INSTITUTO POLITÉCNICO NACIONAL

ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELÉCTRICA
UNIDAD CULHUACAN

DISEÑO DE DIRECCIONAMIENTO IP PARA LA EMPRESA QUICK LEARNING

TESINA

QUE PARA OBTENER EL TÍTULO DE
INGENIERO EN COMPUTACIÓN

PRESENTAN: CARLOS ALBERTO HERNÁNDEZ VÁZQUEZ, MARÍA DEL CARMEN REYES MARTÍNEZ,
SALOMÓN VALLARTA SÁNCHEZ

QUE PARA OBTENER EL TÍTULO DE
INGENIERO EN COMUNICACIONES Y ELECTRONICA

PRESENTAN: MARGARITA CUERVO HERNÁNDEZ, FLOR EDEN GALICIA VEGA

ASESOR: M. en C. RAYMUNDO SANTANA ALQUICIRA

MÉXICO, D. F. NOVIEMBRE 2009

IPN

ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELÉCTRICA

UNIDAD CULHUACAN

TESINA

QUE PARA OBTENER EL TITULO DE:
INGENIERO EN COMPUTACION

DEBERA DESARROLLAR: CARLOS ALBERTO HERNÁNDEZ VÁZQUEZ, MARIA DEL CARMEN REYES MARTÍNEZ, SALOMÓN VALLARTA SÁNCHEZ

QUE PARA OBTENER EL TITULO DE:
INGENIERO EN COMUNICACIONES Y ELECTRONICA

DEBERA DESARROLLAR: MARGARITA CUERVO HERNÁNDEZ, FLOR EDEN GALICIA VEGA

NOMBRE DEL SEMINARIO: INTERCONECTIVIDAD Y SEGMENTACION EN REDES DE ALTA VELOCIDAD

NOMBRE DEL TEMA
"DISEÑO DE DIRECCIONAMIENTO IP PARA LA EMPRESA QUICK LEARNING"

INTRODUCCION

La empresa Quick Learning maneja un direccionamiento IP en la actualidad que evita que la funcionalidad de la red sea eficiente debido a que maneja un gran dominio de broadcast, existe un enorme desperdicio de IPs a causa de la mala administración de la red. Se propondrá a la empresa un direccionamiento IP para mejorar las condiciones de la red.

CAPITULADO

I.INTRODCCION A LAS REDES
II. TCP/IP
III. DIRECCIONAMIENTO IP
IV. RUTEO
V. SOLUCION DEL PROBLEMA

Fecha: México D.F. Noviembre de 2009

M. EN C. RAYMUNDO SANTANA ALQUICIRA
Coordinador del Seminario

ING. PEDRO AVILA BUSTAMANTE
Instructor del Seminario

M. EN C. LUIS CARLOS CASTRO MADRID
Jefe de la carrera de I.C.

Esta tesis está dedicada a:

A, mis padres y a mis abuelos, por quererme tanto y por que sin su apoyo nada de esto hubiera sido posible.

Carlos Alberto Hernández Vázquez

A mis padres, Margarita y Marcelino y a mi esposo Erick con todo mi amor y agradecimiento. Que Dios los bendiga.

Maria del Carmen Reyes Martínez

A mis padres por su apoyo y confianza. Gracias por ayudarme a cumplir mis objetivos como persona y estudiante .A mi esposo e hija por darme el tiempo para realizarme profesionalmente.

Margarita Cuervo Hernández

Dedico este logro a mi Dios, mi creador y el dador de mi vida quien me ha llenado de gozo y alegría y quien siempre me ha ayudado en los momentos difíciles. También lo dedico a mi Madre quien me ha demostrado que sí se puede salir adelante aun en medio de la adversidad.

Flor Eden Galicia Vega

Dedico este trabajo y logro primeramente a Dios, mis Padres y mi Familia

Salomón Vallarta Sánchez

AGRADECIMIENTOS

Agradezco:

Al Instituto Politécnico Nacional por haberme abierto sus puertas y darme la oportunidad para superarme.

A la Escuela Superior de Ingeniería Mecánica y Eléctrica Unidad Culhuacan, a todos mis maestros, a mis compañeros por la formación que en ella recibí porque es el arma para mí desarrollo.

A mis padres por todo su apoyo en la carrera.

A mis abuelos por haberme inculcado la formación que hoy tengo, por toda su comprensión y por su amor.

A mi tía vero por cuidarme siempre.

A mis hermanos porque aunque no crean son un gran apoyo.

A dios por haberme dejado llegar hasta esta etapa en mi vida.

A todos gracias por quererme tanto, y por que sin su apoyo nada de esto sería realidad.

Carlos Alberto Hernández Vázquez

AGRADECIMIENTOS

Agradezco:

A Dios y a mis padres, Margarita y Marcelino, por darme la vida, el amor, el apoyo, y por todo lo que me han dado, que ha sido lo necesario para lograr lo que me he propuesto a largo de mi vida, ya que sin ellos no hubiera logrado este triunfo.

A mi esposo, Erick, gracias por su amor y apoyo incondicional, sin esto y sin sus consejos no hubiera podido concluir esta parte tan importante en mi vida.

A mis hermanos, Cruz y Luis, y a sus Familias, gracias porque siempre creyeron en mi.

A los profesores de ESIME-Culhucan por compartir sus conocimientos y experiencias con sus alumnos.

Maria del Carmen Reyes Martínez

AGRADECIMIENTOS

Agradezco primeramente a Dios por ser mi mejor amigo, mi fortaleza, darme todo lo que tengo y no dejarme caer nunca.

A los Ingenieros José Manuel Monsiváis y Raymundo Santana por asesorarme a lo largo de la tesis y acompañarme en este camino que hoy culmina en el presente proyecto, y también por compartir su conocimiento conmigo e inspirar en mi mucha admiración.

A mis padres Luis Cuervo y Elena Hernández por ser los mejores y estar conmigo incondicionalmente, gracias porque sin ellos y sus enseñanzas no estaría aquí ni sería quien soy ahora, a ellos les dedico esta tesis.

A mi hija Nicole Yamile motor de mi vida a quien amo y protegeré siempre

A David De Sales, por formar parte de mi.

A mis amigos de la ESIME: Carmen Reyes, Carlos Hernández, Flor Galicia, y Salomón Vallarta por permitirme conocerlos y ser parte de su vida. Por ayudarme y estar conmigo a lo largo de la carrera, y aun después...

Margarita Cuervo Hernández

AGRADECIMIENTOS

Antes que otra cosa agradezco de todo corazón y con toda mi alma a mi Padre; mi único Dios Eterno por proveerme todo lo necesario y abrirme las puertas con todo éxito para que pudiera realizar este seminario, mi titulación.

Agradezco a Dios por la vida de mi Madre quien siempre, siempre me ha apoyado en todo. Gracias mamá porque sin tu apoyo no lo hubiera logrado, TE AMO.

Agradezco a mi familia porque han sido el motorcito para que pudiera salir adelante a pesar de las adversidades. Los quiero mucho.

Agradezco a Dios por la vida de mis mejores amigos porque han sido parte fundamental de éste logro en mi vida. Gracias chicos porque directa o indirectamente me apoyaron en este proceso. Karina gracias por siempre escucharme, te quiero mucho amiga. Liz gracias porque siempre encontré un abrazo contigo, te quiero mucho amiga. Cynthia gracias por tus consejos y abrirte para ser mi amiga, te quiero mucho amiga. Omar gracias también por tu apoyo y amistad y Otoniel gracias por ser mi amigo y por tu pronto apoyo, los quiero. Gracias chicos por las alegrías, el compañerismo, por nuestra amistad, gracias porque sé que puedo contar con ustedes y muchas gracias por ser parte de este proceso en mi vida, los amo.

Flor Eden Galicia Vega

AGRADECIMIENTOS

Agradezco a Dios, mis Padres y mi Familia

Por darme la vida e inculcarme los valores que ahora poseo, por todo el amor que a lo largo de mi existencia he recibido de su parte y haberme apoyado en los momentos más difíciles, ya que sin su amor y comprensión no hubiera podido salir adelante y lograr lo que en estos momentos soy.

Por todo lo que significan en mi vida y por todo lo que me han dado, sólo les puedo decir...

Dios les Bendiga

Salomón Vallarta Sánchez

INDICE

DISEÑO DE DIRECCIONAMIENTO IP PARA LA EMPRESA QUICK LEARNING

Objetivo 6
Problemática 6
Justificación 6
Alcance 6

Capitulo 1. INTRODUCCION A LAS REDES 7
1.1 ¿Qué es una red? 7
1.1.1 Redes de datos 7
1.2 Tipos de enlaces 9
1.2.1 Redes punto a punto 9
1.2.2 Redes punto multipunto 10
1.3 Topologías de red 10
1.3.1 Topologías más Comunes 10
1.4 Clases de redes 11
1.4.1 Redes de área local (LAN) 11
1.4.2 Redes de Área Metropolitana (MAN) 12
1.4.3 Redes de área amplia (WAN) 12
1.5 El modelo OSI 13
1.5.1 Capa de Aplicación 14
1.5.2 Capa de Presentación 15
1.5.3 Capa de Sesión 15
1.5.4 Capa de Transporte 16
1.5.5 Capa de red 16
1.5.6 Capa de Enlace de Datos 16
1.5.7 Capa Física 18

Capitulo 2. TCP/IP 19
2.1 Protocolos TCP/IP de Internet y modelo OSI 19
2.2 Pila del protocolo TCP/IP y la capa de aplicación 20
2.2.1 TCP/IP 20
2.2.2 Protocolos de diagnóstico de fallas 22
2.2.3 Pila del protocolo TCP/IP y la capa de transporte 23
2.3 Formato de segmentos TCP y UDP 24
2.4 Saludo de tres vías/conexión abierta de TCP 27
2.5 Acuse de recibo simple y ventanas de TCP 28
2.5.1 Ventana deslizante de TCP 29
2.6 Secuencia y números de acuse de recibo de TCP 30
2.7 Descripción de tcp-ip 30
2.7.1TCP/IP y la capa Internet 30
2.7.2 Diagrama del datagrama IP 31
2.7.3 Protocolo de Mensajes de Control en Internet (ICMP) 33

2.7.4 Funcionamiento de la prueba de ICMP 33
2.7.5 Funcionamiento de ARP 34

Capitulo 3. DIRECCIONAMIENTO IP 35
3.1. Descripción general. 35
3.1.1 Introducción a las direcciones IP 35
3.1.2 Direcciones de host 36
3.1.3 Direcciones de broadcast 36
3.1.4 Transmisión de broadcast 36
3.2 Direccionamiento IP 37
3.3 Clases de Direccionamiento 38
3.4 Mascara de Red 40
3.5 Subredes 42
3.6 Mascara de subred 44
3.7 Calculo de subredes 45

Capitulo 4. RUTEO 48
4.1 Conceptos básicos sobre enrutamiento 48
4.1.1 Determinación de ruta 48
4.1.2. Enrutamiento de paquetes del origen al destino por parte de los routers 49
4.1.3 Protocolo enrutado versus protocolo de enrutamiento 49
4.1.4 Operaciones de protocolo de capa de red 50
4.2 Rutas estáticas versus rutas dinámicas 51
4.2.1 Por qué usar una ruta estática 52
4.2.2 Uso de una ruta por defecto 53
4.2.3 Por qué es necesario el enrutamiento dinámico 53
4.2.4 Operaciones de enrutamiento dinámico 54
4.2.5 Determinación de las distancias de las rutas en la red a través de diversas métricas 55
4.3 Clases de protocolos de enrutamiento 56
4.3.1 Tiempo de convergencia 57
4.4 Enrutamiento vector-distancia 58
4.4.1 Principios básicos del enrutamiento vector-distancia 58
4.4.2 Intercambio de tablas de enrutamiento por parte de los protocolos vector-distancia 58
4.4.3 El problema de los loops de enrutamiento 59
4.4.4 El problema de la cuenta al infinito 60
4.4.5 Definición de un máximo 60
4.4.6 Split horizon (horizonte dividido) 61
4.5 Temporizadores de espera 62
4.6 Enrutamiento estado de enlace 63
4.6.1 Intercambio de tablas de enrutamiento por parte de los protocolos estado-enlace 64

4.6.2 Propagación de los cambios de topología a través de la red de routers 64
4.6.3 Requisitos de procesamiento y memoria 65
4.6.4 Requisitos de ancho de banda 65
4.6.5 Publicaciones de estado-enlace no sincronizadas (LSA) que llevan a decisiones de ruta incoherentes entre los routers 66
4.7 Comparación de enrutamiento vector-distancia y estado-enlace 67
4.8 Protocolos de enrutamiento híbrido 68
4.9 Enrutamiento LAN a LAN 69
4.10 Enrutamiento LAN a WAN 70
4.10.1Selección de ruta y conmutación para múltiples protocolos y medios 71

Capitulo 5. SOLUCION DEL PROBLEMA 72
5.1 Introducción al problema 72
5.2 Desarrollo de la problemática 73
5.3 Solución de la problemática 73
5.3.1 Subredes Enlaces WAN 74
5.3.2 Subredes Oficinas Generales 76
5.3.3 Subredes Sucursales 78
5.4. Conclusiones 82

ANEXOS 83
Anexo 1 FIGURAS 83
Anexo 2.TABLAS 86

INDICE DE FIGURAS 91

GLOSARIO 93

BIBLIOGRAFIA 102

DISEÑO DE DIRECCIONAMIENTO IP PARA LA EMPRESA QUICK LEARNING

Objetivo

Rediseñar el direccionamiento IP para Oficinas Generales y sucursales de la empresa Quick Learning.

Problemática

- Dificultad para agregar usuarios a la red.
- Saturación de la red.
- Gasto de presupuesto por envío frecuente de personal a sucursales foráneas.

Justificación

Con el rediseño de direccionamiento IP se mejorara el tiempo de respuesta de las peticiones al servidor del sistema y se podrá proporcionar con rapidez direcciones IP para incorporar nuevos host. La empresa obtendrá un ahorro tanto económico como de tiempo en soluciones de problemas presentados en los equipos de red de sucursales foráneas.

Alcance

Se propondrá a la empresa Quick Learning el direccionamiento lógico de IPs para oficinas generales y sucursales.

Capitulo 1. INTRODUCCION A LAS REDES

1.1 ¿Qué es una red?

Una *red* es un sistema de objetos o personas conectados de manera intrincada. Las *redes* están en todas partes, incluso en nuestros propios cuerpos. El sistema nervioso y el sistema cardiovascular son *redes*. El diagrama de racimo de la figura 1.1 muestra algunos tipos de *redes*; puede pensar en algunos más. Observe la forma en que están agrupados:

- comunicaciones
- transporte
- social
- biológico
- servicios públicos

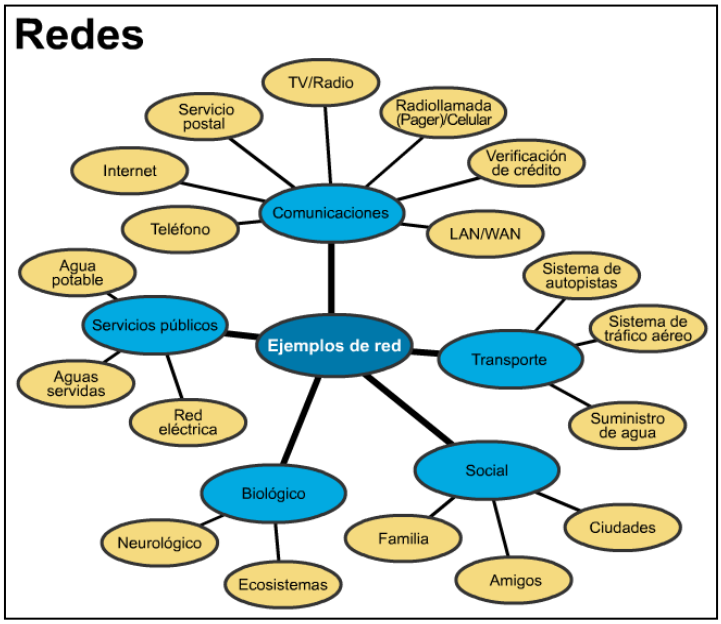

Figura 1.1 Redes

1.1.1 Redes de datos

Las redes de datos surgieron como resultado de las aplicaciones informáticas creadas para las empresas. Sin embargo, en el momento en que se escribieron estas aplicaciones, las empresas poseían computadores que eran dispositivos independientes que operaban de forma individual, sin comunicarse con los demás computadores. Muy pronto se puso de manifiesto que esta no era una forma

eficiente ni rentable para operar en el medio empresarial. Las empresas necesitaban una solución que resolviera con éxito las tres preguntas siguientes:

1. cómo evitar la duplicación de equipos informáticos y de otros recursos
2. cómo comunicarse con eficiencia
3. cómo configurar y administrar una red

Las empresas se dieron cuenta de que podrían ahorrar mucho dinero y aumentar la productividad con la tecnología de networking. Empezaron agregando redes y expandiendo las redes existentes casi tan rápidamente como se producía la introducción de nuevas tecnologías y productos de red. Como resultado, a principios de los 80, se produjo una tremenda expansión de networking. Sin embargo, el temprano desarrollo de las redes resultaba caótico en varios aspectos.

A mediados de la década del 80, comenzaron a presentarse los primeros problemas emergentes de este crecimiento desordenado. Muchas de las tecnologías de red que habían emergido se habían creado con implementaciones de hardware y software distintas. Por lo tanto, muchas de las nuevas tecnologías no eran compatibles entre sí. Se tornó cada vez más difícil la comunicación entre redes que usaban distintas especificaciones.

Una de las primeras soluciones a estos problemas fue la creación de redes de área local (LAN). Como permitían conectar todas las estaciones de trabajo, dispositivos periféricos, terminales y otros dispositivos ubicados dentro de un mismo edificio, las LAN permitieron que las empresas utilizaran la tecnología informática para compartir de manera eficiente archivos e impresoras.

A medida que el uso de los computadores en las empresas aumentaba, pronto resultó obvio que incluso las LAN no eran suficientes. En un sistema LAN, cada departamento o empresa, era una especie de isla electrónica.

Lo que se necesitaba era una forma de que la información se pudiera transferir rápidamente y con eficiencia, no solamente dentro de una misma empresa sino de

Una empresa a otra. Entonces, la solución fue la creación de *redes de área metropolitana (MAN)* y redes de área amplia (WAN). Como las WAN podían conectar redes de usuarios dentro de áreas geográficas extensas, permitieron que las empresas se comunicaran entre sí a través de grandes distancias. Para facilitar su estudio, la mayoría de las redes de datos se han clasificado como *redes de área local (LAN*) o *redes de área amplia (WAN)*. Las *LAN* generalmente se encuentran en su totalidad dentro del mismo edificio o grupo de edificios y manejan las comunicaciones entre las oficinas. Las *WAN* cubren un área geográfica más extensa y conectan ciudades y países. Algunos ejemplos útiles de *LAN* y *WAN* aparecen en la siguiente figura; se deben consultar estos ejemplos

siempre que aparezca una pregunta relativa a la definición de una *LAN* o una *WAN*. *Las LAN* y/o *las WAN* también se pueden conectar entre sí mediante internetworking.

Distancia entre las CPU	Ubicación de las CPU	Nombre
0,1 m	Placa de circuito impreso Asistente Personal de Datos	Motherboard Red de área personal (PAN)
1,0 m	Milímetro Mainframe	Red del sistema del computador
10 m	Habitación	Red de área local (LAN) Su aula
100 m	Edificio	Red de área local (LAN) Su escuela
1000 m = 1 km	Campus	Red de área local (LAN) Universidad Stanford
100.000 m = 100 km	País	Red de área amplia (WAN) Cisco Systems, Inc.
1.000.000 m = 1.000 km	Continente	Red de área amplia (WAN) África
10.000.000 m = 10.000 km	Planeta	Red de área amplia (WAN) La Internet
100.000.000 m = 100.000 km	Sistema tierra-luna	Red de área amplia (WAN) Tierra y satélites artificiales

Figura 1.2 Conexión de CPUs

1.2 Tipos de enlaces

1.2.1 Redes punto a punto

Las **redes punto a punto** son aquellas que responden a un tipo de arquitectura de red en las que cada canal de datos se usa para comunicar únicamente dos nodos, en contraposición a las redes multipunto, en las cuales cada canal de datos se puede usar para comunicarse con diversos nodos.

En una red punto a punto, los dispositivos en red actúan como socios iguales, o pares entre sí. Como pares, cada dispositivo puede tomar el rol de esclavo o la función de maestro. En un momento, el dispositivo A, por ejemplo, puede hacer una petición de un mensaje / dato del dispositivo B, y este es el que le responde enviando el mensaje / dato al dispositivo A. El dispositivo A funciona como esclavo, mientras que B funciona como maestro. Un momento después los dispositivos A y B pueden revertir los roles: B, como esclavo, hace una solicitud a A, y A, como maestro, responde a la solicitud de B. A y B permanecen en una relación reciproca o par entre ellos.

Los enlaces que interconectan los nodos de una red punto a punto se pueden clasificar en tres tipos según el sentido de las comunicaciones que transportan:

Simplex.- La transacción sólo se efectúa en un solo sentido.
Half-dúplex.- La transacción se realiza en ambos sentidos, pero de forma alternativa, es decir solo uno puede transmitir en un momento dado, no pudiendo transmitir los dos al mismo tiempo.
Full-Dúplex.- La transacción se puede llevar a cabo en ambos sentidos simultáneamente.

1.2.2 Redes punto multipunto

Es una configuración en la que dispositivos comparten el mismo enlace. En un entorno multipunto, la capacidad del canales compartida en el espacio. O en el tiempo. Si varios dispositivos pueden utilizar el enlace en forma simultanea se dice que hay una configuración de línea compartida escialmente. Si los usuarios deben compartir la línea por turnos, se dice que se trata de una configuración de línea de tiempo compartido.

1.3 Topologías de red

Las estaciones de trabajo y el servidor de ficheros de una LAN deben estar conectados mediante un medio de transmisión o cableado. La disposición física de la red se denomina 'topología'. La arquitectura también determina la topología de la red de área local. Existen tres topologías básicas que son: estrella, bus y anillo. También podemos encontrarnos derivaciones de las anteriores como las topologías en árbol, doble anillo y malla.

Llegados a este punto, conviene hacer una distinción entre topología física y lógica. La definición que hemos dado antes se refiere a la disposición física de los nodos en la red, con lo que nos estamos refiriendo a la topología física. Con topología lógica nos estamos refiriendo al modo en que se accede al medio.

Así en una red Ethernet podemos tener varias estaciones conectadas mediante un Hub (concentrador) donde la topología física es en estrella, pero el funcionamiento es como si tuviéramos un bus (topología lógica en bus). O tener una red Token Ring donde las estaciones, unidas por una MAU (un concentrador para este tipo de redes), también ienen una topología física en estrella; pero funcionan como si estuvieran conectadas en anillo (topología lógica en anillo).

1.3.1 Topologías más Comunes

- **Bus:** Esta topología permite que todas las estaciones reciban la información que se transmite, una estación transmite y todas las restantes escuchan.
- **Estrella**: Los datos en estas redes fluyen del emisor hasta el concentrador, este realiza todas las funciones de la red, además actúa como amplificador de los datos.

- **Anillo**: topología de red en la que las estaciones se conectan formando un anillo. Cada estación está conectada a la siguiente y la última está conectada a la primera.
- **Anillo doble**: consta de dos anillos concéntricos donde cada host esta conectado a ambos anillos. Es análoga a la topología de anillo con la diferencia de que para incrementar la confiabilidad y flexibilidad de la red, hay un segundo anillo redundante que conecta los mismos dispositivos. Anillo doble actúa como si fueran dos anillos independientes de los cuales se usa solo uno por v
- **Árbol**: topología de red en la que los nodos están colocados en forma de árbol. Desde una visión topológica, la conexión en árbol es parecida a una serie de redes en estrella interconectadas salvo en que no tiene un nodo central.
- **Malla**: la topología en malla es una topología de red en la que cada nodo está conectado a uno o más de los otros nodos.
- **Mixta**: topología de red que combina varias de éstas.
- **Totalmente conexa**: topología de red en la que todas las estaciones están conectadas entre sí.

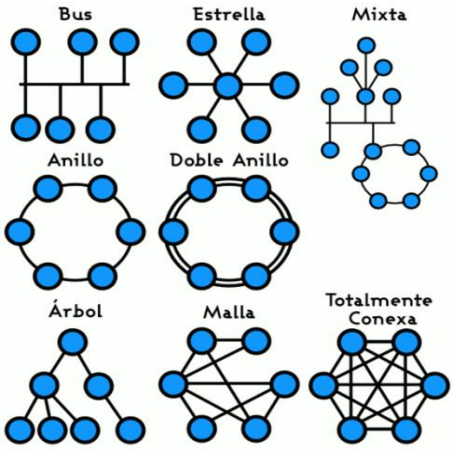

Figura 1.3 Diferentes topologías.

1.4 Clases de redes

1.4.1 Redes de área local (LAN)

Las redes de área local (LAN) se componen de computadores, tarjetas de interfaz de red, medios de networking, dispositivos de control del tráfico de red y dispositivos periféricos. Las LAN hacen posible que las empresas que utilizan tecnología informática compartan de forma eficiente elementos tales como archivos e impresoras, y permiten la comunicación, por ejemplo, a través del

correo electrónico. Unen entre sí: datos, comunicaciones, servidores de computador y de archivo.

Las LAN está diseñadas para realizar lo siguiente:

- Operar dentro de un área geográfica limitada
- Permitir que varios usuarios accedan a medios de ancho de banda alto
- Proporcionar conectividad continua con los servicios locales
- Conectar dispositivos físicamente adyacentes

Figura 1.4 Redes y dispositivos de área local

1.4.2 Redes de Área Metropolitana (MAN)

Son una versión mayor de la LAN y utilizan una tecnología muy similar. Actualmente esta clasificación ha caído en desuso, normalmente sólo distinguiremos entre redes LAN y WAN.

1.4.3 Redes de área amplia (WAN)

A medida que el uso de los computadores en las empresas aumentaba, pronto resultó obvio que incluso las LAN no eran suficientes. Lo que se necesitaba era una forma de transferir información de manera eficiente y rápida de una empresa a otra.

La solución surgió con la creación de las redes de área amplia (WAN). Las WAN interconectaban las LAN, que a su vez proporcionaban acceso a los computadores o a los servidores de archivos ubicados en otros lugares. Como las WAN

conectaban redes de usuarios dentro de un área geográfica extensa, permitieron que las empresas se comunicaran entre sí a través de grandes distancias. Como resultado de la interconexión de los computadores, impresoras y otros dispositivos en una WAN, las empresas pudieron comunicarse entre sí, compartir información y recursos, y tener acceso a Internet.

Algunas de las tecnologías comunes de las WAN son:

- módems
- RDSI (Red digital de servicios integrados)
- DSL (Digital Subscriber Line) (Línea de suscripción digital)
- Frame relay
- ATM (Modo de transferencia asíncrona)
- Series de portadoras T (EE.UU. y Canadá) y E (Europa y América Latina): T1, E1, T3, E3, etc.
- SONET (Red óptica síncrona)

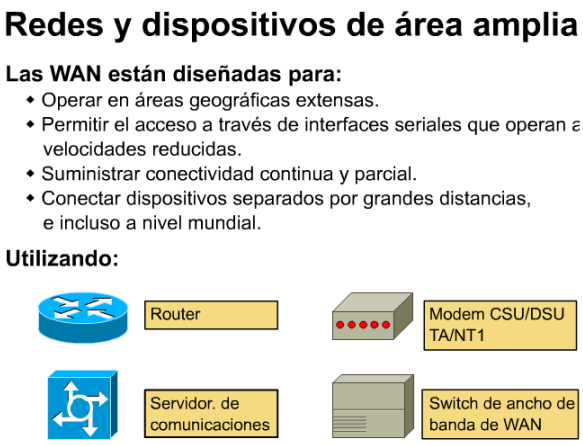

Figura 1.5 Redes y dispositivos de área amplia

1.5 El modelo OSI

El Modelo de Referencia de Interconexión de Sistemas Abiertos, conocido mundialmente como Modelo OSI (Open System Interconnection), fue creado por la ISO (Organizacion Estandar Internacional) y en él pueden modelarse o referenciarse diversos dispositivos que reglamenta la ITU (Unión de Telecomunicación Internacional), con el fin de poner orden entre todos los sistemas y componentes requeridos en la transmisión de datos, además de simplificar la interrelación entre fabricantes. Así, todo dispositivo de cómputo y telecomunicaciones podrá ser referenciado al modelo y por ende concebido como parte de un sistema interdependiente con características muy precisas en cada nivel.

