TECNOLÓGICO DE ESTUDIOS SUPERIORES DE ECATEPEC

DIVISIÓN DE INGENIERÍA ELECTRÓNICA Y TELEMÁTICA

PRÁCTICAS PARA LA REDES II

ASIGNATURA: REDES II

REALIZÓ:

MARÍA CRISTINA LEÓN DOMÍNGUEZ

SEPTIEMBRE 2009.

PRESENTACIÓN

El presente manual de prácticas fue realizado, para la asignatura de redes 2, el cual, intenta proporcionar a los docentes y estudiantes un material de apoyo que facilite el proceso enseñanza-aprendizaje, a través del trabajo en el laboratorio de cómputo, reforzando de esta manera, la teoría mostrada en el salón de clases.

Las prácticas de este manual, son presentadas para que el estudiante logre un aprendizaje significativo, debido a que están diseñadas de forma que el docente actúe como guía y el docente participe activamente, haciendo ejercicios de forma habitual y con el software de redes denominado *Packet Tracer*, versión 5.0, comparando ambos resultados.

Dicho lo anterior, se justifica el brindar a los alumnos un manual que los encamine a la aplicación de los conceptos teóricos, permitiendo profundizar más en los casos prácticos.

ÍNDICE

Practica # 1 Descripción general del direccionamiento IP

Objetivos.
Esta práctica de laboratorio se concentra en las siguientes tareas.

- Nombrar las distintas clases de direcciones IP.
- Describir las características y el uso de las distintas clases de direcciones IP.
- Determinar la parte de la dirección y de host IP.

Desarrollo.
Paso 1: Repaso de las clases de dirección IP y de sus características.
Hay 5 clases de direcciones IP (desde A hasta E). Sólo las primeras 3 clases se utilizan para fines comerciales. Para comenzar, discutiremos una dirección de red clase A de la tabla. La primera columna es la clase de dirección IP. La segunda columna es el primer octeto que se debe ubicar dentro del intervalo indicado para una clase de dirección determinada. La dirección Clase A debe comenzar con un número entre 1 y 126. El primer bit de una dirección clase "A" siempre es un cero, lo que significa que el Bit de primer nivel (HOB) o bit 128 no se puede usar. 127 se reserva para pruebas de loopback. El primer octeto por sí solo define el ID de red para una dirección de red clase A La máscara de subred por defecto usa exclusivamente unos binarios (255 decimal) para enmascarar los primeros 8 bits de la dirección clase A. La máscara de subred por defecto ayuda a los routers y hosts a determinar si el host destino está ubicado en esta red o en otra red. Dado que hay sólo 126 redes clase A, los 24 bits restantes (3 octetos) se pueden usar para los hosts. Cada red clase A puede tener 2^24 (2 elevado a la 24ta potencia) o más de 16 millones de hosts. Es común subdividir a la red en grupos más pequeños denominados subredes usando una máscara de subred personalizada, que se describirá en la siguiente práctica de laboratorio.

La parte de la dirección que corresponde a la red o al host no puede estar formada exclusivamente por unos o por ceros. Como ejemplo, la dirección clase A 118.0.0.5 es una dirección IP válida ya que la parte que corresponde a la red (los primeros ocho bits equivalen a 118) no está formada por sólo ceros y la parte que corresponde al host (los últimos 24 bits) no está formada por sólo ceros o sólo unos. Si la parte que corresponde al host estuviera constituida exclusivamente por ceros, esta sería la dirección de red misma. Si la parte que corresponde al host estuviera formada por sólo unos, sería un broadcast para la dirección de red. El valor de cualquiera de los octetos nunca puede ser mayor que 255 decimal o 11111111 binario.

Cls	**Intervalo decimal del 1er octeto**	**Bits de orden superior del 1er octeto**	**ID de Red / Host (N=Red, H=Host)**	**Máscara de subred por defecto**	**Cantidad de redes**	**Hosts por red** (direcciones utilizables)
A	1 - 126*	0	N.H.H.H	255.0.0.0	126 (2^7 - 2)	16,777,214 (2^{24} - 2)
B	128 - 191	1 0	N.N.H.H	255.255.0.0	16,382 (2^{14} - 2)	65,534 (2^{16} - 2)
C	192 - 223	1 1 0	N.N.N.H	255.255.255.0	2,097,150 (2^{21} - 2)	254 (2^8 - 2)
D	224 - 239	1 1 1 0	Reservado para multicast			
E	240 - 254	1 1 1 1 0	Experimental, se utiliza para fines de investigación			

* La dirección 127 Clase A no se puede utilizar y está reservada para funciones de evaluación del loop de prueba y diagnóstico

Paso 2: Direccionamiento IP básico.

Tarea: Use la tabla de direcciones IP y su conocimiento acerca de las clases de dirección IP para responder a las siguientes preguntas.

1. ¿Cuál es el intervalo decimal y binario del primer octeto para todas las direcciones IP clase "B" posibles?
   Decimal Desde: _____ Hasta: _____
   Binario Desde: _____ Hasta: _____
2. ¿Qué octeto u octetos representan la parte que corresponde a la red de una dirección IP clase C? _____
3. ¿Qué octeto u octetos representan la parte que corresponde al host de una dirección IP clase "A"? _____

Paso 3: Determinar la parte de la dirección IP que corresponde al host y a la red.

Tarea: Conociendo las siguientes direcciones de host IP, indique la clase de cada dirección, el ID o la dirección de red, la parte que corresponde al host, la dirección de broadcast para esta red y la máscara de subred por defecto.

Explicación: En el caso del ID de red, la parte que corresponde al host está formada sólo por ceros. Escriba sólo los octetos que componen el host. En el caso de un broadcast, la parte que corresponde al host está formada por todos unos. En el caso de una máscara de subred, la parte de la dirección que corresponde a la red está formada por todos unos.

1. Complete la siguiente tabla:

Dirección IP del host	Dirección Clase	Dirección de red	Dirección de host	Dirección de broadcast de red	Máscara de subred por defecto
216.14.55.137					
123.1.1.15					
150.127.221.244					
194.125.35.199					
175.12.239.244					

2. Dada una dirección IP **142.226.0.15**
   a. ¿Cuál es el equivalente binario del segundo octeto? _____
   b. ¿Cuál es la Clase de la dirección? _____
   c. ¿Cuál es la dirección de red de esta dirección IP? _____
   d. ¿Es ésta una dirección de host válida (S/N) ? _____
   e. ¿Por qué? (o por qué no)

   _____

   _____

   _____

3. ¿Cuál es la cantidad máxima de hosts que se pueden tener con una dirección de red clase C? _____
4. ¿Cuántas redes Clase B puede haber? _____
5. ¿Cuántos hosts puede tener cada red clase B ? _____
6. ¿Cuántos octetos hay en una dirección IP? _____ ¿Cuántos bits puede haber por octeto? _____

Paso 4: Determinar cuáles son las direcciones de host IP que son válidas para las redes comerciales.

Tarea: Determinar, para las siguientes direcciones de host IP, cuáles son las direcciones que son válidas para redes comerciales. ¿Por qué? o ¿Por qué no?

Explicación: Válida significa que se puede asignar a una estación de trabajo, servidor, impresora, interfaz de router, etc.

1. Complete la siguiente tabla.

Dirección IP	**¿La dirección es válida? (Sí/No)**	**¿Por qué? (o por qué no)**
150.100.255.255		
175.100.255.18		
195.234.253.0		
100.0.0.23		
188.258.221.176		
127.34.25.189		
224.156.217.73		

Practica # 2 Mascaras de Subred de Clase C

Objetivos:
Esta práctica de laboratorio se ocupa de las máscaras de subred Clase C y en su habilidad para cumplir con las siguientes tareas:

- Mencionar algunas de las razones por las cuales es necesaria la máscara de subred
- Diferenciar entre una Máscara de subred por defecto y una Máscara de subred personalizada
- Determinar las subredes disponibles con una dirección de red IP y una máscara de subred específica
- Dada una dirección de red y los requisitos de la cantidad de subredes y hosts, poder determinar cuál es la máscara de subred que se debe utilizar
- Dada una dirección de red y una máscara de subred, determinar la cantidad de subredes y de hosts por subred que se pueden crear así como también las subredes y cantidad de hosts utilizables.
- Usar el proceso de "AND" para determinar si una dirección de IP destino es Local o Remota
- Identificar direcciones de host válidas y no válidas basándose en un número de red y una máscara de subred dados

Desarrollo.
Paso 1 - Conceptos básicos sobre direcciones IP.
Explicación: Las direcciones de red IP son asignadas por el Centro de Informaciones de la Red de Internet (InterNIC). Si su empresa tiene una dirección de red IP clase "A", InterNIC asigna el primer octeto (8 bits) y la empresa puede usar los 24 bits restantes para definir hasta 16.777.214 hosts de la red. ¡Ésta es una gran cantidad de hosts! No es posible colocar todos estos hosts en una red física sin separarlos mediante routers y subredes. Una estación de trabajo puede estar ubicada en una red o subred y un servidor puede estar ubicado en otra red o subred. Cuando la estación de trabajo necesita recuperar un archivo del servidor, debe utilizar su máscara de subred para determinar la red o la subred en la que está ubicado el servidor. El propósito de una máscara de subred es ayudar a los hosts y routers a determinar la ubicación de la red en la que se puede ubicar al host destino. Consulte la siguiente tabla para repasar las clases de dirección IP, las máscaras de subred por defecto y la cantidad de redes y hosts que se pueden crear con cada clase de dirección de red.

Cls	Intervalo decimal del 1er octeto	Bits de orden superior del 1er octeto	ID de Red / Host (N=Red, H=Host)	Máscara de subred por defecto	Cantidad de redes	Hosts por red (direcciones utilizables)
A	1 - 126*	0	N.H.H.H	255.0.0.0	126 (2^7 - 2)	16.777.214 (2^{24} - 2)
B	128 - 191	1 0	N.N.H.H	255.255.0.0	16.382 (2^{14} - 2)	65.534 (2^{16} - 2)
C	192 - 223	1 1 0	N.N.N.H	255.255.255.0	2.097.150 (2^{21} - 2)	254 (2^8 - 2)
D	224 - 239	1 1 1 0	Reservado para multicast			
E	240 - 254	1 1 1 1 0	Experimental, se utiliza para fines de investigación			

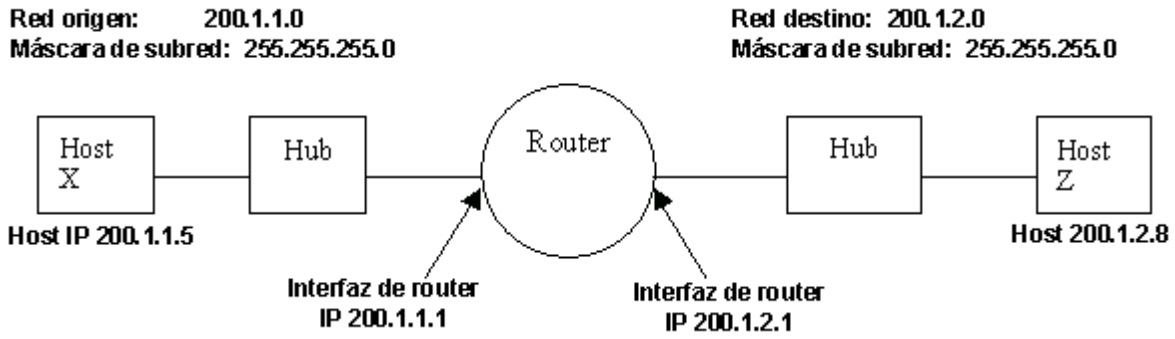
Paso 2: El proceso de "AND".

