ESCUELA POLITÉCNICA DEL EJÉRCITO

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA EN
ELECTRÓNICA, REDES Y COMUNICACIÓN DE DATOS

PROYECTO DE GRADO PARA LA OBTENCIÓN DEL TÍTULO DE INGENIERÍA

DESARROLLO DE GUÍAS PARA EL DISEÑO E IMPLEMENTACIÓN DE REDES LOCALES VIRTUALES, ACCESO REMOTO Y AUTENTICACIÓN EN UN ENTORNO LAN

MAURICIO JAVIER TUFIÑO COLOMA

SANGOLQUÍ – ECUADOR
2013

CERTIFICACIÓN

Certificamos que el presente proyecto de grado titulado: DESARROLLO DE GUÍAS PARA EL DISEÑO E IMPLEMENTACIÓN DE REDES LOCALES VIRTUALES, ACCESO REMOTO Y AUTENTICACIÓN EN UN ENTORNO LAN, ha sido desarrollado en su totalidad por el señor MAURICIO JAVIER TUFIÑO COLOMA, bajo nuestra dirección

Atentamente

Ing. Carlos Romero G.	Ing. Fabián Sáenz E.
DIRECTOR	CODIRECTOR

RESUMEN

Un dispositivo muy utilizado para interconectar computadoras en redes locales era el HUB, con la aparición del SWITCH se mejoró notablemente el rendimiento de la Red y la aparición de funciones avanzadas como es la creación de redes locales virtuales, autenticación y acceso remoto.

En el presente proyecto se desarrolló guías de laboratorio para el diseño e implementación de redes locales virtuales, autenticación y acceso remoto en un entorno LAN, se desarrollaron el total de 19 guías prácticas de la cuales 3 guías son simulaciones que el estudiante podrá realizar desde su hogar utilizando herramientas como son los simuladores de Red.

Los Equipos de laboratorio fueron separados según sus funciones o características avanzadas, de esta manera las guías de laboratorio fueron diseñadas con el fin de aumentar su nivel de complejidad.

Todas las guías constan de un formato específico, la cual será una herramienta muy importante para que los estudiantes desarrollen sus conocimientos en el ámbito de redes locales virtuales, autenticación y acceso remoto.

Se desarrolló un manual en el cual consta el direccionamiento, procedimiento y resultados de cada una de las guías previamente diseñadas, esto permitirá la optimización del tiempo de enseñanza del docente.

DEDICATORIA

El presente proyecto dedico a Dios por ser el autor y consumador de mi Fe, “Y si alguno de vosotros tiene falta de sabiduría, pídala a Dios, el cual da a todos abundantemente y sin reproche, y le será dada.” Santiago 1:5. A mis Padres y familiares que siempre han creído en mí y me han dado el apoyo necesario para seguir adelante a pesar de las adversidades.

AGRADECIMIENTOS

Agradezco a Dios por su hijo Jesús “Porque de tal manera amó Dios al mundo, que ha dado a su Hijo unigénito, para que todo aquel que en él cree, no se pierda, mas tenga vida eterna.” Juan 3:16 y por darme el privilegio de seguirle y servirle.

A mis Padres Mauricio Javier Tufiño Mateus y Eva Adriana Coloma Narváez que siempre han confiado en mí y han sido parte importante de este crecimiento profesional sin ellos no hubiera alcanzado mis metas como estudiante.

A mis hermanas Liset, Maria Soledad, Carolina y Anael han estado conmigo en las buenas y en las malas dándome consejos sabios.

A mi abuelita que con mucho cariño le decimos “Maruja” y mis abuelitos Guillermo Tufiño e Hilda de Tufiño que siempre me reciben con amor y están prestos a escucharme.

A mis familiares como son mis primos, tíos, sobrinos, cuñados.

A mis amigos que permiten que mi vida sea mejor cada día como son: Christian Salas, Vladimir Vizuete, Sebastián Córdova, Tito Álvarez, Christian Cisneros, Lesli Cadena y amigos del colegio/universidad/iglesia/infancia recordarles que siempre van a estar en mi corazón.

Por último pero no menos importante a mi Director Ing. Carlos Romero y Codirector Ing. Fabián Sáenz por sus enseñanzas y tiempo dedicado en la realización de este proyecto.

Mauricio Javier Tufiño Coloma

PRÓLOGO

El dispositivo más utilizado en redes locales es el SWITCH y viendo la necesidad de formar profesionales en el área de redes de información, la elaboración de guías prácticas permitirá al estudiante del Departamento de Electrónica, la posibilidad de entrenarse antes de salir al campo laboral.

Estas guías están orientadas al diseño de redes jerárquicas, creación de redes locales virtuales, acceso remoto y autenticación.

La autenticación en los equipos permite que el acceso al equipo o a un servicio de red sea hecho por la persona autorizada, por lo que se quiere abarcar una guía práctica que permita al estudiante dar seguridad a su red.

Este proyecto pretende servir como complemento del aprendizaje de los estudiantes de la carrera de Ingeniería Electrónica Redes y Comunicación de datos, para sustentar la parte teórica con prácticas de laboratorio donde se afiance todos los conocimiento impartidos por el docente en las respectivas materias, a fin de alcanzar el éxito a corto, mediano y largo plazo de sus estudiantes enfocados al cumplimiento de la visión y misión de la ESPE.

Si bien se han realizado proyectos para la realización de guías prácticas en el Área de Redes de Información, ninguno abarca las temáticas que se pretenden realizar en el presente proyecto como son la creación de redes locales virtuales, acceso remoto y autenticación en un entorno LAN.

ÍNDICE DE CONTENIDO

CAPÍTULO 1

CAPÍTULO 2

CAPÍTULO 3

ÍNDICE DE FIGURAS

CAPÍTULO 1

CAPÍTULO 2

CAPÍTULO 3

CAPÍTULO 4

ÍNDICE DE TABLAS

CAPÍTULO 1

CAPÍTULO 2

GLOSARIO

LAN	Local Area Network
VLAN	Virtual LAN
STP	Spanning Tree Protocol
DHCP	Dynamic Host Configuration Protocol
SNMP	Simple Network Management Protocol
QoS	Quality of Service
TELNET	Telecommunication Network
SSH	Secure Shell
AAA	Authentication Authorization Accounting
ACL	Access List
IP	Internet Protocol
IETF	Internet Engineering Task Force
ITU	International Telecommunication Union
RFC	Request for Comments
OSPF	Open Shortest Path First
RIP	Routing Information Protocol
OSI	Open System Interconnection
UDP	User Datagram Protocol
TCP	Transmission Control Protocol
PoE	Power over Ethernet

CAPÍTULO 1

MARCO TEÓRICO

1.1. 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. La siguiente evolución para la interconexión de dispositivos de red es el Switch, 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]*

Con el aparecimiento de los *Switch* capa 2 y capa 3 se agregan nuevas funcionalidades avanzadas para la creación y administración de redes de Área Local (LAN).con características de alta disponibilidad y redundancia. La correcta utilización de todas las funcionalidades de los *Switch* en el campo laboral permite la creación de redes virtuales, segmenta de manera lógica las redes corporativas.

Los Laboratorios de *Networking* y Redes y Comunicación de Datos de La Escuela Politécnica del Ejército cuentan con equipos de conectividad para *LANs* como son los *Switch* de diversas marcas y características, los cuales por el tiempo limitado para su uso en las diferentes asignaturas del Área de Redes de Información, no se ha podido explotar todas sus funcionalidades avanzadas. Por este motivo se ve la necesidad de desarrollar guías prácticas que abarquen las funcionalidades avanzadas 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.

Estas guías están orientadas al diseño de redes jerárquicas, creación de redes locales virtuales, acceso remoto y autenticación.

La autenticación en los equipos permite que el acceso al equipo o a un servicio de red sea hecho por la persona autorizada, por lo que se quiere abarcar una guía práctica que permita al estudiante dar seguridad a su red.

Este proyecto pretende servir como complemento del aprendizaje de los estudiantes de la carrera de Ingeniería Electrónica, para sustentar la parte teórica con prácticas de laboratorio donde se afiance todos los conocimiento impartidos por el docente en las respectivas materias, a fin de alcanzar el éxito a corto, mediano y largo plazo de sus estudiantes enfocados al cumplimiento de la visión y misión de la ESPE.

Si bien se han realizado proyectos para la realización de guías prácticas en el Área de Redes de Información, ninguno abarca las temáticas que se pretenden realizar en el presente proyecto.

1.1.1. Conceptos y Definiciones de una LAN

La *LAN* o también conocida como red de área local de sus siglas en inglés (Local Area Network), es una red que permite conectar los [1]ordenadores en un área relativamente pequeña y predeterminada (como una habitación, un edificio, o un conjunto de edificios).

Las estaciones de trabajo y los ordenadores personales en oficinas normalmente están conectados en una red *LAN*, lo que permite que los usuarios envíen o reciban archivos con el fin de compartir recursos (Aplicaciones, herramientas, dispositivos). La Figura 1.1. Nos muestra la topología de una red *LAN*.

[1] **Ordenador:** Es una máquina programable. Todos los ordenadores de uso general requieren los siguientes componentes (Memoria, CPU, Dispositivo de Entrada/Salida/Almacenamiento)

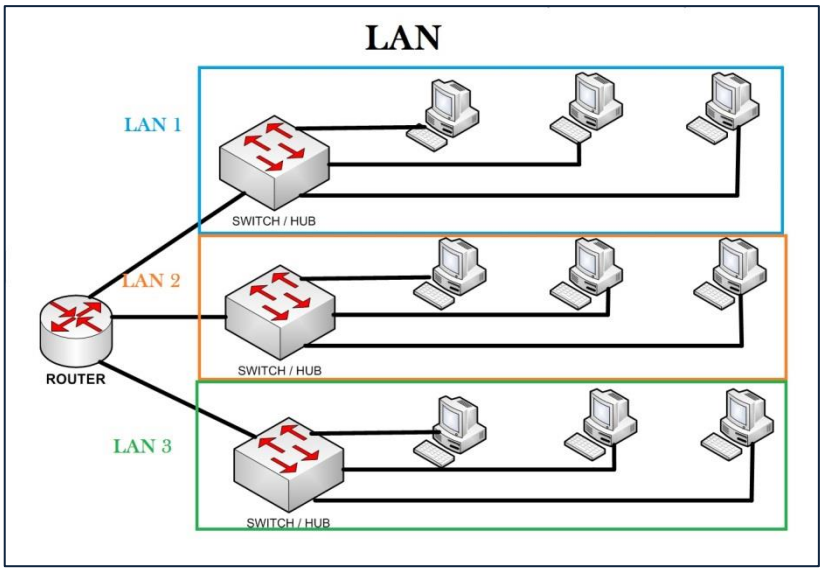


Figura 1.1. Topología de una Red LAN

1.1.2. Conceptos y Definiciones de una 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 [2] *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 (como departamentos de una empresa)." [2]* La Figura 1.2. Nos muestra la topología de una red *VLAN*.

[2] C**onmutador** o **switch** es un dispositivo de interconexión de redes de computadores. Su función es interconectar dos o más segmentos de red.

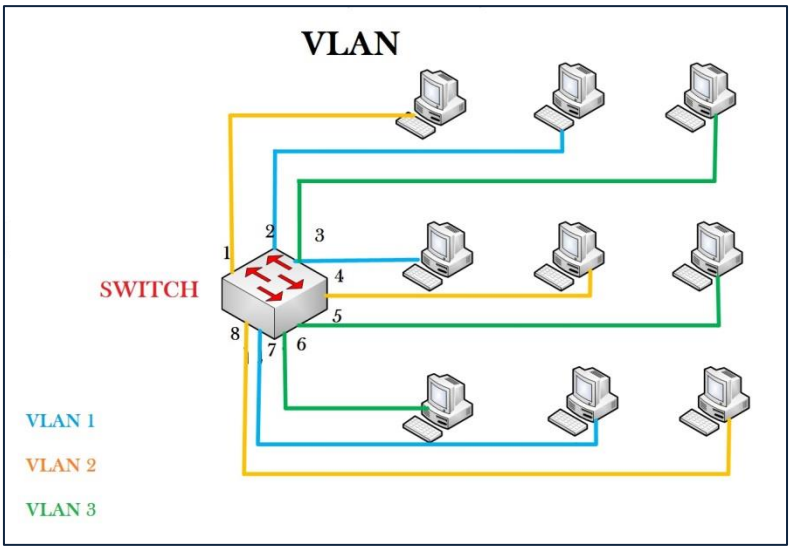


Figura 1.2. Topología de una Red Virtual VLAN

1.2. DISEÑO DE UNA RED LAN

En pequeñas y medianas empresas, la comunicación digital de datos, voz y video es esencial para la supervivencia de la empresa. Por lo tanto, una red *LAN* con un diseño apropiado es un requisito fundamental para el crecimiento de la empresa. El administrador de Red debe tener la capacidad de reconocer una *LAN* bien diseñada y seleccionar los dispositivos apropiados para admitir las especificaciones de las redes de una empresa pequeña o mediana.

1.2.1. Modelo de Redes Jerárquicas

El diseño de una *LAN* que satisfaga las necesidades de empresas pequeñas o medianas tiene más probabilidades de ser exitosa si se utiliza 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.

"*El diseño de redes jerárquicas implica la división de la red en capas independientes. Cada capa cumple funciones específicas que definen su rol dentro de la red general. La separación de las diferentes funciones existentes en una red hace que el*

diseño de la red se vuelva modular y esto facilita la escalabilidad y el rendimiento." [3] El modelo de diseño jerárquico típico se separa en tres capas: capa de acceso, capa de distribución y capa núcleo como muestra la Figura 1.3.

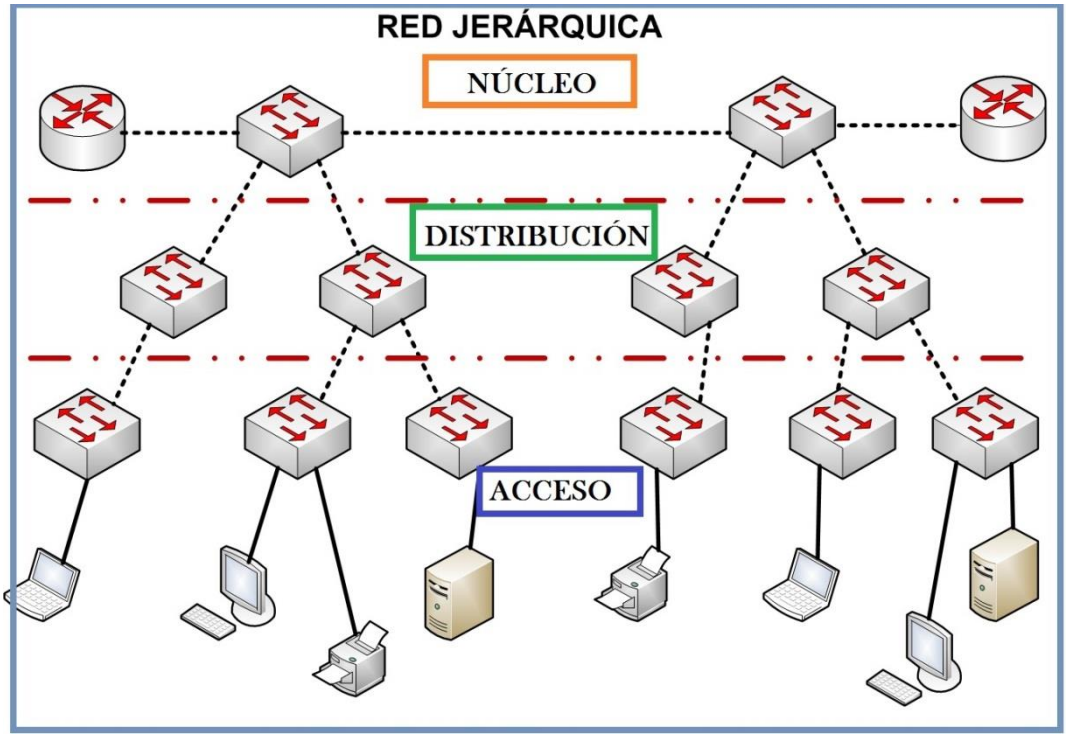


Figura 1.3. Modelo de Redes Jerárquico

1.2.1.1. Capa de Acceso

En la capa de acceso estan los dispositivos finales como las PC, impresoras y teléfonos IP, para proveer acceso al resto de la red. Esta capa de acceso puede incluir *routers*, *switches*, *bridges*, *hubs* y puntos de acceso inalámbricos. El propósito principal de la capa de acceso es aportar un medio de conexión de los dispositivos a la red y controlar qué dispositivos pueden comunicarse en la red.

1.2.1.2. Capa de Distribución

La capa de distribución controla el flujo de tráfico de la red con el uso de políticas y traza los dominios de *broadcast* al realizar el enrutamiento de las funciones entre las *LAN* virtuales (*VLAN*) definidas en la capa de acceso. Las *VLAN* permiten al usuario segmentar el tráfico sobre un *Switch* en subredes separadas. Por ejemplo, en una universidad el

Administrador de Red podría separar el tráfico según se trate de profesores, estudiantes e invitados. Normalmente, los *switches* de la capa de distribución son dispositivos que presentan disponibilidad y redundancia altas para asegurar la fiabilidad.

1.2.1.3. Capa de Núcleo/Core

La capa núcleo en el diseño jerárquico es el *backbone* de alta velocidad de la *internetwork*. La capa núcleo es esencial para la inter conectividad entre los dispositivos de la capa de distribución, por lo tanto, es importante que el núcleo sea sumamente disponible y redundante. El área del núcleo también puede conectarse a los recursos de Internet. El núcleo agrega el tráfico de todos los dispositivos de la capa de distribución, por lo tanto debe poder reenviar grandes cantidades de datos rápidamente.

1.2.2. Beneficios de una Red Jerárquica

Los beneficios que proporcionan el diseño de redes jerárquicas se pueden enlistar de la siguiente manera:

1. RENDIMIENTO.
2. ESCALABILIDAD.
3. SEGURIDAD.
4. REDUNDANCIA.
5. FACIL ADMINISTRACIÓN.

1.2.2.1. Rendimiento

El rendimiento de la comunicación mejora al evitar la transmisión de datos a través de *switches* intermediarios de bajo rendimiento. Los datos se envían a través de enlaces del puerto del *Switch* agregado desde la capa de acceso a la capa de distribución casi a la velocidad de cable en la mayoría de los casos. Luego, la capa de distribución utiliza sus capacidades de conmutar el alto rendimiento para reenviar el tráfico hasta el núcleo, donde

se enruta hacia su destino final. Debido a que las capas núcleo y de distribución realizan sus operaciones a velocidades muy altas, no existe contención para el ancho de banda de la red. Como resultado, las redes jerárquicas con un diseño apropiado pueden lograr casi la velocidad de cable entre todos los dispositivos.

1.2.2.2. Escalabilidad

La modularidad del diseño le permite reproducir exactamente los elementos del diseño a medida que la red crece. Debido a que cada instancia del módulo es consistente, resulta fácil planificar e implementar la expansión. Por ejemplo, si el modelo del diseño consiste en dos *switches* de la capa de distribución por cada 10 *switches* de la capa de acceso, puede continuar agregando *switches* de la capa de acceso hasta tener 10 switches de la capa de acceso interconectados con los dos *switches* de la capa de distribución antes de que necesite agregar *switches* adicionales de la capa de distribución a la topología de la red. Además, a medida que se agregan más *switches* de la capa de distribución para adaptar la carga de los *switches* de la capa de acceso, se pueden agregar *switches* adicionales de la capa núcleo para manejar la carga adicional en el núcleo.

1.2.2.3. Seguridad

Es posible configurar los *switches* de la capa de acceso con varias opciones de seguridad del puerto que proveen control sobre qué dispositivos se permite conectar a la red. Además, se cuenta con la flexibilidad de utilizar políticas de seguridad más avanzadas en la capa de distribución. Puede aplicar las políticas de control de acceso que definen qué protocolos de comunicación se implementan en su red y dónde se les permite dirigirse. Por ejemplo, si desea limitar el uso de HTTP a una comunidad de usuarios específica conectada a la capa de acceso, podría aplicar una política que bloquee el tráfico de HTTP en la capa de distribución. La restricción del tráfico en base a protocolos de capas más elevadas, como IP y HTTP, requiere que sus *switches* puedan procesar las políticas en esa capa. Algunos *switches* de la capa de acceso admiten la funcionalidad de la Capa 3, pero en general es responsabilidad de los *switches* de la capa de distribución procesar los datos de la Capa 3, porque pueden procesarlos con mucha más eficacia.

1.2.2.4. Redundancia

A medida que crece una red, la disponibilidad se torna más importante. Puede aumentar radicalmente la disponibilidad a través de implementaciones redundantes fáciles con redes jerárquicas. Los *switches* de la capa de acceso se conectan con dos *switches* diferentes de la capa de distribución para asegurar la redundancia de la ruta. Si falla uno de los *switches* de la capa de distribución, el switch de la capa de acceso puede conmutar al otro S*witch* de la capa de distribución. Adicionalmente, los *switches* de la capa de distribución se conectan con dos o más *switches* de la capa núcleo para asegurar la disponibilidad de la ruta si falla un *Switch* del núcleo. La única capa en donde se limita la redundancia es la capa de acceso. Habitualmente, los dispositivos de nodo final, como PC, impresoras y teléfonos IP, no tienen la capacidad de conectarse con *switches* múltiples de la capa de acceso para redundancia. Si falla un *Switch* de la capa de acceso, sólo se verían afectados por la interrupción los dispositivos conectados a ese *Switch* en particular. El resto de la Red puede funcionar sin inconvenientes.

1.2.2.5. Fácil Administración

Cada capa del diseño jerárquico cumple funciones específicas que son consistentes en toda esa capa. Por consiguiente, si necesita cambiar la funcionalidad de un *Switch* de la capa de acceso, podría repetir ese cambio en todos los *switches* de la capa de acceso en la red porque presumiblemente cumplen las mismas funciones en su capa.

1.3. CONMUTACIÓN CAPA 2 Y CAPA 3

Un *Switch LAN* que trabaja en la Capa 2 (Enlace de Datos) del modelo OSI lleva a cabo los procesos de conmutación y filtrado basándose solamente en la dirección MAC. El *Switch* de Capa 2 es completamente transparente para los protocolos de la red y las aplicaciones del usuario. Un *Switch* de Capa 2 crea una tabla de direcciones MAC que utiliza para determinar los envíos.

Un *Switch* de Capa 3 funciona de modo similar al *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. En lugar de aprender qué direcciones MAC están vinculadas con cada uno de sus puertos, el *Switch* de Capa 3 puede también conocer qué direcciones IP están relacionadas con sus interfaces. Esto permite que el S*witch* de Capa 3 pueda dirigir el tráfico a través de la red en base a la información de las direcciones IP.

Los *switches* de Capa 3 son también capaces de llevar a cabo funciones de enrutamiento de Capa 3, con lo cual se reduce la necesidad de colocar *routers* dedicados en una LAN. Dado que los *switches* de Capa 3 cuentan con un hardware de conmutación especializado, normalmente, pueden enviar datos con la misma rapidez con la que pueden conmutar.

1.3.1. Comparación entre el *Switch* Capa 3 y el *Router*

El *Switch* de Capa 3 puede enviar paquetes entre distintos segmentos de una LAN de modo similar que los *routers* dedicados. Sin embargo, el S*witch* de Capa 3 no reemplaza completamente la necesidad de utilizar *routers* en una red.

Los *routers* proporcionan servicios adicionales de Capa 3 que el *switch* de Capa 3 no puede realizar. Los *routers* también pueden llevar a cabo tareas de reenvío de paquetes que no realiza el *switch* de Capa 3, como establecer conexiones de acceso remoto con dispositivos y redes remotas. Los *routers* dedicados son más flexibles en cuanto a la admisión de tarjetas de interfaz *WAN* (*WAN Interface Cards*).

El *switch* de Capa 3 ofrece funciones básicas de enrutamiento en una LAN y reduce la necesidad de utilizar routers dedicados. En la siguiente Tabla 1.1. Veremos las diferencias entre el *Switch* de Capa 3 y el *Router*.

Tabla 1.1. Comparación 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	✓	✗

1.4. VLAN

Anteriormente dimos un concepto de lo que es una *VLAN*, algunos de las ventajas que nos brinda son:

- SEGURIDAD.
- RENDIMIENTO.
- COSTO.
- FÁCIL ADMINISTRACIÓN.

SEGURIDAD: La información se encapsula en un nivel adicional, los grupos que tienen datos sensibles se separan del resto de la red, disminuyendo las posibilidades de que ocurran violaciones de información confidencial.

RENDIMIENTO: Al dividir las redes en diferentes grupos lógicos permite que no se envíe tráfico innecesario a la red, esto potencia el rendimiento.

COSTO: Reducen los costes administrativos asociados con el traslado adiciones o cambios. Las capacidades de las *VLAN* están, por lo general, incluidas en el precio de los conmutadores que las ofrecen, y su uso no requiere cambios en la estructura de la red o cableado, sino más bien los evitan, facilitando las reconfiguraciones de la red sin costes adicionales.

FÁCIL ADMINISTRACIÓN: Cada *VLAN* es creada con una función específica esto ayuda al administrador de Red que la adición de usuarios o grupos de usuarios sea fácil.

1.4.1. 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.

1.4.1.1. VLAN Basada en Puerto

Consiste en una agrupación de puertos físicos que puede tener lugar sobre un conmutador o también, en algunos casos, sobre varios conmutadores.

1.4.1.2. VLAN Basada en Protocolo

Se asigna a cada VLAN un protocolo diferente dejando al *Switch* el trabajo de enviar la trama a la interfaz correspondiente.

1.4.1.3. VLAN Basada en Dirección IP

Está basado en el encabezado de la capa 3 (RED) del modelo OSI. Hace un mapeo de direcciones IP y permite entrar a la *VLAN* únicamente las direcciones IP que estén autorizadas.

1.4.1.4. VLAN Basada en Nombre de Usuario

Se basan principalmente por la autenticación del usuario y no en las direcciones MAC de los dispositivos.

1.4.2. 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*. Un enlace troncal de *VLAN* le permite extender las *VLAN* a través de toda una red.

Un enlace troncal de *VLAN* no pertenece a una *VLAN* específica, sino que es un conducto para las *VLAN* entre *switches y routers*.

Al mencionar de *VLAN* y Enlaces Troncales, existe un protocolo de encapsulamiento que forma parte de estos dos conceptos conocido como 802.1Q. ¿Por qué es tan importante este protocolo 802.1Q?

1.4.2.1. El Problema

El problema en una Red *LAN* es transportar tráfico de varias *LAN* sobre *Ethernet*. La Figura1.4. Indica por donde pasaría el tráfico de varias *LAN* sobre Ethernet.

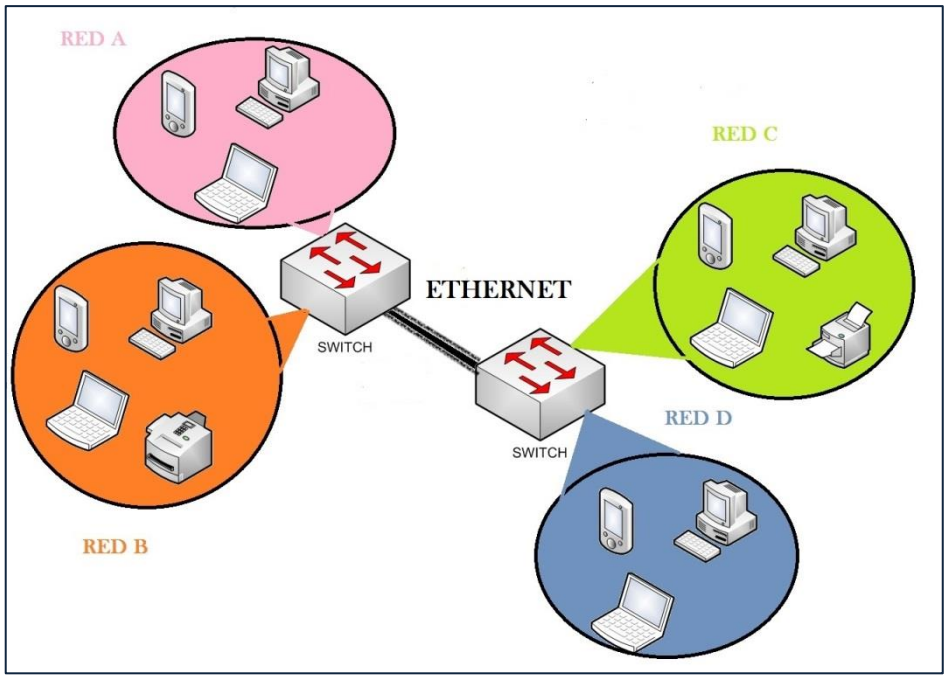


Figura 1.4. Tráfico varias LAN sobre Ethernet.

1.4.2.2. La Posible Solución

Una posible Solución al problema sería usar más enlaces Ethernet o utilizar *Routers*. La Figura 1.5. Nos muestra como puede ser la posible solución añadiendo más enlaces mientras que la Figura 1.6. Nos muestra la solución por medio del *Router*.

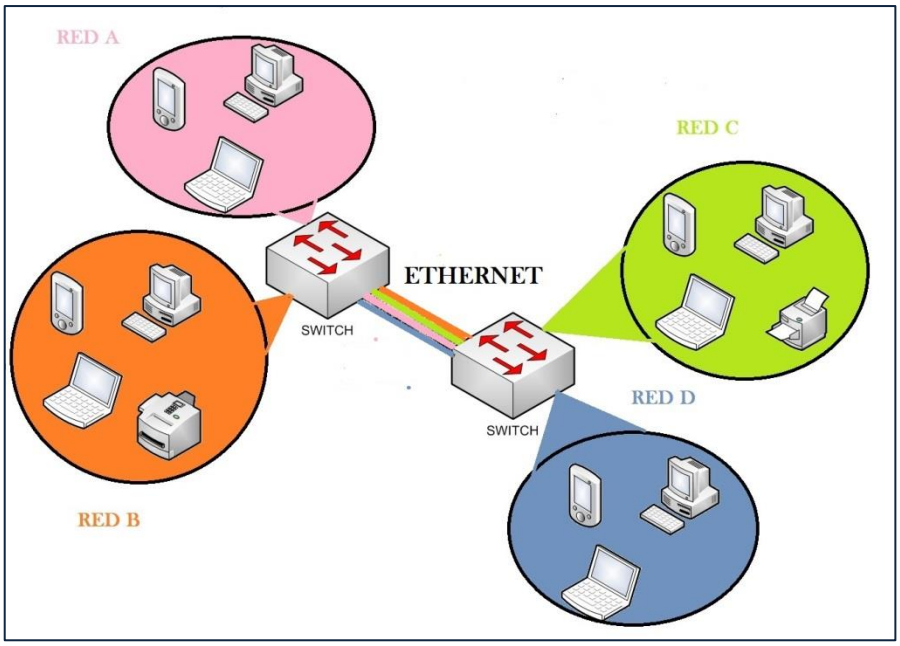


Figura 1.5. Solución uso de varios enlaces Ethernet.

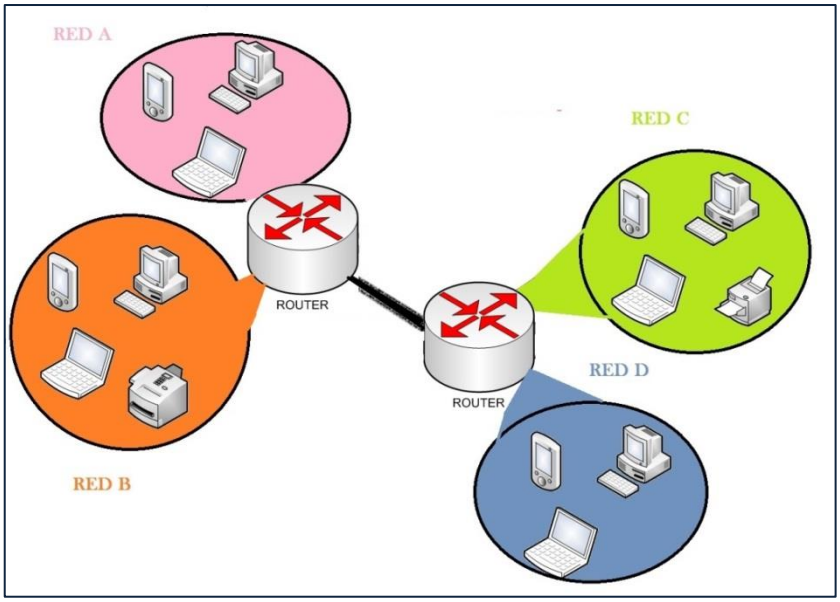


Figura 1.6. Solución uso de Routers.

1.4.2.3. La Solución

La solución óptima es utilizar el protocolo de encapsulamiento 802.1Q, Cada trama se marca con el id (identificador) de la LAN a la que pertenece. La Figura 1.7. indica cómo pueden viajar por Ethernet diferentes *LANs*.

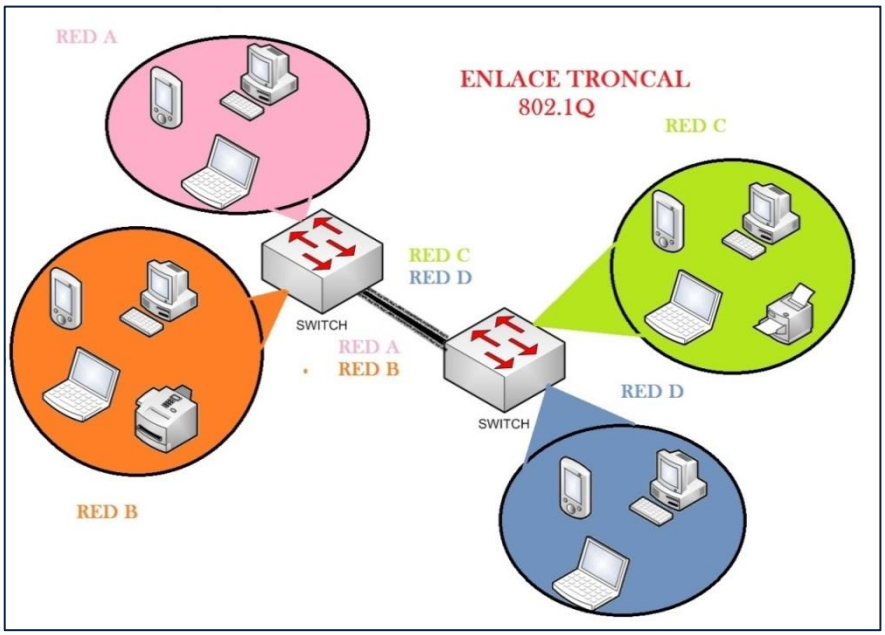


Figura 1.7. Solución utilizar protocolo 802.1Q, cada trama se marca con un id.

1.4.2.4. Trama 802.1Q

"El protocolo 802.1Q en realidad no encapsula la trama original sino que añade 4 bytes al encabezado Ethernet original. El valor del campo EtherType se cambia a 0x8100 para señalar el cambio en el formato de la trama.

Debido a que con el cambio del encabezado se cambia la trama, 802.1Q fuerza a un re cálculo del campo FCS (Frame Check Sum)." [4] La Figura 1.8. nos muestra el encabezado de la trama 802.1Q.

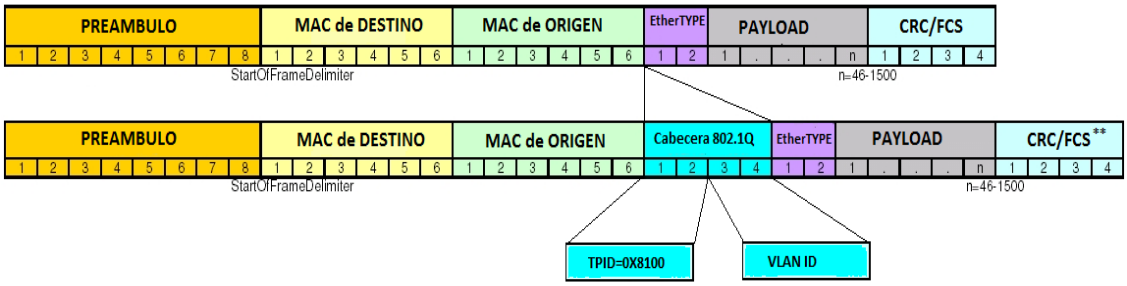


Figura 1.8. Trama IEEE 802.1Q.

Preámbulo Este campo tiene una extensión de 7 bytes que siguen la secuencia (10101010) permite informar a los dispositivos de Red que existe una trama.

StartOfFrameDelimiter Es un campo de 1 byte con la secuencia (10101011), que indica el comienzo de una trama.

Dirección de destino Es un campo 6 bytes que indica la dirección MAC del destino al cual se va a enviar la trama.

Dirección de origen Es un campo 6 bytes que indica la dirección MAC de origen al cual se va a enviar la trama.

Longitud. Este campo de 2 bytes codifica cuántos bytes contiene el campo de datos. Su valor oscila en un rango entre 0 y 1 500.

Datos. Es un campo que puede codificar entre 0 y 1500 bytes en donde se incluye la información de usuario procedente de la capa de red.

Relleno. La norma IEEE 802.3 específica que una trama no puede tener un tamaño inferior a 64 bytes, por tanto, cuando la longitud del campo de datos es muy pequeña se requiere rellenar este campo para completar una trama mínima de al menos 64 bytes. Es un campo que puede, por tanto, tener una longitud comprendida entre 0 y 46 bytes, de modo que la suma total de la trama sea al menos de 64 bytes.

CRC. Es el campo de 4 bytes que permite verificar la integridad de la trama.

TPID. Establecido al valor hexadecimal de 0x8100. Este valor se denomina valor de ID de protocolo de etiqueta (TPID, por su sigla en inglés). Con el campo EtherType configurado al valor TPID, el switch que recibe la trama sabe buscar la información en el campo de VLAN ID.

VLAN ID. Es un número que permite identificar una VLAN.

1.5. STP (SPANNING TREE PROTOCOL)

1.5.1. Redundancia en una Red

La redundancia de Capa 2 mejora la disponibilidad de la red implementando rutas de red alternas mediante el agregado de equipos y cables. Al contar con varias rutas para la transmisión de los datos en la red, la interrupción de una ruta simple no genera impacto en la conectividad de los dispositivos en la red.

1.5.1.1. Funcionamiento de una Red Redundante

Paso 1. En la siguiente topología de red podemos observar 3 enlaces troncales. La Figura 1.9. Nos muestra una topología con enlaces redundantes.

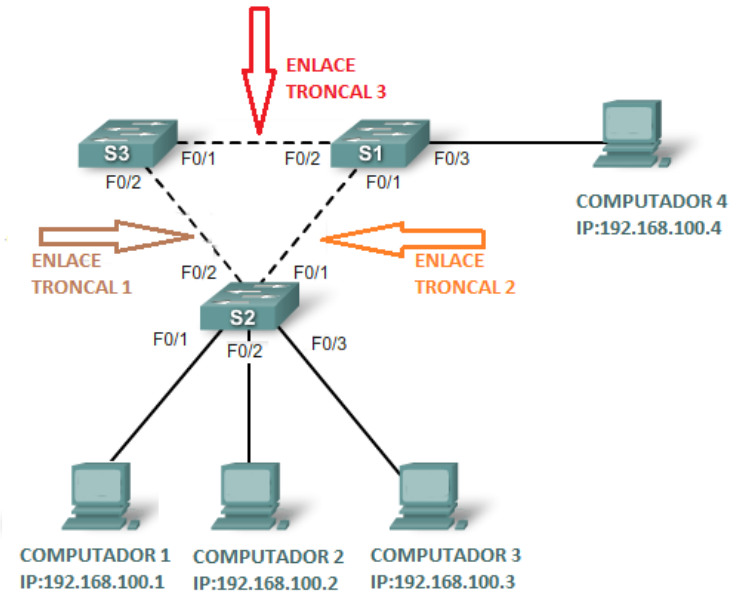


Figura 1.9. Topología de Red Redundante.

Paso 2. Si el computador 1 quiere enviar información al computador 4 el paquete viaja por la red a través del enlace troncal 2 como se muestra en la Figura 1.10.

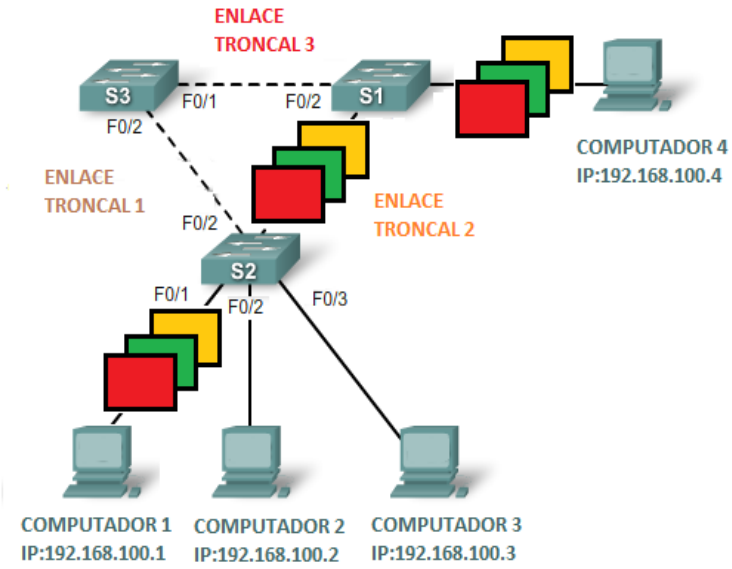


Figura 1.10. Envío de información por enlace troncal 2.

Paso 3. En caso que el enlace troncal 2 falle ya sea por malas condiciones del cable o por desactivación de la interface como muestra la Figura 1.11.

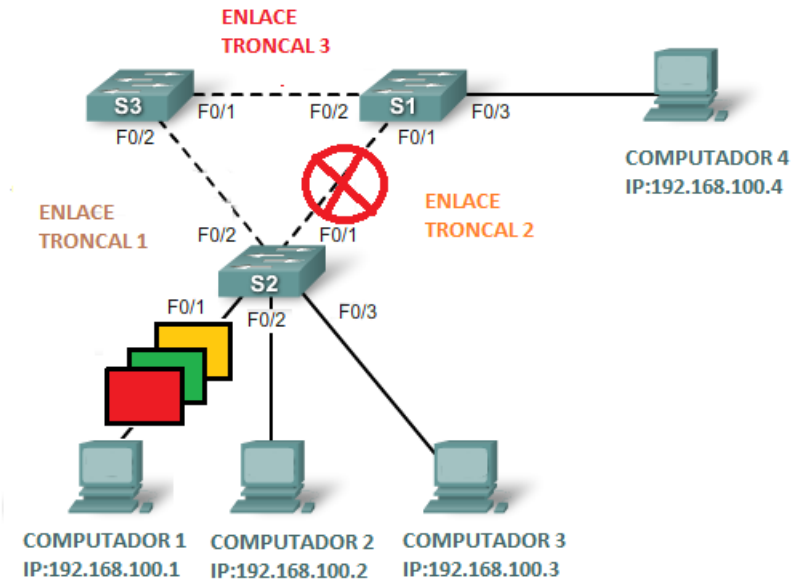


Figura 1.11. Fallo enlace troncal 2.

Paso 4. El enlace troncal 1 servirá como apoyo para que la información enviada desde el computador 1 hasta el computador 4 llegue de forma satisfactoria, como muestra la Figura 1.12.

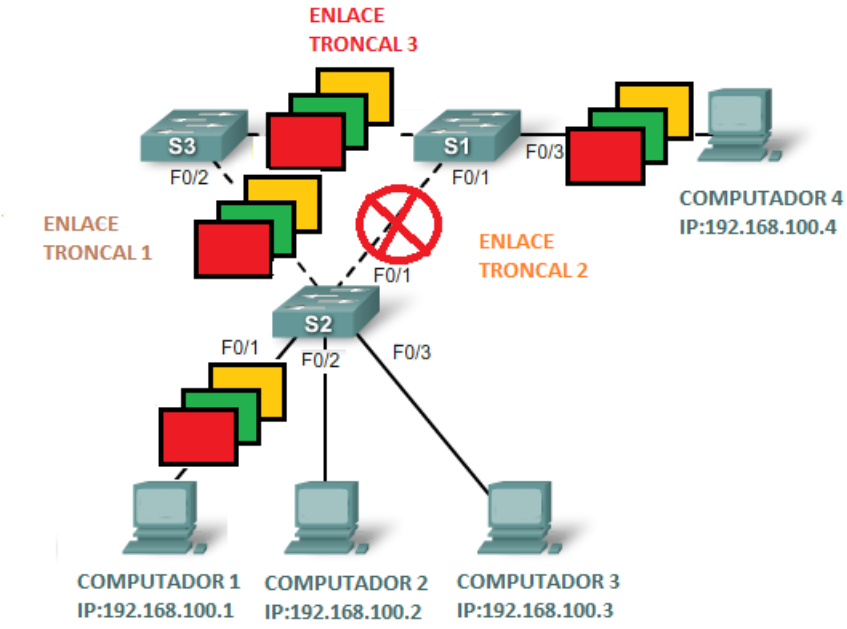


Figura 1.12. Envío de datos enlace troncal 1.

1.5.1.2. Bucles de Capa 2

La redundancia es una parte importante del diseño jerárquico. Pese a que es importante para la disponibilidad, existen algunas consideraciones que deben atenderse antes de que la redundancia sea posible en una red.

Cuando existen varias rutas entre dos dispositivos en la red y STP se ha deshabilitado en los *switches*, puede generarse un bucle de Capa 2. Si STP está habilitado en estos *switches*, que es lo que está predeterminado, el bucle de Capa 2 puede evitarse.

Las tramas de Ethernet no poseen un tiempo de existencia (*TTL, Time to Live*) como los paquetes IP que viajan por los *routers*. En consecuencia, si no finalizan de manera adecuada en una red conmutada, las mismas siguen rebotando de *switch* en *switch* indefinidamente o hasta que se interrumpa un enlace y elimine el bucle.

Las tramas de *broadcast* se envían a todos los puertos de *switch*, excepto el puerto de origen. Esto asegura que todos los dispositivos del dominio de *broadcast* puedan recibir la trama. Si existe más de una ruta para enviar la trama, se puede generar un bucle sin fin.

Paso 1. El computador 1 envía una trama de *broadcast* al *switch* S2. Cuando S2 recibe la trama de *broadcast* actualiza su tabla de direcciones MAC para registrar que el computador 1 está disponible en el puerto Fa0/1, como muestra la Figura 1.13.

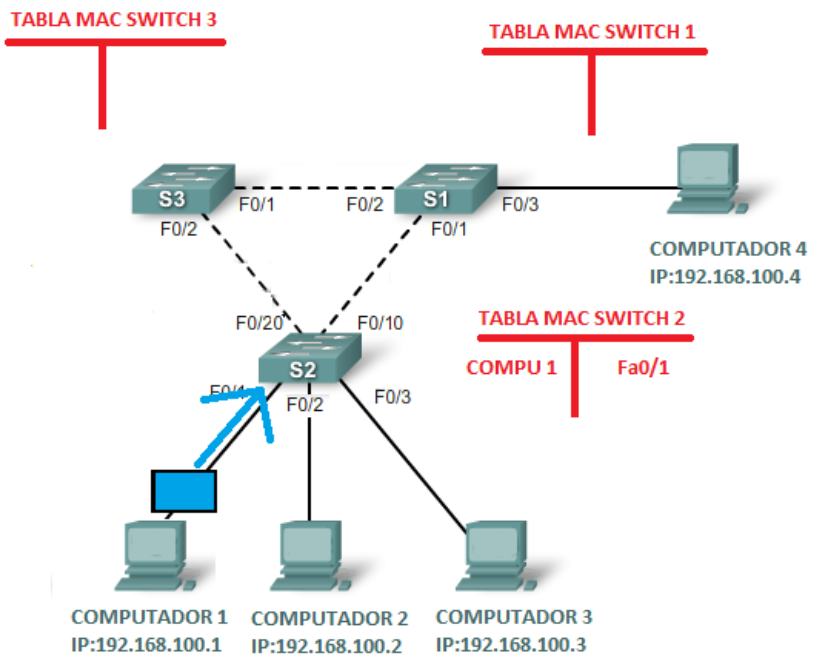


Figura 1.13. Envío trama de broadcast desde el computador 1 al Switch 2.

Paso 2. Ya que es una trama de *broadcast*, el *Switch* 2 envía la trama a todos los puertos de *switch*, incluido el Enlace troncal1 y el Enlace troncal2. Cuando la trama de *broadcast* llega a los *switches* S3 y S1, los mismos actualizan sus tablas de direcciones MAC para indicar que el computador 1 está disponible en el puerto F0/1 para S1 y en el puerto F0/2 para S3, como muestra la Figura 1.14.

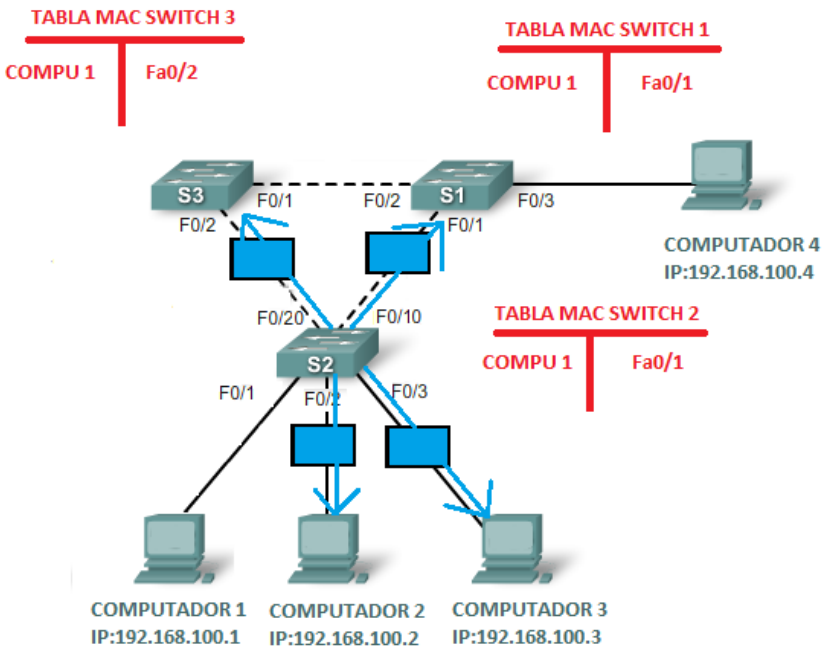


Figura 1.14. Envío trama de broadcast Switch 2 a todas sus interfaces.

Paso 3. Ya que es una trama de *broadcast*, el *Switch* S3 y S1 envían la trama a todos los puertos de *switch*, excepto quien envió la trama (*Switch* S2). S3 envía entonces la trama a S1 y viceversa. Cada *switch* actualiza su tabla de direcciones MAC con el puerto incorrecto para el Computador 1, como muestra la Figura 1.15.

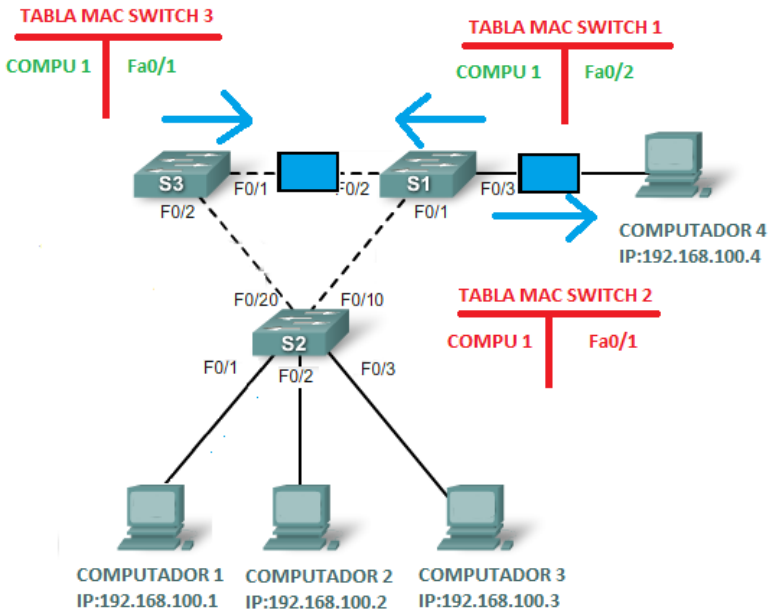


Figura 1.15. Envío trama de broadcast entre Switch 1 Switch 3.

Paso 4. De nuevo, cada *switch* envía la trama de *broadcast* a todos sus puertos, excepto aquel que la envió, lo que produce que ambos *switches* envíen la trama al *Switch* S2. Cuando S2 recibe las tramas de *broadcast* del *Switch* S3 y S1, la tabla de direcciones MAC vuelve a actualizarse, esta vez con la última entrada recibida de los otros dos *switches*, como se muestra en la Figura 1.16.

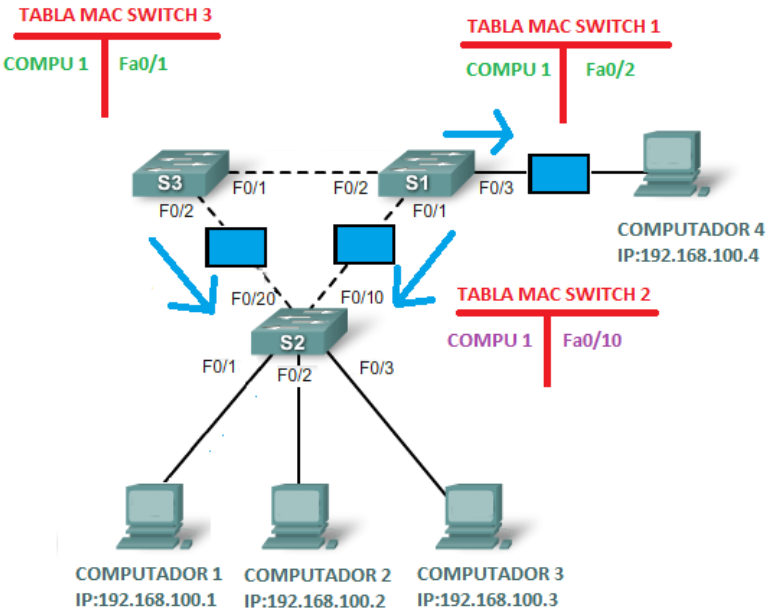


Figura 1.16. Envío trama de broadcast desde los Switch S1 y S3 al Switch 2.

Paso 5. Este proceso se repite indefinidamente hasta que se elimine el bucle mediante la interrupción física de las conexiones que lo producen o de la desconexión de uno de los *switches* del bucle como muestra la Figura 1.17.

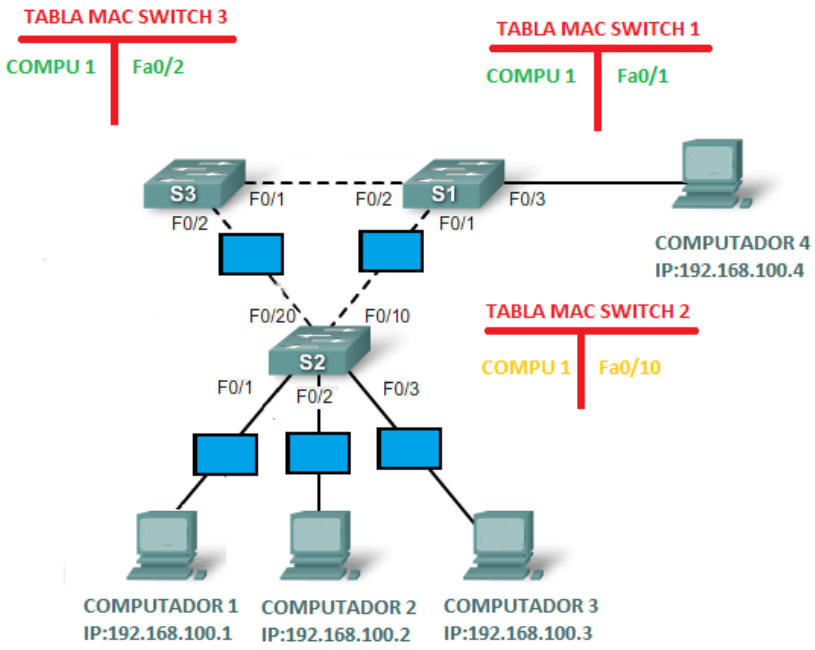


Figura 1.17. Repetición del Bucle en Capa 2.

1.5.2. STP Conceptos y Definiciones

La redundancia aumenta la disponibilidad de la topología de red al proteger la red de un único punto de falla, como un cable de red o switch que fallan. Cuando se introduce la redundancia en un diseño de la Capa 2, pueden generarse bucles y tramas duplicadas.

Los bucles y las tramas duplicadas pueden tener consecuencias graves en la red. El protocolo *spanning tree* (STP) fue desarrollado para enfrentar estos inconvenientes.

STP asegura que exista sólo una ruta lógica entre todos los destinos de la red, al bloquear de forma intencional aquellas rutas redundantes que puedan ocasionar un bucle.

El bloqueo de las rutas redundantes es fundamental para evitar bucles en la red. Las rutas físicas aún existen para proporcionar la redundancia, pero las mismas se deshabilitan para evitar que se generen bucles. Si alguna vez la ruta es necesaria para compensar la falla de un cable de red o de un *switch*, STP vuelve a calcular las rutas y desbloquea los puertos necesarios para permitir que la ruta redundante se active.

1.5.2.1. Trama BPDU

En la Figura 1.18, nos indica los campos que tiene una trama BPDU.

Figura 1.18. Trama BPDU.

ID PROTOCOLO: Indica el tipo de protocolo que se utiliza. Este campo contiene el valor de cero.

VERSIÓN: Indica la versión del protocolo. Este campo contiene el valor de cero.

TIPO DE MENSAJE: Indica el tipo de mensaje. Este campo contiene el valor de cero.

SEÑALADORES: El campo de señaladores puede tener 2 valores:

TC bit de cambio de topología indica un cambio de topología en el caso de que una ruta al puente raíz se haya interrumpido.

TCA bit de acuse de recibo se establece para confirmar que el bit **TC** está configurado.

ID de RAIZ (*ROOT*): Indica el puente Raíz enumerando su prioridad de 2 bytes seguida por su ID de su dirección MAC de 6 bytes. Cuando se inicia el Switch por primera vez, el ID de raíz es igual al ID de bridge. Sin embargo, a medida que se desarrolla el proceso de elección, el ID de bridge más bajo reemplaza al ID de raíz local para identificar al *switch* del puente raíz.

COSTO de la RUTA: Indica el costo de la ruta desde el puente que envía el mensaje de configuración al puente raíz. El campo costo de la ruta es actualizado por cada *switch* de la ruta al puente raíz, la Tabla 1.2. nos indica una comparación entre la velocidad y el costo.

Tabla 1.2. Equivalente Costo vs Ruta

VELOCIDAD	COSTO
10 Gbps	2
1 Gbps	4
100 Mbps	19
10 Mbps	100

ID de BRIDGE: Indica el ID de dirección MAC y de prioridad del puente que envía el mensaje. Esta etiqueta permite que el puente raíz identifique donde se originó el BPDU, así como las rutas múltiples desde el *switch* hasta el puente raíz. Cuando el puente raíz recibe más de un BPDU de un *switch* con distintos costos de ruta, reconoce que existen dos rutas diferentes y utiliza aquella ruta con el menor costo.

ID del PUERTO: indica el número del puerto desde el cual se envía el mensaje de configuración. Este campo permite que los bucles generados por bridge múltiples conectados sean detectados y corregidos.

ANTIGÜEDAD del MENSAJE: indica la cantidad de tiempo que ha transcurrido desde que la raíz envió el mensaje de configuración en el cual se basa el mensaje de configuración actual.

ANTIGÜEDAD MAXIMA: indica el momento en que el mensaje de configuración actual debe ser eliminado. Una vez que la antigüedad del mensaje alcanza la antigüedad máxima, el *switch* elimina la configuración actual e inicia una nueva elección para determinar un puente raíz nuevo, ya que asume que ha sido desconectado del mismo. Este valor está predeterminado en 20 segundos, peri puede ajustarse a intervalos entre 6 y 40 segundos.

HELLO TIME: Indica el tiempo entre los mensajes de configuración del puente raíz. El intervalo define la cantidad de tiempo que el puente raíz espera para enviar BPDU de mensajes de configuración. Este valor está predeterminado en 2 segundos pero puede ajustarse a intervalos entre 1 y 10 segundos.

FORWARD DELAY: Indica la cantidad de tiempo que los puentes deben esperar antes de sufrir la transición a un nuevo estado luego de un cambio de topología. Si la transición de un puente es muy repentina, es posible que no todos los enlaces de la red estén preparados para cambiar sus estados, lo que puede generar bucles. Este valor es igual a 15 segundos de manera predeterminada para cada estado pero puede ajustarse a intervalos entre 4 y 30 segundos.

1.5.2.2. Algoritmo STP

"STP utiliza el algoritmo spanning tree (STA) consiste en la construcción de un árbol a partir de la definición de un switch raíz (root). Cuando un switch se habilita por primera vez, se anuncia como root a la red. En ese momento, se produce el envío de tramas BPDU (Bridge Protocol Data Unit) por parte de todos los switches de la red, cuya

finalidad es elegir el switch root que será el que tenga la ID más baja (MAC + Prioridad). "[5]

Los puertos de los switch son definidos de una de las siguientes maneras:

Puerto raíz: el que asegura el camino con menor costo hacia el root.

Puerto designado: uno solo por cada segmento de red, asegura que ese switch ofrece el camino de menor coste hacia el root.

Puerto bloqueado: no permiten el paso de tramas Ethernet, sólo escuchan BPDU.

El *switch* definido como *root* tendrá todos sus puertos designados. Cada 2 segundos (*Hello* Time), el *root* envía una trama BPDU anunciándose como *switch* raíz para mantener la topología en árbol. Cuando un *switch* recibe una BPDU con un ID mayor que el suyo, intenta convertirse en raíz y envía BPDU en las que el ID de la raíz es su propio identificador.

Por otro lado, si un *switch* recibe una BPDU con coste hacia el *root* mayor del que él ofrece, intenta convertirse en designado. El algoritmo converge cuando todos los puertos de los *switches* están en estado de bloqueo o envío.

Los diferentes estados por los que puede pasar un puerto de un *switch* son:

Bloqueo: En este estado sólo se procesan BPDU. Las tramas de datos se descartan.

Escucha: Los *switches* sólo reciben BPDU y determinan si existen otras rutas hacia el *root*. Si reciben una BPDU en la que el coste hacia el *root* es menor del que ellos pueden ofrecer, pasan a estado de Bloqueo, de lo contrario, pasan a Aprendizaje. En este estado se descartan las tramas Ethernet.

Aprendizaje: Los *switches* procesan las BPDU y empiezan a aprender las direcciones MAC para llenar sus tablas. Las tramas de datos se siguen descartando en este estado.

Envío: se procesan las BPDU y se envían las tramas de datos.

También se siguen actualizando las tablas de direcciones MAC.

La convergencia del árbol STP puede tardar hasta 60 segundos. Por ello, se han diseñado nuevos protocolos como el Rapid-STP (definido en el IEEE 802.1W), el cual converge en cuestión de milisegundos ya que define dos nuevos estados para los puertos, alternativo y respaldo, los cuales son activados rápidamente ante la caída de un enlace.

Además incluye la definición de *edge-port* en aquellos puertos que se sabe que nunca serán conectados hacia otro *switch*, de manera que evita pasar por el estado de escucha y aprendizaje, pasando directamente de bloqueo a envío.

1.5.3. Ejemplo STP

Paso 1. Todos los conmutadores envían las tramas BPDU a todas las interfaces auto-proclamándose Conmutador Raíz. (*Root Bridge*). Los BPDU son enviados periódicamente para determinar la topología, como muestra la Figura 1.19.

