Desarrollo de Guías para el Diseño e Implementación de Redes Locales Virtuales, Acceso Remoto y Autenticación en un entorno LAN

Mauricio Javier Tufiño Coloma

Departamento de Eléctrica y Electrónica, Escuela Politécnica del Ejército
Av. El Progreso S/N, Sangolquí, Ecuador

maut10@live.com

Resumen-- El presente documento expone el desarrollo de guías para el diseño e implementación de redes locales virtuales, autenticación y acceso remoto en un entorno LAN, además las guías están diseñadas de tal manera sirva como una herramienta importante, permitirá que los estudiantes desarrollen sus conocimientos en el ámbito de redes locales virtuales, autenticación y acceso remoto. Tiene como propósito el familiarizarse con términos técnicos y problemas de la vida real. Con el fin de que su desarrollo profesional sea de éxito.

I. INTRODUCCIÓN

En el pasado el HUB era un dispositivo muy utilizado para interconectar computadoras en redes locales. El HUB recibe datos procedentes de una computadora y los transmite a las demás, en el caso del Switch los datos provenientes de la computadora de origen solamente son enviados a la computadora de destino, lo que permite un aumento en el rendimiento de la red. [1].

La Escuela Politécnica del Ejército en el laboratorio de Networking dispone de equipos Switch los cuales no han sido utilizados para sacar el mayor provecho de estos. Ya que el tiempo que disponen los docentes en el departamento de electrónica no es suficiente para abarcar todos los temas vistos en clases. Por lo cual se ve la necesidad de desarrollar guías prácticas para la creación de redes locales virtuales, acceso remoto y autenticación. Con el fin de optimizar el tiempo del docente y permitir que el estudiante por medio de las guías interactué con un equipo real.

La utilización de los switch en el campo laboral permite la creación de redes virtuales, segmenta de manera lógica las redes conmutadas basadas en equipos de proyectos, funciones o departamentos. [2].

Uno de los problemas en la seguridad de las redes es la falta de autenticación o la intrusión no autorizada lo que se pretende con el desarrollo de las guías prácticas es concientizar al alumno, que la inseguridad en las redes es una realidad si esta no se prevé.

II. MARCO TEÓRICO

2.1. CONCEPTOS Y DEFINICIONES

LAN: es una red que permite conectar los ordenadores en un área relativamente pequeña y predeterminada (como una habitación, un edificio, o un conjunto de edificios). La Figura 1. Nos muestra la topología de una red LAN.

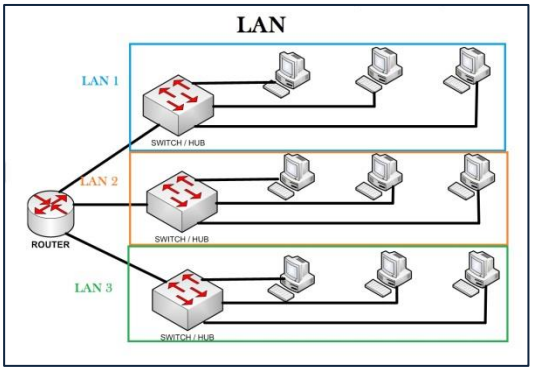


Fig. 1. Topología de una Red LAN

VLAN: Es una Red de Área Local Virtual (Virtual LAN) es un método para crear redes lógicamente independientes dentro de una misma red física. Varias VLAN pueden coexistir en un único conmutador físico o en una única red física. [3].

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 (como departamentos de una empresa). La Figura 2. Nos muestra la Topología de una Red con VLANs.

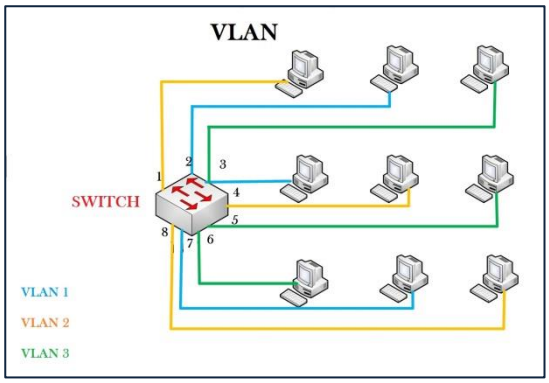


Fig. 2. Topología de una Red VLAN

2.2. MODELO DE REDES JERÁRQUICAS

El diseño de una LAN que cumpla las necesidades de empresas pequeñas o medianas tiene más probabilidades de ser exitosa si utilizamos un modelo de diseño jerárquico. En comparación con otros diseños de redes, una red jerárquica se administra y expande con más facilidad y los problemas se resuelven con mayor rapidez.

2.2.1. Capas en una Red Jerárquica

En una Red Jerárquica encontramos tres capas: Capa de Acceso, Capa de Distribución y Capa de Núcleo como muestra la Figura 3.

