

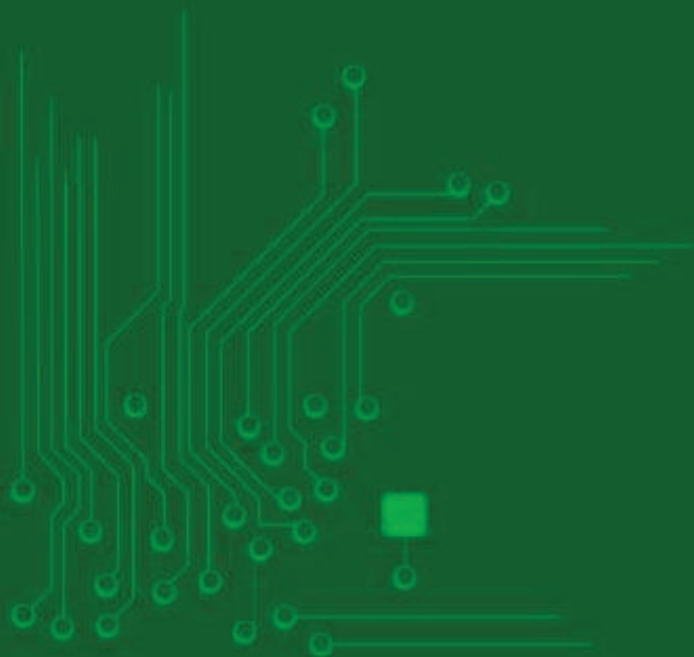
Biblioteca CCNA



Apunte rápido CCNA R&S

v5.0 CCNA 200-120

Oscar Antonio Gerometta



Biblioteca CCNA®

Apunte rápido CCNA R&S

CCNA 200-120

Versión 5.0

Oscar Antonio Gerometta

*Todos los derechos reservados.
Ninguna parte de este libro puede reproducirse o transmitirse
bajo ninguna forma o por ningún medio impreso, electrónico o
mecánico, ni por ningún sistema de almacenamiento y
recuperación de información sin permiso por escrito del autor.*

*Derechos reservados © 2013.
ISBN 978-987-27966-6-2:*

CCNA, CCNP, CCDA, CCDP, CCIP, CCVP, CCSP, CCIE, CCDE, Cisco, Cisco IOS, Aironet, BPX, Catalyst, Cisco Press, Cisco Unity, EtherChannel, EtherFast, EtherSwitch, Fat Step, GigaDrive, GigaStack, HomeLink, IP/TV, LightStream, Linksys, MGX, Networking Academy, Network Registrar, Packet, PIX, SMARTnet, StackWise, CallManager, CallManager Express, CCA, CNA, Cisco Systems, el logo de Cisco Systems, son marcas registradas o marcas de Cisco Systems Inc. y/o sus afiliados en los Estados Unidos y otros países. Toda otra marca mencionada en este documento es propiedad de sus respectivos dueños.

A todos aquellos alumnos que confían y confiaron en mí
para preparar su examen de certificación.
A quienes desde hacen años utilizan las diferentes versiones
que ha tenido este texto y han contribuido a su evolución.
A todos los que contribuyen permanentemente
al crecimiento de la comunidad CCNA.

Contenidos

Contenidos	7
Introducción	9
1. El Examen de certificación CCNA.....	13
2. Los Contenidos del examen de certificación	21
2.1. Principios de operación de redes TCP/IP.....	23
2.2. Direccionamiento IP (IPv4 / IPv6)	51
2.3. Operación de dispositivos Cisco IOS	71
2.4. Conmutación LAN.....	99
2.5. Enrutamiento IP	125
2.6. Servicios IP.....	147
2.7. Tecnologías WAN.....	177
Anexo 1: Guía de Comandos.....	195
Índice.....	207

Introducción

Las certificaciones respaldadas por diferentes actores de la industria de las TICs se han convertido en un elemento de referencia esencial en cuanto a los conocimientos y habilidades de quienes han de desempeñarse en tareas técnicas y gerenciales de las áreas de comunicaciones, tecnología, redes y sistemas.

Ahora bien, ¿Qué es una certificación?

Una certificación o calificación es una designación obtenida por una persona como resultado de un proceso pre-definido, generalmente un examen. La certificación puede ser utilizada como sinónimo de licencia, pero la licencia aplica solamente a personas y es exigida por la ley para desempeñar algunas tareas, mientras que la certificación es en términos generales, voluntaria.

La certificación de una persona indica que ese individuo tiene determinados conocimientos, destrezas o habilidades específicas de acuerdo al cuerpo de certificaciones de que se trate. Pero también algo más importante, la disposición personal a someterse a evaluaciones para demostrar y compartir sus conocimientos y habilidades; y por sobre todo la capacidad y aptitud necesaria para desarrollar un esfuerzo sistemático y prolongado con el objetivo de alcanzar un propósito concreto.

Si está leyendo este libro, es quizás porque su objetivo sea presentar el examen de certificación CCNA R&S.

En el universo de certificaciones actualmente disponibles, las elaboradas por Cisco Systems ocupan un lugar privilegiado. Y si bien el Cisco Career Certification se ha convertido en una maraña compleja de certificaciones y especializaciones, la certificación CCNA R&S sigue siendo la más conocida y en términos generales la puerta de acceso para la mayoría de los técnicos que aspiran a integrarse al universo Cisco.

La preparación de este examen de certificación constituye un verdadero desafío ya que se implementa una metodología propia y todavía desconocida para quienes desean aprobar el examen. Por este motivo se requieren elementos de ayuda que acompañen el proceso de estudio y preparación, y que despejen en buena medida las incógnitas que el examen mismo planteo al neófito.

Entre estas herramientas de estudio tienen un lugar muy importante las guías de preparación para el examen, y en este sentido recomiendo encarecidamente mi Guía de Preparación para el Examen de Certificación CCNA R&S v5.0, de próxima aparición. El libro que usted está leyendo ahora no es propiamente un texto de preparación para el examen. Es una síntesis, un resumen, especialmente preparado para quienes están estudiando y necesitan hacer un repaso rápido, o están preparando su examen de certificación. Puede ser también una guía de consulta cuando es necesario de modo rápido y claro encontrar un dato, un comando, una clasificación.

Es por esto importante hacer una advertencia: esta no es propiamente una guía de estudio para el examen CCNA R&S, su propósito es más humilde. Es una síntesis de los contenidos que es necesario conocer, y que permite tener una visión completa y sintética de los contenidos del examen.

En una guía de estudio Usted encontrará una colección de herramientas que no están presentes en este libro.

Sin embargo, este “apunte” tiene una indudable utilidad, comprobada a través de más de 12 años de trabajo acompañando la preparación de numerosos técnicos CCNA ya certificados. Ha tenido varios precedentes que pueden ser encontrados en Internet con el nombre de “Fast Track CCNA” o “Fast Note CCNA”. Ahora, esta tercer revisión del “Apunte Rápido CCNA ” es un complemento a la Guía de Preparación para el Examen de Certificación CCNA R&S 200-120 que aparecerá en los próximos meses.

¿Qué aporta esta nueva versión del Apunte Rápido?

El texto ha sido completamente renovado y reordenado para ajustarlo a lo requerido por el nuevo examen de certificación CCNA R&S 200-120. Se reorganizaron todos los contenidos, se suprimieron temas que han sido retirados del examen y se incorporaron aquellos que han sido incluidos en la actualidad. Por supuesto que también he corregido errores, incorporado gráficos y nuevas tablas, pero por sobre todo, se trata de un manual completamente nuevo y ajustado en función del nuevo examen de certificación CCNA R&S 200-120.

Es mi sincero deseo que sea una ayuda eficaz para todos aquellos que aspiran a obtener su certificación o están preparando su recertificación. Por este motivo, cualquier comentario, sugerencia o aporte que pueda hacer será de gran importancia para enriquecer las publicaciones sucesivas.

Además, y teniendo en cuenta que el examen de certificación es una realidad cambiante, desde el blog “Mis Libros de Networking” me ocuparé de brindar como desde ya varios años, información sobre cualquier novedad que surja respecto del examen.



Un texto de preparación para el examen de certificación: Guía de Preparación para el Examen de Certificación CCNA R&S, Oscar Gerometta, Ediciones EduBooks, 2013.



Para mantener actualizados estos materiales:
Blog “Mis Libros de Networking”: <http://librosnetworking.blogspot.com>
Correo electrónico: libros.networking@gmail.com
Con gusto recibiré su comentario en cualquiera de estas dos herramientas de trabajo.

El Autor

Oscar Antonio Gerometta es CCNA R&S / CCNA Sec / CCNA Wi / CCDA / CCSI / CCBF.

Con una larga trayectoria docente en esta área, ha sido el primer Cisco Certified Academy Instructor (CCAI) de la Región y responsable durante varios años de la Capacitación de la comunidad de Instructores CCNA de Cisco Networking Academy en Argentina, Bolivia, Paraguay y Uruguay.

Ha liderado numerosos proyectos e iniciativas como desarrollador de e-learning. Ha sido miembro del Curriculum Review Board de Cisco Networking Academy y uno de los docentes más reconocidos dentro del Programa en la Región Sud América Sur.

Desde el año 2000 brinda cursos de apoyo especialmente diseñados por él para quienes se preparan a rendir su examen de certificación CCNA, CCNA Sec, CCNA Wi, CCDA o CCNP, logrando entre sus alumnos un nivel de aprobación superior al 95%.

Es el autor de Principios Básicos de Networking para Redes Cisco IOS® y la Guía de Preparación para el Examen de Certificación CCNA®, partes de esta Biblioteca CCNA ® y también publicados por EduBooks.

1. El Examen de certificación CCNA

Para obtener la certificación CCNA R&S hay dos caminos posibles:

- Aprobando un único examen de certificación conocido en algunos ambientes como “Composite”: 200-120 CCNA
- Aprobando 2 exámenes independientes:

100-101 ICND1, que otorga la certificación CCENT.

200-201 ICND2, que completa el requerimiento para obtener la certificación CCNA R&S.

En ambos casos la certificación obtenida es siempre la misma: Cisco Certified Network Associate Routing & Switching, e incluye la certificación CCENT (Cisco Certified Entry Networking Technician) que es el pre-requisito para otros trayectos de certificación. El camino elegido no cambia en nada las certificaciones obtenidas.

Respecto de CCNA R&S la diferencia más notable entre ambos caminos o trayectos es que en el primer caso se evalúan en conjunto todos los objetivos de la certificación, mientras que cuando se opta por realizar dos exámenes estos objetivos se encuentran distribuidos entre las dos evaluaciones. En ambos casos se recibe también la certificación intermedia CCENT.



CCENT no es condición necesaria para acceder a CCNA R&S. Es posible rendir directamente el examen de certificación CCNA.

Si es pre-requisito obligatorio para otros CCNAs como son CCNA Security, CCNA Wireless, CCNA Voice, CCNA Service Provider Operations y CCDA.



Para obtener información oficial respecto de la certificación Cisco Certified Network Associate, visite el sitio oficial de Cisco:

<http://www.cisco.com/go/ccna>



Para obtener información oficial respecto de la certificación Cisco Certified Entry Networking Technician visite el sitio de Cisco:

<http://www.cisco.com/go/ccent>

Recertificación

Cisco Systems tiene una política de recertificación para cada una de sus certificaciones, lo que asegura el nivel de actualización de los técnicos certificados y la necesaria adecuación de los perfiles técnicos a las características cambiantes de las diferentes tecnologías de comunicaciones que se despliegan.

En el caso particular de CCNA R&S, Cisco otorga a la certificación una validez de 3 años, por lo que si se desea mantener el nivel adquirido es preciso recertificar antes de que se cumpla ese período de validez de 3 años.

La recertificación de CCNA R&S se puede obtener por cualquiera de los siguientes caminos:

- Aprobar solamente el examen ICND2 en la versión que se encuentre vigente al momento de recertificar.
- Aprobar cualquier examen de nivel asociado (CCNA Wi, CCNA Sec, etc.), excepto ICND1.
- Aprobar cualquiera de los exámenes de la serie 642. Estos exámenes son los que corresponden al nivel Professional (CCNP).
- Aprobar cualquiera de los exámenes de especialización (Cisco Specialist).
- Aprobar un examen escrito de nivel Expert (CCIE o CCDE).
- Aprobar la entrevista y el board review de CCAr (Cisco Certified Architect).

Hay que tener en cuenta que al obtener una certificación de nivel superior, mientras se mantenga actualizada esa certificación permanece actualizada la certificación CCNA R&S. En caso de que la certificación de nivel superior caduque, por cualquier motivo, de modo conjunto caduca la certificación CCNA R&S que se encontraba asociada, a menos que se recertifique por otro medio.

1.1. Las Características del Examen de Certificación

Como ya mencioné, la certificación CCNA R&S se puede obtener siguiendo 2 caminos diferentes pero igualmente válidos:

- Aprobando el examen de certificación 200-120 CCNA
- Aprobando 2 exámenes independientes:
 - 100-101 ICND1
 - 200-101 ICND2

Vamos entonces a revisar cada uno de estos exámenes:

Examen 200-120 CCNA – Cisco Certified Network Associate Exam

- También denominado CCNA Composite por reunir los temarios que abarcan los exámenes 100-101 y 200-101.
- Duración: 90 minutos.
Si toma este examen en inglés en países de lengua hispana, se otorgan 30 minutos adicionales para compensar el hecho de realizarlo en lengua no materna.



Cuando usted se acredite para rendir el examen de certificación, recibirá un correo electrónico de confirmación en el que, entre otras cosas se le informa que usted cuenta con 140 minutos para completar el examen: 20 minutos para el tutorial previo y 120 para el examen.



No se confunda, el tiempo no es acumulativo. Aunque usted utilice menos de 20 minutos para el tutorial, siempre tendrá los mismos 120 minutos para completar el examen.

- Cantidad de preguntas: entre 50 y 60.
Las preguntas son seleccionadas al azar a partir de una base de datos organizada según las áreas definidas en los objetivos. El volumen total de la base de datos es desconocido, pero es importante tener en cuenta que las preguntas se renuevan periódicamente.
Para ser claros, si bien los objetivos y contenidos del examen no varían las preguntas son periódicamente renovadas.
El conjunto de preguntas que componen el examen NO varían de acuerdo a las respuestas, sino que las preguntas del examen están completamente definidas al momento de iniciarlo.
- Idiomas en que se encuentra disponible: inglés y japonés.
Al momento de redactar esta versión del Apunte Rápido CCNA R&S no se ha anunciado una versión en español.
- Puntaje de aprobación: 825/1000.
El puntaje final y el asignado a cada pregunta pueden variar en cada examen individual. El sistema de puntuación se basa en una escala que va de 300 a 1000.
Cada pregunta tiene asignado en el sistema un puntaje. Al responder bien el Candidato suma en su score el puntaje asignado a la pregunta. Si responde mal, no se resta ningún puntaje sino que simplemente no suma los puntos correspondientes.
El alumno recibe 300 puntos por iniciar el examen y puede obtener como máximo 1000 puntos respondiendo con exactitud todas las preguntas.

El camino alternativo para obtener la certificación es rendir dos exámenes, el 100-101 ICND1 y el 200-101 ICND2. En este caso no se trata de una certificación diferente de la anterior, sino simplemente de otra forma de obtenerla.

Cisco no establece ningún orden obligatorio para rendir ambos exámenes, aunque la lógica indica que en un proceso de adquisición sistemática de conocimientos lo ordenado sería aprobar en primera instancia el examen ICND1 y luego el ICND2.



Rendir dos exámenes en lugar de uno es más costoso, pero hay que considerar que es más fácil aprobar dos exámenes más pequeños que uno solo más extenso. Sobre todo si no se tiene experiencia previa o no se ha cursado en una Academia o un Cisco Learning Partner.
Es una elección personal.
Tenga presente que este manual está preparado para ayudarlo a prepararse para el examen 200-120 CCNA Composite. Sin embargo, sus contenidos también incluyen todos los conocimientos necesarios para afrontar los exámenes 100-101 y 200-101.

Veamos en qué consiste cada uno de estos exámenes.

Examen 100-101 ICND1 – Interconnecting Cisco Networking Devices Part 1

- Certificación para la que acredita: CCENT.
- Duración: 90 minutos.
- Cantidad de pregunta: 40 a 50.
- Idiomas en que se encuentra disponible: inglés y japonés.
El sistema le asigna 30 minutos adicionales (un total de 120 minutos), por realizarlo en una lengua no materna.

Examen 200-101 ICND2 – Interconnecting Cisco Networking Devices Part 2

- Certificación para la que acredita: CCNA R&S.
- Duración: 75 minutos.
- Cantidad de preguntas: ente 50 y 60.
- Idiomas en que se encuentra disponible: inglés y japonés.

Si bien no se aclara formalmente en ninguno de los puntos referidos, tenga en cuenta las siguientes notas al momento de preparar su examen de certificación:

- Las preguntas referidas a switches, toman como modelo de referencia el switch Cisco Catalyst 2960.
- Las preguntas referidas a routers, toman como modelos de referencia a los routers Cisco Series Cisco 29xx.
- Las preguntas referidas a sistemas operativos, toman como referencia Cisco IOS 15.0 y siguientes.

Esto es de suma importancia ya que, las características, prestaciones y comandos varían sensiblemente de acuerdo al modelo de dispositivo y la versión de sistema operativo de la que se trate.



La mayoría de los simuladores que se ofrecen actualmente en el mercado para preparar el examen de certificación permiten armar topologías utilizando dispositivos como los mencionados.

El formato de las preguntas

En el momento en que usted se presente a rendir su examen de certificación y antes de comenzar con el examen propiamente dicho podrá recorrer un tutorial en

el que se explican los diferentes formatos de preguntas que ha implementado Cisco Systems para sus exámenes de certificación.

Sin embargo, al momento de prepararse para un examen es conveniente conocer previamente el formato que va a revestir el examen, los diferentes tipos de preguntas que pueden aparecer, y el modo en que cada una de ellas influye en la calificación final. Cuantas menos sorpresas en el momento del examen, mejor.

Cisco Systems utiliza en sus exámenes de certificación 6 formatos básicos de preguntas:

- Respuesta única a partir de opciones múltiples.
- Respuestas múltiples a partir de opciones múltiples.
- Respuestas drag & drop.
- Espacios en blanco para completar.
- Ejercicios de simulación.
- Simlets



Cisco ha publicado un tutorial en línea con los diferentes tipos de preguntas:

<http://www.cisco.com/go/tutorial>

Las preguntas de ejemplo son interactivas y es posible ensayar el modo de responder.

Tenga presente que en ese tutorial (como el que podrá recorrer en el momento en que se habilite su examen) se muestran 7 tipos de preguntas. Sin embargo en los exámenes de certificación CCNA R&S se implementan solo los 6 tipos mencionados.

1.2. El Procedimiento para Presentar el Examen

Los exámenes de certificación de Cisco Systems son administrados desde el año 2007 únicamente por Pearson VUE. Usted puede presentar su examen en cualquier Pearson VUE® Authorized Testing Center. Para verificar cuál es el Testing Center más cercano y la información de contacto pertinente, consulte la página web de la empresa.



La página web oficial de Pearson VUE®:

<http://www.vue.com>

Para presentar el examen de certificación propongo un sencillo proceso de 5 pasos:

1. Elija la fecha.

La fecha para presentar el examen es de su decisión y solamente depende de la disponibilidad del Testing Center en la fecha y horario que haya elegido.

2. Regístrese en el Testing Center.

Usted debe reservar su fecha de examen haciendo el registro en el Testing Center que ha elegido.

Tenga en cuenta que cada Testing Center tiene asignados días y horarios en los que puede habilitar exámenes. Consulte los horarios y formas de pago que hay disponibles. Puede verlos en la página web de Pearson VUE. También tenga en cuenta que en algunos Testing Center se requiere registrarse con cierta anticipación a la fecha. No deje este trámite para último momento y asegúrese su fecha de examen.

La fecha de registro puede ser modificada hasta 48 horas hábiles antes. Pasado ese lapso es inmodificable.

3. Los días inmediatamente anteriores al examen.

En la agenda de preparación hay que prever terminar el estudio del temario completo unos 10 días antes de la fecha fijada para el examen. Estos últimos 10 días son parte de la preparación pero tienen un propósito específico: repasar la integridad del temario y fijar los conocimientos.

Un buen recurso para realizar este repaso en estos 10 días anteriores al examen son los cuestionarios. Los cuestionarios no son una herramienta adecuada para el estudio inicial, pero sí son muy útiles para revisar los conocimientos y detectar puntos débiles en los últimos días antes del examen.

4. El día del examen.

Preséntese en el Testing Center con al menos 15 minutos de anticipación al horario fijado para el examen. No llegue sobre la hora. Debe estar tranquilo, relajado y concentrado en el examen que va a presentar.

Tenga en cuenta que debe presentar 2 documentos de identidad con foto. Esta es una condición para acreditación de identidad en los Testing Centers.



No lo olvide: debe acreditar su identidad presentando dos documentos con fotografía.

Mientras espera para ingresar al área de examen aproveche los últimos minutos para revisar los puntos que por experiencia ya sabe que recuerda menos: comandos, clasificaciones etc. En este momento es muy útil tener una hoja de repaso rápido. No es momento para cuestionarios o para conversar con amigos que hacen preguntas que nos pueden hacer dudar. Al examen hay que ingresar seguro y tranquilo.

Para ingresar al examen debe dejar todo elemento fuera. No puede ingresar con computadoras personales, calculadoras o cualquier otro elemento; ni aún con su propio papel y lápiz. El Testing Center le proveerá una tablilla y un marcador para que pueda realizar sus anotaciones.



Aunque es obvio: No se puede ingresar con calculadora o apuntes de cualquier tipo.



Un video ilustrativo del procedimiento puede ser revisado en:
http://youtu.be/y6WFmbw_RIA

5. El examen.

Una vez que ingresa a la sala del examen, el personal de administración del Testing Center habilitará la terminal en la que deberá realizar su evaluación, y le entregará una tablilla y un marcador para sus notas personales.

Tenga en cuenta que:


- El personal del Testing Center no tiene formación técnica, por lo que solamente puede brindarle asistencia y responder preguntas en lo que se refiere al funcionamiento del sistema.
- Si bien le entregan una sola tablilla y un marcador, si necesita más podrá solicitar durante el desarrollo del examen tablillas adicionales. Las tablillas debe entregarlas luego de terminado el examen y no podrá llevarse ninguna nota sobre el mismo.


El examen de certificación CCNA está compuesto de 3 elementos:

- El tutorial del examen.
Tiene asignado 20 minutos para recorrer el tutorial del examen de certificación. Como he señalado antes, este tutorial también está disponible en el sitio web de Cisco.
Al terminar de recorrer el tutorial o al finalizar los 20 minutos que tiene asignados para esto, si no lo hizo manualmente comenzará automáticamente el examen de certificación.
- La encuesta.
Se trata de una breve encuesta de marketing que releva información sobre su relación con el área del networking, tiempo y metodología de preparación que ha utilizado, información demográfica, etc.
Sus respuestas a esta encuesta no tienen ninguna influencia en la composición o resultados del examen y tienen un propósito meramente estadístico.
- El examen de certificación.
Recuerde que durante este tiempo sólo puede requerir asistencia para temas relacionados con el funcionamiento del sistema. No tiene disponible ningún recurso del entorno de base, ni tampoco calculadora o elementos de consulta.
Durante todo este tiempo tendrá en pantalla el reloj que marca el tiempo

restante para concluir el examen, adminístrelo de la mejor manera posible. Tenga en cuenta que no hay modo de saber antes del final cuántas simulaciones debe afrontar y de qué tipo. Al finalizar el examen aparecerá una pantalla de felicitación por haber completado la evaluación. Es el momento de avisarle al personal del Testing Center que finalizó.

Finalizado el examen, usted podrá ver el resultado del mismo en pantalla y el Testing Center imprimirá y le entregará una copia impresa de su “score report”.

 El score report es el único documento o registro de su examen con el que contará hasta tanto tenga habilitado su acceso al sitio web de Cisco para técnicos certificados, y reciba por correo su “kit CCNA”. Guarde su exam score con cuidado.

 Esta es la única información que podrá obtener respecto de su examen. Cisco no brinda la posibilidad de revisar las preguntas del cuestionario que usted realizó.

5. La recertificación.

La certificación CCNA tiene un período de validez de 3 años que se cuentan a partir del día en que rindió su examen de certificación.

Tenga presente la fecha y consulte con anticipación el sitio web de Cisco para verificar las condiciones de recertificación vigentes en ese momento.

2. Los Contenidos del examen de certificación

Vamos ahora a centrarnos en el estudio de los contenidos temáticos propios del examen de certificación.

Para esto he reunido los diferentes temas en 7 ejes temáticos que permiten una aproximación más sistemática y ordenada que el simple seguimiento de los objetivos enunciados por Cisco para el examen.

Los 7 ejes temáticos son:

1. Principios de operación de redes TCP/IP.
2. Direccionamiento IP (IPv4 / IPv6).
3. Operación de dispositivos Cisco IOS.
4. Conmutación LAN.
5. Enrutamiento IP.
6. Servicios IP.
7. Tecnologías WAN.

2.1. Principios de operación de redes TPC/IP

Una red es un conjunto de dispositivos y estaciones terminales interconectadas de modo que pueden comunicarse entre ellas.

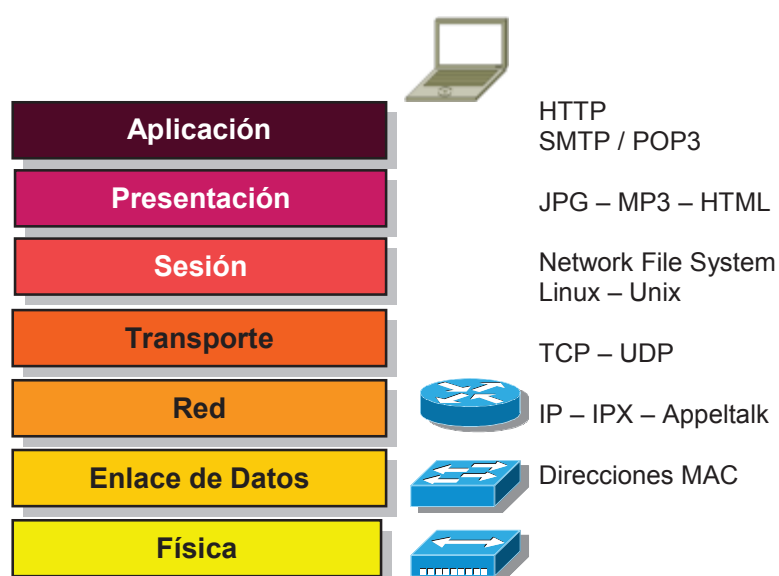
Sus componentes físicos más comunes son:

- Terminales.
Computadoras, impresoras, servidores, cámaras IP, teléfonos IP, etc.
- Elementos de interconexión:
 - Placas de red (NIC).
 - Medios de red.
Cables de cobre o fibra óptica, inalámbricos.
 - Conectores.
- Switches.
- Routers.
- Dispositivos inalámbricos.

Introducción a los modelos de referencia

Modelo OSI

Es el modelo de arquitectura primaria para redes. Describe cómo los datos y la información de la red fluyen desde una terminal, a través de los medios de red, hasta otra terminal.



Divide el proceso global en grupos lógicos más pequeños de procesos a los que denomina “capas” o “layers”. Por este motivo se habla de una “arquitectura de capas”.

7	Aplicación	<p>Suministra servicios de red a los procesos de aplicaciones de usuario que están fuera del modelo OSI.</p> <p>Determina la identidad y disponibilidad de la contraparte en la comunicación; e implementa procedimientos de autenticación de usuario, recuperación de errores y control de integridad.</p>
6	Presentación	<p>Garantiza que la información que es enviada desde la capa de aplicación del origen es legible por la capa de aplicación del dispositivo destino.</p> <p>También puede ocuparse de encriptar los datos que se enviarán a través de la red.</p>
5	Sesión	<p>Establece, administra y termina sesiones entre dos nodos de comunicación. También sincroniza el diálogo entre las capas de presentación de ambas terminales.</p>
4	Transporte	<p>Segmenta, transfiere y reensambla los datos que corresponden a una comunicación entre dispositivos terminales.</p> <p>Para asegurar una transferencia de datos confiable establece, mantiene y termina circuitos virtuales.</p> <p>Detección de fallos, control de flujo de la información y recuperación de errores son algunas de sus funciones.</p> <p>PDU: Segmento.</p>
3	Red	<p>Provee conectividad y selección de la ruta entre dos dispositivos terminales que pueden estar ubicados en diferentes redes.</p> <p>Direccionamiento lógico.</p> <p>PDU: Datagrama o paquete.</p> <p>Dispositivos que operan en esta capa: routers, switches multilayer.</p>
2	Enlace de Datos	<p>Define el formato que ha de darse a los datos para ser transmitidos, y cómo se controla el acceso a la red.</p> <p>Direccionamiento físico.</p> <p>PDU: Trama.</p> <p>Dispositivos que operan en esta capa: switches LAN, bridges.</p>

1 Física	Define las especificaciones eléctricas, mecánicas y funcionales necesarias para activar, mantener y desactivar un enlace físico utilizado para la transmisión de bits entre dispositivos. Dispositivos que operan en esta capa: hubs.
----------	--

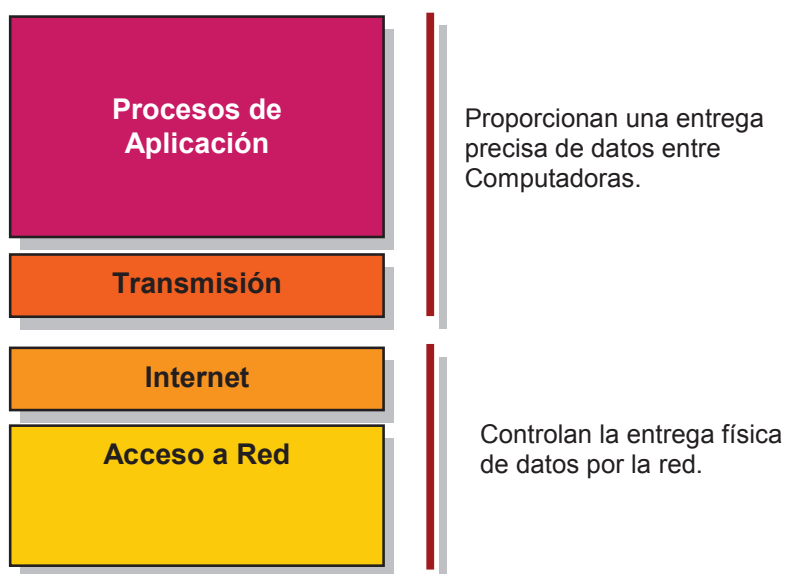
Modelo TCP/IP

El modelo TCP/IP es un modelo en capas desarrollado inicialmente para facilitar el establecimiento de comunicaciones extremo a extremo.

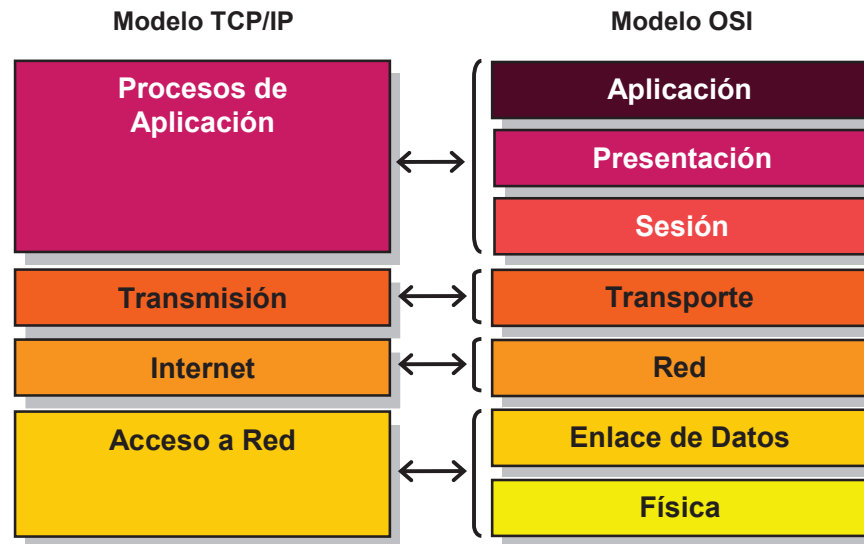
Es el modelo de aplicación en Internet. Por este motivo es el más difundido, y muchos de los protocolos originales de Internet refieren a este modelo de capas. En la actualidad sigue siendo de gran aplicación, aunque en términos generales se prefiere el modelo OSI para el estudio y análisis.

Más allá de su utilidad como modelo, también se suele denominar TCP/IP a un conjunto de protocolos que trabajan a partir de la implementación del protocolo TCP en capa de transporte y el protocolo IP en la capa de Internet.

- **Capa de Aplicación**
En ella se desarrollan procesos de alto nivel referidos a la presentación, codificación y control del diálogo.
- **Capa de Transporte**
Proporciona servicios de transporte de datos entre origen y destino creando un circuito virtual entre esos dos puntos. En esta capa se segmentan y reensamblan los datos, y se implementan servicios de control de flujo y secuenciación con acuses de recibo para controlar el flujo de datos y corregir errores en la transmisión.
- **Capa de Internet**
Su objetivo es proporcionar direccionamiento jerárquico y encontrar la mejor ruta entre origen y destino.



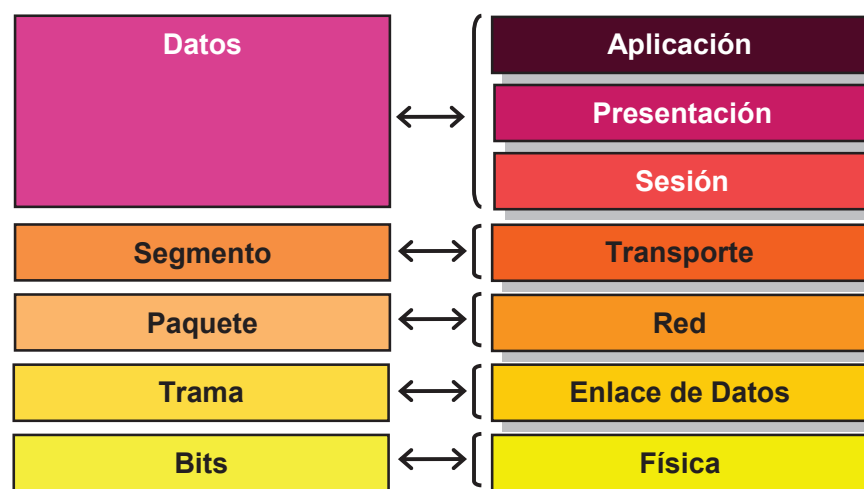
- **Capa de Acceso a Red**
También llamada de Host a Red. Controla todos los aspectos relacionados al enlace físico con los medios de red. Define la interfaz con el hardware de red para tener acceso al medio de transmisión.



Encapsulación / Desencapsulación

Cada capa del modelo OSI en el dispositivo origen debe comunicarse con su capa homóloga (par o peer) en el destino.

Durante el proceso de transporte ente origen y destino, los protocolos de cada capa deben intercambiar bloques de información que reciben la denominación de unidades de datos del protocolo (PDU).

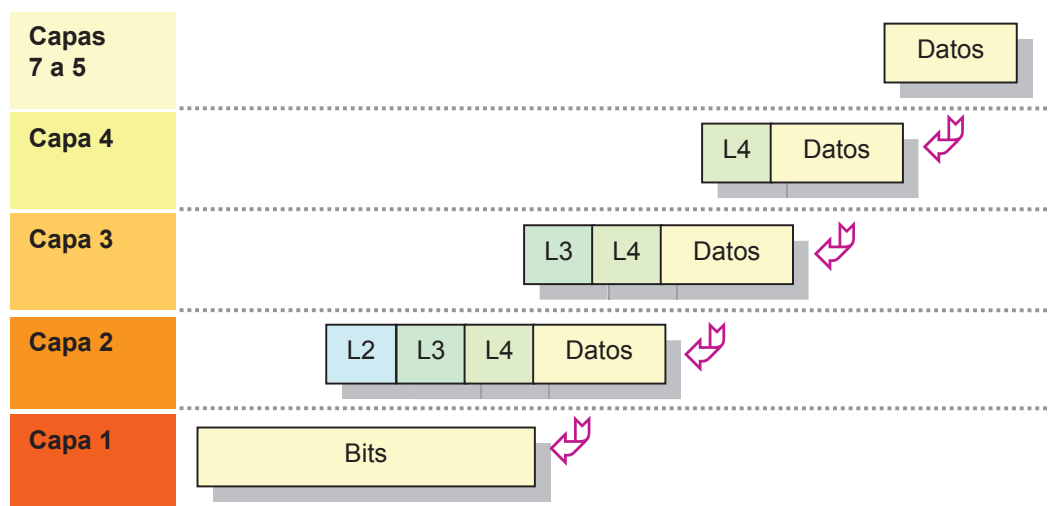


Cada capa depende de su capa inferior en el dispositivo origen para poder establecer el intercambio con su capa par en el destino. Para esto cada capa encapsula el PDU que recibe de la capa superior con un encabezado que incorpora la información que corresponde a su nivel de acuerdo al protocolo que está implementando.

Cada encabezado contiene información de control para los dispositivos que componen la red y para que el receptor pueda interpretar correctamente la información que recibe.

Este proceso se completa siguiendo cinco pasos básicos:

1. En las capas superiores del modelo OSI se convierte la información del usuario en datos. Las capas superiores agregan la información correspondiente a los protocolos involucrados.
2. En la capa de transporte se preparan los datos para el transporte end-to-end. Son fragmentados en segmentos y encapsulados con información de control para lograr una conexión confiable.
3. En la capa de red se agregan las direcciones lógicas de origen y destino en el encabezado de red. Los datos son colocados dentro de un paquete datagrama.
4. En la capa de enlace de datos se agregan las direcciones físicas en el encabezado de enlace de datos y se conforma la trama para su transmisión a través de una interfaz y los medios físicos.
5. Finalmente, los datos se transmiten en forma de bits a través de los medios físicos.



Cuando la información es recibida en el destino se realiza el proceso inverso, desde la capa física hacia la capa de aplicación, analizando en cada paso la capa

correspondiente al protocolo que ha operado en ese nivel que está contenida en el encabezado correspondiente.

Capa física del modelo OSI

En los dispositivos terminales se requiere un componente de hardware que es la interfaz de red (NIC) que conecta a la terminal con la red. Además de la placa de red y asociado a la misma, se requiere un IRQ, una dirección I/O, un driver de software y un espacio de memoria.

Se utilizan diferentes medios de transporte de la señal:

- Alambres de cobre.
- Filamentos de fibra óptica.
- Transmisión de radiofrecuencia sobre el medio atmosférico.

Medios de cobre

- Cable coaxial.
 - Thicknet o cable coaxial grueso.
Redes Ethernet 10Base5.
 - Tinte o cable coaxial fino.
Redes Ethernet 10Base2.
- Cable de par trenzado de cobre.
 - UTP.
 - STP.
 - FTP.

Cable de par trenzado de cobre

Cable especialmente diseñado para redes de comunicaciones que combina técnicas de blindaje y cancelación de ruido eléctrico que permiten controlar el problema de interferencias electromagnéticas.

Se compone de 8 hilos (4 pares) de alambre de cobre revestidos cada uno con una vaina aislante de plástico de diferente color y trenzados de a pares para lograr el efecto de cancelación y blindaje que le permite rechazar interferencias.

Hay diferentes categorías de UTP:

- Cat.3 – Apto para redes 10Base-T.

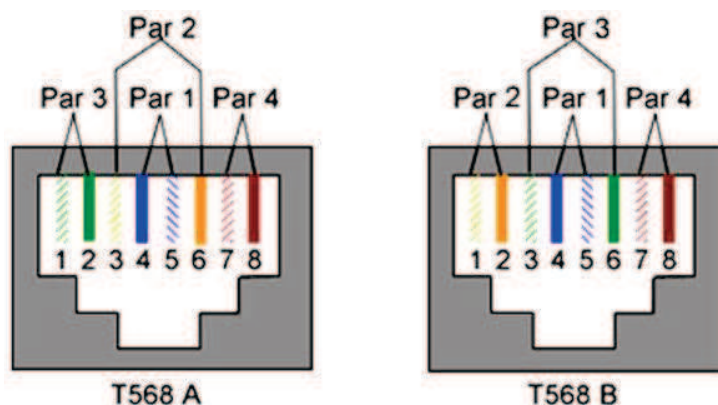
- Cat. 5 – Apto para transmisiones de hasta 100 Mbps con segmentos de 100 m. de cable.
- Cat. 5e – Apto para instalaciones de hasta 1 Gbps, con longitudes de hasta 100 m. por segmento de cable.
- Cat. 6 – Sugerido para redes de 1 Gbps.
- Cat. 6a – Apto para redes de hasta 10 Gbps; mantiene la posibilidad de trabajar con segmentos de cables de hasta 100 m.

Conectorizado RJ-45

Estándar para el conectorizado originalmente utilizado en el cableado telefónico que especifica las características físicas de los conectores macho y hembra, al mismo tiempo que la asignación de los diferentes cables que componen el UTP.

Utiliza conectores 8P8C que por extensión reciben el nombre genérico de RJ-45.

La asignación de los cables utilizados en sistemas Ethernet está definida por el estándar EIA/TIA-568-B que establece dos formatos básicos para el armado de fichas RJ-45: T568 A y T568 B.

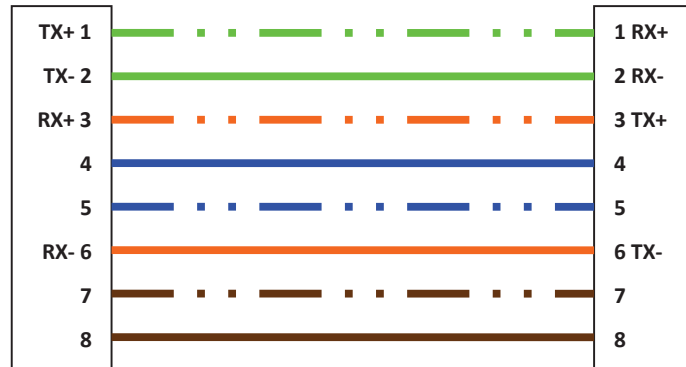


En cualquiera de estos esquemas, cuando se trata de redes Ethernet 10BaseT y 100BaseT, sólo se utilizan los pares verde y naranja para la transmisión de datos. En sistemas Ethernet de Gigabit, se utilizan los 4 pares.

A partir de estos 2 formatos básicos se pueden armar diferentes tipos de cable para distintos usos.

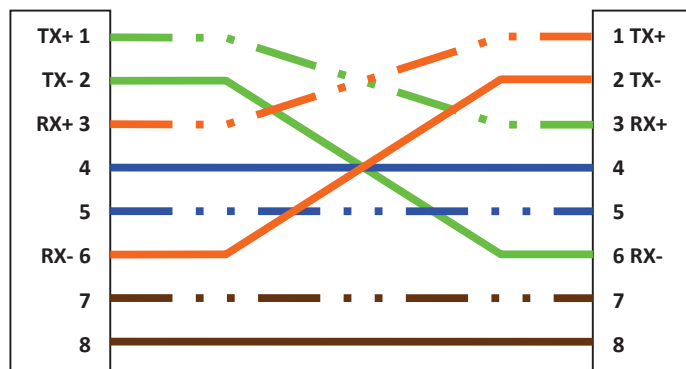
Los distintos tipos de cable se diferencian por el formato utilizado en cada uno de sus extremos:

- **Cable Derecho**
Utiliza el mismo formato en ambos extremos del cable. Puede ser tanto 568 A como 568 B.

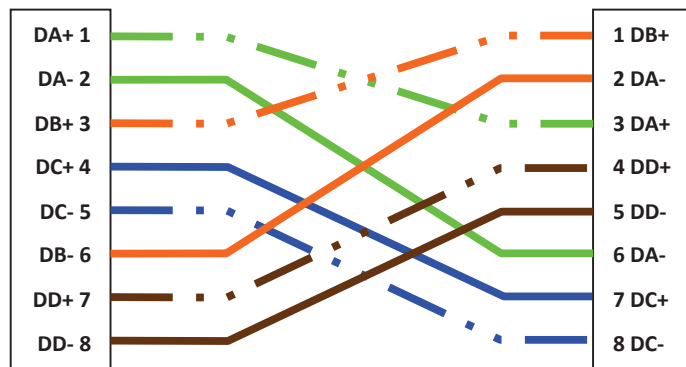


- **Cable Cruzado**
Utiliza diferente formato en ambos extremos del cable.
En sistemas Ethernet 10BaseT y 100BaseT se cruzan los pines 1-2 en un extremo con los 3-6 en el otro; y los pines 3-6 del primer extremo con los 1-2 del otro.

Cable cruzado FastEthernet



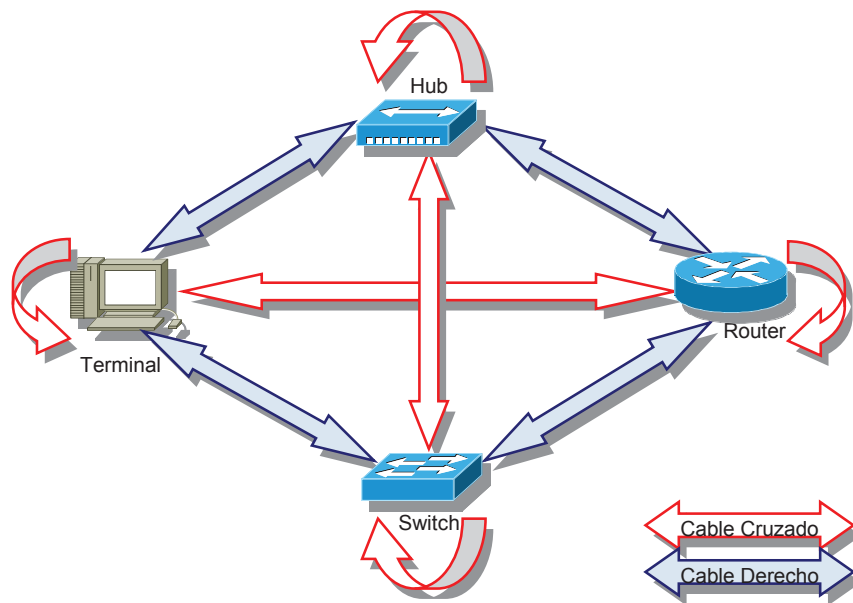
Cable cruzado GigabitEthernet



En sistemas GigabitEthernet, a lo anterior se requiere sumar que los pines 4-5 de un extremo se crucen con los 7-8 en el otro, y los pines 7-8 del primer extremo con los 4-5 del otro.

- **Cable Consola**
En este caso el orden de los alambres en un extremo del cable es el espejo exacto del otro extremo. El pinado en ambos extremos es inverso: 1-2-3-4-5-6-7-8 en un extremo, 8-7-6-5-4-3-2-1 en el otro.

