolo del sistema, haga un ping al gateway predeterminado con la dirección IP registrada en el paso 1.

Paso 5: Dejar de capturar el tráfico de la NIC

Haga clic en el ícono Detener captura para dejar de capturar el tráfico.

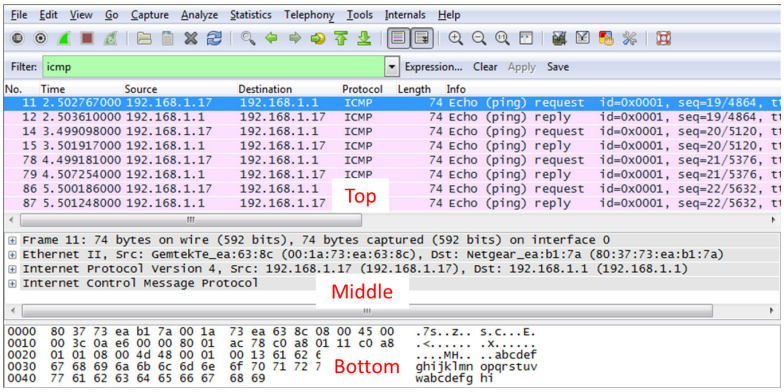
Figura 21. Ícono Detener captura



Paso 6: Examinar la primera solicitud de eco (*ping*) en Wireshark

La ventana principal de Wireshark se divide en tres secciones: el panel Packet List en la parte superior, el panel Packet Details (Detalles del paquete) en la parte central y el panel Packet Bytes (*bytes* del paquete) en la parte inferior. Si seleccionó la interfaz correcta para la captura de paquetes en el paso 3, Wireshark debería mostrar la información de ICMP en el panel Packet List (Lista de paquetes), de manera similar a la de la figura 22.

Figura 22. Ventana principal de Wireshark



a. En el panel Packet List (Lista de paquetes) de la parte superior, haga clic en la primera trama de la lista. Debería ver el texto **Echo (ping) request (Solicitud de eco [ping])** debajo del encabezado **Info** (Información). Con esta acción, se debe resaltar la línea con color azul.

b. Examine la primera línea del panel Packet Details (Detalles del paquete) de la parte central. En esta línea, se muestra la longitud de la trama (en el ejemplo, 74 bytes).

c. En la segunda línea del panel Packet Details (Detalles del paquete), se muestra que es una trama de Ethernet II. También se muestran las direcciones MAC de origen y de destino.

   ¿Cuál es la dirección MAC de la NIC de la PC?

   _____

   ¿Cuál es la dirección MAC del gateway predeterminado?

   _____

d. Puede hacer clic en el signo más (+) al principio de la segunda línea para obtener más información sobre la trama de Ethernet II. Observe que el signo ***más*** se transforma en un signo ***menos*** (-).

   ¿Qué tipo de trama se muestra?

   _____

e. En las últimas dos líneas de la parte central, se proporciona información sobre el campo de datos de la trama. Observe que los datos contienen información sobre las direcciones IPv4 de origen y de destino.

   ¿Cuál es la dirección IP de origen?

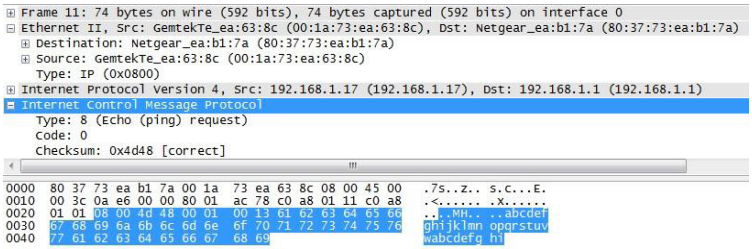
   _____

   ¿Cuál es la dirección IP de destino?

   _____

   Puede hacer clic en cualquier línea de la parte central para resaltar esa parte de la trama (hexadecimal y ASCII) en el panel Packet Bytes de la parte inferior. Haga clic en la línea **Internet Control Message Protocol** (Protocolo de mensajes de control de Internet) de la parte central y examine lo que se resalta en el panel Packet Bytes.

Figura 23. Topología de enrutamiento



¿Qué texto muestran los últimos dos octetos resaltados?

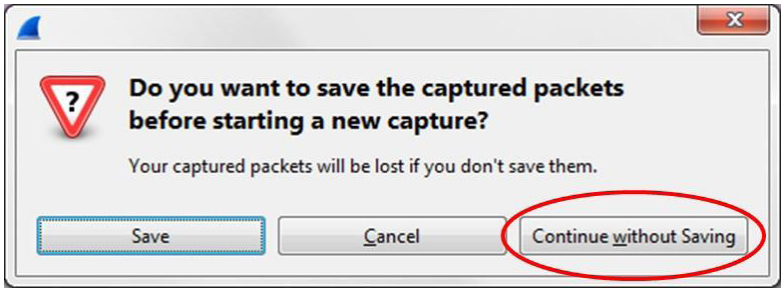
f. Haga clic en la siguiente trama de la parte superior y examine una trama de respuesta de eco. Observe que las direcciones MAC de origen y de destino se invirtieron porque esta trama se envió desde el router del gateway predeterminado como respuesta al primer ping.

   ¿Qué dispositivo y qué dirección MAC se muestran como dirección de destino?

Paso 7: Reiniciar la captura de paquetes en Wireshark

Haga clic en el ícono **Iniciar captura** para iniciar una nueva captura de Wireshark. Se muestra una ventana emergente que le pregunta si desea guardar los anteriores paquetes capturados en un archivo antes de iniciar la nueva captura. Haga clic en **Continue without Saving** (Continuar sin guardar).

Figura 24. Topología de enrutamiento



Paso 8: En la ventana del símbolo del sistema, haga ping a www.cisco.com

Paso 9: Dejar de capturar paquetes

Paso 10: Examinar los nuevos datos del panel de la lista de paquetes de Wireshark

En la primera trama de solicitud de eco (ping), ¿cuáles son las direcciones MAC de origen y de destino?

Origen _____

Destino _____

¿Cuáles son las direcciones IP de origen y de destino que contiene el campo de datos de la trama?

Origen _____

Destino _____

Compare estas direcciones con las direcciones que recibió en el paso 6. La única dirección que cambió es la dirección IP de destino. ¿Por qué cambió la dirección IP de destino mientras que la dirección MAC permaneció igual?

_____

_____

_____

_____

Semana 7

Enrutamiento estático

Sección: ..... Fecha: ...../...../2022 Duración: 270 min.

Docente: ..... Unidad: 2

Apellidos y nombres: .....

Instrucciones

A continuación, de manera colaborativa, siga las siguientes instrucciones.

I. Objetivo

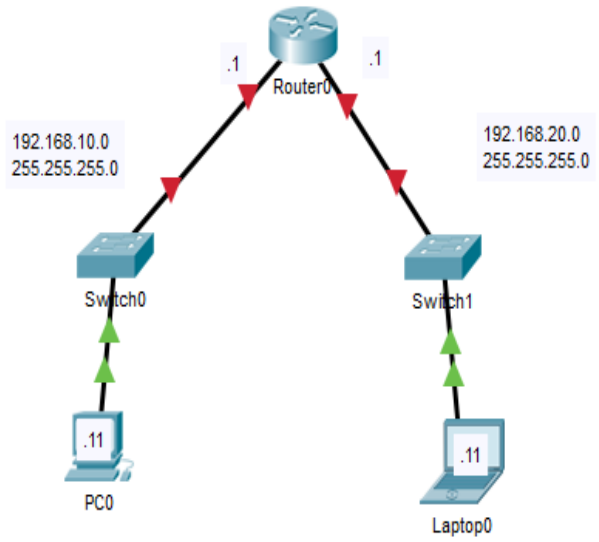
El estudiante será capaz de configurar rutas estáticas, de manera recursiva y directamente conectadas de forma básica e intermedia. En todos los casos se le pide que configure el direccionamiento IP y la configuración de rutas estáticas, de tal manera que los equipos finales que se hagan ping. Es decir, tengan conectividad, así sean de redes distintas.