Explicación: Los hosts y routers utilizan el proceso de "AND" para determinar si un host destino está ubicado o no en la misma red. El proceso de AND se ejecuta cada vez que un host desea enviar un paquete hacia otro host de una red IP. Si desea conectarse a un servidor, es posible que conozca la dirección IP del servidor al que se desea conectar o simplemente puede escribir el nombre del host (por ej., www.cisco.com) y un Servidor de denominación de dominio (DNS) convertirá el nombre de host en una dirección IP. En primer lugar, el host origen compara (AND) su propia dirección IP con su propia máscara de subred. El resultado de AND es identificar la red en la que reside el host origen. Luego compara la dirección IP destino con su propia máscara de subred. El resultado del 2do AND es la red en la que está ubicado el host destino. Si las direcciones de red origen y destino son las mismas, se pueden comunicar directamente. Si los resultados son distintos, entonces están ubicados en distintas redes o subredes y se deben comunicar a través de routers o es posible que no se puedan comunicar en absoluto.

AND depende de la máscara de subred. La máscara de subred por defecto para una red Clase C es 255.255.255.0 ó 11111111.11111111.11111111.00000000. Esta se compara bit por bit con la dirección IP origen. El primer bit de la dirección IP se compara con el primer bit de la máscara de subred y el segundo bit se compara con el segundo, etc. Si los dos bits son unos, el **resultado de AND es un UNO**. Si los dos bits son cero y un uno o dos ceros, el **resultado de AND es un CERO**. Básicamente, esto significa que una combinación de 2 unos da como resultado un UNO, cualquier otra combinación da como resultado cero. El resultado del proceso de AND es el número de red o de subred en la que está ubicada la dirección origen o destino.

Paso 3: Dos redes Clase C que utilizan la máscara de subred por defecto.

Explicación: Este ejemplo muestra la forma en que se puede utilizar una máscara de subred por defecto Clase C para determinar cuál es la red en la que está ubicado un host. Una máscara de subred por defecto no separa una dirección en subredes. Si se utiliza la máscara de subred por defecto, la red no se "divide en subredes". El host X (origen) de la red 200.1.1.0 tiene una dirección IP 200.1.1.5 y desea enviar un paquete al host Z (destino) de la red 200.1.2.0 y tiene una dirección IP 200.1.2.8. Todos los hosts de cada red están conectados a hubs o switches y luego a un router. Recuerde que en el caso de una dirección de red Clase C, el American Registry for Internet Numbers (ARIN) asigna los 3 primeros octetos (24 bits) como la dirección de red de modo que estas son dos redes Clase C distintas. Esto deja un octeto (8 bits) para los hosts de modo que cada red Clase C puede tener hasta 254 hosts (2^8 = 256 - 2 = 254).



El proceso de AND ayuda a que el paquete llegue desde el host 200.1.1.5 de la red 200.1.1.0 hasta el host 200.1.2.8 de la red 200.1.2.0 siguiendo estos pasos.

a. El host X compara su propia dirección IP con su propia máscara de subred utilizando el proceso de AND

Dirección IP del host X 200.1.1.5	11001000.00000001.00000001.00000101
Máscara de subred 255.255.255.0	11111111.11111111.11111111.00000000
Resultado de AND (200.10,1.0)	11001000.00000001.00000001.00000000

NOTA: El resultado del paso 3a del proceso de AND es la dirección de red del host X, que es 200.1.1.0

b. A continuación, el host X compara la dirección IP del Host Z destino con su propia máscara de subred utilizando el proceso de AND.

Dirección IP del Host Z 200.1.2.8	11001000.00000001.00000010.00001000
Máscara de subred 255.255.255.0	11111111.11111111.11111111.00000000
Resultado de AND (200.1.2.0)	11001000.00000001.00000010.00000000

NOTA: El resultado del paso 3b del proceso de AND es la dirección de red del host Z, que es 200.1.2.0.

El host X compara los resultados de AND del paso A y el resultado de AND del paso B y observa que son distintos. Ahora el host X sabe que el host Z no está ubicado en su Red de área local (LAN) y que debe enviar el paquete hacia su "Gateway por defecto", que es la dirección IP de la interfaz del router de 200.1.1.1 de la red 200.1.1.0. Luego el router repite el proceso de AND para determinar cuál es la interfaz del router a través de la cual debe enviar el paquete.

Paso 4: Red Clase C que utiliza una máscara de subred personalizada.

Explicación: En este ejemplo se utiliza una sola dirección de red Clase C (200.1.1.0) y se mostrará cómo se puede utilizar una máscara de subred Clase C personalizada para determinar cuál es la subred en la que está ubicado un host y cómo enrutar paquetes desde una subred a otra. Recuerde que en el caso de una dirección de red Clase C, ARIN asigna los 3 primeros octetos (24 bits) como la dirección de red. Esto deja 8 bits (un octeto) para los hosts de modo que cada red Clase C puede tener hasta 254 hosts (2^8 = 256 - 2 = 254).

Tal vez desea tener menos de 254 hosts (estaciones de trabajo y servidores) en una red y desea crear 2 subredes y separarlos utilizando un router por motivos de seguridad o para reducir el tráfico. Esto hará que se creen dominios de broadcast más pequeños e independientes y puede mejorar el desempeño de la red y aumentar la seguridad ya que estas subredes estarán separadas por un router. Suponga que necesita por lo menos 2 subredes y 50 hosts por subred. Como sólo tiene una dirección de red Clase C, sólo tiene 8 bits disponibles en el cuarto octeto para un total de 254 hosts posibles, debe crear una máscara de subred personalizada. Utilizará la máscara de subred personalizada para "PEDIR PRESTADOS" bits de la parte de la dirección que corresponde al host. Los siguientes pasos lo ayudarán a lograr esto:

a. El primer paso para "realizar la división en subredes" es determinar cuántas subredes se necesitan. En este caso, se necesitan 2 subredes. Para ver cuántos bits se deben pedir prestados a la parte de la dirección de red que corresponde al host, agregue los valores de bit de derecha a izquierda hasta que el total sea igual o mayor que la cantidad de subredes que se necesitan. Como se necesitan 2 subredes, agregue el bit uno y el bit dos, lo que equivale a tres. Esta cantidad es mayor que la cantidad de subredes que son necesarias, de modo que se deben pedir prestados por lo menos dos bits de la dirección de host comenzando desde el lado izquierdo del octeto que contiene la dirección host.

Dirección de red 200.1.1.0								
4to octeto de bits de la dirección de host:	1	1	1	1	1	1	1	1
Valores de bits de la dirección de host (desde la derecha)	128	64	32	16	8	4	**2**	**1**

(Agregue bits desde el lado derecho (el 1 y el 2) hasta obtener una cantidad mayor que la del número de subredes que son necesarias)

b. Una vez que sabemos cuántos bits se deben pedir prestados, los bits se toman empezando por el lado izquierdo del primer octeto de la dirección host. Cada bit que se le pide prestado al host hace que queden menos bits para los hosts. Aunque la cantidad de subredes aumenta, la cantidad de hosts por subred disminuye. Como se deben pedir prestados 2 bits del lado izquierdo, se debe indicar ese nuevo valor en la máscara de subred. La máscara de subred por defecto era 255.255.255.0 y la nueva máscara de subred "personalizada" es 255.255.255.192. El 192 proviene del valor de los dos primeros bits de la izquierda (128 + 64 = 192). Ahora estos bits se transforman en 1 (unos) y forman parte de la máscara de subred general. Esto deja 6 bits para las direcciones IP de host o 2^6 = 64 hosts por subred.

Bits prestados por el 4to octeto para subred:	**1**	**1**	1	1	1	1	1	1
Valores de bits de subred: (desde la izquierda)	**128**	**64**	32	16	8	4	2	1

Con esta información, puede crear la siguiente tabla. Los dos primeros bits son el valor binario de la subred. Los últimos 6 bits son los bits del host. Al pedir prestados 2 bits de los 8 bits de la dirección de host, se pueden crear 4 subredes con 64 hosts cada una. Las 4 redes creadas son la red "0", la red "64", la red "128" y la red "192". La red "0" y la red "192" se

consideran no utilizables. Esto se debe a que la red "0" tiene sólo ceros en la parte de la dirección que corresponde a la subred y la red 192 tiene sólo unos en la parte de la dirección que corresponde a la subred.

Nro. de subred	Valor binario de los bits de subred prestados	Valor decimal de los bits de subred	Valores (intervalo) binarios posibles de bits de host (6 bits)	Intervalo en decimales de subred / Host	¿Utilizables?
Subred 0	00	0	000000 - 111111	0 - 63	NO
Subred 1	01		64 000000 - 111111	64 - 127	SÍ
Subred 2	10		128 000000 - 111111	128 - 191	SÍ
Subred 3	11		192 000000 - 111111	192 - 254	NO

Tenga en cuenta que la primera subred siempre comienza en 0 y, en este caso, aumenta de 64 en 64 que es la cantidad de hosts de cada subred. Una de las formas en que se puede determinar la cantidad de hosts de cada subred o el inicio de cada subred es elevar los bits de host restantes al cuadrado. Como se han pedido prestados dos de los 8 bits para subredes y quedan seis bits, la cantidad de hosts por subred es 2^6 ó 64. Otra de las formas para calcular la cantidad de hosts por subred o el "incremento" de una subred a la siguiente es restar el valor de la máscara de subred en decimales (192 en el cuarto octeto) a 256 (que es la cantidad máxima de combinaciones de 8 bits posibles) que equivale a 64. Esto significa que se comienza en 0 para la primera red y se agrega 64 para cada subred adicional. Si se toma la segunda subred (la red 64) como ejemplo de la dirección IP 200.1.1.64 no se puede utilizar para un ID de host porque es el "ID de red" de la subred "64" (la parte que corresponde al host son todos ceros) y la dirección IP 200.1.1.127 no se puede utilizar porque es la dirección de broadcast de la red 64 (la parte que corresponde al host son todos unos).

Paso 5: Red Clase C que utiliza una máscara de subred personalizada.

Tarea: Use la siguiente información y los ejemplos anteriores para responder las siguientes preguntas sobre las subredes.