Implementación de cables UTP cruzados o derechos



El uso adecuado de cada tipo de cable es el siguiente:

- **Cable Derecho:**
 - Router a hub o switch.
 - Servidor a hub o switch.
 - Estación de trabajo a hub o switch.
- **Cable Cruzado:**
 - Uplinks entre switches.
 - Hubs a switches.
 - Hub a hub.
 - Puerto de un router a otro puerto de un router.

- Conectar dos terminales directamente.
- Cable Consola:
 - Conectarse al Puerto consola de un dispositivo.

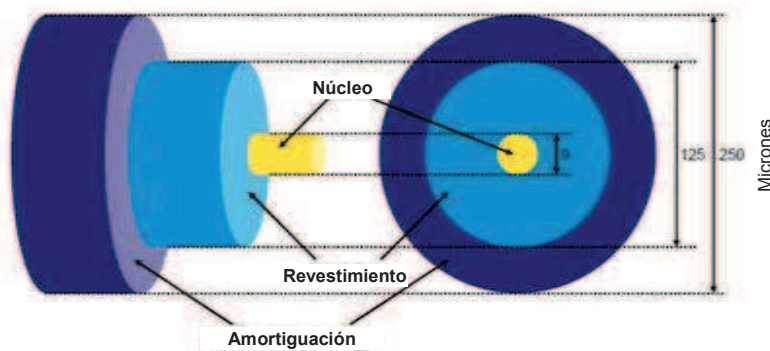
A partir de la implementación de la detección automática de la electrónica de las interfaces (Auto-MDIX), en muchos casos el mismo dispositivo adapta sus puertos haciendo innecesaria la utilización de cables cruzados.

Medios de fibra óptica

El medio de transmisión comúnmente denominado “fibra óptica” permite conexiones de alto ancho de banda a mayores distancias debido a que sufre menos atenuación y es inmune al ruido electro-magnético.

Es una pieza compleja compuesta básicamente de 5 elementos:

- Núcleo de vidrio o silicio, que es propiamente el elemento transmisor. Actúa como una guía de onda que transmite la luz entre los puntos conectados. Su diámetro varía en los diferentes tipos de fibra.
- Revestimiento o blindaje, compuesto por material similar al núcleo pero con diferentes propiedades ópticas, lo que asegura que el haz de luz quede confinado dentro del núcleo. Su diámetro estándar es de 125 micrones.
- Una capa de material amortiguador o buffer, que brinda protección al revestimiento y al núcleo que son muy frágiles.



Cada circuito de fibra óptica está compuesto por 2 hilos de fibra, cada uno de ellos destinado a establecer la comunicación en un sentido, asegurando de esta manera una comunicación bidireccional.



Hay 2 tipos básicos de fibra óptica a considerar:

- **Fibra Multimodo.**
Es utilizada mayormente para distancias cortas con menores anchos de banda.
Tiene un core de 50 o 62,5 micrones de diámetro lo que permite múltiples caminos posibles del haz de luz entre origen y destino.
- **Fibra Monomodo.**
Es la preferida para cubrir distancias extensas.
Tiene un core de 9 micrones de diámetro, lo que reduce a uno solo el camino posible del haz de luz.

La señal eléctrica es convertida en señal lumínica utilizando una fuente de luz. Hay dos tipos de fuentes de luz:

- **LED.**
Son emisores de energía de baja potencia y baja velocidad. Esto también significa menor distancia de alcance.
Hay 2 tipos de LEDs disponibles: SLED y ELED.
- **Emisores láser.**
Permiten cubrir mayores distancias. Tienen haces de luz más estrechos y mejor enfocados, por lo que suelen utilizarse con fibra monomodo.
Hay varios tipos de emisores láser: FP, DFB y VCSEL.
Como requieren un proceso de fabricación más complejo, son de mayor costo.

Conectorizado de fibra óptica

Hay múltiples tipos de conectores posibles para utilizar, los que varían básicamente en su tamaño y el método mecánico de acople al puerto.

Hay conectores metálicos o de material plástico, que se acoplan al puerto por presión, o utilizando el método bayoneta. Adicionalmente hay conectores simplex (de un solo pelo de fibra) o dúplex (de dos pelos de fibra).

Los conectores simplex más frecuentes son ST, SC o FC. Los conectores dúplex habituales son: FDDI, SC dúplex y ESCON.

La tendencia es la implementación de conectores SFF que, si bien no son una solución estándar, permiten mayor densidad de puertos. Hay múltiples conectores diferentes disponibles. Uno de los más populares es el MT-RJ debido a que utiliza un espacio semejante al del cableado estructural convencional. Otros conectores de este tipo son el Volition, el LC, el Opti-Jack, MU, etc.



Fibra multimodo: Cable color naranja / LEDs como emisores.



Fibra monomodo: Cable color amarillo / láser como emisores.

Medios inalámbricos

Con el término “inalámbrico” (wireless) se comprende un conjunto muy amplio de tecnologías inalámbricas que utilizan básicamente señales de radio frecuencia para la transmisión de datos.

Entre las principales tecnologías wireless se pueden mencionar:

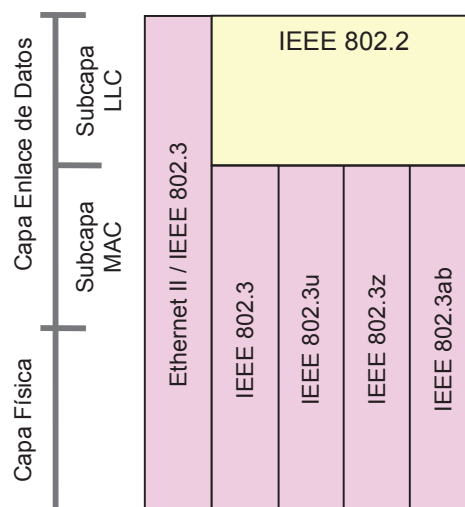
- **Satélite**
Tiene gran cobertura, pero con retardos muy altos que lo hacen inadecuado para utilizar con aplicaciones sensibles al delay.
Ventaja comparativa: cobertura geográfica.
- **Wireless LAN por onda corta**
Utiliza emisiones de radiofrecuencia de onda corta. Permite trabajar a distancias considerables pero con anchos de banda muy bajos.
- **Wireless LAN infrarroja (IR)**
Brinda importante ancho de banda en distancias muy cortas.
Ventaja comparativa: conexión PDA to Laptop o Laptop to Laptop.
- **Wireless LAN con microondas**
Utiliza la emisión de radiofrecuencia de 2.4 o 5 GHz de acuerdo a varios estándares en uso actualmente. Es la tecnología más difundida en la actualidad.

La Arquitectura Ethernet

Con el término Ethernet se suele referenciar a una familia de tecnologías LAN comprendidas actualmente en el estándar IEEE 802.3

Ethernet es originalmente una tecnología propietaria desarrollada por Digital, Intel y Xerox (DIX) en la década de 1970 y que luego fue estandarizada por la IEEE a través de la comisión 802.3 a mediados de la década de 1980. Si bien hay diferencias, básicamente Ethernet e IEEE 802.3 son tecnologías compatibles y muy semejantes.

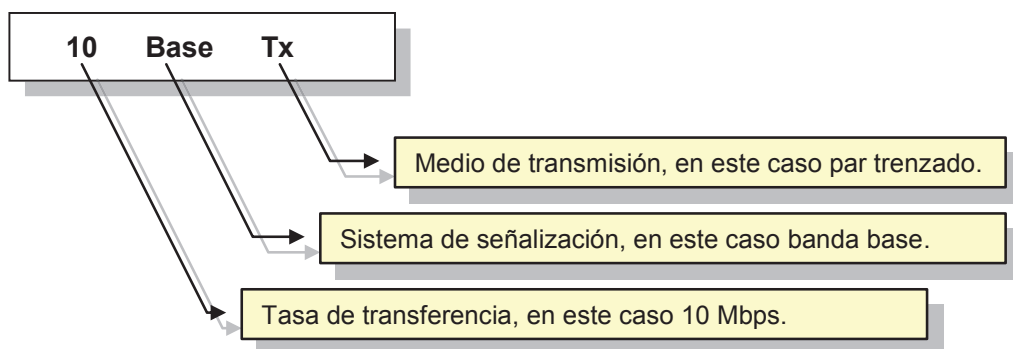
Esta tecnología se ubica también dentro del modelo OSI:



- La Subcapa LLC.
Proporciona mayor flexibilidad para implementar múltiples servicios de capa de red sobre una amplia variedad de tecnologías de las capas inferiores.
- La subcapa MAC.
Se ocupa del acceso al medio físico. Aquí se define la dirección MAC.

Nomenclatura y estándares

A las tecnologías Ethernet se aplica una terminología estándar establecida por la IEEE, que permite identificar fácilmente varias características de cada una de ellas



La nomenclatura de los diferentes medios es la siguiente:

- T – Cable de par trenzado.
- S – Cable de fibra óptica multimodo de corto alcance.
- L – Cable de fibra óptica monomodo o multimodo de largo alcance.

La segunda letra indica la codificación utilizada:

- X – Codificación 4B/5B para FastEthernet u 8B/10B para GigabitEthernet.
- R – Codificación 64B/66B.

Estándar	Sub Capa MAC	Medio Físico	Distancia Máxima	Observaciones
10Base 2	802.3	Cable coaxial de 50 ohm RG-58 con conector BNC.	185 m.	Conectores AUI. Topología en bus serial. Solo opera half-dúplex.
10Base 5	802.3	Cable coaxial de 50 ohm. Utiliza interfaces AUI.	500 m.	Solo opera half-dúplex.
10BaseF	802.3	Denominación genérica para referirse a tecnologías Ethernet de 10 Mbps sobre cables de fibra óptica.		

Estándar	Sub Capa MAC	Medio Físico	Distancia Máxima	Observaciones
10BaseFB	802.3	Fibra óptica	2.000 m.	Provee cableado de backbone. No soporta dispositivos DTE.
10BaseFL	802.3	Fibra óptica	2.000 m.	Provee cableado de backbone. No soporta DTE.
10BaseFP	802.3	Fibra óptica	500 m.	Permite establecer terminales en una topología de estrella.
10BaseT	802.3	UTP cat. 3, 4, 5 o 5e, con conectores RJ-45.	100 m.	Topología en estrella. Utiliza 2 pares de cables de un cable de par trenzado. Opera half o full-dúplex.
100BaseFX	802.3u	Dos hilos de fibra óptica multimodo de 62.5/125 micrones	412 m.	Conectores ST o SC. Topología en estrella.
100BaseT4	802.3u	Cable UTP cat. 3, 4 ó 5	100 m.	Utiliza los 4 pares de cables. No son posibles conexiones full dúplex.
100BaseTX	802.3u	Cable UTP cat. 5, 5e, 6 ó 7 ó STP cat. 1, con conectores RJ-45.	100 m.	FastEthernet. Topología de estrella. Utiliza 2 pares de cables. Opera half o full-duplex
1000BaseT	802.3ab	UTP cat. 5e o 6, con conector RJ-45	100 m.	Utiliza los 4 pares de cables para generar 4 circuitos de transmisión full-dúplex paralelos.
1000BaseCX	802.3z	Par trenzado de cobre blindado con conectores RJ-45, o coaxial balanceado de 150 Ohm. con conector mini-DB9	25 m.	Diseñado para cubrir pequeñas distancias entre servidores. Topología en estrella.
1000BaseSX	802.3z	Fibra óptica multimodo de 62.5 / 125 micrones con conectores SC	220 m.	Utiliza un emisor láser de 850nm. Opera como full-dúplex.
		Fibra óptica multimodo de 50 / 125 micrones con conectores SC	550 m.	Utiliza un LED emisor. Topología en estrella. Opera como full-dúplex.
1000BaseLX	802.3z	Fibra óptica Multimodo o Monomodo de 9/125 micrones	Multimodo 550 m. Monomodo 10 km.	Utiliza un emisor láser de 1310 nm. Topología en estrella. Opera como full-dúplex.

Estándar	Sub Capa MAC	Medio Físico	Distancia Máxima	Observaciones
10GBaseSR	802.3ae	Fibra óptica multimodo de 62,5 o 50 micrones	62,5 mic. 82 m. 50 mic. a 300 m.	
10GBaseLR	802.3ae	Fibra monomodo de 9 micrones	25 km.	
10GBaseT	802.3an	UTP o STP cat. 6a con conectores RJ-45	100 m.	
40GBase	802.3ba	Fibra monomodo	10 km.	
		Fibra multimodo	100 m.	
		UTP	7 m.	
100GBase	802.3ba	Fibra monomodo	40 km.	
		Fibra multimodo	100 m.	
		UTP	7 m.	

Elementos comunes:

Lo que caracteriza y define la pertenencia a la familia de estándares Ethernet, es un conjunto de elementos comunes que aseguran la compatibilidad entre ellos.

Estos elementos comunes son:

- Estructura de la trama.
- Dimensiones de la trama:
- Mínima (64 bytes).
- Máxima (1518 bytes).
- Método de acceso al medio: CSMA/CD. Se utiliza solamente en conexiones half dúplex.
- Requerimiento de un slot time para conexiones half dúplex.

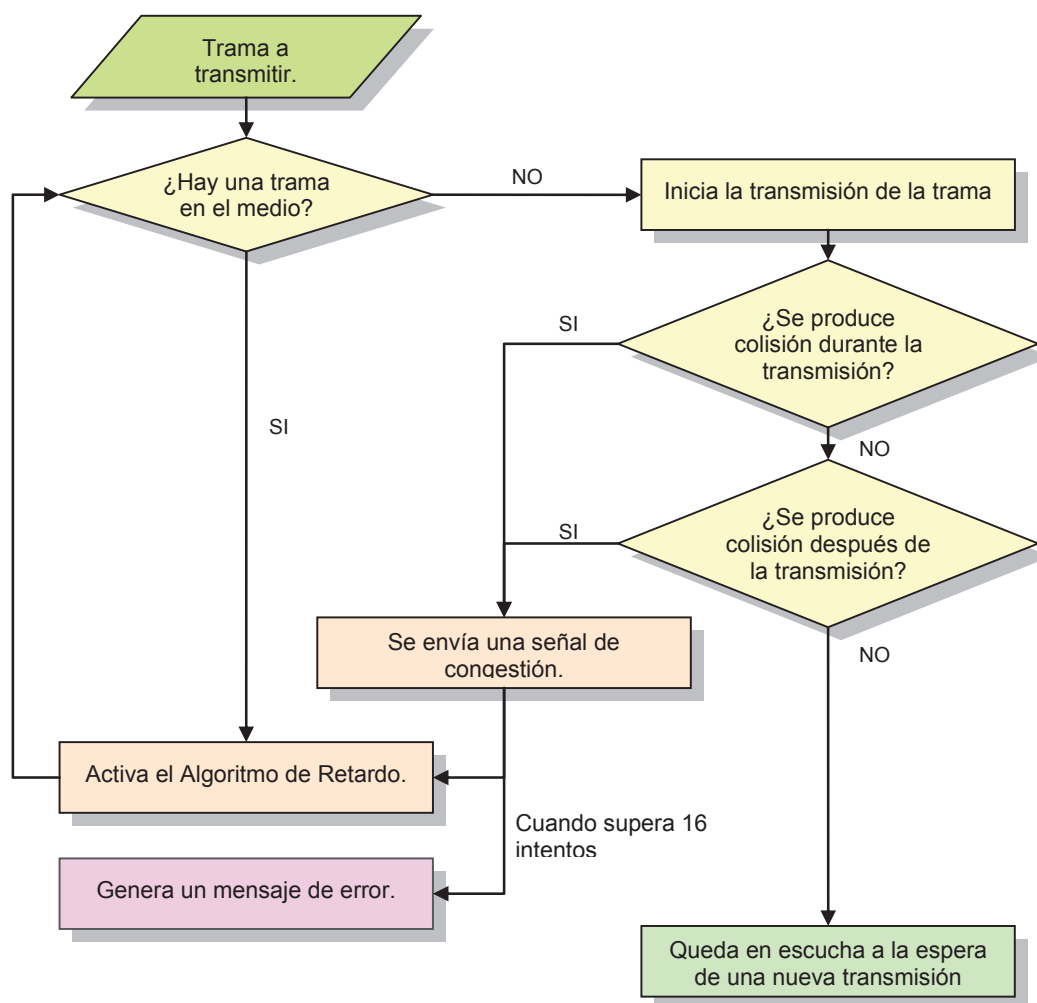
El protocolo CSMA/CD

La clave de la operación de Ethernet en medios compartidos es el protocolo CSMA/CD.

CSMA/CD es el protocolo que administra los procedimientos de acceso al medio, o lo que es lo mismo, administra la señal portadora sobre el medio físico.

Su operación supone:

- No existen prioridades, por lo tanto todos los nodos conectados al medio físico compiten por el acceso al medio.
- Puede ocurrir que 2 o más nodos intenten el envío al mismo tiempo, lo que dará lugar a una colisión.
- Una colisión daña la transmisión, por lo que los nodos involucrados deberán reenviar la información.
- Las estaciones deben ser capaces de detectar una colisión.



La operación de este protocolo puede describirse así:

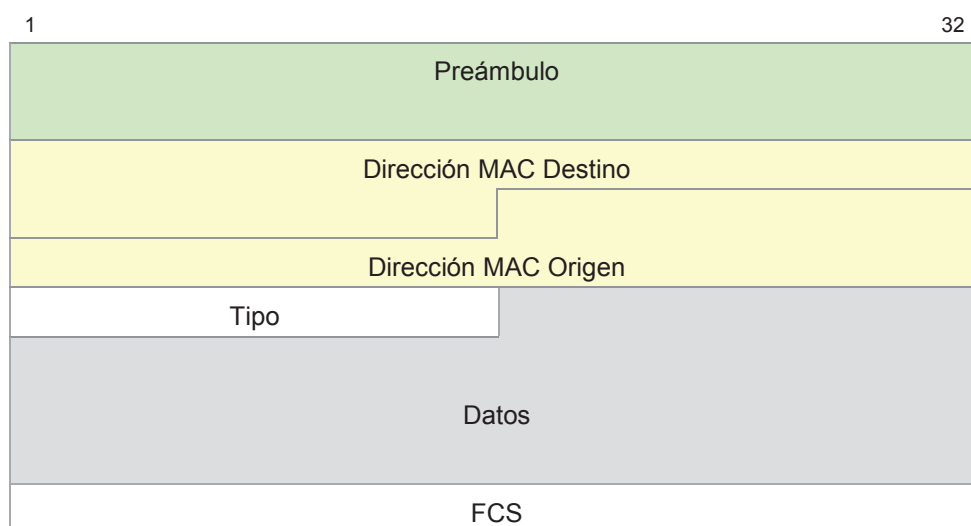
1. El nodo tiene una trama que debe transmitir utilizando el medio físico.

2. El nodo transmisor verifica que ningún otro nodo esté transmitiendo sobre el medio.
 - Si no hay portadora en el medio el nodo transmisor inicia su transmisión.
 - Mientras se realiza la transmisión, permanece en escucha.
 - Concluida la transmisión queda en escucha por un slot time (512 bit-time).
 - Si durante la transmisión detecta una colisión la placa envía una señal de congestión de 32 bits, cesa la transmisión y activa un algoritmo de retardo. Todas las placas que reciben la señal de congestión activan también el algoritmo de retardo.
 - Reintenta la transmisión.
 - Si hay portadora en el medio, el nodo transmisor activa el algoritmo de retardo y aguarda.
 - Reintenta la transmisión.
3. Si después de 16 intentos el nodo no puede transmitir la trama, genera un mensaje de error y ya no lo intenta más.



CSMA-CD es un protocolo vinculado a la operación half-dúplex. Cuando se opera en modo full-dúplex no se utiliza.

Encabezado de una trama Ethernet II



Longitud mínima de la trama Ethernet = 64 bytes.

Longitud máxima de la trama Ethernet = 1518 bytes.

Longitud total del encabezado de la trama: 14 bytes.

FCS: 4 bytes.

Datos: entre 46 y 1500 bytes.

Espacio entre tramas (Preámbulo): 12 bytes (96 bit times).

Direccionamiento de capa 2 y capa 3

Para poder establecer una comunicación ente origen y destino, es preciso:

- Localizar las terminales intervinientes utilizando direcciones lógicas (direcciones de capa 3 – IP).
- Individualizar las terminales utilizando direcciones físicas (direcciones de capa 2 – MAC).

Definición de destinatarios

Una comunicación puede tener 3 tipos de destinatario diferentes:

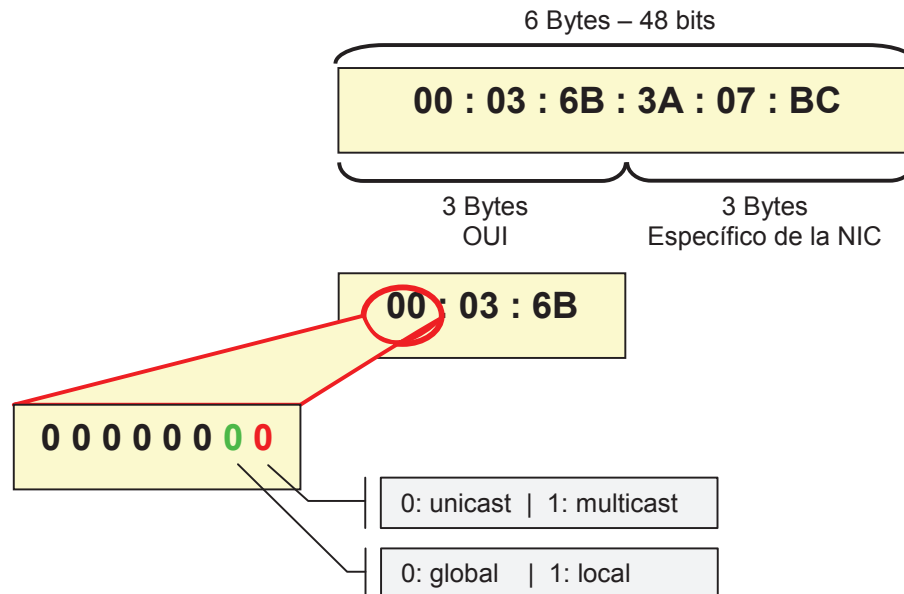
- Unicast
Se trata de una comunicación de uno a uno.
- Multicast
Se trata de una comunicación de uno a un grupo definido dentro de una red.
- Broadcast
Es una comunicación de uno a todos los nodos en una red.

Estos diferentes tipos de destinatarios se identifican tanto en capa 2 como en capa 3 del modelo OSI.

Direcciones MAC

- Es el esquema de direccionamiento físico utilizado en redes Ethernet.
- La dirección se expresa en formato hexadecimal.
- Se encuentra “impresa” en la placa de red (de allí la denominación BIA).
- Cada dispositivo debe contar con una MAC globalmente única.
- Puede ser modificada para responder a requerimientos locales.

Las direcciones MAC Ethernet tienen 48 bits de longitud, expresados como 12 dígitos hexadecimales y tienen la siguiente estructura:



Direcciones IPv4

El protocolo IP suministra un esquema de direccionamiento jerárquico que identifica cada puerto conectado a una red con una dirección de 32 bits.

Las direcciones IP están compuestas por 32 dígitos binarios que para mayor facilidad pueden ser representados como 4 octetos de 8 bits.

Para mayor comodidad, las direcciones IP suelen expresarse utilizando 4 cifras decimales separadas por puntos, que representan cada uno de los 4 octetos binarios. A esta forma de expresión se la denomina notación decimal o de punto.

Ejemplo: 192.160.0.126

Binaria	11000000	.	10100001	.	00000000	.	01111110
Decimal o de punto	192	.	168	.	0	.	126
	Red						Nodo

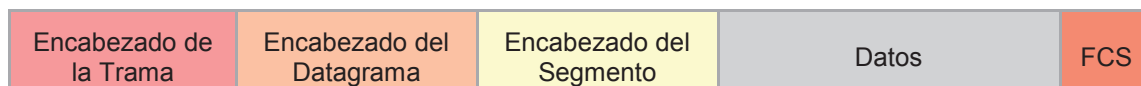
Encabezado de un paquete IP

1			32		
Versión	HLEN	Tipo de Servicio	Longitud Total		
Identificación		Flags	Desplazamiento del fragmento		
TTL		Protocolo	Suma de Comprobación		
Dirección IP de origen					
Dirección IP de destino					
Opciones IP		Relleno			
Datos					

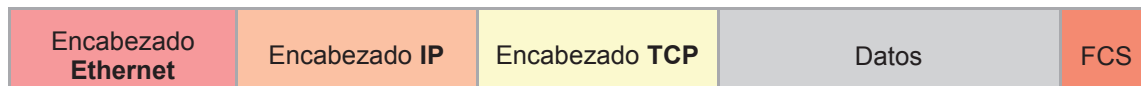
Longitud total del encabezado IP: 24 bytes

Composición de una trama

La estructura básica de una trama es la siguiente:



Un ejemplo:



La capa de Transporte

Es la capa responsable de asegurar la transferencia de los datos entre ambos extremos de la comunicación.

Los 2 protocolos más utilizados en esta capa son TCP y UDP.

Los servicios ofrecidos por esta capa, son:

- Multiplexación de sesiones.
El servicio básico ofrecido por la capa de transporte es el seguimiento individual de las comunicaciones entre aplicaciones en las terminales origen y destino.
- Identificación de aplicaciones.
Para poder identificar las diferentes aplicaciones que operan sobre un mismo dispositivo, la capa de transporte utiliza el identificador de puerto.

Cada proceso de software que necesita acceder a la red es asignado a un número de puerto que debe ser único en ese dispositivo terminal.

- Segmentación.
El flujo de información que se recibe de las aplicaciones se divide en segmentos más pequeños de acuerdo al MTU de la capa de red.
- Control de flujo.
Sobre la base de un mecanismo de acknowledgments generados por el receptor y la definición de una “ventana” de transmisión, el dispositivo receptor puede notificar al transmisor el volumen de datos que está en capacidad de procesar para evitar saturaciones y reenvíos.
- Transporte orientado a la conexión.
Adicionalmente, en el caso de TCP, el mecanismo permite mantener la conexión entre origen y destino durante todo el tiempo que requiera la comunicación.

Conexión confiable o best-effort

En el stack TCP/IP hay 2 tipos diferentes de conexiones:

Confiable	Best-effort
TCP	UDP
Orientado a la conexión	No orientado a la conexión
Se negocia una conexión entre origen y destino.	No negocia una conexión.
Utiliza secuenciamiento	No utiliza secuenciamiento
<ul style="list-style-type: none">• Correo electrónico.• Transferencia de archivos.• Navegación web.	<ul style="list-style-type: none">• Streaming de voz• Streaming de video• Aplicaciones de tiempo real.
Servicios adicionales: <ul style="list-style-type: none">• Detección y recuperación de datos perdidos.• Detección de segmentos duplicados o fuera de orden.• Control de congestión.	Son aplicaciones que soportan la pérdida de paquetes mientras se mantengan en niveles bajos.

El protocolo UDP

- Protocolo de capa de transporte.
- No orientado a la conexión.

- Tiene bajo overhead.
- Provee las funciones básicas de transporte.
- Realiza una verificación de errores muy limitada, en base a su campo checksum.
- No hay ninguna garantía de la entrega de los datos al destino.

1			32
Puerto de Origen		Puerto de Destino	
Longitud		Suma de Comprobación	
Datos			

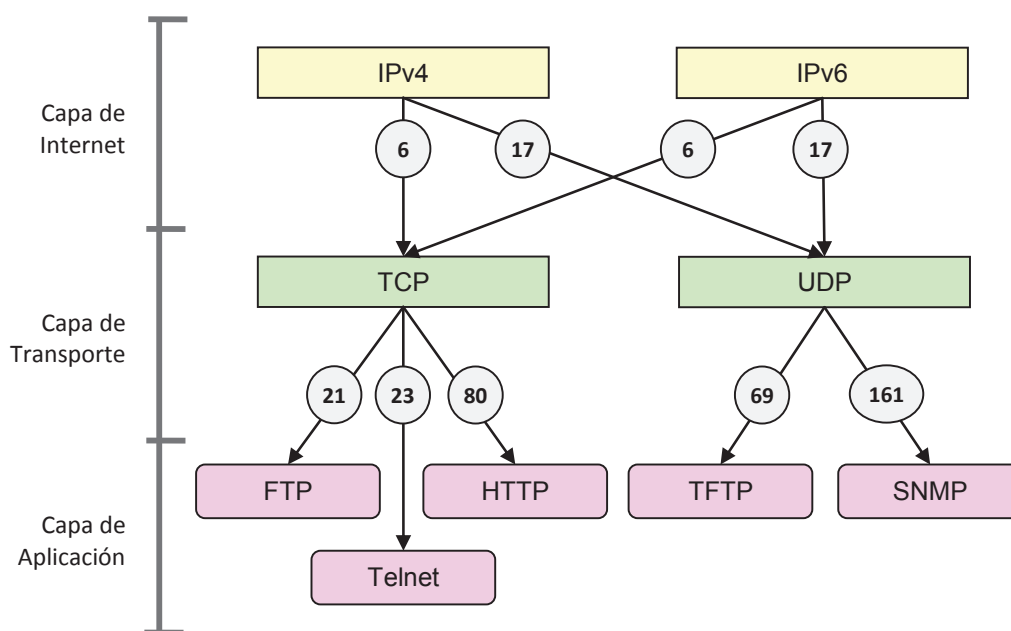
El protocolo TCP

- Protocolo de capa de transporte.
- Orientado a la conexión. Ambos dispositivos terminales se sincronizan entre sí para adaptarse a la congestión de la red.
- Verifica potenciales errores utilizando el checksum.
- Capa paquete va secuenciado.
- Se utiliza un sistema de acknowledgements que son la base de la confiabilidad del sistema.
- Permite utilizar un servicio de reenvío de tráfico bajo petición.
- Incluye un mecanismo de control de flujo.

1			32		
Puerto de Origen			Puerto de Destino		
Número de Secuencia					
N° Acuse de Recibo					
HLEN	Reservado	Bits de Código	Ventana		
Suma de Comprobación			Señalador		
Opciones					
Datos					

Interacción con la capa de red y la de aplicación

El encabezado IP incluye un campo (protocol en IPv4, next header en IPv6) que identifica el protocolo que está contenido dentro del paquete. Este campo es utilizado por la capa de red de la terminal que recibe el paquete para pasar la información al protocolo de capa de transporte adecuado (TCP o UDP), o el protocolo de capa de red correspondiente (SNMP, enrutamiento, etc.).



Tanto UDP como TCP utilizan puertos para operar múltiples conversaciones simultáneamente. Esto permite multiplexar múltiples sesiones a través de la misma interfaz de red.

Por este motivo, en el encabezado de cada segmento se incluye el puerto de origen y destino. El puerto origen está asociado con la aplicación que inicia la comunicación en el dispositivo local. El puerto de destino está asociado con la aplicación a la que se dirige la comunicación en el dispositivo remoto.

Los servicios utilizan números de puerto estáticos que han sido asignados con ese propósito, mientras los clientes utilizan puertos asignados dinámicamente para cada conversación. El cliente debe conocer el puerto asignado a un servicio, para solicitar a ese número de puerto el inicio de una conversación.

Rango ID de Puertos	Uso
1 – 1023	Puertos Bien Conocidos Asignados por IANA de modo permanente para aplicaciones básicas de Internet.
1024 – 49151	Puertos Registrados. Puertos utilizados por servicios de aplicaciones propietarias.

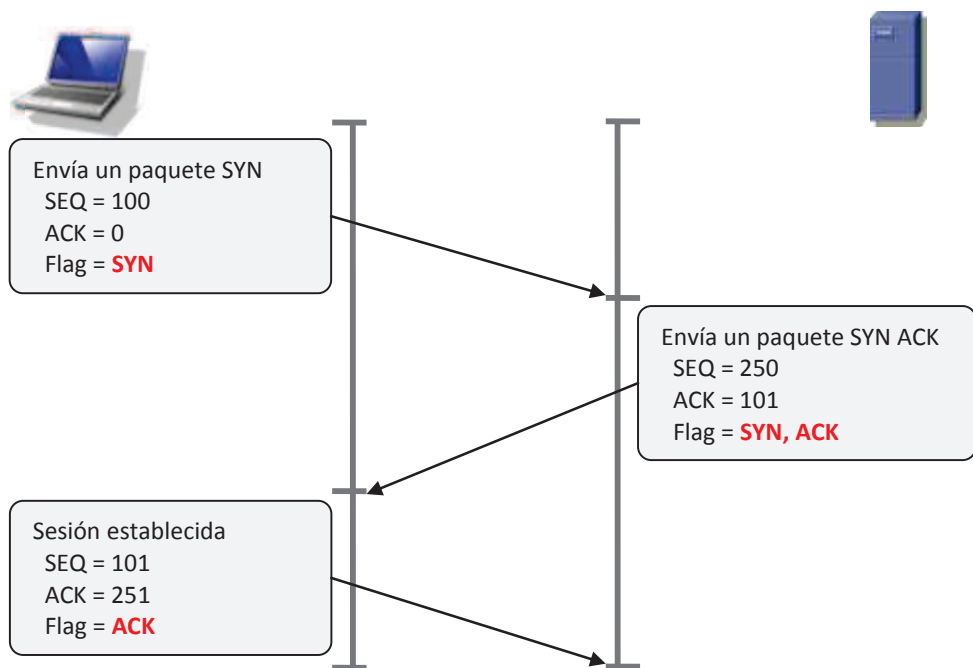
49152 – 65535	Puertos de asignación dinámica. Utilizados por un cliente como puerto de origen por el tiempo que dure una sesión específica.
---------------	--

Establecimiento de una sesión TCP

El establecimiento de sesiones orientadas a la conexión requiere que antes de iniciar la negociación del protocolo se preparen las aplicaciones en ambos extremos (origen y destino) para que se comuniquen entre sí.

Este proceso es conocido como intercambio de triple vía o three way handshake. Tiene por objeto informar al sistema operativo de ambas terminales que se va a iniciar una conexión o conversación. El dispositivo que inicia la conexión es el cliente (origen), el que es destino de la solicitud de conexión es el servidor.

Una vez que se haya concluido la negociación entre ambos extremos de la comunicación, comenzará propiamente la negociación del protocolo de aplicación involucrado y la transferencia de información.



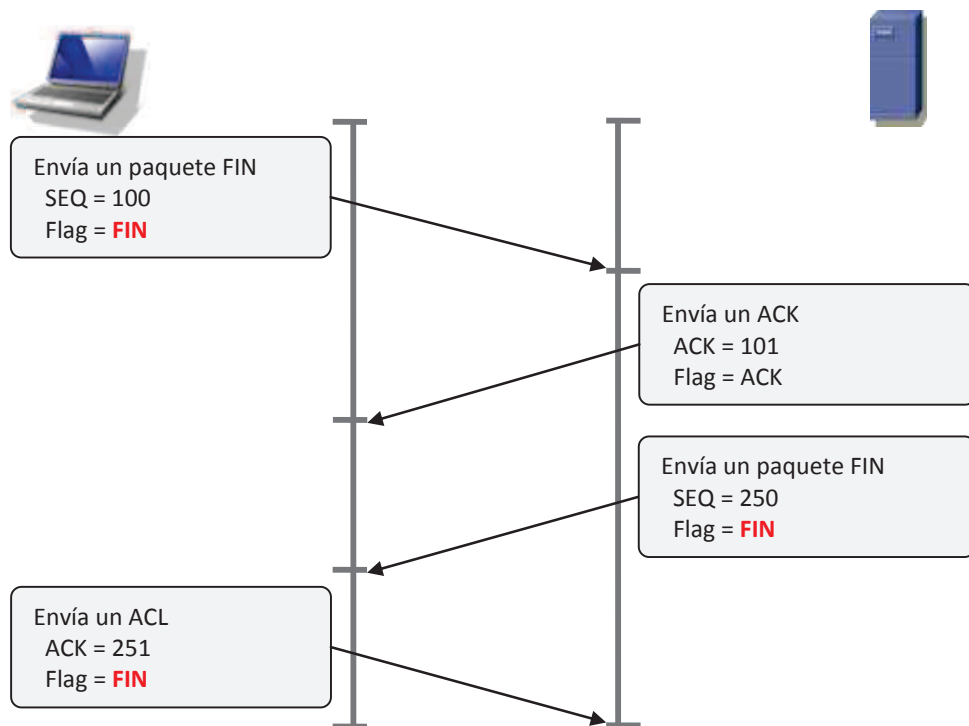
Como resultado del proceso:

- El cliente verifica que el servidor (el dispositivo) está disponible en la red.
- El cliente verifica que el servicio está activo y acepta solicitudes en el puerto destino que utilizamos para la sesión.
- Informa al servidor que el cliente intenta establecer una comunicación.

Cierre de una sesión TCP

En una sesión TCP cada extremo de la comunicación puede detener el envío de información por separado.

Típicamente uno de los extremos de la comunicación informa que desea cerrar la conexión mientras el otro extremo acepta o no que la misma finalice, por lo que también hay un proceso para el cierre de la sesión en ambos terminales sin que se pierda información.



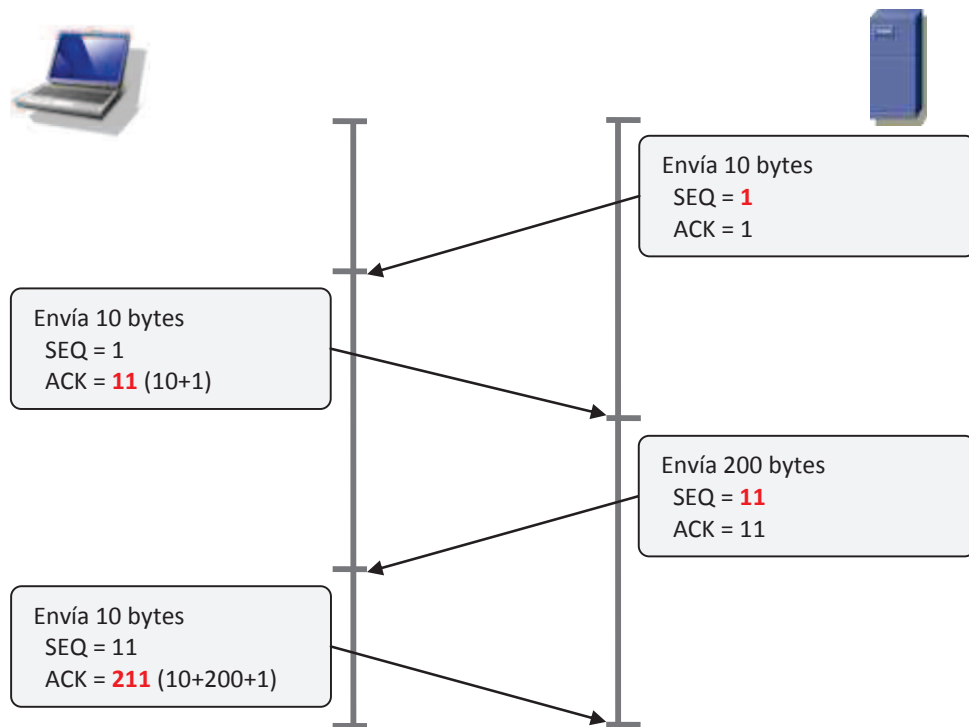
La sesión se concluye cuando ambos extremos han enviado su notificación de FIN y recibido el correspondiente ACK.

Control de flujo en TCP

TCP provee mecanismos de control de flujo que permiten responder a problemas de disponibilidad de capacidad en la red o en los dispositivos receptores. Realiza un ajuste de la tasa de transmisión efectiva entre los dos dispositivos terminales.

Para esta tarea, a la vez que dar confiabilidad a la comunicación, TCP realiza un secuenciamiento y confirmación de recepción de los segmentos.

- El número de secuencia permite reensamblar la información en el dispositivo receptor.
Se utiliza el número de bytes que el origen envía.
- El número de acknowledgment permite confirmar la recepción de los segmentos y solicitar el envío de los siguientes.
- Si se pierde un número de secuencia en la serie, ese segmento y todos los siguientes se retransmiten.



El mecanismo de acknowledgment es el que permite:

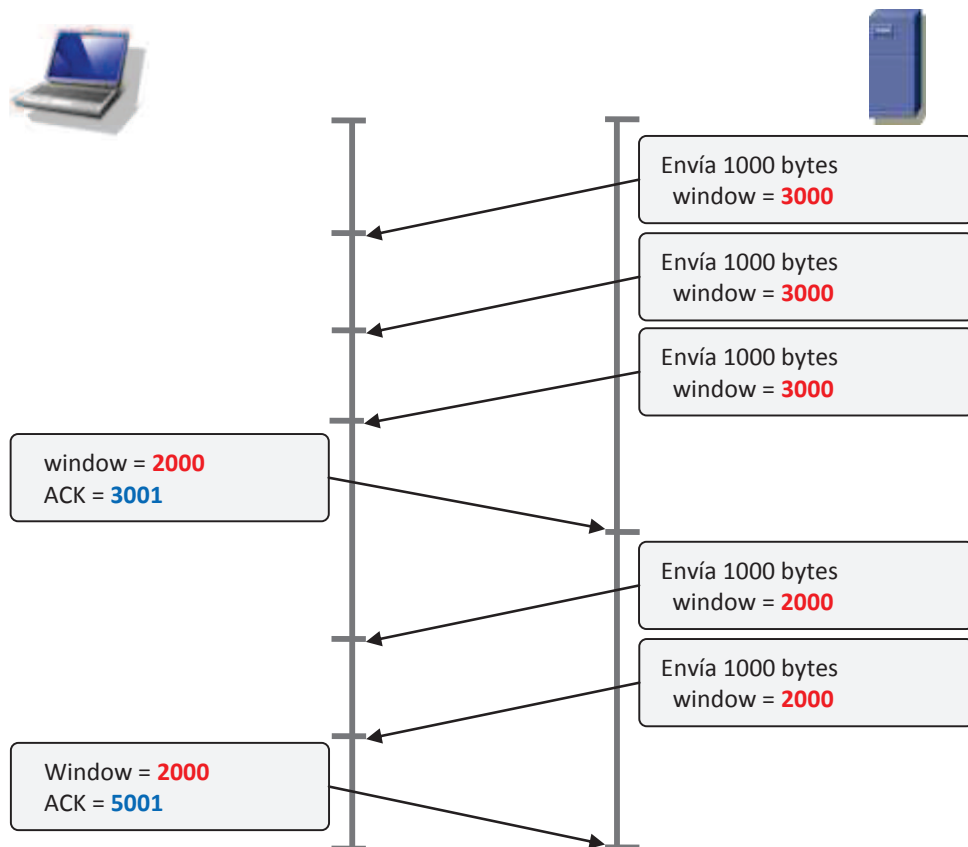
- Asegurar que los segmentos son recibidos sin errores y en el orden correcto.
- Indicar al dispositivo de origen cuál es el segmento que el destino espera recibir a continuación.

El sistema de ventana

Permite que un dispositivo envíe un determinado volumen de información (varios segmentos) sin esperar a recibir un acknowledgment por cada segmento.


- Mejora la performance de la conexión reduciendo el overhead.
- Permite controlar la tasa de transmisión evitando la congestión y la pérdida de información.

Llamamos “ventana” a la cantidad de bytes de datos que puede enviar un dispositivo sin esperar por un acknowledgment del receptor.



Esta ventana (CWS) recibe el adjetivo de “deslizante” ya que su tamaño varía en función del estado (congestión) de la red y la capacidad del dispositivo receptor.

- El tamaño es negociado en el inicio de la sesión.
- Puede cambiar dinámicamente en el desarrollo de la conversación.
- Si el tamaño de la ventana se define en 0, se interrumpe el envío de información hasta que se comuniquen un nuevo valor de tamaño.
- Si un segmento se pierde, el CWS se reduce a la mitad.
- Una desventaja de este procedimiento es la posibilidad de sincronización de las sesiones TCP.

 Para profundizar o tener mayor información sobre cualquiera de estos puntos, sugiero consultar mi libro “Guía de Preparación para el Examen de Certificación CCNA”.

2.2. Direccionamiento IP (IPv4 / IPv6)

Dentro del conjunto de protocolos, tecnologías y dispositivos que hacen posible estas comunicaciones, ocupan un lugar muy importante en la actualidad dos protocolos: TCP como protocolo de capa de transporte e IP como protocolo de capa de red.

Ambos son los ejes en torno a los cuales se ha desarrollado Internet, y son el centro conceptual de las tecnologías de mayor difusión en la actualidad para entornos LAN y WAN.

El Protocolo IP (Internet Protocol)

Protocolo de capa de red, no orientado a la conexión; su versión 4 ha sido definida en el RFC 791.

Es el único protocolo del stack TCP/IP que proporciona funcionalidades de ruteo.

Direccionamiento IP versión 4

El protocolo IP suministra un esquema de direccionamiento jerárquico que identifica cada puerto conectado a una red con una dirección de 32 bits.

Las direcciones IP están compuestas por 32 dígitos binarios que para mayor facilidad pueden ser representados como 4 octetos de 8 bits.

Estas direcciones IP están compuestas por hasta 2 partes:

- Una dirección de red.
- Una dirección de nodo.

Para mayor comodidad, las direcciones IP suelen expresarse utilizando 4 cifras decimales separadas por puntos, que representan cada uno de los 4 octetos binarios. A esta forma de expresión se la denomina notación decimal o de punto.

Ejemplo: 192.160.0.126

Binaria	11000000	.	10100001	.	00000000	.	01111110
Decimal o de punto	192	.	168	.	0	.	126
	Red						Nodo

Estructura de clases

IPv4 aplica el concepto de “clase”, para establecer cuántos bits u octetos se utilizan para definir o identificar la red, y cuántos quedan para identificar cada nodo individual.

Clase A

Primer octeto:	00000001 a 01111111
Rango de direcciones clase A:	1.0.0.0 a 127.255.255.255
	0.0.0.0 dirección reservada
	127.0.0.0 – reservada para loopback
Direcciones privadas (RFC 1918):	10.0.0.0 a 10.255.255.255
Esquema:	Red Nodo . Nodo . Nodo
Número de redes posibles:	126
Número de nodos útiles por red:	16.777.214
Representan el 50% del número total de direcciones IP posible.	

Clase B

Primer octeto:	10000000 a 10111111
Rango de direcciones clase B:	128.0.0.0 a 191.255.255.255
Direcciones privadas (RFC 1918):	172.16.0.0 a 172.31.255.255
Esquema:	Red . Red Nodo. Nodo
Número de redes posibles:	16.384
Número de nodos útiles por red:	65.534
Representan el 25% del número total de direcciones IP posible.	

Clase C

Primer octeto:	11000000 a 11011111
Rango de direcciones clase C:	192.0.0.0 a 223.255.255.255
Direcciones privadas (RFC 1918):	192.168.0.0 a 192.168.255.255
Esquema:	Red . Red . Red Nodo
Número de redes posibles:	2.097.152
Número de nodos útiles por red:	254
Representan el 12.5% del número total de direcciones IP posible.	