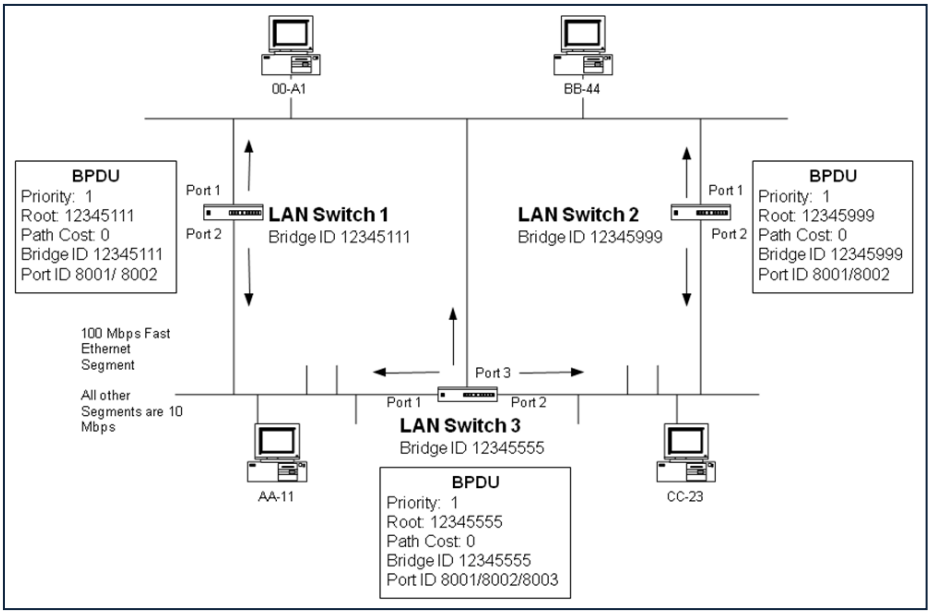


Figura 1.19. Envío BPDU entre todos los Switch.

Paso 2. En la Figura 1.20. Los *Switch* 1 y 3 comparan sus valores de conformidad con el STA.

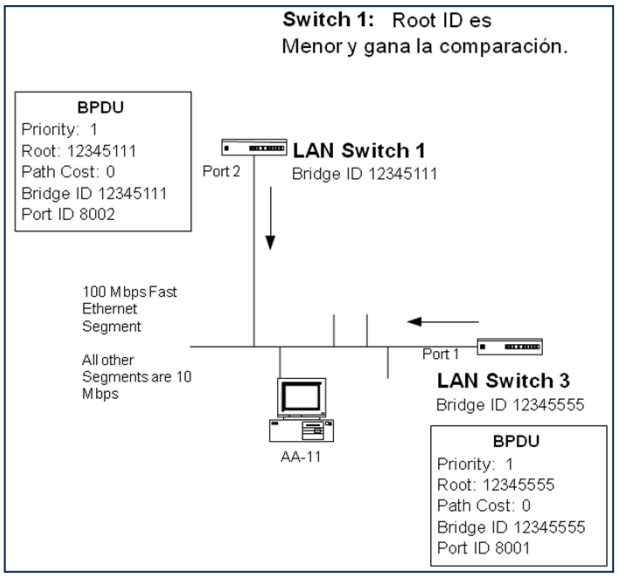


Figura 1.20. Comparación BPDU Switch 1 y Switch 3.

Paso 3. En la Figura 1.21. Los *switches* 2 y 3 comparan sus valores de conformidad con el STA.

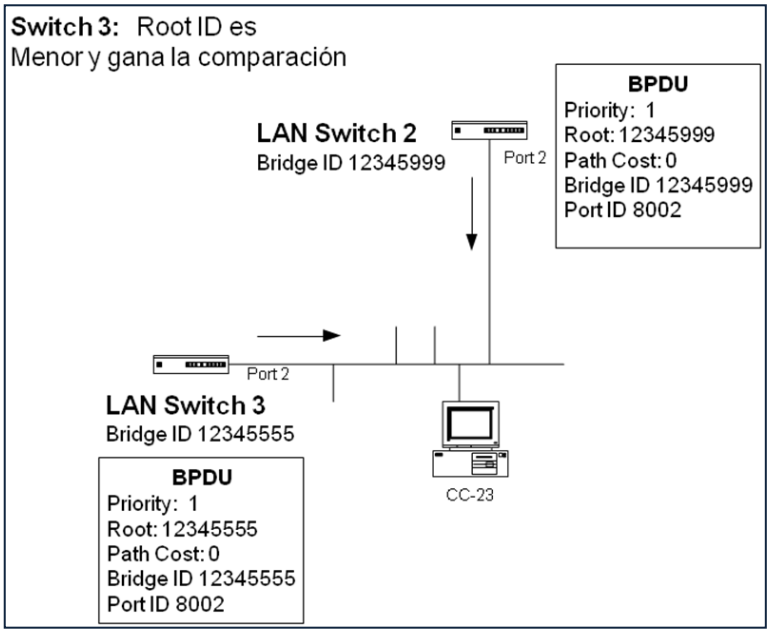


Figura 1.21. Comparación BPDU Switch 2 y Switch 3.

Paso 4. En la Figura 1.22. Los *switches* 1, 2 y 3 comparan sus valores de conformidad con el STA.

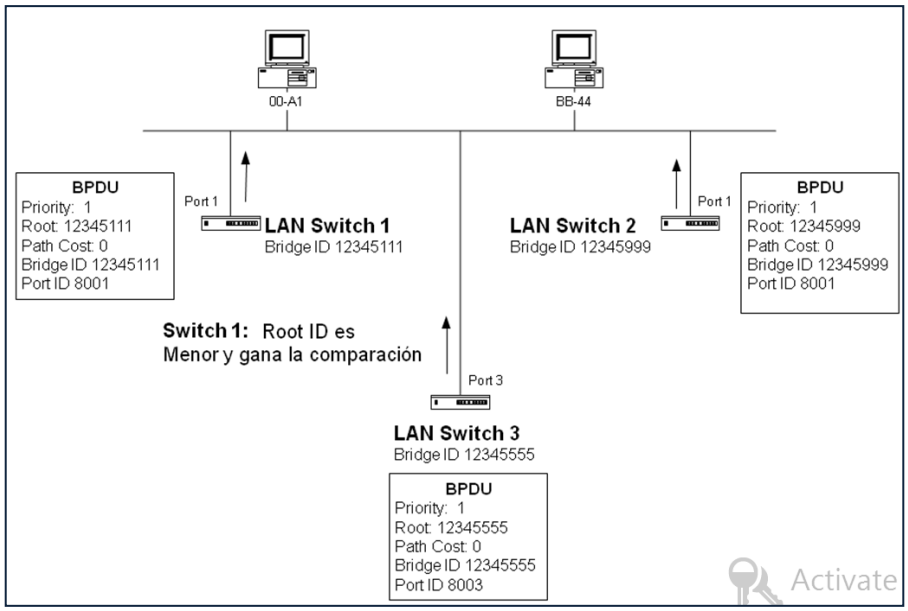


Figura 1.22. Comparación BPDU Switch 1, Switch 2 y Switch 3.

Paso 5. En la Figura 1.23. El *Root* ID del *Switch* 1 es menor que el de los *switches* restantes. El *Switch* 1 gana. Todos los enlaces paralelos deben de discriminarse cual estará en estado de reenvío y cual en estado de bloqueo, utilizando el mismo criterio de selección. Para cada segmento seleccionará un *switch* basado en el costo del ROOT y en el Bridge ID. (*Switch* 3 utilizará el Port 1 debido al costo del *Root*.)

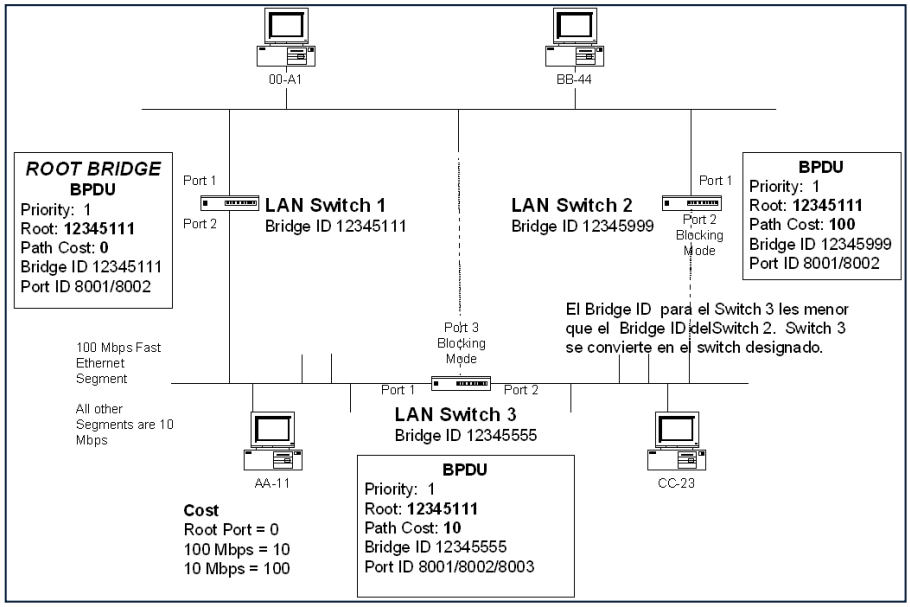


Figura 1.23. Asignación Switch 1 como ROOT.

1.6. 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.

Otra de las ventajas de esta solución es el aumento de la productividad laboral al permitir la movilidad a los profesionales en Redes.

1.6.1. TELNET

*"Telnet (**TEL**ecommunication **NET**work) descrito en el RFC 854, es un protocolo de Internet estándar que permite conectar terminales y aplicaciones en Internet. El protocolo proporciona reglas básicas que permiten vincular a un cliente (sistema compuesto de una pantalla y un teclado) con un intérprete de comandos (del lado del servidor o dispositivo de red)." [6]*

El protocolo Telnet se aplica en una conexión TCP para enviar datos en formato ASCII codificados en 8 bits, entre los cuales se encuentran secuencias de verificación Telnet.

El protocolo Telnet se basa en tres conceptos básicos:

- Terminal virtual de red (NVT).
- Principio de opciones negociadas.
- Reglas de negociación.

Telnet fue desarrollado cuando la seguridad no era un problema, por lo tanto, todo el tráfico de Telnet se envía en texto plano. Al usar este protocolo, los datos críticos, como configuraciones del *Router/Switch*, son de fácil acceso para los atacantes

1.6.1.1. Terminal Virtual De Red (NVT)

Cuando surgió Internet, la red (ARPANET) estaba compuesta de equipos cuyas configuraciones eran muy poco homogéneas (teclados, juegos de caracteres, resoluciones, longitud de las líneas visualizadas). Además, las sesiones de los terminales también tenían su propia manera de controlar el flujo de datos entrante/saliente.

Por lo tanto, en lugar de crear adaptadores para cada tipo de terminal, para que pudiera haber interoperabilidad entre estos sistemas, se decidió desarrollar una interfaz estándar denominada *NVT* (*Terminal virtual de red*). Así, se proporcionó una base de comunicación estándar, compuesta de:

- Caracteres ASCII de 7 bits, a los cuales se les agrega el código ASCII extendido
- Tres caracteres de control
- Cinco caracteres de control opcionales
- Un juego de señales de control básicas.

Por lo tanto, el protocolo Telnet consiste en crear una abstracción del terminal que permita a cualquier host (cliente o servidor) comunicarse con otro host sin conocer sus características.

1.6.1.2. Principios de Opciones Negociadas

Las especificaciones del protocolo Telnet permiten tener en cuenta el hecho de que ciertos terminales ofrecen servicios adicionales, no definidos en las especificaciones básicas para poder utilizar funciones avanzadas. Estas funcionalidades se reflejan como opciones. Por lo tanto, el protocolo Telnet ofrece un sistema de negociaciones de opciones

que permite el uso de funciones avanzadas en forma de opciones, en ambos lados, al iniciar solicitudes para su autorización desde el sistema remoto.

Las opciones de Telnet afectan por separado cada dirección del canal de datos. Entonces, cada parte puede negociar las opciones, es decir, definir las opciones que:

- Desea usar (*DO*);
- Se niega a usar (*DON'T*);
- Desea que la otra parte utilice (*WILL*);
- sS niega a que la otra parte utilice (*WON'T*).

De esta manera, cada parte puede enviar una solicitud para utilizar una opción. La otra parte debe responder si acepta o no el uso de la opción. Cuando la solicitud se refiere a la desactivación de una opción, el destinatario de la solicitud no debe rechazarla para ser completamente compatible con el modelo NVT.

1.6.1.3. Reglas de Negociación

Las reglas de negociación para las opciones permiten evitar situaciones de enrollo automático.

1. Las solicitudes sólo deben enviarse en el momento de un cambio de modo.
2. Cuando una de las partes recibe la solicitud de cambio de modo, sólo debe confirmar su recepción si todavía no se encuentra en el modo apropiado.
3. Sólo debe insertarse una solicitud en el flujo de datos en el lugar en el que surte efecto.

Algunos de los clientes telnet pueden ser:

- PuTTY
- AbsoluteTelnet
- Host Explorer
- NCSA Telnet

- TeraTerm
- ZOC Terminal
- SyncTERM

La Figura 1.24. Nos muestra como es una conexión desde un Cliente a un Servidor TELNET, mientras que la Figura 1.25. Nos muestra como viaja la información de la conexión Telnet.

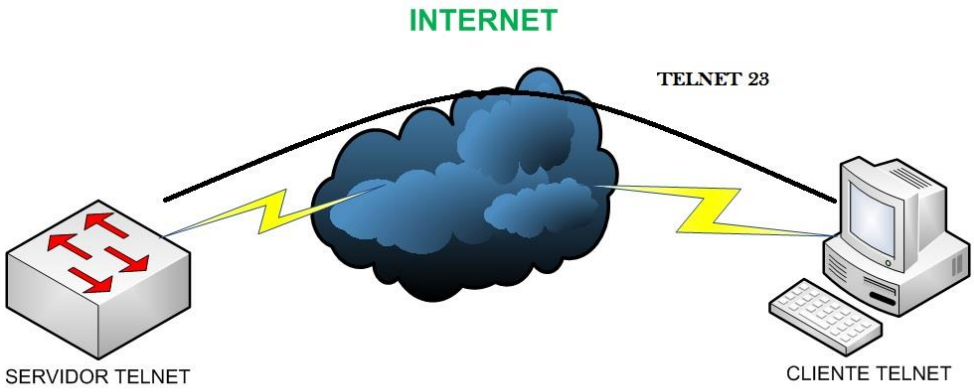


Figura 1.24. Conexión Cliente Servidor TELNET.

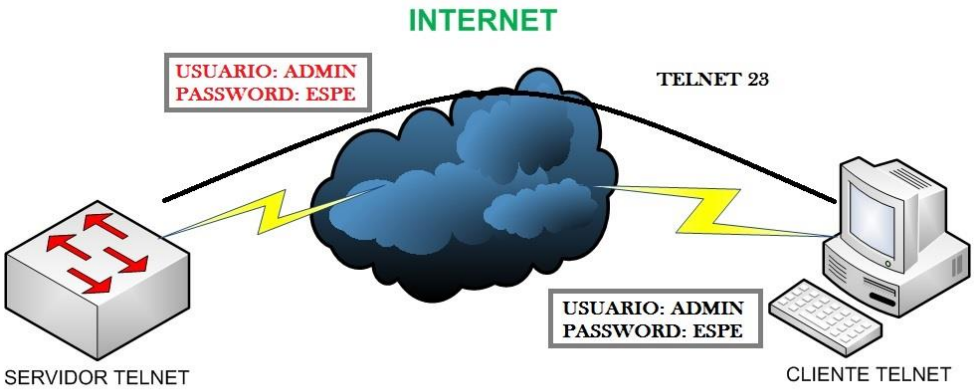


Figura 1.25. Envío de la información en texto plano.

1.6.2. SSH

*SSH **S**ecure **SH**ell ha reemplazado a Telnet como práctica recomendada para proveer administración de un dispositivo de red remota con conexiones que soportan confidencialidad e integridad de la sesión. Provee una funcionalidad similar a una conexión Telnet de salida, con la excepción de que la conexión está cifrada y opera en el puerto 22. Con autenticación y cifrado, SSH permite comunicaciones seguras sobre una red no segura. [7]*

Existen 2 versiones de SSH, la versión 1 de SSH hace uso de muchos algoritmos de encriptación patentados (sin embargo, algunas de estas patentes han expirado) y es vulnerable a un hueco de seguridad que potencialmente permite a un intruso insertar datos en el sentido de la comunicación. La suite OpenSSH bajo Red Hat Enterprise Linux utiliza por defecto la versión 2 de SSH, la cual tiene un algoritmo de intercambio de llaves mejorado que no es vulnerable al hueco de seguridad en la versión 1. Sin embargo, la suite OpenSSH también soporta las conexiones de la versión 1.

1.6.2.1. Características SSH

- El cliente puede verificar que se está conectado a un mismo servidor.
- Información de autenticación encriptado con 128 bits.
- Datos enviados y recibidos encriptados con 128 bits.

Algoritmos de Cifrado

El Protocolo SSH, dependiendo de su versión utiliza diferentes algoritmos de cifrado.

- **SSH1:** DES, 3DES, IDEA, Blowfish
- **SSH2:** 3DES, Blowfish, Twofish, Arcfour, Cast128-cbc

El cifrado utilizado para cuestiones de autentificación utiliza RSA para SSH1 y DSA para SSH2.

Autenticación

SSH permite autentificarse utilizando uno o varios de los siguientes métodos:

- Password.
- Sistema de clave pública.
- Kerberos (SSH1).
- Basado en el cliente (por relaciones de confianza en SSH1 y sistema de clave pública en SSH2).

La Figura 1.26. Nos muestra como es una conexión desde un Cliente a un Servidor SSH, mientras que la Figura 1.27. Nos muestra como viaja la información de la conexión SSH.

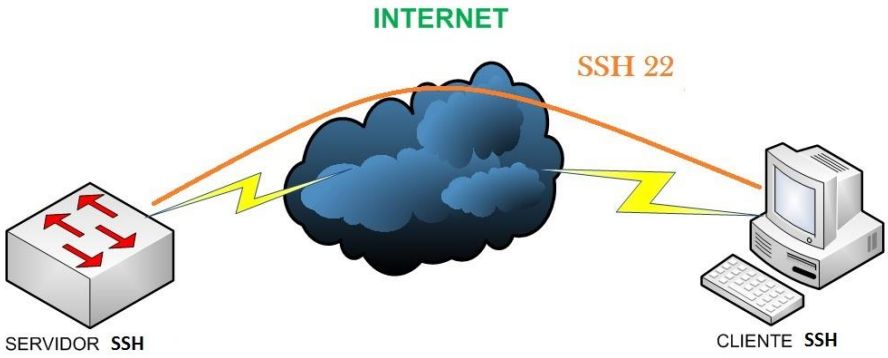


Figura 1.26. Conexión SSH entre Cliente Servidor.

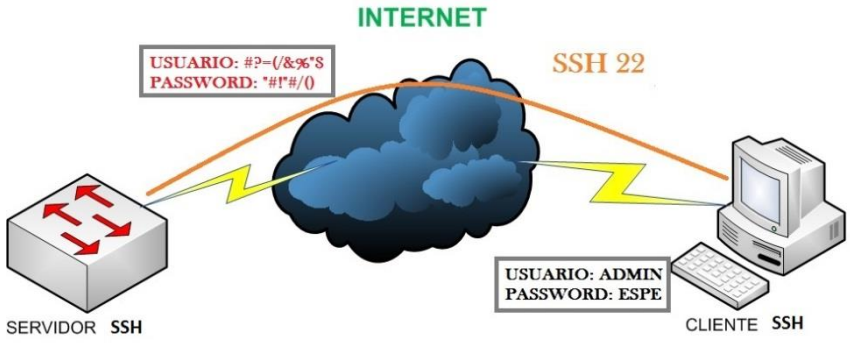


Figura 1.27. Envío de la información en texto cifrado.

1.7. 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. Es utilizado en algunos puntos de acceso inalámbricos cerrados y se basa en el protocolo de autenticación extensible (EAP– RFC 2284)". [8]

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.

Muchas veces se implementa 802.1X en puntos de acceso inalámbricos que pueden utilizarse en ciertas situaciones, las cuales el punto de acceso necesita operarse como un punto de acceso cerrado, corrigiendo deficiencias de seguridad WEP. Esta autenticación es realizada normalmente por un tercero, tal como un servidor RADIUS. Esto permite la autenticación sólo del cliente o, más apropiadamente, una autenticación mutua utilizando protocolos como EAP-TLS.

1.7.1. AAA (Authentication, Authorization, and Accounting)

Un intruso puede ganar acceso a equipamiento de red y servicios sensibles. Para ayudar a prevenir el acceso no deseado, el control de acceso es necesario. El control de acceso limita quién o qué puede usar recursos específicos así como servicios u opciones disponibles una vez que se otorga el acceso.

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).

1.7.1.1. Características AAA

Autenticación AAA

Puede utilizarse AAA para autenticar usuarios para acceso administrativo o para acceso remoto a una red. Estos dos métodos de acceso usan diferentes modos para solicitar los servicios de AAA:

Modo carácter - El usuario envía una solicitud para establecer un proceso de modo Privilegiado con el *Switch* con fines administrativos.

Modo paquete - El usuario envía una solicitud para establecer una conexión con un dispositivo en la red a través del *Router/Switch.*

A excepción de los comandos de registro de auditoría, todos los comandos AAA se aplican a ambos modos. Esta sección se concentra en asegurar el acceso de modo carácter. Para una red verdaderamente segura, también es importante configurar el *Router/Switch* para acceso administrativo y acceso remoto a la red LAN seguros mediante el uso de los servicios AAA.

Autorización AAA

Una vez que los usuarios han ido autenticados exitosamente contra la fuente de datos AAA seleccionada (ya sea local o basada en servidor), se les autoriza el acceso a recursos específicos en la red. La autorización consiste básicamente en lo que un usuario puede y no puede hacer en la red luego de que es autenticado.

En general, la autorización se implementa usando una solución de AAA basada en servidor. La autorización usa un grupo de atributos creado que describe el acceso del usuario a la red. Estos atributos se comparan con la información contenida dentro de la base de datos AAA y se determinan las restricciones para ese usuario, que son enviadas al *Router/Switch* local donde el usuario está conectado.

La autorización, que se implementa inmediatamente después de que el usuario se autentica, es automática: no se requiere participación de parte del usuario luego de la autenticación.

Registro de Auditoría AAA

El registro de auditoría recolecta y reporta datos de uso para que puedan ser empleados para auditorías o emisión de facturas. Los datos recolectados pueden incluir el inicio y fin de conexiones, comandos ejecutados, números de paquetes y número de bytes. El registro de auditoría se implementa usando una solución AAA basada en servidor.

1.7.2. RADIUS

RADIUS, desarrollado por *Livingston Enterprises,* es un protocolo AAA abierto de estándar IETF con aplicaciones en acceso a las redes y movilidad IP. Se lo define en los RFCs 2865, 2866, 2867 y 2868.

"*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". [9]*

RADIUS combina autenticación y autorización en un solo proceso. Cuando el usuario se autentica, también está autorizado. RADIUS usa el puerto UDP 1645 o el 1812 para la autenticación y el puerto UDP 1646 o el 1813 para los registros de auditoría.

RADIUS es muy popular entre los proveedores de servicio VoIP. Pasa las credenciales de inicio de sesión de un nodo SIP (protocolo de inicio de sesión), como un teléfono de banda ancha, a un nodo SIP registrante usando autenticación *digest*, para luego enviarlas a un servidor RADIUS usando RADIUS. También es el protocolo utilizado por el estándar de seguridad 802.1X.

1.8. STACKING

1.8.1. Conceptos y Definiciones

Algunas unidades de *Switch* pueden ser interconectados para formar un STACK (Pila), cada conmutador es una unidad. Los puertos que se usan para interconectar cada unidad tienen el nombre de puerto de *Stacking*, mientras que los otros puertos que son usados para interconectar el STACK con el usuario se los denominan puertos de Usuario. De esta manera se puede aumentar los puertos y la capacidad de conmutación mediante la adición de dispositivos al STACK.

Adicionalmente la fiabilidad del sistema puede ser mejorado ya que los dispositivos que estén en él están pueden compartir información de *backup*, por consiguiente trae las siguientes ventajas.

- 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 1.28. Nos muestra como es la conexión entre *Switches* que permiten el uso del *Stacking*.

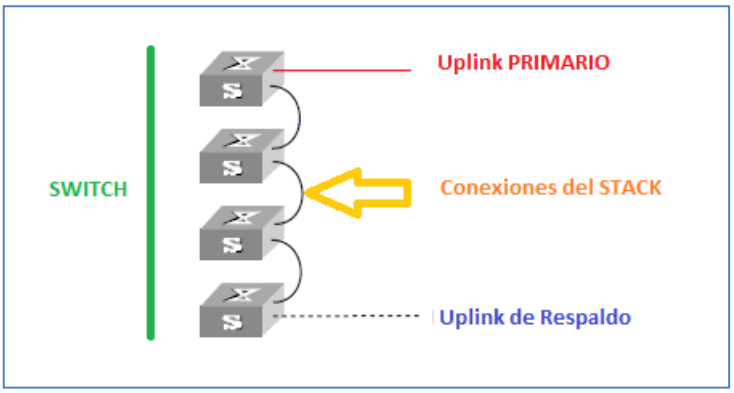


Figura 1.28. Ejemplo STACKING.

1.9. QOS (QUALITY OF SERVICE)

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.

1.9.1. 802.1P

"IEEE 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)." [10]

Existen 8 clases diferentes de servicios, expresados por medio de 3 bits del campo prioridad de usuario (*user_priority*) de la cabecera IEEE 802.1Q añadida a la trama, asignando a cada paquete un nivel de prioridad entre 0 y 7. Aunque es un método de priorización bastante utilizado en entornos LAN, cuenta con varios inconvenientes, como el requerimiento de una etiqueta adicional de 4 bytes (definida en el estándar IEEE802.1Q). Además solo puede ser soportada en una LAN, ya que las etiquetas 802.1Q se eliminan cuando los paquetes pasan a través de un *router*.

No está definida la manera de cómo tratar el tráfico que tiene asignada una determinada clase o prioridad, dejando libertad a las implementaciones. IEEE, sin embargo, ha hecho amplias recomendaciones al respecto. La Figura 1.29. Nos muestra la cabecera 802.1Q. Mientras que la Tabla 1.3. Nos indica las prioridades del campo Prioridad según el tipo de Red.

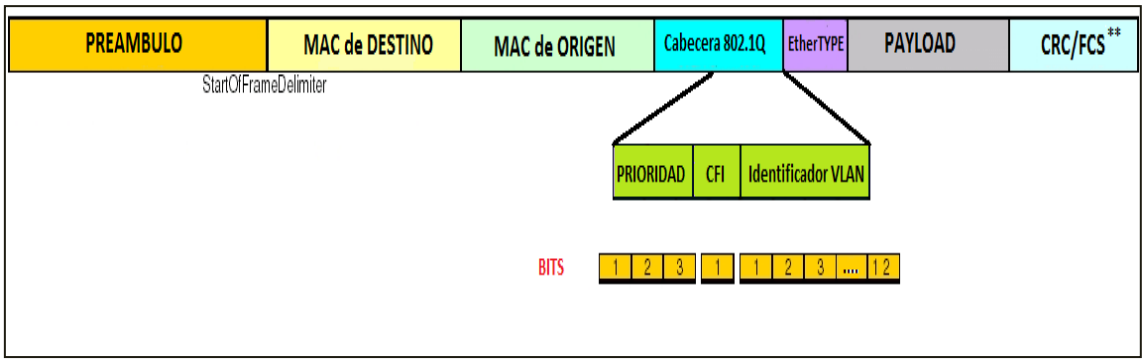


Figura 1.29. Cabecera 802.1Q con Campos Prioridad, CFI y VLAN ID

Tabla 1.3. Tabla del Campo de 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

CAPÍTULO 2

ESPECIFICACIONES TÉCNICAS DE LOS EQUIPOS

2.1. EQUIPOS EN EL LABORATORIO DE NETWORKING

En el siguiente capítulo se especificará las funciones básicas y avanzadas de los *switches*, los cuales nos permitirá realizar una previa selección para el diseño óptimo de las prácticas.

El laboratorio de *Networking* dispone de los siguientes equipos:

1) 3 Switch 3com 4210 de 26 puertos.

2) 2 Switch 3com 4500 de 26 puertos.

3) 2 Switch Cisco Catalyst Express 500 de 24 puertos.

4) 2 Switch D-link DGS-3627 de 24 puertos.

5) 1 Switch 3com 5500 de 28 puertos.

6) 1 Switch Cisco Catalyst 3560 de 24 puertos.

7) 2 Switch HP 2512 de 12 puertos.

8) 1 Switch D-link DES-3526 de 24 puertos.

2.2. CARACTERÍSTICAS GENERALES DE LOS EQUIPOS

2.2.1. Switch 3Com 4210

2.2.1.1. Resumen Características

El *Switch* 3com 4210, es un *Switch* de capa 2 (Enlace de Datos) administrable de clase empresarial que permite calidad de servicio, seguridad y características administrativas.

Ofreciendo cada puerto [3]*PoE* (*Power over Ethernet)* para el uso ideal de VoIP e instalaciones de redes inalámbricas. El *Switch* 3com 4210 soporta la interface de línea de comandos (CLI), administración vía Web y administración mediante el protocolo SNMP.

La Figura 2.1. Nos muestra una imagen del *Switch* 3Com 4210.

Figura 2.1. Switch 3com 4210

[3] **Power over Ethernet** por medio del par trenzado de un cable UTP, brinda energía a un dispositivo final estos pueden ser: teléfonos IP, Access Points, cargadores para dispositivos portátiles, cámaras de red entre otros.

2.2.2. Switch 3Com 4500

2.2.2.1. Resumen Características

El *switch* 3Com 4500 de 26 puertos ofrece *switching* de Capa 2 y enrutamiento dinámico de Capa 3 del modelo OSI con amplia variedad de características, en una plataforma competitiva de alto rendimiento.

Con una seguridad robusta, y amplias funcionalidades de administración, priorización de tráfico, y calidad de servicio, el *Switch* 3com 4500 es capaz de manejar aplicaciones empresariales emergentes.

Se pueden apilar hasta ocho *switches* mediante puertos GigabitEthernet, por lo que toda una pila (*Stacking*) puede administrarse como una única entidad de administración IP.

24 puertos con *Power over Ethernet*, y dos puertos GigabitEthernet de uso dual permiten al *Switch* 4500 proporcionar una conectividad de LAN segura y fiable, y soportar aplicaciones de voz de próxima generación para redes de pequeñas y medianas empresas y de sucursales. La Figura 2.2. Nos muestra una imagen del *Switch* 3Com 4500.

Figura 2.2. Switch 3com 4500

2.2.3. Switch Cisco Catalyst Express 500

2.2.3.1. Resumen Características

Los *switches* de la serie Cisco *Catalyst* Express 500 proporcionan redes adaptadas para negocios de hasta 250 empleados. Esta familia de *switches* administrables de capa 2

Fast Ethernet y *GigabitEthernet* brinda un rendimiento de antibloqueo y velocidad *wirespeed* (velocidad de cable), que proporciona una base de redes segura y

optimizada para datos y voz. Las características de seguridad avanzada incorporadas ayudan a garantizar la protección de los dispositivos y las redes. La Figura 2.3. Nos muestra una imagen del *Switch* Cisco Catalyst Express 500.

Figura 2.3. Switch Cisco Catalyst Express 500

2.2.4. Switch D-link DGS-3627

2.2.4.1. Resumen Características

El Switch D-link DGS-3627 es un Switch de capa 3 de 24 puertos GigabitEthernet, 4 puertos para [4] sfp (Small Form-factor Pluggable) y 3 slots 10 GigabitEthernet, brinda Seguridad gracias a D-Link Zone DefenseTM. Permite Alto Rendimiento y Funcionalidades de Switching capa 3 avanzadas así como seguridad RADIUS cliente, SSH versión 2. Soporte Avanzado de ACL (listas de acceso) y soporte para fuente de poder redundante (RPS). La Figura 2.4. Nos muestra una imagen del Switch D-link DGS-3627.

Figura 2.4. Switch Cisco D-link DGS-3627

[4] **SPF:** Permite conectar deferentes tipos de medio en un mismo puerto, dependiendo del módulo se puede convertir de SPF a RJ-45/Fibra Óptica.

2.2.5. Switch 3Com 5500

2.2.5.1. Resumen Características

El Switch 3com 5500 ofrece niveles de rendimiento Premium, consiste en un Switch capa 3 con 28 puertos FastEthernet con funcionalidad PoE y características avanzadas que se adaptan a las aplicaciones de más demanda.

Ofrece resistencia, seguridad en la conectividad y las últimas tecnologías de priorización de tráfico para optimizar las aplicaciones en redes convergentes. La Figura 2.5. Nos muestra una imagen del Switch 3Com 5500.

Figura 2.5. Switch 3Com 5500

2.2.6. Switch Cisco Catalyst 3560

2.2.6.1. Resumen Características

El Switch Cisco Catalyst 3560 es un Switch capa 3 de alto rendimiento diseñado para ayudar a los usuarios a que pasen de forma sencilla de las redes LAN compartidas tradicionales a redes completamente conmutadas. Ofrece rendimiento, administración y escalabilidad, con 24 puertos FastEthernet y con opciones modulares las cuales permiten adaptarlos a las necesidades del negocio. La Figura 2.6. Nos muestra una imagen del Switch Cisco Catalyst 3560.

Figura 2.6. Switch Cisco Catalyst 3560

2.2.7. Switch HP 2512

2.2.7.1. Resumen Características

El Switch HP 2512 es un Switch de capa 2 administrable con funciones de Stacking.Tiene12 puertos, con detección automática 10/100 Mbps por puerto y 2 ranuras para transceptores para GigabitEthernet o 100Base-FX. El Switch 2512 ofrece ProCurve/IEEE Auto-MDIX en todos los puertos 10/100, así como funcionalidades de alta disponibilidad. La Figura 2.7. Nos muestra una imagen del Switch HP 2512.

Figura 2.7. Switch HP 2512

2.3. TABLA COMPARATIVA ENTRE EQUIPOS CAPA 2 Y CAPA 3

Las Tablas 2.1. Y 2.2. Contienen información, sobre las funciones o características que se necesitan para el diseño óptimo de las prácticas de laboratorio que veremos en el capítulo 3.

Tabla 2.1. Tabla Comparativa entre Switch Capa 2

CARATERISTICA	Switch *3com 4210*	Switch *Cisco Catalyst Express 500*	Switch *HP 2512*
Número de Puertos	26 Puertos	24 Puertos / 2 Uplink	12 Puertos / 2 Slots
Velocidad de los Puertos	24 Puertos 10BASE-T/100BASE-TX y 2 dual-personality 10/100/1000 o puertos SFP	24 Puertos 10/100 Mbps 2 Puertos10/100/1000 BASE-T para uplink o conectividad con servidores	12 Puertos 10/100 Mbps 2 transceiver slots para Gigabit o 100Base-FX
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

Tabla 2.2. Tabla Comparativa entre Switch Capa 3

CARATERISTICA	**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
Velocidad de los Puertos	24 Puertos10 BASE-T/100BASE -TX 2 Puertos SFP	24 Puertos10 BASE-T/100BASE -TX 2 Puertos SFP	24 Puertos 10/100/1000 BASE-T 4 Puertos para SFP	24 Puertos10 BASE-T/100BASE -TX 4 Puertos SFP
Soporte PoE (Power over Ethernet)	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
Dimensiones (Altura x Ancho x Profundidad)	43.6mm x 440 mm x 427 mm	44mm x 445 mm x 300 mm	44 mm x 441 mm x 389 mm	43.6mm x 440 mm x 427 mm
PESO	6.3 Kg	5.1 Kg	5.5 Kg	6.3 Kg
Costo Aproximado 2012	~$1,000	~$1,200	~$2,200	~$2,050

CAPÍTULO 3

DISEÑO DE PRÁCTICAS DE LABORATORIO PARA EL ESTUDIANTE

3.1. INTRODUCCIÓN

En este capítulo, se detallará el diseño de las guías prácticas para el laboratorio de *Networking*.

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.

3.2. 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.

I) TEMA: En el campo Tema, estará descrito el nombre de la práctica este nombre dependerá si la práctica es: general o específica.

II) OBJETIVOS: El campo 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.

III) MARCO TEORICO: En el campo Marco Teórico, se dará un resumen del o los temas que abarcará la práctica. Sirve como refuerzo a los temas que son profundizados en clases.

IV) EQUIPOS: El campo 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.

V) 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.

VI) NOTA/ADVERTENCIA: Nota/Advertencia permitirá al alumno no cometer errores en el desarrollo de la práctica o a su vez dar instrucciones al finalizar la práctica.

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

VIII) 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.

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

A continuación se detallara cada práctica, exceptuando los campos CONFIGURACIÓN DIRECCIONAMIENTO y CONCLUCSIONES RECOMENDACIONES que serán detallados en los siguientes capítulos.

3.3. PRÁCTICAS DE LABORATORIO

3.3.1. Práctica #1 Configuración Básica del Switch

TEMA: Configuración Básica del Switch.

OBJETIVOS:

a) Conocer la configuración Básica del Switch.

b) Utilizar herramientas (Software) y cables para la conexión con el Switch.

c) ***Este Objetivo se plantea el alumno.***

MARCO TEORICO:

Debemos recordar que para la configuración de un Switch, se puede acceder al Switch ya sea por CLI (Interfaz de Línea de Comandos), WEB (HTTP) o Acceso Remoto (TELNET/SSH) en este caso será un tema que se abarcara en las siguientes practicas con más detalle.

El Switch dispone de un puerto de Consola el cual nos permitirá el acceso por CLI.

Entre las configuraciones básicas del Switch está poner un nombre, dirección, contraseña habilitar el acceso remoto (TELNET).

La Práctica incluirá la configuración de nombre, usuario, contraseña, dirección IP al Switch y el almacenamiento de los archivos de configuración en un Servidor TFTP.

EQUIPOS:

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

1. - Switch *3com 4500* (Acceso CLI).

2. - Switch *D-link DES-3526* (Acceso WEB).

3. - Switch *HP 2512.*

4.- Cable de Consola, Cable de Red.

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

NOTA/ADVERTENCIA:

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

TOPOLOGÍA:

La Figura 3.1. Nos muestra la topología de Red, de la práctica #1.

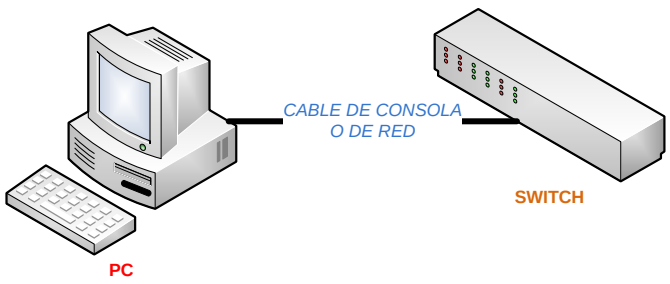


Figura 3.1. Topología de Red Práctica #1

3.3.2. Práctica #2 Configuración TELNET en el Switch

TEMA: Configuración Telnet en el Switch.

OBJETIVOS:

a) Conocer la configuración de Telnet en el Switch.

b) Verificar la contraseña almacenada en texto plano.

c) ***Este Objetivo se plantea el alumno.***

MARCO TEORICO:

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.

TELNET: Telnet (***TEL****ecommunication* ***NET****work*) descrito en el RFC 854, es un protocolo de Internet estándar. El protocolo proporciona reglas básicas que permiten vincular a un cliente (sistema compuesto de una pantalla y un teclado) con un intérprete de comandos (del lado del servidor o dispositivo de red).

La contraseña almacenada para el acceso entre el cliente y el servidor está en texto plano esto conlleva una desventaja en la seguridad de la red.

EQUIPOS:

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

1. - Switch *CISCO Catalyst 3560*.

2. - Switch *3COM 4210.*

3.- Cable de Consola, Cable de Red.

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

NOTA/ADVERTENCIA:

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

TOPOLOGÍA:

La Figura 3.2. Nos muestra la topología de Red, de la práctica #2.

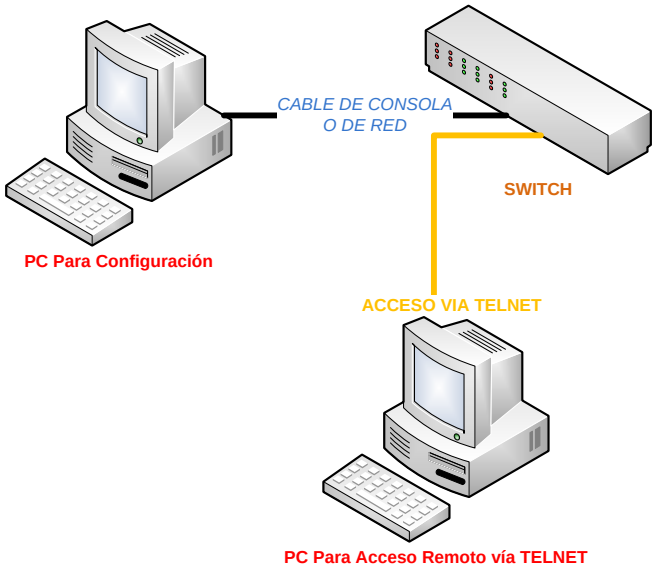


Figura 3.2. Topología de Red Práctica #2

3.3.3. Práctica #3 Configuración SSH en el Switch

TEMA: Configuración SSH en el Switch.

OBJETIVOS:

a) Conocer la configuración de SSH en el Switch.

b) Verificar la contraseña almacenada en texto cifrado.

c) ***Este Objetivo se plantea el alumno.***

MARCO TEORICO:

SSH **S**ecure **SH**ell ha reemplazado a Telnet como práctica recomendada para proveer administración de un dispositivo de red remota con conexiones que soportan confidencialidad e integridad de la sesión. Provee una funcionalidad similar a una conexión Telnet de salida, con la excepción de que la conexión está cifrada y opera en el puerto 22. Con autenticación y cifrado, SSH permite comunicaciones seguras sobre una red no segura.

EQUIPOS:

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

1. - Switch *3com 5500*.

2. - Switch *D-link DGS-3627*.

3.- Cable de Consola, Cable de Red.

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

NOTA/ADVERTENCIA:

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

TOPOLOGÍA:

La Figura 3.3. Nos muestra la topología de Red, de la práctica #3.

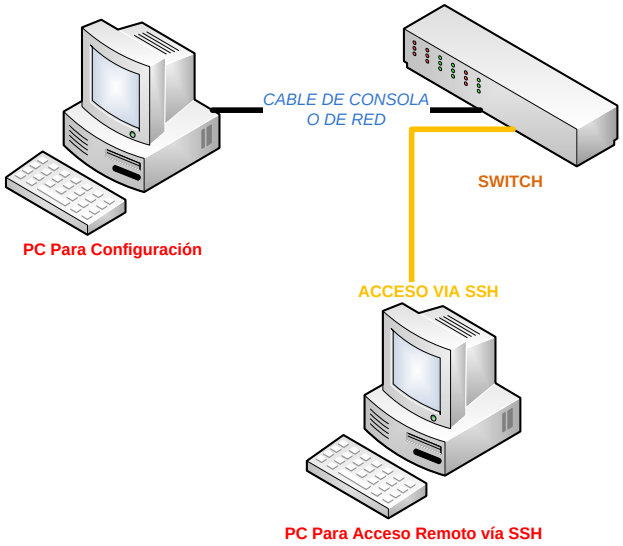


Figura 3.3. Topología de Red Práctica #3

3.3.4. Práctica #4 Configuración de una VLAN por puerto

TEMA: Configuración de una VLAN basada en puerto.

OBJETIVOS:

a) Conocer la importancia de las Vlans.

b) Comprender y configurar una Vlan basada en puerto.

c) ***Este Objetivo se plantea el alumno.***

MARCO TEORICO:

Vlan (Virtual LAN) es un método para crear redes lógicamente independientes dentro de una misma red física. Varias VLAN pueden coexistir en un único Switch 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 (como departamentos de una empresa).

Vlan basada en puerto consiste en una agrupación de puertos físicos que puede tener lugar sobre un Switch o también, en algunos casos, sobre varios Switches.

EQUIPOS:

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

1. - Switch *3com 4500*.

2. - Switch *HP 2512*.

3.- Cable de Consola, Cable de Red.

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

NOTA/ADVERTENCIA:

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

TOPOLOGÍA:

La Figura 3.4. Nos muestra la topología de Red, de la práctica #4.

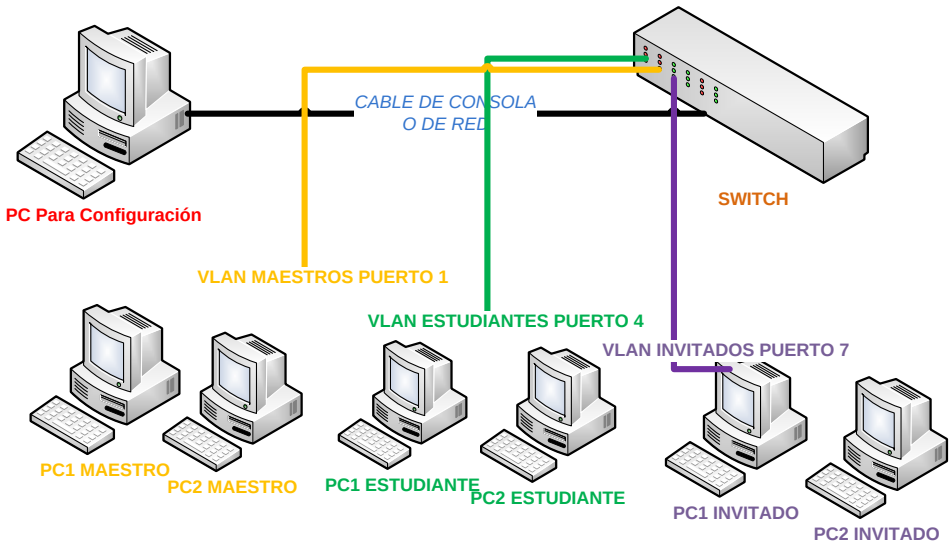


Figura 3.4. Topología de Red Práctica #4

3.3.5. Práctica #5 Configuración DHCP con VLAN

TEMA: Configuración DHCP con VLAN.

OBJETIVOS:

a) Conocer la importancia de DHCP en VLANS.

b) ***Este Objetivo se plantea el alumno.***

MARCO TEORICO:

"DHCP *(Dynamic Host Configuration Protocol) 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 que equipo dentro de la red ha estado en posesión de la dirección IP, cuánto tiempo la ha tenido y a cual equipo se le puede asignar después." [11]*

EQUIPOS:

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

1. - Switch *CISCO 3560.*

2.- Cable de Consola, Cable de Red.

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

NOTA/ADVERTENCIA:

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

TOPOLOGÍA:

La Figura 3.5. Nos muestra la topología de Red, de la práctica #5.

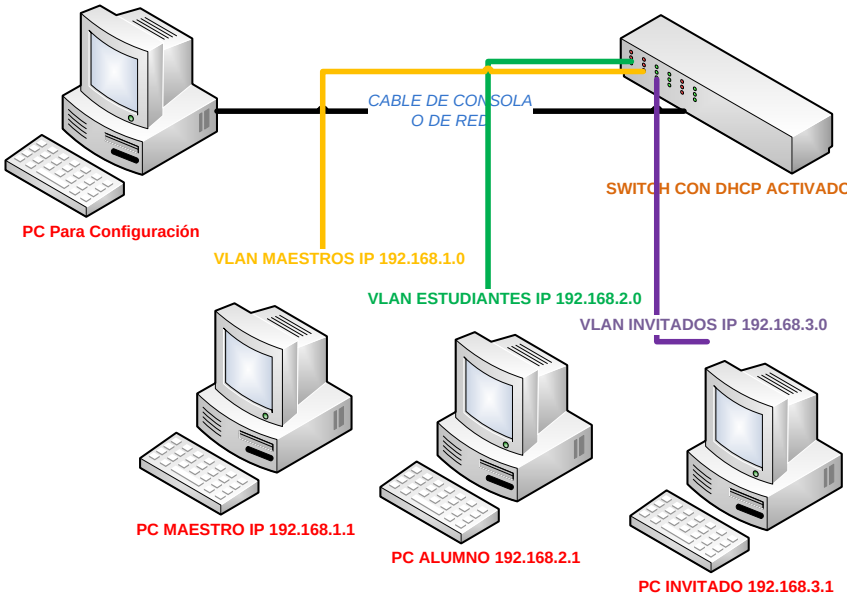


Figura 3.5 Topología de Red Práctica #5.

3.3.6. Práctica #6 Configuración de Spanning Tree Protocol (STP) y Enlaces Troncales

TEMA: Configuración de Spanning Tree Protocol (STP) y enlaces troncales.

OBJETIVOS:

a) Conocer el funcionamiento del protocolo STP.

b) Comprender la importancia de los enlaces troncales.

c) ***Este Objetivo se plantea el alumno.***

MARCO TEORICO:

STP: Es un protocolo de red de nivel 2 de la capa OSI (nivel de enlace de datos), su función es gestionar la presencia de bucles en topologías de red. El protocolo permite a los dispositivos de interconexión activar o desactivar automáticamente los enlaces de conexión, de forma que se garantice que la topología esté libre de bucles. STP es transparente a las estaciones de usuario.

Un enlace troncal es un enlace punto a punto, entre dos dispositivos de red, que transporta más de una VLAN. Un enlace troncal de VLAN le permite extender las VLAN a través de toda una red. No pertenece a una VLAN específica, sino que es un conducto para las VLAN entre switches y routers.

EQUIPOS:

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

1. - Switch *3com 4210*.

2. – Switch *D-link DES-3526.*

3. – Switch *HP 2512.*

4.- Cable de Consola, Cable de Red.

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

NOTA/ADVERTENCIA:

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

TOPOLOGÍA:

La Figura 3.6. Nos muestra la topología de Red, de la práctica #6.

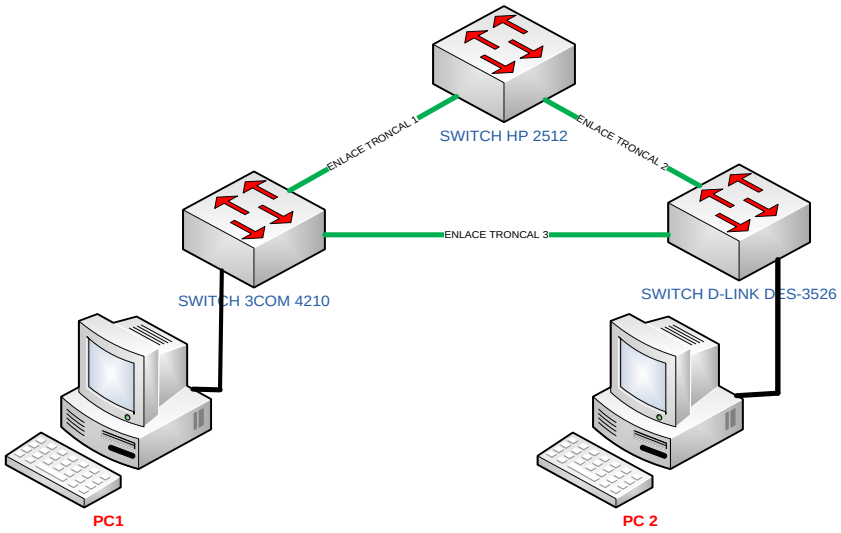


Figura 3.6. Topología de Red Práctica #6

3.3.7. Práctica #7 Interconexión de VLANs por medio del Router

TEMA: Interconexión de VLANs por medio del Router.

OBJETIVOS:

a) Conocer el papel del Router.

b) Entender la importancia del enrutamiento entre Vlans.

c) ***Este Objetivo se plantea el alumno.***

MARCO TEORICO:

El enrutamiento entre vlans o inter vlan routing, resulta necesario una vez que se posee una infraestructura de red con vlan implementadas, debido a que los usuarios necesitaran intercambiar información de una red a otra.

EQUIPOS:

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

1. - Switch *3com 4210*.

2. – Switch *D-link DES-3526.*

3. – Switch *HP 2512.*

4.- Router *CISCO Serie 2000 o superior*.

5.- Cable de Consola, Cable de Red.

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

NOTA/ADVERTENCIA:

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

TOPOLOGÍA:

La Figura 3.7. Nos muestra la topología de Red, de la práctica #7.

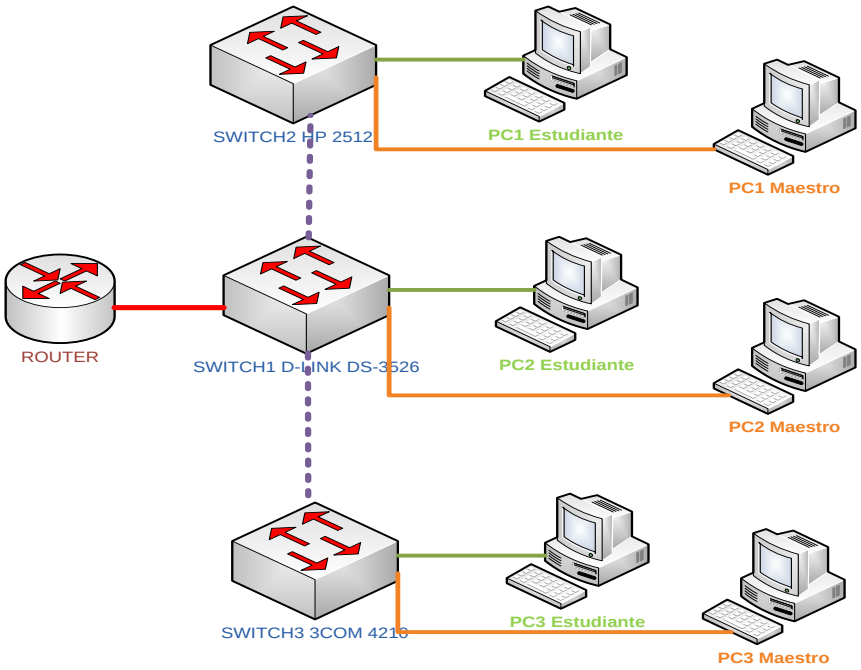


Figura 3.7. Topología de Red Práctica #7

3.3.8. Práctica #8 Configuración (Estándar-Extendida) en el Switch

TEMA: Configuración Estándar y Extendida en el Switch.

OBJETIVOS:

a) Configurar una Lista de Acceso Estándar y Extendida.

b) Comprender la importancia de las Listas de Acceso.

c) ***Este Objetivo se plantea el alumno.***

MARCO TEORICO:

La ACL Tienen como propósito controlar y administrar el acceso al Switch. Filtrar paquetes permitirá a la Red prevenir el acceso no autorizado.

De acuerdo al uso de las aplicaciones las ACL pueden ser de 3 tipos:

- ACL Básica.
- ACL Avanzada.
- ACL Capa 2.
-

ACL ESTÁNDAR.- Las reglas se basan únicamente en la dirección IP de origen.

ACL EXTENDIDA.- Las reglas se basan ya sea por la dirección IP de origen/destino, tipo de protocolo o por la información recibida de capa 3 y capa 4.

ACL CAPA 2.- Las reglas se basan por la información de Capa 2 así como dirección MAC origen/destino, prioridad de Vlan o tipo de protocolo Capa 2.

EQUIPOS:

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

1. - Switch *3com 4500.*

2. – Switch *CISCO 3560.*

3. – Switch *D-link DGS-3627.*

4.- Cable de Consola, Cable de Red.

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

PROBLEMA PROPUESTO:

Se requiere que una lista de acceso estándar sea configurada en el equipo 3COM 4500 con el fin de negar el tráfico que viene de las PC1 y PC4, mientras que el en Switch CISCO 3560 se deberá crear una lista de acceso extendida que bloquee el trafico telnet generado por la PC1 hacia el Switch D-LINK DGS-3627.

NOTA/ADVERTENCIA:

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

TOPOLOGÍA:

La Figura 3.8. Nos muestra la topología de Red, de la práctica #8.

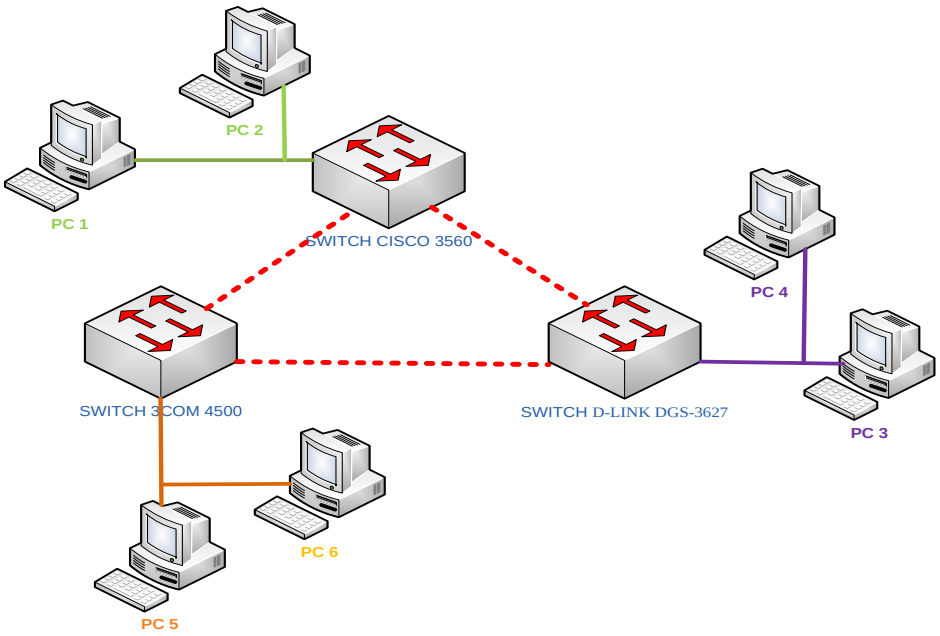


Figura 3.8. Topología de Red Práctica #8

3.3.9. Práctica #9 Simulación de una Red que permita dividir departamentos en una Empresa y dar prioridad de acceso a ciertos empleados por medio de ACL

TEMA: Simulación de una red que permita dividir departamentos en una empresa y dar prioridad de acceso a ciertos empleados por medio de ACL.

OBJETIVOS:

a) Utilizar los simuladores de Red para completar con éxito la práctica.

b) Aplicar los conocimientos aprendidos anteriormente.

c) ***Este Objetivo se plantea el alumno.***

PROBLEMA PROPUESTO:

La Empresa "Microwive" necesita dividir sus departamentos en redes diferentes: Administrativo, Humanístico y Gerencial. En la empresa existen 3 impresoras para cada departamento.

Se requiere dar acceso total al gerente general esto significa que tiene conectividad con cualquiera de las redes de los departamentos. Mientras que el jefe del departamento administrativo tiene conectividad con su red y a las 3 impresoras. El jefe del departamento humanístico solo puede acceder a su impresora y tiene conectividad solo con su departamento. La utilización de Listas de accesos (ACL) nos ayudara con la solución del problema propuesto.

EQUIPOS:

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

1. - Router *CISCO 2811.*

2. – Switch *CISCO 2960.*

3. – Simulador a utilizar GNS o Packet Tracer.

NOTA/ADVERTENCIA:

Las listas de acceso pueden ser aplicadas ya sea en el Router o en el Switch.

Luego de terminar con la práctica de laboratorio guardar la simulación con su nombre y apellido.

TOPOLOGÍA:

La Figura 3.9. Nos muestra la topología de Red, de la práctica #9.

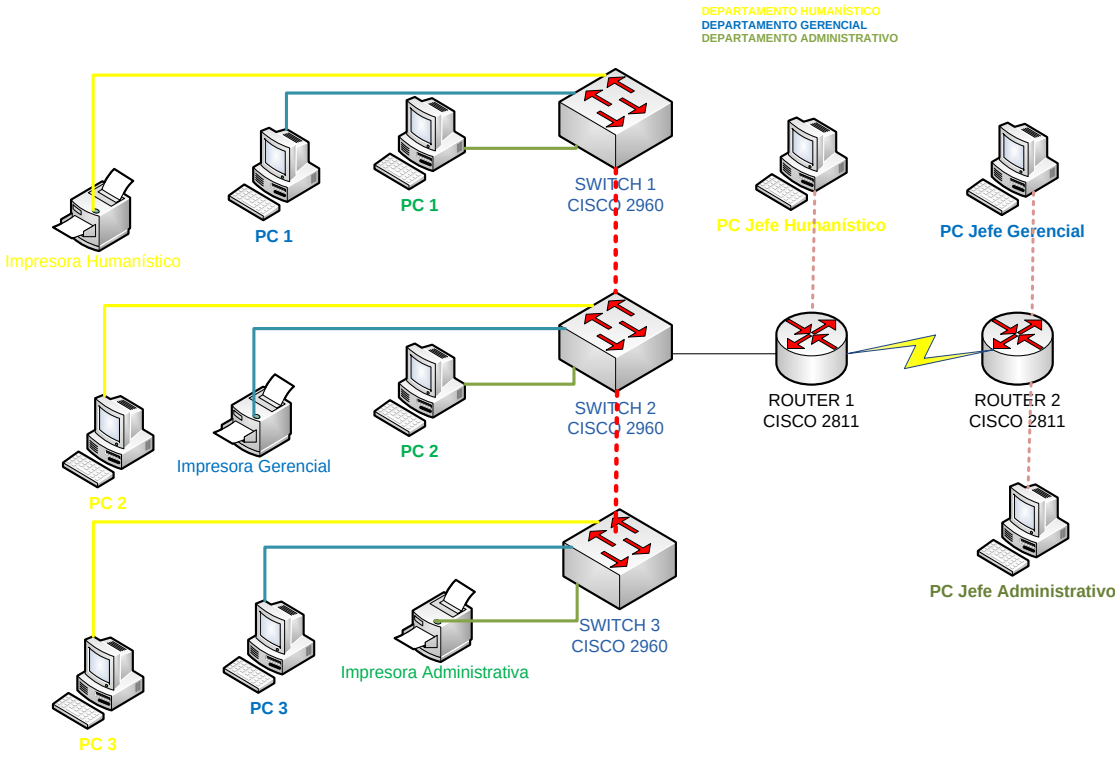


Figura 3.9. Topología de Red Práctica #9

3.3.10. Práctica #10 Implementación de una Red Jerárquica con Redundancia

TEMA: Diseño e implementación de una red Jerárquica con redundancia.

OBJETIVOS:

a) Entender los conceptos que se aplican para el diseño en una Red Jerárquica.

b) Verificar el funcionamiento de una Red Jerárquica Redundante.

c) ***Este Objetivo se plantea el alumno.***

MARCO TEORICO:

El diseño de una LAN que satisfaga las necesidades de empresas pequeñas o medianas tiene más probabilidades de ser exitosa si se utiliza 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.

El diseño de redes jerárquicas implica la división de la red en capas independientes. Cada capa cumple funciones específicas que definen su rol dentro de la red general. La separación de las diferentes funciones existentes en una red hace que el diseño de la red se vuelva modular y esto facilita la escalabilidad y el rendimiento. El modelo de diseño jerárquico típico se separa en tres capas: capa de acceso, capa de distribución y capa núcleo.

EQUIPOS:

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

Capa de Acceso.

1. - Switch *3com 4210.*

2. - Switch *HP 2512.*

Capa de Administración.

1. - Switch *3com 4500.*

2. - Switch *3com 5500.*

3. - Switch *Cisco Catalyst 3560*

Capa de Núcleo.

1. - Switch *D-link DGS-3627.*

2. – Router *Cisco2600/2800 Series.*

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

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

NOTA/ADVERTENCIA:

Una vez implementada la Red, desconectar cables conectados a los Switches de la Capa de distribución para hacer la comprobación de la redundancia en la Red.

No es necesaria la configuración de listas de acceso en la siguiente topología.

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

TOPOLOGÍA:

La Figura 3.10. Nos muestra la topología de Red, de la práctica #10.

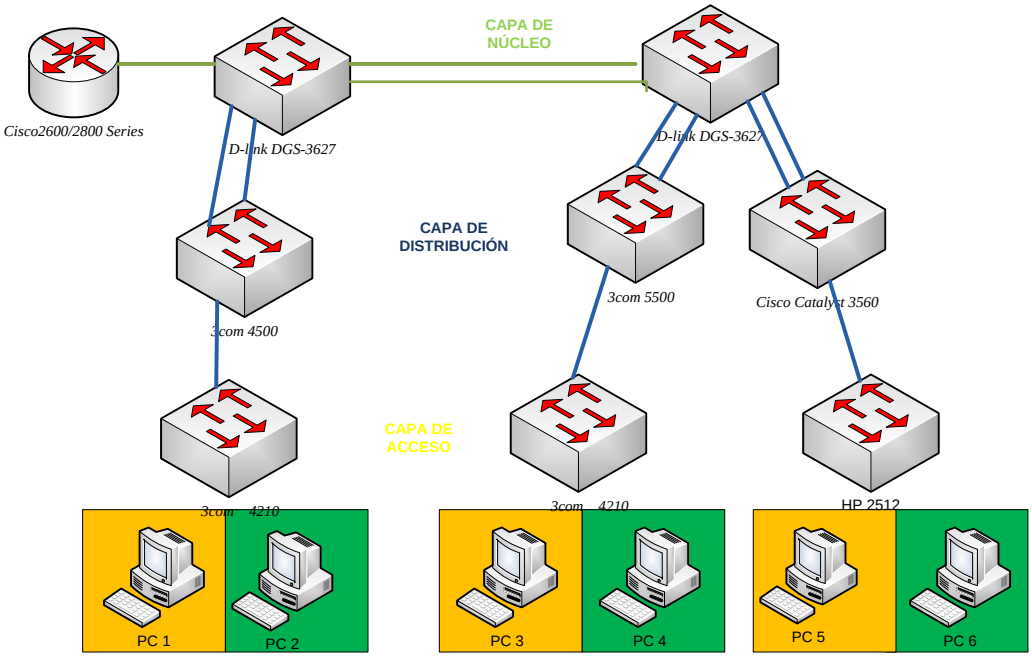


Figura 3.10. Topología de Red Práctica #10

3.3.11. Práctica #11 Implementación de una Red Jerárquica que permita la administración por medio de Acceso Remoto (SSH)

TEMA: Implementación de una Red Jerárquica que permita la administración por medio de acceso remoto (SSH).