Explicación: Su empresa ha presentado una solicitud para una dirección de red Clase C 197.15.22.0 que ha sido aprobada. Desea subdividir la red física en 4 subredes, interconectadas por routers. Necesitará por lo menos 25 hosts por subred. Deberá utilizar una máscara de subred personalizada Clase C y tendrá un router entre las subredes para enrutar el paquete desde una subred a otra. Determine la cantidad de bits que debe pedir prestados a la parte de la dirección de red que corresponde al host y luego la cantidad de bits que quedan para las direcciones de host. (Ayuda: Habrá 8 subredes)

1. Complete la tabla que aparece a continuación y responda las siguientes preguntas:

No. de subred	Valor binario de los bits de subred prestados	Nro. de subred decimal y de los bits de subred.	Valores (intervalo) binarios posibles de bits de host (6 bits)	Intervalo en decimales de subred / Host	¿Utilizar?
Subred 0					
Subred 1					
Subred 2					
Subred 3					
Subred 4					
Subred 5					
Subred 6					
Subred 7					

PREGUNTAS: Use la tabla que ha desarrollado anteriormente como ayuda para responder las siguientes preguntas:

2. ¿Qué octeto u octetos representan la parte que corresponde a la red de una dirección IP Clase C?

_____

3. ¿Qué octeto u octetos representan la parte que corresponde al host de una dirección IP Clase C?

_____

4. ¿Cuál es el equivalente binario de la dirección de red Clase C en el ejemplo (197.15.22.0)?
   Dirección de red en decimales: _____ . _____ . _____ . _____
   Dirección de red en binarios: _____ . _____ . _____ . _____
5. ¿Cuántos bits de orden superior se pidieron prestados a los bits de host en el cuarto octeto?

_____

6. ¿Cuál es la máscara de subred que debe usar (mostrar la máscara de subred en decimales y binarios)?
   Máscara de subred en decimales: _____ . _____ . _____ . _____
   Máscara de subred en binarios: _____ . _____ . _____ . _____
7. ¿Cuál es la cantidad máxima de subredes utilizables que se pueden crear con esta máscara de subred?

_____

8. ¿Cuál es la cantidad máxima de subredes utilizables que se pueden crear con esta máscara?

_____

9. ¿Cuántos bits quedaron en el 4to octeto para los ID de hosts?

_____

10. ¿Cuántos hosts por subred se pueden definir con esta máscara de subred?

_____

11. ¿Cuál es la cantidad máxima de hosts que se pueden definir para todas las subredes para este ejemplo (suponiendo que no se pueden utilizar los números más bajos y más altos de subred ni los ID de host más bajo y más alto de cada subred) ?

_____

12. ¿Es 197.15.220.63 una dirección IP de host válida para este ejemplo?

_____

13. ¿Por qué? (o por qué no)

_____

14. ¿Es 197.15.22.160 una dirección IP de host válida para este ejemplo?

_____

15. ¿Por qué? (o por qué no)

_____

16. El host "A" tiene una dirección IP 197.15.22.126. El host "B" tiene una dirección IP 197.15.22.129. ¿Estos hosts están ubicados en la misma subred?

¿Por qué?

Practica # 3 Mascaras de Subred de Clase B

Objetivos:
Esta práctica de laboratorio se concentrará en su capacidad para realizar las siguientes tareas:

- Trabajar con direcciones de red y subredes Clase B
- Determinar las subredes disponibles con una dirección de red IP y una máscara de subred específica
- Dados una dirección y requisitos de red, ser capaz de determinar la cantidad de subredes y hosts
- Poder determinar el tipo de máscara de subred que se debe utilizar para asignar la cantidad adecuada de hosts y subredes
- Asignar direcciones IP y máscaras de subred a los hosts y las interfaces del router
- Utilizar el proceso "AND" para rastrear un paquete IP desde un host local hasta un host remoto a través de un router

Desarrollo.
Paso 1 - Conceptos básicos sobre direcciones IP
Explicación: Para fines de referencia, se incluye aquí la tabla de direccionamiento IP. ARIN asigna las direcciones de red IP. Usted trabajará con una red Clase B.

Cls	1er Octeto de intervalo decimal	1er Octeto de bits de alto nivel	ID de Red / Host (N=Red, H=Host)	Máscara de subred por defecto	Cantidad de redes	Hosts por red (direcciones utilizables)
A	1 - 126*	0	N.H.H.H	255.0.0.0	126 (2^7 - 2)	16.777.214 (2^{24} - 2)
B	128 - 191	1 0	N.N.H.H	255.255.0.0	16.382 (2^{14} - 2)	65.534 (2^{16} - 2)
C	192 - 223	1 1 0	N.N.N.H	255.255.255.0	2.097.150 (2^{21} - 2)	254 (2^8 - 2)
D	224 - 239	1 1 1 0	Reservado para multicast			
E	240 - 254	1 1 1 1 0	Experimental, se utiliza para fines de investigación			

Paso 2 - Dirección de red Clase B con 3 subredes.

Tarea: Use la información que aparece a continuación y la de las prácticas de laboratorio anteriores para ayudar a determinar las subredes y las direcciones IP de host válidas. Responda las siguientes preguntas.

Explicación: Su institución tiene una dirección de red Clase B 150.193.0.0. Esta dirección de red Clase B se subdividirá para albergar la red física y necesitará por lo menos 50 subredes interconectadas con routers. Cada subred debe poder acomodar por lo menos 750 hosts por subred (estaciones de trabajo, servidores e interfaces de routers). En su calidad de administrador de red del campus local de la institución, se le otorgaron las primeras 10 de estas subredes para que las utilice en el campus local. En este momento, usted utilizará 6 de estas subredes y guardará las restantes para el crecimiento futuro. **NO** utilice la primera o la última subred.

1. ¿Cuál es el equivalente en números binarios de la dirección de red Clase B 150.193.0.0 del ejercicio?
   _____ . _____ . _____ . _____
2. ¿Cuál(es) es (son) el (los) octeto(s) y cuántos bits se utilizan para representar la porción de red de esta dirección de red?

   _____

3. ¿Cuál(es) es (son) el (los) octeto(s) y cuántos bits se utilizan para representar la porción de host de esta dirección de red Clase B?

4. ¿Cuántas redes Clase B originales hay?

5. ¿Cuál es la cantidad total de hosts que se pueden crear con una dirección de red Clase B si ésta no se ha subdividido?

6. ¿Cuántos bits debe pedir prestados a la porción de host de la dirección de red para suministrar por lo menos 50 subredes y 750 hosts por subred?

7. ¿Cuál será la Máscara de subred (utilizando la notación decimal punteada) basándose en la cantidad de bits que se pidieron prestados en el paso 6?

8. ¿Cuál es el equivalente en números binarios de la máscara de subred a la que se hace referencia anteriormente?:

_____ . _____ . _____ . _____

Paso 3 - Dirección de red Clase B con 3 subredes.

Tarea: Complete la tabla a continuación siguiendo las instrucciones. Utilice la información de la tabla para responder las preguntas y complete el diagrama al final de la práctica de laboratorio.

Explicación: Asegúrese de especificar cuáles son los cuatro octetos para la dirección de subred y la máscara de subred. Se debe utilizar la misma máscara de subred para todos los hosts, interfaces del router y subredes. Si tiene una máscara de subred común, esto le permitirá a los hosts y routers determinar cuál es la subred hacia la que se envía el paquete IP. Generalmente, las interfaces del router se numeran primero al asignar las direcciones IP y a los hosts se les asignarán números más altos.

1. Complete la siguiente tabla para cada una de las subredes posibles que se pueden crear pidiendo prestados 6 bits para subredes al tercer octeto (1er octeto host). Identifique la dirección de red, la máscara de subred, el intervalo de direcciones IP de host posibles para cada subred, la dirección de broadcast para cada subred y también indique si la subred se puede utilizar o no. Para este ejercicio, usted utilizará solamente 3 de estas subredes.

SN#	Dirección de red	Máscara de subred	Dirección de subred	Intervalo de direcciones IP de host posibles	Dirección de broadcast	¿Utilizar?
0						
1						
2						
3						
4						

5						
6						
7						
8						
9						

2. Asigne una dirección IP y una máscara de subred a la interfaz del router A y escríbala aquí.

_____

_____

3. Asigne una dirección y una máscara de subred IP a la interfaz del router B y escríbala aquí.

_____

_____

4. Asigne una dirección y una máscara de subred IP a la interfaz del router C y escríbala aquí.

_____

_____

5. Asigne una Dirección IP de host al Host X de la Subred A y asigne una dirección IP al Host Z de la Subred C (las respuestas pueden variar) Describa los pasos (utilizando AND) del proceso que se utiliza para enviar un paquete IP desde el Host X hacia el Host Z a través del router. Recuerde, cuando se realiza un AND de dos unos juntos, el resultado es un 1, si se realiza un AND de cualquier otra combinación (1 y 0, 0 y 1 ó 0 y 0) esto da como resultado cero (0). Del mismo modo, cuando se realiza un AND de dos direcciones IP de red, el resultado de este proceso de AND es la dirección de red (o subred) de la dirección IP destino del paquete. Use la información del diagrama anterior para ayudar a asignar direcciones y máscaras de subred IP.

_____

_____

_____

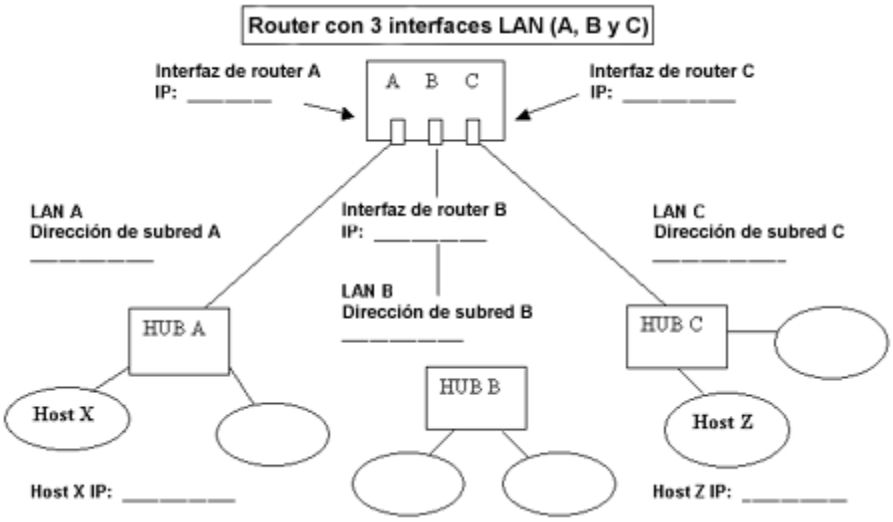
_____

6. ¿Cuál es el resultado del proceso de AND para el Host X?
   Dir. IP del Host X en decimales: _____ . _____ . _____ . _____
   Dir. IP del Host X en binarios: _____ . _____ . _____ . _____
   Máscara de subred en binarios: _____ . _____ . _____ . _____
   Resultado de AND en binarios: _____ . _____ . _____ . _____
   Resultado de AND en decimales: _____ . _____ . _____ . _____
7. ¿Cuál es el resultado del proceso de AND para el Host Z?
   Dir. IP del Host X en decimales: ____ . _____ . _____ . _____
   Dir. IP del Host X en binarios: _____ . _____ . _____ . _____
   Máscara de subred en binarios: _____ . _____ . _____ . _____
   Resultado de AND en binarios: _____ . _____ . _____ . _____
   Resultado de AND en decimales: _____ . _____ . _____ . _____
8. El resultado del AND en números decimales para la pregunta 7 es la red/subred en la que se encuentra el Host X. El resultado del AND en números decimales para la pregunta 8 es la red/subred en la que se encuentra el Host Z. ¿El Host X y el Host Z están en la misma red/subred?