Clase D

Direcciones de Multicast o Multidifusión.

Primer octeto: 11100000 a 11101111

Rango de direcciones clase D: 224.0.0.0 a 239.255.255.255




No se utilizan para identificar nodos individuales.

Clase E

Direcciones de Investigación. Estas direcciones no son utilizadas en Internet.

Primer octeto: 11110000 a 11111111

Rango de direcciones clase E: 240.0.0.0 a 255.255.255.255

 Clase A	00000000 a	01111110	1 a 126
 Clase B	10000000 a	10111111	128 a 191
 Clase C	11000000 a	11011111	192 a 223

Direcciones IP Privadas

Han sido definidas a través del RFC 1918. Estas direcciones no se enrutan hacia el backbone de Internet.

IP Privadas Clase A 10.0.0.0 a 10.255.255.255

IP Privadas Clase B 172.16.0.0 a 172.31.255.255



IP Privadas Clase C 192.168.0.0 a 192.168.255.255

Direcciones IPv4 reservadas

Se trata de direcciones que no pueden asignarse a dispositivos individuales.

- Direcciones de red.
Es el modo estándar de referirse a una red.
Tiene todos los bits que corresponden al nodo en cero.
- Dirección de broadcast dirigido.
Dirección IP que permite establecer una comunicación con un único paquete hacia todos los nodos de una red específica.
Es la dirección que tiene todos los bits correspondientes al nodo en uno.
- Dirección de broadcast local.
Es la dirección compuesta por todos bits en uno.
Permite enviar un paquete de broadcast solamente a la red local.

- Dirección de loopback local.
Es la dirección utilizada para que un sistema envíe un mensaje a sí mismo con fines de verificación.
La dirección típica utilizada es 127.0.0.1.
- Dirección IP de autoconfiguración.
El bloque de direcciones 169.254.0.0 a 169.254.255.255 está reservado para utilización como direcciones de link local. Pueden ser asignadas automáticamente por el sistema operativo al nodo en entornos en los que no hay configuración de IP disponible.
Estas direcciones no pueden ser ruteadas.

 Dirección reservada de red	0s en el nodo
 Dirección reservada de broadcast	1s en el nodo

Direcciones IPv4 Privadas

Los dispositivos que no utilizan Internet para conectarse entre sí pueden utilizar cualquier dirección IP válida mientras que sea única dentro del entorno en el que se establece la comunicación.

Con este propósito la IETF definió un grupo de bloques de direcciones específicos en el RFC 1918. Estas direcciones no se enrutan hacia el backbone de Internet.

- IP Privadas Clase A 10.0.0.0 a 10.255.255.255
- IP Privadas Clase B 172.16.0.0 a 172.31.255.255
- IP Privadas Clase C 192.168.0.0 a 192.168.255.255

Si un nodo que utiliza una de estas direcciones, para conectarse a Internet es necesario que su dirección sea “traducida” utilizando NAT.

Encabezado IPv4

1				32	
Versión	HLEN	Tipo de Servicio	Longitud Total		
Identificación			Flags	Desplazamiento del fragmento	
TTL		Protocolo	Suma de Comprobación		
Dirección IP de origen					
Dirección IP de destino					
Opciones IP			Relleno		
Datos					

Protocolo ARP

Es un protocolo de la pila TCP/IP que permite resolver o mapear direcciones IP a direcciones MAC.

ARP construye y mantiene en la memoria RAM de cada dispositivo o terminal una tabla denominada caché ARP que contiene el mapeo IP / MAC.

En el caso en el que la dirección IP de destino pertenezca a otra red, los router pueden ejecutar un ARP proxy.

Las direcciones MAC son solamente de relevancia local, y se utilizan para establecer comunicaciones en el entorno del dominio de broadcast. Por lo tanto, no sirve de nada conocer la dirección física de un dispositivo remoto. Por el contrario, para conectarse a un dispositivo remoto es necesario que la trama sea tomada por el puerto de gateway para que sea enviada al dispositivo remoto.



Protocolo ARP: Se conoce la IP destino y se necesita la MAC.

Procedimiento para obtener una dirección IP

Una terminal puede obtener su dirección IP a través de diversos procedimientos:

- Configuración manual.
- Configuración automática:
 - Protocolo RARP.
 - Protocolo BootP.
 - Protocolo DHCP.

Protocolo RARP

Permite resolver u obtener una dirección IP a partir de una dirección MAC conocida que es el dato que se tiene por conocido.

Su operación requiere como condición la presencia de un servidor RARP en la red para responder a las peticiones RARP de los clientes.



Para no confundirse:

Tengo la IP y busco la MAC	ARP
Tengo la MAC y busco la IP	RARP

ICMP

ICMP proporciona un conjunto de mensajes de control y error que permiten detectar y resolver problemas en la red de modo automático. Permite el reporte de

errores en un entorno IP ya que el mismo protocolo IP no tiene posibilidad alguna de detectar o reportar errores a nivel de capa de red.



Atención, ICMP no soluciona la falla ya que no puede determinar el reenvío de un paquete que se ha descartado; para esto debe descansarse en los protocolos de capa de transporte.

Si bien ICMP reporta errores en la transmisión de cualquier datagrama, los paquetes ICMP no generan a su vez mensajes de error ICMP. Esto evita generar congestiones en la red, pero puede provocar que un mensaje de error nunca llegue a su destinatario.

ICMP genera 15 tipos de mensajes diferentes que se agrupan en 2 funciones básicas: mensajes de error y mensajes de control:

Tipo	Mensaje	Función
0	Echo Replay	Error
3	Destination Unreachable	Error
4	Source Quench	Control
5	Redirect / Change Request	Control
8	Echo Request	Error
9	Router Advertisement	Control
10	Router Selection	Control
11	Time Exceeded	Error
12	Parameter Problem	Error
13	Timestamp Request	Control
14	Timestamp Reply	Control
15	Information Request	Control
16	Information Reply	Control
17	Address Mask Request	Control
18	Address Mask Reply	Control

Direccionamiento IP versión 6

Esquema de direccionamiento jerárquico que utiliza direcciones de 128 bits.

Características principales

- Direcciones de 128 bits.
- Expresadas con 32 dígitos hexadecimales.
- Suministra un total de 3.4×10^{38} direcciones posibles.
- Utiliza un encabezamiento de capa de red simplificado.
- No utiliza broadcast.
- Incluye las prestaciones estándar de IPsec y Mobile IP.
- Implementa etiquetado de flujos de tráfico.
- Una interfaz física puede tener varias direcciones IPv6.

Representación de direcciones IPv6

- Están compuestas por 8 campos de 4 dígitos hexadecimales (16 bits).
- Se pueden suprimir los 0s iniciales.
- Campos sucesivos en 0 pueden ser suprimidos y reemplazados por “:”.

Un ejemplo:

2001 : 0ab1 : 0000 : 0000 : 09bc : 45ff : fe23 : 13ac

2001 : ab1 : 0 : 0 : 9bc : 45ff : fe23 : 13ac

2001 : ab1 : : : 9bc : 45ff : fe23 : 13ac

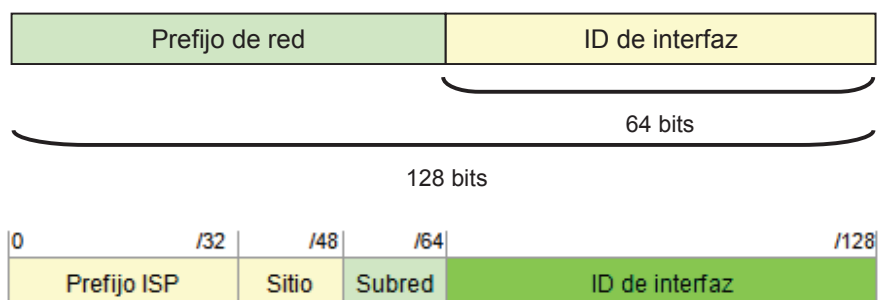
2001:ab1::9bc:45ff:fe23:13ac

Direcciones IPv6

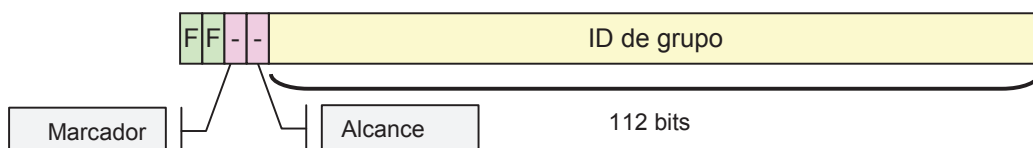
IPv6 utiliza diferentes tipos de direcciones:

- Direcciones de Unicast.
Identifican una única interfaz.
Hay diferentes tipos de direcciones unicast IPv6:
 - Direcciones globales.
IANA está asignado actualmente direcciones del rango 2000::/3

- Direcciones de link local.
FE80::/10
- Direcciones unique local.
FC00::/7
- Direcciones reservadas.
::1/128 Dirección de loopback.
::/128 Dirección no especificada.



- Direcciones de Anycast.
Identifican un conjunto de dispositivos o nodos. El que esté más cercano al dispositivo de origen será el que recibirá el paquete.
No son diferenciables de las direcciones de unicast, ya que se toman del bloque de direcciones de unicast.
- Direcciones de Multicast.
Representan un grupo de interfaces. Son una respuesta efectiva a las dificultades que provoca el tráfico de broadcast.
Ocupan un rango a partir de FF00::/8



- NO hay direcciones de broadcast en IPv6.

Una interfaz en una red IPv6 puede tener asignadas múltiples direcciones IPv6.

Asignación de direcciones IPv6

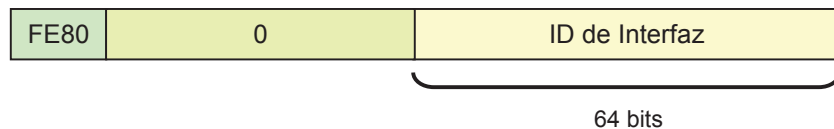
- Asignación estática:
 - Asignación manual de direcciones.
 - Asignación de direcciones utilizando ID EUI-64

- Asignación dinámica.
 - Autoconfiguración.
 - DHCPv6.

Direcciones IPv6 de link local

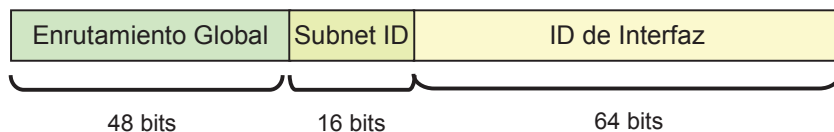
Toda interfaz en la que se habilita el protocolo IPv6 cuenta con una dirección de link local.

- Tienen un alcance solamente local y se utilizan para establecer comunicaciones sobre el mismo enlace.
- Se crean automáticamente utilizando el prefijo FE80::/10
- Se utilizan en múltiples procesos a nivel de infraestructura de la red.



Direcciones IPv6 globales de unicast

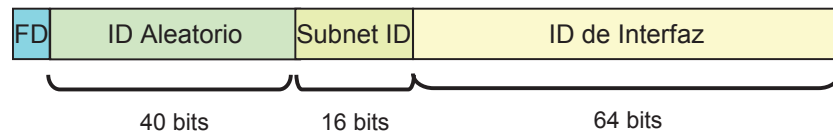
- Son las direcciones para establecer comunicaciones sobre Internet.
- Tiene una estructura de 3 niveles:
 - Un prefijo de enrutamiento global, típicamente de 48 bits.
 - Un ID de subred, generalmente de 16 bits de longitud.
 - Un ID de interfaz de 64 bits de longitud que puede ser asignado estática o dinámicamente.



Direcciones IPv6 unique local

- Son direcciones definidas para utilizar dentro de una red específica (no sobre Internet), aunque es muy probable que puedan ser globalmente únicas.
- Tiene una estructura de 4 niveles:
 - Un prefijo de 8 bits FD00::/8
 - Un identificador aleatorio de 40 bits.

- Un ID de subred de 16 bits de longitud,
- Un ID de interfaz de 64 bits.



Direcciones IPv6 de anycast

- Son direcciones que se asignan a una o más interfaces.
- Cuando se envía un paquete a una dirección de anycast, es ruteado a la interfaz más cercana de acuerdo a la métrica de los protocolos de enrutamiento.
- Son direcciones tomadas del espacio de direccionamiento de unicast. Se debe configurar expresamente la interfaz para que opere de esa manera.

Encabezado IPv6

1				32
Versión	Clase de Tráfico	Etiqueta de Flujo		
Longitud de la Carga		Próximo encabezado	Límite de Saltos	
Dirección IP de origen				
Dirección IP de destino				
Datos				

Respecto del encabezado IPv4:

- Se removieron la mitad de los campos, lo que hace más sencillo su procesamiento.
- Todos los campos están alineados a 64 bits.

- No hay checksum o suma de comprobación, lo que mejora la eficiencia del enrutamiento.

Mecanismos de transición

Permiten la integración de redes IPv4 con IPv6.

- Dual stack.
- Tunnelizado.
 - Túnel manual IPv6-over-IPv4.
 - Dynamic 6to4.
 - Intra-Site Automatic Tunnel Addressing Protocol (ISATAP).
 - Teredo.
- Traducción (NAT-PT).

Implementación de subredes en redes IPv4

Subred

Una red puede ser internamente dividida en dominios de broadcast más pequeños a partir de la estructura del direccionamiento IP. A estos segmentos de red se los denomina subredes. El concepto de subred fue introducido en 1985 por la RFC 950.

Cada subred se comporta dentro de la red como un dominio de broadcast, y es identificada utilizando al menos los primeros 2 bits (desde la izquierda) de la porción del nodo de la dirección IP.

Para poder dividir la red de esta manera se utiliza una herramienta denominada máscara de subred.

La máscara de subred es un número binario de 32 dígitos que actúa como una contraparte de la dirección IP.

Las posiciones de bits que en la máscara de subred se colocan en “0” son las que se utilizarán para identificar los nodos, y las posiciones que se colocan en “1” serán las que definan las subredes.

Un ejemplo:

Notación Binaria	10101100	.	00010000	.	00000010	.	01111110
Decimal	172	.	16	.	2	.	126
Sin Subredes	RED			.	NODO		
Máscara de Subred	11111111	.	11111111	.	11111111	.	00000000
Máscara de Subred	255	.	255	.	255	.	0
Con Subredes	RED			.	SUBRED	.	HOST

Es importante tener presente que dentro de cada subred se mantienen las mismas reglas de direccionamiento que se aplican a las redes:

- La dirección que en números binarios tiene todos 0s en los bits correspondientes al nodo está reservada para identificar a la subred. Se la denomina dirección reservada de subred.
- La dirección que en notación binaria tiene todos 1s en los bits correspondientes al nodo está reservada para identificar los broadcasts. Se la denomina dirección reservada de broadcast.
- Las restantes direcciones son las disponibles para asignar a cada uno de los puertos de la subred. Se las suele denominar direcciones útiles o direcciones de nodo.
- Tradicionalmente se recomienda que las subred cero y la última subred no sean utilizadas. Cisco IOS no permitió utilizar estas 2 subredes hasta IOS 12.0 a menos que se utilizara el comando `ip subnet-zero`.



Cantidad de subredes creadas: 2^n

Cantidad de subredes útiles: $2^n - 2$

Donde n es la cantidad de bits de la porción de subred de la máscara.

Cantidad de direcciones de nodo en cada subred: 2^m

Cantidad de direcciones de nodo útiles en cada subred: $2^m - 2$

Donde m es la cantidad de bits de la porción de host de la máscara.

Método sencillo para el cálculo de subredes:

Antes de comenzar con la tarea usted debe tener 2 datos básicos:

- Cuál es el número total de subredes que se requieren, incluyendo la consideración del posible crecimiento de la red.
- Cuál es el número de nodos que se prevén en cada subred, teniendo en cuenta también en este caso las consideraciones de expansión y crecimiento.

A partir de aquí, responda estas 6 preguntas básicas:

1. ¿Cuántas subredes son necesarias?
2. ¿Cuántos nodos se necesitan por subred?
3. ¿Cuáles son los números reservados de subred?
4. ¿Cuáles son las direcciones reservadas de broadcast?
5. ¿Cuál es la primera dirección de nodo válida?
6. ¿Cuál es la última dirección de nodo válida?

Con lo que debe obtener 6 respuestas.

Se ve mucho mejor con un ejemplo: red 192.168.1.0 máscara 255.255.255.224

1. La cantidad de subredes utilizables se calcula tomando como base la cantidad de bits de la porción del nodo que se toman para generar subredes, y aplicando la fórmula siguiente:

$$2^{\text{bits de subred}} - 2 = \text{subredes utilizables}$$

Ejemplo:

$$2^3 - 2 = 6$$

2. La cantidad de direcciones de nodo útiles que soporta cada subred, surge de la aplicación de la siguiente fórmula, que toma como base la cantidad de bits que quedan para identificar los nodos:

$$2^{\text{bits de nodo}} - 2 = \text{nodos útiles}$$

Ejemplo:

$$2^5 - 2 = 30$$

3. La dirección reservada de la primera subred útil surge de restar a 256 el valor decimal de la porción de la máscara de subred en la que se define el límite entre subred y nodo:

$$256 - [\text{máscara}] = [\text{primera subred útil y rango de nodos}]$$

Las direcciones de las subredes siguientes surgen de seguir sumando la misma cifra.

Ejemplo:

$$256 - 224 = 32$$

	192.168.1.0	subred 0 – no es útil
	192.168.1.32	subred 1 – primer subred útil
+ 32	192.168.1.64	subred 2
+ 32	192.168.1.96	subred 3
+ 32	192.168.1.128	subred 4
+ 32	...	

4. Las direcciones reservadas de broadcast se obtienen restando 1 a la dirección reservada de subred de la subred siguiente:

Ejemplo:

$32 - 1 = 31$	192.168.1.31	subred 0
$64 - 1 = 63$	192.168.1.63	subred 1
$96 - 1 = 95$	192.168.1.95	subred 2
$128 - 1 = 127$	192.168.1.127	subred 3

... ..

5. La dirección IP del primer nodo útil de cada subred se obtiene sumando uno a la dirección reservada de subred:

Reservada de subred + 1 = primer nodo utilizable

Ejemplo:

$32 + 1 = 33$	192.168.1.33	primer nodo subred 1
$64 + 1 = 65$	192.168.1.65	primer nodo subred 2
$96 + 1 = 97$	192.168.1.97	primer nodo subred 3
$128 + 1 = 129$	192.168.1.129	primer nodo subred 4

... ..

6. La dirección IP del último nodo útil de cada subred se obtiene restando 1 a la dirección reservada de broadcast:

$63 - 1 = 62$	192.168.1.62	último nodo subred 1
$95 - 1 = 94$	192.168.1.94	último nodo subred 2
$127 - 1 = 126$	192.168.1.126	último nodo subred 3

... ..






256 – [máscara] Nos indica el valor decimal del octeto crítico de la primera subred útil.



[máscara] Nos indica el valor decimal del octeto crítico de la última subred, que no es utilizable.

Todo este procedimiento permite conformar como resultado, la siguiente tabla:


#	Subred	Primer nodo útil	Último nodo útil	Broadcast
0	192.168.1.0	Reservada		
1	192.168.1.32	192.168.1.33	192.168.1.62	192.168.1.63
2	192.168.1.64	192.168.1.65	192.168.1.94	192.168.1.95
3	192.168.1.96	192.168.1.97	192.168.1.126	192.168.1.127
4	192.168.1.128	192.168.1.129	192.168.1.158	192.168.1.159
5	192.168.1.160	192.168.1.161	192.168.1.190	192.168.1.191
6	192.168.1.192	192.168.1.193	192.168.1.222	192.168.1.223
7	192.168.1.224	Reservada		


 La dirección reservada de subred...	es siempre par.
 La dirección reservada de broadcast...	es siempre impar.
 El rango de direcciones útiles...	comienza impar y termina par.


Variable-Length Subnet Mask (VLSM)

La implementación de protocolos de enrutamiento classless permite variar la máscara de subred, lo que se hace a través de 2 técnicas básicas:

- VLSM – Máscara de Subred de Longitud Variable.
- CIDR – Enrutamiento entre Dominios Sin Clases.

 Cuando se utiliza enrutamiento classful: la máscara de subred debe ser la misma en todos los puertos de la red.

 Cuando se utilizan enrutamiento classless: no hay limitaciones para la implementación de máscaras de subred.

 El examen CCNA considera los siguientes protocolos de enrutamiento:
Classful: RIP.
Classless: RIPv2, EIGRP, OSPF.

La implementación de VLSM permite a una organización dividir un único sistema autónomo utilizando más de una máscara de subred, generando de esta manera subredes de diferente tamaño dentro de la misma red.

Para implementar VLSM se deben tener en cuenta algunos pre-requisitos:

- Es imprescindible utilizar protocolos de enrutamiento classless.
- Es importante tener muy en cuenta el diseño topológico junto al diseño lógico.

Un ejemplo:

Red: 192.168.1.0/24

Se requiere brindar soporte a 5 redes de 30 nodos máximo cada una, unidas a través de 4 enlaces punto a punto una a una. Esto requeriría en un esquema classful de 9 subredes, y sería imposible con una dirección de red clase C como esta.

1. Cálculo de la subred mayor.
Máximo de nodos necesarios: 30
Cantidad de bits en la porción del nodo: $5 (2^5 - 2 = 30)$
Máscara de subred para crear estas subredes: 255.255.255.224
Cantidad de bits en la porción de la subred: $3 (8 - 5 = 3)$
Cantidad de subredes creadas: $8 (2^3)$

2. División de la red en subredes

Red	192	.	168	.	1	.	0	
Máscara 27 bits	11111111	.	11111111	.	11111111	.	11100000	
Subred #0	192	.	168	.	1	.	0	Sin asignar
Subred #1	192	.	168	.	1	.	32	Red 1
Subred #2	192	.	168	.	1	.	64	Red 2
Subred #3	192	.	168	.	1	.	96	Red 3
Subred #4	192	.	168	.	1	.	128	Red 4
Subred #5	192	.	168	.	1	.	169	Red 5
Subred #6	192	.	168	.	1	.	192	Sin asignar
Subred #7	192	.	168	.	1	.	224	Sin asignar

3. Fraccionamiento de una subred no utilizada para generar subredes de menor tamaño.
Se le aplica una máscara de 30 bits, ya que se necesitan subredes para asignar a los enlaces punto a punto, y estos solo tienen 2 nodos.

Subred #0	192	.	168	.	1	.	0	
Máscara 27 bits	11111111	.	11111111	.	11111111	.	11100000	
Máscara 30 bits	11111111	.	11111111	.	11111111	.	11111100	
Subred #0	192	.	168	.	1	.	0	Sin asignar
Subred #1	192	.	168	.	1	.	4	Enlace 1
Subred #2	192	.	168	.	1	.	8	Enlace 2
Subred #3	192	.	168	.	1	.	12	Enlace 3
Subred #4	192	.	168	.	1	.	16	Enlace 4
Subred #5	192	.	168	.	1	.	20	Sin asignar

Análisis final del direccionamiento para este ejemplo:

Red	192	.	168	.	1	.	0	
Máscara 30 bits	11111111	.	11111111	.	11111111	.	11111100	
Subred #0	192	.	168	.	1	.	0	Sin asignar
Subred #1	192	.	168	.	1	.	4	Enlace 1
Subred #2	192	.	168	.	1	.	8	Enlace 2
Subred #3	192	.	168	.	1	.	12	Enlace 3
Subred #4	192	.	168	.	1	.	16	Enlace 4
Máscara 27 bits	11111111	.	11111111	.	11111111	.	11100000	
Subred #1	192	.	168	.	1	.	32	Red 1
Subred #2	192	.	168	.	1	.	64	Red 2
Subred #3	192	.	168	.	1	.	96	Red 3
Subred #4	192	.	168	.	1	.	128	Red 4
Subred #5	192	.	168	.	1	.	169	Red 5
Subred #6	192	.	168	.	1	.	192	Sin asignar
Subred #7	192	.	168	.	1	.	224	Sin asignar

Classless Interdomain Routing (CIDR)

Técnica que se aplica en sistemas de direccionamiento IPv4 que ignora la estructura de clases, utilizando solamente la máscara de subred y no ya las clases para determinar las porciones de red y de nodo en cada dirección.

Está relacionado con VLSM, pero es una técnica diferente. Cuando se implementa VLSM, se genera subredes dentro de subredes, permitiendo crear dominios de broadcast de diferentes tamaños dentro de una red y reducir así sensiblemente el desperdicio de direcciones IP.

CIDR por su parte, prescindiendo de las fronteras que introducen las clases de IPv4, permite representar conjuntos de redes o subredes utilizando una única dirección y máscara. De este modo posibilita reducir el tamaño de las tablas de enrutamiento y las listas de acceso, mejorando consecuentemente la performance de los dispositivos asociados.

Sumarización de rutas

Se utiliza una única dirección de red con una máscara de subred para identificar un conjunto de redes.

Un ejemplo permite entender mejor el concepto:

Una empresa de telecomunicaciones ha entregado 8 redes clase B a un proveedor de servicio de acceso a Internet para su uso.

Utilizando un esquema de direccionamiento classful, la empresa debería mantener 8 rutas para direccionar el tráfico de este proveedor de servicio, lo cual es redundante ya que el proveedor tiene un único punto de acceso a la red de la empresa.

En consecuencia, se pueden sumarizar las 8 rutas a cada red clase B, en una única ruta con una máscara de subred diferente:

Rutas al ISP:

172.24.0.0/16	10101100	00011000	00000000	00000000
172.25.0.0/16	10101100	00011001	00000000	00000000
172.26.0.0/16	10101100	00011010	00000000	00000000
172.27.0.0/16	10101100	00011011	00000000	00000000
172.28.0.0/16	10101100	00011100	00000000	00000000
172.29.0.0/16	10101100	00011101	00000000	00000000
172.30.0.0/16	10101100	00011110	00000000	00000000
172.31.0.0/16	10101100	00011111	00000000	00000000
Máscara de Subred	11111111	11111111	00000000	00000000
Red Sumarizada: 172.24.0.0/13				
	172	24	0	0
	10101100	00011	000	00000000
Máscara de Subred	11111111	11111	000	00000000

La ruta sumarizada es la que considera como ID del conjunto de redes todos los bits (y solamente aquellos bits) que tienen un valor idéntico en todas las redes del grupo.

Las ventajas de la sumarización de rutas son:

- Mayor eficiencia en el enrutamiento.
- Se reduce el número de ciclos de la CPU del router necesarios para recalcular u ordenar las entradas de las tablas de enrutamiento.
- Reduce los requerimientos de memoria RAM del router.
- Mayor estabilidad de las tablas de enrutamiento.

Características de los bloque de rutas

El proceso de sumarización de rutas al utilizar posiciones binarias, genera bloques de rutas expresadas en notación decimal que tienen características definidas:

- La amplitud del rango de redes sumarizadas, expresado en valores decimales, es siempre una potencia de 2.
Por ejemplo: 2, 4, 8, 16...
- El valor inicial del rango decimal sumarizado es un múltiplo de la potencia de 2 utilizada como amplitud del rango.
Por ejemplo, si es un rango de 8 redes, el valor inicial será 0, 8, 16, ,24...



Para profundizar o tener mayor información sobre cualquiera de estos puntos, sugiero consultar mi libro "Guía de Preparación para el Examen de Certificación CCNA".

2.3. Operación de dispositivos Cisco IOS

Cisco IOS

El Cisco IOS (Internetwork Operating System) es el kernel de los routers y muchos de los otros dispositivos fabricados Cisco.

Las funciones básicas que brinda son:

- La implementación de protocolos de red.
- El direccionamiento o conmutación de tráfico entre dispositivos a alta velocidad.
- Características de seguridad al control de acceso y bloqueo al posible uso no autorizado de la red.
- Características de escalabilidad para facilitar el crecimiento de la red.
- Brinda confiabilidad en la conexión a los recursos de red.

Conexión al dispositivo

En este sentido, se cuenta con 3 vías de acceso posibles:

- El puerto consola.
- El puerto auxiliar.
- Los puertos virtuales.

Estas 3 formas de acceso no siempre están disponibles en todos los modelos. Por ejemplo, los switches Catalyst 29xx no cuentan con un puerto auxiliar.

Cuando un switch con Cisco IOS se enciende por primera vez, cuenta con una configuración por defecto que es suficiente para que inicie operaciones básicas de capa 2. En comparación, un router Cisco IOS al encenderse por primera vez cuenta con una configuración por defecto que no es suficiente para su operación básica.

Terminal de Consola

- Conexión física: cable consola (rollover) con conector RJ-45 desde un puerto COM de una terminal al puerto consola del dispositivo.
- Requiere la utilización de un programa de emulación de terminal (p.e. Putty u otro semejante) configurado de la siguiente forma:
 - 9600 baudios.
 - Bits de datos: 8.

- Paridad ninguna.
- Bit de parada 1.
- Control de flujo ninguno.
- Por defecto no requiere clave de acceso.

Terminal Remota

- Conexión física: cable consola con conector RJ-45 desde un módem telefónico al puerto auxiliar del dispositivo.
- Se necesita un módem telefónico de 14.400 bps.
- Requiere la utilización de un programa de emulación de terminal (p.e. Putty).
 - 9600 baudios.
 - Bits de datos.
 - Paridad ninguna.
 - Bit de parada 1.
 - Control de flujo por hardware.
- Por defecto no requiere clave de acceso.

Terminales Virtuales

Una vez que se ha realizado la configuración básica es posible acceder al management a través de la dirección IP del dispositivo.

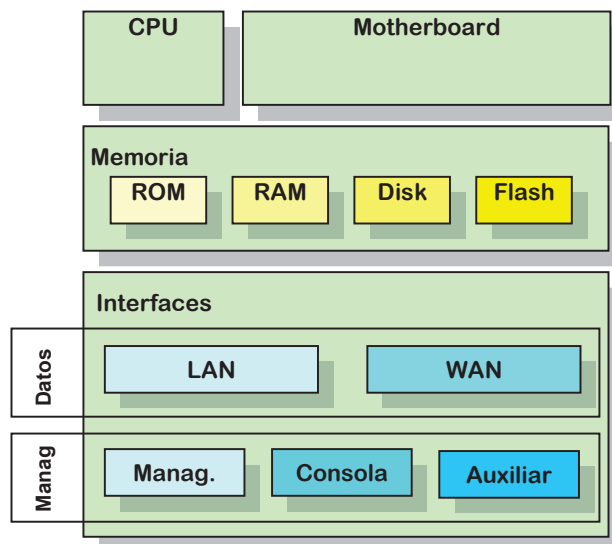
- Conexión física: se accede desde una terminal conectada a la red en cualquier punto de la misma.
- Requiere que al menos la interfaz por la que se desea acceder esté configurada y accesible a través de la red.
- Por defecto requiere clave.
- Estas terminales virtuales permiten acceder:
 - Utilización Telnet.
 - Utilizando SSH.

Consola	Auxiliar	Terminal Virtual
En el router: Puerto CON	En el router: Puerto AUX	En el router: Puerto de red
En la terminal: Puerto COM o USB	Módem telefónico	En la terminal: Puerto Ethernet.
Cable Consola	Cable Consola	Cable derecho.
No solicita clave por defecto	No solicita clave por defecto	Solicita clave por defecto.
Programa de emulación de terminales.	Programa de emulación de terminales.	Telnet, SSH.
Out band.	Out band.	In band.

Componentes de Hardware de un dispositivo

- CPU.
Ejecuta las instrucciones del sistema operativo incluyendo la inicialización del sistema.
- Motherboard.
Circuito central del dispositivo, que contiene los componentes electrónicos críticos del sistema.
- ROM
Memoria no volátil de solo lectura que contiene el microcódigo que permite a la CPU realizar las funciones básicas para iniciar y mantener el dispositivo. Incluye el Bootstrap y el POST.
Contiene también el monitor de ROM que es un sistema operativo de bajo nivel que se utiliza para tareas de prueba y resolución de problemas.
- RAM.
Memoria volátil de lectura y escritura que almacena datos durante su procesamiento por la CPU. Contiene la imagen de Cisco IOS en ejecución, el archivo de configuración activo, las tablas de enrutamiento y los buffers de paquetes.
- NVRAM.
Memoria no volátil de lectura y escritura utilizada para almacenar una copia de respaldo del archivo de configuración y el registro de configuración.
- Memoria Flash.
Memoria no volátil de lectura y escritura utilizada primariamente para almacenar la imagen de Cisco IOS.
- Disk.
Unidades de almacenamiento digital de datos no volátiles de acceso aleatorio.

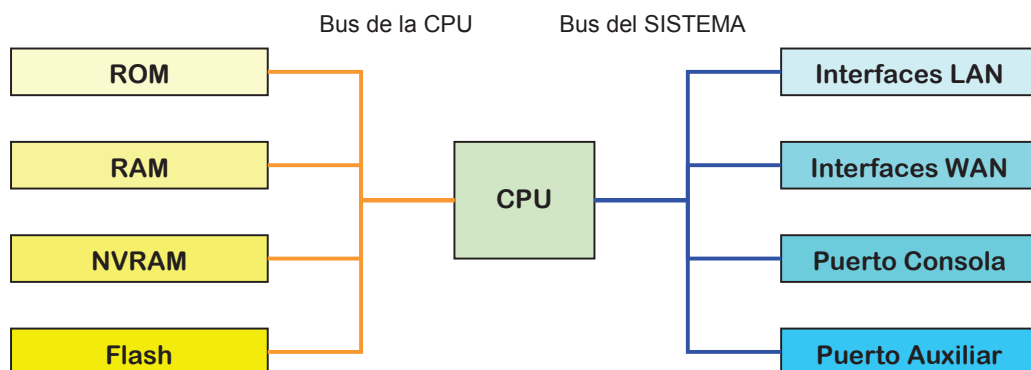
- Interfaces.
Conectan físicamente el dispositivo a las diferentes redes.
Los dispositivos pueden contar con diferentes tipos de interfaces:
 - LAN.
Permiten conectar el router a diferentes segmentos de red.
 - WAN.
Integran el dispositivo con diferentes redes WAN. Es propio de los routers contar con este tipo de interfaces.
 - Puertos consola, auxiliar y de management.
No son puertos de networking. Son puertos utilizados para tareas de administración.
El puerto auxiliar se utiliza para management remoto, típicamente a través de un módem telefónico.
Algunos dispositivos tienen puertos Ethernet utilizados exclusivamente para propósitos de administración. A estos puertos se puede asignar una dirección IP que pertenezca a la subred de management.



CPU	Ejecuta las instrucciones del sistema operativo incluyendo la inicialización del sistema.
Memoria	Almacena:
ROM	POST Bootstrap
RAM	Archivo de configuración Tablas de enrutamiento Buffers de paquetes Ejecución del IOS

NVRAM	Archivo de configuración de respaldo
Flash	Imagen del sistema operativo
Bus	
Bus del Sistema	Comunica la CPU con las interfaces y las ranuras de expansión.
Bus de CPU	Comunica la CPU con los componentes de almacenamiento.
Interfaces	
Conectan el dispositivo a las diferentes redes.	
LAN	Permiten conectar el router a diferentes tecnologías LAN.
WAN	Integran el dispositivo con diferentes redes WAN.
Puerto Manag.	No son puertos de networking. Son puertos utilizados para tareas de administración.
Puerto Consola	
Puerto Auxiliar	
Fuente de alimentación	Proporciona la energía necesaria para operar los diferentes componentes.

Esquema Básico de la Estructura de hardware del Router



Modos

Cisco IOS ofrece 3 entornos o modos básicos de operación por línea de comando:

- Modo Setup.
- Modo Monitor.
- Modo EXEC.

Modo Setup o Inicial

Este modo permite realizar una configuración en modo asistido, cuando no hay una configuración para el arranque. Ofrece un asistente que guía a través de los principales pasos utilizando una secuencia de preguntas.

Ofrece 2 posibilidades: setup básico y setup extendido.

El modo setup está disponible en routers y switches que corren Cisco IOS. De la misma manera, los switches y router que corren Cisco IOS si no encuentran un archivo de configuración pueden iniciar un procedimiento denominado autoinstall para buscar un archivo de configuración desde un servidor TFTP a través de las interfaces LAN o seriales que tengan conexión de red.


Modo monitor de ROM

Puede ser utilizado para realizar un arranque manual del dispositivo y en los procesos de recuperación de claves.

Este modo solo es accesible a través de una conexión de consola y en un modo de operación normal se accede al interrumpir el proceso de arranque.

Cisco IOS

Cuando se trabaja con una imagen completa del Cisco IOS, esta está dotada de un intérprete de servicios conocido como EXEC; luego de que cada comando es ingresado lo valida y lo ejecuta. Por motivos de seguridad las sesiones EXEC se encuentran divididas en 2 modos. Modo EXEC usuario y modo EXEC privilegiado.

 Entornos básicos de operación por CLI de Cisco IOS:

- Setup o inicial.
- Monitor.
- Cisco IOS.

Por motivos de seguridad las sesiones EXEC se encuentran divididas en 2 niveles de acceso: modo usuario y modo privilegiado.

Cada uno de los modos de operación de IOS puede identificarse por el prompt del sistema operativo:

Modo monitor de ROM

```
rommon>  
>
```

Modo EXEC usuario

```
Router>
```

Modo EXEC privilegiado

```
Router>enable  
Router#
```

La línea de comando (CLI) de Cisco IOS

Comandos de ayuda

Cisco IOS ofrece un completo sistema de asistencia en línea para el operador que incluye:

- Menú de ayuda.
- Comandos de edición.
- Mensajes de error.
- Avisos de cambio de estado en línea.

```
Router#cl?  
clear  clock
```

```
Router#clock ?  
set    Set the time and date
```

```
Router#clock set ?  
hh:mm:ss  Current Time
```

```
Router#clock set _
```

Comandos de edición

El conjunto de comandos de edición incluye, entre otros, los que se enumeran a continuación:

Ctrl	+ A	[ahead] Desplazarse al comienzo de la línea de comando.
	+ E	[end] Desplazarse al final de la línea de comando.
	+ B	[back] Desplazarse un carácter hacia atrás.
	+ F	[forward] Desplazarse un carácter hacia adelante.
	+ P / ↑	[previous] Trae el comando que se ingresó antes.
	+ N / ↓	[next] Trae al prompt el comando que se ingresó después.
	+ Z	Concluye el modo configuración y regresa a privilegiado.
	+ C	Sale del modo setup.
Esc	+ B	[back] Desplazarse una palabra hacia atrás.
	+ F	[forward] Desplazarse una palabra hacia adelante.
Retroceso		Borra un carácter a la izquierda del cursor.

Tab

Completa un comando introducido parcialmente.



Regla mnemotécnica:

La letra que se utiliza en la combinación de teclas es la primera letra de la palabra en inglés que identifica la acción.

Router>**show history**

Muestra los últimos comandos almacenados en el buffer de comandos.

Router>**terminal history size [líneas]**

Define el tamaño del buffer de comandos. Por defecto es de 10 comandos.

Mensajes de error en el ingreso de comandos:

Los mensajes de error de Cisco IOS se identifican fácilmente por estar precedidos por el signo de porcentual (%).

Router#cl

% **Ambiguous command:** "cl"

Router#clock

% **Incomplete command.**

Router#clock sot

^

% **Invalid input detected at '^' marker.**

Router#clack

Translating "clack"...domain server (255.255.255.255)

Translating "clack"...domain server (255.255.255.255)

(255.255.255.255)% Unknown command or computer name, or unable to find computer address

Comandos show

En la CLI de Cisco IOS los comandos **show** permiten acceder a información de configuración, operación o estadísticas de diferentes protocolos o sistemas. Cada función o protocolo tiene sus propios comandos **show**, del mismo modo que otros comandos permiten verificar los aspectos globales de operación y estado del dispositivo:

Switch#**show version**

Permite verificar la configuración de hardware, la imagen y versión de IOS que está utilizando el dispositivo, la ubicación desde la que se leyó la imagen de IOS, la disponibilidad de memoria y el registro de configuración entre otros valores.

Switch#**show flash**

Permite verificar el contenido de la memoria flash incluyendo el nombre de los archivos y sus dimensiones. También indica la memoria flash disponible y cuánto está siendo utilizado.

Modo de configuración global

Es el modo que permite acceder a los comandos de configuración de todo el dispositivo. A partir de este punto se abren diferentes submodos para las diferentes tareas de configuración (interfaz, protocolo de enrutamiento, etc.).

En este modo no son accesibles directamente los comandos **show** ni los comandos **copy**.

```
Switch>enable
Switch#configure terminal
Switch(config)#_
```

Modo de configuración global.

Permite definir parámetros que se aplican a todo el dispositivo.

```
Switch(config)#interface fastethernet 0/0
Switch(config-if)#exit
```

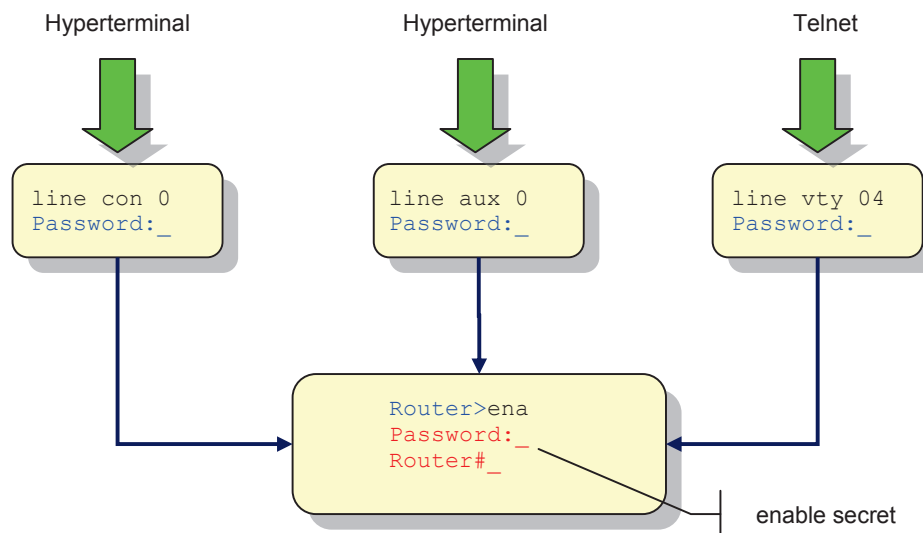
Modo de configuración de la interfaz.

```
Switch#_
Switch(config-if)#Ctrl + Z
Switch#_
```

Claves de acceso

Clave de acceso a modo usuario. Se configuran diferentes claves de acceso de acuerdo al modo de conexión.

- Clave de acceso por consola.
- Clave de acceso por puerto auxiliar.
- Clave de acceso por terminal virtual.
Es requerida por defecto y si no está configurada no se podrá acceder al router por Telnet o http.
- Clave de acceso a modo privilegiado.



Procedimiento de configuración de un Router Cisco

Supondremos que estamos trabajando en la consola de un router Cisco 2911, con un sistema operativo Cisco IOS 15.1(4).

Cada uno de los features incluidos en esta configuración será descrito en el capítulo correspondiente. Se incluyen en este punto con el solo propósito de generar un procedimiento de configuración completo, no parcial.

1. Ingrese en el modo privilegiado

```
Router>enable
```

2. Configuración de parámetros globales:

2.1. Nombre del dispositivo

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname LAB_A
LAB_A(config)#ip name-server 192.5.5.18
LAB_A(config)#ip domain-lookup
LAB_A(config)#banner motd #Dispositivo de pruebas#
LAB_A(config)#service password-encryption
LAB_A(config)#username cisco password 0 cisco
LAB_A(config)#ip domain-name muydomain.com
LAB_A(config)#crypto key generate rsa
LAB_A(config)#ip ssh version 2
```

2.2. Habilitación del acceso por consola y por terminal virtual

```
LAB_A(config)#line vty 0 4
LAB_A(config-line)#login
LAB_A(config-line)#password cisco
```



```
LAB_A(config-line)#exec-timeout 5 0
LAB_A(config-line)#transport input ssh
LAB_A(config-line)#exit
```



El procedimiento descrito hasta aquí habilita el acceso por terminal virtual. Tenga en cuenta que por defecto está habilitado el login (se requiere autenticación de clave para acceder), y si no se configura una clave será rechazada toda solicitud utilizando telnet.

```
LAB_A(config)#line con 0
LAB_A(config-line)#login
LAB_A(config-line)#password cisco
LAB_A(config-line)#exec-timeout 5 0
LAB_A(config-line)#logging synchronous
LAB_A(config)#line aux 0
LAB_A(config-line)#login
LAB_A(config-line)#password cisco
LAB_A(config-line)#exec-timeout 5 0
LAB_A(config-line)#^Z
%SYS-5-CONFIG_I: Configured from console by console
LAB_A#copy run start
Building configuration...
[OK]
```

2.3. Configuración de clave de acceso al modo privilegiado

```
LAB_A#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
LAB_A(config)#enable password cisco
LAB_A(config)#enable secret class
LAB_A(config)#^Z
%SYS-5-CONFIG_I: Configured from console by console
LAB_A#copy run start
Building configuration...
[OK]
```

3. Configuración de las interfaces

3.1. Interfaz LAN

```
LAB_A#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
LAB_A(config)#interface gigabitethernet 0/0
LAB_A(config-if)#ip address 192.5.5.1 255.255.255.0
LAB_A(config-if)#description Gateway de la LAN de Ingenieria
LAB_A(config-if)#no shutdown
```



Atención, Cisco IOS coloca todas las interfaces en modo inactivo (shutdown) por defecto, por lo que es necesario ejecutar este comando para que la interfaz comience a operar, aún cuando esté configurada.

Por este motivo, cuando se copia una configuración en modo texto, debe editarse para agregar este comando en cada interfaz.