II. Descripción de la actividad a realizar (práctica)

En esta actividad se va a realizar la configuración de rutas estáticas, de manera recursiva y directamente conectadas de forma básica e intermedia. En todos los casos se le pide que configure el direccionamiento IP y la configuración de rutas estáticas, de tal manera que los equipos finales hagan ping, es decir tengan conectividad, así sean de redes distintas.

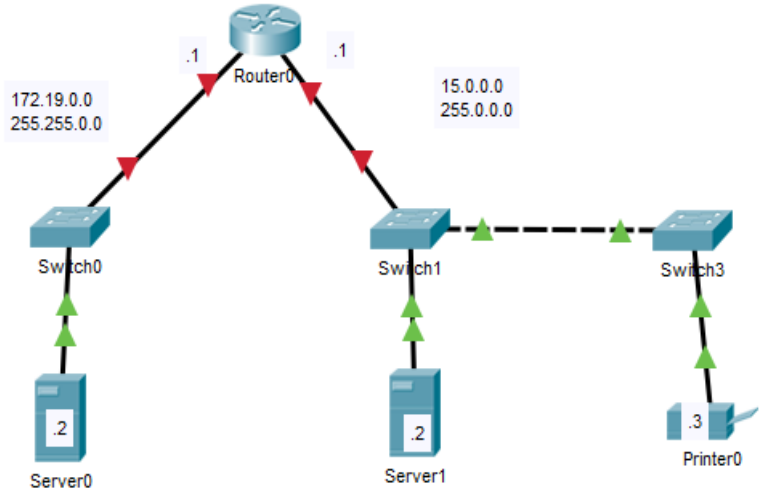
Práctica 1

Figura 25. Topología de enrutamiento



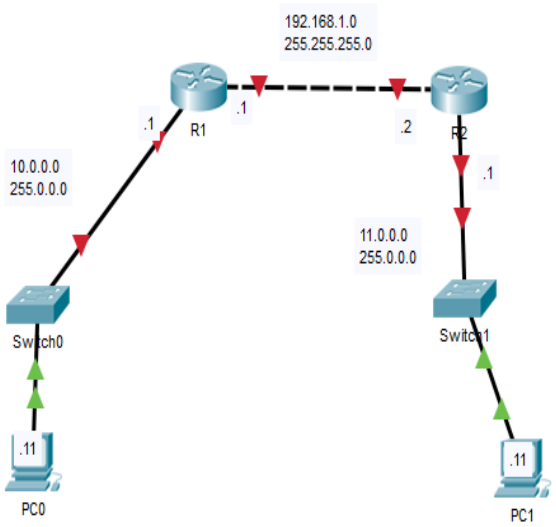
Práctica 2

Figura 26. Topología de enrutamiento



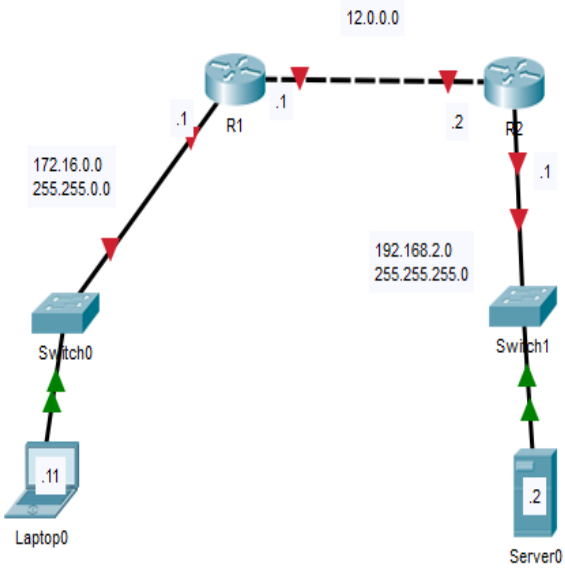
Práctica 3

Figura 27. Topología de enrutamiento



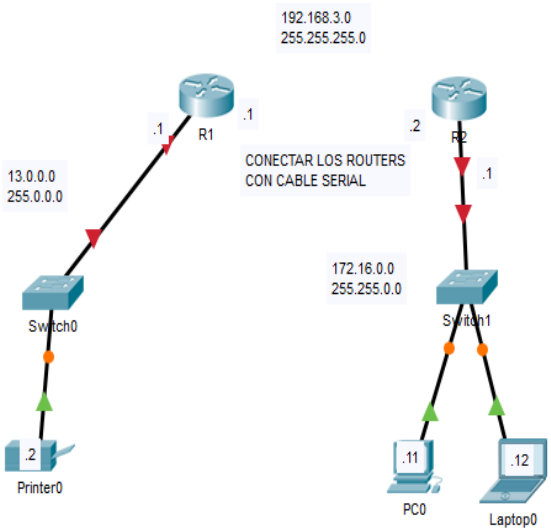
Práctica 4

Figura 28. Topología de enrutamiento



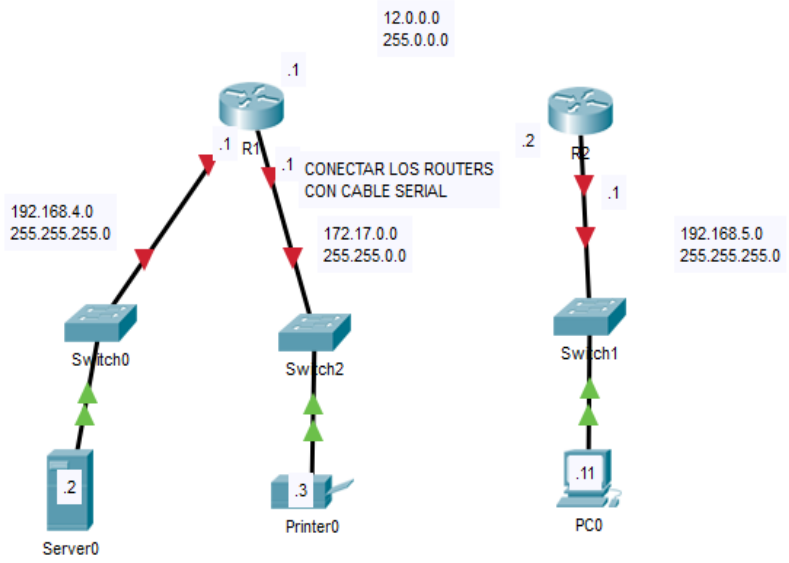
Práctica 5

Figura 29. Topología de enrutamiento



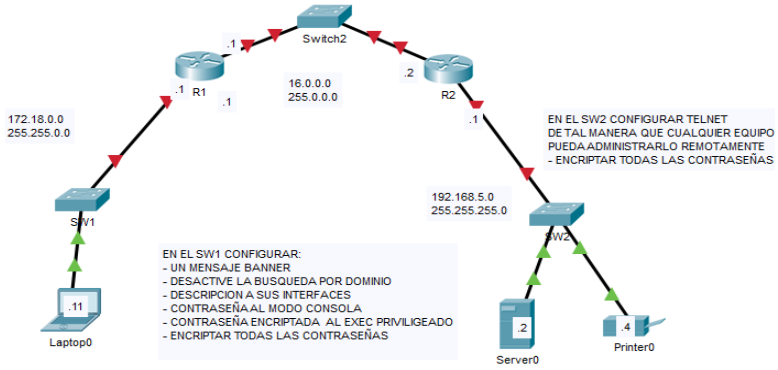
Práctica 6

Figura 30. Topología de enrutamiento



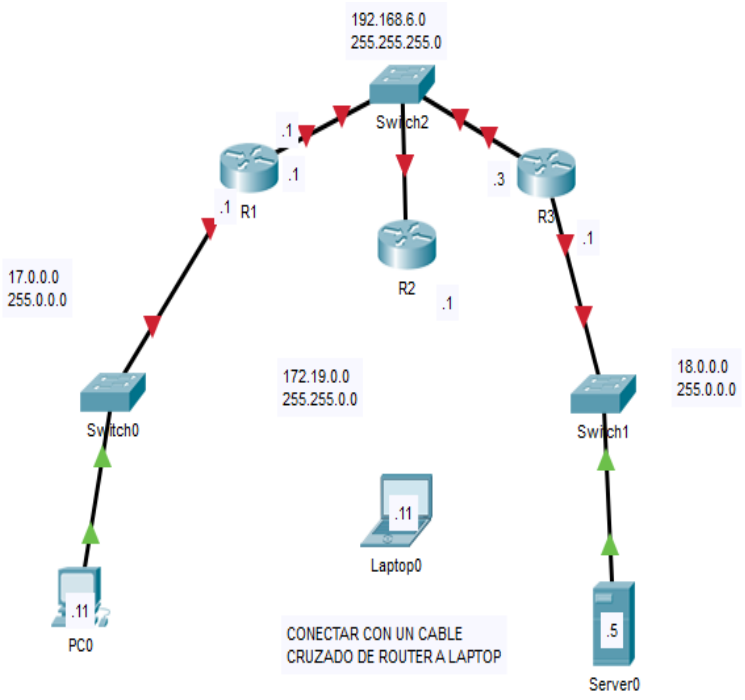
Práctica 7

Figura 31. Topología de enrutamiento



Práctica 8

Figura 32. Topología de enrutamiento



Práctica 9

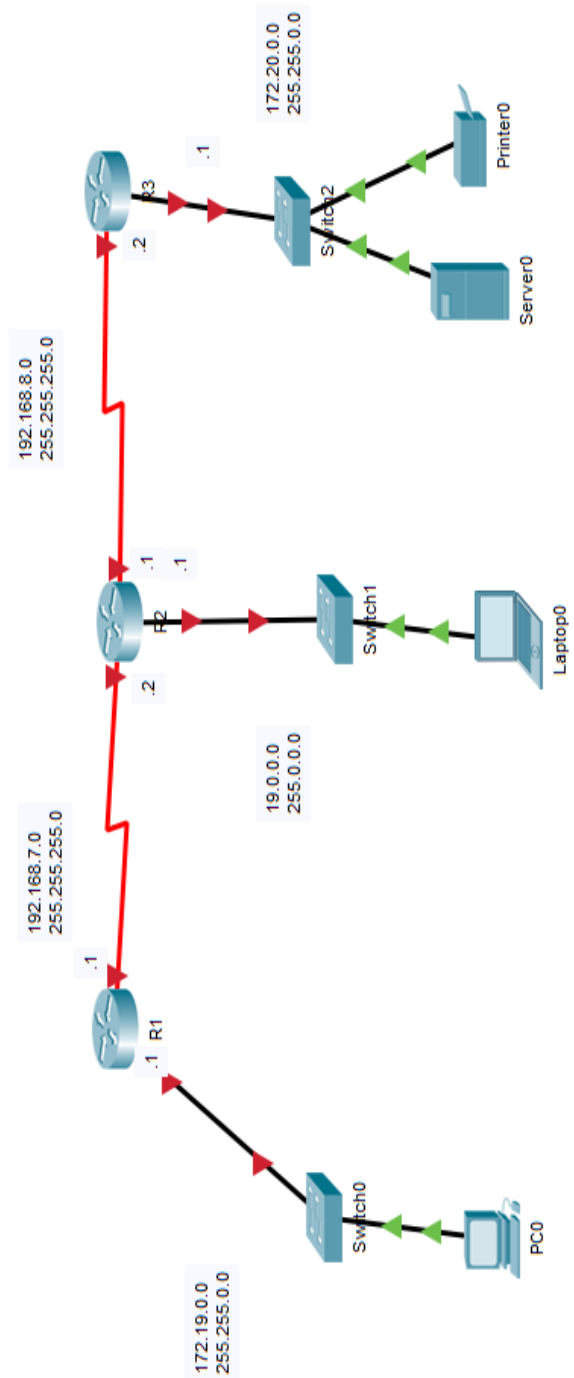


Figura 33. Topología de enrutamiento

Semana 8

Enrutamiento estático parte 2

Sección: ..... Fecha: ...../...../2022 Duración: 90 min.