OBJETIVOS:

a) Aplicar las funciones que nos ofrece el Acceso Remoto por medio de SSH.

b) Administrar la Red Jerárquica haciendo el uso de herramientas como PUTTY/TERATERM.

c) ***Este Objetivo se plantea el alumno.***

MARCO TEORICO:

SSH: **S**ecure **SH**ell como reemplazo de Telnet y práctica recomendada para proveer administración de un dispositivo de red remota con conexiones que soportan confidencialidad e integridad de la sesión. Provee una funcionalidad similar a una conexión Telnet de salida, con la excepción de que la conexión está cifrada y opera en el puerto 22. Con autenticación y cifrado, SSH permite comunicaciones seguras sobre una red no segura.

CARACTERISTICAS DE SSH

- El cliente puede verificar que se está conectado a un mismo servidor.
- Información de autenticación encriptado con 128 bits.
- Datos enviados y recibidos encriptados con 128 bits.

EQUIPOS:

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

1. - Switch *HP 2512.*

2. - Switch *3com 4210.*

3. - Switch *3com 4500.*

4. - Switch *3com 5500.*

5. - Switch *Cisco Catalyst 3560*

6. - Switch *D-link DGS-3627.*

7. – Router *Cisco2600/2800 Series.*

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

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

NOTA/ADVERTENCIA:

No es necesaria la configuración de listas de acceso en la siguiente topología.

Una vez implementada la Red correr el programa (PUTTY, TERATERM) para la modificación de claves y nombres de los Switches y Routers.

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

TOPOLOGÍA:

La Figura 3.11. Nos muestra la topología de Red, de la práctica #11.

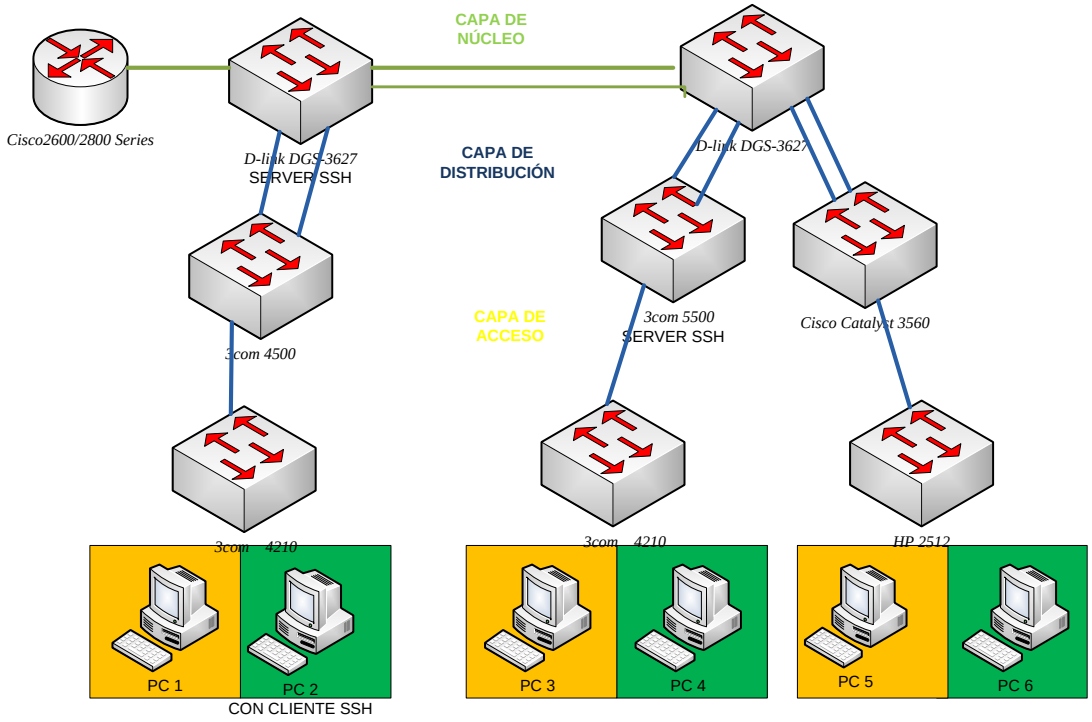


Figura 3.11. Topología de Red Práctica #11

3.3.12. Práctica #12 Simulación de una Red Jerárquica que permita la Administración con SNMP (SIMPLE NETWORK MANAGEMENT PROTOCOL)

TEMA: Simulación de una Red Jerárquica que permita la administración con SNMP (Simple Network Management Protocol).

OBJETIVOS:

a) Aplicar las funciones que nos ofrece la administración con SNMP.

b) Simular una Red Jerárquica que permita la administración con SNMP.

c) ***Este Objetivo se plantea el alumno.***

MARCO TEORICO:

SNMP

Es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. Permite a los administradores supervisar el funcionamiento de la red, buscar y resolver sus problemas, y planear su crecimiento.

Las versiones de SNMP más utilizadas son SNMP versión 1 (SNMPv1) y SNMP versión 2 (SNMPv2).

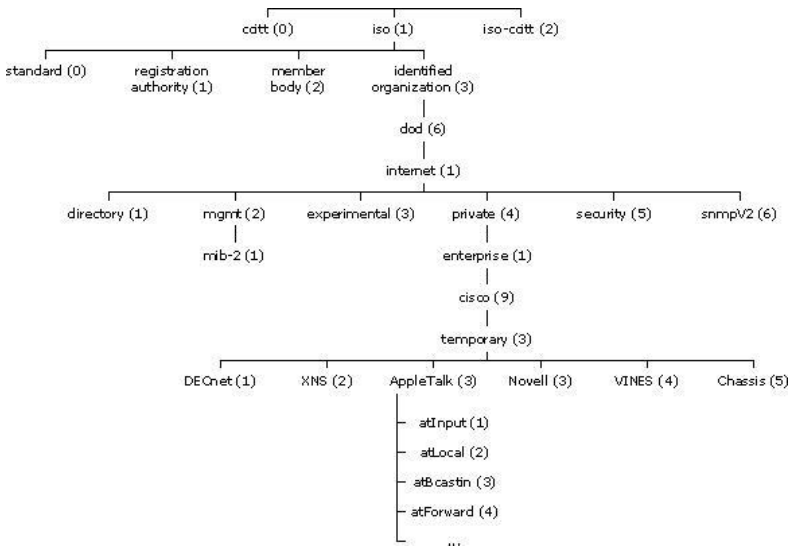
SNMP en su última versión (SNMPv3) posee cambios significativos con relación a sus predecesores, sobre todo en aspectos de seguridad

SNMP MIB (Base de Información de Administración)

"Es una colección de información que está organizada jerárquicamente. Las MIB's son accedidas usando un protocolo de administración de red (SNMP).

Un objeto administrado es uno de cualquier número de características específicas de un dispositivo administrado. Los objetos administrados están compuestos de una o más instancias de objeto, que son esencialmente variables." [12]

Un identificador de objeto (*object ID*) identifica únicamente a un objeto administrado en la jerarquía MIB. La jerarquía MIB puede ser representada como un árbol con una raíz anónima y los niveles, que son asignados por diferentes organizaciones.



El objeto administrado atInput podría ser identificado por el nombre de objeto *so.identified-organization.dod.internet.private.enterprise.cisco.temporary.AppleTalk.atInput* o por el descriptor de objeto equivalente *1.3.6.1.4.1.9.3.3.1*.

EQUIPOS:

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

1. - Software a utilizar (PACKET TRACER).

2. - Switch *Cisco 2960.*

3. - Switch *Cisco 3560.*

4. – Router *Cisco 2811 Series.*

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

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

NOTA/ADVERTENCIA:

No es necesaria la configuración de listas de acceso en la siguiente topología.

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

TOPOLOGÍA:

La Figura 3.12. Nos muestra la topología de Red, de la práctica #12.

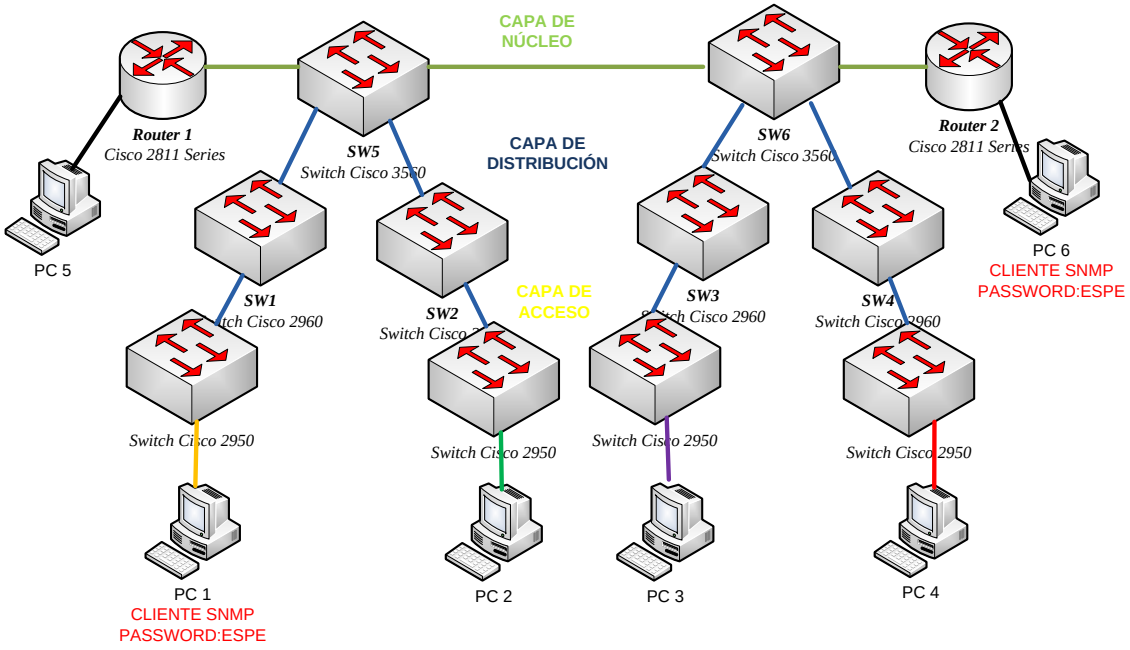


Figura 3.12. Topología de Red Práctica #12

3.3.13. Práctica #13 Configuración IPv6 en un Switch Capa 3

TEMA: Configuración IPv6 en un Switch capa 3.

OBJETIVOS:

a) Utilizar los comandos necesarios para la configuración IPv6 en un Switch capa 3

b) Entender la importancia de IPv6 en la actualidad que ventajas nos brinda.

c) ***Este Objetivo se plantea el alumno.***

MARCO TEORICO:

IPv6:

Cuando utilizamos Internet para cualquier actividad, ya sea correo electrónico, navegación web, descarga de ficheros, o cualquier otro servicio o aplicación, la

comunicación entre los diferentes elementos de la red y nuestro propio ordenador o teléfono, utiliza un protocolo que denominamos Protocolo de Internet (IP, Internet Protocol).

En los últimos años, prácticamente desde que Internet tiene un uso comercial, la versión de este protocolo es el número 4 (IPv4).

"*Para que los dispositivos se conecten a la red, necesitan una dirección IP. Cuando se diseñó IPv4, casi como un experimento, no se pensó que pudiera tener tanto éxito comercial, y dado que sólo dispone de 2^32 direcciones (direcciones con una longitud de 32 bits, es decir, 4.294.967.296 direcciones), junto con el imparable crecimiento de usuarios y dispositivos, implica que en pocos meses estas direcciones se agotarán." [13]*

Por este motivo, y previendo la situación, el organismo que se encarga de la estandarización de los protocolos de Internet (IETF, Internet Engineering Task Force), ha trabajado en los últimos años en una nueva versión del Protocolo de Internet, concretamente la versión 6 (IPv6), que posee direcciones con una longitud de 128 bits, es decir 2^128 posibles direcciones (340.282.366.920.938.463.463.374.607.431.768.211.456), o dicho de otro modo, 340 sextillones.

El protocolo IPv6 tiene las características siguientes:

- Nuevo formato de encabezado.
- Espacio de direcciones más grande.
- Infraestructura de direcciones y enrutamiento eficaz y jerárquica.
- Configuración de direcciones con y sin estado.
- Seguridad integrada.
- Mejora de la compatibilidad para la calidad de servicio (QoS).
- Nuevo protocolo para la interacción de nodos vecinos.
- Capacidad de ampliación.

EQUIPOS:

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

1. – Switch *3com 5500.*

2. - Switch *Cisco 3560.*

3. - Switch *D-link DGS-3627.*

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

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

NOTA/ADVERTENCIA:

No es necesaria la configuración de listas de acceso en la siguiente topología.

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

TOPOLOGÍA:

La Figura 3.13. Nos muestra la topología de Red, de la práctica #13.

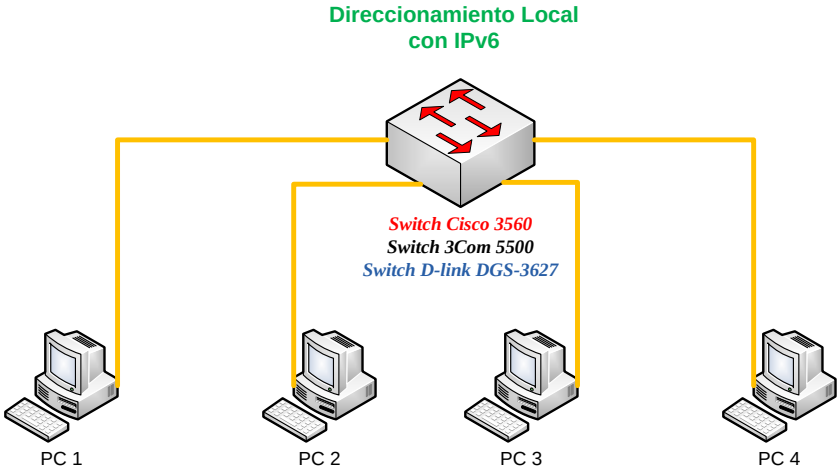


Figura 3.13. Topología de Red Práctica #13

3.3.14. Práctica #14 Enrutamiento Dinámico (RIPng) IPv6 en un entorno LAN con Switch Capa 3

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

OBJETIVOS:

a) Conocer el Enrutamiento Dinámico RIPng que utiliza el Switch capa 3 con soporte IPv6.

b) Entender la importancia de IPv6 en la actualidad y que ventajas nos brinda.

c) ***Este Objetivo se plantea el alumno.***

MARCO TEORICO:

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." [14]*

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).

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:

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

TOPOLOGÍA:

La Figura 3.14. Nos muestra la topología de Red, de la práctica #14.

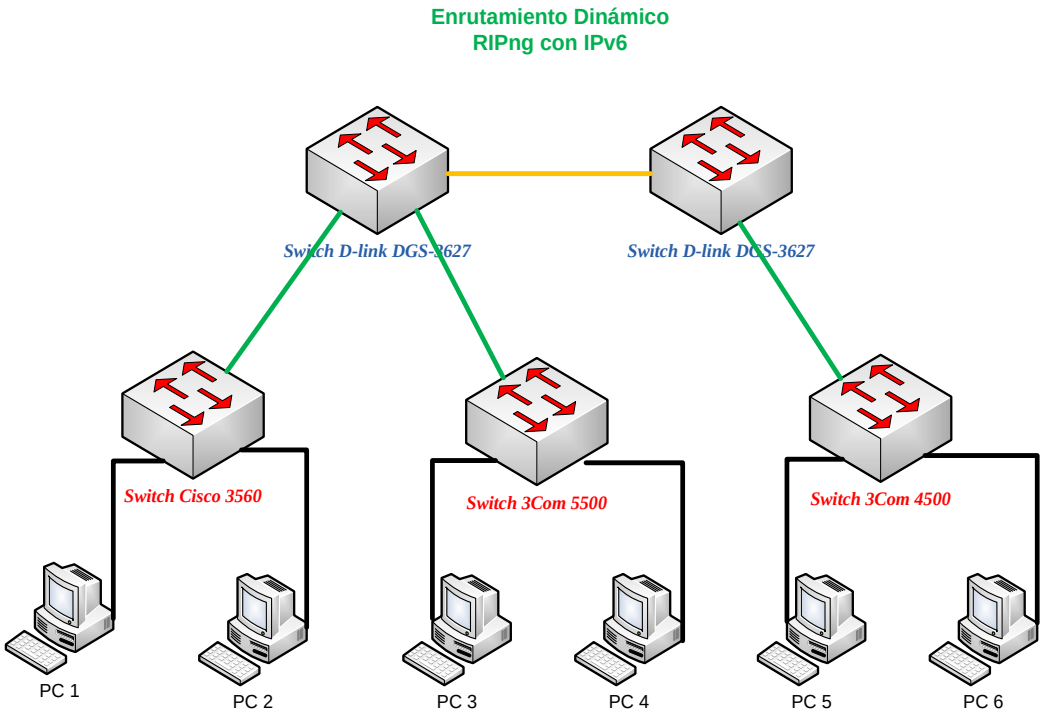


Figura 3.14. Topología de Red Práctica #14

3.3.15. Práctica #15 Configuración de IPv6 Tunneling en un entorno LAN

TEMA: Configuración de IPv6 Tunneling en un entorno LAN.

OBJETIVOS:

a) Conocer la configuración IPv6 Tunneling Switch capa 3.

b) ***Este Objetivo se plantea el alumno.***

MARCO TEORICO:

IPv6 tunneling: *"Consiste en encapsular los paquetes de IPv6 dentro de los headers de IPv4 para transportarlos sobre las estructuras de enrutamiento actuales. Los dos tipos de túneles que se emplean son: configurados y automáticos.*

La infraestructura IPv6 está en una constante evolución. Mientras esta infraestructura se desarrolla y se expande, la infraestructura de enrutamiento existente (IPv4) puede seguir funcionando y ser utilizada para transportar trafico IPv6. Tunneling provee un camino para lograr esto" [15].

Los hosts y routers IPv6/IPv4 pueden pasar datagramas IPv6 sobre regiones de topología de enrutamiento IPv4 encapsulándolos dentro de paquetes IPv4.

Tunneling puede ser usado en una variedad de formas:

- ***Router-to-Router*:** Los routers IPv6/IPv4 interconectados con una infraestructura IPv4 pueden pasarse entre sí paquetes IPv6. En este caso el túnel abarca un segmento del trayecto que toma el paquete IPv6.
- ***Host*-to-Router:** Los host IPv6/IPv4 pueden pasar paquetes IPv6 por un router IPv6/IPv4 intermediario que sea alcanzable por la infraestructura IPv4. Este tipo de túnel abarca el primer segmento del trayecto del paquete.
- ***Host-to-Host*:** Los hosts IPv6/IPv4 interconectados con una infraestructura IPv4 pueden pasarse paquetes IPv6 entre sí. En este caso el túnel abarca el recorrido completo que toman los paquetes.
- ***Router-to-Host*:** Los routers IPv6/IPv4 pueden pasar paquetes IPv6 hasta su host IPv6/IPv4 destinatario (final). Este túnel abarca el último segmento del recorrido.

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 4500.*

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

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

NOTA/ADVERTENCIA:

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

TOPOLOGÍA:

La Figura 3.15. Nos muestra la topología de Red, de la práctica #15.

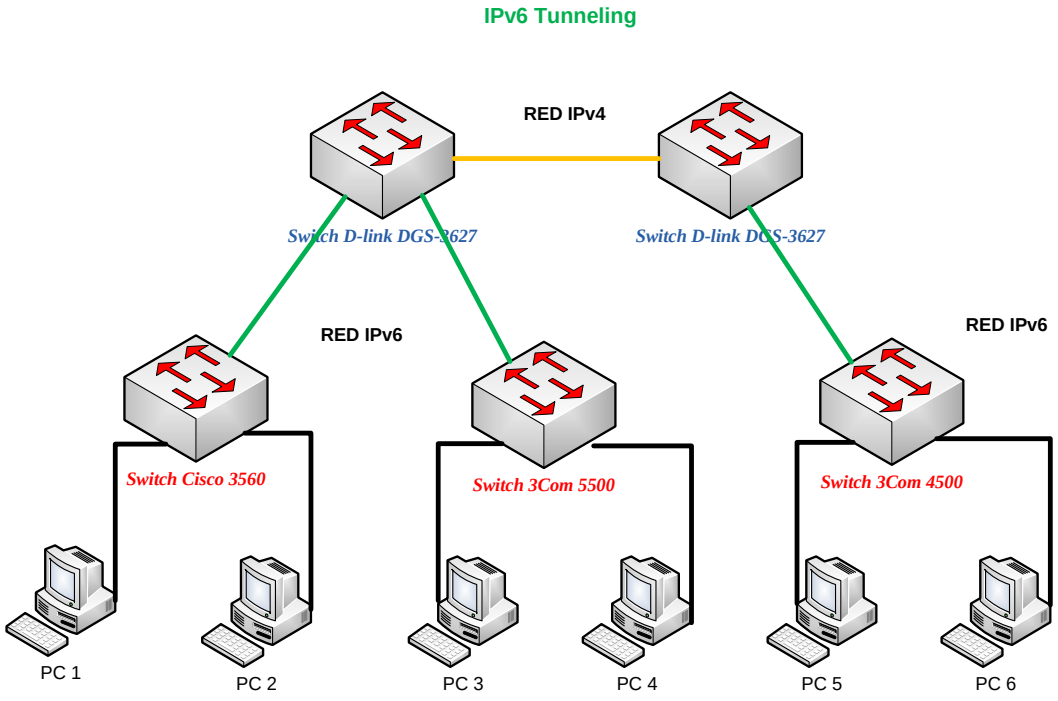


Figura 3.15. Topología de Red Práctica #15

3.3.16. Práctica #16 Configuración del Servidor AAA para Acceso TELNET en un entorno LAN

TEMA: Configuración del Servidor AAA para acceso TELNET en un entorno LAN.

OBJETIVOS:

a) Conocer la configuración del Servidor AAA.

b) Entender la importancia de un Servidor de autenticación como sistema de seguridad.

c) ***Este Objetivo se plantea el alumno.***

MARCO TEORICO:

SERVIDOR AAA

Un intruso puede ganar acceso a equipamiento de red y servicios sensibles. Para ayudar a prevenir el acceso no deseado, el control de acceso es necesario. El control de acceso limita quién o qué puede usar recursos específicos así como servicios u opciones disponibles una vez que se otorga el acceso.

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).

EQUIPOS:

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

1. – Switch *3Com 4500.*

2. - Switch *HP 2512.*

3.- Computador con Cliente/Servidor AAA.

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

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

NOTA/ADVERTENCIA:

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

TOPOLOGÍA:

La Figura 3.16. Nos muestra la topología de Red, de la práctica #16.

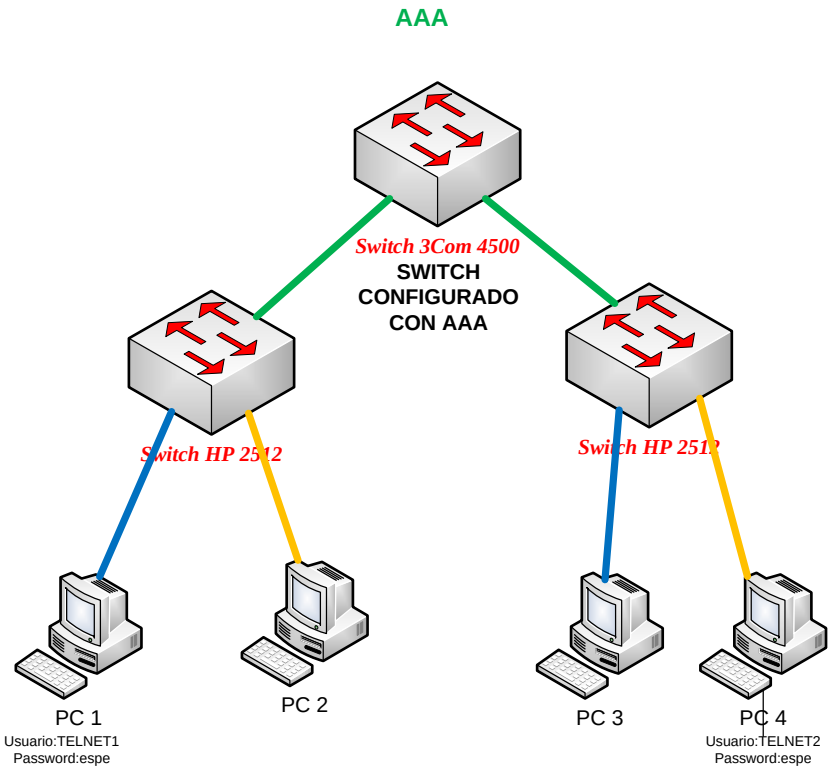


Figura 3.16. Topología de Red Práctica #16

3.3.17. Práctica #17 Simulación de una Red que brinde Autenticación (AAA) y QoS (802.1p)

TEMA: Simulación de una Red que brinde Autenticación (AAA) y QoS (802.1p).

OBJETIVOS:

a) Simular una Red que permita Autenticación y QoS.

b) Comprender la importancia de brindar QoS en un entorno LAN.

c) ***Este Objetivo se plantea el alumno.***

PROBLEMA PROPUESTO:

La empresa "Redes" necesita como medio de seguridad autenticar al empleado "técnico" con el fin de acceder remotamente al Router (R3) y al empleado "jefe de seguridad" para acceder remotamente al Router (R2), por consiguiente se tendrá que implementar un servidor AAA (PC) y la configuración de un Router que permita la autenticación de los empleados. La empresa también requiere que se dé prioridad (802.1p) a los puertos que están conectados los gerentes de la empresa. Resolver el problema basándose en la topología propuesta.

EQUIPOS:

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

1. – Switch *Cisco 2960.*

2. - Router *Cisco 2811*.

3. – Servidor Radius.

4. - Software a utilizar (PACKET TRACER).

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:

La Figura 3.17. Nos muestra la topología de Red, de la práctica #17.

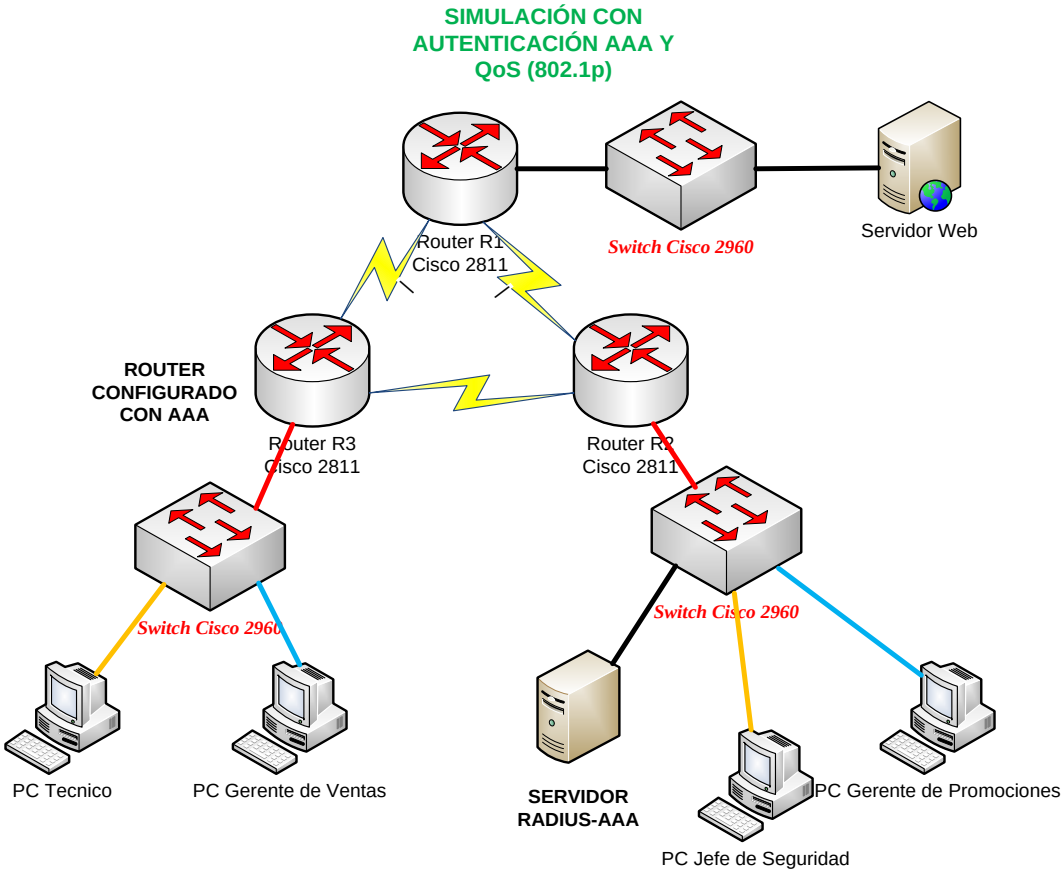


Figura 3.17. Topología de Red Práctica #17

3.3.18. Práctica #18 Implementación de una Red IPv4 Operativa que brinde (VLAN, ACL, AAA, SSH, QoS)

TEMA: Diseño e implementación de una red IPv4 operativa que brinde (Vlan, ACL, AAA, SSH, QoS).

OBJETIVOS:

a) Aplicar los conocimientos aprendidos acerca de (VLAN, ACL, AAA, SSH, QoS).

b) Determinar la Solución más óptima para cumplir con los requerimientos propuestos.

c) ***Este Objetivo se plantea el alumno.***

PROBLEMA PROPUESTO:

La empresa "Networking" requiere la implementación de una Red operativa IPv4 que brinde (VLAN, ACL, AAA, SSH, QoS), para lo cual se necesita que la Red Local esté dividida en diferentes departamentos estos son: Empleados, Gerentes, Administradores de Red. El Gerente 3 puede ver a todas las computadoras al igual que los administradores de Red, mientras que los empleados y los otros dos gerentes no podrán verle al Gerente 3 ni a los administradores de Red.

La prioridad en el tráfico de la Red tendrá los puertos a los que estén conectados los Gerentes.

Existen 3 Administradores de Red el primero tendrá acceso Remoto al Switch SW2 por medio de SSH. El segundo podrá acceder al Switch SW3 vía telnet configurando en el Switch AAA el tercero podrá configurar los Routers y el Switch 4 vía Telnet.

EQUIPOS:

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

1. – Switch *3Com 4210.*

2. – Switch *3Com 4500.*

3. – Switch *D-Link DGS-3627.*

4. - Router *Cisco 2000 series.*

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

NOTA/ADVERTENCIA:

Los Routers/Switch L3 estarán configurados con el protocolo de enrutamiento vector distancia RIP v2

Las listas de acceso serán configuradas de la forma más óptima posible dependiendo el criterio del estudiante

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

TOPOLOGÍA:

La Figura 3.18. Nos muestra la topología de Red, de la práctica #18.

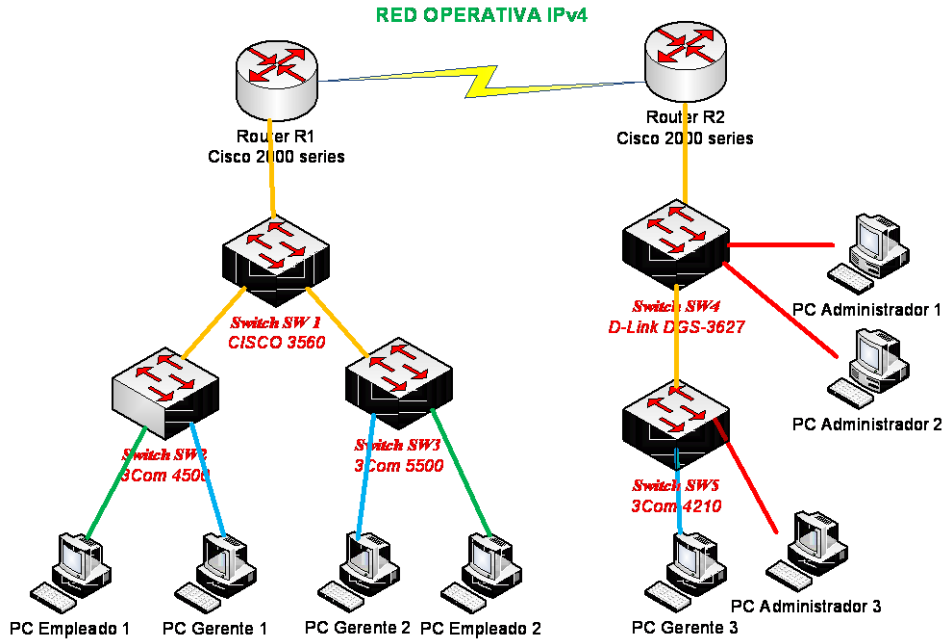


Figura 3.18. Topología de Red Práctica #18

3.3.19. Práctica #19 Implementación de una Red Operativa IPv6 con OSPFv3

TEMA: Implementación de una Red operativa IPv6 con OSPFv3.

OBJETIVOS:

a) Implementar una Red operativa IPv6 aplicando conceptos de OSPFv3.

b) ***Este Objetivo se plantea el alumno***

MARCO TEORICO:

OSPFv3.

"Es un protocolo de enrutamiento por estado del enlace el cual fue descrito por primera vez en el RFC 2740. El protocolo OSPFv3 trabaja con direcciones IPv6, distribuyendo por la red solamente el prefijo de estas direcciones." [16] No posee soporte para direcciones IPv4, razón por la cual si se desea tener dentro de la misma

red direcciones IPv6 y direcciones IPv4 se deben configurar tanto el protocolo OSPFv2 como su versión 3.

El protocolo OSPFv3 tiene los mismos fundamentos que el protocolo OSPFv2 (Algoritmo SPF, inundaciones, elección del DR, áreas, métricas, temporizadores), pero a pesar de tener ciertas similitudes también poseen diferencias entre las cuales tenemos:

· OSPFv3 trabaja sobre un enlace en vez de hacerlo sobre subred.

· La topología OSPFv2 no soporta el protocolo IPv6.

· OSPFv3 posee un mecanismo de autenticación (RFC 4552).

· OSPFv3 posee multiples instancias por enlace.

EQUIPOS:

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

1. – Switch *3Com 5500.*

2. – Switch *3Com 4500.*

3. - Switch *3Com 4210.*

4. – Switch *D-link DGS-3627.*

5. – Switch *CISCO 3560.*

6. – Router *CISCO 2800.*

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

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

PROBLEMA PROPUESTO:

La empresa “Networking” la implementación de una Red operativa IPv6 que brinde: Enrutamiento dinámico OSFPv3 y administración por medio de SSH al Switch 2 D-link 3627.

Se requiere que el Router Cisco 2800 pueda ser configurado Remotamente vía telnet

Para cumplir con el éxito de la práctica se deberá realizar la implementación que se muestra en la siguiente Topología

NOTA/ADVERTENCIA:

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

TOPOLOGÍA:

La Figura 3.19. Nos muestra la topología de Red, de la práctica #19.

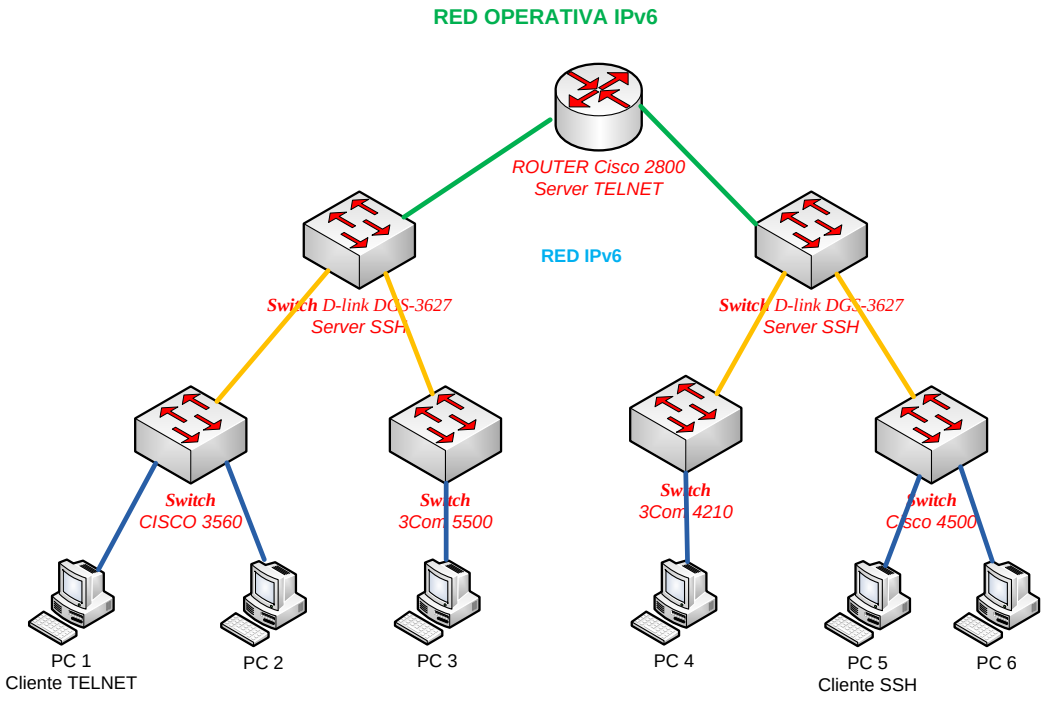


Figura 3.19. Topología de Red Práctica #19

CAPÍTULO 4

DESARROLLO DE PRÁCTICAS DE LABORATORIO Y MANUAL DEL DOCENTE

4.1. INTRODUCCIÓN

En el siguiente Capítulo se llevará a cabo el desarrollo de las prácticas propuestas en el Capítulo 3, indicando paso a paso cada configuración utilizada con el fin de crear un manual para el docente y facilitar el método de enseñanza del mismo.

Cada práctica en este Capítulo se basará exclusivamente en el desarrollo del campo CONFIGURACIONES/DIRECCIONAMIENTO propuesto en el Capítulo 3.

4.2. DESARROLLO PRÁCTICA #1 CONFIGURACIÓN BÁSICA DEL SWITCH

4.2.1. Configuraciones/Direccionamiento

En esta práctica se accederá al Switch (*3com 4500, HP 2512*) con un cable de consola y el Switch *D-link DES-3526* con un cable de Red.

Configuración:

- Switch (*3com 4500, HP 2512*) acceso via hyperterminal (TERA TERM, PUTTY)
- Switch *D-link DES-3526* acceso vía dirección IP 10.90.90.90

4.2.2. Procedimiento

4.2.2.1. Configuración Hyperterminal TERATERM

1.- Accedemos al Hyperterminal (TERA TERM). La Figura 4.1. Nos muestra la imagen de inicio del programa TERATERM

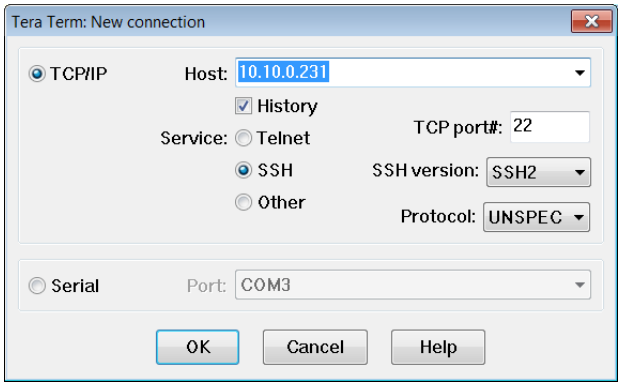


Figura 4.1. Inicio TeraTerm Práctica #1

2.- En la Figura 4.2. Escogemos la opción SERIAL y el puerto COM 6 y presionamos OK.

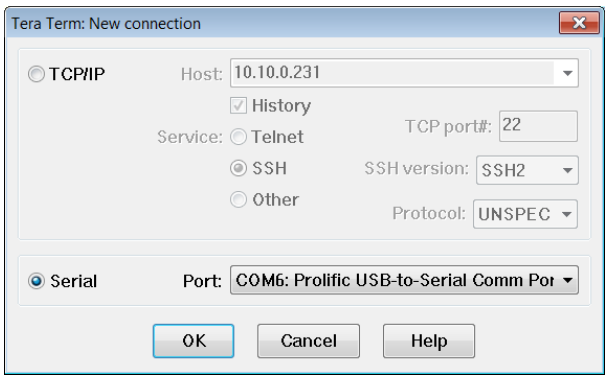


Figura 4.2. Configuración TeraTerm Práctica #1

3.- Una vez que se muestra la pantalla de conexión cambiamos el parámetro baud rate del Serial Port (*Setup --- Serial Port*) en algunos equipos se debe poner 19200 y en otros se deja la configuración predeterminada (9600). En la Figura 4.3. Nos muestra la pantalla de Setup del puerto Serial

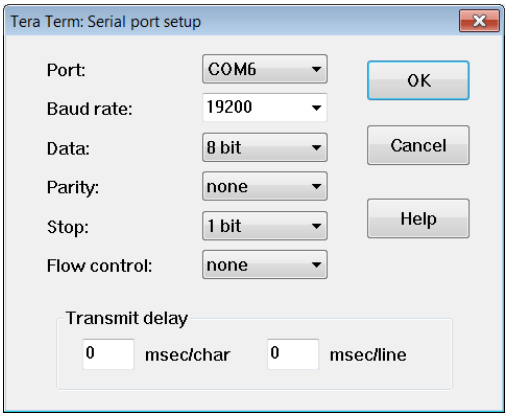


Figura 4.3. Setup Puerto Serial TeraTerm Práctica #1

4.- Configurado de manera correcta el Serial Port nos saldrá una pantalla como la siguiente. La Figura 4.4. Nos muestra la Pantalla de Inicio del Switch.

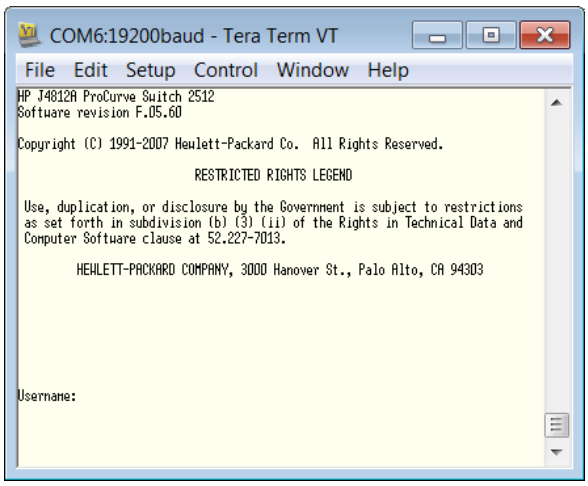


Figura 4.4. Inicio Switch Práctica #1

4.2.2.2. Configuración Switch 3com 4500

1.- Ingresamos al Switch como usuario: admin y sin password entraremos al modo usuario del Switch

```
Login authentication


Username:admin
Password:
<4500>
%Apr  2 00:19:28:685 2000 4500 SHELL/5/LOGIN:- 1 - admin(aux0) in unit1 login
<4500>
```

2.- Para acceder al modo privilegiado/configuración escribimos *system-view*

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]
```

3.- Si deseamos cambiar el nombre al equipo lo hacemos mediante el comando *sysname "nombre"*

```
[4500]sysname  SWITCH
[SWITCH]
```

4.- Agregamos una dirección IP 192.168.1.5/24 al Switch.

```
[SWITCH]interface vlan-interface 1
[SWITCH-Vlan-interface1]ip address 192.168.1.5 255.255.255.0
[SWITCH-Vlan-interface1]quit
```

5.- Cambiamos la contraseña al iniciar al Switch que por defecto esta deshabilitado.

```
[SWITCH]local-user admin
[SWITCH-luser-admin]password simple espe
[SWITCH-luser-admin]quit
```

6.- El comando para ver la información del sistema del Switch es *display seguido del parámetro que queramos observar.*

```
[SWITCH] display ip interface vlan 1
Vlan-interface1 current state :DOWN
Line protocol current state :DOWN
Internet Address is 192.168.1.5/24 Primary
Broadcast address : 192.168.1.255
The Maximum Transmit Unit : 1500 bytes
```

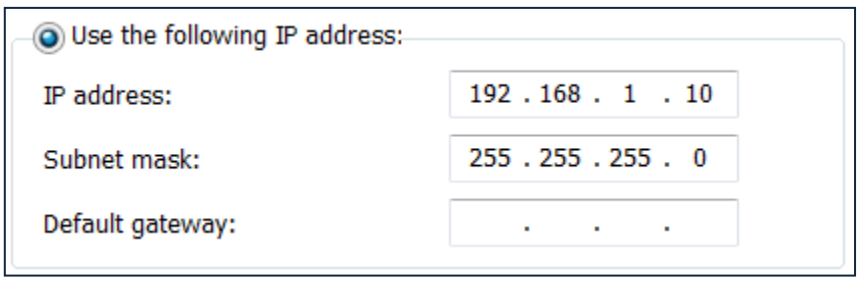
```
[SWITCH]display current-configuration
#
 sysname SWITCH
#
 local-server nas-ip 127.0.0.1 key 3com
#
 igmp-snooping enable
#
radius scheme system
#
domain system
#
local-user admin
 password simple espe
 service-type ssh telnet terminal
 level 3
local-user manager
 password simple manager
 service-type ssh telnet terminal
 level 2
local-user monitor
 password simple monitor
 service-type ssh telnet terminal
  ---- More ----
```

7.- Guardamos la configuración realizada en memoria flash con el comando *save.*

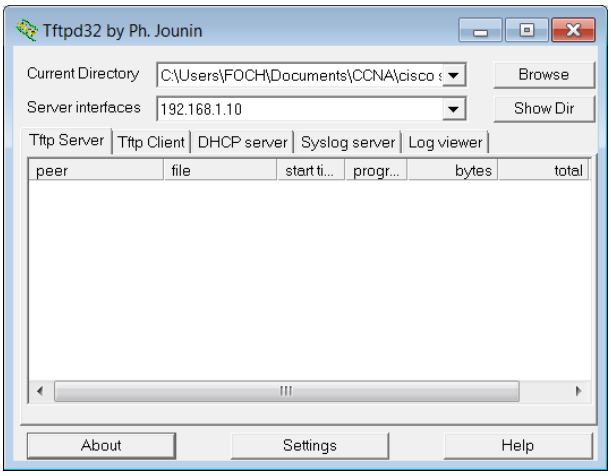
```
[SWITCH]save
The configuration will be written to the device.
Are you sure?[Y/N]y
Please input the file name(*.cfg)(To leave the existing filename
 unchanged press the enter key):
Now saving current configuration to the device.
Saving configuration. Please wait...
....
 Unit1 save configuration flash:/vlan1.cfg successfully

[SWITCH]
%Apr  2 01:03:52:832 2000 SWITCH CFM/3/CFM_LOG:- 1 -Unit1 saved configuration su
ccessfully.
```

8.- Una vez configurado el Switch podemos guardar el archivo de configuración en un Servidor TFTP (*tftpd32*).

I.- configuramos la IP del host que va actuar como servidor TFTP, *la dirección IP debe estar en la misma Red Asignada a la vlan del Switch.*



II.- Abrimos el programa tftpd32 y configuramos la IP.



III.- Guardamos el archivo de configuración desde el Switch al Servidor TFTP, primero vemos el directorio del Switch para conocer que archivo queremos subir o bajar del servidor y con el comando ***tftp*** *ip-servidor* ***put/get*** *Nombre archivo orig. Nombre archivo dest* accedemos al servidor. La Figura 4.5. Nos indica la imagen de confirmación del Servidor TFTP.

```
<SWITCH>dir
Directory of unit1>flash:/

  1 (*)   -rw-   3924102  Feb 29 2008 12:00:00   s3n03_03_00s56.app
  2 (*)   -rw-    957047  Feb 29 2008 12:00:00   s3p03_00.web
  3       -rw-      5769  Feb 29 2008 12:00:00   3comoscfg.def
  4       -rw-      5454  Apr 02 2000 00:04:48   3comoscfg.cfg
  5       -rw-      5425  Apr 01 2000 23:58:59   decimo.cfg
  6 (*)   -rw-      4865  Apr 02 2000 01:25:24   vlan1.cfg
```

```
<SWITCH>tftp 192.168.1.10 put 3comoscfg.cfg 3com.cfg
 File will be transferred in binary mode.
 Sending file to remote tftp server. Please wait... /
 TFTP:     5454 bytes sent in 0 second(s).
 File uploaded successfully.
```

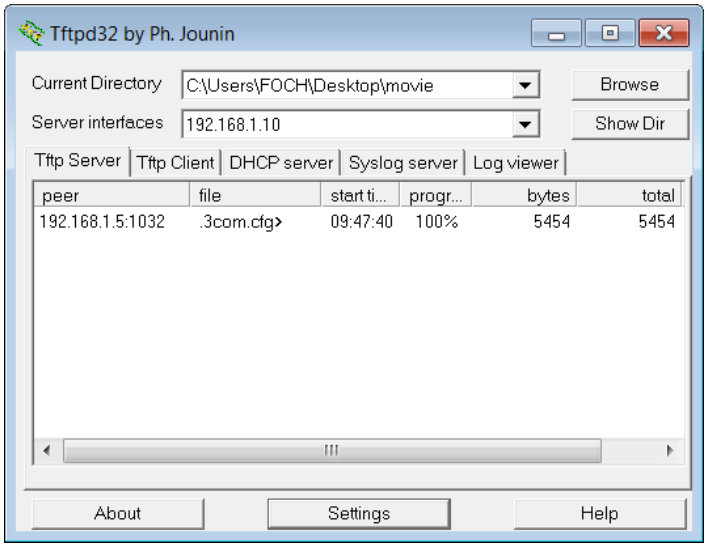


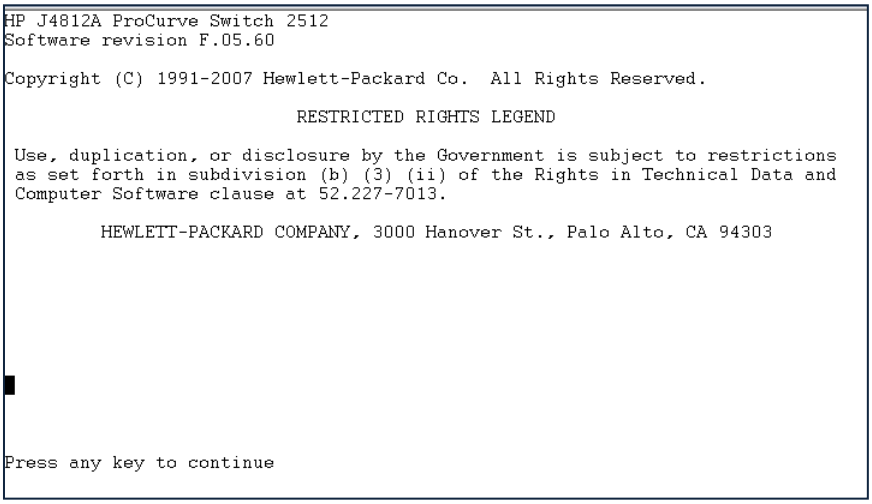
Figura 4.5. Servidor TFTP Switch 3com 4500 Práctica #1

9.- Para dejar al Switch con las configuraciones por defecto ponemos el comando *reset saved-configuration,* luego reiniciamos el equipo.

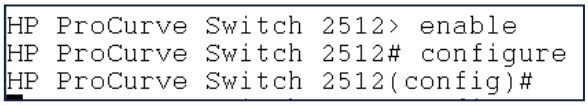
```
<SWITCH>reset saved-configuration
The saved configuration will be erased.
Are you sure?[Y/N]y
Configuration in flash memory is being cleared.
Please wait ...
...
 Unit1 reset saved-configuration successfully.
```

4.2.2.3. Configuración Switch HP 2512

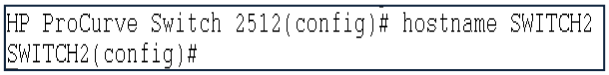
1.- Ingresamos al Switch y presionamos cualquier tecla, *en el caso que pida un usuario y contraseña el usuario: admin y sin contraseña.*



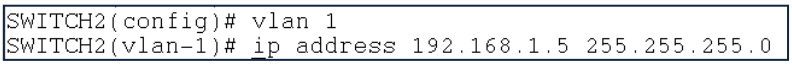
2.- Para acceder al modo privilegiado y configuración escribimos *enable, configure*



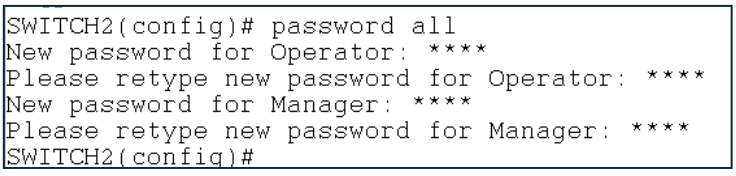
3.- Si deseamos cambiar el nombre al equipo lo hacemos mediante el comando *hostname "nombre"*



4.- Agregamos una dirección IP 192.168.1.5/24 al Switch.



5.- Cambiamos la contraseña al iniciar al Switch que por defecto esta deshabilitado, la clave ahora es "espe".



6.- El comando para ver la información del sistema del Switch es *show seguido del parámetro que queramos observar.*

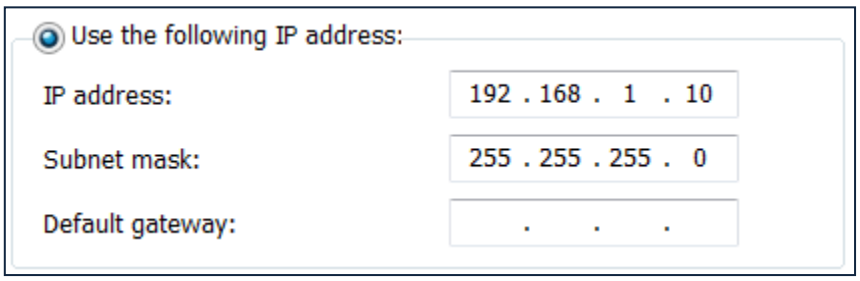
```
SWITCH2# show ip

 Internet (IP) Service


  Default Gateway :
  Default TTL     : 64

  VLAN          | IP Config  IP Address      Subnet Mask
  ------------- + ---------- --------------- ---------------
  DEFAULT_VLAN  | Manual     192.168.1.5     255.255.255.0


  SWITCH2# show config

  Startup configuration:

  ; J4812A Configuration Editor; Created on release #F.05.60

  hostname "HP ProCurve Switch 2512"
  snmp-server community "public" Unrestricted
  vlan 1
     name "DEFAULT_VLAN"
     untagged 1-14
     ip address dhcp-bootp
     exit
  no aaa port-access authenticator active
  password manager
  password operator
```

7.- Guardamos la configuración realizada en memoria flash con el comando *write memory.*

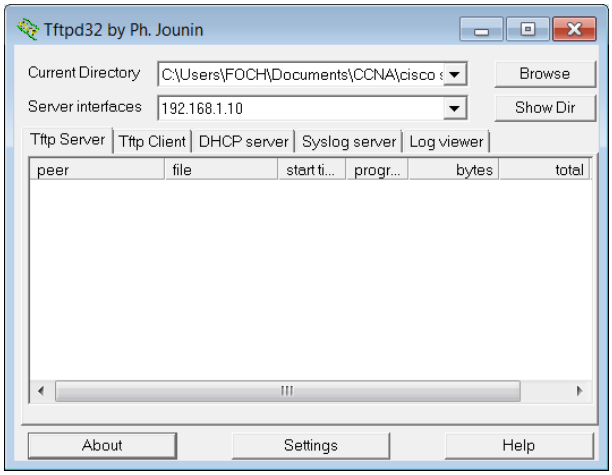
```
SWITCH2# write memory
SWITCH2#
```

8.- Una vez configurado el Switch podemos guardar el archivo de configuración en un Servidor TFTP (*tftpd32*).

I.- configuramos la IP del host que va actuar como servidor TFTP, *la dirección IP debe estar en la misma Red Asignada a la vlan del Switch.*



II.- Abrimos el programa tftpd32 y configuramos la IP.



III.- Guardamos el archivo de configuración desde el Switch al Servidor TFTP, con el comando ***copy startup-config tftp*** *ip-servidor Nombre archivo dest.* La Figura 4.6. Nos indica la imagen de confirmación del Servidor TFTP.

```
SWITCH2# configure
SWITCH2(config)# copy startup-config  tftp 192.168.1.10 pract1sw2
SWITCH2(config)#
```

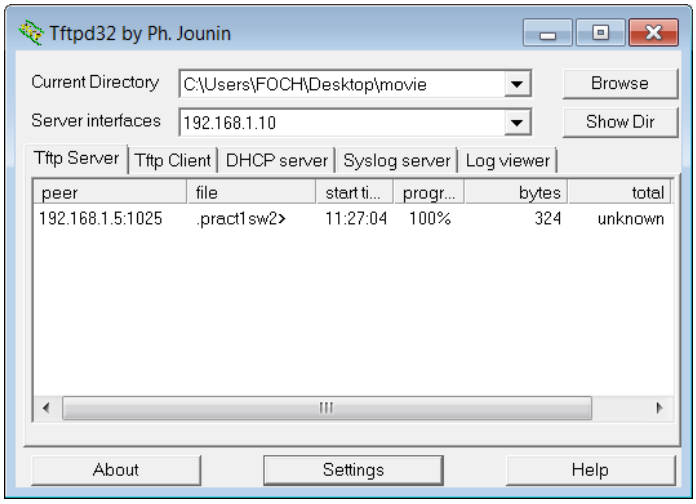


Figura 4.6. Servidor TFTP Switch HP 2512 Práctica #1

9.- Para dejar al Switch con las configuraciones por defecto primero eliminamos los passwords y luego ponemos el comando *erase startup-config, presionamos "y"* luego se reinicia automáticamente el equipo.

```
SWITCH2(config)# no password all
Password protection will be deleted, do you want to continue [y/n]? y
SWITCH2(config)#
```

```
SWITCH2# erase startup-config
Configuration will be deleted and device rebooted, continue [y/n]?  y
```

4.2.2.4. Configuración Switch D-Link DES-3526

1.- Ingresamos al Switch y presionamos 2 veces la tecla “ENTER”.

```
            DES-3526 Fast Ethernet Switch Command Line Interface

                          Firmware: Build 5.00-B28
        Copyright(C) 2000-2004 D-Link Corporation. All rights reserved.
username:
password:

DES-3526:admin#
```

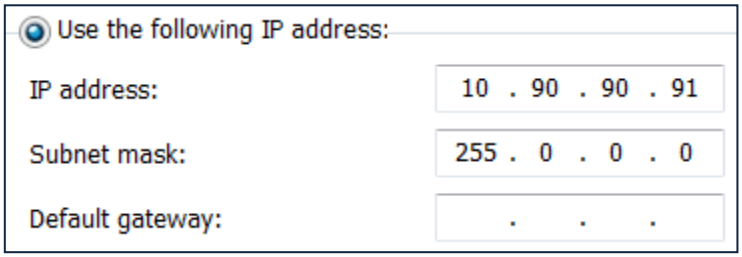
2.- Para crear una cuenta de administrador *create account admin “espe”, password “espe”*

```
DES-3526:admin#create account admin espe
Command: create account admin espe

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

3.- Verificamos la IP del switch con el comando *show ipif*

```
DES-3526:admin#show ipif
Command: show ipif

IP Interface Settings

Interface Name : System
IP Address     : 10.90.90.90     (MANUAL)
Subnet Mask    : 255.0.0.0
VLAN Name      : default
Admin. State   : Enabled
Link Status    : Link DOWN
Member Ports   : 1-26

Total Entries : 1
```

4.- Configuramos la dirección IP en el Pc que nos va a permitir acceder vía web.



5.- Accedemos al Switch mediante un navegador web (firefox, Chrome, etc) *http: //10.90.90.90*, escribimos el usuario y el password de la cuenta creada anteriormente. La Figura 4.7. Nos muestra la pantalla de autenticación del Switch D-link mientras que las Figuras 4.8. Y 4.9. Nos muestran las Pantallas de Configuración del Switch.

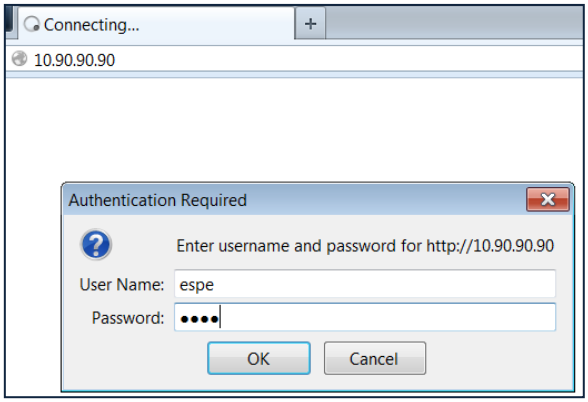


Figura 4.7. Pantalla Autenticación Switch D-Link Práctica #1

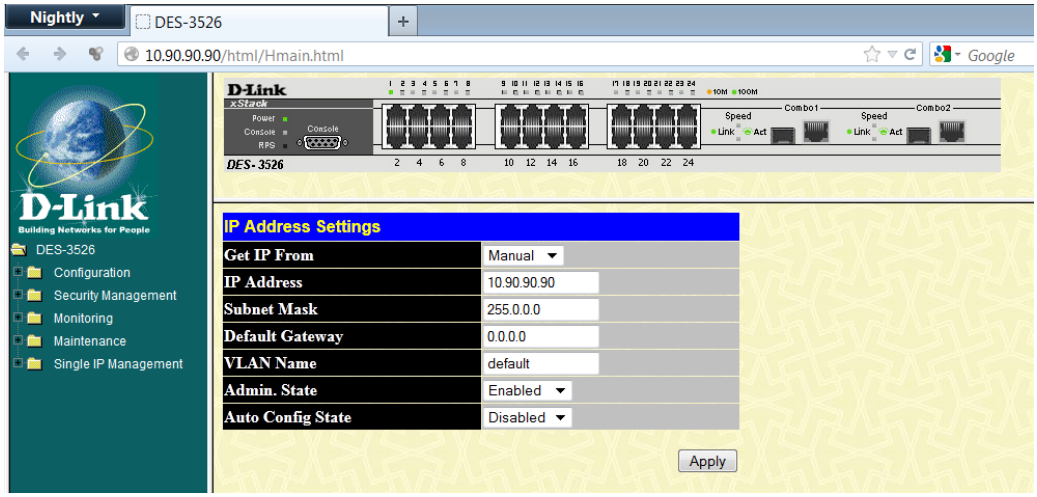


Figura 4.8. Pantalla Configuración 1 Switch D-Link Práctica #1

6.- Cambiamos el nombre del Switch ingresando a las pestañas *Configuration---Switch Information*, aplicando los cambios se guardan las configuraciones hechas.

