UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

"IMPLEMENTACIÓN DEL PROGRAMA DE INTERCONECTIVIDAD ACADÉMICO DE CISCO EN UN LABORATORIO DE REDES"

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

INGENIERO EN COMPUTACIÓN
E
INGENIERO EN TELECOMUNICACIONES

P R E S E N T A N:

SERGIO AARÓN CERVANTES ARROYO
DAVID ANTONIO MONROY GUERRERO

DIRECTOR DE TESIS:
DR. VÍCTOR RANGEL LICEA

CD.UNIVERSITARIA, MÉXICO, D.F. SEPTIEMBRE 2008

Agradecimientos

Agradecemos a nuestras familias por el apoyo recibido no sólo durante el transcurso de nuestras carreras profesionales, sino también por habernos formado, educado y haber tomado cuidado de nosotros desde el momento de nuestro nacimiento hasta el día de hoy, como en el caso de Margarita Gonzalez Vazquez por parte de David Antonio Monroy Guerrero quien siempre lo apoyó y le brindo cariño incondicionalmente. De parte de Sergio Aarón Cervantes Arroyo, quiero agradecer a mis padres, el Sr. Sergio Eduardo Cervantes Gómez y a la Sra. Ma. Del Carmen Arroyo Gómez por su cariño y apoyo incondicional. También se agradece a la DGAPA por el proyecto PE103807.

INDICE

Lista de Figuras

Lista de Tablas

CAPÍTULO 1

INTRODUCCIÓN

1.1 Antecedentes

Hoy en día las redes de datos y la interconexión de redes juegan un papel indispensable para el buen funcionamiento y la operación en muchos sectores productivos y educativos del país, como son:

Industrias o empresas, bancos, escuelas, universidades, institutos, dependencias del gobierno, ejército, la marina, entre muchos más. La interconexión de redes locales de computadoras (alámbricas e inalámbricas), es una necesidad en las organizaciones modernas, no se podría pensar, por ejemplo en una empresa en la que sus diferentes departamentos tuvieran cada uno sus propias redes, pero sin poderse comunicar y sin compartir recursos o información con otras áreas de la misma organización.

La importancia de contar con este tipo de equipo de interconectividad, adquiere mayor relevancia debido a que en los últimos años ha habido un enorme desarrollo tecnológico en el área de telecomunicaciones; ejemplo de esto son la convergencia de diferentes redes de voz y datos a redes con tecnología IP, las redes inalámbricas locales, redes inalámbricas de banda ancha y su integración con las redes de telefonía celular, el uso de Internet para redes privadas (VPN), etc.

Sin embargo, los grandes avances tecnológicos han hecho que muchas instituciones educativas de nivel superior se estén quedando muy rezagadas en cuanto a la enseñanza de esta área de interconectividad y que sus planes de estudio en carreras afines, como son Ingeniería en Telecomunicaciones, Ingeniería en Computación o Licenciatura en Informática, se enfoquen solamente a cursos teóricos. En particular, en la Facultad de Ingeniería de la UNAM, se imparten las carreras de Ingeniería en Telecomunicaciones e Ingeniería en Computación, y ambas tienen un módulo de salida similar: Redes de Telecomunicaciones y Redes y Seguridad, respectivamente. No obstante, se tiene una carencia en lo referente a equipos de telecomunicaciones enfocados a la

interconexión e integración de redes locales de computadoras con redes generales más amplias (WAN, MAN) por medio de equipos y enlaces de telecomunicaciones. Para apoyo de las actividades académicas en el módulo de Redes y Seguridad, existen actualmente varios laboratorios equipados con computadoras aisladas y también Conectadas en redes locales (LAN) que permiten llevar a cabo prácticas enfocadas principalmente a la programación de computadoras y al funcionamiento de las mismas. Así como también, los únicos equipos con los que cuenta el módulo de Redes de Telecomunicaciones, para propósitos didácticos, son dos routers (3com Superstack) que fueron donados, los cuales tienen una antigüedad de más de 10 años, y que no tienen la capacidad para funcionar con las nuevas tecnologías convergentes IP para la transmisión de voz, datos y video.

Existen por supuesto en la UNAM, una amplia variedad de equipos de telecomunicaciones de la DGSCA para las redes de computadoras utilizadas en las labores administrativas. Pero estos equipos están en servicio y los alumnos no tienen posibilidad de llevar a cabo prácticas diarias en los mismos para configurarlos y familiarizarse con su funcionamiento.

Si bien, por más de 5 años la Facultad de Ingeniería, ha intentado adquirir esta tecnología de interconectividad con recursos propios en los Departamentos de Ingeniería en Telecomunicaciones, y Computación, el costo asociado y la falta de especialistas en Redes han hecho que esta nueva tecnología no se pueda poner en práctica y que nuestros egresados estén en desventaja con algunos centros de educación superior privados que ya cuentan con esta tecnología, como lo son:

Centro Cultural Universitario Justo Sierra, ITESM, UNITEC, Universidad Anáhuac, Universidad de las Américas, Universidad del Valle de México, Universidad ICEL, Universidad La Salle, Universidad Panamericana, Universidad Tecnológica Americana, Universidad Tecnológica de México[1], entre otras.

En estas instituciones privadas, sus programas de estudio en carreras afines, ya contienen parte del Programa Académico de Interconectividad (Networking Academy Program, denominado NETACAD), el cual permite al profesionista obtener las diversas certificaciones de validez internacional que ofrecen algunas compañías de telecomunicaciones destacadas como Cisco, Nortel, etc. Estas certificaciones son de gran importancia para el futuro ingeniero y la mayoría de ellos, especialmente los de la carrera de Ing. en Telecomunicaciones, tienen que pagar por realizar estos cursos y prácticas didácticas en otras instituciones, por más de 6 meses para que puedan tener un nivel más competitivo en esta área.

Como antecedente al proyecto esta el despliegue del laboratorio de redes del Posgrado en Ciencia e Ingeniería de la Computación del Instituto de Matemáticas Aplicadas y Sistemas (IIMAS) de la UNAM[2], el cual ha proporcionado la infraestructura para realizar pruebas y diseño de prácticas de laboratorio e infraestructuras propuestas en el cual se impartió durante el semestre escolar 2008-2, una clase a un grupo de 4 alumnos que aprendieron a configurar equipos de Red Switch y Routers CISCO por los autores del presente proyecto, basándonos en el programa de networking y el material de certificación CCNA.

1.2 Definición del problema

El mundo actual está completamente interconectado, requiere de fuertes habilidades profesionales de conocimientos tanto teóricos como habilidades técnicas para asegurar el desarrollo y el progreso. La Facultad de Ingeniería en su afán por mantener la excelencia y la mejora continua de la enseñanza ha tenido lagunas debido a los extremadamente rápidos, agitados y continuos cambios que la tecnología experimenta día a día. Este es el caso de las redes de datos, campo en el cual, la tecnología ha avanzado a pasos gigantescos en periodos cortos de tiempo logrando con ello la necesidad de profesionistas provistos de habilidades y herramientas específicas en la materia.

El campo instrumental y de implementación de proyectos de infraestructura de telecomunicaciones, ha sido descuidado debido a los enfoques excesivamente teóricos, lo cual brinda la oportunidad de aplicar todos los conceptos, habilidades y herramientas que el ingeniero adquiere en su etapa formativa.

El caso que nos ocupa es controlado por diferentes agentes que determinan el camino de la tecnología, organismos de normalización y fabricantes, habiendo estos últimos acaparado el control del rumbo de las redes de datos. Es importante señalar que existen tecnologías que dominan el mercado y para un mejor desempeño profesional del futuro ingeniero, es necesario contar con certificaciones, las cuales requieren de conocimientos tanto teóricos como prácticos para que de esta esta forma puedan ofrecer sus servicios de manera competente. Lamentablemente estos cursos se caracterizan por ser de alto costo y actualmente la Facultad de Ingeniería no cuenta con la capacidad para que sus alumnos cuenten con este tipo de competencias profesionales, dejándolos en desventaja frente aquellos egresados de instituciones que de hecho tienen vínculos comerciales con empresas que imparten este tipo de programas.

1.2.1 Alcance

El alcance de este proyecto está determinado por dos factores. Primero las restricciones tecnológicas debidas a los recursos disponibles del laboratorio y segundo, la profundidad, la cual estará limitada a nivel de configuración requerido para preparar un examen de certificación inicial de redes según el *Networking Academic Program* con las reservas que el primer factor impone. Debido a este segundo factor, solamente se detallará el entorno de certificación de nivel asociado e ilustrando de manera general los niveles Profesional y Experto ya que no son objetivo de la presente tesis.

Debido a las carencias de equipamiento no se podrá desarrollar actividades para la configuración, estudio y puesta en marcha de protocolos de transporte *SONET/SDH, ISDN* ni *Frame Relay.*

1.2.2 Método

Se diseñaran actividades específicas para prácticas de laboratorio, utilizando como referencia los modelos *OSI*, *TCP/IP*, *IEEE 802* y el *Networking Academy Program*; haciendo énfasis en este último, se adaptaran las metodologías de configuración y disposición de los equipos de red a las necesidades de la Facultad.

El orden de las prácticas para un adecuado entendimiento deberá comenzar por la descripción de los equipos de red, Switches y Routers, sus características electrónicas y lógicas, una vez cubierto se hará la descripción de la normatividad básica de cableado estructurado para la interconexión de los dispositivos, el nivel de enlace de datos será determinado mediante el estudio de las funciones básicas y extendidas del Switch y los protocolos de comunicación definidos en IEEE 802.3, IEEE 802.1Q, IEEE 802.1D y el VTP (VLAN Trunking Protocol), el nivel de red y de transporte se basará en el modelo TCP/IP en el cual se hará énfasis en el direccionamiento IP y la configuración de los protocolos de enrutamiento RIP (Routing Information Protocol) y OSPF (Open Shortest Path First), para el nivel de transporte se tratarán tópicos de configuración como ACL (Access Control List) y NAT (Network Address Translation), el nivel de aplicación se atacará mediante la implementación de un servidor de TFTP, acceso remoto y pruebas de conectividad mediante TELNET.

1.3 El Laboratorio de Redes de Telecomunicaciones de la Facultad de Ingeniería[3]

Como ya se mencionó anteriormente el laboratorio de redes de telecomunicaciones desde principios del 2008 dispone solamente de infraestructura limitada que no es capaz de utilizarse para la impartición de un adecuado nivel de cátedra en tecnologías de la información, es por ello que a partir del proyecto PAPIME PE103807, al cual se le agradece por su colaboración en el presente trabajo, esta siendo posible la actualización del Laboratorio Multidisciplinario de Redes de Telecomunicaciones, de acuerdo a los cambios tecnológicos que demanda el país, en el cual los alumnos de licenciatura de las carreras de Ing. en Telecomunicaciones e Ing. en Computación, así como también los alumnos del Posgrado de Ingeniería Eléctrica, en el módulo de Redes de Telecomunicaciones podrán hacer uso de la infraestructura implementada para realizar sus proyectos de investigación, tareas, prácticas didácticas e incluso su tesis.

1.4 Objetivo y Contribuciones

El objetivo primordial del proyecto es contribuir con la adaptación del Programa Académico de Interconectividad (NETACAD) didáctico mediante el diseño de prácticas de laboratorio, implementación de infraestructura tecnológica adecuada para preparar un examen de certificación CCNA.

Con la integración e implementación de la tecnología, también se contribuye con la elaboración de material didáctico de apoyo, para las diferentes asignaturas del modulo de Redes de Telecomunicaciones para las siguientes asignaturas:

- Redes de Datos I
- Redes de Datos II
- Telefonía Digital
- Redes Inalámbricas y Móviles
- Redes Inalámbricas Avanzadas
- Análisis y Diseño de Redes
- Temas Especiales de Redes Inalámbricas de Banda Ancha

1.5 Estructura de la Tesis

La presente tesis se compone de 6 capítulos, a continuación se da una breve descripción de los mismos.

El Capítulo 2 consiste de la descripción tecnológica de los protocolos que intervienen en la implementación del proyecto de tesis.

En el Capítulo 3 se abarca la descripción de los panoramas de certificación vigentes dentro de la industria de las redes de telecomunicaciones.

El cuarto Capítulo 4 se detalla la descripción tecnológica de los equipos a utilizar, características electrónicas, de hardware y software utilizado por los switches y routers.

El quinto Capítulo es un compendio de documentación generada para el desarrollo de prácticas de laboratorio basadas en los conocimientos necesarios para preparar una certificación con sus respectivas limitaciones impuestas por la ausencia de dispositivos de hardware y facilidades de software.

El sexto Capítulo consta de los resultados, comentarios finales y conclusiones desarrolladas tras la implementación del proyecto así como un compendio de configuraciones que son las soluciones explícitas a cada una de las actividades propuestas en el capítulo correspondiente.

CAPÍTULO 2

DESCRIPCIÓN DE PROTOCOLOS

2.1 Nivel de Enlace de Datos y sus Protocolos

El nivel de Enlace de Datos es el segundo nivel del modelo de referencia OSI, su función es fácil de describir pero nada trivial de realizar, consiste en el envío de datos que recibe del nivel de red (nivel 3) de un equipo origen hacia el nivel de red de un equipo destino; este envío de datos se realiza conceptualmente como si ambos equipos estuvieran directamente conectados por un canal de comunicación (un cable coaxial ó una línea telefónica por ejemplo). Para llevar a cabo la tarea antes mencionada el nivel de Enlace de Datos se vale de una serie de protocolos para realizar la transferencia de datos y manejar adecuadamente los errores que pudieran presentarse.

2.1.1 Ethernet y Fastethernet

Ethernet es una especificación con una larga historia, se basa en un tipo de red (ALOHANET) creada en 1970 por Norm Abramson y su equipo de trabajo en la Universidad de Hawai, Abramson utilizó ondas de radio para transmitir información de una computadora a otra situadas en diferentes islas, el problema de esa red estaba en su protocolo MAC, el cual funcionaba de la siguiente forma: un equipo enviaba datos sin verificar si el canal estaba ocupado (si había una portadora) o no, y esperaba por un aviso de parte del equipo destinatario informando la recepción satisfactoria de la información, si después de un cierto tiempo no se recibía dicho aviso, el equipo origen espera un tiempo aleatorio y vuelve a enviar la información; la eficiencia de esta red era baja y si se tuvieran muchos equipos tratando de enviar información la red podría caerse fácilmente.

También en el año de 1970, un estudiante del Massachusetts Institute of Technology (MIT) llamado Robert Metcalfe estudió el funcionamiento de ALOHANET y considero que podría ser mejorado si un equipo verificaba la existencia de una portadora ocupando el canal antes de tratar de enviar datos a través de él. Dicha consideración fue el principio de la tesis doctoral de Robert Metcalfe y el principio

de funcionamiento de CSMA/CD, en 1972 Metcalfe se mudo a California y entró a trabajar a Xerox, Robert Metcalfe junto con un ayudante de la Universidad de Stanford crearon la primer implementación de Ethernet.

En el año de 1979 se crea una alianza entre DEC, Intel y Xerox (conocida como DIX) para impulsar el desarrollo tecnológico de Ethernet, la cuál todavía tenía mucho por crecer. Gracias a esto la IEEE crea el estándar 802 orientado a la implementación de LAN's y MAN's, además aprueba el estándar 802.3 (CSMA/CD) comúnmente conocido como Ethernet.

Conforme las tecnologías electrónicas de los dispositivos fueron mejorando al igual que los protocolos utilizados en el nivel de Enlace de Datos, se crearon nuevos estándares con tasas de transferencia muy altas, para el caso de Ethernet sus predecesores son FastEthernet y GigabitEthernet.

La siguiente figura muestra en que niveles de modelo de referencia OSI esta situado el estándar IEEE 802.3 (Ethernet) y el IEEE 802.2 (LLC).

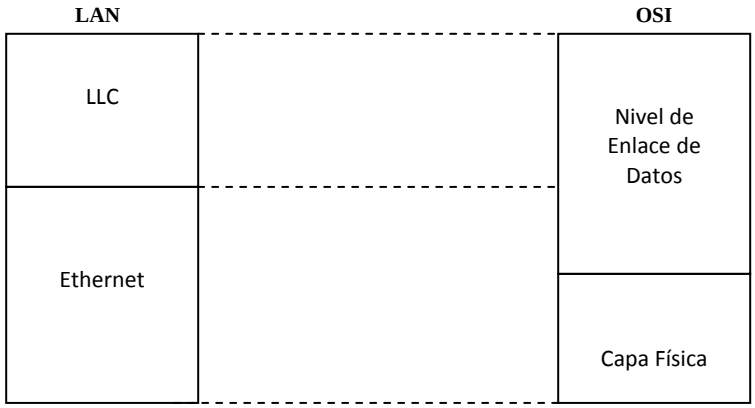


Figura 2.1 - Relación del Modelo de Referencia OSI con los estándares IEEE 802.2 y 802.3[4].

Capa Física

El estándar de Ethernet no sólo define las características del nivel de Enlace de Datos, sino que también define características del nivel Físico tales como las eléctricas, mecánicas, operacionales y funcionales.

Cabe mencionar que para enviar los datos, estos se codifican por medio de la codificación Manchester, disminuyendo así los posibles errores por ambigüedad y ofreciendo un reloj confiable incluido en los propios datos.

2.1.1.1 Métodos de Acceso

Un método de acceso es aquél que nos sirve de interfaz entre el nivel Físico (nivel 1) y el nivel de Enlace de Datos (nivel 2), nos permite encapsular la información proveniente del nivel de Red para enviarla al nivel Físico y también nos permite realizar el proceso inverso.

Existen diversos métodos de acceso (también conocidos como medios de acceso), dentro del proyecto IEEE 802 hay 7 métodos de acceso cada uno con su respectivo medio físico asociado, los siguientes son algunos ejemplos:

- CSMA/CD
- Token Ring
- Token Bus
- DQDB

A continuación se describe el funcionamiento de CSMA/CD ya que es el método de acceso más representativo.

CSMA/CD: Es un protocolo de Control de Acceso al Medio (MAC), su funcionamiento se describe en los siguientes puntos.

- Un equipo verifica si el canal esta ocupado (si existe una portadora).
- Si el canal no está ocupado comienza a transmitir.
- Si el canal está ocupado el equipo sigue escuchando el canal en espera de que se libere.
- Si durante la transmisión de datos ocurre una colisión (que otro equipo comience a transmitir) el equipo que estaba transmitiendo inicialmente deja de hacerlo en lugar de enviar la trama completa en vano y espera un intervalo de tiempo para volver a revisar el canal y transmitir.

2.1.1.2 Trama

Algunos protocolos encapsulan los datos que se quieren enviar a través de una red (payload), también agregan campos de información que ellos necesitan para su correcto funcionamiento y lo almacenan en una unidad de información llamada *trama*.

El siguiente es el formato general de una trama:

Figura 2.2 - Formato General de una Trama

A continuación se describe cada uno de los campos.

Encabezado: El encabezado de una trama suele estar formado por los siguientes elementos:

- *Preámbulo:* Sirve para sincronizar y estabilizar el medio físico antes de comenzar la transmisión de los datos.

- *Direcciones de Destino y Origen:* Son las direcciones MAC de los equipos destino y origen respectivamente.

- *Bits propios del protocolo:* Pueden ser para distinguir un subtipo de protocolo, un protocolo de un nivel superior, la longitud del payload o algunas otras características que necesite el protocolo para su funcionamiento.

Payload: Es la información que lleva la trama, esta información es interpretada siempre por un protocolo de nivel superior al protocolo que lleve dicho payload, un protocolo que tenga un cierto payload por lo general no necesita saber nada acerca de la información del mismo, si acaso, debe de contar los bits para calcular el checksum, el CRC ó para utilizar algún otro método de detección de errores.

Cola: Está formada de campos utilizados para completar el tamaño mínimo o máximo de una trama para un protocolo determinado, también son utilizados para almacenar valores tales como el CRC, el Checksum y el Frame Check Sequence que, como ya se mencionó antes, son utilizados en la detección de errores.

Ethernet utiliza una trama llamada trama Ethernet, sus elementos son mostrados en la figura 2.3.

Preámbulo	SOF	Dirección de Destino	Dirección de Origen	Longitud de la trama	Payload	Pad	Checksum

Figura 2.3 – Formato de una trama Ethernet[5]

2.1.1.3 Tasas de Transferencia

En la sección 2.2.1 se hablo de Ethernet y de sus predecesores, FastEthernet y GigabitEthernet, es importante destacar que las tasas de transferencia de estos protocolos varían dependiendo de ciertas características físicas, tales como el ruido eléctrico, la temperatura del cable, el tipo de cable entre otros, respecto al tipo de cable, existen tecnologías tales como cable coaxial, fibra óptica, cable UTP y STP y cada una tiene sus propios rangos de tasas de transferencia.

2.1.1.4 Medios de Transmisión

Un medio de transmisión es el medio físico por el cual se transmite la información de un nodo de la red a otro, es conocido también como el canal de comunicación.

La siguiente tabla muestra algunos de los medios de transmisión que se han utilizado para Ethernet así como los medios que se utilizan actualmente.

Tabla 2.1 - Tipos y características de algunos medios de transmisión.

Tipo	Tipo de cable	Longitud máx/segmento	Velocidad de transmisión
10Base5	Coaxial grueso (Thick)	500 m	10 Mbps
10Base2	Coaxial delgado (Thin)	185 m	10 Mbps
10BaseT	UTP	100 m	10 Mbps
10BaseF	Fibra Óptica	2000 m	10 Mbps
100BaseT	UTP	100 m	100 Mbps
100BaseF	Fibra Óptica	100 m	100 Mbps
1000BaseT	UTP	100 m	1000 Mbps

2.1.2 Conceptos del nivel de Enlace

El nivel de Enlace de Datos cumple con las siguientes dos funciones principales:

- Proveer de acceso al medio a una serie de equipos terminales de datos (DCE).
- Proveer una interfaz confiable y estándar para dar servicios al nivel de Red.

2.1.2.1 Sub-capas MAC y LLC

Como se mencionó en el punto anterior, el nivel de Enlace de Datos tiene dos propósitos principales, para los cuales tiene dos sub-capas encargados de satisfacer dichas funciones.

Sub-capa MAC
Esta sub-capa realiza la gestión o control de acceso al medio, para esto, se apoya de un protocolo de acceso al medio (Por ejemplo Ethernet, FasthEthernet, entre otros), además se encarga del control de errores y el control de flujo.

Sub-capa LLC
Esta sub-capa sirve como interfaz, entre el protocolo de acceso al medio (protocolo MAC) que se este utilizando y los protocolos del nivel de Red, debido a que es utilizada por varios protocolos MAC simplifica y mejora la comunicación entre las capas de Enlace y la de Red. También puede brindar servicios orientados a conexión y envío de acuses de recibido para ofrecer una conexión más confiable.

2.1.2.2 LAN Switching

El LAN Switching son todos aquellos mecanismos para la distribución y acceso de la información y al medio de red local respectivamente. Los protocolos LAN se encuentran dentro de la capa de enlace de datos del Modelo de Referencia OSI y entre ellos podemos encontrar:

- IEEE 802.3 Ethernet
- IEEE 802.5 Token Ring
- IEEE 802.11 Wi-Fi

En esta práctica se abordarán los mecanismos de configuración para el caso de la Tecnología Ethernet.

El IEEE 802.3 es un protocolo de enlace de datos, sus funciones son las de proveer los mecanismos para el acceso a los recursos de la red y asignar un direccionamiento físico. Esta tecnología de red local se basa en una comunicación no orientada a conexión y brinda un mecanismo de detección de errores (FCS).

Una red Ethernet esta constituida por una topología de Bus, actualmente utiliza el cable UTP como medio de transmisión y conectores RJ-45.

Como dispositivos de interconexión, Ethernet puede utilizar de capa física como Regeneradores y/o Hubs o bien, de capa de enlace como Puentes (bridges) y/o Switches. Un Switch es un Puente ultipuestos caracterizado por disponer de una tabla de direccionamiento físico, comúnmente llamada tabla de direccionamiento MAC, esta tabla relaciona los puertos del dispositivo con las direcciones físicas de las máquinas directamente conectadas. La ventaja de los dispositivos de capa 2 sobre los de capa 1 es el agrupamiento en dominios de colisión.

Los dominios de colisión tienen las siguientes características:

- Las colisiones se reducen únicamente a los dispositivos existentes en el mismo dominio.
- Mejoran el rendimiento de la red discriminando el tráfico.

El Switch decide entre reenviar tramas Ethernet o descartarlas (filtrarlas) mediante la identificación de direcciones MAC de origen y de destino que lee de cada trama que recibe.

Existen diferentes tipos de direcciones MAC:

- *Unicast:* Identifica a un solo dispositivo.

- *Broadcast:* Su valor es FFFF.FFFF.FFFF.FFFF (en notación hexadecimal), cuando un Switch recibe una trama con esta dirección la reenvía por todos sus puertos y todos los dispositivos lo escuchan. Esta dirección solo puede ser escrita en el campo de destino de una trama.

- *Multicast:* Determinan que la trama tiene como destino un conjunto de dispositivos.

Funciones de un Switch

Un Switch tiene 3 funciones:

- Aprendizaje (learning).
- Reenvío (forwarding).
- Prevención de conexiones redundantes.

Aprendizaje

La decisión entre reenviar o descartar una trama está en función del contenido de la tabla de direcciones físicas de la que dispone el Switch. Un Switch aprende automáticamente las direcciones MAC de la red dinámicamente conforme va leyendo los encabezados de las tramas que recibe e incluye estas MAC en su tabla de direcciones MAC. El Switch sólo incluye las direcciones MAC de origen porque sabe con certeza por cual interfaz recibió la trama con esa dirección de origen.
Algoritmo de aprendizaje de direcciones MAC en el Switch.

1. Llega una trama al Switch.
2. Si la MAC de origen del encabezado de la trama no está en la tabla de direcciones MAC, el Switch la incluye.
3. Decide que hacer con la trama (si debe reenviarla o descartarla).

Cabe mencionar que cuando el Switch recibe una trama con una dirección MAC de destino que no tiene en su tabla de direcciones, la reenvía por todas sus interfaces.

Reenvío y filtrado

Para determinar cuándo reenviar una trama, el Switch usa la tabla MAC address table. Cada vez que llega una trama al Switch, la examina y decide entre reenviar la trama por alguna de sus interfaces, o si la debe descartar.

La decisión de reenviar la trama o descartarla depende simplemente de la dirección MAC de destino del encabezado, si la MAC de destino se encuentra en la misma interfaz por donde el Switch recibió la trama, entonces no hay necesidad de reenviar la trama por alguna interfaz y esta es descartada.

Prevención de conexiones redundantes

Un Switch crea un ambiente libre de lazos con otros Switches mediante el uso del Spanning Tree Protocol (STP). Tener enlaces físicos redundantes aumenta la disponibilidad de la LAN y por medio del STP se evita que la lógica que utiliza el Switch (para reenvío de tramas) permita a la información viajar en un circuito (lazo) de forma indefinida, congestionando así la LAN.

