Universidad Tecnológica de El Salvador

INFORMÁTICA Y CIENCIAS APLICADAS

TÉCNICO EN INGENIERÍA DE REDES COMPUTACIONALES

TEMA:

"ELABORACIÓN DE UN MANUAL DE PRÁCTICAS CON ÉNFASIS EN IPV6 PARA LA ASIGNATURA TECNOLOGÍA CERTIFICADA EN REDES III DE LA UNIVERSIDAD TECNOLÓGICA DE EL SALVADOR"

TRABAJO DE GRADUACIÓN PRESENTADO POR:

JAVIER ERNESTO SALGUERO ABARCA
JOSE DAVID HERNANDEZ PINEDA
FABRICIO ERNESTO FLORES

PARA OPTAR AL GRADO DE:

TÉCNICO EN INGENIERÍA DE REDES COMPUTACIONALES

ABRIL, 2016
SAN SALVADOR, EL SALVADOR, CENTRO AMÉRICA

AUTORIDADES UNIVERSITARIAS

ING. NELSON ZÁRATE SÁNCHEZ

RECTOR

LIC. JOSÉ MODESTO VENTURA

VICERRECTOR ACADEMICO

ING. FRANCISCO ARMANDO ZEPEDA

DECANO

JURADO EXAMINADOR

LIC. LUIS RODRIGO PALOMO

PRESIDENTE

TEC. WILLIAM ENRIQUE GARCIA

PRIMER VOCAL

TEC. JUAN CARLOS AGUILAR

SEGUNDO VOCAL

ABRIL, 2016

SAN SALVADOR, EL SALVADOR, CENTROAMÉRICA

Universidad Tecnológica de El Salvador

ACTA DE EXAMEN PROFESIONAL

HABIÉNDOSE REUNIDO EL JURADO CALIFICADOR INTEGRADO POR:
Tec.William Enrique García Arias, Lic. Luis Rodrigo Palomo Quiñonez, Tec.Juan Carlos Aguilar Solorzano, a las 12:30m del día Jueves, 3 de diciembre de dos mil quince.
Y LUEGO DE HABER DELIBERADO SOBRE EL EXAMEN PROFESIONAL DE LOS ALUMNOS:

1- Javier Ernesto Salguero Abarca Carnet 26-4659-2012
2- José David Hernández Pineda Carnet 26-0363-2012
3- Fabricio Ernesto Flores Carnet 26-5145-2012

QUIENES PRESENTARON DEFENSA DE SU TRABAJO DE GRADUACION TITULADO:
"Elaboración de un manual de prácticas con énfasis en Ipv6 para la asignatura tecnología certificada en Redes III de la Universidad Tecnológica de El Salvador"

PARA OPTAR AL GRADO DE:

TÉCNICO EN INGENIERIA DE REDES COMPUTACIONALES

Y DEL CUAL TAMBIEN EVALUARON LOS CONOCIMIENTOS RELACIONADOS CON EL TEMA DEL MISMO. POR LO QUE ESTE JURADO RESUELVE DECLARAR EL EXAMEN COMO:

Aprobado

YA QUE CUMPLE CON LOS REQUISITOS ESTABLECIDOS EN EL REGLAMENTO DE GRADUACION DE LA UNIVERSIDAD.

San Salvador, 3 de diciembre de dos mil quince.

F._____
PRIMER VOCAL
Tec. William Enrique García Arias

F._____
SEGUNDO VOCAL
Lic. Luis Rodrigo Palomo Quiñonez

F._____
PRESIDENTE
Tec. Juan Carlos Aguilar Solorzano

AGRADECIMIENTOS

Damos gracias a Dios Todopoderoso por los logros hoy alcanzados, por el tiempo de vida, prosperidad y salud, por ser el primero y el último en aportar aquel esfuerzo, aquel soplo de aire y aliento, y el protagonista principal de nuestras vidas, “

Agradecemos a nuestras familias por todo el apoyo bridado durante este proceso, porque siempre nos dieron ánimos para seguir adelante.

Para nuestro asesor de trabajo de tesis, “Lic. Luis Palomo” por su tiempo, dedicación y tino en la guía en los proyectos desarrollados en nuestra tesis, Gracias.

Y a todos nuestros amigos, o personas que fueron parte de este gran proyecto que por motivos de espacio no podemos colocar todos sus nombres, **“muchas gracias”**

Atentamente,

Javier Ernesto Salguero

José David Hernández

Fabricio Ernesto Flores

Contenido

Introducción

En este documento se presenta información acerca de la elaboración de un manual de prácticas con énfasis en IPv6 para la asignatura tecnología certificada en redes III de la Universidad Tecnológica de El Salvador. El manual se desarrollará en dicha universidad en un periodo de tiempo que comprende desde el mes de agosto hasta diciembre de 2015. En el primer capítulo se explican las generalidades del proyecto, tales como la situación problemática, y se exponen las dificultades con las que se encuentran los estudiantes de la Universidad Tecnológica de El Salvador que cursan la materia de tecnología certificada en redes III, al momento de realizar sus prácticas con el Protocolo IP versión 6; seguido de esto se hace referencia de lo útil que será la creación de este manual y que beneficiará a los estudiantes de la carrera de técnico en ingeniería de redes computacionales, en relación sobre los conocimientos en IPv6 y su aplicación.

Con este material se pretende, que los alumnos aprendan de una manera sencilla pero eficaz, la implementación y uso del protocolo IPv6, al momento de configurar los equipos con esta nueva versión del protocolo IP, de la capa de Red del Modelo OSI.

CAPÍTULO I
SITUACIÓN ACTUAL

1.1 Situación problemática

En San Salvador capital de El Salvador en la dirección 19 Av. Norte 19 AV Sur, Se ubica la Universidad Tecnológica de El Salvador la cual desde 1981 con innovación como su lema abre las puertas a todos los salvadoreños dentro como fuera del el país con el objetivo de que cada estudiante sea capaz de trabajar en el mundo laboral con carreras de gran importancia en el mercado laboral, dicha universidad en su facultad de Informática y Ciencias Aplicadas ofrece la carrera de técnico en ingeniería de redes computacionales, la cual imparte el fundamento y orientación a la implementación y administración de redes de comunicación de datos. En La materia de Tecnología Certificada en Redes III de la carrera, se imparten conocimientos sobre el protocolo IPv6, pero no son los suficientes debido a que muchos de los estudiantes de esta materia no alcanzan a dominar, aprender y administrar el dicho protocolo, esto hace que muchos no logren adquirir las habilidades y competencias necesarias para desarrollar actividades que requieran el uso del protocolo IPV6.

1.2 Justificación

En la Actualidad, hay muchos estudiantes de la carrera de Técnico en Ingeniería de Redes Computacionales de la Universidad Tecnológica de El Salvador que no logran desarrollar al 100% las competencias con respecto al funcionamiento del protocolo IPv6; Esto debido al poco tiempo que se le dedica, o la falta de prácticas para que los estudiantes comprendan a totalidad el manejo y configuración de dicho protocolo.

Por lo cual se hace necesaria la creación de prácticas, para los estudiantes de la materia Tecnología Certificada en Redes III, con las que se pretende aumentar el nivel de aprendizaje de los mismos.

Es por ello que se crea un manual que facilite las herramientas para implementar varias de las características del protocolo IPv6, que permita generar competencias en el área de redes de datos y que dan la oportunidad de ser desarrolladas en el laboratorio de CISCO, ubicado en el edificio Francisco Morazán de dicha universidad, por si al estudiante le quedan ciertas dudas, pueda ir a desarrollarla nuevamente las veces que sean necesarias para aclarar y solventar generando un aprendizaje significativo.

1.3 Objetivos

1.3.1 Objetivo general

- Elaborar un manual de prácticas paso a paso sobre el protocolo de internet versión 6, para la asignatura de Tecnología Certificada en Redes III, como apoyo de enseñanza y aprendizaje en la cátedra de redes de la Universidad Tecnológica De El Salvador.

1.3.2 Objetivos específicos

- Conocer el nivel de conocimiento que existe en los estudiantes de la materia Tecnología Certificada en Redes III, sobre configuración e implementación del protocolo IPv6.

- Diseñar un modelo de prácticas de laboratorio para un dominio más práctico y claro en el manejo del protocolo IPv6.

- Crear un manual de prácticas paso a paso para reforzar y fortalecer el conocimiento de los estudiantes de la materia Tecnología Certificada en Redes III sobre el protocolo IPv6.

1.4 Alcances

- Mediante la administración de un instrumento, como la encuesta medir el nivel de conocimiento de los estudiantes de la asignatura de Tecnología Certificada de Redes III, de la Universidad Tecnológica de El Salvador acerca del manejo de protocolo IPv6.

- Ayudar a los estudiantes de la asignatura Tecnología Certificada en Redes III de la Universidad Tecnológica de El Salvador, para que desarrollen competencias tales como dominio y manejo del Protocolo IPv6.

- Aplicar las configuraciones de IPv6 a los diferentes equipos con la ayuda del manual de prácticas paso a paso, dirigido a los estudiantes de la materia de Tecnología Certificada en Redes III.

1.5 Estudio de factibilidad

1.5.1 Factibilidad técnica

Se observa las siguientes especificaciones técnicas en el laboratorio de CISCO de la Universidad Tecnológica de El Salvador, el cual se utilizará para el desarrollo de las prácticas de la asignatura Tecnología Certificada en Redes III; cuenta con hardware y software en buen estado para realizar dichas prácticas. (Cuadro 1.1)

ESPECIFICACIONES TÉCNICAS DE LOS EQUIPOS DEL LABORATORIO DE CISCO
HARDWARE ● Modelo: HP Compaq 6005 Pro SFF PC ● Procesador: AMD Phenom™ II X2 B55 Processor (2 CPUs), ~3.0GHz ● Memoria: 4096MB RAM **SOFTWARE** ● Sistema operativo: Windows 8.1 Pro 64 bits.

Cuadro 1.1 Especificaciones Técnicas

1.5.2 Factibilidad económica

La Universidad Tecnológica de El Salvador, cuenta con el equipamiento necesario para realizar las prácticas paso a paso, el grupo de trabajo no incurrirá en gasto alguno para este proyecto, puesto que el software a utilizar

es parte del laboratorio de CISCO, el cual cuenta con la autorización y licencia necesaria.

1.5.3 Factibilidad operacional

A continuación se presenta la factibilidad operacional, el cual permite observar el detalle de las prácticas de laboratorio para alcanzar los objetivos planteados. (Cuadro 1.2)

Operacional		
Número de practica	**Nombre de la practica**	**Duración**
#1	Subneteo con IPv6	60 minutos
# 2	Configuración de interfaces en un router y computadoras con IPv6.	60 minutos
# 3	Configuraciones de vlan´s con IPv6.	60 minutos
# 4	Configuración de intervlan con IPv6.	60 minutos
# 5	Configuración de enrutamiento con IPv6: Rutas estáticas.	60 minutos
# 6	Configuración de enrutamiento con IPv6: RIPng.	60 minutos
# 7	Configuración de enrutamiento con IPv6: OSPFv3.	60 minutos
# 8	Configuración de servicios con IPv6:DHCP.	60 minutos
#9	Configuración de TFTP con IPv6.	60 minutos

# 10	Configuración de ACL's con IPv6: estándar.	60 minutos
# 11	Configuración de ACL's con IPv6: extendidas.	60 minutos

Cuadro 1.2 Factibilidad Operacional

1.6 Carta de aceptación

San Salvador, Agosto del 2015

Universidad Tecnológica de El Salvador
Lic. Juan Pablo Ortiz Cinco
Responsable de la cátedra de redes
Presente

Reciba un cordial saludo de parte de los alumnos de la Universidad Tecnológica.

Por este medio queremos hacer de su conocimiento que se está desarrollando el proyecto de tesis “Elaboración de un manual de prácticas con énfasis en IPv6 para la asignatura Tecnología Certificada en Redes III de la Universidad Tecnológica de El Salvador", que está orientado a los Estudiantes de la carrera Técnico en Ingeniería de Redes Computacionales, para facilitarles el aprendizaje sobre el manejo y configuración del protocolo IPv6.

Dándoles a conocer nuestro proyecto de tesis el cual se entregará en el mes de noviembre del presente año y el personal involucrado para el desarrollo son:

Lic. Juan Pablo Ortiz Cinco Responsable de la cátedra	Tec. Luis Rodrigo Palomo Asesor y docente
Javier Ernesto Salguero Abarca Alumno	José David Hernández Alumno
Fabricio Ernesto Flores Alumno	

CAPÍTULO II
DOCUMENTACION TECNICA Y DISEÑO DE LA SOLUCION

2.1 Marco teórico de la solución.

2.1.1 Protocolo de internet (IP)

IP es un protocolo de comunicación de datos digitales clasificado, que funciona en la capa de red, basado en el modelo OSI. Su función principal es el uso bidireccional en origen o destino de comunicación para transmitir datos mediante un protocolo no orientado a conexión, que transfiere paquetes conmutados a través de distintas redes físicas previamente enlazadas según la norma OSI de enlace de datos. El diseño del protocolo IP se realizó presuponiendo que la entrega de los paquetes de datos sería no confiable. Así, IP tratará de realizarla del mejor modo posible, mediante técnicas de encaminamiento, no teniendo garantía de llegar a su destino final pero tratando de buscar la mejor ruta entre las conocidas por la máquina que esté usando IP.

Los datos en una red basada en IP son enviados en bloques conocidos como paquetes o datagramas. En particular, en IP no se necesita ninguna configuración antes de que un equipo intente enviar paquetes a otro con el que no se había comunicado antes.

IP provee un servicio de datagramas no fiable (IP no provee ningún mecanismo para determinar si un paquete alcanza o no su destino y únicamente proporciona seguridad (mediante checksums o sumas de comprobación) de sus cabeceras y no de los datos transmitidos. Por ejemplo, al no garantizar nada sobre la recepción del paquete, éste podría llegar dañado, en otro orden con respecto a otros paquetes, duplicado o simplemente no llegar. Si se necesita fiabilidad, ésta es proporcionada por los protocolos de la capa de transporte, como TCP. Las cabeceras IP contienen las direcciones de las máquinas de origen y destino (direcciones IP), direcciones que serán usadas por los enrutadores (Routers) para decidir el tramo de red por el que reenviarán los paquetes. El IP es el elemento común en el Internet de hoy. El actual y más popular protocolo de red es IPv4. IPv6 es el sucesor propuesto de IPv4; poco a poco Internet está agotando las direcciones disponibles por lo que IPv6 utiliza direcciones de fuente y destino de 128 bits, muchas más direcciones que las que provee IPv4 con 32 bits. Las versiones de la 0 a la 3 están reservadas o no fueron usadas. La versión 5 fue usada para un protocolo experimental. Otros números han sido asignados, usualmente para protocolos experimentales, pero no han sido muy extendidos.

Si la información a transmitir ("datagramas") supera el tamaño máximo "negociado" (MTU) en el tramo de red por el que va a circular podrá ser dividida en paquetes más pequeños, y reensamblada luego cuando sea necesario.

Estos fragmentos podrán ir cada uno por un camino diferente dependiendo de cómo estén de congestionadas las rutas en cada momento.

Las cabeceras IP contienen las direcciones de las máquinas de origen y destino (direcciones IP), direcciones que serán usadas por los enrutadores (Routers) para decidir el tramo de red por el que reenviarán los paquetes

2.1.2 Mecanismos de transición IPv6.

Los mecanismos de transición a IPv6 son las tecnologías que preparan y facilitan la transición de Internet de su infraestructura IPv4 al sistema de direccionamiento de nueva generación IPv6. Concretamente, hay métodos que permitirán a hosts conectados únicamente a IPv4 o IPv6 acceder a recursos sólo disponibles utilizando el otro protocolo.

La Internet Engineering Task Force (IETF) gestiona a los grupos de trabajo y discusiones hacia los Internet Drafts y procesos Request for Comments para desarrollar estos métodos. La traducción IP/ICMP sin estado (asíncrona) traduce entre los formatos de cabecera IPv6 y IPv4. El método SIIT define un rango de direcciones IPv6 llamado direcciones IPv4-traducidas (IPv4-translated). Es el prefijo (subred) ::ffff:0:0:0/96 y se puede escribir como ::ffff:0:a.b.c.d, donde la dirección en formato IPv4 a.b.c.d se refiere a un nodo "IPv6-disponible" (IPv6-enabled). Se ha elegido el prefijo para que diera un checksum de 0, evitando cambios en el checksum de la cabecera del protocolo de transporte.

El algoritmo permite que hosts IPv6 sin dirección IPv4 asignada se comuniquen con host sólo-IPv4. La asignación de direcciones y los detalles del encaminamiento no se abordan en la especificación.

La especificación es un producto de un grupo de trabajo IETF NGTRANS.

Los problemas y algoritmos en la traducción de los datagramas que contienen segmentos TCP se describen en RFC5382.

La fragmentación de paquetes IPv4 UDP que no contienen una suma de comprobación UDP (es decir, el campo checksum UDP es cero) no son de uso significativo en el Internet, y en general no se traduce por el IP / ICMP traductor. Sin embargo, cuando se configura el traductor para reenviar el paquete sin una suma de comprobación UDP, los paquetes IPv4 UDP fragmentados serán traducidos.

Paquetes ICMP / ICMPv6 fragmentados no se traducirán por la IP / ICMP traductor.

La traducción cabecera IP / ICMP se especifica en este documento es consistente con los requisitos de las cabeceras IP / ICMP multidifusión. Sin embargo, IPv4 direcciones multicast [RFC5771] no se pueden asignar a IPv6 multicast direcciones [RFC3307] basado en la regla de asignación unicast [RFC6052].

2.1.3 Generalidades de IPv6

Actualmente se utiliza con más frecuencia la versión 4 del Protocolo de Internet, el aumento de usuarios, aplicaciones, servicios y dispositivos está provocando la migración a una nueva versión.

IPv4 soporta 4.294.967.296 (232) direcciones de red, este es un número pequeño cuando se necesita otorgar a cada computadora, teléfonos, PDA, autos, etc.

IPv6 soporta 340.282.366.920.938.463.463.374.607.431.768.211.456 (2128 ó 340 sextillones) direcciones de red.

Por lo general las direcciones IPv6 están compuestas por dos partes lógicas: un prefijo de 64 bits y otra parte de 64 bits que corresponde al identificador de interfaz, que casi siempre se genera automáticamente a partir de la dirección MAC (Media Access Control Address) de la interfaz a la que está asignada la dirección.

La función de la dirección IPv6 es exactamente la misma a su predecesor IPv4, pero dentro del protocolo IPv6.

Está compuesta por 8 segmentos de 2 bytes cada uno, que suman un total de 128 bits, el equivalente a unos 3.4×1038 hosts direccionables. La ventaja con respecto a la dirección IPv4 es obvia en cuanto a su capacidad de direccionamiento.

La dirección 2001:BBBB:0000:1118:0000:0000:0000:0A00se divide:

2001 ----> Primer Hexteto

BBBB ----> Segundo Hexteto
0000 ----> Tercer Hexteto
....
0A00 ----> Octavo Hexteto

En total 8X16= 128 bits

Su representación suele ser hexadecimal y para la separación de cada par de octetos se emplea el símbolo "**:**". Un bloque abarca desde 0000 hasta FFFF.Para formar un número en hexadecimal sólo requerimos de 4 bits, diferente al sistema binario donde se necesita mínimo 8 bits. Observe la siguiente Tabla:

DECIMAL	BINARIO	HEXADECIMAL
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

Cuadro 2.13.1 Sistema Hexadecimal de IPv6

Los números decimales del 0 al 9 se expresan de esa misma forma en Hexadecimal, pero del número 10 al 15 se expresan con letras.

Algunas reglas acerca de la representación de direcciones IPv6 son:

- Los ceros iniciales, como en IPv4, se pueden obviar.

  Ejemplo:

  2001:0123:0004:00ab:0cde:3403:0001:0063 -> 2001:123:4:ab:cde:3403:1:63.

- Los bloques contiguos de ceros se pueden comprimir empleando "**::**". Esta operación sólo se puede hacer una vez.

  Ejemplo: 2001:0:0:0:0:0:0:4 -> 2001::4.

  Ejemplo no válido: 2001:0:0:0:2:0:0:1 -> 2001::2::1 (debería ser 2001::2:0:0:1ó 2001:0:0:0:2::1).