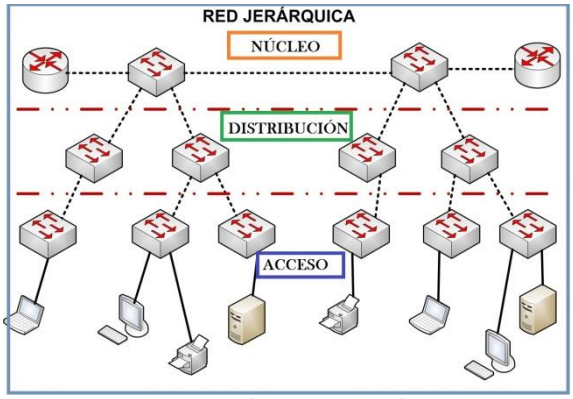


Fig. 3. Topología de una Red Jerárquica

2.3. CONMUTACIÓN CAPA 2 Y CAPA 3

El switch de Capa 2 es completamente transparente para los protocolos de la red y las aplicaciones del usuario.

Un switch de Capa 3 funciona de modo similar a un switch de Capa 2, pero en lugar de utilizar sólo la información de las direcciones MAC para determinar los envíos, el switch de Capa 3 puede también emplear la información de la dirección IP. [4].

2.3.1. Comparación entre Switch Capa 3 y Router

Para comprender las diferencias entre cada dispositivo observamos la Tabla 1. Colocando que funciones cumple cada dispositivo de Red.

Tabla. 1. Diferencia entre Switch Capa 3 y Router

CARACTERÍSTICA	SWITCH CAPA3	ROUTER
ENRUTAMIENTO CAPA 3	✓	✓
VELOCIDAD DE SWITCHING MAYOR	✓	✗
ADMINISTRACIÓN DEL TRAFICO	✓	✓
MAYOR DENSIDAD DE PUERTOS LAN	✓	✗
SOPORTE INTERFACES PARA CONEXIÓN WAN	✗	✓
PROTOCOLOS DE ENRUTAMIENTO AVANZADOS	✗	✓
SOPORTE PARA VLAN	✓	✗

2.4. TIPOS DE VLAN

Las VLAN pueden ser ya sea Estáticas o Dinámicas. Si hablamos de VLAN Estática quiere decir que los administradores de la red configuran puerto por puerto. Cada puerto está asociado a una VLAN específica. El administrador de red es responsable de escribir las asignaciones entre los puertos y las VLAN.

En el caso de una VLAN dinámica los puertos pueden calcular dinámicamente. Utiliza una base de datos centralizada en la cual cada direcciones MAC está asignada a su respectiva VLAN, el administrador de red debe configurar previamente.

Las VLAN, se dividen en cuatro tipos principales:

1. VLAN Basada en Puerto.
2. VLAN Basada en Protocolo.
3. VLAN Basada en Dirección IP.
4. VLAN Basada en Nombre de Usuario.

2.5. ENLACE TRONCAL EN UNA VLAN

Un enlace troncal es un enlace punto a punto, entre dos dispositivos de red, que transporta más de una VLAN.

La Solución al problema es el protocolo 802.1Q como muestra la Figura 4.

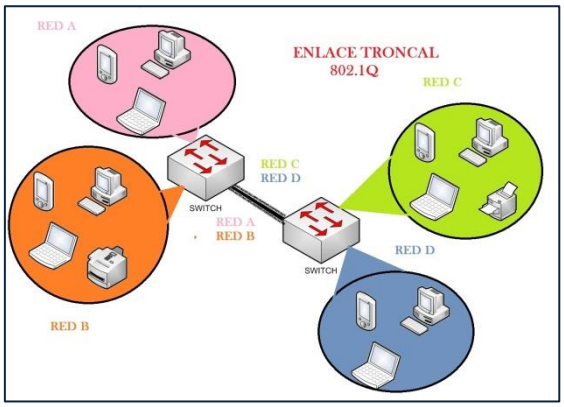


Fig. 4. Solución utilizar protocolo 802.1Q

2.6. ACCESO REMOTO

El acceso remoto a un dispositivo de Red permite el ahorro de tiempo y costes, la posibilidad de realizar asistencia remota ayuda a los profesionales en el área de redes, tener acceso al equipo mediante una línea telefónica o simplemente teniendo conexión a internet.

Antes, el administrador de Red tenía que desplazarse hasta el dispositivo de Red que tenía algún problema. Eso conllevaba un tiempo de demora y de inactividad del usuario afectado que repercutía en su trabajo. Con la solución de acceso remoto, el usuario es atendido de forma remota desde su puesto de trabajo en el momento en que da el aviso, por lo que se reducen los tiempos de soporte por teléfono, se ahorran desplazamientos y se reducen costes.

2.6.1. TELNET

Telnet es un protocolo de acceso remoto que como indica la Figura 5. Y la Figura 6. Maneja un modelo Cliente-Servidor y los datos viajan en texto plano. [5].