2.1.2.3 IEEE 802.1D (Spanning Tree Protocol)

El STP es un protocolo que nos ayuda a prevenir que una trama viaje por tiempo indefinido en algún lazo que exista en la Red congestionando esta última. Su funcionamiento es muy sencillo, se trata de poner en estado de reenvio o de bloqueo a todos los puertos de los Switches, de tal manera que si hubiera una delta de Switches en la Red, un puerto de esa delta quedará bloqueado, evitando así que una trama pueda viajar por la delta indefinidamente, a continuación se describe más detalladamente.

Funcionamiento de STP

- Todos los Switches de la Red comienzan a enviar mensajes (llamados BPDU's) a los demás Switches donde informan su ID de prioridad, mientras menor sea el ID, mayor será la capacidad del Switch en cuanto a características físicas.

- Cuando un Switch recibe un mensaje BPDU de algún otro Switch, compara el ID del mensaje con su propio ID, si el ID del mensaje es mayor que el suyo, deja de reenviar el mensaje que recibió y continua enviando el suyo, de lo contrario, si el ID del mensaje que le llego es menor que el suyo, deja de enviar el suyo y reenvía el mensaje que recibió.

- Al final, todos los Switches están reenviando periódicamente el mensaje de aquel con menor ID, este Switch es denominado Switch Raíz (Root Switch) y todas sus interfaces se fijan en modo de reenvío.

- Una vez elegido el Switch Raíz, los Switches continúan enviando mensajes pero ahora para calcular las distancias más cortas de sus interfaces al Switch Raíz, para esto utilizan los costos asignados a cada interfaz de la Red por las cuales tienen que pasar para llegar al Switch Raíz, para cada segmento de la Red se van fijando interfaces en estado de reenvío siempre y cuando sean las de menor costo para llegar desde un Switch determinado al Switch Root.

- En una conexión punto a punto entre dos Switches, de las dos interfaces (una por Switch) que forman la conexión, se elige la de menor costo al Switch Raíz y se bloquea la otra, tomando todas estas consideraciones, cuando STP se estabiliza, sólo habrá un camino por el cual podrán viajar las tramas en la Red de un equipo de origen a uno de destino, teniendo como ventaja que si falla alguna Ruta, STP calculará si se puede reparar el daño modificando el estado de alguna interfaz bloqueada a estado de reenvío.

2.1.2.4 VLAN y VLAN troncales

Las Virtual LAN's (VLAN's), son en esencia dominios de difusión y facilitan al Switch separar sus puertos en diferentes grupos para mantener el tráfico de cada grupo de manera independiente, sin la necesidad de utilizar varios Switches o Hubs.

La siguiente figura muestra gráficamente la distribución de equipos en las diferentes VLAN's que un Switch puede tener.

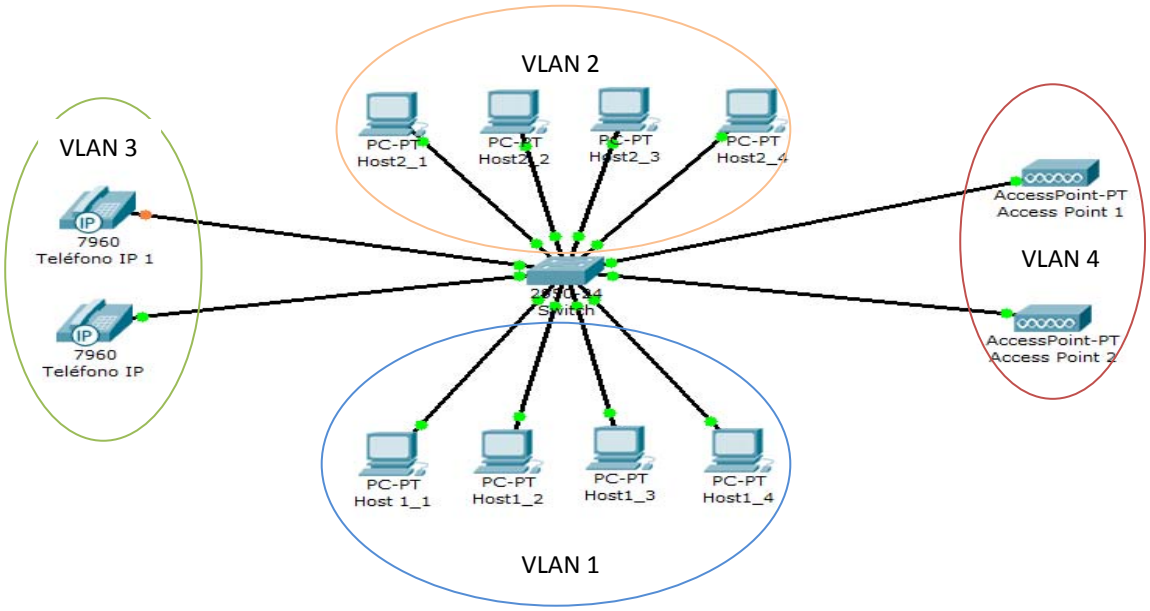


Figura 2.4 - Ejemplo de VLAN's en un Switch.

Características de la comunicación:

- Los Switches capa 2, reenvían tramas pertenecientes a dispositivos de la misma VLAN dentro de sí misma y no pueden hacerlo entre VLANs por ser en esencia dominios de difusión.
- Los Switches capa 3, pueden reenviar tramas entre dispositivos de diferentes VLANs.
- Los dispositivos de una VLAN, también son parte de la misma subred.

Por defecto los Switches CISCO tienen todos sus puertos en la VLAN 1 o VLAN nativa, y no es sino hasta que se crean más VLANs cuando el Switch requiere de hacer la diferencia entre tramas de distintas VLANs.

VLAN Trunking

Consiste del despliegue de VLANs sobre varios Switches transportando el tráfico de varias VLANs entre ellos. Gracias a esta herramienta, se pueden soportar varias VLANs con dispositivos conectados a distintos Switches. Los Switches son interconectados mediante la configuración de sus puertos como **puertos troncales**, los cuales serán como su nombre lo dice utilizados para transportar el tráfico de diferentes VLAN troncales.

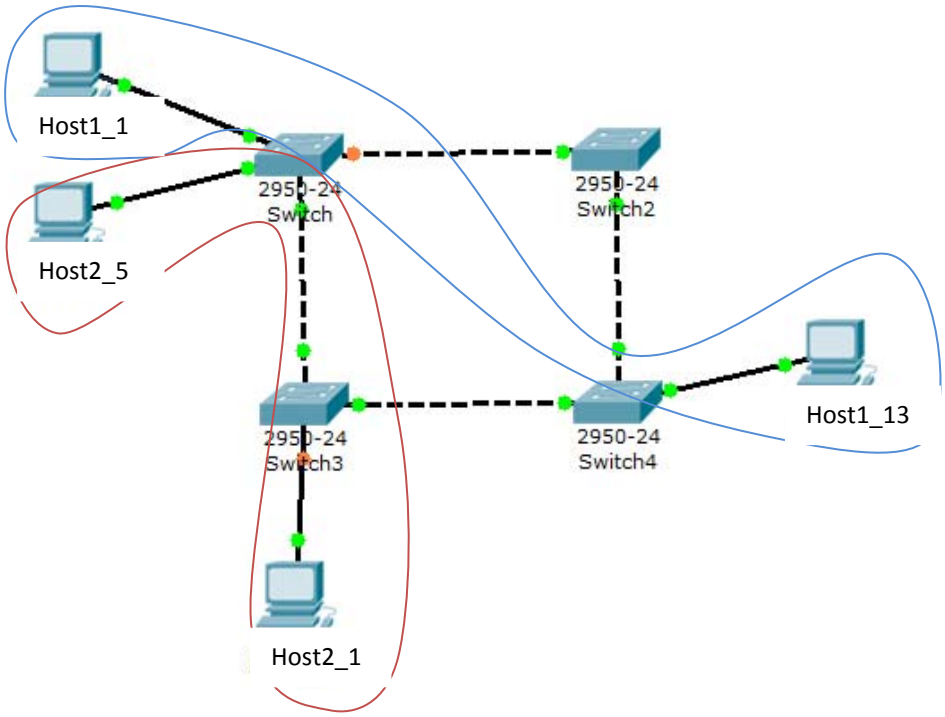


Figura 2.5 - VLANs Troncales

Para transportar el tráfico troncal, los puertos de interconexión de los Switches o puertos troncales utilizan un protocolo especifico, en el caso de los Switches CISCO utilizan el ISL por defecto, sin embargo, este es un protocolo propietario y no funciona si disponemos de equipos de otros fabricantes, por lo tanto, para contribuir con el avance de los sistemas abiertos, utilizaremos el protocolo dot1Q o mejor conocido como el IEEE 802.1Q, el cual sí es soportado por dispositivos de diferentes fabricantes debido a su naturaleza estándar.

2.1.2.5 IEEE 802.1Q

El IEEE 802.1Q es un protocolo que agrega un identificador a cada trama Ethernet tradicional, lo cual ocasiona que se tenga que re calcular el FCS, a diferencia del ISL de CISCO el cual determina un encapsulamiento específico. Es muy importante especificar que el dot1Q solamente es utilizado por Switches, bridges e interfaces Ethernet de los Routers, no por las tarjetas de red de las maquinas de la LAN debido a que se redefine un nuevo formato de encabezado para las tramas, el cual es imposible ser reconocido por las tarjetas Ethernet convencionales.

Sus características son las siguientes:

- No encapsula, solo adiciona un nuevo campo identificador en el encabezado de la trama Ethernet.
- La longitud del campo adicional es de 4 bytes.
- El identificador incluye un campo en el cual se específica el número de VLAN a la cual pertenece la trama.
- Se fuerza a recalcular el FCS.

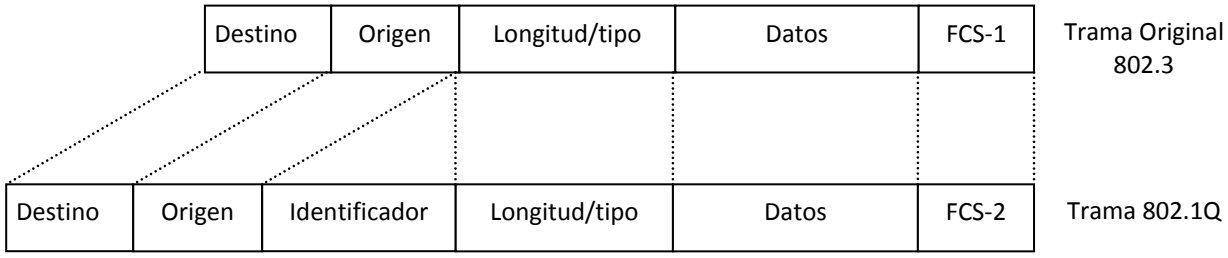


Figura 2.6 - Encabezado de la trama 802.1Q

2.1.2.6 VTP (VLAN Trunking Protocol)

VTP es el protocolo propietario de CISCO que facilita la configuración de VLANs en una red, determina 3 modos de operación:

- Servidor
- Cliente
- Transparente

Si un equipo ha sido configurado como servidor VTP, este deberá disponer de la información de todas las VLANs troncales y distribuirá dicha información por la red. Dado que puede haber varios niveles o zonas de administración, el servidor determina el alcance en el cual distribuirá las configuraciones de las VLANs, es decir el dominio VTP en el cual serán válidas.

Sus funciones son:

- Crear, modificar y eliminar VLANs.
- Originar avisos VTP reenviarlos por los puertos troncales.
- Guarda la configuración de VLANs en su NVRAM.

Un cliente VTP espera por la información de las VLANs troncales para guardarla en su configuración y poder trabajar con ellas, también las reenvía por sus puertos troncales, pero no es capaz de modificar la configuración.

Sus funciones son:

- Procesa los avisos recibidos y sincroniza la información de VLANs con otros Switches.
- Guarda la configuración de VLANs en su NVRAM.
- Reenviar los avisos VTP del servidor por los puertos troncales.

Un Switch en modo transparente, hace caso omiso a los avisos del servidor, pero los reenvía a través de sus puertos troncales.

Sus funciones son:

- Guarda la configuración de VLANs en su NVRAM.
- Puede crear, modificar y eliminar VLANs pero no distribuye los avisos por la red.
- Reenviar los avisos VTP del servidor por los puertos troncales.

Es importante mencionar que con los protocolos anteriores se logra la comunicación en el nivel de enlace, sin embargo y dado que cada VLAN es una diferente subred, la comunicación entre VLANs no se puede dar sin la intervención de un dispositivo de capa de red, es decir, se requiere de un Router para la comunicación entre VLANs, la implementación del Router consiste de la creación de unas sub-interfaces en la interfaz Fastethernet que conecta con el nivel de enlace, es decir con Switch principal. Dado que se transportará información de diferentes VLANs, este puerto deberá utilizar el protocolo dot1Q para poder entender las tramas que recibe de los Switches de las redes LAN. Se utilizan mecanismos de conexión con el nivel de enlace de naturaleza sub interfaz por el hecho de que el Router las tendrá conectadas lógicamente a través de una sola interfaz física. De hecho, esta implementación permitirá también comprobar conectividad dentro de la misma VLAN.

2.1.2 Enlaces WAN

Una vez especificada la comunicación en redes de área local, es importante determinar las tecnologías de comunicación que se utilizan para interconectar las redes LAN y con ello formar redes de mayor tamaño como las redes de área extensa WAN (por sus siglas en inglés Wide Area Network).

Una red WAN se vale de enlaces de datos que proporcionan el transporte de información y con ello interconectar redes y dispositivos a lo largo de grandes distancias. Un enlace WAN puede transportar distintos tipos de tráfico como voz, video y datos.

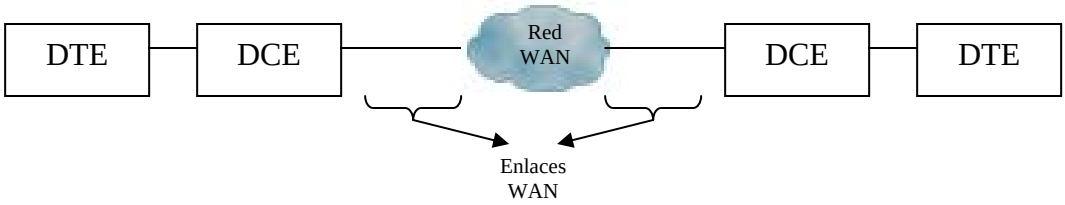


Figura 2.7 - Enlaces WAN

En el proceso de la comunicación en el enlace WAN intervienen dos tipos de dispositivos:

- DCE (Data Circuit-Terminating Equipment o Data Communication Equipment).
  Es el dispositivo que se encarga de gestionar la comunicación entre los extremos del enlace. Coloca los datos en el enlace de manera adecuada para su transmisión.

- DTE (Data Terminal Equipment).
  Es el equipo que genera la información.

Como caso particular de dispositivos DCE y DTE imagine el caso de la transmisión de información binaria a través de la línea telefónica. Se necesita que un equipo como el MODEM que gestione la

conexión y comunicación con el otro extremo del enlace, entonces, el MODEM es el DCE y el equipo que genera la información es el DTE.

La ruta de la WAN entre los DTE se denomina enlace, circuito, canal o línea. El DCE suministra una interfaz para el DTE hacia el enlace de comunicación en la nube WAN.

Normalmente, el DTE es el router y el DCE es el dispositivo que se utiliza para convertir los datos del usuario del DTE en una forma que sea aceptable para el transporte por la red WAN

La comunicación en la interfaz DTE/DCE se da mediante protocolos como HSSI (High Serial Speed Interface), V.35, X.21 y otros.

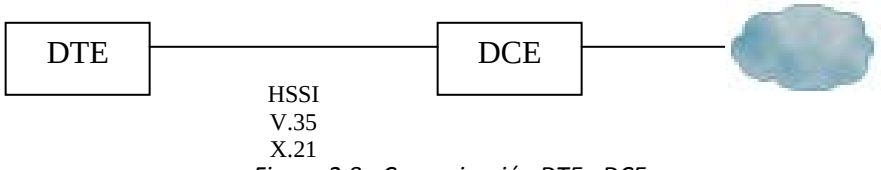


Figura 2.8 - Comunicación DTE - DCE

2.1.2.1 Protocolos de los enlaces WAN

Los enlaces WAN utilizan protocolos y tecnologías de nivel físico y de nivel de enlace de datos para llevar a cabo la adecuada comunicación. Además cada protocolo puede funcionar de acuerdo al esquema de conmutación de circuitos, conmutación de paquetes o una combinación de conmutación de paquetes y circuitos.

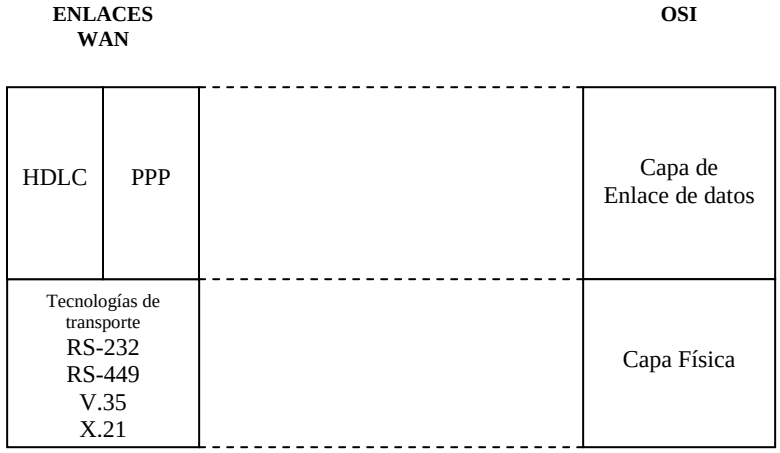


Figura 2.9 – Relación de los protocolos de los enlaces WAN con el Modelo de Referencia OSI.

2.1.2.2 Capa Física

Las tecnologías de capa física utilizadas por los enlaces WAN definen características eléctricas, mecánicas, operacionales y funcionales entre las más comunes se encuentran las mostradas en la tabla 2.2.

Tabla 2.2 - Tecnologías de capa física

Protocolo	Características
EIA[6]/TIA[7] 232 (RS-232)	Tasas de transferencia de hasta 64 kbps, conector DB-25
EIA/TIA 449 EIA-530	Soporta hasta 2 Mbps, utiliza el conector DB-36 y funciona a mayores distancias que el RS-232 también se le conoce como RS-422 y RS-423. Soporta una distancia máxima de 10 m.
EIA/TIA 612 / 613	HSSI, tasa hasta de 52 Mbps mediante el conector DB-50 y distancias hasta 15 m, utiliza un cable de pares torcidos blindado.
V.35	Datos síncronos desde 56 kbps hasta 2 Mbps y distancias desde 45 hasta 914 m, conectores tipo DB-15 y RMAC-34
X.21	Datos síncronos que utiliza un conector DB-15, con tasas desde 600 bps hasta 64 kbps.

2.1.2.3 Capa de Enlace de Datos

Los protocolos de enlace de datos utilizados en los enlaces WAN de la tecnología CISCO para interconexión de Routers pueden ser HDLC (High Data Link Control), PPP (Point to Point Protocol), Frame Relay, ATM y otros. Los alcances de la tesis solo permiten abarcar HDLC y PPP porque son las interfaces disponibles en los equipos provistos.

Las funciones de la capa de enlace son el encapsulamiento en tramas de estructura predefinida, mecanismos de transferencia de tramas, direccionamiento físico y flujo de datos. Las características específicas dependen de cada protocolo, sin embargo tanto PPP y HDLC utilizan el mismo marco de referencia de encapsulamiento HDLC[8] con ligeras variantes.

2.1.2.4 HDLC

HDLC es una norma de la ISO[9] que determina un protocolo de nivel de enlace de encapsulamiento de datos para enlaces seriales síncronos. La norma original de ISO no soporta el transporte de información de distintos protocolos de red dado que no incluye un campo identificador de protocolo de nivel superior, tampoco posee la facilidad de autenticación.

2.1.2.5 Trama HDLC

El encapsulamiento de realiza una vez que la capa de red ha entregado la información a la capa de enlace para su distribución por el medio físico que generalmente punto a punto. El entramado HDLC consiste de agregación de información para el control de flujo y errores. La trama siempre comienza y finaliza con una secuencia numérica de ocho bits de valor ‘01111110’ u 0x7E, debido a que esta secuencia podría corresponder al valor de algún campo de información, HDLC agrega un ‘0’ a cada secuencia continua de cinco ‘1’ que aparezcan en el campo de datos y el receptor quita esas modificaciones añadidas, la bandera de 8 bits final de una trama constituye la bandera de inicio de la siguiente trama ya que son enviadas de manera consecutiva.

Se agrega un campo de dirección que no es necesario por las disposiciones generalmente punto a punto de los enlaces WAN y puede tener uno o dos bytes de longitud. También agrega un campo de control que indica si la trama es de información, supervisión o no está numerada, las tramas no numeradas contienen información de configuración de línea, las de información paquetes de la capa de red y las de supervisión controlan el flujo de de tramas de información y retransmisión. El campo de control es de generalmente 1 byte, sin embargo puede modificarse hasta 2 bytes en algunos sistemas, por lo tanto la cabecera de trama está constituida del campo de dirección y control. Posterior a la cabecera de la trama siguen los datos encapsulados y al final la secuencia de verificación de trama FCS (Frame Check Sequence) que consiste de un mecanismo de comprobación de redundancia cíclica de longitud dos o cuatro bytes.

Existe una versión de HDLC (CISCO HDLC) que agrega un campo identificador de protocolo, el cual facilita el transporte de información de múltiples capas de red

01111110	DIRECCIÓN	CONTROL	INFORMACIÓN	FCS	01111110

Figura 2.10 - Formato de una trama HDLC

2.1.2.6 PPP Point to Point Protocol

Es un protocolo orientado a conexión con un modelo de capas que facilita, la configuración y comprobación de un enlace, el cual puede transportar información de múltiples protocolos de red, además provee de herramientas de autenticación, notificación de direccionamiento y monitoreo de los enlaces. Está definido en el RFC 1661, puede ser utilizado para establecer conexiones router a router, host a red sobre circuitos síncronos y asíncronos además este tipo de enlaces proveen conectividad bidireccional full duplex y orden en la entrega de paquetes; su MTU por defecto es de 1550 bytes; sus principales caracteristicas son las siguientes:

- Provee de control en la configuración de los enlaces.
- Es utilizado para asignar y administrar direcciones IP.
- Mutiplexa los protocolos de red.
- Posee mecanismos de detección de errores.

Su arquitectura por capas abarca el nivel de enlace de datos del modelo de referencia de OSI y define tres subcapas comenzando por la inmediata superior a la de red que es la capa de control de protocolo de red (NCP), seguida de la capa de control del enlace (LCP) y finalmente la capa de control de enlace de datos (HDLC).

2.1.2.7 Trama PPP

La trama PPP se compone de una bandera al igual que HDLC ‘01111110’ que indica el fin y el comienzo de la trama, un campo de dirección con valor ‘11111111’ debido a que PPP es un protocolo punto a punto no es necesario especificar la dirección. Un campo de control de un byte de longitud con una secuencia ‘00000011’ que se utiliza si la trama de datos no esta incluida en secuencia alguna

de tramas. Se puede especificar un servicio no orientado a conexión similar al especificado por LLC. El capo de protocolo especifica el protocolo al cual pertenece la trama, en el caso de IP se utiliza el NCP IPCP con valor del campo de protocolo 8021, para Novell IPX 802b, para tramas LCP c021, PAP c023, CHAP c223. el campo de información es de longitud variable y dispone de una secuencia de verificación de trama FCS de 2 o 4 bytes.

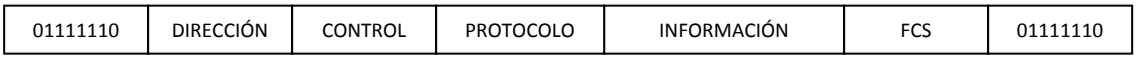


Figura 2.11 - Formato de una trama PPP

2.1.2.8 Funcionamiento de PPP

El establecimiento de la conectividad PPP consiste de los siguientes pasos:

- Establecimiento del enlace y la configuración.
  Uno de los nodos extremos del enlace PPP envía tramas LCP para configurar y establecer el enlace de datos.

- Determinación de la calidad del enlace.
  El enlace se prueba para determinar si la calidad del enlace es suficiente para acceder a los protocolos de capa de red, esta fase es opcional.

- Negociación de la configuración del protocolo de red.
  El nodo PPP de origen envía tramas NCP para elegir y configurar los protocolos de capa de red. Los protocolos elegidos son configurados y se dispone hasta este momento conectividad a nivel de red con lo cual se pueden enviar libremente los paquetes.

- Terminación del enlace.
  El enlace permanece activo para la comunicación hasta que las ramas LCP o NCP cierren el enlace o hasta que tenga lugar un evento externo.

2.1.2.9 Tipos de tramas LCP

- De establecimiento de conexión.
- De terminación de conexión.
- De mantenimiento del enlace.

2.1.2.10 Autenticación de PPP

PPP provee de un par de herramientas de autenticación del enlace para evitar que dispositivos no deseados accedan a los recursos de la red. Las herramientas son PAP y CHAP.

2.1.2.11 Autenticación PAP

PAP (Password Authentication Protocol) es un mecanismo de autenticación de 2 vías, es decir el dispositivo que solicita la autenticación envía un mensaje de petición donde especifica el nombre de usuario y contraseña en texto plano hacia el dispositivo que efectuará la autenticación y este le responde con un mensaje de aceptación o negación de la conexión.

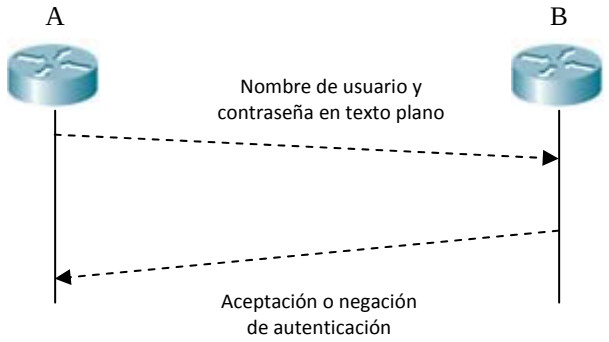


Figura 2.12 - Proceso de Autenticación PAP

2.1.2.12 Autenticación CHAP

La autenticación CHAP (Challenge Handshake Authentication Protocol), es mecanismo de autenticación de tres vías que se utiliza en el inicio de un enlace y en la verificación periódica del nodo remoto.