2.1.3.1 Paquetes IPv6

La cabecera se encuentra en los primeros 40 bytes del paquete, contiene las direcciones de origen y destino con 128 bits cada una, la versión 4 bits, la clase de tráfico 8 bits, etiqueta de flujo 20 bits, longitud del campo de datos 16 bits, cabecera siguiente 8 bits, y límite de saltos 8 bits.

Una dirección IP es un número que identifica de manera lógica y jerárquica a una interfaz de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP.

No debemos confundir la dirección MAC que es un número hexadecimal fijo que es asignado a la tarjeta o dispositivo de red por el fabricante por la dirección IP, mientras que la dirección IP se puede cambiar.

Quizás las principales características de la IPv6 se sintetizan en el mayor espacio de direccionamiento, seguridad, autoconfiguración y movilidad. Pero también hay otras que son importantes mencionar:

- Infraestructura de direcciones y enrutamiento eficaz y jerárquica.
- Mejora de compatibilidad para Calidad de Servicio (QoS) y Clase de Servicio (CoS).
- Multicast: envío de un mismo paquete a un grupo de receptores.
- Anycast: envío de un paquete a un receptor dentro de un grupo.
- Movilidad: una de las características obligatorias de IPv6 es la posibilidad de conexión y desconexión de nuestro ordenador de redes IPv6 y, por tanto, el poder viajar con él sin necesitar otra aplicación que nos permita que ese enchufe/desenchufe se pueda hacer directamente.
- Seguridad Integrada (IPsec): IPv6 incluye IPsec, que permite autenticación y encriptación del propio protocolo base, de forma que todas las aplicaciones se pueden beneficiar de ello.

- Capacidad de ampliación.
- Calidad del servicio.
- Velocidad.

2.1.3.2 Tipos de direcciones IP

A nivel general, podemos clasificar las direcciones IPv6 en tres grandes categorías:

- **Direcciones Unicast**
- **Direcciones Multicast**
- **Direcciones Anycast**

Unicast:

Las direcciones Unicast, al igual que IPv4, son las más comunes y utilizadas. Estas son asignadas a una Interface o nodo permitiendo la comunicación directa entre dos nodos de la red. Esta técnica de comunicación es conocida como uno a uno (one-to-one). A continuación podemos ver un ejemplo de una dirección IPv6 Unicast.

2001:0db8:3c4d:0015:0000:0000:1a2f:1a2b/64

Existen diferentes tipos de direcciones IPv6 dentro de la categoría Unicast:

- Link-Local
- Site-Local
- Global

Las direcciones Link-Local son el equivalente a las direcciones IP privadas en IPv4. Estas son asignadas a una interfaz de manera automática a partir del momento que activamos el protocolo IPv6 en un nodo.

El prefijo de estas direcciones es FE80::/10. Estas direcciones NO pueden ser encaminadas a través de los Routers fuera del segmento local, de ahí deriva su nombre. El propósito principal es proporcionar direccionamiento IP automático a los nodos en caso que NO exista un servidor DHCP.

Una dirección IPv6 Link-Local comienza con el prefijo FE80::/10 (los primeros 10 bits), luego los bits del 11 hasta 64 (los siguientes 54 bits) se configuran con valores de ceros (0000). De esta manera se forma la porción de red representada por los primeros 64 bits.

FE80:0000:0000:0000:0000:0000:0000:0000/10

La porción de nodo, que son los últimos 64 bits, se forma con el formato EUI-64. El formato EUI-64 toma los 48 bits de la dirección MAC de la tarjeta Ethernet y le coloca 16 bits adicionales predefinidos por el protocolo IPv6 (FFFE). A continuación tenemos un ejemplo de una dirección Link-Local.

FE80::211:21FF:FE6C:C86B

Las direcciones IPv6 Site-Local son también el equivalente a las direcciones IP privadas en IPv4. A diferencias de las direcciones Link-Local, estas pueden ser encaminadas fuera del segmento local, es decir, podemos enviar paquetes entre diferentes segmentos de la red pero NO hacia el Internet.

En las direcciones Site-Local, los primeros 10 bits se establecen con los valores 1111111011, por lo tanto, el prefijo de estas direcciones tendrá un valor en hexadecimal de FEC0 :: /10. Los siguientes 54 bits están compuestos por el ID de red. Los últimos 64 bits son el identificador de la interfaz o nodo, y estos se configuran de la misma forma que las direcciones Link-Local, tomando 48 bits de la dirección MAC y luego agregando 16 bits con los valores FFFE.

A continuación tenemos un ejemplo de una dirección Site-Local.

FEC0::CE00:3BFF:FE85:0

Las direcciones Global en IPv6 son el equivalente de las direcciones IP públicas en IPv4. Estas direcciones pueden ser encaminadas a través de la Internet. Los primeros 3 bits están compuestos por los valores 001 (en notación binaria), por lo tanto, el prefijo de estas direcciones IP tendrá un valor en hexadecimal de 2000 con una máscara /3.

Las direcciones Global son el tipo de dirección IPv6 más utilizado.

Multicast:

Las direcciones Multicast permiten identificar múltiples interfaces o nodos en una red. Con este tipo de direcciones podemos comunicarnos con múltiples nodos de manera simultánea. Esta técnica de comunicación es conocida como uno a mucho (one-to-many). A continuación podemos ver un ejemplo de una dirección IPv6 Multicast.

FF02:0:0:0:0:0:0:9

Anycast:

Las direcciones Anycast son un nuevo tipo de dirección en IPv6. Al igual que una dirección Multicast, una dirección Anycast identifican múltiples interfaces, sin embargo, mientras que los paquetes de Multicast son aceptados por varios equipos, los paquetes Anycast sólo se entregan a una interfaz o nodo. A continuación podemos ver un ejemplo de una dirección IPv6 Anycast.

2002:0db8:6301::/128

¿Y qué pasa con las direcciones Broadcast?

A diferencia de IPv4, el protocolo IPv6 NO soporta direcciones Broadcast. Para los que no conocen las direcciones Broadcast, estas son las direcciones utilizadas para la comunicación de un nodo con todos los nodos dentro de un segmento de red. Este tipo de dirección fue eliminado en IPv6.

2.1.4 VLAN

Una Virtual LAN (VLAN) es una división lógica del dominio de Broadcast a nivel de la Capa 2 del modelo OSI. También podemos decir que una VLAN es una agrupación lógica de dispositivos que se pueden comunicar en sí. Una VLAN es (red de área local virtual), es un método para crear redes lógicas independientes dentro de una misma red física. Varias VLAN pueden coexistir en un único conmutador físico o en una única red física. Son útiles para reducir el tamaño del dominio de difusión y ayudan en la administración de la red,

separando segmentos lógicos de una red de área local por ejemplo, los departamentos de una empresa, que no deberían intercambiar datos usando la red local; aunque podrían hacerlo a través de un enrutador o un conmutador de capa 3 y 4.

Una VLAN consiste en dos redes de computadoras que se comportan como si estuviesen conectados al mismo PCI, aunque se encuentren físicamente conectados a diferentes segmentos de una red de área local (LAN). Los administradores de red configuran las VLAN mediante hardware en lugar de software, lo que las hace extremadamente fuertes.

Aunque las más habituales son las VLAN basadas en puertos (nivel 1), las redes de área local virtuales se pueden clasificar en cuatro tipos según el nivel de la jerarquía OSI en el que operen, también se tiene varios tipos de VLAN como por ejemplo:

VLAN de nivel 1 (por puerto), también conocida como “portswitching”, Se especifica qué puertos del switch pertenecen a la VLAN, los miembros de dicha VLAN son los que se conecten a esos puertos. No permite la movilidad de los usuarios, habría que volver a configurar las VLAN si el usuario se mueve físicamente.

VLAN de nivel 2 por direcciones MAC. Se asignan hosts a una VLAN en función de su dirección MAC. Tiene la ventaja de que no hay que reconfigurar el dispositivo de conmutación si el usuario cambia su localización, es decir, se

conecta a otro puerto de ese u otro dispositivo. El principal inconveniente es que si hay cientos de usuarios habría que asignar los miembros uno a uno.

VLAN de nivel 2 por tipo de protocolo. La VLAN queda determinada por el contenido del campo tipo de protocolo de la trama MAC. Por ejemplo, se asociaría VLAN 1 al protocolo IPv4, VLAN 2 al protocolo IPv6, VLAN 3 a AppleTalk, VLAN 4 a IPX.

VLAN de nivel 3 por direcciones de subred (subred virtual). La cabecera de nivel 3 se utiliza para mapear la VLAN a la que pertenece. En este tipo de VLAN son los paquetes, y no las estaciones, quienes pertenecen a la VLAN. Estaciones con múltiples protocolos de red (nivel 3) estarán en múltiples VLAN.

VLAN de niveles superiores. Se crea una VLAN para cada aplicación: FTP, flujos multimedia, correo electrónico... La pertenencia a una VLAN puede basarse en una combinación de factores como puertos, direcciones MAC, subred, hora del día, forma de acceso, condiciones de seguridad del equipo.

2.1.5INTER-VLAN con IPv6

Cuando creamos VLANs, agrupamos varios dispositivos en un mismo dominio de broadcast, totalmente aislado del resto. Por ello, cada VLAN debe tener un direccionamiento IP diferente al de todas las demás.

Si queremos que puedan comunicarse las VLANs entre sí, es necesario contar con un dispositivo de capa 3 que enrute los paquetes, ya sea un switch multicapa o un router.

Si se conecta un router a un switch para que sea capaz de enrutar estos paquetes, la interfaz del router será un enlace troncal con el switch configurado como “router-on-a-stick” que, básicamente, es una única interfaz física con una serie de sub-interfaces para comunicar una VLAN con otra. Su funcionamiento es simple, acepta las tramas etiquetadas a través del troncal y las conmuta entre las diferentes sub-interfaces (interfaces lógicas o virtuales que pertenecen a cada una de las VLANs configuradas en el switch) para enviarlas a la VLAN que corresponda.

Cada una de las subinterfaces deberá tener una dirección IP del rango de la VLAN a la que pertenece y hará de su puerta de enlace.

Si en lugar de un router conectamos un switch multicapa, no necesitamos un dispositivo dedicado para este enrutamiento, sino que el propio switch puede llevar a cabo esa labor porque trabaja con las capa 2 y 3. Para ello, el switch debe tener habilitado el enrutamiento IP.

Un switch multicapa tiene ciertas ventajas con respecto a un router, como por ejemplo que puede enrutar más rápido el tráfico entre VLANs ya que lo hace internamente a nivel de hardware, mientras que un router tiene que compartir

un solo enlace troncal para todas las VLANs. En ese caso, será la propia velocidad del enlace la que marque la velocidad de transmisión.

Sin embargo, también hay desventajas: un router puede tener funcionalidades de seguridad que un switch multicapa no tiene.

2.1.6 Protocolos de enrutamiento.

Los protocolos de enrutamiento permiten a los routers poder dirigir o enrutar los paquetes hacia diferentes redes usando tablas. Existen protocolos de enrutamiento estático y dinámicos.

Protocolo de Enrutamiento Estático: Es generado por el propio administrador, todas las rutas estáticas que se le ingresen son las que el router “conocerá”, por lo tanto sabrá enrutar paquetes hacia dichas redes.

Protocolos de Enrutamiento Dinámico: Con un protocolo de enrutamiento dinámico, el administrador sólo se encarga de configurar el protocolo de enrutamiento mediante comandos IOS,en todos los routers de la red y estos automáticamente intercambiarán sus tablas de enrutamiento con sus routers vecinos, por lo tanto cada router conoce la red gracias a las publicaciones de las otras redes que recibe de otros routers.

2.1.6.1 Enrutamiento estático

Las rutas estáticas se definen administrativamente y establecen rutas específicas que han de seguir los paquetes para pasar de un puerto de origen

hasta un puerto de destino. Se establece un control preciso del enrutamiento según los parámetros del administrador.

Las rutas estáticas por default especifican un gateway (puerta de enlace) de último recurso, a la que el router debe enviar un paquete destinado a una red que no aparece en su tabla de enrutamiento, es decir que desconoce.

Las rutas estáticas se utilizan habitualmente en enrutamientos desde una red hasta una red de conexión única, ya que no existe más que una ruta de entrada y salida en una red de conexión única, evitando de este modo la sobrecarga de tráfico que genera un protocolo de enrutamiento. La ruta estática se configura para conseguir conectividad con un enlace de datos que no esté directamente conectado al router. Para conectividad de extremo a extremo, es necesario configurar la ruta en ambas direcciones. Las rutas estáticas permiten la construcción manual de la tabla de enrutamiento.

El comando iproute configura una ruta estática, los parámetros del comando definen la ruta estática.

Las entradas creadas en la tabla usando este procedimiento permanecerán en dicha tabla mientras la ruta siga activa. Con la opción permanent, la ruta seguirá en la tabla aunque la ruta en cuestión haya dejado de estar activa.

La sintaxis de configuración de una ruta estática es la siguiente:

Router(config)#iproute[red][máscara][direcciónip/interfaz][distancia][permanent]

Red: Es la red o subred de destino.

Máscara: Es la máscara de subred.

Dirección: Es la dirección IP del router del próximo salto.

Interfaz: es el nombre de la interfaz que debe usarse para llegar a le red de destino.

Distancia: Es un parámetro opcional, que define la distancia administrativa.

Permanent: un parámetro opcional que especifica que la ruta no debe se eliminada, aunque la interfaz deje de estar activa.

Cuando configuramos una ruta estática en IPv6 utilizando Cisco IOS, el procedimiento es el siguiente:

1. Habilitar el enrutamiento IPv6 (por defecto no está activo).

2. Definir las rutas estáticas.

Router#configure terminal

Router(config)#ipv6 unicast-routing

Ya que el enrutamiento IPv6 no se encuentra habilitado por defecto en IOS, es necesario habilitarlo explícitamente.

Router(config)#ipv6 route [prefijo] [próximo salto] [distancia administrativa]

La sintaxis del comando que crea rutas IPv6 es semejante a la que utilizamos en redes IPv4.

¿Cómo se configura entonces una ruta IPv6 por defecto?

Nada muy complejo. Siguiendo la misma lógica aplicada hasta aquí:

Router(config)#ipv6 route::/0 [próximo salto]

2.1.6.2 OSPFV3

OSPFv3 es un estado de vínculos protocolos de enrutamiento como su predecesor en IPv4. Se sigue utilizando las zonas autónomas para separar las redes en áreas.

OSPFv3 usa un rango de direcciones IPv6 multicast FF02 :: de 5 para las rutas OSPF y FF02 :: 6 para OSPF designado routers al enviar actualizaciones y reconocimientos.

Routers OSPF generan actualizaciones de enrutamiento sólo cuando se produce un cambio en la topología de red.

Cuando un enlace de ruta cambia de estado, el dispositivo de red que detecta el cambio crea un enlace de Estado Advertisement (LSA) y lo reenvía a la DR utilizando FF02 :: 6 dirección de multidifusión que informa a todos los dispositivos dentro de un área usando FF02 :: 5 dirección de multidifusión. Cada dispositivo se actualiza su base de datos de estado de enlace.

Una de las nuevas características de OSPFv3 es la posibilidad de asignar el ID de router, ID de área y de estado de enlace ID con un valor de 32 bits sin direcciones IP. Esta característica permite OSPFv3 sea enrutable sobre casi cualquier protocolo de capa de red. Al igual que otros protocolos de enrutamiento IPv6 - RIPng y EIGRPv6, debe habilitar directamente en la interfaz del router para que el proceso funcione.

Requisitos de configuración OSPFv3:

- Requisitos de configuración OSPFv3:
- Habilitar IPv6 enrutamiento unicast
- Habilitar el proceso de enrutamiento OSPFv3
- Habilitar OSPFv3 en la interfaz
- Configurar las interfaces pasivas para suprimir las actualizaciones de enrutamiento hacia y desde una interfaz.

El proceso de configuración de la interfaz es sólo para asignar una ID de proceso OSPFv3 y zona.

2.1.6.3Ripng

El avance de la implementación de IPv6 exige que, no sólo conozcamos la versión actual del protocolo de direccionamiento de capa de red, sino también los protocolos de enrutamiento asociados al mismo.
IPv6 es un protocolo enrutado completamente diferente de IPv4. En consecuencia los protocolos de enrutamiento IP que se utilizan en el entorno tradicional no son aplicables en redes IPv6. Por esto son necesarios protocolos de enrutamiento específicos que respondan a la nueva arquitectura de IPv6.

- Routing Information Protocol next generation.
- RFC 2080.
- Protocolo de enrutamiento de vector distancia.
- Básicamente es una actualización de RIPv2.
- Número máximo de saltos: 15.
- Implementa splithorizon y poison reverse.
- Utiliza el puerto 521 de UDP para las comunicaciones.
- NO es compatible con RIPv2.
- Actualizaciones dirigidas a la dirección multicast FF02::9.
- Utiliza la dirección link-local de la interfaz del próximo salto en la tabla de enrutamiento.
- Cisco IOS soporta hasta 4 instancias de RIPng por dispositivo.

Ripng incluye varias funciones avanzadas:

- Puede generar rutas por defecto.

- Soporta redistribución de rutas originadas en otros protocolos o estáticas.
- Se requiere definir manualmente una métrica al redistribuir rutas dentro de RIPng.
- Permite la implementación de tags en las rutas.
- Soporta balanceo de tráfico por defecto, entre hasta 4 rutas de igual métrica.

Configuración básica de RIPng:

Router(config)#ipv6 router rip [tag]

Router(config-router)# exit

Router(config)#interface [interfaz]

Router(config-if)#ipv6 rip [tag] enable

Router(config-if)#ipv6 rip [tag] default-information originate

Monitoreo de RIPng:

Router#show ipv6 protocols

Router#show ipv6 rip

Router#show ipv6 rip database

Router#show ipv6 route rip

Router#debug ipv6 rip

2.1.7 Servicios de red con IPV6

Un servicio de red es la creación de una red de trabajo en un ordenador. Generalmente los servicios de red son instalados en uno o más servidores para permitir el compartir recursos a computadoras clientes.

Algunos servicios de red más comunes son:

2.1.7.1 DHCP

DHCPv6 El Protocolo de configuración dinámica de host (DHCP) se diseñó para encargarse de la asignación de direcciones IP y otra información de red a los equipos, de forma que puedan comunicarse en la red automáticamente. DHCP para IPv6 (DHCPv6) puede proporcionar configuración de direcciones con estado o configuración sin estado a hosts de IPv6.

La asignación dinámica de direcciones IPv6 de unidifusión global se puede configurar de tres maneras:

- Solo mediante configuración automática de dirección sin estado (SLAAC)
- Mediante el protocolo de configuración dinámica de host sin estado para IPv6 (DHCPv6)

- Mediante DHCPv6 con estado Con SLAAC (se pronuncia “slac”), no se necesita un servidor de DHCPv6 para que los hosts adquieran direcciones IPv6. Se puede usar para recibir información adicional que necesita el host, como el nombre de dominio y la dirección del servidor de nombres de dominio (DNS). El uso de SLAAC para asignar direcciones host IPv6 y de DHCPv6 para asignar otros parámetros de red se denomina “DHCPv6 sin estado”. Con DHCPv6 con estado, el servidor de DHCP asigna toda la información, incluida la dirección host IPv6. La determinación de cómo los hosts obtienen la información de direccionamiento dinámico IPv6 depende de la configuración de indicadores incluida en los mensajes de anuncio de router (RA).

2.1.7.2 TFTP

Son las siglas de Trivial file transfer Protocol (Protocolo de transferencia de archivos trivial). Es un protocolo de transferencia muy simple semejante a una versión básica de FTP. TFTP a menudo se utiliza para transferir pequeños archivos entre ordenadores en una red, como cuando un terminal X Window o cualquier otro cliente ligero arranca desde un servidor de red.

Algunos detalles del TFTP:

- Utiliza UDP (en el puerto 69) como protocolo de transporte (a diferencia de FTP que utiliza el puerto 21 TCP).

- No puede listar el contenido de los directorios.
- No existen mecanismos de autenticación o cifrado.
- Se utiliza para leer o escribir archivos de un servidor remoto.
- Soporta tres modos diferentes de transferencia, “netascii”, “octet” y “mail”, de los que los dos primeros corresponden a los modos “ascii” e “imagen” (binario) del protocolo FTP.