```
%LINEPROTO-5-UPDOWN:Line protocol on Interface GigabitEthernet0/0,
changed state to up
%LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to up
```

3.2. Interfaz WAN

```
LAB_A(config-if)#interface serial 0/0/0
LAB_A(config-if)#description Puerto de conexión con la red LAB_B
LAB_A(config-if)#ip address 201.100.11.1 255.255.255.0
LAB_A(config-if)#clock rate 64000
LAB_A(config-if)#bandwidth 64
LAB_A(config-if)#no shutdown
%LINEPROTO-5-UPDOWN:Line protocol on Interface Serial0/0/0, changed
state to up
%LINK-3-UPDOWN: Interface Serial0/0/0, changed state to up
```

3.3. Interfaz lógica

```
LAB_A(config-if)#interface loopback 0
LAB_A(config-if)#description Interfaz de administracion
LAB_A(config-if)#ip address 10.0.0.1 255.255.255.255
LAB_A(config-if)#exit
LAB_A(config)#exit
%SYS-5-CONFIG_I: Configured from console by console
```

4. Configuración del enrutamiento

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

 En las versiones actuales de Cisco IOS, el enrutamiento IP está habilitado por defecto.

4.1. Protocolo de enrutamiento

```
LAB_A(config)#router rip
LAB_A(config-router)#version 2
LAB_A(config-router)#network 192.5.5.0
LAB_A(config-router)#network 201.100.11.0
LAB_A(config-router)#network 10.0.0.0
LAB_A(config-router)#exit
```

4.2. Rutas estáticas

```
LAB_A(config)#ip route 196.17.15.0 255.255.255.0 201.100.11.2
LAB_A(config)#ip route 207.7.68.0 255.255.255.0 201.100.11.2 130
LAB_A(config)#ip route 0.0.0.0 0.0.0.0 201.100.11.2
LAB_A(config)#^Z
```

```
%SYS-5-CONFIG_I: Configured from console by console
LAB_A#copy run start
Building configuration...
```

[OK]


Configuración de direccionamiento IPv6

```
Router#configure terminal
Router(config)#ipv6 unicast-routing
Router(config)#ipv6 router rip RTE
Router(config)#interface fastethernet 0/0
Router(config-if)#ipv6 address 2001:ab1:32F4:1::1/64
Router(config-if)#ipv6 address 2001:ab1:32F4:1::/64 eui-64
Router(config-if)#ipv6 rip RTE enable

Router#show ipv6 interface FastEthernet 0/0
Router#show ipv6 rip
Router#show ipv6 route
```

Comandos show:

Los comandos `show` permiten verificar y monitorear el estado de configuración de diferentes componentes (interfaces, archivos de configuración, etc.) y estadísticas de funcionamiento de routers y switches que implementan Cisco IOS.

 La mayoría de estos comandos funcionan solamente en el modo privilegiado. Hay un subconjunto reducido que es accesible en modo usuario.

 No están disponibles en el modo configuración global y sus submodos.

Comandos para la visualización de los archivos de configuración

Switch#`show startup-config`

Muestra el contenido del archivo de configuración de respaldo que se almacena en la memoria NVRAM.

La respuesta está encabezada por el mensaje `Using xxxx out of xxxxxx bytes` para indicar la cantidad de memoria utilizada para almacenar el archivo.

Switch#`show running-config`

Muestra el contenido del archivo de configuración activo en la memoria RAM del dispositivo.

Se puede identificar por el texto `Current configuración...` que la encabeza, y que va

acompañado por la medida del archivo expresada en bytes.

```
Current configuration:
!
version 15.1
```

Indica la versión del sistema operativo Cisco IOS actualmente corriendo en el dispositivo.

```
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
```

Indica el estado del servicio de encriptación de claves. En este caso no está activo.

```
!
hostname LAB_A
```

Nombre asignado al dispositivo.

```
!
enable secret 5 $1$TXpV$PmHtTS8FqkaMVJce3qa9t.
```

Contraseña secreta de acceso al modo privilegiado codificada con encriptación de nivel 5.

```
!
username LAB_B password 0 cisco
```

Nombre de usuario y contraseña correspondiente (sin encriptar pues el servicio no ha sido activado). En este caso, pueden ser utilizados por una interfaz con autenticación chap.

```
!
license udi pid CISCO2911/K9 sn FTX15247QJ1
!
!
Spanning-tree mode pvst
!
!
!
ip name-server 172.16.30.56
```

Indica la dirección del servidor de nombre asignado.

```
!
interface GigabitEthernet0/0
```

A partir de aquí comienza la descripción de la interfaz GigabitEthernet 0/0.

```
description Red LAN de produccion
```

Comentario del administrador para describir la interfaz.

```
ip address 172.16.30.1 255.255.255.0
```

Indica la dirección de red y máscara de subred asignadas a la interfaz.

```
duplex auto
speed auto
!
```

```

interface GigabitEthernet0/1
  no ip address
  duplex auto
  speed auto
  shutdown
!
interface GigabitEthernet0/2
  no ip address
  duplex auto
  speed auto
  shutdown
!
interface Serial0/0/0
  description Puerto de conexión con la red de la sucursal Lomas
  ip address 172.16.10.2 255.255.255.0
  clock rate 64000

bandwidth 64
ip access-group 10 in

!
interface Serial0/0/1
  ip address 172.16.20.1 255.255.255.0
  encapsulation ppp

bandwidth 64
!
!
interface Vlan1
  no ip address
  shutdown
!
!
access list 10 deny host 172.16.40.3
access list 10 permit any

!
router rip
network 172.16.0.0

!
ip classless

```

Indica el valor del reloj de sincronización asignado para este puerto serial, que debe tener conectado un cable DCE. El valor indica el ancho de banda en bps que tendrá este enlace.

Indica que se ha asociado a este puerto la lista de acceso IP estándar 10 para que filtre el tráfico entrante.

Esta interfaz utiliza el estándar ppp para la encapsulación de tramas.

Muestra las listas de acceso configuradas en este dispositivo.

Protocolo de enrutamiento configurado y redes directamente conectadas que “escucha” el protocolo.

Utiliza las reglas de enrutamiento classless.

```

!
ip http server
no ip http secure-server
!
line con 0
  password cisco
  login
  logging synchronous
line aux 0

```

Presenta los valores de configuración de acceso a través de los puertos consola y auxiliar.

```
line vty 0 4
```

Presenta los valores de configuración del acceso a través de terminales virtuales.

```
exec-timeout 5 0
```

Indica que la sesión de terminal virtual se dará por concluida transcurridos 5 minutos sin actividad.

```
password cisco
```

Indica la clave para acceso a través de terminales virtuales.

```
login
```

Indica que está activado el servicio de requerimiento de clave de acceso.

```

!
end

```

Fin del archivo de configuración activo.



Los features incluidos en esta configuración serán descriptos en los capítulos correspondientes. Se incluyen en este punto con el solo propósito de mostrar un archivo de configuración completo, no parcial.

Comando para visualización de la memoria flash

```
Router#show flash
```

```

System flash directory:
File   Length   Name/status
  3    33591768 c2900-universalk9-mz.SPA.151-4.M4.bin
  2     28282  sigdef-category.xml
  1     227537  sigdef-default.xml
[33847587 bytes used, 221896413 available, 255744000 total]
249856K bytes of processor board System flash (Read/Write)

```

Comandos para la visualización de las interfaces

```
Router#show interfaces serial 0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is HD64570
  Description: Puerto de conexion con la red de la sucursal Lomas
  Internet address is 172.16.10.2/30
  MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
    Conversations 0/0/256 (active/max active/max total)
    Reserved Conversations 0/0 (allocated/max allocated)
    Available Bandwidth 48 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 packets output, 0 bytes, 0 underruns
    0 output errors, 0 collisions, 1 interface resets
    0 output buffer failures, 0 output buffers swapped out
    0 carrier transitions
  DCD=down DSR=down DTR=down RTS=down CTS=down
```

Posibles resultados de la primera línea de show interfaces

Serial0/0/0 is _____, line protocol is _____

La primera porción indica el estado de la porción de hardware (capa 1) de la interfaz; la segunda porción indica el estado de la porción lógica (capa 2).

Serial0/0/0 is **administratively down**, line protocol is **down**

Interfaz que no ha sido habilitada por el Administrador.

Serial0/0/0 is **down**, line protocol is **down**

Indica problemas de capa física.

Serial0/0/0 is **up**, line protocol is **down**

Denota un problema de conexión por un posible fallo en la capa de enlace de datos.

Serial0/0/0 is **up**, line protocol is **down (disabled)**

Debido a un problema con el proveedor de servicio hay un elevado porcentaje de error o hay un problema de hardware.

Serial0/0/0 is **up**, line protocol is **up**

Interfaz plenamente operativa a nivel de capa 1 y 2.

Una presentación sintética del estado de las interfaces

Router#**show ip interfaces brief**

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0	172.16.2.1	YES	NVRAM	up	up
Loopback0	10.50.0.3	YES	NVRAM	up	up
Serial0/0/0	unassigned	YES	manual	up	up
Serial0/0/0.20	172.16.100.6	YES	manual	down	down
Serial0/0/0.21	172.16.100.10	YES	manual	up	up
Serial0/0/1	unassigned	YES	NVRAM	admin. down	down

Otros comandos show

Router#**show ip route**
Router#**show ip protocols**
Router#**show controllers**
Router#**show processes cpu**
Router#**show processes memory**
Router#**show tcp [line-number]**
Router#**show tcp brief [all]**

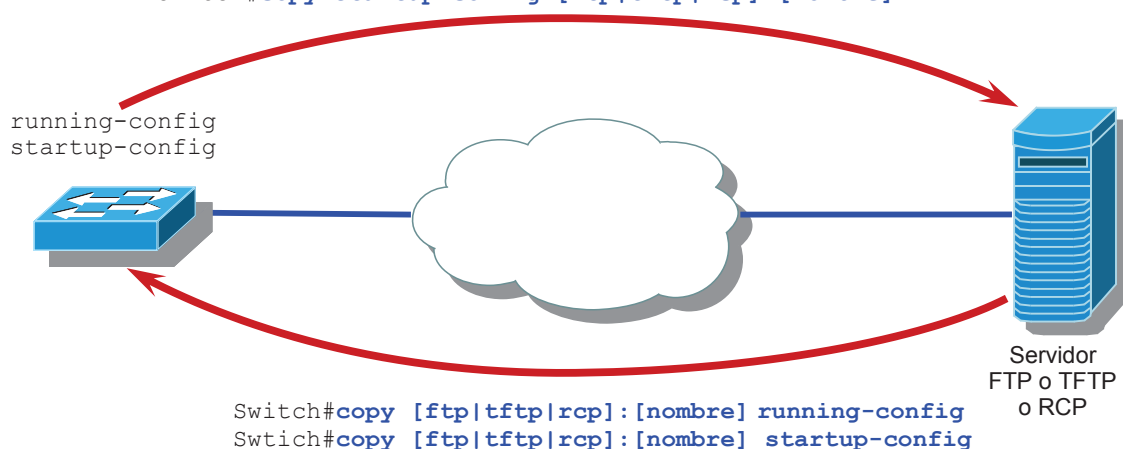
Administración del archivo de configuración

Los dispositivos IOS mantienen 2 archivos de configuración:

- El archivo de configuración activo o running-config, que se mantiene en la memoria RAM.
- El archivo de configuración de respaldo o startup-config que se almacena en la memoria NVRAM para ser leído a la RAM en el momento de arrancar el dispositivo.

Ambos archivos pueden ser copiados hacia o desde diferentes servidores (FTP, TFTP, RCP), según sea necesario en cada red:

```
Switch#copy running-config [ftp|tftp|rcp] : [nombre]  
Switch#copy startup-config [ftp|tftp|rcp] : [nombre]
```



El comando copy

Es el comando del sistema de archivos de IOS que permite copiar desde y hacia diferentes fuentes diversos elementos, tales como el archivo de configuración.

El comando se ejecuta en modo privilegiado, y su estructura básica es:

```
Switch#copy [origen]:[nombre] [destino]:[nombre]
```

Tanto origen como destino pueden ser especificados utilizando la convención de URL para indicar archivos sobre dispositivos específicos en la red: bootflash: | flash: | ftp: | nvram: | rcp: | slot0: | slot1: | system: | tftp:

```
Switch#copy running-config tftp:
```

Copia el archivo de configuración activo a un servidor TFTP.

Una serie de signos de exclamación (!) muestran el progreso del proceso de copia.

```
Switch#copy tftp: running-config
```

Recupera el archivo de configuración que ha sido almacenado previamente en un servidor TFTP.

```
Switch#copy running-config startup-config
```

Sobrescribe el archivo de configuración de respaldo con el archivo de configuración activo actualmente en la RAM.

Pruebas de conectividad de la red

Prueba de conexiones utilizando el comando ping

```
Router#ping [protocol] {host | address}
```

Si se omite el parámetro de protocolo, Cisco IOS asume por defecto IP.

Las respuestas posibles cuando se ejecuta el comando desde la línea de comando de un router Cisco IOS son:

- | | |
|---|---------------------------------------|
| ! | Se recibe exitosamente un echo reply. |
| . | Indica tiempo de espera agotado. |
| U | El destino es inalcanzable. |
| C | Indica congestión en la ruta. |
| / | Ping interrumpido. |

Esta prueba puede realizarse desde el modo usuario en su formato básico; desde el modo privilegiado está disponible tanto en el formato básico como en el extendido.

```
Router#ping
Protocol [ip]:
Target IP address: 172.16.1.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
32/34/36 ms
```

Algunos resultados posibles del diagnóstico utilizando `ping` desde una terminal:

- `ping 127.0.0.1` – Prueba interna de loopback.
- `ping [propia IP]` – Verifica la configuración de la dirección IP.
- `ping [IP del gateway]` – Verifica si se puede alcanzar el gateway.
- `ping [IP remota]` – Verifica la conectividad a un dispositivo remoto.

Prueba para el descubrimiento de rutas

El descubrimiento o “trazo” de rutas se puede realizar utilizando el programa `traceroute` presente en Cisco IOS.

Utiliza igual que `ping` el protocolo ICMP.

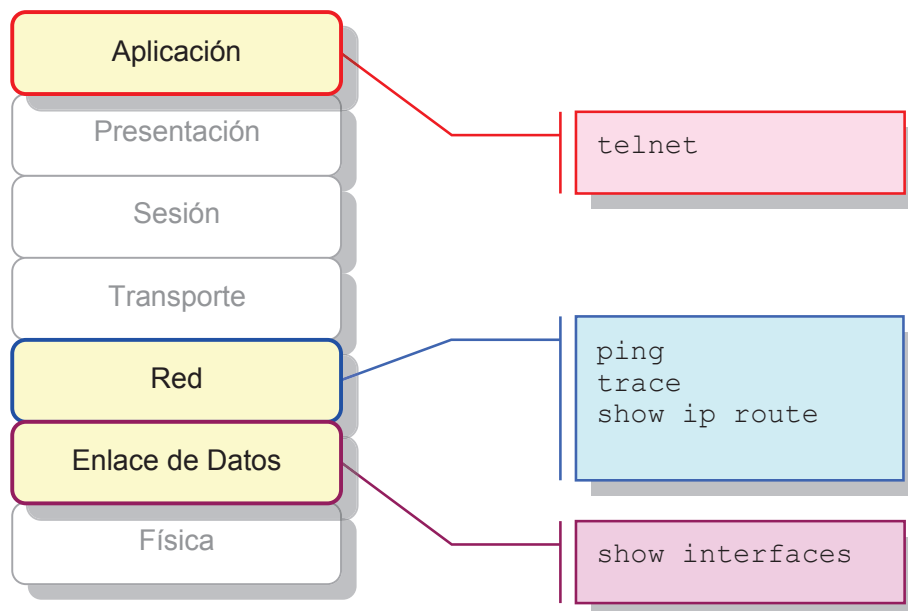
```
Router#traceroute [protocol] [destination]
```

Las respuestas posibles cuando se ejecuta el comando desde la línea de comando de un router Cisco son:

- | | |
|-----------------|-------------------------------------|
| <code>!H</code> | El router no ha enviado el comando. |
| <code>P</code> | El protocolo es inalcanzable. |
| <code>N</code> | La red es inalcanzable. |
| <code>*</code> | Time out |

Prueba de conectividad completa extremo a extremo

Con este propósito se utiliza el protocolo `telnet`, ya que es un protocolo de capa de aplicación. Su ejecución exitosa asegura conectividad completa extremo a extremo.



Comandos de visualización y diagnóstico en DOS

Los más importantes para el examen de certificación son:

```
C:>ipconfig
C:>ipconfig/all

C:>ping localhost
C:>ping 127.0.0.1
C:>ping [IP]

C:>tracert [IP]
```

Secuencia o rutina de Inicio

Cuando se enciende un dispositivo Cisco se realizan 3 operaciones principales: se verifica el hardware del dispositivo, se carga una imagen de sistema operativo y se aplica una configuración.

En primer lugar, se ejecutan las rutinas de verificación inicial del hardware:

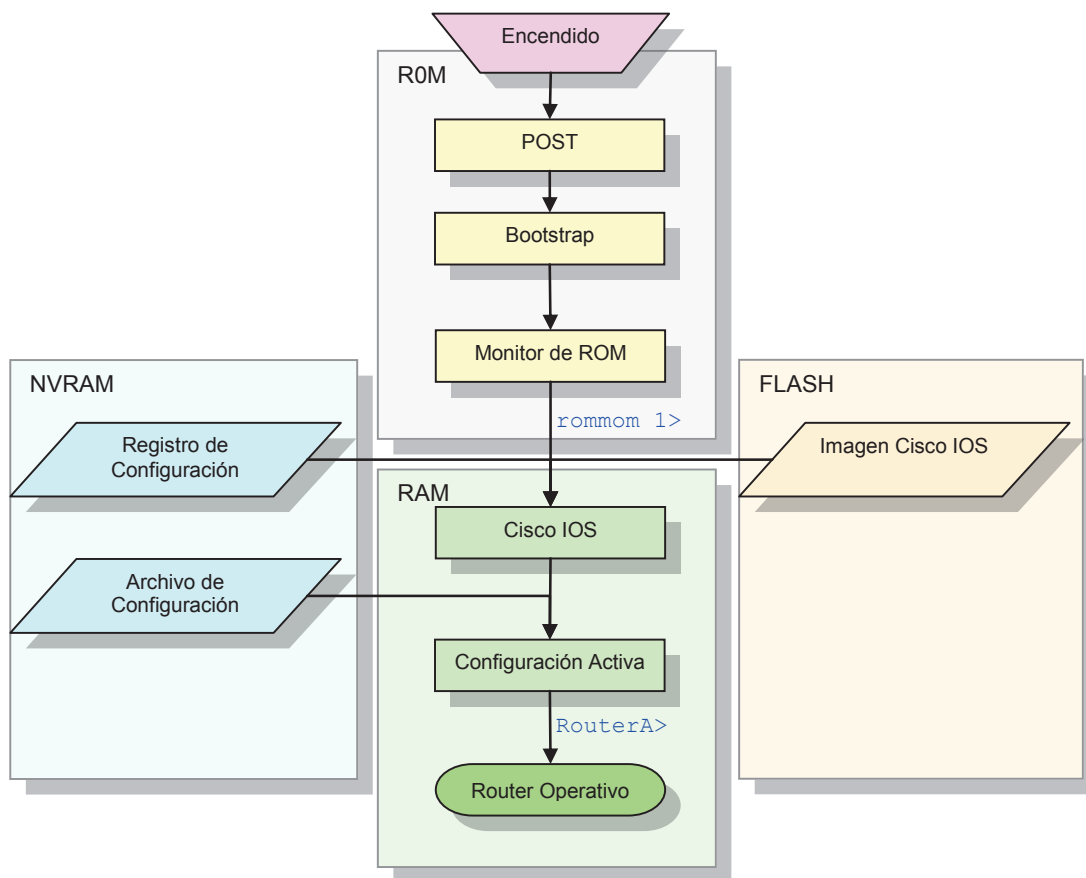
- El dispositivo es encendido.
- Se ejecuta el POST del dispositivo desde la ROM.

A continuación, se ejecutan las rutinas de inicio que concluyen con la carga del sistema operativo.

- Carga el Bootstrap que se encuentra en la ROM y lo ejecuta.
- Carga el Monitor de ROM y lo ejecuta.
- El Monitor de ROM revisa el campo de booteo del registro de configuración para obtener información sobre el lugar en el que buscar la imagen del sistema operativo.
 - Si el último dígito del campo de booteo es 0 (p.e. 0x2100), no continua y entra en el modo monitor de ROM.
 - Si el último dígito es 1 (p.e. 0x2101), se carga la primera imagen disponible en la memoria flash.
 - Si el último dígito está entre 2 y F (p.e. 0x2102) carga la primer imagen válida especificada utilizando los comandos `boot system`.
 - Los comandos `boot system` se ejecutan de modo secuencial, de acuerdo al orden en que fueron ingresados.
 - Si todos los comandos `boot system` fallan, intenta bootear con la primer imagen válida de la memoria flash.
 - Si no encuentra una imagen válida en la flash, intentará 5 veces encontrar un servidor TFTP con una imagen que utilice el nombre por defecto.
 - Si no encuentra una imagen válida del IOS, inicializa la imagen de booteo almacenada en la ROM, cuando existe.
 - Si esta opción no es válida, el sistema mostrará el prompt del monitor de ROM y esperará la intervención del usuario.
- Carga la imagen del sistema operativo a la RAM. Algunos dispositivos ejecutan IOS directamente desde la flash.

Finalmente, el dispositivo busca un archivo de configuración y lo aplica.

- Busca un archivo de configuración válido.
 - Si encuentra un archivo válido, lo carga en la RAM y lo ejecuta.
 - Si no encuentra un archivo válido, ingresa en el modo setup y pide al operador que ingrese parámetros de configuración o inicia el proceso de autoinstall.



Sintetizando:

- Se enciende el dispositivo.
- Ejecuta el POST.
- Carga del Bootstrap.
- Lee el Registro de Configuración.
- Carga el Cisco IOS.
- Carga del Archivo de Configuración.

El Registro de Configuración

Se trata de un registro de 16 bits de longitud guardado en una posición fija NVRAM y que contiene las instrucciones básicas para el arranque del dispositivo: dónde buscar la imagen del IOS, si debe leer o no la NVRAM, la velocidad del puerto consola, etc.

Se expresa en nomenclatura hexadecimal: 0x2102. Los caracteres 0x sólo indican que lo que se encuentra a continuación está expresado en hexadecimales.

Valor por defecto en routers: 0x2102

Los últimos 4 bits (el último dígito hexadecimal) conforman el campo de inicio (boot field) e indican el modo en que el dispositivo debe arrancar.

Valores más frecuentes:

- **0x2100**
El router no carga una imagen del IOS sino que ingresa en modo monitor ROM.
- **0x2101**
Indica que el dispositivo debe iniciar utilizando la imagen de IOS en la ROM. En las plataformas que no tienen esta posibilidad, indica que se arranca utilizando la primera imagen válida en la memoria flash.
- **0x2102 a 0x210F**
Indica al router que debe cargar los comandos `boot system` que se encuentran en la NVRAM.
Si no hay comando `boot system` configurado, se lee la primer imagen válida almacenada en la flash.
- **0x2142**
Indica que el router debe examinar los comandos `boot systems`, pero ignorar la configuración almacenada en la NVRAM, forzando el modo setup.

Modificación del registro de configuración

```
Router#configure terminal
```

```
Router(config)#config-register 0x2102
```

Modifica el valor actual del registro de configuración y lo define como 0x2102.

```
Router(config)#boot system flash [nombre]
```

```
Router(config)#boot system tftp [nombre]
```

Definen la fuente desde la cual se debe leer la imagen de IOS y el nombre de la misma.

```
Router#show version
```



El único comando que permite verificar el valor del registro de configuración es `show version`.

Comandos para copia de resguardo de la imagen de Cisco IOS



Como para esta tarea se utiliza el comando `copy`, se aplican en este caso todas las consideraciones respecto de la estructura del comando que se desarrollaron antes.

Para copiar una imagen del sistema operativo almacenada en un servidor tftp a la memoria flash del dispositivo:

```
Router#copy tftp:c2600-is-mz.121-5 flash:
```

Para hacer una copia de respaldo de la imagen del sistema operativo contenida en la memoria flash a un servidor tftp.

```
Router#copy flash:c2600-is-mz.121-5 tftp:
```

Procedimiento para recuperación de claves

El procedimiento es el que se describe a continuación:

Reinicie el dispositivo.

Interrumpa la secuencia de arranque para forzar el ingreso en el modo Monitor de ROM utilizando la combinación de teclas **Ctrl+Break**:

```
rommon 1>_
```

Cambie el registro de configuración de modo tal que al arrancar no busque el archivo de configuración en la NVRAM.

```
rommon 1>confreg 0x2142
```

Reinicie el router para que tome el nuevo registro de configuración.

```
rommon 2>reset
```

El router ingresará al modo de setup Salga del modo setup.

Ingrese al modo privilegiado.

```
Router>_  
Router>enable  
Router#_
```

Copie la configuración de la NVRAM a la RAM.

```
Router#copy startup-config running-config  
LAB_A#_
```

Cambie la clave de acceso a modo privilegiado por aquella que desea.

```
LAB_A#config terminal
LAB_A(config)#enable secret [clave]
```

Vuelva ahora el registro de configuración a su valor original.

```
LAB_A(config)#config-register 0x2102
```

Grabe en la startup-config los cambios realizados.

```
LAB_A#copy running-config startup-config
```

CDP Cisco Discovery Protocol

CDP es un protocolo de capa de enlace de datos, independiente de los medios y los protocolos de capa de red.

En los dispositivos Cisco, todas las interfaces son CDP activas por defecto.

Se propaga en formato de broadcast de capa 2.

Comandos CDP

```
Router#show cdp
Global CDP information:
    Sending CDP packets every 60 seconds
    Sending a holdtime value of 180 seconds
```

```
Router#configure terminal
Router(config)#cdp run
Router(config)#no cdp run
! Disable CDP Globally
```



Atención: CDP tiene 2 niveles de activación. Activación global es decir, en todo el dispositivo; y activación por interfaz. Sea cuidadoso, los comandos en cada caso son diferentes.

```
Router(config)#interface serial 0/0/0
Router(config-if)#cdp enable
Router(config-if)#no cdp enable
! Disable on just this interface
Router(config-if)#exit
Router(config)#cdp timer 90
Router(config)#cdp holdtime 270
```

```
Router#clear cdp counters
Router#clear cdp table
```

Monitoreo de información CDP

```
Router#show cdp ?
entry      Information for specific neighbor entry
interface  CDP interface status and configuration
```



```
neighbors    CDP neighbor entries
traffic      CDP statistics
<cr>
```

```
Router#show cdp neighborg
```

```
Capability Codes: R - Router, T - Trans Bridge, B - Source Route
                  Bridge, S - Switch, H - Host, I - IGMP,
                  r - Repeater
```

Dev.ID	Local Intrfce	Holdtme	Capability	Platform	Port ID
Sistemas	Gig 0/0	238	S I	WS-2960	Fa0/1
Central	Ser 0/0/0	138	R S I	2911	S0/0/0
Server	Ser 0/0/1	138	R S I	2911	S0/0/0

```
Router#show cdp entry [ID del dispositivo]
```

```
-----
Device ID: Router
Entry address(es):
  IP address: 10.9.9.3
Platform: Cisco 2911, Capabilities: Router
Interface: GigabitEthernet0/2, Port ID (outgoing port):
GigabitEthernet0/0
Holdtime : 133 sec
```

```
Version :
Cisco IOS Software, 2900 Software (C2900-UNIVERSALK9-M), Version
15.1(4)M4
, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thurs 5-Jan-12 15:41 by ccai
```

```
advertisement version: 2
Duplex: full
```

```
Router#show cdp entry *
Router#show cdp neighborg detail
Router#show cdp traffic
CDP counters :
```

```
  Packets output: 0, Input: 0
  Hdr syntax: 0, Chksum error: 0, Encaps failed: 0
  No memory: 0, Invalid packet: 0, Fragmented: 0
```

```
Router#show cdp interface [tipo] [ID]
```

Comandos relacionados con el acceso vía terminal virtual

Para conectarnos a las terminales virtuales de dispositivos remotos se puede utilizar la aplicación Telnet.

```
Router#telnet [IP/nombre]
Router#connect [IP/nombre]
Router#[IP/nombre]
```



Estos comandos son operativos tanto en modo usuario como privilegiado.

Verificación y visualización de las sesiones telnet

```
Router#show sessions
Router#show users
```

Para desplazarse entre diferentes sesiones telnet abiertas

```
Router#session limit

Router#telnet Router_B
Router_B#Ctrl+shift+6 luego x
Router#_

Router#[Enter]
Router_B#_

Router#resume #
Router_B#_

Router_B#exit
Router#_

Router_B#logout
Router#_

Router#disconnect [IP/Nombre]
Router#clear line #
```



Para profundizar o tener mayor información sobre cualquiera de estos puntos, sugiero consultar mi libro “Guía de Preparación para el Examen de Certificación CCNA”.

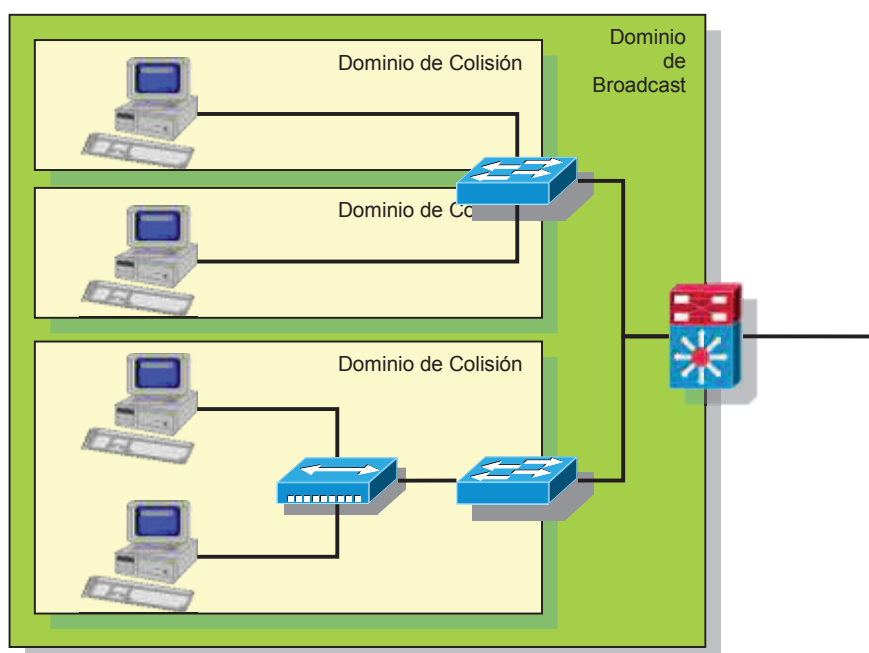
2.4. Conmutación LAN

Las redes LAN Ethernet están sometidas a múltiples limitaciones fruto de utilizar un medio compartido sometido a ruido y atenuaciones, y la existencia de condiciones operativas como la presencia potencial de colisiones y una ventana de tiempo asociada (ventana de colisiones).

Dominios de colisión y dominios de broadcast

La forma de expandir una red LAN Ethernet sin afectar la performance de la misma, es separando segmentos de red. Hay 2 formas de segmentar la red:

- **Dividir Dominios de Colisión.**
Es un segmento de red que comparte el ancho de banda disponible entre múltiples dispositivos terminales; como consecuencia cuando dos o más dispositivos conectados al mismo segmento intentan comunicarse entre sí es posible que se produzca una colisión.
En este sentido es deseable reducir el tamaño de los dominios de colisión, para lo cual se deben utilizar dispositivos que operan en la capa 2 o superiores del modelo OSI.
Los hubs extienden los dominios de colisión, mientras que switches y routers los limitan. Los switches reducen las colisiones y permiten una mejor utilización del ancho de banda en los segmentos de red, ya que ofrecen un ancho de banda dedicado para cada segmento de red.



- **Dividir Dominios de Broadcast.**
Se trata de una porción de red en la que, a pesar de que pudo haber sido segmentada en capa 2 es aún una unidad a nivel de capa 3 por lo que un paquete de broadcast es transmitido a todos los puertos conectados.
Si bien los switches filtran la mayoría de las tramas según las direcciones

MAC de destino, no hacen lo mismo con las tramas de broadcast. Un conjunto de switches interconectados forma un dominio de broadcast simple.

Para dividir dominios de broadcast es necesario implementar VLANs o dispositivos que operan en la capa 3 del modelo OSI, tales como switches multilayer o routers.

Características básicas de un switch

- Alta densidad de puertos.
- Gran disponibilidad de buffers de memoria para las tramas.
- Alta velocidad de los puertos.
- Conmutación interna más rápida.

Los switches permiten:

- Conectar segmentos de LAN aislando las colisiones.
- Utilizan tablas de direcciones MAC para identificar el puerto al que deben enviar la trama.
- Establecen comunicaciones dedicadas entre dispositivos.
- Permiten múltiples conversaciones simultáneas.
- Es posible establecer comunicaciones full dúplex.
- Adaptan la velocidad de transmisión a cada equipo terminal.

Operaciones básicas de un switch

- Conmutación de tramas
- Mantenimiento de operaciones
 - Aprendizaje de direcciones MAC
 - Resolución de bucles de capa 2.



Si un dispositivo de capa 2 no encuentra la dirección de destino de la trama en su tabla de direccionamiento, envía la trama por todos los puertos salvo por el puerto de origen (flooding).



Si un dispositivo de capa 3 no encuentra la dirección de destino del paquete en su tabla de enrutamiento, descarta el paquete.

Los switches permiten:

- Aislar el tráfico entre los segmentos y en consecuencia reducir el tamaño de los dominios de colisión.
- Obtener mayor disponibilidad de ancho de banda por usuario.



Los switches reducen el tamaño de los dominios de colisión, aumentando la cantidad de dominios de colisión existentes.

Métodos de conmutación

Dos métodos de conmutación básicos:

- Almacenamiento y envío.
El dispositivo recibe la trama completa, la copia a su memoria RAM y ejecuta un checksum para verificar la integridad de la trama antes de conmutar el paquete al puerto de salida en función de la dirección MAC de destino.
- Método de Corte.
La trama se envía al puerto de salida antes de que sea recibida completamente, lo que reduce notablemente la latencia.
El método de corte tiene dos variantes:
 - Conmutación rápida.
Envía el paquete inmediatamente después de leer la dirección MAC de destino.
 - Libre de fragmentos (Método de corte modificado).
Espera hasta recibir el byte 64 antes de conmutar la trama al puerto de salida.

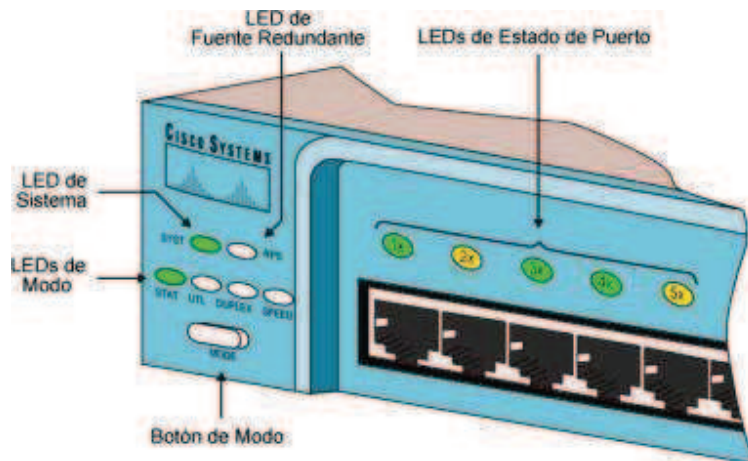
Método	Latencia	Control de errores
Almacenamiento y envío	Alta y variable según el tamaño de la trama	Ejecuta checksum
Conmutación Rápida	Fija. Más baja.	Ninguno
Libre de Fragmentos	Fija	Filtra paquetes menores de 64B

Cuando un switch recibe una trama de unicast utiliza la tabla de direcciones MAC para definir la acción a tomar:

- Si la dirección MAC de destino reside en el mismo segmento de red que el origen, la trama es filtrada (no se reenvía).
- Si la dirección MAC de destino reside en otro segmento de red, se reenvía al segmento correspondiente.

- Si la dirección MAC de destino no se encuentra en la tabla de direcciones, el switch hace flooding: la trama se trasmite a través de todos los puertos excepto aquel a través del cual se recibió.

La tabla de direcciones MAC se conforma con la información obtenida a partir del análisis de las direcciones MAC de origen de las tramas que se reciben en cada puerto del switch.



LEDs indicadores del switch

LED de sistema:

- Apagado: El sistema no está encendido.
- Verde: Sistema encendido y operacional.
- Ámbar: Error en el POST.

LED de fuente redundante:

- Apagado: Fuente redundante apagada o no instalada.
- Verde: Fuente operacional.
- Parpadeando en verde: La fuente no está disponible pues está proveyendo a otro dispositivo.
- Ámbar: La fuente redundante no está operacional.
- Parpadeando en ámbar: La fuente interna ha fallado y está operando la fuente redundante.

Port Stat

- Apagados: No hay un enlace activo.

- Verde: Enlace activo, sin actividad.
- Parpadeante en verde: Enlace activo con actividad de tráfico.
- Alternando verde y ámbar: Fallo en el enlace.
- Ámbar: puerto bloqueado administrativamente.

Configuración básica del switch Catalyst 2960



El dispositivo que se toma de base para el examen de certificación CCNA es el switch Cisco Catalyst 2960.

- Configuración de claves de acceso.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#username xxxxxx password 0 xxxxxx
Switch(config)#ip domain-name mydomain.com
```

Define un nombre de dominio por defecto que completa el hostname. Cuando no se define ningún nombre de dominio se utiliza por defecto cisco.com

```
Switch(config)#crypto key generate rsa
Switch(config)#ip ssh version 2
Switch(config)#line vty 0 15
Switch(config-line)#login local
Switch(config-line)#transport input ssh
Switch(config-line)#exit
Switch(config)#line con 0
Switch(config-line)#login
% Login disabled on line 0, until 'password' is set
Switch(config-line)#password [clave]
Switch(config-line)#exit
Switch(config)#enable secret [clave]
Switch(config)#service password-encryption
Switch(config)#ip http server
```

- Configuración del nombre del dispositivo.

```
Switch(config)#hostname Swtich_2960
```

- Configuración de una dirección IP.

```
Switch_2960(config)#interface vlan1
```

En los switches LAN la VLAN de management por defecto es la VLAN 1.

El comando crea una interfaz virtual para la VLAN 1, a la que se le puede asignar una dirección IP con propósitos de management.



¡Atención!: No se está configurando una IP en un puerto del switch. Es la dirección IP del dispositivo con propósito exclusivamente de administración.

```
Switch_2960(config-if)#ip address 172.16.5.2 255.255.255.0
Switch_2960(config-if)#no shutdown
```

Se requiere habilitar la interfaz administrativamente para que comience a ser operacional.

```
Switch_2960(config-if)#exit
Switch_2960(config)#ip default-gateway 172.16.5.1
```

Permite definir un default-gateway para el switch. No es necesario aplicar este comando en switches capa 3.

- Configuración de interfaces.

```
Switch_2960(config)#interface FastEthernet 0/1
```



Por defecto, todas las interfaces están en modo de auto negociación para velocidad y modo full / half-dúplex, y pertenecen a la VLAN 1.



A diferencia de las interfaces del router, las interfaces del switch están todas administrativamente habilitadas por defecto.

```
Switch_2960(config-if)#duplex full
Switch_2960(config-if)#speed 100
Switch_2960(config-if)#description puerto servidor 2
```

- Comandos de monitoreo

```
Switch_2960#show ip interface brief
Switch_2960#show mac-address-table
Switch_2960#clear mac-address-table
Switch_2960#show running-config
Switch_2960#show version
Switch_2960#show flash
```



Para revisar las prestaciones de los comandos `show` que son comunes con los routers, verifique los capítulos correspondientes.

```
Switch_2960#show flash
Directory of flash:/

 2  -rwx  736 Mar 1 1993 22:58:54 +00:00  vlan.dat
 3  drwx  512 Mar 1 1993 00:07:35 +00:00  c2960-lanbase-mz.122-35.SE
```


27998208 bytes total (19312640 bytes free)

Switch_2960#**show mac-address-table**

Mac Address Table

Vlan	Mac Address	Type	Ports
All	000a.f450.5d40	STATIC	CPU
All	0100.0ccc.cccc	STATIC	CPU
All	0100.0ccc.cccd	STATIC	CPU
All	0100.0cdd.dddd	STATIC	CPU
1	0004.75cd.b87e	DYNAMIC	Fa0/3
1	0007.eb33.aa19	DYNAMIC	Fa0/6
1	00e0.59aa.195b	STATIC	Fa0/23

Total Mac Addresses for this criterion: 7

Switch_2960#**clear mac-address-table**

Switch_2960#**show spanning-tree brief**

Control de acceso a la red switchheada

Cisco IOS incorpora en los switches una serie de funciones de seguridad avanzada denominadas port-security.

Port-security permite definir un conjunto específico o cantidad de direcciones MAC que pueden asociarse a un puerto en la tabla de direcciones MAC. De esta manera se limita la cantidad y cuáles son las direcciones MAC que pueden conectarse efectivamente a la red a través de un puerto específico.

Configuración de port-security:

Switch_2960 (config)#interface fastethernet [#]
Switch_2960 (config-if)#**switchport mode access**

Las características de port-security sólo se pueden aplicar a interfaces que se establecen en modo de acceso. Las interfaces del switch están por defecto en modo dinámico.

Switch_2960 (config-if)#**switchport port-security**

Habilita las funciones de port-security en el puerto.

Switch_2960 (config-if)#**switchport port-security maximum [#]**

Establece el número máximo de direcciones MAC que se permitirán en el puerto. Por defecto se permite solo una.

Switch_2960 (config-if)#**switchport port-security mac-address [MAC]**

Opcionalmente se pueden especificar las direcciones MAC que estarán permitidas en ese puerto.

Switch_2960 (config-if)#**switchport port-security violation [action]**

Define la acción que se tomará en este puerto en caso de que se reciba tráfico desde una dirección MAC no permitida.

Hay 3 acciones posibles:

`shutdown` – la interface se coloca en estado `errdisabled` y se genera un mensaje de error. Se requiere la intervención manual para que la interfaz vuelva a ser operativa.

`restrict` – deniega el tráfico considerado ilícito y genera un mensaje de error.

`protect` – deniega el tráfico considerado ilícito y no genera ningún mensaje.

Switch_2960 (config-if) # **switchport port-security mac-address sticky**

Permite limitar la utilización de la interfaz a una MAC específica, sin necesidad de ingresar la dirección propiamente dicha.

Convierte la dirección MAC aprendida dinámicamente en una entrada estática en la running-config.

Comandos de verificación:

Switch_2960# **show port-security**

Muestra las interfaces en las que se ha habilitado port-security. Adicionalmente presenta un contador y las acciones que se toman por interfaz.

Switch_2960# **show port-security interface [interfaz]**

Muestra la configuración de port-security en un puerto específico.

Switch_2960# **show port-security address**

Permite verificar las direcciones MAC que están asociadas a cada puerto como resultado de la utilización de port-security.

Optimización de performance de la red conmutada

Las redes Ethernet complejas tienen requerimientos particulares en función de la diversidad de dispositivos conectados, de capacidad de los enlaces y los requerimientos de redundancia. En función de esto, es necesario trabajar con tecnologías vinculadas a Ethernet que expanden su capacidad.

Determinación de dúplex y velocidad

La implementación de enlaces Ethernet full dúplex mejora significativamente la performance de los enlaces sin necesidad de cambiar el medio físico (cobre) utilizando en el enlace.

- Se utilizan 2 circuitos separados para transmitir y recibir, en un solo puerto.
- Es un entorno libre de colisiones. Se trata de conexiones punto a punto.
- Mejora realmente el ancho de banda del enlace ya que ambos extremos pueden transmitir simultáneamente.

Adicionalmente, en una red de mediana o gran complejidad encontramos enlaces de diferentes velocidades en diferentes puntos de la red. Para facilitar la operación

en un mismo enlace de puertos de diferente capacidad, se pueden utilizar las funciones de auto negociación previstas en el estándar.

Configuración de condiciones de dúplex y velocidad:

```
SwitchCore(config)#interface FastEthernet 0/1
SwitchCore(config-if)#dúplex full
```

Define el modo de operación dúplex del puerto.

Las opciones disponibles son `auto` | `full` | `half`. La opción por defecto es `auto`. En puertos 100Base FX la opción por defecto es `full`. La opción `half` no está disponible en puertos configurados para una interfaz Gigabit Ethernet.

```
SwitchCore(config-if)#speed 100
```

Permite definir la velocidad a la que operará el puerto.

Las opciones disponibles son `10` | `100` | `1000` | `auto` | `nonegotiate`.

```
SwitchCore(config-if)#description puerto servidor 2
```



Para utilizar auto negociación es necesario que ambos extremos del enlace la soporten. Si uno de los extremos no utiliza auto negociación tanto dúplex como velocidad deben definirse manualmente en ambos extremos.
En caso de no poder negociar IOS coloca el puerto en modo half dúplex.

Para verificar la operación de dúplex y velocidad:

```
SwitchCore#show interfaces FastEthernet 0/1
```

Spanning Tree Protocol

Redundancia en enlaces de capa 2

La implementación de redundancia de enlaces permite evitar la existencia de un único punto de fallos, pero al mismo tiempo puede generar algunos problemas:

- Tormentas de broadcast.
- Transmisión de múltiples copias de una misma trama.
- Inestabilidad de las tablas de direcciones MAC.

Spanning Tree Protocol

STP es un protocolo de capa 2 para administración de enlaces que permite implementar rutas redundantes a la vez que administra los potenciales bucles en la red, permitiendo que sólo exista una única ruta activa entre dos estaciones.

Hay diferentes variantes del protocolo:

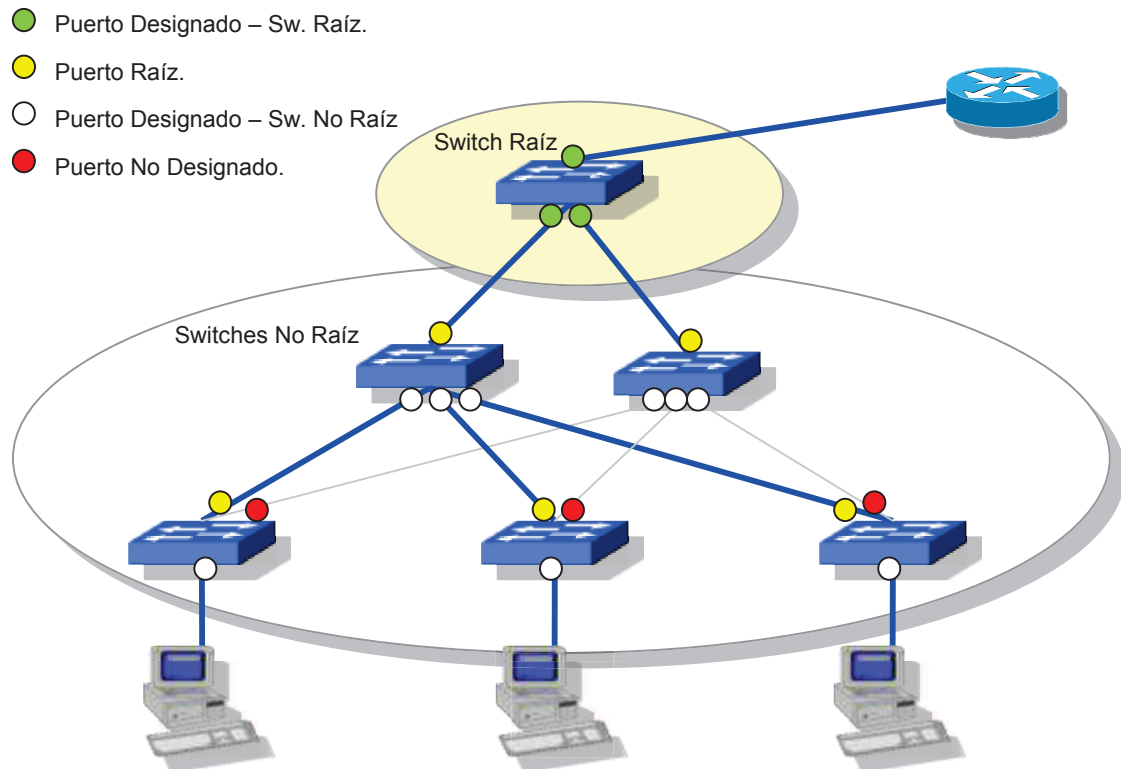
- **STP (802.1D)**
Genera una única instancia de STP para toda la red independientemente del número de VLANs existentes.
Generalmente genera rutas subóptimas para el tráfico de la red.
- **RSTP (802.1w)**
Es una evolución de 802.1D que ofrece mejores tiempos de convergencia. Ya que mantiene una única instancia de STP, sigue vigente la posibilidad de la utilización de rutas subóptimas.
Dadas sus características tiene requerimientos de hardware superiores a STP.
- **MST (802.1s)**
Mapea múltiples VLANs a una o varias instancias de RSTP.
Requiere más recursos que RSTP, pero menos que RPVST+
- **PVST+ (propietario de Cisco)**
Es una extensión de 802.11D que genera una instancia de STP para cada VLAN. Esto genera un mayor requerimiento de recursos, al mismo tiempo que permite una mejor administración de las rutas disponibles.
- **RPVST+ (propietario de Cisco)**
Es una mejora a 802.1w propietaria de Cisco.
Genera una instancia de RSTP para cada VLAN, lo que resuelve tanto los problemas de convergencia como de uso de rutas subóptimas. Esto tiene grandes requerimientos de CPU y memoria.