El modelo OSI existe potencialmente en todo sistema de cómputo y telecomunicaciones, pero que solo cobra importancia al momento de concebir o llevar a cabo la transmisión de datos.

El Modelo OSI cuenta con 7 capas o niveles:

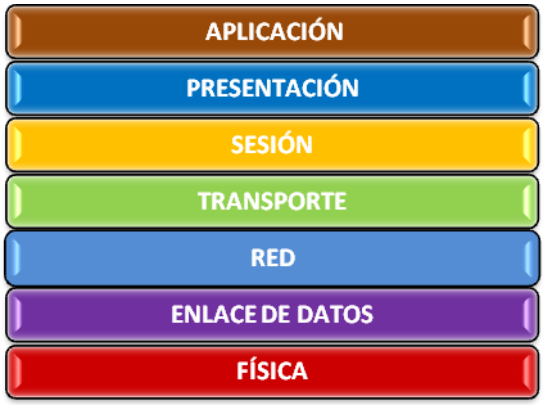

Figura 1.6 Modelo OSI

1.5.1 Capa de Aplicación

Es el nivel más cercano al usuario y a diferencia de los demás niveles, por ser el más alto o el último, no proporciona un servicio a ningún otro nivel.

Cuando se habla de aplicaciones lo primero que viene a la mente son las aplicaciones que procesamos, es decir, nuestra base de datos, una hoja de cálculo, un archivo de texto, etc., lo cual tiene sentido ya que son las aplicaciones que finalmente deseamos transmitir. Sin embargo, en el contexto del Modelo de Referencia de Interconexión de Sistemas Abiertos, al hablar del nivel de Aplicación no nos estamos refiriendo a las aplicaciones que acabamos de citar. En OSI el nivel de aplicación se refiere a las aplicaciones de red que vamos a utilizar para transportar las aplicaciones del usuario.

FTP (File Transfer Protocol), Mail, Rlogin, Telnet, son entre otras las aplicaciones incluidas en el nivel 7 del modelo OSI y sólo cobran vida al momento de requerir una comunicación entre dos entidades. Es por eso que al principio se citó que el modelo OSI tiene relevancia en el momento de surgir la necesidad de intercomunicar dos dispositivos disímiles, aunque OSI vive potencialmente en todo dispositivo de cómputo y de telecomunicaciones.

En Resumen se puede decir que la capa de Aplicación se dice que es una sesión específico de aplicación (API),es decir, son los programas que ve el usuario.

1.5.2 Capa de Presentación

Se refiere a la forma en que los datos son representados en una computadora. Proporciona conversión de códigos y reformateo de datos de la aplicación del usuario. Es sabido que la información es procesada en forma binaria y en este nivel se llevan a cabo las adaptaciones necesarias para que pueda ser presentada de una manera más accesible.

Códigos como ASCII (American Standard Code for Information Interchange) y EBCDIC (Extended Binary Coded Decimal Interchange Code), que permiten interpretar los datos binarios en caracteres que puedan ser fácilmente manejados, tienen su posicionamiento en el nivel de presentación del modelo OSI.

Los sistemas operativos como DOS y UNIX también se ubican en este nivel, al igual que los códigos de comprensión y encriptamiento de datos. El nivel de Presentación negocia la sintaxis de la transferencia de datos hacia el nivel de aplicación.

En Resumen se dice que la capa de Presentación es aquella que provee representación de datos, es decir, mantener la integridad y valor de los datos independientemente de la representación.

1.5.3 Capa de Sesión

Este nivel es el encargado de proveer servicios de conexión entre las aplicaciones, tales como iniciar, mantener y finalizar una sesión. Establece, mantiene, sincroniza y administra el diálogo entre aplicaciones remotas.

Cuando establecemos una comunicación y que se nos solicita un comando como login, estamos iniciando una sesión con un host remoto y podemos referenciar esta función con el nivel de sesión del modelo OSI. Del mismo modo, cuando se nos notifica de una suspensión en el proceso de impresión por falta de papel en la impresora, es el nivel de sesión el encargado de notificarnos de esto y de todo lo relacionado con la administración de la sesión. Cuando deseamos finalizar una sesión, quizá mediante un logout, es el nivel de sesión el que se encargará de sincronizar y atender nuestra petición a fin de liberar los recursos de procesos y canales (lógicos y físicos) que se hayan estado utilizando.

NetBIOS (Network Basic Input/Output System) es un protocolo que se referencia en el nivel de sesión del modelo OSI, al igual que el RPC (Remote Procedure Call) utilizado en el modelo cliente-servidor.

En Resumen se puede decir que la capa de Sesión es un espacio en tiempo que se asigna al acceder al sistema por medio de un login en el cual obtenemos acceso a los recursos del mismo servidor conocido como "circuitos virtuales".La

información que utiliza nodos intermedios que puede seguir una trayectoria no lineal se conoce como "sin conexión".

1.5.4 Capa de Transporte

En este nivel se realiza y se garantiza la calidad de la comunicación, ya que asegura la integridad de los datos. Es aquí donde se realizan las retransmisiones cuando la información fue corrompida o porque alguna trama (del nivel 2) detectó errores en el formato y se requiere volver a enviar el paquete o datagrama.

El nivel de transporte notifica a las capas superiores si se está logrando la calidad requerida. Este nivel utiliza reconocimientos, números de secuencia y control de flujo.

Los protocolos TCP (Transmission Control Protocol) y UDP (User Datagram Protocol) son característicos del nivel del transporte del modelo OSI, al igual que SPX (Sequenced Packet Exchange) de Novell.

En Resumen se dice que la capa de Transporte es la integridad de datos de extremo a extremo o sea que se encarga el flujo de datos del transmisor al receptor verificando la integridad de los mismos por medio de algoritmos de detección y corrección de errores, la capa de Red es la encargada de la información de enrutador e interceptores y aquella que maneja el Hardware (HW), ruteadores, puentes, multiplexores para mejorar el enrutamiento de los paquetes.

1.5.5 Capa de red

La capa de red se encarga de llevar los bloques de información desde el origen al destino. Para llevar la información al destino puede ser necesario que la información pase por una serie de nodos intermedios. Esta característica diferencia la capa de red de la de enlace que solo se preocupa de la comunicación entre estaciones conectadas al mismo cable. En una Lan con el medio compartido solo existe una ruta posible para comunicar dos estaciones por lo que el nivel de red apenas tiene trabajo en cuanto al nivel de enlace deberá realizar la tarea de comprobar si el mensaje va destinado a esa estación y si procede capturarlo comprobando la dirección MAC del destinatario.

1.5.6 Capa de Enlace de Datos

Conocido también como nivel de Trama (Frame) o Marco, es el encargado de preparar la información codificada en forma binaria en formatos previamente definidos por el protocolo a utilizar.

Tiene su aplicación en el contexto de redes WAN y LAN ya que como se estableció previamente la transmisión de datos no es mas que el envió en forma

ordenada de bits de información. Podríamos de hecho concebir a ésta como una cadena de bits que marchan en una fila inmensa (para el caso de transmisiones seriales), cadena que carece de significado hasta el momento en que las señales binarias se agrupan bajo reglas, a fin de permitir su interpretación en el lado receptor de una manera constante.

Este nivel ensambla los datos en tramas y las transmite a través del medio (LAN o WAN). Es el encargado de ofrecer un control de flujo entre tramas, así como un sencillo mecanismo para detectar errores. Es en este nivel y mediante algoritmos como CRC(Cyclic Redundancy Check), donde se podrá validar la integridad física de la trama; mas no será corregida a este nivel sino que se le notificará al transmisor para su retransmisión.

En el nivel de enlace de datos se lleva a cabo el direccionamiento físico de la información; es decir, se leerán los encabezados que definen las direcciones de los nodos (para el caso WAN) o de los segmentos (para el caso LAN) por donde viajarán las tramas. Decimos que son direcciones físicas ya que las direcciones lógicas o de la aplicación que pretendemos transmitir serán direccionadas o enrutadas en un nivel superior llamado nivel de red. En este nivel de enlace sólo se da tratamiento a las direcciones MAC (Media Access Control) para el caso de LAN y a las direcciones de las tramas síncronas como HDLC (High-Level Data Link Control), SDLC (Synchronous Data Link Control, de IBM), LAP B (Link Access Procedure Balance) por citar algunos para el caso WAN.

Como se ha expuesto hasta este momento, en el nivel dos del modelo OSI o nivel de enlace, vienen los protocolos que manejan tramas como HDLC, SDLC, LAP B, direcciones MAC, LLC, estándares de red como Token Ring, Ethernet, FDDI, ya que estos últimos manejan tramas específicas que involucran direcciones MAC. (Las topologías de Bus, Anillo o Estrella se pueden referenciar al nivel físico del modelo OSI, ya que son infraestructuras de transmisión mas que protocolos y carecen de direcciones. Aunque cierto es que están relacionadas con formatos como Ethernet y como no habrían de estarlo si son capas adyacentes que necesitan comunicarse entre sí, siendo este uno de los principios de intercomunicación dentro del modelo OSI.)

No sólo protocolos pueden ser referenciados al nivel de enlace del modelo OSI; también hay dispositivos como los puentes LAN Bridges), que por su funcionamiento (operación con base en direcciones MAC únicamente) se les puede ubicar en este nivel del modelo de referencia. El puente, a diferencia del repetidor, puede segmentar y direccionar estaciones de trabajo en función de la lectura e interpretación de las direcciones físicas de cada dispositivo conectado a la red.

En Resumen se puede decir que la capa de Enlace de Datos es aquella que transmite la información como grupos de bits, o sea que transforma los bits en

frames o paquetes por lo cual si recibimos se espera en conjunto de señales para convertirlos en caracteres en cambio si se manda se convierte directamente cada carácter en señales ya sean digitales o analógicos.

1.5.7 Capa Física

Es el primer nivel del modelo OSI y en él se definen y reglamentan todas las características físicas-mecánicas y eléctricas que debe cumplir el sistema para poder operar. Como es el nivel más bajo, es el que se va a encargar de las comunicaciones físicas entre dispositivos y de cuidar su correcta operación. Es bien sabido que la información computarizada es procesada y transmitida en forma digital siendo esta de bits: 1 y 0. Por lo que, toda aplicación que se desee enviar, será transmitida en forma serial mediante la representación de unos y ceros.

En este nivel, se encuentran reglamentadas las interfaces de sistemas de cómputo y telecomunicaciones (RS-232 o V.24, V.35) además de los tipos de conectores o ensambles mecánicos asociados a las interfaces (DB-24 y RJ-45 para RS-232 o V.24, así como Coaxial 75 ohms para G703)

En el nivel 1 del modelo OSI o nivel físico se ubican también todos los medios de transmisión como los sistemas de telecomunicaciones para el mundo WAN (Wide Area Network), tales como sistemas satelitales, microondas, radio enlaces, canales digitales y líneas privadas, así como los medios de transmisión para redes de área locales (LAN: Local Area Network), cables de cobre (UTP,STP) y fibra óptica. Además, en este nivel se ubican todos aquellos dispositivos pasivos y activos que permiten la conexión de los medios de comunicación como repetidores de redes LAN, repetidores de microondas y fibra óptica, concentradores de cableado (HUBs), conmutadores de circuitos físicos de telefonía o datos, equipos de modulación y demodulación (modems) y hasta los aparatos receptores telefónicos convencionales o de células que operan a nivel hardware como sistemas terminales.

En Resumen se dice que la capa Físico transmite el flujo de bits sobre un medio físico y aquella que representa el cableado, las tarjetas y las señales de los dispositivos.

Capitulo 2. TCP/IP

2.1 Protocolos TCP/IP de Internet y modelo OSI

El conjunto de protocolos TCP/IP se desarrolló como parte de la investigación realizada por la Agencia de Proyectos de Investigación Avanzada para la Defensa (DARPA). Originalmente, se desarrolló para suministrar comunicaciones a través de DARPA. Posteriormente, TCP/IP se incluyó en la Distribución del Software Berkeley de UNIX. TCP/IP es hoy el estándar de facto para las comunicaciones de internetwork y funciona como el protocolo de transporte para Internet, permitiendo que millones de computadores se comuniquen a nivel mundial.

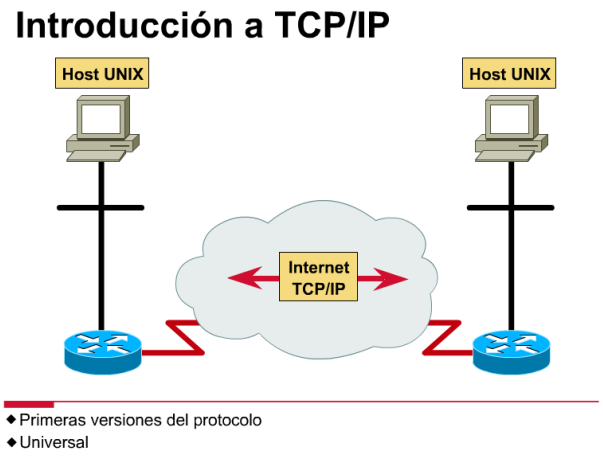

Figura 2.1 Introducción a TCP/IP

Este currículum se centra en TCP/IP por varios motivos:

- TCP/IP es un protocolo disponible a nivel mundial que, muy probablemente, usted mismo esté usando para trabajar.
- TCP/IP es una referencia útil para comprender otros protocolos porque incluye elementos que son representativos de otros protocolos.
- TCP/IP es importante porque el router lo utiliza como una herramienta de configuración.

La función de la pila, o conjunto, de protocolo TCP/IP es la transferencia de información desde un dispositivo de red a otro. Al hacer esto, se asemeja al modelo de referencia OSI (**véase figura 2.2**) en las capas inferiores y soporta todos los protocolos físicos y de enlace de datos.

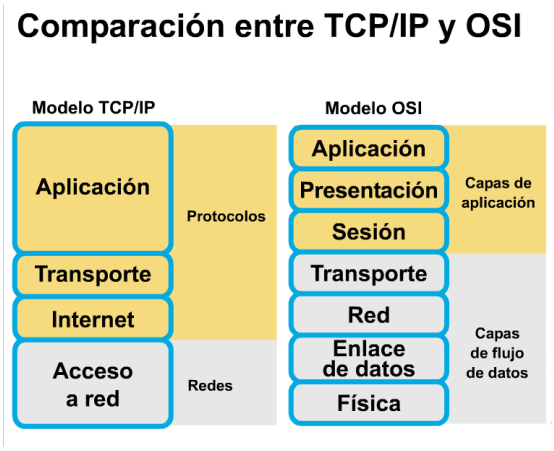

Figura 2.2 Comparación entre TCP/IP

Las capas que se ven más afectadas por TCP/IP son la Capa 7 (aplicación), la Capa 4 (transporte) y la Capa 3 (red), (**véase figura 2.3**). Dentro de estas capas se incluyen otros tipos de protocolo que tienen varios propósitos/funciones, todos ellos relacionados con la transferencia de información.

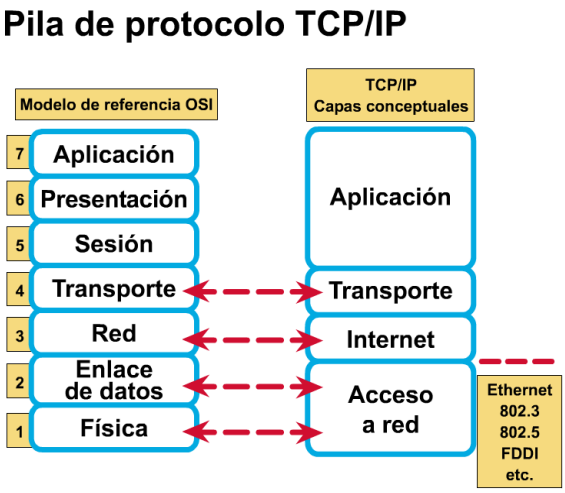

Figura 2.3 Pila de protocolo TCP/IP

2.2 Pila del protocolo TCP/IP y la capa de aplicación

2.2.1 TCP/IP

Permite la comunicación entre cualquier conjunto de redes interconectadas y sirve tanto para las comunicaciones LAN como para las de WAN. TCP/IP incluye no sólo las especificaciones de las Capas 3 y 4 (como, por ejemplo, IP y TCP) sino también especificaciones para aplicaciones tan comunes como el correo

electrónico, la conexión remota, la emulación de terminales y la transferencia de archivos.

La capa de aplicación soporta los protocolos de direccionamiento y la administración de red (**véase figura 2.4**). Además tiene protocolos para transferencia de archivos, correo electrónico y conexión remota.

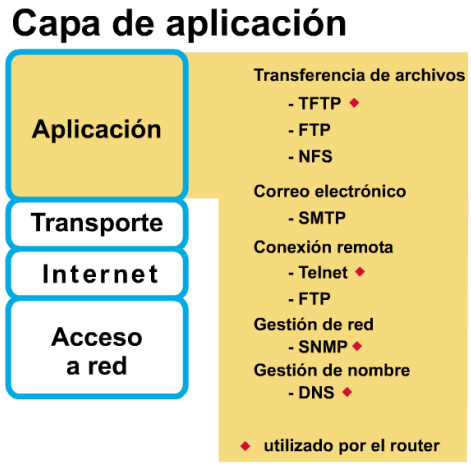

Figura 2.4 Capa de Aplicación

DNS (Sistema de denominación de dominio) es un sistema utilizado en Internet para convertir los nombres de los dominios y de sus nodos de red publicados abiertamente en direcciones (**véase figura 2.5**).

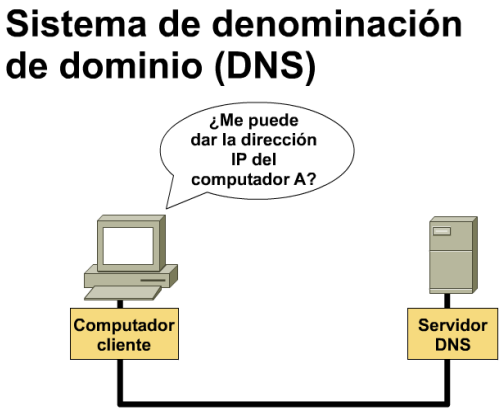

Figura 2.5 Sistema de denominación de dominio (DNS)

WINS (Servicio de nombre para Internet de Windows) es un estándar desarrollado para Windows NT de Microsoft que asocia las estaciones de trabajo NT con los nombres de dominio de Internet de forma automática.

HOSTS es un archivo creado por los administradores de red que se mantiene en los servidores. Se utiliza para suministrar asignación estática entre direcciones IP y nombres de computadores.

POP3 (Protocolo de la oficina de correos) es un estándar de Internet para almacenar correo electrónico en un servidor de correo hasta que se pueda acceder a él y descargarlo al computador. Permite que los usuarios reciban correo desde sus buzones de entrada utilizando varios niveles de seguridad.

SMTP (Protocolo simple de transferencia de correo) maneja la transmisión de correo electrónico a través de las redes informáticas. El único soporte para la transmisión de datos que suministra es texto simple.

SNMP (Protocolo simple de administración de red) es un protocolo que suministra un medio para monitorear y controlar dispositivos de red, y para administrar configuraciones, recolección de estadísticas, desempeño y seguridad.

FTP (Protocolo de transferencia de archivos) es un servicio confiable orientado a conexión que utiliza TCP para transferir archivos entre sistemas que soportan FTP. Soporta transferencias bidireccionales de archivos binarios y archivos ASCII.

TFTP (Protocolo trivial de transferencia de archivos) es un servicio no confiable no orientado a conexión que utiliza UDP para transferir archivos entre sistemas que soportan el Protocolo TFTP. Es útil en algunas LAN porque opera más rápidamente que FTP en un entorno estable.

HTTP (Protocolo de transferencia de hipertexto) es el estándar Internet que soporta el intercambio de información en la World Wide Web, así como también en redes internas. Soporta muchos tipos de archivos distintos, incluyendo texto, gráfico, sonido y vídeo. Define el proceso a través del cual los navegadores de la Web originan solicitudes de información para enviar a los servidores de Web.

2.2.2 Protocolos de diagnóstico de fallas

Telnet es un protocolo estándar de emulación de terminal utilizado por los clientes con el propósito de realizar conexiones de terminal remota con los servicios del servidor Telnet; permite que los usuarios se conecten de forma remota con los routers para introducir comandos de configuración.

PING (Packet Internet Groper) es una utilidad de diagnóstico que se utiliza para determinar si un computador está conectado correctamente a los dispositivos o a Internet.

Traceroute es un programa que está disponible en varios sistemas y es similar a PING, excepto que traceroute suministra más información que PING. Traceroute rastrea la ruta que toma un paquete hacia el destino y se utiliza para depurar problemas de enrutamiento.
También hay algunos protocolos basados en Windows con los que debe familiarizarse:

NBSTAT utilitario para diagnosticar las fallas de la resolución de nombres NetBIOS; se utiliza para visualizar y eliminar entradas del caché de nombres.

NETSTAT utilidad que suministra información acerca de estadísticas TCP/IP; se puede utilizar para suministrar información acerca del estado de las conexiones TCP/IP y resúmenes de ICMP, TCP y UDP.

ipconfig/winipcfg utilitarios para visualizar las configuraciones actuales de red para todos los adaptadores ip (nic) de un dispositivo; se puede utilizar para visualizar la dirección MAC, la dirección IP y el gateway.

2.2.3 Pila del protocolo TCP/IP y la capa de transporte

La capa de transporte (**véase figura 2.6**) permite que un dispositivo de usuario divida en segmentos varias aplicaciones de capas superiores para colocarlas en la misma corriente de datos de la Capa 4, y permite que un dispositivo receptor pueda reensamblar los segmentos de las aplicaciones de las capas superiores. La corriente de datos de Capa 4 es una conexión lógica entre los extremos de una red, y brinda servicios de transporte desde un host hasta un destino. Este servicio a veces se denomina servicio de extremo a extremo.

La capa de transporte también proporciona dos protocolos:

- *TCP*: un protocolo confiable, orientado a conexión; suministra control de flujo a través de ventanas deslizantes, y confiabilidad a través de los números de secuencia y acuses de recibo. TCP vuelve a enviar cualquier mensaje que no se reciba y suministra un circuito virtual entre las aplicaciones del usuario final. La ventaja de TCP es que proporciona una entrega garantizada de los segmentos.
- *UDP*: protocolo no orientado a conexión y no confiable; aunque tiene la responsabilidad de transmitir mensajes, en esta capa no se suministra ninguna verificación de software para la entrega de segmentos. La ventaja de UDP es la velocidad.
- Como UDP no suministra acuses de recibo, se envía menos cantidad de tráfico a través de la red, lo que agiliza la transferencia.

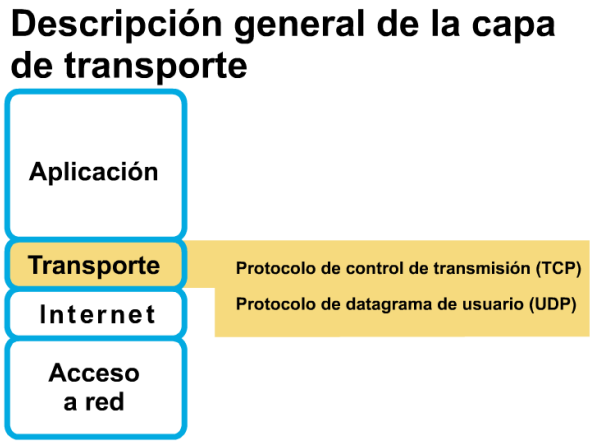

Figura 2.6 Descripción general de la capa de transporte

2.3 Formato de segmentos TCP y UDP

El segmento TCP está formado por los siguientes campos (**véase figura 2.7**):

- *puerto origen*: número del puerto que realiza la llamada
- *puerto destino*: número del puerto que recibe la llamada
- *número de secuencia*: número que se utiliza para asegurar el secuencia miento correcto de los datos que se reciben
- *número de acuse de recibo*: siguiente octeto TCP esperado
- *HLEN*: cantidad de palabras de 32 bits del encabezado
- *reservado*: se establece en 0
- *bits de código*: funciones de control (por ej., establecimiento y terminación de una sesión)
- *ventana*: cantidad de octetos que el emisor está dispuesto a aceptar
- *suma de comprobación*: suma de comprobación calculada de los campos de encabezado y datos
- *señalador urgente*: indica el final de los datos urgentes
- *opción*: la definida en la actualidad: tamaño máximo del segmento TCP
- *datos*: Datos de protocolo de capa superior

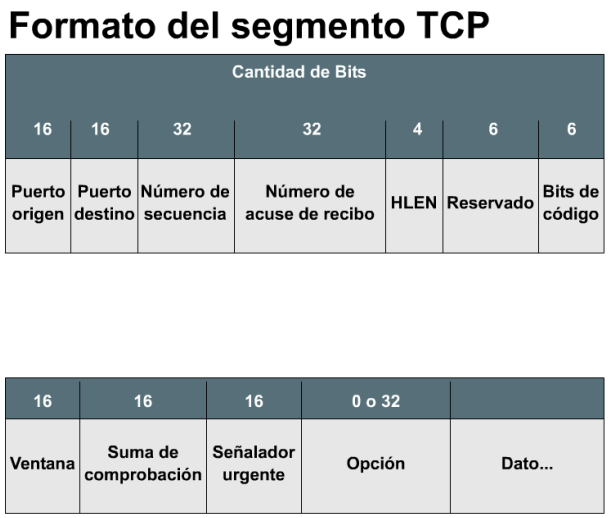

Figura 2.7 Formato del segmento TCP

Los protocolos de capa de aplicación deben brindar confiabilidad en caso de ser necesario. UDP no utiliza ventanas ni acuses de recibo. Está diseñado para aplicaciones que no necesitan ensamblar secuencias de segmentos. Como se puede observar en la figura 2.3.2 el encabezado UDP es relativamente pequeño.

Entre los protocolos que usan UDP se incluyen los siguientes (**véase figura 2.8**):

- TFTP
- SNMP
- Sistema de archivos de red (NFS)
- Sistema de denominación de dominio (DNS)

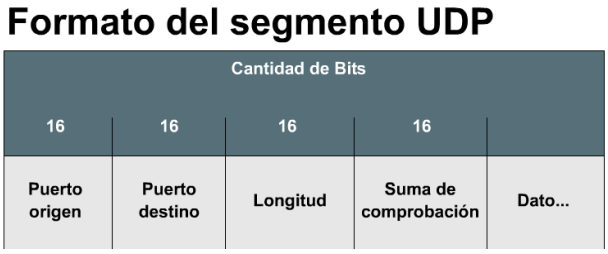

Figura 2.8 Formato del segmento UDP

Tanto TCP como UDP utilizan números de puerto (o socket) para enviar información a las capas superiores. Los números de puerto se utilizan para mantener un registro de las distintas conversaciones que atraviesan la red al mismo tiempo.

Los creadores del software de aplicación han acordado utilizar los números de puerto conocidos que se definen en RFC 1700. Por ejemplo, cualquier

conversación destinada a una aplicación FTP utiliza el número de puerto 21 (**véase figura 2.9**) como estándar.

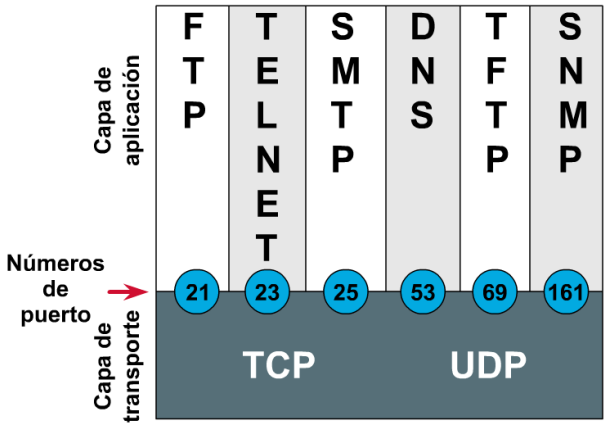

Figura 2.9 Números de puerto

En cambio, a las conversaciones que no involucran ninguna aplicación que tenga un número de puerto conocido, se les asignan números de puerto que se seleccionan de forma aleatoria dentro de un intervalo específico. Estos números de puerto se usan como direcciones origen y destino en el segmento TCP/UDP.

Algunos puertos son puertos reservados, tanto en TCP como en UDP, aunque es posible que algunas aplicaciones no estén hechas para soportarlos. Los números de puerto tienen los siguientes intervalos asignados:

- Los números inferiores a 255 corresponden a aplicaciones públicas.
- Los números entre 255-1023 se asignan a empresas para aplicaciones comercializables.
- Los números superiores a 1023 no están regulados.