Recuperación TFTP

IP ADDRESS= IP de la primera interfaz del Router.

IP SUBNET MASK= Máscara de la primera interfaz del Router.

DEFAULT GATEWAY= Puerta de enlace.

TFTP SERVER= IP del servidor TFTP que contiene la imagen a restaurar. TFTP FILE= Nombre de la IOS en el servidor TFTP.

(Tftpdnld) Ejecuta el modo de recuperación.

(Reset) Reinicia el dispositivo para cargar la IOS.

2.1.8 ¿Qué es seguridad IPv6?

Una de las promesas de IPv6 es de más seguridad, IPv4 se ha ganado su reputación en las últimas décadas, y nos hemos familiarizado con lo que puede

y no puede hacer, por otro lado, se tiene poca o ninguna experiencia con IPv6 en el mundo real ya que en papel, IPv6 parece ser excelente, En el mejor de los casos, IPv6 ofrece mejor seguridad pero no la garantiza.

Caso en cuestión: IPSec. Esencialmente, esto asegura la comunicación IP al encriptar y autenticar paquetes IP. En IPv4, era una característica opcional; en IPv6, es obligatoria. Volver una característica obligatoria, no significa que tendrá un amplio soporte; el punto es que IPv6 no es automáticamente más seguro. Va a tomar mucha preparación de pre-lanzamiento y una inmensa cantidad de vigilancia de seguridad para ejecutarla correctamente.

Para las empresas, hay mucho que considerar, y esto muy seguramente cae en la responsabilidad del Jefe de Seguridad de la Oficina. Hay muchas trampas y obstáculos que evitar, y a continuación se analizan los que se deben cuidar muy cerca.

2.1.8.1 ACL estándar

Las ACL estándar son el tipo más antiguo de ACL. Su aparición se remonta a la versión 8.3 del software Cisco IOS. Las ACL estándar controlan el tráfico por medio de la comparación de la dirección de origen de los paquetes IP con las direcciones configuradas en la ACL.

Este es el formato de la sintaxis de los comandos de una ACL estándar.

access-list*access-list-number* {permit|deny} {*host*|*sourcesource-wildcard*|any}

En todas las versiones del software, *access-list-number* puede ser cualquier número del 1 al 99. En la versión 12.0.1 del software Cisco IOS, las ACL estándar empiezan a usar más números (del 1300 al 1999). Estos números adicionales se denominan ACL IP ampliadas. En la versión 11.2 del software Cisco IOS se añadió la posibilidad de utilizar un valor *name* de lista en las ACL estándar.

Después de definir la ACL, se debe aplicar a la interfaz (entrante y saliente). En versiones anteriores del software, "out" era el valor predeterminado cuando la palabra clave "out" o "in" no se había especificado. En las versiones posteriores del software, se debe especificar la dirección.

interface<interface>ip access-group number {in|out}

2.1.8.2 ACL extendidas

A diferencia de lo que sucede con la ACL estándar, las extendidas permiten especificar hacia dónde se dirige el tráfico y con ésta característica, yo puedo bloquear o permitir un tráfico mucho más específico: sólo tráfico que proviene del host pero se dirige a una red en particular o a otro host en particular o sólo el tráfico de una red que se dirige a otra red en particular. El truco se logra con el hecho de permitir comparar las direcciones destino de los paquetes contra la acl, no sólo las direcciones origen. Dentro de lo que hemos venido manejando, hablamos que una acl está compuesta por un conjunto de reglas todas con el mismo identificador, que cada regla era una línea compuesta por una acción y

una condición que el paquete debe cumplir para aplicarle la acción (permitir o denegar). Las condiciones en las acl estándar están compuestas por una dirección de referencia y una wildcard que dice qué bits de la dirección origen de los paquetes se deben comparar con la dirección de referencia, en las acls extendidas se especifica dos pares de direcciones de referencia/wildcard, un par para la dirección origen de los paquetes y otro par para la dirección destino de los mismos.

En ésta lista observamos varias cosas nuevas: *ip*, las acl extendidas no sólo permiten especificar las direcciones origen y destino sino discriminar por protocolos e incluso por parámetros particulares de cada protocolo pero eso lo veremos luego, por lo pronto lo importante es que *ip* indica que todos los protocolos que se encapsulan dentro de ip serán afectados por ésta lista de acceso. En este caso, la palabra *ip* para los protocolos es similar a *any* en las direcciones, casi todo se encapsula en ip por lo tanto especificar ip es como especificar cualquier protocolo (de capa 4 en adelante). En vez de *ip* se puede poner un protocolo equivalente o de capa 4, por ejemplo se puede filtrar *icmp, tcp o udp,* cambiando la palabra *ip* por éstas últimas.

Otra cosa importante y nueva es un segundo par de dirección de referencia/máscara wildcard, éste segundo par compara la dirección destino de los paquetes con la dirección de la regla. Para las acls extendidas, el paquete debe coincidir tanto en la dirección origen como en la destino.

CAPÍTULO III
PROPUESTA DE LA SOLUCION

3.1 Propuesta de la Solución

En este capítulo, se dará a conocer la solución propuesta para que este proyecto pueda llevarse a cabo o mejor dicho tenga una finalización satisfactoria con la realización del mismo.

Formulación de una solución al problema.

En el capítulo anterior, se recolectaron todos los datos necesarios que servirán para dar paso a la propuesta de solución planteada. En este capítulo se presentan los componentes principales concernientes al desarrollo de la investigación, tales como: generalidades, diseño, desarrollo y requerimientos del manual de prácticas propuesto.

Antes de desarrollar el contenido de este capítulo, cabe mencionar que desde el inicio del trabajo se conceptualizó que el proyecto se orientaría al apoyo de los estudiantes de la carrera Técnico en Ingeniería de Redes Computacionales de la Universidad Tecnológica de El Salvador.

El Manual contará con 11prácticas, 10 de ellas contarán con su respectivo archivo en formato (.pka).

3.1.1 Planteamiento del Proyecto Temático

A continuación de detallará cada una de las fases que compone la realización del manual de prácticas, siendo estas las siguientes:

Fase 1: Investigación

Se realizará una investigación exhaustiva sobre los temas relacionados al protocolo IPv6 que dará como resultado el Capítulo II de este trabajo de graduación, en el cual quedaran/ron reflejadas todas las generalidades de cada uno de los temas propuestos para la creación de las prácticas.

Fase 2: Diseño de las prácticas.

Se crearán 11prácticas que formarán parte del manual propuesto para fortalecer el conocimiento de los estudiantes acerca del protocolo IPv6.

Cada práctica contara con la siguiente estructura:

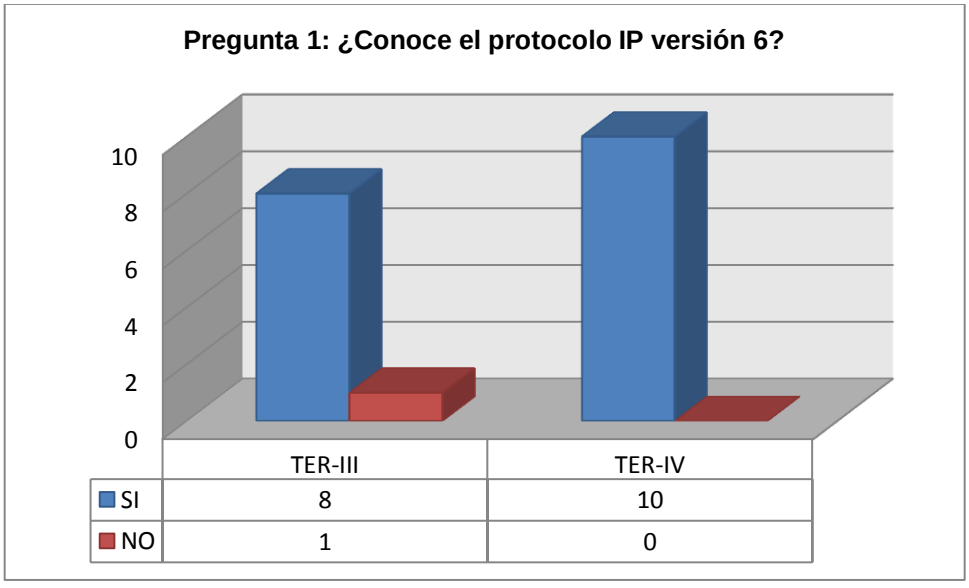
- Número de la práctica.
- Tema.
- Topología propuesta
- Tabla de direccionamiento.
- Objetivo de la práctica.
- Procedimiento a seguir.

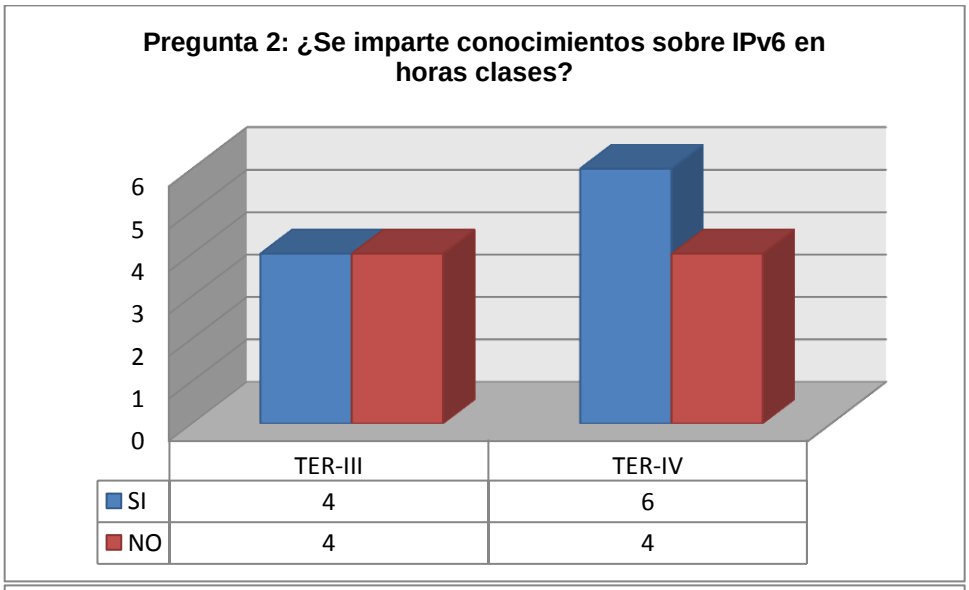
Fase 3: Implementación.

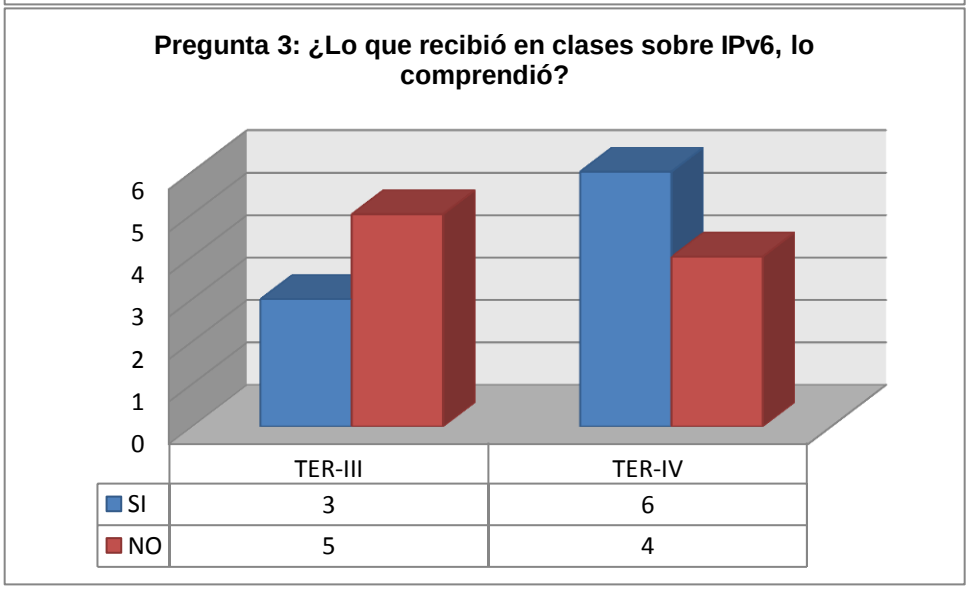
Una vez las prácticas estén finalizadas, se procederá a ubicarlas en una carpeta en el escritorio de las maquinas instaladas en el laboratorio de CISCO (Escritorio/Curricula CISCO/PracticasIPV6),todo esto con el propósito que los estudiantes puedan hacer uso de ellas en horas de prácticas libres.

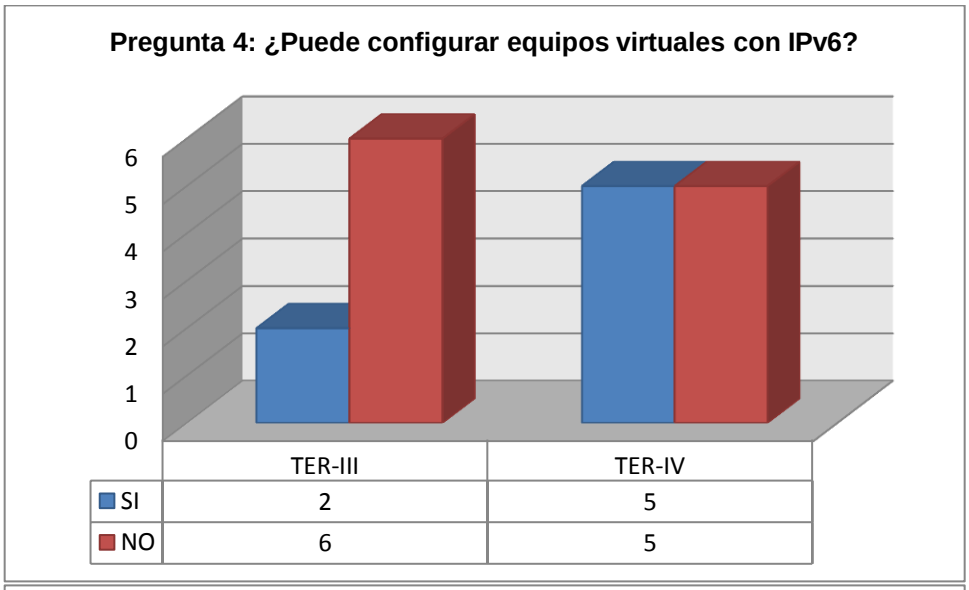
3.1.2 Instrumento de medición de la situación actual

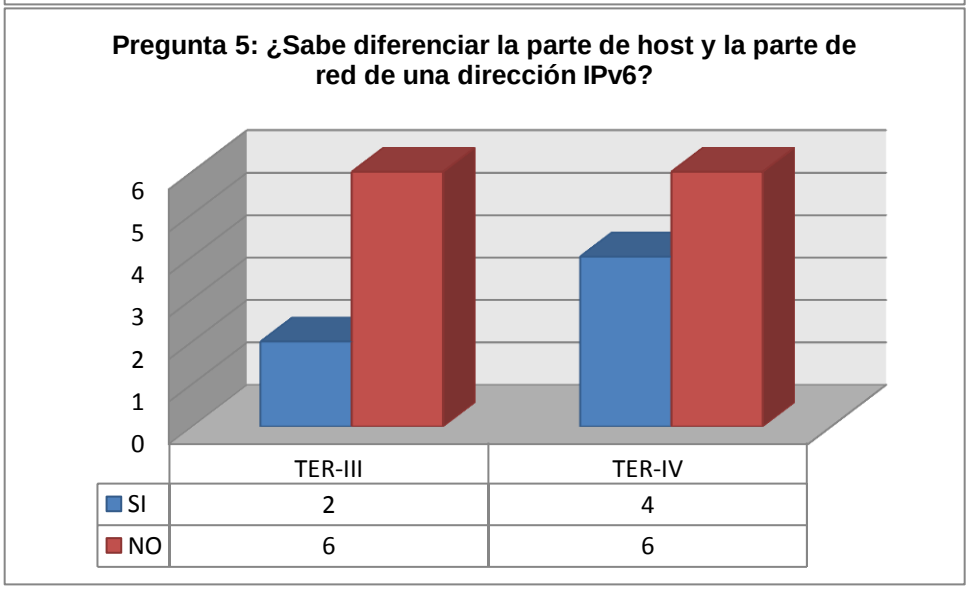
Se realizó una encuesta a estudiantes activos de la materia Tecnología Certificada en Redes III y IV (Anexo 1), con la que se identificó la situación actual de los mismos en materia de IPv6, logrando hacer una comparación entre las dos materias, siendo los resultados los siguientes:



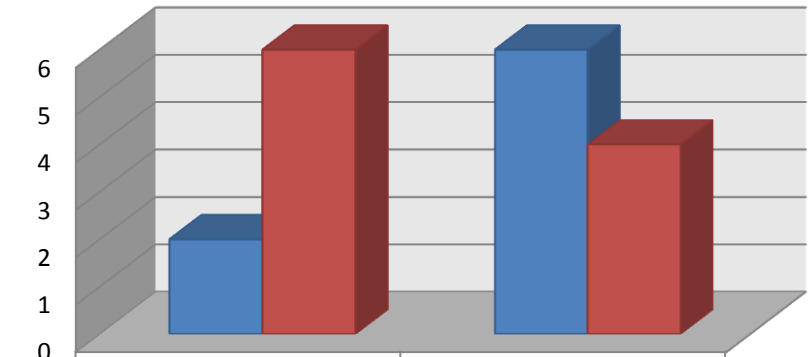

Pregunta 2: ¿Se imparte conocimientos sobre IPv6 en horas clases?
6
5
4
3
2
1
0
TER-III
TER-IV
SI
4
6
NO
4
4


Pregunta 3: ¿Lo que recibió en clases sobre IPv6, lo comprendió?
6
5
4
3
2
1
0
TER-III
TER-IV
SI
3
6
NO
5
4


Pregunta 4: ¿Puede configurar equipos virtuales con IPv6?
6
5
4
3
2
1
0
TER-III
TER-IV
SI
2
5
NO
6
5

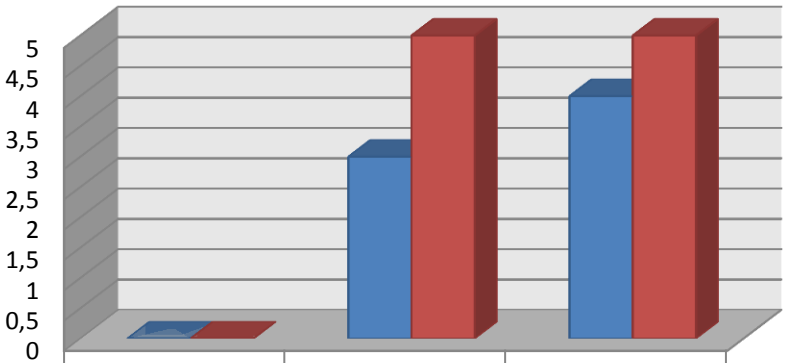

Pregunta 5: ¿Sabe diferenciar la parte de host y la parte de red de una dirección IPv6?
6
5
4
3
2
1
0
TER-III
TER-IV
SI
2
4
NO
6
6

Pregunta 6: ¿Puede configurar equipos físicos con Ipv6?