	Estándar/Propietario	Recursos	Convergencia
STP	802.1D	Pocos	Lenta
PVST+	Cisco	Muchos	Lenta
RSTP	802.1w	Medios	Rápida
RPVST+	Cisco	Muy altos	Rápida
MSTP	802.1s	Medios	Rápida

Operación de STP

El protocolo completa 3 tareas para determinar una ruta libre de bucles:

1. Se elige un switch raíz (root bridge o bridge raíz).
 - Sólo hay un puente raíz en cada dominio de broadcast.
 - Todos los puertos del switch raíz son "puertos designados" (designated ports). Los puertos designados están en estado de forwarding.



2. Cada uno de los demás switches (non root bridge) selecciona un puerto raíz.

- Cada switch no-raíz tiene un solo puerto raíz en cada dominio de broadcast.
- Selecciona como puerto raíz (root port) al puerto de menor costo hacia el switch raíz y lo pone en estado de forwarding.

3. En cada segmento se selecciona un puerto designado.

- Se elige como puerto designado el que pertenece al switch con una ruta con menor costo hacia el switch raíz. El puerto designado está en estado de forwarding.
- Los puertos no-designados quedan en estado de blocking.

En consecuencia, hay 3 roles de puertos STP:

- Puerto Raíz.
- Puerto Designado.
- Puerto No Designado.

Selección del switch raíz

Para compartir la información de switches y puertos que le permite luego calcular el árbol de rutas, STP envía cada 2 segundos paquetes BPDU. Los paquetes BPDU se inundan por todos los puertos en formato multicast.

Uno de los datos que se transmiten en el BPDU es el ID del puente o BID. El BID es un número de 8 bytes de extensión:

Prioridad	MAC Address del switch
2 Bytes	6 Bytes

La prioridad puede tener un valor de entre 0 y 65535. El valor por defecto es de 32768 (0x8000).

Se considera switch raíz el switch con menor BID.

Costos y prioridades

Para determinar el mejor camino hacia el switch raíz se utiliza como parámetro el “costo”.

Cada puerto está asociado a un costo que se encuentra definido por el protocolo en función de la velocidad del enlace. El costo de una ruta se calcula sumando los costos de todos los enlaces que la componen.

Velocidad del puerto	Costo
10 Gbps.	1
1 Gbps.	4
100 Mbps.	19
10 Mbps.	100

Cuando 2 rutas tienen igual costo, se selecciona utilizando el valor de prioridad. La prioridad es resultado de un valor por defecto (128) y el número de puerto; de esta manera el puerto con menor ID es el puerto preferido por defecto.

Estados de los puertos STP

De acuerdo a su situación operativa respecto de la red, los puertos de cada dispositivo pueden pasar por 5 estados diferentes:

- Bloqueado (Blocking).
Recibe BPDUs, pero no participa en la conmutación de tramas.
- Escuchando (Listening).
Recibe y envía BPDUs, pero no participa en la conmutación de tramas.

- Aprendiendo (Learning).
Comienza a poblar la tabla de direcciones MAC.
- Enviando (Forwarding).
Es parte de la topología activa enviando y recibiendo tramas, al mismo tiempo que envía y recibe BPDUs.
- Desactivado (Shutdown).
No participa del árbol STP. No es estrictamente parte del protocolo.

Cuando se enciende un switch, STP se encuentra activo por defecto y coloca todos los puertos en estado de blocking. A partir de este punto cada puerto debe pasar por los estados de transición (listening y learning) para luego llegar al estado de forwarding.

Cuando un puerto opera con STP se estabiliza en 2 estados posibles: blocking o forwarding.



Propiamente, los estados de STP son los 4 mencionados. Si se habla de los estados del puerto, entonces hay que agregar “desactivado”. No es STP el que pone al puerto en ese estado como en los otros casos. Ese estado es generado por el administrador a través del comando `shutdown`.

Port Fast

En su operación por defecto STP indica que cuando un puerto pasa a estar operativo (up/up) inicie es estado de blocking, pase luego a listening, luego a learning y finalmente a forwarding.

PortFast modifica la operación por defecto de STP de modo tal que, cuando pasa a estado operativo el puerto de acceso inicia directamente en estado de forwarding. Si el puerto recibe un BPDU, entonces pasa a estado bloqueado e inicia la negociación de STP.

De esta manera PortFast reduce notablemente el tiempo de negociación de los puertos de acceso a los que se conectas terminales.

Per VLAN Spanning Tree +

Define varias instancias de STP en una sola red: una instancia STP por VLAN.

- Permite distribuir el tráfico.
- Optimiza el aprovechamiento de los enlaces de backbone redundantes.
- Puede sobrecargar excesivamente el procesamiento del CPU.
- Utiliza un ID Bridge extendido.

Prioridad	VLAN ID	MAC Address del switch
4 bits	12 bits	6 Bytes

- Mantiene compatibilidad de prioridad con STP IEEE 802.1d.
- Utiliza el campo prioridad para transportar el VLAN ID.
- El valor de prioridad incrementa en bloques de 4096.
- PVSTP+ se utiliza sobre troncales IEEE 802.1Q.

Rapid Spanning Tree Protocol

RSTP ofrece un servicio de convergencia más rápido en caso de cambios de topología.

Ha sido especificado en el estándar IEEE 802.1w, manteniendo compatibilidad con IEEE 802.1d.

Los estados de puertos en RSTP son 3:

- Discarding.
- Learning.
- Forwarding.

Se introducen nuevos roles de puertos:

- Puerto raíz.
- Puerto designado.
- Puerto alternativo.
Puerto que ofrece una ruta alternativa al switch raíz. Se encuentra en estado de discarding. Pasa a ser puerto designado en caso de que el puerto designado falle.
- Puerto de backup.
Puerto del switch designado que corresponde a un enlace redundante. Se encuentra en estado de discarding.

Multiple Spanning Tree Protocol (MSTP)

- Definido a través del estándar 802.1s.
- Define varias instancias de RSTP en un switch (no necesariamente una por VLAN), cada una de ellas puede abarcar a múltiples VLANs.

STP Estados de puerto	RSTP Estados de puerto	Incluido en la topología activa
Blocking	Discarding	No
Listening	Discarding	No
Learning	Learning	No
Forwarding	Forwarding	Si

Operación de STP por defecto

Los switches Cisco Catalyst soportan:

- PVST+.
- PVRST+.
- MSTP.

Las opciones por defecto de STP en switches Catalyst son las siguientes:

- PVST+
- Está habilitado en todos los puertos, que también se encuentran en la VLAN1.

Configuración de Spanning Tree

- Habilitación de PortFast.

```
Switch_2960(config)#spanning-tree portfast default
Switch_2960(config)#interface FastEthernet 0/1
Switch_2960(config-if)#spanning-tree portfast
```

- Configuración de STP

```
Switch_2960(config)#spanning-tree mode rapid-pvst
Switch_2960(config)#spanning-tree vlan [ID] priority [#]
Switch_2960(config)#spanning-tree vlan [ID] primary
Switch_2960(config)#spanning-tree vlan [ID] secondary
```

```
Switch_2960#show spanning-tree vlan [ID]
Switch_2960#debug spanning-tree pvst+
```

Administración del archivo de configuración y la imagen del IOS

Borrar la configuración

```
Switch_2960#erase startup-config
Erasing the nvram filesystem will remove all files! Continue?
[confirm]
[OK]
Erase the nvram:complete

Switch_2960#delete flash:config.text
Delete filename [config.text]?
Delete flash:config.text? [confirm]

Switch_2960#delete flash:vlan.dat
Delete filename [vlan.dat]?
Delete flash:vlan.dat? [confirm]
```

En el caso de los switches Catalyst, si se desea volver el dispositivo a valores por defecto, es necesario no sólo borrar el archivo de configuración de respaldo sino también la base de datos de VLANs que se guarda en un archivo aparte.

La configuración completa de un switch Catalyst 2960

```
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname Switch_2960
!
enable secret 5 $1$SK0h$khm4DuXmgQ6p4xkArG6RQ1
!
no aaa new-model
system mtu routing 1500
!
ip subnet-zero
!
no ip domain-lookup
!
no file verify auto
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
interface FastEthernet0/1
description puesto de trabajo de ventas
switchport mode access
switchport port-security
switchport port-security maximum 2
```

```

switchport port-security mac-address sticky
speed 100
duplex full
!
interface FastEthernet0/2
description puesto de trabajo de ventas
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
speed 100
duplex full
!
interface FastEthernet0/3
description puesto de trabajo de ventas
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
speed 100
duplex full
!
interface FastEthernet0/4
description puesto de trabajo de ventas
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
speed 100
duplex full
!
interface FastEthernet0/5
description puesto de trabajo de soporte tecnico
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
speed 100
duplex full
!
interface FastEthernet0/6
description puesto de trabajo de soporte tecnico
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
speed 100
duplex full
!
interface FastEthernet0/7
description puesto de trabajo de soporte tecnico
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky

```

```

speed 100
duplex full
!
interface FastEthernet0/8
description puesto de trabajo de management
switchport mode access
switchport port-security
switchport port-security mac-address 00e0.59aa.195b
speed 100
duplex full
!
interface GigabitEthernet0/1
description backbone hacia switch de distribucion
!
interface Vlan1
ip address 172.16.5.2 255.255.255.0
no ip route-cache
!
ip default-gateway 172.16.5.1
!
ip http server
banner motd ^C ***** Acceso Restringido ***** ^C
!
control-plane
!
!
line con 0
password 7 060506324F41
logging synchronous
login
line vty 0 4
password 7 14141B180F0B
login
line vty 5 15
password 7 14141B180F0B
login
!
!
end

```

EtherChannel

Tecnología que permite crear enlaces lógicos que agrupan múltiples (entre 2 y 8) enlaces físicos.

- Mejora la escalabilidad de la red ya que permite aumentar el ancho de banda disponible agrupando puertos ya existentes en los dispositivos.
- Una vez establecido el enlace lógico, la mayor parte de las tareas de configuración se pueden realizar sobre la interfaz lógica, facilitando las tareas.
- Mejora la redundancia de la red ya que mientras uno sólo de los enlaces físicos esté disponible, el canal se mantiene activo.

- Soluciona problemas de STP ya que para El protocolo los enlaces físicos agrupados se comportan como un único enlace lógico.
- Es posible balancear tráfico entre los múltiples enlaces físicos que componen el canal.

Configuración de EtherChannel

La configuración de los canales EtherChannel puede realizarse de modo estático o utilizando protocolos de negociación dinámicos:

- PAgP – Es el protocolo propietario de Cisco.
- LACP – Es el protocolo estándar para esta tarea.

Al configurar interfaces EtherChannel es conveniente tener presentes algunos puntos:

- Una vez configurado un EtherChannel, cualquier configuración que se aplica a la interfaz port channel afecta a la operación de todo el canal. Cualquier modificación de configuración que se realiza sobre un puerto físico afecta exclusivamente a ese puerto físico.
- Todas las interfaces físicas deben estar configuradas para operar a la misma velocidad y en el mismo modo dúplex.
- Todas las interfaces físicas deben estar asignadas a la misma VLAN o estar configuradas como troncales.
- Las interfaces físicas que conforman un un canal pueden tener asignado diferente costo de STP.
- En los switches Catalyst ME, solamente los puertos NNI y ENI soportan negociación dinámica con LACP o PAgP.

Switch_2960 (config) #**interface range FastEthernet0/1 - 2**

Aunque no es obligatorio utilizar el comando interface range, es conveniente aprovecharlo para asegurar una configuración uniforme de los puertos que han de conformar el canal.

Switch_2960 (config-if) #**channel-group 1 mode on**

Asigna las interfaces a un canal específico. Si la interfaz port-channel no existe, la crea.

El modo dependerá del protocolo utilizado para la negociación dinámica. En este caso no hay negociación dinámica, sino configuración estática. Ambos extremos deben ser configurados en modo estático.

Para verificar la operación de EtherChannel hay disponibles comandos específicos:

Switch_2960#**show etherchannel summary**

Muestra una síntesis de la operación de cada interfaz port-channel.

Switch_2960#**show interfaces port-channel 1**

Muestra la configuración, estado y estadísticas de la interfaz de canal que se especifica, del mismo modo que se trataría de una interfaz física.

Switch_2960#**show interfaces FastEthernet 0/1 etherchannel**

Proporciona información respecto del rol que la interfaz especificada juega en la constitución de los channel-groups.

Segmentación de la red implementando VLANs

Beneficios de la implementación de VLANs

- Reducen los costos de administración.
- Controlan el broadcast.
- Mejoran la seguridad de la red.
- Permiten agrupar de manera lógica a los usuarios de la red.

Modos de membresía VLAN

- Estática.
La asignación del puerto a una VLAN específica es realizada por el Administrador manualmente y sólo puede ser modificada por él.
- Dinámica.
Requiere de un VLAN Membership Policy Server (VMPS) o servidor de políticas de gestión de VLANs.
- Voice VLAN.
Puerto de acceso asignado a un Cisco IP Phone. Utiliza una VLAN para tráfico de voz y otra para tráfico de datos.

Tipos de puertos o enlaces

- Puertos de acceso.
Es el puerto al que se conecta una terminal y que pertenece a una única VLAN.
- Puerto troncal.
Permiten el transporte de varias VLANs a través de varios switches manteniendo sus identidades.

Tips

- Por defecto todos los puertos de los switches Cisco están asignados a la VLAN 1.
- La VLAN 1 es la VLAN de gestión o management por defecto.
- Sólo se puede acceder vía telnet al dispositivo a través de la VLAN de management.
- La dirección IP del switch debe pertenecer a la red o subred de la VLAN de management.

¿Qué es un Enlace Troncal?

Se denomina enlace troncal (en inglés trunk link) a un enlace punto a punto que transporta múltiples VLANs. Permite optimizar el empleo de los enlaces disponibles.

Su implementación acarrea los siguientes beneficios, entre otros:

- Disminuye el requerimiento de puertos físicos.
- Permite un manejo más eficiente de la carga.

Un enlace troncal se establece activando la funcionalidad de puerto troncal en los puertos ubicados en cada extremo del enlace.



Los puertos del switch Catalyst 2960 están por defecto en modo “dynamic auto”, es decir, implementan el protocolo DTP en función del cual, si detectan en el otro extremo del cable una terminal, trabajan en modo acceso; si detectan en el otro extremo un puerto troncal, pasan a modalidad troncal.

Se puede implementar sobre enlaces de 100Mbps o superiores que conectan punto a punto dos switches, un switch con un router o con un servidor (en este caso el servidor debe contar con una placa con soporte para el protocolo IEEE 802.1Q).

Al habilitar un puerto como troncal en un switch Catalyst, por defecto transporta todas las VLANs configuradas en el switch.

Hay 2 mecanismos posibles para administrar la transferencia de tramas de diferentes VLANs sobre un enlace troncal:

- ISL (Inter-Switch Link).
Protocolo propietario de Cisco.
- IEEE 802.1Q.
Protocolo Estándar de IEEE. Implementa etiquetado de tramas.

Para identificar cada VLAN inserta un nuevo campo de información, de 4 bytes de longitud, en el encabezado de la trama.

IEEE 802.1Q

Protocolo estándar para marcado de tramas sobre enlaces troncales.

- Inserta una etiqueta de 4 bytes en el encabezado Ethernet.
- Debe recalcular el campo FCS.
- Permite establecer 8 diferentes niveles de prioridad (IEEE 802.1p).
- Implementa el concepto de VLAN nativa. No marca las tramas pertenecientes a esta VLAN.

VLAN Trunk Protocol (VTP)

VTP es un protocolo de capa 2 propietario de Cisco utilizado para compartir la información de las VLANs (base de datos de VLANs) entre switches que pertenecen a una misma administración (es decir, pertenecen a un dominio administrativo único) y que se comunican a través de enlaces troncales.

VTP utiliza tramas multicast de capa 2 para agregar, borrar y modificar las VLANs de un dominio, permitiendo realizar cambios en la red conmutada de modo centralizado.

El protocolo VTP permite definir dominios de administración a partir del nombre de dominio.

Las publicaciones VTP contienen parte o toda esta información:

- Nombre de dominio de administración.
- Número de revisión de configuración.
- Clave utilizando MD5, cuando se ha activado el uso de contraseña.
- Identidad del dispositivo que envía la actualización.

Por defecto, en los switches Cisco Catalyst:

- Todos son servidores VTP.
- No tienen configurado ningún dominio VTP.
- La implementación de VTP pruning es variable de acuerdo al modelo.

Modos VTP

Los switches que operan en un entorno VTP, pueden hacerlo de uno de tres modos diferentes:

- Servidor.
- Cliente.
- Transparente.

Tarea	Servidor VTP	Cliente VTP	VTP Transp.
Envía mensajes VTP	Si	Si	No
Reenvía mensajes VTP	Si	Si	Si
Escucha mensajes VTP	Si	Si	No
Permite crear VLANs	Si	No	Si, localmente
Permite borrar VLANs	Si	No	Si, localmente

Configuración de VLANs y enlaces troncales

Comandos para la verificación de VTP

```
Switch_2960#show vtp status
VTP Version                : 2
Configuration Revision      : 0
Maximum VLANs supported locally : 64
Number of existing VLANs    : 5
VTP Operating Mode          : Server
VTP Domain Name             : ICND
VTP Pruning Mode            : Disabled
VTP V2 Mode                 : Disabled
VTP Traps Generation        : Disabled
MD5 digest                  : 0xBF 0x86 0x94 0x45 0xFC 0xDF
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
```

Configuración de VTP

```
Switch_2960#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch_2960(config)#vtp mode [client|server|transparent]
Setting device to VTP CLIENT mode.

Switch_2960(config)#vtp domain [nombre]
Changing VTP domain name from NULL to ICND

Switch_2960(config)#vtp password [clave]
Switch_2960(config)#vtp pruning
Switch_2960(config)#exit
```

Configuración de puertos troncales

```
Switch_2960(config)#interface FastEthernet 0/1
Switch_2960(config-if)#switchport mode [access/dynamic/trunk]
Switch_2960(config-if)#switchport mode trunk
```

Cuando DTP se encuentra activo (es la opción por defecto), el modo del puerto se negocia dinámicamente. El resultado final depende de la configuración de ambos puertos al negociar.

	Acceso	Dynamic / Auto	Dynamic / Desirable	Troncal
Acceso	Acceso	Acceso	Acceso	n/a
Dynamic / Auto	Acceso	Acceso	Troncal	Troncal
Dynamic / Desirable	Acceso	Troncal	Troncal	Troncal
Troncal	n/a	Troncal	Troncal	Troncal

Monitoreo de los puertos troncales

```
Switch_2960#show interface GigabitEthernet 0/1 switchport
Name: Gi0/1
Operational Mode: trunk
Administrative Trunking Encapsulation: 802.1q
Operational Trunking Encapsulation: 802.1q
Negotiation of Trunking: Disabled
Access Mode VLAN: 0 ((Inactive))
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: NONE
Pruning VLANs Enabled: NONE
Priority for untagged frames: 0
Override vlan tag priority: FALSE
Voice VLAN: none
Appliance trust: none
```

```
Switch_2960#show interfaces trunk
Port      Mode      Encapsulation  Status      Native vlan
Gi0/1     on        802.1q         trunking    1
Gi0/2     on        802.1q         trunking    1
```

Creación de VLANs.

```
Switch_2960#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch_2960 (config)#vlan [#]
Switch_2960 (config-vlan)#name [nombre]
Switch_2960 (config-vlan)#^Z
%SYS-5-CONFIG_I: Configured from console by console
Switch_2960#
```

Asignación de puertos a las VLANs.

```
Switch_2960#configure terminal
Enter configuration commands, one per line. End with CNTL/Z
Switch_2960(config)#interface fastEthernet 0/4
Switch_2960(config-if)#switchport mode access
Switch_2960(config-if)#switchport access vlan [#]
Switch_2960(config-if)#no switchport access vlan [#]
```

Comandos para verificar la asignación de puertos

```
Switch_2960#show vlan
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/5
2	Prueba	active	Fa0/6, Fa0/7, Fa0/8, Fa0/9, Fa0/10, Fa0/11
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

VLAN	Type	SAID	MTU	Parent	RingNo	BridNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
2	enet	100002	1500	-	-	-	-	-	0	0
1002	fddi	101002	1500	-	-	-	-	-	0	0
1003	tr	101003	1500	-	-	-	-	-	0	0
1004	fdnet	101004	1500	-	-	-	-	ieee	0	0
1005	trnet	101005	1500	-	-	-	-	ibm	0	0

```
Switch_2960#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/5
2	Prueba	active	Fa0/6, Fa0/7, Fa0/8, Fa0/9, Fa0/10, Fa0/11
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

```
Switch_2960#show vlan id [#]
```

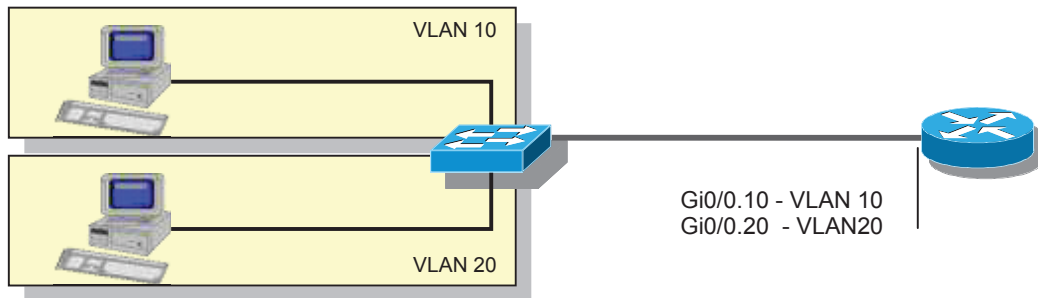
Configuración de un “router on stick”

Cuando se desea comunicar terminales conectadas a diferentes VLANs entre sí, se requiere:

- Que cada VLAN tenga asignada una red o subred diferente.

- Que ambas redes o subredes estén comunicadas entre sí a través de un dispositivo de capa 3 (router o switch multilayer).

Cuando para esa tarea se utiliza un router, la implementación recibe el nombre de “router on stick”:



- Un enlace troncal une el switch con el router.
- El router tiene una sub-interfaz para definir el gateway de cada una de las VLANs (subredes).
- En el router se puede enrutar (comunicar) entre ambas subredes.

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

```
Router(config)#interface GigabitEthernet 0/0
Router(config-if)#no shutdown
Router(config-if)#interface GigabitEthernet 0/0.10
Router(config-subif)#encapsulation dot1q 10
Router(config-subif)#ip address 172.18.10.1 255.255.255.0
Router(config-subif)#interface GigabitEthernet 0/0.20
Router(config-subif)#encapsulation dot1q 20
Router(config-subif)#ip address 172.18.20.1 255.255.255.0
Router(config-subif)#_
```



Para profundizar o tener mayor información sobre cualquiera de estos puntos, sugiero consultar mi libro “Guía de Preparación para el Examen de Certificación CCNA”.

2.5. Enrutamiento IP

Principios del enrutamiento IP

Para establecer comunicación entre dispositivos alojados en redes diferentes es necesario acudir a un dispositivo de capa 3, típicamente un router. Cada interfaz del router es una red diferente, y está en capacidad de conmutar tráfico entre redes.

Los procesos de enrutamiento IP permiten descubrir la ruta que ha de utilizar un paquete IP para recorrer el camino entre origen y destino a través de la red y almacenar esa información en una base de datos que denominamos tabla de enrutamiento.

La tabla de enrutamiento contiene la información correspondiente a todos los destinos posibles conocidos, e incluye como mínimo:

- Identificador de la red de destino.
- Dispositivo vecino a partir del cual se puede acceder a la red destino.
- Forma en que se mantiene y verifica la información de enrutamiento.
- La mejor ruta a cada red remota.

El router aprende acerca de las redes remotas:

- Dinámicamente, de los demás dispositivos de capa 3 de la red.
- Estáticamente, a partir de la información ingresada por un Administrador

Con esta información el router construye las tablas de enrutamiento.

El router tiene cumple 2 funciones básicas:

- Determinación de las rutas.
El comando `show ip route` permite verificar las rutas elegidas en cada dispositivo como caminos para alcanzar las diferentes redes de destino.
- Reenvío de paquetes.
Utilizando la información de la tabla de enrutamiento y la dirección IP de destino del paquete, se determina hacia dónde se debe reenviar el tráfico. Si el dispositivo no tiene una entrada en la tabla de enrutamiento para el destino que se busca, el paquete es descartado.

El proceso de enrutamiento que se corre en el router debe estar en capacidad de evaluar la información de enrutamiento que recibe y seleccionar la ruta a utilizar en base a criterios específicos.

La tabla de enrutamiento

Es un conjunto ordenado de información referida al modo de alcanzar diferentes redes de destino.

La información puede ser obtenida estática o dinámicamente. Todas las redes directamente conectadas se agregan automáticamente a la tabla de enrutamiento en el momento en que la interfaz asociada a esa red alcanza estado operativo.

Cuando la red de destino no está directamente conectada, la tabla de enrutamiento indica a cuál de los dispositivos directamente conectados (próximo salto) se debe enviar el paquete para que alcance el destino final.

Si la tabla de enrutamiento no cuenta con una ruta a la red de destino, el paquete es descartado y se envía un mensaje ICMP al origen.

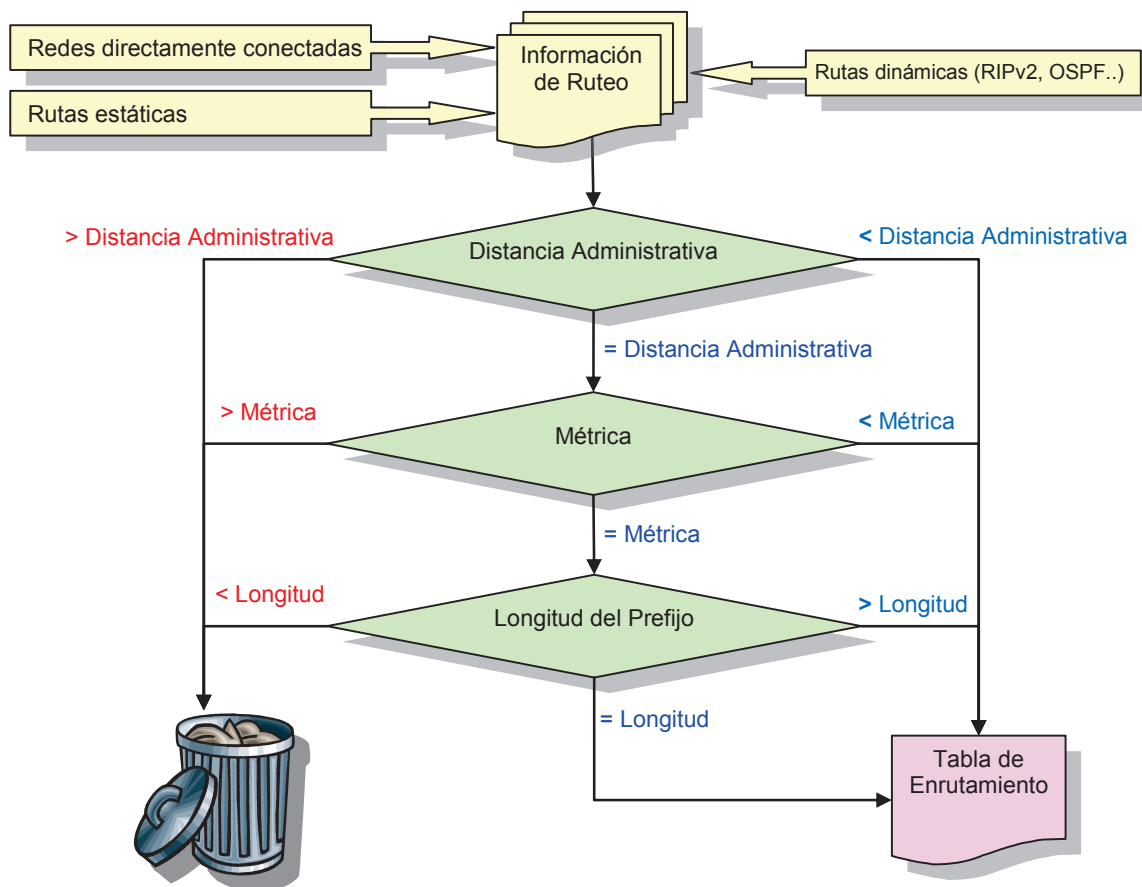
Generación de la tabla de enrutamiento

En Cisco IOS hay 3 métodos para ingresar información en la tabla de enrutamiento:

- Redes directamente conectadas.
El origen de la información es el segmento de red directamente conectado a las interfaces del dispositivo.
Si la interfaz deja de ser operativa, la red es removida de la tabla de enrutamiento. Su distancia administrativa es 0 y son preferidas a cualquier otra ruta.
- Rutas estáticas.
Son ingresadas manualmente por el Administrador de la red.
Su distancia administrativa por defecto es 1.
Son un método efectivo de adquisición de información de enrutamiento para redes pequeñas y simples que no experimentan cambios frecuentes.
- Rutas dinámicas.
Son rutas aprendidas automáticamente a través de la operación del intercambio de protocolos de enrutamiento con dispositivos vecinos.
Estas pueden modificarse automáticamente en respuesta a cambios en la red.
- Ruta por defecto.
Es una entrada opcional en la tabla de enrutamiento que se utiliza cuando no hay una ruta explícita hacia la red de destino.

La tabla de enrutamiento se construye utilizando un algoritmo para seleccionar la mejor ruta a cada destino a partir de los siguientes parámetros:

Cuando el dispositivo encuentra varias rutas a la misma red de destino con igual distancia administrativa e igual métrica, las conserva en la tabla de enrutamiento y realiza balanceo de tráfico entre esas rutas de igual costo.



La métrica

Es el parámetro generado por el algoritmo de enrutamiento para cada ruta hacia una red de destino y que refleja la “distancia” existente entre el dispositivo y la red de destino.

La métrica puede ser el resultado de la medición de uno o varios parámetros combinados. La menor métrica es la que corresponde a la mejor ruta.

Se puede basar en diferentes características de la ruta:

- Ancho de banda.
- Delay.
- Cantidad de saltos.
- Costo.
Valor arbitrario que puede ser asignado por el Administrador.

La Distancia Administrativa

Es el valor que permite clasificar las diferentes rutas que se aprenden a un mismo destino de acuerdo a la confiabilidad de la fuente de información de enrutamiento.

Cisco IOS utiliza este parámetro para seleccionar la mejor ruta cuando hay rutas al mismo destino de diferente origen.

Es un valor entero entre 0 y 255, que a menor valor denota mayor confiabilidad. Cada fuente de información tiene un valor asignado por defecto, que puede ser modificado por configuración.

Fuente de información de ruteo	Valor
Ruta a una red directamente conectada	0
Ruta estática (por defecto)	1
Ruta sumaria EIGRP	5
Ruta EBGp	20
Ruta EIGRP interna	90
Ruta OSPF	110
Ruta IS-IS	115
Ruta RIP	120
Ruta EIGRP externa	170
Ruta IBGP	200
Ruta inalcanzable	255

Protocolos de enrutamiento

Hay disponibles diferentes protocolos de enrutamiento dinámico para operar en redes IP. Estos protocolos pueden clasificarse, en primera instancia, en función de su diseño para operar mejor en el enrutamiento interno de un sistema autónomo (protocolos de enrutamiento interior) o entre sistemas autónomos (protocolos de enrutamiento exterior).

Un sistema autónomo o dominio de enrutamiento es un conjunto de dispositivos bajo una administración única.

Protocolos de Enrutamiento Interior:

- RIP
- EIGRP
- OSPF
- IS-IS

Protocolos de Enrutamiento Exterior:

- BGPv4

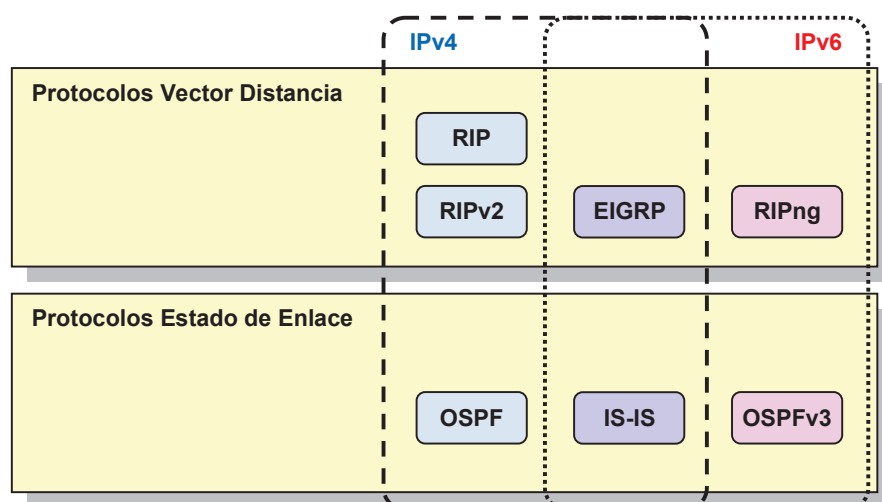
Comparación entre enrutamiento vector distancia y estado de enlace

Los protocolos de enrutamiento interior también se diferencian en función del algoritmo que utilizan para procesar la información de enrutamiento que intercambian y definir cuál es la mejor ruta a un destino posible.

Hay 2 tipos de protocolos de enrutamiento interior:

- Protocolos de vector distancia.
Determina básicamente la dirección y distancia a la que se encuentra la red de destino.
- Protocolos de estado de enlace.
Cada router construye su propio mapa interno de la topología de la red.

Protocolos por vector distancia	Protocolos por estado de enlace
Implementan el algoritmo Bellman-Ford.	Implementan el algoritmo de Dijkstra o algoritmo SPF.
Visualiza la red sólo desde la perspectiva de los vecinos.	Elaboran una visión común de la topología de la red entera.
Realizan actualizaciones periódicas, por lo que son de convergencia lenta.	Los eventos activan la actualización lo que posibilita una convergencia más rápida.
Transmiten copias completas o parciales de la tabla de enrutamiento a los dispositivos vecinos.	Transmiten básicamente solo actualizaciones del estado de los enlaces a los otros dispositivos.
Requieren menor procesamiento y cantidad de memoria RAM en el dispositivo; pero utilizan más ancho de banda para el intercambio.	Requieren mayor procesamiento y cantidad de memoria RAM en el dispositivo, pero utilizan menos ancho de banda para el intercambio.



Enrutamiento estático

Una ruta estática es una ruta manualmente ingresada en la tabla de enrutamiento del dispositivo. Esta información de enrutamiento requiere ser mantenida manualmente por el Administrador de la red.

Ventajas	Desventajas
No genera carga de procesamiento.	El Administrador debe tener una comprensión amplia de la red.
No utiliza ancho de banda.	El Administrador debe agregar manualmente la ruta hacia cada red.
Son más seguras.	La actualización de rutas puede convertirse en un trabajo full-time.
Fácil diagnóstico.	Requiere alto mantenimiento y no tiene adaptabilidad a los cambios.

Puede ser conveniente utilizar rutas estáticas cuando:

- La red está constituida por unas pocas rutas.
- La red está conectada a Internet a través de un único service provider.
- La red está configurada sobre un modelo hub-and-spoke.

Configuración de una ruta estática

Ruta estática IPv4:

```
Router(config)#ip route [red destino] [máscara] [próximo salto]
[distancia administrativa]
```

Ruta estática IPv6:

```
Router#configure terminal
Router(config)#ipv6 unicast-routing
```

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

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

Rutas por Defecto

Las rutas por defecto son rutas utilizadas para enrutar paquetes que tienen como destino una dirección perteneciente a una red para la cual no hay una ruta específica en la tabla de enrutamiento.

Es una ruta que puede ser utilizada por cualquier dirección IP de destino. Generalmente es utilizada cuando la dirección IP de destino no tiene coincidencia con una ruta más específica.

Configuración de una ruta por defecto

Cisco IOS ofrece 2 procedimientos de configuración diferentes para rutas IPv4 por defecto:

```
Router (config) #ip route 0.0.0.0 0.0.0.0 [próximo salto]
Router (config) #ip default-network [red destino por defecto]
```

Para configurar una ruta por defecto para enrutamiento IPv6:

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

Enrutamiento Dinámico

Un protocolo de enrutamiento dinámico es un conjunto de procesos, algoritmos y formatos de mensajes que permiten intercambiar información de enrutamiento entre dispositivos con el propósito de construir las tablas de enrutamiento.

De esta manera, y a partir del intercambio de información actualizada, cada dispositivo puede construir una tabla de enrutamiento ajustada que se actualiza dinámicamente y puede aprender respecto de redes remotas y cómo llegar hasta ellas.

Ventajas	Desventajas
Alto grado de adaptabilidad a los cambios.	Requieren cantidades significativas de procesamiento y memoria RAM.
Requiere muy poco mantenimiento.	Eleva el uso de ancho de banda.

Protocolos de enrutamiento por vector distancia

Este tipo de protocolos, envía a los dispositivos vecinos la información contenida en la tabla de enrutamiento. El envío se hace cada intervalos fijos de tiempo.

Cuando se recibe una actualización, se compara la información recibida con la contenida en la propia tabla de enrutamiento:

- Para establecer la métrica se toma la métrica recibida en la actualización y se le agrega la del propio enlace.
- Si la ruta aprendida es mejor (menor métrica) que la contenida en la tabla de enrutamiento, se actualiza la tabla de enrutamiento con la nueva información.

Los eventos que pueden provocar una actualización son varios:

- La falla de un enlace.

- La introducción de un nuevo enlace.
- La falla de un dispositivo.
- El cambio de los parámetros de un enlace.

Estos protocolos son sensibles a la posibilidad de generación de bucles de enrutamiento. Un bucle de enrutamiento es una condición por la cual un paquete se transmite continuamente dentro de una serie definida de dispositivos, sin que alcance nunca la red de destino.

Para prevenir o solucionar este inconveniente, implementan varios recursos:

- Cuenta al infinito.
Es una contramedida que soluciona un posible bucle de enrutamiento. Para esto se define "infinito" como una cantidad máxima de saltos (dispositivos de capa 3) que puede contener una ruta para alcanzar un destino.
Cuando la ruta alcanza la cantidad de saltos máxima definida por el protocolo, se considera que la red de destino está a una distancia infinita y por lo tanto es inalcanzable.



Número máximo de saltos RIP = 15
Número máximo de saltos EIGRP=224

- Horizonte dividido (Split horizon).
Técnica para prevenir la formación de bucles.
La regla indica que nunca es útil reenviar información sobre una ruta, a través de la misma interfaz a través de la cual se recibió esa información.
- Ruta envenenada (Route poisoning).
Mecanismo para prevenir la formación de bucles.
Permite marcar una ruta como inalcanzable y enviarla utilizando una actualización de enrutamiento. De esta manera se evita que los dispositivos vecinos reciban actualizaciones incorrectas respecto de una nueva ruta hacia la red que ha salido de operación.
- Temporizadores de espera (Hold-down timers).
Se utilizan para evitar que las actualizaciones regulares reinstalen una ruta inapropiada en la tabla de enrutamiento.
Fuerzan a que el dispositivo retenga algunos cambios, por un período de tiempo determinado, antes de incorporarlos en la tabla de enrutamiento.
Habitualmente es un período de tiempo equivalente a tres veces el intervalo de actualización utilizado por el protocolo.
- Actualizaciones desencadenadas.
Es un mecanismo diseñado para acelerar la convergencia en caso de cambios en la red.
Para esto se utilizan actualizaciones desencadenadas que se envían inmediatamente en respuesta a un cambio, sin esperar el período de actualización regular.

Comparación entre Enrutamiento Vector Distancia y Estado de Enlace

Protocolos por vector distancia	Protocolos por estado de enlace
Implementan el algoritmo Bellman-Ford.	Implementan el algoritmo de Dijkstra.
Visualiza la red sólo desde la perspectiva de los vecinos.	Buscan una visión común de la topología de la red íntegra.
Realizan actualizaciones periódicas, por lo que son de convergencia lenta.	Los eventos activan la actualización lo que posibilita una convergencia más rápida.
Transmiten copias completas o parciales de la tabla de enrutamiento a los dispositivos vecinos.	Transmiten básicamente solo actualizaciones del estado de los enlaces a los otros dispositivos.
Requieren menor procesamiento y disponibilidad de memoria RAM en el dispositivo; pero utilizan mayor ancho de banda.	Requieren mayor procesamiento y cantidad de memoria RAM en el dispositivo, pero utilizan menor ancho de banda.
RIP EIGRP	OSPF IS-IS

Enhanced Interior Gateway Routing Protocol (EIGRP)

Sus principales características son:

- Protocolo de enrutamiento por vector distancia avanzado.
- Protocolo propietario de Cisco.



Atención:

Si bien a efectos del examen de certificación EIGRP sigue siendo un protocolo propietario de Cisco, en enero de 2013 Cisco Systems anunció su apertura, y ha pasado a ser un protocolo de tipo abierto detallado en un conjunto de RFCs de la IETF.

- Algoritmo de selección de mejor ruta: DUAL
Utiliza la Máquina de Estado Finito DUAL (FSM).
Calcula las rutas con la información que le proveen la tabla de vecindades y la tabla topológica.
- Mantiene una tabla de vecindades y una tabla topológica.
- Implementa el concepto de “rutas sucesoras”.
- No realiza actualizaciones periódicas.
Sólo se envían actualizaciones cuando una ruta cambia. Estas actualizaciones se envían solamente a los dispositivos que son afectados por los cambios.

- Actualizaciones utilizando multicast: 224.0.0.10 o FF02::A.
- Soporta VLSM y sumarización de rutas.
- Por defecto no sumariza rutas.
Se puede activar sumarización automática, al límite de la clase; o se puede realizar sumarización manual de rutas.
- Soporta autenticación con intercambio de claves predefinidas y cifradas con MD5.
Se autentica el origen de cada actualización de enrutamiento.
- Diseño modular utilizando PDM.
Soporta múltiples protocolos enrutados: IPv4, IPv6, IPX y AppleTalk
- Utiliza RTP (protocolo propietario de capa de transporte) para asegurar una comunicación confiable.
- Métrica de 32 bits compuesta: ancho de banda, retraso, confiabilidad y carga.
Métrica por defecto = ancho de banda + retardo.
- Balancea tráfico entre rutas de igual métrica. 4 por defecto, máximo 32.
Es posible definir balanceo de tráfico entre rutas de diferente métrica.
- Cantidad máxima de saltos: 224.
- ID en la tabla de enrutamiento: D (para rutas externas D EX).
- Distancia Administrativa: 90 (170 para rutas externas).
- Su configuración requiere que se defina un número de Sistema Autónomo (AS).

Los routers EIGRP mantienen tablas de información interna del protocolo:

- Una Tabla de vecinos.
Es un registro de los vecinos que descubre a través del intercambio de paquetes de hello y con los que establece adyacencias.
- Una tabla topológica.
Contiene todas las rutas a cada destino posible, descubiertas por el protocolo a través de los dispositivos vecinos

En la tabla topológica se mantiene para cada una de las redes destino posibles:

- La métrica con la que cada vecino publica cada una de esas redes destino (AD).
- La métrica que el dispositivo calcula para alcanzar esa red destino a través de ese sucesor (FD).
 $FD = AD + \text{Métrica para alcanzar el vecino}$

La feasible distance será la métrica de enrutamiento que se asignará a esa ruta si es colocada en la tabla de enrutamiento.

Como resultado del análisis de estas métricas, la ruta con menor métrica (successor route) es propuesta a la tabla de enrutamiento como la mejor ruta; y se elige una ruta de respaldo o feasible successor route.

EIGRP implementa una métrica compuesta calculada a partir de 4 parámetros; 2 por defecto y 2 opcionales.

Componentes por defecto:

- Ancho de banda.
El menor ancho de banda en la ruta entre origen y destino expresado en kilobits por segundo.
- Delay.
Delay que acumulan todas las interfaces a lo largo de la ruta al destino, expresado en decenas de microsegundos.

Adicionalmente puede considerar:

- Confiabilidad.
Representa el tramo menos confiable en la ruta entre origen y destino, tomando como base los keepalives.
- Carga.
Representa el enlace con mayor carga en la ruta entre origen y destino, tomando como base la tasa de paquetes y el ancho de banda configurado en las interfaces.

Estos 4 parámetros se integran en una fórmula de cálculo en la que son modificados utilizando valores constantes (K1, K2, K3, K4 y K5) que pueden ser modificados por configuración y que reciben la denominación de “pesos”.

Configuración de EIGRP en redes IPv4

```
Router(config)#router eigrp 1
```

Selecciona el protocolo de enrutamiento e ingresa al submodo de configuración del mismo.

Requiere la asignación de un ID de sistema autónomo (1 a 65535), que debe ser igual en todos los dispositivos que participan del mismo dominio de enrutamiento.

```
Router(config-router)#network 172.16.1.0 0.0.0.255
```

Declara las interfaces que participan del intercambio de información de enrutamiento enunciando las redes a las que pertenecen. Se puede utilizar máscara de wildcard para especificar una subred en particular.

```
Router(config-router)#maximum-paths 2
```

Ajusta el balanceo de tráfico entre hasta 2 rutas con igual métrica. El máximo posibles es 32.