_____

9. ¿Qué es lo que hará ahora el Host X con el paquete?

10. Complete los espacios en blanco del siguiente diagrama con las direcciones IP y de red correspondientes.



Practica # 4 Diseño de un esquema de direccionamiento IP de clase C

Objetivos:
Esta práctica de laboratorio se concentrará en su capacidad para realizar las siguientes tareas:

- Trabajar con un ejemplo de subred Clase C más complejo
- Determinar las subredes disponibles con una dirección de red IP y una máscara de subred específica
- Dados una dirección y requisitos de red, sea capaz de determinar de qué manera muchas de las subredes y hosts

Poder determinar el tipo de máscara de subred que se debe utilizar para asignar la cantidad adecuada de hosts y subredes
Asignar direcciones IP y máscaras de subred a los hosts y las interfaces del router
Usar el proceso de "AND" para desplazar un paquete IP desde un host local hacia un host remoto a través de un router

Desarrollo.
Paso 1 - Conceptos básicos sobre direcciones IP
Explicación: Para fines de referencia, se incluye aquí la tabla de direccionamiento IP de la práctica de laboratorio anterior. El Centro de Información para la Red de Internet (InterNIC) asigna las direcciones de red IP. Usted trabajará con una red Clase C.

Cls	1er Octeto de intervalo decimal	1er Octeto de bits de alto nivel	ID de Red / Host (N=Red, H=Host)	Máscara de subred por defecto	Cantidad de redes	Hosts por red (direcciones utilizables)
A	1 - 126*	0	N.H.H.H	255.0.0.0	126 (2^7 - 2)	16.777.214 (2^{24} - 2)
B	128 - 191	1 0	N.N.H.H	255.255.0.0	16.382 (2^{14} - 2)	65.534 (2^{16} - 2)
C	192 - 223	1 1 0	N.N.N.H	255.255.255.0	2.097.150 (2^{21} - 2)	254 (2^8 - 2)
D	224 - 239	1 1 1 0	Reservado para multicast			
E	240 - 254	1 1 1 1 0	Experimental, se utiliza para fines de investigación			

Paso 2 - Dirección de red Clase C con 3 subredes.

Tarea: Use la siguiente información y la información de la planilla de trabajo de la práctica de laboratorio anterior para ayudarlo a determinar las subredes y las direcciones IP de host válidas. **NO** utilice la subred cero ni la última subred.

Explicación: Su empresa tiene una dirección de red Clase C de 200.10.57.0. Desea subdividir la red física en 3 subredes (A, B y C) utilizando un router como se indica en el diagrama que aparece al final de la planilla de trabajo Necesitará por lo menos 20 hosts por subred. Responda las siguientes preguntas.

1. ¿Cuál es el equivalente en números binarios de la dirección de red Clase C **200.10.57.0** de este ejercicio?
   _____ . _____ . _____ . _____
2. ¿Cuál(es) es (son) el (los) octeto(s)que representa(n) la porción de red y cuál(es) es (son) el (los) octeto(s) que representa(n) la porción de host de esta dirección de red Clase C?

   _____

3. ¿Cuántos bits debe pedir prestados a la porción de host de la dirección de red para suministrar por lo menos 3 subredes y 20 hosts por subred?

   _____

4. ¿Cuál será la Máscara de subred (utilizando la notación decimal punteada) basándose en la cantidad de bits que se pidieron prestados en el paso 3?

_____ . _____ . _____ . _____

5. ¿Cuál es el equivalente en números binarios de la máscara de subred a la que se hace referencia anteriormente?:

_____ . _____ . _____ . _____

Paso 3 - Dirección de red Clase C con 3 subredes.

Tarea: Complete la tabla a continuación siguiendo las instrucciones. Utilice la información de la tabla para responder las preguntas y complete el diagrama al final de la práctica de laboratorio.

Explicación: Asegúrese de especificar cuáles son los cuatro octetos para la dirección de subred y la máscara de subred. Se debe utilizar la misma máscara de subred para todos los hosts, interfaces del router y subredes. Si tiene una máscara de subred común, esto le permitirá a los hosts y routers determinar cuál es la subred hacia la que se envía el paquete IP. Generalmente, las interfaces del router se numeran primero al asignar las direcciones IP y a los hosts se les asignarán números más altos.

1. Complete la siguiente tabla para cada una de las posibles subredes que se pueden crear pidiendo prestados 3 bits para subredes al cuarto octeto (octeto de host). Identifique la dirección de red, la máscara de subred, el intervalo de direcciones IP de host posibles para cada subred, la dirección de broadcast para cada subred y también indique si la subred se puede utilizar o no. Para este ejercicio, utilizará solamente 3 de estas subredes.

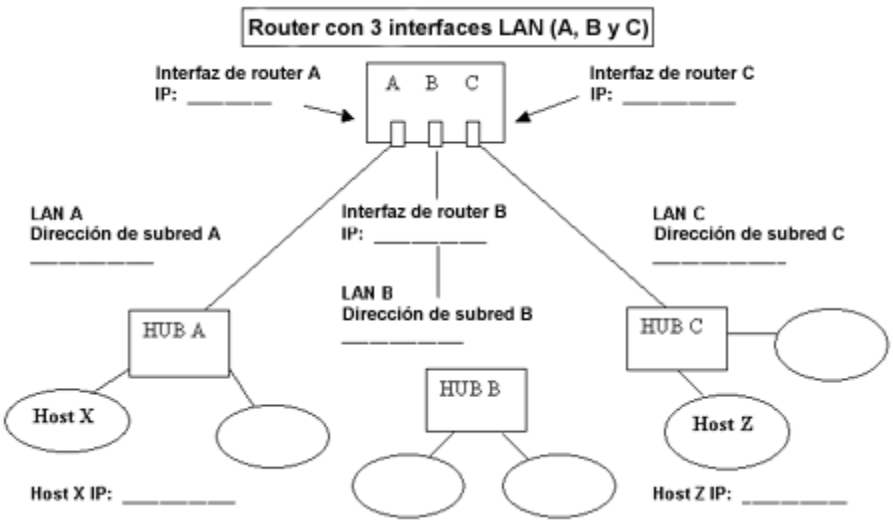
SN#	Dirección de red	Máscara de subred	Dirección de subred	Intervalo de direcciones IP de host posibles	Dirección de broadcast	¿Utilizar?
1er						
2do						
3er						
4to						
5to						
6to						
7mo						
8vo						

2. Asigne una dirección y una máscara de subred IP a la interfaz del router A y escríbala aquí.
   _____ / _____
3. Asigne una dirección y una máscara de subred IP a la interfaz del router B y escríbala aquí.
   _____ / _____
4. Asigne una dirección y una máscara de subred IP a la interfaz del router C y escríbala aquí.
   _____ / _____
5. Asigne una Dirección IP de host al Host X de la Subred A y asigne una dirección IP al Host Z de la Subred C (las respuestas pueden variar). Describa los pasos (utilizando AND) del proceso que se utiliza para enviar un paquete IP desde el Host X hacia el host Z a través del router. Recuerde, cuando se realiza un AND de dos unos juntos, el resultado es un 1, si se realiza un AND de cualquier otra combinación (1 y 0, 0 y 1 ó 0 y 0) esto da como resultado cero (0). Del mismo modo, cuando se realiza un AND de dos direcciones IP de red, el resultado de este proceso de AND es la dirección de red (o subred) de la dirección IP destino del paquete. Use la información del diagrama anterior y de la práctica de laboratorio anterior para ayudar a asignar direcciones y máscaras de subred IP.

6. ¿Cuál es el resultado del proceso de AND para el Host X?
   Dir. IP del Host X en decimales: _____ . _____ . _____ . _____
   Dir. IP del Host X en binarios: _____ . _____ . _____ . _____
   Máscara de subred en binarios: _____. _____ . _____ . _____
   Resultado de AND en binarios: _____ . _____ . _____ . _____
   Resultado de AND en decimales: _____ . _____ . _____ . _____
7. ¿Cuál es el resultado del proceso de AND para el Host Z?
   Dir. IP del Host X en decimales: _____ . _____ . _____ . _____
   Dir. IP del Host X en binarios: _____ . _____ . _____ . _____
   Máscara de subred en binarios: _____ . _____ . _____ . _____
   Resultado de AND en binarios: _____ . _____ . _____ . _____
   Resultado de AND en decimales: _____ . _____ . _____ . _____
8. El resultado del AND en números decimales para la pregunta 6 es la red/subred en la que se encuentra el Host X. El resultado del AND en números decimales para la pregunta 7 es la red/subred en la que se encuentra el Host Z. ¿El Host X y el Host Z están en la misma red/subred?

9. ¿Qué es lo que hará ahora el Host X con el paquete?

10. Complete los espacios en blanco del siguiente diagrama con las direcciones IP y de red correspondientes.



Practica # 5 Uso del software Protocol Inspector y ARP

Objetivos:
Utilizar el software Protocol Inspector (o equivalente) para estudiar las peticiones y respuestas ARP.

Desarrollo.
El software de análisis de protocolo tiene una función denominada captura. Esta función permite que todas las tramas que recorren una interfaz puedan ser capturadas para su análisis. Con esta función, puede observar el proceso del Protocolo de resolución de direcciones. Es posible que considere que ARP es un poco abstracto, pero con el analizador de protocolo se puede ver la importancia de ARP para el funcionamiento normal de una red.
Herramientas / Preparación:
Cada PC debe ejecutar la pila Microsoft TCP/IP de Windows 95, 98 o NT, y Winsock 2.0. Se debe instalar Network Inspector 3.0 de Fluke (o equivalente) en cada PC. Durante la instalación del software debe especificar cuál es el adaptador de red (NIC, acceso telefónico, etc.) que desea verificar: especifique la NIC que conecta los PC a la Ethernet. Los PC deben estar en una red 10Base-T o 100Base-TX Ethernet que, de preferencia, incluya servidores, switches, routers e impresoras o, preferentemente, Internet. (esto hará que el análisis del protocolo sea más interesante).

Planilla de trabajo

1. Abra el software Protocol Inspector.

2. Vaya a la vista detallada (Detail). ¿Qué es lo que ve?

3. Inicie una captura. ¿Qué es lo que sucede?

4. Abra una ventana MS-DOS.

5. Utilizando arp -a examine el contenido de la tabla ARP. ¿Qué es lo que ve?

6. Utilizando arp -d a.b.c.d borre todas las entradas de la tabla ARP. Utilice arp -a para reexaminar la tabla ARP. ¿Qué es lo que sucede?

7. Utilice ping a.b.c.d para crear una trama ARP. ¿Qué es lo que sucede? Haga ping su propia máquina u otra máquina en la red.