Los sistemas finales utilizan números de puerto para seleccionar la aplicación adecuada (**véase figura 2.10**) El host origen asigna dinámicamente los números de puerto origen, por lo general un número mayor que 1023.

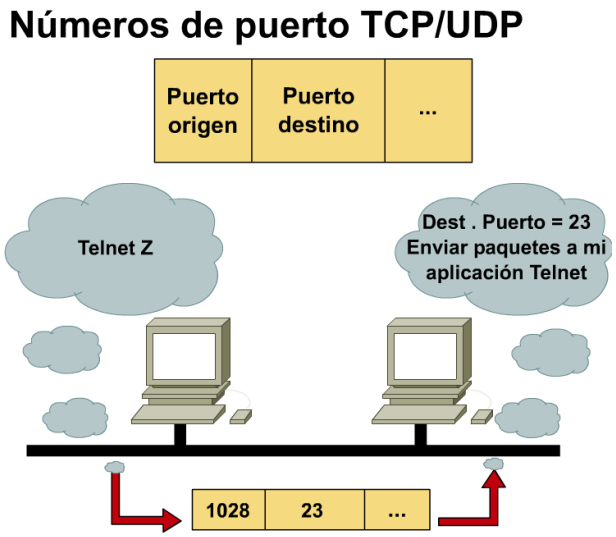

Figura 2.10 Números de puerto TCP/UDP

2.4 Saludo de tres vías/conexión abierta de TCP

Para que se establezca una conexión, las dos estaciones finales deben sincronizarse con los números de secuencia TCP iniciales de la otra estación (ISN). Los números de secuencia se utilizan para rastrear el orden de los paquetes y para garantizar que ningún paquete se pierda durante la transmisión. El número de secuencia inicial es el número de inicio que se utiliza cuando se establece la conexión TCP. El intercambio de los números iniciales de la secuencia durante la secuencia de conexión asegura que los datos perdidos se puedan recuperar.

La *sincronización* se logra intercambiando segmentos que transportan los ISN y un bit de control denominado *SYN*, que significa *sincronizar*. (Los segmentos que transportan el bit SYN también se denominan SYNs.) Para que la conexión tenga éxito, se requiere un mecanismo adecuado para elegir una secuencia inicial y un proceso levemente complicado para intercambiar los ISN. La sincronización requiere que cada uno de los lados envíe su propio ISN y reciba una confirmación y un ISN desde el otro lado de la conexión. Cada uno de los lados debe recibir el ISN del otro lado y enviar un acuse de recibo de confirmación (ACK) según un orden específico (véase figura 2.11), que se describe en los siguientes pasos:

A ->B SYN - Mi número de secuencia es X.
A <- B ACK -Su número de secuencia es X.
A <- B SYN - Mi número de secuencia es Y.
A ->B ACK - Su número de secuencia es Y

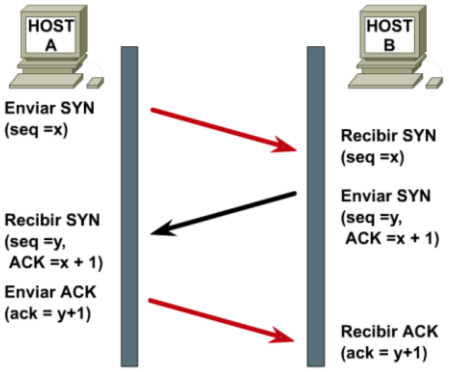

Figura 2.11 Saludo de tres vías/conexión abierta TCP

Como el segundo y el tercer paso se pueden combinar en un solo mensaje, el intercambio se denomina saludo de tres vías/conexión abierta. Como se ilustra en la figura 2.11, ambos extremos de una conexión se sincronizan mediante una secuencia de saludo de tres vías/conexión abierta.

Es necesario un saludo de tres vías porque los TCP pueden utilizar distintos mecanismos para elegir el ISN. El receptor del primer SYN no tiene forma de saber si el segmento es un segmento antiguo demorado a menos que recuerde el último número de secuencia utilizado en la conexión, lo que no siempre es posible, de modo que debe solicitar al emisor que verifique este SYN.

En este punto, cualquiera de los dos lados puede comenzar la comunicación, y cualquiera de los dos lados puede interrumpirla, dado que TCP es un método de comunicación de par a par (balanceado).

2.5 Acuse de recibo simple y ventanas de TCP

Para regular el flujo de datos entre dispositivos, TCP utiliza un mecanismo de control de flujo de par a par. La capa TCP del host receptor indica un tamaño de ventana a la capa TCP del host emisor. Este tamaño de ventana especifica la cantidad de bytes, comenzando por el número de acuse de recibo, que la capa TCP del host receptor actualmente está preparada para recibir.

Tamaño de ventana se refiere a la cantidad de bytes que se transmiten antes de recibir un acuse de recibo. Después de transmitir la cantidad máxima de bytes que permite el tamaño de la ventana, debe recibir un acuse de recibo antes de poder enviar más datosEl tamaño de la ventana determina qué cantidad de datos la estación receptora puede aceptar de una sola vez. Con un tamaño de ventana de 1, cada segmento transporta sólo un byte de datos y se debe recibir un acuse de recibo antes de poder transmitir otro segmento. Esto da como resultado un uso ineficaz del ancho de banda por parte del host.

El propósito de las ventanas es mejorar la confiabilidad y el control del flujo. Infelizmente, con un tamaño de ventana de 1, se produce un uso ineficaz del ancho de banda, como se ve en la figura 2.12.

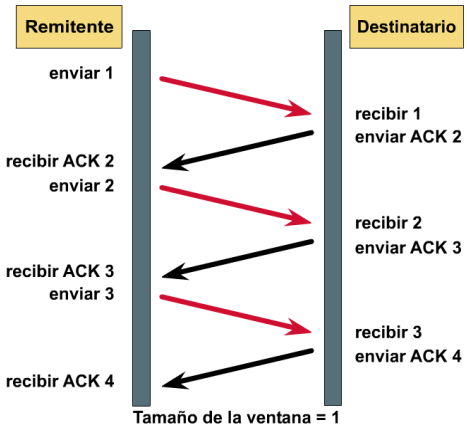

Figura 2.12 Acuse de recibo simple TCP

2.5.1 Ventana deslizante de TCP

TCP utiliza acuses de recibo de expectativa, lo que significa que el número de acuse de recibo se refiere al siguiente octeto esperado. El calificativo de *"deslizante"* de *la ventana deslizante* se refiere al hecho de que el tamaño de la ventana se negocia de forma dinámica durante la sesión TCP (**véase figura 2.13**). Una ventana deslizante da como resultado un uso más eficiente del ancho de banda por parte del host, dado que un tamaño de ventana más grande permite que se transmitan más datos antes de recibir el acuse de recibo.

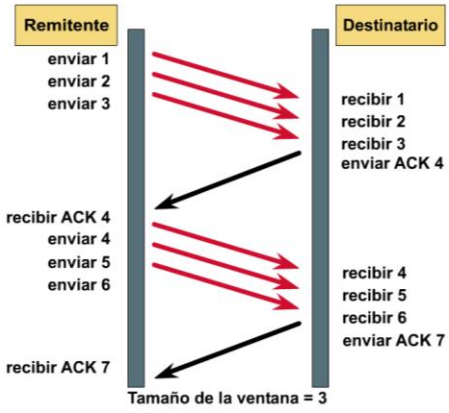

Figura 2.13 Ventana deslizante TCP

2.6 Secuencia y números de acuse de recibo de TCP

TCP proporciona un secuencia miento de segmentos con un acuse de recibo de referencia de envío. Cada datagrama se numera antes de la transmisión. En la estación receptora, TCP re ensambla los segmentos hasta formar un mensaje completo. Si falta un número de secuencia en la serie, el segmento se vuelve a transmitir. Si no se envía un acuse de recibo de los segmentos dentro de un período de tiempo determinado, se lleva a cabo la retransmisión.

Los números de secuencia y de acuse de recibo son direccionales, lo que significa que la comunicación se produce en ambas direcciones. La figura 2.14 ilustra la comunicación que se produce en una dirección. La secuencia y los acuses de recibo se producen con el emisor ubicado a la derecha de la pantalla.

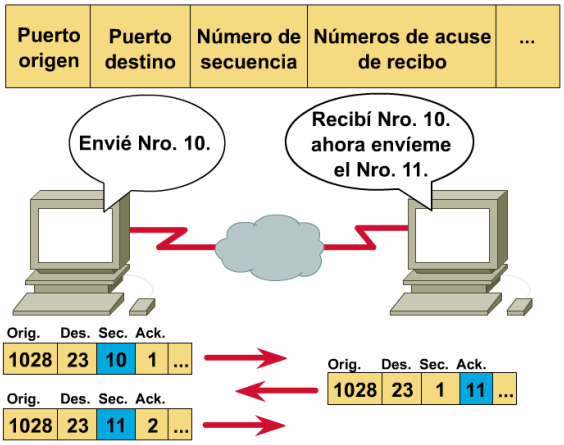

Figura 2.14 Secuencia TCP y Números de acuse de recibo

2.7 Descripción de tcp-ip

2.7.1TCP/IP y la capa Internet

La capa de Internet de la pila de TCP/IP corresponde a la capa de red del modelo OSI. Estas capas tiene la responsabilidad de transportar paquetes a través de una red utilizando el direccionamiento por software.

Como se muestra en la figura, varios protocolos operan en la capa Internet de TCP/IP, que corresponde a la capa de red del modelo OSI:

- *IP* : suministra enrutamiento de datagramas no orientado a conexión, de máximo esfuerzo de entrega; no se ocupa del contenido de los datagramas; busca la forma de desplazar los datagramas al destino
- *ICMP* : aporta capacidad de control y mensajería

- *ARP* : determina direcciones a nivel de capa de enlace de datos para las direcciones IP conocidas
- *RARP* : determina las direcciones de red cuando se conocen las direcciones a nivel de la capa de enlace de datos

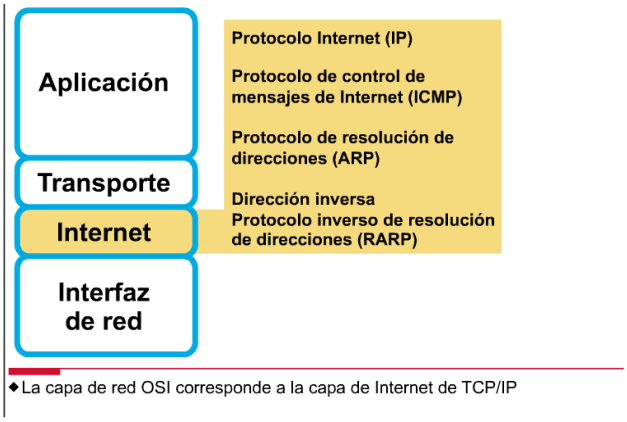

Figura 2.15 Descripción general de la capa de red

2.7.2 Diagrama del datagrama IP

La figura 2.16 ilustra el formato de un datagrama IP. Un datagrama IP contiene un encabezado IP y datos, y está rodeado por el encabezado de la capa de Control de Acceso al Medio (MAC) y la información final de la capa MAC. Un mensaje se puede transmitir como un conjunto de datagramas que se vuelven a ensamblar en el mensaje en la ubicación receptora. Los campos de este datagrama IP son los siguientes:

- *VERS* : número de versión
- *HLEN* : longitud del encabezado, en palabras de 32 bits
- *tipo de servicio*: cómo se debe administrar el datagrama
- *longitud total*: longitud total (encabezado + datos)
- *identificación, señaladores, compensación de fragmentos*: suministra fragmentación de datagramas para permitir distintas MTU en la internetwork
- *TTL*: Tiempo de existencia
- *protocolo*: protocolo de capa superior (Capa 4) que envía el datagrama
- *checksum del encabezado*: verificación de integridad del encabezado
- *dirección IP origen* y *dirección IP destino*: direcciones IP de 32 bits
- *opciones IP*: verificación de la red, depuración, seguridad y otras opciones

Cantidad de Bits							
4	4	8	16	16	3	13	8
VERS	HLEN	Tipo de servicio	Longitud total	Ident-ificación	Señal-adores	Compensación de fragmentos	TTL

8	16	32	32	var	
Protocolo	Encabezado suma de comprobación	Dirección IP origen	Dirección IP destino	Opciones IP	Datos...

Figura 2.16 El datagrama IP

El campo de protocolo (**véase figura 2.17**) determina el protocolo de Capa 4 que se transporta dentro de un datagrama IP. Aunque la mayoría del tráfico IP utiliza TCP, otros protocolos también pueden utilizar IP. Cada encabezado IP debe identificar el protocolo de Capa 4 destino para el datagrama. Los protocolos de la capa de transporte se numeran, de forma similar a los números de puerto. IP incluye el número de protocolo en el campo de protocolo.

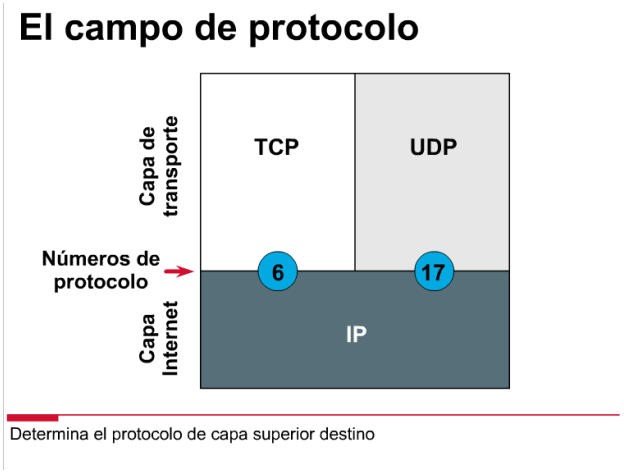

Figura 2.17 El campo de protocolo

2.7.3 Protocolo de Mensajes de Control en Internet (ICMP)

Todos los hosts TCP/IP implementan ICMP. Los mensajes de ICMP se transportan en datagramas IP y se utilizan para enviar mensajes de error y control (**véase figura 2.18**). ICMP utiliza los siguientes tipos de mensajes definidos. Hay otros mensajes que no se incluyen en esta lista:

- Destination Unreachable (Destino inalcanzable)
- Time to Live Exceeded (Tiempo de existencia superado)
- Parameter Problem (Problema de parámetros)
- Source Quench (Suprimir origen)
- Redirect (Redirigir)
- Echo (Eco)
- Echo Reply (Respuesta de eco)
- Timestamp (Marca horaria)
- Timestamp Reply (Respuesta de marca horaria)
- Information Request (Petición de información)
- Information Reply (Respuesta de información)
- Address Request (Petición de dirección)
- Address Reply (Respuesta de dirección)

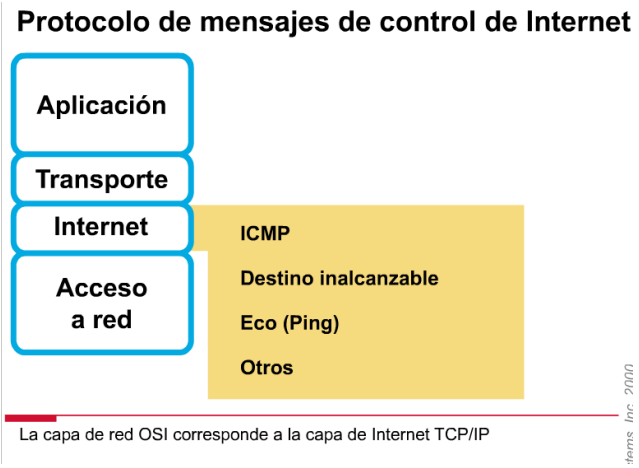

Figura 2.18 Protocolo de mensajes de control de Internet

2.7.4 Funcionamiento de la prueba de ICMP

Si un router recibe un paquete que no puede enviar a su destino final, envía al origen un mensaje ICMP destino inalcanzable, como se indica en la figura 2.19 Es posible que el mensaje no se pueda entregar porque no hay ninguna ruta conocida hacia el destino.

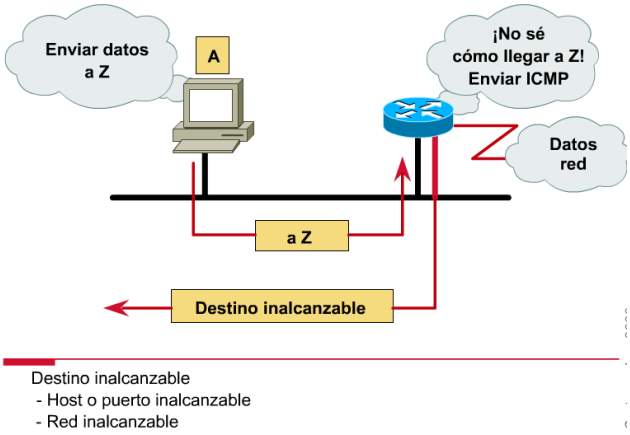

Figura 2.19 Prueba de ICMP

En la figura 2.20 una respuesta de eco es una respuesta exitosa a un comando **ping**. Sin embargo, los resultados pueden incluir otros mensajes ICMP como, por ejemplo, mensajes destino inalcanzable o límite de tiempo excedido.

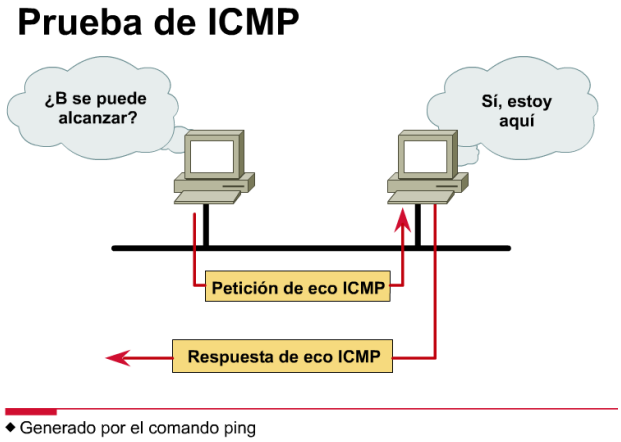

Figura 2.20 Prueba de ICMP

2.7.5 Funcionamiento de ARP

ARP se utiliza para resolver o asignar una dirección IP conocida a una dirección de subcapa MAC para permitir la comunicación a través de un medio de acceso múltiple como, por ejemplo, Ethernet. Para determinar una dirección MAC destino para un datagrama, se verifica una tabla denominada caché ARP. Si la dirección no figura en la tabla, ARP envía un broadcast que se recibe en cada estación de la red, buscando la estación destino.

El término "ARP local" se utiliza para describir la búsqueda de una dirección cuando el host que la solicita y el host destino comparten el mismo medio o cable.

Como se indica en la figura 2.21, antes de emitir el ARP, se debe consultar la máscara de subred. En este caso, la máscara determina que los nodos se encuentran en la misma subred.

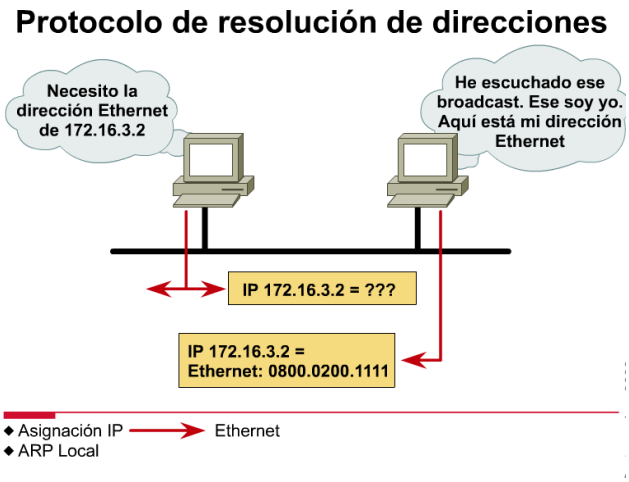

Figura 2.21 Protocolo de resolución de direcciones

Capitulo 3. DIRECCIONAMIENTO IP

3.1. Descripción general.

En "TCP/IP" se analizó el Protocolo de Control de Transmisión/Protocolo Internet (TCP/IP) y su funcionamiento para asegurar la comunicación a través de cualquier conjunto de redes interconectadas. En este capítulo, aprenderá los detalles de las clases de direcciones IP, las direcciones de nodo y de red y las máscaras de subred. Además, aprenderá los conceptos que debe conocer antes de configurar una dirección IP.

3.1.1 Introducción a las direcciones IP

En un entorno TCP/IP, las estaciones finales se comunican con servidores u otras estaciones finales. Esto puede ocurrir porque cada nodo que utiliza el conjunto de protocolos TCP/IP tiene una dirección lógica distinta de 32 bits.

Esta dirección se denomina dirección IP y se especifica en formato decimal separado por puntos de 32 bits. Las interfaces del router se deben configurar con una dirección IP si el protocolo IP se debe enrutar hacia o desde la interfaz. Se

pueden utilizar los comandos **ping** y **trace** para verificar la configuración de dirección IP.

Cada empresa u organización conectada a Internet aparece como una sola red a la que se debe llegar antes de que se pueda contactar un host en particular dentro de esa empresa.

3.1.2 Direcciones de host

En esta sección, aprenderá los conceptos básicos que debe conocer antes de configurar una dirección IP. Al examinar diversos requisitos de red, puede seleccionar la clase de dirección correcta y definir cómo establecer subredes IP. Cada dispositivo o interfaz debe tener un número de host que no tenga sólo ceros en el campo de host. Una dirección de host de sólo unos está reservada para un broadcast IP hacia esa red. Un valor de host de 0 significa "esta red" o "el cable en sí mismo" (por ej., 172.16.0.0). También, aunque rara vez, se utiliza un valor 0, para los broadcasts IP en algunas implementaciones TCP/IP más antiguas. La tabla de enrutamiento contiene entradas para las direcciones de red o de cable. Por lo general, no contiene información acerca de los hosts.

Una dirección IP y una máscara de subred en una interfaz cumplen tres propósitos:

- Permiten que el sistema procese la recepción y transmisión de paquetes.
- Especifican la dirección local del dispositivo.
- Especifican un intervalo de direcciones que comparten el cable con el dispositivo.

3.1.3 Direcciones de broadcast

IP soporta el broadcast. Se pretende que los mensajes sean vistos por todos los hosts de la red. La dirección de broadcast se forma utilizando sólo unos en una parte de la dirección IP.El software Cisco IOS soporta dos tipos de broadcasts: broadcasts dirigidos y broadcasts inundados. Los broadcasts dirigidos hacia una red/subred específica son autorizados y retransmitidos por el router.

Estos broadcasts dirigidos contienen sólo unos en la parte de la dirección correspondiente al host. Los broadcasts inundados (255.255.255.255) no se propagan, sino que se consideran broadcasts locales.

3.1.4 Transmisión de broadcast

Una transmisión de broadcast esta constituida por un único paquete de datos que se envía hacia la red, donde se lo copia y se lo envía a todos los nodos de red. El

nodo origen agrega a los paquetes una dirección de broadcast que especifica que el paquete se debe enviar a todos los nodos destinos posibles. Entonces los paquetes se envían a la red. La red copia los paquetes y los envía hacia todos los nodos de la red.

3.2 Direccionamiento IP

Para poder identificar un host cada uno de ellos tiene una dirección IP. Las direcciones IP tienen 32 bits de longitud con 4 campos de 8 bits cada uno, con lo cual se tiene la posibilidad de manejar 4, 294, 967,296 direcciones diferentes. De los 32 bits una parte representa el identificador red y otra el host.

Una dirección IP se representa por cuatro campos decimales separados por puntos, como 172.16.122.204, los cuales no pueden superar el valor 255 (11111111 en binario). (**véase figura 3.1**)

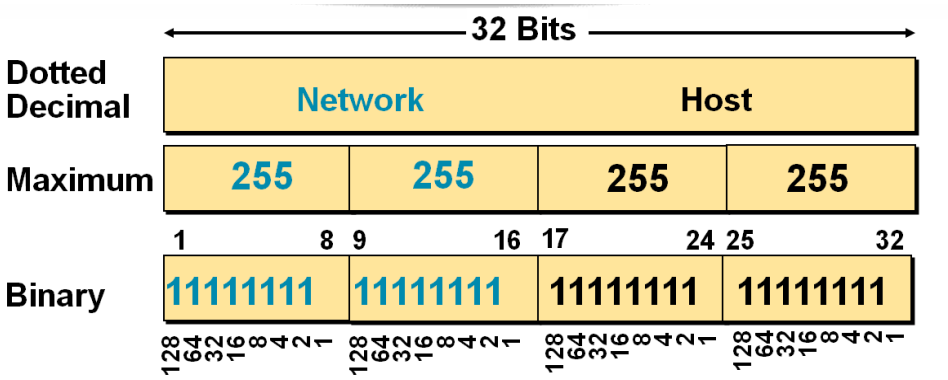

Figura 3.1 Una dirección IP está compuesta por 32 bits

Las direcciones se escriben en un formato decimal aunque normalmente se pasan de binario a decimal como se muestra en la **figura 3.2**.

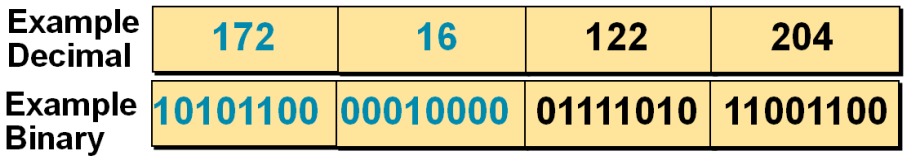

Figura 3.2 Ejemplo de número binario a decimal

3.3 Clases de Direccionamiento

Las direcciones IP se clasifican en 5 clases diferentes:

Clase A: Direcciones para redes muy grandes, con 7 bits para la dirección de red en el primer octeto (de los cuatro que representa la dirección IP) y 24 bits (3 últimos octetos) que se asignan a los Host. (**véase figura 3.3**)

El rango de direcciones valido para la clase A va del 1.0.0.0 (00000001 en binario en el primer octeto) al 126.0.0.0 (01111110 en binario en el primer octeto). La dirección 0.0.0.0 (00000000 en el primer octeto) es utilizada por las máquinas cuando están arrancando o no se les ha asignado dirección y las direcciones 127.x.x.x se reservan para pruebas de retroalimentación. Se denomina **dirección de bucle local** o **loopback**. (**véase figura 3.4**)

De modo que la cantidad máxima de hosts es 2^{24} – 2 es decir, 16 777 214 hosts. Se restan 2 por las direcciones reservadas de broadcast (últimos octetos a 255) y de red (últimos octetos a 0).
Clase B: Utilizan 14 bits para la dirección de red (primeros 2 octetos) y16 bits (últimos 2 octetos) que se asignan a los host. (**véase figura 3.3**)

El rango de direcciones valido para la clase B va del 128.0.0.0 (10000000 en binario en el primer octeto) al 191.0.0.0 (10111111 en binario en el primer octeto). (**véase figura 3.4**).

De modo que la cantidad máxima de hosts es 2^{16} - 2, o 65 534 hosts. . Se restan 2 por las direcciones reservadas de broadcast (últimos octetos a 255) y de red (últimos octetos a 0).

Clase C: Utilizan 22 bits para la dirección de red (3 primeros octetos) y 8 bits (ultimo octeto) que se asignan a los host. (**véase figura 3.3**).

La cantidad de hosts es limitada. De modo que la cantidad máxima de hosts es 2^{8} - 2, ó 254 hosts.

EL rango de direcciones valido la clase C va del 192.0.0.0 (11000000 en binario en el primer octeto) al 223.0.0.0 (11011111 en binario en el primer octeto) (**véase figura 3.4**).

Clase D: Esta clase está reservada para servicio multicast.

Clase E: Esta clase se encuentra reservada para uso futuro.