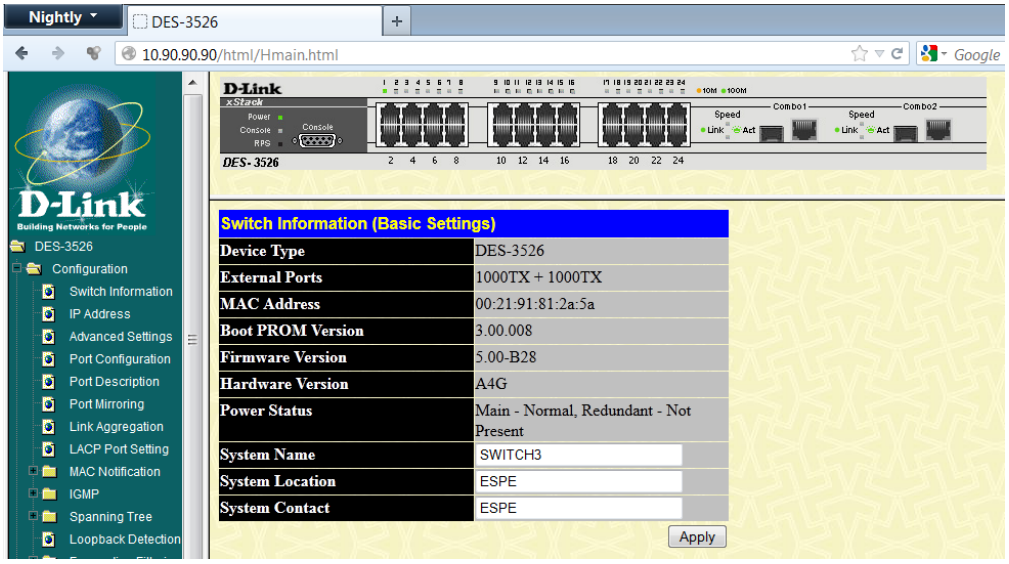
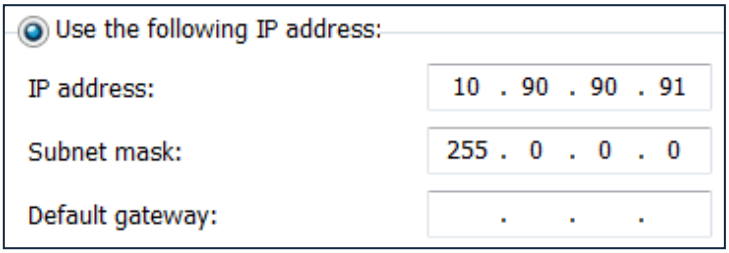


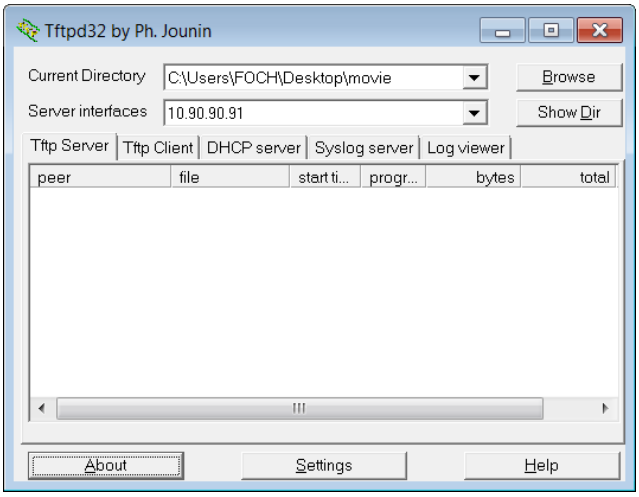
Figura 4.9. Pantalla Configuración 2 Switch D-Link Práctica #1

7.- Una vez configurado el Switch podemos guardar el archivo de configuración en un Servidor TFTP (*tftpd32*).

I.- configuramos la IP del host que va actuar como servidor TFTP, *la dirección IP debe estar en la misma Red Asignada a la vlan del Switch.*



II.- Abrimos el programa tftpd32 y configuramos la IP.



III.- Guardamos el archivo de configuración desde el Switch al Servidor TFTP, con el comando *upload cfg_toTFTP ip-servidor Nombre archivo dest.* La Figura 4.10. Nos indica la imagen de confirmación del Servidor TFTP.

```
DES-3526:admin#upload cfg_toTFTP 10.90.90.91  pract1sw3
Command: upload cfg_toTFTP 10.90.90.91 pract1sw3

Connecting to server................... Done.
Upload configuration................... Done.
```

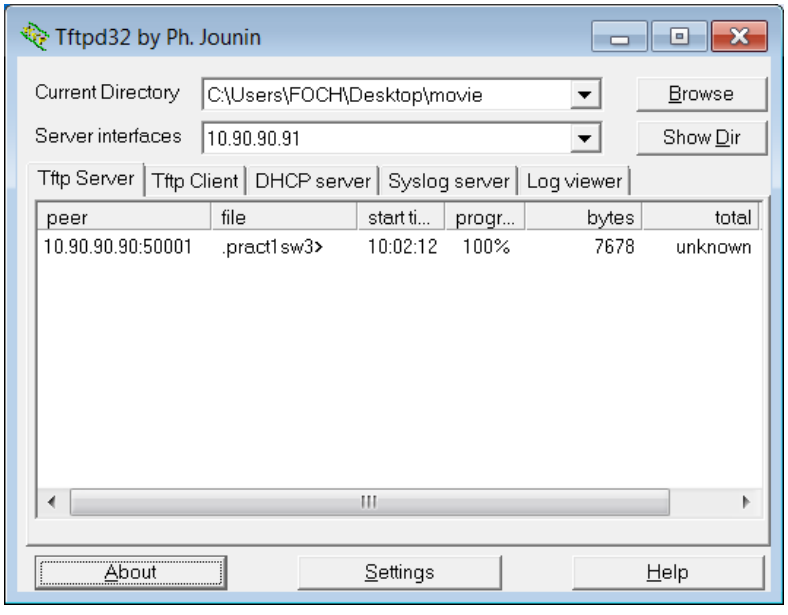


Figura 4.10. Servidor TFTP Switch D-link Práctica #1

8.- Para dejar al Switch con las configuraciones por defecto primero eliminamos los passwords y luego ponemos el comando *reset config*, presionamos *"y"* luego se reinicia automáticamente el equipo.

```
DES-3526:admin#reset config
Command: reset config

Are you sure to proceed with system reset?(y/n)
Success.
```

4.3. DESARROLLO PRÁCTICA #2 CONFIGURACIÓN DE TELNET

4.3.1. Configuraciones/Direccionamiento

Direccionamiento:

DISPOSITIVO	Dirección IP	Máscara de Red	Interfaz
Switch	**192.168.1.1**	**255.255.255.0**	**Vlan 1**
PC1	**192.168.1.2**	**255.255.255.0**	**Ethernet**

Usuario y Password:

Usuario: admin

Password: espe

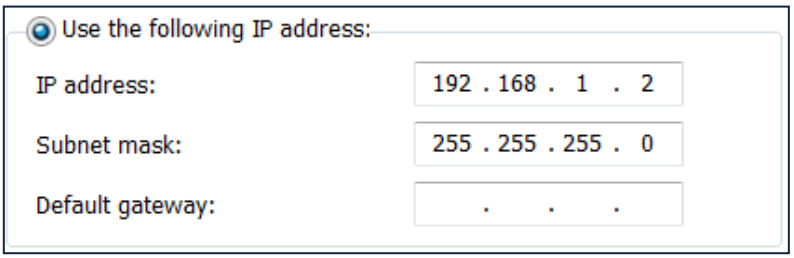
4.3.2. Procedimiento

4.3.2.1. Configuración TELNET Cisco Catalyst 3560

1.- Accedemos al Switch y configuramos nombre, contraseña, y una dirección IP.

```
Press RETURN to get started.


CISCO>enable
CISCO#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
CISCO(config)#hostname Switch
Switch(config)#enable password espe
Switch(config)#interface vlan 1
Switch(config-if)#ip address 192.168.1.1 255.255.255.0
```

2.- Configuramos la dirección de PC1 y hacemos prueba de conectividad con el switch utilizando el comando *Ping*.




```
C:\Users\FOCH>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=4ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 4ms, Average = 1ms
```

3.- Para configurar Telnet en el Switch Cisco Catalyst 3560 utilizamos los siguientes comandos.

```
Switch(config)#line vty 0 15
Switch(config-line)#password espe
Switch(config-line)#login
```

4.- Comprobamos el acceso vía Telnet utilizando el programa TERA TERM, Abrimos el programa y escogemos la opción *TCP/IP---Telnet y ponemos la dirección IP del Switch.* Presionamos “OK”. En la Figura 4.11. Nos muestra la pantalla de Conexión para acceso TELNET.

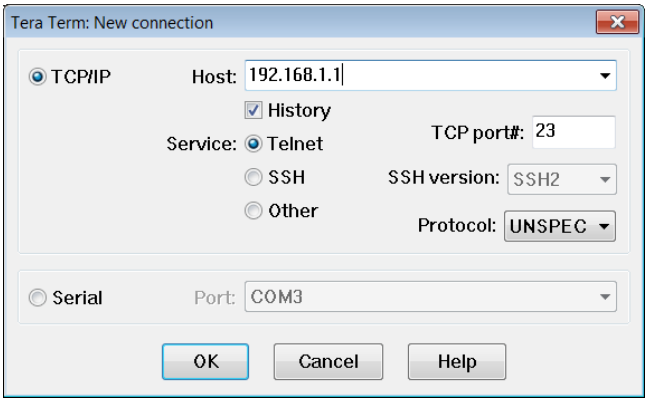


Figura 4.11. TeraTerm Conexión TELNET Switch Cisco 3560 Práctica #2

5.- Una vez que ingresemos nos pedirá las contraseñas correspondientes al acceso vía telnet y para ingresar al Switch con modo privilegiado. También podemos cambiar el nombre del dispositivo. En la Figura 4.12. Nos muestra la imagen de Acceso vía TELNET al Switch Cisco Catalyst 3560.

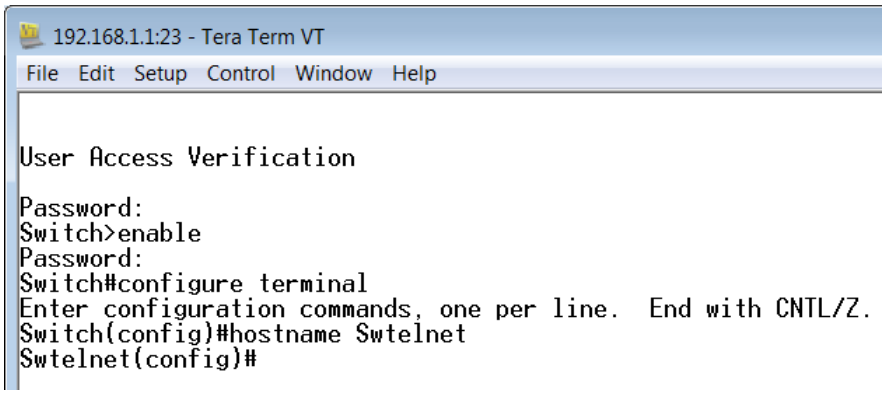


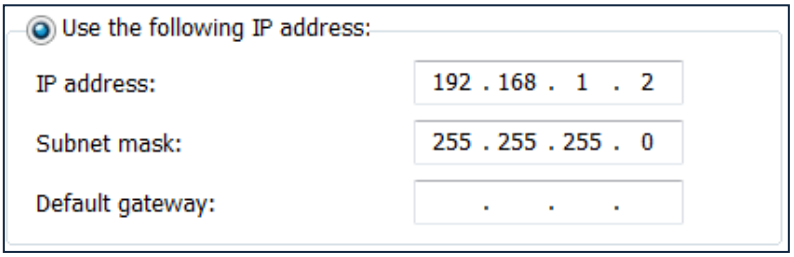
Figura 4.12. Conexión TELNET Cisco Catalyst 3560 Práctica #2

4.3.2.2. Configuración TELNET Switch 3Com 4210

1.- Accedemos al Switch y configuramos nombre, contraseña, y una dirección IP.

```
<4210>system-view
System View: return to User View with Ctrl+Z.
[4210]sysname Switch1
[Switch1]interface vlan 1
[Switch1-Vlan-interface1]ip address 192.168.1.1 255.255.255.0
```

2.- Configuramos la dirección de PC1 y hacemos prueba de conectividad con el switch utilizando el comando *Ping*.




```
C:\Users\FOCH>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=4ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 4ms, Average = 1ms
```

3.- Para configurar Telnet en el Switch 3com 4210 utilizamos los siguientes comandos.

```
<Switch1>system-view
System View: return to User View with Ctrl+Z.
[Switch1]user-interface vty 0
[Switch1-ui-vty0]set authentication password simple espe
```

4.- Comprobamos el acceso vía Telnet utilizando el programa TERA TERM, Abrimos el programa y escogemos la opción *TCP/IP---Telnet y ponemos la dirección IP del Switch.* Presionamos "OK". En la Figura 4.13. Nos muestra la pantalla de Conexión para acceso TELNET.

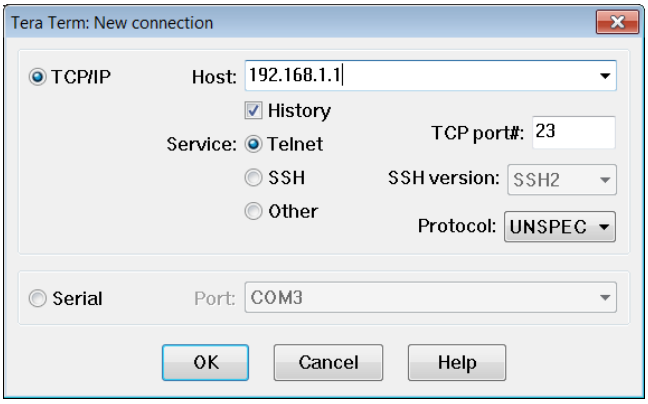


Figura 4.13. TeraTerm Conexión TELNET Switch 3Com 4210 Práctica #2

5.- Una vez que ingresemos nos pedirá las contraseñas correspondientes al acceso vía telnet y para ingresar al Switch con modo privilegiado. También podemos cambiar el nombre del dispositivo. En la Figura 4.14. Nos muestra la imagen de Acceso vía TELNET al Switch 3Com 4210.

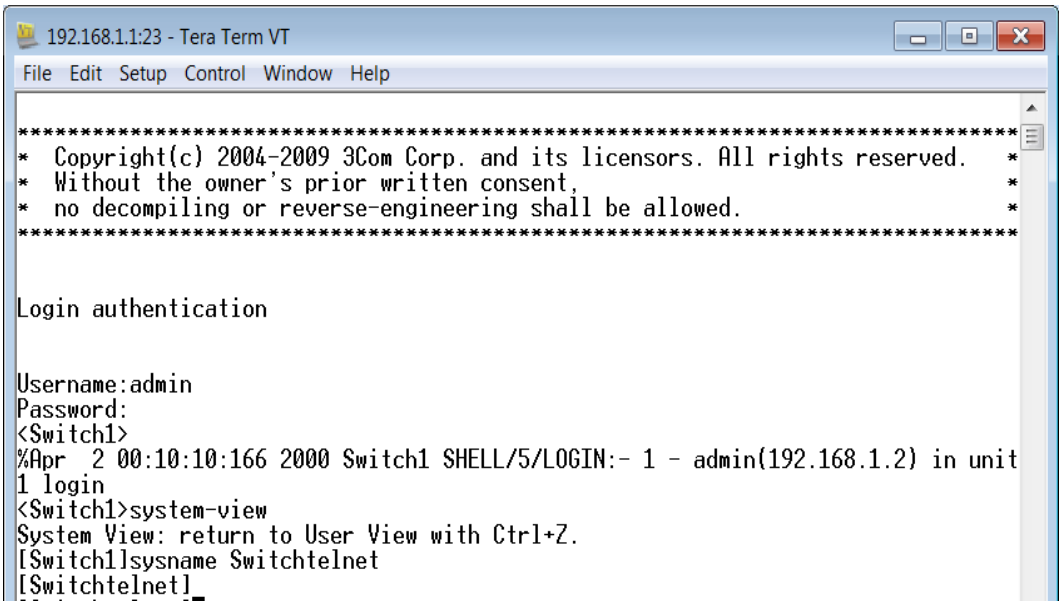


Figura 4.14. Conexión TELNET 3Com 4210 Práctica #2

4.4. DESARROLLO PRÁCTICA #3 CONFIGURACIÓN DE SSH

4.4.1. Configuraciones/Direccionamiento

Direccionamiento:

DISPOSITIVO	Dirección IP	Máscara de Red	Interfaz
Switch	**192.168.1.1**	**255.255.255.0**	**Vlan 1**
PC1	**192.168.1.2**	**255.255.255.0**	**Ethernet**

Usuario y Password:

Usuario: admin

Password: espe

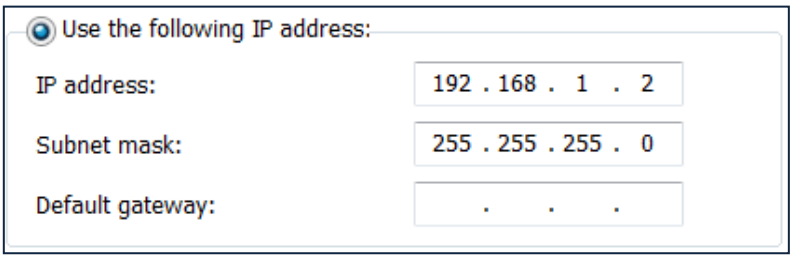
4.4.2. Procedimiento

4.4.2.1. Configuración SSH 3Com 5500

1.- Accedemos al Switch y configuramos nombre y una dirección IP.

```
<5500-EI>
%Apr  1 23:59:18:909 2000 5500-EI SHELL/5/LOGIN:- 1 - admin(aux0) in unit1 login
<5500-EI>system-view
System View: return to User View with Ctrl+Z.
[5500-EI]sysname Switch1
[Switch1]interface vlan 1
[Switch1-Vlan-interface1]ip address 192.168.1.1 255.255.255.0
```

2.- Configuramos la dirección de PC1 y hacemos prueba de conectividad con el switch utilizando el comando *Ping*.




```
C:\Users\FOCH>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=4ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 4ms, Average = 1ms
```

3.- Para configurar SSH en el Switch 3 3Com 5500 utilizamos los siguientes comandos, Creamos las claves RSA.

```
<Switch1>system-view
System View: return to User View with Ctrl+Z.
[Switch1]rsa local-key-pair create
The local-key-pair will be created.
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
       It will take a few minutes.
Input the bits in the modulus[default = 1024]:
Generating keys...
.....++++++
.....++++++
.....++++++++
...++++++++
....Done!
[Switch1]
```

4.- Ponemos la Autenticación AAA y ponemos el tipo de protocolo de entrada.

```
[Switch1]user-interface vty 0 4
[Switch1-ui-vty0-4]authentication-mode scheme
[Switch1-ui-vty0-4]protocol inbound ssh
```

5.- Creamos el usuario:"PC1" y ponemos la contraseña:"espe".

```
[Switch1]local-user PC1
New local user added.
[Switch1-luser-PC1]password simple espe
[Switch1-luser-PC1]service-type ssh
```

```
[Switch1]ssh user PC1 authentication-type password
```

6.- Comprobamos el acceso vía SSH utilizando el programa TERA TERM, Abrimos el programa y escogemos la opción *TCP/IP---SSH y ponemos la dirección IP del Switch.* Presionamos "OK". En la Figura 4.15. Nos muestra la pantalla de Conexión para acceso SSH.

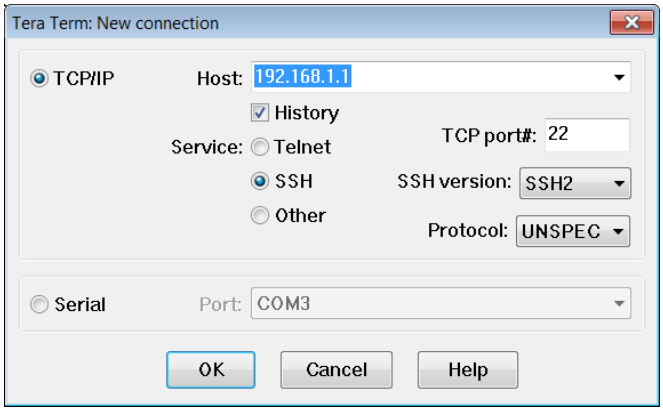


Figura 4.15. TeraTerm Conexión SSH 3Com 5500 Práctica #3

7.- Nos pedirá el nombre de usuario: “PC1” y la contraseña: “espe” para poder acceder al Switch. La Figura 4.16. Nos muestra la pantalla de Autenticacion para el Acceso SSH, mientras que la Figura 4.17. Es la imagen de Acceso Remoto al Switch.

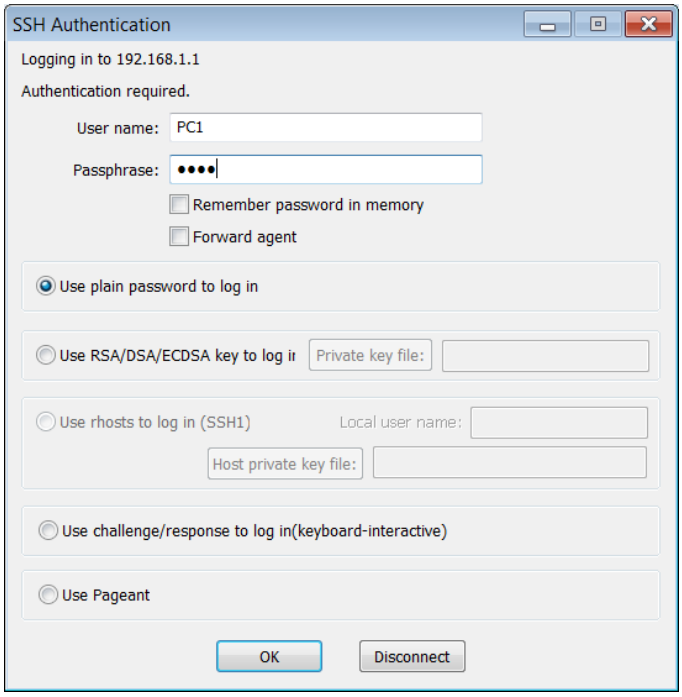


Figura 4.16. Autenticación SSH 3Com 5500 Práctica #3

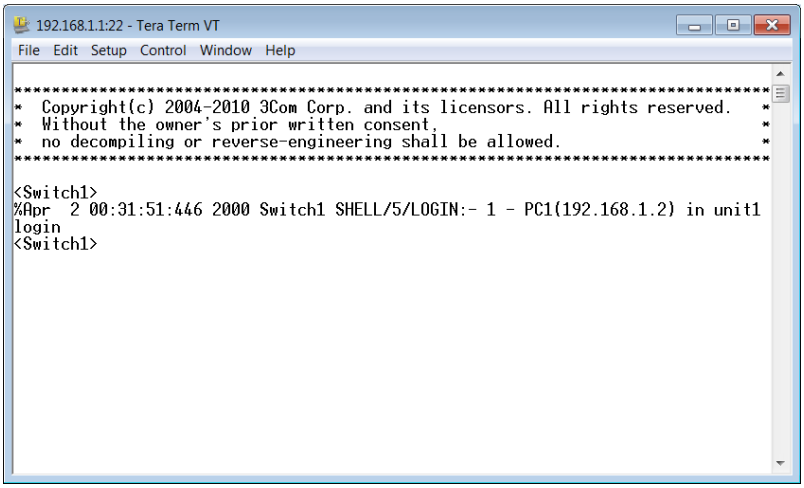


Figura 4.17. Conexión SSH 3Com 5500 Práctica #3

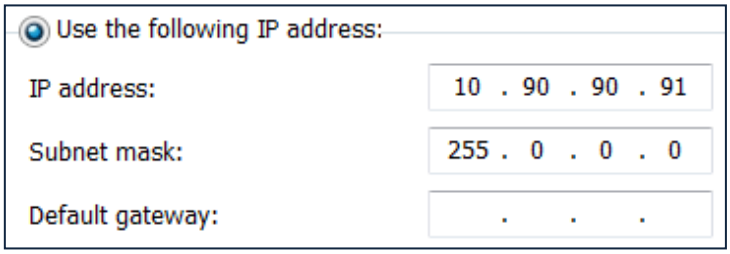
4.4.2.2. Configuración SSH Switch D-Link 3627

1.- Accedemos al Switch y configuramos nombre y vemos la dirección IP por defecto.

```
DGS-3627:4#create account admin  espe
Command: create account admin espe

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

```
DGS-3627:4#show ipif
Command: show ipif

 IP Interface Settings

 Interface Name : System
 Secondary      : FALSE
 IP Address     : 10.90.90.90     (MANUAL)
 Subnet Mask    : 255.0.0.0
 VLAN Name      : default
 Admin. State   : Enabled
 Link Status    : Link DOWN
 Member Ports   : 1-27

Total Entries : 1
```

2.- Configuramos la dirección de PC1 y hacemos prueba de conectividad con el switch utilizando el comando *Ping*.




```
C:\Users\FOCH>ping 10.90.90.90

Pinging 10.90.90.90 with 32 bytes of data:
Reply from 10.90.90.90: bytes=32 time=2ms TTL=255
Reply from 10.90.90.90: bytes=32 time<1ms TTL=255
Reply from 10.90.90.90: bytes=32 time<1ms TTL=255
Reply from 10.90.90.90: bytes=32 time<1ms TTL=255

Ping statistics for 10.90.90.90:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms
```

3.- Para configurar SSH en el Switch D-link 3627 utilizamos los siguientes comandos.

```
DGS-3627:4#config ssh user espe authmode password
Command: config ssh user espe authmode password

Success.
```

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

```
DGS-3627:4#config ssh algorithm RSA enable
Command: config ssh algorithm RSA enable

Success.

DGS-3627:4
```

5.- Habilitamos SSH en el Switch.

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

TELNET will be disabled when enable SSH.
Success.

DGS-3627:4
```

6.- Comprobamos el acceso vía SSH utilizando el programa TERA TERM, Abrimos el programa y escogemos la opción *TCP/IP---SSH y ponemos la dirección IP del Switch.* Presionamos "OK". En la Figura 4.18. Nos muestra la pantalla de Conexión para acceso SSH.

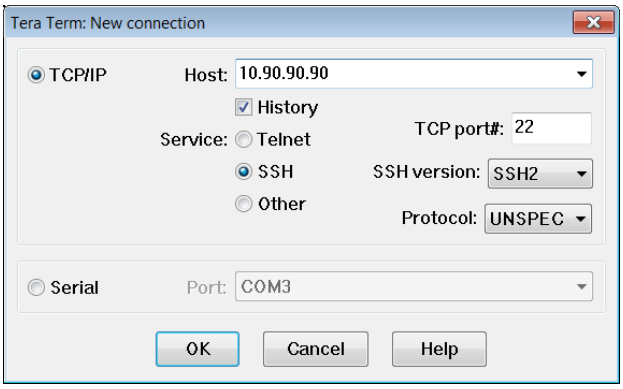


Figura 4.18. TeraTerm Conexión SSH D-Link 3627 Práctica #3

7.- Nos pedirá el nombre de usuario: “espe” y la contraseña: “espe” para poder acceder al Switch. La Figura 4.19. Nos muestra la pantalla de Autenticacion para el Acceso SSH, mientras que la Figura 4.20. Es la imagen de Acceso Remoto al Switch.

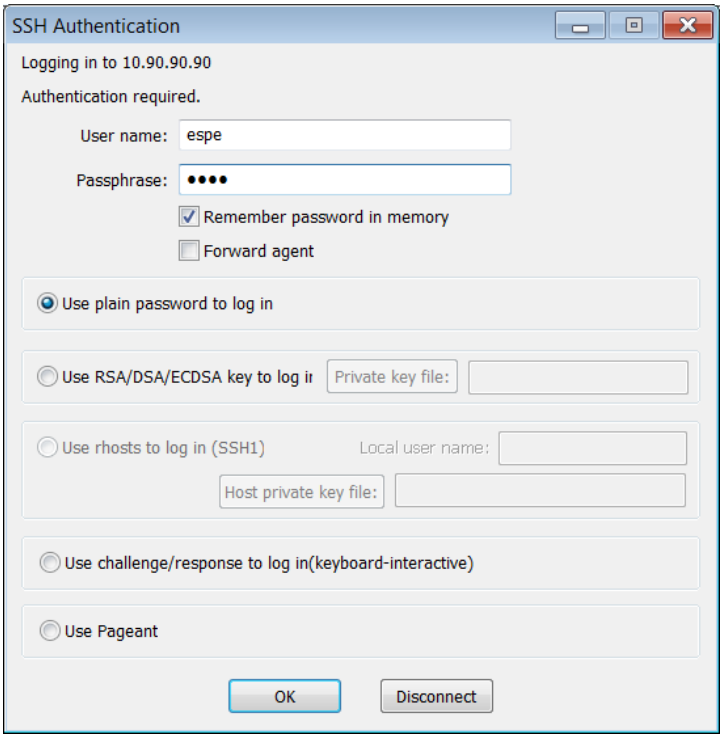


Figura 4.19. Autenticación SSH D-Link 3627 Práctica #3

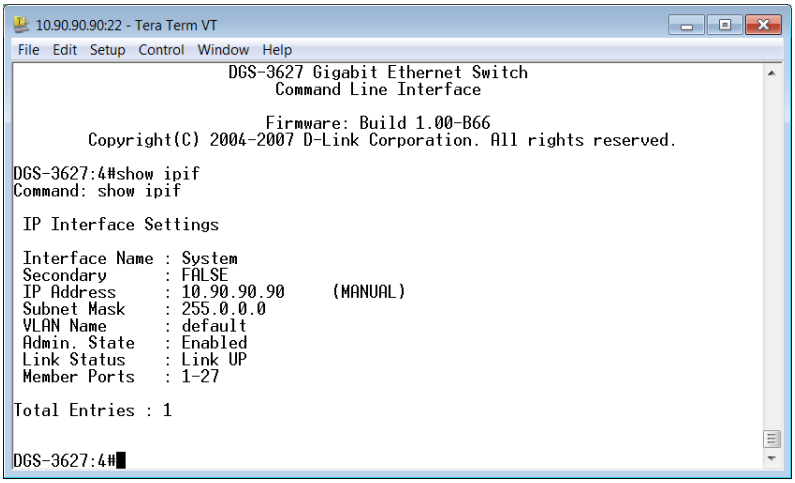


Figura 4.20. Conexión SSH D-Link 3627 Práctica #3

4.5. DESARROLLO PRÁCTICA #4 CONFIGURACIÓN DE UNA VLAN BASADA EN PUERTO

4.5.1. Configuraciones/Direccionamiento

Direccionamiento:

DISPOSITIVO	Dirección IP	Máscara de Red	Interfaz
SWITCH			
VLAN 10 (MAESTROS)	**192.168.1.0**	**255.255.255.0**	**Ethernet 1-3**
VLAN 20 (ESTUDIANTES)	**192.168.2.0**	**255.255.255.0**	**Ethernet 4-6**
VLAN 30 (INVITADOS)	**192.168.3.0**	**255.255.255.0**	**Ethernet 7-9**
PC1 MAESTRO	**192.168.1.2**	**255.255.255.0**	**Ethernet**
PC2 MAESTRO	**192.168.1.3**	**255.255.255.0**	**Ethernet**
PC1 ESTIDIANTE	**192.168.2.2**	**255.255.255.0**	**Ethernet**
PC2 ESTUDIANTE	**192.168.2.3**	**255.255.255.0**	**Ethernet**
PC1 INVITADO	**192.168.3.2**	**255.255.255.0**	**Ethernet**
PC2 INVITADO	**192.168.3.3**	**255.255.255.0**	**Ethernet**

Usuario y Password:

Usuario: admin

Password: espe

4.5.2. Procedimiento

4.5.2.1. Configuración VLAN basada en Puerto 3Com 4500

1.- Accedemos al Switch y creamos una Vlan con el comando ***vlan*** *vlan_id* o eliminamos la vlan con el comando ***undo vlan*** *vlan_id* le damos un nombre a la Vlan con el comando ***name*** **"**nombre**"**.

```
[SWITCH1]vlan 10
[SWITCH1-vlan10]name MAESTROS
[SWITCH1-vlan10]quit
```

```
[SWITCH1]vlan 20
[SWITCH1-vlan20]name ESTUDIANTES
[SWITCH1-vlan20]quit
```

```
[SWITCH1]vlan 30
[SWITCH1-vlan30]name INVITADOS
[SWITCH1-vlan30]quit
```

2.- Añadimos los puertos a las respectivas Vlans.

```
[SWITCH1]vlan 10
[SWITCH1-vlan10]port ethernet 1/0/1 to ethernet 1/0/3
[SWITCH1-vlan10]
```

```
[SWITCH1]vlan 20
[SWITCH1-vlan20]port ethernet 1/0/4 to ethernet 1/0/6
[SWITCH1-vlan20]
```

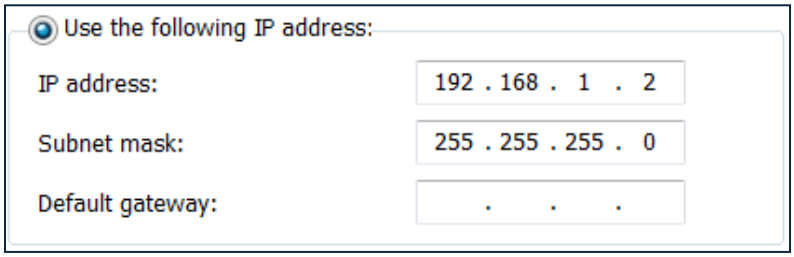
```
[SWITCH1]vlan 30
[SWITCH1-vlan30]port ethernet 1/0/7 to ethernet 1/0/9
[SWITCH1-vlan30]_
```

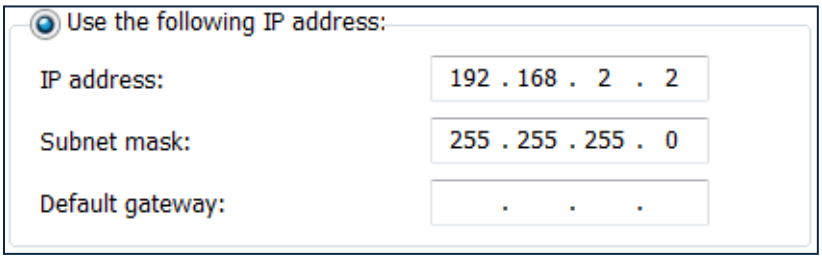
3.- Podemos observar las configuración de las Vlans con los comandos ***display vlan, display vlan all, display vlan*** *vlan_id*.

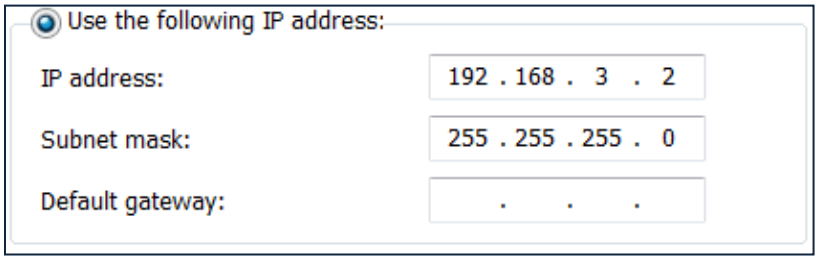
```
[SWITCH1]display vlan
 Total 4 VLAN exist(s).
 The following VLANs exist:
  1(default), 10, 20, 30
```

```
[SWITCH1]display vlan 30
 VLAN ID: 30
 VLAN Type: static
 Route Interface: not configured
 Description: VLAN 0030
 Name: INVITADOS
 Tagged   Ports: none
 Untagged Ports:
  Ethernet1/0/7            Ethernet1/0/8            Ethernet1/0/9
```

4.- Configuración de Computadoras pertenecientes a cada Vlan.

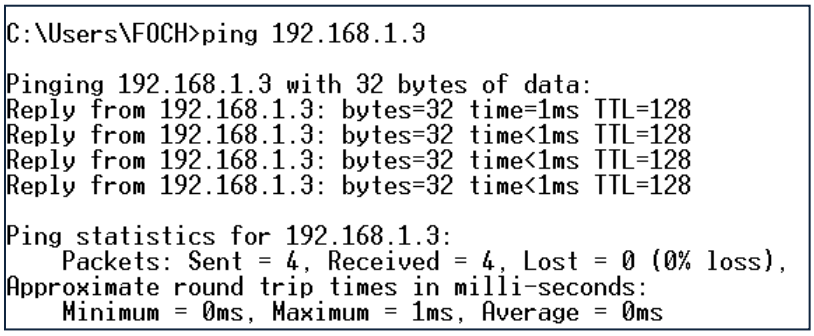


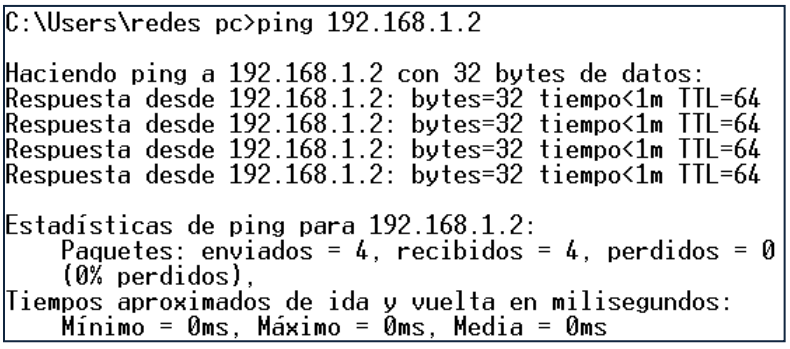




4.5.2.1.1. Pruebas de Conectividad

VLAN MAESTROS





VLAN ESTUDIANTES

```
C:\Users\FOCH>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
C:\Users\redes pc>ping 192.168.2.2

Haciendo ping a 192.168.2.2 con 32 bytes de datos:
Respuesta desde 192.168.2.2: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.2.2: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.2.2: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.2.2: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 192.168.2.2:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

VLAN INVITADOS

```
C:\Users\FOCH>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:
Reply from 192.168.3.3: bytes=32 time<1ms TTL=128
Reply from 192.168.3.3: bytes=32 time<1ms TTL=128
Reply from 192.168.3.3: bytes=32 time<1ms TTL=128
Reply from 192.168.3.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
C:\Users\redes pc>ping 192.168.3.2

Haciendo ping a 192.168.3.2 con 32 bytes de datos:
Respuesta desde 192.168.3.2: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.3.2: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.3.2: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.3.2: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 192.168.3.2:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

ENTRE VLAN MAESTROS Y VLAN INVITADOS

```
C:\Users\FOCH>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:
Reply from 192.168.3.2: Destination host unreachable.
Reply from 192.168.3.2: Destination host unreachable.
Reply from 192.168.3.2: Destination host unreachable.
Reply from 192.168.3.2: Destination host unreachable.

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

ENTRE VLAN MAESTROS Y VLAN ESTUDIANTES

```
C:\Users\FOCH>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:
PING: transmit failed. General failure.
PING: transmit failed. General failure.
PING: transmit failed. General failure.
PING: transmit failed. General failure.

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

4.5.2.2. Configuración VLAN basada en Puerto HP 2512

1.- Accedemos al Switch y creamos una Vlan con el comando ***vlan*** *vlan_id* o eliminamos la vlan con el comando ***no vlan*** *vlan_id* le damos un nombre a la Vlan con el comando ***name*** **"**nombre**"**.

```
SWITCH2> enable
SWITCH2# configure
SWITCH2(config)# vlan 10
SWITCH2(vlan-10)# name MAESTROS
SWITCH2(vlan-10)# exit
```

```
SWITCH2(config)# vlan 20
SWITCH2(vlan-20)# name ESTUDIANTES
SWITCH2(vlan-20)# exit
```

```
SWITCH2(config)# vlan 30
SWITCH2(vlan-30)# name INVITADOS
SWITCH2(vlan-30)# exit
SWITCH2(config)#
```

2.- Añadimos los puertos a las respectivas Vlans.

```
SWITCH2(config)# vlan 10
SWITCH2(vlan-10)# untagged ethernet 1
SWITCH2(vlan-10)# untagged ethernet 2
SWITCH2(vlan-10)# untagged ethernet 3
SWITCH2(vlan-10)#
```

```
SWITCH2(config)# vlan 20
SWITCH2(vlan-20)# untagged ethernet 4
SWITCH2(vlan-20)# untagged ethernet 5
SWITCH2(vlan-20)# untagged ethernet 6
SWITCH2(vlan-20)#
```

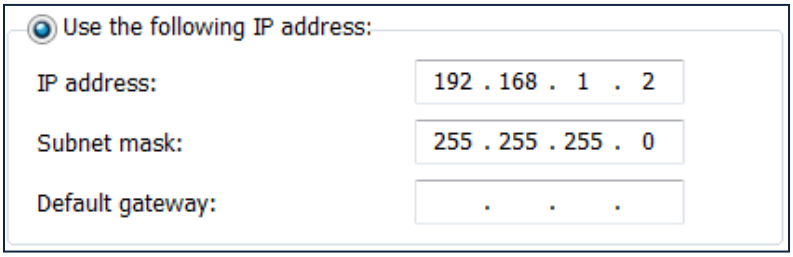
```
SWITCH2(config)# vlan 30
SWITCH2(vlan-30)# untagged ethernet 7
SWITCH2(vlan-30)# untagged ethernet 8
SWITCH2(vlan-30)# untagged ethernet 9
SWITCH2(vlan-30)#
```

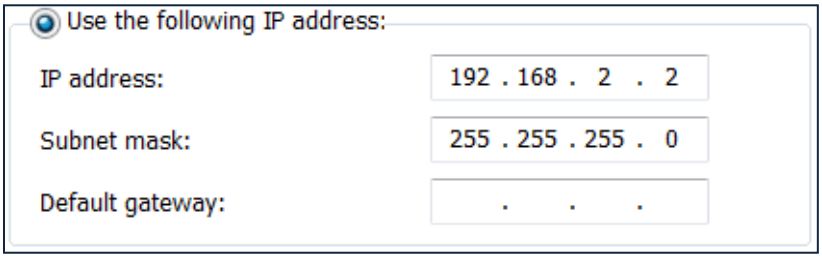
3.- Podemos observar las configuración de las Vlans con los comandos ***show vlans,*** ***show vlan*** *vlan_id.*

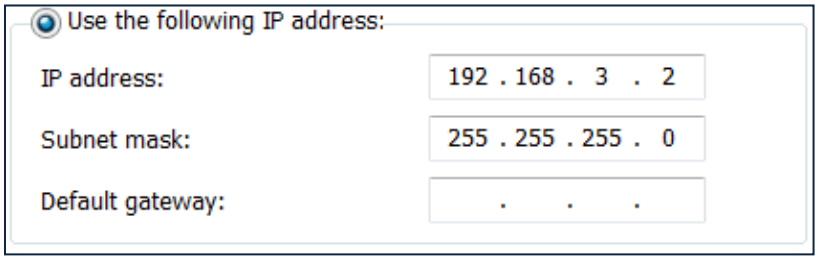
```
SWITCH2# show vlans

 Status and Counters - VLAN Information

  Maximum VLANs to support : 8
  Primary VLAN : DEFAULT_VLAN
  Management VLAN :

  802.1Q VLAN ID Name          Status
  -------------- ------------- -------------
  1              DEFAULT_VLAN  Static
  10             MAESTROS      Static
  20             ESTUDIANTES   Static
  30             INVITADOS     Static
```

```
SWITCH2# show vlan 20

 Status and Counters - VLAN Information - Ports - VLAN 20

  802.1Q VLAN ID : 20
  Name           : ESTUDIANTES
  Status         : Static

  Port Information Mode     Unknown VLAN Status
  ---------------- -------- ------------ ----------
  4                Untagged Learn        Down
  5                Untagged Learn        Down
  6                Untagged Learn        Down
```

4.- Configuración de Computadoras pertenecientes a cada Vlan.







4.5.2.2.1. Pruebas de Conectividad

VLAN MAESTROS

```
C:\Users\FOCH>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:
Reply from 192.168.1.3: bytes=32 time=1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

```
C:\Users\redes pc>ping 192.168.1.2

Haciendo ping a 192.168.1.2 con 32 bytes de datos:
Respuesta desde 192.168.1.2: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.1.2: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.1.2: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.1.2: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 192.168.1.2:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

VLAN ESTUDIANTES

```
C:\Users\FOCH>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
C:\Users\redes pc>ping 192.168.2.2

Haciendo ping a 192.168.2.2 con 32 bytes de datos:
Respuesta desde 192.168.2.2: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.2.2: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.2.2: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.2.2: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 192.168.2.2:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

VLAN INVITADOS

```
C:\Users\FOCH>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:
Reply from 192.168.3.3: bytes=32 time<1ms TTL=128
Reply from 192.168.3.3: bytes=32 time<1ms TTL=128
Reply from 192.168.3.3: bytes=32 time<1ms TTL=128
Reply from 192.168.3.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
C:\Users\redes pc>ping 192.168.3.2

Haciendo ping a 192.168.3.2 con 32 bytes de datos:
Respuesta desde 192.168.3.2: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.3.2: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.3.2: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.3.2: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 192.168.3.2:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

ENTRE VLAN MAESTROS Y VLAN INVITADOS

```
C:\Users\FOCH>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:
PING: transmit failed. General failure.
PING: transmit failed. General failure.
PING: transmit failed. General failure.
PING: transmit failed. General failure.

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

ENTRE VLAN MAESTROS Y VLAN ESTUDIANTES

```
C:\Users\FOCH>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:
PING: transmit failed. General failure.
PING: transmit failed. General failure.
PING: transmit failed. General failure.
PING: transmit failed. General failure.

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

4.6. DESARROLLO PRÁCTICA #5 CONFIGURACIÓN DHCP EN VLANS

4.6.1. Configuraciones/Direccionamiento

Direccionamiento:

DISPOSITIVO	Dirección IP	Máscara de Red	Interfaz
SWITCH			
VLAN 10 (MAESTROS)	**192.168.1.0**	**255.255.255.0**	**Ethernet 1-3**
VLAN 20 (ESTUDIANTES)	**192.168.2.0**	**255.255.255.0**	**Ethernet 4-6**
VLAN 30 (INVITADOS)	**192.168.3.0**	**255.255.255.0**	**Ethernet 7-9**
PC1 MAESTRO	**192.168.1.X**	**255.255.255.0**	**Ethernet**
PC2 MAESTRO	**192.168.1.X**	**255.255.255.0**	**Ethernet**
PC1 ESTIDIANTE	**192.168.2.X**	**255.255.255.0**	**Ethernet**
PC2 ESTUDIANTE	**192.168.2.X**	**255.255.255.0**	**Ethernet**

PC1 INVITADO	**192.168.3.X**	**255.255.255.0**	**Ethernet**
PC2 INVITADO	**192.168.3.X**	**255.255.255.0**	**Ethernet**

Usuario y Password:

Usuario: admin

Password: espe

4.6.2. Procedimiento

4.6.2.1. Configuración DHCP VLAN CISCO 3560

1.- Accedemos al Switch y creamos una Vlan con el comando ***vlan*** *vlan_id* o eliminamos la vlan con el comando ***no vlan*** *vlan_id* le damos un nombre a la Vlan con el comando ***name*** **"**nombre**"**.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name MAESTROS
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name ESTUDIANTES
Switch(config-vlan)#exit
Switch(config)#vlan 30
Switch(config-vlan)#name INVITADOS
```

2.- Añadimos los puertos a las respectivas Vlans.

```
Switch(config)#interface range fa0/1-3
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
```

```
Switch(config)#interface range fa0/4-6
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 20
Switch(config-if-range)#exit
```

```
Switch(config)#interface range fa0/7-9
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 30
```

3.- La Figura 4.21. Nos indica la configuración de Computadoras la cual debe estar en forma automática.

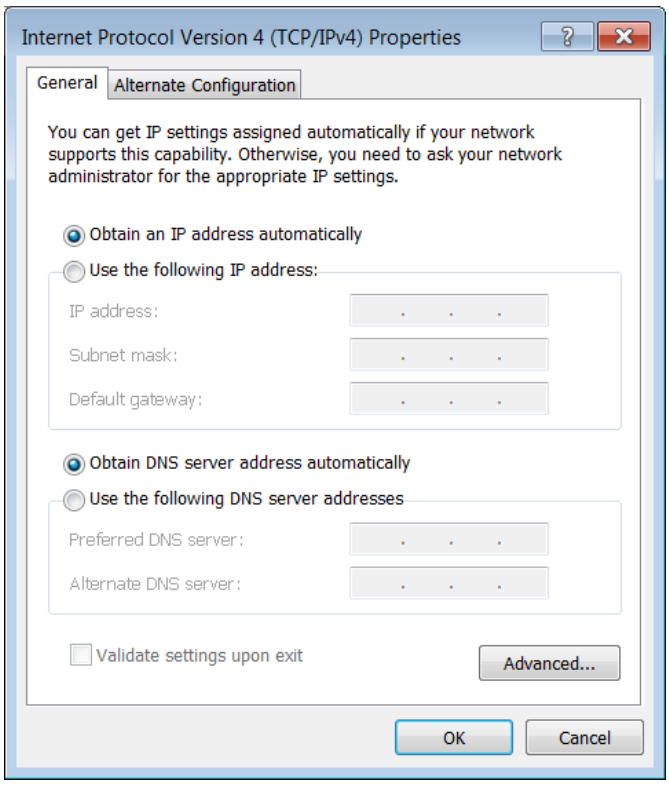


Figura 4.21. Configuración IP Automática Computador Práctica #4

4.- Configuración de Dirección IP a cada VLAN.

```
Switch(config)#interface vlan 10
Switch(config-if)#
*Mar  1 00:14:43.748: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10,
anged state to down
Switch(config-if)#ip address 192.168.1.1 255.255.255.0
Switch(config-if)#description DHCP
```

```
Switch(config)#interface vlan 20
Switch(config-if)#
*Mar  1 00:17:22.292: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan20,
anged state to down
Switch(config-if)#ip address 192.168.2.1 255.255.255.0
Switch(config-if)#description DHCP
```

```
Switch(config)#interface vlan 30
Switch(config-if)#
*Mar  1 00:18:49.744: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan30,
anged state to down
Switch(config-if)#ip address 192.168.3.1 255.255.255.0
Switch(config-if)#description DHCP
```

5.- Configuración de DHCP en el Switch y habilitación del enrutamiento con el comando ***ip routing***.

```
Switch(config)#ip routing
Switch(config)#ip dhcp pool vlan10
Switch(dhcp-config)#network 192.168.1.0 255.255.255.0
Switch(dhcp-config)#default-router 192.168.1.1
```

```
Switch(config)#ip dhcp pool vlan20
Switch(dhcp-config)#network 192.168.2.0 255.255.255.0
Switch(dhcp-config)#default-router 192.168.2.1
```

```
Switch(config)#ip dhcp pool vlan30
Switch(dhcp-config)#network 192.168.3.0 255.255.255.0
Switch(dhcp-config)#default-router 192.168.3.1
```

6.- Exclusión de IP de la Vlans.

```
Switch(config)#ip dhcp excluded-address  192.168.1.1
Switch(config)#ip dhcp excluded-address  192.168.2.1
Switch(config)#ip dhcp excluded-address  192.168.3.1
```

7.- Asignación dinámica de Direcciones.

DHCP Enabled	Yes
IPv4 Address	192.168.1.2
IPv4 Subnet Mask	255.255.255.0
Lease Obtained	lunes, 13 de agosto de 2012 13:38:06
Lease Expires	martes, 14 de agosto de 2012 13:38:05
IPv4 Default Gateway	192.168.1.1
IPv4 DHCP Server	192.168.1.1

DHCP Enabled	Yes
IPv4 Address	192.168.2.2
IPv4 Subnet Mask	255.255.255.0
Lease Obtained	lunes, 13 de agosto de 2012 13:40:43
Lease Expires	martes, 14 de agosto de 2012 13:40:43
IPv4 Default Gateway	192.168.2.1
IPv4 DHCP Server	192.168.2.1

DHCP Enabled	Yes
IPv4 Address	192.168.3.2
IPv4 Subnet Mask	255.255.255.0
Lease Obtained	lunes, 13 de agosto de 2012 13:42:26
Lease Expires	martes, 14 de agosto de 2012 13:42:26
IPv4 Default Gateway	192.168.3.1
IPv4 DHCP Server	192.168.3.1

4.6.2.1.1. Pruebas de Conectividad

VLAN MAESTROS

```
C:\Users\FOCH>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:
Reply from 192.168.1.3: bytes=32 time=1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

```
C:\Users\redes pc>ping 192.168.1.2

Haciendo ping a 192.168.1.2 con 32 bytes de datos:
Respuesta desde 192.168.1.2: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.1.2: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.1.2: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.1.2: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 192.168.1.2:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

VLAN ESTUDIANTES

```
C:\Users\FOCH>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
C:\Users\redes pc>ping 192.168.2.2

Haciendo ping a 192.168.2.2 con 32 bytes de datos:
Respuesta desde 192.168.2.2: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.2.2: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.2.2: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.2.2: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 192.168.2.2:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

VLAN INVITADOS

```
C:\Users\FOCH>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:
Reply from 192.168.3.3: bytes=32 time<1ms TTL=128
Reply from 192.168.3.3: bytes=32 time<1ms TTL=128
Reply from 192.168.3.3: bytes=32 time<1ms TTL=128
Reply from 192.168.3.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
C:\Users\redes pc>ping 192.168.3.2

Haciendo ping a 192.168.3.2 con 32 bytes de datos:
Respuesta desde 192.168.3.2: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.3.2: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.3.2: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.3.2: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 192.168.3.2:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

ENTRE VLAN MAESTROS Y VLAN INVITADOS

```
C:\Users\FOCH>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:
Reply from 192.168.3.2: Destination host unreachable.
Reply from 192.168.3.2: Destination host unreachable.
Reply from 192.168.3.2: Destination host unreachable.
Reply from 192.168.3.2: Destination host unreachable.

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

ENTRE VLAN MAESTROS Y VLAN ESTUDIANTES

```
C:\Users\FOCH>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:
PING: transmit failed. General failure.
PING: transmit failed. General failure.
PING: transmit failed. General failure.
PING: transmit failed. General failure.

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

4.7. DESARROLLO PRÁCTICA #6 CONFIGURACIÓN DE ESPANNING TREE PROTOCOL (STP) Y ENLACES TRONCALES

4.7.1. Configuraciones/Direccionamiento

Direccionamiento:

DISPOSITIVO	Dirección IP	Máscara de Red	Interfaz
SWITCH 1			
VLAN 20 (ESTUDIANTES)	**192.168.2.0**	**255.255.255.0**	**Ethernet 4-6**
ENLACE TRONCAL	**--**	**--**	**Ethernet 11-12**
SWITCH 2			
VLAN 20 (ESTUDIANTES)	**192.168.2.0**	**255.255.255.0**	**Ethernet 4-6**
ENLACE TRONCAL	**--**	**--**	**Ethernet 11-12**
SWITCH 3			
VLAN 20 (ESTUDIANTES)	**192.168.2.0**	**255.255.255.0**	**Ethernet 4-6**
ENLACE TRONCAL	**--**	**--**	**Ethernet 11-12**
PC1 ESTIDIANTE	**192.168.2.2**	**255.255.255.0**	**Ethernet**
PC2 ESTUDIANTE	**192.168.2.3**	**255.255.255.0**	**Ethernet**

Usuario y Password:

Usuario: admin

Password: espe

4.7.2. Procedimiento

4.7.2.1. Configuración STP y ENLACES TRONCALES 3COM 4210

1.- Accedemos al Switch y creamos la Vlan "ESTUDIANTES".

```
[SWITCH1]vlan 20
[SWITCH1-vlan20]name ESTUDIANTES
```

2.- Añadimos los puertos a la VLAN.

```
[SWITCH1-vlan20]port ethernet 1/0/4 to ethernet 1/0/6
```

3.- Configuración de Enlace Troncales.

```
[SWITCH1]interface ethernet 1/0/11
[SWITCH1-Ethernet1/0/11]port link-type trunk
[SWITCH1-Ethernet1/0/11]port trunk permit vlan 20
 Please wait... Done.
[SWITCH1-Ethernet1/0/11]quit
[SWITCH1]interface ethernet 1/0/12
[SWITCH1-Ethernet1/0/12]port link-type trunk
[SWITCH1-Ethernet1/0/12]port trunk permit vlan 20
 Please wait... Done.
```

4.- Habilitación protocolo STP.

```
<SWITCH1>system-view
System View: return to User View with Ctrl+Z.
[SWITCH1]stp enable
[SWITCH1]stp root secondary
```

4.7.2.2. Configuración STP y ENLACES TRONCALES D-Link DES-3526

1.- Accedemos al Switch y creamos la Vlan "ESTUDIANTES".

```
DES-3526:admin#create vlan ESTUDIANTES tag 20
Command: create vlan ESTUDIANTES tag 20

Success.
```

2.- Añadimos los puertos a la VLAN.

```
DES-3526:admin#config vlan default delete 4-6
Command: config vlan default delete 4-6

Success.
```

```
DES-3526:admin#config vlan ESTUDIANTES add untagged 4-6
Command: config vlan ESTUDIANTES add untagged 4-6

Success.
```

3. - Configuración de Enlace Troncales.

```
DES-3526:admin#config vlan ESTUDIANTES add tagged 11-12
Command: config vlan ESTUDIANTES add tagged 11-12

Success.
```

4. - Habilitación protocolo STP.

```
DES-3526:admin#enable stp
Command: enable stp

Success.
```

4.7.2.3. Configuración STP y ENLACES TRONCALES HP 2512

1.- Accedemos al Switch y creamos la Vlan “ESTUDIANTES”.

```
SWITCH3# configure
SWITCH3(config)# vlan 20
SWITCH3(vlan-20)# name ESTUDIANTES
```

2.- Añadimos los puertos a la VLAN.

```
SWITCH3(config)# vlan 20
SWITCH3(vlan-20)# untagged ethernet 4
SWITCH3(vlan-20)# untagged ethernet 5
SWITCH3(vlan-20)# untagged ethernet 6
```

3.- Configuración de Enlace Troncales.

```
SWITCH3# configure
SWITCH3(config)# trunk ethernet 11 trk1 trunk
SWITCH3(config)# trunk ethernet 12 trk1 trunk
```

4.- Habilitación protocolo STP.

```
SWITCH3# configure
SWITCH3(config)# spanning-tree
```

4.7.2.4. Prueba de Conectividad

1.- Conectividad entre PC1 y PC2

```
C:\Users\FOCH>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:
Reply from 192.168.2.3: bytes=32 time=1ms TTL=128
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

4.8. DESARROLLO PRÁCTICA #7 INTERCONEXIÓN DE VLANS POR MEDIO DEL ROUTER

4.8.1. Configuraciones/Direccionamiento

Direccionamiento:

DISPOSITIVO	Dirección IP	Máscara de Red	Interfaz
SWITCH 1			
VLAN 20	**192.168.2.0**	**255.255.255.0**	**Ethernet 4-6**

(ESTUDIANTES)			
VLAN 10 (MAESTROS)	**192.168.1.0**	**255.255.255.0**	**Ethernet 1-3**
ENLACE TRONCAL	**--**	**--**	**Ethernet 10-11-12**
SWITCH 2			
VLAN 20 (ESTUDIANTES)	**192.168.2.0**	**255.255.255.0**	**Ethernet 4-6**
VLAN 10 (MAESTROS)	**192.168.1.0**	**255.255.255.0**	**Ethernet 1-3**
ENLACE TRONCAL	**--**	**--**	**Ethernet 11**
SWITCH 3			
VLAN 20 (ESTUDIANTES)	**192.168.2.0**	**255.255.255.0**	**Ethernet 4-6**
VLAN 10 (MAESTROS)	**192.168.1.0**	**255.255.255.0**	**Ethernet 1-3**
ENLACE TRONCAL	**--**	**--**	**Ethernet 11**
ROUTER			
SUBINTERFAZ 10	**192.168.1.10**	**255.255.255.0**	**Ethernet**
SUBINTERFAZ 20	**192.168.2.10**	**255.255.255.0**	**Ethernet**
PC1 ESTIDIANTE	**192.168.2.2**	**255.255.255.0**	**Ethernet**
PC2 ESTUDIANTE	**192.168.2.3**	**255.255.255.0**	**Ethernet**
PC3 ESTUDIANTE	**192.168.2.4**	**255.255.255.0**	**Ethernet**
PC1 MAESTRO	**192.168.1.2**	**255.255.255.0**	**Ethernet**

PC2 MAESTRO	**192.168.1.3**	**255.255.255.0**	**Ethernet**
PC3 MAESTRO	**192.168.1.4**	**255.255.255.0**	**Ethernet**

Usuario y Password:

Usuario: admin

Password: espe

4.8.2. Procedimiento

4.8.2.1. Configuración 3COM 4210

1.- Accedemos al Switch y creamos la Vlan "MAESTROS" y "ESTUDIANTES".

```
[4210]vlan 10
[4210-vlan10]name MAESTROS
[4210-vlan10]quit
[4210]vlan 20
[4210-vlan20]name ESTUDIANTES
[4210-vlan20]
```

2.- Añadimos los puertos a las VLANs.

```
[4210]vlan 10
[4210-vlan10]port ethernet 1/0/1 to ethernet 1/0/3
[4210-vlan10]quit
[4210]vlan 20
[4210-vlan20]port ethernet 1/0/4 to ethernet 1/0/6
```

3.- Configuración de Enlace Troncales.

```
[4210]interface ethernet 1/0/11
[4210-Ethernet1/0/11]port link-type trunk
[4210-Ethernet1/0/11]port trunk permit vlan 10
 Please wait... Done.
[4210-Ethernet1/0/11]port trunk permit vlan 20
 Please wait... Done.
```

4.8.2.2. Configuración D-Link DES-3526

1.- Accedemos al Switch y creamos la Vlan "MAESTROS" y "ESTUDIANTES".

```
DES-3526:admin#create vlan MAESTROS tag 10
Command: create vlan MAESTROS tag 10

Success.

DES-3526:admin#create vlan ESTUDIANTES tag 20
Command: create vlan ESTUDIANTES tag 20

Success.
```

2.- Añadimos los puertos a la VLANs.

```
DES-3526:admin#config vlan default delete 1-6
Command: config vlan default delete 1-6

Success.
```

```
DES-3526:admin#config vlan MAESTROS add untagged 1-3
Command: config vlan MAESTROS add untagged 1-3

Success.

DES-3526:admin#config vlan ESTUDIANTES add untagged 4-6
Command: config vlan ESTUDIANTES add untagged 4-6

Success.
```

3.- Configuración de Enlace Troncales.

```
DES-3526:admin#config vlan MAESTROS add tagged 10-12
Command: config vlan MAESTROS add tagged 10-12

Success.

DES-3526:admin#config vlan ESTUDIANTES add tagged 10-12
Command: config vlan ESTUDIANTES add tagged 10-12

Success.
```

4.8.2.3. Configuración HP 2512

1.- Accedemos al Switch y creamos la Vlan “MAESTROS” y “ESTUDIANTES”.

```
SWITCH3# configure
SWITCH3(config)# vlan 10
SWITCH3(vlan-10)# name MAESTROS
SWITCH3(vlan-10)# exit
SWITCH3(config)# vlan 20
SWITCH3(vlan-20)# name ESTUDIANTES
```

2.- Añadimos los puertos a la VLANs.

```
SWITCH3(config)# vlan 10
SWITCH3(vlan-10)# untagged ethernet 1
SWITCH3(vlan-10)# untagged ethernet 2
SWITCH3(vlan-10)# untagged ethernet 3
```

```
SWITCH3(config)# vlan 20
SWITCH3(vlan-20)# untagged ethernet 4
SWITCH3(vlan-20)# untagged ethernet 5
SWITCH3(vlan-20)# untagged ethernet 6
```

3.- Configuración de Enlace Troncales.

```
SWITCH3# configure
SWITCH3(config)# trunk ethernet 11 trk1 trunk
```

```
SWITCH3(config)# vlan 10
SWITCH3(vlan-10)# tagged trk1
SWITCH3(vlan-10)# exit
SWITCH3(config)# vlan 20
SWITCH3(vlan-20)# tagged trk1
```

4.8.2.4. Configuración CISCO 2800

1.- Accedemos al Router configuramos la interfaces virtuales o sub interfaces añadimos el tipo de encapsulación.

```
ROUTER(config)#interface f0/0.20
ROUTER(config-subif)#encapsulation dot1q 20
ROUTER(config-subif)#ip address 192.168.2.10 255.255.255.0
ROUTER(config-subif)#exit
ROUTER(config)#interface f0/0.10
ROUTER(config-subif)#encapsulation dot1q 10
ROUTER(config-subif)#ip address 192.168.1.10 255.255.255.0
```

2.- Configuramos el protocolo de Enrutamiento en este caso RIPv2.

```
ROUTER(config)#router rip
ROUTER(config-router)#version 2
ROUTER(config-router)#network 192.168.1.0
ROUTER(config-router)#network 192.168.2.0
```

4.8.2.5. Pruebas de Conectividad

1.- Conectividad entre PC1ESTUDIANTE y PC2 ESTUDIANTE

```
C:\Users\FOCH>PING 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:
Reply from 192.168.2.3: bytes=32 time=2ms TTL=128
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms
```

2.- Conectividad entre PC1MAESTRO y PC2MAESTRO

```
C:\Users\FOCH>PING 192.168.1.4

Pinging 192.168.1.4 with 32 bytes of data:
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

3.- Conectividad entre PC3MAESTRO y PC3ESTUDIANTE

```
C:\Users\FOCH>PING 192.168.2.4

Pinging 192.168.2.4 with 32 bytes of data:
Reply from 192.168.2.4: bytes=32 time<1ms TTL=128
Reply from 192.168.2.4: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.2.4:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

4.9. DESARROLLO PRÁCTICA#8 CONFIGURACIÓN DE ACL (ESTANDAR-EXTENDIDA) EN EL SWITCH

4.9.1. Configuraciones/Direccionamiento

Direccionamiento:

DISPOSITIVO	Dirección IP	Máscara de Red	Interfaz
SWITCH 1			
VLAN 20	**192.168.2.0**	**255.255.255.0**	**Ethernet 4-6**

(ESTUDIANTES)			
VLAN 10 (MAESTROS)	**192.168.1.0**	**255.255.255.0**	**Ethernet 1-3**
ENLACE TRONCAL	**--**	**--**	**Ethernet 11-12**
SWITCH 2	192.168.1.10	255.255.255.0	VLAN 10
VLAN 20 (ESTUDIANTES)	**192.168.2.0**	**255.255.255.0**	**Ethernet 4-6**
VLAN 10 (MAESTROS)	**192.168.1.0**	**255.255.255.0**	**Ethernet 1-3**
ENLACE TRONCAL	**--**	**--**	**Ethernet 11-12**
SWITCH 3			
VLAN 20 (ESTUDIANTES)	**192.168.2.0**	**255.255.255.0**	**Ethernet 4-6**
VLAN 10 (MAESTROS)	**192.168.1.0**	**255.255.255.0**	**Ethernet 1-3**
ENLACE TRONCAL	**--**	**--**	**Ethernet 11**
PC1 ESTIDIANTE	**192.168.2.2**	**255.255.255.0**	**Ethernet**
PC2 MAESTRO	**192.168.1.2**	**255.255.255.0**	**Ethernet**
PC3 ESTUDIANTE	**192.168.2.3**	**255.255.255.0**	**Ethernet**
PC4 MAESTRO	**192.168.1.3**	**255.255.255.0**	**Ethernet**
PC5 ESTUDIANTE	**192.168.2.4**	**255.255.255.0**	**Ethernet**
PC6 MAESTRO	**192.168.1.4**	**255.255.255.0**	**Ethernet**

Usuario y Password:

Usuario: admin

Password: espe

4.9.2. Procedimiento

4.9.2.1. Configuración 3COM 4500

1.- Accedemos al Switch y creamos la Vlan “MAESTROS” y “ESTUDIANTES”.

```
[4500]vlan 10
[4500-vlan10]name MAESTROS
[4500-vlan10]quit
[4500]vlan 20
[4500-vlan20]name ESTUDIANTES
```

2.- Añadimos los puertos a las VLANs.

```
[4500]vlan 10
[4500-vlan10]port ethernet 1/0/1 to ethernet 1/0/3
[4500-vlan10]quit
[4500]vlan 20
[4500-vlan20]port ethernet 1/0/4 to ethernet 1/0/6
```

3.- Configuración de Enlace Troncales.

```
[4500] interface ethernet 1/0/11
[4500-Ethernet1/0/11]port link-type trunk
[4500-Ethernet1/0/11]port trunk permit vlan 10
 Please wait... Done.
[4500-Ethernet1/0/11]port trunk permit vlan 20
 Please wait... Done.
[4500-Ethernet1/0/11]quit
[4500]interface ethernet 1/0/12
[4500-Ethernet1/0/12]port link-type trunk
[4500-Ethernet1/0/12]port trunk permit vlan 10
 Please wait... Done.
[4500-Ethernet1/0/12]port trunk permit vlan 20
 Please wait... Done.
```

4.- habilitación de STP.