Docente: ..... Unidad: 2
Apellidos y nombres: .....

Instrucciones

A continuación, de manera colaborativa, siga las siguientes instrucciones.

I. Objetivo

El estudiante será capaz de configurar rutas estáticas, de manera recursiva y directamente conectadas de forma básica e intermedia. En todos los casos se le pide que configure el direccionamiento IP y la configuración de rutas estáticas, de tal manera que los equipos finales que se hagan ping, es decir tengan conectividad, así sean de redes distintas.

II. Descripción de la actividad a realizar (práctica)

En esta actividad se va a realizar la configuración de rutas estáticas, de manera recursiva y directamente conectadas de forma básica e intermedia. En todos los casos se le pide configurar el direccionamiento IP y la configuración de rutas estáticas, de tal manera que los equipos finales hagan ping, es decir tengan conectividad, así sean de redes distintas.

Práctica 10

En el SW4 configurar Telnet, de tal manera que cualquier equipo le pueda hacer Telnet. Encriptar todas las contraseñas.

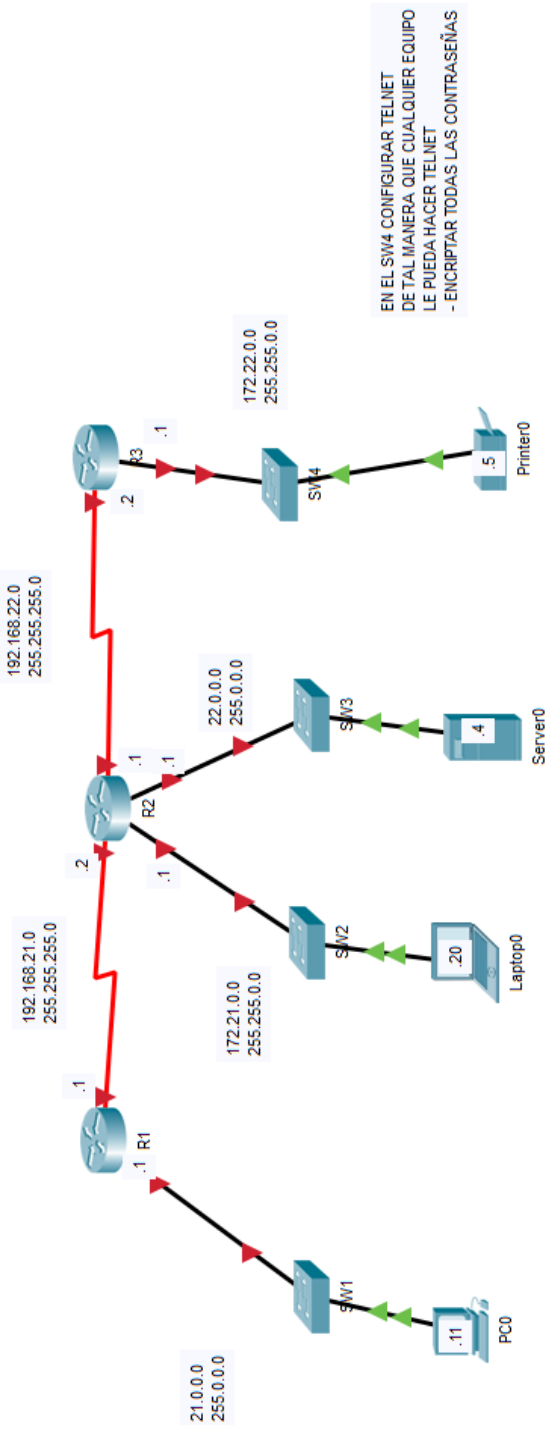
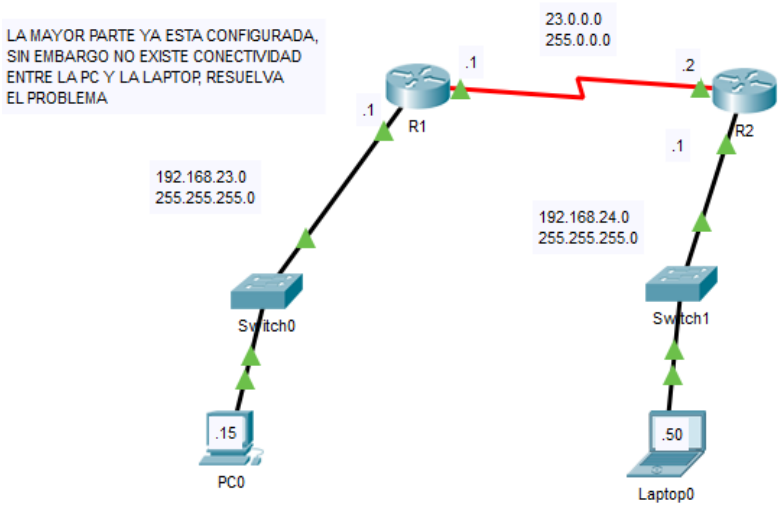


Figura 34. Topología de enrutamiento: configuración de rutas estáticas

Práctica 11

Restaurar la conectividad entre la PC y la laptop. La mayor parte ya está configurada.