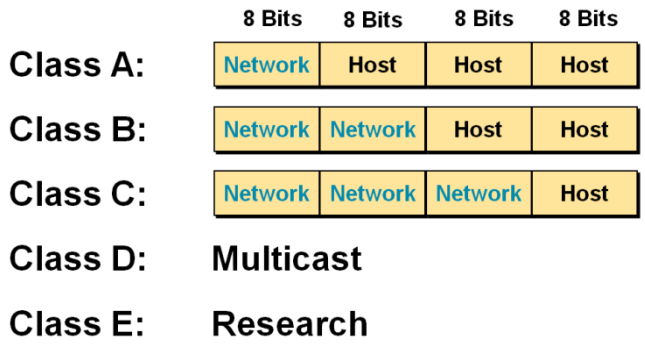

Figura 3.3 Asignación de bits a la parte de red y de host

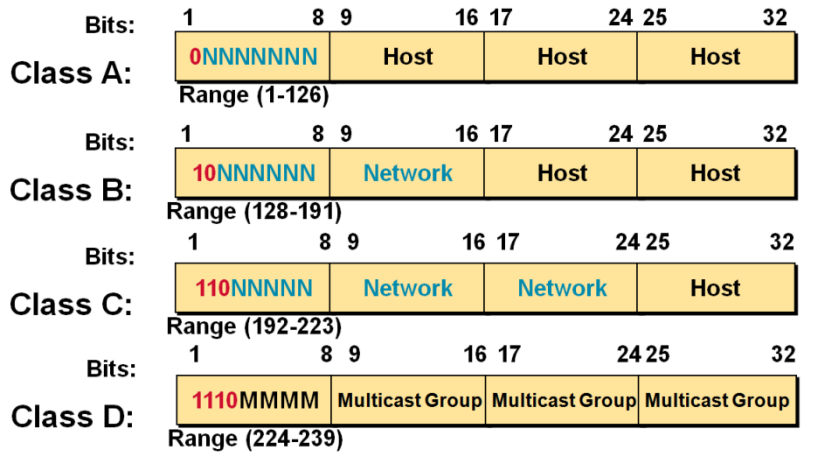

Figura 3.4 Rango de direcciones IP valido

Hay ciertas direcciones en cada clase de dirección IP que no están asignadas y que se denominan direcciones privadas. Las direcciones privadas pueden ser utilizadas por los hosts que usan traducción de dirección de red (NAT) para conectarse a una red pública o por los hosts que no se conectan a Internet. En una misma red no pueden existir dos direcciones iguales, pero sí se pueden repetir en dos redes privadas que no tengan conexión entre sí o que se sea a través de NAT. Las direcciones privadas son:

- Clase A: 10.0.0.0 a 10.255.255.255 \\Uso VIP Ej.: La red militar norte-americana
- Clase B: 172.16.0.0 a 172.31.255.255 (12 bits red, 20 bits hosts)\\Uso universidades y grandes compañías.
- Clase C: 192.168.0.0 a 192.168.255.255 (16 bits red, 16 bits hosts)\\Uso de compañías medias y pequeñas además pequeños proveedores de internet(ISP)

Un ejemplo para comprender mejor como obtener el número de host validos dependiendo la clase de direccionamiento (A, B o C) se muestra en la figura 3.5. En este ejemplo tenemos que la dirección es de clase B por lo tanto los dos últimos octetos nos indicaran cuantos host podemos tener en esta red (172.16.0.0) El primer host que se puede asignar a esta red es el 172.16.0.1 (0000000 en el tercer octeto y 00000001 en el cuarto octeto) y el ultimo host es el 172.16.255.254 (11111111 en el tercer octeto y 11111110 en el cuarto octeto). Recuerde que la dirección 172.16.0.0 nos sirve para identificar la red y la 172.16.255.255 es el brocadast. Por lo tanto la fórmula para obtener el numero de host es 2 a la N menos 2, (2 a la N porque es sistema binario) donde N es el numero de bits que se pueden asignar a los host dependiendo la clase de dirección y se restan 2 una que corresponde al identificador de red y una al broadcast.

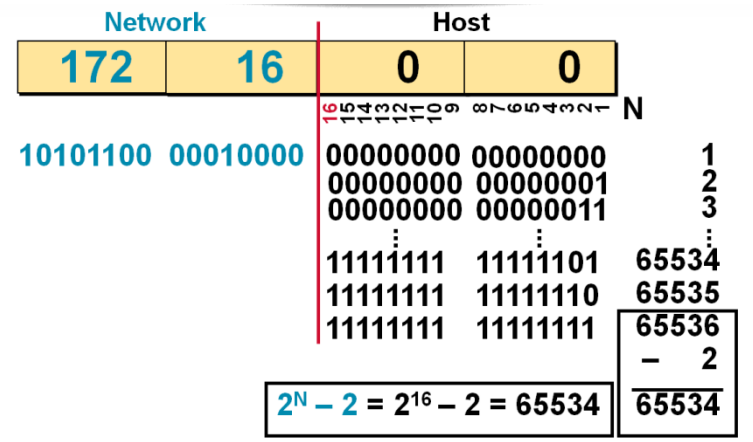

Figura 3.5 Determinar numero de host validos

3.4 Mascara de Red

La máscara de red es una combinación de bits que sirve para delimitar el ámbito de una red de computadoras. Su función es indicar a los dispositivos qué parte de la dirección IP es el número de la red, incluyendo la subred, y qué parte es la correspondiente al host.

Básicamente, mediante la máscara de red una computadora (principalmente la puerta de enlace, router...) podrá saber si debe enviar los datos dentro o fuera de la red. Por ejemplo, si el router tiene la ip 192.168.1.1 y máscara de red 255.255.255.0, entiende que todo lo que se envía a una IP que empiece por 192.168.1 va para la red local y todo lo que va a otras ips, para fuera (internet, otra red local mayor...).

Supongamos que tenemos un rango de direcciones IP desde 10.0.0.0 hasta 10.255.255.255. Si todas ellas formaran parte de la misma red, su máscara de red sería: 255.0.0.0. También se puede escribir como 10.0.0.0/8

Como la máscara consiste en una seguidilla de unos consecutivos, y luego ceros (si los hay), los números permitidos para representar la secuencia son los siguientes: 0, 128, 192, 224, 240, 248, 252, 254, y 255 (**véase figura 3.6**).

La representación utilizada se define colocando en 1 todos los bits de red (máscara natural) y en el caso de subredes, se coloca en 1 los bits de red y los bits de host usados por las subredes. Así, en esta forma de representación (10.0.0.0/8) el 8 sería la cantidad de bits puestos a 1 que contiene la máscara en binario, comenzando desde la izquierda. Para el ejemplo dado (/8), sería 11111111.00000000.00000000.00000000 y en su representación en decimal sería 255.0.0.0.

Una máscara de red representada en binario son 4 octetos de bits (11111111.11111111.11111111.11111111).

De esta manera de acuerdo a cada clase de direccionamiento se tiene la máscara de red:

Para clase A

8bits x 1 octetos = 8 bits. (11111111.00000000.00000000.00000000) = 255.0.0.0

Para clase B

8bits x 2 octetos = 16 bits. (11111111.11111111.00000000.00000000) = 255.255.0.0

Para clase C

8bits x 3 octetos = 24 bits. (11111111.11111111.11111111.00000000) = 255.255.255.0

Las máscaras, se utilizan como validación de direcciones realizando una operación AND lógica entre la dirección IP y la máscara para validar al equipo cosa que permite realizar una verificación de la dirección de la Red.

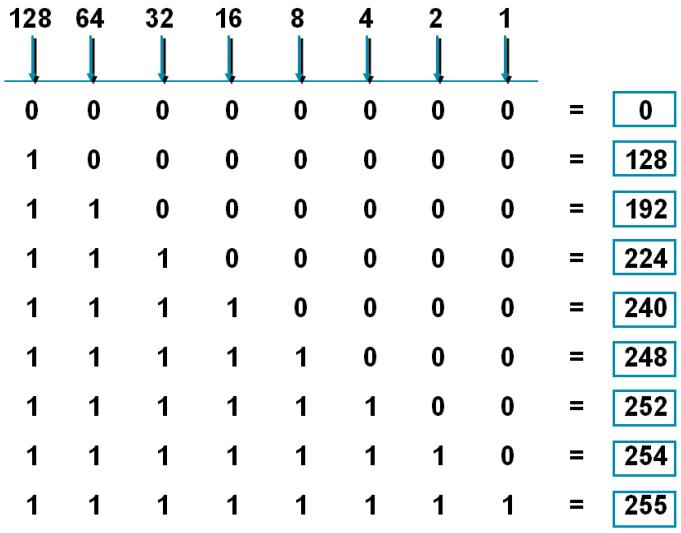

Figura 3.6 Equivalentes decimales para mascara de red

3.5 Subredes

En redes de computadoras, una subred es un rango de direcciones lógicas. Cuando una red de computadoras se vuelve muy grande, conviene dividirla en subredes, por los siguientes motivos:

- Reducir el tamaño de los dominios de broadcast.
- Hacer la red más manejable, administrativamente. Entre otros, se puede controlar el tráfico entre diferentes subredes, mediante ACLs.

Se puede dividir una red en subredes de tamaño fijo (todas las subredes tienen el mismo tamaño). Sin embargo, por la escasez de direcciones IP, hoy en día frecuentemente se usan subredes de tamaño variable.

Las subredes simplifican el enrutamiento, ya que cada subred típicamente es representada como una fila en las tablas de ruteo en cada router conectado. Las subredes fueron utilizadas antes de la introducción de las direcciones IPv4, para permitir a una red grande, tener un número importante de redes más pequeñas dentro, controladas por varios routers. Para que las computadoras puedan comunicarse con una red, es necesario contar con números IP propios, pero si tenemos dos o más redes, es fácil dividir una dirección IP entre todos los hosts de la red. De esta forma se pueden partir redes grandes en redes más pequeñas.

Los routers constituyen los límites entre las subredes. La comunicación desde y hasta otras subredes es hecha mediante un puerto específico de un router específico, por lo menos momentáneamente.

Dentro de cada subred - como también en la red original, sin subdivisión - no se puede asignar la primera y la última dirección a ningún host. La primera dirección de la subred se utiliza como dirección de la subred, mientras que la última está reservada para broadcast locales (dentro de la subred).

Además, en algunas partes se puede leer que no se puede utilizar la primera y la última subred. Es posible que éstos causen problemas de compatibilidad en algunos equipos, pero en general, por la escasez de direcciones IP, hay una tendencia creciente de usar todas las subredes posibles.

En la Figura 3.7 se muestra un ejemplo en donde una dirección clase B **no está** dividida en subredes los dos primeros octetos representan a la parte de red y los dos últimos a la de host. En este caso aunque la lógica indica la existencia de dos redes la tabla de ruteo encuentra dos rutas por donde llegar a la red 172.16.0.0 porque no hay nada que le indique que esta red está dividida en subredes.

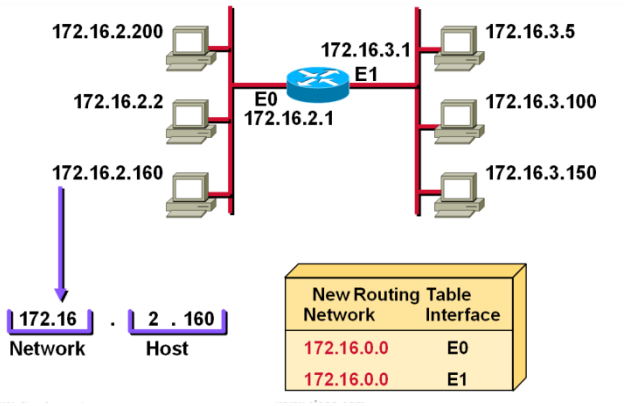

Figura 3.7 Direccionamiento sin subred

En la Figura 3.8 se muestra un ejemplo en donde una dirección clase B está dividida en subredes (o segmentos) los dos primeros octetos representan a la parte de red el tercer octeto a la subred (o segmento) tomando 8 bits de los correspondientes al host y el último octeto representa el host. En este caso la tabla de ruteo ya reconoce que la red está dividida en subredes y sabe que para llegar a la subred 172.16.2.0 debe dirigirse por el puerto E0 y para la subred 172.16.3.0 debe dirigirse por el puerto E1.

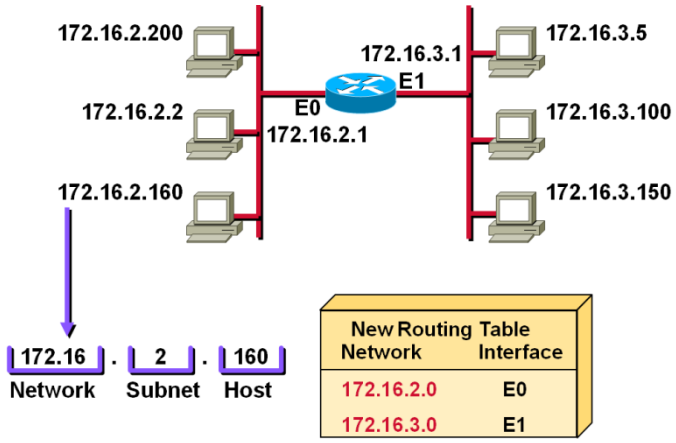

Figura 3.8 Direccionamiento con subred

3.6 Mascara de subred

Cada nodo de una red IP tiene asociado a su dirección una máscara de subred. La máscara de subred identifica qué bits (o qué porción) de su dirección es el identificador de la red. La máscara consiste en una secuencia de unos seguidos de una secuencia de ceros escrita de la misma manera que una dirección IP, por ejemplo, una máscara de 20 bits se escribiría 255.255.240.0, es decir una dirección IP con 20 bits en uno seguidos por 12 bits en 0, pero separada en bloques de a 8 bits escritos en decimal. La máscara determina todos los parámetros de una subred: dirección de red, dirección de difusión (broadcast) y direcciones asignables a nodos de red (hosts).

La representación utilizada se define colocando en 1 todos los bits de red (máscara natural) y en el caso de subredes, se coloca en 1 los bits de red y los bits de host usados por las subredes. (**véase figura 3.9**)

Como se vio en el tema 3.5, la máscara consiste en una seguidilla de unos consecutivos, y luego ceros (si los hay), los números permitidos para representar la secuencia son los siguientes: 0, 128, 192, 224, 240, 248, 252, 254, y 255. (**véase figura 3.9**),

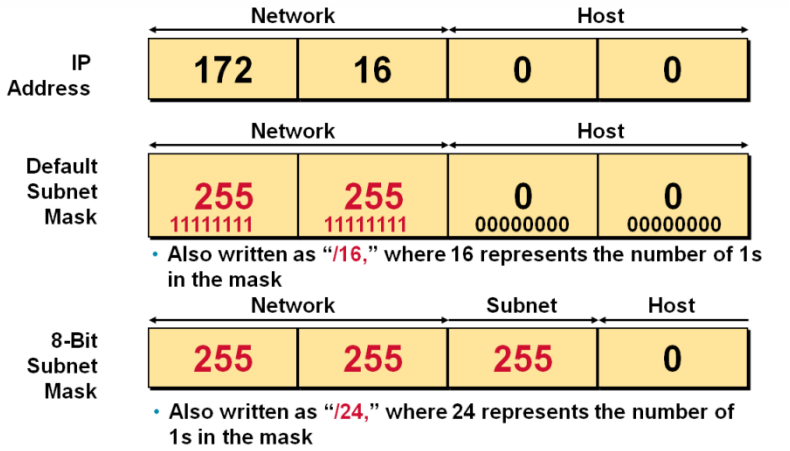

Figura 3.9 Mascara de subred

3.7 Calculo de subredes

Cuando se nos presenta la situación en donde se desea saber a qué red pertenece una dirección IP, se debe recurrir al cálculo de identificador de red.

Un ejemplo de esto se muestra en la figura 3.10.En este ejemplo se muestra el cálculo para obtener el numero o identificador de red a partir de un numero de Mascara de red y una dirección IP mediante una operación AND. En la figura 3.10 se observa que para obtener el identificador de la red se convierte el numero que corresponde a la dirección de clase B (172.16.0.0) en binario así como la máscara correspondiente a esta clase (255.255.0.0), se realiza la operación AND entre los dos numero en binario para obtener el identificador de red como se puede observar en la figura 3.10. En este caso la red no está dividida en subredes.

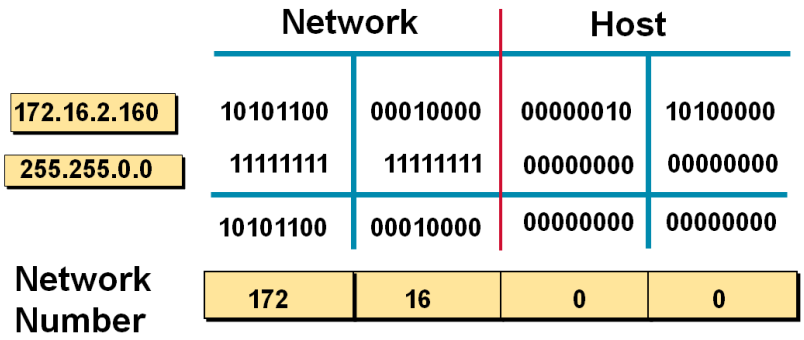

Figura 3.10 Cálculo de identificador de red. Red sin subredes

En el caso de tener una máscara ampliada se realiza el mismo cálculo con la operación AND para conocer a que subred (segmento) pertenece esa dirección IP, como se muestra en la figura 3.11, donde la máscara es ampliada 8 bits mas. En este caso se obtiene un identificador de red con subred o segmento.

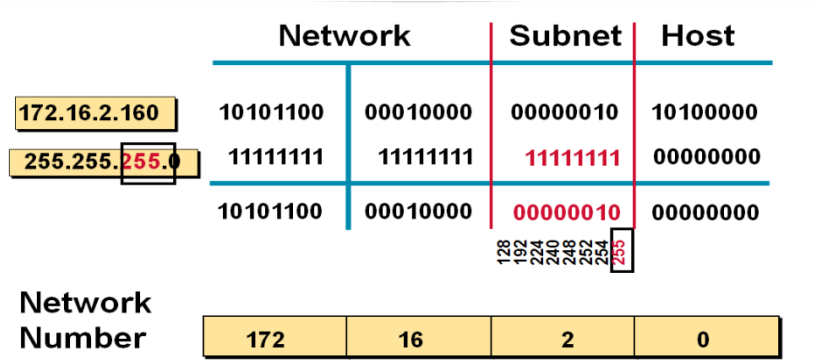

Figura 3.11 Cálculo de Identificador de subred

En el ejemplo de la figura 3.12 tenemos una subred (o segmento) dividida en subredes para saber cual es el identificador de subred se realiza el mismo cálculo de los ejemplos 3.10 y 3.11.

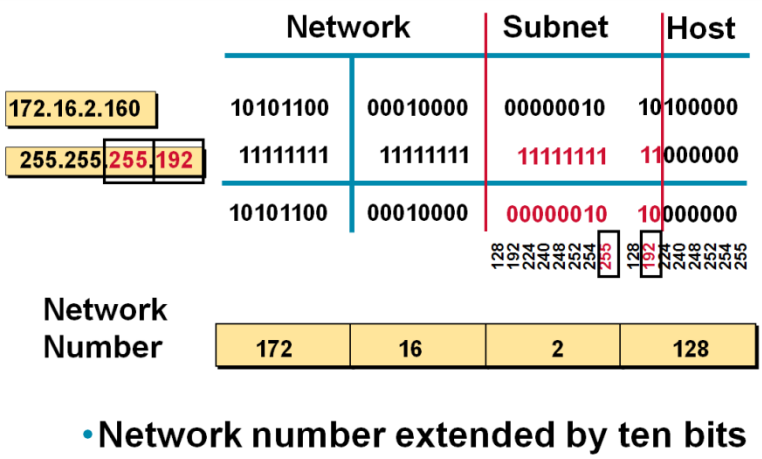

Figura 3.12 Cálculo de Identificador de Subred dividida en Subredes

En los ejemplos anteriores vimos como se puede obtener el identificador de red a partir de una dirección IP y una máscara de red, ahora, a partir de este Identificador de red o subred se puede conocer la dirección de Broadcast, la dirección del primer Host, y la dirección del último host y el numero de Hosts que se pueden asignar a una red.

De acuerdo al ejemplo de la figura 3.13, lo que se debe hacer para obtener estas direcciones es:

Paso número 1 y 2 (identificados en la figura encerrados con un círculo negro). Convertir a binario los datos que tenemos (la dirección IP y la máscara proporcionada).

Paso numero 3. Identificar de acuerdo a la tabla de la Figura 3.6 el número de bits que se toman prestados a la parte de Host para la máscara de subred.

Paso numero 4. Realizar la operación AND entre estas dos direcciones en binario para conocer el identificador de subred.

Paso numero 5. Para conocer la dirección de broadcast se ponen a unos los bits de host descartando los que fueron tomados para la máscara de subred. En la figura numero 3.13 se indica con una línea roja a partir de que bit comienzan los bits de host (2do. Bit del cuarto octeto).

Paso numero 6. Los mismos bits que se pusieron en unos en el paso 5 para conocer el broadcast, ahora se ponen en ceros excepto el último bit que se pone a uno para conocer el primer host a asignar en la red.

Paso numero 7. Se manejan el mismo número de bits que en el paso 5 y 6 para ponerlos ahora todos en unos excepto el ultimo bit que se pone en cero para conocer el ultimo host que se puede asignar en la red.

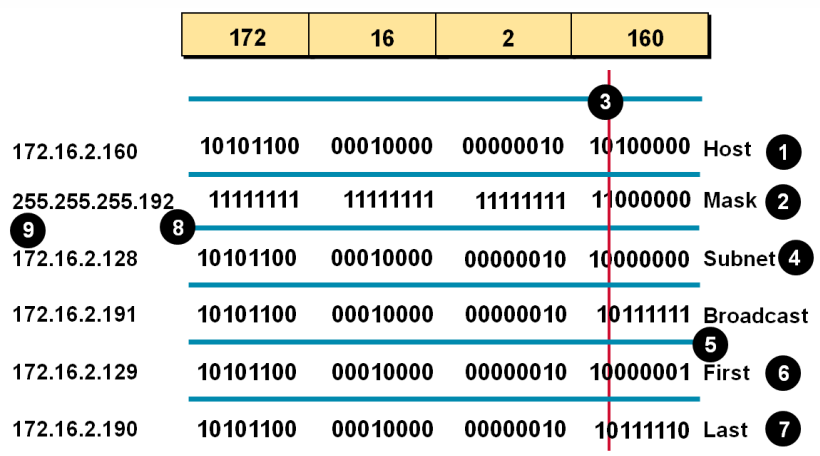

Figura 3.13 Cálculo de Identificador de red, dirección de broadcast, primer y último host

Paso 8 y 9. Se convierten todas las direcciones obtenidas a sistema decimal para obtener las direcciones validas de Identificador de subred, broadcast y primera y última dirección para asignar a los hosts en la red.

Nota: No olvidar que en el octeto (el ultimo en este ejemplo) donde se toman bits prestados para la máscara de subred, para la conversión a decimal deben tomarse en cuenta.

Para saber el número de host de la red se debe realizar el cálculo de **2^N-2** (recuerde que dos direcciones están reservadas una para identificador de red y otra para broadcast), en el ejemplo de la figura 3.13 se puede realizar **2^6-2=61** (2^6 porque seis son los bits que restan de tomar 2 prestados para la máscara de subred).

Capitulo 4. RUTEO

4.1 Conceptos básicos sobre enrutamiento

4.1.1 Determinación de ruta

Para el tráfico que atraviesa una nube de red, la determinación de ruta se produce en la capa de red (Capa 3). La función de determinación de ruta permite al router evaluar las rutas disponibles hacia un destino y establecer el mejor manejo de un paquete. Los servicios de enrutamiento utilizan la información de topología de red al evaluar las rutas de red (**véase figura 4.1**). Esta información la puede configurar el administrador de red o se puede recopilar a través de procesos dinámicos ejecutados en la red.

La capa de red proporciona entrega de paquetes de máximo esfuerzo y de extremo a extremo a través de redes interconectadas.

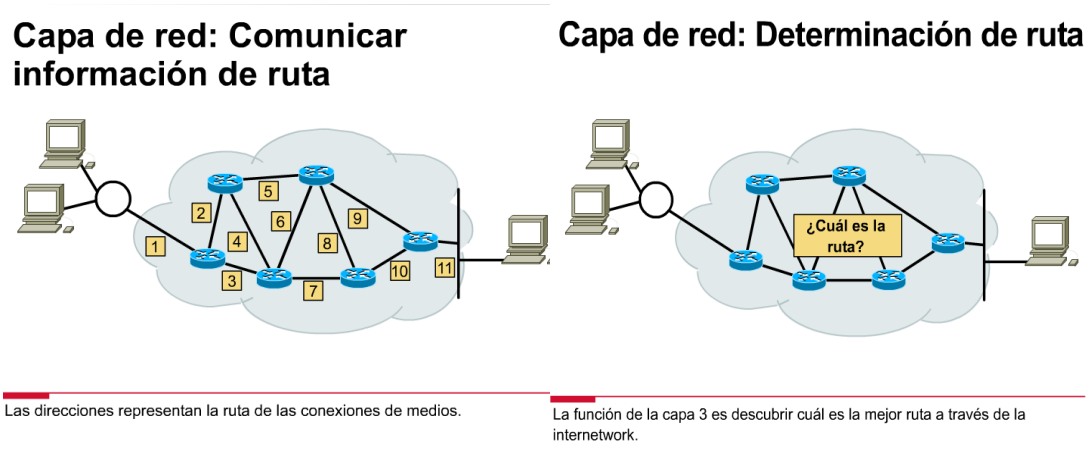

Fig. 4.1Capa de Red Determinación de ruta.

4.1.2. Enrutamiento de paquetes del origen al destino por parte de los routers

Para ser realmente práctica, una red debe representar de manera coherente las rutas disponibles entre los routers. Como vemos en la figura 4.1, cada línea que se encuentra entre los routers posee un número que los routers utilizan como dirección de red. Estas direcciones deben proporcionar información que un proceso de enrutamiento puede utilizar para transportar paquetes desde un origen hacia un destino. Mediante estas direcciones, la capa de red puede proporcionar una conexión de transmisión que interconecta redes independientes.

La coherencia de las direcciones de Capa 3 en toda la internetwork también mejora el uso del ancho de banda evitando los broadcasts innecesarios. Los broadcasts representan un gasto de proceso innecesario y un desperdicio de capacidad en cualquier dispositivo o enlace que no necesite recibir broadcasts. Al utilizar un direccionamiento de extremo a extremo coherente para representar la ruta de las conexiones de medios, la capa de red puede encontrar una ruta hacia el destino sin sobrecargar innecesariamente con broadcasts los dispositivos o enlaces en la internetwork.

4.1.3 Protocolo enrutado versus protocolo de enrutamiento

Debido a la similitud entre los dos términos, se produce a menudo confusión entre protocolo *enrutado* y protocolo *de enrutamiento*.

Protocolo *enrutado* es cualquier protocolo de red que proporcione suficiente información en su dirección de capa de red para permitir que un paquete se envíe desde un host a otro tomando como base el esquema de direccionamiento. Los protocolos enrutados definen los formatos de campo dentro de un paquete. Los paquetes generalmente se transfieren de un sistema final a otro. El Protocolo Internet (IP) es un ejemplo de protocolo enrutado.

Los protocolos de *enrutamiento* soportan un protocolo enrutado proporcionando mecanismos para compartir la información de enrutamiento (**véase figura 4.2**). Los mensajes de protocolo de enrutamiento se desplazan entre los routers. Un protocolo de enrutamiento permite que los routers se comuniquen con otros routers para actualizar y mantener las tablas. Los siguientes son ejemplos de protocolos de enrutamiento TCP/IP:

- RIP (Routing Information Protocol o Protocolo de información de enrutamiento)
- IGRP (Interior Gateway Routing Protocol o Protocolo de enrutamiento de gateway interior)
- EIGRP (Enhanced Interior Gateway Routing Protocol o Protocolo de enrutamiento de gateway interior mejorado)

- OSPF (Open Shortest Path First o Primero la ruta libre más corta)

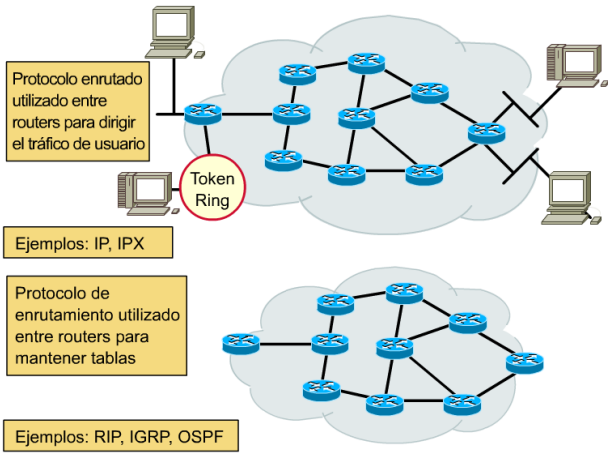

Figura 4.2 Protocolo enrutado & protocolo de enrutamiento

4.1.4 Operaciones de protocolo de capa de red

Cuando una aplicación del host necesita enviar un paquete a un destino en una red distinta, el host direcciona la trama de enlace de datos hacia el router, utilizando la dirección de una de las interfaces del router (**véase figura 4.3**). El proceso de la capa de red del router examina el encabezado del paquete de entrada para determinar la red destino y luego consulta la tabla de enrutamiento que asocia las redes con las interfaces de salida. El paquete se encapsula nuevamente en la trama de enlace de datos apropiada para la interfaz seleccionada y se ubica en la cola para su entrega al siguiente salto en la ruta.