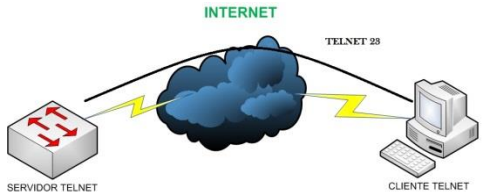


Fig. 5. Conexión Cliente Servidor TELNET

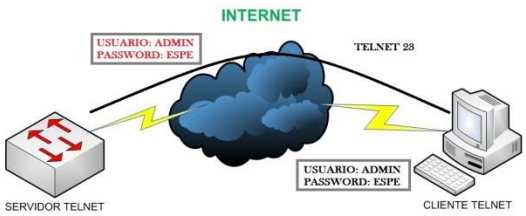


Fig. 6. Envío de la información en texto plano

2.6.2. SSH

SSH es un protocolo de acceso remoto que como indica la Figura 7. Y la Figura 8. Maneja un modelo Cliente-Servidor y los datos viajan en texto cifrado. A diferencia de Telnet este protocolo es más seguro. [6].

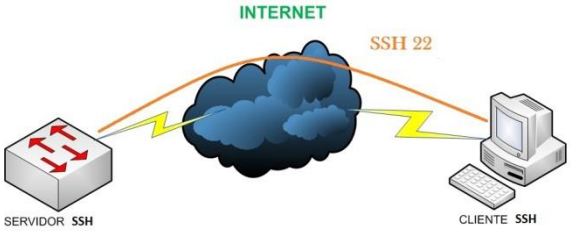


Fig. 7. Conexión Cliente Servidor TELNET

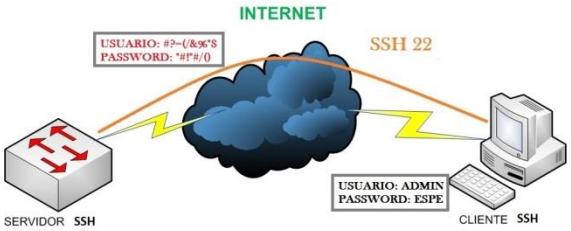


Fig. 8. Envío de la información en texto cifrado

2.7. 802.1X

La IEEE 802.1X es una norma de la IEEE para el control de acceso a la red basada en puertos. Es parte del grupo de protocolos IEEE 802 (IEEE 802.1). Permite la autenticación de dispositivos conectados a un puerto LAN, estableciendo una conexión punto a punto o previniendo el acceso por ese puerto si la autenticación falla.

802.1X está disponible en ciertos Switch y puede configurarse para autenticar nodos que están equipados con software suplicante. Esto elimina el acceso no autorizado a la red al nivel de la capa de enlace de datos

2.7.1. AAA (Authentication, Authorization, and Accounting).

Los servicios de seguridad AAA proporcionan un marco inicial para montar control de acceso en un dispositivo de red. AAA es una manera de controlar a quién se le permite acceso a una red (autenticación) y qué pueden hacer mientras están allí (autorización), así como auditar qué acciones realizaron al acceder a la red (registro de auditoría).

2.7.2. RADIUS

El protocolo RADIUS esconde las contraseñas durante la transmisión, incluso con el Protocolo de Autenticación de Contraseñas (Password Authentication Protocol - PAP), usando una operación bastante compleja que involucra la dispersión a través de MD5 (Message Digest 5) y una contraseña compartida. Sin embargo, el resto del paquete se envía en texto plano.

2.8. STACKING

2.8.1. Conceptos y ventajas

Algunos Switch pueden ser interconectados para formar un STACK (Pila), cada conmutador es una unidad.

Realiza administración unificada de múltiples dispositivos. Solo una conexión y una Dirección IP será necesaria para administrar todo el STACK. Por lo tanto el costo de administración es reducido.

Permite comprar dispositivos para expandir la capacidad de la red rápidamente. Protege la inversión durante toda la actualización de la red.

La Figura 9. Nos un ejemplo de STACKING.

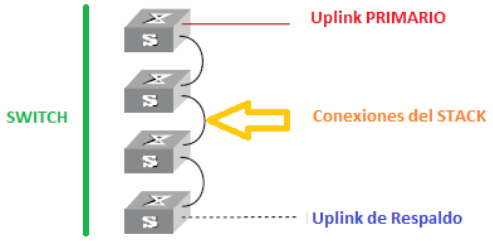


Fig. 9. Ejemplo de STACKING

2.9. QOS (Quality Of Service)

2.9.1. Definición

ITU E.800: "Efecto global de las prestaciones de un servicio que determinan el grado de satisfacción de un usuario al utilizar dicho servicio."

IETF RFC 2386: "Conjunto de requisitos del servicio que debe cumplir la red en el transporte de un flujo."

QoS permite que los programas en tiempo real optimicen el uso del ancho de banda de la red.

QoS asegura cierto nivel de garantía en los recursos de la red suficientes, ofrece a una red compartida un nivel de servicio similar al de una red dedicada.

2.9.2. 802.1P

EEE 802.1p es un estándar que proporciona priorización de tráfico y filtrado multicast dinámico. Esencialmente, proporciona un mecanismo para implementar Calidad de Servicio (QoS) a nivel de MAC (Media Access Control).