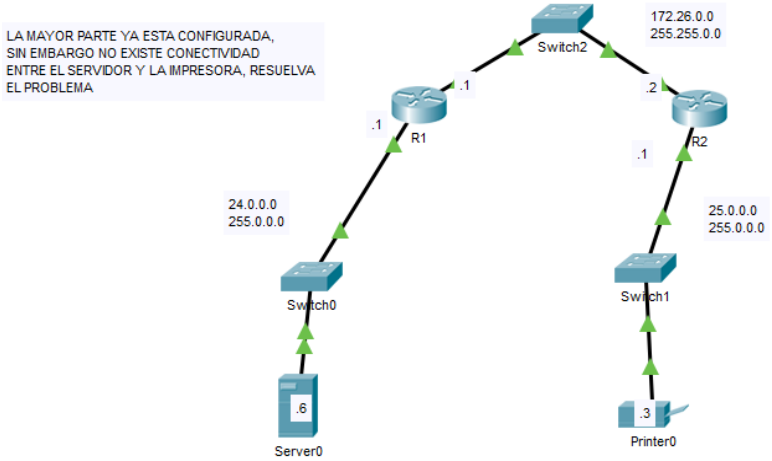
Figura 35. Topología de enrutamiento



Práctica 12

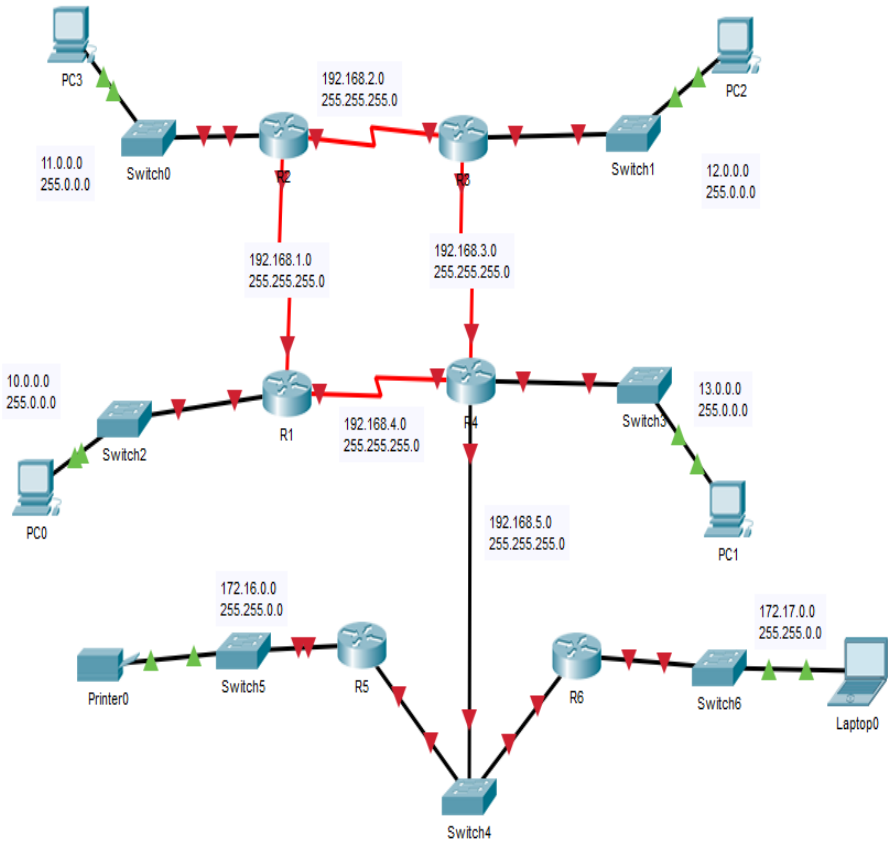
Restaurar la conectividad entre el servidor y la impresora. La mayor parte ya está configurada.

Figura 36. Topología de enrutamiento



Práctica 13

Figura 37. Topología de enrutamiento



Tercera Unidad

Semana 9

Direccionamiento IP

Sección: ..... Fecha: ...../...../2022 Duración: 120 min.
Docente: ..... Unidad: 3
Apellidos y nombres: .....

Instrucciones

A continuación, de manera colaborativa, siga las siguientes instrucciones.

I. Objetivo

El estudiante será capaz de examinar detalladamente la estructura de las direcciones IP y su aplicación en la construcción y la puesta a prueba de redes y subredes IP a través de diferentes ejercicios que se le proporcionará.

II. Descripción de la actividad a realizar (práctica)

En esta actividad se va a analizar la estructura de las direcciones IP y su aplicación en la construcción y la puesta a prueba de redes y subredes IP a través de diferentes ejercicios que se le proporcionará.

III. Procedimientos

1) **Conversión de binario a decimal**

   https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#7.1.1.5

2) **Conversión de decimal a binario**

   https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#7.1.1.8

3) **Juego de conversiones**

https://learningnetwork.cisco.com/docs/DOC-1803

4) **Cálculo de máscaras de subred y prefijos**

http://static-course-assets.s3.amazonaws.com/IT-N50ES/module9/index.html#9.1.3.9

5) **Cálculo de cantidad de host**

http://static-course-assets.s3.amazonaws.com/IT-N50ES/module9/index.html#9.1.3.14

6) **Bits por prestarse**

https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#8.1.4.4

7) **Cálculo de dirección de red**

https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#7.1.2.4

8) **Cálculo de direcciones de red-host-broadcast**

http://static-course-assets.s3.amazonaws.com/IT-N50ES/module9/index.html#9.1.3.15

Semana 10

Direccionamiento IPv4 e IPv6

Sección: ..... Fecha: ...../...../2022 Duración: 120 min.
Docente: ..... Unidad: 3
Apellidos y nombres: .....

Instrucciones

A continuación, de manera colaborativa, siga las siguientes instrucciones.

I. Objetivo

El estudiante será capaz de examinar detalladamente la estructura de las direcciones IPv6 y IPv4 y su aplicación en la construcción y la puesta a prueba de redes y subredes IP a través de diferentes ejercicios que se le proporcionará.

II. Descripción de la actividad a realizar (práctica)

En esta actividad se va a analizar la estructura de las direcciones IPv6 y Ipv4 y su aplicación en la construcción y la puesta a prueba de redes y subredes IP a través de diferentes ejercicios que se le proporcionará.

III. Procedimientos

1) **Representaciones de Ipv6**

   https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#7.2.2.4

2) **Cálculo de direcciones de broadcast, de red, y de host**

   http://static-course-assets.s3.amazonaws.com/ITN50ES/module8/index.html#8.1.3.7

Semana 11

Cálculo Ipv4 avanzado

Sección: ..... Fecha: ...../...../2022 Duración: 40 min.
Docente: ..... Unidad: 3
Apellidos y nombres: .....

Instrucciones

A continuación, de manera colaborativa, siga las siguientes instrucciones.

I. Objetivo

El estudiante será capaz de examinar detalladamente la estructura de las direcciones IPv6 y IPv4 y su aplicación en la construcción y la puesta a prueba de redes y subredes IP a través de diferentes ejercicios que se le proporcionará.