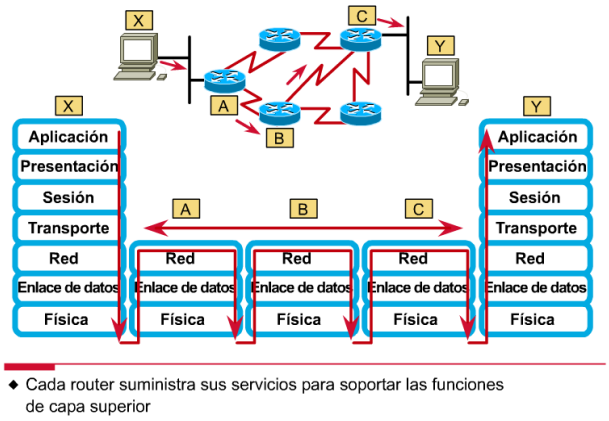

Figura 4.3 Opciones de protocolo de red

Este proceso tiene lugar cada vez que el paquete se envía a través de otro router. En el router que se encuentra conectado a la red del host destino, el paquete se encapsula en el tipo de trama de enlace de datos de la LAN destino y se entrega al host destino. Los routers pueden soportar varios protocolos de enrutamiento independientes y mantener tablas de enrutamiento para varios protocolos enrutados(**véase figura 4.4**). Esta capacidad le permite al router entregar paquetes desde varios protocolos enrutados a través de los mismos enlaces de datos.

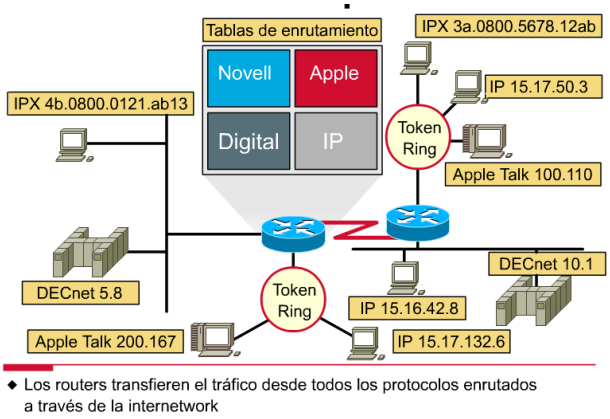

Figura 4.4 Enrutamiento multiprotocolo

4.2 Rutas estáticas versus rutas dinámicas

El conocimiento de las rutas estáticas es gestionado manualmente por el administrador de red, que lo introduce en la configuración de un router. El administrador debe actualizar manualmente esta entrada de ruta estática siempre que un cambio en la topología de la internetwork requiera una actualización.

El conocimiento de las rutas dinámicas funciona de manera diferente. Después de que un administrador de red introduce comandos de configuración para empezar el enrutamiento dinámico, el conocimiento de la ruta se actualiza automáticamente a través de un proceso de enrutamiento siempre que se reciba nueva información de la internetwork. Los cambios en el conocimiento dinámico se intercambian entre routers como parte del proceso de actualización (**véase figura 4.5**).

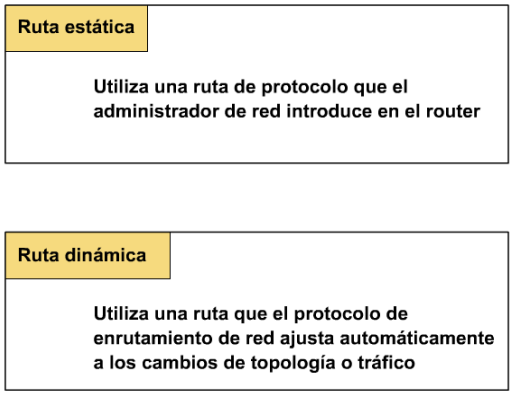

Figura 4.5 Rutas estáticas & rutas dinámicas

4.2.1 Por qué usar una ruta estática

El enrutamiento estático posee varias aplicaciones útiles. Mientras que el enrutamiento dinámico tiende a revelar todo lo que se conoce acerca de la internetwork, es posible que por razones de seguridad se desee ocultar parte de una internetwork. El enrutamiento estático le permite especificar la información que desea revelar acerca de redes restringidas.

Cuando se puede acceder a una red a través de un solo camino, una ruta estática hacia la red puede ser suficiente. Este tipo de red se denomina red de conexión única. La configuración del enrutamiento estático para una red de conexión única (stub) evita el gasto que implica el enrutamiento dinámico.

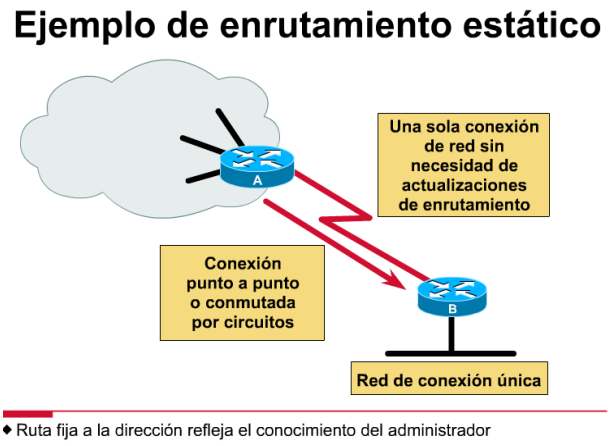

Figura 4.6 Ejemplo de enrutamiento estático

4.2.2 Uso de una ruta por defecto

La figura muestra el uso de una ruta por defecto: una entrada en la tabla de enrutamiento que dirige los paquetes hacia el salto siguiente, cuando este salto no se encuentra explícitamente determinado en la tabla de enrutamiento. Se pueden establecer rutas por defecto como parte de la configuración estática.

En este ejemplo, los routers de la empresa X poseen un conocimiento específico de la topología de la red de la empresa X, pero no de las demás redes. Mantener el conocimiento de cada una de las demás redes accesibles a través de la nube de Internet es totalmente innecesario y poco razonable, si no imposible. En lugar de mantener un conocimiento específico de cada red, se informa a cada router de la empresa X la ruta por defecto que puede utilizar para llegar a cualquier destino desconocido direccionando el paquete hacia Internet (**véase figura 4.7**).

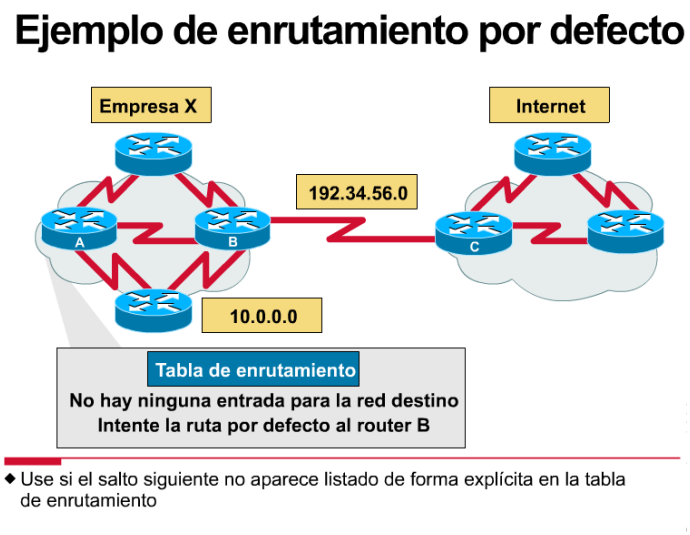

Figura 4.7 Ejemplo de enrutamiento por defecto

4.2.3 Por qué es necesario el enrutamiento dinámico

La red que aparece en la figura se adapta de forma diferente a los cambios de topología, según si usa la información de enrutamiento configurada de forma estática o dinámica.

El enrutamiento estático permite que los routers enruten correctamente un paquete desde una red a otra tomando como base la información configurada. El router consulta su tabla de enrutamiento y utiliza el conocimiento estático que reside allí para transferir el paquete hacia el Router D. El Router D hace lo mismo y transfiere el paquete al Router C. El Router C entrega el paquete al host destino.

Si la ruta entre el Router A y el Router D falla, el Router A no podrá transferir el paquete al Router D utilizando esa ruta estática. Hasta que el Router A se reconfigure manualmente para enviar paquetes a través del Router B, la comunicación con la red destino es imposible.

El enrutamiento dinámico ofrece más flexibilidad. Según la tabla de enrutamiento generada por el Router A, un paquete puede llegar a destino por la ruta preferida a través del Router D. Sin embargo, una segunda ruta hacia el destino está disponible a través del Router B. Cuando el Router A reconoce que el enlace al Router D está caído, ajusta su propia tabla de enrutamiento, haciendo que la ruta a través del Router B se convierta en la ruta preferida hacia el destino. Los routers siguen enviando paquetes a través de este enlace.

Cuando se restaura la ruta entre los Routers A y D, el Router A puede nuevamente cambiar su tabla de enrutamiento para indicar una preferencia por la ruta orientada en dirección contraria a la de las agujas del reloj a través de los Routers D y C hacia la red destino. Los protocolos de enrutamiento dinámico también pueden dirigir el tráfico de una misma sesión a través de distintas rutas de una red para lograr un mejor rendimiento. Esto se conoce como carga compartida.

4.2.4 Operaciones de enrutamiento dinámico

El éxito del enrutamiento dinámico depende de dos funciones básicas del router:

- el mantenimiento de una tabla de enrutamiento
- la distribución oportuna del conocimiento, bajo la forma de actualizaciones de enrutamiento, hacia otros routers

El enrutamiento dinámico se basa en un protocolo de enrutamiento para compartir el conocimiento entre los routers (**véase figura 4.8**). Un protocolo de enrutamiento define el conjunto de reglas utilizadas por un router cuando se comunica con los routers vecinos. Por ejemplo, un protocolo de enrutamiento describe:

- cómo enviar actualizaciones
- qué conocimiento contienen esas actualizaciones
- cuándo enviar ese conocimiento
- cómo ubicar a los destinatarios de las actualizaciones

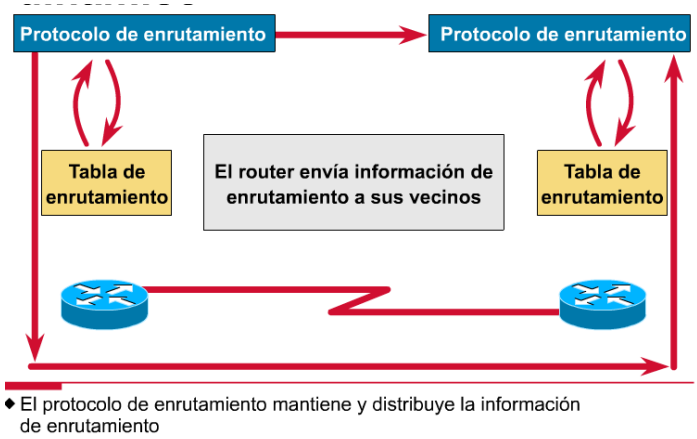

Figura 4.8 Operaciones de enrutamiento dinámico

4.2.5 Determinación de las distancias de las rutas en la red a través de diversas métricas

Cuando un algoritmo de enrutamiento actualiza una tabla de enrutamiento, su objetivo principal es determinar cuál es la mejor información que debe incluir en la tabla. Cada algoritmo de enrutamiento interpreta lo que es mejor a su manera. El algoritmo genera un número, denominado métrica, (**véase figura 4.9**) para cada ruta a través de la red. Normalmente, cuanto menor sea la métrica, mejor será la ruta.

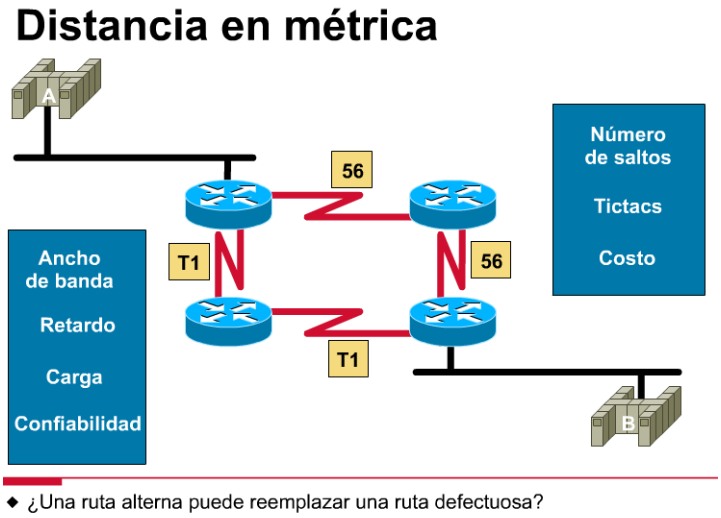

Figura 4.9 Distancia en métrica

Se pueden calcular las métricas tomando como base una sola característica de la ruta. Se pueden calcular métricas más complejas combinando varias características. Las métricas utilizadas con mayor frecuencia por los routers son las siguientes:

- *ancho de banda*: capacidad de transmisión de datos de un enlace; (normalmente, se prefiere un enlace Ethernet de 10 Mbps a una línea arrendada de 64 kbps)
- *retardo*: cantidad de tiempo requerido para transportar un paquete por cada enlace desde el origen hacia el destino
- *carga*: cantidad de actividad en un recurso de red tal como un router o un enlace
- *confiabilidad*: generalmente se refiere al índice de error de cada enlace de red
- *número de saltos*: cantidad de routers que un paquete debe atravesar antes de llegar a su destino
- *tictacs*: retardo en un enlace de datos en unidades de tictacs del reloj de los PC IBM (aproximadamente 55 milisegundos).
- *costo*: valor arbitrario, generalmente basado en el ancho de banda, el gasto monetario u otras mediciones, asignado por un administrador de red

4.3 Clases de protocolos de enrutamiento

La mayoría de los algoritmos de enrutamiento se pueden clasificar como uno de dos algoritmos básicos:

- vector-distancia, o
- estado-enlace.

El enrutamiento por vector-distancia determina la dirección (vector) y la distancia hacia cualquier enlace en la internetwork. El enrutamiento estado-enlace (también denominado *primero la ruta libre más corta*) recrea la topología exacta de toda la internetwork (o por lo menos la porción en la que se ubica el router).

El enrutamiento híbrido balanceado combina aspectos de los algoritmos de estado-enlace y vector-distancia (**véase figura 4.10**). En las páginas siguientes se hará referencia a los procedimientos y problemas para cada uno de estos algoritmos de enrutamiento y se presentan técnicas para reducir al mínimo los problemas.

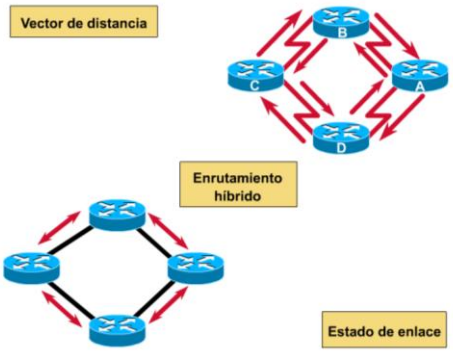

Figura 4.10 Clases de protocolos de enrutamiento

4.3.1 Tiempo de convergencia

El algoritmo de enrutamiento es fundamental para el enrutamiento dinámico. Siempre que la topología de una red cambia por razones de crecimiento, reconfiguración o falla, la base del conocimiento de la red también debe cambiar. El conocimiento debe reflejar una visión exacta y coherente de la nueva topología. Esta visión se denomina *convergencia* (**véase figura 4.11**).

Cuando todos los routers de una internetwork se encuentran operando con el mismo conocimiento, se dice que la internetwork ha *convergido*. La convergencia rápida es una función de red deseable, ya que reduce el período de tiempo durante el cual los routers continúan tomando decisiones de enrutamiento incorrectas o que causan desperdicio.

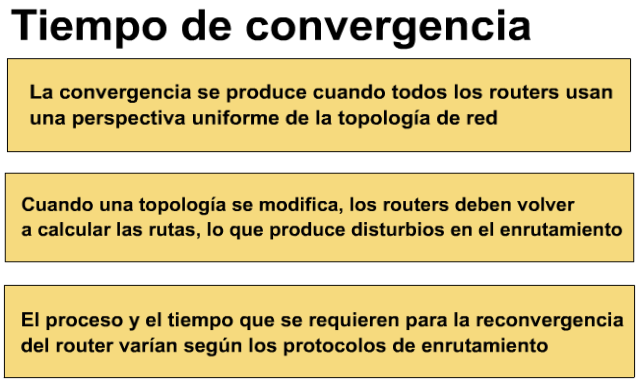

Figura 4.11 Tiempo de convergencia

4.4 Enrutamiento vector-distancia

4.4.1 Principios básicos del enrutamiento vector-distancia

Los algoritmos de enrutamiento basados en vector-distancia envían copias periódicas de una tabla de enrutamiento de un router a otro. Estas actualizaciones regulares entre routers comunican los cambios de topología.

Cada router recibe una tabla de enrutamiento de los routers vecinos directamente conectados. Por ejemplo, en el gráfico, el Router B recibe información del Router A. El Router B agrega un número de vector-distancia (como, por ejemplo, el número de saltos), aumentando de esta manera el vector-distancia y luego transfiere esta nueva tabla de enrutamiento a su otro vecino, el Router C. Este mismo proceso paso a paso se produce en todas las direcciones entre los routers directamente vecinos (**véase figura 4.12**).

El algoritmo eventualmente acumula distancias de red para poder mantener una base de datos de información de topología de la red. Los algoritmos vector-distancia no permiten, sin embargo, que un router conozca la topología exacta de una internetwork.

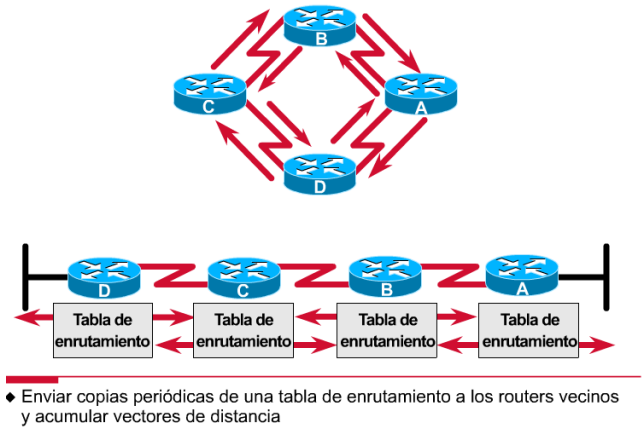

Figura 4.12 Conceptos del vector de distancia

4.4.2 Intercambio de tablas de enrutamiento por parte de los protocolos vector-distancia

Como se ve en la figura 4.12 cada router que utiliza el enrutamiento vector-distancia empieza identificando sus propios vecinos. En la figura, la interfaz que lleva a cada red directamente conectada tiene una distancia de 0. A medida que el proceso de descubrimiento de red vector-distancia continúa, los routers descubren la mejor ruta hacia las redes destino basándose en la información que reciben de

cada vecino. Por ejemplo, el Router A obtiene conocimiento acerca de otras redes tomando como base la información que recibe del Router B. Cada una de las demás entradas de red en la tabla de enrutamiento posee un vector-distancia acumulado para demostrar la distancia a la que se encuentra esta red en una dirección determinada.

4.4.3 El problema de los loops de enrutamiento

Los loops de enrutamiento se pueden producir si la convergencia lenta de una red en una nueva configuración hace que las entradas de enrutamiento sean incorrectas (**véase figura 4.13**). La figura ilustra cómo se puede producir un loop de enrutamiento:

1. Antes de la falla de la Red 1, todos los routers poseen un conocimiento coherente y tablas de enrutamiento correctas. Se dice que la red ha convergido. Supongamos, para el resto de este ejemplo, que la ruta preferida del Router C hacia la Red 1 es a través del Router B y que la distancia del Router C a la Red 1 es 3
2. En el momento en que la Red 1 falla, el Router E envía una actualización al Router A. El Router A deja de enrutar paquetes hacia la Red 1, pero los Routers B, C y D siguen operando porque todavía no se les ha informado acerca de la falla. Cuando el Router A envía su actualización, los Routers B y D detienen el enrutamiento hacia la Red 1; sin embargo, el Router C no ha recibido la actualización. Para el Router C, la Red 1 todavía se puede alcanzar a través del Router B.
3. Ahora, el Router C envía una actualización periódica al Router D, indicando una ruta hacia la Red 1 a través del Router B. El Router D cambia su tabla de enrutamiento para introducir esta información buena pero incorrecta y transmite la información al Router A. El Router A transmite la información a los Routers B y E, etc. Cualquier paquete destinado a la Red 1 ahora realizará un loop desde el Router C al B al A al D y volverá nuevamente al C.

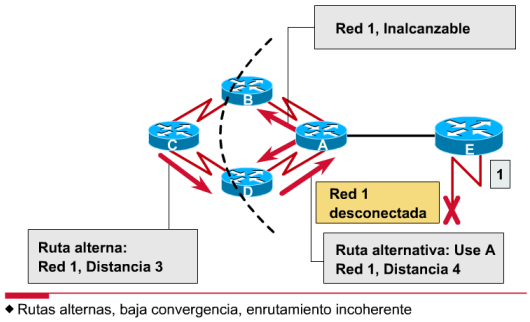

Figura 4.13 Problema: Loops de enrutamiento

4.4.4 El problema de la cuenta al infinito

Continuando con el ejemplo de la página anterior, las actualizaciones no válidas de la Red 1 seguirán andando en círculos hasta que algún otro proceso detenga el recorrido del loop. Esta condición, denominada *conteo al infinito*, hace que los paquetes recorran la red continuamente, a pesar del hecho fundamental de que la red destino, la Red 1, está caída (**véase figura 4.14**). Mientras los routers cuentan al infinito, la información no válida permite que se produzca un loop de enrutamiento.

Si no se toman medidas para detener el proceso, el vector-distancia (métrica) de número de saltos se incrementa cada vez que el paquete atraviesa otro router. Estos paquetes recorren la red formando loops (bucles) debido a la información incorrecta de las tablas de enrutamiento.

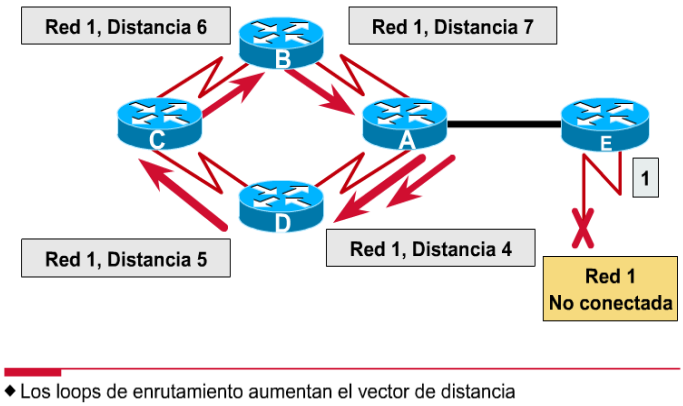

Figura 4.14 Problema: Cuenta al infinito

4.4.5 Definición de un máximo

Los algoritmos de enrutamiento vector-distancia se corrigen automáticamente, pero un problema de loop de enrutamiento puede requerir primero una cuenta al infinito. Para evitar que este problema se prolongue, los protocolos vector-distancia definen el infinito como un número máximo específico (**véase figura 4.15**). Este número se refiere a la *métrica de enrutamiento* (por ej., un número de saltos simple).

Con este enfoque, el protocolo de enrutamiento permite que el loop de enrutamiento continúe hasta que la métrica supere su máximo valor permitido. El gráfico muestra el valor de la métrica como 16 saltos, lo que supera el máximo vector-distancia por defecto de 15 saltos, por lo tanto, el router descarta el paquete. En cualquiera de los casos, cuando el valor de la métrica supera el valor máximo, se considera que la Red 1 no se puede alcanzar.

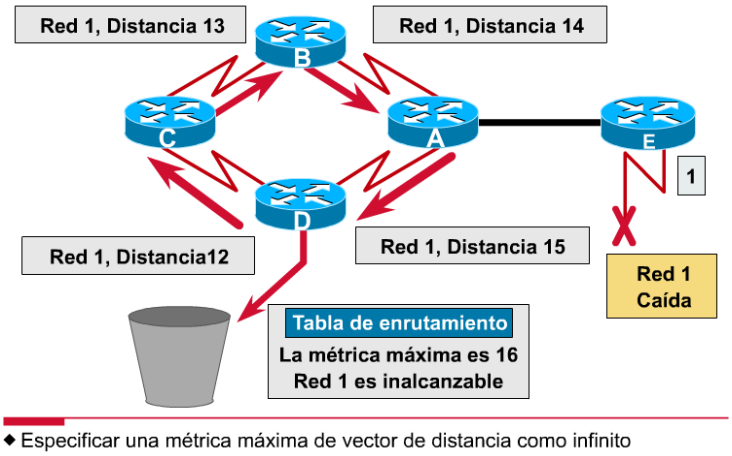

Figura 4.15 Solución: Definición de un máximo

4.4.6 Split horizon (horizonte dividido)

Otro origen posible de un loop de enrutamiento es cuando información incorrecta que se ha enviado a un router se contradice con la información correcta que éste envió. Así es como se produce el problema:

1. El Router A transfiere una actualización al Router B y al Router D, indicando que la Red 1 está fuera de servicio. El Router C, sin embargo, transmite una actualización al Router B, indicando que la Red 1 está disponible a una distancia de 4, a través del Router D. Esto no infringe las reglas del split horizon.
2. El Router B concluye erróneamente que el Router C todavía tiene una ruta válida hacia la Red 1, aunque con una métrica mucho menos favorable. El Router B envía una actualización al Router A comunicándole al Router A la nueva ruta hacia la Red 1.
3. El Router A ahora determina que puede realizar los envíos a la Red 1 a través del Router B, el Router B determina que puede realizar los envíos a la Red 1 a través del Router C, y el Router C determina que puede realizar los envíos a la Red 1 a través del Router D. Cualquier paquete introducido en este entorno quedará atrapado en un loop entre los Reuters.
4. El split horizon intenta evitar esta situación. Como vemos en la figura 4.16, si llega una actualización de enrutamiento acerca de la Red 1 desde Router A, el Router B o D no pueden enviar información acerca de la Red 1 nuevamente hacia el Router A.
5. El split horizon reduce así la cantidad de información de enrutamiento incorrecta y reduce también el gasto de enrutamiento.

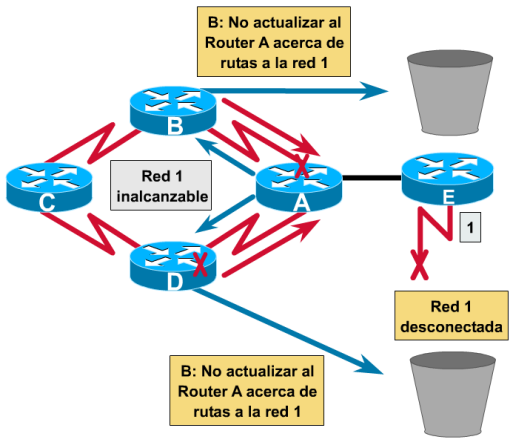

Figura 4.16 Solución: Horizonte dividido

4.5 Temporizadores de espera

Se puede evitar el problema de cuenta al infinito mediante *temporizadores de espera* (**véase figura 4.17**) que funcionan de la siguiente manera:

1. Cuando un router recibe una actualización por parte de un vecino que indica que una red previamente accesible ahora se encuentra inaccesible, el router marca la ruta como inaccesible e inicia un temporizador de espera. Si en algún momento, antes de que expire el temporizador de espera, se recibe una actualización por parte del mismo vecino indicando que la red se encuentra nuevamente accesible, el router marca la red como accesible y elimina el temporizador de espera.
2. Si llega una actualización desde un router vecino distinto con una métrica más conveniente que la originalmente registrada para la red, el router marca la red como accesible y elimina el temporizador de espera.
3. Si en algún momento antes de que expire el temporizador de espera se recibe una actualización de un router vecino diferente con una métrica inferior, se ignorará la actualización. El ignorar una actualización con una métrica inferior mientras el temporizador de espera se encuentra activado, permite ganar más tiempo para que el conocimiento de un cambio perjudicial se propague a través de toda la red.