La Tabla 2. Nos muestra las 8 prioridades que tiene el estándar 802.1p en el campo PRIORIDAD. [7].

Tabla. 2. Campo Prioridad

PRIORIDAD bits	PRIORIDAD EN LA RED	CARACTERÍSTICAS DEL TRÁFICO
001	0 (menor)	Segundo Plano
000	1	Mejor Esfuerzo
010	2	Excelente Esfuerzo
011	3	Aplicaciones Criticas
100	4	Video, 100ms de Latencia
101	5	Video, 10ms de Latencia
110	6	Internetwork Control
111	7 (mayor)	Control de la RED

III. ESPECIFICACIONES TECNICAS DE LOS EQUIPOS

3.1. EQUIPOS EN EL LABORATORIO DE NETWORKING

El laboratorio de Networking cuenta con los siguientes equipos, distribuidos en equipos de Capa 2 y equipos de Capa 3:

a) 3 Switch 3com 4210 de 26 puertos.

b) 2 Switch 3com 4500 de 26 puertos.

c) 2 Switch Cisco Catalyst Express 500 de 24 puertos.

d) 2 Switch D-link DGS-3627 de 24 puertos.

e) 1 Switch 3com 5500 de 28 puertos.

f) 1 Switch Cisco Catalyst 3560 de 24 puertos.

g) 2 Switch HP 2512 de 12 puertos.

h) 1 Switch D-link DES-3526 de 24 puertos.

La Tabla 3. Nos indica las características de los equipos de Capa 2.

Tabla. 3. Características Switch Capa 2

CARATERISTICA	Switch *3com 4210*	Switch *Cisco Catalyst Express 500*	Switch *HP 2512*
Número de Puertos	26 Puertos	24 Puertos	12 Puertos
Soporte PoE (Power over Ethernet)	SI	SI	NO
Rendimiento	8.8 Gbps	8.8 Gbps	9.6 Gbps
Soporte VLAN	SI	SI	SI
Soporte STP o variaciones	STP/RSTP/MSTP	STP/RSTP	STP/RSTP
Soporte TELNET	SI	NO	SI
Soporte SSH	SSH v2	NO	SSH v1
SNMP	SNMP v3	SNMP v3	SNMP v2
IGMP SNOOPING	IGMP v1	IGMP v3	IGMP v3
Soporte TFTP	SI	NO	SI
Soporte 802.1x	SI	SI	SI
Soporte Stacking	NO	NO	SI
Soporte QoS (802.1p)	SI	SI	SI
Soporte IPv6	SI	NO	NO
PESO	2.14 Kg	3.2 Kg	2.7 Kg
Costo Aproximado 2012	~ $335	~ $180	~ $210

La Tabla 4. Nos indica las características de los equipos de Capa 3.

Tabla. 4. Características Switch Capa 3

	Switch *3com 4500*	Switch *Cisco Catalyst 3560*	Switch *D-link DGS-3627*	Switch *3com 5500*
Número de Puertos	26 Puertos	24 Puertos	24 Puertos	28 Puertos
Soporte PoE	SI	SI	NO	SI
Rendimiento	8.8 Gbps	32 Gbps	108 Gbps	12.8 Gbps
Soporte VLAN	SI	SI	SI	SI
Soporte STP o variaciones	STP / RSTP/ MSTP	RSTP / PVRST+	STP /RSTP /MSTP	STP /RSTP /MSTP
Soporte TELNET	SI	SI	SI	SI
Soporte SSH	SSH v2	SSH v2	SSH v2	SSH v2
SNMP	SNMP v3	SNMP v3	SNMP v3	SNMP v3
IGMP SNOOPING	IGMP v1	IGMP v3	IGMP v3	IGMP v3
Soporte TFTP	SI	SI	SI	SI
Soporte 802.1x	SI	SI	SI	SI
Soporte Stacking	SI	SI	SI	SI
Soporte QoS (802.1p)	SI	SI	SI	SI
Enrutamiento Estático	SI	SI	SI	SI
Enrutamiento Dinámico	RIP v1, RIP v2	RIP v1, RIP v2, RIPng, OSPF, EIGRP, BGP ,IS-IS	RIP v1, RIP v2, RIPng, OSPF v2.	RIP v1, RIP v2, OSPF
Soporte ACL´S	SI	SI	SI	SI
Soporte IPv6	SI	SI	SI	SI
PESO	6.3 Kg	5.1 Kg	5.5 Kg	6.3 Kg
Costo Aproximado 2012	~$1,000	~$1,200	~$2,200	~$2,050

IV. DISEÑO DE PRÁCTICAS DE LABORATORIO PARA ESTUDIANTE

El objetivo fundamental de las guías prácticas de laboratorio es fomentar al alumno una enseñanza más activa, participativa e individualizada.

De este modo se favorece que el alumno:

- Desarrolle habilidades.
- Aprenda técnicas elementales.
- Se familiarice con el manejo de equipos de Networking.