Si se define el valor 1, se suprime el balanceo de tráfico.

```
Router(config-router) #variance 2
```

Define un valor ente 1 y 128 para ser utilizado como múltiplo de los valores de métrica que son aceptables para realizar balanceo de tráfico entre rutas de diferente métrica.

```
Router(config-router) #exit
```

```
Router#show ip route eigrp
```

Muestra las rutas aprendidas utilizando EIGRP que se han ingresado en la tabla de enrutamiento.

```
Router#show ip protocols
```

```
Router#show ip eigrp interfaces
```

Visualiza las interfaces sobre las cuáles EIGRP se encuentra activo

```
Router#show ip eigrp neighbors
```

Muestra los dispositivos vecinos que EIGRP ha descubierto.

```
Router#show ip eigrp topology
```

Muestra la tabla topológica de EIGRP.

Configuración de EIGRP en redes IPv6

```
Router(config) #ipv6 unicast routing
```

```
Router(config) #ipv6 router eigrp 1
```

Crea una instancia de enrutamiento EIGRP, e ingresa al submodo de configuración del protocolo.

El número de sistema autónomo debe ser el mismo en todos los dispositivos que conforman un dominio de enrutamiento.

```
Router(config-router) #interface GigabitEthernet 0/0
```

```
Router(config-if) #ipv6 enable
```

```
Router(config-if) #ipv6 address FC00:1:1:1::/64 eui-64
```

```
Router(config-if) #ipv6 eigrp 1
```

Inicia la operación de la instancia de EIGRP previamente creada, en la interfaz.

```
Router(config-router) #Ctrl-Z
```

```
Router#show ipv6 router eigrp
```

Muestra las rutas IPv6 aprendidas utilizando el protocolo EIGRP que se han ingresado en la tabla de enrutamiento.

```
Router#show ipv6 eigrp 1 interfaces
```

```
Router#show ipv6 eigrp 1 neighbors
```

```
Router#show ipv6 eigrp 1 topology
```


Configuración de autenticación en EIGRP

```
Router(config)#key chain LAB
```

Crea una cadena o grupo de llaves de cifrado, identificado con un nombre.

```
Router(config-keychain)#key 1
```

Asigna un ID para la llave.

```
Router(config-keychain-key)#key-string cisco123
```

Define una llave de cifrado.

```
Router(config-keychain-key)#key 2
```

```
Router(config-keychain-key)#key-string laboratorio2
```

```
Router(config)#router eigrp 1
```

```
Router(config-router)#network 172.16.1.0 0.0.0.255
```

```
Router(config-router)#maximum-paths 2
```

```
Router(config-router)#variance 2
```

```
Router(config-router)#exit
```

```
Router(config)#ipv6 unicast routing
```

```
Router(config)#ipv6 router eigrp 1
```

```
Router(config-router)#exit
```

```
Router(config)#interface GigabitEthernet 0/0
```

```
Router(config-if)#ip authentication mode eigrp 1 md5
```

Habilita el uso de autenticación MD5 para el enrutamiento EIGRP de IPv4 en la interfaz.

```
Router(config-if)#ip authentication key-chain eigrp 1 LAB
```

Especifica el grupo de llaves de cifrado que se deben aplicar en esta interfaz.

```
Router(config-if)#ipv6 enable
```

```
Router(config-if)#ipv6 address FC00:1:1:1::/64 eui-64
```

```
Router(config-if)#ipv6 eigrp 1
```

```
Router(config-if)#ipv6 authentication mode eigrp 1 md5
```

Habilita el uso de autenticación MD5 para el enrutamiento EIGRP de IPv6 en la interfaz.

```
Router(config-if)#ipv6 authentication key-chain eigrp 1 LAB
```

Open Shortest Path First (OSPF)

Las principales características de OSPF son las siguientes:

- Protocolo de enrutamiento abierto por estado de enlace.
Cada uno de los dispositivos tiene una visión completa de la topología de la red.
- Protocolo de enrutamiento classless.
Soporta VLSM y CIDR.
- Métrica: costo.
El costo es un valor arbitrario que califica el enlace. Puede ser configurado por el Administrador; Cisco IOS utiliza por defecto el ancho de banda

declarado en el comando `bandwidth` para hacer el cálculo utilizando la fórmula $10^8 / \text{ancho de banda en bps}$.

- Balancea tráfico entre rutas de igual métrica.
4 rutas de igual métrica por defecto, máximo 16.
- Algoritmo de cálculo de la mejor ruta: Dijkstra, también llamado SPF (Shortest Path First).
- ID en la tabla de enrutamiento: 0.
- Distancia Administrativa: 110.
- Utiliza paquetes hello para descubrir dispositivos OSPF vecinos y mantener la relación de vecindad.
El período de actualización de paquetes hello depende del tipo de red:
10 segundos en redes multiacceso y punto a punto.
30 segundos en redes NBMA.
- Además del intercambio de hellos, cuando se produce un evento en la red se desencadena el intercambio de LSA para actualizar información.
- Permite realizar sumarización manual de rutas.
- Soporta autenticación con intercambio de claves en texto plano o cifradas con MD5.

Utiliza un Router ID para identificar el dispositivo que genera LSAs. Ese router ID:

- Es configurado manualmente por el Administrador.
- Si el Administrador no configura un ID se utiliza la IP de la interfaz lógica (loopback) más alta.
- Si no hay interfaz de loopback configurada se utiliza la IP de la interfaz física con IP más alta que esté activa al momento de levantar el proceso de OSPF.

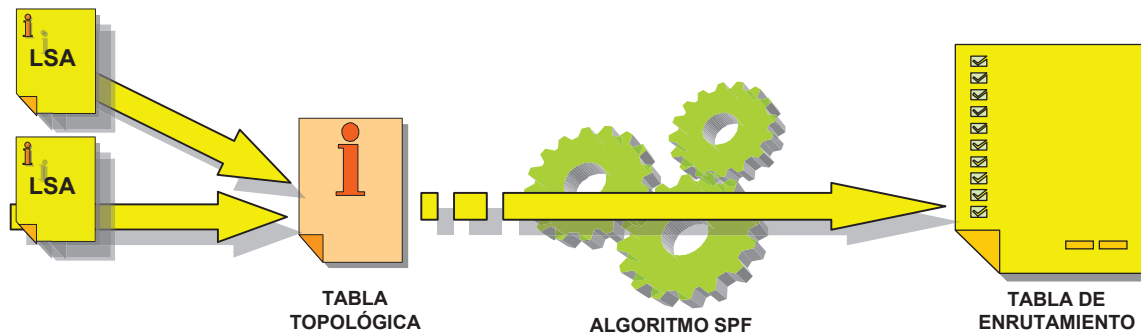
Para optimizar recursos y dar mayor estabilidad al protocolo, implementa el concepto de Área.

- El ID de área es un valor entero entre 0 y 4.294.967.295
- El Área 0 está reservada como área de backbone.

Para su operación mantiene varias tablas o bases de datos:

- Base de datos de adyacencias.
Mantiene una base de datos de los dispositivos OSPF directamente conectados con los que mantiene intercambio de información.

- Base de datos topológica.
Mantiene una base de datos con la información del estado de todos los enlaces que componen la red.



La operación del protocolo es diferente en distintos tipos de red:

- Redes multiacceso de broadcast.
- Redes multiacceso sin broadcast (NBMA).
- Redes punto a punto. No elige DR.
- Redes punto a multipunto. No elige DR.

Cuando se corre OSPF en redes multiacceso se elige:

- Router designado (DR).
- Router designado de respaldo (BDR).

Esto permite reducir La cantidad de procesamiento necesario en las redes multiacceso para procesar los LSAs que notifican cambios en la red. De esta manera solamente el DR procesa las actualizaciones y si esto significa un cambio en la tabla topológica se comunica el cambio a los demás vecinos en la red multiacceso.

OSPF es un protocolo de enrutamiento exclusivamente IP. En la actualidad utilizamos 2 versiones de OSPF:

- OSPFv2 para redes IPv4.
- OSPFv3 para redes IPV6.

Son 2 protocolos diferentes que corren de modo completamente independiente uno del otro.

Configuración de OSPFv2

```
Router(config)#interface loopback 0
Router(config-if)#ip address [address] 255.255.255.255
Router(config-if)#exit
```

```

Router(config)#router ospf [process-id]
Router(config-router)#network [address] [wildcard] area [area-id]
Router(config-router)#area [id] authentication [message-digest]
Router(config-router)#exit
Router(config)#interface serial 0/0/0
Router(config-if)#bandwidth 64
Router(config-if)#ip ospf authentication-key [clave]
Router(config-if)#ip ospf cost [#]
Router(config-if)#ip ospf priority [#]

```

Monitoreo de OSPFv2

```

Router#show ip protocols
Router#show ip ospf
Router#show ip ospf database
Router#show ip ospf neighbor
Router#show ip ospf interface
Router#debug ip ospf events

```

Configuración de OSPFv3

```

Router(config)#ipv6 unicast-routing
Router(config)#ipv6 router ospf [process-id]
Router(config-router)#router-id X.X.X.X

```

El router ID es un identificador de 32 bits que se expresa en formato de 4 octetos decimales.

NO es una dirección IP. Tiene el mismo formato.

```

Router(config-router)#exit
Router(config)#interface serial 0/0/0
Router(config-if)#bandwidth 64
Router(config-if)#ipv6 enable
Router(config-if)#ipv6 address FC00:1:1:2::/64 eui-64
Router(config-if)#ipv6 ospf [process-id] area [area-id]

```

Inicia la operación de OSPF previamente creada, en la interfaz.

Monitoreo de OSPFv3

```

Router#show ipv6 protocols
Router#show ipv6 ospf
Router#show ipv6 ospf database
Router#show ipv6 ospf neighbor
Router#show ipv6 ospf interface

```

Comandos de verificación

El comando show ip route

Este comando muestra el contenido de las tablas de enrutamiento IP.

Router#**show ip route**

Codes: L - local, C - connected, S - static, I - IGRP, R - RIP,
B - BGP, D - EIGRP, EX - EIGRP external, O - OSPF,
IA - OSPF inter area, N1 - OSPF NSSA external type 1,
N2 - OSPF NSSA external type 2, E1 - OSPF external type 1,
E2 - OSPF external type 2, E - EGP, i - IS-IS,
* - candidate default, U - per-user static route, o - ODR

Gateway of last resort is not set

```
172.16.0.0/16 is variably subnetted with 2 masks
R    172.16.40.0/24 [120/1] via 172.16.20.1. 00:00:18. Serial0/0/1
C    172.16.30.0/24 is directly connected. GigabitEthernet0/0
L    172.16.30.1/32 is directly connected. GigabitEthernet0/0
C    172.16.20.0/30 is directly connected. Serial0/0/1
L    172.16.20.2/32 is directly connected. Serial0/0/1
R    172.16.10.0/24 [120/1] via 172.16.20.1. 00:00:18. Serial0/0/0
R    172.16.1.0/24 [120/1] via 172.16.20.1. 00:00:18. Serial0/0/0
```

Variantes del comando

```
Router#show ip route [red]
Router#show ip route eigrp
Router#show ip route ospf
Router#show ip route static
Router#show ip route connected
Router#show ipv6 route [red]
Router#show ipv6 route rip
Router#show ipv6 route eigrp
Router#show ipv6 route ospf
Router#show ipv6 route static
Router#show ipv6 route connected
```

Otro comando: show ip protocols

Este comando permite revisar la información correspondiente a configuración de los protocolos de enrutamiento IPv4 activos en el router.

Router#**show ip protocols**

```
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 10.0.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    10.0.1.1 0.0.0.0 area 0
    10.1.1.0 0.0.0.255 area 0
    10.2.1.0 0.0.0.255 area 0
    10.4.1.0 0.0.0.255 area 0
  Reference bandwidth unit is 100 mbps
  Routing Information Sources:
    Gateway          Distance          Last Update
```

```

10.10.20.20      110      3d02h
10.0.2.1         110      3d02h
10.100.100.100   110      1w1d
10.10.10.200     110      1w1d
Distance: (default is 110)

```

Redundancia en el primer salto (FHRP)

Cuando una red LAN tiene más de una puerta de salida (gateway), la implementación de un protocolo de redundancia en el primer salto (First Hop Redundancy Protocol (FHRP) es una de las maneras privilegiadas de administrar esa redundancia.

Estos protocolos posibilitan que los múltiples gateways existentes sean vistos por las terminales de la red como un único default gateway. De esta manera el usuario de un dispositivo terminal no debe hacer nada para sacar provecho de la redundancia de puertas de salida: siempre utiliza el mismo default gateway y su tabla ARP no cambia.

Si bien hay varios protocolos que cubren esta tarea, tienen características comunes:

- Todas las terminales tienen una única configuración de default gateway que no se modifica.
- Los routers de borde comparten una dirección IP virtual.
- Las terminales utilizan la dirección IP virtual como default-gateway.
- Los routers intercambian mensajes del protocolo FHRP para coordinar cuál es el router operativo en cada momento.
- Cuando el router operativo falla, FHRP define cuál es el dispositivo que lo reemplaza en la tarea.

Hay 3 protocolos que desempeñan esta tarea:

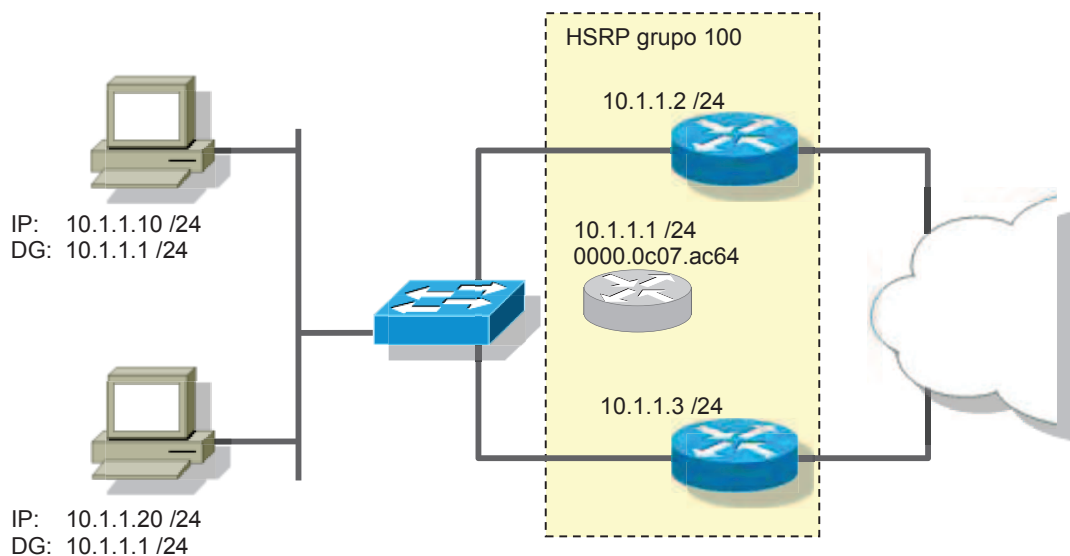
Protocolo	Tipo	Redundancia	Balanceo
HSRP – Hot Standby Router Protocol	Cisco	Activo/Standby	No
VRRP – Virtual Router Redundancy Protocol	IETP	Activo/Standby	No
GLBP – Gateway Load Balancing Protocol	Cisco	Activo/Activo	Si

Hot Standby Router Protocol (HSRP)

Permite que 2 o más dispositivos cooperen brindando el servicio de gateway de la red, pero sólo uno está en modo activo, los demás permanecen en standby como respaldo en caso de que el dispositivo activo deje de operar.

Para su operación se utiliza una dirección IP virtual y una dirección MAC también virtual.

- La IP virtual es definida en la configuración, debe pertenecer a la red o subred que la IP de las interfaces, pero debe ser única.
- La MAC virtual es derivada automáticamente por el protocolo a partir de la configuración. El formato de esta dirección es 0000.0c07.acxx, donde xx es el ID de grupo HSRP en hexadecimal.
- Todos los routers asociados al proceso de HSRP conocen esta dirección virtual, pero solamente el dispositivo activo utiliza esta dirección.
- Las terminales de la red utilizan la IP virtual como dirección del default gateway.



Los dispositivos incluidos en el grupo de HSRP intercambian mensajes entre sí que les permiten:

- Negociar cuál es el dispositivo que quedará como activo y cuál/es como standby.
- Detectar el fallo del dispositivo activo para que el dispositivo standby cambie de estado y pase a operar como activo.
- Cuando se detecta un fallo y el dispositivo standby pasa a modo activo, entonces envía un gratuitous ARP con la MAC virtual como dirección de origen para actualizar la tabla CAM de todos los switches en la red.

HSRP no permite hacer balanceo de tráfico ya que inevitablemente, dentro de un grupo HSRP, sólo puede haber un dispositivo activo a la vez.

Sin embargo es posible distribuir tráfico entre diferentes dispositivos a partir del diseño. Si la red está segmentada en más de una VLAN, y cada VLAN corresponde a una subred diferente, entonces cada VLAN deberá tener un gateway diferente. De este modo se han de configurar diferentes grupos de HSRP

(1 para cada VLAN), y en cada grupo es posible forzar, utilizando el parámetro de prioridad, que el dispositivo activo para cada VLAN sea diferente.

Por ejemplo:

- La red está segmentada en 2 VLANs: VLAN 1 (10.1.1.0/24) y VLAN 2 (10.1.2.0/24).
- Hay 2 routers de borde, cada uno configurado con subinterfaces para ambas VLANs.
- Se configuran en ambos dispositivos 2 grupos HSRP: Grupo 1 para la VLAN 1 con IP virtual 10.1.1.1; Grupo 2 para la VLAN 2 con IP virtual 10.1.2.1.
- RouterA será activo para el Grupo 1, con lo que operará como default gateway para la VLAN 1; RouterB será activo para el Grupo 2, con lo que operará como default gateway para la VLAN 2.
- A su vez, cada uno será respaldo (standby) para su contraparte en la VLAN para la que no está activo.

Configuración de HSRP

La operación de HSRP requiere que todos los dispositivos que van a actuar en redundancia estén configurados con:

- El mismo número de grupo.
- La misma IP virtual.
- Opcionalmente se puede configurar un valor de prioridad para definir cuál de los dispositivos quedará como activo y cuál/es como standby. El dispositivo con prioridad más alta será el activo.

```
RouterA(config)#interface GigabitEthernet 0/0
RouterA(config-if)#ip address 10.1.1.2 255.255.255.0
RouterA(config-if)#standby 100 ip 10.1.1.1
RouterA(config-if)#standby 100 priority 110
```

```
RouterB(config)#interface GigabitEthernet 0/0
RouterB(config-if)#ip address 10.1.1.3 255.255.255.0
RouterB(config-if)#standby 100 ip 10.1.1.1
```

Para verificar la configuración de HSRP:

```
Router#show standby brief
```

Permite verificar la operación del protocolo.

```
Router#show standby
```

Da información detallada de estado y operación del protocolo.

Gateway Load Balancing Protocol (GLBP)

Protocolo propietario de Cisco que permite balancear carga en cada subred utilizando un esquema de redundancia activo/activo.

- Utiliza una dirección IP virtual que será utilizada como dirección de default gateway por las terminales.
- Cada dispositivo del grupo tiene asignada una MAC virtual diferente, que se corresponde a la misma IP virtual del default gateway.
- Uno de los dispositivos del grupo actuará como AVG (Active Virtual Gateway). Su tarea es responder todas las solicitudes ARP que busquen la dirección IP virtual definida, cada una, con la MAC virtual de un dispositivo diferente del grupo.
- Como resultado, las terminales de la subred tienen diferente MAC en su tabla de direcciones MAC para el default gateway. Como resultado de esto, cada terminal utilizará diferente dispositivo para encaminar el tráfico que debe salir de la red.

De esta forma, todos los dispositivos que conforman el grupo se encuentran activos, y se balancea la carga de tráfico en función de que el AVG va respondiendo con diferente MAC virtual a las solicitudes ARP que se realizan en la subred.

Por lo demás, los mecanismos que mantienen las comunicaciones dentro del grupo para asegurar que se responda en caso de un fallo, son semejantes a los de HSRP.

Configuración de GLBP

La configuración de GLBP es semejante a la de HSRP y requiere que todos los dispositivos que van a actuar en redundancia estén configurados con:

- El mismo número de grupo.
- La misma IP virtual.
- Opcionalmente se puede configurar un valor de prioridad para definir cuál de los dispositivos actuará como AVG. El dispositivo con prioridad más alta será el AVG.

```
RouterA(config)#interface GigabitEthernet 0/0
RouterA(config-if)#ip address 10.1.1.2 255.255.255.0
RouterA(config-if)#glbp 100 ip 10.1.1.1
RouterA(config-if)#glbp 100 priority 110
```

```
RouterB(config)#interface GigabitEthernet 0/0
RouterB(config-if)#ip address 10.1.1.3 255.255.255.0
RouterB(config-if)#glbp 100 ip 10.1.1.1
```

Para verificar la configuración de HSRP:

Router#**show glbp brief**

Permite verificar la operación del protocolo.

Router#**show glbp**

Da información detallada de estado y operación del protocolo.



Para profundizar o tener mayor información sobre cualquiera de estos puntos, sugiero consultar mi libro “Guía de Preparación para el Examen de Certificación CCNA”.

2.6. Servicios IP

Asignación automática de direcciones IP

Todo dispositivo que opera en una red IP necesita contar con una configuración IP básica (dirección IP, máscara de subred, default gateway, servidor DNS, etc.). Esta configuración puede lograrse a partir de diferentes mecanismos.

Los dispositivos IPv4 prevén en la actualidad varios mecanismos para asignar la configuración IP, los más frecuentemente utilizados son:

- Configuración estática.
- Asignación automática utilizando DHCP.

IPv6, por su parte, introduce junto a estos mecanismos ya en uso, nuevas modalidades de realizar esta tarea:

- Asignación estática definiendo manualmente el ID de interfaz.
- Asignación estática definiendo el ID de interfaz por EUI-64.
- Asignación dinámica utilizando autoconfiguración stateless.
- Asignación dinámica utilizando DHCPv6.

La amplitud del espacio de direccionamiento ofrecido por IPv6 ha permitido la implementación de sistemas de asignación automática de la porción del ID del puerto tales como EUI-64 y la configuración stateless.

Dynamic Host Configuration Protocol – DHCPv4

Aplicación que permite realizar de modo automatizado y dinámico la configuración IP de los dispositivos de la red. Opera sobre los puertos UDP 67 y 68.

Los parámetros de configuración que pueden ser suministrados a través de DHCP son:

- Dirección IP / Máscara de Subred.
- Default Gateway.
- Nombre de dominio.
- Servidor de nombres de dominio (DNS).
- Time Servers.
- WINS Server.
- Duración de la asignación.

- Información opcional.

Hay 3 modalidades de asignación de las direcciones IP por este medio:

- **Asignación dinámica.**
Realiza una asignación dinámica de una dirección comprendida en un rango definido en el servidor, por un tiempo determinado.
El cliente deberá volver a solicitar una asignación antes de que expire el tiempo especificado.
- **Asignación automática.**
El servidor realiza una asignación dinámica de una dirección comprendida en el rango definido en el servidor, de modo permanente.
- **Asignación estática.**
El servidor realiza la asignación de direcciones en base a una tabla que mapea direcciones MAC a direcciones IP. Sólo reciben dirección los clientes que están enlistados en esta tabla.

El procedimiento para obtener la configuración IP es el siguiente:

1. **DHCP Discovery.**
El cliente DHCP envía una solicitud en formato de broadcast.
2. **DHCP Offer.**
El servidor DHCP reserva una dirección IP para el cliente y responde enviando una propuesta de configuración en formato de broadcast.
3. **DHCP Request.**
El cliente responde en formato broadcast realizando una solicitud explícita de la configuración ofrecida por el servidor.
Pueden recibirse múltiples ofertas, pero sólo una es aceptada.
Cuando deba renovar su configuración enviará un nuevo request en formato unicast al servidor.
4. **DHCP Acknowledgement.**
Se envía un paquete en formato broadcast al cliente, incluyendo la información de configuración que el cliente ha aceptado.
Esto completa el proceso.

Sintetizando:

	RARP	BOOTP	DHCP
Capa modelo OSI	3	7	7
Protocolo capa transporte	---	UDP	UDP / TCP
Requiere un servidor	Si	Si	Si
Suministra			
Dirección IP	Fija	Fija	Fija / Dinámica
Máscara subred	---	Si	Si
Default gateway	---	Si	Si
Servidor DNS	---	Si	Si
Servidor WINS	---	---	Si
Nombre de dominio	---	---	Si

Configuración de servicios DHCP en IOS

El procedimiento para esto, es el siguiente:

- Definición del pool de direcciones a asignar.
- Definición de los parámetros opcionales de DHCP (dirección del servidor DNS, WINS, etc.)
- Definición del período de asignación.

```
Router#configure terminal
```

El servicio DHCP se encuentra habilitado por defecto en Cisco IOS.

```
Router(config)#ip dhcp excluded-address 172.16.1.1 172.16.1.3
Router(config)#ip dhcp pool [nombre]
Router(dhcp-config)#network 172.16.1.0/24
```

```
Router(dhcp-config)#dns-server 172.16.1.3
Router(dhcp-config)#netbios-name-server 172.16.1.3
Router(dhcp-config)#default-router 172.16.1.1
Router(dhcp-config)#domain-name [nombre]
```

```
Router(dhcp-config)#lease 1 8 0
```

Para verificar la operación del servicio:

```
Router#show ip dhcp pool [nombre]
Router#show ip dhcp binding
Router#show ip dhcp conflict
Router#show ip dhcp server statistics
```

DHCP Relay

Dado que el inicio de la operación del protocolo se realiza sin contar una dirección de origen y utilizando broadcast como destino las solicitudes (discovery) no son de suyo ruteables hacia otras subredes. De aquí que en principio el protocolo supone que el servidor y el cliente DHCP están conectados a la misma red o subred.

Cuando se desea utilizar servidores DHCP que se encuentran alojados en una red o subred diferente se puede utilizar un agente DHCP relay. Un DHCP relay es un dispositivo que recibe las solicitudes de los clientes en formato de broadcast y las reenvía como unicast a la dirección del servidor DHCP.

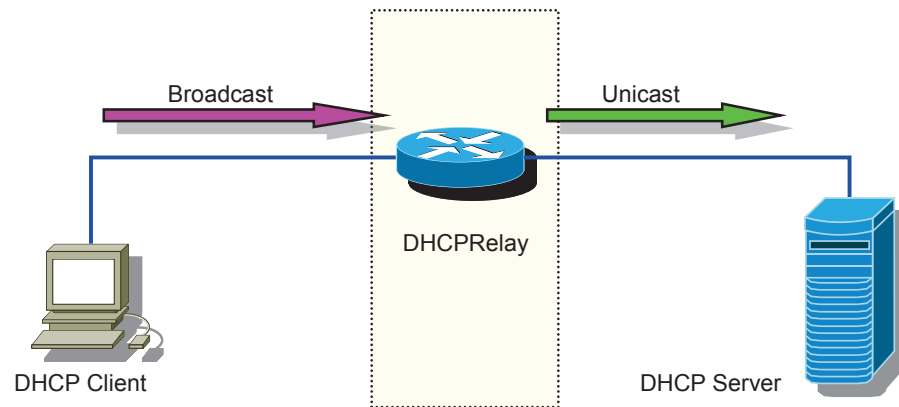
1. **DHCP Discovery.**
El cliente DHCP envía una solicitud en formato de broadcast.
2. **DHCP Relay.**
El agente DHCP relay que recibe el broadcast lo retransmite a uno o más servidores utilizando unicast e incluyendo su dirección como dirección de gateway.
3. **DHCP Offer.**
El servidor utiliza la dirección de gateway que recibe en la solicitud para determinar a qué subred pertenece el host solicitante y asigna entonces una configuración que corresponda esa subred.

El servidor DHCP reserva una dirección IP para el cliente y envía la respuesta en un unicast a la dirección del gateway, que luego lo reenvía a la red local.
4. **DHCP Request.**
El cliente responde en formato broadcast realizando una solicitud explícita de la configuración ofrecida por el servidor.
El agente DHCP relay interviene nuevamente reenviando la información al servidor DHCP.
5. **DHCP Acknowledgement.**
Se envía un paquete en formato unicast al DHCP relay que luego lo reenvía al cliente, incluyendo la información de configuración que el cliente ha aceptado.
Esto completa el proceso.

En estos casos el servidor DHCP responde al DHCP relay y este se ocupa de reenviarlo al cliente DHCP.

Configuración de un router como DHCP relay

El servicio de DHCP relay se habilita en la interfaz de capa 3 más cercana al cliente DHCP (usualmente, la que opera como default-gateway de la red o subred).



En la configuración es necesario especificar la dirección IP de uno o más servidores DHCP que han de responder las solicitudes. Si hay varios servidores DHCP en una misma subred se puede especificar directamente la dirección reservada de subred, de este modo responderá cualquiera de los servidores DHCP de esa subred.

```
Router#configure terminal
Router(config)#interface GigabitEthernet 0/0
Router(config-if)#ip helper-address [IP servidor DHCP]
```

Internet Control Message Protocol (ICMP)

ICMP es un protocolo que proporciona un conjunto de mensajes de control y error que permiten detectar y resolver problemas en la red de modo automático. Permite el reporte de errores en un entorno IP ya que el mismo protocolo IP no tiene posibilidad alguna de detectar o reportar errores a nivel de capa de red.



Atención, ICMP no soluciona la falla ya que no puede determinar el reenvío de un paquete que se ha descartado; para esto debe descansarse en los protocolos de capa de transporte.

ICMP genera diferentes tipos de mensajes que se agrupan en 2 funciones básicas: mensajes de error y mensajes de control:

Tipo IPv4	Tipo IPv6	Mensaje	Función
0	129	Echo Reply	Error
3	1	Destination Unreachable	Error
4	-	Source Quench	Control

5	137	Redirect / Change Request	Control
8	128	Echo Request	Error
9	134	Router Advertisement	Control
10	-	Router Selection	Control
11	3	Time Exceeded	Error
12	4	Parameter Problem	Error
13	-	Timestamp Request	Control
14	-	Timestamp Reply	Control
15	-	Information Request	Control
16	-	Information Reply	Control
17	-	Address Mask Request	Control
18	-	Address Mask Reply	Control
-	2	Packet Too Big	Error
-	133	Router Solicitation	Control
-	135	Neighbor Solicitation	Control
-	136	Neighbor Advertisement	Control
-	130	Multicast Listener Query	Control
-	131	MLDv1 Multicast Listener Report	Control
-	132	MLDv1 Multicast Listener Done	Control
-	143	MLDv2 Multicast Listener Report	Control
-	144	Home Agent Address Discovery Request	Control
-	145	Home Agent Address Discovery Reply	Control
-	146	Mobile Prefix Solicitation	Control
-	147	Mobile Prefix Advertisement	Control

Los mensajes de ICMP son la base sobre la que operan programas de diagnóstico básicos presentes en los sistemas operativos, como `tracert`, `ping` y `pathping`.

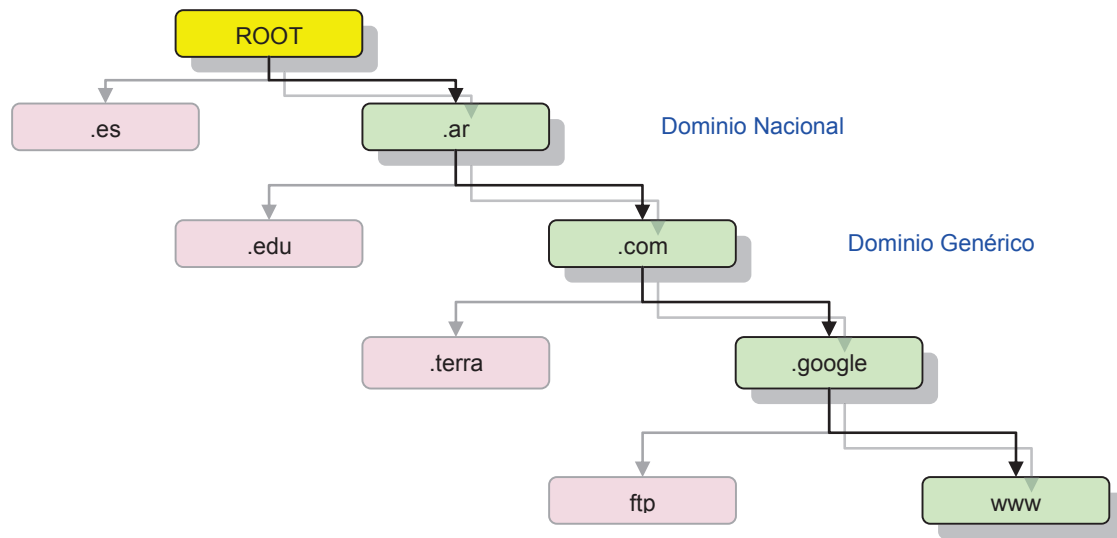
ICMPv4 es bloqueado en muchas redes corporativas por políticas de seguridad para evitar algunos ataques conocidos que se basan en su funcionamiento.

ICMPv6 no es diferente de su predecesor pero puede implementar autenticación y encriptación IPsec, lo que reduce las posibilidades de que sea aprovechado para un ataque. Esto es importante ya que en el caso de IPv6 ICMP se utiliza para la determinación del MTU, en el descubrimiento de vecinos, y reemplaza ARP. Es un protocolo esencial para el funcionamiento de redes IPv6.

Domain Name System - DNS

Protocolo que permite reemplazar el uso por parte del usuario final de direcciones IP por nombres para identificar los nodos.

Se trata de un protocolo de capa de aplicación que utiliza el puerto 53 tanto TCP como UDP en la capa de transporte. Las consultas estándar utilizan el puerto 53 de UDP.



DNS utiliza una estructura jerárquica de dominios de red, completamente independiente de la estructura propia del direccionamiento IP. En esta estructura existen dominios y subdominios.

¿Cómo se realiza una consulta?

- La terminal que requiere traducir un nombre por una dirección IP realiza una consulta al servidor DNS que tiene en su configuración IP. Supongamos a los fines de este análisis que deseamos acceder a sss.google.com.ar
- Si el servidor DNS local tiene esta búsqueda en su tabla de resolución de nombre, responderá directamente la consulta.
- Si el servidor DNS local no tiene una entrada para este dominio, reenvía la consulta al servidor raíz.
- Si el servidor raíz no tiene este dominio en su caché, reenvía a su vez la consulta al servidor que tiene la delegación .ar
- El servidor del dominio .ar, si no tiene este dominio en su caché, reenvía la consulta al servidor que tiene la delegación .com.
- El proceso continúa de esta manera hasta que el cliente recibe la respuesta solicitada.

Los nombres DNS están representados por conjuntos de etiquetas separadas por puntos. Un nombre es un conjunto de etiquetas compuestas por entre 1 y 63 caracteres alfanuméricos, comenzando con un carácter alfabético. No se distinguen mayúsculas y minúsculas.

Los servidores DNS mantienen una base de datos que relaciona los nombres de dominio con las direcciones IP. Estas bases de datos están compuestas por diferentes tipos de registros:

- Registros A.
Para mapear nombres a direcciones IPv4.
- Registros AAAA.
Para mapear nombres a direcciones IPv6.
- Registros MX.
Para mapear direcciones IP de servidores de correo.

Para dar soporte DNS a implementaciones IPv6 se requiere:

- Actualizar cliente y servidor DNS para aceptar registros en formato IPv6.
- Actualizar cliente y servidor para operar (transportar) sobre IPv6.

Cuando el servidor que tiene la consulta opera tanto con IPv4 como IPv6, entonces envía ambos registros: IPv4 e IPv6. Al recibirlo la terminal, por defecto, utiliza el registro IPv6.



Las aplicaciones que son independientes del protocolo, realizan la búsqueda de nombre para ambos protocolos (IPv4 e IPv6) y prefieren la respuesta IPv6.

Configuración del servicio de nombres en Cisco IOS

IOS, por defecto, interpreta toda cadena alfanumérica ingresada en la línea de comando que no puede interpretar como un comando, como si se tratara de un nombre e intenta traducirla por una dirección IP.

La consulta para traducir un nombre la realiza:

- En primer lugar verifica si se trata de un nombre definido en la tabla local.
- Si no se encuentra en la tabla local, realiza la consulta a un servidor DNS configurado.
- Si no hay un DNS configurado genera una consulta DNS a la dirección de broadcast (255.255.255.255) intentando encontrar un servidor que lo resuelva.

```
Router#configure terminal
Router(config)# ip domain-lookup
```

Habilita el servicio de traducción de nombres (se encuentra habilitado por defecto). Para apagar el servicio se niega este comando.

```
Router (config) #ip name-server [IP servidor DNS]
```

Define la dirección IP del servidor DNS externo para realizar consultas de nombre.

```
Router (config) #ip host [nombre] [IP]
```

Asocia el nombre referido a una o varias direcciones IP.

Listas de Control de Acceso

Las listas de control de acceso (ACL – Access Control List) son una herramienta que permiten filtrar tráfico en función de la información contenida en los diferentes encabezados (capa 2, 3 o 4) de una trama.

Se suelen utilizar ACLs para:

- Limitar el tráfico de la red para mejorar su performance.
- Implementar controles para el flujo de tráfico.
- Brindar un nivel de seguridad básico.
- Especificar que determinado tipo de tráfico (aplicación o protocolo) sea reenviado o bloqueado en una interfaz de un dispositivo.
- Definir el rango de direcciones IP privadas que deben ser traducidas a IP públicas por un servicio de NAT.
- Definir flujos de tráfico a los que se han de aplicar políticas de calidad de servicio (QoS) o seguridad.

Reglas de funcionamiento de las ACL

En IOS las ACLs están sometidas a un conjunto de reglas básicas de operación:

- Se puede configurar una sola lista en cada interfaz, por sentido del tráfico (entrante / saliente), por protocolo (IP, IPX, etc.).
- Cada lista de acceso es identificada por un ID único (numérico o alfanumérico).
- Cada paquete que ingresa o sale a través de una interfaz que tiene asociada una lista de acceso es comparado con cada sentencia de la ACL secuencialmente, en el mismo orden en que fueron ingresadas, comenzando por la primera.
- La comparación se sigue realizando hasta tanto se encuentre una coincidencia. Una vez que el paquete cumple la condición de una sentencia (la primera coincidencia), se ejecuta la acción indicada y no se sigue comparando.

- Hay un `deny any any` (denegación de todo tráfico) implícito al final de cada lista de acceso, que no es visible.
- Los filtros que se aplican sobre el tráfico saliente no afectan el tráfico originado en el mismo router.

Tipos de listas de acceso IP

- Listas de acceso estándar numeradas.
Permiten filtrar únicamente considerando la dirección IP de origen.
- Listas de acceso extendidas numeradas.
Verifican múltiples elementos del encabezado: direcciones de origen y destino, protocolo de capa 3 y puerto de capa 4.
- Listas de acceso IP nombradas.
Listas de acceso IP tanto estándar como extendidas que verifican direcciones de origen y destino, protocolos de capa 3 y puertos de capa 4, pero identificadas con una cadena de caracteres alfanuméricos.

Tipos especiales:

- Listas de acceso dinámicas.
- Listas de acceso reflexivas.
- Listas de acceso por tiempo.

El ID de las listas de acceso numeradas

En el caso de las listas de acceso numeradas, el ID indica el tipo de ACL de que se trata:

Router(config) #`access-list ?`

1-99	IP estándar
100-199	IP extendida
700-799	48 bit MAC address standard
1100-1199	48 bit MAC address extendida
1300 - 1999	IP estándar (a partir de IOS 12.0.1)
2000 - 2699	IP extendida (a partir de IOS 12.0.1)

La máscara de wildcard

Las máscaras de wildcard son secuencias de 32 bits divididas en 4 octetos de 8 bits cada uno (el mismo formato que una dirección IP o máscara de subred) utilizadas para generar filtros de direcciones IP. Se utilizan en combinación con una dirección IP.

En las máscaras de wildcard los unos y ceros de la máscara indican cómo se deben tratar los bits de la dirección IP correspondiente. El dígito en 0 (cero) indica una posición que debe ser comprobada, mientras que el dígito 1 (uno) indica una posición que carece de importancia.



Las máscaras de wildcard no tienen ninguna relación funcional con las máscaras de subred, son dos entidades absolutamente independientes entre sí.

Algunos ejemplos:

172.16.14.33 0.0.0.0

Indica que se debe seleccionar únicamente la dirección IP declarada.

172.16.14.44 0.0.0.255

Selecciona todas las direcciones IP comprendidas entre 172.16.14.0 y 172.16.14.255 (no discrimina respecto del cuarto octeto).

172.16.14.44 0.0.255.255

Selecciona todas las direcciones IP de la red 172.16.0.0 comprendidas entre 172.16.0.0 y 172.16.255.255 (no discrimina respecto de los dos últimos octetos).

Algunas reglas prácticas de cálculo

Cuando contamos con una máscara de subred como punto de partida (porque deseamos filtrar una red o subred completa), la máscara de wildcard es el “complemento” de esa máscara de subred. Al decir complemento me refiero al valor necesario para obtener una dirección IP de broadcast:

Máscara de subred:	255.255.224.000
IP de Broadcast:	255.255.255.255
Máscara de wildcard:	000.000.031.255

Cuando se desea filtrar una red completa, la máscara de wildcard es el complemento de la máscara de subred por defecto:

Dirección de red:	172.016.000.000 /16
Máscara de subred por defecto:	255.255.000.000
Máscara de wildcard:	000.000.255.255

Cuando se desea filtrar una subred completa, la máscara de wildcard es el complemento de la máscara de subred que se esté aplicando:

Dirección de subred:	172.016.030.000 /24
Máscara de subred:	255.255.255.000
Máscara de wildcard:	000.000.000.255

Dirección de subred:	172.016.032.000 /20
----------------------	---------------------

Máscara de subred: 255.255.240.000

Máscara de wildcard: 000.000.015.255

Cuando se desea filtrar un conjunto de direcciones de nodo o subredes, tenga en cuenta las siguientes pautas:

- La amplitud del rango de direcciones a filtrar, expresado en valores decimales, es siempre una potencia de 2.
- El valor inicial del rango decimal a filtrar es un múltiplo de la potencia de 2 utilizada como amplitud del rango.
- En este caso el valor del octeto crítico de la máscara de wildcard será igual a la amplitud del rango menos uno.

Un ejemplo:

- Filtrar las direcciones de nodo desde la 192.168.1.32 a la 192.168.1.47
Se trata de un grupo de 16 direcciones IP de la red 192.168.1.0/24
- Amplitud del rango: $16 = 2^4$
- Valor del inicio del rango: $32 = 2 \times 16$
- Valor del octeto crítico de la máscara de wildcard: $16 - 1 = 15$
- Solución: 192.168.1.32 **0.0.0.15**

Casos especiales

`xxx.xxx.xxx.xxx 0.0.0.0 = host xxx.xxx.xxx.xxx`

`0.0.0.0 255.255.255.255 = any`

Remark

Configuración de las listas de acceso

Listas de acceso IP estándar numeradas.

```
Router(config)#access-list [ID] [permit/deny] [IP origen]
Router(config)#no access-list [ID]
Router(config)#interface serial 0/0/1
Router(config-if)#ip access-group [ID] [in/out]
```



La lista de acceso ya configurada no es operativa hasta tanto sea aplicada a una interfaz.

Listas de acceso IP extendida numeradas.

```
Router(config)#access-list [ID] [permit/deny] [protocol] [IP  
origen] [pto. origen] [IP destino] [pto. destino]  
Router(config)#no access-list [ID]  
Router(config)#interface serial 0/0/1  
Router(config-if)#ip access-group [ID] [in/out]
```

Listas de acceso IP nombradas.

```
Router(config)#ip access-list [standard/extended] [nombre]  
Router(config-ext-nacl)#[permit/deny] [protocol] [IP origen] [pto.  
origen] [IP destino] [pto. destino]  
Router(config)#interface serial 0/0/1  
Router(config-if)#ip access-group [nombre] [in/out]
```

Edición de listas de acceso.

```
Router#show ip access-lists  
Extended IP access list 110  
    10 permit tcp any host 172.16.1.14 eq www  
    20 permit tcp any host 172.16.1.15 eq ftp  
    30 deny tcp any 172.16.1.0 0.0.0.255 eq www  
    40 deny tcp any 172.16.1.0 0.0.0.255 eq ftp  
    50 permit ip any any  
Router#configure terminal  
Enter configuration commands, one per line.  End with CNTL/Z.  
Router(config)#ip access-list extended 110  
Router(config-ext-nacl)#45 deny icmp any 172.16.1.0 0.0.0.255 echo
```

Inserta una sentencia entre las identificadas con el número de secuencia 50 y la 50 en la ACL original.

```
Router(config-ext-nacl)#^Z  
Router#show ip access-lists  
Extended IP access list 110  
    10 permit tcp any host 172.16.1.14 eq www  
    20 permit tcp any host 172.16.1.15 eq ftp  
    30 deny tcp any 172.16.1.0 0.0.0.255 eq www  
    40 deny tcp any 172.16.1.0 0.0.0.255 eq ftp  
    45 deny icmp any 172.16.1.0 0.0.0.255 echo  
    50 permit ip any any  
Router#_
```

Aplicación de filtros de tráfico a puertos virtuales.

```
Router(config)#access-list 10 permit host 172.16.10.3
```



¡Atención!: Sólo se pueden utilizar listas de acceso numeradas.

```
Router(config)#line vty 0 4  
Router(config-line)#access-class 10 in
```

Monitoreo de las listas de acceso.

```

Router#show access-list [#]
Router#show ip access-lists
Extended IP access list 110
  10 permit tcp any host 172.16.1.14 eq www
  20 permit tcp any host 172.16.1.15 eq ftp
  30 deny tcp any 172.16.1.0 0.0.0.255 eq www
  40 deny tcp any 172.16.1.0 0.0.0.255 eq ftp
  50 permit ip any any

Router#show ip interfaces serial 0/0/0
Serial0/0/0 is up, line protocol is up
Internet address is 172.16.10.2
Broadcast address is 255.255.255.255
Address determined by non-volatile memory
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Outgoing access list is not set
Inbound access list is 110
Proxy ARP is enabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachable are always sent
ICMP mask replies are never sent
IP fast switching is enabled
IP fast switching on the same interface is disabled
IP Fast switching turbo vector
IP multicast fast switching is enabled
IP multicast distributed fast switching is disabled
IP route-cache flags are Fast
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
RTP/IP header compression is disabled
Probe proxy name replies are disabled
Policy routing is disabled
Network address translation is disabled
Web Cache Redirect is disabled
BGP Policy Mapping is disabled

Router#show running-config

```

	ACL	Interfaz
show access-list	Si	No
show ip interfaces	No	Si
show running-config	Si	Si

Network Address Translation (NAT)

Procedimiento estándar que modifica la dirección IP de origen de los paquetes IP, traduciéndola por otra dirección IP compatible con la red de destino. Definido, entre otros, en el RFC 2633.

Esta traducción se realiza en un dispositivo NAT, también denominado NAT box, que opera típicamente en el borde de un área stub y es el responsable de traducir las direcciones IP y mantener las tablas respectivas. Un dispositivo NAT puede ser:

- Un router Cisco.
- Un firewall ASA.
- Un sistema UNIX.
- Un servidor Windows XP.
- Otro tipo de dispositivo.