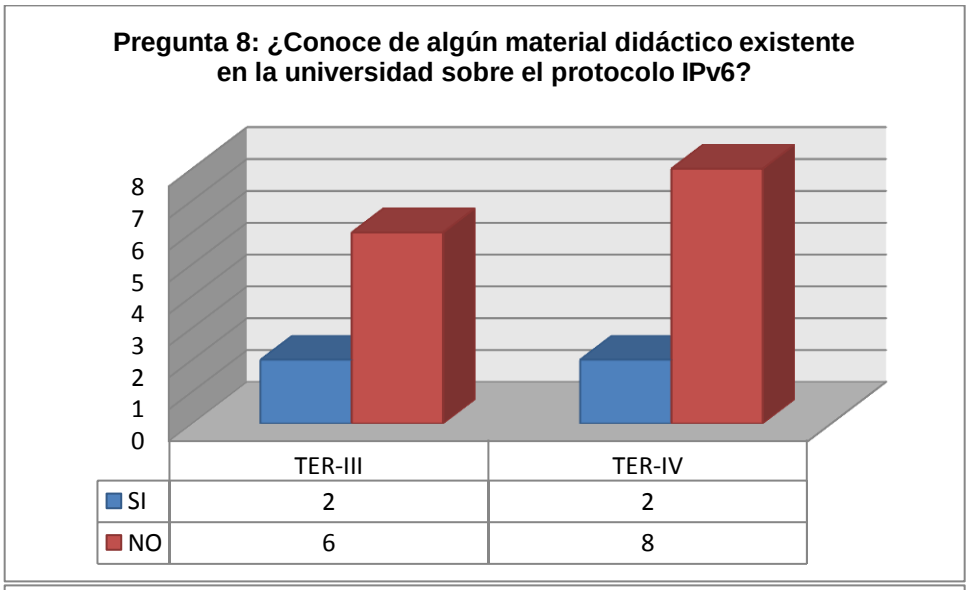


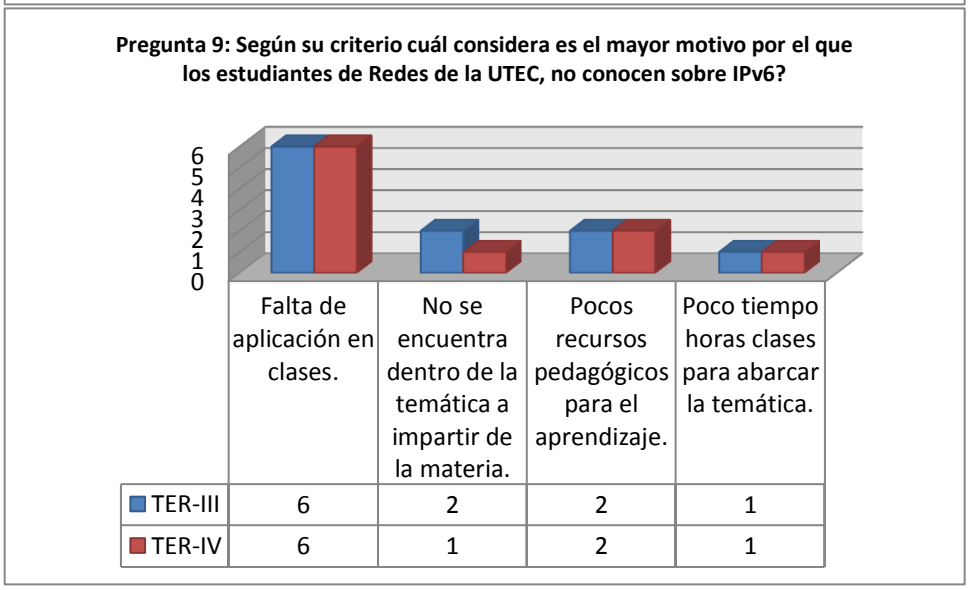
	TER-III	TER-IV
SI	2	6
NO	6	4

Pregunta 7: ¿Qué tanto conocimiento maneja sobre IPv6?



	BASTANTE	LO BASICO	MUY POCO
TER-III	0	3	4
TER-IV	0	5	5



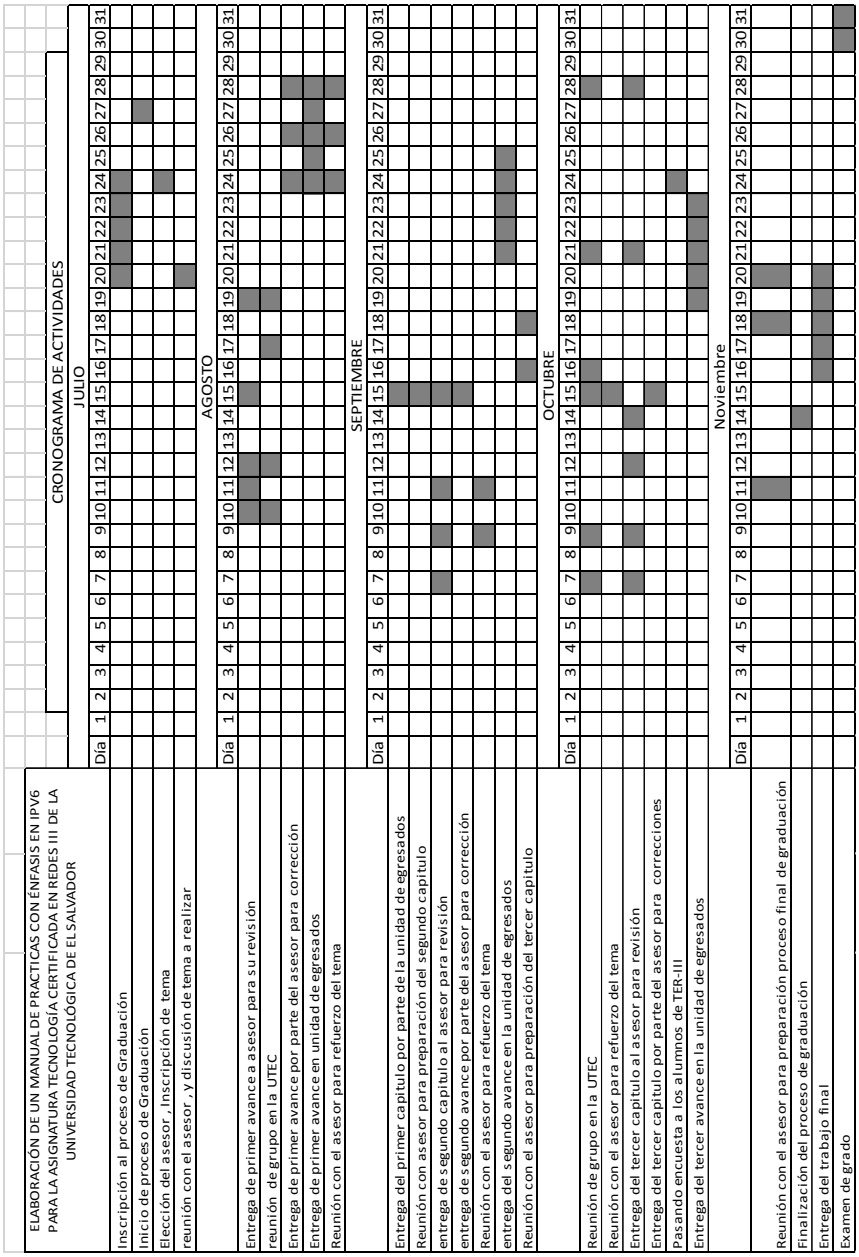


Interpretación de los resultados

Con los resultados obtenidos de la encuesta realizada, se identificó que los conocimientos de los estudiantes de la materia Tecnología Certificada en Redes III son básicos, y que no existe material didáctico en el laboratorio de CISCO de la universidad que los ayude a reforzar esos conocimientos. Con lo cual se

hace necesaria la creación de un manual de prácticaspaso a paso para fortalecer los conocimientos en materia de IPv6.

3.1.3 Cronograma de actividades



3.1.4 Tecnologías y Recursos Seleccionados

A continuación se presenta un cuadro que contiene una breve descripción de las tecnologías seleccionadas a nivel de hardware y software para el desarrollo del presente proyecto:

Equipo	Modelo	Descripción
Computadora	HP Compaq 6005 pro sff pc	Computadora de escritorio de uso múltiple para el desarrollo de actividades tanto de educación aprendizaje, ocio, etc.

PacketTracer	Versión 6.2	Software diseñado por la compañía cisco la cual está para emplear diseños, configuraciones e implementación de protocolos en una red virtual. Ofrece la oportunidad de desempeñar topologías simples o complejas de escala para redes de área local o redes extendidas, sistemas de internet inalámbrico y físico.

Adobe Reader		Software diseñado para visualizar documentos de texto en formato PDF. Este programa ofrece la oportunidad de visualizar documentos de texto como prácticas, presentaciones, diagramas, etc.

Cuadro 3.1 Recursos seleccionados.

3.1.5 Diseño de la Propuesta

Objetivos:

Parte 1: Obtener la habilidad de subnetear una dirección ipv6

Parte 2: Comprender los prefijos en una dirección ipv6

Parte 1

Procedimiento

Paso 1: Nos brindan la siguiente dirección IPv6 : 2001:db8::/64 , y solicitan que realicemos lo siguiente:

- Modificar el /64 a /75
- Tomar la tercera red calculada y cambiar de /75 a /80
- Tomar la segunda red calculada del /80 y llevarla a /82

Paso 2: modificar el prefijo de /64 a /75, para lograr esto primero se necesita identificar la longitud de partida de la dirección.

2001:bd4:0:0::/64 = 2001:0bd4:0000:0000::/64

Paso 3: Ahora tendremos que identificar la longitud final que en este caso sería con un nuevo prefijo, el cual es el /75, la longitud final quedaría de la siguiente forma:

2001:0bd4:0000:0000:0000 0000 0000 0000::/75

El segmento 5 es transformado en forma binaria

Lo que se realizó en el paso anterior es lo siguiente, en el segmento 5 pasamos cada valor hexadecimal a binario, para contar los bits que nos hacen falta para lograr obtener el prefijo /75. Es importante mencionar que en el segmento 5 no se toman los 16 bits, sino que solo ocuparemos los bits necesario para llegar al prefijo /75.

Paso 4: Ahora calcular la dirección del siguiente salto, para lograr esto vamos a contar la cantidad de bits que nos han sobrado del número hexadecimal que estamos trabajando. en el segmento 5 estamos trabajando en el numero hexadecimal que está en la tercera posición

0000 0000 0000 0000

1ª 2ª 3ª 4ª

Como en esa tercera posición ha sobrado un cero el salto será de la siguiente forma:

Exponente = Salto

Base binario $2^1 = 2$ Resultado

El salto para determinar cada subred será de 2, podemos notar que es sencillo encontrar este valor.

Paso 5: Ahora regresamos los bits de binario a notación hexadecimal e identificaremos el número hexadecimal donde se realizara el cambio.

2001:0bd4:0000:0000:0000::/75

Paso 6: Ya que hemos identificado donde será el salto nos dispondremos a construir nuestra tabla de red, para este ejemplo solo colocaremos 4 subredes. La tabla nos quedaría de la siguiente forma:

Nº	Dirección Inicial	Dirección Final
1	2001:0bd4:0000:0000:0000::/75	2001:0bd4:0:0:001F:FFFF:FFFF:FFFF/75
2	2001:0bd4:0000:0000:0020::/75	2001:0bd4:0:0:003F:FFFF:FFFF:FFFF/75
3	2001:0bd4:0000:0000:0040::/75	2001:0bd4:0:0:005F:FFFF:FFFF:FFFF/75
4	2001:0bd4:0000:0000:0080::/75	2001:0bd4:0:0:009F:FFFF:FFFF:FFFF/75

Paso 7: Siguiendo con el ejercicio ahora tomaremos la tercera subred del cuadro anterior y la cambiaremos de /75 a /80, realizaremos los mismos pasos que hicimos anteriormente, primero identificamos la longitud de partida y la longitud final que se necesita de dirección.

2001:0bd4:0000:0000:0040::/75 (Dirección de partida)

2001:0bd4:0000:0000:0040::/80 (Dirección final)

Si nos damos cuenta solo necesitamos 5 bits para completar el prefijo de /75 a /80 y esos 5 bits están en el segmento 5.

2001:0bd4:0000:0000:0000 0000 0100 0000/80

Paso 8: Ahora nos dispondremos a encontrar el salto, el salto seria la cantidad de bits que nos han sobrado en el número hexadecimal que estamos trabajando, como podemos observar no nos ha sobrado ningún bit así que el cálculo será el siguiente:

Exponente = Salto

Base binario $2^0 = 1$ Resultado

Paso 9: Ahora regresamos los bits de binario a notación hexadecimal e identificaremos el número hexadecimal donde se realizara el cambio.

2001:0bd4:0000:0000:0040::/80

Paso 10: Ya que hemos identificado donde será el salto nos dispondremos a construir nuestra tabla de red, para este ejemplo solo colocaremos 4 subredes. La tabla nos quedaría de la siguiente forma:

Nº	Dirección Inicial	Dirección Final
1	2001:0bd4:0:0:0040::/80	2001:0bd4:0:0:0040:FFFF:FFFF:FFFF/80
2	2001:0bd4:0:0:0041::/80	2001:0bd4:0:0:0041:FFFF:FFFF:FFFF/80
3	2001:0bd4:0:0:0042::/80	2001:0bd4:0:0:0042:FFFF:FFFF:FFFF/80
4	2001:0bd4:0:0:0043::/80	2001:0bd4:0:0:0043:FFFF:FFFF:FFFF/80

Paso 11: Siguiendo con el ejercicio ahora tomaremos la segunda subred del cuadro anterior y la cambiaremos de /80 a 82, realizaremos los mimos pasos que hicimos anteriormente, primero identificamos la longitud de partida y la longitud final que se necesita de dirección.

2001:0bd4:0:0:0041::/80 (Dirección de partida)

2001:0bd4:0000:0000:0041:000::/82 (Dirección final)

Si notamos solo necesitamos 2 bits para completar el prefijo de /80 a /82 y esos 2 bits están en el segmento 6.

2001:0bd4:0000:0000:0041: 0000 0000 0000 0000::/80

Paso 12: Ahora nos dispondremos a encontrar el salto, el salto seria la cantidad de bits que nos han sobrado en el número hexadecimal que estamos trabajando.

Exponente = Salto

Base binario $2^2 = 4$ Resultado

Paso 13: Ahora regresamos los bits de binario a notación hexadecimal e identificaremos el número hexadecimal donde se realizara el cambio.

2001:0bd4:0000:0000:0040:0000::/82

Paso 14: Como último paso nos dispondremos a construir nuestra tabla de red, para este ejemplo solo colocaremos 4 subredes. La tabla nos quedaría de la siguiente forma:

Nº	Dirección Inicial	Dirección Final
1	2001:0bd4:0:0:0040:0000::/82	2001:0bd4:0:0:0040:3FFF:FFFF:FFFF/82
2	2001:0bd4:0:0:0041:4000::/82	2001:0bd4:0:0:0041:7FFF:FFFF:FFFF/82
3	2001:0bd4:0:0:0041:8000::/82	2001:0bd4:0:0:0041:bFFF:FFFF:FFFF/82
4	2001:0bd4:0:0:0041:C000::/82	2001:0bd4:0:0:0041:FFFF:FFFF:FFFF/82

Parte:2 practicar con otras direcciones de IPv6, lo anteriormente aprendido!

Práctica # 2: Configuración de interfaces en un Router y computadora con IPv6

Topología de Red

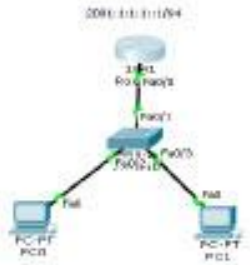


Tabla de enrutamiento

Dispositivos	Interfaces	Direccionamiento/Prefijo	Gateway Predeterminado
R1	F0/0	2001:1:1:1::1/64	N/A
Pc1	F0/1	2001:1:1:1::2/64	2001:1:1:1::1
Pc2	F0/2	2001:1:1:1::3/64	2001:1:1:1::1

Objetivo:

Parte 1. Configuración básica en los equipos

Parte 2. Comprobar la conexión de las interfaces

Paso 1. Abrimos el packet tracer y elegimos los dispositivos a utilizar para armar la red.

Paso 2. Ingresamos al R1 en modo CLI y comenzamos con la configuración ingresamos al modo usuario.

Router>enable

Ingresamos al modo privilegiado

Router1#configure terminal

Cambiamos el nombre del router

Router (config)#hostname R1

Paso 3. Configuramos las interfaces

Habilitamos la configuración para ipv6

R1(config)#ipv6 unicast-routing

Ingresamos a la interface

R1(config)#interface fastEthernet 0/0

Asignamos la dirección ipv6

R1(config-if)#ipv6 address 2001:1:1:1::1/64 eui-64

Encendemos el puerto

R1(config)#no shutdown

-Eui-64 es el identificador de interfaz de IPv6, "identificador único extendido"

Con esa configuración hemos logrado asignarle una dirección IP a la F0/0, con el protocolo versión 6.

Paso 4. Luego vamos a configurar esto en el Router R1

a. Ingresar al router modo usuario

Router>enable

b. Ingresar como modo configuración global

Router# configure terminal

c. añadir banner

Router (config) # banner motd #acceso solo personal autorizado#

d. añadir Contraseña

R1 (config) # enable password cisco

e. añadir Contraseña de linea de control

R1 (config) # line console 0

f. añadir Contraseña de consola

R1 (config-line) # password cisco

g. activar Contraseña

R1 (config-line) # login

h. salir

R1(config-line) # exit

i. añadir contraseña al line vty

R1 (config) # line vty 0 4

j. añadir Contraseña del line vty

R1(config-line) # password cisco

k. activar Contraseña

R1 (config-line) # login

l. salir

R1 (config-line) # exit

m. encriptar contraseñas

R1(config) # service password-encryption

n. añadir Contraseña secreta

R1 (config) # enable secret cisco123

ñ. Salir

R1 (config-if) # Exit

o. Salir

R1 (config) # Exit

p. Guardar

R1 # write

-Con esto hemos configurado mensaje de bienvenida, y las diferentes formas de seguridad para nuestra red, por si alguien quisiera realizar algún cambio sin previa autorización.

Paso 5. Vamos a la Pc0 y colocamos manualmente la IP estática

IP de Pc0: 2001:1:1:1::2/64

Gateway: 2001:1:1:1::1

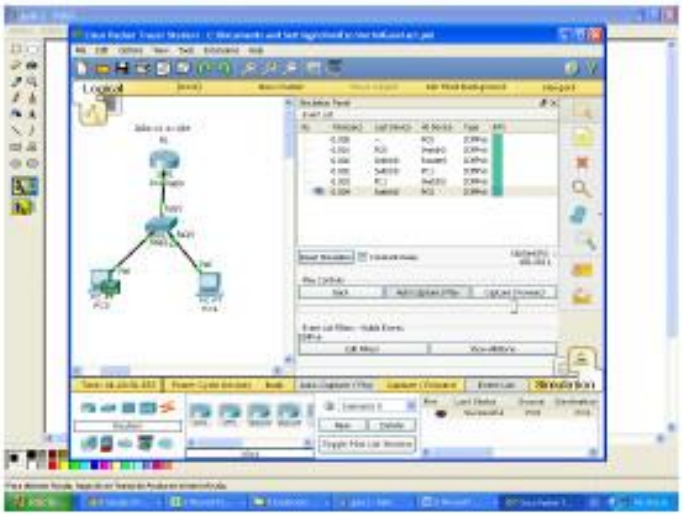
Y en la Pc1 de igual manera colocamos su respectiva IP

IP de Pc1: 2001:1:1:1::3/64

Gateway: 2001:1:1:1::1

Parte 2. Comprobar la conexión de las interfaces

En este punto solo nos resta comprobar las configuraciones mediante Ping o en su defecto enviar un paquete.



Práctica # 3: Configuraciones de Vlan´s con IPv6

Topología de Red

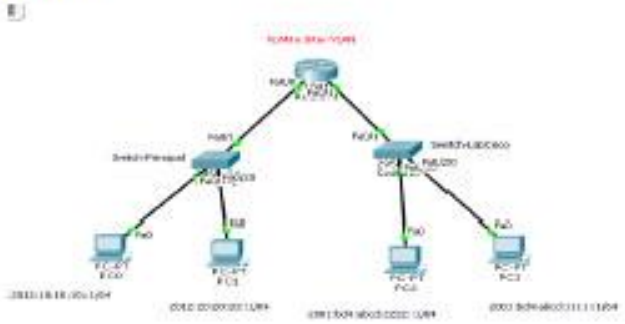


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección/Prefijo	Gateway Predeterminado
RCentral	Fa0/10 Switch Principal	2012:10:10:10::1/64	2012:10:10:10::1
RCentral	Fa0/20 Switch Principal	2012:20:20:20::1/64	2012:20:20:20::1
RCentral	Fa0/10 Switch LabCisco	2001:bd4:abcd:2222::1/64	2001:bd4:abcd:2222::1
RCentral	Fa0/20Switch LabCisco	2001:bd4:abcd:1111::1/64	2001:bd4:abcd:1111::1

Objetivos:

Parte 1. Crear la topología de las VLan´s

Parte 2. Configuración y Comprobación de las VLan´s

Paso 1. Abrimos el packet tracer y elegimos los dispositivos a utilizar

Paso 2. Armar la topología a utilizar y conectar los dispositivos, según el cable que estos requieran.