Por otra parte, el enfoque que se va a dar a las guías prácticas depende de los objetivos específicos que se quieran conseguir tras su realización.

La realización de las guías prácticas permite poner en desarrollo el pensamiento espontáneo del alumno, al aumentar la motivación y la comprensión respecto a los conceptos impartidos por el profesor.

4.1. FORMATO DE LAS GUÍAS DE LABORATORIO

Las guías prácticas tendrán un formato específico, para lo cual se va a detallar cada uno de los campos.

TEMA: Estará descrito el nombre de la práctica este nombre dependerá si la práctica es: general o específica.

OBJETIVOS: Contendrá todos los objetivos ya sean específicos o generales, los cuales tendrán como propósito mejorar el aprendizaje y desempeño en el alumno. Un Objetivo será planteado por el alumno, a fin de que el alumno se interese por el aprendizaje.

MARCO TEORICO: Se dará un resumen del o los temas que va abarcar la práctica. Sirve como refuerzo de los temas profundizados en clases.

EQUIPOS: En este caso particular se detallara cuales equipos del laboratorio de Networking necesitaremos para el desarrollo de las prácticas. También incluirá instrumentos o equipos adicionales que se requieran para la realización de las prácticas.

PROBLEMA PROPUESTO: En el campo Problema Propuesto, si lo requiere la práctica se describirá un problema a la que el estudiante deberá encontrar una o varias soluciones.

NOTA/ADVERTENCIA: Permitirá al alumno no cometer errores en el desarrollo de la práctica o a su vez dar instrucciones al finalizar la práctica.

TOPOLOGÍA: Muestra la topología de Red que se debe implementar o simular.

CONFIGURACIONES/DIRECCIONAMIENTO Al mencionar este campo debemos recordar que para el éxito de las prácticas se tomara en cuenta, un buen direccionamiento y la correcta configuración de los equipos los cuales deberán ser llenados paso a paso.

CONCLUSIONES/RECOMENDACIONES: El alumno describirá su experiencia con la práctica anotando que concluyó y que recomienda de la misma.

4.2. PRACTICAS DISEÑADAS

Para el correcto desarrollo del Estudiante con el manejo de equipos en el laboratorio de Networking, se diseñaron el total de 19 prácticas que incluyen: prácticas de laboratorio y prácticas que se pueden realizar en los simuladores de Red.

La Tabla 5. Nos muestra el número y el nombre de la práctica.

Tabla. 5. Nombre de Prácticas Diseñadas

NÚMERO PRÁCTICA	NOMBRE DE LA PRÁCTICA
1	CONFIGURACIÓN BASICA DEL SWITCH.
2	CONFIGURACIÓN DE TELNET.
3	CONFIGURACIÓN DE SSH.
4	CONFIGURACIÓN DE UNA VLAN POR PUERTO.
5	CONFIGURACIÓN DHCP CON VLAN.
6	CONFIGURACIÓN DE SPANNING TREE PROTOCOL (STP) Y ENLACES TRONCALES.
7	INTERCONEXIÓN DE VLANS POR MEDIO DEL ROUTER.
8	CONFIGURACIÓN DE ACL (ESTANDAR-EXTENDIDA) EN EL SWITCH.
9	SIMULACIÓN DE UNA RED QUE PERMITA DIVIDIR DEPARTAMENTOS EN UNA EMPRESA Y DAR PRIORIDAD DE SERVICIOS A CIERTOS EMPLEADOS POR MEDIO DE ACL.
10	IMPLEMENTACIÓN DE UNA RED JERARQUICA CON REDUNDANCIA.
11	IMPLEMENTACIÓN DE UNA RED JERARQUICA QUE PERMITA LA ADMINISTRACIÓN POR MEDIO DE ACCESO REMOTO (SSH).
12	SIMULACIÓN DE UNA RED JERARQUICA QUE PERMITA LA ADMINISTRACIÓN CON SNMP (SIMPLE NETWORK MANAGEMENT PROTOCOL).
13	CONFIGURACIÓN IPv6 EN UN SWITCH CAPA 3.
14	ENRUTAMIENTO DINAMICO (RIPng) IPv6 EN UN ENTORNO LAN CON SWITCH CAPA 3.
15	CONFIGURACIÓN DE IPv6 TUNNELING EN UN ENTORNO LAN.
16	CONFIGURACIÓN DEL SERVIDOR AAA PARA ACCESO TELNET EN UNA RED DE AREA LOCAL.

17	**SIMULACIÓN DE UNA RED QUE BRINDE AUTENTICACIÓN (AAA) Y QoS (802.1p).**
18	**IMPLEMENTACIÓN DE UNA RED IPv4 OPERATIVA QUE BRINDE (VLAN, ACL, AAA, SSH, QoS)**
19	**IMPLEMENTACION DE UNA RED OPERATIVA CON IPv6 CON OSPFv3**

V. DESARROLLO DE LA PRÁCTICA #14 Y MANUAL DEL DOCENTE

En Este caso en particular nos enfocaremos en como fue el desarrollo de la práctica #14.