Una vez completada la fase de establecimiento del enlace PPP, el nodo local envía un mensaje "desafío" al nodo remoto. Este último responde con un valor que es calculado utilizando una función *hash* de una vía (generalmente con el algoritmo MD5) basada en la contraseña y mensaje desafió. El nodo local compara la respuesta con su calculo del valor hash esperado y si coinciden, se efectúa la autenticación, en caso contrario la conexión se termina inmediatamente.

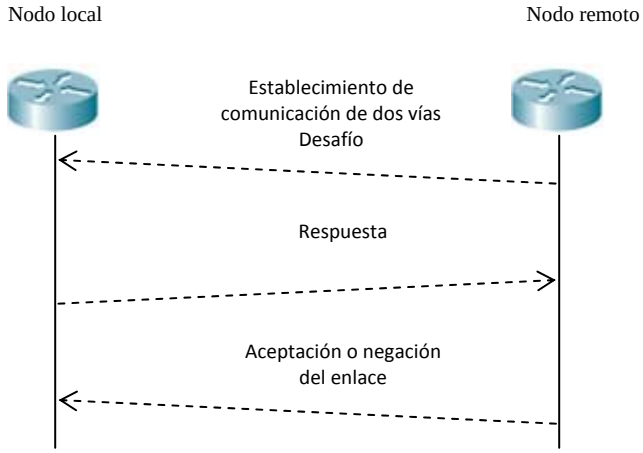


Figura 2.13 - Proceso de Autenticación CHAP

2.2 Nivel de Red y sus Protocolos

2.2.1 Capa de red o Capa de Internet

La capa de red está ubicada entre las capas de transporte y de enlace de datos del modelo OSI, por lo tanto provee de servicios al nivel de transporte y utiliza los servicios de la capa de enlace de datos. Tiene fundamentalmente las siguientes funciones:

- Proporcionar servicios al nivel de transporte.
- Direccionamiento
- Enrutamiento

La capa de red según el modelo OSI o capa de Internet según el modelo TCP/IP, es el corazón de las redes de telecomunicaciones modernas, y es donde se establecen los protocolos que llevan a cabo las acciones necesarias para la entrega de paquetes.

Descripción de la comunicación

El mecanismo de comunicación a través de Internet comienza cuando la capa de transporte segmenta el flujo de datos para que la capa de red logre encapsularlos en paquetes IP, cada paquete es transmitido a través de la red y puede ser fragmentado en paquetes de menor tamaño especificado por la MTU (Maximum Data Unit) de cada segmento de red, finalmente al llegar a su destino, la información es des encapsulada y reensamblada adecuadamente.

La red es la Internet, la cual consiste de una malla de nodos interconectados que forman las posibles rutas que un paquete puede tomar en su camino hacia su destino, el mecanismo mediante el cual se elige la ruta para que el paquete viaje, se llama enrutamiento.

El enrutamiento se consigue mediante el compartimiento entre los equipos de red de la información que describe la topología o parte de ella, es decir, los equipos de red se comunican información que especifica las conexiones establecidas con sus pares de tal forma que el equipo conoce los caminos posibles a utilizar y pone en marcha un algoritmo de elección de rutas. El mecanismo de elección de rutas está en función del protocolo a utilizar.

Los nodos dentro de la red se comunican mediante mensajes de actualización y descubrimiento que también son determinados por el protocolo de enrutamiento utilizado.

No solo es necesario conocer la topología alrededor de cada equipo en el interior de la red, sino que también es necesario que los nodos conozcan el estado de la red para evitar utilizar rutas congestionadas o problemáticas que puedan afectar el desempeño de esta, por tanto se pensó en la necesidad de protocolos que se encarguen de propagar mensajes de aviso a través de los equipos.

Una vez que el paquete está en la red de destino es necesario tener comunicación con el nivel de enlace de datos con la finalidad de saber hacia qué equipo será direccionado físicamente el paquete, lo cual se averigua con un protocolo específico y en función de la naturaleza de la red a la que llegue.

Los equipos que ejecutan las funciones del nivel de red se llaman Routers (o Ruteadores) y son sencillamente computadoras diseñadas, construidas y programadas para desarrollar específicamente las funciones de la capa de red mediante la ejecución de los programas que ponen en marcha los protocolos específicos.

Los protocolos que trabajan en el nivel de red desempeñan funciones para que se logre la comunicación anteriormente detallada, como primera clasificación podemos distinguir entre dos tipos:

- Enrutables
- De enrutamiento

2.2.2 Protocolos Enrutables

Los primeros, se encargan de determinar el formato de encapsulamiento y fragmentación de la información en el nivel de red, el caso de TCP/IP este protocolo es IP (Internet Protocol) y sus características son las siguientes:

2.2.2.1 IP[10]

- Fragmenta la información en un formato específico, el paquete IP.
- Determina un direccionamiento jerárquico basado en direcciones de 32 bits y un mecanismo de identificación para diferenciar entre una red y un host.
- Es un protocolo no orientado a conexión
- Los paquetes de información son procesados independientemente unos de otros, lo cual implica que pueden seguir distintas trayectorias a través de la red
- Es un protocolo llamado “Best-effort”, lo que significa que IP hará llegar lo mejor posible a un paquete dentro de sus limitaciones, sin embargo, no se asegura de que así sea.
- No posee características de control de errores.

Paquete IP

Consiste de un encabezado y un campo de carga útil de tamaño variable, la cabecera se muestra a continuación.

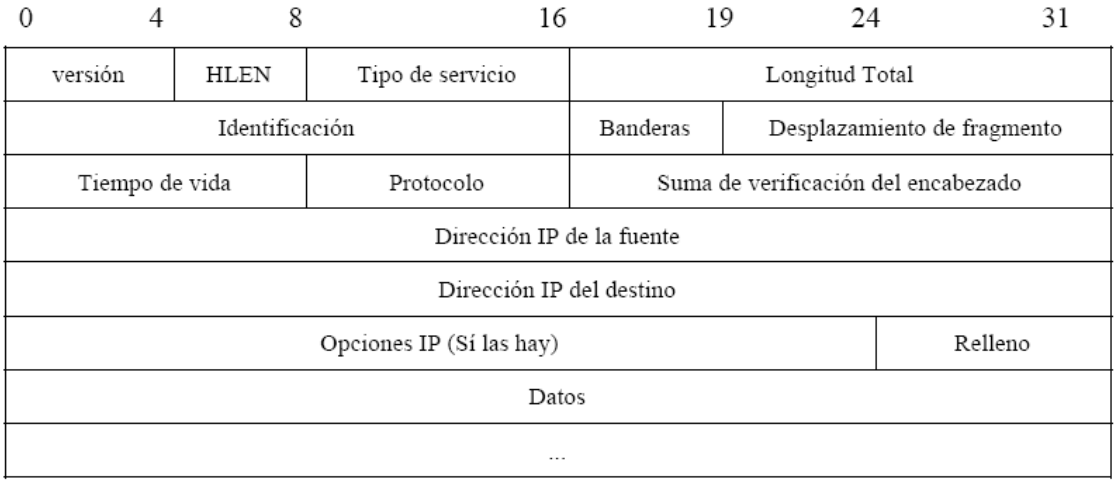


Figura 2.14 - Cabecera del Paquete IP

2.2.3 Protocolos de enrutamiento

Los protocolos de enrutamiento son los encargados de implementar el algoritmo de elección de caminos y de comunicar la información de la topología de la red entre los equipos de red y de acuerdo con la naturaleza del algoritmo de elección que utilizan se clasifican como sigue:

- Vector Distancia.
- Estado de Enlace.

2.2.3.1 Enrutamiento estático y RIP

El enrutamiento es el conjunto de mecanismos utilizados por el nivel de red, para la entrega de paquetes IP a través de múltiples trayectorias o rutas.

Los mecanismos implementan las siguientes funciones:

- Determinación de la ruta que deberá seguir un paquete para llegar de un origen a un destino.
- Comunicación entre dispositivos para actualización de rutas y estado de la red.

Las rutas pueden ser:

- Directas
  - Se llega a ella(s) directamente sin la necesidad de otro(s) dispositivo(s) del nivel de red.

- Indirectas
    - Para llegar a ellas es necesario pasar por uno o mas dispositivos del nivel de red.

El dispositivo almacena la información de las distintas rutas en su tabla de enrutamiento, la cual contiene información como la interfaz por la que se llega a determinada ruta, el tipo de ruta, dirección del siguiente salto (o vecino) y su métrica.

El enrutamiento puede ser estático o dinámico. El estático consiste en agregar a la tabla de enrutamiento manualmente cada una de las rutas posibles. El dinámico consiste de un protocolo que se encarga de propagar los mensajes que especifican las rutas existentes en la red de manera automática para evitar hacerlo manualmente e identificar el estado de conectividad y reaccionar ante los posibles cambios de topología.

Los protocolos Vector Distancia llevan este nombre porque la técnica que utilizan para enviar un paquete sólo requiere saber el "siguiente salto" (Next-Hop), que es lo mismo que la IP de la interfaz del Router por el cual pueden alcanzar la IP de destino, y la métrica, que es el número de Routers por los que tendrá que pasar el paquete. Así, el Router que va a enviar el paquete apunta (como si fuera un vector) al siguiente salto con una métrica (distancia) determinada.

2.2.3.2 OSPF Open Shortest Path First

OSPF es un protocolo de enrutamiento dinámico de tipo estado de enlace, de naturaleza classless y no propietario especificado en su versión mas reciente en el RFC 2328. El objetivo de este tipo de protocolos es el mismo que el de los Vector Distancia (V.D.): llenar la tabla de enrutamiento con las mejores rutas.

Los Routers con OSPF, implementan los siguientes pasos para la determinación de la mejor ruta:

- Descubrimiento de vecinos o establecimiento de adyacencias.
- Intercambio confiable de LSUs.
- Registro de las topologías aprendidas en la base de datos de topología.
- Calculo de mejores rutas mediante el algoritmo SPF

A diferencia de RIP, OSPF primero realiza una búsqueda de sus vecinos mediante el protocolo "OSPF Hello" informando el identificador del Router que envia, una vez aprendido el estado de los enlaces de los vecinos y mediante un proceso llamado "Flooding" redistribuye la información aprendida a través de todos los puertos excepto por aquel por el cual la recibió. Un vecino es aquel Router que comparte la subred con alguna de las interfaces de dicho Router.

Los protocolos estado-enlace requieren mayor capacidad de procesamiento y memoria en el Router a diferencia de los protocolos vector-distancia. Con la finalidad de implementar adecuadamente el protocolo OSPF el CISCO IOS utiliza unas entidades llamadas:

- Neighbor table o base de datos de adyacencias.
    - Contiene la información de las interfaces vecinas directamente conectadas, así como el estado de los enlaces.
- Topology database o de estado de los enlaces.
    - Contiene la información de los enlaces (métrica), Routers alrededor de los vecinos y sus subredes.

El identificador del Router se le llama interfaz Loopback la cual debe ser establecida antes de activar cualquier otra interfaz y consiste de una dirección IP tradicional, La finalidad de la interfaz Loopback es la de estar siempre activa pase lo que pase con el estado de las interfaces físicas que intervienen en la red.

Una vez que el router ha identificado los vecinos, comienza a enviar mensajes de actualización LSUs (por sus siglas en ingle Link State Updates), los cuales son formados LSAs (Link State Advertisements) los cuales pueden contener información como número de ruta, mascara de subred entre otras. Cabe mencionar que a diferencia de los protocolos VD, los de estado de enlace envían actualizaciones parciales de la topología en cada intento hasta que toda la topología de la red es conocida por todos los Routers. Además OSPF dispone de 5 tipos de mensajes a diferencia de RIP el cual solamente dispone del envió de tablas de enrutamiento completas a intervalos fijos.
Tipos de mensajes OSPF:

- Hello. Establece y mantiene información con los vecinos adyacentes.
- DBD (Data Base Description) descripción del contenido de la base de datos de los estados de los enlaces OSPF.
- LSR (Link State Request). Petición de secciones específicas de de la base de datos.
- LSU (Link State Update).
- LSAck(Link State Acknowledgment). Acuse de recibo de los LSAs recibidos.

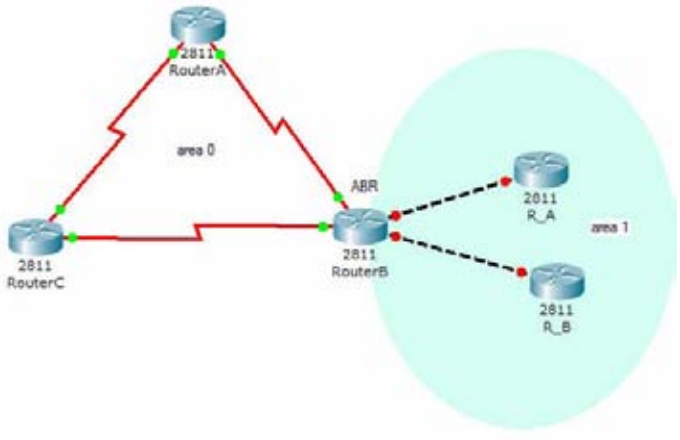


Figura 2.15 - Ejemplo de un área del protocolo OSPF

Los protocolos de estado-enlace calculan el costo de cada enlace de todas las rutas mediante el algoritmo llamado Shortest Path First (SPF) también conocido como Dijkstra SPF.

Una vez determinados los costos, *la mejor ruta será aquella que tenga un menor costo*, y se registrará en la tabla de enrutamiento.
OSPF determina dentro de la red un par de routers, llamados DR (Designated Router) y DBR (Designated Backup Router), los cuales funcionan como punto central de todas las actualizaciones de enlaces y LSAs, siendo el DR necesario y el DBR es respaldo del DR.

OSPF se emplea comúnmente en redes grandes (15 o mas saltos en el caso de RIP) debido a que este protocolo permite escalar redes mediante principios de diseño jerárquicos a partir de un área central de la que se desprenden otras redes la cual se llama Backbone (en OSPF se le llama area 0), de tal forma que se controlan las actualizaciones de enrutamiento y con ello se reducen la sobrecarga de información de actualización y el tiempo de convergencia de la red porque las áreas de acción son mas pequeñas. El router que está en el extremo de dos areas se le llama ABR (Area Border Router) y será el único con interfaces en dos áreas.

2.2.4 Mecanismos de comunicación de nivel de red

Existen protocolos que contribuyen a la plena comunicación en el nivel de red, los cuales participan interactuando con otras capas del modelo TCP/IP y detectando fallos de conectividad.

2.2.4.1 ARP Address Resolution Protocol

ARP no es un protocolo IP, es decir, no utiliza cabecera IP. Su misión es identificar y relacionar las direcciones IP con las direcciones de hardware. Esto resulta fundamental en redes de área local para identificar el destino de la transmisión.

Para explicar la función de este protocolo hay que considerar que una computadora que transmite un paquete a otra computadora que está en su mismo tramo de red, tiene que conocer dos datos sobre el destino, la dirección hardware y la dirección IP. Mientras que la dirección IP es un dato conocido para casi todas las transmisiones, la dirección hardware no siempre es un dato conocido. Es posible que esté almacenada en una caché temporal o en unos archivo del sistema. Sin embargo, resulta habitual que esta dirección haya que averiguarla en el momento justo en el que se va a realizar la transmisión.

Hay que considerar que el protocolo con el que funcionan las redes Ethernet hace que las máquinas identifiquen a los paquetes como dirigidos a ellas si ven su dirección hardware en el nivel de enlace. Es decir, no examinan la dirección IP, esto sólo lo hacen los Routers para ver a qué tramo de red tiene que dirigir el paquete, sino que miran la coincidencia de su dirección hardware con la que lleva el paquete. De hecho, cuando un paquete se envía a través de varios Routers, la información del nivel de enlace va variando en cada salto y refleja la dirección hardware del nodo inmediatamente siguiente en su destino, mientras que la dirección IP de origen y destino permanece constante durante todo el recorrido. Pues bien, como se ha dicho anteriormente, existen numerosas ocasiones donde se conoce la dirección IP destino, pero no la dirección hardware. En este caso se utiliza el protocolo ARP para enviar un mensaje de difusión por la red para preguntar por la dirección hardware asociada a la dirección IP a la que se quiere enviar el paquete. Como la máquina destino tiene que estar

necesariamente dentro de la red donde se actúa, ésta examinará el mensaje de difusión y enviará uno de respuesta identificándose y facilitando su dirección de hardware. Posteriormente, la computadora origen ya podrá enviar correctamente el paquete a la maquina destino poniendo en su nivel de enlace la dirección hardware correspondiente.

2.2.4.2 ICMP Internet Control Message Protocol.

Los hosts en las redes suelen comunicarse eventos tales como destinos inalcanzables, errores en el procesamiento de los datos y otros sucesos que puedan interferir con el funcionamiento de la red.

ICMP forma parte de la pila de protocolos TCP/IP y opera en el nivel de red utilizando el formato de paquete IP para ser transportado y consiste de un conjunto de mensajes para diversos propósitos.

La finalidad de ICMP consiste de proveer medio de comunicación entre los dispositivos en la red para llevar a cabo acciones que corrijan las problemáticas posibles, sin el afán de hacer de IP un protocolo confiable (es decir no intenta que IP deje de ser un protocolo “Best Effort”).

Los mensajes ICMP son enviados por diversas causas como las siguientes:

- Aviso de paquetes que no pueden alcanzar su destino.
- Algún Router carece de la capacidad suficiente para contener y reenviar los paquetes.
- El re direccionamiento del tráfico hacia otra ruta.

Formato de mensajes ICMP.

Como ya se mencionó previamente, los mensajes ICMP son encapsulados en paquetes IP, el primer octeto de la carga útil del paquete (Payload), es utilizado como encabezado ICMP el cual determina el contenido y la especificación del mensaje ICMP.

Los paquetes IP que transportan mensajes ICMP se diferencian mediante el valor 0 en el campo “protocolo” del encabezado IP.

Los mensajes ICMP son diferenciados a partir de un campo dentro del encabezado ICMP, presentamos diversos tipos de mensajes ICMP.

Tabla 2.3 - Tipos de mensajes ICMP

Tipo de mensaje	Valor del campo TYPE.
0	Petición de eco
3	Destino inalcanzable
4	Source Quench (petición de disminución de envío de tráfico).
5	Re direccionamiento hacia Routers con mejor posicionamiento para el ruteo.
8	Contestación a la petición de eco
11	Tiempo excedido

2.3 Nivel de Transporte y sus Protocolos

2.3.1 Capa de Transporte

La función de la capa de Transporte es la de proveer de una comunicación confiable procesos-a-proceso entre dos computadoras no importando que estas se encuentren cada una en una distinta red física. El software que implemente las funciones de esta capa es llamado **entidad de transporte**, esta puede ser encontrada por ejemplo en el Kernel del Sistema Operativo, en una librería de una aplicación de red e incluso en algunas tarjetas de interfaz de Red (NIC son sus siglas en Inglés).

Dado que la capa de transporte se implementa por medio de Software, da la enorme ventaja de poder brindar calidad del servicio de una manera relativamente sencilla.

Las unidades de información de esta capa son llamadas TPDU, estas unidades hacen la función de mensajes entre las entidades de transporte en una conexión.

2.3.2 Protocolos de transporte

2.3.2.1 TCP

TCP es el acrónimo de Transport Control Protocol ó Protocolo de Control de Transporte y es un protocolo orientado a conexión, esto es, para realizar el transporte o envío de información de una computadora a otra, es necesario establecer una conexión. Una conexión consta de los siguientes tres elementos:

1. Establecimiento de la conexión
2. Transferencia de Datos
3. Finalización de la conexión

En parte, son estos tres pasos los que le dan a TCP su confiabilidad ya que durante la transferencia de datos si algún segmento no llegara, o llegara con errores que no se pudieran corregir, la capa de transporte se encargaría de solicitar de nuevo el segmento después de un cierto tiempo (timeout), este es un método de control de errores conocido como ARQ y es parte de la confiabilidad de la Capa de Transporte.

Específicamente, las funciones descritas en el punto 3.3.1 referentes a la capa de transporte son implementadas y realizadas por el protocolo TCP, ofreciendo servicios a las capas superiores del Modelo de Referencia OSI.

2.3.2.1.1 Segmento TCP

La siguiente figura muestra la estructura de un segmento TCP.

<table>
<tr><td colspan="3">Puerto de Origen</td><td>Puerto de Destino</td></tr>
<tr><td colspan="4">Número de Secuencia</td></tr>
<tr><td colspan="4">Número de ACK</td></tr>
<tr><td>Offset de Datos</td><td>Reservado</td><td>Banderas de Control</td><td>Ventana</td></tr>
<tr><td colspan="3">Cheksum</td><td>Apuntador urgente</td></tr>
<tr><td colspan="3">Opciones</td><td>Pad</td></tr>
<tr><td colspan="4">Datos</td></tr>
</table>

Figura 2.16 - Segmento TCP

La siguiente tabla muestra la descripción de los campos del encabezado TCP.

Tabla 2.4 - Campos del encabezado TCP.

Campo	Descripción	Tamaño [bits]
Puerto de origen	Indica el número de puerto de origen.	16
Puerto de Destino	Indica el número de puerto de destino.	16
Número de Secuencia	Indica el número de secuencia del primer octeto de datos del segmento.	32
Número de ACK	Es el número de secuencia del siguiente segmento que el equipo receptor espera recibir, también sirve para informar al equipo que envía datos que el (los) segmento(s) anterior(es) fueron recibidos satistafctoriamente.	32
Offset de Datos	Indica el bit en el que comienzan los datos en el segmento.	4
Reservado	Es un campo reservado para uso futuro.	6
Banderas de Control	Este campo cuenta con 6 banderas de control, una por bit. Contiene funciones como reinicializar la conexión o sincronizar los números de secuencia.	6
Ventana	Es el número de octeto de datos que el equipo destino está esperando recibir.	16
Checksum	Es un número de verificación, sirve para corroborar que la información que recibe el equipo destino no contenga errores.	16
Apuntador urgente	Indica que se debe de procesar un segmento lo antes posible, se utiliza junto con una bandera de control (URG).	16

Opciones	Esta campo puede tener varios sub-campos, multiplos de 8 bits, como por ejemplo la longitud del segmento.	Variable
Pad	Sirve para completar el último octeto del encabezado con ceros para que pueda ser utilizado para calcular el checksum.	Variable
Datos	Son los datos que se desean enviar de un equipo a otro.	Variable

Establecimiento de la conexión

El establecimiento de una conexión se realiza mediante un procedimiento llamado *handshake*, específicamente para el caso de TCP se utiliza un procedimiento llamado 3-way handshake o handshake de tres pasos (también es conocido como tri-direccional).

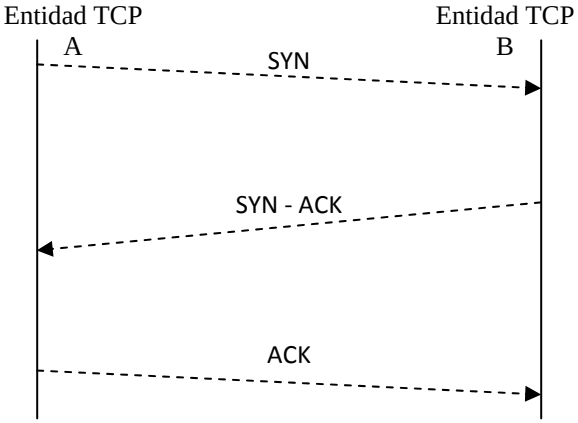


Figura 2.17 - 3-way handshake

2.3.2.2 UDP

UDP es el acrónimo de User Datagram Protocol o Protocolo de Datagrama de Usuario, fue desarrollado para proveer datagramas en un modo ce comunicación packet-switched en un ambiente de Redes interconectadas. Este protocolo asume que el protocolo IP es usado en la capa inmediatamente inferior del Modelo de Referencia OSI. UDP utiliza puertos para llevar a cabo la comunicación proceso-a-proceso.

UDP provee procedimientos a las aplicaciones de capas superiores permitiendo el envío de mensajes a otras aplicaciones utilizando un mínimo de mecanismos del protocolo. Es no orientado a conexión, esto es, se envían los segmentos sin saber si el equipo al cual están dirigidos está preparado para recibirlos; por esta razón UDP no ofrece garantía de entrega de segmentos ni algún tipo de protección contra segmentos duplicados, esta aparente desventaja puede ser utilizada como una ventaja si se necesita enviar datos de un equipo a otro de manera rápida y con una cierta tolerancia a los errores, ejemplos de este tipo de necesidades son juegos multijugador en tiempo real y VoIP.

2.3.2.2.1 Segmento UDP

La siguiente figura muestra la estructura de un segmento UDP.

Puerto de Origen	Puerto de Destino
Longitud	Checksum
Datos	

Figura 2.18 - Estructura de un Segmento UDP

La siguiente tabla muestra la descripción de los campos del encabezado UDP.

Tabla 2.5 - Campos del encabezado UDP.

Campo	Descripción	Tamaño [bits]
Puerto de Origen	Indica el número de puerto de origen.	16
Puerto de Destino	Indica el número de puerto de destino.	16
Longitud		16
Checksum	Es un número de verificación, sirve para corroborar que la información que recibe el equipo destino no contenga errores.	16
Datos	Son los datos que se desean enviar de un equipo a otro.	Variable

CAPÍTULO 3

NETACAD

3.1 Programa académico de Networking de CISCO[11]

Cisco Networking Academy es un programa de e-learning que enseña a los estudiantes las habilidades tecnológicas de Internet esenciales en una economía global. El programa proporciona contenido basado en el Web, pruebas en línea, seguimiento del desempeño de los estudiantes, laboratorios en vivo, soporte y entrenamiento por parte de los instructores y preparación para las certificaciones estándares de la industria.

El programa fue lanzado en octubre de 1997 en 64 instituciones educativas en siete estados - Arizona, California, Florida, Minnesota, Missouri, Nueva York y Carolina del Norte. Hoy en día Cisco Networking Academy Program se ha extendido a más de 150 países y a los 50 estados norteamericanos. Cuenta con más de 500,000 estudiantes inscritos en más de 11,000 Academias en escuelas secundarias, escuelas técnicas, preparatorias, universidades y organizaciones comunitarias. Cisco Systems capacita a los CATC (Cisco Academy Training Centers; Centros de Capacitación para las Academias Cisco), los CATC capacitan a las Academias Regionales y las Academias Regionales capacitan a los instructores de las Academias Locales, quienes a su vez capacitan a los estudiantes.

Los socios de CISCO (empresas, gobierno y organizaciones comunitarias) forman un ecosistema para ofrecer todo el rango de servicios y soporte necesario para el crecimiento de la fuerza laboral del mañana. Inicialmente creado para preparar estudiantes para los niveles CCNA (Cisco Certified Network Associate) y CCNP (Cisco Certified Network Professional), el Academy Curriculum se ha extendido, gracias a los cursos patrocinados por los socios del ecosistema. Dentro de los cursos opcionales se incluyen: Fundamentos de Tecnologías de Información, patrocinados por Hewlett-Packard; Fundamentos de Cableado de Voz y Datos patrocinado por Panduit y Fundamentos de Unix y Java.