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]stp enable
[4500]stp root secondary
```

5.- Creación lista de acceso estandar.

```
[4500]acl number 2000
[4500-acl-basic-2000]rule 0 deny source 192.168.1.3 0
[4500-acl-basic-2000]rule 1 deny source 192.168.2.2 0
```

6.- Aplicación de la lista de acceso a la interfaz correspondiente.

```
[4500]interface ethernet 1/0/11
[4500-Ethernet1/0/11]packet-filter inbound ip-group 2000
[4500-Ethernet1/0/11]quit
[4500]interface ethernet 1/0/12
[4500-Ethernet1/0/12]packet-filter inbound ip-group 2000
```

4.9.2.2. Configuración D-Link DES-3627

1.- Accedemos al Switch y creamos la Vlan “MAESTROS” y “ESTUDIANTES”.

```
DGS-3627:4#create vlan MAESTROS tag 10
Command: create vlan MAESTROS tag 10

Success.

DGS-3627:4#create vlan ESTUDIANTES tag 20
Command: create vlan ESTUDIANTES tag 20

Success.
```

2.- Añadimos los puertos a la VLANs.

```
DGS-3627:4#config vlan default delete 1-6
Command: config vlan default delete 1-6

Success.

DGS-3627:4#config vlan MAESTROS add untagged 1-3
Command: config vlan MAESTROS add untagged 1-3

Success.

DGS-3627:4#config vlan ESTUDIANTES add untagged 4-6
Command: config vlan ESTUDIANTES add untagged 4-6

Success.
```

3. - Configuración de Enlace Troncales.

```
DGS-3627:4#config vlan MAESTROS add tagged 10-12
Command: config vlan MAESTROS add tagged 10-12

Success.

DGS-3627:4#config vlan ESTUDIANTES add tagged 11-12
Command: config vlan ESTUDIANTES add tagged 11-12

Success.
```

4. - habilitación de STP.

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

Success.
```

5.- habilitación de Telnet y configuración de una dirección IP.

```
DGS-3627:4#enable telnet 23
Command: enable telnet 23

Success.
```

```
DGS-3627:4#config ipif System ipaddress 192.168.10.10/24
Command: config ipif System ipaddress 192.168.10.10/24

Success.
```

4.9.2.3. Configuración CISCO 3560

1.- Accedemos al Switch y creamos la Vlan “MAESTROS” y “ESTUDIANTES”.

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name MAESTROS
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name ESTUDIANTES
```

2.- Añadimos los puertos a la VLANs.

```
Switch(config)#interface range f0/1-3
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#exit
Switch(config)#interface range f0/4-6
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 20
```

3.- Configuración de Enlace Troncales.

```
Switch(config)#interface range f0/11-12
Switch(config-if-range)#switchport mode trunk
```

4.- Creación lista de acceso extendida.

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#access-list 120 deny tcp any eq 23 host 192.168.1.2
Switch(config)#access-list 120 permit ip any any
```

5.- Aplicación de la lista de acceso a la interfaz correspondiente.

```
Switch(config)#interface f0/11
Switch(config-if)#ip access-group 120 in
Switch(config-if)#exit
Switch(config)#interface f0/12
Switch(config-if)#ip access-group 120 in
```

4.9.2.4. Pruebas de Conectividad

1.- Conectividad entre PC4 y PC6 *la lista de acceso deberá bloquear el tráfico destinado a la PC6*

```
C:\Users\FOCH>ping 192.168.1.4

Pinging 192.168.1.4 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.4:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

2.- Conectividad entre PC2 y PC6 *en este caso la lista de acceso debe permitir el tráfico destinado a PC6.*

```
C:\Users\FOCH>ping 192.168.1.4

Pinging 192.168.1.4 with 32 bytes of data:
Reply from 192.168.1.4: bytes=32 time=1ms TTL=128
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

3.- Conectividad entre PC1 y PC5 *la lista de acceso deberá bloquear el tráfico destinado a la PC5*

```
C:\Users\FOCH>ping 192.168.2.4

Pinging 192.168.2.4 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.2.4:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

4.- Conectividad entre PC3 y PC5 *en este caso la lista de acceso debe permitir el tráfico destinado a PC5.*

```
C:\Users\FOCH>ping 192.168.2.4

Pinging 192.168.2.4 with 32 bytes of data:
Reply from 192.168.2.4: bytes=32 time=1ms TTL=128
Reply from 192.168.2.4: bytes=32 time<1ms TTL=128
Reply from 192.168.2.4: bytes=32 time<1ms TTL=128
Reply from 192.168.2.4: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.2.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

5.- Prueba TELNET desde PC3 a Switch D-link *en este caso la lista de acceso debe permitir el tráfico TELNET destinado al Switch.* En la Figura 4.22. Nos muestra la pantalla de Conexión para acceso TELNET, mientras que la Figura 4. 23. Nos indica la Conexión Aceptada por el Switch.

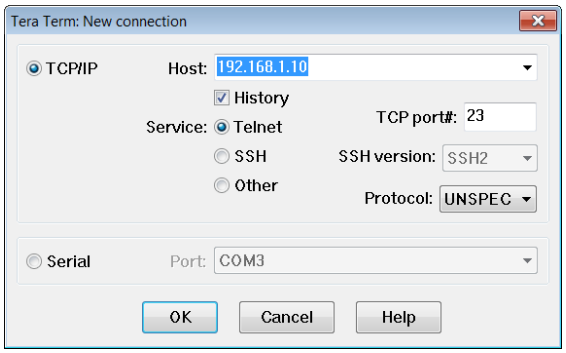


Figura 4.22. TeraTerm Conexión TELNET D-Link 3627 Práctica #8

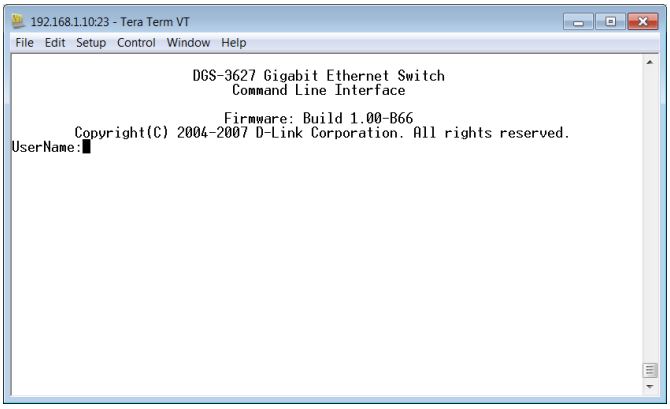


Figura 4.23. Conexión TELNET Establecida D-Link 3627 Práctica #8

6.- Prueba TELNET desde PC1 a Switch D-link *en este caso la lista de acceso debe bloquear el tráfico TELNET destinado al Switch.* La Figura 4.24. Nos indica la Conexión Rechazada por el Switch.

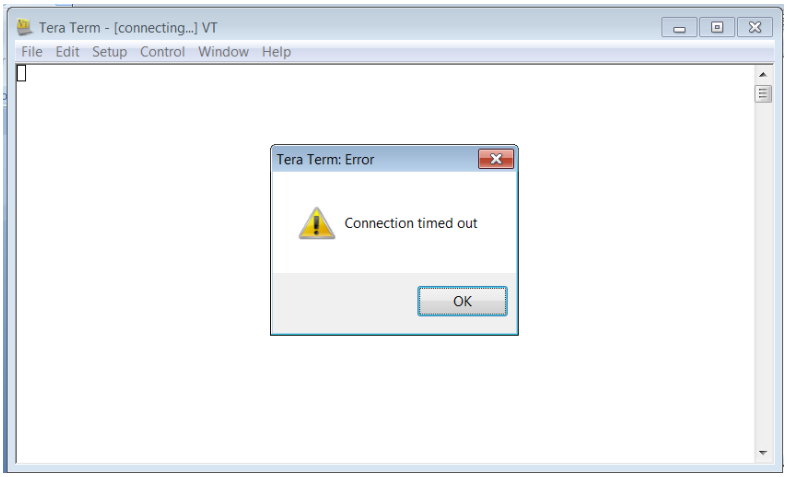


Figura 4.24. Conexión TELNET Rechazada D-Link 3627 Práctica #8

4.10. DESARROLLO PRÁCTICA#9 SIMULACIÓN DE UNA RED QUE PERMITA DIVIDIR DEPARTAMENTOS EN UNA EMPRESA Y DAR PRIORIDAD DE ACCESO A CIERTOS EMPLEADOS POR MEDIO DE ACL

4.10.1. Configuraciones/Direccionamiento

Direccionamiento:

DISPOSITIVO	Dirección IP	Máscara de Red	Interfaz
SWITCH 1			
VLAN 10 (ADMINISTRATIVA)	**192.168.10.10**	**255.255.255.0**	**Ethernet 1-3**
VLAN 20 (GERENCIAL)	**192.168.20.10**	**255.255.255.0**	**Ethernet 4-6**
VLAN 30 (HUMANISTICA)	**192.168.30.10**	**255.255.255.0**	**Ethernet 7-9**
ENLACE TRONCAL	**--**	**--**	**Ethernet 12**
SWITCH 2			
VLAN 10 (ADMINISTRATIVA)	**192.168.10.11**	**255.255.255.0**	**Ethernet 1-3**

VLAN 20 (GERENCIAL)	**192.168.20.11**	**255.255.255.0**	**Ethernet 4-6**
VLAN 30 (HUMANISTICA)	**192.168.30.11**	**255.255.255.0**	**Ethernet 7-9**
ENLACE TRONCAL	**--**	**--**	**Ethernet 11-12**
SWITCH 3			
VLAN 10 (ADMINISTRATIVA)	**192.168.10.12**	**255.255.255.0**	**Ethernet 1-3**
VLAN 20 (GERENCIAL)	**192.168.20.12**	**255.255.255.0**	**Ethernet 4-6**
VLAN 30 (HUMANISTICA)	**192.168.30.12**	**255.255.255.0**	**Ethernet 7-9**
ENLACE TRONCAL	**--**	**--**	**Ethernet 12**
ROUTER 1			
FAST ETHERNET 0/.10	**192.168.10.1**	**255.255.255.0**	**Ethernet**
FAST ETHERNET 0/.20	**192.168.20.1**	**255.255.255.0**	**Ethernet**
FAST ETHERNET 0/.30	**192.168.30.1**	**255.255.255.0**	**Ethernet**
FAST ETHERNET 0/1	**192.168.40.1**	**255.255.255.0**	**Ethernet**
SERIAL 0/1/0 *Clock Rate*	**200.0.0.1** ***128 Kbps***	**255.255.255.252**	**Serial**
ROUTER 2			
FAST ETHERNET 0/0	**192.168.50.1**	**255.255.255.0**	**Ethernet**
FAST ETHERNET 0/.1	**192.168.60.1**	**255.255.255.0**	**Ethernet**
SERIAL 0/1/0	**200.0.0.2**	**255.255.255.252**	**Serial**
HOSTS			

ADMINISTRATIVO			
PC1	**192.168.10.2**	**255.255.255.0**	**Ethernet**
PC2	**192.168.10.3**	**255.255.255.0**	**Ethernet**
IMPRESORA-1	**192.168.10.4**	**255.255.255.0**	**Ethernet**
HOSTS GERENCIAL			
PC1	**192.168.20.2**	**255.255.255.0**	**Ethernet**
IMPRESORA-2	**192.168.20.3**	**255.255.255.0**	**Ethernet**
PC3	**192.168.20.4**	**255.255.255.0**	**Ethernet**
HOSTS GERENCIAL			
IMPRESORA-3	**192.168.30.2**	**255.255.255.0**	**Ethernet**
PC2	**192.168.30.3**	**255.255.255.0**	**Ethernet**
PC3	**192.168.30.4**	**255.255.255.0**	**Ethernet**
JEFES			
HUMANISTICO	**192.168.40.2**	**255.255.255.0**	**Ethernet**
GERENCIAL	**192.168.50.2**	**255.255.255.0**	**Ethernet**
ADMINISTRATIVO	**192.168.60.2**	**255.255.255.0**	**Ethernet**

Usuario y Password:

Password: espe

4.10.2. Procedimiento

4.10.2.1. Topología Práctica 9 Simulador Packet Tracer

La Figura 4.25. Nos muestra la Topología de Red en el Simulador Packet Tracer.

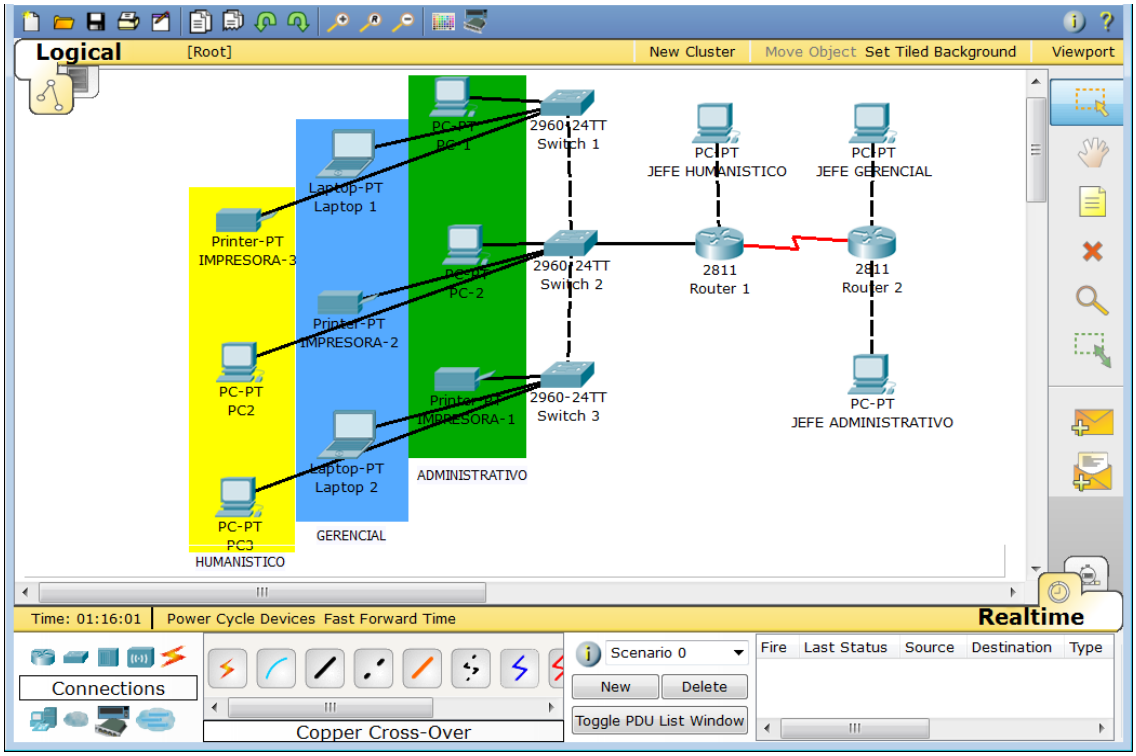


Figura 4.25. Simulación Topología de Red Práctica #9

4.10.2.2. Configuración SWITCH 1 CISCO 2960

1.- Accedemos al Switch y creamos la Vlan "ADMINISTRATIVA", "GERENCIAL" y "HUMANISTICA".

```
SWITCH1(config)#vlan 10
SWITCH1(config-vlan)#name ADMINISTRATIVO
SWITCH1(config-vlan)#EXIT
SWITCH1(config)#vlan 20
SWITCH1(config-vlan)#name GERENCIAL
SWITCH1(config-vlan)#exit
SWITCH1(config)#vlan 30
SWITCH1(config-vlan)#name HUMANISTICO
SWITCH1(config-vlan)#
```

2.- Añadimos los puertos a la VLANs.

```
SWITCH1(config)#interface range f0/1-3
SWITCH1(config-if-range)#switchport mode access
SWITCH1(config-if-range)#switchport access vlan 10
SWITCH1(config-if-range)#exit
SWITCH1(config)#interface range f0/4-6
SWITCH1(config-if-range)#switchport mode access
SWITCH1(config-if-range)#switchport access vlan 20
SWITCH1(config-if-range)#exit
SWITCH1(config)#interface range f0/7-9
SWITCH1(config-if-range)#switchport mode access
SWITCH1(config-if-range)#switchport access vlan 30
```

3.- Añadimos una dirección IP a las Vlans creadas.

```
SWITCH1(config)#interface vlan 10
SWITCH1(config-if)#ip add 192.168.10.10 255.255.255.0
SWITCH1(config-if)#exit
SWITCH1(config)#interface vlan 20
SWITCH1(config-if)#ip add 192.168.20.10 255.255.255.0
SWITCH1(config-if)#exit
SWITCH1(config)#interface vlan 30
SWITCH1(config-if)#ip add 192.168.30.10 255.255.255.0
```

4.- Configuración de Enlace Troncales.

```
SWITCH1(config)#interface f0/12
SWITCH1(config-if)#switchport mode trunk
SWITCH1(config-if)#switchport trunk allowed vlan all
```

4.10.2.3. Configuración SWITCH 2 CISCO 2960

1.- Accedemos al Switch y creamos la Vlan “ADMINISTRATIVA”, “GERENCIAL” y “HUMANISTICA”.

```
SWITCH2(config)#vlan 10
SWITCH2(config-vlan)#name ADMINISTRATIVO
SWITCH2(config-vlan)#exit
SWITCH2(config)#vlan 20
SWITCH2(config-vlan)#name GERENCIAL
SWITCH2(config-vlan)#exit
SWITCH2(config)#vlan 30
SWITCH2(config-vlan)#name HUMANISTICO
```

2.- Añadimos los puertos a la VLANs.

```
SWITCH2(config)#interface range f0/1-3
SWITCH2(config-if-range)#switchport mode access
SWITCH2(config-if-range)#switchport access vlan 10
SWITCH2(config-if-range)#exit
SWITCH2(config)#interface range f0/4-6
SWITCH2(config-if-range)#switchport mode access
SWITCH2(config-if-range)#switchport access vlan 20
SWITCH2(config-if-range)#exit
SWITCH2(config)#interface range f0/7-9
SWITCH2(config-if-range)#switchport mode access
SWITCH2(config-if-range)#switchport access vlan 30
```

3.- Añadimos una dirección IP a las Vlans creadas.

```
SWITCH2(config)#interface vlan 10
SWITCH2(config-if)#ip add 192.168.10.11 255.255.255.0
SWITCH2(config-if)#exit
SWITCH2(config)#interface vlan 20
SWITCH2(config-if)#ip add 192.168.20.11 255.255.255.0
SWITCH2(config-if)#exit
SWITCH2(config)#interface vlan 30
SWITCH2(config-if)#ip add 192.168.30.11 255.255.255.0
```

4.- Configuración de Enlace Troncales.

```
SWITCH2(config)#interface range f0/11-13
SWITCH2(config-if-range)#switchport mode trunk
SWITCH2(config-if-range)#switchport trunk allowed vlan all
```

4.10.2.4. Configuración SWITCH 3 CISCO 2960

1.- Accedemos al Switch y creamos la Vlan “ADMINISTRATIVA”, “GERENCIAL” y “HUMANISTICA”.

```
SWITCH3(config)#vlan 10
SWITCH3(config-vlan)#name ADMINISTRATIVO
SWITCH3(config-vlan)#exit
SWITCH3(config)#vlan 20
SWITCH3(config-vlan)#name GERENCIAL
SWITCH3(config-vlan)#exit
SWITCH3(config)#vlan 30
SWITCH3(config-vlan)#name HUMANISTICO
```

2.- Añadimos los puertos a la VLANs.

```
SWITCH3(config)#interface range f0/1-3
SWITCH3(config-if-range)#switchport mode access
SWITCH3(config-if-range)#switchport access vlan 10
SWITCH3(config-if-range)#exit
SWITCH3(config)#interface range f0/4-6
SWITCH3(config-if-range)#switchport mode access
SWITCH3(config-if-range)#switchport access vlan 20
SWITCH3(config-if-range)#exit
SWITCH3(config)#interface range f0/7-9
SWITCH3(config-if-range)#switchport mode access
SWITCH3(config-if-range)#switchport access vlan 30
```

3.- Añadimos una dirección IP a las Vlans creadas.

```
SWITCH3(config)#interface vlan 10
SWITCH3(config-if)#ip add 192.168.10.12 255.255.255.0
SWITCH3(config-if)#exit
SWITCH3(config)#interface vlan 20
SWITCH3(config-if)#ip add 192.168.20.12 255.255.255.0
SWITCH3(config-if)#exit
SWITCH3(config)#interface vlan 30
SWITCH3(config-if)#ip add 192.168.30.12 255.255.255.0
```

4.- Configuración de Enlace Troncales.

```
SWITCH3(config)#interface f0/12
SWITCH3(config-if)#switchport mode trunk
SWITCH3(config-if)#switchport trunk allowed vlan all
```

4.10.2.5. Configuración ROUTER 1 CISCO 2811

1.- Accedemos al Router configuramos la interfaces virtuales o sub interfaces añadimos el tipo de encapsulación.

```
ROUTER1(config)#interface f0/0
ROUTER1(config-if)#no shutdown
ROUTER1(config-if)#exit
ROUTER1(config)#interface f0/0.10
ROUTER1(config-subif)#encapsulation dot1q 10
ROUTER1(config-subif)#ip address 192.168.10.1 255.255.255.0
ROUTER1(config-subif)#exit
ROUTER1(config)#interface f0/0.20
ROUTER1(config-subif)#encapsulation dot1q 20
ROUTER1(config-subif)#ip address 192.168.20.1 255.255.255.0
ROUTER1(config-subif)#exit
ROUTER1(config)#interface f0/0.30
ROUTER1(config-subif)#encapsulation dot1q 30
ROUTER1(config-subif)#ip address 192.168.30.1 255.255.255.0
```

2.- Configuramos la interface Serial 0/1/0 y Fast Ethernet 0/1 del Router 1.

```
ROUTER1(config)#interface s0/1/0
ROUTER1(config-if)#ip address 200.0.0.1 255.255.255.252
ROUTER1(config-if)#clock rate 128000
ROUTER1(config-if)#no shutdown
ROUTER1(config-if)#exit
ROUTER1(config)#interface f0/1
ROUTER1(config-if)#ip address 192.168.40.1 255.255.255.0
ROUTER1(config-if)#no shutdown
```

3.- Configuramos el protocolo de Enrutamiento en este caso RIPv2.

```
ROUTER1(config)#router rip
ROUTER1(config-router)#version 2
ROUTER1(config-router)#network 192.168.10.0
ROUTER1(config-router)#network 192.168.20.0
ROUTER1(config-router)#network 192.168.30.0
ROUTER1(config-router)#network 192.168.40.0
ROUTER1(config-router)#network 200.0.0.0
```

4.- Creación lista de acceso extendida.

```
Extended IP access list VLAN10
    deny icmp host 192.168.40.2 192.168.10.0 0.0.0.255 echo (3 match(es))
    permit ip any any (6 match(es))
Extended IP access list VLAN20
    permit icmp host 192.168.60.2 host 192.168.20.3 echo (3 match(es))
    deny icmp host 192.168.60.2 192.168.20.0 0.0.0.255 echo (2 match(es))
    deny icmp host 192.168.40.2 192.168.20.0 0.0.0.255 echo (2 match(es))
    permit ip any any (3 match(es))
Extended IP access list VLAN30
    permit icmp host 192.168.60.2 host 192.168.30.2 echo (2 match(es))
    deny icmp host 192.168.60.2 192.168.30.0 0.0.0.255 echo (2 match(es))
    permit ip any any (2 match(es))
```

5.- Aplicación de la lista de acceso a la interfaz correspondiente.

```
ROUTER1(config)#interface f0/0.10
ROUTER1(config-subif)#ip access-group VLAN10 out
ROUTER1(config-subif)#exit
ROUTER1(config)#interface f0/0.20
ROUTER1(config-subif)#ip access-group VLAN20 out
ROUTER1(config-subif)#exit
ROUTER1(config)#interface f0/0.30
ROUTER1(config-subif)#ip access-group VLAN30 out
```

4.10.2.6. Configuración ROUTER 2 CISCO 2811

1.- Accedemos al Router configuramos las interfaces Serial y Fast Ethernet.

```
ROUTER2(config)#interface s0/1/0
ROUTER2(config-if)#ip address 200.0.0.2 255.255.255.252
ROUTER2(config-if)#no shutdown
ROUTER2(config-if)#exit
ROUTER2(config)#interface f0/0
ROUTER2(config-if)#ip address 192.168.50.1 255.255.255.0
ROUTER2(config-if)#no shutdown
ROUTER2(config-if)#exit
ROUTER2(config)#interface f0/1
ROUTER2(config-if)#ip address 192.168.60.1 255.255.255.0
ROUTER2(config-if)#no shutdown
```

2.- Configuramos el protocolo de Enrutamiento en este caso RIPv2.

```
ROUTER2(config)#router rip
ROUTER2(config-router)#version 2
ROUTER2(config-router)#network 192.168.50.0
ROUTER2(config-router)#network 192.168.60.0
ROUTER2(config-router)#network 200.0.0.0
```

4.10.2.7. Tablas De Enrutamiento Router 1 y Router 2

ROUTER1

```
ROUTER1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inte
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.10.0/24 is directly connected, FastEthernet0/0.10
C    192.168.20.0/24 is directly connected, FastEthernet0/0.20
C    192.168.30.0/24 is directly connected, FastEthernet0/0.30
C    192.168.40.0/24 is directly connected, FastEthernet0/1
R    192.168.50.0/24 [120/1] via 200.0.0.2, 00:00:09, Serial0/1/0
R    192.168.60.0/24 [120/1] via 200.0.0.2, 00:00:09, Serial0/1/0
     200.0.0.0/30 is subnetted, 1 subnets
C       200.0.0.0 is directly connected, Serial0/1/0
```

ROUTER2

```
ROUTER2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inte
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

R    192.168.10.0/24 [120/1] via 200.0.0.1, 00:00:14, Serial0/1/0
R    192.168.20.0/24 [120/1] via 200.0.0.1, 00:00:14, Serial0/1/0
R    192.168.30.0/24 [120/1] via 200.0.0.1, 00:00:14, Serial0/1/0
R    192.168.40.0/24 [120/1] via 200.0.0.1, 00:00:14, Serial0/1/0
C    192.168.50.0/24 is directly connected, FastEthernet0/0
C    192.168.60.0/24 is directly connected, FastEthernet0/1
     200.0.0.0/30 is subnetted, 1 subnets
C       200.0.0.0 is directly connected, Serial0/1/0
```

4.10.2.8. Pruebas de Conectividad

JEFE GERENCIAL

1.- Conectividad entre PC JEFE GERENCIAL y PC1 ADMINISTRATIVA *la lista de acceso deberá permitir el tráfico destinado a la PC1ADMINISTRATIVA.*

```
PC>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:

Reply from 192.168.10.2: bytes=32 time=66ms TTL=126
Reply from 192.168.10.2: bytes=32 time=100ms TTL=126
Reply from 192.168.10.2: bytes=32 time=120ms TTL=126
Reply from 192.168.10.2: bytes=32 time=80ms TTL=126

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 66ms, Maximum = 120ms, Average = 91ms
```

2.- Conectividad entre PC JEFE GERENCIAL y IMPRESORA-3 HUMANISTICA *la lista de acceso deberá permitir el tráfico destinado a la IMPRESORA-3 HUMANISTICA*

```
PC>ping 192.168.30.2

Pinging 192.168.30.2 with 32 bytes of data:

Reply from 192.168.30.2: bytes=32 time=110ms TTL=126
Reply from 192.168.30.2: bytes=32 time=100ms TTL=126
Reply from 192.168.30.2: bytes=32 time=100ms TTL=126
Reply from 192.168.30.2: bytes=32 time=100ms TTL=126

Ping statistics for 192.168.30.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 100ms, Maximum = 110ms, Average = 102ms
```

3.- Conectividad entre PC JEFE GERENCIAL y PC3 GERENCIAL *la lista de acceso deberá permitir el tráfico destinado a la PC3 GERENCIAL*

```
PC>ping 192.168.20.4

Pinging 192.168.20.4 with 32 bytes of data:

Reply from 192.168.20.4: bytes=32 time=90ms TTL=126
Reply from 192.168.20.4: bytes=32 time=100ms TTL=126
Reply from 192.168.20.4: bytes=32 time=80ms TTL=126
Reply from 192.168.20.4: bytes=32 time=100ms TTL=126

Ping statistics for 192.168.20.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 80ms, Maximum = 100ms, Average = 92ms
```

JEFE ADMINISTRATIVO

1.- Conectividad entre PC JEFE ADMNISTRATIVO y PC2 ADMINISTRATIVA *la lista de acceso deberá permitir el tráfico destinado a la PC2 ADMINISTRATIVA.*

```
PC>ping 192.168.10.3

Pinging 192.168.10.3 with 32 bytes of data:

Reply from 192.168.10.3: bytes=32 time=70ms TTL=126
Reply from 192.168.10.3: bytes=32 time=30ms TTL=126
Reply from 192.168.10.3: bytes=32 time=80ms TTL=126
Reply from 192.168.10.3: bytes=32 time=80ms TTL=126

Ping statistics for 192.168.10.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 30ms, Maximum = 80ms, Average = 65ms
```

2.- Conectividad entre PC JEFE ADMINISTRATIVO y IMPRESORA-2 GERENCIAL *la lista de acceso deberá permitir el tráfico destinado a la IMPRESORA-2 GERENCIAL*

```
PC>ping 192.168.20.3

Pinging 192.168.20.3 with 32 bytes of data:

Reply from 192.168.20.3: bytes=32 time=70ms TTL=126
Reply from 192.168.20.3: bytes=32 time=70ms TTL=126
Reply from 192.168.20.3: bytes=32 time=60ms TTL=126
Reply from 192.168.20.3: bytes=32 time=60ms TTL=126

Ping statistics for 192.168.20.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 60ms, Maximum = 70ms, Average = 65ms
```

3.- Conectividad entre PC JEFE ADMINISTRATIVO y PC3 HUMANISTICO *la lista de acceso deberá bloquear el tráfico destinado a la PC3 HUMANISTICO*

```
PC>ping 192.168.30.4

Pinging 192.168.30.4 with 32 bytes of data:

Reply from 200.0.0.1: Destination host unreachable.
Reply from 200.0.0.1: Destination host unreachable.
Reply from 200.0.0.1: Destination host unreachable.
Reply from 200.0.0.1: Destination host unreachable.

Ping statistics for 192.168.30.4:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

JEFE HUMANISTICO

1.- Conectividad entre PC JEFE HUMANISTICO y PC1 ADMINISTRATIVA *la lista de acceso deberá bloquear el tráfico destinado a la PC1 ADMINISTRATIVA.*

```
PC>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:

Reply from 192.168.40.1: Destination host unreachable.
Reply from 192.168.40.1: Destination host unreachable.
Reply from 192.168.40.1: Destination host unreachable.
Reply from 192.168.40.1: Destination host unreachable.

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

2.- Conectividad entre PC JEFE HUMANISTICO y IMPRESORA-2 GERENCIAL *la lista de acceso deberá bloquear el tráfico destinado a la IMPRESORA-2 GERENCIAL*

```
PC>ping 192.168.20.3

Pinging 192.168.20.3 with 32 bytes of data:

Reply from 192.168.40.1: Destination host unreachable.
Reply from 192.168.40.1: Destination host unreachable.
Reply from 192.168.40.1: Destination host unreachable.
Reply from 192.168.40.1: Destination host unreachable.

Ping statistics for 192.168.20.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

3.- Conectividad entre PC JEFE HUMANISTICO y PC3 HUMANISTICO *la lista de acceso deberá permitir el tráfico destinado a la PC3 HUMANISTICO*

```
PC>ping 192.168.30.4

Pinging 192.168.30.4 with 32 bytes of data:

Reply from 192.168.30.4: bytes=32 time=50ms TTL=127
Reply from 192.168.30.4: bytes=32 time=18ms TTL=127
Reply from 192.168.30.4: bytes=32 time=60ms TTL=127
Reply from 192.168.30.4: bytes=32 time=90ms TTL=127

Ping statistics for 192.168.30.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 18ms, Maximum = 90ms, Average = 54ms
```

4.11. DESARROLLO PRÁCTICA#10 IMPLEMENTACIÓN DE UNA RED JERARQUICA CON REDUNDANCIA

4.11.1. Configuraciones/Direccionamiento

Direccionamiento:

	DISPOSITIVO	Dirección IP	Máscara de Red	Interfaz
CAPA DE ACCESO				

	SWITCH *3COM 4210 /HP 2512*			
	VLAN 20 (ESTUDIANTES)	**192.168.2.0**	**255.255.255.0**	**Ethernet 4-6**
	VLAN 10 (MAESTROS)	**192.168.1.0**	**255.255.255.0**	**Ethernet 1-3**
	ENLACE TRONCAL	**--**	**--**	**Ethernet 11**
CAPA DE DISTRIBUCIÓN				
	SWITCH *3COM 4500*			
	VLAN 20 (ESTUDIANTES)	**192.168.2.0**	**255.255.255.0**	**Ethernet 4-6**
	VLAN 10 (MAESTROS)	**192.168.1.0**	**255.255.255.0**	**Ethernet 1-3**
	ENLACE TRONCAL	**--**	**--**	**Ethernet 10-11-12**
	SWITCH *3COM 5500*			
	VLAN 20 (ESTUDIANTES)	**192.168.2.0**	**255.255.255.0**	**Ethernet 4-6**
	VLAN 10 (MAESTROS)	**192.168.1.0**	**255.255.255.0**	**Ethernet 1-3**
	ENLACE TRONCAL	**--**	**--**	**Ethernet 10-11-12**
	SWITCH *CISCO 3560*			
	VLAN 20 (ESTUDIANTES)	**192.168.2.0**	**255.255.255.0**	**Ethernet 4-6**

	VLAN 10 (MAESTROS)	**192.168.1.0**	**255.255.255.0**	**Ethernet 1-3**
	ENLACE TRONCAL	--	--	**Ethernet 10-11-12**
CAPA DE NUCLEO				
	SWITCH-1 ***D-Link 3627***			
	VLAN 20 (ESTUDIANTES)	**192.168.2.0**	**255.255.255.0**	**Ethernet 4-6**
	VLAN 10 (MAESTROS)	**192.168.1.0**	**255.255.255.0**	**Ethernet 1-3**
	ENLACE TRONCAL	--	--	**Ethernet 8-9-10-11-12**
	SWITCH-2 ***D-Link 3627***			
	VLAN 20 (ESTUDIANTES)	**192.168.2.0**	**255.255.255.0**	**Ethernet 4-6**
	VLAN 10 (MAESTROS)	**192.168.1.0**	**255.255.255.0**	**Ethernet 1-3**
	ENLACE TRONCAL	--	--	**Ethernet 7-8-9-10-11-12**
	ROUTER ***CISCO 2800***			
	SUBINTERFAZ 10	**192.168.1.10**	**255.255.255.0**	**Ethernet**
	SUBINTERFAZ 20	**192.168.2.10**	**255.255.255.0**	**Ethernet**
HOST				
	PC1 ESTUDIANT	**192.168.2.2**	**255.255.255.0**	**Ethernet**

	E			
	PC2 MAESTRO	**192.168.1.2**	**255.255.255.0**	**Ethernet**
	PC3 ESTUDIANTE	**192.168.2.3**	**255.255.255.0**	**Ethernet**
	PC4 MAESTRO	**192.168.1.3**	**255.255.255.0**	**Ethernet**
	PC5 ESTUDIANTE	**192.168.2.4**	**255.255.255.0**	**Ethernet**
	PC6 MAESTRO	**192.168.1.4**	**255.255.255.0**	**Ethernet**

Usuario y Password:

Usuario: admin

Password: espe

4.11.2. Procedimiento

4.11.2.1. Configuración Equipos Capa de Acceso

4.11.2.1.1. Configuración Equipos 3COM 4210

1.- Accedemos al Switch y creamos la Vlan “MAESTROS” y “ESTUDIANTES”.

```
[SWITCH1]vlan 10
[SWITCH1-vlan10]name MAESTROS
[SWITCH1-vlan10]quit
[SWITCH1]vlan 20
[SWITCH1-vlan20]name ESTUDIANTES
```

2.- Añadimos los puertos a las VLANs.

```
[SWITCH1]vlan 10
[SWITCH1-vlan10]port ethernet 1/0/1 to ethernet 1/0/3
[SWITCH1-vlan10]quit
[SWITCH1]vlan 20
[SWITCH1-vlan20]port ethernet 1/0/4 to ethernet 1/0/6
```

3.- Configuración de Enlace Troncales.

```
[SWITCH1]interface ethernet 1/0/12
[SWITCH1-Ethernet1/0/12]port link-type trunk
[SWITCH1-Ethernet1/0/12]port trunk permit vlan 10
 Please wait... Done.
[SWITCH1-Ethernet1/0/12]port trunk permit vlan 20
 Please wait... Done.
```

4.11.2.1.2. Configuración Equipo HP 2512

1.- Accedemos al Switch y creamos la Vlan "MAESTROS" y "ESTUDIANTES".

```
SWITCH3(config)# vlan 10
SWITCH3(vlan-10)# name MAESTROS
SWITCH3(vlan-10)# exit
SWITCH3(config)# vlan 20
SWITCH3(vlan-20)# name ESTUDIANTES
```

2.- Añadimos los puertos a las VLANs.

```
SWITCH3(config)# vlan 10
SWITCH3(vlan-10)# untagged ethernet 1
SWITCH3(vlan-10)# untagged ethernet 2
SWITCH3(vlan-10)# untagged ethernet 3
```

```
SWITCH3(config)# vlan 20
SWITCH3(vlan-20)# untagged ethernet 4
SWITCH3(vlan-20)# untagged ethernet 5
SWITCH3(vlan-20)# untagged ethernet 6
```

3.- Configuración de Enlace Troncales.

```
SWITCH3# configure
SWITCH3(config)# trunk ethernet 12 trk1 trunk
```

4.11.2.2. Configuración Equipos Capa de Distribución

4.11.2.2.1. Configuración Equipos 3COM 4500

1.- Accedemos al Switch y creamos la Vlan "MAESTROS" y "ESTUDIANTES".

```
[4500]vlan 10
[4500-vlan10]name MAESTROS
[4500-vlan10]quit
[4500]vlan 20
[4500-vlan20]name ESTUDIANTES
```

2.- Añadimos los puertos a las VLANs.

```
[4500]vlan 10
[4500-vlan10]port ethernet 1/0/1 to ethernet 1/0/3
[4500-vlan10]quit
[4500]vlan 20
[4500-vlan20]port ethernet 1/0/4 to ethernet 1/0/6
```

3.- Configuración de Enlace Troncales.

```
[4500]interface ethernet 1/0/10
[4500-Ethernet1/0/10]port link-type trunk
[4500-Ethernet1/0/10]port trunk permit vlan 10
 Please wait... Done.
[4500-Ethernet1/0/10]port trunk permit vlan 20
 Please wait... Done._
```

```
[4500]interface ethernet 1/0/11
[4500-Ethernet1/0/11]port link-type trunk
[4500-Ethernet1/0/11]port trunk permit vlan 10
 Please wait... Done.
[4500-Ethernet1/0/11]port trunk permit vlan 20
 Please wait... Done._
```

```
[4500]interface ethernet 1/0/12
[4500-Ethernet1/0/12]port link-type trunk
[4500-Ethernet1/0/12]port trunk permit vlan 10
 Please wait... Done.
[4500-Ethernet1/0/12]port trunk permit vlan 20
 Please wait... Done._
```

4.11.2.2.2. Configuración Equipos 3COM 5500

1.- Accedemos al Switch y creamos la Vlan “MAESTROS” y “ESTUDIANTES”.

```
[5500-EI]vlan 10
[5500-EI-vlan10]name MAESTROS
[5500-EI-vlan10]quit
[5500-EI]vlan 20
[5500-EI-vlan20]name ESTUDIANTES
```

2.- Añadimos los puertos a las VLANs.

```
[5500-EI]vlan 10
[5500-EI-vlan10]port ethernet 1/0/1 to ethernet 1/0/3
[5500-EI-vlan10]quit
[5500-EI]vlan 20
[5500-EI-vlan20]port ethernet 1/0/4 to ethernet 1/0/6
```

3.- Configuración de Enlace Troncales.

```
[5500-EI]interface ethernet 1/0/10
[5500-EI-Ethernet1/0/10]port link-type trunk
[5500-EI-Ethernet1/0/10]port trunk permit vlan 10
 Please wait... Done.
[5500-EI-Ethernet1/0/10]port trunk permit vlan 20
 Please wait... Done.
```

```
[5500-EI]interface ethernet 1/0/11
[5500-EI-Ethernet1/0/11]port link-type trunk
[5500-EI-Ethernet1/0/11]port trunk permit vlan 10
 Please wait... Done.
[5500-EI-Ethernet1/0/11]port trunk permit vlan 20
 Please wait... Done.
```

```
[5500-EI]interface ethernet 1/0/12
[5500-EI-Ethernet1/0/12]port link-type trunk
[5500-EI-Ethernet1/0/12]port trunk permit vlan 10
 Please wait... Done.
[5500-EI-Ethernet1/0/12]port trunk permit vlan 20
 Please wait... Done.
```

4.11.2.2.3. Configuración CISCO 3560

1.- Accedemos al Switch y creamos la Vlan “MAESTROS” y “ESTUDIANTES”.

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name MAESTROS
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name ESTUDIANTES
```

2.- Añadimos los puertos a la VLANs.

```
Switch(config)#interface range f0/1-3
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#exit
Switch(config)#interface range f0/4-6
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 20
```

3.- Configuración de Enlace Troncales.

```
Switch(config)#interface range f0/10-12
Switch(config-if-range)#duplex full
Switch(config-if-range)#switchport trunk encapsulation dot1q
Switch(config-if-range)#switchport mode trunk
```

4.11.2.3. Configuración Equipos Capa de Core

En esta capa la configuración será la misma para los 2 Switch D-link 3627 se detallará la configuración de un equipo y se repitirá el proceso para otro

4.11.2.3.1. Configuración D-Link DES-3627

1.- Accedemos al Switch y creamos la Vlan “MAESTROS” y “ESTUDIANTES”.

```
DGS-3627:4#create vlan MAESTROS tag 10
Command: create vlan MAESTROS tag 10

Success.

DGS-3627:4#create vlan ESTUDIANTES tag 20
Command: create vlan ESTUDIANTES tag 20

Success.
```

2.- Añadimos los puertos a la VLANs.

```
DGS-3627:4#config vlan default delete 1-6
Command: config vlan default delete 1-6

Success.

DGS-3627:4#config vlan MAESTROS add untagged 1-3
Command: config vlan MAESTROS add untagged 1-3

Success.

DGS-3627:4#config vlan ESTUDIANTES add untagged 4-6
Command: config vlan ESTUDIANTES add untagged 4-6

Success.
```

3.- Configuración de Enlace Troncales.

```
DGS-3627:4#config vlan MAESTROS add tagged 8-12
Command: config vlan MAESTROS add tagged 8-12

Success.

DGS-3627:4#config vlan ESTUDIANTES add tagged 8-12
Command: config vlan ESTUDIANTES add tagged 8-12

Success.
```

4.11.2.3.2. Configuración CISCO 2800

1.- Accedemos al Router configuramos la interfaces virtuales o sub interfaces añadimos el tipo de encapsulación.

```
ROUTER(config)#interface f0/0.20
ROUTER(config-subif)#encapsulation dot1q 20
ROUTER(config-subif)#ip address 192.168.2.10 255.255.255.0
ROUTER(config-subif)#exit
ROUTER(config)#interface f0/0.10
ROUTER(config-subif)#encapsulation dot1q 10
ROUTER(config-subif)#ip address 192.168.1.10 255.255.255.0
```

2.- Configuramos el protocolo de Enrutamiento en este caso RIPv2.

```
ROUTER(config)#router rip
ROUTER(config-router)#version 2
ROUTER(config-router)#network 192.168.1.0
ROUTER(config-router)#network 192.168.2.0
```

4.11.2.4. Pruebas de Conectividad Sin Enlaces Caídos

La Figura 4.26. Nos muestra la Topología de Red de la Práctica # 10 Sin Enlaces caídos.

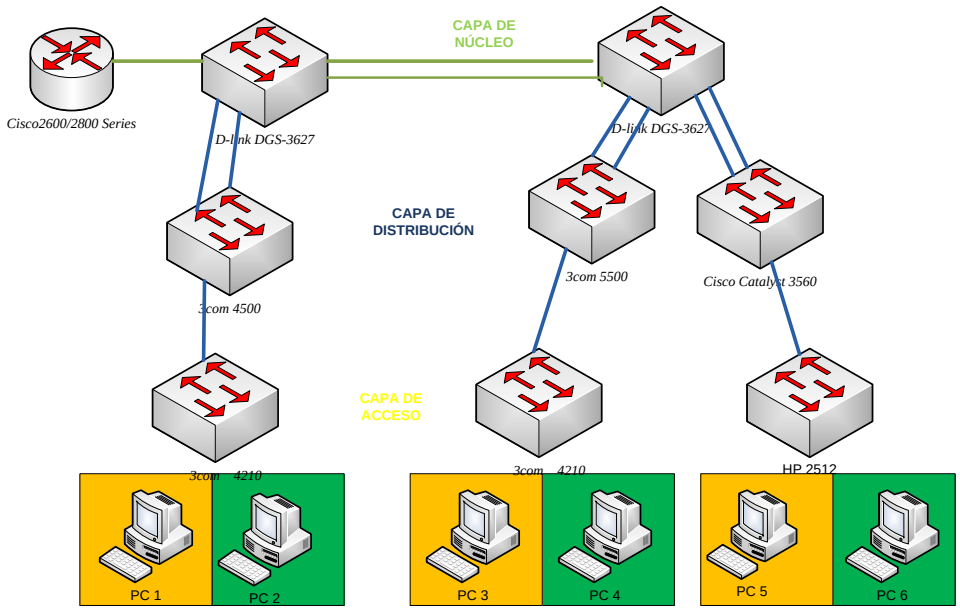


Figura 4.26. Topología de Red Sin Enlaces Caídos Práctica #10

1.- Conectividad entre PC1 y PC3

```
C:\Users\FOCH>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:
Reply from 192.168.2.3: bytes=32 time=1ms TTL=128
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

2.- Conectividad entre PC2 y PC6.

```
C:\Users\FOCH>ping 192.168.1.4

Pinging 192.168.1.4 with 32 bytes of data:
Reply from 192.168.1.4: bytes=32 time=2ms TTL=128
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms
```

3.- Conectividad entre PC2 y PC4.

```
C:\Users\FOCH>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:
Reply from 192.168.1.3: bytes=32 time=1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

4.11.2.5. Pruebas de Conectividad Con Enlaces Caídos

La Figura 4.27. Nos muestra la Topología de Red de la Práctica # 10 Con Enlaces caídos.

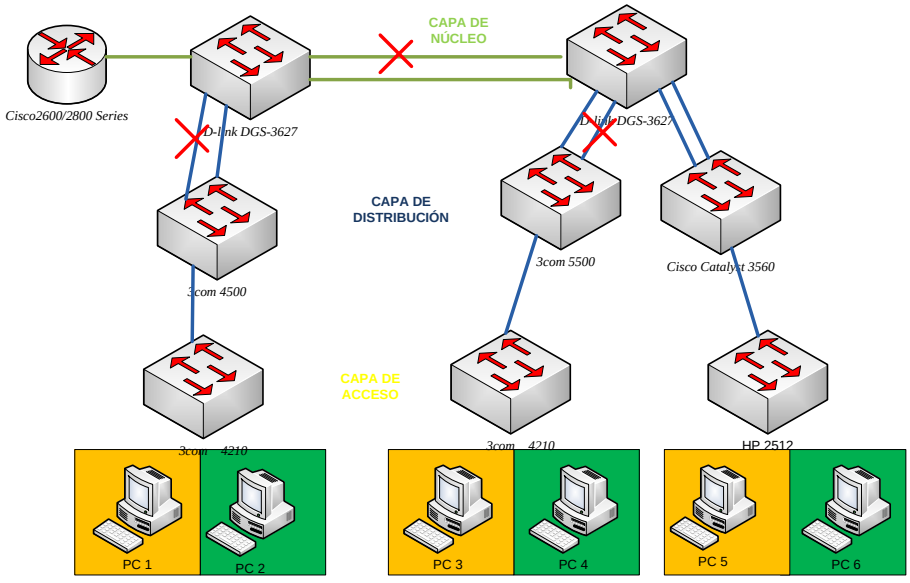


Figura 4.26. Topología de Red Sin Enlaces Caídos Práctica #10

1.- Conectividad entre PC1 y PC3

```
C:\Users\FOCH>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:
Reply from 192.168.2.3: bytes=32 time=1ms TTL=128
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

2.- Conectividad entre PC2 y PC6.

```
C:\Users\FOCH>ping 192.168.1.4

Pinging 192.168.1.4 with 32 bytes of data:
Reply from 192.168.1.4: bytes=32 time=2ms TTL=128
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms
```

3.- Conectividad entre PC2 y PC4.

```
C:\Users\FOCH>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:
Reply from 192.168.1.3: bytes=32 time=1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

4.12. DESARROLLO PRÁCTICA#11 IMPLEMENTACIÓN DE UNA RED JERARQUICA QUE PERMITA LA ADMINISTRACIÓN POR MEDIO DE ACCESSO REMOTO (SSH)

4.12.1. Configuraciones/Direccionamiento

Direccionamiento:

	DISPOSITIVO	Dirección IP	Máscara de Red	Interfaz
CAPA DE ACCESO				
	SWITCH *3COM 4210 /HP 2512*			
	VLAN 20 (ESTUDIANTES)	**192.168.2.0**	**255.255.255.0**	**Ethernet 4-6**
	VLAN 10 (MAESTROS)	**192.168.1.0**	**255.255.255.0**	**Ethernet 1-3**
	ENLACE TRONCAL	**--**	**--**	**Ethernet 11**
CAPA DE DISTRIBUCIÓN				
	SWITCH *3COM 4500*			
	VLAN 20 (ESTUDIANTES)	**192.168.2.0**	**255.255.255.0**	**Ethernet 4-6**
	VLAN 10 (MAESTROS)	**192.168.1.0**	**255.255.255.0**	**Ethernet 1-3**
	ENLACE TRONCAL	**--**	**--**	**Ethernet 10-11-12**
	SWITCH *3COM 5500*			
	VLAN 20 (ESTUDIANTES)	**192.168.2.0**	**255.255.255.0**	**Ethernet 4-6**
	VLAN 10 (MAESTROS)	**192.168.1.0**	**255.255.255.0**	**Ethernet 1-3**
	ENLACE TRONCAL	**--**	**--**	**Ethernet 10-11-12**
	SWITCH *CISCO 3560*			
	VLAN 20 (ESTUDIANTES)	**192.168.2.0**	**255.255.255.0**	**Ethernet 4-6**
	VLAN 10 (MAESTROS)	**192.168.1.0**	**255.255.255.0**	**Ethernet 1-3**
	ENLACE TRONCAL	**--**	**--**	**Ethernet 10-11-12**
CAPA DE NUCLEO				
	SWITCH-1 *D-Link 3627*			
	VLAN 20 (ESTUDIANTES)	**192.168.2.0**	**255.255.255.0**	**Ethernet 4-6**
	VLAN 10 (MAESTROS)	**192.168.1.0**	**255.255.255.0**	**Ethernet 1-3**
	ENLACE TRONCAL	**--**	**--**	**Ethernet 8-9-10-11-12**
	SWITCH-2 *D-Link 3627*			
	VLAN 20 (ESTUDIANTES)	**192.168.2.0**	**255.255.255.0**	**Ethernet 4-6**

	VLAN 10 (MAESTROS)	**192.168.1.0**	**255.255.255.0**	**Ethernet 1-3**
	ENLACE TRONCAL	**--**	**--**	**Ethernet 7-8-9-10-11-12**
	ROUTER *CISCO 2800*			
	SUBINTERFAZ 10	**192.168.1.10**	**255.255.255.0**	**Ethernet**
	SUBINTERFAZ 20	**192.168.2.10**	**255.255.255.0**	**Ethernet**
HOST				
	PC1 ESTUDIANTE	**192.168.2.2**	**255.255.255.0**	**Ethernet**
	PC2 MAESTRO	**192.168.1.2**	**255.255.255.0**	**Ethernet**
	PC3 ESTUDIANTE	**192.168.2.3**	**255.255.255.0**	**Ethernet**
	PC4 MAESTRO	**192.168.1.3**	**255.255.255.0**	**Ethernet**
	PC5 ESTUDIANTE	**192.168.2.4**	**255.255.255.0**	**Ethernet**
	PC6 MAESTRO	**192.168.1.4**	**255.255.255.0**	**Ethernet**

Usuario y Password:

Usuario: admin

Password: espe

4.12.2. Procedimiento

4.12.2.1. Configuración Equipos Capa de Acceso

En esta capa la configuración será la misma para los 2 Switch 3com 4210 se detallará la configuración de un equipo y se repetirá el proceso para otro

4.12.2.1.1. Configuración Equipos 3COM 4210

1.- Accedemos al Switch y creamos la Vlan “MAESTROS” y “ESTUDIANTES”.

```
[SWITCH1]vlan 10
[SWITCH1-vlan10]name MAESTROS
[SWITCH1-vlan10]quit
[SWITCH1]vlan 20
[SWITCH1-vlan20]name ESTUDIANTES
```

2.- Añadimos los puertos a las VLANs.

```
[SWITCH1]vlan 10
[SWITCH1-vlan10]port ethernet 1/0/1 to ethernet 1/0/3
[SWITCH1-vlan10]quit
[SWITCH1]vlan 20
[SWITCH1-vlan20]port ethernet 1/0/4 to ethernet 1/0/6
```

3.- Configuración de Enlace Troncales.

```
[SWITCH1]interface ethernet 1/0/12
[SWITCH1-Ethernet1/0/12]port link-type trunk
[SWITCH1-Ethernet1/0/12]port trunk permit vlan 10
 Please wait... Done.
[SWITCH1-Ethernet1/0/12]port trunk permit vlan 20
 Please wait... Done.
```

4.12.2.1.2. Configuración Equipo HP 2512

1.- Accedemos al Switch y creamos la Vlan “MAESTROS” y “ESTUDIANTES”.

```
SWITCH3(config)# vlan 10
SWITCH3(vlan-10)# name MAESTROS
SWITCH3(vlan-10)# exit
SWITCH3(config)# vlan 20
SWITCH3(vlan-20)# name ESTUDIANTES
```

2.- Añadimos los puertos a las VLANs.

```
SWITCH3(config)# vlan 10
SWITCH3(vlan-10)# untagged ethernet 1
SWITCH3(vlan-10)# untagged ethernet 2
SWITCH3(vlan-10)# untagged ethernet 3
```

```
SWITCH3(config)# vlan 20
SWITCH3(vlan-20)# untagged ethernet 4
SWITCH3(vlan-20)# untagged ethernet 5
SWITCH3(vlan-20)# untagged ethernet 6
```

3.- Configuración de Enlace Troncales.

```
SWITCH3# configure
SWITCH3(config)# trunk ethernet 12 trk1 trunk
```

4.12.2.2. Configuración Equipos Capa de Distribución

4.12.2.2.1. Configuración Equipos 3COM 4500

1.- Accedemos al Switch y creamos la Vlan “MAESTROS” y “ESTUDIANTES”.

```
[4500]vlan 10
[4500-vlan10]name MAESTROS
[4500-vlan10]quit
[4500]vlan 20
[4500-vlan20]name ESTUDIANTES
```

2.- Añadimos los puertos a las VLANs.

```
[4500]vlan 10
[4500-vlan10]port ethernet 1/0/1 to ethernet 1/0/3
[4500-vlan10]quit
[4500]vlan 20
[4500-vlan20]port ethernet 1/0/4 to ethernet 1/0/6
```

3.- Configuración de Enlace Troncales.

```
[4500]interface ethernet 1/0/10
[4500-Ethernet1/0/10]port link-type trunk
[4500-Ethernet1/0/10]port trunk permit vlan 10
 Please wait... Done.
[4500-Ethernet1/0/10]port trunk permit vlan 20
 Please wait... Done._
```

```
[4500]interface ethernet 1/0/11
[4500-Ethernet1/0/11]port link-type trunk
[4500-Ethernet1/0/11]port trunk permit vlan 10
 Please wait... Done.
[4500-Ethernet1/0/11]port trunk permit vlan 20
 Please wait... Done._
```

```
[4500]interface ethernet 1/0/12
[4500-Ethernet1/0/12]port link-type trunk
[4500-Ethernet1/0/12]port trunk permit vlan 10
 Please wait... Done.
[4500-Ethernet1/0/12]port trunk permit vlan 20
 Please wait... Done._
```

4.12.2.2.2. Configuración Equipos 3COM 5500

1.- Accedemos al Switch y creamos la Vlan “MAESTROS” y “ESTUDIANTES” y añadimos una dirección IP a la “VLAN MAESTROS”.

```
[5500-EI]vlan 10
[5500-EI-vlan10]name MAESTROS
[5500-EI-vlan10]quit
[5500-EI]vlan 20
[5500-EI-vlan20]name ESTUDIANTES
```

```
[5500-EI]interface Vlan-interface 10
[5500-EI-Vlan-interface10]
%Apr  2 02:52:21:544 2000 5500-EI L2INF/5/VLANIF LINK STATUS CHANGE:- 1 -
 Vlan-interface10 is UP

[5500-EI-Vlan-interface10]ip add 192.168.1.11 255.255.255.0
```

2.- Añadimos los puertos a las VLANs.

```
[5500-EI]vlan 10
[5500-EI-vlan10]port ethernet 1/0/1 to ethernet 1/0/3
[5500-EI-vlan10]quit
[5500-EI]vlan 20
[5500-EI-vlan20]port ethernet 1/0/4 to ethernet 1/0/6
```

3.- Configuración de Enlace Troncales.

```
[5500-EI]interface ethernet 1/0/10
[5500-EI-Ethernet1/0/10]port link-type trunk
[5500-EI-Ethernet1/0/10]port trunk permit vlan 10
 Please wait... Done.
[5500-EI-Ethernet1/0/10]port trunk permit vlan 20
 Please wait... Done.
```

```
[5500-EI]interface ethernet 1/0/11
[5500-EI-Ethernet1/0/11]port link-type trunk
[5500-EI-Ethernet1/0/11]port trunk permit vlan 10
 Please wait... Done.
[5500-EI-Ethernet1/0/11]port trunk permit vlan 20
 Please wait... Done.
```

```
[5500-EI]interface ethernet 1/0/12
[5500-EI-Ethernet1/0/12]port link-type trunk
[5500-EI-Ethernet1/0/12]port trunk permit vlan 10
 Please wait... Done.
[5500-EI-Ethernet1/0/12]port trunk permit vlan 20
 Please wait... Done.
```

4.- Creamos las claves RSA

```
<5500-EI>system-view
System View: return to User View with Ctrl+Z.
[5500-EI]rsa local-key-pair create
The local-key-pair will be created.
% The local-key-pair already exist.
Confirm to replace them? [Y/N]:y
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
       It will take a few minutes.
Input the bits in the modulus[default = 1024]:1024
Generating keys...
.++++++
.....++++++
.........++++++++
.............................++++++++
......Done!
```

5.- Ponemos la Autenticación AAA y ponemos el tipo de protocolo de entrada.

```
[5500-EI]user-interface vty 0 4
[5500-EI-ui-vty0-4]authentication-mode scheme
[5500-EI-ui-vty0-4]protocol inbound ssh
```

6.- Creamos el usuario:”PC1” y ponemos la contraseña:”espe”.

```
[5500-EI]local-user PC1
New local user added.
[5500-EI-luser-PC1]password simple espe
[5500-EI-luser-PC1]service-type ssh
[5500-EI-luser-PC1]quit
[5500-EI]ssh user PC1 authentication-type password
```

4.12.2.2.3. Configuración CISCO 3560

1.- Accedemos al Switch y creamos la Vlan "MAESTROS" y "ESTUDIANTES".

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name MAESTROS
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name ESTUDIANTES
```

2.- Añadimos los puertos a la VLANs.

```
Switch(config)#interface range f0/1-3
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#exit
Switch(config)#interface range f0/4-6
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 20
```

3.- Configuración de Enlace Troncales.

```
Switch(config)#interface range f0/10-12
Switch(config-if-range)#duplex full
Switch(config-if-range)#switchport trunk encapsulation dot1q
Switch(config-if-range)#switchport mode trunk
```

4.12.2.3. Configuración Equipos Capa de Core

En esta capa la configuración será la misma para los 2 Switch D-link 3627 se detallará la configuración de un equipo y se repetirá el proceso para otro

4.12.2.3.1. Configuración D-Link DES-3627

1.- Accedemos al Switch y creamos la Vlan "MAESTROS" y "ESTUDIANTES".

```
DGS-3627:4#create vlan MAESTROS tag 10
Command: create vlan MAESTROS tag 10

Success.

DGS-3627:4#create vlan ESTUDIANTES tag 20
Command: create vlan ESTUDIANTES tag 20

Success.
```

2.- Añadimos los puertos a la VLANs.

```
DGS-3627:4#config vlan default delete 1-6
Command: config vlan default delete 1-6

Success.

DGS-3627:4#config vlan MAESTROS add untagged 1-3
Command: config vlan MAESTROS add untagged 1-3

Success.

DGS-3627:4#config vlan ESTUDIANTES add untagged 4-6
Command: config vlan ESTUDIANTES add untagged 4-6

Success.
```

3.- Configuración de Enlace Troncales.

```
DGS-3627:4#config vlan MAESTROS add tagged 8-12
Command: config vlan MAESTROS add tagged 8-12

Success.

DGS-3627:4#config vlan ESTUDIANTES add tagged 8-12
Command: config vlan ESTUDIANTES add tagged 8-12

Success.
```

4.- Accedemos al Switch y configuramos una cuenta como administrador.