5.1. ESQUEMA DE LA PRÁCTICA # 14

TEMA: Enrutamiento Dinámico (RIPng) IPv6 en un entorno LAN con Switch capa 3.

OBJETIVOS:

a) Implementar una Red operativa IPv6 aplicando conceptos Ripng.

b) Encontrar la solución más óptima para el desarrollo del mismo.

PROBLEMA PROPUESTO:

RIPng para IPv6:

Es un protocolo pensado para pequeñas redes, y por tanto se incluye en el grupo de protocolos de pasarela interior (IGP - "Interior Gateway Protocol"), y emplea un algoritmo denominado "Vector-Distancia". Se basa en el intercambio de información entre routers, de forma que puedan calcular las rutas más adecuadas, de forma automática.

RIPng sólo puede ser implementado en Routers/Switches, donde requerirá como información fundamental, la métrica o número de saltos (entre 1 y 15), que un paquete ha de emplear, para llegar a determinado destino. Cada salto supone un cambio de red, por to general atravesando un nuevo Router/Switch.

Estos parámetros se configuran en el Switch.

- El prefijo IPv6 del destino.
- La dirección IPv6 del siguiente Router/Switch, así como la ruta para llegar a él.
- Un indicador relativo al cambio de ruta.
- Varios contadores asociados con la ruta.

RIPng es un protocolo basado en UDP. Cada Router/Switch tiene un proceso que envía y recibe datagramas en el puerto 521 (puerto RIPng). [8].

El inconveniente de RIPng, al igual que en IPv4, siguen siendo, además de su orientación a pequeñas redes (diámetro de 15 saltos como máximo), en que su métrica es fija, es decir, no puede variar en función de circunstancias de tiempo real (retardos, fiabilidad, carga, etc.).

EQUIPOS:

Los Equipos los cuales nos permitirán el desarrollo de la práctica son:

1. – Switch D-link DGS-3627.

2. - Switch Cisco 3560.

3. - Switch 3Com 4500.

4. - Switch 3Com 5500.

5.- Cable de Consola, Cable(s) de Red.

6.- Software a utilizar (PUTTY, TERA TERM).

NOTA/ADVERTENCIA:

Los Routers estarán configurados con el protocolo de enrutamiento vector distancia RIP v2

Luego de terminar con la práctica de laboratorio dejar el Equipo con la configuración por defecto.

TOPOLOGÍA:

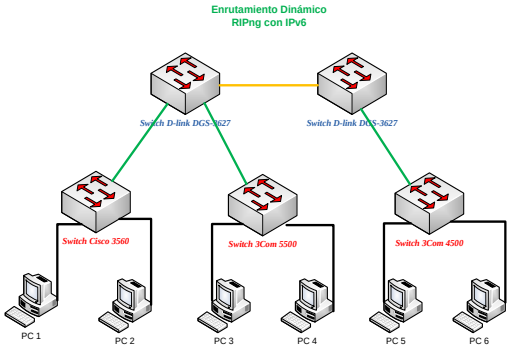


Fig. 10. Topología de Red Práctica # 14

5.1.1. Direccionamiento

La Tabla 6. Nos indica el Direccionamiento IP que necesita la Red para su funcionamiento.

Tabla. 6. Direccionamiento IP Práctica # 14

DISPOSITIVO	Dirección IPv6	Interfaz
Switch D-LINK SW1		
	2001:450:2002:E8::1	**Vlan 1**
	2800:270:0:A::10	**Vlan RED1**
	2800:270:0:B::10	**Vlan RED2**
Switch D-LINK SW2		
	2001:450:2002:E8::2	**Vlan 1**
	2800:270:0:C::10	**Vlan RED1**
PC1	2800:270:0:A::20	**Ethernet**
PC2	2800:270:0:A::21	**Ethernet**
PC3	2800:270:0:B::20	**Ethernet**
PC4	2800:270:0:B::21	**Ethernet**
PC5	2800:270:0:C::20	**Ethernet**
PC6	2800:270:0:C::21	**Ethernet**

5.1.2. PROCEDIMIENTO

5.1.2.1. Configuración Equipos

5.1.2.1.1. Switch D-Link DGS-3627 SW1

Accedemos al Switch SW1 y creamos la Vlan “RED1” y “RED2”.

```
DGS-3627:5#create vlan RED1 tag 10
Command: create vlan RED1 tag 10

Success.

DGS-3627:5#create vlan RED2 tag 20
Command: create vlan RED2 tag 20

Success.
```

Añadimos puertos a la VLAN.

```
DGS-3627:admin#config vlan RED1 add untagged 2
Command: config vlan RED1 add untagged 2

Success.

DGS-3627:admin#config vlan RED2 add untagged 3
Command: config vlan RED2 add untagged 3

Success.
```