Internet permite que los alumnos estudien en cualquier lugar a cualquier hora, independientemente de su ubicación, nivel socioeconómico, sexo o raza. Con el Programa de las Naciones Unidas para el Desarrollo, la Agencia de los Estados Unidos para el Desarrollo Internacional (USAID) y la Unión Internacional de Telecomunicaciones (ITU), Cisco ha podido ofrecer Cisco Networking Academy Program en países subdesarrollados, ayudándoles en la construcción de la economía de su país[12].

Cisco Networking Academy Program constantemente aumenta el nivel de los procesos educativos y de e-learning. Utilizando la retroalimentación de la comunidad y la evaluación electrónica. Cisco Networking Academy Program adapta su curriculum para mejorar los resultados y los logros de los estudiantes. La infraestructura de Global Learning Network diseñada para la Academia, ofrece a los estudiantes de todo el mundo un curriculum completo, interactivo y personalizado. Internet tiene el poder de cambiar la manera en que la gente aprende, trabaja y juega y Cisco Networking Academy Program está a la vanguardia de esta transformación.

3.2 Funcionamiento del programa

Cisco Networking Academy Program se desarrolla a partir de la colaboración con gobiernos, instituciones educativas públicas y privadas, organismos no gubernamentales e internacionales y empresas líderes en la industria en TI.

El programa funciona a partir de un convenio, donde las partes se comprometen a ofrecer los elementos necesarios para el buen funcionamiento del programa. Cisco provee: curriculum, entrenamiento a profesores, soporte y una comunidad virtual. La institución educativa proporciona profesores, espacio físico y acceso a Internet.

La organización de Cisco Networking Academy se compone de los “Cisco Academy Training Centers” (CATCs), Academias Regionales y Academias Locales.

La función de un CATC es proveer entrenamiento a los instructores y dar soporte a las Academias Regionales, el convenio será directamente con Cisco.
Las Academias Regionales también firmarán el convenio directamente con Cisco, brindarán soporte a 10 Academias Locales y proporcionarán instrucción gratuita a dos profesores.

Las Academias Locales firman contrato directamente con la Academia Regional y son las encargadas de ofrecer los cursos a los estudiantes[13].

3.3 Beneficios del programa académico de Networking[14]

Cisco Networking Academy Program está presente en más de 11,000 Academias ubicadas en escuelas secundarias, escuelas técnicas, preparatorias, universidades, organizaciones internacionales y organizaciones comunitarias, alrededor del mundo. Estas organizaciones aportan su experiencia y sus instalaciones para ofrecer a sus integrantes el Academy Curriculum de la más alta calidad.

Creado por profesionales de la industria y educación, el curriculum prepara estudiantes para las demandas de sus lugares de trabajo y los motiva a que continúen con su educación y aprendizaje. Ofrecido de manera global en múltiples idiomas, el programa usa datos de evaluación para adaptar y mejorar las lecciones, los laboratorios y la capacitación de los instructores. El programa reconoce múltiples estilos de estudio de los alumnos y por lo tanto utiliza contenido basado en Web con multimedia, asesorías y evaluaciones en línea a lo largo de todo el curso, ejercicios prácticos, capacitación con instructor y soporte. Al terminar el curso, los estudiantes tendrán la oportunidad de presentar el examen de certificación.

Las organizaciones participantes se integran a una comunidad global de aprendizaje que incluye estudiantes, instructores y socios, ya sean de las Academias, empresas, gobierno o de la comunidad. A través de un sistema de soporte de múltiples niveles, cada Academia tiene una Academia de soporte. Cisco Systems capacita a los CATC (Cisco Academy Training Centers, Centros de Capacitación para las Academias Cisco), los CATC capacitan a las Academias Regionales y las Academias Regionales capacitan a los instructores de las Academias Locales, quienes a su vez capacitan a los estudiantes. A través del Academy Connection, los participantes tienen acceso a una comunidad de usuarios para compartir sus mejores prácticas, resolver problemas, acceder a descuentos y solicitar ayuda. Los socios del ecosistema de Cisco aportan experiencia, recursos con descuento y oportunidades laborales orientadas al aprendizaje.

3.4 Programa académico de Networking en México[15]

En nuestro país el programa se imparte en gran parte del territorio nacional, y habiendo hacho una exhaustiva recopilación de información presentamos todas las instituciones educativas que al 17 de febrero de 2008 disponen del programa:

Aguascalientes
ITA, ITESM Aguascalientes, UAA, UPA, UTA, UTNA, UVM Aguascalientes.

Baja California
ITM, UTT.

Campeche
ITS de Calkini, UA de Ciudad del Carmen, UTM, UT de Campeche.

Chiapas
GE del Sureste S.C., UA de Chiapas, FCy A, UT de la Selva, U Valle de Grijalva Zona Centro A.C.

Chihuahua
IT Ciudad Cuauhtémoc, IT de Chihuahua II, ITS de Nuevo Casas Grandes, ITESM Chihuahua, ITESM Ciudad Juárez, UA de Ciudad Juárez, UT Ciudad Juárez, UT de Chihuahua.

Coahuila
UA de Coahuila, ITES de la Región Carbonífera, ITS de Monclova, ITESM Laguna, ITESM Saltillo, UT de Coahuila, UT de Torreón, UT del Norte de Coahuila.

Colima
BachTec #16, BachTec # 2, BachTec # 8, U de C DIGESET, U de Colima, FCyA de Manzanillo, FCyA de Tecomán, FIE, FIM y E, F de Telemática.

Distrito Federal
IPN CECYT No. 8 Narciso Bassols, CC Anáhuac S.C., CC Universitario Justo Sierra, A.C., ICEL Berlín, ICEL Cantera La Villa, ICEL Ermita Iztapalapa, ICEL Fundación Azteca, ICEL Tlalpan, ICEL Zaragoza, ICEL Zona Rosa, ITESM Ciudad de México, ITESM Santa Fe, Sistema UNID, UNITEC Coyoacán, UNITEC IEC Sur, UNITEC ISC Cuitláhuac, UNITEC ISC Sur, UA del Sur, U de las Américas, D.F. UVM Chapultepec, ULSA, U Panamericana, U TECMILENIO Ferrería, UT Americana, UVM San Rafael, UVM Insurgentes Norte, UVM San Ángel, UVM Tlalpan.

Durango
IT de Villa Montemorelos, IT Superior de Lerdo, U Politécnica de Gomez Palacio.

Guanajuato
CECYTE Guanajuato, CONALEP de Guanajuato, CONALEP Moroleón, CONALEP Salvatierra, IT de Celaya, IT de León, IT de Roque, IT S de Irapuato, ITS del Sur de Guanajuato, ISCEI Irapuato, ITESM Campus León, ITESM Campus Morelia, Promoción de la cultura y de la educación del Bajío, A.C. (Ibero), U de Celaya, U de La Salle Bajío, A.C., ULSA del Bajío, A.C. Campus León, U Quetzalcóatl en Irapuato, UT de León UT del Norte de Guanajuato UT del Suroeste de Guanajuato.

Guerrero
U Americana de Acapulco, UA de Guerrero, UT de la Región Norte de Guerrero, U T del Norte de Guerrero (Región Montaña).

Hidalgo
ITS del Occidente del Estado de Hidalgo, ITESM Campus Hidalgo, U A del Estado de Hidalgo, ULSA Pachuca A.C., U Politécnica de Tulancingo, UT de Tulancingo, UT del Valle del Mezquital, UT Sierra Hidalguense.

Jalisco
Centro de Enseñanza Técnica Industrial Providencia (CETI), CU CIENEGA, U de Guadalajara, CU de Ciencias Económicas Administrativas de la UDG, CU de la Costa - U de Guadalajara, CU de la Costa Sur, CU de los Valles, CU NORTE, U de G, CU SUR, U de G, CETI Tonalá, IT de Tlajomulco Jalisco, IT El Salto, ITS de Arandas, ITS de El Grullo, ITS de los Reyes, ITS de Puerto Vallarta, ITS de Tequila, ITS de Zapopan, ITS de Zapotlanejo, ITS Zapopan Sistemas Computacionales, ITESM Guadalajara, ITESO, UNITEC Zapopan, UNIVA, UA de Guadalajara, U Politécnica de la Zona Metropolitana de Guadalajara, UT de Jalisco, UT Zona Metropolitana de Guadalajara, U Valle México, Campus Guadalajara (Tlaquepaque).

México
Administración del Valle de Toluca S.A. de C.V., Centro de Integración Juvenil, Centro Escolar del Lago, CU Etac/ Campus Viveros, ICEL Campus Coacalco, ICEL Campus Cuautitlán, ICEL Campus Lomas Verdes, ICEL Campus Metepec, IT de Tlalnepantla, IT de Toluca, ITESM Estado de México, ITESM Toluca, T de E S de Coacalco, T de E S de Cuautitlán Izcalli, T de E S de Ecatepec, TES de Ixtapaluca, UNITEC ISC Atizapán, UNITEC ISC Ecatepec, UNITEC LIA Atizapán, U Anáhuac del Norte, U de Cuautitlán Izcalli, U del Valle de México/ Campus Lomas Verdes, U Hispanoamericana (UVM Campus Hispano), U Politécnica del Valle de México, U TECMILENIO Cuautitlán Izcalli, UT de Nezahualcóyotl, UT de Nezahualcóyotl (Informática), UT de Tecamac, UT del Sur del Estado de México, UT del Valle de Chalco, A.C., UT del Valle de Toluca, UT Fidel Velázquez, UVM Lago de Guadalupe (Formación Completa S.C.), Centro Universitario ETAC/Campus Coacalco, UVM Campus Texcoco.

Michoacán
CONALEP Lázaro Cárdenas, IT de Estudios Ses de Zamora, IT de Lázaro Cárdenas, ITS de Apatzingán, ITS de Ciudad Hidalgo.

Hidalgo
ITS de Huetamo, ITS de Morelia, ITS de Uruapan, U Don Vasco, A.C., U Latina de América, UT de Morelia, UT Tula – Tepeji.

Morelos
Centro de Investigación en Ingeniería y Ciencias Aplicadas, CONALEP Temixco, I de Capacitación para el Trabajo del Estado de Morelos, I Universitario Internacional, ITESM Cuernavaca, Patronato para el Fomento de la Educación S.C., Stratford Colegio de Estudios Universitarios, U del Valle de Cuernavaca, U Fray Luca Faccioli, U Interamericana para el Desarrollo, U Politécnica del Estado de Morelos, UT Emiliano Zapata.

Nayarit
U T Bahía de Banderas, U T de la Costa.

Nuevo León
C.B.T.I.S. No. 22, Ciudad de los niños Monterrey Mujeres, Ciudad de los niños Monterrey Varones, ITESM Monterrey, UNITEC Cumbres, UA de Nuevo León, UA de Nuevo León, FIME Ingeniería Administrador de Sistemas, FIME Ingeniería en Electrónica y Comunicaciones, U de Montemorelos, U de Monterrey, U del Norte A.C., U Regiomontana, A.C., U TECMILENIO Campus Las Torres, U TECMILENIO Campus Monterrey Cumbres, U TECMILENIO San Nicolás,U T de Matamoros, UT de Santa Catarina, UT General Mariano Escobedo.

Oaxaca
U Anáhuac de Oaxaca.

Puebla
Fundación U de las Américas, IT de Puebla, IT de Tehuacán, ITS de Acatlan de Osorio, ITS de Huauchinango, ITS de la Sierra, ITS de la Sierra Norte de Puebla, ITS de Libres, ITS de Tepeaca, ITS de Teziutlán, ITS de Zacapoaxtla, Instituto Universitario Puebla S.C., ITESM Puebla, U del Valle de México, Campus Puebla, U Madero, U Politécnica de Puebla, U Popular A del Estado de Puebla, UT de Huejotzingo, UT de Izúcar de Matamoros, UT de Puebla, UT de Tecamachalco, UT de Xicotepec de Juárez (Informática).

Querétaro
IT de Querétaro, IT de San Juan del Río, ITESM Querétaro, UA de Querétaro, UT de Querétaro, UVM Querétaro.

Quintana Roo
COBAQROO Cancún 2, COBAQROO Cancún 3 Bonfil, COBAQROO Chetumal 1, COBAQROO Cozumel, COBAQROO Playa del Carmen, Colegio de Bachilleres de Quintana Roo (COBAQROO) Bacalar, CEPTTQ- Plantel Cancún II, CEPTTQ - Plantel Lic. Jesus Martínez Ross IT de Cancún, IT de Chetumal, IT de Felipe Carrillo Puerto, U de Quintana Roo, U del Caribe, U del Tercer Milenio Unidad Chetumal, UT de Cancún.

San Luís Potosí
Grupo Educativo Potosino A.C., IT de Matehuala, ITESM San Luis Potosí, UP de San Luis Potosí.

Sinaloa
ITS de Sinaloa, IT de Los Mochis, ITESM Campus Mazatlán, ITESM Campus Sinaloa, UA de Sinaloa - Culiacán, UA de Sinaloa - Mazatlán, U de Occidente, Unidad Culiacán, Unidad Guamuchil, Unidad Guasave, Unidad Los Mochis Unidad Mazatlán, U Politécnica de Sinaloa.

Sonora
IT de Hermosillo, ITS de Cajeme, ITS de Cananea, ITESM Sonora Norte, U de Sonora, U del Noroeste, U Kino, A.C., U T de Hermosillo, UT de Nogales, UT del Sur de Sonora.

Tabasco
Colegio de Educación Profesional Técnica del Estado de Tabasco, Estrategia Educativa y Cultural de Tabasco, S.C., ITS de Comalcalco, ITS de los Ríos, ITS de Macuspana, ITS de Villa La Venta, Plantel Conalep Cárdenas 052, Plantel CONALEP Huimanguillo 099, UA de G Campus Tabasco, U Juárez A de Tabasco, División de Informática y Sistemas, U Mundo Maya U Olmeca A.C., UT de Tabasco.

Tamaulipas
Intituto de Cultura Superior Valle del Bravo de Reynosa A.C. (Tampico), IT de Estudios Superiores de Tamaulipas, ITESM Campus Tampico UAT, Centro de Excelencia Tampico UAT, Unidad académica de la Salud y Tecnología, UAT, Vallehermoso (Prepa), UAT, Victoria (CAUCE), UA de Tamaulipas, ULSA A. C., Tlaxcala, UA de Tlaxcala.

Veracruz
COBAEV Agua Dulce, COBAEV Alamo, COBAEV Coatzacoalcos, COBAEV Coatzintla, COBAEV Córdoba, COBAEV Cosoleacaque, COBAEV Jaltipan, COBAEV Martinez de la Torre, COBAEV Nogales, COBAEV Pueblo Viejo, COBAEV Xalapa, Colegio de Bachilleres del Estado de Veracruz (COBAEV), COVBAEV Huatusco, IT de Veracruz, ITS de Ciudad Serdán, ITS de Misantla, IT S de Poza Rica, IT S de Xalapa, ITESM Veracruz, U Anáhuac de Xalapa, U Atenas Veracruzana, UA de Veracruz (Villa Rica), U Cristobal Colón, U del Golfo de México, U del Golfo de México A. C. , (Centro), UT del Centro de Veracruz, UV, UV, F Contaduría y Administración, UV, F Contaduría y Administración de Nogales, UV, F Estadística e Informática, UV, F de Ingeniería, UV, F de Ingeniería Electrónica y Telecomunicaciones

UV, Fde Ingeniería en Electrónica y Comunicaciones, Región Poza Rica – Tuxpan.

Yucatán

U del Mayab, U del Tercer Milenio S. C., U del Tercer Milenio S. C. (U Interamericana para el Desarrollo sede Mérida), UT de la Riviera Maya, UT Metropolitana, UT Regional del Sur.

Zacatecas

ITS de Fresnillo, ITS de Zacatecas Occidente, ITS de Zacatecas Sur, ITESM Campus Z, UA de Zacatecas, Campus Jalpa, UA de Zacatecas, Unidad Académica de Ingeniería Eléctrica, U Politécnica de Zacatecas, UT del Estado de Zacatecas.

Total: 357 instituciones.

3.5 Panorama de los programas de certificación[16]

Dentro del mundo de las redes de datos, existen certificaciones que acreditan que los profesionistas poseen lo conocimientos necesarios para implementar, operar y administrar adecuadamente los recursos de una red, dichas certificaciones brindan al profesionista de un respaldo que acredita sus conocimientos en el ámbito de las redes CISCO de pequeño y mediano tamaño (menores a 100 nodos) y entonces emplearse convenientemente y así contribuir con el desarrollo tecnológico y económico de su país. En el caso particular de la carrera de certificaciones CISCO se incluyen tres niveles:

- Asociado
- Profesional
- Experto

Para alcanzar dichas certificaciones existen 6 diferentes formas de hacerlo las cuales están en función del ámbito de especialización deseado entre los que se encuentran el enrutamiento y el switching, la seguridad de la red, y otros tantos.

3.6 Certificación de nivel Asociado[17]

CCNA es Cisco Certified Network Associate y es el primer paso en el camino de las certificaciones de la carrera de CISCO. Consta de un programa de 280 horas y hace especial énfasis en el uso de técnicas para la toma de decisiones, solución de problemas y aplicación de conceptos de las redes para solucionar los problemas de la conectividad. El estudiante aprenderá a instalar y configurar Switches y Routers CISCO en redes multiprotocolo, utilizando redes locales (LAN) y de área extensa (WAN), a solucionar problemas y mejorar el desempeño y seguridad de las redes. Además se instruye y capacita para el cuidado, mantenimiento y uso adecuado de herramientas de software y redes y equipo así como códigos y reglamentos de seguridad, construcción y del medio ambiente, tanto locales como estatales y nacionales.

El programa de certificación CCNA se imparte a nivel universitario y en un inicio ha estado compuesto de los siguientes cursos[18]:

CCNA1 – Conocimientos básicos de Networking
- TCP/IP
- Medios de red
- Tratamiento IP
- Enrutamiento

CCNA2 – Conocimientos básicos de Routers y Switches
- Protocolos de enrutamiento
- Conceptos de TCP/IP
- Listas de Acceso
- Destrezas en la solución de problemas de redes

CCNA3 – Conocimientos básicos de Switching y Enrutamiento intermedio
- Elementos básicos de OSPF
- Elementos básicos de EIGRP
- Configuración de switches
- Protocolo Spaning Tree
- VLANs

CCNA4 – Tecnologías WAN
- ISDN
- Frame Relay
- PPP
- Tecnologías emergentes

3.6.1 VERSIÓN ACTUAL DEL PROGRAMA DE CERTIFICACIÓN CCNA[19]

Como ya se mencionó anteriormente, la certificación es una herramienta que el profesionista tiene para demostrar la posesión de sus conocimientos, en el mundo de la tecnología, cada día se tienen muchos y rápidos cambios en los requerimientos, lo cual provoca que lo que hoy es técnicamente útil, mañana probablemente sea obsoleto, lo cual obliga a una rápida adecuación. Tal es el caso de los contenidos a cubrir para acreditar una certificación de CISCO, se dispone de versiones que a lo largo del tiempo se han ido acoplando a los requerimientos de la industria de las telecomunicaciones, actualmente la versión de la certificación CCNA es la 640-802
La versión actual de la certificación CCNA valida las habilidades de:
- Instalación.
- Configuración.
- Operación.
- Resolución de problemas

De equipos de red en redes de ruteo y switcheo.

El contenido del programa de certificación actual está compuesto de los siguientes tópicos:

- Introducción al Networking inalámbrico.
- Protocolos de red, IP, EIGRP, OSPF, RIP v2.
- Protocolos de enlace de datos, Frame Relay, PPP, Ethernet, VLANs
- Access Control List

La certificación puede ser alcanzada mediante dos formas:

- La acreditación del examen **CCNA 640-802**
- La acreditación de los exámenes **ICND1 640-822** e **ICND2 640-816**

La acreditación del examen **CCNA 640-802,** consiste de la aprobación de una sola evaluación que contempla contenidos tanto teóricos como prácticos y habilidades de configuración y resolución de problemas, los conocimientos teóricos pueden ser adquiridos mediante el estudio de la bibliografía que se menciona a continuación.

- Interconnecting Cisco Networking Devices Parte 1 (ICND1) v1.0
- Interconnecting Cisco Networking Devices Parte 2 (ICND2) v1.0

Los conocimientos prácticos y habilidades de configuración y resolución de problemas, son la meta a lograr de la implementación del laboratorio de redes, con lo cual el alumno podrá adquirir las habilidades y la experiencia necesaria tanto para obtener una certificación CCNA actual como para prepararse para el campo laboral de hoy en día.
La acreditación de los exámenes **ICND1 640-822** e **ICND2 640-816** consiste de la aprobación de la evaluación que al igual que en el primer caso contempla contenidos teóricos, prácticos y habilidades de configuración y resolución de problemas. La parte teórica puede ser cubierta mediante la bibliografía siguiente:

- Interconnecting Cisco Networking Devices Parte 1 (ICND1) v1.0
- Interconnecting Cisco Networking Devices Parte 2 (ICND2) v1.0

Como bibliografía adicional complementaria[20] hemos encontrado que es conveniente como fuente de entrenamiento para el o los exámenes de certificación el libro:

- Authorized Self-Study Guide, CCNA Preparation Library, Seventh Edition, Cisco authorized self-study books for CCNA 640-802 foundation learning de Steve McQuerry, CCIE® No. 6108

3.7 Certificación de nivel Profesional

El segundo nivel de certificación es la certificación profesional, corresponde a las certificaciones CCNP (Cisco Certified Network Professional), CCSP (Cisco Certified Security Professional), CCDP (Cisco Certified Design Professional), CCIP (Cisco Certified Internetwork Professional) y CCVP –(Cisco Certified Voice Professional). Donde cada una de ellas requiere una especialización determinada dentro del mundo de las redes de datos.

3.7.1 Certificación CCDP

El primer requisito para obtener esta certificación es el estar certificado en el nivel asociado vigente. La certificación CCDP asegura que se tienen los conocimientos y habilidades para un adecuado diseño de la red basado en sus primordiales conceptos y principios. Los profesionistas con esta certificación tienen las habilidades de diseñar, discutir y crear un avanzado esquema de direccionamiento, enrutamiento, seguridad, manejo de la red, de centros de datos y de infraestructura de red de aquellas empresas que basa su infraestructura en una arquitectura compleja de IP multicast, la cual incluye redes privadas virtuales, y dominios de red inalámbricos.

3.7.2 Certificación CCNP

El primer requisito para obtener esta certificación es el estar certificado en el nivel asociado vigente. La certificación CCNP valida las habilidades profesionales para instalar, configurar y resolver problemas de conectividad uy convergencia en redes locales y de área extensa desde cien hasta quinientos nodos o más. Los profesionistas que han logrado esta certificación disponen de los conocimientos y habilidades requeridas para manejar routers y switches que conforman el núcleo de la red, así como las aplicaciones de frontera que integran voz, aplicaciones inalámbricas y seguridad dentro de la red.

3.7.3 Certificación CCSP

El primer requisito para obtener esta certificación es el estar certificado en el nivel asociado vigente. Esta certificación garantiza que el profesionista dispone de los conocimientos y habilidades necesarias para tener un adecuado esquema de seguridad en la red, de tal manera que pueda manejar la infraestructura CISCO, VPN (Virtual Private Network), PIX Firewall, Dispositivos adaptivo de seguridad, sistemas de prevención de intrusos.

3.7.4 Certificación CCIP

El primer requisito para obtener esta certificación es el estar certificado en el nivel asociado vigente. Esta certificación asegura el desempeño del profesionista dentro en el entorno de la prestación de servicios de conectividad IP, los cuales disponen de un detallado entendimiento de las tecnologías de networking del área del ISP como enrutamiento IP, calidad del servicio QoS, BGP y MPLS.

3.7.5 Certificación CCVP

El primer requisito para obtener esta certificación es el estar certificado en el nivel asociado vigente. Esta certificación de nivel profesional, hace énfasis en la importancia que los profesionales de las teorías de la información requieren en la integración de servicios de telecomunicaciones como la tecnología de voz, tecnologías telefónicas escalables y manejables, además se garantiza el dominio en la operación, configuración y resolución de problemas en una red IP convergente de tal manera que el profesionista conoce sistemas de comunicaciones unificadas, calidad del servicio, Gateways, Gatekeepers, teléfonos IP, aplicaciones de voz y utilidades basadas en tecnología de Routers y Swithces CISCO.

3.8 Certificación de nivel Experto

Cualquier certificación del nivel experto como primer requisito pide la tenencia de alguna de las certificaciones de nivel profesional.

La certificación CCIE consiste de los siguientes enfoques de especialización[21]

- Routing y Switching
- Seguridad
- Provisión de servicios
- Almacenamiento distribuido
- Voz

Cabe mencionar que la certificación CCIE en cualquiera de sus variantes constituye un conjunto de profesionistas de élite reconocidos a nivel mundial por su alta capacidad y conocimientos en el entorno de cada una de las especializaciones.

CAPÍTULO 4

DESCRIPCIÓN TECNOLÓGICA

En este capítulo se describe la estructura electrónica y física, así como las capacidades y posibilidades de expansión de los dispositivos de interconexión Router CISCO 2811 y Switch CISCO 2950.

4.1 Descripción de la estructura electrónica del equipo CISCO 2811

El equipo CISCO 2811 es un Router de Servicios Integrados, esto significa que puede proveer servicios como VoIP, Wíreless, entre otras. Dentro de sus características generales cuenta con soporte para un modulo NME[a] (modulo de red mejorado), 4 tarjetas HWIC[b] (Tarjetas de interfaz WAN de alta velocidad) ó 2 tarjetas dobles HWIC, 2 AIMs (Advanced Integration Modules), 2 módulos para voz y datos (PVDMs), 2 conexiones Fast Ethernet y 24 puertos para salida de alimentación de teléfonos IP.

Descripción General Física del Router

La siguiente lista muestra los dispositivos de almacenamiento de un Router CISCO 2811.

- Memoria ROM
- Memoria FLASH
- Memoria RAM
- Memoria NVRAM

Entre las interfaces más comunes podemos encontrar las siguientes:

- Ethernet
- Fastethernet

[a] Por sus siglas en inglés: Network Module Enhanced:
[b] Por sus siglas en inglés: High-speed WAN Interface Cards

- Gigabitethernet
- Ópticas
- Seriales
- Loopback
- De voz FXS/FXO
- VLAN
- ISDN

Router de Servicios Integrados (RSI)

El siguiente diagrama trata de ilustrar los servicios y beneficios que otorga el utilizar un Router de Servicios Integrados.