8. Detenga la captura. ¿Qué es lo que sucede?

9. Estudie las tramas ARP, las tramas ping y las estadísticas que usan varias visualizaciones, especialmente la vista detallada. Describa las distintas visualizaciones y lo que ha aprendido acerca de ARP.

10. Inicie otra captura para examinar la red en la que se encuentra.
11. Utilice la red durante aproximadamente un minuto (enviando mensajes de correo electrónico, descargando páginas web, etc.) durante un período de tiempo determinado (digamos, 2 minutos) y observe, en detalle, cuántas tramas ARP se producen. ¿Se produce alguna? Si es así, ¿por qué?

Reflexión

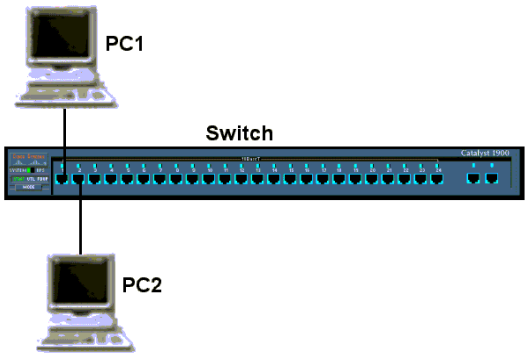
¿Por qué es necesario ARP para el funcionamiento de las LAN?

MODULO 2 "Tecnología LAN Switching"

Practica # 1 "Verificación de la configuración por defecto del switch"

Objetivo.

Conocer los parámetros de configuración básicos de un LAN-switch.



Paso 1 Entrar al modo privilegiado

a.El modo privilegiado da acceso a todos los comandos del switch. Muchos de los comandos privilegiados configuran los parámetros de operación. Por lo tanto, el acceso privilegiado debe estar protegido mediante contraseñas para evitar el uso no autorizado.

Modos de comando del Switch Catalyst 2950			
Modo de comando	**Método de Acceso**	**Prompt desplegado**	**Método de salida**
User EXEC (Modo usuario)	Log in	Switch>	Usar el comando *logout*
Privileged EXEC (Modo privilegiado)	Desde User EXEC, ingresar el comando *enable*	Switch#	Para regresar a modo User EXEC, ingresar los comandos *disable, exit* o *logout*
Configuración Global	Desde el modo privilegiado ingresar el comando *configure terminal*	Switch(config)#	Para regresar a modo privilegiado, ingresar el comando *exit* o presionar Ctrl-z
Configuración de interface	Desde el modo de configuración global ingresar el comando *interface type number*	Switch(config-if)#	Para regresar a modo de configuración global, ingresar el comando *exit*

El conjunto de comandos privilegiados incluye aquellos comandos del modo EXEC usuario, así como también el comando **configure** a través del cual se obtiene acceso a los modos de comando restantes.

Switch>**enable**
Switch#

b. Observe que la petición de entrada de la configuración cambia para reflejar el modo EXEC privilegiado.

Paso 2 Examinar el archivo de configuración activo (1900: realizar a, b y k)

a. Examine el archivo de configuración activa actual.

Switch#**show running-config**

b. ¿Cuántas interfaces de Ethernet o Fast Ethernet tiene el switch? _____

c. ¿Cuál es el intervalo de valores que se muestra para las líneas VTY?
_____

d. Examine el contenido actual de la NVRAM de la siguiente manera:

Switch#**show startup-config**
%% Non-volatile configuration memory is not present

e. ¿Por qué emite esta respuesta el switch?
_____
_____

f. Ejecute el siguiente comando para mostrar la dirección IP actual del switch.
Switch#**show interface VLAN 1**

g. ¿Tiene el switch una dirección IP establecida?

---

h. ¿Cuál es la dirección MAC de esta interfaz virtual de switch?
_____

i. ¿Está activada esta interfaz?
_____

j. Las propiedades IP de la interfaz se pueden mostrar introduciendo el siguiente comando:

Switch#**show ip interface VLAN 1**

k. Los siguientes comandos proporcionan información acerca de la dirección IP del switch para el switch serie 1900:

#**show ip**

Paso 3 Mostrar información acerca del IOS
a. Examine la siguiente información acerca de la versión generada por el switch.

Switch#**show version**

b. ¿Cuál es la versión del IOS que ejecuta el switch? _____

c. ¿Cuál es el nombre del archivo de imagen del sistema?
_____

d. ¿Cuál es la dirección MAC base de este switch? _____

e. ¿Ejecuta el switch la edición empresarial del software? (serie 1900)
_____

¿Ejecuta el switch el software de Imagen Mejorada, lo cual se indica a través de las letras "EA" en el nombre de archivo de IOS? (serie 2950)
_____

Paso 4 Examinar las interfaces Fast Ethernet
a. Examine las propiedades por defecto de las interfaces Fast Ethernet. A modo de ejemplo, examine las propiedades de la cuarta interfaz:
1900:

#**show interface fastethernet 0/26** (Nota: este es un puerto troncal).

#**show interface ethernet 0/4** (Nota: este es un puerto de acceso).

2950:
#**show interface fastethernet 0/4** (Nota: este puede ser un puerto troncal o de acceso).

#**show interface gigabitethernet 0/1** (Nota: este puede ser un puerto troncal o de acceso).

b. ¿Está activada o desactivada la interfaz?
_____

c. ¿Qué cosa puede hacer que una interfaz se active?
_____

d. ¿Cuál es la dirección MAC de la interfaz? _____

e. ¿Cuál es la configuración de velocidad y de dúplex de la interfaz?
_____

Paso 5 Examinar la información de VLAN
a. Examine la siguiente configuración VLAN por defecto del switch.

Switch>**show vlan**

b. ¿Cuál es el nombre de la VLAN 1?
_____

c. ¿Cuáles son los puertos que hay en esta VLAN?
_____

d. ¿Está activada la VLAN 1?
_____
e. ¿Qué tipo de VLAN es la VLAN por defecto?
_____

Paso 6 Examinar la memoria Flash (1900: Vaya directamente al paso 8).
a. Ejecute una de los siguientes comandos para examinar el contenido del directorio flash

Switch#**dir flash:**

Switch#**show flash**

b. Enumere los archivos y los directorios encontrados.
_____
_____

Paso 7 Examinar el archivo de configuración inicial
a. Para ver el contenido del archivo de configuración inicial, escriba el comando **show startupconfig** en el modo EXEC privilegiado de la siguiente manera:

Switch#**show startup-config**

b. El switch responderá de la siguiente manera:
Non-volatile configuration memory is not present

c. ¿Por qué aparece este mensaje? _____

d. Copie la siguiente configuración a la NVRAM.

Nota: Este paso garantiza que cualquier cambio realizado estará disponible para el switch si se produce una recarga o un corte de energía eléctrica.

Switch#**copy running-config startup-config**
Destination filename [startup-config]?
Building configuration...
[OK]
Switch#

e. Ejecute el siguiente comando para mostrar el contenido de la NVRAM:

Switch#**show startup-config**

f. ¿Cuál es la información que aparece ahora en pantalla?

_____

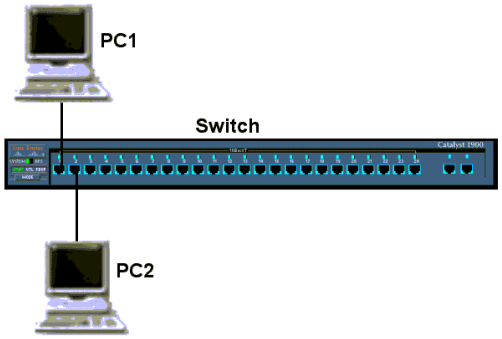
Paso 8 Salir del switch
Escriba **exit**, como se indica a continuación, para salir de la pantalla de bienvenida del switch:

Switch#**exit**

Al completar estos pasos, termine la sesión escribiendo **exit** y apague todos los dispositivos. Entonces, quite y guarde los cables y el adaptador.

Practica # 2 "Configuración básica del switch"

Objetivo.
Configurar los parámetros de operación basicos de un LAN-Switch.



Paso 1 Entrar al modo privilegiado
a. El modo privilegiado da acceso a todos los comandos del switch. Muchos de los comandos privilegiados configuran los parámetros de operación. Por lo tanto, el acceso privilegiado debe estar protegido mediante contraseñas para evitar el uso no autorizado. El conjunto de comandos privilegiados incluye aquellos comandos del modo EXEC usuario, así como también el comando **configure** a través del cual se obtiene acceso a los modos de comando restantes.

Switch>**enable**
Switch#
1900:
>**enable**
#

b. Observe que la petición de entrada de la configuración cambia para reflejar el modo EXEC privilegiado.

Paso 2 Examinar la configuración activa del switch
a. Examine el siguiente archivo de configuración activa actual:

Switch#**show running-config**

b. ¿Cuántas interfaces de Ethernet o Fast Ethernet tiene el switch? _____

c. ¿Cuál es el intervalo de valores que se muestra para las líneas VTY?
_____

d. Examine el contenido actual de la NVRAM de la siguiente manera:
Switch#**show startup-config**
%% Non-volatile configuration memory is not present

e. ¿Por qué emite esta respuesta el switch?
_____

Paso 3 Asignar un nombre al switch
a. Escriba **enable** y luego el modo de configuración. El modo de configuración permite la gestión del switch. Escriba **ALSwitch**, el nombre con el que se hará referencia a este switch en el siguiente comando:

Switch#**configure terminal**

Introduzca los comandos de configuración, uno por cada línea. Finalice presionando **Ctrl-Z**.

Switch(config)#**hostname ALSwitch**
ALSwitch(config)#**exit**

b. Observe que la petición de entrada de la configuración cambia para reflejar el nuevo nombre. Escriba **exit** o presione **Ctrl-Z** para volver al modo privilegiado.

Paso 4 Examinar la configuración activa actual
a. Examine la configuración activa que aparece a continuación para verificar que no hay ninguna configuración, excepto el nombre de host:

ALSwitch#**show running-config**

b. ¿Hay alguna contraseña configurada en las líneas?
_____

c. ¿Qué muestra la configuración como el nombre de host de este switch?
_____

Paso 5 Configurar las contraseñas de acceso (1900: Vaya directamente al paso 6).
Entre al modo de configuración de línea para la consola. Establezca **cisco** como contraseña en esta línea para iniciar una sesión. Configure las líneas vty 0 a 15 con la contraseña cisco de la siguiente manera:

ALSwitch#**configure terminal**

Introduzca los comandos de configuración, uno por cada línea. Finalice presionando **Ctrl-Z**.