II. Descripción de la actividad a realizar (práctica)

En esta actividad se va a analizar la estructura de las direcciones IPv6 y IPv4 y su aplicación en la construcción y la puesta a prueba de redes y subredes IP a través de diferentes ejercicios que se le proporcionará.

III. Procedimientos

1) **De la siguiente dirección IP: 192.70.10.251, me piden subnetear para 13 *host*, ¿cuál será la tercera dirección de subred?**

2) **Si tengo la dirección de red. 172.50.0.0 y me piden hacer subneting para 28 *host*, ¿Cuál será la dirección de broadcast de la quinta subred?**

3) Si tengo una red para 800 *host*, haciendo el subneteo, ¿cuántas subredes podré obtener?

4) Si la siguiente dirección de red: 195.223.48.0, se considera como primera subred y me piden subnetear para 1500 *host*, ¿cuál será la sexta dirección de subred?

5) ¿Cuál será el prefijo de máscara de subred para 300 *host*?

6) Si tengo 36 *host* y deseo hacer subredes, ¿cuántos bits debo prestarme de izquierda a derecha en la máscara de red?

7) De la siguiente dirección IP: 165.100.131.0, me piden subnetear para 4500 *host*, ¿cuál será el rango de IP válidos para la cuarta subred?

Semana 12

Enrutamiento de subredes y VLSM

Sección: ..... Fecha: ...../...../2022 Duración: 120 min.
Docente: ..... Unidad: 3
Apellidos y nombres: .....

Instrucciones

A continuación, de manera colaborativa, siga las siguientes instrucciones.

I. Objetivo

El estudiante será capaz de configurar rutas estáticas, de manera recursiva y directamente conectadas haciendo uso de subredes y VLSM, de tal manera que los equipos finales que se hagan ping, es decir, que tengan conectividad, así sean de redes distintas.

También se configurarán servicios de red como DNS, WEB, correo y DHCP.

II. Descripción de la actividad a realizar (práctica)

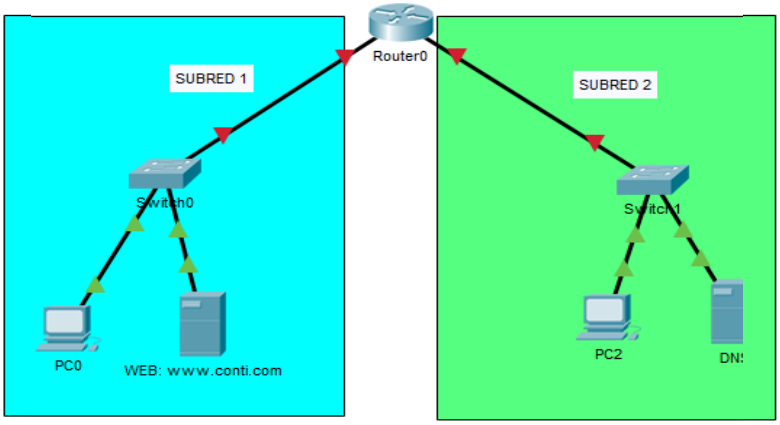
En esta actividad se va a realizar la configuración de las rutas estáticas, de manera recursiva y directamente conectadas haciendo uso de subredes y VLSM, de tal manera que los equipos finales hagan ping, es decir, que tengan conectividad, así sean de redes distintas.

III. Procedimientos

Ejercicio 1

Calcular las dos subredes. Ver Figura 38 en la siguiente página.
El IP otorgado es 195.185.175.195 /25

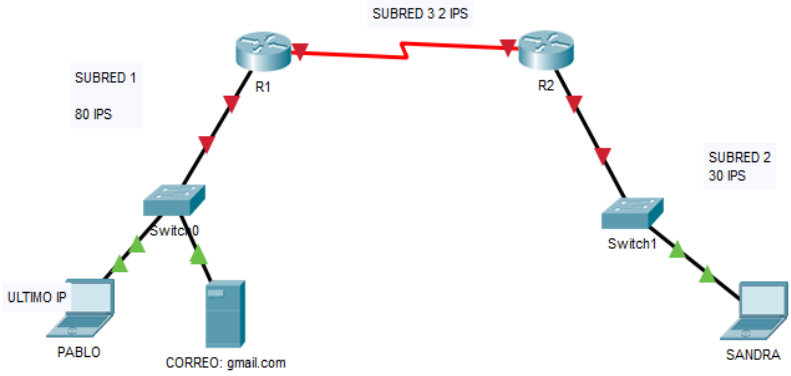
Figura 38. Topología de enrutamiento



Ejercicio 2

En la siguiente imagen, calcular el VLSM. El IP es 25.35.45.55 /12

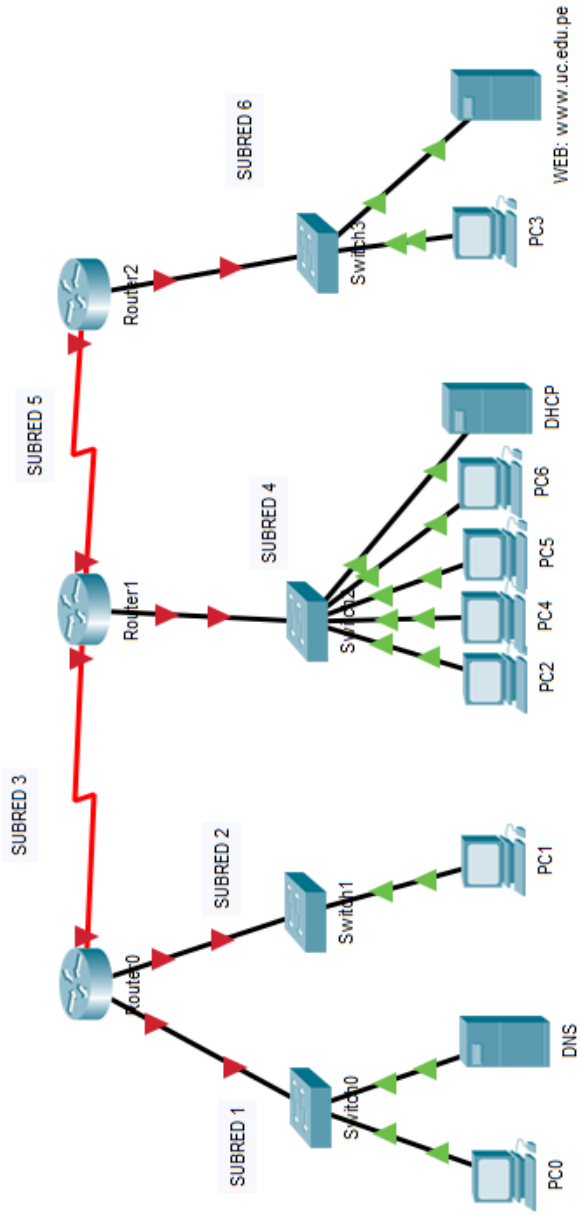
Figura 39. Topología de enrutamiento



Ejercicio 3

Brindar los últimos IP a la PC, y a los servidores brindar los segundos IP. La red es 172.16.0.0 /23.