Ingresamos al Switch "Principal" en modo CLI, damos inicio a la Configuración Vlan´s

Switch Principal

Switch>enable

Ingresamos a modo usuario

Switch#configure terminal

Luego ingresamos en modo privilegiado

Switch(config)#Hostname Principal

Asignamos un nombre al Switch

Paso 3. Creamos las Vlan con los comandos siguientes (dentro del modo de modo privilegiado)

a. Creamos la primera VLan

Principal (config)#vlan 10

b. Luego creamos la segunda VLan

Principal (config-vlan)#vlan 20

c. Entramos a la interface FE 0/10

Principal (config-vlan)#interface fastethernet 0/10

d. Activamos el modo de acceso

Principal (config-if)#switchport mode access

e. Activamos la VLan 10

Principal (config-if)#switchport access vlan 10

f. Luego entramos a la interface FE 0/20

Principal (config-if)#interface fastethernet 0/20

g. Activamos el modo de acceso

Principal (config-if)#switchport mode access

h. Activamos la VLan 20

Principal (config-if)#switchport access vlan 20

i. ingresamos a la interface FE 0/1

Principal (config-if)#interface fastethernet 0/1

j. activamos el modo tunel, este sirve para la comunicación entre VLan's

Principal (config-if)#switchport mode trunk

Paso 5. Creamos las VLan's del siguiente Switch, en este caso son las mismas configuraciones que en el "Switch Principal". De igual manera ingresamos al Switch LabCisco

Switch LabCisco

Switch>enable

Switch#configure terminal

Switch(config)#Hostname LabCisco

Inicia la configuración en LabCisco

a. Creamos la primera VLan

LabCisco (config)#vlan 30

b. Luego creamos la segunda VLan

LabCisco (config-vlan)#vlan 40

c. Entramos a la interface FE 0/10

LabCisco (config-vlan)#interface fastethernet 0/10

d. Activamos el modo de acceso

LabCisco (config-if)#switchport mode access

e. Activamos la VLan 10

LabCisco (config-if)#switchport access vlan 10

f. Luego entramos a la interface FE 0/20

LabCisco (config-if)#interface fastethernet 0/20

g. Activamos el modo de acceso

LabCisco (config-if)#switchport mode access

h. Activamos la VLan 20

LabCisco (config-if)#switchport access vlan 20

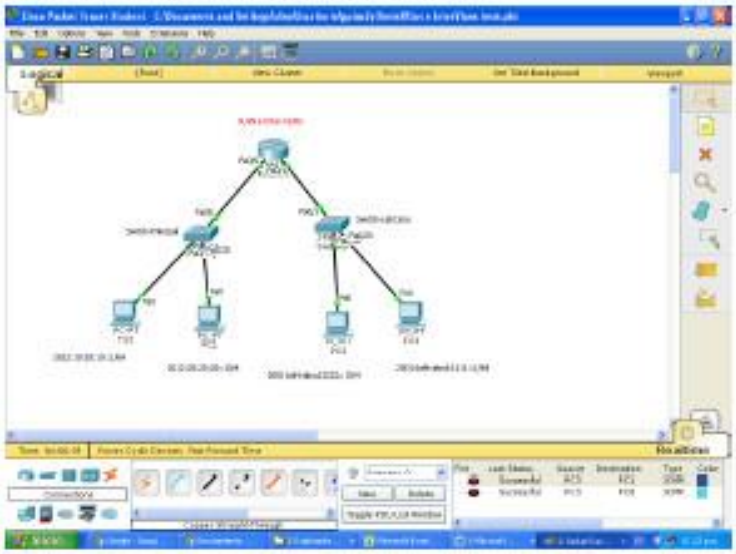
i. ingresamos a la interface FE 0/1

LabCisco (config-if)#interface fastethernet 0/1

j. activamos el modo tunel, este sirve para la comunicación entre VLan´s

LabCisco (config-if)#switchport mode trunk

Parte 2. Configuración y Comprobación de las VLan´s



Paso1. Con este comando podremos ver la asociación de las Vlan´s con los puertos asignados Principal #show vlan / LabCisco#show vlan

Paso2. Verificar las configuraciones de todas las Vlan´s

Práctica # 4: Configuración de Inter-VLAN's

Topología de Red

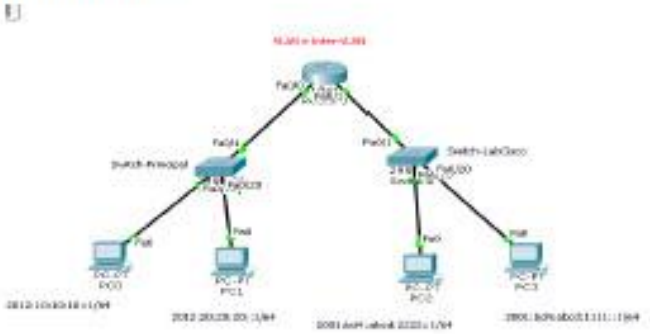


Tabla de enrutamiento

Dispositivo	Interfaz	Dirección/Prefijo	Gateway Predeterminado
RCentral	Fa0/10 Switch Principal	2012:10:10:10::1/64	2012:10:10:10::1
RCentral	Fa0/20 Switch Principal	2012:20:20:20::1/64	2012:20:20:20::1
RCentral	Fa0/10 Switch LabCisco	2001:bd4:abcd:2222::1/64	2001:bd4:abcd:2222::1
RCentral	Fa0/20Switch LabCisco	2001:bd4:abcd:1111::1/64	2001:bd4:abcd:1111::1

Objetivos:

Parte 1. Configuración de Inter-VLan's

Parte 2. Comprobar las configuraciones con ping o también enviando paquetes que vendría a ser lo mismo.

En esta guía prácticamente es la misma topología de la guía 2, puesto que es parte de la configuración total, para que funcionen las Vlan´s y su respectiva conexión (Inter-VLan´s)

Paso 1. Ingresamos al modo CLI del Router Llamado "RCentral". Configurando conexión inter-vlan´s.

Paso 2. Iniciamos las configuraciones en el router, y le cambiamos nombre (RCentral). A la misma vez encendemos el Puerto.

Router>enable

ingresamos al modo usuario

Router#configure terminal

Ingresamos al modo privilegiado

Router(config)#Hostname RCentral

Cambiamos el nombre del Router

RCentral (config)#interface fastethernet 0/0

Ingresamos a la interface

RCentral (config-if)#no shutdown

Encendemos el puerto

RCentral (config-if)#exit

salimos

Paso 3. Ahora creamos una sub interface (asociación de puertos)

Siempre en modo privilegiado

a. ingresamos al la interface y seguido colocamos el puerto a asociar (.10)

RCentral (config)#interface fastethernet 0/0.10

b. ingresamos el comando para asociar el puerto con la VLan

RCentral (config-subif)#encapsulation dot1Q 10

c. salimos

RCentral (config-subif)#exit

d. partimos desde este modo

RCentral (config)#

e. habilitamos la configuracion para IPv6

RCentral (config)#ipv6 unicast-routing

f. Ingresamos a la interface (ya asociada al puerto 10 del Switch)

RCentral (config)#interface fastethernet 0/0.10

g. asignamos la dirección ipv6

RCentral (config-subif)#ipv6 address 2012:10:10:10::1/64

Ya tenemos configurado una parte del router (para la conexión Inter-VLan)

Paso 4. Ahora pasamos al cliente (PC 0), damos click en la viñeta "Desktop" y colocamos una IP estática.

IP de PC0: 2012:10:10:10::2/64

Gateway: 2012:10:10:10::1

Hasta aquí ya debe dar una conexión exitosa.

Paso 5. Hacemos el mismo procedimiento para la otra VLAN

a. ingresamos al la interface y seguido colocamos el puerto a asociar (.20)

RCentral (config)#interface fastethernet 0/0.20

b. ingresamos el comando para asociar el puerto con la VLan

RCentral (config-subif)#encapsulation dot1Q 20

c. salimos

RCentral (config-subif)#exit

d. partimos desde este modo

RCentral (config)#

e. Ingresamos a la interface (ya asociada al puerto 20 del Switch)

RCentral (config)#interface fastethernet 0/0.20

f. asignamos la dirección ipv6

RCentral (config-subif)#ipv6 address 2012:20:20:20::1/64

Ya tenemos configurado la otra parte del router (para la conexion Inter-VLan)

Paso 6. Vamos a la PC1 damos click en la viñeta "Desktop" y colocamos una IP estática.

IP de PC1: 2012:20:20:20::2/64

Gateway : 2012:20:20:20::1

Paso 7. En este paso haremos las mismas configuraciones que en la interface f0/0

RCentral (config)#interface fastethernet 0/1

Ingresamos a la interface

RCentral (config-if)#no shutdown

Encendemos el puerto

RCentral (config-if)#exit

salimos

Paso 8. Ahora creamos una sub interface (asociación de puertos)

Siempre en modo privilegiado

a. ingresamos a la interface y seguido colocamos el puerto a asociar (.10)

RCentral (config)#interface fastethernet 0/1.10

b. ingresamos el comando para asociar el puerto con la VLan

RCentral (config-subif)#encapsulation dot1Q 30

c. salimos

RCentral (config-subif)#exit

d. partimos desde este modo

RCentral (config)#

e. habilitamos la configuración IPv6

RCentral (config)#ipv6 unicast-routing

f. Ingresamos a la interface (ya asociada al puerto 10 del Switch)

RCentral (config)#interface fastethernet 0/1.10

g. asignamos una dirección IPv6

RCentral (config-subif)#ipv6 address 2001:bd4:abcd:2222::1/64

Ahora pasamos al cliente (PC) damos click en la viñeta "Desktop" y colocamos una IP estática.

IP de PC0: 2001:bd4:abcd:2222::2

Gateway: 2001:bd4:abcd:2222::1

Paso 9. Hacemos el mismo procedimiento para la otra VLAN

a. ingresamos a la interface y seguido colocamos el puerto a asociar (.20)

RCentral (config)#interface fastethernet 0/1.20

b. ingresamos el comando para asociar el puerto con la VLan

RCentral (config-subif)#encapsulation dot1Q 40

c. salimos

RCentral (config-subif)#exit

d. partimos desde este modo

RCentral (config)#

e. Ingresamos a la interface (ya asociada al puerto 20 del Switch)

RCentral (config)#interface fastethernet 0/1.20

f. asignamos una dirección IPv6

RCentral (config-subif)#ipv6 address 2001:bd4:abcd:1111::1/64

Vamos a la pc 3 y configuramos de forma manual la ruta estática para la respectiva conexión

IP de PC0: 2001:bd4:abcd:1111::2

Gateway: 2001:bd4:abcd:1111::1

Paso 10. Luego vamos a configurar esto en el Router RCentral

a. Ingresar al router modo usuario

RCentral >enable

b. Ingresar como modo configuración global

RCentral # configure terminal

c. añadir banner

RCentral (config) # banner motd #acceso solo personal autorizado#

d. añadir Contraseña

RCentral (config) # enable password cisco

e. añadir Contraseña de linea de control

RCentral (config) # line console 0

f. añadir Contraseña de consola

RCentral (config-line) # password cisco

g. activar Contraseña

RCentral (config-line) # login

h. salir

RCentral (config-line) # exit

i. añadir contraseña al line vty

RCentral (config) # line vty 0 4

j. añadir Contraseña del line vty

RCentral (config-line) # password cisco

k. activar Contraseña

RCentral (config-line) # login

l. salir

RCentral (config-line) # exit

m. encriptar contraseñas

RCentral (config) # service password-encryption

n. añadir Contraseña secreta

RCentral (config) # enable secret cisco123

ñ. Salir

RCentral (config-if) # Exit

o. Salir

RCentral (config) # Exit

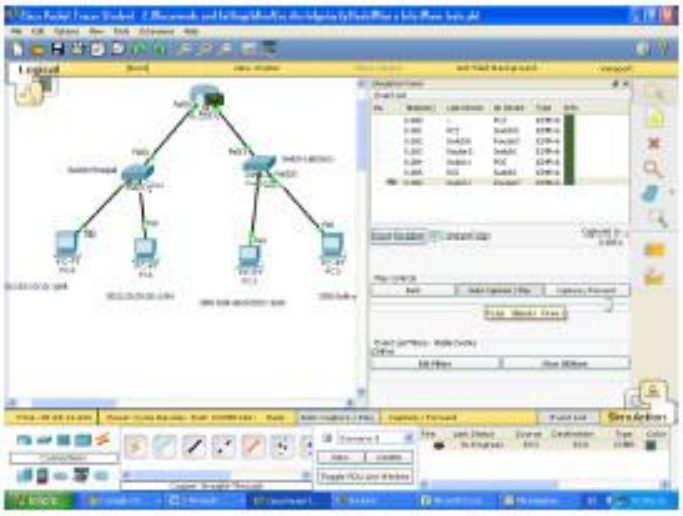
p. Guardar

RCentral # write

-Con esto hemos configurado mensaje de bienvenida, y las diferentes formas de seguridad para nuestra red, por si alguien quisiera realizar algún cambio sin previa autorización.

Parte 2. Comprobar las configuraciones con ping o también enviando paquetes que vendría a ser lo mismo.

¡Hasta este punto ya toda la topología debe dar conexión exitosa!



Práctica # 5: Configuración de rutas estáticas y predeterminadas IPv6

Topología de Red

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IPv6/longitud de prefijo	Gateway predeterminado
ROUTER-A	G0/0	2001:0:0:1::1/64	N/A
	S0/1/0	2001:A:A:A::1/64	N/A
ROUTER-B	G0/0	2001:0:0:2::1/64	N/A
	S0/1/0	2001:A:A:A::2/64	N/A
PC-A	NIC	2001:0:0:1::2/64	2001:0:0:1::1
PC-B	NIC	2001:0:0:2::2/64	2001:0:0:2::1

Objetivo: Aprender a configurar rutas estáticas con IPV6.

Desarrollo:

Parte 1. Armar la topología y configurar los parámetros básicos de los dispositivos

Paso 1. Armar la topología usando 2 routers, 2 switch y 2 PC según como se muestra en la figura de la topología de red.

Paso2. Habilitar el routing de unidifusión IPv6 y configurar el direccionamiento IPv6 en los routers.

a. Acceda a los routers y asígnele el correspondiente nombre.

Eje.

```
Router>enable
Router#configure terminal
Router(config)#hostname ROUTER-A
ROUTER-A(config)#

Router>enable
Router#configure terminal
Router(config)#hostname ROUTER-B
ROUTER-B(config)#
```

b. En el modo de configuración global, habilite el routing IPv6.

Eje.

```
ROUTER-A(config)#ipv6 unicast-routing
ROUTER-B(config)#ipv6 unicast-routing
```

c. Configure las interfaces de red en los routers con direcciones IPv6. Observe que IPv6 está habilitado en cada interfaz

Eje.

```
*ROUTER-A(config)#interface GigabitEthernet 0/0
ROUTER-A(config-if)#ipv6 address 2001:0:0:1::1/64
ROUTER-A(config-if)#no shutdown
ROUTER-A(config)#interface serial 0/1/0
ROUTER-A(config-if)#ipv6 address 2001:A:A:A::1/64
ROUTER-A(config-if)#no shutdown
ROUTER-A(config-if)#exit

*ROUTER-B(config)#interface GigabitEthernet 0/0
ROUTER-B(config-if)#ipv6 address 2001:0:0:2::1/64
ROUTER-B(config-if)#no shutdown
ROUTER-B(config)#interface serial 0/1/0
ROUTER-B(config-if)#ipv6 address 2001:A:A:A::2/64
ROUTER-B(config-if)#clock rate 64000
ROUTER-B(config-if)#no shutdown
ROUTER-B(config-if)#exit
```

Paso 3. Configurar lo siguiente en los router A y B.

```
Router>Enable
Router#Configure terminal
```

```
Router(config)#Line console 0
Router(config-line)#Password cisco
Router(config-line)#Login
Router(config-line)#Exit
Router(config)#Enable password cisco123
Router(config)#Enable secret cisco123
Router(config)#Line vty 0 4
Router(config-line)#Password cisco
Router(config-line)#Login
Router(config-line)#exit
Router(config)#service password-encryption
Router(config)#banner motd #Welcome Authorized Users UTEC!#
Router(config)#exit
Router# copy running-config startup-config
```

Paso 4. Configurar el direccionamiento IPv6 para las interfaces de red de las computadoras.

a. En la PC-A y la PC-B, navegue hasta el menú Inicio > Desktop. Haga clic en el enlace IP Configuration en la vista por íconos.

b. Configure dirección IPv6 y Gateway, según el direccionamiento proporcionado.

Parte 2. Configurar rutas estáticas y predeterminadas IPv6.

Ruta estática IPv6 conectada directamente: una ruta estática conectada directamente se crea al especificar la interfaz de salida.

Paso 1. Configurar una ruta estática IPv6 conectada directamente.

En una ruta estática IPv6 conectada directamente, la entrada de ruta especifica la interfaz de salida del router. En general, una ruta estática conectada directamente se utiliza con una interfaz serial punto a punto. Para configurar una ruta estática IPv6 conectada directamente, utilice el siguiente formato de comando: Router(config)# ipv6 route <ipv6-prefix/prefix-length> <outgoing-interface-type> <outgoing-interface-number>

a. En el router ROUTER-A, configure una ruta estática IPv6 mediante la interfaz de salida S0/1/0 del Router.

   Eje.

   ROUTER-A(config)# ipv6 route 2001:0:0:2::/64 Serial0/1/0

b. En el router ROUTER-B, configure una ruta estática IPv6 mediante la interfaz de salida S0/1/0 del Router.

   Eje.

   ROUTER-B(config)# ipv6 route 2001:0:0:1::/64 Serial0/1/0

Ahora que ambos routers tienen rutas estáticas, intente hacer ping de IPv6 desde la PC-A hasta la dirección IPv6 de unidifusión global de la PC-B.

Práctica # 6: Configuración de RIPng

Topología de Red

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección/Prefijo IPv6	Gateway Predeterminado
Router_A	G0/1	2001::1:0:0:0:1/64	N/A
	S0/0/0	2001:A:A:A::1/64	N/A
Router_B	G0/0	2001::2:0:0:0:1/64	N/A
	S0/0/0	2001:A:A:A::2/64	N/A
	S0/0/1	2001:B:A:A::1/64	N/A
Router_C	G0/0	2001::3:0:0:0:1/64	N/A
	S0/0/1	2001:B:A:A::2/64	N/A
PC1	NIC	2001:0:0:1::2	2001:0:0:1::1
PC2	NIC	2001:0:0:2::2	2001:0:0:2::1
PC3	NIC	2001:0:0:3::2	2001:0:0:3::1

Objetivos

Parte 1: configurar RIPng

Parte 2: verificar las configuraciones y la conectividad

Información básica:

RIP de última generación (RIPng) es un protocolo de routing vector distancia para enrutar direcciones IPv6. RIPng se basa en RIPv2 y tiene la misma distancia administrativa y limitación de 15 saltos. Esta actividad lo ayudará a familiarizarse con RIPng.

Parte 1: Armar la topología y configurar las interfaces de los Routers

Paso 1: Armar la topología usando 3 routers, 3 switch y 3 PC según como se muestra en la figura de topología de red.

Paso 2: Asignar un nombre y habilitar el routing IPv6 en cada uno de los routers.