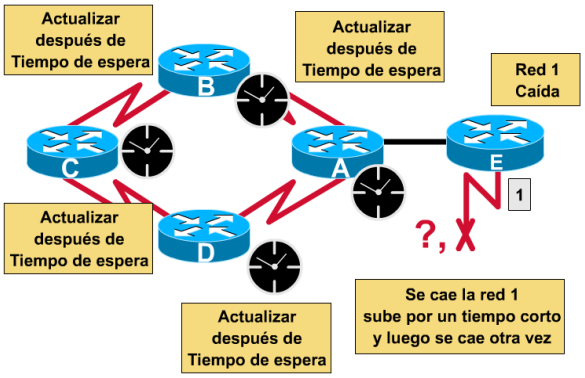

Figura 4.17 Solución: Temporizadores de espera

4.6 Enrutamiento estado de enlace

El segundo algoritmo básico utilizado para el enrutamiento es el algoritmo estado de enlace (**véase figura 4.18**). Los algoritmos de enrutamiento basados en estado de enlace, también conocidos como algoritmos *SPF (primero la ruta libre más corta)*, mantienen una compleja base de datos de información de topología. Mientras que el algoritmo vector-distancia posee información no específica acerca de las redes distantes y ningún conocimiento acerca de los routers distantes, un algoritmo de enrutamiento estado de enlace conoce perfectamente los routers distantes y cómo se interconectan.

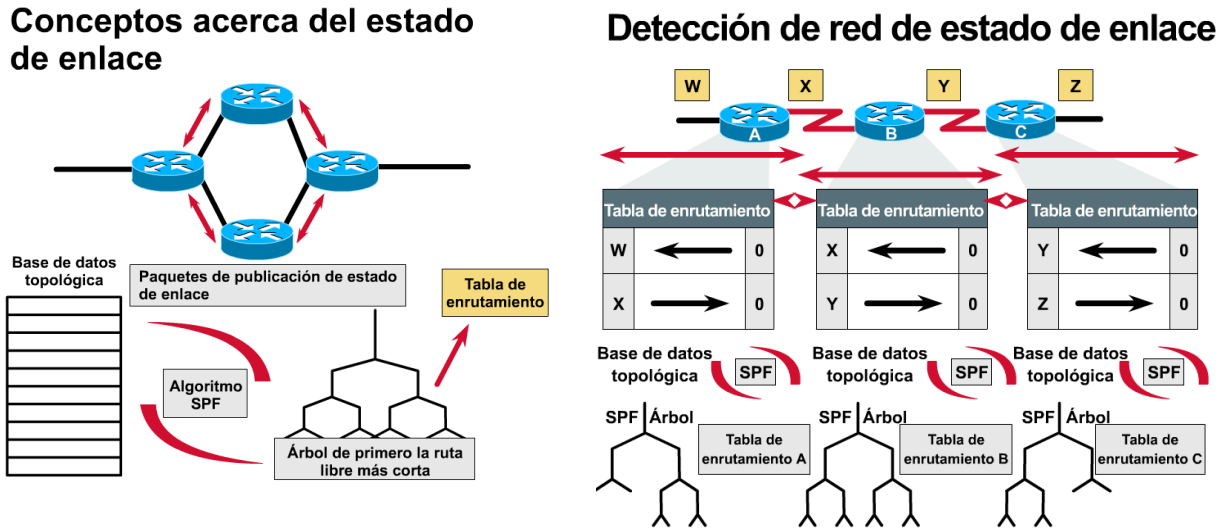

Figura 4.18 Conceptos acerca del estado de enlace

4.6.1 Intercambio de tablas de enrutamiento por parte de los protocolos estado-enlace

El descubrimiento de red para el enrutamiento estado-enlace utiliza los siguientes procesos:

1. Los routers intercambian LSA entre sí. Cada router empieza con redes directamente conectadas para las cuales posee información directa.
2. Cada router en paralelo con los demás routers genera una base de datos topológica que contiene todas las LSA de la internetwork.
3. El algoritmo SPF calcula la accesibilidad de la red. El router construye esta topología lógica como un árbol, con él mismo como raíz, y con todas las rutas posibles hacia cada red dentro de la internetwork que usa el protocolo estado-enlace. Entonces clasifica estas rutas, colocando la ruta más corta primero (SPF).
4. El router hace una lista de sus mejores rutas y de los puertos que permiten acceder a estas redes destino, dentro de la tabla de enrutamiento. También mantiene otras bases de datos con elementos de la topología y detalles de los estados.

4.6.2 Propagación de los cambios de topología a través de la red de routers

Los algoritmos de estado-enlace se basan en el uso de las mismas actualizaciones de estado-enlace. Siempre que una topología estado-enlace cambia, el router que primero se da cuenta del cambio envía la información a los demás routers o a un router designado que todos los demás routers pueden utilizar para realizar las actualizaciones. Esto implica el envío de información de enrutamiento común a todos los routers de la internetwork. Para lograr la convergencia, cada router debe realizar lo siguiente:

- mantener un seguimiento de los routers vecinos: el nombre de cada vecino, si se encuentra conectado o desconectado y el costo del enlace con el router vecino.
- la construcción de un paquete LSA que describa los nombres de los routers vecinos y los costos de enlace, incluyendo los nuevos vecinos, los cambios en los costos de enlace y los enlaces con los vecinos que se han desconectado.
- el envío de este paquete LSA para que todos los demás routers lo reciban
- una vez recibido el paquete LSA, registrar el paquete LSA en la base de datos para que actualice el paquete LSA generado más recientemente por cada router.
- completar un mapa de la internetwork utilizando datos de los paquetes LSA acumulados y luego calcular rutas hacia todas las demás redes utilizando el algoritmo SPF.

Cada vez que un paquete LSA provoca un cambio en la base de datos estado-enlace, el algoritmo de estado-enlace (SPF) vuelve a calcular cuáles son las mejores rutas y actualiza la tabla de enrutamiento. Desde ese momento, cada router toma en cuenta el cambio de topología en el momento de determinar cuál es la ruta más corta para el enrutamiento de paquetes (**véase figura 4.19**).

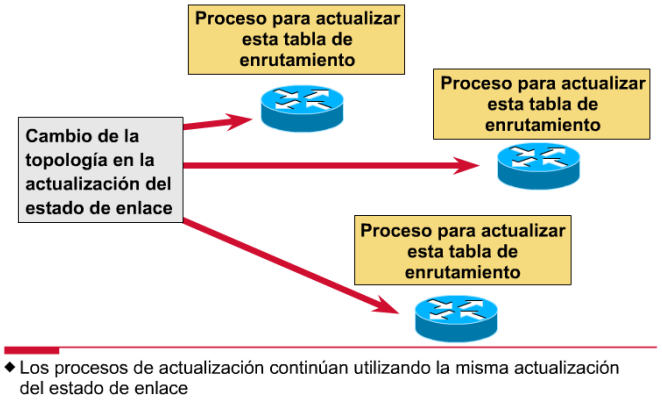

Figura 4.19 Cambios de la topologia del estado de enlace

4.6.3 Requisitos de procesamiento y memoria

En la mayoría de los casos, ejecutar los protocolos de enrutamiento estado-enlace significa que los routers deben utilizar más memoria y realizar más procesamiento que los protocolos de enrutamiento por vector-distancia. Los administradores de red deben garantizar que los routers que seleccionen sean capaces de proporcionar estos recursos necesarios.

Los routers realizan el seguimiento de todos los demás routers dentro de un mismo grupo y de las redes que cada uno puede alcanzar directamente. Para el enrutamiento estado-enlace, la memoria debe tener la capacidad de almacenar la información de varias bases de datos, del árbol de topología y de la tabla de enrutamiento. El uso del *algoritmo de Dijkstra* para calcular la SPF requiere una tarea de procesamiento proporcional a la cantidad de enlaces de la internetwork, multiplicada por la cantidad de routers de la misma.

4.6.4 Requisitos de ancho de banda

Otro punto que puede ser motivo de preocupación es el ancho de banda que se debe utilizar para realizar la técnica de inundación inicial de paquetes de estado-enlace(**véase figura 4.20**). Durante el proceso de descubrimiento inicial, todos los routers que utilicen protocolos de enrutamiento estado-enlace envían paquetes LSA a todos los demás routers. Esta acción inunda la internetwork a medida que los routers demandan ancho de banda en forma masiva y reducen temporalmente el ancho de banda disponible para el tráfico enrutado que transporta los datos del usuario. Después de esta técnica de inundación inicial, los protocolos de

enrutamiento estado-enlace generalmente requieren un ancho de banda mínimo para enviar paquetes LSA no frecuentes o generados por sucesos que reflejen los cambios de topología.

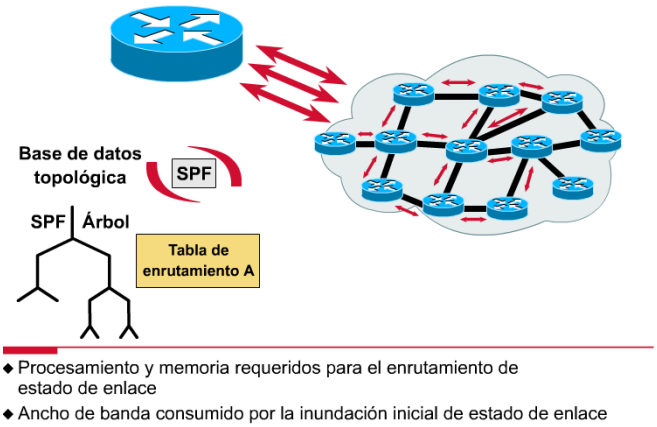

Figura 4.20 Aspectos que preocupan del estado del enlace

4.6.5 Publicaciones de estado-enlace no sincronizadas (LSA) que llevan a decisiones de ruta incoherentes entre los routers

El aspecto más complejo y más importante del enrutamiento estado-enlace es asegurarse de que todos los routers obtengan los paquetes LSA necesarios. Los routers con distintos conjuntos de LSA calculan las rutas tomando como base distintos datos topológicos. Entonces, las redes se vuelven inaccesibles como resultado del desacuerdo entre los routers acerca de un enlace. A continuación, presentamos un ejemplo de información de ruta incoherente(**véase figura 4.21**):

1. Entre los Routers C y D, la Red 1 queda fuera de servicio. Ambos routers construyen un paquete LSA para reflejar este estado de inaccesibilidad.
2. Poco después, la Red 1 se activa nuevamente. Se necesita otro paquete LSA para reflejar este nuevo cambio de topología.
3. Si el mensaje "Red 1, Inaccesible" original del Router C utiliza una ruta lenta para su actualización, dicha actualización llegará tarde. Ese paquete LSA puede llegar al Router A después del paquete LSA con el mensaje "Red 1, Nuevamente activa" del Router D.
4. Con las LSA fuera de sincronía, el Router A debe enfrentarse al dilema de qué árbol SPF debe construir. ¿Debe utilizar rutas que incluyan la Red 1 o rutas sin la Red 1, que recientemente se describió como inaccesible?

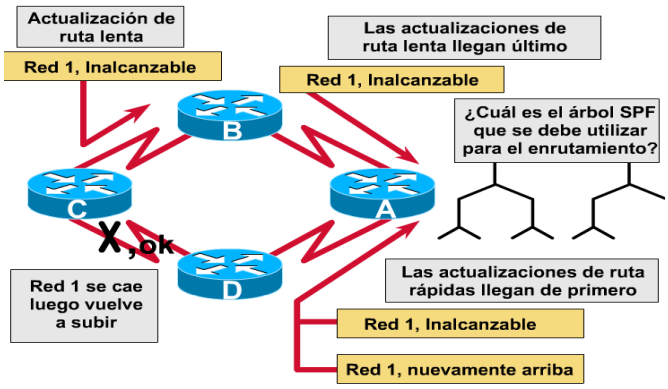

Figura 4.21 Problema: Actualizaciones del estado del enlace

Si la distribución de las LSA a todos los routers no se realiza correctamente, el enrutamiento por estado-enlace puede dar como resultado rutas no válidas. El escalamiento con protocolos estado-enlace en internetworks de gran tamaño puede agravar el problema de distribución incorrecta de paquetes LSA. Si una parte de la red se activa antes que otras partes, el orden para enviar y recibir paquetes LSA varía.

Esta variación puede alterar e impedir la convergencia. Es posible que los routers obtengan distintas versiones de la topología antes de construir sus árboles SPF y tablas de enrutamiento. En una internetwork de gran tamaño, las partes que se actualizan más rápidamente pueden provocar problemas a las partes que se actualizan con más lentitud.

4.7 Comparación de enrutamiento vector-distancia y estado-enlace

Se puede comparar el enrutamiento por vector-distancia con el enrutamiento estado-enlace (**véase figura 4.22**) en varias áreas claves:

- El enrutamiento por vector-distancia obtiene datos topológicos de la información de la tabla de enrutamiento de sus vecinos. El enrutamiento estado-enlace obtiene una amplia visión de la topología de internetwork completa acumulando todas las LSA necesarias.
- El enrutamiento por vector-distancia determina la mejor ruta agregando el valor métrico que recibe a medida que la información de enrutamiento pasa de un router a otro. Para el enrutamiento estado-enlace, cada router trabaja independientemente para calcular su propia ruta más corta hacia las redes destino.

- Con la mayoría de los protocolos de enrutamiento por vector-distancia, las actualizaciones para los cambios de topología consisten en actualizaciones periódicas de las tablas. La información pasa de un router a otro, dando generalmente como resultado una convergencia más lenta. Con los protocolos de enrutamiento estado-enlace, las actualizaciones son provocadas generalmente por cambios en la topología. Las LSA relativamente pequeñas que se han pasado a todos los demás routers generalmente dan como resultado tiempos más rápidos de convergencia con cualquier cambio de topología de la internetwork.

Vector -Distancia	Estado -Enlace
Visualizar la topología de red desde la perspectiva del vecino	Obtiene una visión común de toda la topología de red
Agrega vectores de distancia de router a router	Calcula la ruta más corta hacia los otros routers
Actualizaciones frecuentes, periódicas: Convergencia lenta	Actualizaciones activadas por eventos: Convergencia más rápida
Envía copias de las tablas de enrutamiento hacia los routers vecinos	Envía actualizaciones de enrutamiento de estado de enlace hacia los otros routers

Figura 4.22 Comparación del enrutamiento por vector de distancia y de estado de enlace

4.8 Protocolos de enrutamiento híbrido

Un tercer tipo emergente de protocolo de enrutamiento combina los aspectos del enrutamiento por vector-distancia y de estado de enlace. Este tercer tipo se denomina *enrutamiento híbrido balanceado* (**véase figura 4.23**). Los protocolos de enrutamiento híbrido balanceado utilizan vectores de distancia con métricas más precisas para determinar las mejores rutas hacia las redes destino. Sin embargo, difieren de la mayoría de los protocolos por vector-distancia porque utilizan cambios de topología para provocar actualizaciones en las bases de datos de enrutamiento.

El protocolo de enrutamiento híbrido balanceado converge rápidamente, como los protocolos de estado de enlace. Sin embargo, difiere de los protocolos por vector-distancia y de estado de enlace en el sentido de que utiliza menos recursos de ancho de banda, memoria y ciclos del procesador. Ejemplos de protocolos híbridos son *IS-IS de OSI (Sistema intermedio a Sistema intermedio)* y *el protocolo EIGRP (Protocolo de enrutamiento de gateway interior mejorado) de Cisco*.

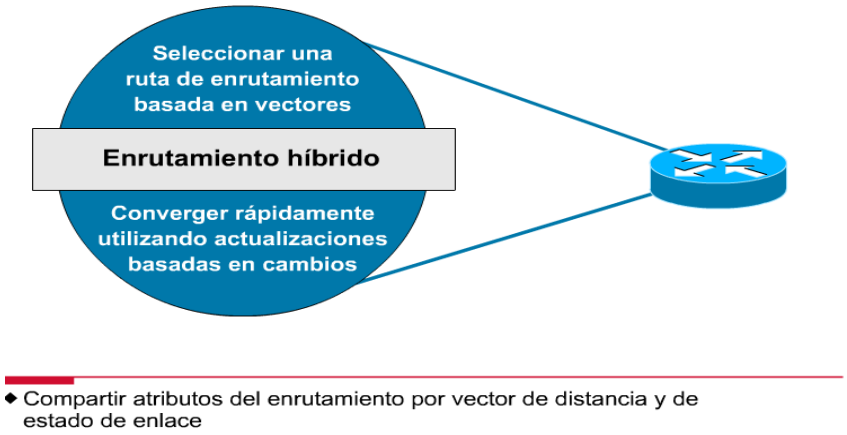

Figura 4.23 Enrutamiento híbrido

4.9 Enrutamiento LAN a LAN

La capa de red debe comprender y ser capaz de comunicarse con varias capas inferiores. Los routers deben poder manejar, en forma transparente, paquetes encapsulados en diversas tramas de nivel inferior sin cambiar el direccionamiento de Capa 3 de los paquetes.

La figura 4.24 muestra un ejemplo de esto en el enrutamiento LAN a LAN. En este ejemplo, el tráfico de paquetes del Host 4 origen en la Red Ethernet 1 necesita una ruta hacia el Host 5 destino en la Red 2. Los hosts de la LAN dependen del router y de su direccionamiento de red para encontrar la mejor ruta.

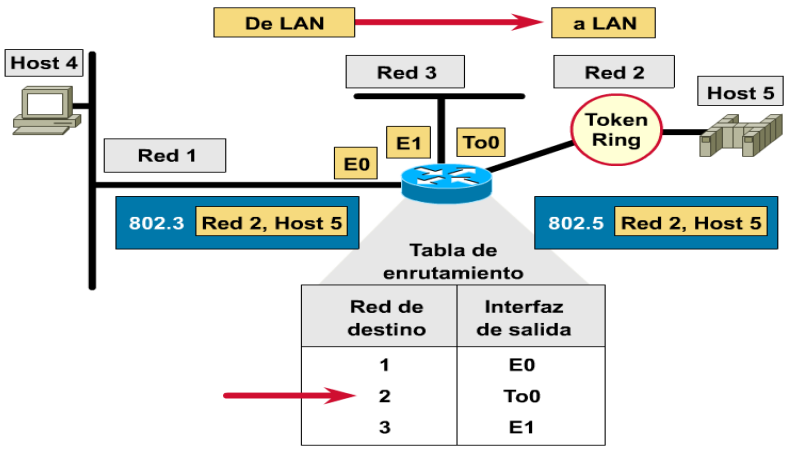

Figura 4.24 enrutamiento LAN a LAN

4.10 Enrutamiento LAN a WAN

La capa de red debe relacionarse y tener comunicación con distintas capas inferiores para el tráfico LAN a WAN. A medida que la internetwork aumenta de tamaño, la ruta elegida por un paquete puede encontrar varios puntos de transferencia y una gran variedad de tipos de enlaces de datos más allá de las LAN. Por ejemplo, en la figura ocurre lo siguiente:

1. Un paquete de la estación de trabajo superior con dirección 1.3 debe atravesar tres enlaces de datos para alcanzar el servidor de archivos en la dirección 2.4, que aparece en la parte inferior.
2. La estación de trabajo envía un paquete al servidor de archivos encapsulándolo en primer lugar en una trama token-ring dirigida al Router A.
3. Una vez que el Router A recibe la trama, retira el paquete de la trama token-ring, lo encapsula en una trama Frame Relay y envía la trama al Router B.
4. El Router B retira el paquete de la trama Frame Relay y lo envía al servidor de archivos en una trama Ethernet recién creada.
5. Una vez que el servidor de archivos en 2.4 recibe la trama Ethernet, extrae y transfiere el paquete al proceso de capa superior correspondiente.

Los routers permiten el flujo de paquetes desde una LAN a una WAN manteniendo constantes las direcciones origen y destino extremo a extremo mientras se encapsula el paquete en tramas de enlace de datos, según sea necesario, para el siguiente salto a lo largo de la ruta (**véase figura 4.25**).

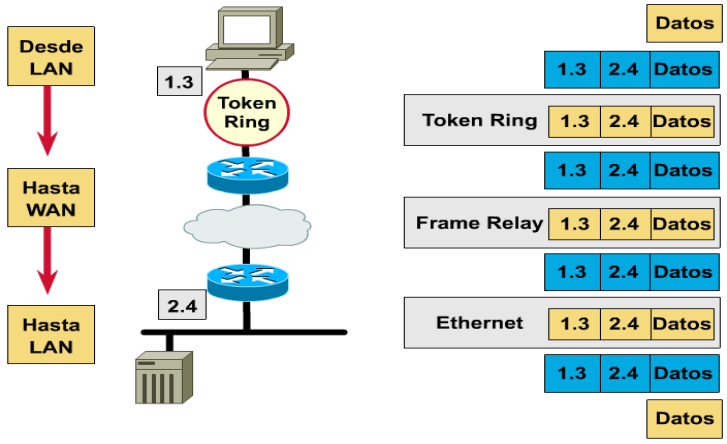

Figura 4.25 Enrutamiento de LAN y WAN

4.10.1Selección de ruta y conmutación para múltiples protocolos y medios

Los routers son dispositivos que implementan servicios de red. Proporcionan interfaces para una amplia gama de enlaces y subredes, con una gran variedad de velocidades. Los routers son nodos de red activos e inteligentes que pueden participar en la administración de una red. Los routers manejan las redes proporcionando control dinámico sobre los recursos y respaldando las tareas y objetivos para la conectividad de internetwork, desempeño confiable, control administrativo y flexibilidad.

Además de las funciones de conmutación y enrutamiento básicas, los routers poseen una gran variedad de funciones adicionales que ayudan a reducir los costos de la internetwork. Estas funciones incluyen el secuenciamiento de tráfico basado en prioridad y el filtraje del tráfico.

Normalmente, se necesita que los routers soporten múltiples pilas de protocolo, cada una con sus propios protocolos de enrutamiento y que permitan que estos distintos entornos operen en paralelo. En la práctica, los routers también incorporan las funciones de puenteo y a veces operan como un hub limitado.

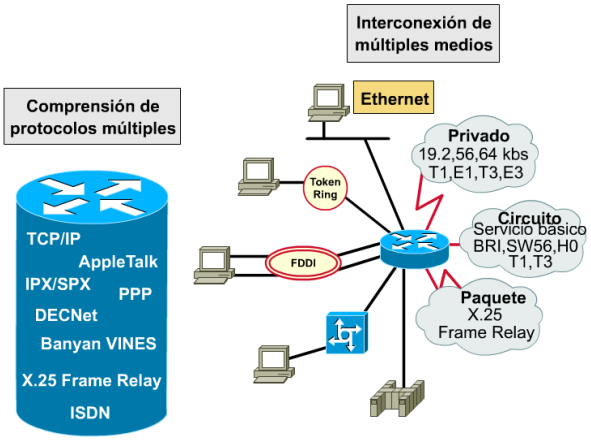

Figura 4.26 funciones de un Router

Capitulo 5. SOLUCION DEL PROBLEMA

5.1 Introducción al problema

La empresa Quick Learning tiene aproximadamente tres años sin personal para la administración de la red.

Quick Learning es una empresa de giro educativo que cuenta con oficinas generales para la administración de la empresa y 46 sucursales alrededor del país y en parte de USA, para la enseñanza de la lengua inglesa **Ver Anexo 1 figura 1.1.** Las oficinas generales se encuentran divididas en 19 departamentos. En la **tabla 1.1** se enlistan los departamentos con que cuenta la empresa en oficinas generales y número de Hosts que se requieren en cada departamento.

Tabla 1.1 Descripcion de departamentos de Oficinas Generales de Quick Learning. 142 hosts en total actualmente

Depto.	Hosts	Depto.	Hosts
Caja	2	Capacitación	3
Rec. Hum.	5	Control Calidad	5
Dir. Gral. Suc.	2	Personal	3
Dir. Gral.	3	Arquitectura	4
Computación	2	Sistemas	6
Ventas	1	Dirección U.V.	2
Jurídico	2	Admón.. U.V.	8
Mercadotecnia	2	Centro Inf.	42
Contabilidad	7	Lab. Computo	40
Editorial	3	Sucursales	4* + 1**

*Las sucursales cuentan con Hosts en los departamentos de: Dirección (1), Recepción (2) y Ventas (1).

**La biométrica para checar entrada y salida de personal es IP por lo que se necesita contemplar un host más para sucursales.

5.2 Desarrollo de la problemática

El dominio que adquirió la empresa es el 192.168.0.0 por lo que la disponibilidad de IPs es de la 192.168.0.0 a la 192.168.255.255. La empresa requiere tener direcciones IP disponibles para oficinas generales y para futura apertura de sucursales.

En la actualidad no se sabe que direcciones IP están disponibles, en oficinas generales se utiliza el segmento 192.168.100.0 pero no se puede agregar fácilmente un Host a la red debido a que no se tiene una relación de Hosts con la IP que tienen asignada actualmente, si se agrega un usuario a la red sin saber si la IP ya está ocupada genera problemas de acceso a la red tanto al usuario que ya dispone de ella como al que quiere usarla, se realiza este proceso hasta que se encuentra una IP que no genere el problema, lo que consume mucho tiempo de trabajo.

En oficinas generales se cuenta con un servidor que contiene el sistema de administración al cual están conectadas todas las sucursales y departamentos de oficinas generales, actualmente la red se satura debido a que todas las sucursales manejan un direccionamiento de la siguiente manera: Las sucursales están numeradas de la 1 a la 46, el direccionamiento esta tomado de acuerdo al número de la sucursal en el tercer octeto de la dirección IP. Es decir para la sucursal 1 el segmento de red tomando es el 192.168.101.0, para la sucursal 2 el segmento es el 192.168.102.0 y así sucesivamente. Debido a que solo se tienen cinco hosts por segmento se maneja un gran dominio de broadcast lo que provoca que el tiempo de respuesta de la red sea muy lento. **Ver Anexo 1 figura 1.2** donde se muestra un diagrama lógico con el direccionamiento IP actual de la empresa.

Todas las sucursales deben poder ser administradas remotamente desde oficinas generales, en la actualidad se envía personal muy frecuentemente a sitio a resolver problemas de administración de equipos de acceso a la red ya que es desconocido el direccionamiento IP y no se puede manejar la administración remotamente. **Ver Anexo 1 figura 1.2.**

5.3 Solución de la problemática

Tomando en cuenta el dominio adquirido por la empresa (192.168.0.0) y el número de Hosts descritos en la tabla 1.2, se toman las subredes de la siguiente manera:

Para enlaces WAN (direccionamiento IP de los routers) se necesitan subredes de 2 Hosts, utilizando el segmento 192.168.1.0 en adelante hasta cubrir los 46 enlaces hacia las sucursales. Se requieren solo 2 direcciones, una para el enlace que llega a la sucursal y una que va hacia nuestro carrier.

El cálculo de las subredes y la máscara de subred se obtienen de la siguiente manera:

5.3.1 Subredes Enlaces WAN

Es posible tener **2** equipos por subred, porque hay suficientes bits a 0 en la máscara, hay 8 bits a cero (y 2^8 - 2 es mayor que 2), como se puede observar en la mascara. **11111111.11111111.11111111.00000000 (255.255.255.0)**

Nota: La mascara natural de la red 192.168.0.0 es 255.255.0.0 por ser de clase B pero como se toma un segmento de esta red se pondrán a '1' 8 bits más de la máscara. Esta mascara la ampliaremos para crear subredes, la ampliaremos cambiando ceros por unos de forma que volvamos a obtener una máscara que sea correcta.

Para tener los equipos especificados es necesario utilizar al menos **2** bits, porque **2^2-2=2** son el número de hosts especificados.

Ahora, calculamos la mascara ampliada cambiando los ceros que no serán utilizados para host en unos. Tal y como se indica a continuación:

Mascara subred: **11111111.11111111.11111111.00000000** (255.255.255.0)

Mascara ampliada:**11111111.11111111.11111111.11111100** (255.255.255.252)

A partir de ahora, todas las subredes que tengamos usarán esta máscara ampliada de 30 bits.

Para calcular el total de subredes se debe realizar 2^6 subredes, ya que se han tomado 6 bits prestados a la dirección de host. Lo que nos da un total de 64 subredes, por lo tanto se cubre la necesidad de conexión de las 46 sucursales en el segmento que va del 192.168.1.0 al 192.168.1.255.