Figura 40. Topología de enrutamiento



Ejercicio 4

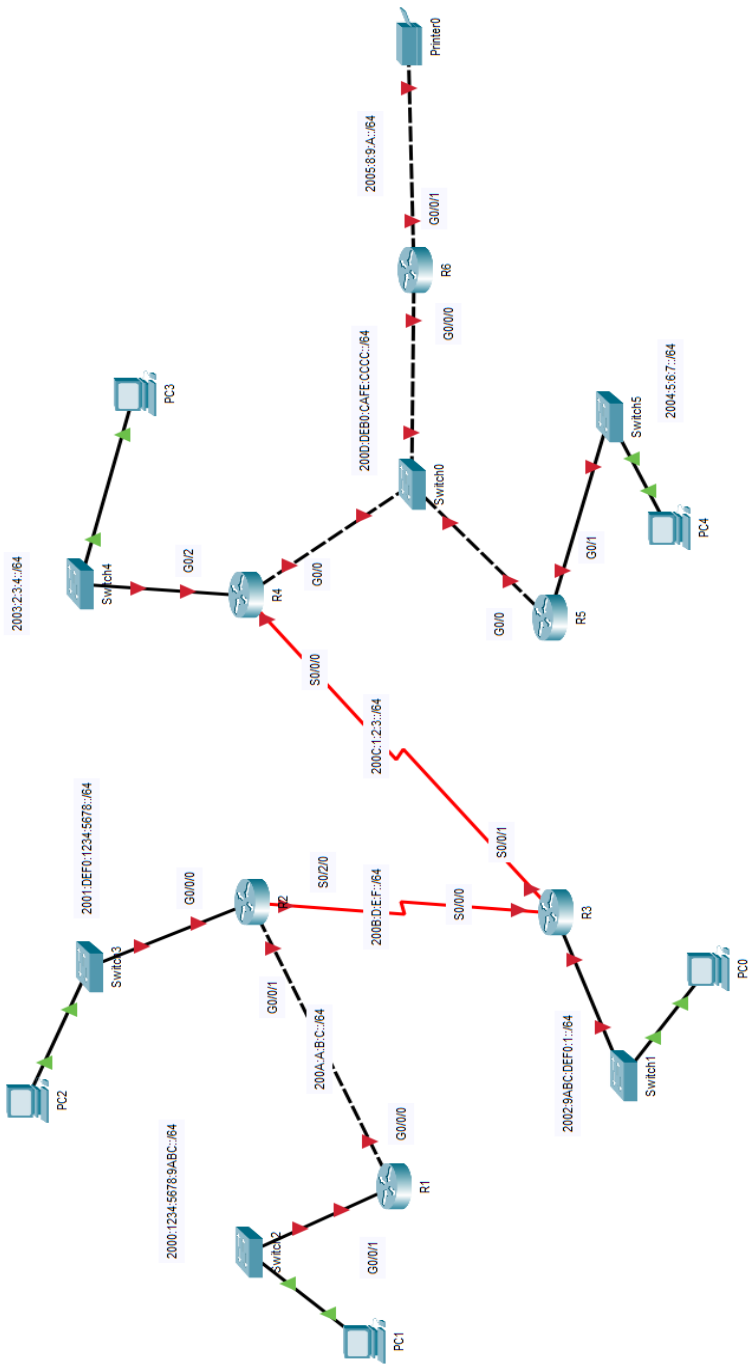


Figura 41. Topología de enrutamiento

Ejercicio 5

Calcular el VLSM. La red base es 15.0.0.0. A cada subred asignar los IPS como sigue:

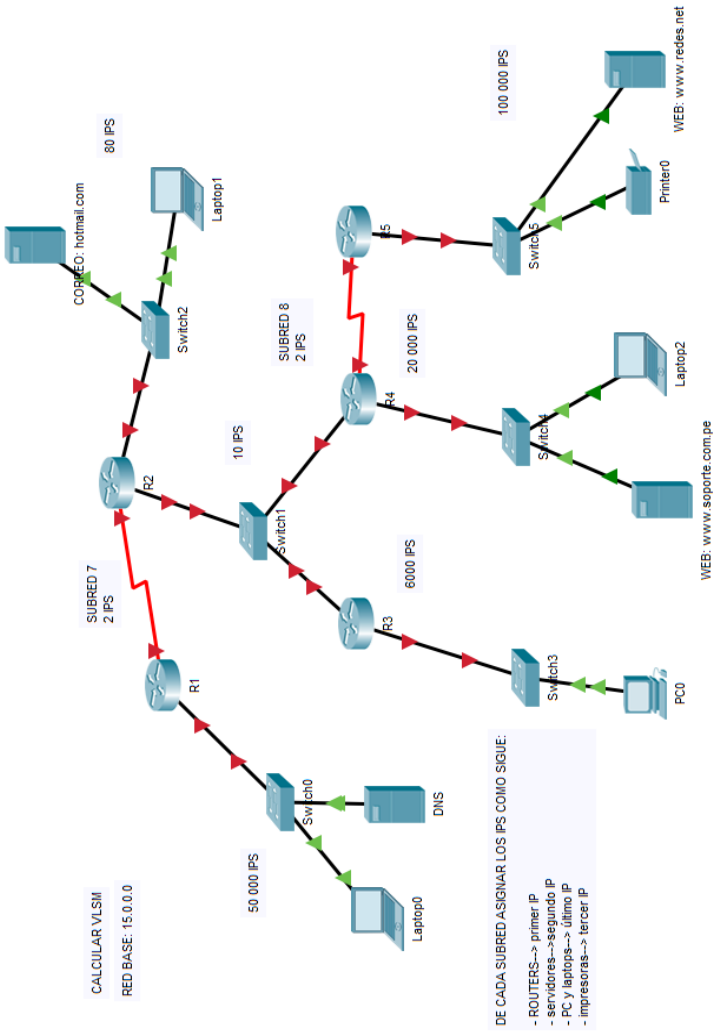
Routers: Primer IP

Servidores: segundo IP

PC y laptops: último IP

Impresoras: tercer IP

Figura 42. Topología de enrutamiento



Cuarta Unidad

Semana 13

Capa de aplicación

Sección: ..... Fecha: ...../...../2022 Duración: .....
Docente: ..... Unidad: 4
Apellidos y nombres: .....

Instrucciones

A continuación, de manera colaborativa, siga las siguientes instrucciones.

I. Objetivo

El estudiante será capaz de configurar rutas estáticas, de manera recursiva y directamente conectadas haciendo uso de subredes y VLSM, de tal manera que los equipos finales que se hagan ping, es decir tengan conectividad, así sean de redes distintas, a esto también se le integra los servicios de red como DNS, WEB, DHCP y correo.

II. Descripción de la actividad a realizar (práctica)

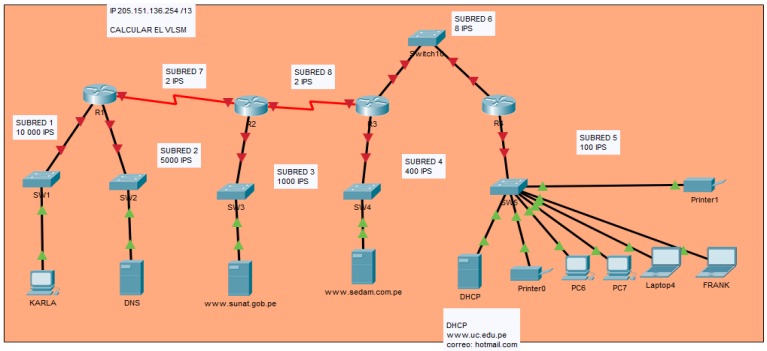
En esta actividad se va a realizar la configuración de las rutas estáticas, de manera recursiva y directamente conectadas haciendo uso de subredes y VLSM, de tal manera que los equipos finales hagan ping, es decir, que tengan conectividad, así sean de redes distintas.

III. Procedimientos

Ejercicio 1

Calcular el VLSM. Ver Figura 43 en la siguiente página.
El IP es 205.151.136.254 /13