Eje. Router_A

```
Router>Enable
Router#Configure terminal
Router(config)#Hostname Router_A
Router_A(config)# ipv6 unicast-routing
```

Paso 3: Configurar las direcciones IP.

```
Router-A(config)#interface serial 0/0/0
Router-A(config-if)#ipv6 address 2001:A:A:A::1/64
Router-A(config-if)#clock rate 64000
Router-A(config-if)#interface GigabitEthernet 0/1
Router-A(config-if)#ipv6 address 2001::1:0:0:0:1/64
```

```
Router-A(config-if)#no shutdown
Router-B(config)#interface serial 0/0/0
Router-B(config-if)#ipv6 address 2001:A:A:A::2/64
Router-B(config-if)#interface serial 0/0/1
Router-B(config-if)#ipv6 address 2001:B:A:A::1/64
Router-B(config-if)#clock rate 64000
Router-B(config-if)#interface GigabitEthernet 0/0
Router-B(config-if)#ipv6 address 2001::2:0:0:0:1/64
Router-B(config-if)#no shutdown
Router-C(config)#interface serial 0/0/1
Router-C(config-if)#ipv6 address 2001:B:A:A::2/64
Router-C(config-if)#interface GigabitEthernet 0/0
Router-C(config-if)#ipv6 address 2001::3:0:0:0:1/64
Router-C(config-if)#no shutdown
```

Paso 4: Configurar los siguientes comandos en los routers.

```
Router>Enable
Router#Configure terminal
Router(config)#Line console 0
Router(config-line)#Password cisco
Router(config-line)#Login
Router(config-line)#Exit
Router(config)#Enable password cisco123
```

```
Router(config)#Enable secret cisco123
Router(config)#Line vty 0 4
Router(config-line)#Password cisco
Router(config-line)#Login
Router(config-line)#exit
Router(config)#service password-encryption
Router(config)#banner motd #Welcome Authorized Users UTEC!#
Router(config)#exit
Router# copy running-config startup-config
```

Paso 5: Configurar las direcciones IP en la diferentes PCs, según la tabla de direccionamiento.

Paso 6: configurar RIPng en el Router_A.

a. Ingrese al modo de configuración del protocolo RIPng.

```
Router_A(config)#ipv6 router rip CISCO
```

b. Habilite RIPng para las redes que se conectan al Router_A.

```
Router_A(config-rtr)#interface GigabitEthernet 0/1
Router_A(config-if)#ipv6 rip CISCO enable
Router_A(config-if)#interface serial 0/0/0
Router_A(config-if)#ipv6 rip CISCO enable
```

c. Guarde la configuración.

Paso 7: configurar RIPng en el Router_B y el Router_C.

Repita los pasos 5a hasta 5c en el Router_B y el Router_C.

Parte 2: verificar las configuraciones y la conectividad

Paso 1: ver las tablas de routing de Router_A, Router_B y Router_C.

a. Utilice el comando adecuado para ver la tabla de routing de los routers. RIPng (R) ahora aparece con rutas conectadas (C) y rutas locales (L) en la tabla de routing. Todas las redes tienen una entrada.

b. Verifique que las interfaces adecuadas utilicen RIPng.

Router# show ipv6 route

Router# show ipv6 protocols

Paso 2: verificar la plena conectividad.

Ahora todos los dispositivos deberían poder hacer ping a todos los demás dispositivos. De lo contrario, revise las configuraciones para detectar errores e implemente las soluciones adecuadas.

Práctica # 7: Configuración de OSPFv3 básico en un área única

Topología de Red

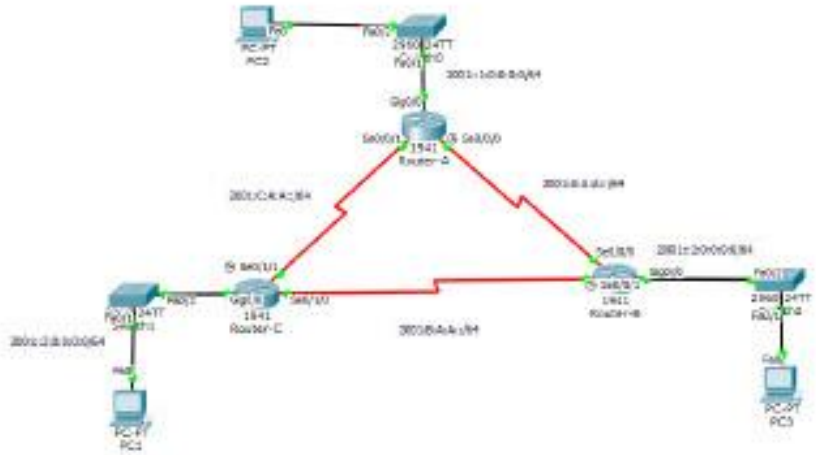


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección/Prefijo IPv6	Gateway predeterminado
Router-A	G0/0	2001::1:0:0:0:1/64	N/A
	S0/0/0	2001:A:A:A::1/64	N/A
	S0/0/1	2001:C:A:A::1/64	N/A
Router-B	G0/0	2001::2:0:0:0:1/64	N/A
	S0/0/0	2001:A:A:A::2/64	N/A
	S0/0/1	2001:B:A:A::1/64	N/A
Router-C	G0/0	2001::3:0:0:0:1/64	N/A
	S0/1/0	2001:B:A:A::2/64	N/A
	S0/1/1	2001:C:A:A::2/64	N/A
PC1	NIC	2001:0:0:3::2/64	2001:0:0:3::1
PC2	NIC	2001:0:0:1::2/64	2001:0:0:1::1
PC3	NIC	2001:0:0:2::2/64	2001:0:0:2::1

Objetivos

Parte 1: Configurar el routing OSPFv3

Parte 2: verificar la conectividad.

Información básica:

El uso de OSPFv3 multiárea en la implementación de redes IPv6 grandes puede reducir el procesamiento del router mediante la creación de tablas de routing más pequeñas y menos requisitos de sobrecarga de memoria.

Parte 1: Armar la topología propuesta y configurar el routing OSPFv3

Paso 1: Armar la topología usando 3 routers, 3 switch y 3 PC según como se muestra en la figura de la topología de red.

Paso 2: Asignar un nombre y habilitar el routing IPv6 en cada uno de los routers.

Eje. Router-A

```
Router>Enable
Router#Configure terminal
Router(config)#Hostname Router-A
Router-A(config)# ipv6 unicast-routing
```

Paso 3: configurar las interfaces de los Router (A, B y C) siguiendo las tabla de direccionamiento.

Eje. (Router-A)

```
Router-A(config)#interface serial 0/0/1
Router-A(config-if)#ipv6 address 2001:C:A:A::1/64
Router-A(config-if)#no shutdown
Router-A(config-if)#int serial 0/0/0
```

```
Router-A(config-if)#ipv6 address 2001:A:A:A::1/64
Router-A(config-if)#clock rate 64000
Router-A(config-if)#no shutdown
Router-A(config-if)#int gigabitEthernet 0/0
Router-A(config-if)#ipv6 address 2001::1:0:0:0:1/64
Router-A(config-if)#no shutdown
```

Paso 4: Configurar lo siguiente en los 3 Routers.

```
Router>Enable
Router#Configure terminal
Router(config)#Line console 0
Router(config-line)#Password cisco
Router(config-line)#Login
Router(config-line)#Exit
Router(config)#Enable password cisco123
Router(config)#Enable secret cisco123
Router(config)#Line vty 0 4
Router(config-line)#Password cisco
Router(config-line)#Login
Router(config-line)#exit
Router(config)#service password-encryption
Router(config)#banner motd #Welcome Authorized Users UTEC!#
Router(config)#exit
```

Router# copy running-config startup-config

Paso 5. Configurar OSPFv3 en Router-A, Router-B y Router-C.

Utilice los siguientes requisitos para configurar el routing OSPF en los tres routers:

-Habilitación del routing IPv6

-ID de proceso 10

-ID del router para cada router: Router-A= 1.1.1.1; Router-B= 2.2.2.2; Router-C= 3.3.3.3

-Habilitación de OSPFv3 en cada interfaz

Eje.

```
Router(config)#ipv6 router ospf 10
Router(config-rtr)#router-id 3.3.3.3
Router(config-rtr)#exit
Router(config)#interface serial 0/1/1
Router(config-if)#ipv6 ospf 10 area 0
Router(config-if)#interface serial 0/1/0
Router(config-if)#ipv6 ospf 10 area 0
Router(config-if)#interface gigabitEthernet 0/0
Router(config-if)#ipv6 ospf 10 area 0
```

Paso 6. Configurar el direccionamiento IPv6 para las interfaces de red de las computadoras.

a. Navegue hasta el menú Inicio > Desktop. Haga clic en el enlace IP Configuration en la vista por íconos.

b. Configure dirección IPv6 y Gateway, según el direccionamiento proporcionado.

Paso 7: verificar que el routing OSPF funcione.

Verifique que todos los routers hayan establecido adyacencia con los otros dos routers. Verifique que en la tabla de routing haya una ruta a cada red de la topología, mediante los siguientes protocolos:

Show ipv6 protocols: este comando se utiliza para verificar información fundamental de configuración de OSPFv3, incluidas la ID del proceso OSPFv3, la ID del router y las interfaces de las que el router recibe actualizaciones.

Show ipv6 ospf neighbor: se usa para verificar que el router formó una adyacencia con los routers vecinos. Este resultado muestra la ID del router vecino, la prioridad del vecino, el estado de OSPFv3, el temporizador de tiempo muerto, la ID de la interfaz vecina y la interfaz mediante la cual se puede acceder al vecino. Si no se muestra la ID del router vecino o este no se muestra en el estado FULL o 2WAY, los dos routers no formaron una adyacencia OSPFv3. Si dos routers no establecieron adyacencia, no se intercambiará la información de link-state. Las bases de datos de link-state incompletas pueden crear árboles SPF y tablas de enrutamiento imprecisos. Es posible que no existan rutas hacia las redes de destino o que estas no constituyan las mejores rutas.

Show ipv6 ospf interface: se usa para mostrar los parámetros de OSPFv3 que se configuraron en una interfaz, como la ID del proceso OSPFv3 a la que se asignó la interfaz, el área en la que están las interfaces, el costo de la interfaz y los intervalos de saludo y muerto. Si se agrega el nombre y el número de interfaz al comando, se muestra el resultado para una interfaz específica.

Show ipv6 ospf: se usa para examinar la ID del proceso OSPF y la ID del router, así como la información sobre las transmisiones de LSA.

Show ipv6 route ospf: se utiliza para mostrar solo las rutas OSPFv3 descubiertas en la tabla de routing. El resultado muestra que el R1 descubrió alrededor de cuatro redes remotas mediante OSPFv3.

Clear ipv6 ospf [id-proceso] process: se usa para restablecer las adyacencias de vecinos OSPFv3.

Parte 2: Verificar la conectividad en la topología de red.

Cada computadora debe poder hacer ping a las otras dos computadoras. De lo contrario, revise las configuraciones.

Práctica # 8: Configuración de DHCP con IPv6

Topología de red

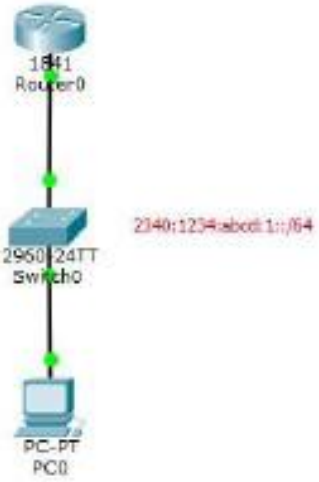


Tabla de direccionamiento

Dispositiv	Interfaz	Dirección/Prefijo	Gateway predetermina
Router	Fa0/0	2340:1234:abcd:1::1/64	
Pc0	NIC	DHCP	DCHP

Objetivos

Parte 1: construcción de la topología y configuración básica

Parte 2: configurar, aplicar y verificar DHCP con IPv6

Paso 1: Armar la topologia

Armamos la topología de un router cisco 1841, un switch cisco 2960 y una pc genérica

Paso 2: Configurar básica de router

a. Ingresar al router modo global
   Router>**enable**

b. Ingresar como modo configuración global
   Router# **configure terminal**

c. añadir nombre al router
   Router (config) # **hostname Utec**

d. añadir banner
   Router (config) # **banner motd #acceso solo personal autorizado#**

e. añadir Contraseña
   Utec (config) # **enable password cisco**

f. añadir Contraseña de linea de control
   Utec (config) # **line console 0**

g. añadir Contraseña de consola
   Utec (config-line) # **password cisco**

h. activar Contraseña
   Utec (config-line) # **login**

i. salir
   Utec (config-line) # **exit**

j. añadir contraseña al line vty
   Utec (config) # **line vty 0 4**

k. añadir Contraseña del line vty
   Utec (config-line) # **password cisco**

l. activar Contraseña
   Utec (config-line) # **login**

m. salir
   Utec (config-line) # **exit**

n. encriptar contraseñas
   Utec (config) # **service password-encryption**

o. añadir Contraseña secreta
Utec (config) # **enable secret cisco123**

p. Salir
Utec (config) # **Exit**

q. Guardar
Utec # **write**

Parte 2: Configurar DHCP y verificar asignación de IPv6

Paso 1: Configurar DHCP con IPv6 en Router0

Entrar a router0 y configurar el router

a. Ingresar a modo de configuración global
Utec # **configure terminal**

b. Activar direccionamiento ipv6
Utec (config) **#ipv6 unicast-routing**

c. Ingresar la entra para empezar la configuracion DHCPv6 con nombre
Utec (config) # **ipv6 dhcp pool cisco**

d. salir
Utec (config-dhcp)**#exit**

e. ingresamos la dirección de red la cual el router empezara a brindar ipv6
Utec (config)**#ipv6 general-prefix cisco 2340:1234:abcd:1::/64**

f. ingresaremos el rango de ipv6 que dara
Utec (config)**#ipv6 local pool cisco 2340:1234:abcd:1::/40 64**

g. Ingresar a la interfaz que llevara el protocol
Utec (config)**#interface FastEthernet0/0**

h. Asignar ipv6 al Puerto
Utec (config-if)**#ipv6 address 2340:1234:abcd:1::1/64**

i. Ensender el Puerto
Utec (config-if)**#no shutdown**

j. Ingresar la entrada que le de la orden de administrar el DHCP
FMUtec (config-if)**#ipv6 dhcp server cisco**

k. salir
Utec (config-if)**#exit**

l. validar configuración con la entrada Show ipv6 route
Utec (config)**#do show ipv6 route**

```
IPv6 Routing Table - 3 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
C 2340:1234:ABCD:1::/64 [0/0]
       via ::, FastEthernet0/0
L 2340:1234:ABCD:1::1/128 [0/0]
       via ::, FastEthernet0/0
L FF00::/8 [0/0]
       via ::, Null0

Utec (config)#
```

Paso 2: comprobar DCHPv6 en Pc0

Práctica # 9: Configuración de TFTP con IPv6

Topología de Red

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección/Prefijo IPv6	Gateway predeterminado
BJUtec	F0/0	2001:DB8:1:1::1	N/A
ServerUtec	Fa0	2001:DB8:1:1::2	2001:DB8:1:1::1

Objetivos

Parte 1: configurar y aplicar TFTP con Ipv6

Parte 2: Comprobar servicio de tftp

Información básica/situación. Puede crearse copias de seguridad con el servicio de TFTP para almacenar pequeños archivos entre ordenadores en una red como pueden ser IOS o configuraciones.

Práctica de laboratorio: configuración y verificación de TFTP de IPv6. Este documento es información pública de la Universidad Tecnológica de El Salvador.

Nota: asegúrese de que los routers y los switches se hayan borrado y no tengan configuraciones de inicio. Si no está seguro, consulte con el instructor.

Recursos necesarios

- 1 router (Cisco 1841)
- 1 switch (Cisco 2960)

- 1 Servidor (genérico)
- Cables de UTP para configurar los dispositivos.

Parte 1: configurar y aplicar TFTP con IPv6

Paso 1: Montar la topología

Armamos la topología de un router cisco 1841, un switch cisco 2960 y un servidor genérico.

Paso 2: Configurar servidor añadiendo IPv6.

Vamos a el servidor e ingresamos a la opciónDesktop y seleccionamos la opción de IP configuration.

Al estar ahí ingresar la IPv6 2001:DB8:1:1::2/64 poniendo en el IPv6 Gateway la IPv6 de nuestro Router 2001:DB8:1:1::1

Paso 3: Configurar Router con Direccion Ipv6

a. Ingresar al router modo global
Router>**enable**

b. Ingresar como modo configuración global
Router# **configure terminal**

c. añadir nombre al router
Router (config) # **hostname BJUtec**

d. añadir banner
Router (config) # **banner motd #acceso solo personal autorizado#**

e. añadir Contraseña
BJUtec (config) # **enable password cisco**

f. añadir Contraseña de linea de control
BJUtec (config) # **line console 0**

g. añadir Contraseña de consola
BJUtec (config-line) # **password cisco**

h. activar Contraseña
BJUtec (config-line) # **login**

i. salir
BJUtec (config-line) # **exit**

j. añadir contraseña al line vty
BJUtec (config) # **line vty 0 4**

k. añadir Contraseña del line vty
BJUtec (config-line) # **password cisco**

l. activar Contraseña
BJUtec (config-line) # **login**

m. salir
BJUtec (config-line) # **exit**

n. encriptar contraseñas
BJUtec (config) # **service password-encryption**

o. añadir Contraseña secreta
BJUtec (config) # **enable secret cisco123**

p. Ingresar el comando para IPv6
BJUtec (config) # **Ipv6 unicast-routing**

q. Ingresar a la interface Ethernet0/0
BJUtec (config) # **interface Fastethernet0/0**

r. Colocar la IPv6
BJUtec (config-if) # **ipv6 add 2001:DB8:1:1::1/64**

s. Encender el puerto
BJUtec (config-if) # **No Shutdown**

t. Salir
BJUtec (config-if) # **Exit**

u. Salir
BJUtec (config) # **Exit**

v. Guardar
BJUtec # **write**

Parte 2: Comprobar servicio de tftp

Paso 1: hacer una copia de respaldo de Runing-config

a. En el router BJUtec hacemos los siguiente
BJUtec # **copy running-config tftp**

El sistema preguntara en ingles cual es el nombre o dirección IPv6 a la cual nos conectaremos: Address or name of remote host [ ]?

b. Ingresamos la dirección IPv6 de el servidor, ServerUtec **2001:DB8:1:1::2**

El sistema preguntara en ingles como se llamara nuestro archivo: Destination filename [BJUtec-config]?

c. Añadimos el nombre que deseamos con fecha actual **router01-config-20151226.bak**

El sistema una ves termine la copia nos arrojara un texto siguiente:

Writing running-config...!!

[OK - 574 bytes]

d. Verificamos en el servidor ServerUtec / Services / tftp / si esta nuestro archivo **router01-config-20151226.bak**

Práctica # 10: Configuración y verificación de ACL estándar con IPv6

Topología de Red

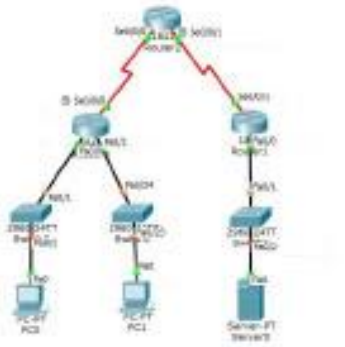


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Gateway predeterminado
Router0	FA0/0	2001:db8:1:10::1/64	N/A
	FA0/1	2001:db8:1:11::1/64	N/A
	S0/0/0 (DCE)	2001:db8:1:12::1/64	N/A
Router2	S0/0/0	2001:db8:1:12::2/64	N/A
	S0/0/1 (DCE)	2001:db8:1:13::1/64	N/A
Router1	S0/0/1	2001:db8:1:13::2/64	N/A
	FA0/0	2001:db8:1:30::1/64	N/A
PC-0	NIC	2001:db8:1:10::2/64	2001:db8:1:10::1
PC-1	NIC	2001:db8:1:11::2/64	2001:db8:1:11::1
Server0	NIC	2001:db8:1:30::2/64	2001:db8:1:30::1

Objetivos

Parte 1: establecer la topología e inicializar los dispositivos

Parte 2: configurar los dispositivos y verificar la conectividad

Parte 3: configurar y verificar las ACL de IPv6

Información básica/situación

Puede filtrar el tráfico IPv6 mediante la creación de listas de control de acceso (ACL) de IPv6 y su aplicación a las interfaces. El tipo de ACL de IPv6 son estandar.

En esta práctica de laboratorio, aplicará reglas de filtrado IPv6 y luego verificará que restrinjan el acceso según lo esperado.

Nota: los routers que se utilizan en las práctica son routers de servicios integrados (ISR) Cisco 1841 con IOS de Cisco versión 15.2(4)M3 (imagen universalk9). Los switches que se utilizan son Cisco Catalyst 2960s con IOS de Cisco versión 15.0(2) (imagen de lanbasek9). PCs de escritorios genéricas. Servidor Generico. Se pueden utilizar otros routers, switches y otras versiones del IOS de Cisco. Según el modelo y la versión de IOS de Cisco, los comandos disponibles y los resultados que se obtienen pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces del router que se encuentra al comienzo de la práctica de laboratorio para obtener los identificadores de interfaz correctos.