Terminología NAT

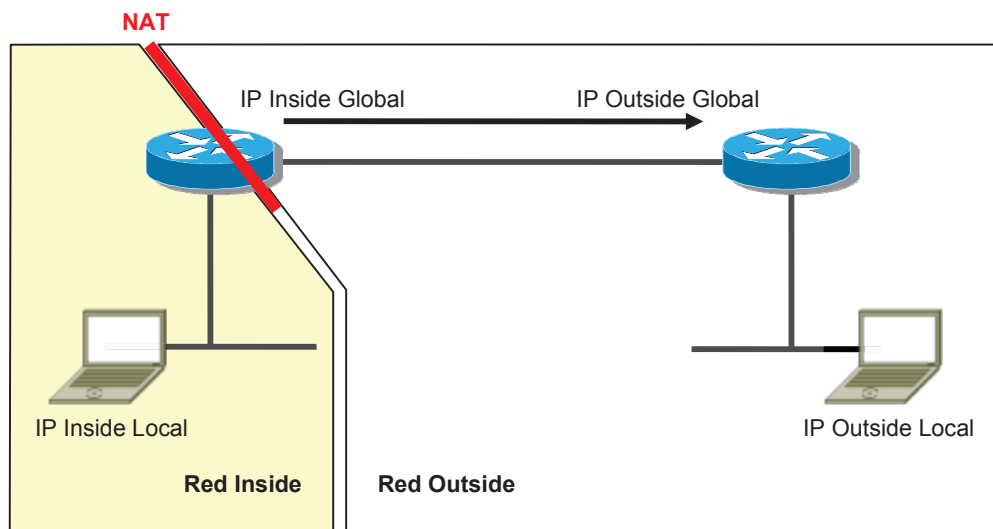
Al implementar y analizar NAT es fundamental tener presente una terminología propia.

- Red inside.
Red que se encuentra del lado “interno” del dispositivo NAT, y cuyas direcciones requieren traducción.
Habitualmente coincide con la red LAN.
- Red outside.
Red del lado “externo” del dispositivo NAT que requiere direcciones IP válidas.
Habitualmente coincide con la red WAN o Internet.

Se distinguen 4 tipos de direcciones IP:

- Inside Local Address.
Direcciones que tienen configurados los dispositivos que se encuentran conectados a la red Inside y que utilizan para sus comunicaciones locales.
- Inside Global Address.
Direcciones válidas en la red Outside que han de utilizar los dispositivos de la red Inside para establecer comunicaciones con dispositivos que se encuentran en la red Outside.
Es la dirección que representa a una terminal de la red Inside en la red Outside.
- Outside Local Address.
Dirección configurada en los dispositivos que se encuentran conectados a la red Outside.

- **Outside Global Address.**
Dirección que representa a un dispositivo de la red Outside en la red Inside.
Si el dispositivo de la red Outside también atraviesa un sistema NAT, entonces la dirección Outside Global y la Outside Local serán diferentes, aunque el dispositivo de la red Inside no podrá diferenciarlo.



Además, hay diferentes modalidades de NAT:

- **NAT estático.**
La traducción se define manualmente de IP local a IP global. Se asegura de este modo que un nodo de la red Inside esté siempre representado por la misma dirección global en la red Outside. Generalmente utilizado para habilitar desde la red Global el acceso a un servidor alojado en la red Inside.
- **NAT dinámico.**
No hay una asignación uno a uno de IP local a IP global, sino que se define un conjunto de direcciones locales de origen que se traducen dinámicamente utilizando un conjunto de direcciones globales. Se asigna una IP global por cada IP local que atraviesa el dispositivo NAT.
- **NAT overload o PAT.**
La asignación dinámica se realiza ahora por conversación, no por IP. El origen de cada conversación generada en la red Inside (IP local : puerto origen) se traduce por una IP y puerto aptos en la red Outside (IP global : puerto).

En la definición de un dispositivo de NAT se pueden aplicar una o más de estas modalidades.

Configuración de NAT:

Procedimiento para la configuración de NAT en IOS:

1. Definición de la interfaz que conecta a la red Inside para NAT.
2. Definición de la interfaz que conecta a la red Outside de NAT.
3. Definición de los parámetros de traducción.

```
Router#configure terminal
Router(config)#interface fastethernet 0/0
Router(config-if)#ip nat inside
```

Define la interfaz que conecta a la red Inside.

```
Router(config-if)#interface serial 0/0/0
Router(config-if)#ip nat outside
```

Define la interfaz que conecta a la red Outside.

Definición de traducción de NAT estática.

```
Router(config)#ip nat inside source static [ip local] [ip global]
```

Definición de la traducción de NAT dinámica.

1. Definir las direcciones locales a traducir:

```
Router(config)#access-list [1-99] permit [ip local]
```

2. Definir el conjunto de direcciones globales a utilizar:

```
Router(config)#ip nat pool [name] [ip inicial] [ip final] netmask
X.X.X.X
```

3. Establecer la traducción de direcciones:

```
Router(config)#ip nat inside source list [X] pool [name]
```

Definición de traducción PAT utilizando una sola dirección IP pública.

```
Router(config)#access-list [1-99] permit [ip local]
Router(config)#ip nat inside source list [X] interface [int]
overload
```

Definición de traducción PAT utilizando más de una dirección IP pública.

```
Router(config)#access-list [1-99] permit [ip local]
Router(config)#ip nat pool [name] [ip] [ip] netmask X.X.X.X
Router(config)#ip nat inside source list [X] pool [name] overload
```

Comandos adicionales

```
Router#clear ip nat translation *
Router(config)#ip nat translation timeout [segundos]
```

Comandos de monitoreo de NAT

```
Router#show ip nat translation
Router#show ip nat statistics
Router#debug ip nat
```

Seguridad de la red

Los riesgos potenciales a los que están sometidas las redes de datos han experimentado en los últimos años una complejidad y sofisticación crecientes. La red está expuesta no sólo a amenazas externas (un atacante ajeno a la propia empresa u organización), sino también internas. Por esto la preocupación por la seguridad debe estar presente aún en el caso de redes que no tienen conexión con redes externas o con Internet.

- Amenazas Internas.
Amenazas a la seguridad de la red originadas al interior de la organización. Son las más serias.
La principal contramedida para responder a este tipo de amenazas son las políticas de seguridad.
Son particularmente importantes porque:
 - El usuario de la red tiene conocimientos de la red y los recursos disponibles.
 - El usuario típicamente tiene algún nivel de acceso relacionado con la naturaleza de su tarea.
 - Los mecanismos de seguridad tradicionales suelen no ser efectivos contra el potencial uso abusivo de un permiso de acceso legítimo.
- Amenazas Externas.
Son ataques de naturaleza más técnica, que se inician con menor conocimiento del interior de la red.
A estas amenazas se responde principalmente implementando defensas técnicas.

Requerimientos de seguridad básicos

Para asegurar una protección adecuada de los recursos de red, se deben garantizar 3 aspectos.

- Confidencialidad.
Permite garantizar que solamente usuarios autorizados pueden acceder a información sensible.
Implica restringir y controlar el acceso a la información. Algunos de los mecanismos que apuntan a este objetivo son:
 - Mecanismos para evitar el acceso no autorizado a los recursos de red.

- Necesidad de la presentación de credenciales para obtener acceso.
- Encriptación de tráfico.
- Integridad.
Garantiza que solamente personas autorizadas pueden cambiar la información sensible.
- Disponibilidad.
Garantiza el acceso ininterrumpido de los usuarios autorizados a los recursos de cómputo y a los datos.
Previene las interrupciones de servicio accidentales o intencionales (tales como ataques DoS).
Es quizás el aspecto más difícil de garantizar.

Cisco Network Foundation Protection

Es la estrategia de protección de la infraestructura de red utilizada por Cisco IOS, que permite responder a ataques de complejidad creciente para asegurar la disponibilidad de los dispositivos de red en cualquier circunstancia.

Para su desarrollo considera el dispositivo en 3 planos diferentes:

- Plano de Control.
Refiere a la capacidad del dispositivo para mantener una estructura de información referida a la red.
- Plano de Management.
Refiere a la capacidad de administrar o gestionar el dispositivo.
- Plano de Datos.
Refiere a la capacidad del dispositivo de reenviar tráfico.

Seguridad de dispositivos Cisco IOS

Al momento de asegurar un dispositivo es necesario tener presente una visión amplia y completa de los riesgos existentes para no reducirse exclusivamente a algunos puntos de configuración.

Hay múltiples amenazas de seguridad que deben ser consideradas:

- Amenazas físicas.
Hay diferentes tipos de amenazas físicas en primer lugar están aquellas que pueden producir daño físico al hardware de los dispositivos; también hay amenazas de tipo ambiental que pueden afectar el desempeño del hardware; amenazas que se generan a partir del suministro eléctrico indispensable para el funcionamiento de los equipos; y situaciones generadas en torno a las tareas de mantenimiento que están asociadas a la manipulación inapropiada de dispositivos y conectorizado.

- Ataques de reconocimiento.
Es la recopilación no autorizada de información de la red, que luego puede ser utilizada para ejecutar otros tipos de ataques, como DoS.
- Ataques de acceso.
Son intentos de explotar vulnerabilidades conocidas en los servicios de autenticación u otros, de modo de ganar acceso a información.
- Ataques de claves.
“Password attacks” es la denominación que se da comúnmente a los intentos repetidos de descubrimiento de credenciales de autenticación. También se los denomina ataques de fuerza bruta.

Cisco IOS provee un conjunto de prestaciones que permiten asegurar los planos de control y management de los routers.

Algunas best practices a implementar en dispositivos nuevos son:

- El management out-band es más difícil de vulnerar por parte de un atacante.
- Utilice protocolos de management encriptados (SSH y HTTPS).
- Implemente múltiples cuentas de usuarios con diferentes niveles de privilegio para asignar al staff técnico solamente los privilegios que son necesarios para cumplir su tarea.
- La administración centralizada de los usuarios facilita la tarea.
- Almacenar los registros de eventos (logs) en servidores remotos para poder analizar los eventos en caso de incidentes de seguridad en la red.
- Utilizar claves protegidas por hash incrementa significativamente el tiempo necesario para romperlas por fuerza bruta.
- La implementación de SNMPv3 con cuentas de usuario y autenticación HMAC mejora significativamente la seguridad.

Configuración de claves de acceso

IOS permite configurar claves de acceso y niveles de privilegios de acuerdo al modo de conexión.

- Clave de acceso por terminal virtual.
Se trata de los puertos a través de los cuales se establecen sesiones Telnet o SSH.
Es requerida por defecto y si no está configurada no se podrá acceder al router por Telnet o SSH.
- Clave de acceso por consola.

Adicionalmente, Cisco IOS permite configurar una clave de acceso al modo privilegiado.

Router (config) #**service password-encryption**

Encripta las claves que se guardan por defecto en texto plano en el archivo de configuración.

Router (config) #**line vty 0 4**

Ingresa al submodo de configuración del acceso por terminal virtual.

Router (config-line) #**password cisco**

Define una clave de acceso.

Router (config-line) #**login**

Habilita el requerimiento de clave para el acceso por terminal virtual.

Router (config-line) #**exec-timeout 5 0**

Define un umbral de tiempo de inactividad en las líneas de terminal virtual, tras el cual la sesión se cerrará automáticamente. En este caso es de 5 minutos 0 segundos.

Router (config-line) #exit

Router (config) #**line con 0**

Ingresa al submodo de configuración del acceso por puerto consola.

Router (config-line) #password cisco

Router (config-line) #login

Router (config-line) #exec-timeout 5 0

Router (config-line) #**logging synchronous**

Fuerza la sincronización de los mensajes de actividad del sistema operativo con los comandos ingresados por el operador, en la consola.

Router (config-line) #exit

Router (config) #**enable secret cisco123**

Establece una clave de acceso a modo privilegiado. Esta clave se guarda encriptada con MD5 en el archivo de configuración.

Cuando se desea utilizar un esquema de usuario y clave para autenticar el acceso a través de las terminales virtuales, puede utilizarse el siguiente formato:

Router (config) #**username xxxxxx password 0 xxxxx**

Define una base de datos de usuario y clave en el dispositivo. La clave puede ingresarse en texto plano (0) o encriptada utilizando MD5 (5).

Router (config) #**line vty 0 4**

Router (config-line) #**login local**

Indica que se desea utilizar la base de datos local de credenciales de autenticación para autenticar usuarios en el acceso.

También es posible definir un mensaje que se mostrará en la pantalla de la terminal de acceso al momento de ingresar al dispositivo.

```
Router(config)#banner motd # ATENCION. RED DE USO PRIVADO.  
Ingrese sus credenciales de autenticacion. #
```

Este mensaje se muestra en todas las terminales que se conectan antes del prompt que requiere las credenciales de acceso.

Implementación de SSH

Tanto Telnet como SSH son protocolos de terminal virtual (VTPs) que son parte del stack TCP/IP. Permiten iniciar sesiones de consola de modo remoto.

Si bien estos protocolos son sumamente importantes para facilitar el acceso al management de los dispositivos, es preciso trabajar de modo seguro ya que a través de ello se maneja información sensible de la red; por este motivo es recomendable utilizar siempre SSH y no Telnet.

La utilización de SSH proporciona un mecanismo seguro para reemplazar el uso de Telnet en el management de dispositivos ya que autentica y encripta la comunicación entre cliente y servidor (terminal de management y dispositivo de red).

Para implementar SSH en el management se requiere:

- Contar la posibilidad de habilitar el dispositivo como servidor SSH. Para esto IOS soporta tanto SSHv1 como SSHv2.
- Utilizar un programa emulador de terminal con soporte SSH. La mayoría de los programas de este tipo, disponibles en la actualidad (Putty, Teraterm, etc.); cuentan con esta posibilidad. Cisco IOS también incluye un cliente SSH.

Para implementar SSH es necesario, previamente, generar una llave de cifrado RSA en el dispositivo. Esto requiere que se cuente con un hostname (ya se tiene uno por defecto) y un dominio IP asignado al router.

La configuración del servicio en los dispositivos es relativamente simple:

```
Router(config)#hostname LAB_A  
LAB_A(config)#username cisco password cisco123
```

Define un usuario y clave en una base de datos local, para ser luego utilizado en el proceso de autenticación.

```
LAB_A(config)#ip domain-name mydomain.com
```

Define un nombre de dominio que se utilizará en el dispositivo.

```
LAB_A(config)#crypto key generate rsa
```

Genera la clave RSA que se requiere para operar con SSH.

El sistema operativo le requerirá que ingrese la longitud de la clave de cifrado que desea utilizar. Puede tener entre 360 y 2048 bits de longitud. La longitud por defecto es 512 bits. La longitud mínima recomendada es 1024 bits.


```
LAB_A(config)#ip ssh version 2
```

Establece el uso de SSH versión 2.

```
LAB_A(config)#line vty 0 4
```

```
LAB_A(config-line)#login local
```

Indica que se utilizará las credenciales de la base de datos de usuarios local para la autenticación.

```
LAB_A(config-line)#transport input ssh
```

Establece SSH como el protocolo para establecer sesiones de terminal virtual hacia el dispositivo.

Para iniciar una sesión SSH desde un dispositivo Cisco, se puede utilizar el cliente SSH incluido con el sistema operativo:

IOS incluye también un cliente SSH que puede ser utilizado para establecer sesiones hacia otros dispositivos:

```
LAB_A#ssh -l user 172.16.100.25
```

Para verificar la configuración de SSH:

```
LAB_A#show ip ssh
```

Muestra la versión y configuración de SSH en el dispositivo que actúa como SSH server.

```
LAB_A#show ssh
```

Permite monitorear las conexiones SSH que se han establecido hacia ese dispositivo.

Administración de múltiples sesiones de terminal virtual

Cisco IOS también ofrecen varias posibilidades para administrar múltiples sesiones vty abiertas desde un dispositivo.

Para suspender una sesión en curso y retornar al sistema local: Ctrl + Shift + 6 y luego x.

Para volver a una sesión suspendida:

- Enter.
- resume + número de sesión.

Para cerrar una sesión:

- En el dispositivo remoto: exit, logout o clear line.
- En el dispositivo local: disconnect.

```
Router#telnet Router_B
Router_B#Ctrl+shift+6 luego x
Router#
Router#[Enter]
Router_B#_
```

```

Router_B#exit
Router#_
Router#resume #
Router_B#_
Router_B#logout
Router#_

Router#disconnect [IP/Nombre]
Router#clear line #

```

Implementación de un registro de eventos

Syslog es un sistema de mensajes que permite que múltiples dispositivos en la red generen mensajes de estado y los almacenen en un dispositivo (servidor) centralizado para su posterior revisión por el Administrador.

En los dispositivos Cisco el sistema de mensajes de estado y eventos que genera puede ser enviado a distintas posiciones:

- A la pantalla de la consola (`console`).
- A la pantalla de una sesión telnet o SSH (`monitor`).
- A una consola SNMP en la red (`trap`).
- A un buffer de memoria local (`buffered`).

Los mensajes tienen un formato establecido:

```
*Dec 18 17:10:15.079: %LINEPROTO-5-UPDOWN: Line protocol on
Interface FastEthernet0/0, changed state to down
```

- Un registro de tiempo (fecha y hora).
Dec 18 17:10:15.079
- La porción del dispositivo que genera el mensaje.
%LINEPROTO
- Nivel de severidad del mensaje:
5
- Clave mnemotécnica.
UPDOWN
- Descripción del mensaje.
Line protocol on Interface FastEthernet0/0...

Los mensajes de logging tienen 8 niveles de severidad:

0	Emergency
1	Alert

2	Critical
3	Error
4	Warning
5	Notification
6	Informational
7	Debugging

Los niveles 0 a 4 representan eventos que pueden tener serio impacto en la operación del dispositivo. El Administrador tiene la posibilidad de definir hasta qué nivel de severidad desea recibir en cada una de las diferentes posiciones. Por ejemplo, almacenar hasta nivel 5 en el servidor de Syslog y recibir hasta nivel 7 en la terminal de consola.

Por defecto se envían todos los mensajes hasta nivel 7 al puerto de consola.

Configuración de los registros:

Router(config) #**service timestamps**

Habilita la inclusión de fecha y hora en el encabezado de los mensajes.

Router(config) #**service sequence-numbers**

Habilita la inclusión de un número de secuencia en el encabezado de los mensajes.

Router(config) #**logging on**

Activa el proceso de logging.

Router(config) #**logging buffered 200000**

Determina el buffer de memoria que ha de dedicarse a los mensajes de syslog. Los mensajes almacenados en este buffer se pueden revisar con el comando `show logging`.

El tamaño del buffer se establece en bytes. Por defecto, el tamaño es 4096 bytes y el nivel de severidad es debugging.

Router(config) #**logging 172.16.1.2**

Indica un servidor de syslog como destino para almacenar los mensajes.

Router(config) #**logging trap warnings**

Limita los mensajes enviados al servidor de syslog en base al nivel de severidad.

El nivel de severidad también puede expresarse en forma numérica, en este caso: 4.

Router(config) #**logging monitor notifications**

Limita los mensajes que se enviará a las terminales virtuales, en base al nivel de severidad.

Router (config) **#logging console**

Habilita los mensajes de syslog en la terminal de consola. Estos mensajes están habilitados por defecto.

Simple Network Management Protocol (SNMP)

Protocolo de capa de aplicación que proporciona un servicio de mensajería entre dispositivos (agentes SNMP) y una consola de gestión (SNMP Manager). SNMP permite desarrollar una estructura de administración (NMF) basada en estándares elaborados a partir de múltiples RFCs.

- **SNMP Manager.**
Aplicación de gestión de red que proporciona funcionalidades de monitoreo y gestión al Administrador.
También denominado NMS (Network Management Station).
- **Agente SNMP.**
Software que opera en un dispositivo de red que se desea gestionar.
Recoge información en una base de datos (MIB – Management Information Base) que contienen variables de estadística y configuración del dispositivo.



El SNMP Manager periódicamente consulta al Agente SNMP para recolectar información sobre la que luego realiza análisis; también puede realizar modificaciones en la configuración a través del Agente SNMP, si esto se permite.

Se utilizan 3 tipos de mensajes:

- **Mensajes GET.**
Permite que el SNMP Manager requiera información de los Agentes SNMP que almacena en su base de datos para luego poder analizarla o consultarla.
La mayoría de las consolas SNMP permiten que el Administrador configure intervalos de tiempo para que la consulta se realice de modo automático.
- **Mensajes SET.**
Mensajes SNMP que envían modificaciones en los parámetros de configuración que se almacenan en la MIB para que luego se modifique la configuración del dispositivo.
- **Mensajes Trap.**
Notificaciones generadas por el mismo Agente SMNP que se envían al

NMS sin que haya consulta previa para informar algún evento en particular.
Estos mensajes pueden desencadenar algún proceso tal como mostrar una alarma en pantalla o disparar la notificación por SMS al Administrador del evento.

Hay 3 versiones principales de SNMP:

- SNMPv1 con control de acceso basado en la comunidad.
- SNMPv2c.
Mejoró el sistema de mensajes, lo que permite obtener mayor cantidad de información del dispositivo de modo más eficiente.
Utiliza el mismo sistema de autenticación basado en el nombre de comunidad que la versión 1.
El nombre de comunidad opera como una clave de autenticación que viaja en texto plano, por lo que su nivel de seguridad es bajo y lo hace susceptible de ataque tipo man-in-the-middle
Hay 2 tipos de comunidades:
- Read-only (RO) – Permite solamente el monitoreo del dispositivo.
- Read-write (RW) – Permite acceso de lectura y escritura.
- SNMPv3 con autenticación de usuario y encriptación.
Incorpora prestaciones de seguridad: Integridad, autenticación y encriptación.

El protocolo versión 3 permite 3 variantes de seguridad:

Nivel	Keyword	Autenticación	Encriptación
NoAuthNoPriv	noaut	Username	---
AuthNoPriv	auth	MD5 o SHA	---
AuthPriv	pri	MD5 o SHA	DES o AES

Configuración de SNMP v2c

Dada la vulnerabilidad de la versión 2c de SNMP, generalmente es implementado exclusivamente en modalidad read-only.

```
Router(config)# ip access-list standard SNMP
Router(config-std-nacl)# permit host 172.16.10.101
Router(config-std-nacl)# exit
Router(config)# ip access-list standard SNMP2
Router(config-std-nacl)# permit host 172.16.20.54
Router(config-std-nacl)# exit
Router(config)# snmp-server community LabCisco RO SNMP
```

Define un nombre de comunidad read-only, y limita el acceso al host permitido en la lista de acceso.

```
Router(config)# snmp-server location BuenosAires
Router(config)# snmp-server contact Oscar Gerometta
Router(config)# snmp-server community LabCisco2 RW SNMP2
```

Define un nombre de comunidad read-write, y limita el acceso al host permitido en la lista de acceso.

NetFlow

Aplicación diseñada por Cisco y embebida en IOS que permite relevar información estadística de tráfico en la red.

Responde a 2 premisas básicas:

- Es completamente transparente a las aplicaciones y dispositivos que operan en la red.
- No es necesario que sea soportado en todos los dispositivos de la red.

Su implementación tiene múltiples aplicaciones posibles, las más frecuentes son:

- Registro estadístico de tráfico para realizar un análisis de línea base.
- Facturación de servicios de red a usuarios.
- Diseño o rediseño de redes, para analizar el tráfico y aplicaciones que están corriendo sobre la red.
- Diseño general de seguridad de la red.
- Detección y prevención de ataques DoS o DDoS.
- Monitoreo de la red.

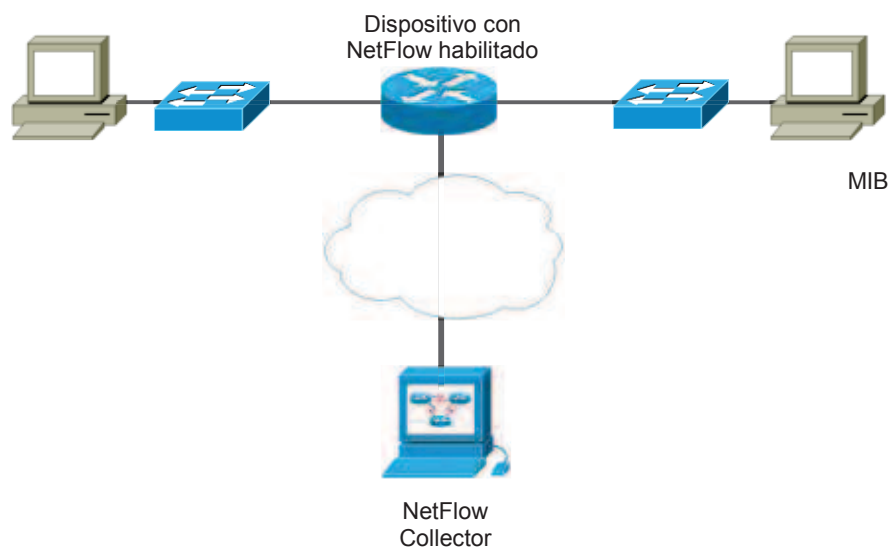
Para esto, Netflow releva estadística de comunicaciones utilizando el concepto de flujo (flow): Stream unidireccional de paquetes entre un sistema de origen y un sistema destino específicos.

Esta definición de flujo se hace en base a 7 parámetros específicos:

- Dirección IP origen.
- Dirección ID destino.
- Puerto de origen.
- Puerto de destino.
- Tipo de protocolo (campo del encabezado IP).
- Tipo de servicio (campo del encabezado IP).
- Interfaz lógica de ingreso.

La implementación de NetFlow supone una arquitectura específica:

- Un dispositivo que tiene NetFlow habilitado.
- Un NetFlow Collector, que es la consola que concentra y permite concentrar la información.



Configuración de NetFlow

El procedimiento de configuración requiere 2 tareas:

- Definir el punto (interfaz) de captura de información.
- Definir la ubicación del NetFlow Collector.

```
Router(config)#interface GigabitEthernet0/0
Router(config-if)#ip flow ingress
```

Define la captura de datos correspondientes al tráfico que ingresa a través de la interfaz.

```
Router(config-if)#ip flow egress
```

Define la captura de datos correspondientes al tráfico que egresa a través de la interfaz.

```
Router(config-if)#exit
Router(config)#ip flow-export destination 10.1.10.100 99
```

Configura la dirección IP y puerto a la cual se debe dirigir la información de NetFlow que surja de la captura en la interfaz.

```
Router(config)#ip flow-export version 9
```

Define la versión de NetFlow a utilizar en el diálogo con el collector.

Router(config)#**ip flow-export source loopback 0**

Dirección que se utilizará como dirección IP de origen para enviar la información hacia el collector.

Router(config)#end

Comandos para verificar y acceder a la información de NetFlow:

Router#**show ip cache flow**

Permite verificar la operación de NetFlow en el dispositivo, la cantidad de paquetes analizados y las estadísticas correspondientes a cada uno de los flujos capturados.

Router#**show ip flow interface**

Verifica la configuración de NetFlow en las interfaces.

Router#**show ip flow export**

Permite verificar la configuración de los parámetros de exportación de la información y las estadísticas correspondientes.



Para profundizar o tener mayor información sobre cualquiera de estos puntos, sugiero consultar mi libro “Guía de Preparación para el Examen de Certificación CCNA”.

2.7. Tecnologías WAN

Terminología WAN

- Punto de demarcación.
- Bucle local.
- POP – Punto de presencia.
- CO – Central Office.
- CPE – Customer Premises Equipment.

Cuando se conecta a una línea digital se utiliza un CSU/DSU.

Cuando se conecta a una línea analógica utiliza un módem.

- DTE y DCE.

Tipos de conexión WAN

Redes WAN privadas

Líneas Dedicadas.

Mayor control, ancho de banda dedicado, alto costo.

No está sometida a latencia ni fluctuaciones de fase.

Enlaces de acceso: T1, E1 y siguientes.

Interfaz del router: Serial.

Protocolos de encapsulación: HDLC, PPP.

Redes de Paquetes Conmutados.

Operan sobre la base del establecimiento de circuitos virtuales.

- X.25.
Bajo control, ancho de banda compartido, costo variable.
Puede presentar latencia y fluctuaciones de fase. Para un uso limitado de alta confiabilidad.
- Frame Relay.
Control medio, ancho de banda compartido de hasta 8 Mbps, costo medio.
Puede presentar latencia y fluctuaciones de fase.
Enlace de acceso: T1, E1 y siguientes.
Interfaz del router: Serial.
Protocolo de encapsulación: Frame Relay.

Redes de Celdas Conmutadas.

- ATM.
Ancho de banda compartido, de baja latencia y ancho de banda de hasta 155 Mbps.

Puede transmitir tanto tráfico de voz y video como de datos. Presenta baja latencia y fluctuación de fase.

Redes Ethernet WAN.

Redes de fibra óptica, de largo alcance que utilizan tecnología Ethernet.

Enlace de acceso: pueden llegar a 100 Mbps o 1 Gbps.

Interfaz del router: Ethernet.

Protocolo de encapsulación: Ethernet.

- Ethernet over MPLS (EoMPLS).
- Metropolitan Ethernet (MetroE)
- Virtual Private LAN Service (VPLS)

Multiprotocol Label Switching (MPLS)

Hay diversos tipos de servicio posibles.

Permite conectar sitios a una nube MPLS que reenvía el tráfico a los diferentes destinos. Se basa en la entrega de paquetes IP, no ya de tramas.

Es mucho más flexible que otros servicios WAN.

Enlace de acceso: Cualquiera que soporte IP.

Interfaz del router: Cualquiera que soporte IP.

Protocolo de encapsulación: Cualquiera que soporte IP.

- MPLS VPN.

VSAT

Permite brindar servicios de acceso en sitios en los que no es posible llegar con cableado. Se genera una red WAN utilizando un satélite de comunicaciones y terminales VSAT.

Redes WAN públicas y acceso a Internet

Enlaces de acceso a Internet.

Cada tecnología WAN de las en redes WAN privadas puede ser también utilizada para brindar acceso a Internet.

Redes de Circuitos Conmutados.

- Dial up asincrónico
Bajo control, costo del servicio variable y bajo costo de implementación.
Para uso limitado en conexiones DDR.
Utiliza líneas telefónicas analógicas y un módem telefónico para modular la señal digital de una terminal sobre la línea analógica.
Presentan poca latencia y fluctuaciones de fase. Tienen una capacidad máxima de 56 Kbps.
Enlace de acceso: línea telefónica.
- Integrated Services Digital Network (ISDN).
Bajo control, mayor ancho de banda disponible que con un dial-up y mayor velocidad en el establecimiento de la llamada sobre líneas digitales.
Permite la transmisión simultánea de voz, video y datos. No está sometida a latencia ni fluctuaciones de fase.
Posibilita conexiones de 128 Kbps (BRI) y hasta 2 Mbps (PRI).

Utiliza un módem ISDN para terminar las conexiones.
Enlace de acceso: línea telefónica.

xDSL.

Tecnología de banda ancha que utiliza líneas telefónicas para transportar datos con alto ancho de banda en frecuencias superiores a los 4 KHz.
Permiten superar las limitaciones de ancho de banda de los servicios de circuito conmutado, a la vez que implementan múltiples servicios (telefonía y datos) sobre el mismo enlace de acceso.

- ADSL – Asimétrico.
- SDSL – Simétrico.
- HDSL – de alta velocidad

Cable módem.

Servicio de acceso a redes por tecnología de banda ancha que utiliza cable coaxial de televisión para proveer alto ancho de banda de 1 ó 2 vías a frecuencias de 6 Mhz.

Interfaces WAN de los routers Cisco

Las interfaces WAN de los routers, usualmente se conectan a un CSU/DSU externo utilizando un cable serial a la interfaz serial del router.

Serial asincrónica.

Utilizan un conector RJ-45, con capacidad de soportar conexiones asincrónicas dial up utilizando un módem.

Serial sincrónica.

En el caso de routers Cisco estas interfaces están integradas en una WIC (WAN Interface Cards). Soportan líneas dedicadas, Frame Relay y X-25.

Del lado de la interfaz del router, hay 2 tipos de conectores:

- Conector DB-60.
- Conector Smart-Serial.
Utiliza un conector de 26 pins.

El conector a la CSU/DSU habitualmente es uno de los siguientes:

- EIA/TIA-232
- V.35
- X.21

También se cuenta con placas WIC que integran la CSU/DSU, en cuyo caso el cable serial no es necesario y el cable que viene del service provider se conecta directamente al puerto del router, sin necesidad de una CSU/DSU externa.

Protocolos WAN de capa de enlace de datos

Las tramas más frecuentemente utilizadas son:

- HDLC (High-level Data Link Control).
- PPP (Point to Point Protocol).
- Frame Relay.
- ATM (Asynchronous Transfer Mode).

Líneas dedicadas

Bases de una conexión serial

La velocidad de las líneas dedicadas sigue las definiciones que se generaron en su momento en base al estándar de las líneas telefónicas. La base de definición de velocidad de las líneas es la de una línea telefónica digital o DS0 que es de 64 Kbps. De ahí que la asignación de ancho de banda de estas líneas es siempre un múltiplo de 64:

Denominación	T-Carrier	E-Carrier
DS0	0,064 Mbps	0,064 Mbps
DS1	T1 - 1,544 Mbps	E1 - 2,048 Mbps
DS2	T2 - 6,312 Mbps	E2 - 8,448 Mbps
DS3	T3 - 44,736 Mbps	E3 - 34,368 Mbps

La línea del service provider, típicamente se conecta a un CSU/DSU, que a través de una conexión serial es conectado al router de borde de la red corporativa. Este dispositivo opera en la capa física y actúa como intermediario entre la red del service provider y el router.

La conexión entre la CSU/DSU y el router es una conexión serial sincrónica. Como toda conexión sincrónica tiene un extremo DCE (la CSU/DSU) que controla la velocidad de la conexión, y otro extremo DTE (el router) cuya sincronía es controlada desde el extremo DCE. De este modo el router envía y recibe bits solamente cuando el DCE genera el pulso eléctrico (clocking) correcto en el cable que envía señal de clock.



El extremo DCE de la conexión es el que define la velocidad de la misma.

Encapsulación HDLC

- Protocolo de encapsulación de capa de enlace de datos.
- Provee servicios de encapsulación de tramas en enlaces sincrónicos punto a punto.
- Provee un preámbulo que indica la recepción a continuación de una trama, y un FCS para verificar posibles errores en la transmisión.
- La versión propietaria de Cisco agrega un campo tipo que le permite soportar múltiples protocolos de capa de red. Esto permite, por ejemplo, transportar IPv4 e IPv6 sobre el mismo enlace.

Flag	Direc	Ctrl	Tipo	Datos	FCS
------	-------	------	------	-------	-----

- Es la opción de encapsulación por defecto en enlaces seriales con IOS.

Configuración de HDLC

```
Router(config)#interface Serial0/0/0
Router(config)#encapsulation hdlc
```

HDLC es la opción por defecto en interfaces seriales. Si hay otro protocolo configurado, se puede utilizar este comando (no está soportado en todas las plataformas) o se puede negar el protocolo ya configurado: `no encapsulation ppp`

```
Router(config)#ip address 192.168.2.1 255.255.255.0
Router(config)#clock rate 2000000
```

Cuando la interfaz del router debe operar como DCE (para esto es necesario que se haya utilizado un cable DCE), se debe definir el clocking de la interfaz.

Este comando no se utiliza cuando el puerto está conectado a una DCU/CSU.

```
Router(config)#no shutdown
```

Encapsulación PPP

PPP es un protocolo estándar de encapsulación de capa 2 que puede ser utilizado sobre diferentes tipos de enlaces. PPP puede operar sobre una variedad muy amplia de tecnologías de capa física (enlaces sincrónicos y asincrónicos).

Protocolos que confluyen en la implementación de PPP:

- HDLC.
Se utiliza para el transporte de datos.
- LCP.
Negocia las condiciones de establecimiento y cierre del enlace.

- NCP.
Permite detectar y operar con múltiples protocolos de capa 3.

Se utiliza una instancia de LCP por cada enlace, y una instancia de NCP por cada protocolo de capa 3 que se negocia en cada enlace.

El protocolo incluye importantes opciones de configuración:

- Autenticación: PAP / CHAP.
- Compresión.
- Detección de errores.
- Multilink.

El establecimiento de un enlace PPP pasa por varias etapas:

- | | |
|--|-------|
| 1. Fase de establecimiento de la conexión. | LCP. |
| 2. Fase de autenticación (opcional). | LCP. |
| 3. Fase de protocolo de red. | NCP. |
| 4. Transferencia de datos. | HDLC. |
| 5. Fase de cierre de la sesión. | LCP. |

Configuración de PPP

```
Router#config terminal
Router(config)#interface serial 0/0/0
Router(config-if)#encapsulation ppp
Define PPP como protocolo de encapsulación del enlace.
Router(config-if)#ppp authentication [chap/pap/pap chap/chap pap]
```

Comandos de monitoreo de PPP

```
Router#show interfaces serial 0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is HD64570
  Internet address is 192.168.13.1/24
  MTU 1500 bytes, BW 64Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation PPP, loopback not set, keepalive set (10 sec)
  LCP Open
  Open: IPCP, CDPCP
  [continúa...]
```

```
Router#show running-config
Router#debug ppp negotiation
Router#debug ppp authentication
1d01h: %LINK-3-UPDOWN: Interface Serial0/0/0, changed state to up
1d01h: Se0/0/0 PPP: Testing connection as a dedicated line
1d01h: Se0/0/0 PPP: Phase is AUTHENTICATING, by both
```

```
1d01h: Se0/0/0 CHAP: O CHALLENGE id 2 len 28 from "Router"
1d01h: Se0/0/0 CHAP: I RESPONSE id 2 len 28 from "LAB_A"
1d01h: Se0/0/0 CHAP: O SUCCESS id 2 len 4
1d01h: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, change state to up
```

```
Router#debug ppp packet
```

Autenticación de PPP

PPP define 2 protocolos de autenticación: PAP (Password Authentication Protocol) y CHAP (Challenge Handshake Authentication Protocol).

- PAP.
El dispositivo que inicia la conexión solicita ser autenticado enviando la clave en texto plano. El dispositivo que recibe la clave confirma que es la correcta y envía un mensaje de acknowledgment para informar que la autenticación fue exitosa.
Está en desuso porque el intercambio de la clave en texto plano lo hace muy vulnerable.
- CHAP.
Es la opción más segura, y la más implementada.
El dispositivo que requiere autenticación inicia el intercambio enviando un texto de desafío (challenge) solicitando respuesta. El dispositivo que recibe el desafío devuelve el texto luego de pasarlo por un algoritmo de hash (MD5). Finalmente el que inició el proceso compara el hash recibido para verificar que sea el correcto, y si la comparación es exitosa envía al otro extremo el mensaje de confirmación.

Si la autenticación falla, la interfaz queda en estado up/down.

Configuración de autenticación con CHAP

Para agregar autenticación CHAP en un enlace que utiliza PPP se requiere:

- Definir un nombre (hostname) para los dispositivos.
- Ingresar el nombre del otro dispositivo como username y la clave compartida.
- Aplicar el protocolo de autenticación en la interfaz de cada uno de los extremos del enlace.

```
LAB_A#configure terminal
LAB_A(config)#username LAB_B password cisco
LAB_A(config)#interface serial 0/0/0
LAB_A(config-if)#encapsulation ppp
LAB_A(config-if)#ppp authentication chap
LAB_A(config-if)#no shutdown
```

```
Router#configure terminal
Router(config)#hostname LAB_B
```

```

LAB_B(config)#username LAB_A password cisco
LAB_B(config)#interface serial 0/0/0
LAB_B(config-if)#encapsulation ppp
LAB_B(config-if)#no shutdown

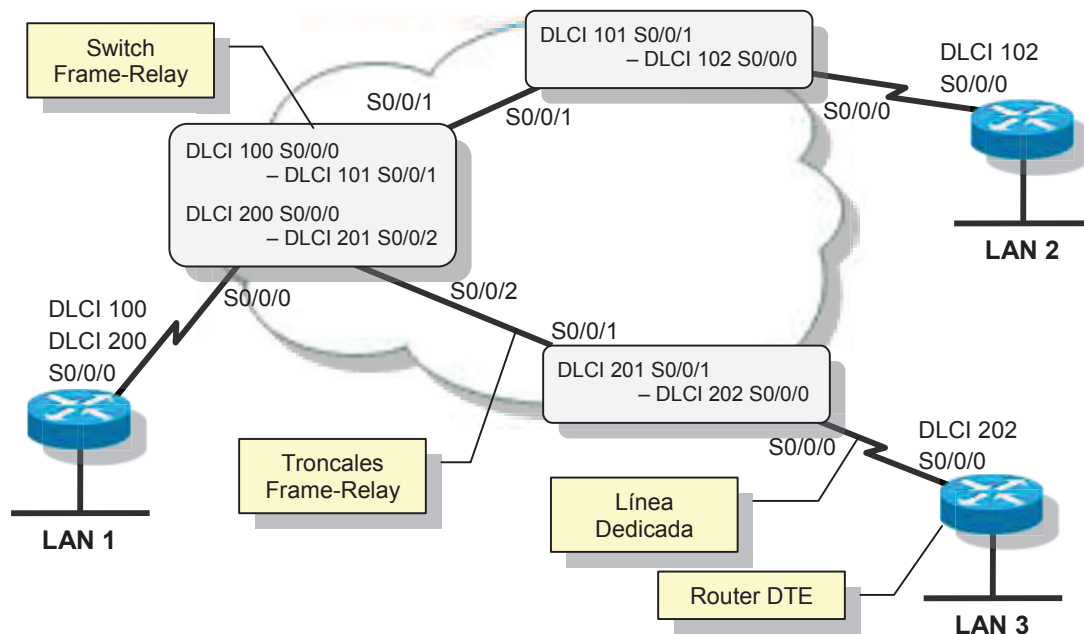
```

Frame Relay

Frame Relay es una tecnología que provee servicios de conmutación de paquetes orientados a la conexión a través de circuitos virtuales, sin corrección de errores, a través de una red multiacceso.

Esta red no soporta tráfico de broadcast, por lo que es denominada como red NonBroadcast MultiAccess (NBMA).

Sus circuitos virtuales (VC) son conexiones lógicas entre dos dispositivos DTE a través de una red de paquetes conmutados. Dado que se trata de una red multiacceso, las interfaces DTE que deben enlazarse se identifican por un DLCI para ser halladas dentro de los múltiples accesos de la red del service provider.



La conexión lógica entre 2 DTEs es lo que denominamos circuito virtual (VC). Hay 2 tipos de VCs:

- PVC – Permanent Virtual Circuits.
- SVC – Switched Virtual Circuits.

Terminología Frame Relay

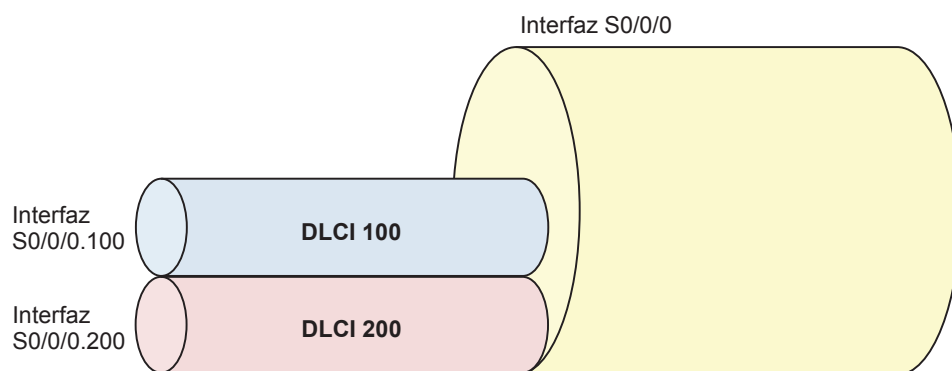
- Circuito Virtual (VC).
Ruta que atraviesan las tramas Frame Relay entre 2 dispositivos DTE.

- Data Terminal Equipment (DTE).
Dispositivo conectado a una servicio Frame Relay.
- Data Communications Equipment (DCE).
Switch Frame Relay.
- Velocidad de acceso (AR).
Velocidad de la línea dedicada que conecta el DTE a la red Frame Relay.
- Velocidad de transmisión de información acordada (CIR).
Velocidad a la que se transmiten los bits sobre un circuito virtual, la que está pautada por el contrato con el proveedor de servicios.
- Data Link Connection Identifier (DLCI).
Dirección de capa de enlace de datos utilizada en el encabezado Frame Relay para identificar el circuito virtual.
- Local Management Interface (LMI).
Protocolo utilizado en el enlace entre DCE y DTE para gestionar la conexión.

Circuitos virtuales

Se trata de una ruta que atraviesa la red Frame Relay para unir 2 dispositivos DTE, uniendo virtualmente esos 2 puntos como se tratara de un enlace punto a punto.

Múltiples circuitos virtuales pueden compartir un mismo enlace físico, lo que posibilita que una interfaz física se conecte con múltiples puntos remotos utilizando múltiples circuitos punto a punto. Cada uno de esos circuitos está identificado con un DLCI diferente.



Esta es la base de una de las ventajas de Frame Relay: es posible conectar múltiples puntos remotos utilizando una única interfaz física y un único enlace de acceso a la red del proveedor de servicio.

Para activar la operación de Frame Relay en la interfaz de un router DTE es necesario en primer lugar configurar la interfaz para que utilice encapsulación Frame Relay.

En Cisco IOS se dispone de dos formas de encapsulación para Frame-Relay:

- Encapsulación propietaria de Cisco (es la opción por defecto).
- Encapsulación estándar IETF.

```
Router(config)#interface serial 0/0/0
Router(config-if)#encapsulation frame-relay cisco
Router(config-if)#encapsulation frame-relay ietf
```

DLCI

Los circuitos virtuales Frame Relay se diferencian utilizando un identificados denominado DLCI.

Este identificador es asignado por el proveedor de servicio; los valores posibles de este ID están entre 0 y 1023, siendo algunos de estos valores reservados:

0	LMI (estándar ANIS e ITU-T).
1 a 15	Reservados para uso futuro.
16 a 1007	Asignables.
1008 a 1022	Reservados para uso futuro.
1019 a 1022	Multicast (Cisco).
1023	LMI (Cisco).

Se pueden asociar varios DLCI a una única interfaz (uno por cada PVC que termina en esa interfaz). El número de DLCI puede ser asignado a la interfaz de modo dinámico a través de los mensajes LMI de actualización y consulta de estado, o bien de modo manual.

Para definir manualmente el DLCI asociado a una interfaz:

```
Router(config)#interface serial 0/0/0
Router(config-if)#encapsulation frame-relay
Router(config-if)#frame-relay interface-dlci [16-992]
```

Cuando se trata de circuitos o conexiones punto a multipunto, cada dirección IP remota debe ser mapeada a un DLCI de modo que el sistema operativo tenga la información necesaria para encapsular tráfico que debe ser enviado a una IP de destino en el VC correcto. Cuando se trata de VCs punto a punto no se requiere el mapeo de direcciones IP ya que el único puerto posible al otro lado del circuito es el que de hecho se encuentra.