Configuración de Enlace Troncales.

```
DGS-3627:admin#config vlan RED1 add tagged 12
Command: config vlan RED1 add tagged 12

Success.

DGS-3627:admin#config vlan RED2 add tagged 12
Command: config vlan RED2 add tagged 12

Success.
```

Configuramos la IP de la VLAN “RED1”, “RED2” y la VLAN 1.

```
DGS-3627:admin#config ipif interface ipv6 ipv6address 2800:270:0:a::10/64
Command: config ipif interface ipv6 ipv6address 2800:270:0:A::10/64

Success.

DGS-3627:admin#config ipif interface2 ipv6 ipv6address 2800:270:0:b::10/64
Command: config ipif interface2 ipv6 ipv6address 2800:270:0:B::10/64

Success.

DGS-3627:admin#config ipif System ipv6 ipv6address 2001:450:2002:e8::1/64
Command: config ipif System ipv6 ipv6address 2001:450:2002:E8::1/64

Success.
```

Habilitamos el protocolo de enrutamiento RIPng a todas las interfaces.

```
DGS-3627:admin#enable ripng
Command: enable ripng

Success.


DGS-3627:admin#config ripng ipif System state enable
Command: config ripng ipif System state enable

Success.

DGS-3627:admin#config ripng ipif interface state enable
Command: config ripng ipif interface state enable

Success.

DGS-3627:admin#config ripng ipif interface2 state enable
Command: config ripng ipif interface2 state enable

Success.
```

5.1.2.1.2. Switch D-Link DGS-3627 SW2

La configuración hasta el protocolo de Enrutamiento se cumple los mismos pasos, por lo cual omitiremos los comandos.

Para configurar SSH en el Switch SW2 utilizamos los siguientes comandos.

```
DGS-3627:admin#create account admin PCAD
Command: create account admin PCAD

Enter a case-sensitive new password:****
Enter the new password again for confirmation:****
Success.

DGS-3627:admin#config ssh user PCAD authmode password
Command: config ssh user PCAD authmode password

Success.
```

Configuramos el tipo de algoritmo por la cual va a ser encriptado la clave.

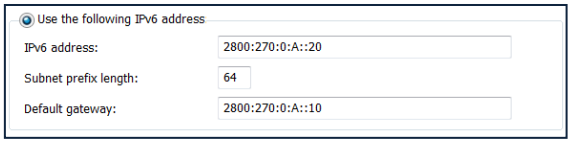
```
DGS-3627:admin#config ssh algorithm RSA enable
Command: config ssh algorithm RSA enable

Success.
```

Habilitamos SSH en el Switch SW2.

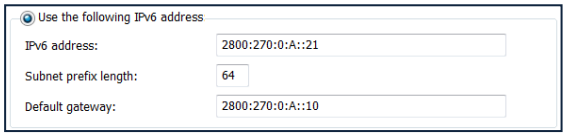
```
DGS-3627:4#enable ssh
Command: enable ssh

TELNET will be disabled when enable SSH.
Success.
```

5.1.2.1.3. Configuración PC1, PC2, PC3 ,PC4

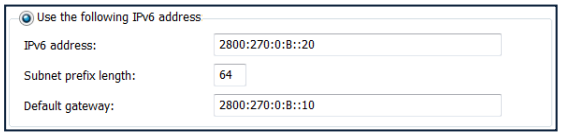
PC1



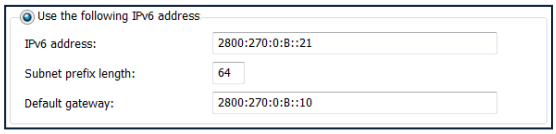
PC2



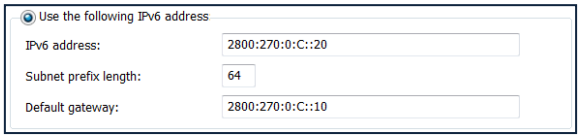
PC3



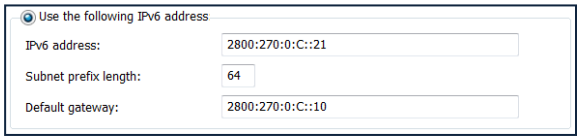
PC4



PC5



PC6



5.1.2.2. Pruebas de Conectividad

Conectividad PC5 con PC1

```
C:\Users\REDES-PC>ping 2800:270:0:a::20

Haciendo ping a 2800:270:0:a::20 con 32 bytes de datos:
Respuesta desde 2800:270:0:a::20: tiempo<1m
Respuesta desde 2800:270:0:a::20: tiempo<1m
Respuesta desde 2800:270:0:a::20: tiempo<1m
Respuesta desde 2800:270:0:a::20: tiempo<1m

Estadísticas de ping para 2800:270:0:a::20:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

Conectividad PC5 con PC3

```
C:\Users\REDES-PC>ping 2800:270:0:b::20

Haciendo ping a 2800:270:0:b::20 con 32 bytes de datos:
Respuesta desde 2800:270:0:b::20: tiempo<1m
Respuesta desde 2800:270:0:b::20: tiempo<1m
Respuesta desde 2800:270:0:b::20: tiempo<1m
Respuesta desde 2800:270:0:b::20: tiempo<1m