```
DGS-3627:4#create account admin espe
Command: create account admin espe

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

5.- Configuramos la IP de la VLAN “MAESTROS”.

```
DGS-3627:4#create ipif MAESTROS 192.168.1.10/24 MAESTROS
Command: create ipif MAESTROS 192.168.1.10/24 MAESTROS

Success.
```

6.- Para configurar SSH en el Switch D-link 3627 utilizamos los siguientes comandos.

```
DGS-3627:4#config ssh user espe authmode password
Command: config ssh user espe authmode password

Success.
```

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

```
DGS-3627:4#config ssh algorithm RSA enable
Command: config ssh algorithm RSA enable

Success.

DGS-3627:4
```

8.- Habilitamos SSH en el Switch.

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

TELNET will be disabled when enable SSH.
Success.

DGS-3627:4
```

4.12.2.3.2. Configuración CISCO 2800

1.- Accedemos al Router configuramos la interfaces virtuales o sub interfaces añadimos el tipo de encapsulación.

```
ROUTER(config)#interface f0/0.20
ROUTER(config-subif)#encapsulation dot1q 20
ROUTER(config-subif)#ip address 192.168.2.10 255.255.255.0
ROUTER(config-subif)#exit
ROUTER(config)#interface f0/0.10
ROUTER(config-subif)#encapsulation dot1q 10
ROUTER(config-subif)#ip address 192.168.1.10 255.255.255.0
```

2.- Configuramos el protocolo de Enrutamiento en este caso RIPv2.

```
ROUTER(config)#router rip
ROUTER(config-router)#version 2
ROUTER(config-router)#network 192.168.1.0
ROUTER(config-router)#network 192.168.2.0
```

4.12.2.4. Prueba Acceso SSH Switch 3COM 5500

1.- Ingresamos al programa TERATERM, ponemos el protocolo SSH la dirección IP 192.168.1.11 y presionamos OK. En la Figura 4.27. Nos muestra la pantalla de Conexión para acceso SSH.

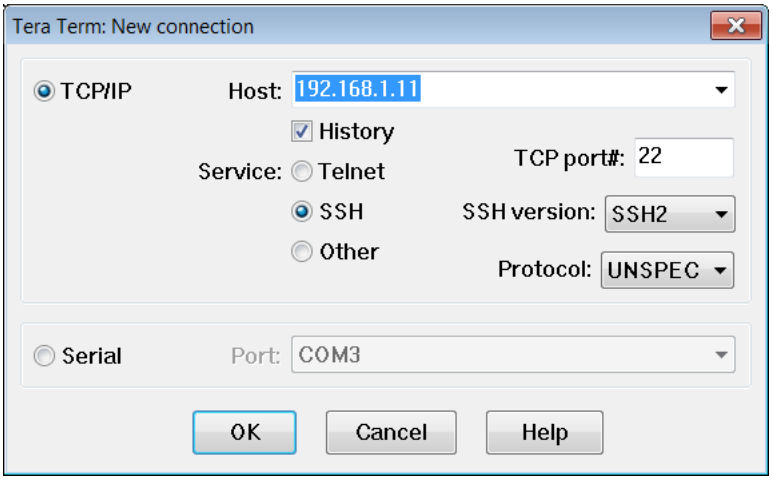


Figura 4.27. TeraTerm Conexión SSH 3Com 5500 Práctica #11

2.- Nos pedirá el nombre de usuario: "PC1" y la contraseña: "espe" para poder acceder al Switch. La Figura 4.28. Nos muestra la pantalla de Autenticación para el Acceso SSH, mientras que la Figura 4.29. Es la imagen de Acceso Remoto al Switch.

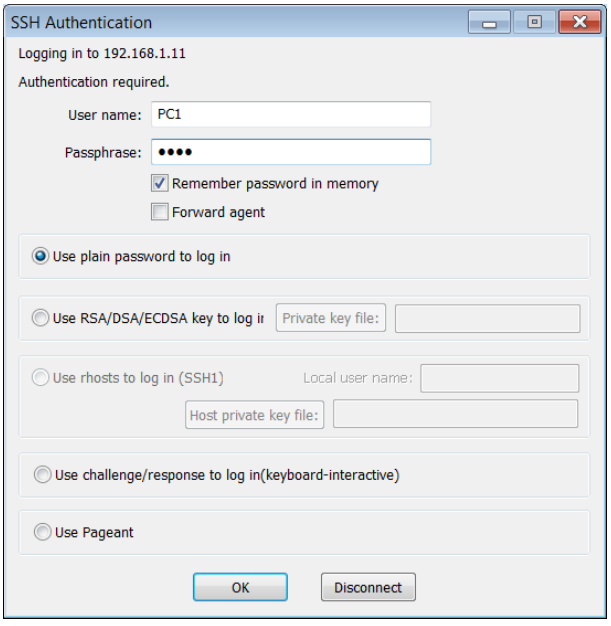


Figura 4.28. Autenticación SSH 3Com 5500 Práctica #11

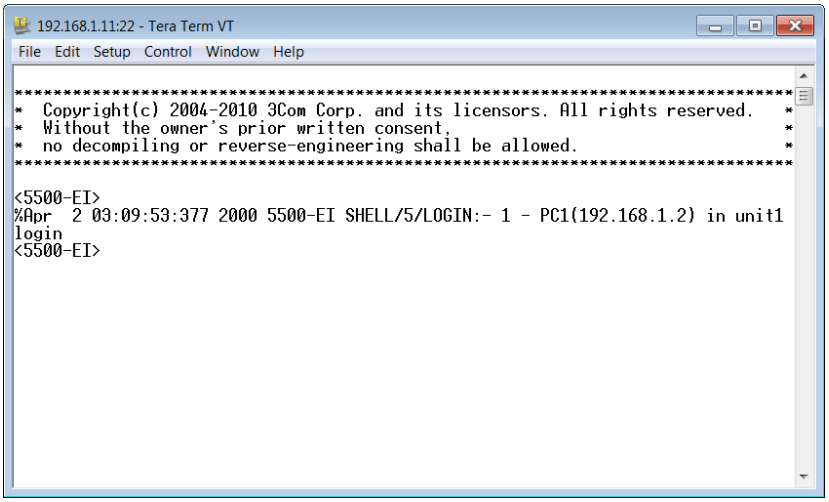


Figura 4.29. Conexión SSH 3Com 5500 Práctica #11

4.13. DESARROLLO PRÁCTICA#12 SIMULACIÓN DE UNA RED JERÁRQUICA QUE PERMITA LA ADMINISTRACIÓN CON SNMP (SIMPLE NETWORK MANAGEMENT PROTOCOL)

4.13.1. Configuraciones/Direccionamiento

Direccionamiento:

DISPOSITIVO	Dirección IP	Máscara de Red	Interfaz
SWITCH 1			
VLAN 10 (MAESTROS)	**192.168.10.10**	**255.255.255.0**	**Ethernet 1-3**
VLAN 20 (ALUMNOS)	**192.168.20.10**	**255.255.255.0**	**Ethernet 4-6**
ENLACE TRONCAL	--	--	**Ethernet 10-11**
SWITCH 2			
VLAN 10 (MAESTROS)	**192.168.10.11**	**255.255.255.0**	**Ethernet 1-3**
VLAN 20	**192.168.20.11**	**255.255.255.0**	**Ethernet 4-6**

(ALUMNOS)			
ENLACE TRONCAL	--	--	**Ethernet 10**
SWITCH 3			
VLAN 10 (MAESTROS)	**192.168.30.10**	**255.255.255.0**	**Ethernet 1-3**
VLAN 20 (ALUMNOS)	**192.168.40.10**	**255.255.255.0**	**Ethernet 4-6**
ENLACE TRONCAL	--	--	**Ethernet 10**
SWITCH 4			
VLAN 10 (MAESTROS)	**192.168.30.11**	**255.255.255.0**	**Ethernet 1-3**
VLAN 20 (ALUMNOS)	**192.168.40.11**	**255.255.255.0**	**Ethernet 4-6**
ENLACE TRONCAL	--	--	**Ethernet 10-11**
SWITCH 5			
VLAN 10 (MAESTROS)	**192.168.10.1**	**255.255.255.0**	**Ethernet 1-3**
VLAN 20 (ALUMNOS)	**192.168.20.1**	**255.255.255.0**	**Ethernet 4-6**
VLAN 1	**192.168.50.1**	**255.255.255.0**	**Ethernet 7**
VLAN 30 (CORE)	**200.0.0.1**	**255.255.255.252**	**Ethernet 8**
ENLACE TRONCAL	--	--	**Ethernet 10-14**
SWITCH 6			
VLAN 10 (MAESTROS)	**192.168.30.1**	**255.255.255.0**	**Ethernet 1-3**
VLAN 20 (ALUMNOS)	**192.168.40.1**	**255.255.255.0**	**Ethernet 4-6**

VLAN 1	**192.168.70.1**	**255.255.255.0**	**Ethernet 7**
VLAN 30 (CORE)	**200.0.0.2**	**255.255.255.252**	**Ethernet 8**
ENLACE TRONCAL	**--**	**--**	**Ethernet 10-14**
ROUTER 1			
FAST ETHERNET 0/0	**192.168.50.2**	**255.255.255.0**	**Ethernet**
FAST ETHERNET 0/1	**192.168.60.1**	**255.255.255.0**	**Ethernet**
ROUTER 2			
FAST ETHERNET 0/0	**192.168.70.2**	**255.255.255.0**	**Ethernet**
FAST ETHERNET 0/.1	**192.168.80.1**	**255.255.255.0**	**Ethernet**
HOSTS			
PC1	**192.168.10.2**	**255.255.255.0**	**Ethernet**
PC2	**192.168.20.2**	**255.255.255.0**	**Ethernet**
PC3	**192.168.30.2**	**255.255.255.0**	**Ethernet**
PC4	**192.168.40.2**	**255.255.255.0**	**Ethernet**
PC5	**192.168.60.2**	**255.255.255.0**	**Ethernet**
PC6	**192.168.80.2**	**255.255.255.0**	**Ethernet**

Usuario y Password:

Password: espe

4.13.2. Procedimiento

4.13.2.1. Topología Práctica 12 Simulador Packet tracer

La Figura 4.30. Nos muestra la Topología de Red en el Simulador Packet Tracer.

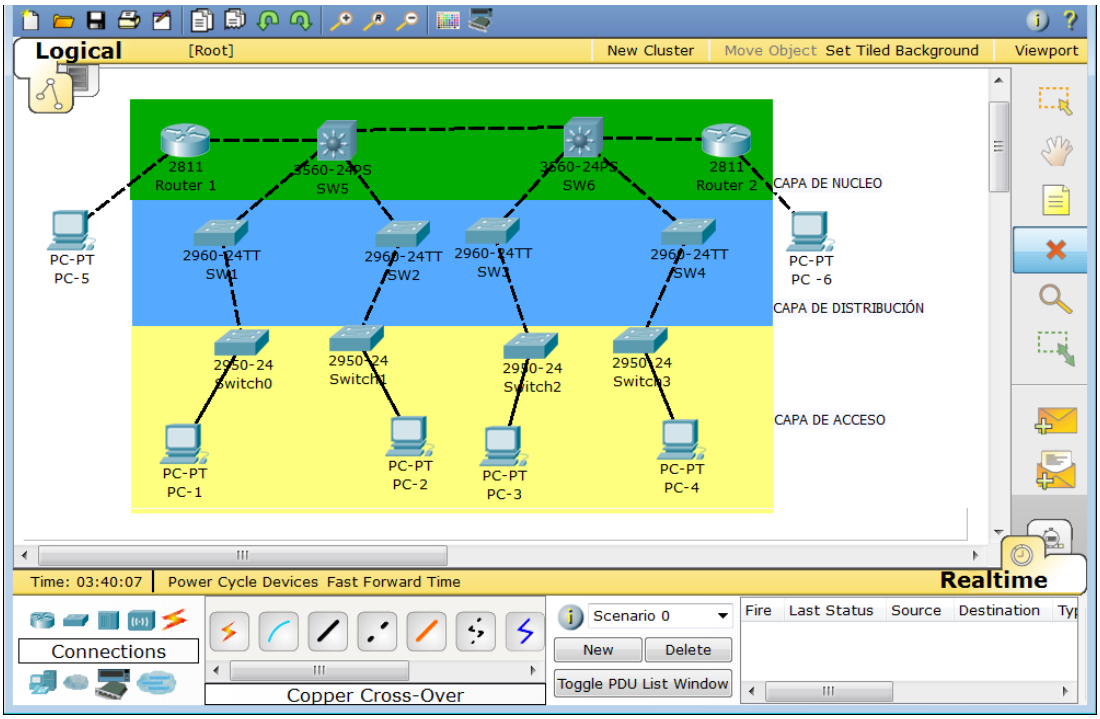


Figura 4.30. Simulación Topología de Red Práctica #12

4.13.2.2. Configuración SW1 CISCO 2960

1.- Accedemos al Switch y creamos la Vlan “MAESTROS” y “ALUMNOS”.

```
SW1(config)#vlan 10
SW1(config-vlan)#name MAESTROS
SW1(config-vlan)#exit
SW1(config)#vlan 20
SW1(config-vlan)#name ALUMNOS
```

2.- Añadimos los puertos a la VLANs.

```
SW1(config)#interface range f0/1-3
SW1(config-if-range)#switchport mode access
SW1(config-if-range)#switchport access vlan 10
SW1(config-if-range)#exit
SW1(config)#interface range f0/4-6
SW1(config-if-range)#switchport mode access
SW1(config-if-range)#switchport access vlan 20
```

3.- Añadimos una dirección IP a las Vlans creadas.

```
SW1(config)#interface vlan 10
SW1(config-if)#ip add 192.168.10.10 255.255.255.0
SW1(config-if)#exit
SW1(config)#interface vlan 20
SW1(config-if)#ip add 192.168.20.10 255.255.255.0
```

4.- Configuración de Enlace Troncales.

```
SW1(config)#interface rang f0/10-11
SW1(config-if-range)#switchport mode trunk
SW1(config-if-range)#switchport trunk allowed vlan all
```

5.- Habilitamos SNMP, comunidad “espe” para que nos permita leer y escribir los parámetros usamos el comando *rw*.

```
SW1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SW1(config)#snmp-server community espe rw
```

4.13.2.3. Configuración SW2 CISCO 2960

1.- Accedemos al Switch y creamos la Vlan “MAESTROS” y “ALUMNOS”.

```
SW2(config)#vlan 10
SW2(config-vlan)#name MAESTROS
SW2(config-vlan)#exit
SW2(config)#vlan 20
SW2(config-vlan)#name ALUMNOS
```

2.- Añadimos los puertos a la VLANs.

```
SW2(config)#interface range f0/1-3
SW2(config-if-range)#switchport mode access
SW2(config-if-range)#switchport access vlan 10
SW2(config-if-range)#exit
SW2(config)#interface range f0/4-6
SW2(config-if-range)#switchport mode access
SW2(config-if-range)#switchport access vlan 20
```

3.- Añadimos una dirección IP a las Vlans creadas.

```
SW2(config)#interface vlan 10
SW2(config-if)#ip add 192.168.10.11 255.255.255.0
SW2(config-if)#exit
SW2(config)#interface vlan 20
SW2(config-if)#ip add 192.168.20.11 255.255.255.0
```

4.- Configuración de Enlace Troncales.

```
SW2(config)#interface f0/10
SW2(config-if)#switchport mode trunk
SW2(config-if)#switchport trunk allowed vlan all
```

5.- Habilitamos SNMP, comunidad “espe” para que nos permita leer y escribir los parámetros usamos el comando *rw*.

```
SW2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SW2(config)#snmp-server community espe rw
```

4.13.2.4. Configuración SW3 CISCO 2960

1.- Accedemos al Switch y creamos la Vlan “MAESTROS” y “ALUMNOS”.

```
SW3(config)#vlan 10
SW3(config-vlan)#name MAESTROS
SW3(config-vlan)#exit
SW3(config)#vlan 20
SW3(config-vlan)#name ALUMNOS
```

2.- Añadimos los puertos a la VLANs.

```
SW3(config)#interface range f0/1-3
SW3(config-if-range)#switchport mode access
SW3(config-if-range)#switchport access vlan 10
SW3(config-if-range)#exit
SW3(config)#interface range f0/4-6
SW3(config-if-range)#switchport mode access
SW3(config-if-range)#switchport access vlan 20
```

3.- Añadimos una dirección IP a las Vlans creadas.

```
SW3(config)#interface vlan 10
SW3(config-if)#ip add 192.168.30.10 255.255.255.0
SW3(config-if)#exit
SW3(config)#interface vlan 20
SW3(config-if)#ip add 192.168.40.10 255.255.255.0
```

4.- Configuración de Enlace Troncales.

```
SW3(config)#interface f0/10
SW3(config-if)#switchport mode trunk
SW3(config-if)#switchport trunk allowed vlan all
```

5.- Habilitamos SNMP, comunidad “espe” para que nos permita leer y escribir los parámetros usamos el comando *rw*.

```
SW3#configure terminal
Enter configuration commands, one per line.
SW3(config)#snmp-server community espe rw
```

4.13.2.5. Configuración SW4 CISCO 2960

1.- Accedemos al Switch y creamos la Vlan “MAESTROS” y “ALUMNOS”.

```
SW4(config)#vlan 10
SW4(config-vlan)#name MAESTROS
SW4(config-vlan)#exit
SW4(config)#vlan 20
SW4(config-vlan)#name ALUMNOS
```

2.- Añadimos los puertos a la VLANs.

```
SW4(config)#interface range f0/1-3
SW4(config-if-range)#switchport mode access
SW4(config-if-range)#switchport access vlan 10
SW4(config-if-range)#exit
SW4(config)#interface range f0/4-6
SW4(config-if-range)#switchport mode access
SW4(config-if-range)#switchport access vlan 20
```

3.- Añadimos una dirección IP a las Vlans creadas.

```
SW4(config)#interface vlan 10
SW4(config-if)#ip add 192.168.30.11 255.255.255.0
SW4(config-if)#exit
SW4(config)#interface vlan 20
SW4(config-if)#ip add 192.168.40.11 255.255.255.0
```

4.- Configuración de Enlace Troncales.

```
SW4(config)#interface range f0/10-11
SW4(config-if-range)#switchport  mode trunk
SW4(config-if-range)#switchport trunk allowed vlan all
```

5.- Habilitamos SNMP, comunidad “espe” para que nos permita leer y escribir los parámetros usamos el comando *rw*.

```
SW4#configure terminal
Enter configuration commands, one per line.
SW4(config)#snmp-server community espe rw
```

4.13.2.6. Configuración SW5 CISCO 3560

1.- Accedemos al Switch y creamos la Vlan “MAESTROS”, “ALUMNOS” y “CORE”.

```
SW5(config)#vlan 10
SW5(config-vlan)#name MAESTROS
SW5(config-vlan)#exit
SW5(config)#vlan 20
SW5(config-vlan)#name ALUMNOS
SW5(config-vlan)#exit
SW5(config)#vlan 30
SW5(config-vlan)#name CORE
```

2.- Añadimos una dirección IP a las Vlans creadas y la VLAN1.

```
SW5(config)#interface vlan 10
SW5(config-if)#ip add 192.168.10.1 255.255.255.0
SW5(config-if)#exit
SW5(config)#interface vlan 20
SW5(config-if)#ip add 192.168.20.1 255.255.255.0
SW5(config-if)#exit
SW5(config)#interface vlan 30
SW5(config-if)#ip add 200.0.0.1 255.255.255.252
SW5(config-if)#exit
SW5(config)#interface vlan 1
SW5(config-if)#ip add 192.168.50.1 255.255.255.0
```

3.- Configuración el protocolo de enrutamiento en este caso RIPv2.

```
SW5(config)#ip routing
SW5(config)#router rip
SW5(config-router)#version 2
SW5(config-router)#network 192.168.10.0
SW5(config-router)#network 192.168.20.0
SW5(config-router)#network 192.168.50.0
SW5(config-router)#network 200.0.0.0
```

4.- Configuración de Enlace Troncales.

```
SW5(config)#interface range f0/10-14
SW5(config-if-range)#switchport mode trunk
SW5(config-if-range)#switchport trunk encapsulation dot1q
SW5(config-if-range)#switchport trunk allowed vlan all
```

5.- Añadimos el puerto a la VLAN “CORE”.

```
SW5(config)#interface f0/8
SW5(config-if)#switchport mode access
SW5(config-if)#switchport access vlan 30
```

6.- Habilitamos SNMP, comunidad "espe" para que nos permita leer y escribir los parámetros usamos el comando *rw*.

```
SW5#configure terminal
Enter configuration commands, one per line.
SW5(config)#snmp-server community espe rw
```

4.13.2.7. Configuración SW6 CISCO 3560

1.- Accedemos al Switch y creamos la Vlan "MAESTROS" , "ALUMNOS" y "CORE".

```
SW6(config)#vlan 10
SW6(config-vlan)#name MAESTROS
SW6(config-vlan)#exit
SW6(config)#vlan 20
SW6(config-vlan)#name ALUMNOS
SW6(config-vlan)#exit
SW6(config)#vlan 30
SW6(config-vlan)#name CORE
```

2.- Añadimos una dirección IP a las Vlans creadas y la VLAN1.

```
SW6(config)#interface vlan 10
SW6(config-if)#ip add 192.168.30.1 255.255.255.0
SW6(config-if)#exit
SW6(config)#interface vlan 20
SW6(config-if)#ip add 192.168.40.1 255.255.255.0
SW6(config-if)#exit
SW6(config)#interface vlan 30
SW6(config-if)#ip add 200.0.0.2 255.255.255.252
SW6(config-if)#exit
SW6(config)#interface vlan 1
SW6(config-if)#ip add 192.168.70.1 255.255.255.0
```

3.- Configuración el protocolo de enrutamiento en este caso RIPv2.

```
SW6(config)#ip routing
SW6(config)#router rip
SW6(config-router)#version 2
SW6(config-router)#network 192.168.30.0
SW6(config-router)#network 192.168.40.0
SW6(config-router)#network 192.168.70.0
SW6(config-router)#network 200.0.0.0
```

4.- Configuración de Enlace Troncales.

```
SW6(config)#interface range f0/10-14
SW6(config-if-range)#switchport mode trunk
SW6(config-if-range)#switchport trunk encapsulation dot1q
SW6(config-if-range)#switchport trunk allowed vlan all
```

5.- Añadimos el puerto a la VLAN “CORE”.

```
SW6(config)#interface f0/8
SW6(config-if)#switchport mode access
SW6(config-if)#switchport access vlan 30
```

6.- Habilitamos SNMP, comunidad “espe” para que nos permita leer y escribir los parámetros usamos el comando *rw*.

```
SW6#configure terminal
Enter configuration commands, one per line.
SW6(config)#snmp-server community espe rw
```

4.13.2.8. Configuración ROUTER 1 CISCO 2811

1.- Accedemos al Router configuramos las interfaces Fast Ethernet.

```
ROUTER1(config)#interface f0/0
ROUTER1(config-if)#ip add 192.168.50.2 255.255.255.0
ROUTER1(config-if)#no shutdown
ROUTER1(config-if)#exit
ROUTER1(config)#interface f0/1
ROUTER1(config-if)#ip add 192.168.60.1 255.255.255.0
ROUTER1(config-if)#no shutdown
```

2.- Configuramos el protocolo de Enrutamiento en este caso RIPv2.

```
ROUTER1(config)#router rip
ROUTER1(config-router)#version 2
ROUTER1(config-router)#network 192.168.50.0
ROUTER1(config-router)#network 192.168.60.0
```

4.13.2.9. Configuración ROUTER 2 CISCO 2811

1.- Accedemos al Router configuramos las interfaces Fast Ethernet.

```
ROUTER2(config)#interface f0/0
ROUTER2(config-if)#ip add 192.168.70.2 255.255.255.0
ROUTER2(config-if)#no shutdown
ROUTER2(config-if)#exit
ROUTER2(config)#interface f0/1
ROUTER2(config-if)#ip add 192.168.80.1 255.255.255.0
ROUTER2(config-if)#no shutdown
```

2.- Configuramos el protocolo de Enrutamiento en este caso RIPv2.

```
ROUTER2(config)#router rip
ROUTER2(config-router)#version 2
ROUTER2(config-router)#network 192.168.70.0
ROUTER2(config-router)#network 192.168.80.0
```

4.13.2.10. Prueba Acceso SNMP

PRUEBA ACCESO SNMP DESDE PC1 A SW1

1.- Ingresamos desde la PC1 al MIB BROWSER y ponemos la dirección IP de SW3 y la comunidad “espe” en la opción avanzado. La Figura 4.31. Nos muestra la pantalla de inicio para Autenticación SNMP.

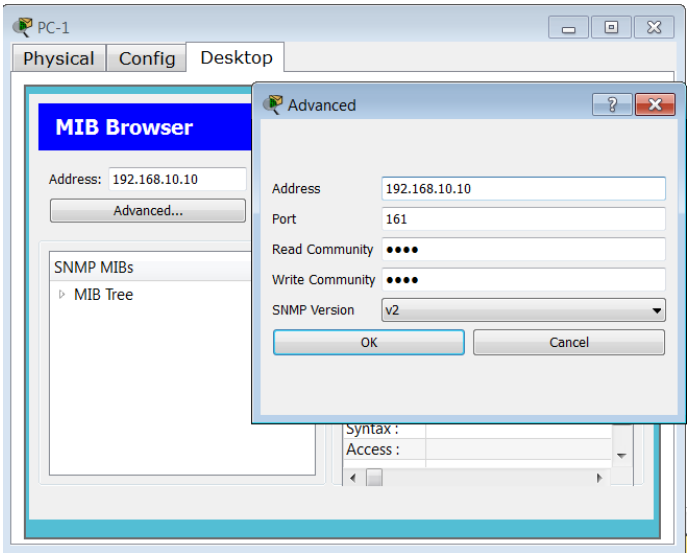


Figura 4.31. Autenticación SNMP SW1 Práctica #12

2.- Deplegamos el MIB Tree hasta “.sysName” y en la operación “get” ponemos “GO”. La Figura 4.32. Nos muestra la pantalla para el Acceso a las MIBs.

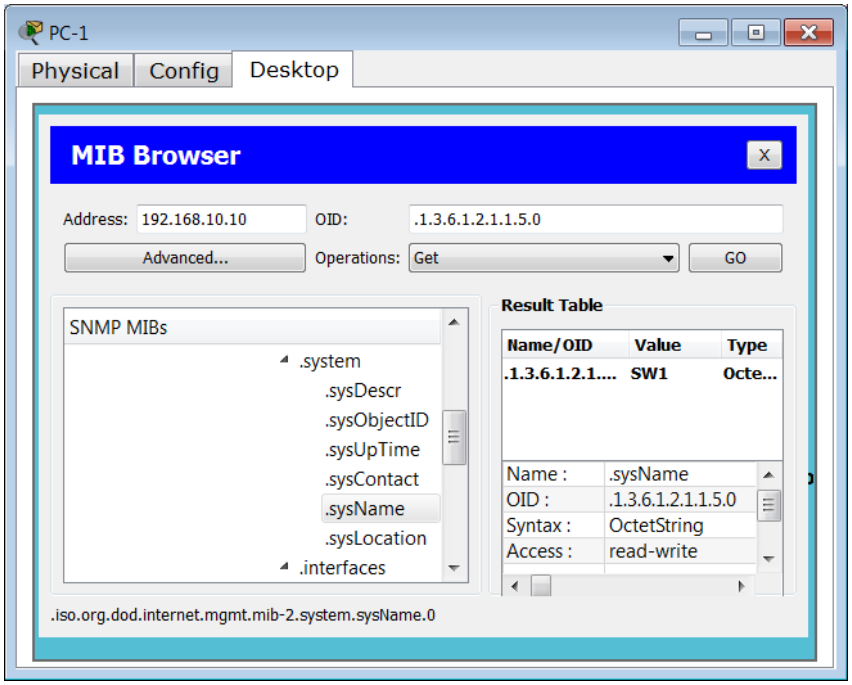


Figura 4.32. Acceso MIB SW1 Práctica #12

PRUEBA ACCESO SNMP DESDE PC6 A SW5

1.- Ingresamos desde la PC1 al MIB BROWSER y ponemos la dirección IP de SW5 y la comunidad “espe” en la opción avanzado. La Figura 4.33. Nos muestra la pantalla de inicio para Autenticación SNMP.

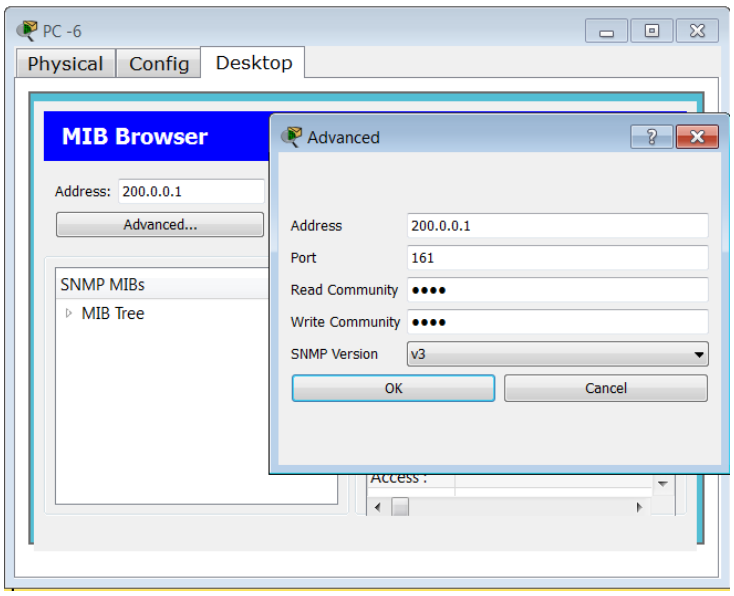


Figura 4.33. Autenticación SNMP SW5 Práctica #12

2.- Deplegamos el MIB Tree hasta ".sysContact" y en la operación "get" ponemos "GO". La Figura 4.34. Nos muestra la pantalla para el Acceso a las MIBs.

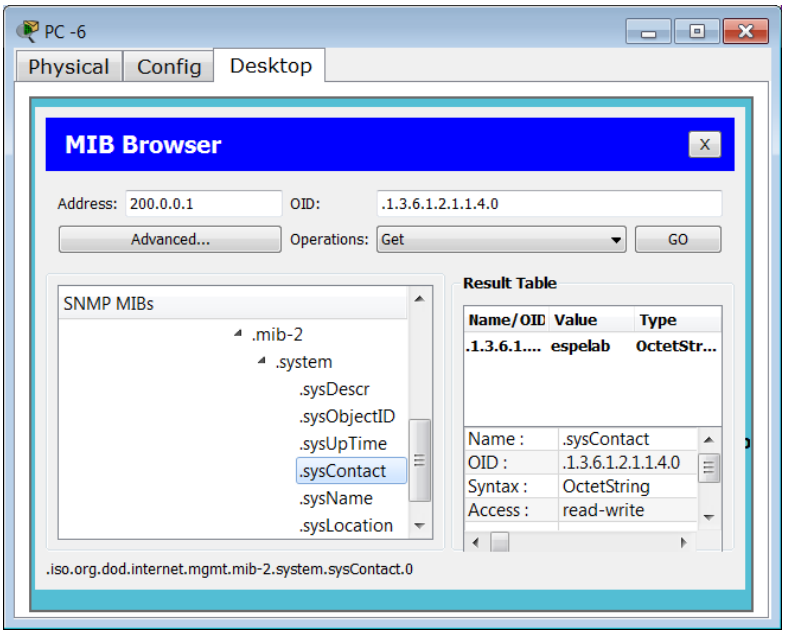


Figura 4.34. Acceso MIB SW5 Práctica #12

4.14. DESARROLLO PRÁCTICA #13 CONFIGURACIÓN IPv6 EN UN SWITCH CAPA 3

4.14.1. Configuraciones/Direccionamiento

Direccionamiento:

DISPOSITIVO	Dirección IPv6	Interfaz
Switch	**2800:270:0:1::12**	**Vlan 1**
PC1	**2800:270:0:1::10**	**Ethernet**
PC2	**2800:270:0:1::20**	**Ethernet**

PC3	**2800:270:0:1::30**	**Ethernet**
PC4	**2800:270:0:1::40**	**Ethernet**

Usuario y Password:

Usuario: admin

Password: espe

4.14.2. Procedimiento

4.14.2.1. Configuración IPv6 3COM 5500

La configuración de IPv6 está habilitada por defecto por lo cual solo veremos las pruebas de conectividad entre las PCs.

4.14.2.2. Configuración IPv6 CISCO 3560

1.- Accedemos al Switch y activamos IPv6 con el siguiente comando *sdm prefer dual-ipv4-and-ipv6 default* y reiniciamos el equipo con el comando *reload.*

```
SW2(config)#sdm prefer dual-ipv4-and-ipv6 default
Changes to the running SDM preferences have been stored, but cannot take effect
until the next reload.
Use 'show sdm prefer' to see what SDM preference is currently active.
```

2.- Configuramos una dirección IPv6 a la VLAN 1.

```
SW2(config)#interface vlan 1
SW2(config-if)#ipv6 address 2800:270:0:1::12/64
```

4.14.2.3. Configuración IPv6 D-Link DGS-3627

Accedemos al Switch y configuramos una dirección IPv6 al sistema recordemos que IPv6 está habilitado por defecto y verificamos el cambio realizado.

```
DGS-3627:5#config ipif System ipv6  ipv6address  2800:270:0:1::12/64
Command: config ipif System ipv6 ipv6address 2800:270::1:0:0:0:12/64

Success.

DGS-3627:5#show ipif
Command: show ipif

IP Interface                 : System
VLAN Name                    : default
Interface Admin state        : Enabled
IPv4 Address                 : 10.90.90.90/8 (Manual)  Primary
Proxy ARP                    : Disabled   (Local : Disabled)
IPv6 Link-Local Address      : FE80::219:5BFF:FEF0:7D80/128
IPv6 Global Unicast Address  : 2800:270::1:0:0:0:12/64
IP MTU                       : 1500
```

4.14.2.4. Configuración PC1, PC2, PC3, PC4

La Figura 4.35. Nos indica la configuración de IPv6 en la PC1

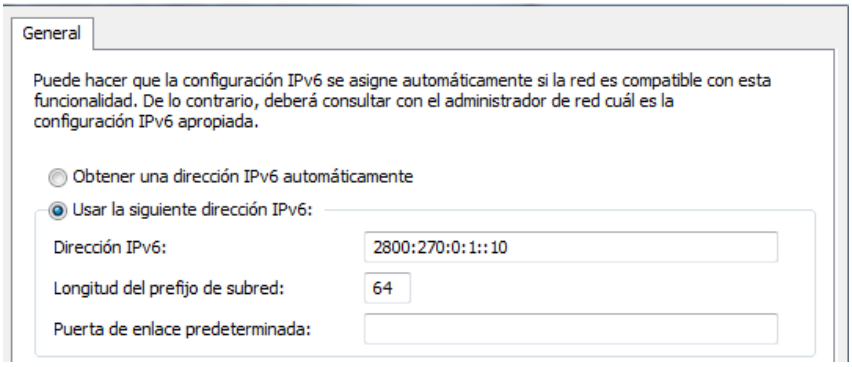


Figura 4.35. Configuración IPv6 PC 1 Práctica #13

La Figura 4.36. Nos indica la configuración de IPv6 en la PC2

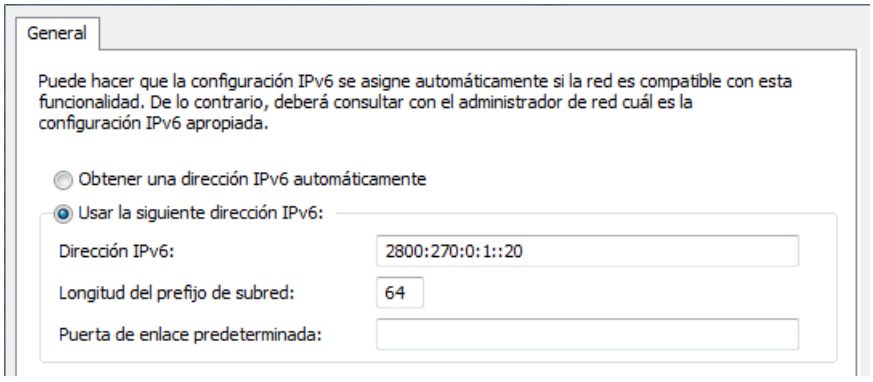


Figura 4.36. Configuración IPv6 PC 2 Práctica #13

La Figura 4.37. Nos indica la configuración de IPv6 en la PC3

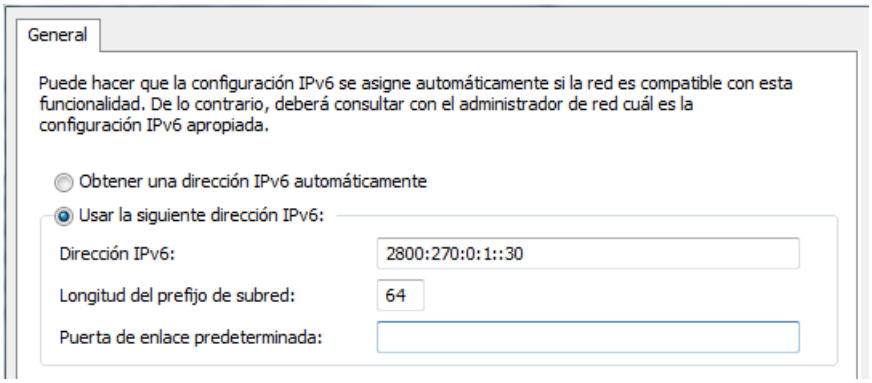


Figura 4.37. Configuración IPv6 PC 3 Práctica #13

La Figura 4.38. Nos indica la configuración de IPv6 en la PC4

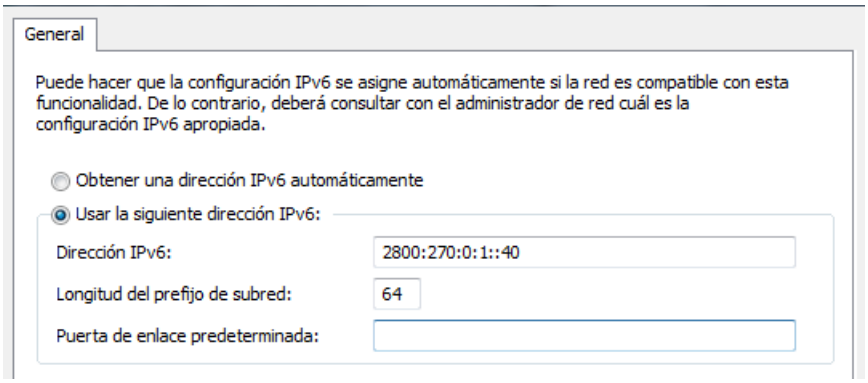


Figura 4.38. Configuración IPv6 PC 4 Práctica #13

4.14.2.5. Pruebas de Conectividad Red Local IPv6

Estas pruebas representan a las configuraciones de los 3 Equipos mencionados por lo que se detallará la conectividad con uno de los dispositivos en este caso el Switch D-Link 3627

CONECTIVIDAD PC1 CON PC2

```
C:\Users\REDES-PC>ping 2800:270:0:1::20

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

Estadísticas de ping para 2800:270:0:1::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 PC3 CON PC1

```
C:\Users\redes pc>ping 2800:270:0:1::10

Haciendo ping a 2800:270:0:1::10 con 32 bytes de datos:
Respuesta desde 2800:270:0:1::10: tiempo<1m
Respuesta desde 2800:270:0:1::10: tiempo<1m
Respuesta desde 2800:270:0:1::10: tiempo<1m
Respuesta desde 2800:270:0:1::10: tiempo<1m

Estadísticas de ping para 2800:270:0:1::10:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

CONECTIVIDAD PC2 CON PC3

```
C:\Users\redes pc>ping 2800:270:0:1::30

Haciendo ping a 2800:270:0:1::30 con 32 bytes de datos:
Respuesta desde 2800:270:0:1::30: tiempo<1m
Respuesta desde 2800:270:0:1::30: tiempo<1m
Respuesta desde 2800:270:0:1::30: tiempo<1m
Respuesta desde 2800:270:0:1::30: tiempo<1m

Estadísticas de ping para 2800:270:0:1::30:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

CONECTIVIDAD PC2 CON PC4

```
C:\Users\redes pc>ping 2800:270:0:1::40

Haciendo ping a 2800:270:0:1::40 con 32 bytes de datos:
Respuesta desde 2800:270:0:1::40: tiempo<1m
Respuesta desde 2800:270:0:1::40: tiempo<1m
Respuesta desde 2800:270:0:1::40: tiempo<1m
Respuesta desde 2800:270:0:1::40: tiempo<1m

Estadísticas de ping para 2800:270:0:1::40:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

CONECTIVIDAD PC1 CON SWITCH D-LINK 3627

```
C:\Users\REDES-PC>ping 2800:270:0:1::12

Haciendo ping a 2800:270:0:1::12 con 32 bytes de datos:
Respuesta desde 2800:270:0:1::12: tiempo=1ms
Respuesta desde 2800:270:0:1::12: tiempo<1m
Respuesta desde 2800:270:0:1::12: tiempo<1m
Respuesta desde 2800:270:0:1::12: tiempo<1m

Estadísticas de ping para 2800:270:0:1::12:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 1ms, Media = 0ms
```

CONECTIVIDAD PC2 CON SWITCH D-LINK 3627

```
C:\Users\redes pc>ping 2800:270:0:1::12

Haciendo ping a 2800:270:0:1::12 con 32 bytes de datos:
Respuesta desde 2800:270:0:1::12: tiempo=1ms
Respuesta desde 2800:270:0:1::12: tiempo<1m
Respuesta desde 2800:270:0:1::12: tiempo<1m
Respuesta desde 2800:270:0:1::12: tiempo<1m

Estadísticas de ping para 2800:270:0:1::12:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 1ms, Media = 0ms
```

4.15. DESARROLLO PRÁCTICA #14 ENRUTAMIENTO DINAMICO (RIPng) IPv6 EN UN ENTORNO LAN CON SWITCH CAPA 3

4.15.1. Configuraciones/Direccionamiento

Direccionamiento:

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**

Usuario y Password:

Usuario: admin

Password: espe

4.15.2. Procedimiento

4.15.2.1. Configuración IPv6 D-Link DGS-3627 SW1

1.- Accedemos al Switch 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.
```

2.- 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.
```

3.- 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.
```

4.-Creamos las interfaces vía configuración web. La Figura 4.39. Nos muestra la Configuración de la interface RED1. Mientras que la Figura 4.40. Nos muestra la Configuración de la interface RED 2.

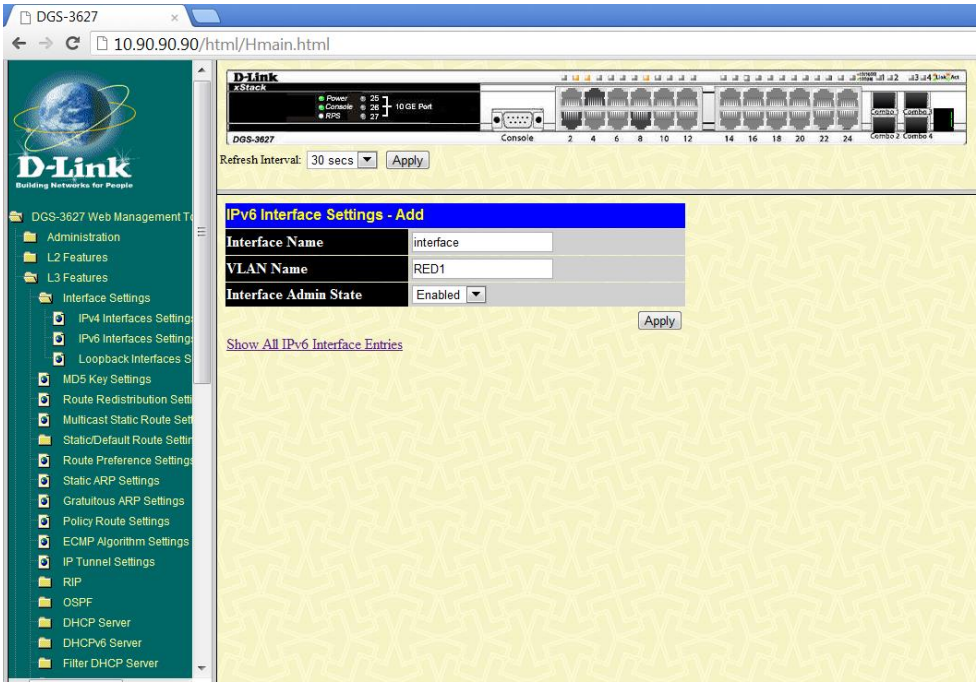


Figura 4.39. Configuración Interface RED 1 Switch D-Link SW1 Práctica #14

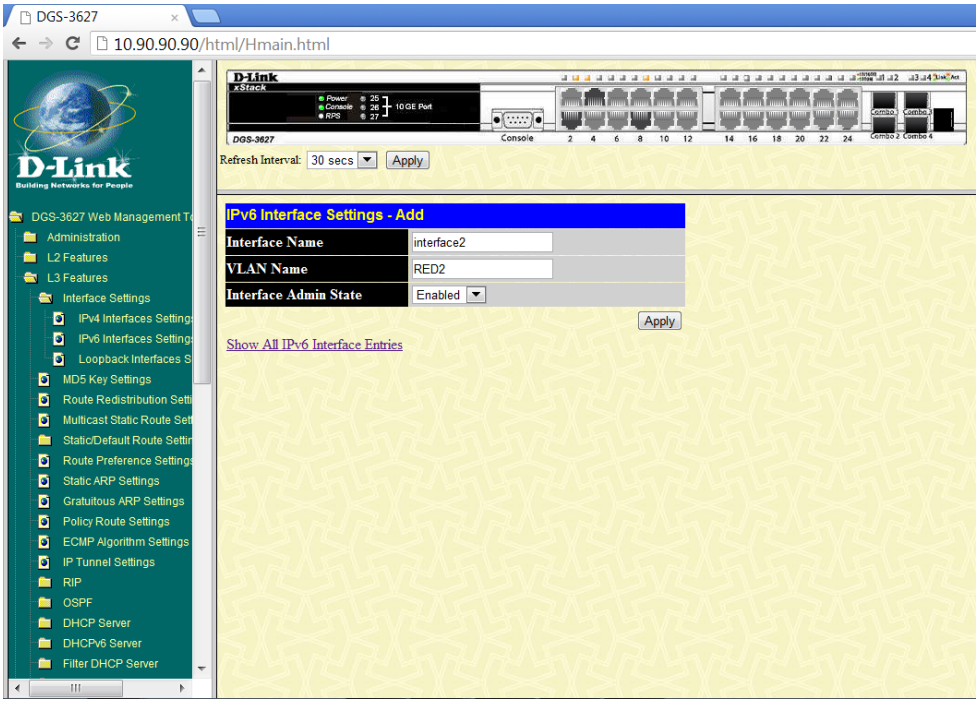


Figura 4.40. Configuración Interface RED 2 Switch D-Link SW1 Práctica #14

5.- 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.
```

6.- Habilitamos el protocolo de enrutamiento RIPng a todas las.

```
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.
```

4.15.2.2. Configuración IPv6 D-Link DGS-3627 SW2

1.- Accedemos al Switch y creamos la Vlan "RED1".

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

Success.
```

2.- Añadimos puertos a la VLAN.

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

Success.
```

3.- Configuración de Enlace Troncales.

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

Success.
```

4.-Creamos la interface vía configuración web. . La Figura 4.41. Nos muestra la Configuración de la interface RED1.

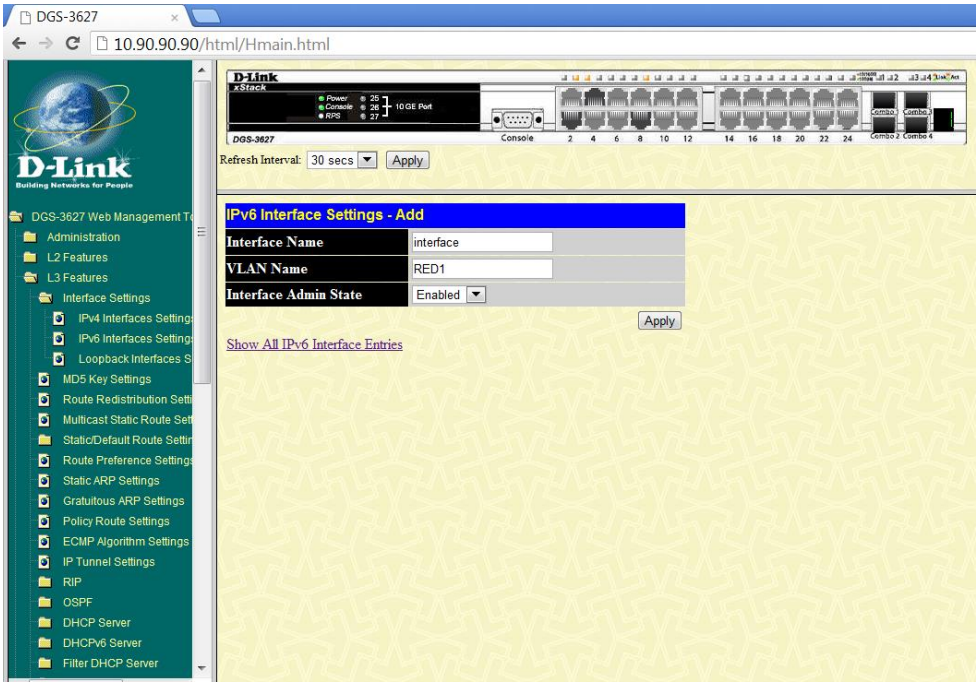


Figura 4.41. Configuración Interface RED 1 Switch D-Link SW2 Práctica #14

5.- Configuramos la IP de la VLAN "RED1" y la VLAN 1.

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

Success.
```

```
DGS-3627:admin#config ipif System  ipv6 ipv6address 2001:450:2002:e8::2/64
Command: config ipif System ipv6 ipv6address 2001:450:2002:E8::2/64

Success.
```

6.- Habilitamos el protocolo de enrutamiento RIPng a todas las.

```
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.
```

4.15.2.3. Configuración PC1, PC2, PC3, PC4, PC5, PC6

La Figura 4.42. Nos indica la configuración de IPv6 en la PC1

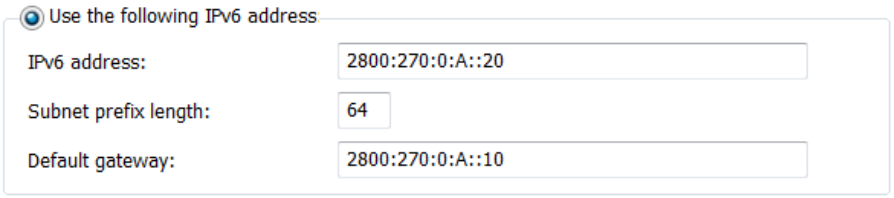


Figura 4.42. Configuración IPv6 PC 1 Práctica #14

La Figura 4.43. Nos indica la configuración de IPv6 en la PC2

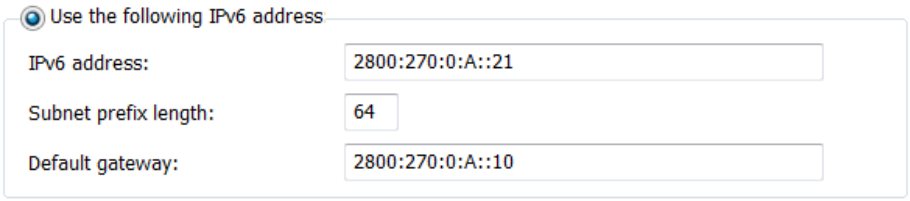


Figura 4.43. Configuración IPv6 PC 2 Práctica #14

La Figura 4.44. Nos indica la configuración de IPv6 en la PC3

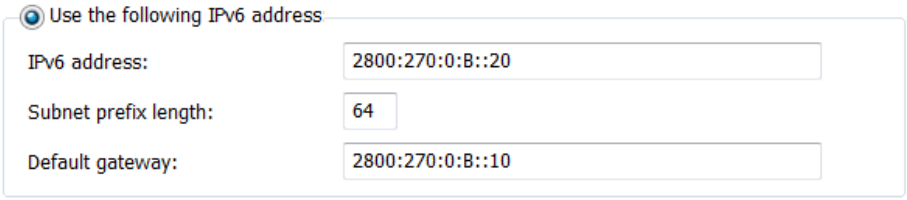


Figura 4.44. Configuración IPv6 PC 3 Práctica #14

La Figura 4.45. Nos indica la configuración de IPv6 en la PC4

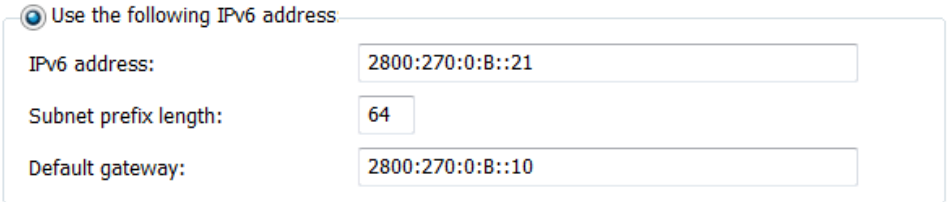


Figura 4.45. Configuración IPv6 PC 4 Práctica #14

La Figura 4.46. Nos indica la configuración de IPv6 en la PC5

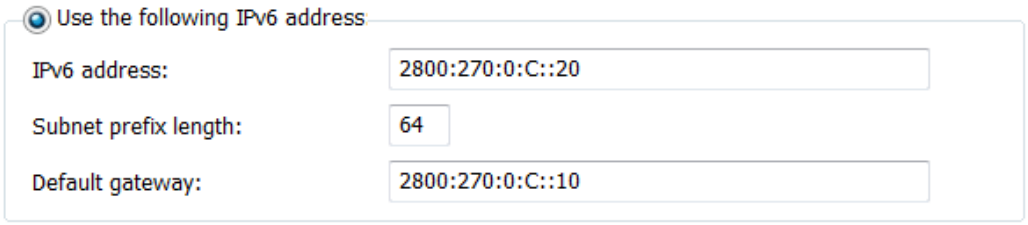


Figura 4.46. Configuración IPv6 PC 5 Práctica #14

La Figura 4.47. Nos indica la configuración de IPv6 en la PC6

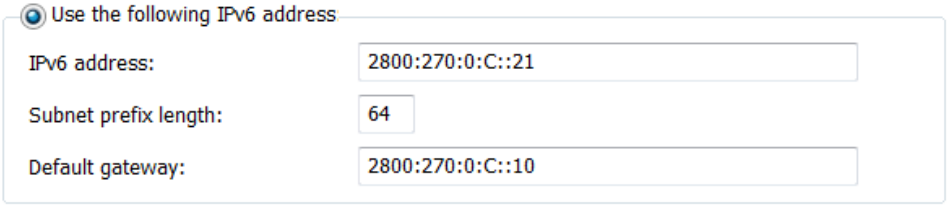


Figura 4.47. Configuración IPv6 PC 6 Práctica #14

4.15.2.4. Pruebas de Conectividad Red Local IPv6

CONECTIVIDAD PC1 CON PC5

```
C:\Users\redes pc>ping 2800:270:0:C::20

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

Estadísticas de ping para 2800:270:0:c::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 PC1 CON PC6

```
C:\Users\redes pc>ping 2800:270:0:C::21

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

Estadísticas de ping para 2800:270:0:c::21:
    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 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
```

4.16. DESARROLLO PRÁCTICA #15 CONFIGURACIÓN DE IPv6 TUNNELING EN UN ENTORNO LAN

4.16.1. Configuraciones/Direccionamiento

Direccionamiento:

DISPOSITIVO	Dirección IPv6 *Dirección IPv4*	Interfaz
Switch D-LINK SW1		
	2001:450:2002:E8::1 *200.0.0.1/30*	**Tunnel**
	2001:450:2002:E9::3	**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 *200.0.0.2/30*	**Tunnel**
	2001:450:2002:E9::4	**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**

Usuario y Password:

Usuario: admin

Password: espe

4.16.2. Procedimiento

4.16.2.1. Configuración IPv6 D-Link DGS-3627 SW1

1.- Accedemos al Switch 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.
```

2.- 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.
```

3.- 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.
```

4.-Creamos las interfaces vía configuración web. La Figura 4.48. Nos muestra la Configuración de la interface RED1. Mientras que la Figura 4.49. Nos muestra la Configuración de la interface RED 2.

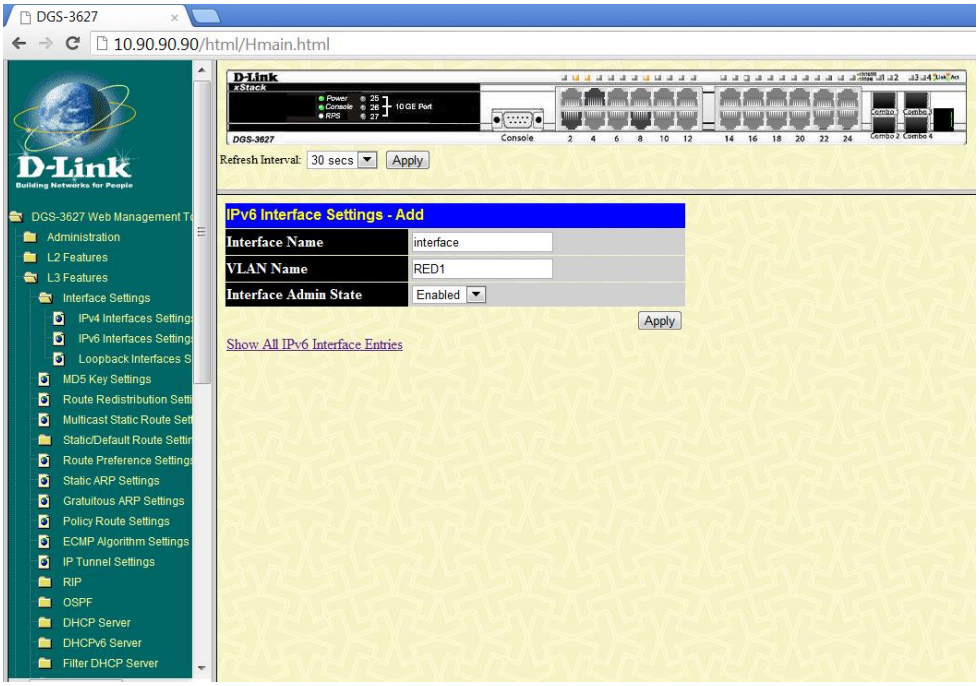


Figura 4.48. Configuración Interface RED 1 Switch D-Link SW1 Práctica #15

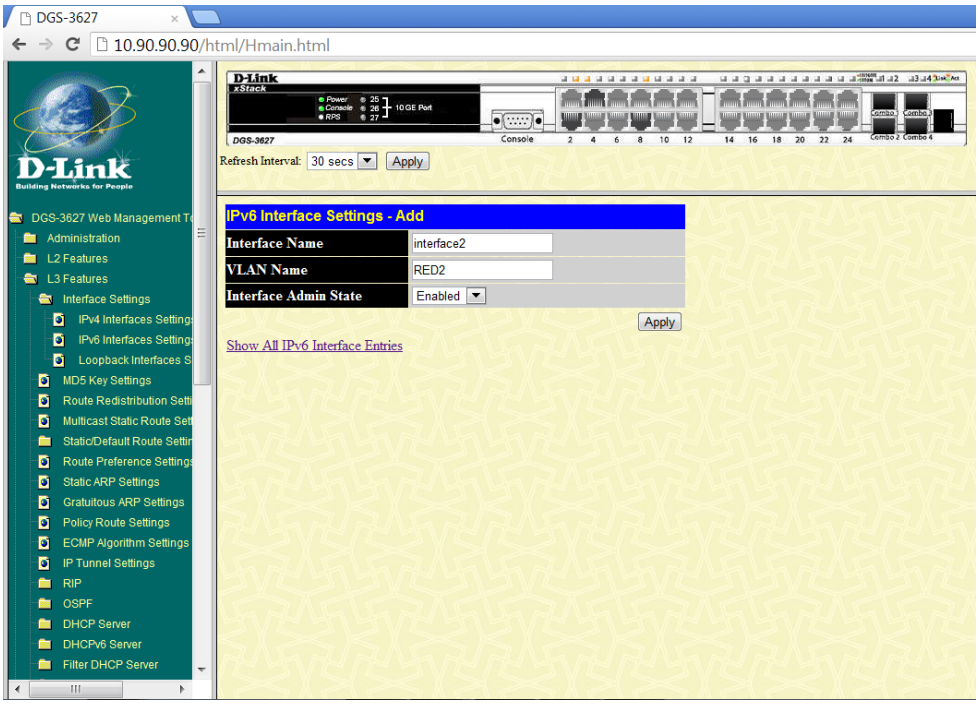


Figura 4.49. Configuración Interface RED 2 Switch D-Link SW2 Práctica #15

5.- Configuramos la IP de la VLAN “RED1”, “RED2”.

```
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.
```

6.- Configuramos la IP de la VLAN 1

```
DGS-3627:admin#config ipif System ipv6 ipv6address 2001:450:2002:e9::3/64
Command: config ipif System ipv6 ipv6address 2001:450:2002:E9::3/64

Success.
```

```
DGS-3627:admin#config ipif System ipaddress 200.0.0.1/30
Command: config ipif System ipaddress 200.0.0.1/30

Success.
```

7.- Creamos el tunnel y lo configuramos en forma manual.

```
DGS-3627:admin#create ip_tunnel tn
Command: create ip_tunnel tn

Success.

DGS-3627:admin#config ip_tunnel manual tn source 200.0.0.1 destination 200.0.0.2

Command: config ip_tunnel manual tn source 200.0.0.1 destination 200.0.0.2

Success.

DGS-3627:admin#config ip_tunnel manual tn ipv6address 2001:450:2002:e8::1/64
Command: config ip_tunnel manual tn ipv6address 2001:450:2002:E8::1/64

Success.
```

8.- Habilitamos el protocolo de enrutamiento RIPng a todas las.

```
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.
```

4.16.2.2. Configuración IPv6 D-Link DGS-3627 SW2

1.- Accedemos al Switch y creamos la Vlan “RED1”.

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

Success.
```

2.- Añadimos puertos a la VLAN.

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

Success.
```

3.- Configuración de Enlace Troncales.

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

Success.
```

4.-Creamos las interfaces vía configuración web. La Figura 4.50. Nos muestra la Configuración de la interface RED1.

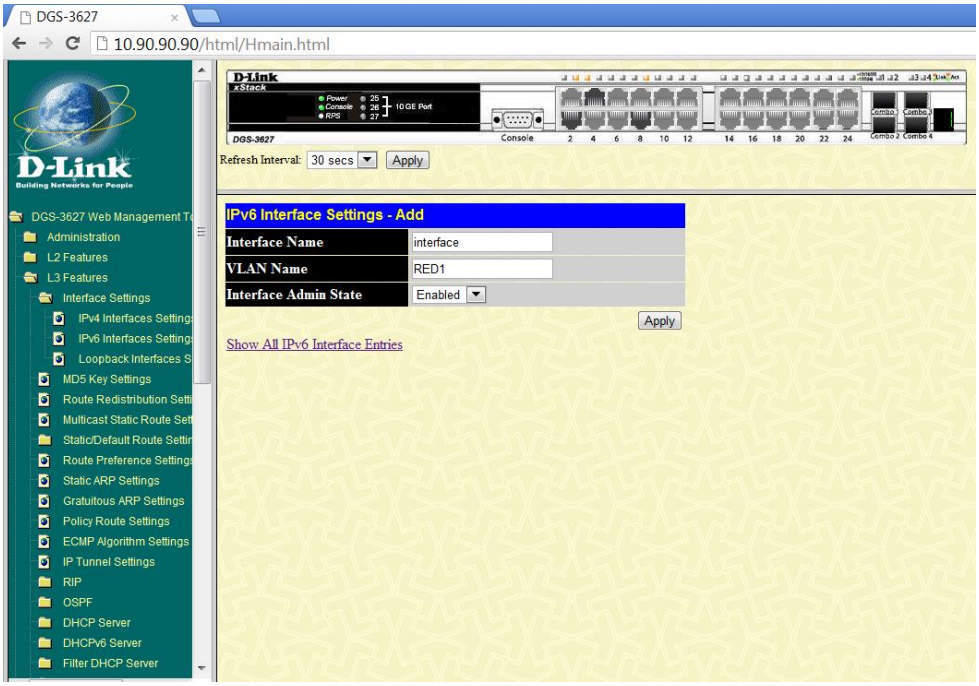


Figura 4.50. Configuración Interface RED 1 Switch D-Link SW2 Práctica #15

5.- Configuramos la IP de la VLAN “RED1” y la VLAN 1.