Nota: asegúrese de que los routers y los switches se hayan borrado y no tengan configuraciones de inicio. Si no está seguro, consulte con el instructor.

Recursos necesarios

- 3 routers (Cisco 1841 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)
- 3 switches (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o similar)
- 3 computadoras genéricas de escritorio
- Servidor Generico
- Cables Ethernet y seriales, como se muestra en la topología

Parte 1: establecer la topología e inicializar los dispositivos

En la parte 1, establecerá la topología de la red y borrará cualquier configuración, en caso de ser necesario.

Paso 1: realizar el cableado de red tal como se

muestra en la topología.

Paso 2: inicializar y volver a cargar los routers y

los switches.

Parte 2: Configurar dispositivos y verificar la conectividad

En la parte 2, configurará los parámetros básicos en los routers y las computadoras. Consulte la topología y la tabla de direccionamiento incluidos al comienzo de esta práctica de laboratorio para conocer los nombres de los dispositivos y obtener información de direcciones.

Paso 1: configurar direcciones IPv6 en todas las computadoras.

a. Ingresar a las PCs para darles las direcciones IPv6 con su gateway según la tabla de direccionamiento

Paso 2: ingrese a cada router y realice las configuraciones básicas en cada uno

(cada router se le asignara las siguientes entradas de configuracion. Los nombres de los routers son Router0: **SBUtec**, router2: **BJUtec** y router1 **FMUtec**)

a. Ingresar al router modo global
Router>**enable**

b. Ingresar como modo configuración global
Router# **configure terminal**

c. añadir nombre al router
Router (config) # **hostname BJUtec**

d. añadir banner
Router (config) # **banner motd #acceso solo personal autorizado#**

e. añadir Contraseña
BJUtec (config) # **enable password cisco**

f. añadir Contraseña de linea de control
BJUtec (config) # **line console 0**

g. añadir Contraseña de consola
BJUtec (config-line) # **password cisco**

h. activar Contraseña
BJUtec (config-line) # **login**

i. salir
BJUtec (config-line) # **exit**

j. añadir contraseña al line vty
BJUtec (config) # **line vty 0 4**

k. añadir Contraseña del line vty
BJUtec (config-line) # **password cisco**

l. activar Contraseña
BJUtec (config-line) # **login**

m. salir
BJUtec (config-line) # **exit**

n. encriptar contraseñas
BJUtec (config) # **service password-encryption**

o. añadir Contraseña secreta
BJUtec (config) # **enable secret cisco123**

p. Activar IPv6
BJUtec (config) # **ipv6 unicast-routing**

q. Salir
BJUtec (config) # **Exit**

r. Guardar
BJUtec # **write**

Se realizara el proceso en cada router según la topología y cuadro de direccionamiento.

Paso 3: añadir IPv6 en cada puerto

a) entre a la fasthethernet a configurar
SBUtec (config)**#interface fastethernet 0/0**

b) añadir la IPv6
SBUtec (config-if)**#IPv6 address 2001:db8:1:10::1/64**

c) encender el Puerto
SBUtec (config-if)**#no shutdown**

d) salir
SBUtec (config-if)**#exit**

Realizar el proceso en cada Puerto de los routers según la tabla de direccionamiento

Paso 4: Configurar enrutamiento en cada Router

configurar RIPng en el BJUtec

a. Ingrese al modo de configuración del protocolo RIPng.
BJUtec(config)**#ipv6 router rip CISCO**

Habilite RIPng para las redes que se conectan al BJUtec.

b. Ingresar a la interfaz Ethernet 0/0
BJUtec (config-if)**#interface fastethernet0/0**

c. Añadir commando ipv6 rip
BJUtec (config-if)**#ipv6 rip CISCO enable**

d. Ingresar a la interfaz Ethernet 0/1
BJUtec (config-if)**#interface fastethernet0/1**

e. Añadir commando ipv6 rip
BJUtec (config-if)**#ipv6 rip CISCO enable**

f. Ingresar a la interfaz serial 0/0/0
BJUtec (config-if)**# interface serial0/0/0**

g. Añadir commando ipv6 rip
BJUtec (config-if)**#ipv6 rip CISCO enable**

h. salir
BJUtec (config-if)**#exit**

i. salir
BJUtec (config)**#exit**

j. guardar
BJUtec **#write**

Paso 5: configurar RIPng en los routers SBUtec y FMUtec

Repita el paso 3 en cada router

Paso 6: Verificar conectividad

a. Mandar paquetes desde PC0 hasta servidor

b. Mandar paquetes desde PC1 hasta servidor

Parte 3: configurar, aplicar y verificar ACL estándar con IPv6

Paso 1: Ingresar a Router1 (FMUtec) para aplicar la ACL Estándar

Router que esta conectado a el servidor

a. Ingresar al router modo global
Router>**enable**

b. Ingresar como modo configuración global
Router# **configure terminal**

c. Ingresar el nombre de la ACL
Router (config)**#ipv6 access-list BLOCK_ICMP**

d. Bloquear icmp
Router (config-ipv6-acl)**# deny icmp any any**

e. Permitir otros hagan icmp
Router (config-ipv6-acl)**# permit ipv6 any any**

f. Salir
Router (config-ipv6-acl)**#exit**

Paso 2: Implementar la ACL a la correcta interfaz

En este caso, el trafico de ICMP podrá venir de cualquier origen. Asegurese que el trafico ICMP este bloqueado. Aplique la ACL mas cerca del destino

a. Ingresar a la interfaz fastethernet 0/0
Router (config)**#interface fastehternet 0/0**

b. Añadir la el trafico de la ACL creada
Router (config-if)**#Ipv6 Traffic-filter BLOCK_ICMP out**

c. Salir
Router (config-if)**#exit**

Paso 2: verificar Implementacion de ACL

- Realizar ping desde PC0 a la 2001:db8:1:30::2 el cual fallará
- Realizar ping desde PC1 a la 2001:db8:1:30::2 el cual fallará
- Abrir el navegador web de la PC1 a la dirección http:// 2001:db8:1:30::30 or https:// 2001:db8:1:30::30 el cual deberá mostrar conexión.

Práctica # 11: Configuración de ACL extendida con IPv6

Topología de Red

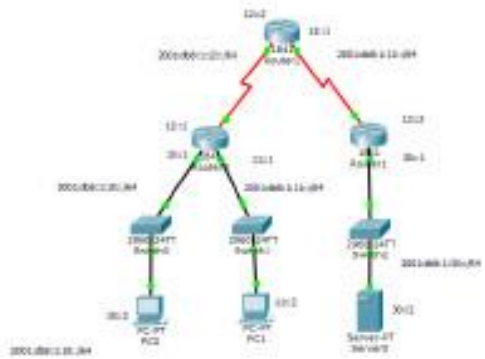


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección/Prefijo IPv6	Gateway predeterminado
Server	NIC	2001:DB8:1:30::30/64	2001:DB8:1:30::1
Router 1	Fa0/0	2001:DB8:1:30::1/64	N/A
Router 1	S0/0/1	2001:DB8:1:13::2/64	N/A
Router 2	S0/0/1	2001:DB8:1:13::1/64	N/A
Router 2	S0/0/0	2001:DB8:1:12::2/64	N/A
Router 0	S0/0/0	2001:DB8:1:12::1/64	N/A
Router 0	Fa0/0	2001:DB8:1:10::1/64	N/A
Router 0	Fa0/1	2001:DB8:1:11::1/64	N/A
PC0	Fa0	2001:DB8:1:10::2/64	2001:DB8:1:10::1
PC1	Fa0	2001:DB8:1:11::2/64	2001:DB8:1:11::1

Objetivos

Parte 1: Instalar y configurar equipos según topologia

Parte 2: configurar, aplicar y verificar una segunda ACL de IPv6

Parte 1: Instalar y configurar equipos según topología

Paso 1: armar topologia con sus correspondientes cables

a. Armar la topología de 3 routers cisco 1841 conectados con cables seriales

b. Añadir 3 switches cisco 2960 conectados con cables utp straight-through a cada router según topología

c. Añadir 3 pcs de escritorio genéricas y conectar con cables utp straight-through

Paso 2: Asignar IPv6 a server y pcs en sus puertos correspondientes según topología, Agregar configuración.

Asigne cada IPv6 a cada puerto según la tabla de direccionamiento a las pc y server

En cada router ingresar configuraciones básicas en los routers

(cada router se le asignara las siguientes entradas de configuracion. Los nombres de los routers son Router0: **SBUtec**, router2: **BJUtec** y router1 **FMUtec**)

a. Ingresar al router modo global
   Router>**enable**

b. Ingresar como modo configuración global
   Router# **configure terminal**

c. añadir nombre al router
Router (config) # **hostname BJUtec**

d. añadir banner
Router (config) # **banner motd #acceso solo personal autorizado#**

e. añadir Contraseña
BJUtec (config) # **enable password cisco**

f. añadir Contraseña de linea de control
BJUtec (config) # **line console 0**

g. añadir Contraseña de consola
BJUtec (config-line) # **password cisco**

h. activar Contraseña
BJUtec (config-line) # **login**

i. salir
BJUtec (config-line) # **exit**

j. añadir contraseña al line vty
BJUtec (config) # **line vty 0 4**

k. añadir Contraseña del line vty
BJUtec (config-line) # **password cisco**

l. activar Contraseña
BJUtec (config-line) # **login**

m. salir
BJUtec (config-line) # **exit**

n. encriptar contraseñas
BJUtec (config) # **service password-encryption**

o. añadir Contraseña secreta
BJUtec (config) # **enable secret cisco123**

p. Salir
BJUtec (config) # **Exit**

q. Activar ipv6 unicast-routing
BJUtec (config) # **ipv6 unicast-routing**

r. Guardar
BJUtec # **write**

Se realizara el proceso en cada router segun la topologia y cuadro de direccionamiento.

Paso 3: añadir IPv6 en cada puerto

a) entre a la fasthethernet a configurar
SBUtec (config)**#interface fastethernet 0/0**

b) añadir la IPv6
SBUtec (config-if)**#IPv6 address 2001:db8:1:10::1/64**

c) encender el Puerto
SBUtec (config-if)**#no shutdown**

d) salir
SBUtec (config-if)**#exit**

Realizar el proceso en cada Puerto de los routers segun la tabla de direccionamiento

Paso 4: Configurar enrutamiento en cada Router

configurar RIPng en el BJUtec

a. Ingrese al modo de configuración del protocolo RIPng.
BJUtec(config)#ipv6 router rip CISCO

Habilite RIPng para las redes que se conectan al BJUtec.

b. Ingresar a la interfaz Ethernet 0/0
BJUtec (config-rtr)#interface fastethernet0/0

c. Añadir commando ipv6 rip
BJUtec (config-if)#ipv6 rip CISCO enable

d. Ingresar a la interfaz Ethernet 0/1
BJUtec (config-if)#interface fastethernet0/1

e. Añadir commando ipv6 rip
BJUtec (config-if)#ipv6 rip CISCO enable

f. Ingresar a la interfaz serial 0/0/0
BJUtec (config-if)# interface serial0/0/0

g. Añadir commando ipv6 rip
BJUtec (config-if)#ipv6 rip CISCO enable

h. salir
BJUtec (config-if)#exit

i. salir
BJUtec (config)#exit

j. guardar
BJUtec #write

Paso 5: configurar RIPng en los routers SBUtec y FMUtec

Repita el paso 3 en cada router

Paso 6: Verificar conectividad

a. Mandar paquetes desde PC0 hasta servidor

b. Mandar paquetes desde PC1 hasta servidor

Parte 2: configurar, aplicar y verificar una segunda ACL de IPv6

Paso 1 Configurar ACL

Ingresar a Router 0 para emperzar configuraciones para la acl ya que negaremos los protocolos de HTTP y HTTPS de la pc2 al servidor.

a. Ingresar a usurio privilegiado

Router>**Enable**

b. Ingresar a modo de configuración global

Router#**Configure terminal**

c. Ingresar el comando Access-list con el nombre con el cual se identificara.

Router (config) # **ipv6 access-list DenyHTTP-S**

d. ahora ingresaremos el commando para indicar cual es la dirección del server con el protocolo a bloquear para que no puedan tener comunicacion

Router (config-ipv6-acl) # **deny tcp any host 2001:DB8:1:30::30 eq www**

Router (config-ipv6-acl) # **deny tcp any host 2001:DB8:1:30::30 eq 443**

e. ingresaremos el commando para que los demás puedan comunicarse con el server

Router (config-ipv6-acl) # **permit ip any any**

f. ingresaremos a el Puerto Fa0/0 que es el puerto de entrada

(puede implementarse a el puerto de salida solo que el comando al final llevaría la palabra "out")

Router (config) # **interface fa0/0**

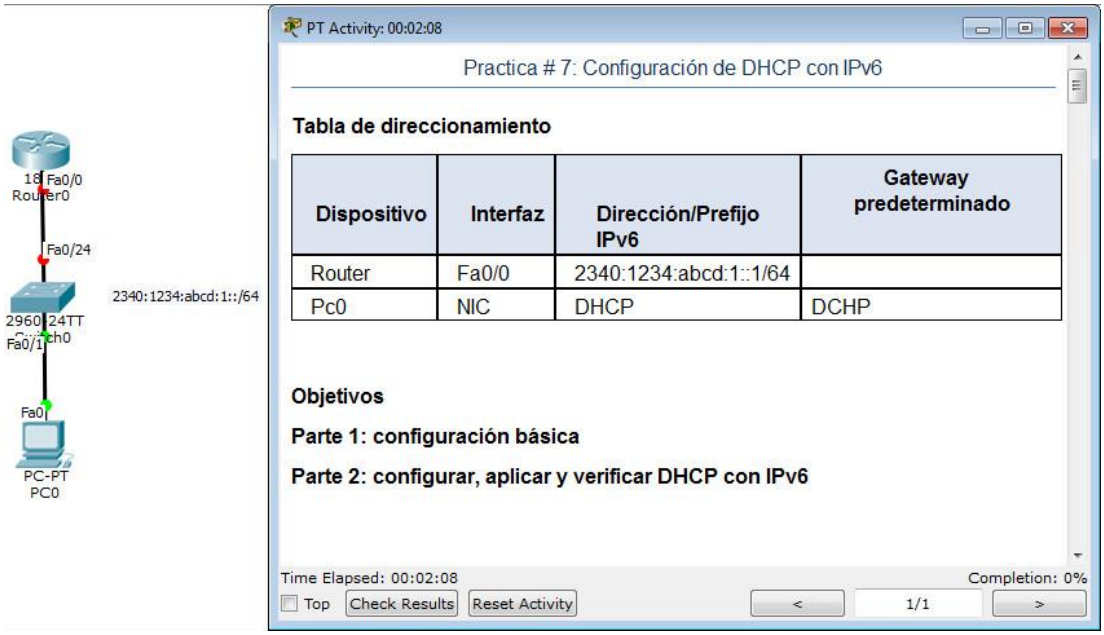
Router (config-if) # **ipv6 traffic-filter DenyHTTP-S in**

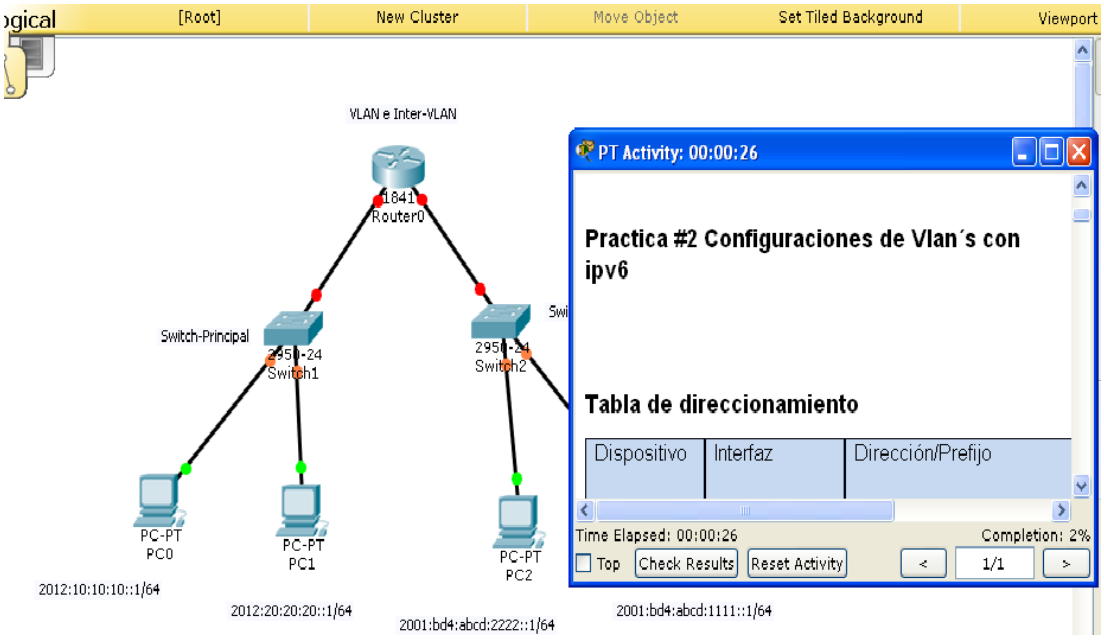
Paso 2: Probar la topología haciendo ping.

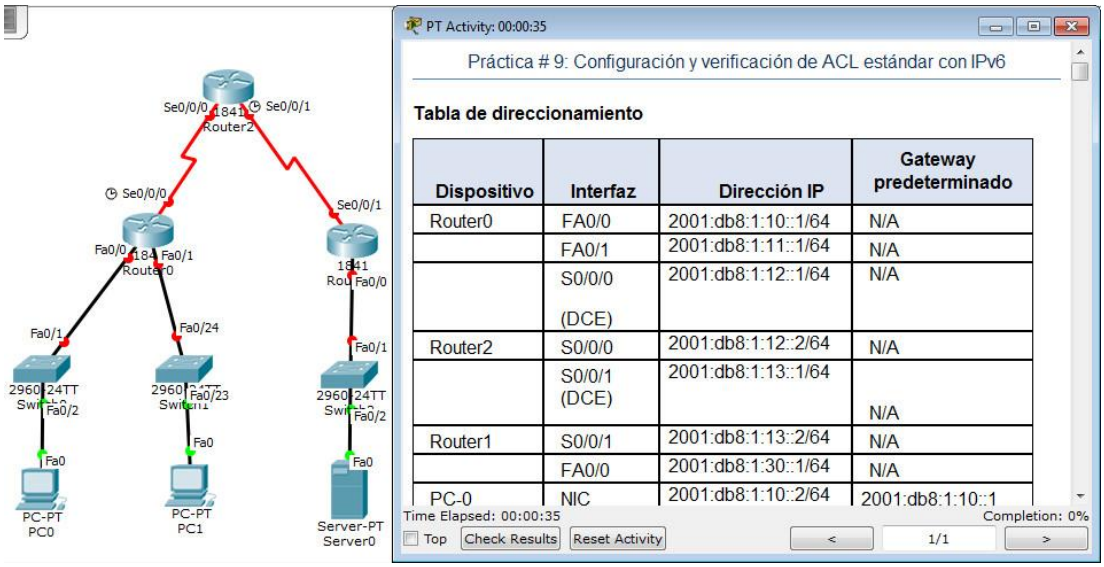
- Se hara la prueba desde la web browser del pc1 hasta el server poniendo http:// 2001:DB8:1:30::30 y https:// 2001:DB8:1:30::30, el cual tendrá que dar Host Name Unresolved.