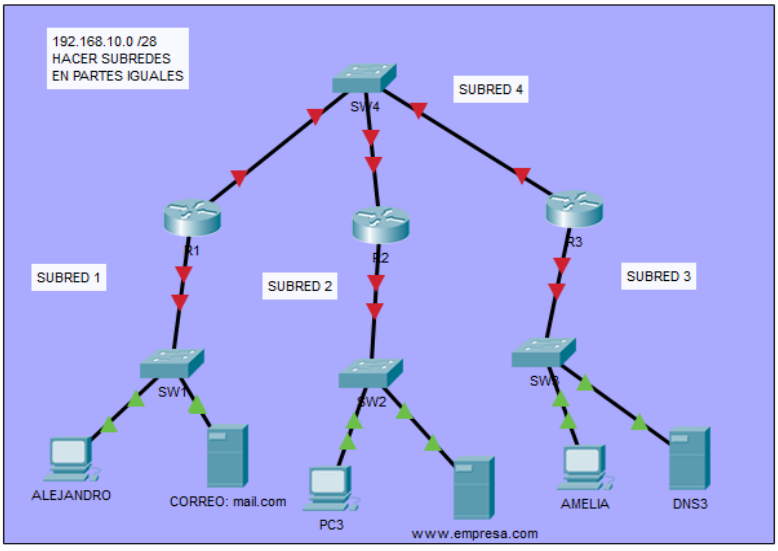
Figura 43. Topología de enrutamiento



Ejercicio 2

Hacer subredes en partes iguales. El IP es 192.168.10.0 /28

Figura 44. Topología de enrutamiento



Ejercicio 3

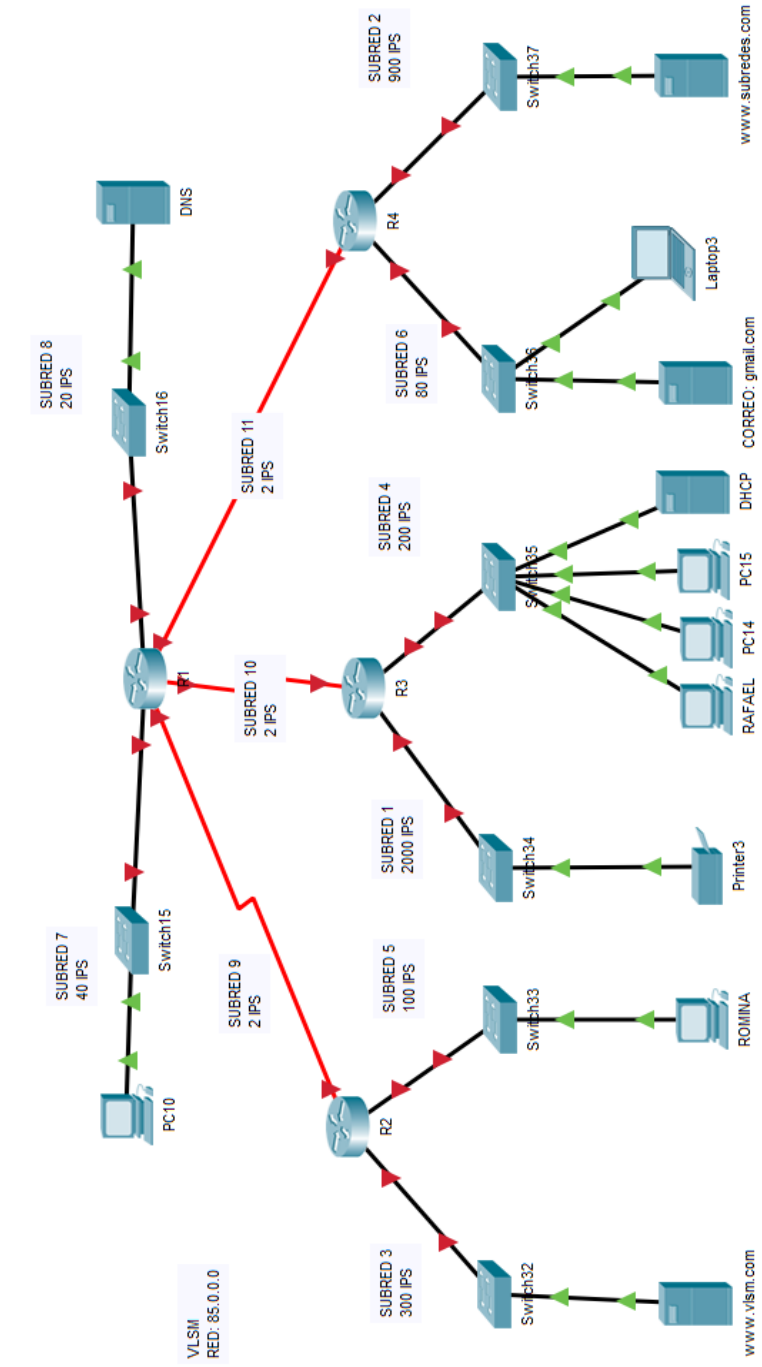


Figura 45. Topología de enrutamiento

Semana 14

Práctica *skill* de Cisco

Sección: ..... Fecha: ...../...../2022 Duración: .....
Docente: ..... Unidad: 4
Apellidos y nombres: .....

Instrucciones

A continuación, de manera colaborativa, siga las siguientes instrucciones.

I. Objetivo

El estudiante será capaz de configurar diferentes servicios aprendidos en el curso de manera integrada y estar preparado para rendir sus evaluaciones finales.

II. Descripción de la actividad a realizar (práctica)

En esta actividad se reforzará la configuración de diferentes servicios aprendidos en el curso de manera integrada y estar preparado para rendir sus evaluaciones finales.

III. Procedimientos

Tabla de direccionamiento

Dispositivo	Interface	IPv4 Address	Subnet Mask	IPv4 Default Gateway
		IPv6 Address		IPv6 Default Gateway
Sistemas	G0/0			N/A
		2001:AAAA:BBBB:1::1/64		N/A
	G0/1			N/A
		2001:BB:AAA:2::1/64		N/A
	Link Local	FE80::1		N/A

continúa...

...viene

Switch: PISO2	Vlan 1	N/A	N/A	N/A
L1	NIC	2001:AAAA:BBBB:1::11/64		
L2	NIC	2001:AAAA:BBBB:1::CC/64		
PC3	NIC	2001:BB:AAA:2::11/64		
TFTP Server	NIC	2001:BB:AAA:2::2/64		

Instrucciones

Paso 1: Determine el esquema de direccionamiento IP

- Diseñe un esquema de direccionamiento IPv4 y complete la tabla de direccionamiento en función de los siguientes requisitos. Usa la tabla para ayudarte a organizar tu trabajo.

Subnet Number	Beginning Address	Ending Address	Mask	Assignment
1	192.168.10.0			
2				
3				**PISO 1**
4				
5				
6				**PISO 2**

- Subnetee la red 192.168.10.0/24 para proporcionar 50 direcciones de host por subred y desperdiciando la menor cantidad de direcciones.
- Asigne la tercera subred a la LAN de **PISO1**.
- Asigne la última dirección de host de red (la más alta) en esta subred a la interfaz G0 / 1 en el *router* **SISTEMAS**.

- Comenzando con la quinta subred, calcular una nueva subred para que proporcionen 20 direcciones de host por subred y desperdicien la menor cantidad de direcciones.
- Asigne la segunda de estas nuevas subredes de 20 hosts a la LAN del **PISO2**.
- Asigne la última dirección de host de red (la más alta) en la subred LAN del **PISO2** a la interfaz G0 / 0 del *router* **SISTEMAS**.
- Asigne la penúltima dirección (la segunda más alta) en esta subred a la interfaz de la VLAN 1 del *switch* del **PISO2**.
- Configure las direcciones en los hosts usando cualquiera de las direcciones restantes en sus respectivas subredes.

Paso 2: Configurar el *router* SISTEMAS

Configure el *router* SISTEMAS con todas las configuraciones iniciales que haya aprendido en el curso hasta el momento:

- Configure el nombre de host del *router*: **SISTEMAS**.
- Configurar para que las contraseñas recién ingresadas deban tener una longitud mínima de diez caracteres.
- Proteja las configuraciones del dispositivo del acceso no autorizado con la contraseña del modo privilegiado encriptado.
- Asegure todas las líneas de acceso en el *router* utilizando los métodos cubiertos en el curso y los laboratorios.
- Evite que todas las contraseñas se vean en texto claro en los archivos de configuración del dispositivo.
- Configure la autenticación de usuario local para las conexiones de administración en banda. Cree un usuario con el nombre **juan** y una contraseña secreta de **Cisco12345**. Configurar para que las contraseñas recién ingresadas deban tener una longitud mínima de 10 caracteres y que brinde al usuario los privilegios administrativos más altos.

- Configure el *router* para que solo acepte conexiones de administración en banda a través del protocolo que sea más seguro que Telnet, como se hizo en los laboratorios. Use el valor 1024 para la intensidad de la clave de cifrado.
- Configure las dos interfaces Gigabit Ethernet utilizando los valores de direccionamiento IPv4 que calculó y los valores IPv6 provistos en la tabla de direccionamiento.
- Vuelva a configurar las direcciones **link local** al valor que se muestra en la tabla.
- Documente las interfaces en el archivo de configuración.