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

Success.
```

```
DGS-3627:admin#config ipif System ipv6 ipv6address 2001:450:2002:e9::4/64
Command: config ipif System ipv6 ipv6address 2001:450:2002:E9::4/64

Success.
```

```
DGS-3627:admin#config ipif System ipaddress 200.0.0.2/30
Command: config ipif System ipaddress 200.0.0.2/30

Success.
```

6.- Creamos el tunnel y lo configuramos en forma manual.

```
DGS-3627:admin#create ip_tunnel tn
Command: create ip_tunnel tn

Success.

DGS-3627:admin#config ip_tunnel manual tn source 200.0.0.2 destination 200.0.0.1

Command: config ip_tunnel manual tn source 200.0.0.2 destination 200.0.0.1

Success.

DGS-3627:admin#config ip_tunnel manual tn ipv6address 2001:450:2002:e8::2/64
Command: config ip_tunnel manual tn ipv6address 2001:450:2002:E8::2/64

Success.
```

7.- Habilitamos el protocolo de enrutamiento RIPng a todas las.

```
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.
```

4.16.2.3. Configuración PC1, PC2, PC3, PC4, PC5, PC6

La Figura 4.51. Nos indica la configuración de IPv6 en la PC1

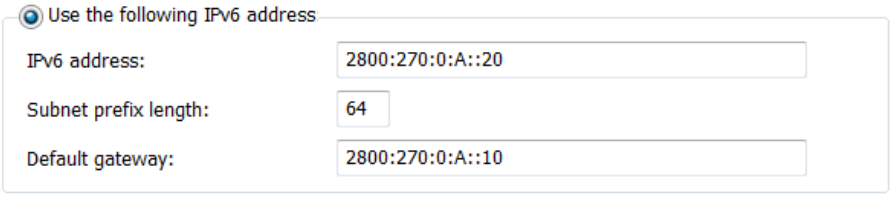


Figura 4.51. Configuración IPv6 PC 1 Práctica #15

La Figura 4.52. Nos indica la configuración de IPv6 en la PC2

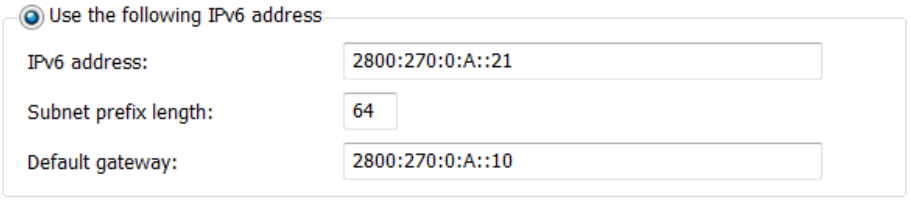


Figura 4.52. Configuración IPv6 PC 2 Práctica #15

La Figura 4.53. Nos indica la configuración de IPv6 en la PC3

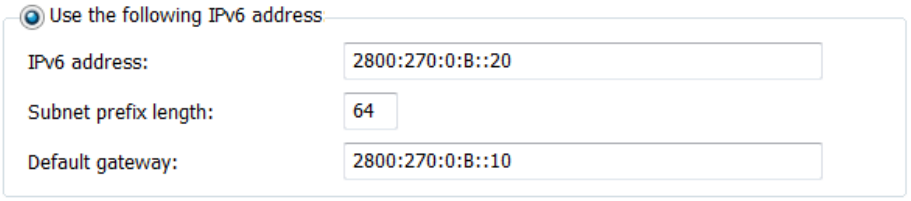


Figura 4.53. Configuración IPv6 PC 3 Práctica #15

La Figura 4.54. Nos indica la configuración de IPv6 en la PC4

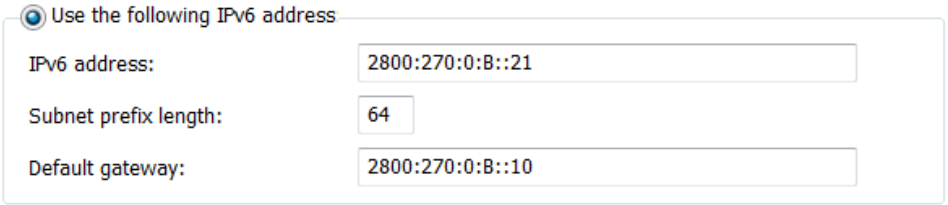


Figura 4.54. Configuración IPv6 PC 4 Práctica #15

La Figura 4.55. Nos indica la configuración de IPv6 en la PC5

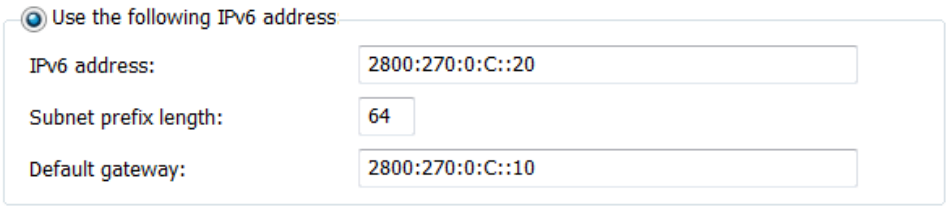


Figura 4.55. Configuración IPv6 PC 5 Práctica #15

La Figura 4.56. Nos indica la configuración de IPv6 en la PC6

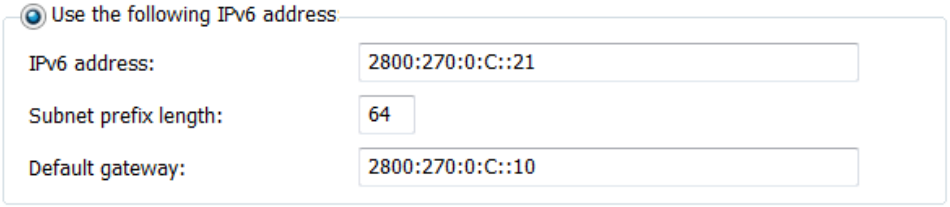


Figura 4.56. Configuración IPv6 PC 6 Práctica #15

4.16.2.4. Tablas de enrutamiento IPv4-IPv6

SW1:

```
DGS-3627:admin#show iproute
Command: show iproute

Routing Table

IP Address/Netmask  Gateway          Interface     Cost      Protocol
------------------  ---------------  ------------  --------  --------
200.0.0.0/30        0.0.0.0          System        1         Local

Total Entries : 1
```

```
DGS-3627:admin#show ipv6route
Command: show ipv6route

IPv6 Prefix: 2001:450:2002:E8::/64            Protocol: Local   Metric: 1
Next Hop   : ::                               IPIF    : tn

IPv6 Prefix: 2001:450:2002:E9::/64            Protocol: Local   Metric: 1
Next Hop   : ::                               IPIF    : System

IPv6 Prefix: 2800:270:0:A::/64                Protocol: Local   Metric: 1
Next Hop   : ::                               IPIF    : interface

IPv6 Prefix: 2800:270:0:B::/64                Protocol: Local   Metric: 1
Next Hop   : ::                               IPIF    : interface2

IPv6 Prefix: 2800:270:0:C::/64                Protocol: RIPng   Metric: 2
Next Hop   : FE80::219:5BFF:FEF0:7D81         IPIF    : interface


Total Entries: 5
```

SW2:

```
DGS-3627:admin#show iproute
Command: show iproute


Routing Table

IP Address/Netmask  Gateway          Interface     Cost      Protocol
------------------  ---------------  ------------  --------  --------
200.0.0.0/30        0.0.0.0          System        1         Local

Total Entries : 1
```

```
DGS-3627:admin#show ipv6route
Command: show ipv6route

IPv6 Prefix: 2001:450:2002:E8::/64            Protocol: Local   Metric: 1
Next Hop   : ::                               IPIF    : tn

IPv6 Prefix: 2001:450:2002:E9::/64            Protocol: Local   Metric: 1
Next Hop   : ::                               IPIF    : System

IPv6 Prefix: 2800:270:0:A::/64                Protocol: RIPng   Metric: 2
Next Hop   : FE80::219:5BFF:FEF0:7241         IPIF    : interface

IPv6 Prefix: 2800:270:0:B::/64                Protocol: RIPng   Metric: 2
Next Hop   : FE80::219:5BFF:FEF0:7241         IPIF    : interface

IPv6 Prefix: 2800:270:0:C::/64                Protocol: Local   Metric: 1
Next Hop   : ::                               IPIF    : interface


Total Entries: 5
```

4.16.2.5. Pruebas de conectividad Red Local IPv6

CONECTIVIDAD SW1 CON SW2 IPV4

```
DGS-3627:admin#traceroute 200.0.0.2
Command: traceroute 200.0.0.2

 <10 ms  200.0.0.2

Trace complete.
```

CONECTIVIDAD SW1 CON SW2 IPV6

```
DGS-3627:admin#traceroute6 2001:450:2002:e8::2
Command: traceroute6 2001:450:2002:E8::2

 <10 ms  2001:450:2002:E8::2

Trace complete.
```

CONECTIVIDAD SW2 CON SW1 IPV4

```
DGS-3627:admin#traceroute 200.0.0.1
Command: traceroute 200.0.0.1

 10  ms  200.0.0.1

Trace complete.
```

CONECTIVIDAD SW2 CON SW1 IPV6

```
DGS-3627:admin#traceroute6 2001:450:2002:e8::1
Command: traceroute6 2001:450:2002:E8::1

 <10 ms  2001:450:2002:E8::1

Trace complete.
```

CONECTIVIDAD PC1 CON PC5

```
C:\Users\redes pc>ping 2800:270:0:C::20

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

Estadísticas de ping para 2800:270:0:c::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 PC1 CON PC6

```
C:\Users\redes pc>ping 2800:270:0:C::21

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

Estadísticas de ping para 2800:270:0:c::21:
    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 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
```

4.17. DESARROLLO PRÁCTICA #16 CONFIGURACIÓN DEL SERVIDOR AAA PARA ACCESO TELNET EN UNA RED DE AREA LOCAL

4.17.1. Configuraciones/Direccionamiento

Direccionamiento:

DISPOSITIVO	Dirección IP	Máscara de Red	Interfaz

SWITCH 3COM			
VLAN 10 (MAESTROS)	**192.168.1.10**	**255.255.255.0**	**Ethernet 1-3**
VLAN 20 (ESTUDIANTES)	**192.168.2.10**	**255.255.255.0**	**Ethernet 4-6**
ENLACE TRONCAL	**--**	**--**	**Ethernet 11-12**
SWITCH 1-2 HP 2512			
VLAN 10 (MAESTROS)	**192.168.1.X**	**255.255.255.0**	**Ethernet 1-3**
VLAN 20 (ESTUDIANTES)	**192.168.2.X**	**255.255.255.0**	**Ethernet 4-6**
ENLACE TRONCAL	**--**	**--**	**Ethernet 11**
PC1 MAESTRO	**192.168.1.2**	**255.255.255.0**	**Ethernet**
PC4 ESTUDIANTE	**192.168.2.2**	**255.255.255.0**	**Ethernet**

Usuario y Password:

Usuario: telnet 1-2

Password: espe

4.17.2. Procedimiento

La configuración será la misma para los 2 Switch HP 2512 se detallará la configuración de un equipo y se repetirá el proceso para el otro.

4.17.2.1. Configuración HP 2512

1.- Accedemos al Switch y creamos la Vlan “MAESTROS” y “ESTUDIANTES”.

```
SWITCH1(config)# vlan 10
SWITCH1(vlan-10)# name MAESTROS
SWITCH1(vlan-10)# exit
SWITCH1(config)# vlan 20
SWITCH1(vlan-20)# name ESTUDIANTES
```

2.- Añadimos los puertos a las VLANs.

```
SWITCH1(config)# vlan 10
SWITCH1(vlan-10)# untagged ethernet 1
SWITCH1(vlan-10)# untagged ethernet 2
SWITCH1(vlan-10)# untagged ethernet 3
SWITCH1(vlan-10)# exit
SWITCH1(config)# vlan 20
SWITCH1(vlan-20)# untagged ethernet 4
SWITCH1(vlan-20)# untagged ethernet 5
SWITCH1(vlan-20)# untagged ethernet 6
```

3.- Configuración de Enlace Troncales.

```
SWITCH1# configure
SWITCH1(config)# trunk ethernet 11 trk1 trunk
```

```
SWITCH1(config)# vlan 10
SWITCH1(vlan-10)# tagged trk1
SWITCH1(vlan-10)# exit
SWITCH1(config)# vlan 20
SWITCH1(vlan-20)# tagged trk1
```

4.17.2.2. Configuración 3COM 4500

1.- Accedemos al Switch y creamos la Vlan “MAESTROS” y “ESTUDIANTES”.

```
[SWITCH3]vlan 10
[SWITCH3-vlan10]name MAESTROS
[SWITCH3-vlan10]quit
[SWITCH3]vlan 20
[SWITCH3-vlan20]name ESTUDIANTES
```

2.- Añadimos los puertos a las VLANs.

```
[SWITCH3]vlan 10
[SWITCH3-vlan10]port ethernet 1/0/1 to ethernet 1/0/3
[SWITCH3-vlan10]quit
[SWITCH3]vlan 20
[SWITCH3-vlan20]port ethernet 1/0/4 to ethernet 1/0/6
```

3.- Configuración de Enlace Troncales.

```
[SWITCH3]interface ethernet 1/0/11
[SWITCH3-Ethernet1/0/11]port link-type trunk
[SWITCH3-Ethernet1/0/11]port trunk permit vlan 10
 Please wait... Done.
[SWITCH3-Ethernet1/0/11]port trunk permit vlan 20
 Please wait... Done.
[SWITCH3-Ethernet1/0/11]quit
[SWITCH3]interface ethernet 1/0/12
[SWITCH3-Ethernet1/0/12]port link-type trunk
[SWITCH3-Ethernet1/0/12]port trunk permit vlan 10
 Please wait... Done.
[SWITCH3-Ethernet1/0/12]port trunk permit vlan 20
 Please wait... Done.
```

4.- Aplicamos la autenticación AAA a los usuarios TELNET.

```
[SWITCH3]user-interface vty 0 4
[SWITCH3-ui-vty0-4]authentication-mode scheme
```

5.- Creamos 2 usuarios locales tipo TELNET.

```
[SWITCH3]local-user telnet1
New local user added.
[SWITCH3-luser-telnet1]service-type telnet
[SWITCH3-luser-telnet1]password simple espe
[SWITCH3-luser-telnet1]attribute idle-cut 300 access-limit 5
```

```
[SWITCH3]local-user telnet2
New local user added.
[SWITCH3-luser-telnet2]service-type telnet
[SWITCH3-luser-telnet2]password simple espe
[SWITCH3-luser-telnet2]attribute idle-cut 300 access-limit 5
```

6.- Creamos el dominio local “laboratorio”.

```
[SWITCH3]domain laboratorio
New Domain added.
[SWITCH3-isp-laboratorio]scheme local
```

7.- Configuramos protocolo RADIUS IP del servidor es la IP de loopback 127.0.0.1 y el puerto es el 1645.

```
[SWITCH3]radius scheme laboratorio
[SWITCH3-radius-laboratorio]primary authentication 127.0.0.1 1645
[SWITCH3-radius-laboratorio]key authentication expert
[SWITCH3-radius-laboratorio]user-name-format without-domain
```

8.- Añadimos una IP tanto a la VLAN “MAESTROS” y “ESTUDIANTES”.

```
[SWITCH3]interface vlan-interface 10
[SWITCH3-Vlan-interface10]ip address 192.168.1.10 255.255.255.0
```

```
[SWITCH3]interface vlan-interface 20
[SWITCH3-Vlan-interface20]ip add 192.168.2.10 255.255.255.0
```

4.17.2.3. Prueba Acceso TELNET con servidor AAA

1. - Acceso PC1 al Switch, ingresamos al TERATERM y colocamos la opción TCP/IP TELNET. En la Figura 4.57. Nos muestra la pantalla de Conexión para acceso TELNET.

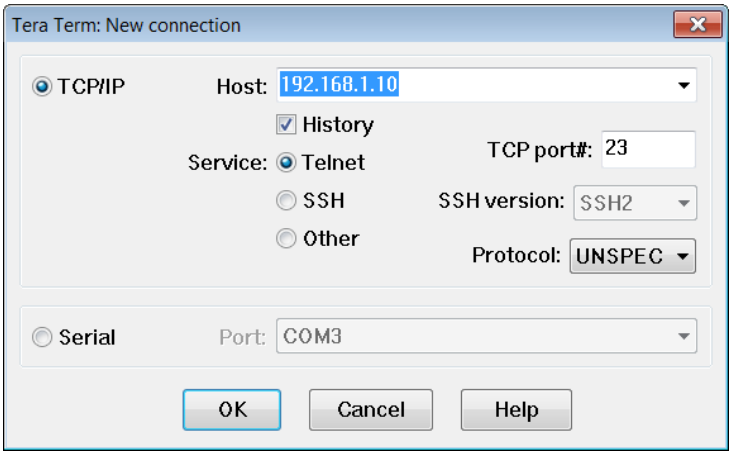


Figura 4.57. TeraTerm Conexión TELNET 3Com 4500 Práctica #16

1.1.- Ingresamos el usuario “telnet1” y la contraseña “espe”. En la Figura 4.58. Nos muestra la imagen de Acceso vía TELNET al Switch 3Com 4500.

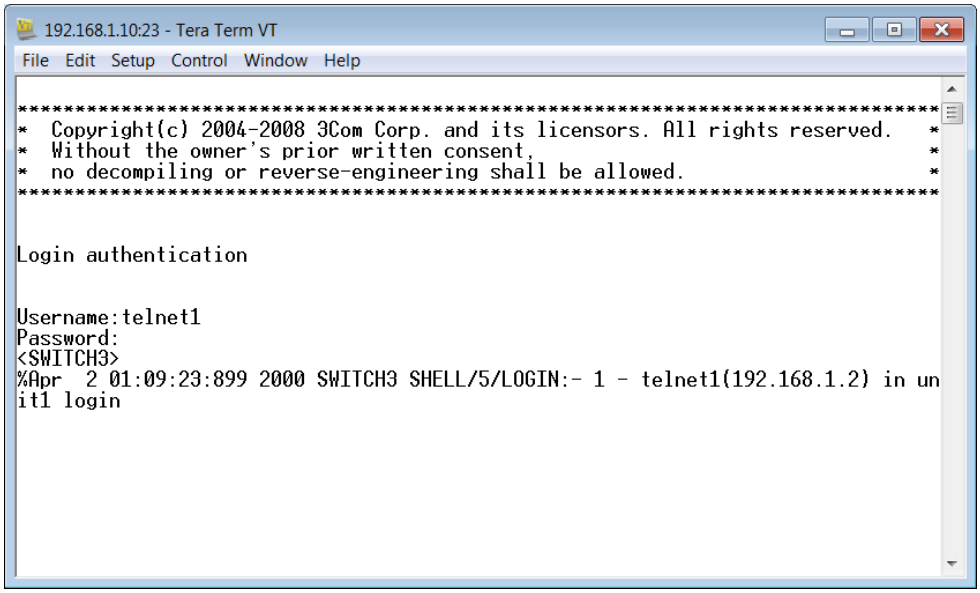


Figura 4.58. Conexión TELNET Switch 3Com 4500 Establecida Práctica #16

2.- Acceso PC4 al Switch, ingresamos al TERATERM y colocamos la opción TCP/IP TELNET. En la Figura 4.59. Nos muestra la pantalla de Conexión para acceso TELNET.

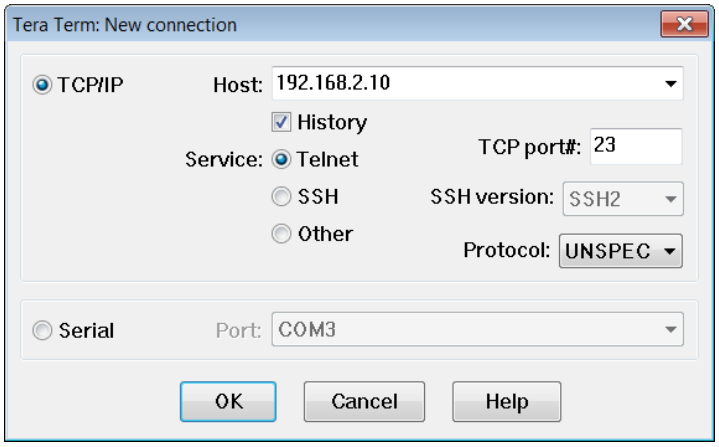


Figura 4.59. TeraTerm Conexión TELNET 3Com 4500 Práctica #16

2.1.- Ingresamos el usuario “telnet2” y el contraseña “espe”. En la Figura 4.60. Nos muestra la imagen de Acceso vía TELNET al Switch 3Com 4500.

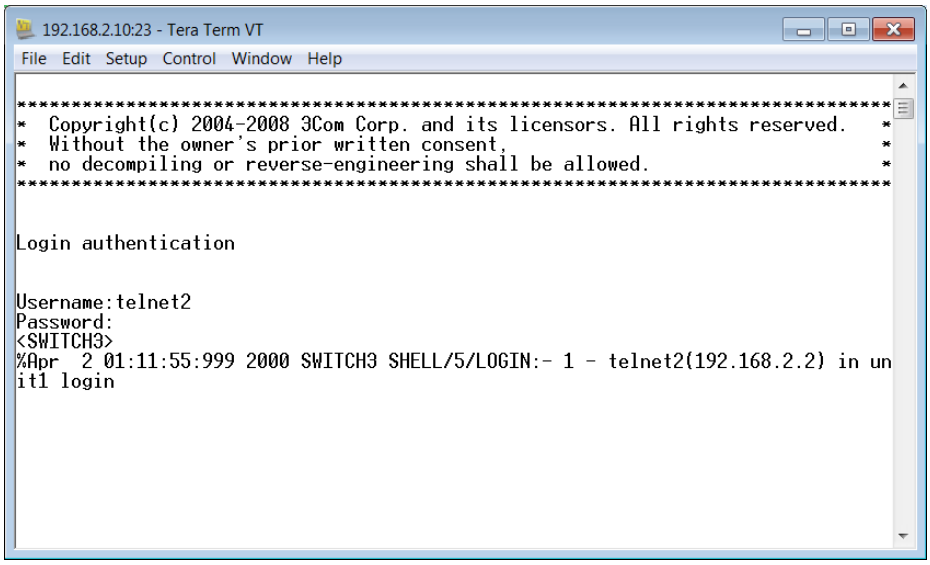


Figura 4.60. Conexión TELNET Switch 3Com 4500 Establecida Práctica #16

3.- Acceso con usuario y contraseña errónea. En la Figura 4.61. Nos muestra la imagen de Acceso vía TELNET al Switch 3Com 4500.

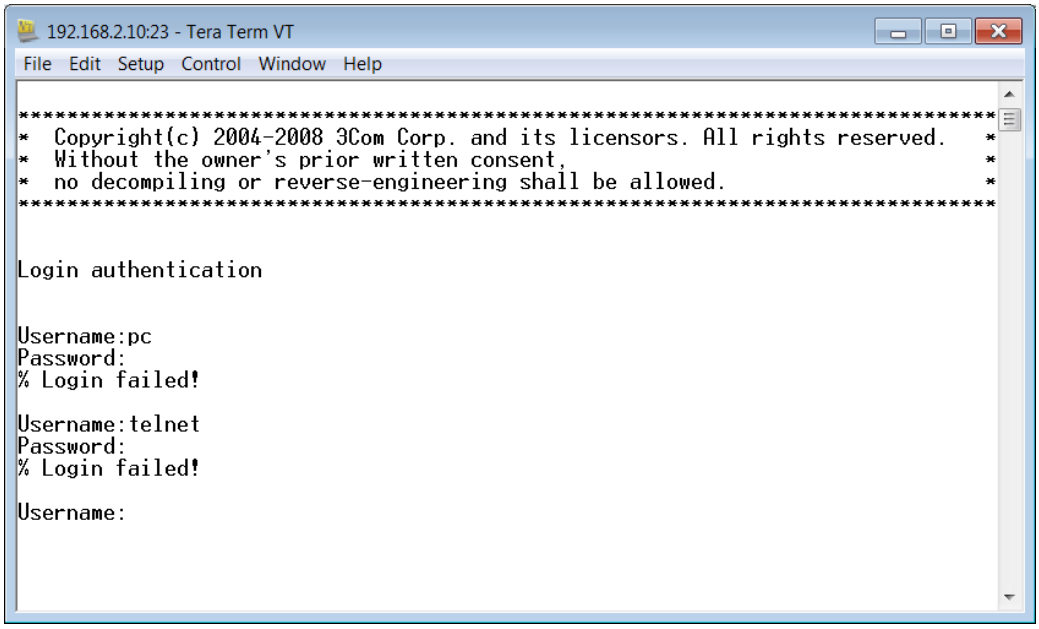


Figura 4.61. Conexión TELNET Switch 3Com 4500 Rechazada Práctica #16

4.18. DESARROLLO PRÁCTICA#17 SIMULACIÓN DE UNA RED QUE BRINDE AUTENTICACIÓN (AAA) Y QoS (802.1p)

4.18.1. Configuraciones/Direccionamiento

Direccionamiento:

DISPOSITIVO	Dirección IP	Máscara de Red	Interfaz
SWITCH 1			
VLAN 10 (TECNICO)	**192.168.10.10**	**255.255.255.0**	**Ethernet 1-3**
VLAN 20 (GERENTE)	**192.168.20.10**	**255.255.255.0**	**Ethernet 4-6**
ENLACE TRONCAL	--	--	**Ethernet 12**
SWITCH 2			
VLAN 10 (TECNICO)	**192.168.30.10**	**255.255.255.0**	**Ethernet 1-3**
VLAN 20	**192.168.40.10**	**255.255.255.0**	**Ethernet 4-6**

(GERENTE)			
ENLACE TRONCAL	**--**	**--**	**Ethernet 12**
ROUTER 1			
FAST ETHERNET 0/0	**192.168.50.1**	**255.255.255.0**	**Ethernet**
SERIAL 0/1/0	**200.0.0.1** ***Clock rate 128Kb***	**255.255.255.252**	**Ethernet**
SERIAL 0/1/1	**200.0.0.5** ***Clock rate 128Kb***	**255.255.255.252**	**Ethernet**
ROUTER 2			
SERIAL 0/1/0	**200.0.0.6**	**255.255.255.252**	**Ethernet**
SERIAL 0/1/1	**200.0.0.9** ***Clock rate 128Kb***	**255.255.255.252**	**Ethernet**
FAST ETHERNET 0/0.10	**192.168.30.1**	**255.255.255.0**	**Ethernet**
FAST ETHERNET 0/0.20	**192.168.40.1**	**255.255.255.0**	**Ethernet**
ROUTER 3			
SERIAL 0/1/0	**200.0.0.2**	**255.255.255.252**	**Ethernet**
SERIAL 0/1/1	**200.0.0.10**	**255.255.255.252**	**Ethernet**
FAST ETHERNET 0/0.10	**192.168.10.1**	**255.255.255.0**	**Ethernet**
FAST ETHERNET 0/0.20	**192.168.20.1**	**255.255.255.0**	**Ethernet**
HOST			
PC TECNICO	**192.168.10.2**	**255.255.255.0**	**Ethernet**
PC Gerente de Ventas	**192.168.20.2**	**255.255.255.0**	**Ethernet**

PC Jefe de Seguridad	**192.168.30.2**	**255.255.255.0**	**Ethernet**
PC Gerente de Promociones	**192.168.40.2**	**255.255.255.0**	**Ethernet**
SERVIDOR AAA	**192.168.30.3**	**255.255.255.0**	**Ethernet**
SERVIDOR WEB	**192.168.50.2**	**255.255.255.0**	**Ethernet**

Usuario y Password:

Usuario: PC

Password: espe

4.18.2. Procedimiento

4.18.2.1. Topología Práctica 17 Simulador Packet tracer

La Figura 4.62. Nos muestra la Topología de Red en el Simulador Packet Tracer.

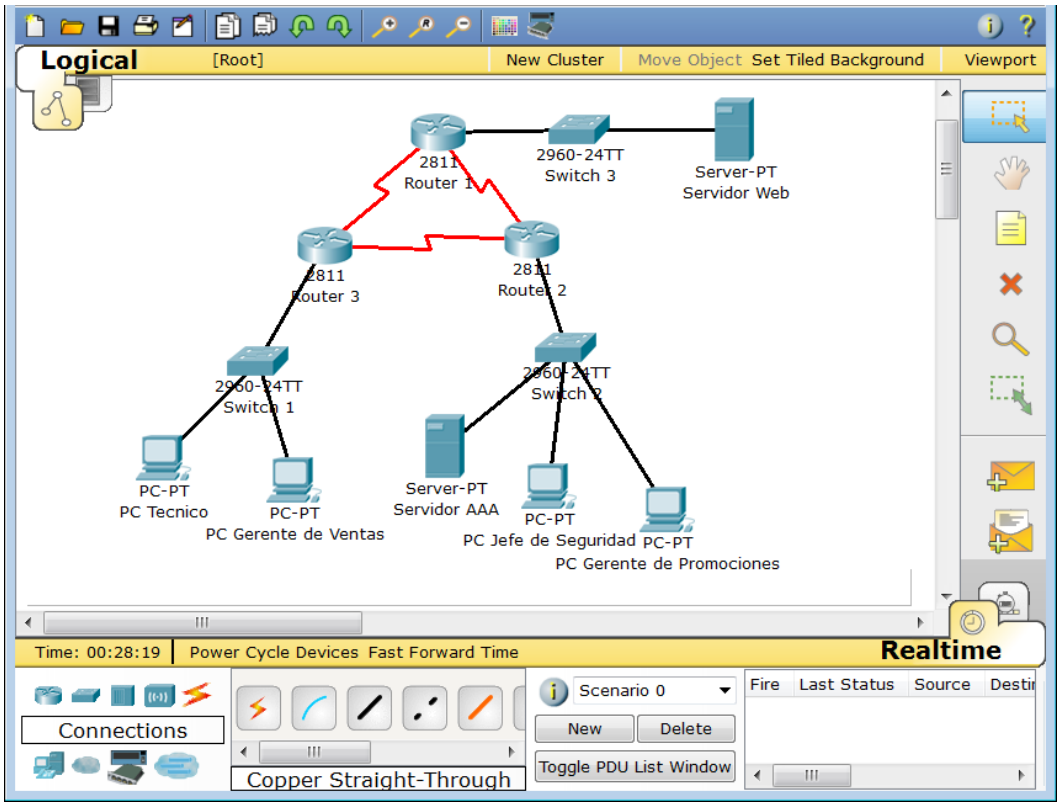


Figura 4.62. Simulación Topología de Red Práctica #17

4.18.2.2. Configuración SW1 CISCO 2960

1.- Accedemos al Switch y creamos la Vlan "TECNICO" y "GERENTE".

```
SW1(config)#vlan 10
SW1(config-vlan)#name TECNICO
SW1(config-vlan)#exit
SW1(config)#vlan 20
SW1(config-vlan)#name GERENTE
```

2.- Añadimos los puertos a la VLANs.

```
SW1(config)#interface range f0/1-3
SW1(config-if-range)#switchport mode access
SW1(config-if-range)#switchport access vlan 10
SW1(config-if-range)#exit
SW1(config)#interface range f0/4-6
SW1(config-if-range)#switchport mode access
SW1(config-if-range)#switchport access vlan 20
```

3.- Añadimos una dirección IP a las Vlans creadas.

```
SW1(config)#interface vlan 10
SW1(config-if)#ip add 192.168.10.10 255.255.255.0
SW1(config-if)#exit
SW1(config)#interface vlan 20
SW1(config-if)#ip add 192.168.20.10 255.255.255.0
```

4.- Configuración de Enlace Troncales.

```
SW1(config)#interface f0/12
SW1(config-if)#switchport mode trunk
SW1(config-if)#switchport trunk allowed vlan all
```

5.- Configuramos la prioridad en los puertos del SW1.

```
SW1(config)#mls qos
SW1(config)#interface range f0/1-3
SW1(config-if-range)#mls qos cos 5
SW1(config-if-range)#exit
SW1(config)#interface range f0/4-6
SW1(config-if-range)#mls qos cos 6
```

4.18.2.3. Configuración SW2 CISCO 2960

1.- Accedemos al Switch y creamos la Vlan “TECNICO” y “GERENTE”.

```
SW2(config)#vlan 10
SW2(config-vlan)#name TECNICO
SW2(config-vlan)#exit
SW2(config)#vlan 20
SW2(config-vlan)#name GERENTE
```

2.- Añadimos los puertos a la VLANs.

```
SW2(config)#interface range f0/1-3
SW2(config-if-range)#switchport mode access
SW2(config-if-range)#switchport access vlan 10
SW2(config-if-range)#exit
SW2(config)#interface range f0/4-6
SW2(config-if-range)#switchport mode access
SW2(config-if-range)#switchport access vlan 20
```

3.- Añadimos una dirección IP a las Vlans creadas.

```
SW2(config)#interface vlan 10
SW2(config-if)#ip add 192.168.30.10 255.255.255.0
SW2(config-if)#exit
SW2(config)#interface vlan 20
SW2(config-if)#ip add 192.168.40.10 255.255.255.0
```

4.- Configuración de Enlace Troncales.

```
SW2(config)#interface f0/12
SW2(config-if)#switchport mode trunk
SW2(config-if)#switchport trunk allowed vlan all
```

5.- Configuramos la prioridad en los puertos del SW2.

```
SW2(config)#mls qos
SW2(config)#interface range f0/1-3
SW2(config-if-range)#mls qos cos 5
SW2(config-if-range)#exit
SW2(config)#interface range f0/4-6
SW2(config-if-range)#mls qos cos 6
```

4.18.2.4. Configuración ROUTER 1 CISCO 2811

1.- Accedemos al Router configuramos las interfaces Fast Ethernet y Seriales.

```
ROUTER1(config)#interface f0/0
ROUTER1(config-if)#ip add 192.168.50.1 255.255.255.0
ROUTER1(config-if)#no shutdown
ROUTER1(config-if)#exit
ROUTER1(config)#interface s0/1/0
ROUTER1(config-if)#ip add 200.0.0.1 255.255.255.252
ROUTER1(config-if)#clock rate 128000
ROUTER1(config-if)#no shutdown
ROUTER1(config-if)#exit
ROUTER1(config)#interface s0/1/1
ROUTER1(config-if)#ip add 200.0.0.5 255.255.255.252
ROUTER1(config-if)#clock rate 128000
ROUTER1(config-if)#no shutdown
```

2.- Configuramos el protocolo de Enrutamiento en este caso RIPv2.

```
ROUTER1(config)#router rip
ROUTER1(config-router)#version 2
ROUTER1(config-router)#network 200.0.0.0
ROUTER1(config-router)#network 200.0.0.4
ROUTER1(config-router)#network 192.168.50.0
```

4.18.2.5. Configuración ROUTER 2 CISCO 2811

1.- Accedemos al Router configuramos las interfaces Seriales.

```
ROUTER2(config)#interface s0/1/0
ROUTER2(config-if)#ip add 200.0.0.6 255.255.255.252
ROUTER2(config-if)#no shutdown
ROUTER2(config-if)#exit
ROUTER2(config)#interface s0/1/1
ROUTER2(config-if)#ip add 200.0.0.9 255.255.255.252
ROUTER2(config-if)#clock rate 128000
ROUTER2(config-if)#no shutdown
```

2.-Configuramos las sub interfaces.

```
ROUTER2(config)#interface f0/0.10
ROUTER2(config-subif)#ip add 192.168.30.1 255.255.255.0
ROUTER2(config-subif)#encapsulation dot1q 10
ROUTER2(config-subif)#exit
ROUTER2(config)#interface f0/0.20
ROUTER2(config-subif)#ip add 192.168.40.1 255.255.255.0
ROUTER2(config-subif)#encapsulation dot1q 20
```

3.- Configuramos el protocolo de Enrutamiento en este caso RIPv2.

```
ROUTER2(config)#router rip
ROUTER2(config-router)#version 2
ROUTER2(config-router)#network 200.0.0.4
ROUTER2(config-router)#network 200.0.0.8
ROUTER2(config-router)#network 192.168.30.0
ROUTER2(config-router)#network 192.168.40.0
```

4.- Configuración AAA.

```
ROUTER2(config)#enable secret espe
ROUTER2(config)#aaa new-model
ROUTER2(config)#aaa authentication login default group radius none
ROUTER2(config)#aaa authentication login telnet group radius
ROUTER2(config)#radius-server host 192.168.30.3 auth-port 1645 key espe
ROUTER2(config)#line vty 0 4
ROUTER2(config-line)#login authentication telnet
```

4.18.2.6. Configuración ROUTER 3 CISCO 2811

1.- Accedemos al Router configuramos las interfaces Seriales.

```
ROUTER3(config)#interface s0/1/0
ROUTER3(config-if)#ip add 200.0.0.2 255.255.255.252
ROUTER3(config-if)#no shutdown
ROUTER3(config-if)#exit
ROUTER3(config)#interface s0/1/1
ROUTER3(config-if)#ip add 200.0.0.10 255.255.255.252
ROUTER3(config-if)#no shutdown
```

2.-Configuramos las sub interfaces.

```
ROUTER3(config)#interface f0/0.10
ROUTER3(config-subif)#ip add 192.168.10.1 255.255.255.0
ROUTER3(config-subif)#encapsulation dot1Q 10
ROUTER3(config-subif)#exit
ROUTER3(config)#interface f0/0.20
ROUTER3(config-subif)#ip add 192.168.20.1 255.255.255.0
ROUTER3(config-subif)#encapsulation dot1Q 20
```

3.- Configuramos el protocolo de Enrutamiento en este caso RIPv2.

```
ROUTER3(config)#router rip
ROUTER3(config-router)#version 2
ROUTER3(config-router)#network 200.0.0.0
ROUTER3(config-router)#network 200.0.0.8
ROUTER3(config-router)#network 192.168.10.0
ROUTER3(config-router)#network 192.168.20.0
```

4.- Configuración AAA.

```
ROUTER3(config)#enable secret espe
ROUTER3(config)#aaa new-model
ROUTER3(config)#aaa authentication login default local none
ROUTER3(config)#aaa authentication login telnet local
ROUTER3(config)#username PC password espe
ROUTER3(config)#line vty 0 4
ROUTER3(config-line)#login authentication telnet
```

4.18.2.7. Configuración PC SERVIDOR AAA

1.- Accedemos al Servidor AAA y nos posicionamos en la pestaña *Desktop---IP Configuration*. La Figura 4.63. Nos muestra la configuración IP del Servidor AAA.

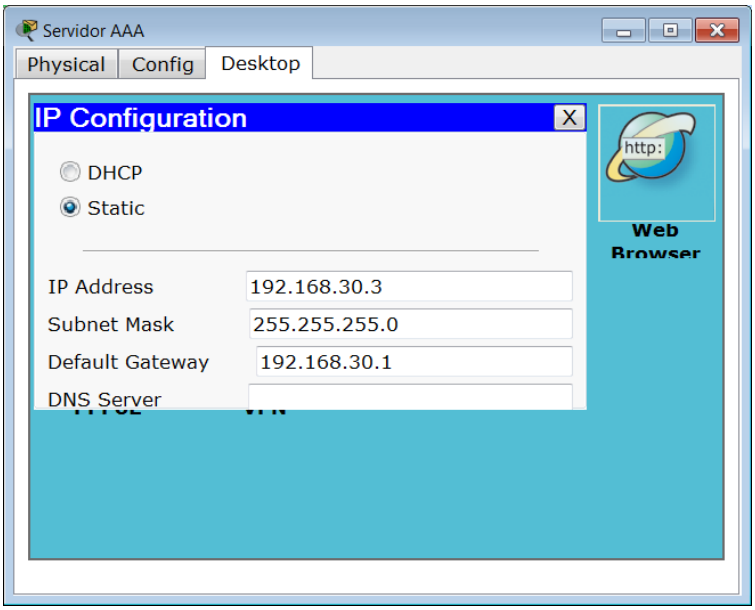


Figura 4.63. Configuración IP Servidor AAA Práctica #17

2.- En la pestaña "Config" accedemos a la configuración AAA y añadimos los siguientes parametros. La Figura 4.64. Nos muestra la configuración Global del Servidor AAA.

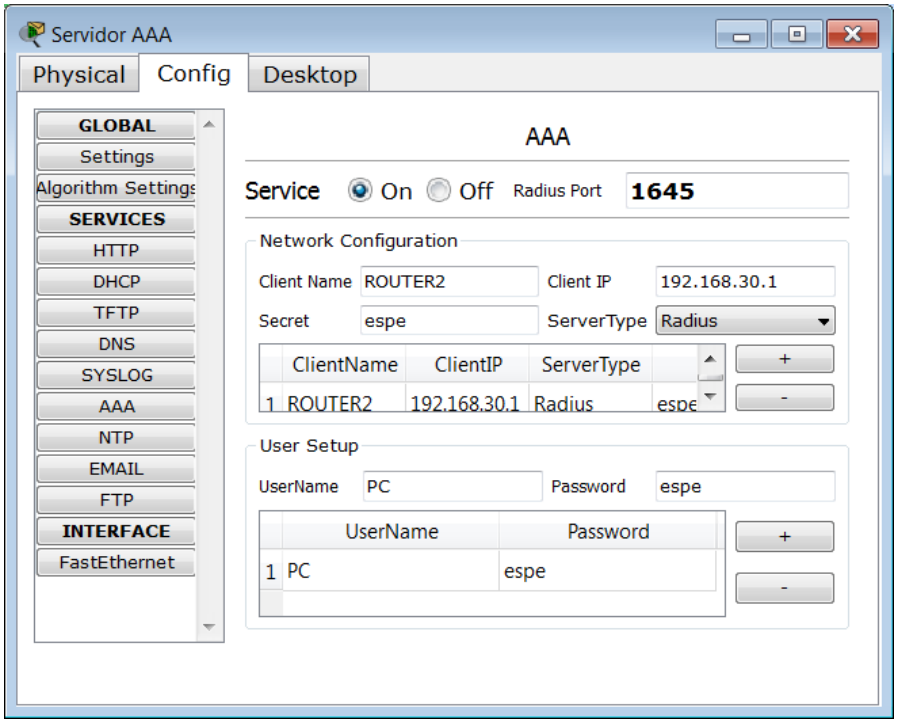


Figura 4.64. Configuración Global Servidor AAA Práctica #17

4.18.2.8. Prueba acceso Remoto desde PC Jefe de Seguridad

La Figura 4.65. Nos muestra la imagen de Acceso al Router 2.

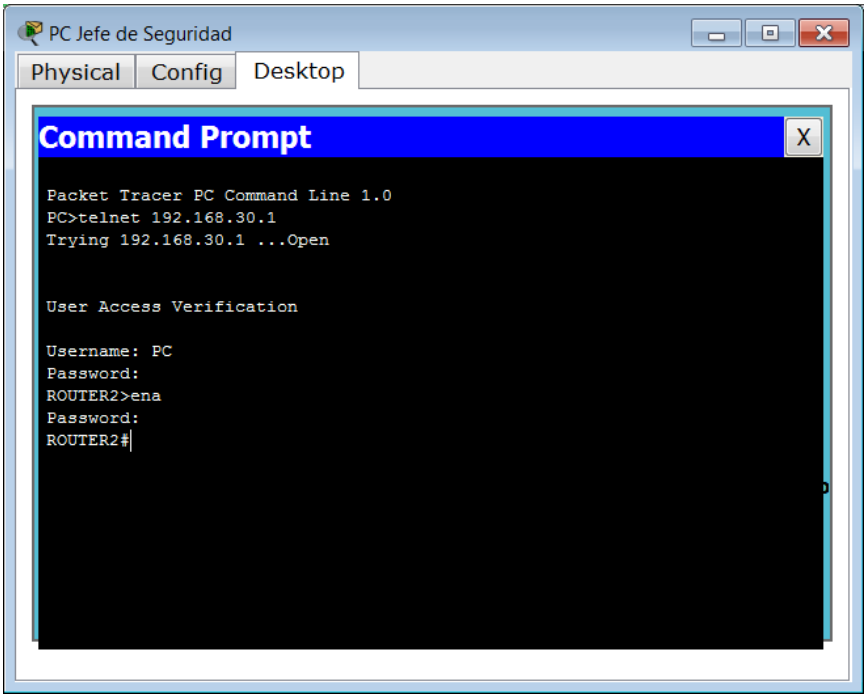


Figura 4.65. Acceso TELNET Router 2 Práctica #17

4.18.2.9. Prueba acceso Remoto desde PC Jefe Técnico

La Figura 4.66. Nos muestra la imagen de Acceso al Router 3.

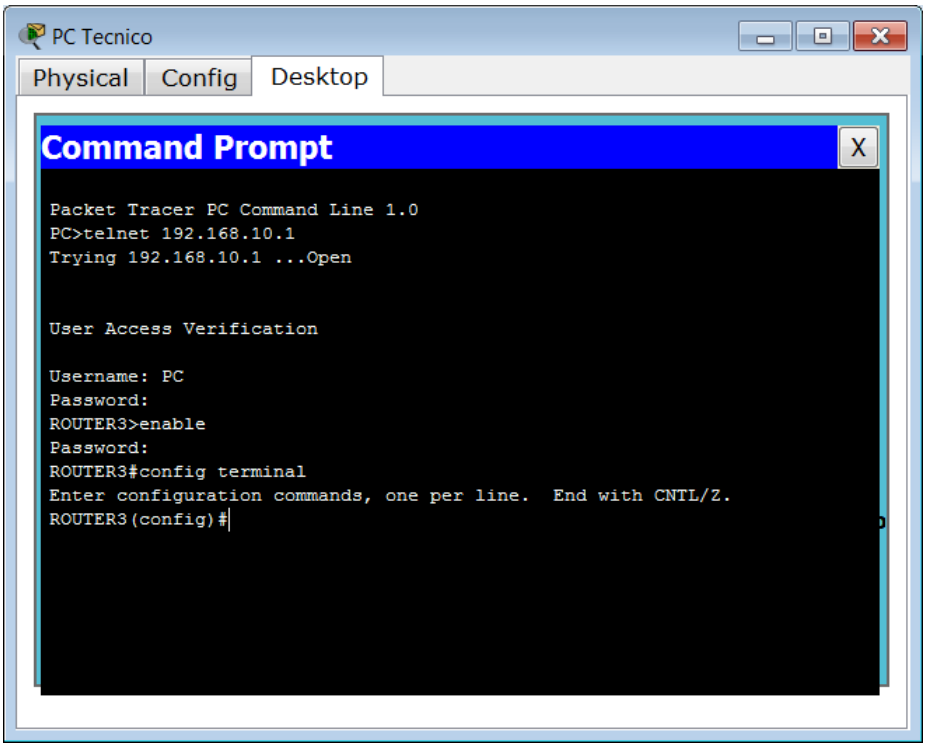


Figura 4.66. Acceso TELNET Router 3 Práctica #17

4.18.2.10. Prueba acceso Servidor Web desde PC Gerente de Promociones

La Figura 4.67. Nos muestra la imagen de Acceso WEB.

Figura 4.67. Acceso WEB Práctica #17

4.19. DESARROLLO PRÁCTICA#18 IMPLEMENTACIÓN DE UNA RED OPERATIVA IPv4 QUE BRINDE (VLAN, ACL, AAA, SSH, QoS)

4.19.1. Configuraciones/Direccionamiento

Direccionamiento:

DISPOSITIVO	Dirección IP	Máscara de Red	Interfaz
SW1 *CISCO 3560*			
VLAN 10 (EMPLEADOS)	**192.168.1.20**	**255.255.255.0**	**Ethernet 1-3**
VLAN 20 (GERENTES)	**192.168.2.20**	**255.255.255.0**	**Ethernet 4-6**
VLAN 30 (ADMINISTRADOR)	**192.168.3.20**	**255.255.255.0**	**Ethernet 7-9**
VLAN 1	**200.0.0.1**	**255.255.255.252**	**Ethernet**

ENLACE TRONCAL	--	--	**Ethernet 10-11-12**
SW2 *3COM 4500*			
VLAN 10 (EMPLEADOS)	**192.168.1.21**	**255.255.255.0**	**Ethernet 1-3**
VLAN 20 (GERENTES)	**192.168.2.21**	**255.255.255.0**	**Ethernet 4-6**
VLAN 30 (ADMINISTRADOR)	**192.168.3.21**	**255.255.255.0**	**Ethernet 7-9**
ENLACE TRONCAL	--	--	**Ethernet 11**
SW3 *3COM 5500*			
VLAN 10 (EMPLEADOS)	**192.168.1.22**	**255.255.255.0**	**Ethernet 1-3**
VLAN 20 (GERENTES)	**192.168.2.22**	**255.255.255.0**	**Ethernet 4-6**
VLAN 30 (ADMINISTRADOR)	**192.168.3.22**	**255.255.255.0**	**Ethernet 7-9**
ENLACE TRONCAL	--	--	**Ethernet 11**
SW4 *D-Link DGS-3627*			
VLAN 10 (EMPLEADOS)	**192.168.10.23**	**255.255.255.0**	**Ethernet 1-3**
VLAN 20 (GERENTES)	**192.168.20.23**	**255.255.255.0**	**Ethernet 4-6**
VLAN 30 (ADMINISTRADOR)	**192.168.30.23**	**255.255.255.0**	**Ethernet 7-9**
VLAN 1	**200.0.0.10**	**255.255.255.252**	
ENLACE TRONCAL	--	--	**Ethernet 11-12**
SW5 *3COM 4210*			
VLAN 10	**192.168.10.24**	**255.255.255.0**	**Ethernet 1-3**

(EMPLEADOS)			
VLAN 20 (GERENTES)	**192.168.20.24**	**255.255.255.0**	**Ethernet 4-6**
VLAN 30 (ADMINISTRADOR)	**192.168.30.24**	**255.255.255.0**	**Ethernet 7-9**
ENLACE TRONCAL	**--**	**--**	**Ethernet 11**
ROUTER 1 ***CISCO 2000 SERIES***			
FAST ETHERNET	**200.0.0.2**	**255.255.255.252**	**Ethernet**
SERIAL	**200.0.0.5**	**255.255.255.252**	**Serial**
ROUTER 2 ***CISCO 2000 SERIES***			
FAST ETHERNET	**200.0.0.9**	**255.255.255.252**	**Ethernet**
SERIAL	**200.0.0.6**	**255.255.255.252**	**Serial**
PC EMPLEADO 1	**192.168.1.2**	**255.255.255.0**	**Ethernet**
PC EMPLEADO 2	**192.168.1.3**	**255.255.255.0**	**Ethernet**
PC EMPLEADO 3	**192.168.1.4**	**255.255.255.0**	**Ethernet**
PC GERENTE 3	**192.168.20.2**	**255.255.255.0**	**Ethernet**
PC GERENTE 1	**192.168.2.2**	**255.255.255.0**	**Ethernet**
PC GERENTE 2	**192.168.2.3**	**255.255.255.0**	**Ethernet**
PC ADMINISTRADOR 1	**192.168.30.2**	**255.255.255.0**	**Ethernet**
PC ADMINISTRADOR 2	**192.168.30.3**	**255.255.255.0**	**Ethernet**

PC ADMINISTRADOR 3	**192.168.30.4**	**255.255.255.0**	**Ethernet**

Usuario y Password telnet/SSH:

Usuario: PCAD

Password: esperedes1

Usuario y Password telnet AAA:

Usuario: adtelnet

Password: espe

4.19.2. Procedimiento

4.19.2.1. Configuración Cisco 3560

1.- Accedemos al Switch y creamos la Vlan “EMPLEADOS”, “GERENTES”, “ADMINISTRADOR”.

```
SW1(config)#vlan 10
SW1(config-vlan)#name EMPLEADOS
SW1(config-vlan)#exit
SW1(config)#vlan 20
SW1(config-vlan)#name GERENTES
SW1(config-vlan)#exit
SW1(config)#vlan 30
SW1(config-vlan)#name ADMINISTRADOR
```

2.- Añadimos los puertos a las VLANs.

```
SW1(config)#interface range f0/1-3
SW1(config-if-range)#switchport access vlan 10
SW1(config-if-range)#no shutdown
SW1(config-if-range)#exit
SW1(config)#interface range f0/4-6
SW1(config-if-range)#switchport access vlan 20
SW1(config-if-range)#no shutdown
SW1(config-if-range)#exit
SW1(config)#interface range f0/7-9
SW1(config-if-range)#switchport access vlan 30
SW1(config-if-range)#no shutdown
```

3.- Configuración de Enlace Troncales.

```
SW1(config)#interface range f0/10-12
SW1(config-if-range)#switchport mode trunk
SW1(config-if-range)#switchport trunk encapsulation dot1q
SW1(config-if-range)#switchport trunk allowed vlan all
SW1(config-if-range)#no shutdown
```

4.- Añadimos una dirección IP a la VLAN 1, VLAN "EMPLEADOS", VLAN "GERENTE", VLAN "ADMINISTRADOR".

```
SW1(config)#interface vlan 1
SW1(config-if)#ip address 200.0.0.1 255.255.255.252
SW1(config-if)#no shutdown
```

```
SW1(config)#interface vlan 10
SW1(config-if)#ip address 192.168.1.20 255.255.255.0
SW1(config-if)#no shutdown
```

```
SW1(config)#interface vlan 20
SW1(config-if)#ip address 192.168.2.20 255.255.255.0
SW1(config-if)#no shutdown
```

```
SW1(config)#interface vlan 30
SW1(config-if)#ip address 192.168.3.20 255.255.255.0
SW1(config-if)#no shutdown
```

5.- Habilitamos el enrutamiento en el Switch y publicamos las redes directamente conectadas.

```
SW1(config)#ip routing
SW1(config)#router rip
SW1(config-router)#version 2
SW1(config-router)#network 192.168.1.0
SW1(config-router)#network 192.168.2.0
SW1(config-router)#network 192.168.3.0
SW1(config-router)#network 200.0.0.0
```

4.19.2.2. Configuración 3COM 4500

1.- Accedemos al Switch y creamos la Vlan "EMPLEADOS", "GERENTES", "ADMINISTRADOR".

```
[SW2]vlan 10
[SW2-vlan10]name EMPLEADOS
[SW2-vlan10]quit
[SW2]vlan 20
[SW2-vlan20]name GERENTES
[SW2-vlan20]quit
[SW2]vlan 30
[SW2-vlan30]name ADMINISTRADOR
```

2.- Añadimos los puertos a las VLANs.

```
[SW2]vlan 10
[SW2-vlan10]port ethernet 1/0/1 to ethernet 1/0/3
[SW2-vlan10]quit
[SW2]vlan 20
[SW2-vlan20]port ethernet 1/0/4 to ethernet 1/0/6
[SW2-vlan20]quit
[SW2]vlan 30
[SW2-vlan30]port ethernet 1/0/7 to ethernet 1/0/9
```

3.- Configuración de Enlace Troncales.

```
[SW2]interface ethernet 1/0/11
[SW2-Ethernet1/0/11]port link-type trunk
[SW2-Ethernet1/0/11]port trunk permit vlan 10
 Please wait... Done.
[SW2-Ethernet1/0/11]port trunk permit vlan 20
 Please wait... Done.
[SW2-Ethernet1/0/11]port trunk permit vlan 30
 Please wait... Done.
```

4.- Configuración de la prioridad QoS (802.1p) en los puertos del Switch recordemos que hay 8 prioridades siendo 0 el menor y 7 el de más prioridad.

4.1.- Damos prioridad 4 a las interfaces que pertenecen a la VLAN "EMPLEADOS".

```
[SW2]interface ethernet 1/0/1
[SW2-Ethernet1/0/1]priority 4
[SW2-Ethernet1/0/1]quit
[SW2]interface ethernet 1/0/2
[SW2-Ethernet1/0/2]priority 4
[SW2-Ethernet1/0/2]quit
[SW2]interface ethernet 1/0/3
[SW2-Ethernet1/0/3]priority 4
```

4.2.- Damos prioridad 5 a las interfaces que pertenecen a la VLAN "ADMINISTRADOR".

```
[SW2]interface ethernet 1/0/7
[SW2-Ethernet1/0/7]priority 5
[SW2-Ethernet1/0/7]quit
[SW2]interface ethernet 1/0/8
[SW2-Ethernet1/0/8]priority 5
[SW2-Ethernet1/0/8]quit
[SW2]interface ethernet 1/0/9
[SW2-Ethernet1/0/9]priority 5
```

4.3.- Damos prioridad 6 a las interfaces que pertenecen a la VLAN "GERENTES".

```
[SW2]interface ethernet 1/0/4
[SW2-Ethernet1/0/4]priority 6
[SW2-Ethernet1/0/4]quit
[SW2]interface ethernet 1/0/5
[SW2-Ethernet1/0/5]priority 6
[SW2-Ethernet1/0/5]quit
[SW2]interface ethernet 1/0/6
[SW2-Ethernet1/0/6]priority 6
```

5.- Creamos las claves RSA para la configuración de SSH.

```
[SW2]rsa local-key-pair create
The local-key-pair will be created.
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
       It will take a few minutes.
Input the bits in the modulus[default = 1024]:1024
Generating keys...
........++++++
.............................................++++++
..Done!
```

6.- Ponemos la Autenticación AAA y ponemos el tipo de protocolo de entrada.

```
[SW2]user-interface vty 0 4
[SW2-ui-vty0-4]authentication-mode scheme
[SW2-ui-vty0-4]protocol inbound ssh
```

7.- Creamos el usuario:"PC1" y ponemos la contraseña:"esperedes1".

```
[SW2]local-user PCAD
New local user added.
[SW2-luser-PCAD]password simple esperedes1
[SW2-luser-PCAD]service-type ssh
[SW2-luser-PCAD]quit
[SW2]ssh user PCAD authentication-type password
```

8.- Añadimos una dirección IP a la VLAN "ADMINISTRADOR" y un gateway.

```
[SW2]interface Vlan-interface 30
[SW2-Vlan-interface30]ip add 192.168.3.21 255.255.255.0
```

```
[SW2]ip route-static  0.0.0.0 0.0.0.0  192.168.3.20
```

4.19.2.3. Configuración 3COM 5500

1.- Accedemos al Switch y creamos la Vlan "EMPLEADOS", "GERENTES", "ADMINISTRADOR".

```
[SW3]vlan 10
[SW3-vlan10]name EMPLEADOS
[SW3-vlan10]quit
[SW3]vlan 20
[SW3-vlan20]name GERENTES
[SW3-vlan20]quit
[SW3]vlan 30
[SW3-vlan30]name ADMINISTRADOR
```

2.- Añadimos los puertos a las VLANs.

```
[SW3]vlan 10
[SW3-vlan10]port ethernet 1/0/1 to ethernet 1/0/3
[SW3-vlan10]quit
[SW3]vlan 20
[SW3-vlan20]port ethernet 1/0/4 to ethernet 1/0/6
[SW3-vlan20]quit
[SW3]vlan 30
[SW3-vlan30]port ethernet 1/0/7 to ethernet 1/0/9
```

3.- Configuración de Enlace Troncales.

```
[SW3]interface ethernet 1/0/11
[SW3-Ethernet1/0/11]port link-type trunk
[SW3-Ethernet1/0/11]port trunk permit vlan 10
 Please wait... Done.
[SW3-Ethernet1/0/11]port trunk permit vlan 20
 Please wait... Done.
[SW3-Ethernet1/0/11]port trunk permit vlan 30
 Please wait... Done.
```

4.- Aplicamos la autenticación AAA a los usuarios TELNET.

```
[SW3]user-interface vty 0 4
[SW3-ui-vty0-4]authentication-mode scheme
```

5.- Creamos el usuario local tipo TELNET.

```
[SW3]local-user adtelnet
New local user added.
[SW3-luser-adtelnet]service-type telnet
[SW3-luser-adtelnet]password simple espe
[SW3-luser-adtelnet]attribute idle-cut 3000 access-limit 5
```

6.- Creamos el dominio local “laboratorio”.

```
[SW3]domain laboratorio
New Domain added.
[SW3-isp-laboratorio]schem local
```

7.- Configuramos protocolo RADIUS IP del servidor es la IP de loopback 127.0.0.1 y el puerto es el 1645.

```
[SW3]radius scheme laboratorio
New Radius scheme
[SW3-radius-laboratorio]primary authentication 127.0.0.1 1645
[SW3-radius-laboratorio]key authentication expert
[SW3-radius-laboratorio]user-name-format without-domain
```

8.- Añadimos una dirección IP a la VLAN “ADMINISTRADOR” y el gateway.

```
[SW3]interface Vlan-interface 30
[SW3-Vlan-interface30]ip address 192.168.3.22 255.255.255.0
```

```
[SW3]ip route-static  0.0.0.0 0.0.0.0 192.168.3.20
```

4.19.2.4. Configuración CISCO 2000 R1

1.- Accedemos al Router configuramos, habilitamos el acceso vía telnet y ponemos password para acceder al modo privilegiado.

```
R1(config)#enable secret espe
R1(config)#line vty 0 4
R1(config-line)#password espe
R1(config-line)#login
```

2.- Configuramos la dirección IP de la interface Serial y la interface Fast Ethernet.

```
R1(config)#interface f0/0
R1(config-if)#ip address 200.0.0.2 255.255.255.252
R1(config-if)#no shutdown
```

```
R1(config)#interface s0/2
R1(config-if)#ip address 200.0.0.5 255.255.255.252
R1(config-if)#clock rate 128000
R1(config-if)#no shutdown
```

3.- Configuramos el protocolo de Enrutamiento en este caso RIPv2.

```
R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#network 200.0.0.0
R1(config-router)#network 200.0.0.4
```

4.19.2.5. Configuración CISCO 2000 R2

1.- Accedemos al Router configuramos, habilitamos el acceso vía telnet y ponemos password para acceder al modo privilegiado.

```
R2(config)#enable secret espe
R2(config)#line vty 0 4
R2(config-line)#password espe
R2(config-line)#login
```

2.- Configuramos la dirección IP de la interface Serial y la interface Fast Ethernet.

```
R2(config)#interface f0/0
R2(config-if)#ip address 200.0.0.9 255.255.255.252
R2(config-if)#no shutdown
```

```
R2(config)#interface s0/3/1
R2(config-if)#ip address 200.0.0.6 255.255.255.252
R2(config-if)#no shutdown
```

3.- Configuramos el protocolo de Enrutamiento en este caso RIPv2.

```
R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#network 200.0.0.4
R2(config-router)#network 200.0.0.8
R2(config-router)#network 192.168.10.0
R2(config-router)#network 192.168.20.0
R2(config-router)#network 192.168.30.0
```

4.- Configuramos la lista de acceso extendida 101 a la interface F0/0 de salida.

```
Extended IP access list 101
    10 deny icmp 192.168.1.0 0.0.0.255 192.168.20.0 0.0.0.255 echo
    20 deny icmp 192.168.1.0 0.0.0.255 192.168.30.0 0.0.0.255 echo
    30 deny icmp 192.168.2.0 0.0.0.255 192.168.20.0 0.0.0.255 echo
    40 deny icmp 192.168.2.0 0.0.0.255 192.168.30.0 0.0.0.255 echo
    50 permit ip any any
```

```
R2(config)#interface f0/0
R2(config-if)#ip access-group 101 out
```

4.19.2.6. Configuración D-Link DES-3627

1.- Accedemos al Switch y creamos la Vlan “EMPLEADOS”, “GERENTES”, “ADMINISTRADOR”.

```
DGS-3627:4#create vlan EMPLEADOS tag 10
Command: create vlan EMPLEADOS tag 10

Success.

DGS-3627:4#create vlan GERENTES tag 20
Command: create vlan GERENTES tag 20

Success.

DGS-3627:4#create vlan ADMINISTRADOR tag 30
Command: create vlan ADMINISTRADOR tag 30

Success.
```

2.- Añadimos los puertos a la VLANs.

```
DGS-3627:4#config vlan default delete 1-9
Command: config vlan default delete 1-9

Success.

DGS-3627:4#config vlan EMPLEADOS add untagged 1-3
Command: config vlan EMPLEADOS add untagged 1-3

Success.

DGS-3627:4#config vlan GERENTES add untagged 4-6
Command: config vlan GERENTES add untagged 4-6

Success.

DGS-3627:4#config vlan ADMINISTRADOR add untagged 7-9
Command: config vlan ADMINISTRADOR add untagged 7-9

Success.
```

3.- Configuración de Enlace Troncales.

```
DGS-3627:4#config vlan EMPLEADOS add tagged 11-12
Command: config vlan EMPLEADOS add tagged 11-12

Success.

DGS-3627:4#config vlan GERENTES add tagged 11-12
Command: config vlan GERENTES add tagged 11-12

Success.

DGS-3627:4#config vlan ADMINISTRADOR add tagged 11-12
Command: config vlan ADMINISTRADOR add tagged 11-12

Success.
```

4.- Accedemos al Switch y configuramos nombre.

```
DGS-3627:4#create account admin PCAD
Command: create account admin PCAD

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

5.- Añadimos una dirección IP a la VLAN 1, VLAN “EMPLEADOS”, VLAN “GERENTE”, VLAN “ADMINISTRADOR”.