La dirección IP donde iniciaremos nuestras subredes es: 192.168.1.0 (tomando el segmento 1 de la red 192.168.0.0), con el cálculo de la máscara ampliada se obtienen las direcciones validas realizando una operación AND como se muestra a continuación:

Dirección de red: **11000000.10101000.00000001.000000**00 (192.168.1.0)
AND
Máscara ampliada: **11111111.11111111.11111111.11111**100 (255.255.255.252)

El resultado indica que:

Identificador de red: **11000000.10101000.00000001.00000000** (192.168.1.0)

A nuestro identificador de red se le cambian a unos los dos bits de host para obtener la dirección de broadcast

Broadcast: 11000000.10101000.00000001.00000**11** (192.168.1.3)

Para obtener las direcciones validas para los hosts de las subredes, se suma uno al identificador de red para el primer host y se resta uno a la dirección de broadcast para obtener la dirección del último host por lo tanto los cálculos nos indican que:

El Primer Host es: 11000000.10101000.00000001.00000**01** (192.168.1.1)
El Ultimo Host es: 11000000.10101000.00000001.00000**10** (192.168.1.2)

De esta manera se comprueba que con esta mascara ampliada se tienen subredes de 2 host.

Para nuestra siguiente subred de acuerdo con el cálculo anterior tenemos que nuestra siguiente subred inicia después de 192.168.1.3 (broadcast subred anterior). Se realizan los mismos cálculos pero con el inicio de la siguiente subred para obtener las siguientes direcciones validas:

Dirección de red**:** **11000000.10101000.00000001.00000100** (192.168.1.4)
AND
Máscara ampliada: **11111111.11111111.11111111.11111100** (255.255.255.252)

Identificador de red: 11000000.10101000.00000001.00000100 (192.168.1.4)

A nuestro identificador de red se le cambian a unos los dos bits de host para obtener la dirección de broadcast

Broadcast: 11000000.10101000.00000001.00000**11** (192.168.1.7)

Para obtener las direcciones validas para los hosts de las subredes, se suma uno al identificador de red para el primer host y se resta uno a la dirección de broadcast para obtener la dirección del último host por lo tanto los cálculos nos indican que:

El Primer Host es: 11000000.10101000.00000001.00000**01** (192.168.1.5)
El Ultimo Host es: 11000000.10101000.00000001.00000**10** (192.168.1.6)

Ver Anexo 1 figura 1.3 donde se muestra el diagrama lógico de asignación de IPs para los enlaces WAN.

Se realiza el mismo cálculo para todas las subredes necesarias. **Ver Anexo 2 tabla 1.1** para obtener todas las direcciones validas para los enlaces WAN.

Se reservaran los segmentos de red 192.168.2.0 al 192.168.9.0 para futuro crecimiento de la empresa y para ayuda de la administración de la red.

5.3.2 Subredes Oficinas Generales

Para los usuarios de Oficinas Generales se necesitan subredes de 61 Hosts (se crearan subredes de 61 por el numero de host en CI (Centro de Información) y Lab. De Cómputo. El CI requiere de 42 Hosts y el Laboratorio de 40 pero se deja un margen para futuro crecimiento de todos los departamentos. Las subredes se calcularan a partir del segmento 192.168.10.0 hasta cubrir la necesidad de 19 subredes para los 19 departamentos descritos en la **tabla 1.1**. A estos 19 le aumentamos una subred para el direccionamiento de Servidores y uno más para direccionamiento de los siwtches y routers, lo que nos aumenta las subredes a 21.

El cálculo de las subredes y la máscara de subred se obtienen de la siguiente manera:

Es posible tener **61** Hosts por subred, porque hay suficientes bits a 0 en la máscara, hay 8 bits a cero (y 2^8 - 2 es mayor que 61), como se puede observar en la máscara. **11111111.11111111.1111111.00000000 (255.255.255.0).**

Nota: La máscara natural de la red 192.168.0.0 es 255.255.0.0 por ser de clase B pero como se toma un segmento de esta red se pondrán a '1' 8 bits más de la máscara. Esta mascara la ampliaremos para crear subredes, la ampliaremos cambiando ceros por unos de forma que volvamos a obtener una máscara que sea correcta.

Para tener los equipos especificados es necesario utilizar al menos 6 bits, porque **2^6-2=61** son el número de hosts especificados.

Ahora, calculamos la máscara ampliada cambiando los ceros que no serán utilizados para host en unos. Tal y como se indica a continuación:

Mascara origen: **11111111.11111111.11111111.00000000** (255.255.255.0)

Mascara ampliada: **11111111.11111111.11111111.11000000** (255.255.255.192)

A partir de ahora, todas las subredes que tengamos usarán esta máscara ampliada de 26 bits.

Para calcular el total de subredes se debe realizar 2^2 subredes, ya que se han tomado 2 bits prestados a la dirección de host. Lo que nos da un total de 4 subredes, como se puede observar con estos 2 bits de subred no se puede cubrir la necesidad de las 21 subredes pero tomemos en cuenta que esto solo es para un segmento de la red, por cada segmento (192.168.10.0,192.168.11.0) se tienen 4 subredes, por lo tanto con el cambio de 6 segmentos se tienen 24 subredes lo

que es mayor a 21 subredes requeridas, por lo tanto se cubre la necesidad de conexión de los 19 departamentos y dos subredes mas para el direccionamiento de los servidores, switches y routers con los segmentos 192.168.10.0 al 192.168.15.0.

La dirección IP donde iniciaremos nuestras subredes es: 192.168.10.0 (tomando el segmento 10 de la red 192.168.0.0), con el cálculo de la máscara ampliada se obtienen las direcciones validas realizando una operación AND como se muestra a continuación:

Dirección de red: **11000000.10101000.00001010.00**000000 (192.168.10.0)
AND
Máscara ampliada: **11111111.11111111.11111111.11**000000 (255.255.255.192)

El resultado indica el
Identificador de red: **11000000.10101000.00001010.00000000** (192.168.10.0)

A nuestro identificador de red se le cambian a unos los dos bits de host para obtener la dirección de broadcast

Broadcast: 11000000.10101000.00001010.00**111111** (192.168.10.63)

Para obtener las direcciones validas para los hosts de las subredes, se suma uno al identificador de red para el primer host y se resta uno a la dirección de broadcast para obtener la dirección del último host por lo tanto los cálculos nos indican que:

El Primer Host es: 11000000.10101000.00001010.00**000001** (192.168.10.1)
11000000.10101000.00001010.00**000010**
11000000.10101000.00001010.00**000011**
...
11000000.10101000.00001010.00**111101**
El Ultimo Host es: 11000000.10101000.00001010.00**111110** (192.168.10.62)

De esta manera se comprueba que con esta mascara ampliada se tienen subredes de 61 hosts.

Esta primera subred se ocupara para direccionamiento de los switches y routers, por lo tanto se propone que el Default Gateway sea la dirección 192.168.10.1 y las direcciones 192.168.10.30 a la 192.168.10.35 se asignen a los 6 switches necesarios para la interconexión de los hosts (se necesitan 6 switches de 24 Puertos para cubrir la necesidad actual de 142 hosts en uso). Las Direcciones 192.168.10.2 a la 192.168.10.29 se reservan para crecimiento en routers y la 192.168.10.36 a la 192.168.10.62 para crecimiento en switches. La siguiente subred se destina para los servidores; de acuerdo con el cálculo anterior tenemos que nuestra siguiente subred inicia después de 192.168.10.63 (broadcast subred

anterior). Se realizan los mismos cálculos pero con el inicio de la siguiente subred para obtener las siguientes direcciones validas:

Dirección de red**:** **11000000.10101000.00001010.01**000000 (192.168.10.64)
AND
Máscara ampliada: **11111111.11111111.11111111.11**000000 (255.255.255.192)

Identificador de red: **11000000.10101000.00001010.01000000** (192.168.10.64)

A nuestro identificador de red se le cambian a unos los dos bits de host para obtener la dirección de broadcast

Broadcast: 11000000.10101000.00001010.01**111111** (192.168.10.127)

Para obtener las direcciones validas para los hosts de las subredes, se suma uno al identificador de red para el primer host y se resta uno a la dirección de broadcast para obtener la dirección del último host por lo tanto los cálculos nos indican que:

El Primer Host es: 11000000.10101000.00001010.01**000001** (192.168.10.65)
11000000.10101000.00001010.01**000010**
…
11000000.10101000.00001010.01**111101**
El Ultimo Host es: 11000000.10101000.00001010.01**111110** (192.168.10.126)

Ver Anexo 1 figura 1.4 donde se muestra el diagrama lógico de asignación de IP de switches y routers.

Se realiza el mismo cálculo para las subredes siguientes que son para la asignación de direcciones IP de los Hosts de departamentos. **Ver Anexo 2 tabla 1.2** para obtener todas las direcciones validas de los Hosts.

Se reservan las subredes de los segmentos 192.168.16.0 al 192.168.19.0 para futuro crecimiento y para ayuda de administración de la red.

5.3.3 Subredes Sucursales

Para las 46 sucursales se necesitan subredes de 13 Host. Se utilizaran los segmentos a partir del 192.168.20.0. Si se observa en la tabla V.2 solo se requiere de 7 direcciones (5 para Hosts, 1 para Switch y 1 para Router) pero se aumentara a 13 para tener posibilidad de crecimiento.

El procedimiento para el cálculo de las subredes y la máscara de subred para el direccionamiento de sucursales es el mismo que se realiza en los cálculos anteriores, el segmento a utilizar es el 192.168.20.0.

Para tener los equipos especificados es necesario utilizar al menos 4 bits, porque **2^4-2=13** son el número de hosts especificados.

Ahora, calculamos la máscara ampliada cambiando los ceros que no serán utilizados para host en unos. Tal y como se indica a continuación:

Mascara origen: **11111111.11111111.11111111.00000000** (255.255.255.0)

Mascara ampliada **11111111.11111111.11111111.11110000** (255.255.255.240)

A partir de ahora, todas las subredes que tengamos usarán esta máscara ampliada de 28 bits.

Para calcular el total de subredes se debe realizar 2^4 subredes, ya que se han tomado 4 bits prestados a la dirección de host. Lo que nos da un total de 16 subredes, como se puede observar con estos 4 bits de subred no se puede cubrir la necesidad de las 46 subredes pero tomemos en cuenta que esto solo es para un segmento de la red, por cada segmento (192.168.20.0,192.168.21.0) se tienen 16 subredes, por lo tanto necesitamos 3 cambios de segmento para cubrir las 46 subredes.

La dirección IP donde iniciaremos nuestras subredes es: 192.168.20.0 (tomando el segmento 20 de la red 192.168.0.0), con el cálculo de la máscara ampliada se obtienen las direcciones validas realizando una operación AND como se muestra a continuación:

Dirección de red: **11000000.10101000.00010100.0000**0000 (192.168.20.0)
AND
Máscara ampliada: **11111111.11111111.11111111.1111**0000 (255.255.255.240)

El resultado indica que:

Identificador de red: **11000000.10101000.00010100.00000000** (192.168.20.0)

A nuestro identificador de red se le cambian a unos los dos bits de host para obtener la dirección de broadcast

Broadcast: 11000000.10101000.00010100.0000**1111** (192.168.20.15)

Para obtener las direcciones validas para los hosts de las subredes, se suma uno al identificador de red para el primer host y se resta uno a la dirección de broadcast para obtener la dirección del último host por lo tanto los cálculos nos indican que:

El Primer Host es: 11000000.10101000.00010100.0000**0001** (192.168.20.1)
11000000.10101000.00010100.0000**0010**
11000000.10101000.00010100.0000**0011**
…
11000000.10101000.00010100.0000**1101**
El Ultimo Host es: 11000000.10101000.00010100.0000**1110** (192.168.20.14)

De esta manera se comprueba que con esta mascara ampliada se tienen subredes de 13 hosts.

Esta primera Subred se utilizara para el direccionamiento de la primera sucursal.

Para llevar un orden en las subredes se propone que la primera dirección de subred sea para el Host Dirección, la segunda para el Host de Ventas, la tercera y cuarta para los host de Recepción, la dirección número 12 para la Biométrica, la 13 para el switch y la 14 para el Default Gateway. **Ver Anexo 1 figura 1.5** donde se muestra un diagrama lógico para el direccionamiento de los Hosts, y equipo de red de las Sucursales.

La siguiente subred se asigna a la segunda Sucursal, de acuerdo con el cálculo anterior tenemos que nuestra siguiente subred inicia después de 192.168.20.15 (broadcast subred anterior). Se realizan los mismos cálculos pero con el inicio de la siguiente subred para obtener las siguientes direcciones validas:

Dirección de red**:** **11000000.10101000.00010100.0001**0000 (192.168.20.16)
AND
Máscara ampliada: **11111111.11111111.11111111.1111**0000 (255.255.255.240)

Identificador de red: 11000000.10101000.00010100.00010000 (192.168.20.16)

A nuestro identificador de red se le cambian a unos los dos bits de host para obtener la dirección de broadcast.

Broadcast: 11000000.10101000.00010100.0001**1111** (192.168.20.31)

Para obtener las direcciones validas para los hosts de las subredes, se suma uno al identificador de red para el primer host y se resta uno a la dirección de broadcast para obtener la dirección del último host por lo tanto los cálculos nos indican que:

El Primer Host es: 11000000.10101000.00010100.0001**0001** (192.168.20.17)
11000000.10101000.00010100.0001**0010**
…
11000000.10101000.00010100.0001**1101**
El Ultimo Host es: 11000000.10101000.00010100.0001**1110** (192.168.20.30)

Se realiza el mismo cálculo para las subredes siguientes que son para la asignación de direcciones IP de los Hosts de las otras sucursales. **Ver Anexo 2 tabla 1.3** para obtener todas las direcciones validas de los Hosts.

Se reservan las subredes de los segmentos 192.168.23.0 al 192.168.29.0 para futuro crecimiento y para ayuda de administración de la red.

5.4. Conclusiones

Con los cálculos anteriores se obtiene todas las subredes necesarias para asignación de todos los Host y equipo necesario para la interconexión de la red de la empresa Quick Learning.

Los cálculos de las subredes nos permiten obtener un ahorro de direcciones IP, para tener posibilidades de crecimiento en números de equipos para redes LAN y WAN.

Con la limitación de números de Host a un número posible a crecimiento en las subredes nos ayuda a tener menor dominio de colisión y a mejorar el tiempo de respuesta de la red.

Las tablas obtenidas de los cálculos de las subredes nos permiten tener una buena administración de las direcciones IP, para asignar fácilmente una dirección a un host que se integra a la red LAN, o un enlace WAN a una sucursal nueva; así mismo nos permite tener el registro de estos enlaces para una conexión remota hacia los equipos de las sucursales para revisión y solución de algún conflicto que pueda ser solucionado desde oficinas generales sin necesidad de acudir a las diferentes sucursales. **Ver Anexo 1 figura 1.6** donde se muestra el diagrama lógico con la propuesta del direccionamiento IP para red de la empresa Quick Learning.

ANEXOS

Anexo 1 FIGURAS

Figura 1.1 Estados de la Republica y USA en señalados en color azul donde se encuentran ubicadas las sucursales de Quick Learning.

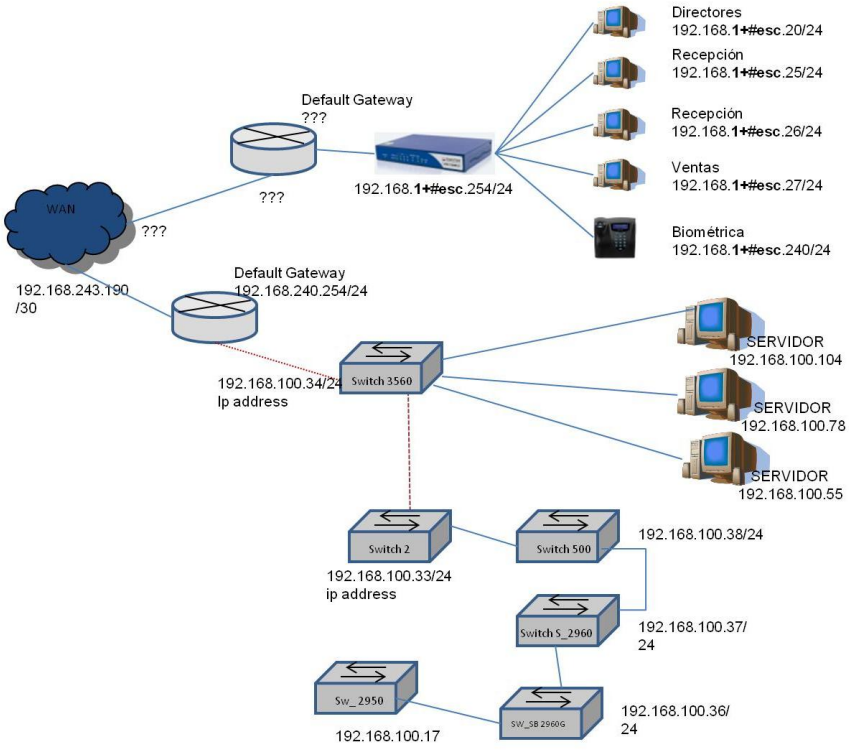

Figura 1.2 Diagrama Lógico general de direccionamiento IP actual de la red de la empresa Quick Learning

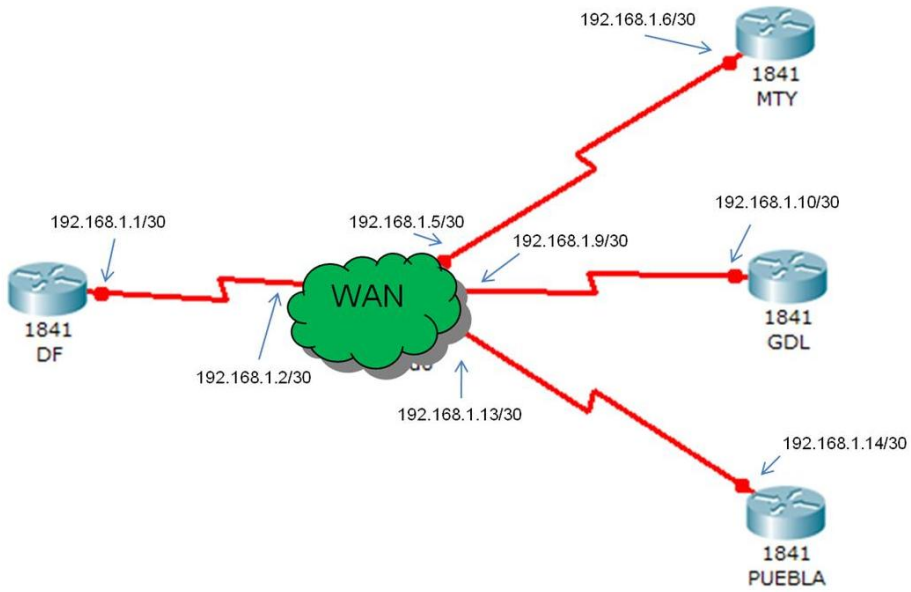

Figura 1.3 Diagrama lógico de asignación de IPs para enlaces WAN

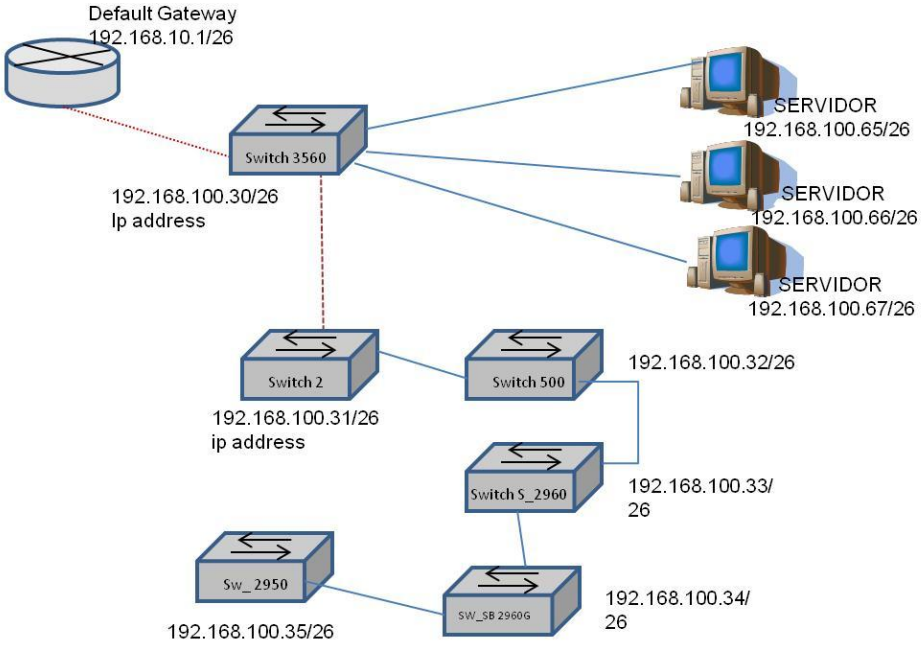

Figura 1.4 Diagrama lógico de Direccionamiento para Switches, Routers y servidores

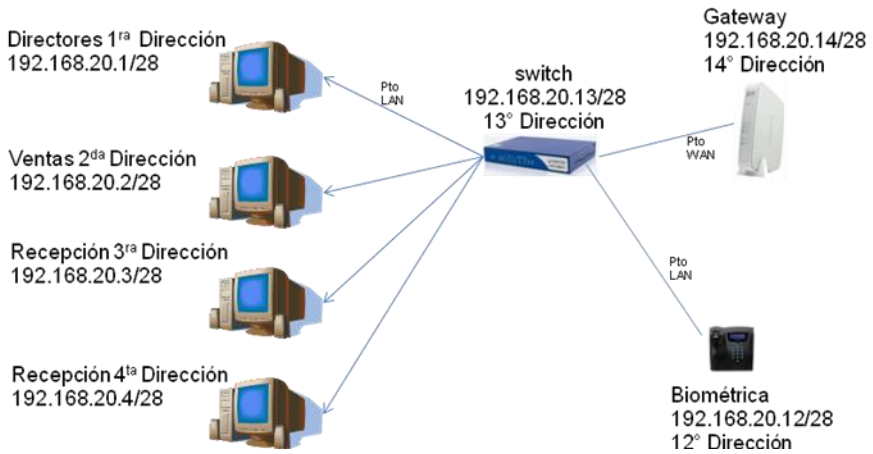

Figura 1.5 Diagrama Lógico de Direccionamiento IP para Sucursales

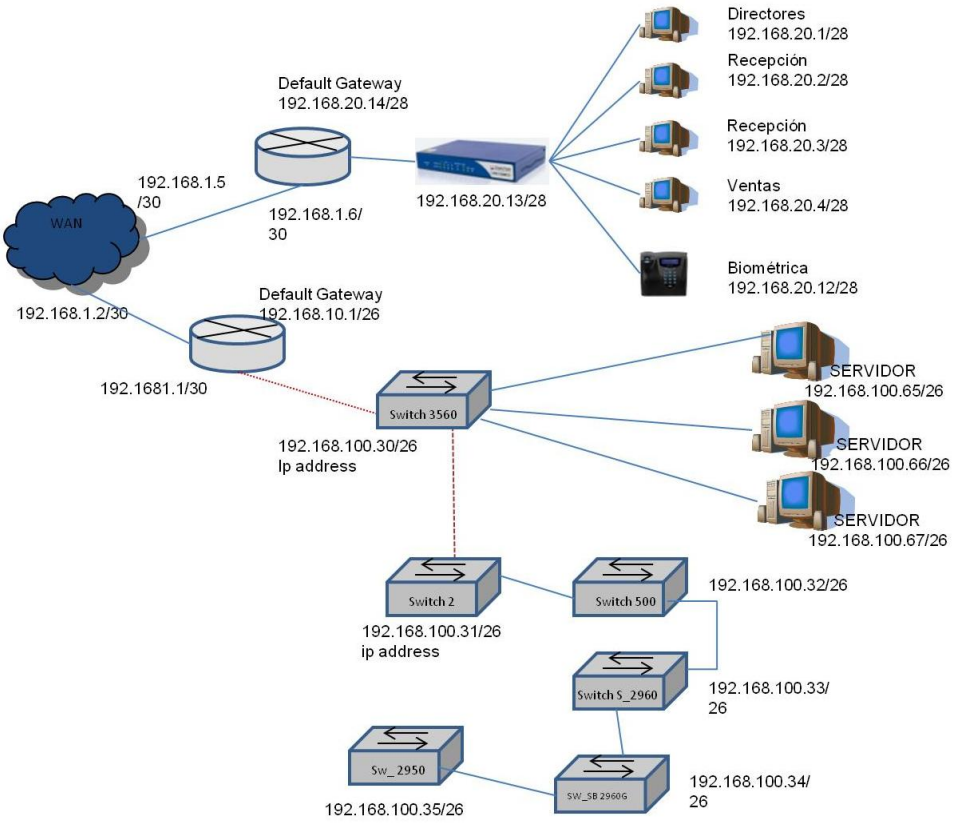

Figura 1.6 Diagrama Lógico General de la Propuesta de direccionamiento IP para la red de la empresa Quick Learning

Anexo 2.TABLAS

Tabla 1.1 Direccionamiento IP para enlaces WAN

			Subred Sucursal	Enlace sucursales	Enlace WAN	Broadcast
Sucursales DF						
1		lomas verdes	192.168.1.0	192.168.1.1	192.168.1.2	192.168.1.3
2		coacalco	192.168.1.4	192.168.1.5	192.168.1.6	192.168.1.7
3		arboledas	192.168.1.8	192.168.1.9	192.168.1.10	192.168.1.11
4		aragon	192.168.1.12	192.168.1.13	192.168.1.14	192.168.1.15
5		neza	192.168.1.16	192.168.1.17	192.168.1.18	192.168.1.19
6		villa coapa	192.168.1.20	192.168.1.21	192.168.1.22	192.168.1.23
7		montevideo	192.168.1.24	192.168.1.25	192.168.1.26	192.168.1.27
8		ecatepec	192.168.1.28	192.168.1.29	192.168.1.30	192.168.1.31
9		chalco	192.168.1.32	192.168.1.33	192.168.1.34	192.168.1.35
10		izacalli	192.168.1.36	192.168.1.37	192.168.1.38	192.168.1.39
11		satelite	192.168.1.40	192.168.1.41	192.168.1.42	192.168.1.43
12		texcoco	192.168.1.44	192.168.1.45	192.168.1.46	192.168.1.47
13		toluca	192.168.1.48	192.168.1.49	192.168.1.50	192.168.1.51
14		toreo	192.168.1.52	192.168.1.53	192.168.1.54	192.168.1.55
Sucursales Int. Republica						
15		tijuana	192.168.1.56	192.168.1.57	192.168.1.58	192.168.1.59
16		Cd Juarez	192.168.1.60	192.168.1.61	192.168.1.62	192.168.1.63
17	MTY	anahuac	192.168.1.64	192.168.1.65	192.168.1.66	192.168.1.67
18		sta catarina	192.168.1.68	192.168.1.69	192.168.1.70	192.168.1.71
19		contry	192.168.1.72	192.168.1.73	192.168.1.74	192.168.1.75
20		cumbres	192.168.1.76	192.168.1.77	192.168.1.78	192.168.1.79
21		lindavista	192.168.1.80	192.168.1.81	192.168.1.82	192.168.1.83
22		sto domingo	192.168.1.84	192.168.1.85	192.168.1.86	192.168.1.87
23		leon	192.168.1.88	192.168.1.89	192.168.1.90	192.168.1.91
24		san luis	192.168.1.92	192.168.1.93	192.168.1.94	192.168.1.95
25		veracruz	192.168.1.96	192.168.1.97	192.168.1.98	192.168.1.99
26		aguas calientes	192.168.1.100	192.168.1.101	192.168.1.102	192.168.1.103
27	GDL	americas	192.168.1.104	192.168.1.105	192.168.1.106	192.168.1.107
28		autonoma	192.168.1.108	192.168.1.109	192.168.1.110	192.168.1.111
29		chapultepec	192.168.1.112	192.168.1.113	192.168.1.114	192.168.1.115
30		independencia	192.168.1.116	192.168.1.117	192.168.1.118	192.168.1.119
31		plaza del sol	192.168.1.120	192.168.1.121	192.168.1.122	192.168.1.123
32		revolucion	192.168.1.124	192.168.1.125	192.168.1.126	192.168.1.127

			Subred Sucursal	Enlace sucursales	Enlace WAN	Broadcast
33	Puebla	loreto	192.168.1.128	192.168.1.129	192.168.1.130	192.168.1.131
34		valsequillo	192.168.1.132	192.168.1.133	192.168.1.134	192.168.1.135
35		queretaro	192.168.1.136	192.168.1.137	192.168.1.138	192.168.1.139
36		cancun	192.168.1.140	192.168.1.141	192.168.1.142	192.168.1.143
37		hermosillo	192.168.1.144	192.168.1.145	192.168.1.146	192.168.1.147
38		tampico	192.168.1.148	192.168.1.149	192.168.1.150	192.168.1.151
Sucursales USA						
39		los angeles	192.168.1.152	192.168.1.153	192.168.1.154	192.168.1.155
40		las vegas	192.168.1.156	192.168.1.157	192.168.1.158	192.168.1.159
41		phoenix	192.168.1.160	192.168.1.161	192.168.1.162	192.168.1.163
42		arlington	192.168.1.164	192.168.1.165	192.168.1.166	192.168.1.167
43		dallas	192.168.1.168	192.168.1.169	192.168.1.170	192.168.1.171
44		north houston	192.168.1.172	192.168.1.173	192.168.1.174	192.168.1.175
45		suth houston	192.168.1.176	192.168.1.177	192.168.1.178	192.168.1.179
46		cobrica	192.168.1.180	192.168.1.181	192.168.1.182	192.168.1.183