Paso 3: configura el switch del piso2

- Configure el *switch* del **piso2** para la administración remota a través de Telnet.
- Guardar los cambios.

Paso 4: configurar y verificar el direccionamiento del host

- Utilice el direccionamiento IPv4 del Paso 1 y los valores de direccionamiento IPv6 proporcionados en la tabla de direccionamiento para configurar todas las PC host con el direccionamiento correcto.
- Use la dirección **Link Local** de la interfaz del *router* como las puertas de enlace predeterminadas de IPv6 en los hosts.

Paso 5: haga una copia de seguridad de la configuración del router SISTEMAS en TFTP

- Complete la configuración del servidor TFTP utilizando los valores de direccionamiento IPv4 del Paso 1 y los valores en la tabla de direccionamiento.

- Haga una copia de seguridad de la configuración en ejecución del *router* **SISTEMAS** en el Servidor TFTP. Use el nombre de archivo predeterminado.

Haga una copia de seguridad de la configuración de inicio del *switch* **PISO2** en el Servidor TFTP. Use el nombre de archivo predeterminado.

Semana 15

Práctica reforzamiento

Sección: ..... Fecha: ...../...../2022 Duración: .....
Docente: ..... Unidad: 4
Apellidos y nombres: .....

Instrucciones

A continuación, de manera colaborativa, siga las siguientes instrucciones.

I. Objetivo

El estudiante será capaz de configurar diferentes servicios aprendidos en el curso de manera integrada y estar preparado para rendir sus evaluaciones finales.

II. Descripción de la actividad a realizar (práctica)

En esta actividad se reforzará la configuración de diferentes servicios aprendidos en el curso de manera integrada y estar preparados para rendir sus evaluaciones finales.

III. Procedimientos

Parte 1: Enrutamiento IPv6

Todos los equipos a excepción de los switches ya tienen direccionamieto IPv6. Configure ek enrutamiento y los correos de tal manera que Juan y Ana se manden mensajes. Ver Figura 46 en la siguiente página.

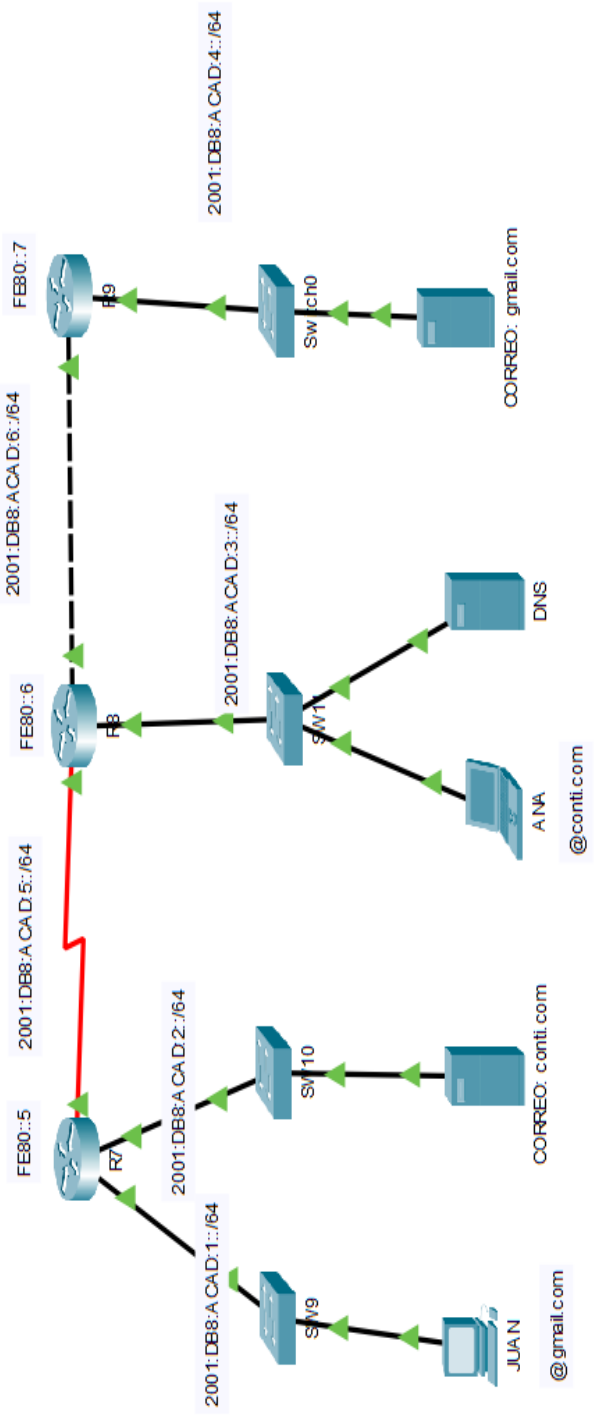


Figura 46. Topología de enrutamiento

Parte 2: Cálculo de subredes y direccionamiento IPv4

1) De la siguiente dirección de red: 192.70.10.0, me piden subnetear para 13 *host*, ¿cuál será la tercera dirección de subred?

2) Si tengo la dirección de red. 172.50.0.0 y me piden hacer subneting para 28 *host*, ¿cuál será la dirección de *broadcast* de la tercera subred?

3) Si tengo una red para 800 *host*, haciendo el subneteo ¿cuántas subredes podré obtener?

4) Si la siguiente dirección de red: 195.223.48.0, se considera como primera subred y me piden subnetear para 1500 *host*, ¿cuál será la quinta dirección de subred?

5) ¿Cuál será el prefijo de máscara de subred para 300 *host*?

6) Si tengo 36 *host*, y deseo hacer subredes, ¿cuántos bits debo de prestarme de izquierda a derecha en la máscara de red?

7) De la siguiente dirección de red: 165.100.0.0, me piden subnetear para 4500 *host*, ¿cuál será el rango de IP válidos para la 3ra subred?

Parte 3: Cálculo VLSM

1) Se plantea hacer VLSM

Tengo las siguientes áreas con su cantidad de dispositivos:

ÁREA 1 -->5

ÁREA 2 -->3

ÁREA 3 -->60

ÁREA 4 -->20

ÁREA 5 -->10

Me dan la red: 192.168.1.0

Responda cuál sería el rango de IP del área 5

2) Se plantea hacer VLSM

Tengo los siguientes pisos con su cantidad de IP requeridos:

PISO 1 -->200

PISO 2 -->100

PISO 3 -->400

PISO 4 -->50

PISO 5 -->30

ROUTERS-->2

Se da como red: 172.25.0.0

Responda cuál sería el rango de IP válidos para los routers

3) Se plantea hacer VLSM

Tengo los siguientes pabellones con su cantidad de IP requeridos:

PABELLÓN A -->2500

PABELLÓN B -->100

PABELLÓN C -->100 000

PABELLÓN D -->80

PABELLÓN E -->8000

PABELLÓN F-->20 000

ROUTERS ---->2 IP

Se da como red: 15.0.0.0

Responda cuál sería el último IP para el pabellón F

Bibliografía

Castillo, J. (2019). Redes de datos. *Contexto y evolución*. (3.ª ed.). Samsara Editorial.

Cisco NetWorking Academy (2021). *Curso CCNA v7. Introducción a las redes*. https://www.netacad.com

Davies, G. (2019). *Networking Fundamentals*. Birmingham. Packt Publishing Ltd.

Gerometta, O. (2018). *Guía de preparación para el examen de certificación CCNA R&S 200-125: versión 6.3*. Edubooks.

Kurose, J. y Ross, K. (2017). *Redes de computadoras. Un enfoque descendente*. (7.ª ed.). Pearson Educación, S. A.

NetWorking Academy Cisco (2019). *Curso CCNA – Módulo 1*. https://www.netacad.com

Oscar, G. (2018). *Guía de preparación para el examen de certificación CCNA R&S 200-125*. Edubooks.

Stalling, W. (2016). *Computer organization and architecture designing for performance*. (10.ª ed.). Pearson. https://bit.ly/336HpJ3