ALSwitch(config)#**line con 0**
ALSwitch(config-line)#**password cisco**
ALSwitch(config-line)#**login**
ALSwitch(config-line)#**line vty 0 15**
ALSwitch(config-line)#**password cisco**
ALSwitch(config-line)#**login**
ALSwitch(config-line)#**exit**

Paso 6 Configurar las contraseñas de los modos de comando
a. Establezca **enable password** en cisco y **enable secret password** en **class** de la siguiente manera:

ALSwitch(config)#**enable password cisco**
ALSwitch(config)#**enable secret class**
1900:
ALSwitch(config)#**enable password level 15 cisco**
ALSwitch(config)#**enable secret class**
2950:

#**show interface fastethernet 0/4** (Nota: este puede ser un puerto troncal o de acceso).
O

#**show interface gigabitethernet 0/1** (Nota: este puede ser un puerto troncal o de acceso).

b. ¿Cuál es la contraseña que tiene prioridad, la contraseña enable o la contraseña enable secret?
_____

Paso 7 Configurar la capa 3 para obtener acceso al switch.
a. Establezca la dirección IP del switch en 192.168.1.2 con una máscara de subred 255.255.255.0 de la siguiente manera:
Nota: Esto se realiza en la interfaz virtual interna VLAN 1.

ALSwitch(config)#**interface VLAN 1**
ALSwitch(config-if)#**ip address 192.168.1.2 255.255.255.0**

ALSwitch(config-if)#**exit**

1900:
ALSwitch(config)#**ip address 192.168.1.2 255.255.255.0**
ALSwitch(config)#**exit**

b. Establezca el gateway por defecto para el switch y la VLAN de administración por defecto en 192.168.1.1 de la siguiente manera:

ALSwitch(config)#**ip default-gateway 192.168.1.1**
ALSwitch(config)#**exit**

1900:
ALSwitch(config)#**ip default-gateway 192.168.1.1**
ALSwitch(config)#**exit**

Paso 8 Verificar los parámetros de administración de las LAN (1900: Vaya directamente al paso 10)
a. Verifique los valores de interfaz de la VLAN 1 de la siguiente manera:

ALSwitch#**show interface VLAN 1**

b. ¿Cuál es el ancho de banda en esta interfaz? _____

c. ¿Cuáles son los estados de la VLAN?: VLAN1 es _____, el Protocolo de línea es _____

d. Habilite la interfaz virtual por medio del comando **no shutdown**

ALSwitch(config)#**interface VLAN 1**
ALSwitch(config-if)#**no shutdown**
ALSwitch(config-if)#**exit**

Paso 9 Guardar la configuración
a.La configuración básica del switch se ha completado. Haga una copia de respaldo del archivo de configuración activa en la NVRAM de la siguiente manera:

Nota: Esto garantizará que los cambios que se han realizado no se pierdan si el sistema se reinicia o se apaga.

ALSwitch#**copy running-config startup-config**
Destination filename [startup-config]?[**Intro**]
Building configuration...
[OK]
ALSwitch#

Paso 10 Examinar el archivo de configuración inicial (1900: Vaya directamente al paso 11)
a. Para ver la configuración que se guarda en la NVRAM, escriba el comando **show startupconfig** en el modo EXEC privilegiado (modo enable):

ALSwitch#**show startup-config**

b. ¿Qué información aparece en pantalla?
_____

c. ¿Todos los cambios realizados están grabados en el archivo?
_____

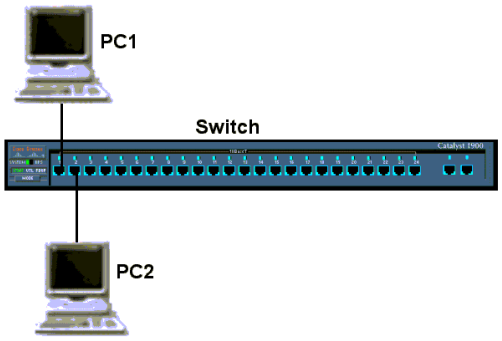
Paso 11 Salir del switch
Escriba **exit**, como se indica a continuación, para salir de la pantalla de bienvenida del switch:

ALSwitch#**exit**

Al completar estos pasos, termine la sesión escribiendo **exit** y apague todos los dispositivos. Entonces, quite y guarde los cables y el adaptador.

Practica # 3 “Configuración de redes VLAN estáticas”

Objetivo
Crear y verificar una configuración básica de switch.
Determinar la versión de firmware del switch.
Crear dos VLAN, otorgarles un nombre y asignarles puertos miembro.



Paso 1 Configurar el switch
Configure el nombre de host, las contraseñas de acceso y modo de comando, así como también los parámetros de administración de la LAN. Estos valores se ilustran en la tabla. Si se producen problemas al ejecutar esta configuración, consulte la Práctica de Laboratorio Configuración básica del switch.

Switch	
Hostname	ALSwitch
Contraseña consola	Cisco
Contraseña privilegiado	Class
Contraseña vty	Cisco
Dir IP	192.168.1.2
Mascara de Subred	255.255.255.0
Puerta de enlace	192.168.1.1

PC1	
Dir IP	192.168.1.3
Mascara de Subred	255.255.255.0
Puerta de enlace	192.168.1.1

PC2	
Dir IP	192.168.1.4
Mascara de Subred	255.255.255.0
Puerta de enlace	192.168.1.1

Paso 2 Configurar los hosts conectados al switch
Configure el host para que utilice la misma subred para la dirección, máscara y gateway por defecto que el switch.

Paso 3 Verificar la conectividad
a. Para verificar que los hosts y los switches estén configurados correctamente, haga ping al switch desde el host.

b. ¿El ping fue exitoso? _____

c. Si la respuesta es no, realice el diagnóstico de fallas en la configuración del host y del switch.

Paso 4 Mostrar la versión de IOS
a. Es sumamente importante saber cuál es la versión del sistema operativo que se utiliza. Las diferencias entre las versiones pueden cambiar la forma en que se introducen los comandos. Escriba el comando **show version** en la petición de entrada del modo EXEC privilegiado como se indica a continuación:

Switch_A#**show version**

b. ¿Qué versión de IOS del switch aparece en pantalla?
_____

c. ¿Este switch tiene software de edición estándar o para empresas? _____

d. ¿Cuál es la versión de firmware o de IOS del switch? _____

Paso 5 Mostrar la información de la interfaz VLAN
a. En el Switch_A, escriba el comando **show vlan** en la petición de entrada del modo EXEC privilegiado como se indica a continuación:

Switch_A#**show vlan**
1900:

Switch_A#**show vlan-membership**

b. ¿Cuáles son los puertos que pertenecen a la VLAN por defecto?
_____

c. ¿Cuántas VLAN están configuradas por defecto en el switch?
_____

d. ¿Qué representa VLAN 1003? _____

e. ¿Cuántos puertos hay en la VLAN 1003?
_____

Paso 6 Crear y otorgar un nombre a dos VLAN
Introduzca los siguientes comandos para crear y otorgar un nombre a dos VLAN:
Switch_A#**vlan database**
Switch_A(vlan)#**vlan 2 name VLAN2**
Switch_A(vlan)#**vlan 3 name VLAN3**
Switch_A(vlan)#**exit**

1900:
Switch_A#**config terminal**
Switch_A(config)#**vlan 2 name VLAN2**
Switch_A(config)#**vlan 3 name VLAN3**

Paso 7 Mostrar la información de la interfaz VLAN
a. En el Switch_A, escriba el comando **show vlan** en la petición de entrada del modo EXEC privilegiado como se indica a continuación:

Switch_A#**show vlan**

b. ¿Hay alguna VLAN en la lista? _____

1900:
Switch_A#**show vlan-membership**

c. ¿Se les ha asignado algún puerto? _____

Paso 8 Asignar puertos a VLAN 2
La asignación de puertos a las VLAN se debe realizar desde el modo de interfaz. Introduzca los siguientes comandos para agregar el puerto 2 a la VLAN 2:

Switch_A#**configure terminal**
Switch_A(config)#**interface fastethernet 0/2**
Switch_A(config-if)#**switchport mode access**
Switch_A(config-if)#**switchport access vlan 2**
Switch_A(config-if)#**end**

1900:
Switch_A#**config terminal**
Switch_A(config)#**interface Ethernet 0/2**
Switch_A(config-if)#**vlan static 2**
Switch_A(config)#**end**

Paso 9 Mostrar la información de la interfaz VLAN
a. En el Switch_A, escriba el comando **show vlan** en la petición de entrada del modo EXEC privilegiado como se indica a continuación:

Switch_A#**show vlan**

1900:
Switch_A#**show vlan-membership**

b. ¿El puerto 2 se ha asignado a la VLAN 2?
_____

c. ¿El puerto aún aparece en la lista de la VLAN por defecto?
_____

Paso 10 Asignar puertos a VLAN 3
La asignación de puertos a las VLAN se debe realizar desde el modo de interfaz. Introduzca los siguientes comandos para agregar el puerto 3 a la VLAN 3:

Switch_A#**configure terminal**
Switch_A(config)#**interface fastethernet 0/3**
Switch_A(config-if)#**switchport mode access**
Switch_A(config-if)#**switchport access vlan 3**
Switch_A(config-if)#**end**

1900:
Switch_A#**config terminal**
Switch_A(config)#**interface Ethernet 0/3**
Switch_A(config)#**vlan static 3**
Switch_A(config)#**end**

Paso 11 Observar la información de la interfaz VLAN
a. En el Switch_A, escriba el comando **show vlan** en la petición de entrada del modo EXEC privilegiado como se indica a continuación:

Switch_A#**show vlan**

1900:
Switch_A#**show vlan-membership**

b. ¿El puerto 3 se ha asignado a la VLAN 3?

_____

c. ¿El puerto aún aparece en la lista de la VLAN por defecto?

_____

Paso 12 Observar sólo la información de la VLAN2

a. En lugar de mostrar todas las VLAN, escriba el comando **show vlan id 2** en la petición de entrada del modo EXEC privilegiado, como se indica a continuación :

Switch_A#**show vlan id 2**

1900:

Switch_A#**show vlan 2**

b. ¿Este comando suministra más información que el comando show VLAN? _____

Paso 13 Observar sólo la información de la VLAN2 con un comando distinto (1900: Omitir este paso)

a. En lugar de mostrar todas las VLAN, escriba el comando **show vlan name VLAN2** en la petición de entrada del modo EXEC privilegiado.

Switch_A#**show vlan name VLAN2**

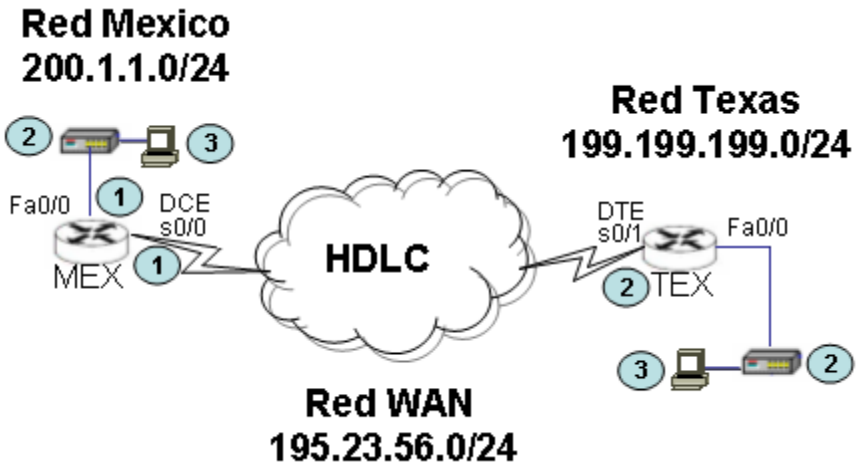
b. ¿Este comando suministra más información que el comando show VLAN? _____

Al completar estos pasos, desconéctese escribiendo **exit** y apague todos los dispositivos. Entonces, quite y guarde los cables y el adaptador.