Tabla 1.2 Direccionamiento IP para Switches, Routers, Servidores y Deptos de oficinas generales

Oficinas Generales		Subred	Primer Host	Ultimo Host	Broadcast
1	Switches	192.168.10.0	192.168.10.1	192.168.10.29	192.168.10.63
	Routers	192.168.10.0	192.168.10.30	192.168.10.62	192.168.10.63
2	Servidores	192.168.10.64	192.168.10.65	192.168.10.126	192.168.10.127
3	Caja	192.168.10.128	192.168.10.129	192.168.10.190	192.168.10.191
4	Rec. Humanos	192.168.10.192	192.168.10.193	192.168.10.254	192.168.10.255
5	Dir. Gral. Suc.	192.168.11.0	192.168.11.1	192.168.11.62	192.168.11.63
6	Dirección General	192.168.11.64	192.168.11.65	192.168.11.126	192.168.11.127
7	Computación	192.168.11.128	192.168.11.129	192.168.11.190	192.168.11.191
8	Ventas	192.168.11.192	192.168.11.193	192.168.11.254	192.168.11.255
9	Jurídico	192.168.12.0	192.168.12.1	192.168.12.62	192.168.12.63
10	Mercadotecnia	192.168.12.64	192.168.12.65	192.168.12.126	192.168.12.127
11	Contabilidad	192.168.12.128	192.168.12.129	192.168.12.190	192.168.12.191
12	Editorial	192.168.12.192	192.168.12.193	192.168.12.254	192.168.12.255
13	Capacitación	192.168.13.0	192.168.13.1	192.168.13.62	192.168.13.63
14	Control de calidad	192.168.13.64	192.168.13.65	192.168.13.126	192.168.13.127
15	Personal	192.168.13.128	192.168.13.129	192.168.13.190	192.168.13.191
16	Arquitectura	192.168.13.192	192.168.13.193	192.168.13.254	192.168.13.255
17	Sistemas	192.168.14.0	192.168.14.1	192.168.14.62	192.168.14.63
18	Dir. UV	192.168.14.64	192.168.14.65	192.168.14.126	192.168.14.127
19	Admón. UV.	192.168.14.128	192.168.14.129	192.168.14.190	192.168.14.191
20	CI	192.168.14.192	192.168.14.193	192.168.14.254	192.168.14.255
21	Lab. Computo UV	192.168.15.0	192.168.15.1	192.168.15.62	192.168.15.63

Tabla 1.3 Direccionamiento IP para sucursales

			Subred Sucursal	primer host	ultimo host	broadcast
Sucursales DF						
1		lomas verdes	192.168.20.0	192.168.20.1	192.168.20.14	192.168.20.15
2		coacalco	192.168.20.16	192.168.20.17	192.168.20.30	192.168.20.31
3		arboledas	192.168.20.32	192.168.20.33	192.168.20.46	192.168.20.47
4		aragon	192.168.20.48	192.168.20.49	192.168.20.62	192.168.20.63
5		neza	192.168.20.64	192.168.20.65	192.168.20.78	192.168.20.79
6		villa coapa	192.168.20.80	192.168.20.81	192.168.20.94	192.168.20.95
7		montevideo	192.168.20.96	192.168.20.97	192.168.20.110	192.168.20.111
8		ecatepec	192.168.20.112	192.168.20.113	192.168.20.126	192.168.20.127
9		chalco	192.168.20.128	192.168.20.129	192.168.20.142	192.168.20.143
10		izacalli	192.168.20.144	192.168.20.145	192.168.20.158	192.168.20.159
11		satelite	192.168.20.160	192.168.20.161	192.168.20.174	192.168.20.175
12		texcoco	192.168.20.176	192.168.20.177	192.168.20.190	192.168.20.191
13		toluca	192.168.20.192	192.168.20.193	192.168.20.206	192.168.20.207
14		toreo	192.168.20.208	192.168.20.209	192.168.20.222	192.168.20.223
Sucursales Int. Republica						
15		tijuana	192.168.20.224	192.168.20.225	192.168.20.238	192.168.20.239
16		Cd Juarez	192.168.20.240	192.168.20.241	192.168.20.254	192.168.20.255
17	MTY	anahuac	192.168.21.0	192.168.21.1	192.168.21.14	192.168.21.15
18		sta catarina	192.168.21.16	192.168.21.17	192.168.21.30	192.168.21.31
19		contry	192.168.21.32	192.168.21.33	192.168.21.46	192.168.21.47
20		cumbres	192.168.21.48	192.168.21.49	192.168.21.62	192.168.21.63
21		lindavista	192.168.21.64	192.168.21.65	192.168.21.78	192.168.21.79
22		sto domingo	192.168.21.80	192.168.21.81	192.168.21.94	192.168.21.95
23		leon	192.168.21.96	192.168.21.97	192.168.21.110	192.168.21.111
24		san luis	192.168.21.112	192.168.21.113	192.168.21.126	192.168.21.127
25		veracruz	192.168.21.128	192.168.21.129	192.168.21.142	192.168.21.143
26		aguas calientes	192.168.21.144	192.168.21.145	192.168.21.158	192.168.21.159
27	GDL	americas	192.168.21.160	192.168.21.161	192.168.21.174	192.168.21.175
28		autonoma	192.168.21.176	192.168.21.177	192.168.21.190	192.168.21.191
29		chapultepec	192.168.21.192	192.168.21.193	192.168.21.206	192.168.21.207
30		independencia	192.168.21.208	192.168.21.209	192.168.21.222	192.168.21.223
31		plaza del sol	192.168.21.224	192.168.21.225	192.168.21.238	192.168.21.239
32		revolucion	192.168.21.240	192.168.21.241	192.168.21.254	192.168.21.255
33	Puebla	loreto	192.168.22.0	192.168.22.1	192.168.22.14	192.168.22.15

			Subred Sucursal	primer host	ultimo host	broadcast
34		valsequillo	192.168.22.16	192.168.22.17	192.168.22.30	192.168.22.31
35		queretaro	192.168.22.32	192.168.22.33	192.168.22.46	192.168.22.47
36		cancun	192.168.22.48	192.168.22.49	192.168.22.62	192.168.22.63
37		hermosillo	192.168.22.64	192.168.22.65	192.168.22.78	192.168.22.79
38		tampico	192.168.22.80	192.168.22.81	192.168.22.94	192.168.22.95
Sucursales USA						
39		los angeles	192.168.22.96	192.168.22.97	192.168.22.110	192.168.22.111
40		las vegas	192.168.22.112	192.168.22.113	192.168.22.126	192.168.22.127
41		phoenix	192.168.22.128	192.168.22.129	192.168.22.142	192.168.22.143
42		arlington	192.168.22.144	192.168.22.145	192.168.22.158	192.168.22.159
43		dallas	192.168.22.160	192.168.22.161	192.168.22.174	192.168.22.175
44		north houston	192.168.22.176	192.168.22.177	192.168.22.190	192.168.22.191
45		suth houston	192.168.22.192	192.168.22.193	192.168.22.206	192.168.22.207
						192.168.22.223
46		cobrica	192.168.22.208	192.168.22.209	192.168.22.222	192.168.22.239

INDICE DE FIGURAS

Figura 1.1 Redes 7
Figura 1.2 Conexión de CPUs 9
Figura 1.3 Diferentes topologías. 11
Figura 1.4 Redes y dispositivos de área local 12
Figura 1.5 Redes y dispositivos de área amplia 13
Figura 1.6 Modelo OSI 14
Figura 2.1 Introducción a TCP/IP 19
Figura 2.2 Comparación entre TCP/IP 20
Figura 2.3 Pila de protocolo TCP/IP 20
Figura 2.4 Capa de Aplicación 21
Figura 2.5 Sistema de denominación de dominio (DNS) 21
Figura 2.6 Descripción general de la capa de transporte 24
Figura 2.7 Formato del segmento TCP 25
Figura 2.8 Formato del segmento UDP 25
Figura 2.9 Números de puerto 26
Figura 2.10 Números de puerto TCP/UDP 27
Figura 2.11 Saludo de tres vías/conexión abierta TCP 28
Figura 2.12 Acuse de recibo simple TCP 29
Figura 2.13 Ventana deslizante TCP 29
Figura 2.14 Secuencia TCP y Números de acuse de recibo 30
Figura 2.15 Descripción general de la capa de red 31
Figura 2.16 El datagrama IP 32
Figura 2.17 El campo de protocolo 32
Figura 2.18 Protocolo de mensajes de control de Internet 33
Figura 2.19 Prueba de ICMP 34
Figura 2.20 Prueba de ICMP 34
Figura 2.21 Protocolo de resolución de direcciones 35
Figura 3.1 Una dirección IP está compuesta por 32 bits 37
Figura 3.2 Ejemplo de número binario a decimal 37
Figura 3.3 Asignación de bits a la parte de red y de host 39
Figura 3.4 Rango de direcciones IP valido 39
Figura 3.5 Determinar numero de host validos 40
Figura 3.6 Equivalentes decimales para mascara de red 42
Figura 3.7 Direccionamiento sin subred 43
Figura 3.8 Direccionamiento con subred 44
Figura 3.9 Mascara de subred 45
Figura 3.10 Cálculo de identificador de red. Red sin subredes 45
Figura 3.11 Cálculo de Identificador de subred 46
Figura 3.12 Cálculo de Identificador de Subred dividida en Subredes 46
Figura 3.13 Cálculo de Identificador de red, dirección de broadcast, primer y último host 47
Fig. 4.1Capa de Red Determinación de ruta. 48
Figura 4.2 Protocolo enrutado & protocolo de enrutamiento 50

Figura 4.3 Opciones de protocolo de red 50
Figura 4.4 Enrutamiento multiprotocolo 51
Figura 4.5 Rutas estáticas & rutas dinámicas 52
Figura 4.6 Ejemplo de enrutamiento estático 52
Figura 4.7 Ejemplo de enrutamiento por defecto 53
Figura 4.8 Operaciones de enrutamiento dinámico 55
Figura 4.9 Distancia en métrica 55
Figura 4.10 Clases de protocolos de enrutamiento 57
Figura 4.11 Tiempo de convergencia 57
Figura 4.12 Conceptos del vector de distancia 58
Figura 4.13 Problema: Loops de enrutamiento 59
Figura 4.14 Problema: Cuenta al infinito 60
Figura 4.15 Solución: Definición de un máximo 61
Figura 4.16 Solución: Horizonte dividido 62
Figura 4.17 Solución: Temporizadores de espera 63
Figura 4.18 Conceptos acerca del estado de enlace 63
Figura 4.19 Cambios de la topologia del estado de enlace 65
Figura 4.20 Aspectos que preocupan del estado del enlace 66
Figura 4.21 Problema: Actualizaciones del estado del enlace 67
Figura 4.22 Comparación del enrutamiento por vector de distancia y de estado de enlace 68
Figura 4.23 Enrutamiento híbrido 69
Figura 4.24 enrutamiento LAN a LAN 69
Figura 4.25 Enrutamiento de LAN y WAN 70
Figura 4.26 funciones de un Router 71

GLOSARIO

A

ACK: Ver acuse de recibo

ACL *(lista de control de acceso)**:*** Lista mantenida por un router de Cisco para controlar el acceso desde o hacia un router para varios servicios.

ADLS (asymmetric digital subscriber line)**:** Línea digital del suscriptor Asimétrica. Una de las cuatro tecnologías DSL

Aplicación: Programa que ejecuta una función directamente para un usuario. Los clientes FTP y Telnet son ejemplos de aplicaciones de red. ATM *(Modo de Transferencia Asíncrono):* Norma internacional para la retransmisión de celdas, en la cual se transmiten múltiples tipos de servicio (como voz, vídeo o datos), en celdas de longitud fija (53 bytes).

B

Banda ancha: Técnica de transmisión de alta velocidad y alta capacidad que permite la transmisión integrada y simultánea de diferentes tipos de señales (voz, datos, imágenes, etc.).

BPDU *(unidad de datos de protocolo de puente)**:*** Paquete Hello del protocolo SpanningTree (árbol- de extensión) -que se envía a intervalos configurables para intercambiar información entre los puentes de la red.

Broadcast: Paquete de datos enviado a todos los nodos de una red. Los broadcasts se identifican por una dirección broadcast. Comparar con multicast y unicast.

Búfer de memoria: Área de la memoria donde el switch almacena los datos destino y de transmisión.

Byte: Serie de dígitos binarios consecutivos que operan como una unidad (por ejemplo, un byte de 8 bits). Ver también bit. .

C

Capa de aplicación: Capa 7 del modelo de referencia 051. Esta capa brinda servicios de red para aplicaciones del usuario.

Capa de distribución: Capa en la que la distribución de los servicios de red se produce en múltiples LAN en un entorno de WAN. Esta es la capa en la que se encuentra la red báckbone de la WAN, normalmente basada en Fast Ethernet.

Capa de enlace: Ver capa de enlace de datos.

Capa de enlace de datos: Capa 2 del modelo de referencia. Esta capa proporciona un tránsito de datos confiable a través de un enlace físico.

Capa de presentación: Capa 6 del modelo de referencia OSI. Esta capa suministra representación de datos y formateo de códigos, junto con la negociación de la sintaxis de transferencia de datos.

Capa de red: Capa 3 del modelo de referencia OS!. Esta capa proporciona conectividad y selección de rutas entre dos sistemas finales.

Capa de sesión: Capa. 5 del modelo de referencia OSI. Esta capa establece, mantiene y administra las sesiones entre las aplicaciones.

Capa de transporte: Capa 4 del modelo de referencia OSI. Esta capa segmenta y reensambla los datos dentro de una corriente de datos. La capa de transporte tiene el potencial de garantizar una conexión y ofrecer transporte confiable.

Capa física: Capa 1 del modelo de referencia OSI. La capa física define las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico entre sistemas finales.

CSMA/CD *(Acceso múltiple con detección de portadora y detección de colisiones)**:*** Mecanismo de acceso a medios dentro del cual los dispositivos que están listos para transmitir datos primero verifican el canal en busca de una portadora.

CSU/DSU *(unidad de servicio de canal/unidad de servicio de datos)**:*** Dispositivo de interfaz digital que conecta el equipamiento del usuario final al par telefónico digital local.

D

Datagrama: Agrupamiento lógico de información enviada como unidad de capa de red a través de un medio de transmisión sin establecer previamente un circuito virtual.

DHCP: Protocolo de configuración dinámica del Host. Protocolo que proporciona un mecanismo para asignar direcciones ip de forma dinámica, de modo que las direcciones se pueden reutilizar automáticamente cuando los hosts ya no las necesitan.

Datagrama IP: Unidad fundamental de información transmitida a través de Internet.

DLCI *(identificador de conexión de enlace de datos)**:*** Valor que especifica un PVC o un SVC en una red Frame-Relay.

DNS *(Sistema de denominación de dominio)**:*** Sistema utilizado en Internet para convertir los nombres de los nodos de red en direcciones.

DoD *(Departamento de Defensa)**:*** Organización gubernamental de los EE.UU. responsable de la defensa nacional. El Departamento de Defensa ha financiado con frecuencia el desarrollo de protocolos de comunicación.

Dominio *(domain)**:*** Nombre empleado para referirse a una máquina o a un servidor determinado en Internet.

Dominio de broadcast: Conjunto de todos los dispositivos que reciben tramas de broadcast que se originan en cualquier dispositivo dentro de ese conjunto.

Dominio de colisión: En Ethernet, el área de la red en la que las tramas que colisionan se propagan. .

DSL (Digital Subscriber Une) *(Línea Digital del Suscriptor)***:** Tecnología de red que permite conexiones de banda ancha sobre el cable de cobre a distancias limitadas.

DTE *(equipo terminal de datos)***:** Dispositivo en el extremo del usuario de" una interfaz usuario a red que sirve como origen de datos, destino, o ambos.

E

Enlace WAN: Canal de comunicaciones de Wan que se compone de un circuito o ruta de transmisión y todo el equipo relacionado entre un emisor y un receptor.

Enrutamiento: Proceso de descubrimiento de una ruta hacia el host destino.

Enrutamiento Dinámico: que se ajusta automáticamente a la topología de la red o a los cambios de tráfico.

Enrutamiento Estático: Ruta que se ha configurado e introducido explícitamente en la tabla de enrutamiento.

Enrutamiento multiprotocolo: enrutamiento en el que un router entrega paquetes desde distintos protocolos enrutados, como TCP/IP e IPX, en los mismos enlaces de datos.

Ethernet: Es un estándar de redes de computadoras de área local con acceso al medio por contienda CSMA/CD. El nombre viene del concepto físico de ether. Ethernet define las características de cableado y señalización de nivel físico y los formatos de tramas de datos del nivel de enlace de datos del modelo OSI.

F

Full dúplex: Capacidad para la transmisión simultánea de datos entre la estación emisora y la estación receptora.

H

Host: Término usado en informática para referirse a los computadores conectados a la red, que proveen y/o utilizan servicios a/de ella. Los usuarios deben utilizar hosts para tener acceso a la red. En general, los hosts son computadores mono o multiusuario que ofrecen servicios de transferencia de archivos, conexión remota, servidores de base de datos, servidores WWW, etc. Los usuarios que hacen uso de los hosts pueden a su vez pedir los mismos servicios a otras máquinas conectadas a la red.

Hub: En general, dispositivo que sirve como centro de una topología en estrella.

I

ICMP: El Protocolo de Mensajes de Control de Internet o ICMP (por sus siglas de ***I****nternet* ***C****ontrol* ***M****essage* ***P****rotocol*) es el sub protocolo de control y notificación de errores del Protocolo de Internet (IP).

IGRP extendido (Protocolo de enrutamiento de gateway interior extendido)**:** Versión avanzada de IGRP desarrollada por Cisco.

Intercambio de señales: Secuencia de mensajes intercambiados entre dos o más dispositivos de red para garantizar la sincronización de transmisión antes de enviar datos del usuario.

Interfaz: Conexión entre dos sistemas o dispositivos. En terminología de enrutamiento, una conexión de red.

Internet: La internetwork de redes más grande del mundo, que conecta decenas de miles de redes de todo el mundo y con una cultura que se concentra en la investigación y estandarización basada en el uso real.

Internetwork: Industria dedicada a la conexión de redes entre sí. Este término se refierea productos, procedimientos y tecnologías. .

IOS *(Sistema Operativo de Internetwork)***:** Ver software Cisco lOS.

K

kb *(kilobit)***:** Aproximadamente 1.000 bits.

kB *(kilobyte)***:** Aproximadamente 1.000 bytes.

kbps *(kilobits por segundo)***:** Medida de velocidad de transferencia.

kBp *(kilobytes por segundo)***:** Medida de velocidad de transferencia. Kilobit: Ver kb.

kilobits por segundo: Ver kbps.

Kilobyte: Ver kB.

Kilobytes por segundo: Ver kBps.

L

LAN *(red de área local)***:** Red de datos de alta velocidad y bajo nivel de errores que cubre un área geográfica relativamente pequeña.

Latencia: Retardo entre el momento en que un dispositivo solicita acceso a una red y el momento en que se le concede el permiso para transmitir.

LLC *(control de enlace lógico):* La más alta de las dos subcapas de enlace de datos definidas por el IEEE. La subcapa LLC maneja el control de errores, control del flujo, entramado y direccionamiento de subcapa MAC.

LSA *(publicación del estado de enlace):* Paquete de broadcast utilizado por los protocolos del estado de enlace que contiene información acerca de vecinos y costos de ruta.

M

MAC *(Control de Acceso al Medio):* Parte de la capa de enlace de datos que incluye la dirección de 6 bytes (48 bits) del origen y del destino, y el método para obtener permiso para transmitir. .

Máscara: Ver máscara de dirección y máscara de subred.

Máscara de subred: Máscara utilizada para extraer información de red y subred de la dirección IP.

Máscara wildcard: Cantidad de 32 bits que se utiliza junto con una dirección IP para determinar qué bits en una dirección IP deben ser ignorados cuando se

compara dicha dirección con otra dirección IP. Una máscara wildcard se especifica al configurar una ACL.

Mb (megabit): Aproximadamente 1.000.000 de bits.

Megabits por segundo: Ver Mbps.

Megabyte: Ver MB.

Modelo de referencia de Internetwork de Sistemas Abiertos: Ver modelo de referencia OS1.

Modelo de referencia OSI *(Modelo de referencia de internetwork de sistemas abiertos):* Modelo de arquitectura de red desarrollado por ISO e UIT-T. El modelo está compuesto por siete capas, cada una de las cuales especifica funciones de red individuales, tales como el direccionamiento, el control de flujo, el control de errores, el encapsulamiento y la transferencia confiable de mensajes.

Módem: Contracción de modulador y demodulador.

MTU *(unidad máxima de transmisión):* Tamaño máximo de paquete, en bytes, que puede manejar una interfaz en particular.

Multicast: Paquetes únicos copiados por una red y enviados a un conjunto de direcciones de red. Estas direcciones están especificadas en el campo de dirección del destino.

N

Networking: Interconexión de estaciones de trabajo, dispositivos y periféricos.

NOS *(sistema operativo de red)***:** Sistema operativo utilizado para hacer funcionar una red, como, por ejemplo, NetWare de Novell y Windows NT.

O

OSI *(internetwork de sistemas abiertos)***:** Programa internacional de estandarización creado por ISO e UIT-T para desarrollar estándares de networking de datos que faciliten la interoperabilidad de equipos de varios fabricantes.

P

Ping *(búsqueda de direcciones de Internet)***:** Mensaje de eco ICMP y su respuesta. A menudo se usa en redes IP para probar el alcance de un dispositivo de red.

Protocolo: Descripción formal de un conjunto de normas y convenciones que establecen la forma en que los dispositivos de una red intercambian información.

Protocolo de árbol de extensión: Protocolo puente que utiliza el algoritmo de árbol de extensión, lo que habilita un puente de aprendizaje para funcionar dinámica mente en torno de bucles en una topología de red creando un árbol de extensión.

Protocolo de enrutamiento: Protocolo que logra el enrutamiento mediante la implementación de un protocolo de enrutamiento específico. Entre los ejemplos de protocolo de enrutamiento se incluyen IGRP, OSPF y RIP.

Protocolo de enrutamiento híbrido balanceado: Protocolo que combina aspectos de los protocolos de estado de enlace y por vector distancia.

Protocolo de enrutamiento por estado de enlace: Protocolo de enrutamiento en el cual cada router realiza un broadcast o multicast de información referente al costo de alcanzar cada uno de sus vecinos a todos los nodos de la internetwork de redes.

Protocolo de enrutamiento por vector distancia: Protocolo que utiliza el número de saltos en una ruta para encontrar la ruta al destino.

Protocolo enrutado: Protocolo que puede ser enrutado por el router.

Protocolo exterior: Protocolo utilizado para intercambiar información de enrutamiento entre redes que no comparten una administración común.

Protocolo interior: Protocolo utilizado para enrutar redes que se encuentran bajo una administración de red común.

Protocolo Internet: Cualquier protocolo que forme parte de la pila de protocolo TCP/IP.

R

Red empresaria: La red de una asociación comercial, agencia, escuela u otra organización que une sus datos, comunicaciones, informática y servidores de archivo.

Red interna: Red interna a la que tienen acceso los usuarios con acceso a la LAN interna de una organización.

Red plana: Red en la cual no hay routers ubicados entre los switches; los broadcasts y las, transmisiones de Capa 2 se envían a todos los puertos conmutados, y hay un dominio de broadcast que ocupa toda la red.

Repetidor: Dispositivo que regenera y propaga las señales eléctricas entre dos segmentos de red.

Router: Dispositivo de capa de red que usa una o más métricas para determinar cuál es la ruta óptima a través de la cual se debe enviar el tráfico de red.

S

Segmentación: Proceso de división de un solo dominio de colisión en dos o más dominios de colisión para reducir las colisiones y la congestión de la red.

Segmento: Sección de una red que está rodeada de puentes, routers o switches.

Sesión: Conjunto relacionado de transacciones de comunicaciones orientadas a conexión entre dos o más dispositivos de red.

Software Cisco IOS *(Sistema Operativo de Internetwork)***:** Software de sistema de Cisco que proporciona funcionalidad, escalabilidad y seguridad comunes a todos los productos bajo la arquitectura CiscoFusion.

T

TCP *(Protocolo de Control de Transmisión)***:** Protocolo de capa de transporte orientado a conexión que provee una transmisión confiable de datos de dúplex completo. TCP es parte de la pila de protocolo TCP/IP,

TCP/IP *(Protocolo de Control de Transmisión /Protocolo Internet)***:** Nombre común para el conjunto de protocolos desarrollados por el DoD de EE.UU. en los años '70 para promover el desarrollo de internetwork de redes a nivel mundial.

Telnet: Protocolo de emulación de terminal estándar de la pila de protocolo TCP/IP. Telnet se usa para la conexión de terminales remotas, permitiendo que los usuarios se registren en sistemas remotos V utilicen los recursos como si estuvieran conectados a un sistema local.

Token: Trama que contiene información de control. La posesión del token permite que un dispositivo de red transmita datos a la red.

Topología: Disposición física de los nodos y medios de red en una estructura de networking a nivel empresarial.

V

Ventana deslizante: Ventana cuyo tamaño se negocia dinámicamente durante la sesión TCP.

VLAN *(LAN virtual)***:** Grupo de dispositivos de una LAN que están configurados (usando el software de administración) de tal modo que se pueden comunicar

como si estuvieran conectados al mismo cable, cuando, en realidad, están ubicados en una serie de segmentos de LAN distintos.

W

WAN *(Red de área amplia)***:** Red de comunicación de datos que sirve a usuarios dentro de un área geográfica extensa y a menudo usa dispositivos de transmisión suministrados por carriers comunes.

BIBLIOGRAFIA

[1] Cisco Networking Academy Program
Semestre 1 Capítulo 2El modelo OSI
Fecha de consulta: 06-12-2009

[2] Cisco Networking Academy Program
Semestre Capítulo 3 Redes LAN
Fecha de consulta: 06-12-2009

[3] Cisco Networking Academy Program
Semestre 2, Capitulo9. TCP/IP
Fecha de consulta: 09-12-2009

[4] Cisco Networking Academy Program
Semestre 2, Capitulo10. Direccionamiento IP
Fecha de consulta: 09-12-2009

[5] Cisco Networking Academy Program
Semestre 2, Capitulo11.Enrutamiento
Fecha de consulta: 20-12-2009

[6] **Redes de computadoras
Andrew S. Tanenbaum
Prentices Hall
Cuarta Edición, 2003

[7] **Transmisión de datos y redes de comunicaciones
Behrouz A. Forouzan
Editorial Mc Graw Hill
Segunda edicion

[8] Artículo: Direccionamiento ip
Fuente: http://technet.microsoft.com/es-es/library/cc787434(WS.10).aspx
Fecha de consulta:9-12-2009

[9] Articulo: procedimiento para la creación de subredes
Fuente: http://aprenderedes.com/2006/07/04/procedimiento-para-la-creacion-de-subredes/
Fecha de consulta:9-12-2009

[10] Articulo: Routing-Basics
Fuente:http://www.cisco.com/en/US/docs/internetworking/technology/handbook/Routing-Basics.html
Fecha de consulta: 12-12-2009

[11] Articulo :IP
Fuente:http://docente.ucol.mx/al008363/public_html/IP.htm
Fecha de consulta12-12-2009

[12] Artículo: Tutorial tcpip
Fuente: http://tcpip.com.mx/soporte/tutorial_tcpip/index.html
Fecha de consulta:12-12-2009

[13] Artículo: TCP/IP
Fuente: http://www.saulo.net/pub/tcpip/
Fecha de consulta: 16-12-2009

[14] Artículo: Clases de direcciones ip
Fuente: http://www.info-ip.net/ip/Clases-de-direcciones-IP.php
Fecha de consulta:16-12-2009

[15] Articulo: tcp-ip
Fuente:http://www.uca.edu.sv/investigacion/tutoriales/tcp-ip.html
Fecha de consulta:16-12-2009