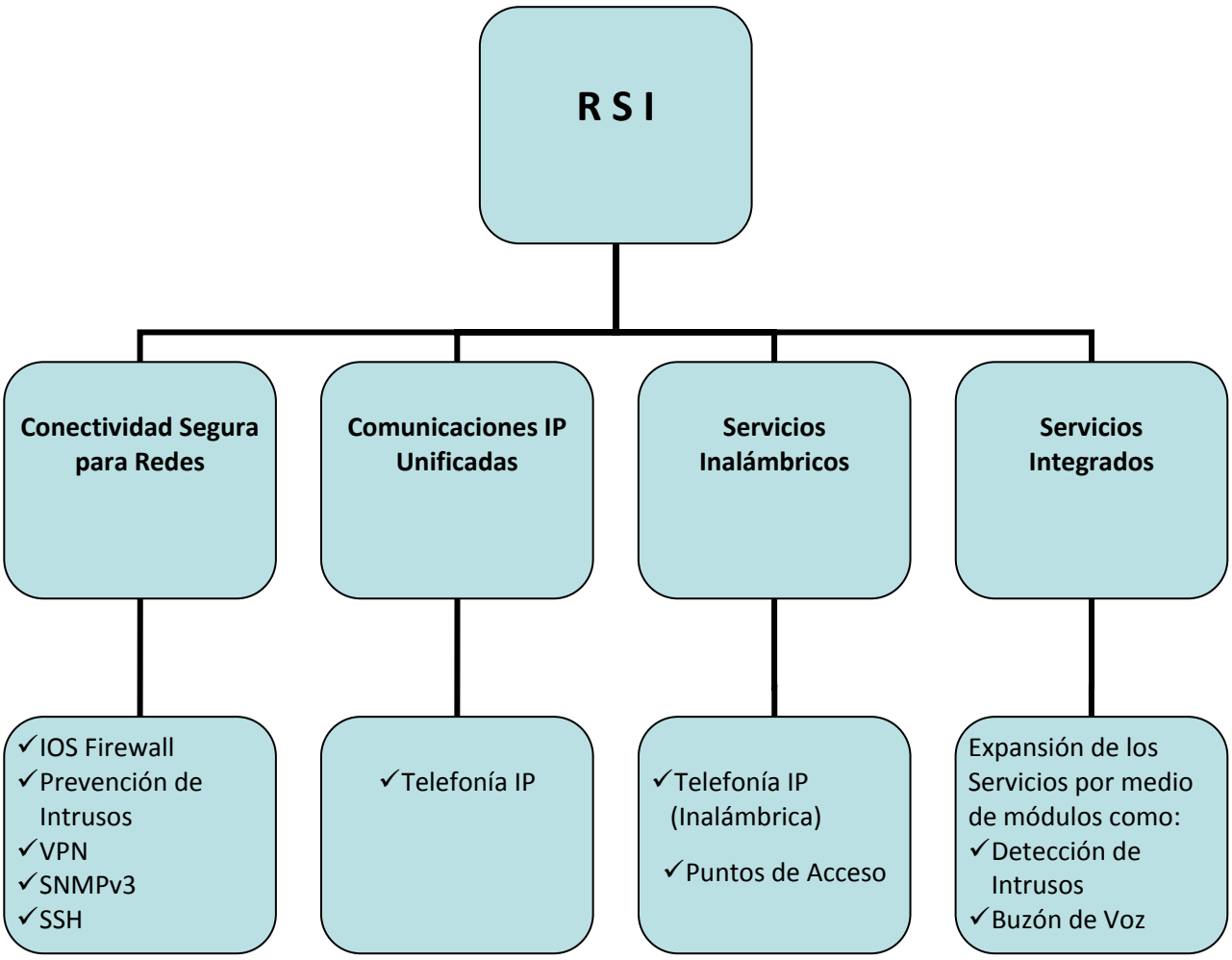


Figura 4.1 - Diagrama de descripción de Servicios de un Router de Servicios Integrados.

Las siguientes tablas describen más a fondo las características de un equipo CISCO 2811, dichas características son con las que cuenta de fábrica.

Tabla 4.1 - Hardware

Categoría	Tipo	Cantidad	Descripción
Interfaces	Fast Ethernet	2	Los puertos Fast Ethernet son 100BASE-T con conectores RJ-45.
	USB	2	Puerto de Bus de Serie Universal.
	Puerto de Consola	1	Permite acceso a la interfaz de comandos o CLI de manera local, conector RJ-45.
	Puerto Auxiliar	1	Permite el acceso remoto a la interfaz de comandos, conector RJ-45.
Procesador	MPC860	1	Procesador del Router.

Como se mencionó al principio de este capítulo, el Router CISCO 2811 cuenta con soporte para varios tipos de módulos y tarjetas que le permiten expandir sus servicios, para instalar uno de esos módulos o tarjetas, es necesario que el Router cuente con ciertos requerimientos físicos mínimos tales como:

- Cantidad de memoria RAM
- Cantidad de memoria Flash
- Versión del sistema operativo (ISO)

Para comprender mejor lo antes mencionado se presenta el siguiente ejemplo, consiste en una tarjeta WIC para el Router 2811 y se especifican los requerimientos físicos mínimos que debe de cumplir un Router para poder utilizar la tarjeta.

Nombre de la Tarjeta
WIC−2A/S (Two−Port Asynchronous/Synchronous WIC)

Tipo de cables que utiliza
Cable V.35 DTE de 3 metros con conector macho.
Cable V.35 DCE de 3 metros con conector hembra.

Tabla 4.2 - Routers que soportan la tarjeta WIC−2A/S (sólo se muestran algunos)

Modelo de Router	Módulo necesario	Versiones de IOS soportados
CISCO 1700	No requerido	Todas las versiones de IOS
CISCO 2600	NM-2W	12.0(7)XK, 12.1(1)T, 12.2 y 12.2T
CISCO 2811	No requerido	12.3 (IPBASE)

Tabla 4.3 - Memoria

Tipo	Subtipo	Memoria de Fábrica	Expansiones y características adicionales	Descripción
RAM	DDR con ECC (Código de Correción de Error)	256 MB	Soporta un máximo de memoria de 768 MB.	Se utiliza para almacenar las configuraciones de inicio y la que se esta ejecutando; también se utiliza para almacenar temporalmente los paquetes recibidos y para cargar el IOS.
NVRAM	Flash (Interna)	2 MB	Se utilizan slots SIMM para esta memoria.	Se utiliza para almacenar el bootstrap, el registro de configuración y la configuración de inicio.
	Flash (Externa)	64 MB	Acepta tarjetas PCMCIA de 128 ó 256 MB.	Se utiliza para almacenar la imagen del IOS.

Indicadores LED

El equipo CISCO 2811 cuenta con LEDs indicadores que sirven para informar el estado de funciones como la alimentación eléctrica, transmisión de paquetes por interfaz y velocidades de los enlaces (10 Mbps ó 100Mbps).

Tabla 4.4 - Características físicas y condiciones de operación

Característica	Descripción
Dimensiones	44.5 x438.2 x 416.6 mm (Altura, Ancho, Profundidad)
Peso	6.36 kg (con todos sus slots ocupados)
Entrada de energía AC	100 - 240 VAC
Humedad en operación	5 -95 % de humedad no condensada
Temperatura en operación	0 - 40 C
Temperatura soportada apagada	-20 - 65 C
Nivel de ruido	47 dBA en un ambiente de temperatura normal

4.2 Descripción de la estructura electrónica del equipo Catalyst 2950

El Switch Catalyst 2950 puede venir con diferente número de puertos, por ejemplo 12 puertos, 24 puertos o 48 puertos y con diferentes anchos de banda. Para nuestro caso en específico hablaremos del Switch de 24 puertos Ethernet 10/100 con conectores RJ-45.

Este tipo de Switch tiene como características generales:

- ✓ Auto-negociación de la velocidad (10, 100)
- ✓ Auto-negociación del modo duplex (half, full)

Puertos

El Switch Catalyst como ya se menciono, cuenta con 24 puertos Ethernet 10/100 a los que se le pueden conectar los siguientes dispositivos:

- ✓ Dispositivos 10BASE-T como Hubs y Estaciones de Trabajo.
- ✓ Dispositivos 10BASE-TX como Servidores, Hubs, Switches y Estaciones de Trabajo.

Otro puerto importante con el que cuenta este equipo es el puerto de consola, con conector RJ-45, este puerto nos permite acceso a la interfaz de comandos o CLI de manera local.

LEDs Indicadores

El equipo Catalyst 2950 cuenta con LED's que indican el estado de cada puerto, la utilización del Switch (UTIL), la velocidad y duplex de cada puerto.

Los LEDs de los puertos también indican el porcentaje de ancho de banda que esta siendo utilizado por el Switch en un momento determinado.

Tabla 4.5 - Características físicas y condiciones de operación

Característica	Descripción
Dimensiones	4.36 x44.45 x 24.18 cm (Altura, Ancho, Profundidad)
Peso	3.0 kg
Entrada de energía AC	100 - 127/200 -240 VAC
Humedad en operación	10 -85 % de humedad no condensada
Temperatura en operación	0 - 45 C
Temperatura soportada apagada	-25 - 70 C

4.3 Descripción del sistema operativo IOS

El equipo de enrutamiento dispone de un sistema operativo llamado *Internetwork Operating System* (IOS), el cual determina las funciones y protocolos que el Router será capaz de ejecutar, por ejemplo existen IOS específicos para el manejo de funciones de voz, o bien para aplicaciones de seguridad como firewalls, servidores de acceso remoto (RAS) o simplemente de enrutamiento. Las diferentes versiones de IOS están disponibles en la página de CISCO para sus socios comerciales, compradores de la tecnología mediante la orden de compra o bien para algunos profesionales con certificación CCIE (CISCO Certified Internetworking Expert). Este sistema operativo también funciona en Switches con sus respectivas diferencias de nivel de red, sin embargo la estructura es la misma. |Un ejemplo de la nomenclatura del archivo imagen IOS es el siguiente: **c3000-js-l_121-3.bin**

- 3000: es el modelo del Router, por ejemplo: 801, 1841, etc.
- js: es el conjunto de funciones (en este caso, empresa con capacidades extendidas)
- l: es el formato de archivo (en este caso, es reubicable y sin comprimir)

- 121-3: es el número de versión (en este caso, 12.13)

Interfaz de configuración.

Por seguridad, IOS establece diferentes sesiones de comando, cada una con distintos comandos.

- Modo de Usuario.
  - Identificable mediante el indicador “>”
  - Puede ejecutar comandos básicos de verificación de estado del sistema.
  - No puede reiniciar el sistema.

- Modo Privilegiado.
  - Identificable mediante el indicador “#”
  - Habilita al usuario para la configuración del sistema.
  - Se habilita mediante el comando enable.
  - Este modo es capaz de hacer cualquier modificación al sistema.

- Modo de configuración.
  - Permite a los usuarios la modificación de la configuración en ejecución.
  - Posee varios submodos
    - Modo de configuración global
      - Identificable mediante: *(config)#*

CAPÍTULO 5

DISEÑO E IMPLEMENTACIÓN DE ACTIVIDADES

En este capítulo presentamos el compendio diseñado de actividades para prácticas de laboratorio, la cual consiste de siete prácticas basadas en las actividades de laboratorio necesarias para preparar una certificación de nivel asociado de CISCO. Las ocho prácticas consisten de título, objetivo y desarrollo con actividades interactivas y con un enfoque autodidacta que permitirá al lector un desarrollo y aprendizaje autónomo. El presente capítulo se desarrolla presentando dichas actividades propuestas.

PRÁCTICA 1

INTRODUCCIÓN A LA CONFIGURACIÓN DE EQUIPOS DE RED

Objetivo.

El alumno se familiarizará con los equipos de red, su sistema operativo, interfaz de línea de comandos y además aprenderá a visualizar y trabajar con las características básicas y de configuración de los equipos del laboratorio y podrá hacer una configuración básica de sus interfaces.

Desarrollo.

1. Preparación para la configuración.

Mediante el cable de consola (cable azul con conectores RJ-45 y DB-9), conéctese al puerto de consola (RJ-45 hembra) del Router, el otro extremo será conectado al puerto serial de la computadora o mediante un adaptador al puerto USB (previa instalación de controladores).

Desde su terminal, ejecute el programa Hyperterminal o cualquier otra aplicación de terminal. Configure los siguientes parámetros de la terminal.

Parámetro	Valor
Nombre de la conexión	Asignado por el usuario
Método de conexión	Puerto COM
Tasa de transferencia	9600 bps
Bits de datos	8
Paridad	Ninguno
Bits de parada	1
Control de flujo	Ninguno

1.1 Nombre de la conexión.

1.2 Mecanismo de conexión, en este caso utilizaremos el acceso local mediante un puerto de nuestra computadora, es decir, el puerto al cual hemos conectado el conector DB-9 del cable de consola.

1.3 Ahora la tarea consiste de ajustar los parámetros de transmisión que manejan los equipos CISCO en sus interfaces de consola.

1.4 Una vez logrado lo anterior, oprima la tecla aceptar y encienda el Router, deberá ver salida similar a la siguiente:

System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fc1)
Copyright (c) 2000 by cisco Systems, Inc.
cisco 2811 (MPC860) processor (revision 0x200) with **60416K/5120K bytes of memory**

Self decompressing the image :
######################System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fc1)
Copyright (c) 2000 by cisco Systems, Inc.
cisco 2811 (MPC860) processor (revision 0x200) with 60416K/5120K bytes of memory

Self decompressing the image :
[OK]
Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706

Cisco IOS Software, 2800 Software (C2800NM-IPBASE-M), Version 12.3(14)T7, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Wed 22-Mar-06 18:40 by pt_team
Image text-base: 0x40095498, data-base: 0x414E0000

cisco 2811 (MPC860) processor (revision 0x200) with 60416K/5120K bytes of memory
Processor board ID JAD05190MTZ (4292891495)
M860 processor: part number 0, mask 49
2 FastEthernet/IEEE 802.3 interface(s)
239K bytes of non-volatile configuration memory.
62720K bytes of processor board System flash (Read/Write)
Cisco IOS Software, 2800 Software (C2800NM-IPBASE-M), Version 12.3(14)T7, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Wed 22-Mar-06 18:40 by pt_team

--- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]: N

```
Press RETURN to get started!

Router>
```

Deberá interrumpir el dialogo de configuración debido a que este se utiliza para funciones avanzadas fuera del alcance de este laboratorio.

1.5 Identifique los siguientes valores de su equipo:

Versión de bootstrap.	
Versión de sistema operativo.	
Interfaces conectadas.	
Capacidad de memoria RAM utilizada disponible y total.	
Capacidad de memoria FLASH y su estado.	
Capacidad de memoria NVRAM.	

2. Verificación de características del equipo mediante el IOS, estructura y niveles en IOS

2.1 Verifique que se encuentra en el modo EXEC de usuario (Router>), visualice los comandos disponibles mediante el comando de ayuda (?). *Deberá observar* una salida similar a la siguiente:

```
Router>?
Exec commands:
  <1-99>     Session number to resume
  connect    Open a terminal connection
  disconnect  Disconnect an existing network connection
  enable     Turn on privileged commands
  exit       Exit from the EXEC
  logout     Exit from the EXEC
  ping       Send echo messages
  resume     Resume an active network connection
  show       Show running system information
  telnet     Open a telnet connection
  traceroute  Trace route to destination
```

2.2 Trabaje con el comando show para visualizar las diferentes características de su equipo:

```
Router>show ?
```

2.3 Una vez identificadas las diferentes opciones de visualización, entre al modo de usuario privilegiado mediante el comando **enable.**

```
Router>enable
Router#
```

2.4 Visualice los comandos disponibles del modo privilegiado mediante el comando correspondiente.

2.5 Desde el modo privilegiado, ejecute el comando **show versión** para visualizar las características del equipo. Su salida deberá ser similar a la siguiente:

```
Router#show version
Cisco IOS Software, 2800 Software (C2800NM-IPBASE-M), Version 12.3(14)T7, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Wed 22-Mar-06 18:40 by pt_team

ROM: System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fc1)
Copyright (c) 2000 by cisco Systems, Inc.

System returned to ROM by power-on
System image file is "flash:c2800nm-ipbase-mz.123-14.T7.bin"

cisco 2811 (MPC860) processor (revision 0x200) with 60416K/5120K bytes of memory
Processor board ID JAD05190MTZ (4292891495)
M860 processor: part number 0, mask 49
2 FastEthernet/IEEE 802.3 interface(s)
239K bytes of NVRAM.
62720K bytes of processor board System flash (Read/Write)

Configuration register is 0x2102
```

2.6 Determine cuales son los parámetros que también puede visualizar al arrancar el equipo y observe los siguientes:

Parámetro	Valor
Contenido de la memoria ROM y ultimo acceso	
Nombre del archivo del sistema operativo	
Función específica del IOS	
Registro de configuración	

Comandos de monitoreo del sistema.

Comando	Descripción
show interface	Despliega el estado y configuración actual de la interfaz invocada
show processes cpu	Despliega la utilización del CPU y los procesos que se están ejecutando actualmente.
show buffers	Muestra los buffers del sistema y su funcionamiento de acuerdo al reenvío de paquetes.
show memory	Muestra el contenido de la memoria, utilización y funciones
show diag	Despliega los detalles de las tarjetas del sistema.
show ip route	Despliega la table de enrutamiento actual.
show arp	Despliega la table de ARP

2.7 Una vez identificados los parámetros anteriores, visualice la configuración actual del equipo mediante el comando **show running-config,** deberá obtener una salida similar a la siguiente.

```
Router#show running-config
Building configuration...

Current configuration : 332 bytes
!
version 12.3
no service password-encryption
!
hostname Router
!
!
!
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
ip classless
!
!
!
!
line con 0
line vty 0 4
 login
!
!
end
```

2.8 Determine el valor de los siguientes parámetros.

Parámetro	Valor
Tamaño del archivo de configuración	
Hostname del equipo	
Estado de alguna interfaz	

2.9 Visualice la configuración de inicio o **startup-config**, mediante el comando **show startup-config**. Deberá obtener una salida similar a la siguiente.

```
Router#show startup-config
startup-config is not present
```

Note que no existe configuración de inicio, debido a que es la primera vez que inicia el Router, deberá copiar la configuración actual a la de inicio mediante los comandos apropiados.

```
Router#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

2.10 Ingrese al modo de configuración global mediante el comando **configure terminal.**

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

2.11 Verifique los comandos disponibles del modo de configuración global.

2.12.1 Desde el modo de configuración global, habilite la seguridad para el modo privilegiado mediante el password y en enable password.

```
Router(config)#enable password cisco1
Router(config)#enable secret cisco2
```

2.12.2 Vea la configuración activa y guarde los cambios en la configuración de inicio (**Router#copy running-config startup-config**). Identifique los passwords de **enable** y el **enable secret**. Verifique que ha sido encriptado el password especificado como **secret**.

2.12.3 Salga del modo de configuración global y del modo privilegiado e intente ingresar nuevamente al modo privilegiado, describa que es lo que sucede.

---

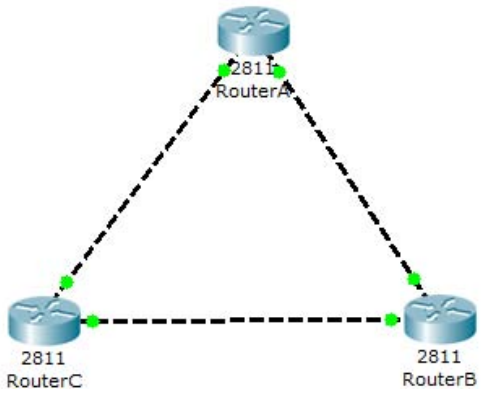
3. Configuración básica de interfaces.

Esta actividad deberá ser desarrollada en colaboración con algún otro equipo.

3.1 Desde el Router asignado, configure la primer y segunda interfaces FastEhternet de acuerdo a la siguiente tabla, el otro equipo deberá hacer lo propio.

Equipo	IP Fa0/0	IP Fa0/1
A	10.1.1.1/24	10.1.2.1/24
B	10.1.2.2/24	10.1.3.1/24
C	10.1.3.2/24	10.1.1.2/24

Implemente la siguiente topología.



Recuerde que los equipos de la misma familia se conectan mediante cables UTP cruzados.

```
RouterA(config)#interface fastethernet0/0
RouterA(config-if)#ip address 10.1.1.1 255.255.255.0
RouterA(config-if)#no shutdown
RouterA(config-if)#exit
RouterA(config)#interface fastethernet0/1
RouterA(config-if)#ip address 10.1.2.1 255.255.255.0
RouterA(config-if)#no shutdown
```

3.2 Mediante un ping compruebe conectividad de la conexión.

```
RouterA#ping 10.1.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/6 ms
```

NOTA: Podrá verificar conectividad solamente con las direcciones pertenecientes a las subredes en las que el Router tenga sus interfaces, de lo contrario, se requeriría la habilitación de enrutamiento estático o de algún protocolo de enrutamiento.

¿Resultó exitoso el ping?, en caso contrario, verifique su procedimiento y corrija el problema.

PRÁCTICA 2

INTERCONEXIÓN Y CONFIGURACIÓN DEL SWITCH

Objetivo.

El alumno aprenderá a configurar los puertos del Switch, realizara la interconexión, trabajara con las características de LAN Switching

Desarrollo

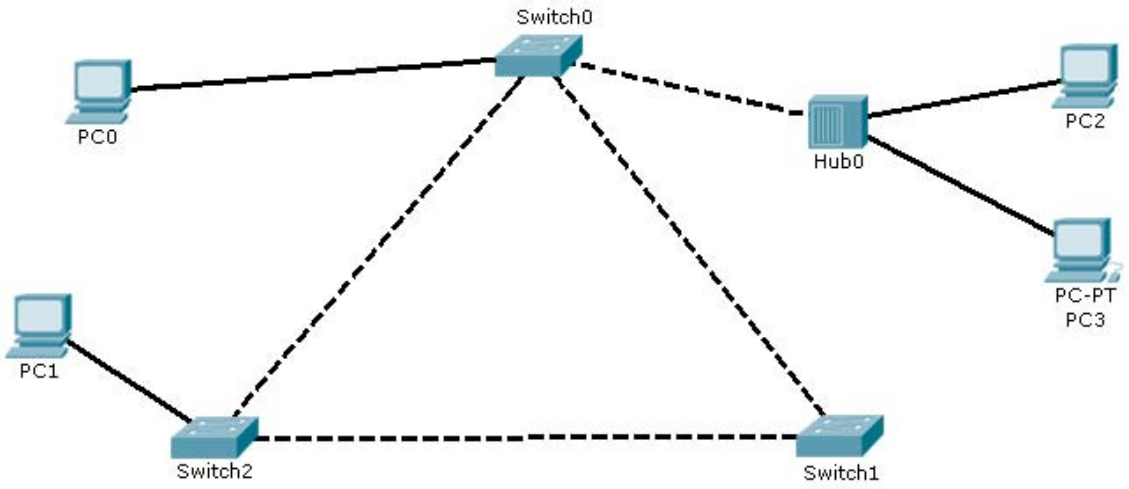
1. Configuración básica del Switch.

A continuación se muestra una tabla con los comandos más relevantes de un Switch.

Comando	Descripción
interface vlan 1	Comando global. Sitúa al usuario en modo de configuración de una interfaz VLAN.
ip address *dirección máscara_de_subred*	Comando de configuración de interfaz que fija la IP para administración del Switch.
ip default-gateway *dirección*	Comando global que fija la puerta de enlace predeterminada para que la interfaz de administración pueda ser alcanzada desde una red que no esté directamente conectada (red remota).
interface fastethernet *0/x*	Si el usuario se encuentra en modo de configuración global este comando permite al usuario entrar a la configuración de la interface elegida.
duplex { *auto* | *full* | *half* }	Comando que fija el modo duplex de una interfaz.
speed { *10* | *100* | *1000* | *auto* | *nonegotiate* }	Comando que fija la velocidad de una interfaz.
switchport port-security mac-address *dirección-mac*	Comando que agrega de manera estática una dirección MAC como una dirección MAC permitida a ser atendida por el Switch.
switchport port-security mac-address sticky	Realiza la misma función que el comando anterior con la diferencia de que no es necesario especificar la dirección MAC del equipo que se desea agregar, sino que la dirección MAC se agrega automáticamente de la primer trama que llega por la interfaz.
switchport port-security maximum *valor*	Fija el número máximo de direcciones estáticas MAC seguras que pueden ser asignadas a una interfaz.
switchport port-security violation { protect | restrict | shutdown }	Indica que acción debe de realizar el Switch en la interfaz cuando una MAC que no esta autorizada trata de acceder a un puerto seguro.

Cabe mencionar que el Switch por contar con un IOS, tiene comandos de operación y despliegue de información como show, hostname, enable password, enable secret, entre otros.

Construya la topología de la figura 2.5 para realizar las siguientes actividades.



Configuración de interfaces y seguridad.

-Ingrese a la línea de comandos del Switch0
-Observe el contenido de la tabla de direcciones MAC por medio del comando *show mac-address-table*.

El resultado deberá ser parecido al siguiente:

```
                Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
```

Hay un comando que indica al switch que debe de hacer cuando una dirección MAC no permitida trata de utilizar una interfaz y ese comando es **switchport port-security violation shutdown**, este comando indica al Switch que debe de apagar la interfaz cuando este bajo las circunstancias antes mencionadas.

-Observe la configuración inicial del Switch por medio del comando *show running-config.*

-Ejecute los siguientes comandos en el Switch0:

```
enable
configure terminal
interface vlan 1
ip address 10.1.1.1 255.255.255.0
exit
interface fastethernet 0/3
```

speed 100
duplex half
switchport mode access
switchport port-security
switchport port-security mac-address 000A.419D.DABC

Lo primero que hacen estos comandos es fijar la dirección IP de la VLAN, después se configura la velocidad y el modo duplex de la interfaz fastethernet 0/3 por medio de los comandos “speed” y ”duplex” respectivamente.

Los últimos 3 comandos permiten indicar al Switch que dicha interfaz trabajará en modo de acceso únicamente (y no en modo “troncal”), que debe de habilitar la seguridad en la interfaz y que la dirección MAC *000A.419D.DABC* puede enviar y recibir tramas por dicha interfaz, respectivamente.

Ahora la tabla de direcciones MAC deberá verse de la siguiente manera:

Mac Address Table

Vlan	Mac Address	Type	Ports
1	000a.419d.dabc	STATIC	Fa0/3

- Repita los 3 últimos pasos en la interfaz fastethernet 0/4 para que acepte el tráfico del equipo terminal **PC2**, llene la siguiente tabla con el contenido de la tabla de direcciones MAC del Switch0 y explique brevemente el porque del contenido de la tabla.

Vlan	MAC Address	Type	Ports

¿A qué cree que se refiera el término “Type”?, explique.

- Ejecute el comando **switchport port-security mac-address sticky** en alguna interfaz y vea la tabla de direcciones MAC antes y después del comando. Anote sus comentarios.

-Observe y guarde la configuración actual (*running-config*) en la configuración de arranque del Switch0 (*startup -config*), que diferencias nota en esta configuración ahora y cuando la observo al inicio de la práctica, anote sus observaciones.

2. Interconexión de Switches mediante configuraciones redundantes

De la topología de la figura 2.5, observe su configuración actual del STP (Spanning Tree Protocol) por medio del comando **show spanning-tree** en cada Switch y deduzca por medio de los Bridge ID y de las direcciones MAC de los Switches cual es la interfaz que esta en estado de "bloqueo" y cual es el "Switch root".

La interfaz _____ del Switch _____ está en estado de bloqueo.
El Switch _____ es el Switch root.

A continuación ejecute los siguientes comandos en alguno de los Switches que no es el Switch root (llamado de aquí en adelante Switchx).