El mapeo de direcciones IP a DLCI se realiza de dos formas diferentes:

- Mapeo dinámico.
Para esto se utiliza el protocolo IARP (ARP Inverso). Es la opción por defecto y no es necesario activarla.

```
Router(config-if)#frame-relay inverse-arp
```

- Mapeo estático.

Lo realiza el Administrador utilizando el comando map

```
Router(config-if)#frame-relay map [protocolo]
[dirección] [dlci] [broadcast]
[encapsulación]
```

Configura el mapeo estático definiendo la correspondencia IP / DLCI.

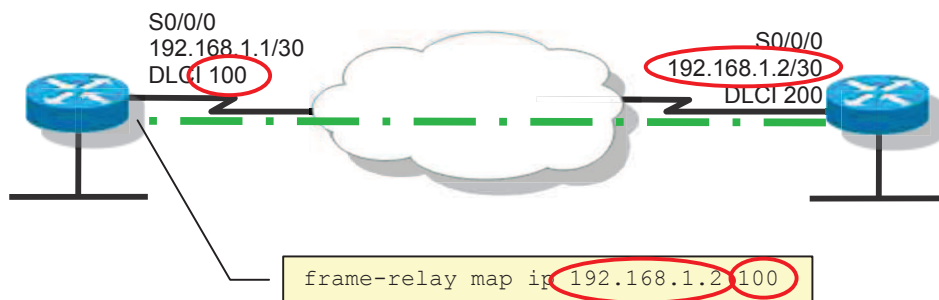
[protocolo] - Protocolo de capa de red que utiliza el VC.

[dirección] - Dirección de capa 3 de la interfaz remota del VC.

[dlci] - DLCI local del VC.

[broadcast] - Permite la utilización del PVC para enviar tráfico de broadcast y multicast (opcional).

[encapsulación] - Permite modificar el formato de encapsulación (cisco o ietf) asignado a la interfaz física, en una subinterfaz (opcional).



Atención:

Se mapea el DLCI local con la dirección IP del punto remoto.

Interfaz de Gestión Local (LMI)

Frame Relay implementa un método de señalización entre el dispositivo CPE y el switch Frame Relay denominado interfaz de gestión local. Este método de señalización es el responsable de mantener y administrar el enlace entre DTE y DCE, y para su circulación utiliza un DLCI específico.

Este método de señalización recibe la denominación de Local Management Interface (LMI) y en el caso de Cisco IOS se puede optar entre diferentes tipos de LMI, todos incompatibles entre sí. Los tipos disponibles de LMI en IOS son:

- Cisco.

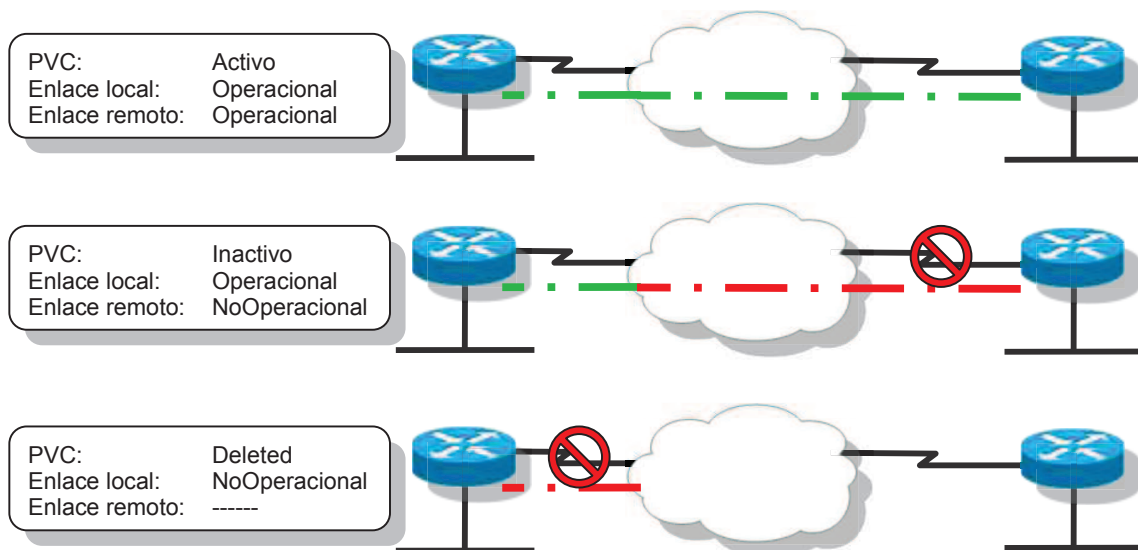
Versión propietaria que es la opción por defecto en los dispositivos Cisco.

- ANSI.
Versión publicada en el estándar T1.617 anexo D de ANSI.
- ITU-T (q933a).
Otra versión estándar publicada en el ITU-T Q933 anexo A.

LMI incluye múltiples funcionalidades o “extensiones”, entre las que se encuentran:

- Keepalive.
Los paquetes LMI son los responsables de mantener el VC en funcionamiento.
- Control del flujo de datos.
- Brinda soporte a la entrega de mensajes de protocolos de enrutamiento y otros mensajes a destinos múltiples o de tipo multicast.
- Puede definir que el DLCI tenga significado local o global.
Esto permite identificar una interfaz específica en toda la red FR de modo que opere de modo semejante a una LAN.
- Proporciona un mecanismo de comunicación y sincronización entre el switch FR y el dispositivo DTE del usuario.

Una de las funciones de los paquetes LMI es brindar información sobre el estado de los PVCs. Esto permite mantener información actualizada sobre el estado de cada circuito virtual, para lo que define tres diferentes estados del PVC:




- **ACTIVE**
Indica que el enlace se encuentra operativo, por lo que los routers DTE de ambos extremos del PVC pueden intercambiar información.
- **INACTIVE**
Indica que la interfaz del router local está operativa, pero la conexión al

router o DTE remoto no es accesible.
Indica un problema en el enlace remoto.

- **DELETED**
Un PVC en este estado indica que no se está recibiendo información LMI desde el switch.
Indica un problema en el enlace local.

Cuando se desea cambiar el tipo de LMI por defecto (Cisco), se utiliza el siguiente comando.

```
Router(config-if) #frame-relay lmi-type [ansi/cisco/q933a]
```

 El tipo de LMI configurado en el router debe coincidir con el que utiliza el proveedor de servicio. Cisco IOS establece por defecto la detección automática del tipo de LMI.

Ejemplo de configuración de una interfaz Frame Relay



```
Router(config)#interface serial0/0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.252
Router(config-if)#encapsulation frame-relay ietf
Router(config-if)#frame-relay lmi-type ansi
Router(config-if)#frame-relay interface-dlci 100
Router(config-if)#no frame-relay inverse-arp
Router(config-if)#frame-relay map ip 192.168.1.2 100 broadcast
Router(config-if)#no shutdown
```

En términos generales, cuando se trata de redes Cisco la configuración de la interfaz, aprovechando las opciones por defecto de IOS se abrevia a lo siguiente:

```
Router(config)#interface serial0/0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.252
Router(config-if)#encapsulation frame-relay
Router(config-if)#no shutdown
```

Creación de subinterfaces sobre enlaces seriales

Las interfaces físicas que utilizan encapsulación Frame Relay se comportan, en todos los casos, como interfaces punto a multipunto. Es decir, permiten la asignación de múltiples DLCIs (múltiples PVCs) para conectarse a múltiples puntos remotos.

Cuando se desea establecer PVCs que operen exclusivamente como enlaces punto a punto; o cuando se deben combinar diferentes tipos de enlaces (punto a punto con punto a multipunto) sobre una misma interfaz física, entonces es preciso recurrir a la creación de subinterfaz.

La creación de subinterfaces en enlaces seriales para la implementación de Frame Relay permite asociar varios circuitos virtuales (cada uno identificado por su DLCI) a una misma interfaz física. Las subinterfaces son interfaces virtuales, lo que permite dar a cada PVC un tratamiento de configuración totalmente independiente.

Las subinterfaces son divisiones lógicas de una única interfaz física. A nivel de capa 2 y 3 cada subinterfaz se comporta de modo independiente. Son una única interfaz a nivel de capa física. Como consecuencia, todo lo que afecta a la interfaz física afecta a todo el conjunto de subinterfaces asociadas a esa interfaz.

Hay 2 tipos de subinterfaces Frame Relay:

- Subinterfaces punto a multipunto.
Se trata de una interfaz lógica que se constituye en centro de una estrella que conecta con múltiples VCs.
En este caso, todas las subinterfaces o interfaces remotas conectadas a la subinterfaz multipunto se deben encontrar en una única red o subred.
Este tipo de subinterfaz requiere mapeo IP / DLCI ya sea estático o dinámico.

```
Router(config)#interface serial0/0/0
Router(config-if)#encapsulation frame-relay
Router(config-if)#interface serial 0.2 multipoint
Router(config-subif)#_
```

- Subinterfaz punto a punto.
Se utiliza para circuitos que conectan un extremo DTE con solamente otro remoto.
Cada par de interfaces conectadas en un enlace Frame Relay punto a punto deben pertenecer a la misma red o subred, y cada subinterfaz tiene asociado un solo DLCI.
Tenga en cuenta que este tipo de subinterfaces no requiere mapeo IP/DLCI.


```
Router(config)#interface serial 0
Router(config-if)#encapsulation frame-relay
Router(config-if)#interface serial 0.1 point-to-point
Router(config-subif)#_
```



En todos los casos, en la interfaz física debe configurarse la encapsulación frame-relay.



NO debe configurarse la dirección de red en la interfaz. La dirección de red se configura en cada subinterfaz.

 La única manera de crear PVCs punto a punto en IOS es utilizando subinterfaces..

La dirección de capa de red, así como el DLCI se configura en cada subinterfaz, El DLCI debe configurarse manualmente porque la operación de LMI no puede descubrir las subinterfaces.

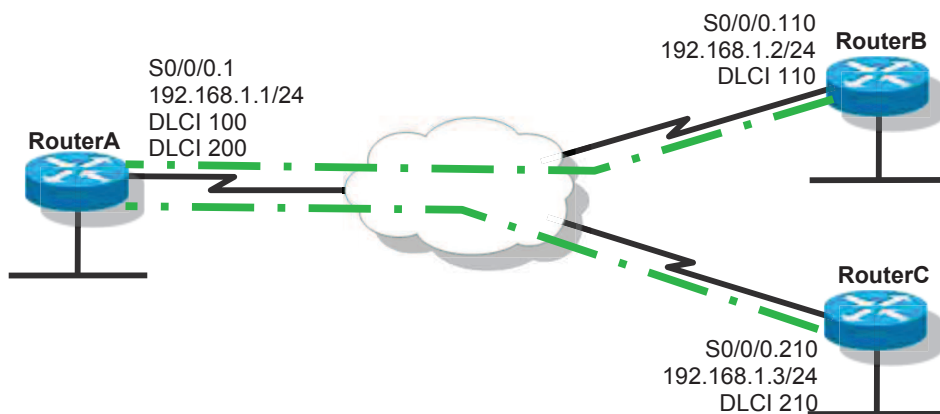
Redes Frame Relay Hub and Spoke

Las redes Frame Relay que implementan una topología física en estrella y lógica punto a multipunto, requieren una consideración particular cuando implementan protocolos de enrutamiento dinámico sobre el enlace Frame Relay.

En este tipo de diseño, todos los dispositivos conectados en la estrella utilizan sobre la red Frame Relay una única subred IP.

Este tipo de diseño requiere algunas consideraciones especiales:

- Todas las interfaces conectadas a la estrella deben pertenecer a la misma subred.
- Los protocolos de enrutamiento propagan sus actualizaciones utilizando multicast o broadcast, pero la red Frame Relay es una red multiacceso sin broadcast.
Para que el protocolo de enrutamiento pueda propagar sus actualizaciones se requiere la utilización de la opción “broadcast” en la configuración del mapeo de IP a DLCI.
- En el router hub (RouterA de nuestro ejemplo), las actualizaciones de enrutamiento que envían los extremos de la estrella (RouterB y RouterC) se reciben todos a través de una única interfaz física.
Cuando se utilizan protocolos de enrutamiento por vector distancia, la regla de Split horizon impide que la actualización que se recibe por una interfaz se propague por la misma interfaz. Esta regla, en este diseño, impide que los routers remotos aprendan rutas unos de otros.
Para solucionar este problema, es preciso desactivar la regla de Split horizon en el enrutamiento.



El modo más simple y recomendado por Cisco para solucionar estos posibles inconvenientes, es configurar todos los PVC como punto a punto, utilizando subredes con máscara de 30 bits de longitud para el direccionamiento IP.

Configuración de Frame Relay

Configuración de una interfaz serial con Frame Relay

```
Router(config)#interface serial 0/0/0
Router(config-if)#encapsulation frame-relay
Router(config-if)#frame-relay lmi-type cisco
Router(config-if)#no shutdown
```



¡Atención!: Si se configurarán subinterfases, NO se debe asignar una dirección IP a la interfaz física.

Subinterfaz punto a punto

```
Router(config-if)#interface serial 0/0/0.20 point-to-point
Router(config-subif)#ip address 172.16.20.1 255.255.255.252
Router(config-subif)#frame-relay interface-dlci 20
```

Subinterfaz punto a multipunto

```
Router(config-if)#interface serial 0/0/0.21 multipoint
Router(config-subif)#ip address 172.16.21.1 255.255.255.0
Router(config-subif)#frame-relay interface-dlci 212
Router(config-subif)#frame-relay interface-dlci 213
Router(config-subif)#no frame-relay inverse-arp
Router(config-subif)#frame-relay map ip 172.16.21.2 212 ietf
Router(config-subif)#frame-relay map ip 172.16.21.3 213 ietf
```

Monitoreo de Frame Relay

```
Router#show interfaces serial 0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is PQUICC Serial
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation FRAME-RELAY IETF, crc 16, keepalive set (10 sec)
  Scramble enabled
  LMI enq sent 22, LMI stat recvd 23, LMI upd recvd 0, DTE LMI up
  LMI enq recvd 0, LMI stat sent 0, LMI upd sent 0
  LMI DLCI 1023 LMI type is CISCO frame relay DTE
  FR SVC disabled, LAPF state down
[continúa]
```

```
Router#show interfaces serial 0/0/0.20
Serial0/0/0.20 is up, line protocol is up
  Hardware is PQUICC Serial
  Internet address is 172.16.20.1/30
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
```


reliability 255/255, txload 1/255, rxload 300/255
Encapsulation FRAME-RELAY IETF

Router#**show frame-relay lmi**

LMI Statistics for int Se0/0/0 (Frame Relay DTE) LMI TYPE = CISCO
Invalid Unnumbered info 0 Invalid Prot Disc 0
Invalid dummy Call Ref 0 Invalid Msg Type 0
Invalid Status Message 0 Invalid Lock Shift 0
Invalid Information ID 0 Invalid Report IE Len 0
Invalid Report Request 0 Invalid Keep IE Len 0
Num Status Enq. Sent 66 Num Status msgs Rcvd 67
Num Update Status Rcvd 0 Num Status Timeouts 0

Router#**show frame-relay pvc [dlci]**

PVC Statistics for interface Serial0/0/0 (Frame Relay DTE)

DLCI=20, DLCI USAGE=LOCAL, PVC STATUS=INACTIVE, INT.=Serial0/0/0.20

input pkts 0	output pkts 2	in bytes 0
out bytes 128	dropped pkts 0	in FECN pkts 0
in BECN pkts 0	out FECN pkts 0	out BECN pkts 0
in DE pkts 0	out DE pkts 0	
out bcast pkts 2	out bcast bytes 128	

pvc create time 00:13:01, last time pvc status changed 00:12:39

DLCI=212, DLCI USAGE=LOCAL, PVC STATUS=ACTIVE, INT.=Serial0/0/0.21

input pkts 195	output pkts 182	in bytes 20075
out bytes 14718	dropped pkts 0	in FECN pkts 0
in BECN pkts 0	out FECN pkts 0	out BECN pkts 0
in DE pkts 0	out DE pkts 0	
out bcast pkts 178	out bcast bytes 14428	

pvc create time 00:14:21, last time pvc status changed 00:14:09

Router#**show frame-relay map**

Serial 0/0/1 (administratively down): ip 131.108.177.177
dlci 177 (0xB1,0x2C10), static, broadcast, CISCO
TCP/IP Header Compression (inherited), passive (inherited)

Router#**clear frame-relay-inarp**

Router#**debug frame-relay lmi**

Frame Relay LMI debugging is on
Displaying all Frame Relay LMI data

Router#

1d18h: Serial0/0/0(out): StEnq, myseq 138, yourseen 135, DTE up

1d18h: datagramstart = 0x1C16998, datagramsize = 13

1d18h: FR encap = 0xFCF10309


1d18h: 00 75 01 01 01 03 02 8A 87

1d18h:

1d18h: Serial0/0/0(in): Status, myseq 138

1d18h: RT IE 1, length 1, type 1

1d18h: KA IE 3, length 2, yourseq 136, myseq 138

 Para profundizar o tener mayor información sobre cualquiera de estos puntos, sugiero consultar mi libro “Guía de Preparación para el Examen de Certificación CCNA”.

Anexo 1: Guía de Comandos

En este anexo se recogen, ordenados por área específica, los diferentes comandos del Cisco IOS que se utilizan en el ámbito de un CCNA R&S.



¡Atención! Este no es un modelo de configuración, ni una secuencia de configuración ordenada completa. Es solamente una colección de comandos para facilitar su revisión. En algunos casos he mantenido cierto orden en la secuencia, pero en muchos casos se reúnen comandos que difícilmente se ejecuten juntos en un caso real.

Comandos de configuración

Ingreso al modo configuración

```
Router>enable
Router#configure terminal
Router(config)#_
```

Clave de acceso a modo usuario

```
Router(config)#line console 0
Router(config-line)#login
Router(config-line)#password cisco
Router(config-line)#exec-timeout 5 0
Router(config-line)#logging synchronous
Router(config-line)#exit
Router(config)#line aux 0
Router(config-line)#login
Router(config-line)#password cisco
Router(config-line)#exec-timeout 5 0
Router(config-line)#exit
Router(config)#line vty 0 4
Router(config-line)#login
Router(config-line)#password cisco
Router(config-line)#exec-timeout 5 0
Router(config-line)#transport input ssh
Router(config-line)#exit
Router(config)#_
```

Clave de acceso a modo privilegiado

```
Router#configure terminal
Router(config)#enable secret cisco
Router(config)#_
```

Configuración de parámetros básicos

```
Router(config)#hostname Router
Router(config)#ip name-server 192.5.5.18
Router(config)#ip domain-lookup
Router(config)#banner motd #mensaje de ingreso#
Router(config)#service password-encryption
Router(config)#username cisco password 0 cisco
Router(config)#ip domain-name muydomain.com
Router(config)#crypto key generate rsa
Router(config)#ip ssh version 2
Router(config)#service timestamps debug datetime localtime
Router(config)#config-register 0x2142
Router(config)#boot network tftp://172.16.14.12/2600.txt
Router(config)#boot system tftp://172.16.14.12/2600-d-mz.t10
Router(config)#_
```

Configuración de una interfaz LAN Ethernet

```
Router(config)#interface GigabitEthernet 0/0
Router(config-if)#ip address 192.5.5.1 255.255.255.0
Router(config-if)#description Gateway de la LAN de ingenieria
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#_
```

Configuración de interfaz WAN HDLC

```
Router(config)#interface serial 0/0/0
Router(config-if)#encapsulation hdlc
Router(config-if)#ip address 201.100.11.1 255.255.255.0
Router(config-if)#description Puerto de conexion con sucursales
Router(config-if)#bandwidth 128
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#_
```

Configuración de interfaz WAN PPP

```
Router(config)#interface serial 0/0/0
Router(config-if)#encapsulation ppp
Router(config-if)#ip address 201.100.11.1 255.255.255.0
Router(config-if)#description Puerto de conexion con Sucursales
Router(config-if)#bandwidth 128
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#_
```

Configuración de interfaz WAN PPP con autenticación CHAP

```
Router(config)#username Remoto password cisco
Router(config)#interface serial 0/0/0
Router(config-if)#encapsulation ppp
Router(config-if)#ppp authentication chap
Router(config-if)#exit
Router(config)#_
```

```
Remoto#configure terminal
Remoto(config)#username Router password cisco
Remoto(config)#interface serial 0/0/0
Remoto(config-if)#encapsulation ppp
```

Configuración de una interfaz lógica

```
Router(config)#interface loopback 0
Router(config-if)#description Interfaz de administracion
Router(config-if)#ip address 10.0.0.1 255.255.255.255
Router(config-if)#exit
Router(config)#_
```

Configuración de direccionamiento IPv6

```
Router#configure terminal
Router(config)#ipv6 unicast-routing
Router(config)#ipv6 router rip RTE
Router(config)#interface gigabitethernet 0/0
Router(config-if)#ipv6 address 2001:ab1:32F4:1::1/64
Router(config-if)#ipv6 address 2001:ab1:32F4:1::/64 eui-64
Router(config-if)#ipv6 rip RTE enable
```

```
Router#show ipv6 interface gigabitethernet 0/0
Router#show ipv6 rip
Router#show ipv6 route
```

Configuración de enrutamiento estático

```
Router(config)#ip route 196.17.15.0 255.255.255.0 201.100.11.2
Router(config)#ip route 207.7.68.0 255.255.255.0 serial 0/0/0 130
Router(config)#ip route 0.0.0.0 0.0.0.0 serial 0/0/1
Router(config)#ip default-network 200.15.17.0
```

```
Router(config)#ipv6 unicast-routing
Router(config)#ipv6 route 2001:0:0:1::/64 2001:0:0:a::2
Router(config)#ipv6 route ::/0 Serial 0/0/0
```

Configuración de enrutamiento EIGRP

```
Router(config)#router eigrp 100
Router(config-router)#network 172.16.0.0
Router(config-router)#passive-interface serial 0/0/0
```

```

Router(config-router)#no auto-summary
Router(config-router)#variance 2
Router(config-router)#exit
Router(config)#key-chain ccna
Router(config-keychain)#key 1
Router(config-keychain-key)#key-string cisco 123
Router(config)#interface serial 0/0/0
Router(config-if)#bandwidth 64
Router(config-if)#ip authentication mode eigrp 100 md5
Router(config-if)#ip authentication key-chain eigrp 100 ccna

Router(config)#ipv6 unicast routing
Router(config)#ipv6 router eigrp 1
Router(config-router)#interface GigabitEthernet 0/0
Router(config-if)#ipv6 enable
Router(config-if)#ipv6 address FC00:1:1:1::/64 eui-64
Router(config-if)#ipv6 eigrp 1
Router(config-if)#ipv6 authentication mode eigrp 1 md5
Router(config-if)#ipv6 authentication key-chain eigrp 1 LAB

```

Configuración de enrutamiento OSPF

```

Router(config)#router ospf 1
Router(config-router)#network 172.6.0.0 0.0.255.255 area 0
Router(config-router)#area 0 authentication message-digest
Router(config-router)#exit
Router(config)#interface serial 0/0/0
Router(config-if)#bandwidth 64
Router(config-if)#ip ospf authentication-key ccna
Router(config-if)#ip ospf cost 10
Router(config-if)#ip ospf priority 1

Router(config)#ipv6 unicast-routing
Router(config)#ipv6 router ospf 1
Router(config-router)#router-id X.X.X.X
Router(config-router)#exit
Router(config)#interface serial 0/0/0
Router(config-if)#bandwidth 64
Router(config-if)#ipv6 enable
Router(config-if)#ipv6 address FC00:1:1:2::/64 eui-64
Router(config-if)#ipv6 ospf 1 area 0

```

Configuración de FHRP

```

RouterA(config)#interface GigabitEthernet 0/0
RouterA(config-if)#ip address 10.1.1.2 255.255.255.0
RouterA(config-if)#standby 100 ip 10.1.1.1
RouterA(config-if)#standby 100 priority 110
RouterB(config)#interface GigabitEthernet 0/0
RouterB(config-if)#ip address 10.1.1.3 255.255.255.0
RouterB(config-if)#standby 100 ip 10.1.1.1

RouterA(config)#interface GigabitEthernet 0/0
RouterA(config-if)#ip address 10.1.1.2 255.255.255.0

```

```
RouterA(config-if)#glbp 100 ip 10.1.1.1
RouterA(config-if)#glbp 100 priority 110
RouterB(config)#interface GigabitEthernet 0/0
RouterB(config-if)#ip address 10.1.1.3 255.255.255.0
RouterB(config-if)#glbp 100 ip 10.1.1.1
```

Configuración del servicio DHCP

```
Router(config)#service dhcp
Router(config)#ip dhcp excluded-address 172.16.1.1 172.16.1.3
Router(config)#ip dhcp pool ccna
Router(dhcp-config)#network 172.16.1.0 255.255.255.0
Router(dhcp-config)#dns-server 172.16.1.3
Router(dhcp-config)#netbios-name-server 172.16.1.3
Router(dhcp-config)#default-router 172.16.1.1
Router(dhcp-config)#domain-name ccna_lab
Router(dhcp-config)#lease 1 8 0
Router(dhcp-config)#exit
Router(config)#_
```

```
Router#configure terminal
Router(config)#interface GigabitEthernet 0/0
Router(config-if)#ip helper-address 172.16.108.19
```

Configuración del servicio NAT

```
Router(config)#interface gigabitethernet 0/0
Router(config-if)#ip nat inside
Router(config-if)#interface serial 0/0/0
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#ip nat inside source static 172.16.1.2 200.15.17.12
Router(config)#ip nat pool ccna 200.15.17.13 200.15.17.20 netmask
255.255.255.0
Router(config)#access-list 1 permit 172.16.1.8 0.0.0.7
Router(config)#ip nat inside source list 1 pool ccna
Router(config)#ip nat inside source list 1 interface serial 0/0/0
overload
Router(config)#ip nat translation timeout 120
Router(config)#exit
Router#clear ip nat translation *
Router#_
```

Configuración de CDP

```
Router(config)#cdp timer 100
Router(config)#cdp holdtime 200
Router(config)#cdp run
Router(config)#interface gigabitethernet 0/0
Router(config-if)#cdp enable
Router(config-if)#^Z
Router#clear cdp counters
Router#clear cdp table
```

Configuración de Listas de Acceso

```
Router(config)#access-list 1 permit host 221.17.15.2
Router(config)#interface serial 0/0/1
Router(config-if)#ip access-group 1 in
Router(config-if)#exit
Router(config)#

Router(config)#access-list 102 deny tcp any host 172.16.1.3 ftp
Router(config)#interface serial 0/0/1
Router(config-if)#ip access-group 102 in
Router(config-if)#exit
Router(config)#

Router(config)#ip access-list standard ccna
Router(config-std-nacl)#permit host 221.17.15.2
Router(config-std-nacl)#exit
Router(config)#interface serial 0/0/1
Router(config-if)#ip access-group ccna in
Router(config-if)#exit
Router(config)#
```

Configuración de filtros de acceso a terminales virtuales

```
Router(config)#access-list 10 permit host 172.16.10.3
Router(config)#line vty 0 4
Router(config-line)#access-class 10 in
Router(config-line)#exit
Router(config)#_
```

Configuración del servicio de Syslog

```
Router(config)#service timestamps
Router(config)#service sequence-numbers
Router(config)#logging on
Router(config)#logging buffered 200000
Router(config)#logging 172.16.1.2
Router(config)#logging trap warnings
Router(config)#logging monitor notifications
Router(config)#logging console
```

Configuración de SNMP v2c

```
Router(config)# ip access-list standard SNMP
Router(config-std-nacl)# permit host 172.16.10.101
Router(config-std-nacl)# exit
Router(config)# ip access-list standard SNMP2
Router(config-std-nacl)# permit host 172.16.20.54
Router(config-std-nacl)# exit
Router(config)# snmp-server community LabCisco RO SNMP
Router(config)# snmp-server location BuenosAires
Router(config)# snmp-server contact Oscar Gerometta
Router(config)# snmp-server community LabCisco2 RW SNMP2
```


Configuración de NetFlow

```
Router(config)#interface GigabitEthernet0/0
Router(config-if)#ip flow ingress
Router(config-if)#ip flow egress
Router(config-if)#exit
Router(config)#ip flow-export destination 10.1.10.100 99
Router(config)#ip flow-export version 9
Router(config)#ip flow-export source loopback 0
```

Configuración de servicios Frame Relay

```
Router(config)#interface serial 0/0/0
Router(config-if)#encapsulation frame-relay
Router(config-if)#frame-relay lmi-type cisco
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#exit

Router(config)#interface serial 0/0/0
Router(config-if)#encapsulation frame-relay
Router(config-if)#no shutdown
Router(config-if)#interface serial 0/0/0.21 point-to-point
Router(config-subif)#ip address 172.16.21.1 255.255.255.252
Router(config-subif)#frame-relay interface-dlci 21
Router(config-subif)#exit
Router(config)#exit

Router(config)#interface serial 0/0/0
Router(config-if)#encapsulation frame-relay
Router(config-if)#no shutdown
Router(config-if)#interface serial 0/0/0.20 multipoint
Router(config-subif)#ip address 172.16.20.1 255.255.255.0
Router(config-subif)#frame-relay interface-dlci 20
Router(config-subif)#no frame-relay inverse-arp
Router(config-subif)#frame-relay map ip 172.16.20.2 20 ietf
Router(config-subif)#exit
Router(config)#exit
```

Configuración de parámetros IP en un switch Catalyst 2960

```
Switch(config)#interface vlan1
Switch(config-if)#ip address 172.16.5.2 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#ip default-gateway 172.16.5.1
Switch(config)#_
```

Configuración de interfaz de un switch Catalyst 2960

```
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#duplex full
Switch(config-if)#speed 100
```

```
Switch(config-if)#spanning-tree portfast
Switch(config-if)#description puerto servidor 2
Switch(config-if)#exit
Switch(config)#_
```

Configuración de EtherChannel

```
Switch(config)#interface range FastEthernet0/1 - 2
Switch(config-if)#channel-group 1 mode on
```

Configuración de STP en un switch Catalyst 2960

```
Switch(config)#spanning-tree mode rapid-pvst
Switch(config)#spanning-tree vlan 2 priority 1
Switch(config)#spanning-tree vlan 2 primary
Switch(config)#spanning-tree vlan 3 secondary
```

Configuración de seguridad por puerto

```
Switch(config)#interface fastethernet 0/9
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#switchport port-security maximum 2
Switch(config-if)#switchport port-security violation shutdown
Switch(config-if)#exit
Switch(config)#_
```

Configuración de VTP en un switch Catalyst 2960

```
Switch#configure terminal
Switch(config)#vtp domain ccna
Switch(config)#vtp mode server
Switch(config)#vtp password cisco
Switch(config)#vtp pruning
Switch(vlan)#exit
Switch#_
```

Configuración de VLANs en un switch Catalyst 2960

```
Switch#configure terminal
Switch(config)#vlan 2
Switch(config-vlan)#name laboratorio
Switch(config-vlan)#exit
Switch(config)#interface fastEthernet 0/4
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 2
Switch(config-if)#exit
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
Switch(config)#_
```

Configuración de una interfaz de router como troncal

```
Router#configure terminal
Router(config)#interface gigabitethernet 0/0
Router(config-if)#no shutdown
Router(config-if)#interface gigabitethernet 0/0.1
Router(config-subif)#encapsulation dot1q 1
Router(config-subif)#ip address 172.18.1.1 255.255.255.0
Router(config-subif)#interface gigabitethernet 0/0.2
Router(config-subif)#encapsulation dot1q 2
Router(config-subif)#ip address 172.18.2.1 255.255.255.0
Router(config-subif)#exit
Router(config)#_
```

Comandos de monitoreo

Visualización de elementos generales del dispositivo

```
Router#show flash
Router#show version
Router#show processes cpu
Router#show processes memory
Router#show tcp brief all
```

Visualización del archivo de configuración

```
Router#show running-config
Router#show startup-config
```

Monitoreo de interfaces

```
Router#show interfaces
Router#show ip interfaces
Router#show ip interfaces brief
Router#show controllers
```

Monitoreo de PPP

```
Router#debug ppp negotiation
Router#debug ppp authentication
Router#debug ppp packet
```

Monitoreo de DHCP

```
Router#show dhcp server
Router#show dhcp lease
```

Monitoreo de NAT

```
Router#show ip nat translation
Router#show ip nat statistics
Router#debug ip nat
```

Monitoreo de NetFlow

```
Router#show ip cache flow
Router#show ip flow interface
Router#show ip flow export
```

Monitoreo del enrutamiento

```
Router#show ip protocols
Router#show ip route
Router#show ipv6 route
```

Monitoreo de enrutamiento EIGRP

```
Router#show ip eigrp neighbors
Router#show ip route eigrp
Router#show ip eigrp topology

Router#show ipv6 router eigrp
Router#show ipv6 eigrp 1 interfaces
Router#show ipv6 eigrp 1 neighbors
Router#show ipv6 eigrp 1 topology
```

Monitoreo de enrutamiento OSPF

```
Router#show ip ospf
Router#show ip ospf database
Router#show ip neighbor detail
Router#show ip ospf interface

Router#show ipv6 protocols
Router#show ipv6 ospf
Router#show ipv6 ospf database
Router#show ipv6 ospf neighbor
Router#show ipv6 ospf interface
```

Monitoreo de FHRP

```
Router#show standby brief
Router#show standby
Router#show glbp brief
Router#show glbp
```

Monitoreo de CDP

```
Router#show cdp
Router#show cdp neighbor
Router#show cdp entry Router
Router#show cdp entry *
Router#show cdp neighbor detail
Router#show cdp traffic
Router#show cdp interface gigabitethernet 0/0
```

Monitoreo de listas de acceso

```
Router#show access-list
Router#show ip access-list
Router#show ip interfaces
Router#show running-config
```

Monitoreo de Frame Relay

```
Router#show frame-relay pvc
Router#show frame-relay lmi
Router#show frame-relay map
Router#debug frame-relay lmi
```

Monitoreo del switch

```
Switch#show mac-address-table
Switch#clear mac-address-table
Switch#show spanning-tree
```

Monitoreo de EtherChannel

```
Switch#show etherchannel summary
Switch#show interfaces port-channel 1
Switch#show interfaces FastEthernet 0/1 etherchannel
```

Monitoreo de VLANs

```
Switch#show vtp status
Switch#show vlan
Switch#show vlan brief
Switch#show vlan id 2
Switch#show interface fastethernet 0/1 switchport
Switch#show interface trunk
```

Acceso a través de terminal virtual

```
Router#telnet 201.100.11.1
Router#connect 201.100.11.1
Router#201.100.11.1
Router#show sessions
Router#show users
Router#Ctrl+shift+6 luego x
Router#resume #
Router#exit
Router#logout
Router#disconnect 201.100.11.1
Router#clear line #
```

Comandos para crear copias de resguardo

```
Router#copy system:running-config tftp:config.txt  
Router#copy running-config startup-config  
Router#copy flash:c2600-is-mz.121-5 tftp:
```

Borrar configuración de un switch Catalyst

```
Switch#delete flash:config.text  
Switch#delete flash:vlan.dat
```

Índice

Contenidos	7
Introducción	9
El Autor	11
1. El Examen de certificación CCNA.....	13
Recertificación.....	13
1.1. Las Características del Examen de Certificación.....	14
Examen 200-120 CCNA – Cisco Certified Network Associate Exam.....	14
Examen 100-101 ICND1 – Interconnecting Cisco Networking Devices Part 1.....	16
Examen 200-101 ICND2 – Interconnecting Cisco Networking Devices Part 2.....	16
El formato de las preguntas	16
1.2. El Procedimiento para Presentar el Examen	17
2. Los Contenidos del examen de certificación	21
2.1. Principios de operación de redes TCP/IP	23
Introducción a los modelos de referencia.....	23
Modelo OSI	23
Modelo TCP/IP	25
Encapsulación / Desencapsulación	26
Capa física del modelo OSI.....	28
Medios de cobre.....	28
Cable de par trenzado de cobre	28
Conectorizado RJ-45	29
Medios de fibra óptica	32
Conectorizado de fibra óptica	33
Medios inalámbricos	34
La Arquitectura Ethernet.....	34
Nomenclatura y estándares	35
Elementos comunes:	37
El protocolo CSMA/CD	37
Encabezado de una trama Ethernet II	39
Direccionamiento de capa 2 y capa 3	40
Definición de destinatarios.....	40
Direcciones MAC	40
Direcciones IPv4	41
Encabezado de un paquete IP.....	42
Composición de una trama	42
La capa de Transporte	42
Conexión confiable o best-effort	43
El protocolo UDP.....	43
El protocolo TCP	44
Interacción con la capa de red y la de aplicación	45
Establecimiento de una sesión TCP	46
Cierre de una sesión TCP.....	47
Control de flujo en TCP.....	47
El sistema de ventana.....	48
2.2. Direccionamiento IP (IPv4 / IPv6)	51
El Protocolo IP (Internet Protocol)	51
Direccionamiento IP versión 4.....	51
Estructura de clases	51
Direcciones IP Privadas.....	53
Direcciones IPv4 reservadas	53

Direcciones IPv4 Privadas	54
Encabezado IPv4	54
Protocolo ARP.....	55
Procedimiento para obtener una dirección IP	55
Protocolo RARP	55
ICMP	55
Direccionamiento IP versión 6	57
Direcciones IPv6	57
Asignación de direcciones IPv6	58
Direcciones IPv6 de link local	59
Direcciones IPv6 globales de unicast	59
Direcciones IPv6 unique local.....	59
Direcciones IPv6 de anycast.....	60
Encabezado IPv6	60
Mecanismos de transición	61
Implementación de subredes en redes IPv4	61
Subred.....	61
Método sencillo para el cálculo de subredes:	62
Variable-Length Subnet Mask (VLSM).....	65
Classless Interdomain Routing (CIDR)	67
Sumarización de rutas	67
Características de los bloque de rutas	69
2.3. Operación de dispositivos Cisco IOS	71
Cisco IOS.....	71
Conexión al dispositivo	71
Terminal de Consola	71
Terminal Remota.....	72
Terminales Virtuales	72
Componentes de Hardware de un dispositivo.....	73
Esquema Básico de la Estructura de hardware del Router	75
Modos	75
Modo Setup o Inicial	76
Modo monitor de ROM.....	76
Cisco IOS	76
La línea de comando (CLI) de Cisco IOS.....	77
Comandos de ayuda.....	77
Comandos de edición	77
Mensajes de error en el ingreso de comandos:.....	78
Comandos show	78
Modo de configuración global	79
Claves de acceso.....	79
Procedimiento de configuración de un Router Cisco	80
Configuración de direccionamiento IPv6	83
Comandos show:	83
Comandos para la visualización de los archivos de configuración	83
Comando para visualización de la memoria flash	86
Comandos para la visualización de las interfaces.....	87
Posibles resultados de la primera línea de show interfaces.....	87
Una presentación sintética del estado de las interfaces	88
Otros comandos show	88
Administración del archivo de configuración	88
El comando copy.....	89
Pruebas de conectividad de la red	89
Prueba de conexiones utilizando el comando ping	89
Prueba para el descubrimiento de rutas	90

Prueba de conectividad completa extremo a extremo.....	91
Comandos de visualización y diagnóstico en DOS	91
Secuencia o rutina de Inicio	91
El Registro de Configuración	93
Modificación del registro de configuración.....	94
Comandos para copia de resguardo de la imagen de Cisco IOS	95
Procedimiento para recuperación de claves	95
CDP Cisco Discovery Protocol.....	96
Comandos CDP	96
Monitoreo de información CDP.....	96
Comandos relacionados con el acceso vía terminal virtual	97
Verificación y visualización de las sesiones telnet	98
Para desplazarse entre diferentes sesiones telnet abiertas	98
2.4. Conmutación LAN	99
Dominios de colisión y dominios de broadcast.....	99
Características básicas de un switch.....	100
Operaciones básicas de un switch	100
Métodos de conmutación.....	101
LEDs indicadores del switch.....	102
Configuración básica del switch Catalyst 2960	103
Control de acceso a la red switchheada	105
Optimización de performance de la red conmutada	106
Determinación de dúplex y velocidad	106
Spanning Tree Protocol.....	107
Redundancia en enlaces de capa 2	107
Spanning Tree Protocol	107
Operación de STP	108
Selección del switch raíz.....	110
Costos y prioridades	110
Estados de los puertos STP	110
Port Fast.....	111
Per VLAN Spanning Tree +	111
Rapid Spanning Tree Protocol.....	112
Multiple Spanning Tree Protocol (MSTP)	112
Operación de STP por defecto	113
Configuración de Spanning Tree	113
Administración del archivo de configuración y la imagen del IOS	114
Borrar la configuración.....	114
La configuración completa de un switch Catalyst 2960.....	114
EtherChannel.....	116
Configuración de EtherChannel.....	117
Segmentación de la red implementando VLANs.....	118
Beneficios de la implementación de VLANs	118
Modos de membresía VLAN.....	118
Tipos de puertos o enlaces.....	118
Tips	119
¿Qué es un Enlace Troncal?	119
IEEE 802.1Q	120
VLAN Trunk Protocol (VTP).....	120
Modos VTP	121
Configuración de VLANs y enlaces troncales	121
Configuración de un "router on stick"	123
2.5. Enrutamiento IP.....	125
Principios del enrutamiento IP.....	125
La tabla de enrutamiento	126

Generación de la tabla de enrutamiento.....	126
La métrica	127
La Distancia Administrativa.....	128
Protocolos de enrutamiento	128
Comparación entre enrutamiento vector distancia y estado de enlace	129
Enrutamiento estático.....	130
Configuración de una ruta estática	130
Rutas por Defecto	130
Configuración de una ruta por defecto	131
Enrutamiento Dinámico	131
Protocolos de enrutamiento por vector distancia.....	131
Comparación entre Enrutamiento Vector Distancia y Estado de Enlace	133
Enhanced Interior Gateway Routing Protocol (EIGRP)	133
Configuración de EIGRP en redes IPv4	135
Configuración de EIGRP en redes IPv6	136
Configuración de autenticación en EIGRP	137
Open Shortest Path First (OSPF).....	137
Configuración de OSPFv2	139
Monitoreo de OSPFv2	140
Configuración de OSPFv3	140
Monitoreo de OSPFv3	140
Comandos de verificación	140
El comando show ip route.....	140
Variantes del comando	141
Otro comando: show ip protocols	141
Redundancia en el primer salto (FHRP)	142
Hot Standby Router Protocol (HSRP).....	142
Configuración de HSRP	144
Gateway Load Balancing Protocol (GLBP).....	145
Configuración de GLBP	145
2.6. Servicios IP	147
Asignación automática de direcciones IP.....	147
Dynamic Host Configuration Protocol – DHCPv4.....	147
Configuración de servicios DHCP en IOS	149
DHCP Relay.....	150
Configuración de un router como DHCP relay	151
Internet Control Message Protocol (ICMP)	151
Domain Name System - DNS.....	153
Configuración del servicio de nombres en Cisco IOS	154
Listas de Control de Acceso.....	155
Reglas de funcionamiento de las ACL.....	155
Tipos de listas de acceso IP	156
El ID de las listas de acceso numeradas	156
La máscara de wildcard	156
Algunas reglas prácticas de cálculo.....	157
Casos especiales	158
Configuración de las listas de acceso	158
Network Address Translation (NAT).....	161
Terminología NAT	161
Configuración de NAT:.....	163
Seguridad de la red	164
Requerimientos de seguridad básicos.....	164
Cisco Network Foundation Protection	165
Seguridad de dispositivos Cisco IOS	165

Configuración de claves de acceso	166
Implementación de SSH	168
Administración de múltiples sesiones de terminal virtual	169
Implementación de un registro de eventos	170
Simple Network Management Protocol (SNMP)	172
Configuración de SNMP v2c	173
NetFlow	174
Configuración de NetFlow	175
2.7. Tecnologías WAN	177
Terminología WAN	177
Tipos de conexión WAN	177
Redes WAN privadas	177
Redes WAN públicas y acceso a Internet	178
Interfaces WAN de los routers Cisco	179
Protocolos WAN de capa de enlace de datos	180
Líneas dedicadas	180
Bases de una conexión serial	180
Encapsulación HDLC	181
Configuración de HDLC	181
Encapsulación PPP	181
Configuración de PPP	182
Autenticación de PPP	183
Configuración de autenticación con CHAP	183
Frame Relay	184
Terminología Frame Relay	184
Circuitos virtuales	185
DLCI	186
Interfaz de Gestión Local (LMI)	187
Ejemplo de configuración de una interfaz Frame Relay	189
Creación de subinterfaces sobre enlaces seriales	189
Redes Frame Relay Hub and Spoke	191
Configuración de Frame Relay	192
Anexo 1: Guía de Comandos	195
Comandos de configuración	195
Ingreso al modo configuración	195
Clave de acceso a modo usuario	195
Clave de acceso a modo privilegiado	195
Configuración de parámetros básicos	196
Configuración de una interfaz LAN Ethernet	196
Configuración de interfaz WAN HDLC	196
Configuración de interfaz WAN PPP	196
Configuración de interfaz WAN PPP con autenticación CHAP	197
Configuración de una interfaz lógica	197
Configuración de direccionamiento IPv6	197
Configuración de enrutamiento estático	197
Configuración de enrutamiento EIGRP	197
Configuración de enrutamiento OSPF	198
Configuración de FHRP	198
Configuración del servicio DHCP	199
Configuración del servicio NAT	199
Configuración de CDP	199
Configuración de Listas de Acceso	200
Configuración de filtros de acceso a terminales virtuales	200
Configuración del servicio de Syslog	200
Configuración de SNMP v2c	200

Configuración de NetFlow	201
Configuración de servicios Frame Relay	201
Configuración de parámetros IP en un switch Catalyst 2960	201
Configuración de interfaz de un switch Catalyst 2960	201
Configuración de EtherChannel	202
Configuración de STP en un switch Catalyst 2960	202
Configuración de seguridad por puerto	202
Configuración de VTP en un switch Catalyst 2960	202
Configuración de VLANs en un switch Catalyst 2960	202
Configuración de una interfaz de router como troncal	203
Comandos de monitoreo	203
Visualización de elementos generales del dispositivo	203
Visualización del archivo de configuración	203
Monitoreo de interfaces	203
Monitoreo de PPP	203
Monitoreo de DHCP	203
Monitoreo de NAT	203
Monitoreo de NetFlow	204
Monitoreo del enrutamiento	204
Monitoreo de enrutamiento EIGRP	204
Monitoreo de enrutamiento OSPF	204
Monitoreo de FHRP	204
Monitoreo de CDP	204
Monitoreo de listas de acceso	205
Monitoreo de Frame Relay	205
Monitoreo del switch	205
Monitoreo de EtherChannel	205
Monitoreo de VLANs	205
Acceso a través de terminal virtual	205
Comandos para crear copias de resguardo	206
Borrar configuración de un switch Catalyst	206
Índice	207