Estadísticas de ping para 2800:270:0:b::20:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

Conectividad PC5 con PC4

```
C:\Users\REDES-PC>ping 2800:270:0:b::21

Haciendo ping a 2800:270:0:b::21 con 32 bytes de datos:
Respuesta desde 2800:270:0:b::21: tiempo<1m
Respuesta desde 2800:270:0:b::21: tiempo<1m
Respuesta desde 2800:270:0:b::21: tiempo<1m
Respuesta desde 2800:270:0:b::21: tiempo<1m

Estadísticas de ping para 2800:270:0:b::21:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

VI. CONCLUSIONES Y RECOMENDACIONES

- El Switch es un dispositivo que a diferencia del HUB mejora el rendimiento de la Red, maneja diferentes protocolos ya sea de Autenticación, Acceso Remoto y Enrutamiento.

- El Switch hace manejo de Redes Locales Virtuales, la implementación en una empresa permitirá el crecimiento y la productividad de la misma.

- Una Red Jerárquica se caracteriza por brindar escalabilidad y seguridad. Su diseño, permitirá al administrador de Red una fácil administración y resolución de problemas.

- Una Red Jerárquica por su topología tiene Redundancia favoreciendo que la Red esté operativa en el caso que exista algún enlace caído.

- El Laboratorio de Networking del departamento de Electrónica cuenta con equipos Switch Capa 2 y Capa 3. Los cuales fueron separados y analizados, para el diseño óptimo de las guías de Laboratorio.

- Las guías de Laboratorio fueron diseñadas y estructuradas en forma gradual aumentando el nivel de dificultad, esto servirá como un apoyo para la formación profesional del estudiante.

- Cada una de las guías de laboratorio fueron desarrolladas comenzando por el direccionamiento de Red y la configuración de los equipos utilizados, de manera que sirva como un manual para el docente, optimizando su tiempo de enseñanza.

- El presente proyecto estableció un manual para el Docente, dicho documento consta de la resolución de las prácticas para el laboratorio de Networking, incluyendo los archivos de configuración de los equipos.

- Para cada práctica de Laboratorio se debe contar con todos los materiales necesarios para el desarrollo de la misma.

- Cada equipo del laboratorio necesita estar configurado con un nombre para que sea diferenciado.

- La utilización de contraseñas en los equipos es importante, para la seguridad de la Red.

- Cada equipo será puesto a la configuración por defecto después de cada práctica.

- Es necesario tener un respaldo de las configuraciones de los equipos.

AGRADECIMIENTO

Agradezco a Jesús por darme el privilegio de servirle aun en mis estudios, a mis padres por ser un apoyo incondicional y a mis amigos que siempre creyeron en mí.

Un profundo agradecimiento a la Escuela Politécnica del Ejército por ser una de las mejores universidades del país, donde aprendí a ser persona útil para la sociedad tanto en el crecimiento intelectual como personal.

A mis profesores que gracias a sus proyectos aprendí a trabajar por muchas horas seguidas y al momento de culminarlos sentir esa alegría única que da la satisfacción de decir, eso lo hice yo.

REFERENCIAS

[1]. "*SWITCH Y HUB, Informática hoy"*, http://www.informatica-hoy.com.ar/redes/Diferencias-entre-Hub-Switch-y-Router.php, Enero 2012

[2]. Jordi Palet, "*VLAN*", http://www.consulintel.es/Html/Tutoriales/Articulos/vlan.html, Enero 2012

[3]. "Redes de Área Local", http://www.masadelante.com/faqs/lan, Enero 2012

[4]. "*ROUTER VS SWITCH CAPA 3, Netstorming*" http://www.netstorming.com.ar/2009/12/14/router-vs-switch-de-capa-3/, Enero 2012

[5]. "*TELNET*", http://es.kioskea.net/contents/internet/telnet.php3, Enero 2012

[6]. "*SSH*", http://linux-cd.com.ar/manuales/rh9.0/rhl-rg-es-9/ch-ssh.html, Enero 2012

[7]. "*Quality of Service*", http://www.dte.us.es/personal/mcromero/masredes/docs/SMARD.0910.qos.pdf, Enero 2012

[8]. "*Rip Next Gen*", http://www.redescisco.net/v2/art/direccionamiento-basico-con-ipv6-ripng/, Junio 2012

BIOGRAFÍA DEL AUTOR

Mauricio Javier Tufiño Coloma

Nace el 10 de Agosto de 1986, en la ciudad de Quito, sus estudios primarios y secundarios los realizó en el Colegio Unidad Educativa "La Salle" de la ciudad de Quito, donde se graduó con el título de Bachiller en Ciencias Experimentales.

Obtuvo el título de Ingeniero Electrónico especialidad Redes y Comunicación de Datos en la Escuela Politécnica del Ejército en el año 2013.