```
DGS-3627:4#config ipif System ipaddress 200.0.0.10/30
Command: config ipif System ipaddress 200.0.0.10/30

Success.
```

```
DGS-3627:4#create ipif EMPLEADOS 192.168.10.23/24 EMPLEADOS
Command: create ipif EMPLEADOS 192.168.10.23/24 EMPLEADOS

Success.
```

```
DGS-3627:4#create ipif GERENTES 192.168.20.23/24 GERENTES
Command: create ipif GERENTES 192.168.20.23/24 GERENTES

Success.
```

```
DGS-3627:4#create ipif ADMINISTRAD 192.168.30.23/24 ADMINISTRADOR
Command: create ipif ADMINISTRAD 192.168.30.23/24 ADMINISTRADOR

Success.
```

6.- Para configurar SSH en el Switch D-link 3627 utilizamos los siguientes comandos.

```
DGS-3627:4#config ssh user PCAD authmode password
Command: config ssh user PCAD authmode password

Success.
```

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

```
DGS-3627:4#config ssh algorithm RSA enable
Command: config ssh algorithm RSA enable

Success.
```

8.- Habilitamos SSH en el Switch.

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

TELNET will be disabled when enable SSH.
Success.

DGS-3627:4
```

9.- Habilitamos el protocolo de enrutamiento RIPv2 a todas las interfaces tanto para enviar como para recibir.

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

Success.
```

```
DGS-3627:4#config rip all rx_mode v2_only state enable
Command: config rip all rx_mode v2_only state enable

Success.

DGS-3627:4#config rip all tx_mode v2_only state enable
Command: config rip all tx_mode v2_only state enable

Success.
```

4.19.2.7. Configuración Equipo 3COM 4210

1.- Accedemos al Switch y creamos la Vlan “EMPLEADOS”, “GERENTES”, “ADMINISTRADOR”.

```
[SW5]vlan 10
[SW5-vlan10]name EMPLEADOS
[SW5-vlan10]quit
[SW5]vlan 20
[SW5-vlan20]name GERENTES
[SW5-vlan20]quit
[SW5]vlan 30
[SW5-vlan30]name ADMINISTRADOR
```

2.- Añadimos los puertos a las VLANs.

```
[SW5]vlan 10
[SW5-vlan10]port ethernet 1/0/1 to ethernet 1/0/3
[SW5-vlan10]quit
[SW5]vlan 20
[SW5-vlan20]port ethernet 1/0/4 to ethernet 1/0/6
[SW5-vlan20]quit
[SW5]vlan 30
[SW5-vlan30]port ethernet 1/0/7 to ethernet 1/0/9
```

3.- Configuración de Enlace Troncales.

```
[SW5]interface ethernet 1/0/11
[SW5-Ethernet1/0/11]port link-type trunk
[SW5-Ethernet1/0/11]port trunk permit vlan 10
 Please wait... Done.
[SW5-Ethernet1/0/11]port trunk permit vlan 20
 Please wait... Done.
[SW5-Ethernet1/0/11]port trunk permit vlan 30
 Please wait... Done.
```

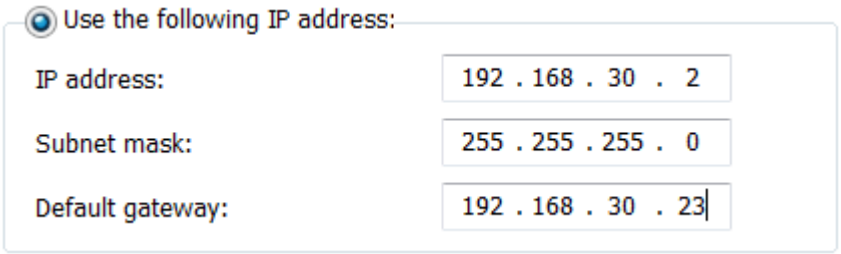
4.19.2.8. Tabla de Enrutamiento R1-R2

```
R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

R    192.168.30.0/24 [120/2] via 200.0.0.6, 00:00:28, Serial0/2
     200.0.0.0/30 is subnetted, 3 subnets
R       200.0.0.8 [120/1] via 200.0.0.6, 00:00:28, Serial0/2
C       200.0.0.0 is directly connected, FastEthernet0/0
C       200.0.0.4 is directly connected, Serial0/2
R    192.168.10.0/24 [120/2] via 200.0.0.6, 00:00:28, Serial0/2
R    192.168.20.0/24 [120/2] via 200.0.0.6, 00:00:28, Serial0/2
R    192.168.1.0/24 [120/1] via 200.0.0.1, 00:00:18, FastEthernet0/0
R    192.168.2.0/24 [120/1] via 200.0.0.1, 00:00:19, FastEthernet0/0
R    192.168.3.0/24 [120/1] via 200.0.0.1, 00:00:19, FastEthernet0/0
```

```
R2#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

R    192.168.30.0/24 [120/1] via 200.0.0.10, 00:00:29, FastEthernet0/0
     200.0.0.0/30 is subnetted, 3 subnets
C       200.0.0.8 is directly connected, FastEthernet0/0
R       200.0.0.0 [120/1] via 200.0.0.5, 00:00:10, Serial0/3/1
C       200.0.0.4 is directly connected, Serial0/3/1
R    192.168.10.0/24 [120/1] via 200.0.0.10, 00:00:29, FastEthernet0/0
R    192.168.20.0/24 [120/1] via 200.0.0.10, 00:00:29, FastEthernet0/0
R    192.168.1.0/24 [120/2] via 200.0.0.5, 00:00:10, Serial0/3/1
R    192.168.2.0/24 [120/2] via 200.0.0.5, 00:00:11, Serial0/3/1
R    192.168.3.0/24 [120/2] via 200.0.0.5, 00:00:11, Serial0/3/1
```

4.19.2.9. Prueba Acceso SSH Administrador 1 Switch 2

1.- Ingresamos al programa TERATERM, ponemos el protocolo SSH la dirección IP 192.168.2.21 y presionamos OK. En la Figura 4.68. Nos muestra la pantalla de Conexión para acceso SSH.



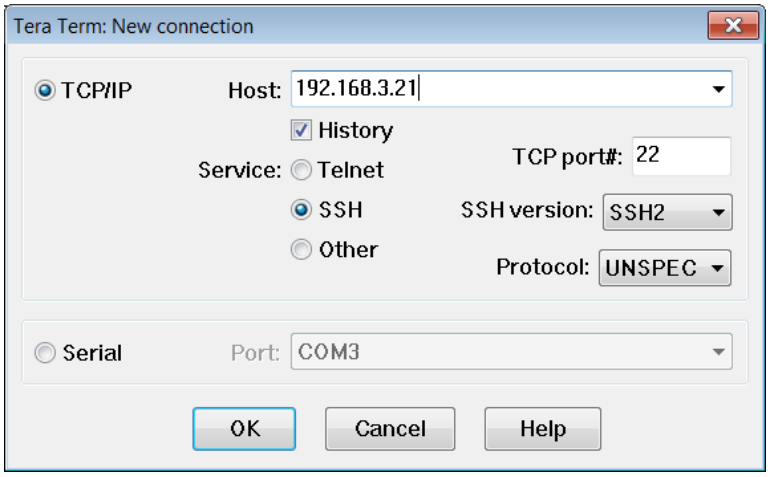


Figura 4.68. TeraTerm Conexión SSH Switch 2 Práctica #18

2.- Nos pedirá el nombre de usuario: "PCAD" y la contraseña: "esperedes1" para poder acceder al Switch. La Figura 4.69. Es la imagen de Acceso Remoto al Switch.

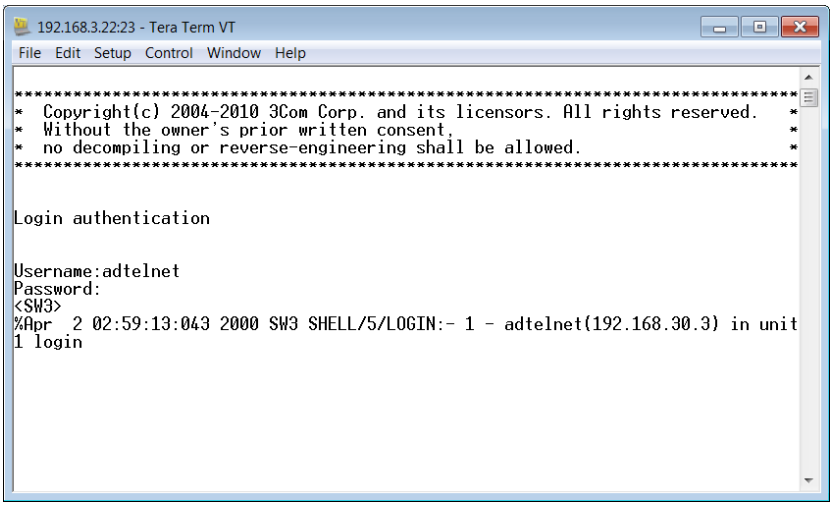


Figura 4.69. Conexión SSH Switch 2 Práctica #18

4.19.2.10. Prueba Acceso TELNET AAA Administrador 2 Switch 3

1.- Ingresamos al programa TERATERM, ponemos el protocolo TELNET la dirección IP 192.168.3.22 y presionames OK. En la Figura 4.70. Nos muestra la pantalla de Conexión para acceso TELNET por medio del Servidor AAA.

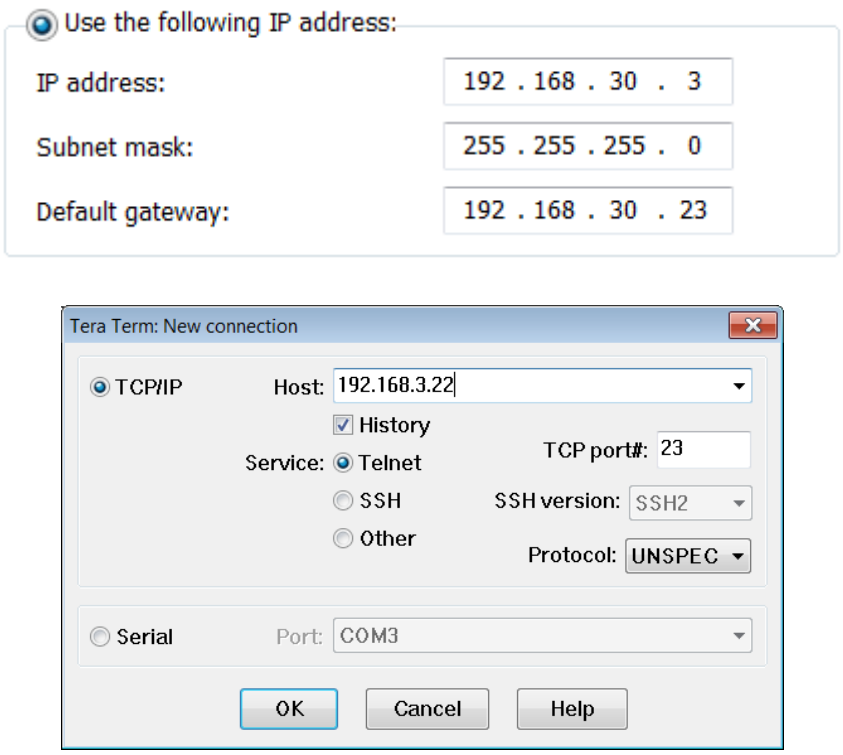


Figura 4.70. TeraTerm Conexión SSH Switch 3 Práctica #18

2.- Nos pedirá el nombre de usuario: "adtelnet" y la contraseña: "espe" para poder acceder al Switch. La Figura 4.71. Es la imagen de Acceso Remoto al Switch.

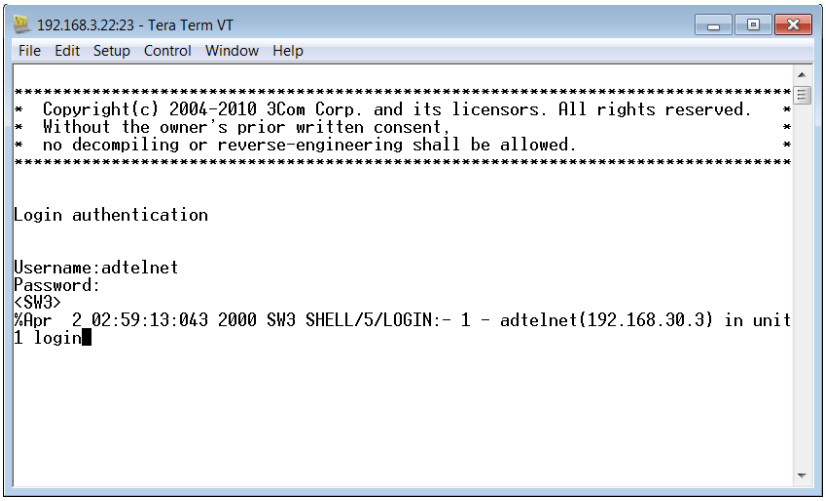


Figura 4.71. Conexión SSH Switch 3 Práctica #18

4.19.2.11. Prueba Acceso TELNET R1

1.- Ingresamos al programa TERATERM, ponemos el protocolo TELNET la dirección IP 200.0.0.5 y presionamos OK. La Figura 4.72. Nos muestra la Configuración IP del Computador. Mientras que la Figura 4.73. Nos muestra la pantalla de Conexión para acceso TELNET.

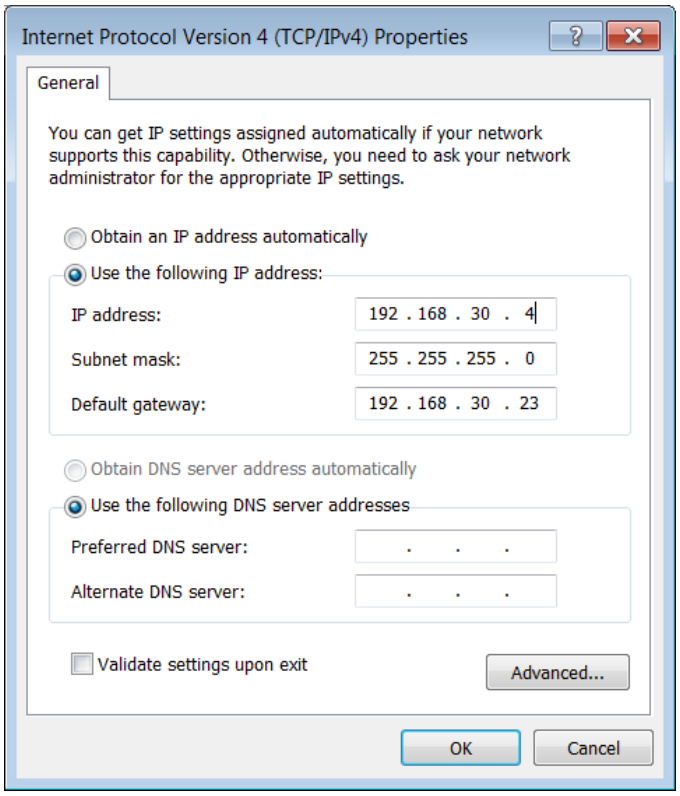


Figura 4.72. Configuración Dirección IP PC Práctica #18

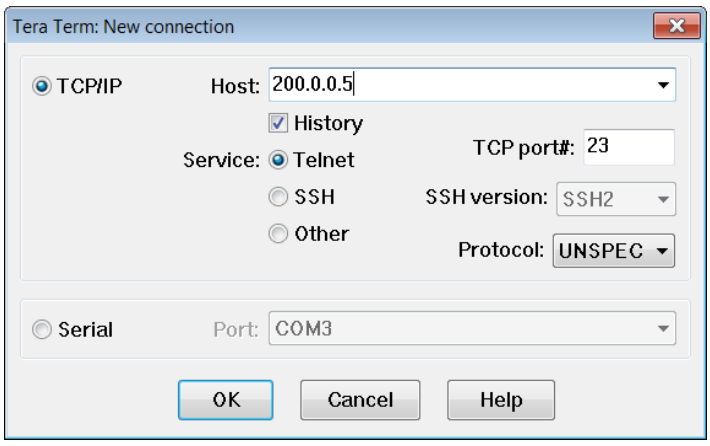


Figura 4.73. TeraTerm Conexión TELNET Router 1 Práctica #18

2.- Nos pedirá la contraseña: “espe” para poder acceder al Router. La Figura 4.74. Es la imagen de Acceso Remoto al Switch.

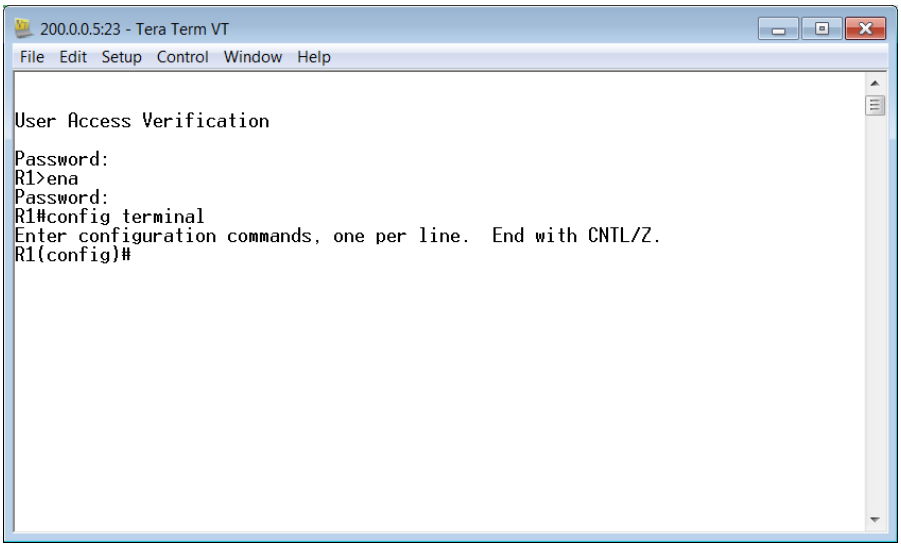


Figura 4.74. Conexión TELNET R1 Práctica #18

4.19.2.12. Prueba Acceso TELNET R2

1.- Ingresamos al programa TERATERM, ponemos el protocolo TELNET la dirección IP 200.0.0.6 y presionamos OK. La Figura 4.75. Nos muestra la Configuración IP del Computador. Mientras que la Figura 4.76. Nos muestra la pantalla de Conexión para acceso TELNET.

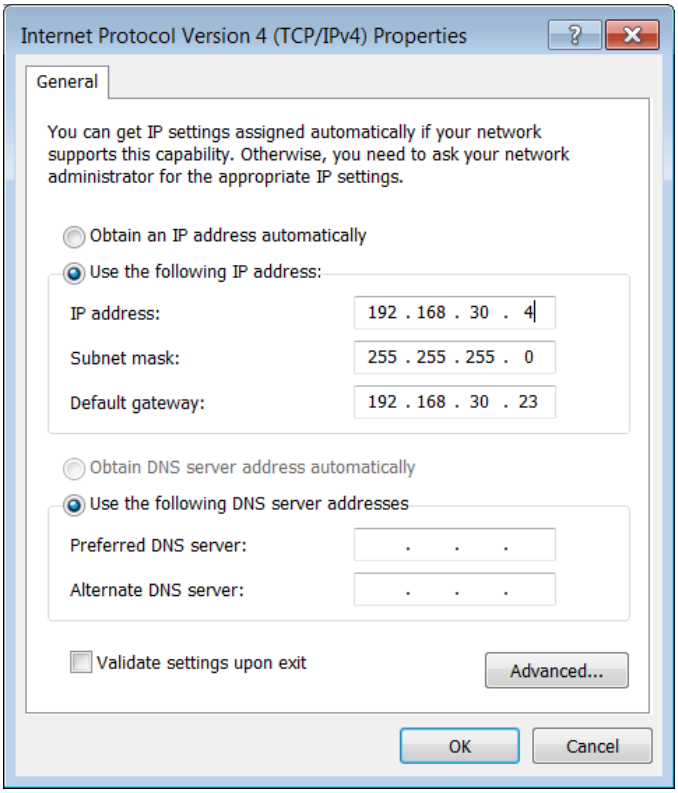


Figura 4.75. Configuración Dirección IP PC Práctica #18

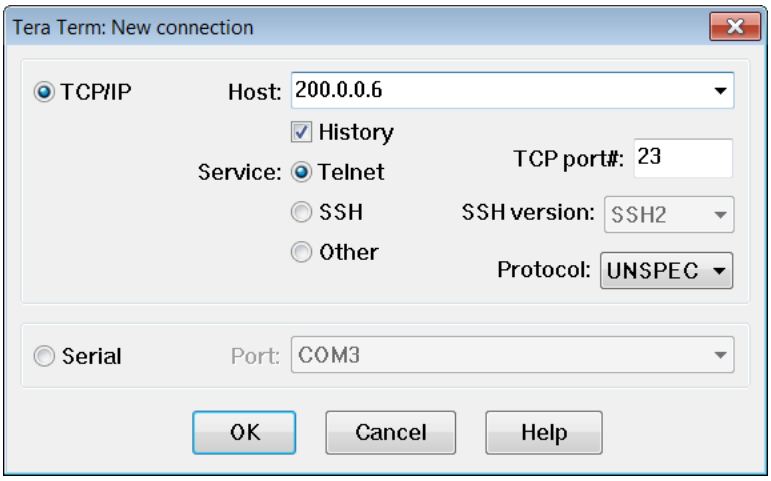


Figura 4.76. TeraTerm Conexión TELNET Router 2 Práctica #18

2.- Nos pedirá la contraseña: “espe” para poder acceder al Router.

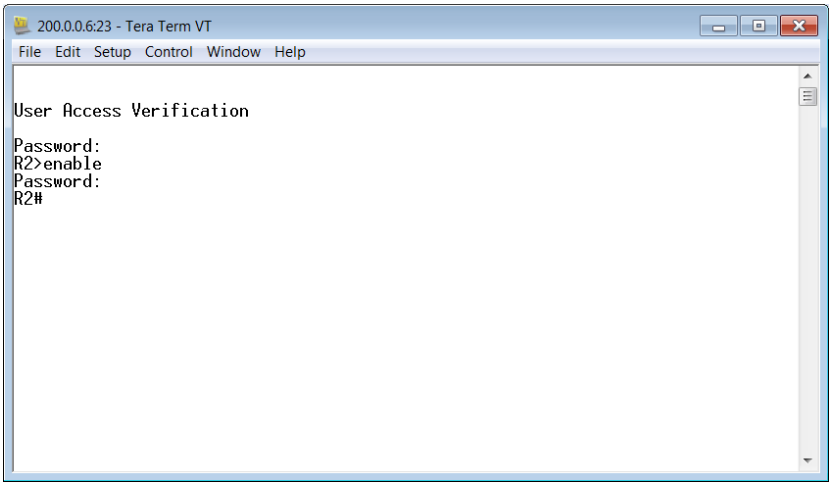


Figura 4.77. Conexión TELNET R2 Práctica #18

4.19.2.13. Pruebas de Conectividad

PRUEBA CONECTIVIDAD EMPLEADO 1 A GERENTE 3

```
C:\Users\redes pc>ping 192.168.20.4

Haciendo ping a 192.168.20.4 con 32 bytes de datos:
Respuesta desde 200.0.0.6: Red de destino inaccesible.
Respuesta desde 200.0.0.6: Red de destino inaccesible.
Respuesta desde 200.0.0.6: Red de destino inaccesible.
Respuesta desde 200.0.0.6: Red de destino inaccesible.

Estadísticas de ping para 192.168.20.4:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
```

PRUEBA CONECTIVIDAD GERENTE 3 A EMPLEADO 1

```
C:\Users\FOCH>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time=2546ms TTL=124
Reply from 192.168.1.2: bytes=32 time=9ms TTL=124
Reply from 192.168.1.2: bytes=32 time=9ms TTL=124
Reply from 192.168.1.2: bytes=32 time=9ms TTL=124

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 9ms, Maximum = 2546ms, Average = 643ms
```

PRUEBA CONECTIVIDAD GERENTE 1 A GERENTE 3

```
C:\Users\redes pc>ping 192.168.20.2

Haciendo ping a 192.168.20.2 con 32 bytes de datos:
Respuesta desde 200.0.0.6: Red de destino inaccesible.
Respuesta desde 200.0.0.6: Red de destino inaccesible.
Respuesta desde 200.0.0.6: Red de destino inaccesible.
Respuesta desde 200.0.0.6: Red de destino inaccesible.

Estadísticas de ping para 192.168.20.2:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
```

PRUEBA CONECTIVIDAD GERENTE 3 A GERENTE 1

```
C:\Users\FOCH>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:
Reply from 192.168.2.2: bytes=32 time=9ms TTL=124
Reply from 192.168.2.2: bytes=32 time=9ms TTL=124
Reply from 192.168.2.2: bytes=32 time=9ms TTL=124
Reply from 192.168.2.2: bytes=32 time=9ms TTL=124

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 9ms, Maximum = 9ms, Average = 9ms
```

PRUEBA CONECTIVIDAD GERENTE 1 A ADMINISTRADOR 3

```
C:\Users\redes pc>ping 192.168.30.4

Haciendo ping a 192.168.30.4 con 32 bytes de datos:
Respuesta desde 200.0.0.6: Red de destino inaccesible.
Respuesta desde 200.0.0.6: Red de destino inaccesible.
Respuesta desde 200.0.0.6: Red de destino inaccesible.
Respuesta desde 200.0.0.6: Red de destino inaccesible.

Estadísticas de ping para 192.168.30.4:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
```

PRUEBA CONECTIVIDAD ADMINISTRADOR 3 A GERENTE 1

```
C:\Users\FOCH>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:
Reply from 192.168.2.2: bytes=32 time=10ms TTL=124
Reply from 192.168.2.2: bytes=32 time=9ms TTL=124
Reply from 192.168.2.2: bytes=32 time=9ms TTL=124
Reply from 192.168.2.2: bytes=32 time=9ms TTL=124

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 9ms, Maximum = 10ms, Average = 9ms
```

4.20. DESARROLLO PRÁCTICA #19 IMPLENTACIÓN DE UNA RED OPERATIVA IPv6 CON OSPFv3

4.20.1. Configuraciones/Direccionamiento

Direccionamiento:

DISPOSITIVO	Dirección IPv6 *Dirección IPv4*	Interfaz
Switch D-LINK SW1		
	2001:450:2002:E8::2	**Vlan 1**
	2800:270:0:A::10	**Vlan RED1**
	2800:270:0:B::10	**Vlan RED2**
ROUTER_ID	**1.1.1.1**	
Switch D-LINK SW2		
	2001:450:2002:E9::2	**Vlan 1**
	2800:270:0:C::10	**Vlan RED1**
	2800:270:0:D::10	**Vlan RED2**
ROUTER_ID	**3.3.3.3**	
Router CISCO 2800		
	2001:450:2002:E8::1	**ETHERNET 0**
	2001:450:2002:E9::1	**ETHERNET 1**
ROUTER_ID	**2.2.2.2**	
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:C::20	**Ethernet**
PC5	2800:270:0:D::20	**Ethernet**
PC6	2800:270:0:D::21	**Ethernet**

Usuario y Password SSH:

SW1

Usuario: PCAD1

Password: espe

SW2

Usuario: PCAD2

Password: espe

Usuario y Password TELNET:

Password: espe

4.20.2. Procedimiento

4.20.2.1. Configuración IPv6 D-Link DGS-3627 SW1

1.- Accedemos al Switch 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.
```

2.- 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.
```

3.- 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.
```

4.-Creamos las interfaces vía configuración web. La Figura 4.78. Nos muestra la Configuración de la interface RED1. Mientras que la Figura 4.79. Nos muestra la Configuración de la interface RED2.

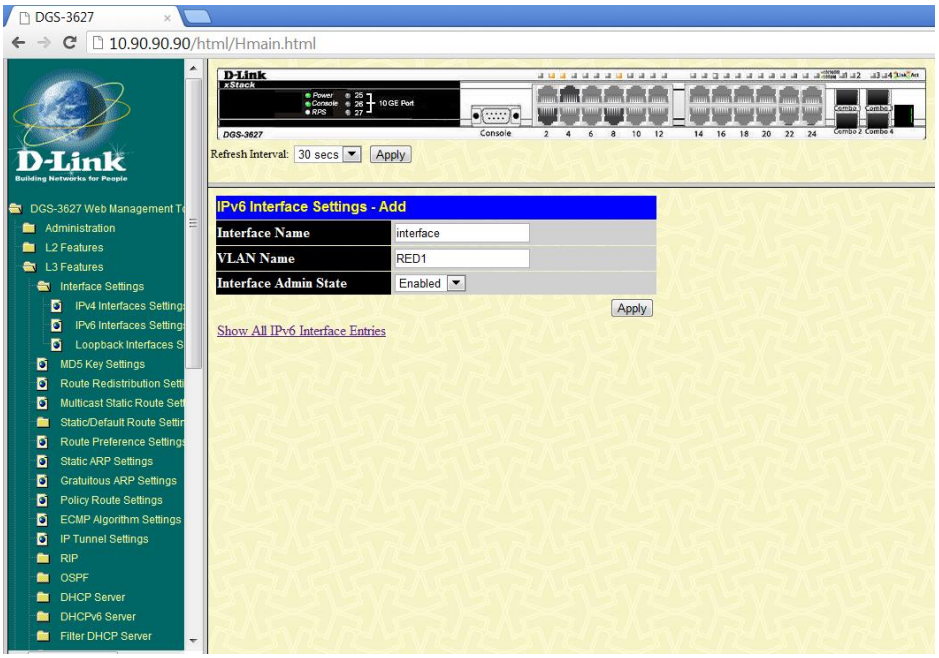


Figura 4.78. Configuración Interface RED 1 Switch D-Link SW1 Práctica #19

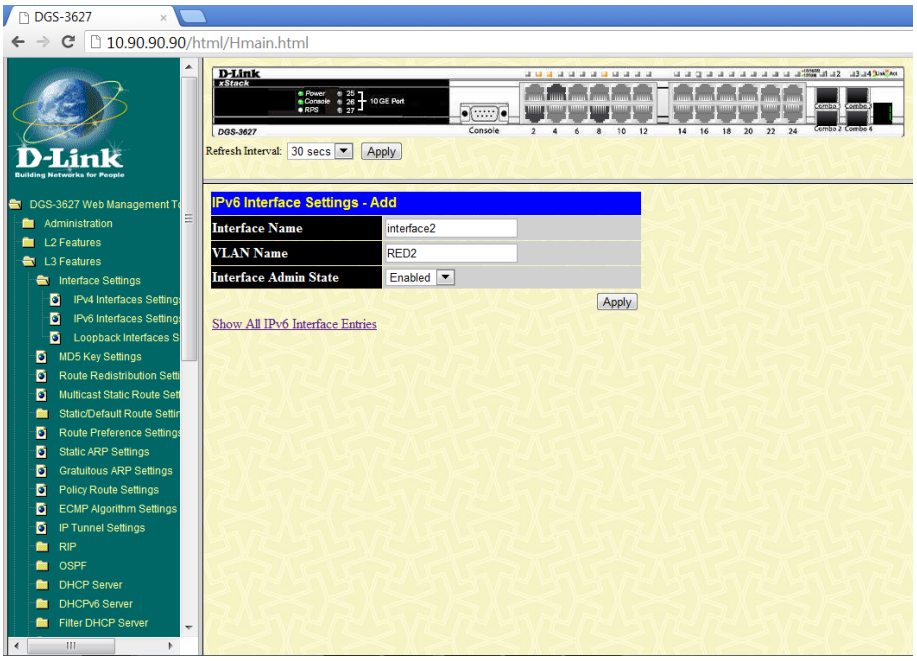


Figura 4.79. Configuración Interface RED 2 Switch D-Link SW1 Práctica #19

5.- Configuramos la IP de la VLAN “RED1”, “RED2”.

```
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.
```

6.- Configuramos la IP de la VLAN 1

```
DGS-3627:admin#config ipif System ipv6 ipv6address 2001:450:2002:e8::2/64
Command: config ipif System ipv6 ipv6address 2001:450:2002:E8::2/64

Success.
```

7.- Configuramos el protocolo de enrutamiento OSPFv3.

7.1.- Habilitamos el protocolo de enrutamiento OSPFv3.

```
DGS-3627:admin#enable ospfv3
Command: enable ospfv3

Success.
```

7.2.- Creación del área 10.10.10.10 para OSPF.

```
DGS-3627:admin#create ospfv3 area 10.10.10.10 type normal
Command: create ospfv3 area 10.10.10.10 type normal

Success.
```

```
DGS-3627:admin#config ospfv3 ipif interface area 10.10.10.10
Command: config ospfv3 ipif interface area 10.10.10.10

Success.

DGS-3627:admin#config ospfv3 ipif interface2 area 10.10.10.10
Command: config ospfv3 ipif interface2 area 10.10.10.10

Success.

DGS-3627:admin#config ospfv3 ipif System area 10.10.10.10
Command: config ospfv3 ipif System area 10.10.10.10

Success.
```

7.3.- Configuramos el Router_id.

```
DGS-3627:admin#config ospfv3 router_id 1.1.1.1
Command: config ospfv3 router_id 1.1.1.1

Success.
```

7.4.- Habilitamos OSPF en la interfaces del Switch.

```
DGS-3627:admin#config ospfv3 ipif interface state enable
Command: config ospfv3 ipif interface state enable

Success.

DGS-3627:admin#config ospfv3 ipif interface2 state enable
Command: config ospfv3 ipif interface2 state enable

Success.

DGS-3627:admin#config ospfv3 ipif System state enable
Command: config ospfv3 ipif System state enable

Success.
```

8.- Para configurar SSH en el Switch D-link 3627 utilizamos los siguientes comandos.

```
DGS-3627:admin#create account admin PCAD1
Command: create account admin PCAD1

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

DGS-3627:admin#config ssh user PCAD1 authmode password
Command: config ssh user PCAD1 authmode password

Success.
```

8.1.- 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.
```

8.2.- Habilitamos SSH en el Switch.

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

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

4.20.2.2. Configuración IPv6 D-Link DGS-3627 SW2

1.- Accedemos al Switch 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.
```

2.- 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.
```

3.- 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.
```

4.-Creamos las interfaces vía configuración web. La Figura 4.80. Nos muestra la Configuración de la interface RED1. Mientras que la Figura 4.81. Nos muestra la Configuración de la interface RED2.

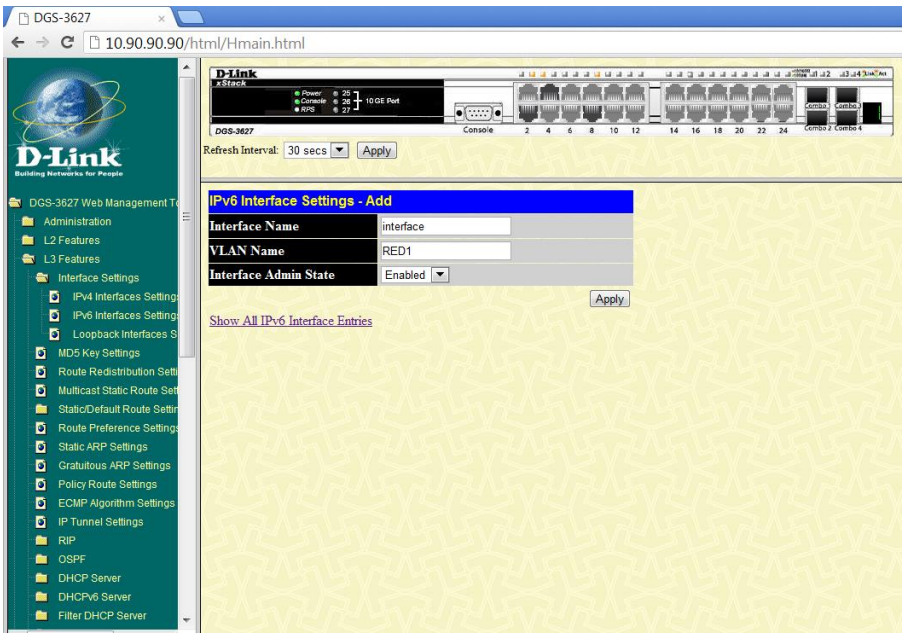


Figura 4.80. Configuración Interface RED 1 Switch D-Link SW2 Práctica #19

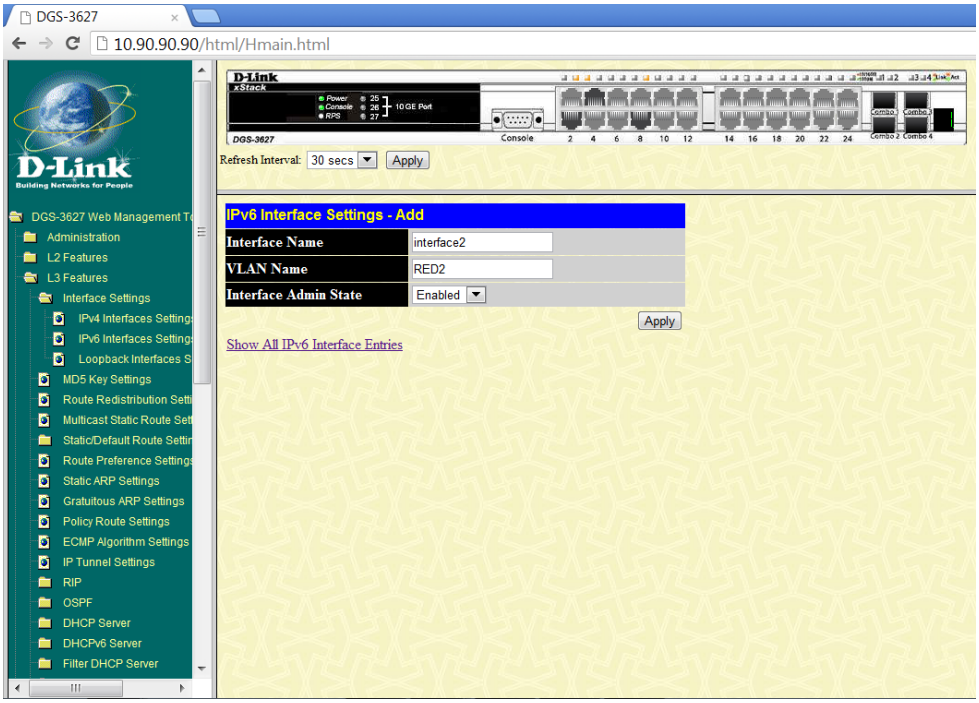


Figura 4.81. Configuración Interface RED 2 Switch D-Link SW2 Práctica #19

5.- Configuramos la IP de la VLAN “RED1”, “RED2”.

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

Success.
```

```
DGS-3627:admin#config ipif interface2 ipv6 ipv6address 2800:270:0:d::10/64
Command: config ipif interface2 ipv6 ipv6address 2800:270:0:D::10/64

Success.
```

6.- Configuramos la IP de la VLAN 1

```
DGS-3627:admin#config ipif System ipv6 ipv6address 2001:450:2002:e9::2/64
Command: config ipif System ipv6 ipv6address 2001:450:2002:E9::2/64

Success.
```

7.- Configuramos el protocolo de enrutamiento OSPFv3.

7.1.- Habilitamos el protocolo de enrutamiento OSPFv3.

```
DGS-3627:admin#enable ospfv3
Command: enable ospfv3

Success.
```

7.2.- Creación del área 10.10.10.10 para OSPF.

```
DGS-3627:admin#create ospfv3 area 10.10.10.10 type normal
Command: create ospfv3 area 10.10.10.10 type normal

Success.
```

```
DGS-3627:admin#config ospfv3 ipif interface area 10.10.10.10
Command: config ospfv3 ipif interface area 10.10.10.10

Success.

DGS-3627:admin#config ospfv3 ipif interface2 area 10.10.10.10
Command: config ospfv3 ipif interface2 area 10.10.10.10

Success.

DGS-3627:admin#config ospfv3 ipif System area 10.10.10.10
Command: config ospfv3 ipif System area 10.10.10.10

Success.
```

7.3.- Configuramos el Router_id.

```
DGS-3627:admin#config ospfv3 router_id 3.3.3.3
Command: config ospfv3 router_id 3.3.3.3

Success.
```

7.4.- Habilitamos OSPF en la interfaces del Switch.

```
DGS-3627:admin#config ospfv3 ipif interface state enable
Command: config ospfv3 ipif interface state enable

Success.

DGS-3627:admin#config ospfv3 ipif interface2 state enable
Command: config ospfv3 ipif interface2 state enable

Success.

DGS-3627:admin#config ospfv3 ipif System state enable
Command: config ospfv3 ipif System state enable

Success.
```

8.- Para configurar SSH en el Switch D-link 3627 utilizamos los siguientes comandos.

```
DGS-3627:admin#create account admin PCAD2
Command: create account admin PCAD2

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

DGS-3627:admin#config ssh user PCAD2 authmode password
Command: config ssh user PCAD2 authmode password

Success.
```

8.1- 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.
```

8.2.- Habilitamos SSH en el Switch.

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

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

4.20.2.3. Configuración CISCO 2000 R1

1.- Accedemos al Router configuramos, habilitamos el acceso vía telnet y ponemos password para acceder al modo privilegiado.

```
R1(config)#enable secret espe
R1(config)#line vty 0 4
R1(config-line)#password espe
R1(config-line)#login
```

2.- Configuramos la dirección IPv6 de las interfaces Fast Ethernet.

```
R1(config)#interface f0/0
R1(config-if)#ipv6 address 2001:450:2002:e8::1/64
R1(config-if)#no shutdown
```

```
R1(config)#interface f0/1
R1(config-if)#ipv6 address 2001:450:2002:e9::1/64
R1(config-if)#no shutdown
```

4.- Configuramos el protocolo de Enrutamiento OSPFv3 área 10.10.10.10.

4.1.- Habilitamos OSPF en el Router.

```
R1(config)#ipv6 unicast-routing
R1(config)#ipv6 router ospf 1
R1(config-rtr)#router-id 2.2.2.2
R1(config-rtr)#auto-cost
```

4.2.- Habilitamos OSPF en las interfaces del Router.

```
R1(config)#interface f0/0
R1(config-if)#ipv6 ospf 1 area 10.10.10.10
R1(config-if)#exit
R1(config)#interface f0/1
R1(config-if)#ipv6 ospf 1 area 10.10.10.10
```

4.20.2.4. Configuración PC1, PC2, PC3, PC4, PC5, PC6

La Figura 4.82. Nos indica la configuración de IPv6 en la PC1

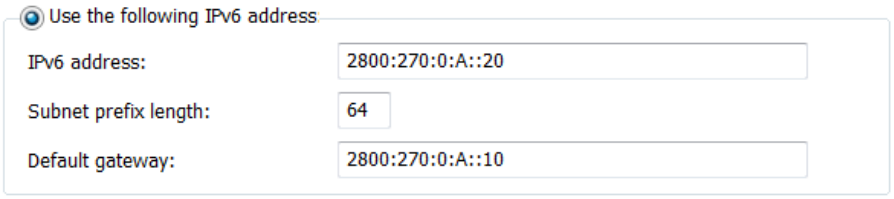


Figura 4.82. Configuración IPv6 PC 1 Práctica #19

La Figura 4.83. Nos indica la configuración de IPv6 en la PC2

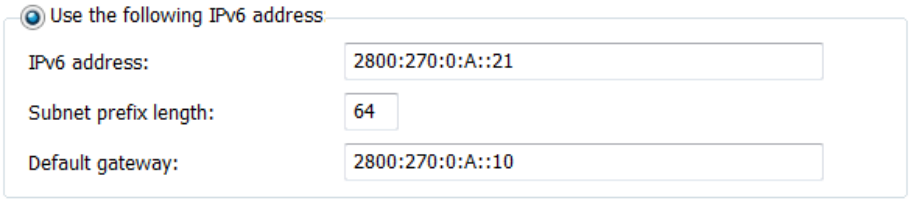


Figura 4.83. Configuración IPv6 PC 2 Práctica #19

La Figura 4.84. Nos indica la configuración de IPv6 en la PC3

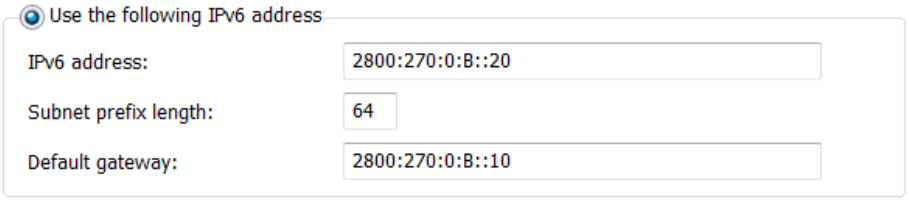


Figura 4.84. Configuración IPv6 PC 3 Práctica #19

La Figura 4.85. Nos indica la configuración de IPv6 en la PC4

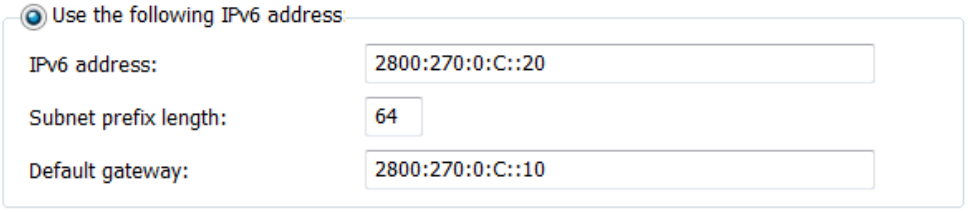


Figura 4.85. Configuración IPv6 PC 4 Práctica #19

La Figura 4.86. Nos indica la configuración de IPv6 en la PC5

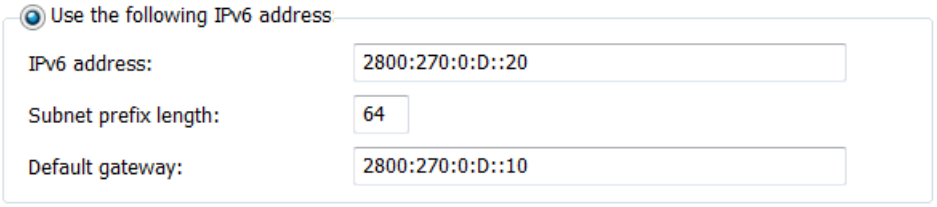


Figura 4.86. Configuración IPv6 PC 5 Práctica #19

La Figura 4.87. Nos indica la configuración de IPv6 en la PC6

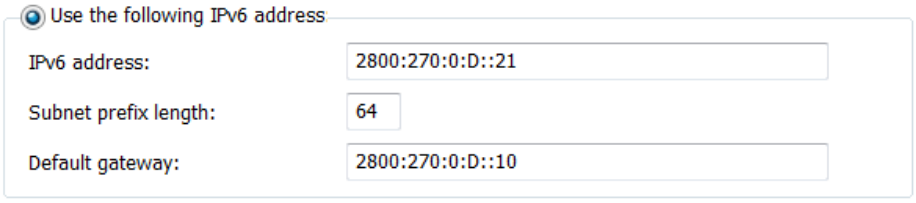


Figura 4.87. Configuración IPv6 PC 6 Práctica #19

4.20.2.5. Tablas de Enrutamiento IPv6

SW1:

```
DGS-3627:admin#show ipv6route
Command: show ipv6route

IPv6 Prefix: 2001:450:2002:E8::/64              Protocol: Local   Metric: 1
Next Hop   : ::                                 IPIF    : System

IPv6 Prefix: 2001:450:2002:E9::/64              Protocol: OSPFv3  Metric: 11
Next Hop   : FE80::21F:9EFF:FE17:DF0            IPIF    : System

IPv6 Prefix: 2800:270:0:A::/64                  Protocol: Local   Metric: 1
Next Hop   : ::                                 IPIF    : interface

IPv6 Prefix: 2800:270:0:B::/64                  Protocol: Local   Metric: 1
Next Hop   : ::                                 IPIF    : interface2

IPv6 Prefix: 2800:270:0:C::/64                  Protocol: OSPFv3  Metric: 21
Next Hop   : FE80::21F:9EFF:FE17:DF0            IPIF    : System

IPv6 Prefix: 2800:270:0:D::/64                  Protocol: OSPFv3  Metric: 21
Next Hop   : FE80::21F:9EFF:FE17:DF0            IPIF    : System
```

SW2:

```
DGS-3627:admin#show ipv6route
Command: show ipv6route

IPv6 Prefix: 2001:450:2002:E8::/64              Protocol: OSPFv3  Metric: 11
Next Hop   : FE80::21F:9EFF:FE17:DF1            IPIF    : System

IPv6 Prefix: 2001:450:2002:E9::/64              Protocol: Local   Metric: 1
Next Hop   : ::                                 IPIF    : System

IPv6 Prefix: 2800:270:0:A::/64                  Protocol: OSPFv3  Metric: 21
Next Hop   : FE80::21F:9EFF:FE17:DF1            IPIF    : System

IPv6 Prefix: 2800:270:0:B::/64                  Protocol: OSPFv3  Metric: 21
Next Hop   : FE80::21F:9EFF:FE17:DF1            IPIF    : System

IPv6 Prefix: 2800:270:0:C::/64                  Protocol: Local   Metric: 1
Next Hop   : ::                                 IPIF    : interface

IPv6 Prefix: 2800:270:0:D::/64                  Protocol: Local   Metric: 1
Next Hop   : ::                                 IPIF    : interface2
```

R1:

```
R1#show ipv6 route
IPv6 Routing Table - 10 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       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
C   2001:450:2002:E8::/64 [0/0]
     via ::, FastEthernet0/0
L   2001:450:2002:E8::1/128 [0/0]
     via ::, FastEthernet0/0
C   2001:450:2002:E9::/64 [0/0]
     via ::, FastEthernet0/1
L   2001:450:2002:E9::1/128 [0/0]
     via ::, FastEthernet0/1
O   2800:270:0:A::/64 [110/11]
     via FE80::219:5BFF:FEF0:7240, FastEthernet0/0
O   2800:270:0:B::/64 [110/11]
     via FE80::219:5BFF:FEF0:7240, FastEthernet0/0
O   2800:270:0:C::/64 [110/11]
     via FE80::219:5BFF:FEF0:7D80, FastEthernet0/1
O   2800:270:0:D::/64 [110/11]
     via FE80::219:5BFF:FEF0:7D80, FastEthernet0/1
```

4.20.2.6. Accesos Remotos y Pruebas de Conectividad

ACCESO REMOTO A SW1

La Figura 4.88. Nos muestra la pantalla de Autenticación para el Acceso SSH, mientras que la Figura 4.89. Es la imagen de Acceso Remoto al Switch.

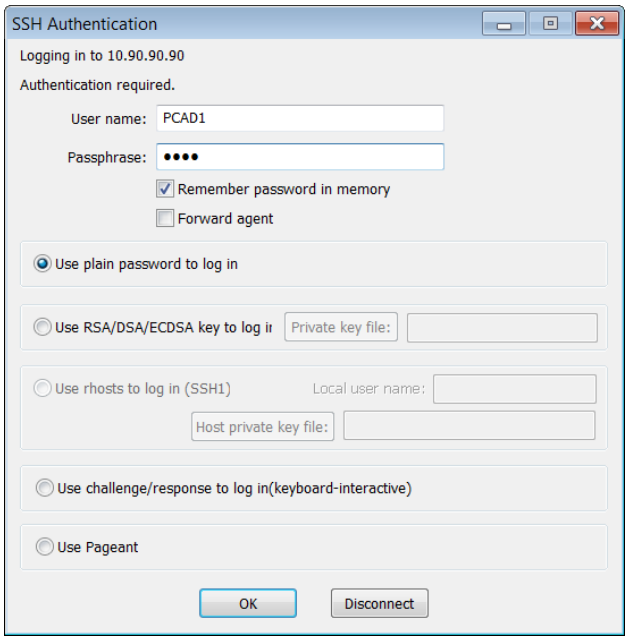


Figura 4.88. Autenticación SSH SW1 Práctica #19

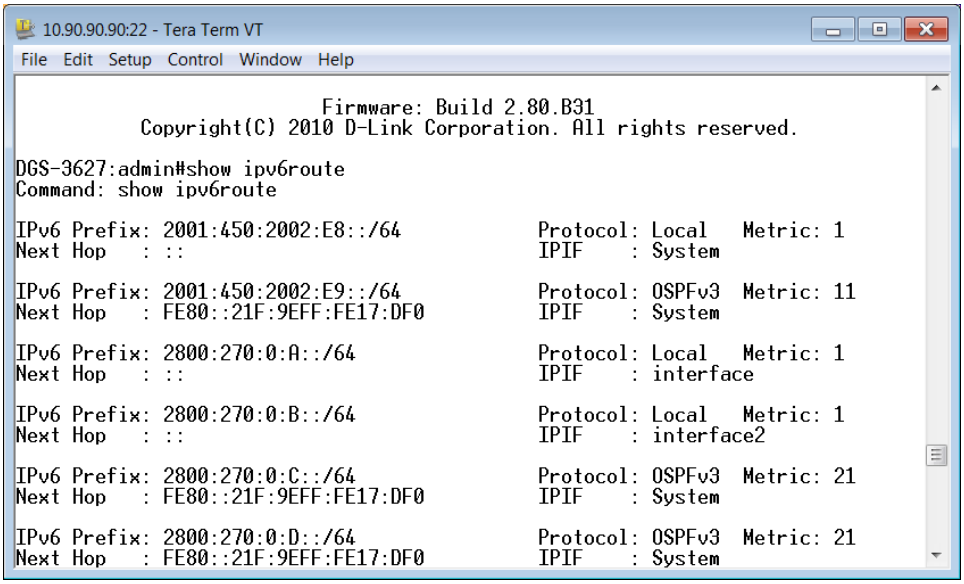


Figura 4.89. Conexión SSH SW1 Práctica #19

ACCESO REMOTO A SW2

La Figura 4.90. Nos muestra la pantalla de Autenticación para el Acceso SSH, mientras que la Figura 4.91. Es la imagen de Acceso Remoto al Switch.

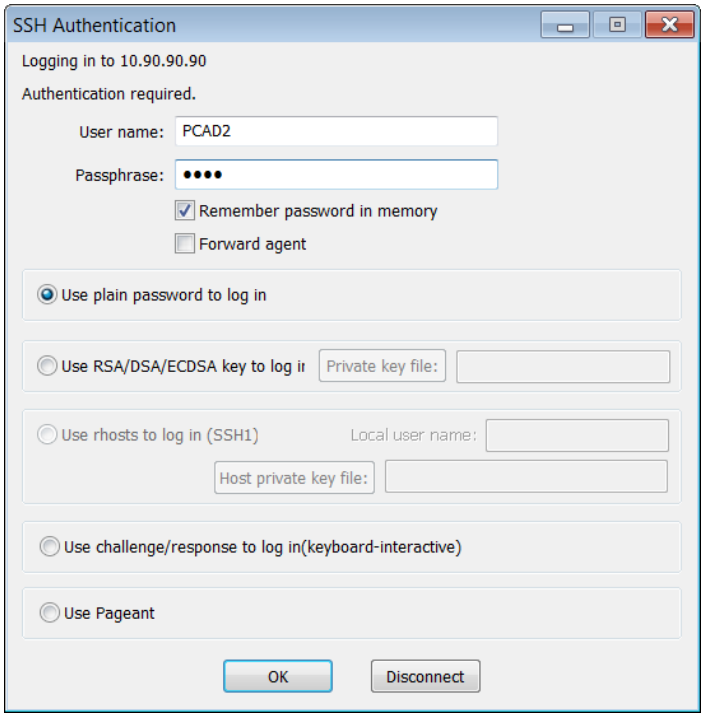


Figura 4.90. Autenticación SSH SW2 Práctica #19

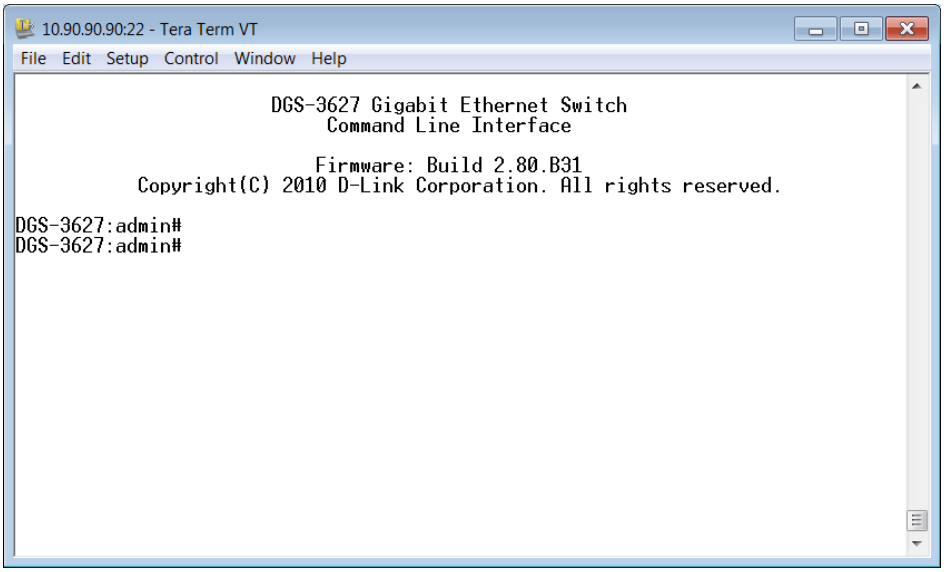


Figura 4.91. Conexión SSH SW1 Práctica #19

ACCESO REMOTO A R1

Ingresamos al programa PUTTY y ponemos la dirección IPV6, el tipo de conexión TELNET y presionamos "OPEN". La Figura 4.92. Nos muestra la Pantalla de configuración de TELNET. Mientras que la Figura 4.93. Nos muestra la imgen de acceso remoto al Router.

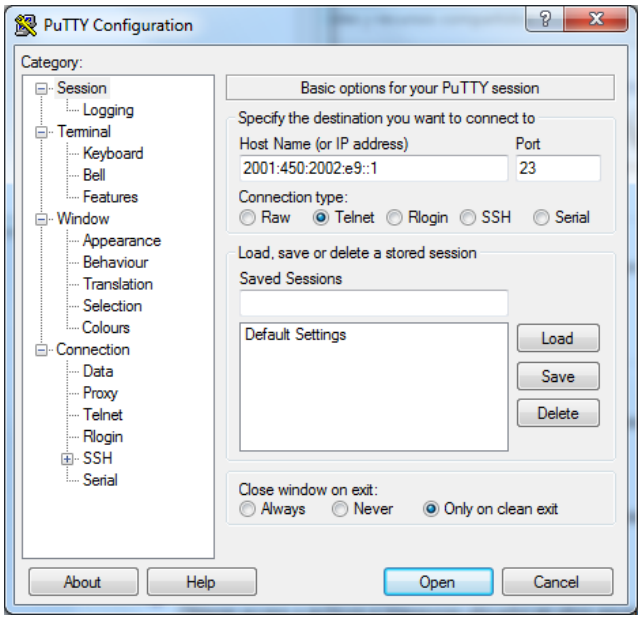


Figura 4.92. PUTTY Configuración TELNET Práctica #19

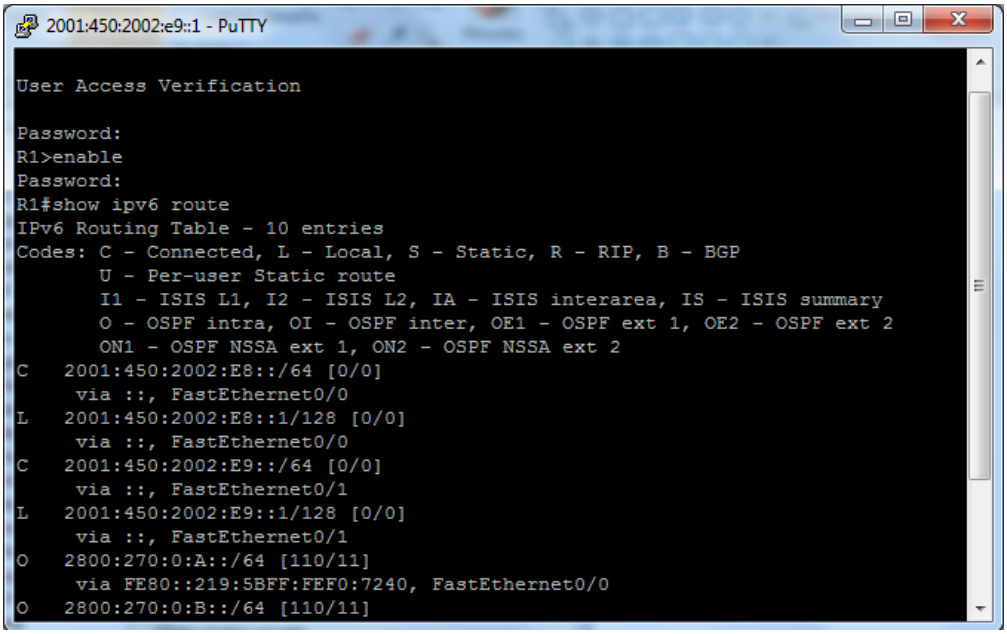


Figura 4.93. Conexión TELNET R1 Práctica #19

CONECTIVIDAD PC1 CON PC4

```
C:\Users\redes pc>ping 2800:270:0:C::20

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

Estadísticas de ping para 2800:270:0:c::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 PC1 CON PC6

```
C:\Users\redes pc>ping 2800:270:0:d::20

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

Estadísticas de ping para 2800:270:0:d::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 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
```

CAPÍTULO 5

CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

Del Proyecto de Tesis "Desarrollo de Guías Prácticas para el Diseño e Implementación de Redes Locales Virtuales, Autenticación y Acceso Remoto en un entorno LAN" se concluyó lo siguiente:

- 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.

5.2. RECOMENDACIONES

Del Proyecto de Tesis "Desarrollo de Guías Prácticas para el Diseño e Implementación de Redes Locales Virtuales, Autenticación y Acceso Remoto en un entorno LAN" se recomienda lo siguiente:

- 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.

REFERENCIAS BIBLIOGRÁFICAS

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

- [2] "*VLAN*", http://es.kioskea.net/contents/internet/vlan.php3, Enero 2012

- [3] "*MODELO JARARQUÍCO*", http://aprenderedes.com/2006/06/las-tres-capas-del-modelo-jerarquico-de-cisco/, Enero 2012

- [4] *"802.1Q*", http://allnetworking.blogspot.com/2008/03/8021q.html, Enero 2012

- [5] *"STP*", http://www.netstorming.com.ar/2009/11/02/protocolo-spanning-tree/, Enero 2012

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

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

- [8] *"802.1X*" http://es.wikipedia.org/wiki/IEEE_802.1X, Enero 2012

- [9] "*RADIUS*" http://searchsecurity.techtarget.com/definition/RADIUS, Enero 2012

- [10] *"Quality of Service 802.1p*", http://www.dte.us.es/personal/mcromero/masredes/docs/SMARD.0910.qos.pdf, Enero 2012

- [11] "*DHCP*", http://www.ordenadores-y-portatiles.com/dhcp.html, Junio 2012

- [12] "*SNMP Simple Network Management Protocol*", http://www.uazuay.edu.ec/estudios/sistemas/teleproceso/apuntes_1/snmp.htm, Junio 2012

- [13] "*IPv6*", http://www.ipv6.es/es-ES/Paginas/Index.aspx, Junio 2012

- [14] "*RIPng*", http://www.redescisco.net/v2/art/direccionamiento-basico-con-ipv6-ripng/, Junio 2012

- [15] "*IPv6 TUNNELING*", http://www.ixp.net.co/contenido/ccit/articles-10/articles-13/14-sample-data-articles/100-modelo-de-conexion-ipv6-nap-colombia, Junio 2012

- [16] "*OSPFv3*", http://www.networkworld.com/subnets/cisco/050107-ch9-ospfv3.html, Junio 2012

FECHA DE ENTREGA

El día 22 de Enero de 2013, en la ciudad de Sangolquí, firma en constancia de la entrega del presente Proyecto de Grado titulado "DESARROLLO DE GUÍAS PARA EL DISEÑO E IMPLEMENTACIÓN DE REDES LOCALES VIRTUALES, ACCESO REMOTO Y AUTENTICACIÓN EN UN ENTORNO LAN", en calidad de Autor el Sr. Mauricio Javier Tufiño Coloma estudiante de la carrera de Ingeniería Electrónica en Redes y Comunicación de Datos, y recibe por parte del Departamento de Eléctrica y Electrónica el Director de Carrera, Redes y Comunicación de Datos, el Señor Doctor Vinicio Carrera.

_____

Mauricio Javier Tufiño Coloma

CI: 1721535548

_____

Doctor Vinicio Carrera

Director de Carrera, Redes y Comunicación de Datos