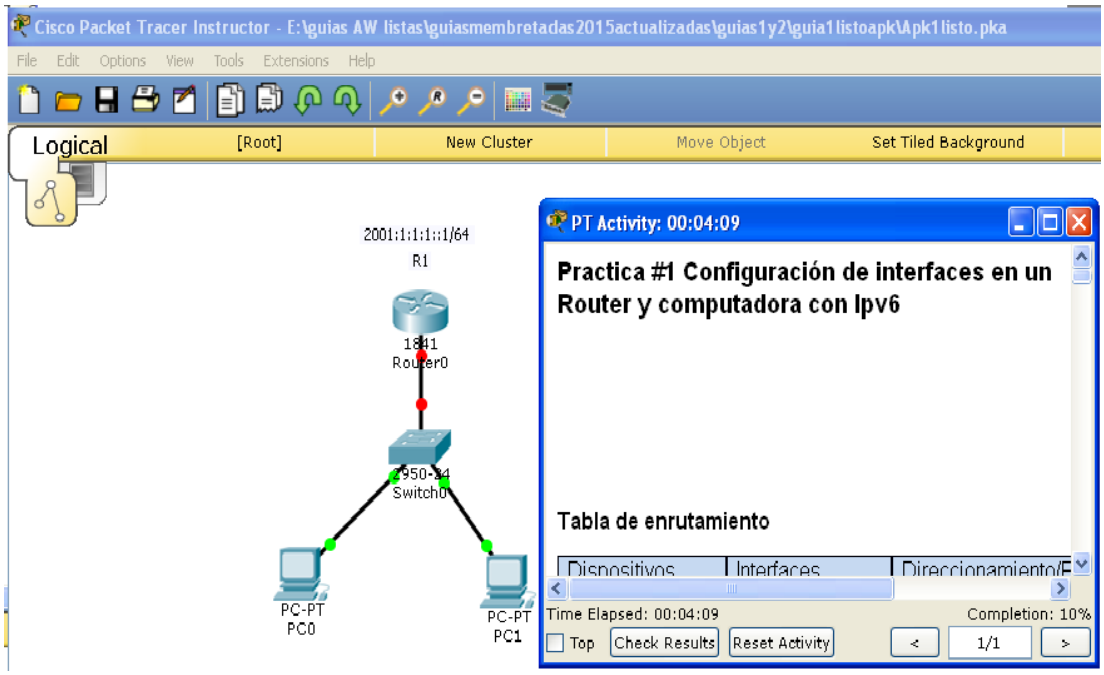
- Haremos la prueba mandando paquetes desde las PC1 y PC2 al servidor el cual dara resultado exitoso

3.1.6 Implementación de la propuesta






Se0/0/0
1841
Router2
Se0/0/1
Se0/0/0
Se0/0/1
Fa0/0
1841
Router0
Fa0/1
1841
Rou
Fa0/0
Fa0/1
Fa0/24
Fa0/1
2960-24TT
Fa0/2
2960-24TT
Fa0/23
2960-24TT
Fa0/2
Fa0
Fa0
Fa0
PC-PT
PC0
PC-PT
PC1
Server-PT
Server0
PT Activity: 00:00:35
Práctica # 9: Configuración y verificación de ACL estándar con IPv6
Tabla de direccionamiento
Dispositivo
Interfaz
Dirección IP
Gateway predeterminado
Router0
FA0/0
2001:db8:1:10::1/64
N/A
FA0/1
2001:db8:1:11::1/64
N/A
S0/0/0 (DCE)
2001:db8:1:12::1/64
N/A
Router2
S0/0/0
2001:db8:1:12::2/64
N/A
S0/0/1 (DCE)
2001:db8:1:13::1/64
N/A
Router1
S0/0/1
2001:db8:1:13::2/64
N/A
FA0/0
2001:db8:1:30::1/64
N/A
PC-0
NIC
2001:db8:1:10::2/64
2001:db8:1:10::1
Time Elapsed: 00:00:35
Completion: 0%
Top
Check Results
Reset Activity
<
1/1
>


Cisco Packet Tracer Instructor - E:\guias AW listas\guiasmembretadas2015actualizadas\guias1y2\guia1listoapk\Apk1listo.pka
File
Edit
Options
View
Tools
Extensions
Help
Logical
[Root]
New Cluster
Move Object
Set Tiled Background
2001:1:1:1::1/64
R1
1841
Router0
2950-24
Switch0
PC-PT
PC0
PC-PT
PC1
PT Activity: 00:04:09
Practica #1 Configuración de interfaces en un Router y computadora con Ipv6
Tabla de enrutamiento
Dispositivos
Interfaces
Direccionamiento/F
Time Elapsed: 00:04:09
Completion: 10%
Top
Check Results
Reset Activity
<
1/1
>

3.1.7 Presentación de la propuesta

3.1.7.1 Oferta Técnica.

Universidad Tecnológica de El Salvador
Ing. Juan Pablo Ortiz
Responsable de la Cátedra de Redes
Presente

Por este medio como es de su conocimiento se está desarrollando el proyecto titulado "Elaboración de un manual de prácticas con énfasis en IPv6 para la asignatura tecnología certificada en redes III de la Universidad Tecnológica de El Salvador", para beneficio de los estudiantes de dicha asignatura. Por esta razón se pretende hacerle saber el beneficio técnico que se obtendrá al ser aplicado dicho manual ya que este contara especialmente con la aplicación de PacketTracer, un software en el cual los estudiantes se vienen familiarizando desde el principio de la carrera. Se le pide a las autoridades competentes de esta rama, evalúen la posibilidad de incluir el manual de prácticas dentro de la curricula de la asignatura Tecnología Certificada en Redes III ya que serán de mucho beneficio para los alumnos de la carrera Técnico en ingeniería de Redes Computacionales.

_____ _____
José David Hernández Javier Ernesto Salguero

_____
Fabricio Ernesto Flores

3.1.7.2 Oferta económica.

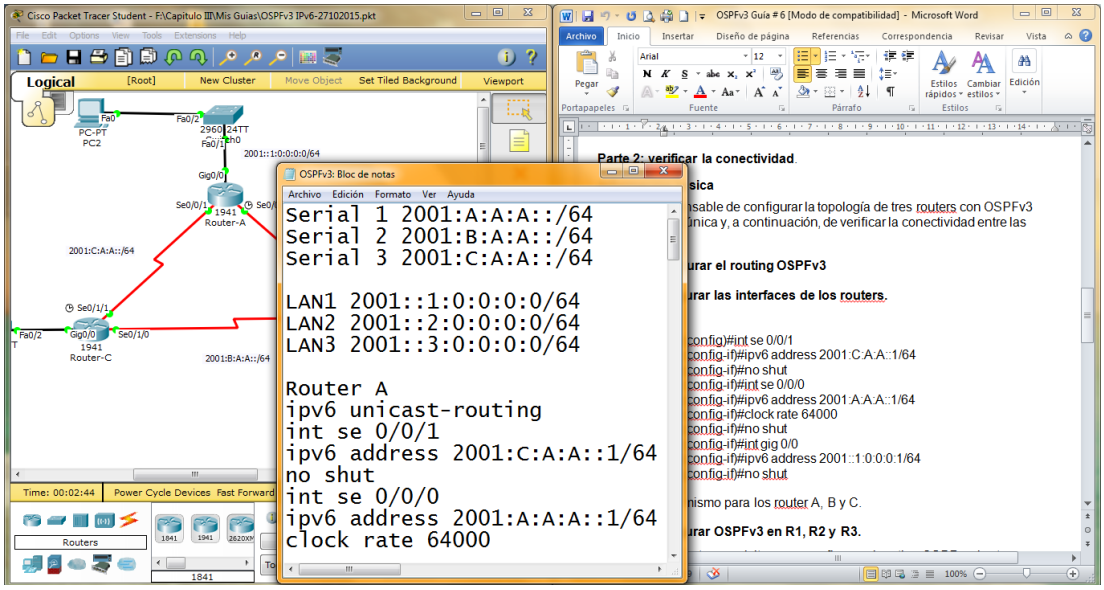
Universidad Tecnológica de El Salvador
Ing. Juan Pablo Ortiz
Responsable de la Cátedra de Redes
Presente

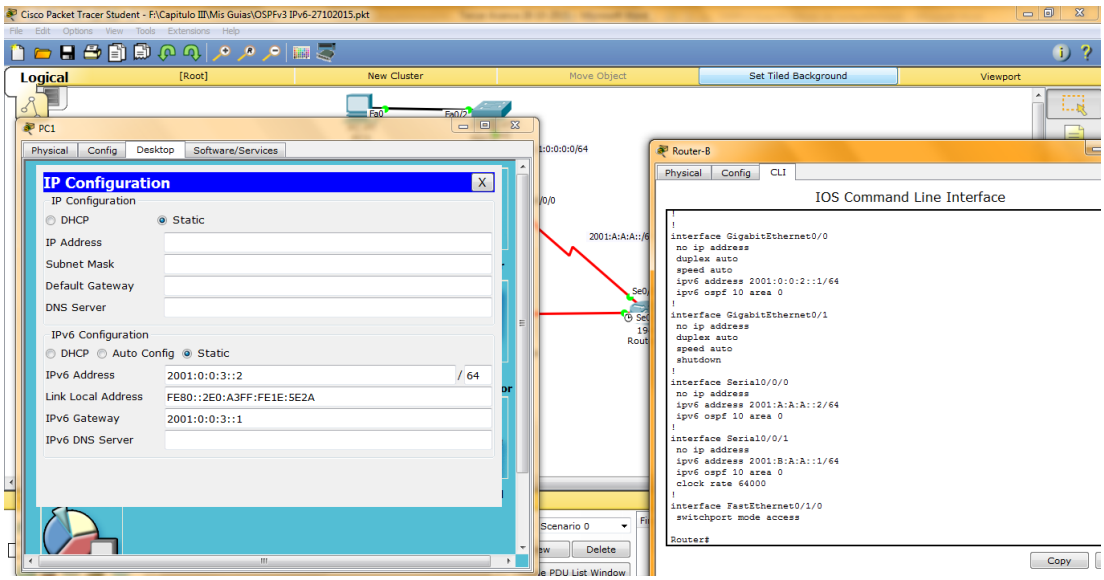
Por este medio se hace de su conocimiento que se está desarrollando el proyecto titulado "Elaboración de un manual de prácticas con énfasis en IPv6", como apoyo al proceso de enseñanza y aprendizaje en la cátedra de Redes de la Universidad Tecnológica de El salvador, el cual será de mucho beneficio tanto para la universidad como para los estudiantes de dicha asignatura. Este será un gran beneficio económico ya que la universidad cuenta con los recursos necesarios para poner en marcha dicho proyecto por lo cual no se verá obligada en incurrir en gastos adicionales, y así los estudiantes podrán hacer uso de este refuerzo académico.

_____ _____
José David Hernández Javier Ernesto Salguero

_____
Fabricio Ernesto Flores

3.1.8 Evidencias del Proyecto





CONCLUSIONES

Mediante una encuesta realizada a los alumnos de la asignatura Tecnología Certificada en Redes III. Se detectó la falta de conocimiento acerca del protocolo IP Versión 6.

Es por ello que en este trabajo se llegó a la conclusión que, los alumnos necesitan de herramientas de fácil manejo y comprensión sobre el protocolo IPv6, puesto que las debilidades encontradas al pasar este instrumento de medición, es evidente que se requiere de mayor fortalecimiento sobre el tema antes mencionado.

La creación de este manual de prácticas paso a paso ayudará a los alumnos de la asignatura de Tecnología Certificada en Redes III, a desarrollar nuevos conocimientos acerca del protocolo IPv6, y a implementar de una manera eficaz todo lo aprendido en las prácticas sobre dicho protocolo. Así mismo, sabemos que esta información será de ayuda para el área de redes de la Universidad Tecnológica de El Salvador.

RECOMENDACIONES

Al final de este trabajo podemos decir que es necesario lo siguiente:

- Se recomienda que a los alumnos de la asignatura Tecnología Certificada en Redes III, le sean incluidas más horas clase sobre IPv6, así como también hagan uso de este manual de prácticas paso a paso sobre IPv6, que han sido diseñadas y creadas con el fin, que los alumnos de redes de la Universidad puedan desarrollar nuevas y mejores competencias tanto en el área educativa como a nivel laboral.
- Es importante mencionar que la Universidad Tecnológica de El Salvador haga uso de las prácticas paso a paso sobre IPv6 y así brindar este material de apoyo para el fortalecimiento de competencias de los alumnos del área de redes de la universidad.
- Se recomienda a los docentes de la carrera Técnico en Ingeniería de Redes Computacionales, que conozcan este manual de prácticas, y que puedan adoptarlo como recurso didáctico para el desarrollo de temas relacionados con IPv6.

REFERENCIAS

BuenasTareas.com. (2011). Mascaras wildcard (redes). Recuperado de http://www.buenastareas.com/ensayos/Mascaras-Wildcard- Redes/3104149.html

Cisco. (2014). IPv6 Access Control Lists. Recuperado de http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_acl/configuration/xe-3s/sec-data-acl-xe-3s-book/ip6-acls-xe.html

Cisco learning network. (2014). Packet Tracer and DHCPv6 (Protocolo de configuración dinámica de host). Recuperado de https://learningnetwork.cisco.com/thread/70481

ElRinconDelGor – Youtube. (2015). VLan-IPv6 (Red de área local virtual). Recuperado de https://www.youtube.com/watch?v=M4p-lntrIPM

ITESA. (2014). Packet Tracer: configuración de RIPng (instrucciones). Recuperado de http://www.itesa.edu.mx/netacad/switching/course/files/7.3.2.3%20Packet%20Tracer%20-%20Configuring%20RIPng%20Instructions.pdf

Kurose, James F. & Ross, Keith W. (2005). VLAN (Red de área local vir tual). Recuperado de https://es.wikipedia.org/wiki/VLAN

LibrosNetworking. (2014). Mis Libros de Networking: IPv6 – Enrutamien to estático. Recuperado de http://librosnetworking.blogspot.com/20 14/07/ipv6-enrutamiento-estatico.html

RITA-INDUSTRIAL. (2013). *5.OSPFv3 (Open Shortest Path First).* Rec uperado de https://rita.udistrital.edu.co/images/pdf/5OSPFv3.pdf

Romero Goyzueta, Christian Augusto. (2015). 9.5.2.6 Packet Tracer – Configuring IPv6 ACLs. Recuperado de https://www.youtube.com/w atch?v=9IzA7N8FS0s

Wikipedia. (2005). TFTP (Protocolo de Transferencia de Archivo Trivial) Recuperado de https://es.wikipedia.org/wiki/TFTP

Wikipedia. (2010). DHCPv6. (Protocolo de Configuración Dinámica de Host). Recuperado de https://es.wikipedia.org/wiki/DHCPv6

ANEXOS

Anexo 1: Encuesta

I

UNIVERSIDAD TECNOLÓGICA DE EL SALVADOR
FACULTAD DE CIENCIAS APLICADAS
TECNICO EN INGENIERIA DE REDES COMPUTACIONALES

Objetivo: La presente encuesta tiene por finalidad, medir los conocimientos de los alumnos de la materia Tecnologia Certificada en redes III, acerca del Protocolo IP versión 6, y su nivel de aplicación en la rama de las redes computacionales.

Instrucciones: A continuación se presenta una serie de preguntas, marque con una "X" la respuesta con cual se identifica.

1. **¿Conoce el protocolo IP versión 6? Si su respuesta es positiva pasar a la siguiente pregunta, de lo contrario pasar a la pregunta 9.**

SI	NO

2. **¿Se imparte conocimientos sobre IPv6 en horas clases?**

SI	NO

3. **¿Lo que recibió en clases sobre IPv6, lo comprendió?**

SI	NO

4. **¿Puede configurar equipos virtuales con IPv6?**

SI	NO

5. **¿Sabe diferenciar la parte de host y la parte de red de una dirección IPv6?**

SI	NO

6. **¿Puede configurar equipos fisicos con Ipv6?**

SI	NO

7. **¿Qué tanto conocimiento maneja sobre IPv6?**

- ☐ Bastante
- ☐ Lo básico
- ☐ Muy poco

8. **¿Conoce de algún material didáctico existente en la universidad sobre el protocolo IPv6?**

SI	NO

9. **Según su criterio cuál considera es el mayor motivo por el que los estudiantes de Redes de la UTEC, no conocen sobre IPv6?**

- ☐ Falta de aplicación en clases.
- ☐ No se encuentra dentro de la temática a impartir de la materia.
- ☐ Pocos recursos pedagógicos para el aprendizaje.
- ☐ Poco tiempo horas clases para abarcar la temática.

GLOSARIO

ACL: Una lista de control de acceso o ACL es un concepto de seguridad informática usado para fomentar la separación de privilegios. Es una forma de determinar los permisos de acceso apropiados a un determinado objeto.

Anycast: Para enviar tráfico a la interfaz más cercana dentro de un grupo. Una dirección IPv6 de Anycast también identifica un conjunto de interfaces en diferentes dispositivos, pero la diferencia de un paquete enviado a una dirección Anycast es que dicho paquete está destinado al dispositivo más cercano.

Datagrama: es un paquete de datos que constituye el mínimo bloque de información en una red de conmutación por datagramas, la cual es uno de los dos tipos de protocolo de comunicación por conmutación de paquetes usados para encaminar por rutas diversas dichas unidades de información entre nodos de una red, por lo que se dice que no está orientado a conexión.

DHCP: protocolo de configuración dinámica de *host*») es un protocolo de red que permite a los clientes de una red IP obtener sus parámetros de configuración automáticamente. Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van estando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después. Conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente.

Dirección MAC: MAC son las siglas de Media Access Control y se refiere al control de acceso al medio físico. O sea que la dirección MAC es una dirección física (también llamada dirección hardware), porque identifica físicamente a un elemento del hardware: insisto en que cada tarjeta Ethernet viene de fábrica con un número MAC distinto. Windows la menciona como Dirección del adaptador. Esto es lo que finalmente permite las transmisiones de datos entre ordenadores dela red, puesto que cada ordenador es reconocido mediante esa dirección MAC, de forma inequívoca.

IP/ICMP:(por sus siglas en inglés de Internet Control Message Protocol) es el sub protocolo de control y notificación de errores del Protocolo de Internet (IP). Como tal, se usa para enviar mensajes de error, indicando por ejemplo que un servicio determinado no está disponible o que un router o host no puede ser localizado.

IPsec: (IP security). Conjunto de protocolos para la seguridad en comunicaciones IP mediante la autentificación y/o encriptación de cada paquete IP.

IPv4: IPv4 es la cuarta versión de este protocolo, pero la primera que ha sido implementada de forma extensiva. Fue descrito en el RFC 791 elaborado por la Internet Engineering Task Force (IETF) en 1981. Es el protocolo que mayormente se usa en la Capa de Red del Modelo TCP/IP para conexiones a Internet.

IPv6: es una actualización del protocolo de internet, el cual es clave para el funcionamiento de la red. El grupo de trabajo de ingeniería de internet, desarrollo las especificaciones básicas de IPv6 durante los años 90, tras una fase de diseño e implementada para seleccionar la mejor solución global.

MTU:(Maximum Transmission Unit o Unidad máxima de transferencia en español) es un parámetro que indica el tamaño máximo que debe tener un datagrama para que sea transmitido por una interfaz IP sin que necesite ser fragmentado en unidades más pequeñas.

Multicast: Para enviar a todas las interfaces del mismo grupo. Una dirección IPv6del mismo grupo multicast identifica un conjunto de interfaces en diferentes dispositivos.

OSPFv3: es similar a OSPFv2 en su funcionamiento y configuración pero son dos protocolos de enrutamiento diferente: un protocolo para enrutamiento IPv4 (OSPFv2) y un protocolo de enrutamiento para IPv6.

RIPng: RIP de última generación (**RIPng**) es un protocolo de routing vector distancia para enrutar direcciones IPv6. Se basa en RIPv2 y tiene la misma distancia administrativa y limitación de 15 saltos.

SLAAC: configuración automática de dirección sin estado (**SLAAC**) es un método que permite que un dispositivo obtenga su prefijo, duración de prefijo e

información de la dirección de gateway predeterminado de un router IPv6 sin utilizar un servidor de DHCPv6.

Unicast: son las más comunes y utilizadas. Estas son asignadas a una interface o nodo permitiendo la comunicación directa entre dos nodos de la red.

VLAN: es una red de área local que agrupa un conjunto de equipos de manera lógica y no física. Efectivamente, la comunicación entre los diferentes equipos en una red de área local está regida por la arquitectura física.

Wildcare: Una máscara wildcard se compara con una dirección IP. Los números en binario uno y cero en la máscara, se usan para identificar cómo se deben manejar los bits de la dirección que desea revisar. Las máscaras wildcard están diseñadas para filtrar direcciones de host individuales o rangos, o incluso se pueden filtrar direcciones de red. Un cero significa que esa posición seráverificada. Un 1 significa que esa posición no se verificará.