Practica # 4 "Configuración básica de una red WAN"

Objetivo.
Entrenarse en el uso de comandos de configuración básica de routers y Switches Cisco.

Implemente en el simulador una red experimental como la que se muestra en el diagrama y acceda a los puertos de consola de los equipos de conectividad.



CONFIGURACIÓN DEL RUTEADOR MEX.
Paso 1. Una vez cableada la red, se ingresa via el puerto de consola a los distintos dispositivos de la red. Ingrese al puerto de consola del ruteador MEX. Al presionar la tecla enter se obtiene respuesta del ruteador.

Router Con0 is now available
Press RETURN to get started!

Router>

Paso 2. Una vez habiendo ingresado en el modo usuario (>), para poder configurar el dispositivo, es necesario ingresar al modo privilegiado (#). Ejecute el comando enable para ingresar a modo privilegiado.

Router>enable
Router#

Paso 3. Estando en modo privilegiado debe activarse el modo de configuración (config). Ejecute el comando configure terminal para ingresar a este modo.

Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z
Router(config)#

Paso 4. Como primera configuración se establecerá el nombre del equipo.

Router(config)#hostname MEX
MEX(config)#

Paso 5. Para proteger el acceso al modo privilegiado es necesario habilitar un password.

MEX(config)#enable password cisco

Paso 6. Para establecer una contraseña de acceso en el Puerto de consola se ejecutan los siguientes commandos.

```
MEX(config)#line console 0
MEX(config-line)#password cisco
MEX(config-line)#login
```

Paso 7. El Puerto de acceso remoto (telnet) del ruteador se protege estableciendo las contraseñas de los puertos telnet (0 a 4).

```
MEX(config-line)#line vty 0 4
MEX(config-line)#password cisco
MEX(config-line)#login
MEX(config-line)#exit
```

Paso 8. El direccionamiento IP de las interfaces se establece activando las direcciones e interfaces respectivas. La dirección IP se configura incluyendo la mascara de subred de la dirección.

```
MEX(config)#int fa0/0
MEX(config-if)#ip address 200.1.1.1 255.255.255.0
MEX(config-if)#no shutdown
MEX(config-if)#int s0/0
MEX(config-if)#ip address 195.23.56.1 255.255.255.0
MEX(config-if)#clock rate 64000
MEX(config-if)#no shutdown
MEX(config-if)#exit
```

Nota. El comando clock rate se establece solo en la interfaz DCE. Al activar una interfaz (no shutdown), observara en la sesión de consola mensajes de activación de la interfaz.

Paso 9. Para establecer la conectividad entre las redes del campus, es necesario habilitar el protocolo de ruteo. En el protocolo de ruteo, solo se dan de alta las redes directamente conectadas al ruteador en cuestión.

```
MEX(config)#router rip
MEX(config-router)#version 2
MEX(config-router)#network 200.1.1.0
MEX(config-router)#network 195.23.56.0
MEX(config-router)#exit
MEX(config)#exit
```

Paso 10. Una vez finalizada la configuración, para evitar perder esta configuración, se requiere salvarla en la memoria NVRAM.

```
MEX#copy run start
```

Paso 11. Una vez salvada la configuración verifique su contenido con el comando show running-config.

```
MEX#show  running-config
```

CONFIGURACIÓN DEL SWITCH SWMEX.

Paso 1. Ingrese al puerto de consola del switch MEX. Al presionar la tecla enter se obtiene respuesta del switch.

```
switch Con0 is now available
Press RETURN to get started!

switch>
```

Paso 2. Una vez habiendo ingresado en el modo usuario (>), para poder configurar el dispositivo, es necesario ingresar al modo privilegiado (#). Ejecute el comando enable para ingresar a modo privilegiado.

```
switch>enable
switch#
```

Paso 3. Estando en modo privilegiado debe activarse el modo de configuración (config). Ejecute el comando configure terminal para ingresar a este modo.

```
switch#
switch#configure terminal
switch(config)#
```

Paso 4. Como primera configuración se establecerá el nombre del equipo.

```
switch(config)#hostname SWMEX
```

Paso 5. El direccionamiento IP del switch se establece a nivel de equipo, configurando la dirección IP en la red VLAN por defecto (VLAN 1).

```
SWMEX(config)#int vlan 1
SWMEX(config-if)#ip address 200.1.1.2 255.255.255.0
SWMEX(config-if)#no shutdown
SWMEX(config-if)#exit
```

Paso 7. Configuración de la puerta de enlace.

```
SWMEX(config)#ip default-gateway 200.1.1.1
SWMEX(config)#exit
SWMEX#
```

Paso 8. Verifique la configuración y guárdela.

```
SWMEX#show run
SWMEX#copy run start
```

CONFIGURACIÓN DEL RUTEADOR TEX.
La configuración del ruteador TEX es la siguiente.

```
Router>
Router>enable
Router#
Router#conf t
Router(config)#
Router(config)#hostname TEX
TEX(config)#
TEX(config)#enable password cisco
TEX(config)#line console 0
TEX(config-line)#password cisco
TEX(config-line)#login
TEX(config-line)#line vty 0 4
TEX(config-line)#password cisco
TEX(config-line)#login
TEX(config-line)#exit
TEX(config)#
TEX(config)#int fa0/0
TEX(config-if)#ip add 199.199.199.1 255.255.255.0
TEX(config-if)#no shut
```

```
TEX(config-if)#int s0/0
TEX(config-if)#ip address 195.23.56.2 255.255.255.0
TEX(config-if)#no shutdown
TEX(config-if)#exit
TEX(config)#
TEX(config)#router rip
TEX(config-router)#version 2
TEX(config-router)#network 195.23.56.0
TEX(config-router)#network 199.199.199.0
TEX(config-router)#exit
TEX(config)#exit
TEX#copy run start
TEX#sh run
```

CONFIGURACIÓN DEL SWITCH SWTEX.
La configuración del switch SWTEX es la siguiente.

```
switch>en
switch#conf t
switch(config)#
switch(config)#hostname SWTEX
SWTEX(config)#
SWTEX(config)#int vlan 1
SWTEX(config-if)#ip address 199.199.199.2 255.255.255.0
SWTEX(config-if)#no shutdown
SWTEX(config-if)#exit
SWTEX(config)#ip default-gateway 199.199.199.1
SWTEX(config)#exit
SWTEX#
SWTEX#copy run start
SWTEX#sh run
```

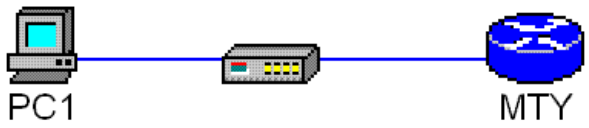
Por ultimo configure los hosts de la red y pruebe conectividad. En caso de no obtener conectividad en su totalidad, verifique las configuraciones y estado de las interfaces.

MODULO 3 "Administración de Redes"

Práctica # 1 "Administración de archivos de configuración mediante TFTP"

Objetivo

- Hacer una copia de respaldo de un archivo de configuración del router.
- Recargar el archivo de configuración de respaldo desde un servidor TFTP a la RAM del router.
- Guardar la nueva configuración activa a la NVRAM.



Nombre del router	**Dir IP e0**
MTY	**192.168.14.1/24**

Paso 1. Configurar el router MTY y Verifique las configuración ejecutando show running-config.

Paso 2. Configure la estación de trabajo PC1. La configuración del host PC1 conectado al router MTY es:

Dirección IP 192.168.14.2
Máscara de subred IP 255.255.255.0
Gateway por defecto 192.168.14.1

Paso 3. Inicie una sesión en el router MTY.

Paso 4. Inicie el servidor TFTP de Cisco en PC1.

Paso 5. Haga ping al servidor TFTP desde el router MTY.

Paso 6. Copie la configuración activa al servidor TFTP**.**

Anote la dirección IP del servidor TFTP.

Paso 7. Ejecute el comando **copy running-config tftp**. Siga los indicadores:

MTY#**copy running-config tftp**
Address or name of remote host []? **192.168.14.2**
Destination filename [MTY-confg]? **startup-config**
!!
667 bytes copied in 0.036 secs (18528 bytes/sec)

Paso 8. Verifique el archivo de registro del servidor TFTP. Haga clic en **View/Log File**. El resultado debe ser similar a lo siguiente:

Mon Sep 16 14:10:08 2003: Receiving 'startup-config' file from
192.168.14.1 in binary mode
Mon Sep 16 14:11:14 2003: Successful.

Paso 9. Ahora que el starup-config ha sido respaldado, pruebe esta imagen recargándola en el router. Se debe suponer que la configuración en el router MTY se ha dañado. Para simular esto, cambie el hostname del router MTY a "Router".

¿Cuál es la dirección IP del servidor TFTP?

Para copiar desde la petición de entrada de EXEC privilegiado, escriba **copy tftp runningconfig**.

Presione **Intro**.
Router#**copy tftp running-config**
Address or name of remote host []? **192.168.14.2**
Source filename []? **startup-config**
Destination filename [running-config]? **[Intro]**
Accessing tftp://192.168.14.2/startup-config...
Loading startup-config from 192.168.14.2 (via Ethernet0): !
[OK - 667 bytes]
667 bytes copied in 9,584 secs (70 bytes/sec)
MTY#

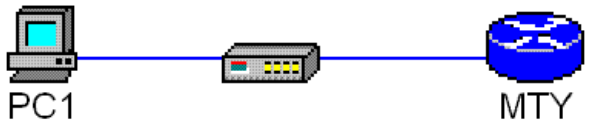
Paso 10. Guarde la nueva configuración activa en la NVRAM.

Paso 11. Si el indicador del router cambia, se ha cargado el archivo. Introduzca el comando **show startup-config** para verificar toda la configuración.

Paso 12. Al restaurar este archivo, las interfaces se desactivan por defecto, a menos que el archivo de configuración se haya modificado y se haya introducido una línea de comando **no shutdown** después de cada perfil de interfaz.

Práctica # 2 "Configuración del agente SNMP en equipo Cisco"

Objetivo:
Activar el agente SNMP en dispositivos Cisco.



Nombre del router	**Dir IP e0**
MTY	**192.168.14.1/24**

Desarrollo.
Paso 1. Implemente una red como la mostrada en el diagrama y direccione en forma apropiada los distintos elementos de la red.

Paso 2. Para administrar un equipo Cisco por medio del protocolo SNMP, es necesario habilitar el agente en el dispositivo. Examine el archivo de configuración y verifique si esta configurado algún parámetro SNMP.