```
Switchx#debug spanning-tree                          //No ejecutar en simulador
Switchx#configure terminal
Switchx(config)#spanning-tree vlan 1 root primary    //No ejecutar en simulador
Switchx(config)#spanning-tree vlan 1 priority 24576  // Dato de simulador, Probar línea anterior en el equipo.
```

Por medio de estos comando se obliga al Switch que se esta configurando a ser el *Switch root* disminuyendo su número de prioridad.
Espere unos minutos a que se estabilice la red y mande un ping desde cualquier Switch a los otros dos para comprobar que hay conectividad y corra el comando **show spanning-tree** en el nuevo Switch root y en el anterior para comprobar que la MAC del Switch root es ahora la del Switch.

PRÁCTICA 3

FUNCIONES EXTENDIDAS DEL SWITCH

Objetivos

El alumno se familiarizará con los conceptos de VLAN, VLAN troncales, el protocolo IEEE 802.1Q, y con el Virtual Trunking Protocol.

Además será capaz de configurar:

- VLANs en el Switch
- VLANs troncales en la topología de Switches
- Dominios, clientes y un servidor VTP
- Comprobar separación de tráfico y conectividad.

Desarrollo:

1. *Configuración de VLANs en el Switch.*

Creará una VLAN y le asignará un puerto (puerto de acceso)

1.1 Desde la base de datos de VLANs, configure una nueva VLAN, llamada VLANx, donde x es el número de su brigada, por ejemplo, si usted forma parte de la brigada 10, su VLAN deberá llamarse VLAN10.

Se ha reservado el número de equipo 1 para la VLAN nativa.

```
Switch10#vlan database
Switch10(vlan)#vlan 10 name VLAN10
VLAN 3 added:
   Name: VLAN10
Switch10(vlan)#apply
APPLY completed
Switch10(vlan)# ^Z
Switch10#
```

1.2 Verifique la creación correcta de la VLAN desde el modo privilegiado mediante el comando show **vlan brief**.

```
Switch10#show vlan brief

VLAN  Name                             Status    Ports
----  -------------------------------- --------- -------------------------------
1     default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gig1/1, Gig1/2
```

10	**VLAN10**	**active**
1002	fddi-default	active
1003	token-ring-default	active
1004	fddinet-default	active
1005	trnet-default	active

Nótese que todos los puertos se encuentran en la VLAN 1, esta es una característica de los Switches CISCO, por lo tanto deberá agregar puertos a las VLANs que vaya creando.

1.3 Desde la interfaz de algún puerto, configúrelo como puerto de acceso y agréguelo a la VLAN que acaba de ser creada.

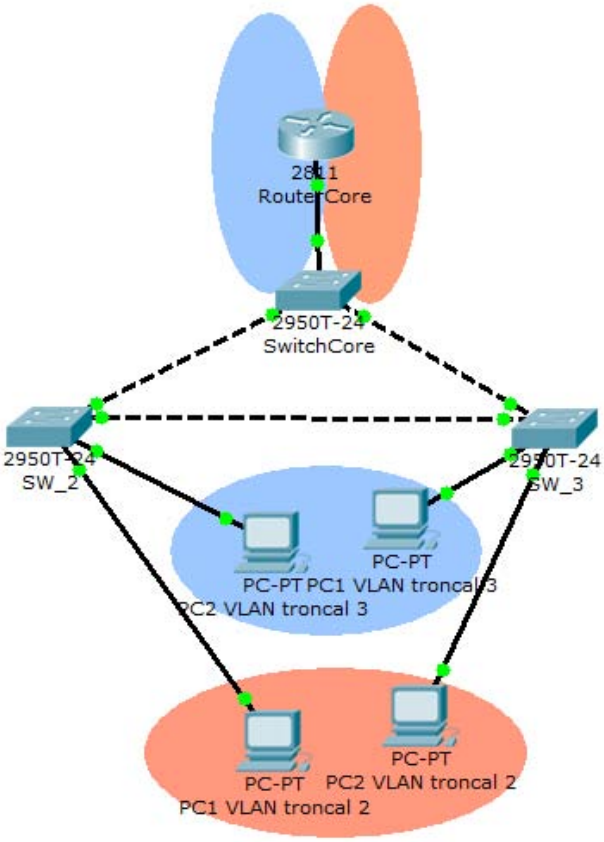
```
Switch10(config-if)#switchport mode access
Switch10(config-if)#switchport access vlan 10
```

1. 4 Verifique que el puerto ha sido correctamente agregado a la VLAN adecuada

VLAN	Name	Status	Ports
1	default	active	Fa0/2, Fa0/3, Fa0/4, Fa0/5 Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/11, Fa0/12, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/18, Fa0/19, Fa0/20, Fa0/21 Fa0/22, Fa0/23, Fa0/24
10	**VLAN10**	**active**	**Fa0/1**
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

2. *Configuración de VTP en el Switch y VLANs troncales.*

Disponga de los equipos según la siguiente topología.



Las VLANs troncales serán configuradas en colaboración con el profesor y todo el grupo en el SwitchCore disponiéndolo en modo servidor y en el RouterCore, lo cual facilitará la creación de VLANs en cada Switch de la red mediante el VTP. *Por facilidad y orden se recomienda que siga las tablas de conexiones y de direccionamiento proporcionadas al final de la práctica.*

2.1 *Configuración del servidor VTP, las VLANs y puertos troncales*

2.1.1 En el SwitchCore, desde la base de datos de VLAN Configure un nuevo dominio VTP llamado: *DOMINIO_VTP* y habilite el SwitchCore como servidor VTP.

```
SwitchCore(vlan)#vtp domain DOMINIO_VTP
Changing VTP domain name from NULL to DOMINIO_VTP
SwitchCore(vlan)#vtp  server
Setting device to VTP SERVER mode
```

2.1.1.2 Verifique la correcta asignación de dominio VTP y operación en modo servidor del SwitchCore mediante el comando **show vtp status**, su salida deberá ser similar a la siguiente.

```
SwitchCore#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 64
Number of existing VLANs        : 5
VTP Operating Mode              : Server
VTP Domain Name                 : DOMINIO_VTP
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
```

```
VTP Traps Generation                : Disabled
MD5 digest                          : 0x7D 0xC1 0xCF 0x2A 0x31 0x72 0x49 0xFC
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)
```

2.1.2 Ahora desde la misma base de datos de VLANs, configure un par de VLANs, llamadas VLAN2 y VLAN3 y verifique su correcta creación.

¿Pudo crear las VLANs?

Describa con sus propias palabras como lograrlo y la forma de verificar.

En caso contrario verifique el procedimiento efectuado en la actividad 1.1 y 1.2. Compruebe su correcta creación.

¿Pudo crear las VLANs?, ¿Por qué?

En caso contrario pida ayuda al profesor y recuerde que el comando -?- muestra los comandos del modo en el que se encuentra.

2.1.2.2 Configure el direccionamiento adecuado a cada interfaz VLAN, de acuerdo con la tabla de direccionamiento.

2.1.3 Ingrese a los puertos del SwitchCore que conectan con los Switches SW1 y SW2 (Fa0/22 y Fa0/23 del SwitchCore), y configúrelos como puertos troncales con encapsulamiento dot1Q, para transportar el tráfico de **todas** las VLANs.

```
SwitchCore(config-if)#switchport mode trunk
SwitchCore(config-if)#switchport trunk allowed vlan all
```

2.1.4 Compruebe que los puertos han desaparecido de las VLANs mediante el comando **show vlan brief** y mediante el comando **show interfaces fa0/22 switchport**, verifique que ha configurado adecuadamente los puertos troncales, su salida deberá ser similar a la siguiente:

```
SwitchCore#show interfaces fa0/22 switchport
Name: Fa0/22
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
```

```
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Appliance trust: none
```

¿Logró que ambas interfaces desplegaran información similar a la que se acaba de presentar?, de lo contrario revise su procedimiento y corrija el problema, deberá tener la interfaces que conectan con los Switches SW2 y SW3 en modo troncal con encapsulamiento dot1q.

2.2 *Configuración de subinterfaces con encapsulamiento troncal para la comunicación inter VLAN.*

ESTA ACTIVIDAD SERÁ REALIZADA POR EL PROFESOR MEDIANTE LA PARTICIPACIÓN DEL GRUPO.

2.2.1 En el RouterCore y desde el modo de configuración global, disponga de subinterfaces de la interfaz física que lo conecta al SwitchCore, habilite un par de ellas asignándolas a la VLAN adecuada, asigne direccionamiento según la tabla de direccionamiento de la actividad 2.4 y habilítelas.

```
RouterCore(config)#interface fa0/0.2
Router(config-subif)#encapsulation dot1Q 2
```

Compruebe la correcta creación, encapsulamiento y direccionamiento de las subinterfaces mediante el despliegue de la configuración activa y de los detalles de las interfaces IP mediante los comandos **show running-config** y el estado mediante **show ip interfaces brief**, deberá visualizar una salida similar a las siguientes:

```
Router#sh run
Building configuration...

Current configuration : 495 bytes
!
version 12.3
no service password-encryption
!
hostname Router
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface FastEthernet0/0.1
 encapsulation dot1Q 1
 ip address 10.1.1.1 255.255.255.0
```

2.3 *Configuración de los Switches cliente y habilitación de los puertos troncales y de acceso.*

Deberá deshabilitar las interfaces que interconectan a los Switches SW2 y SW3, para evitar que el STP disponga de la topología.

Cada brigada deberá configurar el Switch correspondiente, y los pasos a seguir son los siguientes:

2.3.1 Desde la base de datos de VLANs, determine el dominio VTP, llamado DOMINIO_VTP, en modo cliente.
Verifique de acuerdo al punto 2.1.1.2

Escriba los pasos a seguir para lograr lo anterior (no escriba los comandos).

2.3.2 Desde la interfaz que conecta su Switch con SwitchCore, configure como puerto troncal de encapsulamiento dot1q y compruebe las acciones realizadas.

Escriba los pasos a seguir para lograr lo anterior (no escriba los comandos).

2.3.3 Desde las interfaces (puertos del Switch) que conectan con los PCs, configure como puertos de acceso y dispóngalos en las VLANs determinadas según la siguiente tabla de VLANs y puertos de acceso (ver punto 1.3).

Equipo	PC	Interfaz	VLAN
SW2	PC1 VLAN T. 2	Fa0/2	2
SW2	PC2 VLAN T. 3	Fa0/3	3
SW3	PC1 VLAN T. 3	Fa0/2	2
SW#	PC2 VLAN T. 2	Fa0/3	3

Escriba los pasos a seguir para lograr lo anterior (no escriba los comandos).

Llene la siguiente tabla con los comandos necesarios para realizar las acciones mencionadas.

Acción	Comando	Nivel en IOS
Configuración del dominio VTP		
Disposición del equipo como cliente VTP		
Configuración del puerto en modo troncal (2 líneas de comando)		
Configuración de los puertos en modo acceso		
Configuración de los puertos en modo acceso en la VLANs adecuadas		
Verificación de la operación VTP		
Verificación de la operación de interfaces en modo troncal		

2.4 *Comprobación de la conectividad en las VLANs troncales.*

Asigne el direccionamiento a cada PC indicado en la tabla de direccionamiento.

Nota: las interfaces del RouterCore y del SwitchCore deberán ser asignadas por el profesor con la ayuda de todo el grupo.

Compruebe conectividad mediante un ping desde un equipo (desde el CMD) en la VLAN2 hasta otro equipo en el Switch vecino también en la VLAN2. **Asegúrese de que NO existe dispositivo Firewall que impida la comunicación entre los PCs.**

Para finalizar la actividad deberá verificar la comunicación entre miembros de las mismas VLAN y con las interfaces virtuales en el RouterCore, y solamente para ilustrar la función del RouterCore, compruebe la conectividad inter VLAN.

Tabla de conexiones.

Equipo 1	Interfaz	Equipo 2	Interfaz
RouterCore	Fa0/0	SwitchCore	Fa0/1
SwitchCore	Fa0/22	SW2	Fa0/22
SwitchCore	Fa0/23	SW3	Fa0/23
SW2	Fa0/2	PC1 VLAN T. 2	Fa
SW3	Fa0/2	PC2 VLAN T. 2	Fa
SW3	Fa0/3	PC1 VLAN T. 3	Fa
SW2	Fa0/3	PC2 VLAN T. 3	Fa
SW2	Fa0/10	SW3	Fa0/10

Tabla de direccionamiento:

Equipo	Interfaz	Direccionamiento
RouterCore	Fa0/0.2	10.1.2.2/24
	Fa0/0.3	10.1.3.2/24
SwitchCore	VLAN2	10.1.2.1/24
	VLAN3	10.1.3.1/24
PC1 VLAN troncal 2	Fastethernet	10.1.2.10/24
PC2 VLAN troncal 2	Fastethernet	10.1.2.11/24
PC1 VLAN troncal 3	Fastethernet	10.1.3.10/24
PC2 VLAN troncal 3	Fastethernet	10.1.3.11/24

PRÁCTICA 4

INTERCONEXIÓN DE ROUTERS MEDIANTE ENLACES WAN

Objetivo

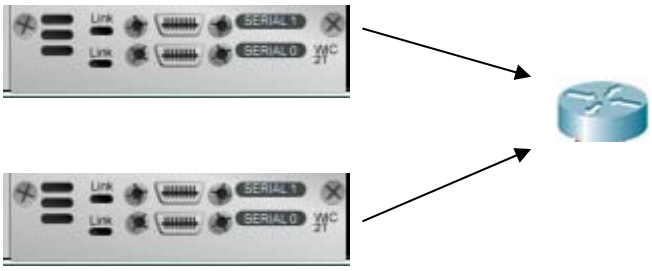
El alumno se familiarizará con los protocolos y conexiones de los enlaces WAN además de:

- Configurará unos enlaces WAN mediante el protocolo por defecto (HDLC) de las interfaces seriales del Router C2811, mediante la asignación de direccionamiento y disposición de las interfaces DCE y DTE.
- Comprobará conectividad.
- Configurará unos enlaces WAN mediante el protocolo PPP, mediante la asignación de direccionamiento y disposición de las interfaces DCE y DTE.
- Comprobará conectividad.
- Asignará el mecanismo de autenticación CHAP a los enlaces.
- Comprobará conectividad

Desarrollo:

1. Estando los equipos apagados, instale dos de las interfaces seriales con que se disponen en los slots 0 y 1.

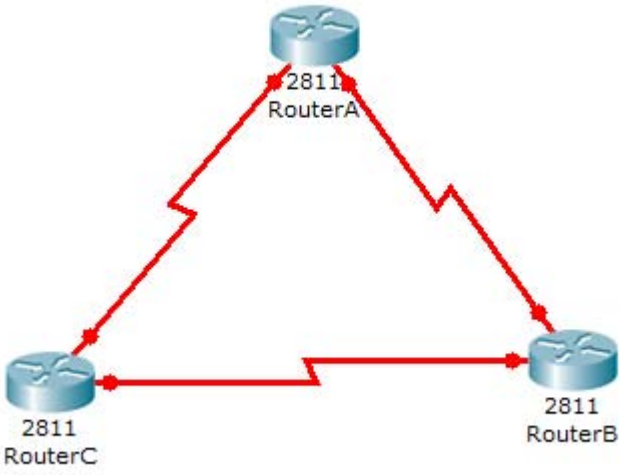
NOTA: Recuerde siempre sujetar las interfaces por el lado que tiene los conectores, es decir, no toque los componentes electrónicos de la tarjeta ya que podría dañarla de manera irreparable.



Asegúrese de haber atornillado adecuadamente los sujetadores y no forzar la entrada.

1.1 Implemente la topología mostrada en la siguiente figura de acuerdo a la tabla de conexiones adjunta al final de la práctica:

1.2 Sin haber encendido los equipos deberá conectar los extremos Smart Serial a las interfaces seriales de tal y los conectores hembra V.35 a los conectores V.35 macho de acuerdo con la tabla de conexiones mostrada al final de la práctica; a este tipo de conexiones se les conoce como Back to Back.



NOTA: Recuerde que una conexión serial WAN siempre tiene un extremo DTE y un extremo DCE.

1.3 Desde el modo de usuario privilegiado, asegúrese que dispone del tipo de cables seriales conectados, es decir, compruebe que conectó un extremo DTE o DCE al la interfaz respectiva.

```
RouterX#show controllers serial 0/0/0
Interface Serial0/0/0
Hardware is PowerQUICC MPC860
DCE V.35, no clock
idb at 0x81081AC4, driver data structure at 0x81084AC0
SCC Registers:
General [GSMR]=0x2:0x00000000, Protocol-specific [PSMR]=0x8
```

>> Se han omitido líneas por el momento innecesarias.

```
RouterX#show controllers serial 0/0/0
Interface Serial0/0/0
Hardware is PowerQUICC MPC860
DTE V.35, no clock
idb at 0x81081AC4, driver data structure at 0x81084AC0
SCC Registers:
General [GSMR]=0x2:0x00000000, Protocol-specific [PSMR]=0x8
```

>> Se han omitido líneas por el momento innecesarias.

1.4 Desde cada una de las interfaces configure la frecuencia de reloj que proveerá cada una de las interfaces DCE a 64000 y habilítela.

NOTA: Si usted dispone del RouterC, esta tarea no será necesaria dado que ninguna de sus interfaces será DCE.

```
RouterX(config-if)#clock rate 64000
```

Verifique que ha configurado adecuadamente el reloj de la interfaz mediante el comando **show controllers interfaces serial X**.

```
RouterX#show controllers serial 0/0/0
Interface Serial0/0/0
Hardware is PowerQUICC MPC860
DCE V.35, clock rate 64000
idb at 0x81081AC4, driver data structure at 0x81084AC0
SCC Registers:
```

>> Se han omitido líneas por el momento innecesarias.

1.5 Asigne el direccionamiento a cada interfaz serial especificado por la tabla de direccionamiento adjunta al final de la práctica.

1.6 Habilite las interfaces y muestre que realmente han sido activadas todas las interfaces, es decir hay conectividad con el otro extremo del router correspondiente. Recuerde que comandos utilizar para verificar estado y direccionamiento de interfaces, elija entre los comandos **show ip interface brief** y el comando **show running-config** y diga cual es mas conveniente en este caso y porque.

1.7 Compruebe conectividad mediante ping a todas las interfaces directamente conectadas.

En caso de que no tenga conectividad revise su configuración y trate de corregir el problema, en dado caso que no logre encontrar la falla, pida ayuda al profesor.

1.8 Mediante el comando **show interface serial X**, verifique el tipo de protocolo de encapsulamiento utilizado por las interfaces seriales y diga si PPP es el protocolo por defecto en las interfaces WAN CISCO y en su defecto diga cual es el protocolo.

2. Configuración de PPP

2.1 Asigne el tipo de encapsulamiento de enlace WAN PPP a cada una de las interfaces seriales del router, observe que este proceso deshabilita las interfaces, por lo tanto deberá habilitarlas.

```
RouterX(config-if)#encapsulation ppp
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down
RouterX(config-if)#no shutdown
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to u
```

2.2 Verifique conectividad con los vecinos.

3. Seguridad en los enlaces

3.1 Una vez verificada la conectividad en la red WAN, deshabilite las interfaces.

3.2 Desde el nivel de configuración global, habilite el nombre de usuario que el router vecino tiene como hostname y la contraseña cisco
Por ejemplo si esta configurando desde el RouterA el enlace con el RouterC, el username deberá ser RouterC

```
RouterA(config)#username RouterC password cisco
```

3.3 Habilite la autenticación CHAP del protocolo PPP para todos los enlaces de la red.

```
RouterA(config-if)#ppp authentication chap
```

3.4 Habilite las interfaces y compruebe conectividad.

Llene la siguiente tabla con los comandos necesarios para realizar las acciones mencionadas.

Acción	Comando	Nivel en IOS
Verificación del tipo de cable serial conectado a la interfaz		
Verificación de estado de conectividad interfaces		
Verificación del protocolo de encapsulamiento WAN utilizado en el enlace		
Configuración de PPP		
Habilitación de la seguridad CHAP en PPP		

Tabla de conexiones y direccionamiento:

Conexión [RouterX-RouterY]	Conector de Interfaz Router X /Dirección		Conector de Interfaz Router Y/Dirección	
RouterA-RouterB	DCE	11.1.2.1/24	DTE	11.1.2.2/24
RouterA-RouterC	DCE	11.1.1.1/24	DTE	11.1.1.2/24
RouterB-RouterC	DCE	11.1.3.1/24	DTE	11.1.3.2/24

PRÁCTICA 5

INTERCONEXIÓN Y CONFIGURACIÓN DE ENRUTAMIENTO ESTÁTICO Y RIP

Objetivo.

El alumno comprenderá:

- El funcionamiento básico del enrutamiento.
- Clasificación de los mecanismos de enrutamiento.
- El protocolo RIP.

Configurará enrutamiento:

- Estático.
- Dinámico (por medio de RIP).

Finalmente comprobará la implementación realizada mediante pruebas de conectividad ICMP.

Desarrollo.

1. Enrutamiento estático.

Implemente la topología de la figura 4.1

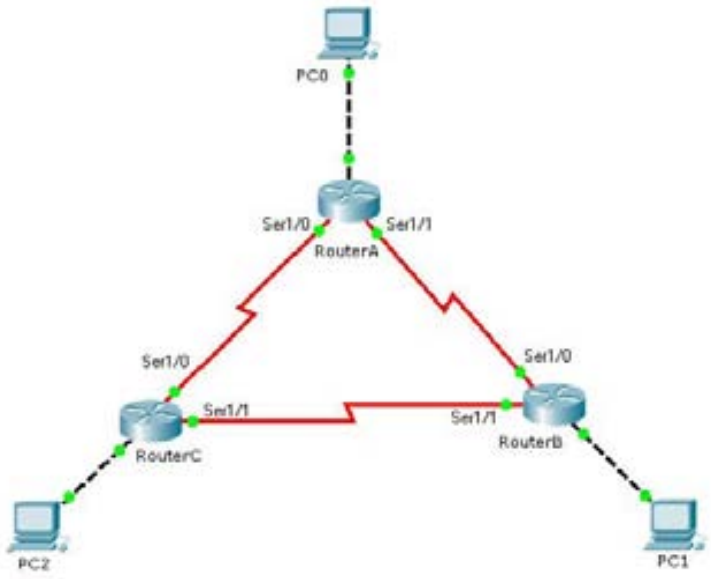


Figura 4.1

Tabla de direccionamiento:

Equipo	IP Serial 1/0	IP Serial 1/1
A	11.1.1.1/24	11.1.2.1/24
B	11.1.2.2/24	11.1.3.1/24
C	11.1.1.2/24	11.1.3.2/24

Verifique conectividad mediante un ping del RouterA a la interfaz Serial 1/1 del RouterC (11.1.3.2).

Deberá ver una salida como la siguiente:

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.32.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

Lo anterior indica que no se obtuvo una respuesta exitosa del ping, ¿a qué cree que se deba?, anote sus comentarios.

(Vea la tabla de enrutamiento (show ip route) detenidamente ya que la comparará con ella misma después de la configuración estática de una ruta).

Ahora configuraremos la ruta que nos permita acceder a la interfaz Serial 1/1 del RouterC mediante los siguientes comandos.

RouterA#configure terminal
RouterA(config)#ip route 11.1.3.0 255.255.255.0 Serial 1/0 //Nativo de simulador
RouterA(config)#ip route 11.1.3.0 255.255.255.0 11.1.1.0 //No ejecutar en simulador
RouterA(config)#exit

Al procedimiento anterior se le llama ***enrutamiento estático***.

Compruebe conectividad de nuevo, ¿Tuvo éxito el ping?, de no haber sido así a qué piensa que se deba, anote sus comentarios.

Vea la tabla de enrutamiento y note que hay una nueva ruta.

3. Configuración de RIP y RIP V2

Para configurar RIP se requiere utilizar el comando *"router rip"* desde el modo de configuración global, además de anunciar las redes que se quieren agregar a los mensajes de actualización que se mandan los Routers, esto último se hace mediante el comando "network A.B.C.D", donde A.B.C.D es la IP de la subred que se desea anunciar.

Es importante mencionar que cuando hay una falla en el funcionamiento de RIP y queremos buscarla, podemos utilizar el comando ***debug ip rip events***, este comando es de gran ayuda ya que nos muestra la información contenida en los mensajes de actualización de RIP, gracias a lo cual podemos saber si dichos mensajes están llegando, si el Router esta enviando sus mensajes de actualización, también podemos saber que redes se están anunciando.

Los siguientes comandos configuran RIP en el RouterA para que anuncie todas las subredes de la topología de la figura 4.1, analice los comandos y haga lo mismo para las subredes de los Routers B y C.

RouterA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
RouterA(config)#router rip
RouterA(config-router)#network 172.16.30.0
RouterA(config-router)#network 11.1.1.0
RouterA(config-router)#network 11.1.2.0
RouterA(config-router)#exit
RouterA(config)#exit

Se propone al alumno investigar las ventajas y desventajas de RIP V2 y compararlas con las de la primera versión de RIP.

4. Pruebas de conectividad

Una vez configurado RIP en los tres Routers, compruebe conectividad entre las 6 interfaces seriales, anote sus comentarios.

Si ya comprobó que hay conectividad, introduzca los siguientes comandos en modo privilegiado de la línea de comandos de cualquier Router, analice la salida de la pantalla y explique que piensa que significa esa información.

RouterB#show ip rip database

Por último, ejecute el comando *traceroute A.B.C.D* desde el modo privilegiado, donde A.B.C.D puede ser la dirección IP de cualquier interfaz serial de algún Router. El resultado obtenido será una lista con las direcciones IP de las interfaces por las cuales tendría que pasar un paquete para llegar a un destino determinado (en este caso A.B.C.D).

PRÁCTICA 6

INTERCONEXIÓN Y CONFIGURACIÓN DE PROTOCOLO DE ENRUTAMIENTO OSPF

Objetivo

Que el alumno sea capaz de realizar:

- La configuración de OSPF en una red delta.
- El aseguramiento de la conectividad

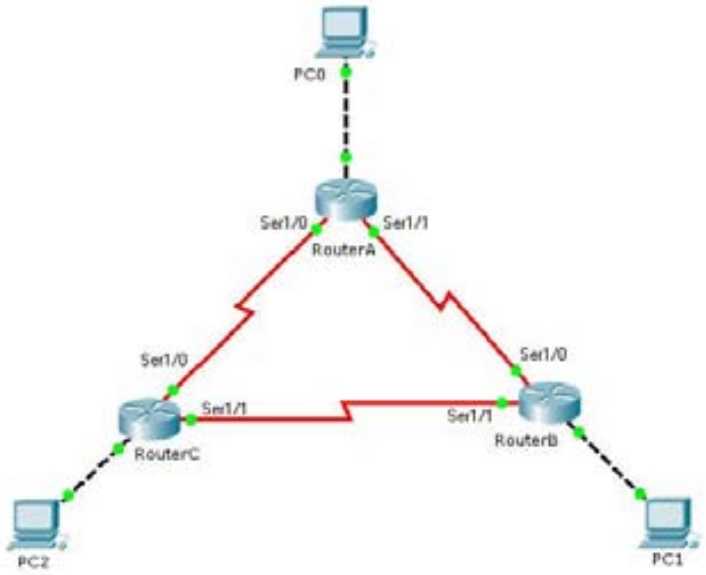
  La configuración de los equipos para el acceso remoto mediante TELNET

Desarrollo

Deberán formarse tres grupos de trabajo, cada uno dispondrá de un router y una PC que servirá como interfaz de configuración y nodo de la topología.

Configuración de OSPF en una red delta y aseguramiento de la conectividad

1. Realice el direccionamiento se indicado en la tabla adjunta al final de la práctica y el proceso deberá, además habilite y direccione la interfaz Loopback 0 de cada Router.



El RouterA, proveerá de los relojes a los enlaces seriales, así como la interfaz S1/1 de RouterC. Por tanto deberá asegurarse de su adecuada configuración.

RouterX(config)#in loopback 0
%LINK-5-CHANGED: Interface Loopback0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up RouterX(config-if)#ip a
RouterX (config-if)#ip address x.x.x.x x.x.x.x
RouterX(config-if)#no shut

Asegúrese que las interfaces Loopback 0 y serial estén habilitadas y direccionadas. ¿Con que comando lo visualiza?

Una vez direccionadas y habilitadas todas las interfaces que intervienen en la topología, ¿Es posible comprobar conectividad con las interfaces loopback 0 de los otros dos routers? En cada caso diga porque si o porque no es posible, en caso de ser posible, ¿Cómo que como comprobaría la conectividad?

2. Configure el enrutamiento OSPF de área única con el número de proceso 100 en cada router, especifique las redes que desea anunciar y asegúrese de que hay conectividad en la red. Note que la sintaxis es diferente que para RIP.

RouterX(config)#router ospf 100
RouterX(config-router)#network x.x.x.x y.y.y.y area 0
RouterX(config-router)#log-adjacency-changes
RouterX(config-router)#end

Note que en vez de especificar la mascara de subred se debe especificar la WILDCARD (y.y.y.y), que para nuestros fines tomaremos como la mascara de subred negada de cada interfaz. Se recomienda que el proceso sea el mismo en cada Router para evitar sobrecargas del procesamiento.

Recuerde que es necesario especificar todas las redes que se desea anunciar, aun las directamente conectadas.

2.1 verifique la correcta configuración de OSPF y las redes en su Router mediante el comando **show ip protocols.**

RouterX#show ip protocols

Routing Protocol is "ospf 100"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Router ID 192.168.10.X ----------→ LOOPBACK 0 DEL ROUTER SOBRE EL QUE SE ESTÁ TRABAJANDO
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Maximum path: 4
Routing for Networks:
X1.X2.X3.X4 Y1.Y2.Y3.Y4 area 0----------→ REDES QUE SE ANUNCIAN
….
….
Routing Information Sources:

```
  Gateway         Distance      Last Update
    X5.X6.X7.X8         110     00:00:03
    X9.XA.XB.XC         110     00:00:03
  Distance: (default is 110)
```

Escriba las redes para las cuales que se están anunciando, es decir las que puede visualizar en la configuración activa y el comando **show ip protocols.**

En caso de no obtener una salida similar verifique su procedimiento y corrija los errores.

2.2 Examine la tabla de adyacencias mediante el comando **show ip ospf neighbor.**

```
RouterX#sh ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.10.33   1     FULL/ -         00:00:38    192.168.10.51   Serial0/0/0
192.168.10.17   1     FULL/ -         00:00:34    192.168.10.67   Serial0/0/1
```

Describa brevemente el contenido de las columnas Neighbor ID, Address e interface.

2.3 verifique la tabla de enrutamiento y explique brevemente su información, compárela además con la tabla de adyacencias previamente obtenida.

¿Porque no aparecen la misma información en la tabla de enrutamiento y en la tabla de adyacencias?

2.4 Observe el intercambio de mensajes OSPF mediante el comando **debug ip ospf events**

RouterX#debug ip ospf events
OSPF events debugging is on
RouterX#
01:23:09: OSPF: Rcv hello from 192.168.10.17 area 0 from Serial0/0/1 192.168.10.67
01:23:09: OSPF: End of hello processing
01:23:13: OSPF: Rcv hello from 192.168.10.33 area 0 from Serial0/0/0 192.168.10.51
01:23:13: OSPF: End of hello processing
01:23:19: OSPF: Rcv hello from 192.168.10.17 area 0 from Serial0/0/1 192.168.10.67
01:23:19: OSPF: End of hello processing
01:23:23: OSPF: Rcv hello from 192.168.10.33 area 0 from Serial0/0/0 192.168.10.51
01:23:23: OSPF: End of hello processing

Determine las IP e interfaces que están enviando y por las que esta recibiendo mensajes el Router.

Deshabilite la visualización de mensajes OSPF, en las redes corporativas no es conveniente mantener activada la visualización de eventos OSPF ya que consume capacidad de procesamiento del Router y con ello aumenta la probabilidad de sobrecarga y deshecho de paquetes, lo cual es de las peores cosas que le pueden pasar a un router.

Configuración de los equipos para el acceso remoto mediante TELNET.

Asegúrese de que no existe previa configuración de seguridad para el ingreso al nivel de usuario privilegiado.

3. Desde el modo de configuración global, habilite la línea de acceso virtual con el password **cisco.**

RouterX(config)#line vty 0 4
RouterX(config-line)#password cisco
RouterX(config-line)#login
RouterX(config-line)#end
%SYS-5-CONFIG_I: Configured from console by console

3.1 Verifique que los cambios se efectuaron adecuadamente en la configuración activa.

3.2 Una vez que los demás equipos han sido configurados para el acceso remoto, haga ping a la Loopback o interfaz alguna de cualquiera de los equipos de los otros dos equipos y describa el proceso:

¿Fue posible ver el prompt del router al cual se trató de acceder?, en caso negativo, avise al equipo que dispone del router que trató de acceder dicha situación.

3.3 Una vez que se ha logrado acceder al nivel de usuario privilegiado del host remoto, trate de accede al nivel de usuario privilegiado.

¿Es posible?, diga que ocurre:

3.4 Termine la conexión remota con el router lejano mediante el comando **end** o pulsando la secuencia **shift + ctrl + 6 + x.**

3.5 Configure el enable password en su Router el cual deberá ser **ciscoX**, donde X es la letra del router que le toco.

3.6 Una vez que todos los equipos han sido configurados con el enable pasword, acceda mediante TELNET hasta el nivel de usuario privilegiado en el CLI remoto.

Anote sus conclusiones:

Tabla de direccionamiento

Router	Loopback 0	Serial 1/0	Serial 1/1
A	192.168.10.1/28	192.168.10.50/28	192.168.10.66/28
B	192.168.10.17/28	192.168.10.67/28	192.168.10.82/28
C	192.168.10.33/28	192.168.10.51/28	192.168.10.83/28

PRÁCTICA 7

INTERCONEXIÓN DEL ROUTER Y SWITCH

Objetivos:

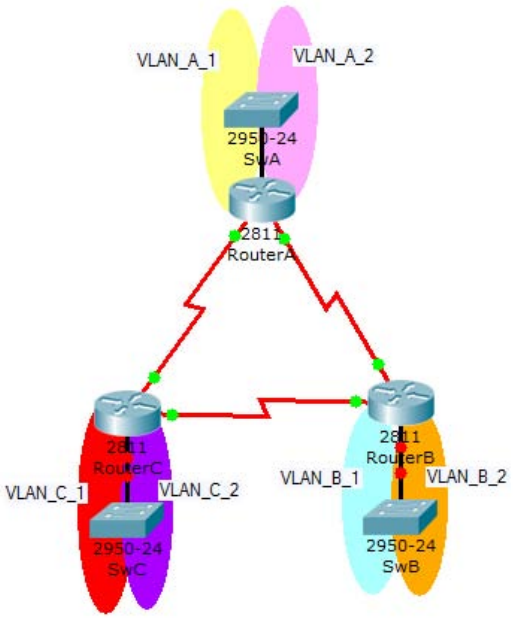
El alumno pondrá en práctica los conocimientos aprendidos hasta el momento en cuanto a configuración de enrutamiento y de implementación LAN sobre Ethernet, además será capaz de realizar la implementación de VLAN trunking en la interfaz de router correspondiente mediante la creación de un par de sub interfaces lógicas. Además será capaz de disponer alguno de los equipos de red como servidor TFTP y compartir archivos bajo el esquema de cliente servidor.

Desarrollo:

Esta práctica deberá ser desarrollada mediante la formación de tres brigadas, cada una tendrá a su cargo un Router y un Switch y deberá seguirse el procedimiento por cada equipo.

1. Configuración de protocolo de enrutamiento.

1.1 Disponga de los equipos de red para implementar la siguiente red.



1.2 Configure enrutamiento OSPF de área única y proceso 100 en cada router con un esquema de direccionamiento proporcionado en la tabla adjunta al final de la práctica. Es necesario especificar que cada Switch dispondrá de un par de VLANs troncales y forzosamente deben ser consideradas al momento de anunciar las redes por el protocolo de enrutamiento. Note que la tabla de direccionamiento no indica valor alguno para la dirección de las interfaces lógicas, por lo tanto deberá asignarlas usted adecuadamente.

1.3 Configuración de subinterfaces con encapsulamiento troncal para la comunicación inter VLAN en la interfaz Ethernet del router.

1.3.1 En el RouterX y desde el modo de configuración global, disponga de subinterfaces en la interfaz física que lo conecta al SwitchX, habilite un par de ellas agregándolas a la VLAN adecuada, asigne direccionamiento y habilítelas.

```
RouterX(config)#interface fa0/0.2
RouterX(config-subif)#encapsulation dot1Q 2
```

Compruebe la correcta creación, encapsulamiento y direccionamiento de las subinterfaces mediante el despliegue de la configuración activa y de los detalles de las interfaces IP mediante los comandos **show running-config** y el estado mediante **show ip interfaces brief**, deberá visualizar una salida similar a las siguientes:

```
RouterX#sh run
Building configuration...

Current configuration : 495 bytes
!
version 12.3
no service password-encryption
!
hostname Router
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface FastEthernet0/0.1
 encapsulation dot1Q 1
 ip address X.X.X.X  Y.Y.Y.Y
```

Compruebe conectividad entre hosts de distintas VLANs para verificar la comunicación inter VLAN.

¿Resulto exitosa la prueba?, ¿Cómo comprobó conectividad?

En caso de no existir conectividad, verifique su procedimiento y corrija lo necesario.

Compruebe conectividad entre hosts de redes de distintos routers para verificar la comunicación a nivel WAN.
¿Resulto exitosa la prueba?, ¿Cómo comprobó conectividad?

En caso de no existir conectividad, verifique su procedimiento y corrija lo necesario.

2. Habilite uno de los routers como servidor TFTP de imágenes de IOS, otro como servidor de configuraciones actuales y otro de configuraciones de inicio.

```
R1#tftp-server nvram:startup-config
R2#tftp-server system:running-config
R3#tftp-server flash: c827v-y6-mz.121-1.XB...
```

Note que c827v-y6-mz.121-1.XB... es el nombre del archivo que contiene la imagen del sistema operativo que está utilizando.

2.1 En conjunto con otra brigada, respalde una copia del archivo imagen del sistema operativo en el servidor TFTP, y asegúrese de no apagar ni detener el router en el proceso de transferencia:

```
Router> enable
Router# copy flash tftp
Source Filename []? (nombre del archivo IOS)
Address or name of remote host []? (IP del Router)
Destination Filename []? (nombre del archivo IOS)
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!
3802992 bytes copied in 27.276 secs (140851 bytes/sec)
```

2.2 Desde el router local copie la configuración de inicio desde el servidor TFTP de configuraciones de inicio.

```
Router# copy tftp flash
Address or name of remote host []? (IP del routers que funciona como TFTP o PC que dispone del software TFTP)
Source Filename []? (nombre del archivo IOS)
Destination Filename []? (nombre del archivo IOS)
Warning:There is a file already existing with this name
Do you want to over write? [confirm]
Accessing tftp://xxx.xxx.xxx.xxx/c827v-y6-mz.121-1.XB...
Erase flash: before copying? [confirm]
Erasing the flash filesystem will remove all files! Continue? [confirm]
Erasing device... eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
ee ...erased
Erase of flash: complete
Loading c827v-y6-mz.121-1.XB from 10.1.1.1 (via Ethernet0): !!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!
[OK - 3802992/7605248 bytes]
Verifying checksum... OK (0x1ABC)
3802992 bytes copied in 58.236 secs (65568 bytes/sec)
```

Llene la siguiente tabla con los comandos necesarios para realizar las acciones mencionadas.

Acción	Comando	Nivel en IOS
Configuración del dominio VTP		
Disposición del equipo como cliente VTP		
Configuración del puerto en modo troncal (2 líneas de comando)		
Configuración de los puertos en modo acceso		
Configuración de los puertos en modo acceso en la VLANs adecuadas		
Verificación de la operación VTP		
Verificación de la operación de interfaces en modo troncal		
Encapsulamiento troncal dot1Q en la interfaz del router		
Creación de subinterfaces		
Verificación del estado de la conectividad		
Habilitación del Router como servidor TFTP		
Transferencia de archivos mediante TFTP		

Tabla de direccionamiento

Interfaz	Dirección IP
Serial 0/0 RouterA	10.1.1.1/24
Serial 0/1 RouterA	10.1.2.1/24
Serial 0/0 RouterB	10.1.2.2/24
Serial 0/1 RouterB	10.1.3.1/24
Serial 0/0 RouterC	10.1.3.2/24
Serial 0/1 RouterC	10.1.1.2/24
VLAN_A_1	10.2.1.1/24
VLAN_A_2	10.2.2.1/24
VLAN_B_1	10.3.1.1/24
VLAN_B_2	10.3.2.1/24
VLAN_C_1	10.4.1.1/24
VLAN_C_1	10.4.2.1/24

CAPÍTULO 6

RESULTADOS Y CONCLUSIONES

6.1 Expansiones y actualizaciones potenciales

El Router de Servicios Integrados CISCO 2811 cuenta con las siguientes capacidades de expansión que le permiten aumentar la cantidad de servicios que ofrece y mejorar el desempeño con el que los puede realizar.

Slots disponibles para futuras expansiones

El Router CISCO 2811 cuenta con los siguientes slots:

- ✓ 2 Módulos de Integración Avanzada (AIM's)
- ✓ 2 Packet Voice Data Modules (PVDM's)
- ✓ 4 Tarjetas de interfaz de alta velocidad para WAN (HWIC's)
- ✓ 1 Módulo de Red Mejorado (NME)
- ✓ 2 Puertos USB

Estos slots permiten la instalación de tarjetas y módulos en el Router CISCO 2811, cabe mencionar que, en parte, gracias a esta modularidad y facilidad de agregar, cambiar o quitar tarjetas y módulos, el Router puede ser llamado de Servicios Integrados; la siguiente tabla muestra algunas de estas tarjetas y módulos.

Tabla 6.1 – Tarjetas y Módulos de Expansión para el Router CISCO 2811

Categoría	Nombre del módulo
Módulos para Ethernet Switching	NME-16ES-1G
	NME-16ES-1G-P

	NM-16ESW
	NM-16ESW-1GIG
Módulos para Conectividad Serial	NM-1T3/E3
	NM-1HSSI
	NM-4A/S
	NM-8A/S
Módulos para enlaces E1/T1 e ISDN	NM-1CE1T1-PRI
	NM-2CE1T1-PRI
	NM-4B-S/T
	NM-4B-U
Módulos para redes ATM	NM-1A-T3
	NM-1A-E3
	NM-1A-T3/E3
Módulos para enlaces Dialup y acceso remoto	NM-8AM-V2
	NM-16AM-V2
Módulos para redes de voz	NM-HD-1V
	NM-HD-2V
	NM-HD-2VE
	NM-HDA-4FXS
Módulos para aplicaciones de red	NME-WAE-302-K9
	NME-WAE-502-K9
	NME-AON-K9
	NM-CE-BP-40G-K9
Módulo para Satélite	NM-1VSAT-GILAT
Tarjetas de interfaz Ethernet de alta velocidad para WAN	HWIC-1FE
	HWIC-1GE-SFP
Tarjetas de interfaz inalámbrica de alta velocidad para WAN	HWIC-AP-G-A
	HWIC-AP-G-E
	HWIC-AP-G-J
	HWIC-AP-AG-A
Tarjetas de interfaz Serial para WAN y de alta	HWIC-4T

velocidad	HWIC-4A/S
	HWIC-8A
	HWIC-8A/S-232
Tarjetas de interfaz DSL para WAN	HWIC-1ADSL
	HWIC-1ADSLI
	HWIC-ADSL-B/ST
	HWIC-ADSLI-B/ST
Módulos 3G Inalámbrico para WAN	HWIC-3G-CDMA-S
	HWIC-3G-CDMA-V
	HWIC-3G-GSM
Tarjetas de interfaz de voz	VIC2-2FXS
	VIC2-2FXO
	VIC2-4FXO
	VIC2-2E/M

Caracteristicas de interfaces de voz en el CISCO 2811

Por la cantidad de equipamiento disponible no es práctico ni necesario describir cada una de las tarjetas que el C2811 puede soportar, es más adecuado describir las caracteristicas que se pueden soportar por el equipo para una posterior expansión de servicios. Además debemos aclarar que la especificación de todos estos servicios queda fuera del alcance de la tesis y solamente se agregan los siguientes rubros para facilitar una posterior actualización del equipo.

Soporte para tecnología de telefonía IP

Algunas de las tarjetas que el C2811 acepta tienen la opción de proveer PoE, el cual facilita la conexión de teléfonos IP sin la necesidad de suministro eléctrico externo, ya que se provee por el cable UTP.

Facilidades EVM (Extensión Voice Modules)

Estas facilidades proporcionan el soporte para conectar servicios de voz y fax analógica y digital para soportar mas de 24 sesiones sin requerir un módulo de red.

PVDM

Son módulos de procesamiento para procesar la voz mediante un DSP (Digital Signal Processor), es donde se realiza la codificación correspondiente, así como conversiones analógicas digital.

Cisco CME (Call Manager Express)

Es una funcionalidad para implementar un sistema de telefonía local basado en un sistema similar a los PBX pero sobre tecnología IP, el cual se realiza por la versión adecuada de sistema operativo CISCO IOS.

Interfaces de voz soportadas

RTPC – hacia la red telefónica pública conmutada.
PBX – hacia un sistema conmutador PBX (Private Branch Exchance)
FXS – hacia teléfonos analógicos.
FXO – hacia líneas telefónicas
E&M – troncales analógicas.
ISDN – interfaces de red ISDN
E1/T1 – enlaces dedicados T1/E1

Expansión de Capacidades Físicas

La siguiente tabla muestra la máxima cantidad de memoria soportada por el Router CISCO 2811.

Tabla 6.2 – Capacidades de Memoria

Tipo de memoria	Número de slots totales	Memoria instalada de fábrica	Cantidad de memoria máx. soportada	Descripción
RAM	2	256 MB	768 MB	El Router soporta una tarjeta de 256 MB y una de 512 MB para sus dos slots.
FLASH	1 (PCMCIA)	64 MB	256 MB	El Router soporta una tarjeta PCMCIA de 128 ó 256 MB como máximo.

Cambio del IOS

Los servicios que puede ofrecer un Router dependen del tipo de IOS y de la versión que tenga instalada, como ya se mencionó anteriormente en el capítulo 4, las tarjetas y módulos instalables en un Router dependen del IOS que este último tenga instalado o que pueda soportar. Para obtener una versión distinta de IOS hay que contactar con un socio de CISCO.

También la versión del IOS es la que define los servicios a los que estará orientado el Router, algunos de estos son:

- IPBase
- Wireless
- Security

6.2 Contribuciones, documentación y soluciones de configuración

6.2.1 Contribuciones y utilidad de la infraestructura implementada.

En la presente tesis hemos diseñado y desarrollado prácticas de laboratorio con la finalidad de preparar un examen de certificación de nivel asociado de CISCO, basándonos en su programa de ínter conectividad académico. Además con el presente trabajo, contribuimos a la adaptación de dicho programa (NETACAD) ayudando también a la elaboración de material didáctico para las diferentes asignaturas de la carrera de Ingeniería en Telecomunicaciones de nuestra Facultad.

El compendio de prácticas consiste de siete de ellas en las cuales aportamos actividades para el aprendizaje de la configuración de equipos de red, en específico Switches Catalyst 2950 y Routers CISCO 2811. La lista de prácticas elaboradas son las siguientes:

- Introducción a la configuración de equipos de red
    - En esta práctica explicamos y proponemos actividades para que el lector se familiarice con los equipos de red, con su sistema operativo y habilitación de interfaces.
- Interconexión y configuración de Switch
    - En esta práctica explicamos los aspectos de configuración básica de switch Catalyst 2950. Familiarizamos al estudiante con el trabajo con la tabla de direccionamiento físico y la disposición de redes Ethernet mediante configuraciones redundantes utilizando protocolos para evitar problemas con tramas duplicadas en la red.
- Funciones avanzadas del Switch
    - En esta práctica desarrollamos conceptos superiores del nivel de enlace de datos en redes LAN Ethernet como redes locales virtuales, redes virtuales distribuidas en una red Ethernet de varios switches, separación de dominios de difusión, utilización de protocolos de configuración distribuida en redes virtuales locales troncales.
- Interconexión mediante enlaces WAN
    - En esta práctica familiarizamos al lector con el nivel de enlace pero de redes de área extensa (WAN), sus protocolos y características de comunicación así como sus especificaciones de nivel físico para una adecuada implementación, además iniciamos al lector en conceptos de seguridad mediante herramientas de autenticación de enlaces punto a punto.

- Configuración de enrutamiento estático y RIP

    - Es en esta práctica donde abordamos tópicos del nivel de red como enrutamiento estático y dinámico, además de las características y tipos de protocolos de enrutamiento dinámico como RIP y mostramos al lector como comprobar conectividad y resolver algunos problemas relacionados al nivel de red.

- Configuración del protocolo de enrutamiento OSPF

    - En esta práctica mostramos la forma de configurar el protocolo de enrutamiento OSPF, además de ilustrar su principio de funcionamiento y una herramienta como TELNET para la configuración de equipos de manera remota.

- Interconexión del Router y Switch

    - En esta práctica dispusimos de la totalidad de los equipos de red disponibles para formar una red delta IP la cual interconecta switches explotando capacidades de división de sus puertos en dos dominios de difusión distintos, con lo cual se pretende ilustrar de manera total, las habilidades adquiridas en las prácticas previamente realizadas, además se enseña al lector como disponer de herramientas basadas en arquitecturas cliente servidor para compartir archivos de configuración entre equipos de red para su fácil manejo.

6.2.2 Soluciones a las Prácticas

Hemos numerado las soluciones de configuración presentadas de acuerdo al número de actividad que se presenta en cada una de las prácticas, por ejemplo: 2-2.1 de la practica 1 corresponde a las soluciones de configuración de los puntos 2 al 2.1 de la práctica 1.

Solución de configuración práctica 1

1-1.3

Parámetro	Valor
Nombre de la conexión	Asignado por el usuario
Método de conexión	Puerto COM
Tasa de transferencia	9600 bps
Bits de datos	8
Paridad	Ninguno
Bits de parada	1
Control de flujo	Ninguno

1.4

System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fc1)
Copyright (c) 2000 by cisco Systems, Inc.

cisco 2811 (MPC860) processor (revision 0x200) with **60416K/5120K bytes of memory**

Self decompressing the image :
######################System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fc1)
Copyright (c) 2000 by cisco Systems, Inc.
cisco 2811 (MPC860) processor (revision 0x200) with 60416K/5120K bytes of memory

Self decompressing the image :
[OK]
Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706

Cisco IOS Software, 2800 Software (C2800NM-IPBASE-M), Version 12.3(14)T7, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Wed 22-Mar-06 18:40 by pt_team
Image text-base: 0x40095498, data-base: 0x414E0000

cisco 2811 (MPC860) processor (revision 0x200) with 60416K/5120K bytes of memory
Processor board ID JAD05190MTZ (4292891495)
M860 processor: part number 0, mask 49
2 FastEthernet/IEEE 802.3 interface(s)
239K bytes of non-volatile configuration memory.
62720K bytes of processor board System flash (Read/Write)
Cisco IOS Software, 2800 Software (C2800NM-IPBASE-M), Version 12.3(14)T7, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Wed 22-Mar-06 18:40 by pt_team

--- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]: N

Press RETURN to get started!

Router>

1.5

Versión de bootstrap.	**System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fc1)**
Versión de sistema operativo.	**Cisco IOS Software, 2800 Software (C2800NM-IPBASE-M), Version 12.3(14)T7, RELEASE SOFTWARE (fc2)**
Interfaces conectadas.	**2 FastEthernet/IEEE 802.3 interface(s)//puede variar en function del numero de ingterfaces que disponga el router.**
Capacidad de memoria RAM utilizada disponible y total.	**60416KB/5120KB (disponible/usada)**
Capacidad de memoria FLASH y su estado.	**62720K bytes of processor board System flash (Read/Write)**
Capacidad de memoria NVRAM.	**239K bytes of non-volatile configuration memory.**

2-2.1

Router>?

```
Exec commands:
  <1-99>     Session number to resume
  connect    Open a terminal connection
  disconnect  Disconnect an existing network connection
  enable     Turn on privileged commands
  exit       Exit from the EXEC
  logout     Exit from the EXEC
  ping       Send echo messages
  resume     Resume an active network connection
  show       Show running system information
  telnet     Open a telnet connection
  traceroute  Trace route to destination
```

2.2-2.3

```
Router>enable
Router#
```

2.4

```
Router#show running-config
Building configuration...