MTY#show running-config

Paso 3. Para habilitar el agente hay que emplear un nombre de comunidad para definir la relación entre el gestor SNMP y el agente. Dicha comunidad actúa como una palabra clave para regular el acceso al agente que se haya en el router. Se pueden especificar opcionalmente algunas características adicionales. Si el agente no esta activo habilítelo de la siguiente forma:

MTY(config)#snmp-server community public RO

Paso 4. Con este parámetro se obtiene permiso para leer las variables MIB, encontradas en el dispositivo. Para ejecutar comandos de control en el equipo, habilite el nombre de comunidad para funciones de control.

MTY(config)#snmp-server community private RW

Paso 5. Para facilitar la administración remota, es conveniente configurar los datos de contacto y ubicación del personal que administra la red. Ejecute los siguientes comandos para facilitar la administración.

MTY(config)#snmp-server contact Admin Redes 52 55 5254
MTY(config)#snmp-server location Site Central, Mexico DF

Paso 6. Para visualizar la información de SNMP ejecute el commando show snmp.

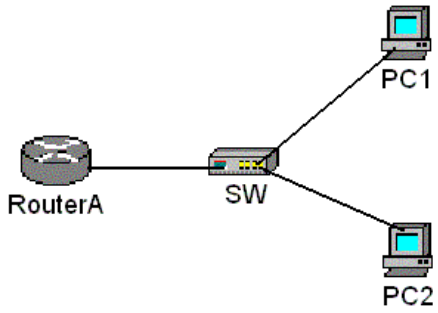
MTY#show snmp

¿Cual es la información que despliega el commando?

Practica # 3 "Configuración de ACLs estándar"

Objetivo

- Configurar y aplicar una ACL estándar para permitir o denegar tráfico específico.
- Probar la ACL para determinar si se lograron los resultados deseados.



Paso 1. Las listas de control de acceso estándar, permiten el filtrado de tráfico hacia cualquier aplicación. En esta practica se implementaran esquemas de filtrado de acuerdo con las direcciones IP origen de los hosts. En el router RouterA, entre al modo de configuración global y configure el nombre de host, las contraseñas de consola, de la terminal virtual y de enable. Configure la interfaz Ethernet en el router de acuerdo al diagrama.

Router RouterA
Dirección IP 192.168.14.1
Máscara de subred 255.255.255.0

Paso 2. Configure los hosts en el segmento Ethernet

Host PC1
Dirección IP 192.168.14.2
Máscara de subred 255.255.255.0
Gateway por defecto 192.168.14.1

Host PC2
Dirección IP 192.168.14.3
Máscara de subred 255.255.255.0
Gateway por defecto 192.168.14.1

Paso 3. Guarde la configuración.

RouterA#copy running-config startup-config

Paso 4. Confirme la conectividad haciendo ping al gateway por defecto desde ambos hosts.

¿Los ping fueron exitosos?

Si los pings no tienen éxito, corrija la configuración y repita este paso hasta que tengan éxito.

Paso 5. Cree una lista de acceso que impida el acceso a Ethernet 0 desde todos los hosts de la red 192.168.14.0.

RouterA(config)#access-list 1 deny 192.168.14.0 0.0.0.255
RouterA(config)#access-list 1 permit any

Paso 6. Ejecute un ping al router desde los hosts

¿Fueron exitosos los pings?

¿Por qué?

Paso 7. Aplicar la lista de acceso a la interfaz ethernet 0. El sentido del tráfico es in debido a que son los hosts internos, los que dirigen sus peticiones hacia la interfaz del router.

RouterA(config-if)#ip access-group 1 in

Paso 8. Ejecute ping hacia el router desde los hosts.

¿Los ping fueron exitosos?

¿Por qué?

Paso 9. Configure una lista de acceso (2) que impida que los hosts con números pares hagan ping al ruteador, la lista debe permitir que los hosts con dirección impar hagan ping al router. Anote su lista a continuación:

Paso 10. Aplique la lista de acceso a la interfaz de router correspondiente (elimine las asignaciones de listas anteriores escribiendo **no ip access-group 1 in** en el modo de configuración de interfaz).

Aplique la lista de acceso escribiendo **ip access-group 2 in**

Paso 11. Ejecute un ping al router desde cada host.

¿Tuvo éxito el ping desde el host PC1?

¿Por qué si o por qué no?

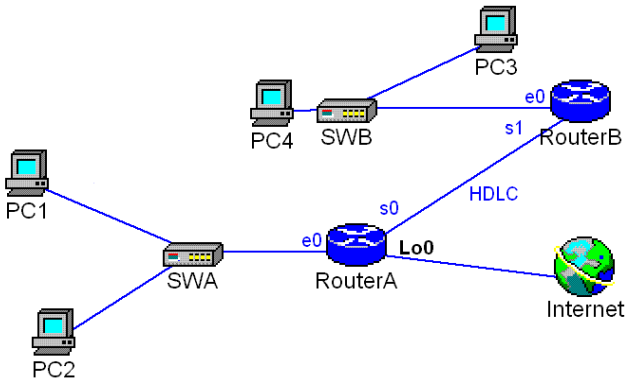
¿Tuvo éxito el ping desde el host PC2?

¿Por qué si o por qué no?

Al completar los pasos anteriores, borre la configuración de nvram y reinicie el router.

Practica # 4 "ACLs estándar y el acceso a Internet"

Objetivo
Planificar, configurar y aplicar una ACL estándar para permitir o denegar tráfico específico y probar la ACL para determinar si se lograron los resultados deseados.



Desarrollo
La empresa CIC desea controlar el tráfico hacia su red, ya que intenta mejorar el desempeño y la seguridad de su red. Implemente los filtros de seguridad necesarios para filtrar el tráfico acorde a las siguientes características.

- El Host PC3 representa una estación de trabajo cuyo acceso a la red, debe limitarse a la red LAN donde se ubica.
- El Host PC4 representa a otro host de la red que cuenta con acceso completo a redes internas o externas.
- La interface Loopback 0 del router RouterA representa la Internet.

Paso 1. Interconecte los routers de acuerdo al diagrama y configure el enrutamiento RIPv2. Los parámetros IP de los dispositivos de la red son los siguientes:

Router RouterA
Dirección IP e0 192.168.1.1/24
Dirección IP s0 192.168.2.1/24

Router RouterB
Dirección IP e0 192.168.3.1/24
Dirección IP s1 192.168.2.2/24

Host PC1
Dirección IP 192.168.1.2/24

Host PC2
Dirección IP 192.168.1.3/24

Host PC3
Dirección IP 192.168.3.2/24

Host PC4
Dirección IP 192.168.3.3/24

Paso 2. Verifique la conectividad haciendo ping a todos los dispositivos. Para simular la Internet, agregue la siguiente configuración al router RouterA.

```
RouterA(config)#interface loopback0
RouterA(config-if)#address 172.16.1.1 255.255.255.0
RouterA(config-if)#exit
```

```
RouterA(config)#router rip
RouterA(config-router)#network 172.16.0.0
RouterA(config-if)#^z
```

Paso 3. Es necesario limitar el acceso de la estación trabajo PC3 la red local. Se determina que es necesario crear una lista de acceso estándar para evitar que el tráfico desde este host llegue a cualquiera de las demás redes. La lista de control de acceso debe bloquear el tráfico desde este host sin afectar otro tráfico desde esta red. Una ACL IP estándar es adecuada, dado que filtra a base de la dirección origen a cualquier destino.

¿Cuál es la dirección IP de la estación de trabajo PC3?

Paso 4. Desarrolle la lista de acceso y anótela.

Paso 5. Ahora que se ha completado la ACL, es necesario confirmarla y probarla. El primer paso es verificar la lista para ver si se ha configurado correctamente en el router. Para verificar la lógica de la ACL use el comando **show access-lists**. Anote el resultado.

Paso 6. A continuación, aplique la lista de acceso.

¿Cuál es el comando utilizado para aplicar la lista?

¿Cuál es el ruteador e interfaz apropiado para aplicar la lista de acceso?

Paso 7. Por último, pruebe la funcionalidad de la ACL y verifique que se permita o deniegue de acuerdo con la dirección origen del host. En este caso, la prueba se realiza con un ping.

Prueba	Exitoso	No exitoso
Ping PC3 hacia PC4		
Ping PC3 hacia PC1		
Ping PC3 hacia PC2		
Ping PC3 hacia Internet (Lo0)		
Ping PC3 hacia RouterA		
Ping PC4 hacia PC1		
Ping PC4 hacia PC2		
Ping PC4 hacia Internet (Lo0)		
Ping PC4 hacia RouterA		

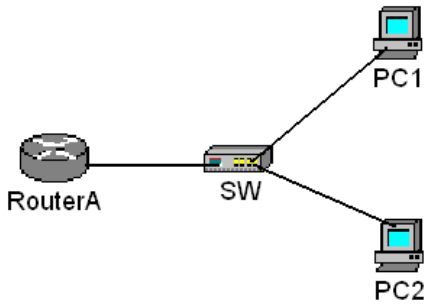
¿La lista funciona de acuerdo a lo esperado?

Al completar los pasos anteriores, borre la configuración de nvram de los equipos y reinicielos.

Práctica # 5 "Configuración de listas de acceso extendidas"

Objetivo

- Configurar y aplicar una ACL extendida para permitir o denegar tráfico específico.
- Probar la ACL para determinar si se lograron los resultados deseados.



Desarrollo.

En esta práctica se muestra la forma de operar de una lista de acceso extendida. Las listas de acceso extendidas, nos permiten controlar el tipo de tráfico de acuerdo con las direcciones origen/destino y el tipo de aplicación.

Paso 1. Configure el nombre de host y las contraseñas en el router MEX.

Paso 2. Permita el acceso HTTP ejecutando el comando **ip http server** en el modo de configuración global.

Paso 3. Configure los hosts en el segmento Ethernet.

Router MEX
Dirección IP 192.168.14.1/24

Host PC1
Dirección IP 192.168.14.2/24

Host PC2
Dirección IP 192.168.14.3/24

Paso 4. Guarde la información de configuración en nvram.

Paso 5. Confirmar la conectividad haciendo ping al gateway por defecto desde ambos hosts.

Paso 6. Acceda al router mediante una sesión web.

Paso 7. Desarrolle una lista de acceso que impida la conexión HTTP (Puerto 80) con el router a los hosts de la red.

MEX(config)#access-list 101 deny tcp 192.168.14.0 0.0.0.255 any eq 80
MEX(config)#access-list 101 permit ip any any

¿Por qué es necesario insertar la segunda sentencia?

Paso 8. Aplique la lista de acceso a la interfaz ethernet.

MEX(config-if)#ip access-group 101 in

Paso 9. Pruebe conectividad hacia el router desde los hosts por medio del comando ping

¿Los pings fueron exitosos?

Si es así, ¿por qué?

Paso 10. Conéctese al router mediante el navegador de Web.

¿Pudo establecer la sesión web?

¿Por qué?

Paso 11. Establezca una sesión telnet al router desde los hosts.

¿Pudo ejecutar con éxito el comando Telnet?

¿Por qué si o por qué no? Si es así, ¿por qué?

Al completar los pasos anteriores, borre la configuración de nvram y reinicie el router.