Current configuration : 332 bytes
!
version 12.3
no service password-encryption
!
hostname Router
!
!
!
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
ip classless
!
!
!
!
line con 0
line vty 0 4
 login
!
!
End
```

2.5

```
Router#show version
```

Cisco IOS Software, 2800 Software (C2800NM-IPBASE-M), Version 12.3(14)T7, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Wed 22-Mar-06 18:40 by pt_team

ROM: System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fc1)
Copyright (c) 2000 by cisco Systems, Inc.

System returned to ROM by power-on
System image file is "flash:c2800nm-ipbase-mz.123-14.T7.bin"

cisco 2811 (MPC860) processor (revision 0x200) with 60416K/5120K bytes of memory
Processor board ID JAD05190MTZ (4292891495)
M860 processor: part number 0, mask 49
2 FastEthernet/IEEE 802.3 interface(s)
239K bytes of NVRAM.
62720K bytes of processor board System flash (Read/Write)

Configuration register is 0x2102

2.6

Parámetro	Valor
Contenido de la memoria ROM y ultimo acceso	**ROM: System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fc1), System returned to ROM by power-on**
Nombre del archivo del sistema operativo	**System image file is "flash:c2800nm-ipbase-mz.123-14.T7.bin"**
función específica del IOS	**ipbase**
Registro de configuración	**Configuration register is 0x2102**

2.7

Router#show running-config
Building configuration...

Current configuration : **332 bytes**
!
version 12.3
no service password-encryption
!
hostname Router
!
!
!
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
ip classless
!
!

```
!
!
line con 0
line vty 0 4
 login
!
!
end
```

2.8

Parámetro	Valor
Tamaño del archivo de configuración	**332 bytes**
Hostname del equipo	**Router**
Estado de alguna interfaz	**interface FastEthernet0/0** **shutdown**

2.9

```
Router#show startup-config
startup-config is not present
```

```
Router#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

2.10

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

2.11 Verifique los comandos disponibles del modo de configuración global.

```
Router#?
Exec commands:
  <1-99>     Session number to resume
  clear      Reset functions
  clock      Manage the system clock
  configure  Enter configuration mode
  connect    Open a terminal connection
  copy       Copy from one file to another
  debug      Debugging functions (see also 'undebug')
  delete     Delete a file
  dir        List files on a filesystem
  disable    Turn off privileged commands
  disconnect  Disconnect an existing network connection
  enable     Turn on privileged commands
  erase      Erase a filesystem
  exit       Exit from the EXEC
  logout     Exit from the EXEC
  no         Disable debugging informations
  ping       Send echo messages
  reload     Halt and perform a cold restart
  resume     Resume an active network connection
  setup      Run the SETUP command facility
```

```
 show       Show running system information
 telnet     Open a telnet connection
 traceroute  Trace route to destination
 undebug    Disable debugging functions (see also 'debug')
 vlan       Configure VLAN parameters
 write      Write running configuration to memory, network, or terminal
```

2.12.1

```
Router(config)#enable password cisco1
Router(config)#enable secret cisco2
```

3.1

```
RouterA(config)#interface fastethernet0/0
RouterA(config-if)#ip address 10.1.1.1 255.255.255.0
RouterA(config-if)#no shutdown
RouterA(config-if)#exit
RouterA(config)#interface fastethernet0/1
RouterA(config-if)#ip address 10.1.2.1 255.255.255.0
RouterA(config-if)#no shutdown
```

3.2

```
RouterA#ping 10.1.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/6 ms
```

Solución de configuración práctica 2

1.

Mac Address Table inicial

```
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
```

```
Switchx>enable
Switchx#configure terminal
Switchx(config)#interface vlan 1
Switchx(config-if)#ip address 10.1.1.1 255.255.255.0
Switchx(config-if)#exit
Switchx(config)#interface fastethernet 0/3
Switchx(config-if)#speed 100
Switchx(config-if)#duplex half
Switchx(config-if)#switchport mode access
Switchx(config-if)#switchport port-security
Switchx(config-if)#switchport port-security mac-address 000A.419D.DABC
```

Ahora la tabla de direcciones MAC deberá verse de la siguiente manera:

```
                    Mac Address Table
-------------------------------------------
```

```
          Vlan    Mac Address       Type        Ports
               ----    -----------       --------    -----

          1    000a.419d.dabc    STATIC      Fa0/3
```

2. Switchx#debug spanning-tree //No ejecutar en simulador
Switchx#configure terminal
Switchx(config)#spanning-tree vlan 1 root primary //No ejecutar en simulador
Switchx(config)#spanning-tree vlan 1 priority 24576 // Dato de simulador, Probar línea anterior en el equipo.

Solución de configuración práctica 3

1-1.1

```
Switch10#vlan database
Switch10(vlan)#vlan 10 name VLAN10
VLAN 3 added:
   Name: VLAN10
Switch10(vlan)#apply
APPLY completed
Switch10(vlan)# ^Z
Switch10#
```

1.2

```
Switch10#show vlan brief

VLAN  Name                             Status    Ports
----  -------------------------------- --------- -------------------------------
1     default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gig1/1, Gig1/2
10    VLAN10                           active
1002  fddi-default                     active
1003  token-ring-default               active
1004  fddinet-default                  active
1005  trnet-default                    active
```

1.3

```
Switch10(config-if)#switchport mode access
Switch10(config-if)#switchport access vlan 10
```

1. 4

```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24
10   VLAN10                           active    Fa0/1
1002 fddi-default                     active
```

```
1003 token-ring-default          active
1004 fddinet-default             active
1005 trnet-default               active
```

2. deberá conectar adecuadamente la topología mostrada según la tabla de conexiones

Equipo	PC	Interfaz	VLAN
SW2	PC1 VLAN T. 2	Fa0/2	2
SW2	PC2 VLAN T. 3	Fa0/3	3
SW3	PC1 VLAN T. 3	Fa0/2	2
SW#	PC2 VLAN T. 2	Fa0/3	3

Equipo 1	Interfaz	Equipo 2	Interfaz
RouterCore	Fa0/0	SwitchCore	Fa0/1
SwitchCore	Fa0/22	SW2	Fa0/22
SwitchCore	Fa0/23	SW3	Fa0/23
SW2	Fa0/2	PC1 VLAN T. 2	Fa
SW3	Fa0/2	PC2 VLAN T. 2	Fa
SW3	Fa0/3	PC1 VLAN T. 3	Fa
SW2	Fa0/3	PC2 VLAN T. 3	Fa
SW2	Fa0/10	SW3	Fa0/10

Equipo	Interfaz	Direccionamiento
RouterCore	Fa0/0.2	10.1.2.2/24
	Fa0/0.3	10.1.3.2/24
SwitchCore	VLAN2	10.1.2.1/24
	VLAN3	10.1.3.1/24
PC1 VLAN troncal 2	Fastethernet	10.1.2.10/24
PC2 VLAN troncal 2	Fastethernet	10.1.2.11/24
PC1 VLAN troncal 3	Fastethernet	10.1.3.10/24
PC2 VLAN troncal 3	Fastethernet	10.1.3.11/24

2.1-2.1.1

```
SwitchCore(vlan)#vtp domain DOMINIO_VTP
Changing VTP domain name from NULL to DOMINIO_VTP
SwitchCore(vlan)#vtp  server
Setting device to VTP SERVER mode
```

2.1.1.2

```
SwitchCore#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 64
Number of existing VLANs        : 5
```

VTP Operating Mode : **Server**
VTP Domain Name : **DOMINIO_VTP**
VTP Pruning Mode : Disabled
VTP V2 Mode : Disabled
VTP Traps Generation : Disabled
MD5 digest : 0x7D 0xC1 0xCF 0x2A 0x31 0x72 0x49 0xFC
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)

2.1.3

SwitchCore(config-if)#switchport mode trunk
SwitchCore(config-if)#switchport trunk allowed vlan all

2.1.4

SwitchCore#show interfaces fa0/22 switchport
Name: Fa0/22
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Appliance trust: none

2.2

ESTA ACTIVIDAD SERÁ REALIZADA POR EL PROFESOR MEDIANTE LA PARTICIPACIÓN DEL GRUPO Y ESTÁ ESPECIFICADA EN EL PUNTO 2.2.1.

2.2.1

RouterCore(config)#interface fa0/0.2
Router(config-subif)#encapsulation dot1Q 2

Comprobación

Router#sh run
Building configuration...

Current configuration : 495 bytes
!
version 12.3
no service password-encryption
!
hostname Router

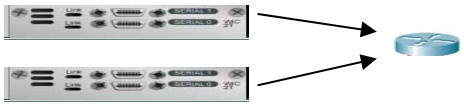
```
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface FastEthernet0/0.1
 encapsulation dot1Q 1
 ip address 10.1.1.1 255.255.255.0
```

Acción	Comando	Nivel en IOS
Configuración del dominio VTP	vtp domain	VLAN DATABASE
Disposición del equipo como cliente VTP	vtp domain client	VLAN DATABASE
Configuración del puerto en modo troncal (2 líneas de comando)	RouterCore(config)#interface fa0/0.2	INTERFAZ ESPECÍFICA
	Router(config-subif)#encapsulation dot1Q 2	INTERFAZ ESPECÍFICA
Configuración de los puertos en modo acceso	interface FastEthernet0/0.1 encapsulation dot1Q 1 **ip address 10.1.1.1 255.255.255.0**	INTERFAZ ESPECÍFICA
Configuración de los puertos en modo acceso en la VLANs adecuadas	SwitchCore(config-if)#switchport mode trunk SwitchCore(config-if)#switchport trunk allowed vlan all	INTERFAZ ESPECÍFICA
Verificación de la operación VTP	SwitchCore#show interfaces fa0/22 switchport	USUARIO PRIVILEGIADO
Verificación de la operación de interfaces en modo troncal	SwitchCore#show interfaces fa0/22 switchport	USUARIO PRIVILEGIADO

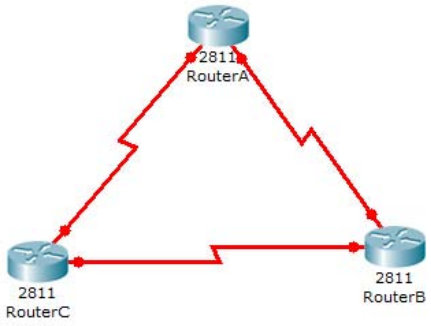
Solución de configuración práctica 4

1. Los Routers deberán estar apagados y con las interfaces WIC 2 A/S desinstaladas, introdúzcalas en las ranuras correspondientes y atornille con cuidado de no barrer o romper los tornillos.

NOTA: Recuerde siempre sujetar las interfaces por el lado que tiene los conectores, es decir, no toque los componentes electrónicos de la tarjeta ya que podría dañarla de manera irreparable.



1.1 Implemente la topología



1.2 Sin haber encendido los equipos deberá conectar los extremos Smart Serial a las interfaces seriales de tal y los conectores hembra V.35 a los conectores V.35 macho de acuerdo con la tabla de conexiones mostrada al final de la práctica; a este tipo de conexiones se les conoce como Back to Back.

NOTA: Recuerde que una conexión serial WAN siempre tiene un extremo DTE y un extremo DCE.

1.3 Desde el modo de usuario privilegiado, asegúrese que dispone del tipo de cables seriales conectados, es decir, compruebe que conectó un extremo DTE o DCE al la interfaz respectiva.

```
RouterX#show controllers serial 0/0/0
Interface Serial0/0/0
Hardware is PowerQUICC MPC860
DCE V.35, no clock
idb at 0x81081AC4, driver data structure at 0x81084AC0
SCC Registers:
General [GSMR]=0x2:0x00000000, Protocol-specific [PSMR]=0x8
```

```
RouterX#show controllers serial 0/0/0
Interface Serial0/0/0
Hardware is PowerQUICC MPC860
DTE V.35, no clock
idb at 0x81081AC4, driver data structure at 0x81084AC0
SCC Registers:
General [GSMR]=0x2:0x00000000, Protocol-specific [PSMR]=0x8
```

1.4 DCE a 64000 y habilítela.

NOTA: Si usted dispone del RouterC, esta tarea no será necesaria dado que ninguna de sus interfaces será DCE.

```
RouterX(config-if)#clock rate 64000
RouterX(config-if)#no shutdown
```

Verifique que ha configurado adecuadamente el reloj de la interfaz mediante el comando **show controllers interfaces serial X**.

RouterX#show controllers serial 0/0/0
Interface Serial0/0/0
Hardware is PowerQUICC MPC860
DCE V.35, **clock rate 64000**
idb at 0x81081AC4, driver data structure at 0x81084AC0
SCC Registers:

1.5

Conexión [RouterX-RouterY]	Conector de Interfaz Router X /Dirección		Conector de Interfaz Router Y/Dirección	
RouterA-RouterB	DCE	11.1.2.1/24	DTE	11.1.2.2/24
RouterA-RouterC	DCE	11.1.1.1/24	DTE	11.1.1.2/24
RouterB-RouterC	DCE	11.1.3.1/24	DTE	11.1.3.2/24

1.6

RouterX(config-if)# show ip interface brief
RouterX(config-if)# show running-config

El comando conveniente es **show ip interface brief**, ya que muestra el estado de cada interfaz.

1.7

RouterX(config-if)# ping x.x.x.x

2-2.1

RouterX(config-if)#encapsulation **ppp**
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down
RouterX(config-if)#no shutdown
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to u

3 - 3.2

RouterA(config)#username RouterC password cisco

3.3

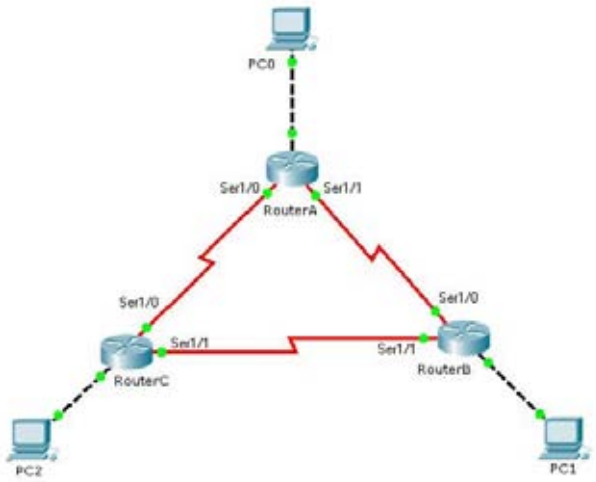
RouterA(config-if)#ppp authentication chap

Acción	Comando	Nivel en IOS
Verificación del tipo de cable serial conectado a la interfaz	Show controllers interface serial X/Y	USUARIO PRIVILEGIADO
Verificación de estado de	Show ip interfaces brief	USUARIO PRIVILEGIADO

conectividad interfaces		
Verificación del protocolo de encapsulamiento WAN utilizado en el enlace	show interface serial X	USUARIO PRIVILEGIADO
Configuración de PPP	RouterX(config-if)#encapsulation ppp	INTERFAZ SERIAL CORRESPONDIENTE
Habilitación de la seguridad CHAP en PPP	RouterA(config-if)#ppp authentication chap	INTERFAZ SERIAL CORRESPONDIENTE

Solución de configuración práctica 5

1.



Equipo	IP Serial 1/0	IP Serial 1/1
A	11.1.1.1/24	11.1.2.1/24
B	11.1.2.2/24	11.1.3.1/24
C	11.1.1.2/24	11.1.3.2/24

2. *Type escape sequence to abort.*
Sending 5, 100-byte ICMP Echos to 172.16.32.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

RouterA#configure terminal
RouterA(config)#ip route 11.1.3.0 255.255.255.0 Serial 1/0 //Nativo de simulador
RouterA(config)#ip route 11.1.3.0 255.255.255.0 11.1.1.0 //No ejecutar en simulador
RouterA(config)#exit

3. *RouterA#configure terminal*

Enter configuration commands, one per line. End with CNTL/Z.
RouterA(config)#router rip
RouterA(config-router)#network 172.16.30.0
RouterA(config-router)#network 11.1.1.0
RouterA(config-router)#network 11.1.2.0
RouterA(config-router)#exit
RouterA(config)#exit

4. *RouterB#show ip rip database*

Solución de configuración práctica 6

1.
RouterX(config)#in loopback 0
%LINK-5-CHANGED: Interface Loopback0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up RouterX(config-if)#ip a
RouterX (config-if)#ip address x.x.x.x x.x.x.x
RouterX(config-if)#no shut

2.
RouterX(config)#router ospf 100
RouterX(config-router)#network x.x.x.x y.y.y.y area 0
RouterX(config-router)#log-adjacency-changes
RouterX(config-router)#end

2.1 *RouterX#show ip protocols*

Routing Protocol is "ospf 100"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Router ID 192.168.10.X ----------→ LOOPBACK 0 DEL ROUTER SOBRE EL QUE SE ESTÁ TRABAJANDO
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Maximum path: 4
Routing for Networks:
X1.X2.X3.X4 Y1.Y2.Y3.Y4 area 0----------→ REDES QUE SE ANUNCIAN
….
….
Routing Information Sources:
Gateway Distance Last Update
X5.X6.X7.X8 110 00:00:03
X9.XA.XB.XC 110 00:00:03
Distance: (default is 110)

2.2 RouterX#sh ip ospf neighbor

Neighbor ID	Pri	State	Dead Time	Address	Interface
192.168.10.33	1	FULL/-	00:00:38	192.168.10.51	Serial0/0/0
192.168.10.17	1	FULL/-	00:00:34	192.168.10.67	Serial0/0/1

2.4 RouterX#debug ip ospf events

```
OSPF events debugging is on
RouterX#
01:23:09: OSPF: Rcv hello from 192.168.10.17 area 0 from Serial0/0/1 192.168.10.67
01:23:09: OSPF: End of hello processing
01:23:13: OSPF: Rcv hello from 192.168.10.33 area 0 from Serial0/0/0 192.168.10.51
01:23:13: OSPF: End of hello processing
01:23:19: OSPF: Rcv hello from 192.168.10.17 area 0 from Serial0/0/1 192.168.10.67
01:23:19: OSPF: End of hello processing
01:23:23: OSPF: Rcv hello from 192.168.10.33 area 0 from Serial0/0/0 192.168.10.51
01:23:23: OSPF: End of hello processing
```

3. Desde el modo de configuración global, habilite la línea de acceso virtual con el password **cisco.**

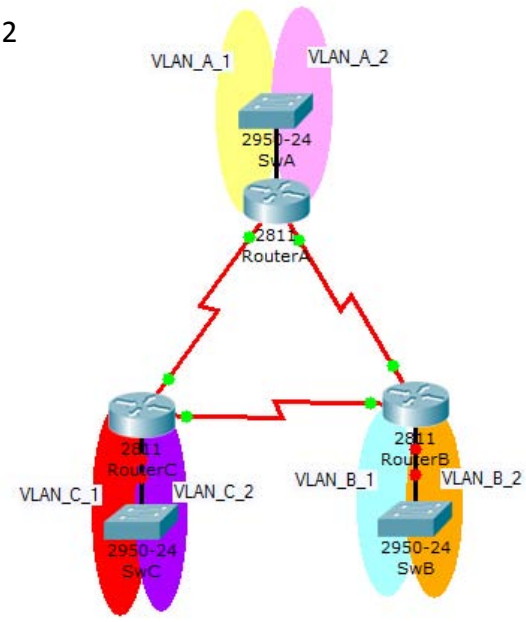
```
RouterX(config)#line vty 0 4
RouterX(config-line)#password cisco
RouterX(config-line)#login
RouterX(config-line)#end
%SYS-5-CONFIG_I: Configured from console by console
```

Termine la conexión remota con el router lejano mediante el comando **end** o pulsando la secuencia **shift + ctrl + 6 + x.**

Router	Loopback 0	Serial 1/0	Serial 1/1
A	192.168.10.1/28	192.168.10.50/28	192.168.10.66/28
B	192.168.10.17/28	192.168.10.67/28	192.168.10.82/28
C	192.168.10.33/28	192.168.10.51/28	192.168.10.83/28

Solución de configuración práctica 7

1-1.2



Interfaz	Dirección IP
Serial 0/0 RouterA	10.1.1.1/24
Serial 0/1 RouterA	10.1.2.1/24
Serial 0/0 RouterB	10.1.2.2/24
Serial 0/1 RouterB	10.1.3.1/24
Serial 0/0 RouterC	10.1.3.2/24
Serial 0/1 RouterC	10.1.1.2/24
VLAN_A_1	10.2.1.1/24
VLAN_A_2	10.2.2.1/24
VLAN_B_1	10.3.1.1/24
VLAN_B_2	10.3.2.1/24
VLAN_C_1	10.4.1.1/24
VLAN_C_1	10.4.2.1/24

1.3

```
RouterX(config)#interface fa0/0.2
RouterX(config-subif)#encapsulation dot1Q 2

RouterX#sh run
Building configuration...

Current configuration : 495 bytes
!
version 12.3
no service password-encryption
!
hostname Router
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface FastEthernet0/0.1
 encapsulation dot1Q 1
 ip address X.X.X.X  Y.Y.Y.Y
```

2.

```
R1#tftp-server nvram:startup-config
R2#tftp-server system:running-config
R3#tftp-server flash: c827v-y6-mz.121-1.XB...
```

2.1

```
Router> enable
Router# copy flash tftp
Source Filename []? (nombre del archivo IOS)
Address or name of remote host []? (IP del Router)
Destination Filename []? (nombre del archivo IOS)
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!
3802992 bytes copied in 27.276 secs (140851 bytes/sec)
```

2.2

```
Router# copy tftp flash
Address or name of remote host []? (IP del routers que funciona como TFTP o PC que dispone del software TFTP)
Source Filename []? (nombre del archivo IOS)
Destination Filename []? (nombre del archivo IOS)
Warning:There is a file already existing with this name
Do you want to over write? [confirm]
Accessing tftp://xxx.xxx.xxx.xxx/c827v-y6-mz.121-1.XB...
Erase flash: before copying? [confirm]
Erasing the flash filesystem will remove all files! Continue? [confirm]
Erasing device... eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
ee ...erased
Erase of flash: complete
```

```
Loading c827v-y6-mz.121-1.XB from 10.1.1.1 (via Ethernet0): !!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!
[OK - 3802992/7605248 bytes]
Verifying checksum... OK (0x1ABC)
3802992 bytes copied in 58.236 secs (65568 bytes/sec)
```

6.3 Conclusiones

Debido a las necesidades de conocimientos teóricos y prácticos con los que los futuros profesionistas de nuestra facultad cuentan en materia de ínter conectividad de dispositivos de red, hemos contribuido con el diseño e implementación de actividades que proveen de la información y habilidades necesarias para el adecuado entendimiento de las tecnologías de telecomunicaciones impartidas en la facultad.

Hemos enfocado las actividades hacia un entorno autodidacta y de trabajo en equipo dado que son habilidades que el ingeniero debe tener ya que se presentan en la vida profesional. El enfoque además permite la aplicación de los conocimientos presentados en las prácticas inmediatas anteriores con lo cual se favorece su rápida asimilación y fomenta el interés que el lector puede tener para conocer más acerca de las tecnologías tratadas y otras. Debido a que se han desarrollado de manera secuencial y con un nivel incremental de dificultad se mejoran las capacidades prácticas y no solamente teóricas que se requieren en el campo de la ingeniería.

Más de 300 instituciones en México han implantado el programa de interconectividad, con lo cual sus egresados disponen de ventajas competitivas inmediatas al terminar sus estudios, lo cual puede poner en desventaja a aquellos que no tienen conocimiento alguno en los tópicos del programa.

Con la implementación y adaptación del programa académico de interconectividad a la facultad, se innova en la enseñanza de los diferentes tópicos en el campo de las tecnologías de la información y las telecomunicaciones, además se provee de la preparación necesaria a los alumnos para obtener la certificación de nivel asociado, que requerirán para su pleno desarrollo como profesionistas y con ello el del país.

Finalmente hemos logrado el alcance del objetivo del proyecto de tesis generando la documentación y configuración para el desarrollo de una infraestructura útil que genera cada vez mayores conocimientos, además de ser actual e innovadora.

GLOSARIO

B

BachTec: Bachillerato Técnico

C

CC: Centro Cultural
CU: Centro Universitario

G

GE: Grupo Educativo

I

ITA: Instituto Tecnológico de Aguascalientes
ITM: Instituto Tecnológico de Mexicali
ITS: Instituto Tecnológico Superior

T

T: Tecnológico
TES: Tecnológico de Estudios Superiores

U

U: Universidad
UA: Universidad Autónoma
UAA: Universidad Autónoma de Aguascalientes
UPA: Universidad Politécnica de Aguascalientes
UT: Universidad Tecnológica
UTA: Universidad Tecnológica de Aguascalientes
UTM: Universidad del Tercer Milenio
UTNA: Universidad Tecnológica del Norte de Aguascalientes
UTT: Universidad Tecnológica de Tijuana

Referencias

[2] Angel R., Diseño, Implementación y puesta en marcha del Laboratorio del Posgrado en Ciencia e Ingeniería de la Computación, México D.F., 2007.

[17] CISCO, Descripción del currículo del Networking Academy Program (Data sheet) CISCO systems, 2008.

[8] CISCO, Guía del Segundo Año; Academia de Networking de CISCO pp. 381

[6] EIA: Electronic Industries Association

[10] IETF, Norma RFC 791.

[9] ISO: Internacional Standard Organization

[3] Proyecto PAPIME PE103807

[4] The Institute of Electrical and Electronics Engineers, Inc., ANSI/IEEE Std 802.2 – Parte 2, New York - USA, 1998.

[5] The Institute of Electrical and Electronics Engineers, Inc., ANSI/IEEE Std 802.3 – Sección 1, New York - USA, 2005.

[7] TIA: Telecommunications Industry Association

Páginas de Internet

[12] http://newsroom.cisco.com/dlls/hd_101503.html

[14] http://www.cisco.com/warp/public/779/edu/espanol/academy/beneficios.html

[13] http://www.cisco.com/warp/public/779/edu/espanol/academy/como_funciona.html

[11] http://www.cisco.com/warp/public/779/edu/espanol/academy/que_es.html

[21] http://www.cisco.com/web/learning/le3/ccie/track_comparison/index.html

[20] http://www.cisco.com/web/learning/le3/current_exams/640-802.html

[16] http://www.cisco.com/web/learning/le3/le2/le0/le9/learning_certification_type_home.html

[18] http://www.cisco.com/web/learning/netacad/downloads/pdf/CCNAds.pdf

[15] http://www.observatoriolaboral.gob.mx/opServicios1.asp?pserv=36

[1] http://www.observatoriolaboral.gob.mx/paginar_cisco.asp?eje=30&page=4&entidad=9

[19] https://ciscobookstore.informit.com/bookstore/product.asp?isbn=1587054647