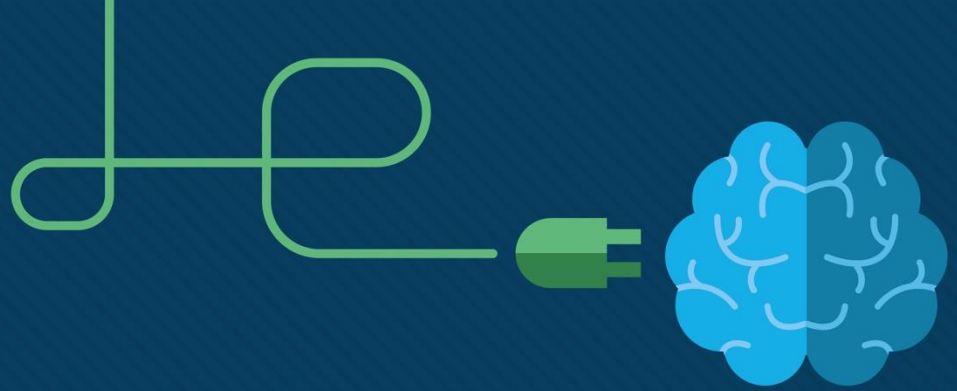


1: Las redes en la actualidad

Introducción a Redes

Objetivos

Objetivo: Presentar los Avances en las tecnologías relacionadas con redes de computadoras

Tema	Objetivo
Las redes impactan nuestra vida	Identificar como las redes afectan nuestra vida diaria
Componentes de una red	Conocer la función de host y los dispositivos de red
Representaciones y topologías de red	Identificar las representaciones de red y cómo se utilizan en las topologías de red.
Tipos comunes de redes	Compare las características de los tipos más comunes de redes.
Conexiones de Internet	Conceptos básicos de LAN y WAN
Redes confiables	Identificar los 4 requisito de una red confiable
Tendencias de redes	Conocer las tendencias BYOD, colaboración en línea, video y computo en la nube y como están cambiando la forma en que interactuamos.
Seguridad en redes	Identifique algunas amenazas de seguridad básicas y soluciones para ellas.
El profesional de TI	Explicar las oportunidades de empleo en el campo de redes.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

1.1 Las redes afectan nuestras vidas

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Las Redes nos conectan

La comunicación es muy importante para nosotros, en la actualidad es fundamental para muchas actividades. En el mundo actual, mediante el uso de redes, estamos conectados como nunca antes.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Video – The Cisco Networking Academy Learning Experience

Cisco Networking Academy: learn how we use technology to make the world a better place.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

No Boundaries

- Mundo sin fronteras
- Comunidades globales
- Red humana

© 2016 Cisco and/or its affiliates. All rights reserved.

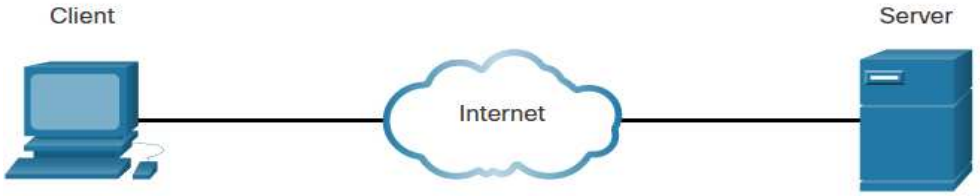
1.2 Componentes de una red

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Host Roles

Cada computadora en una red es un host o dispositivo final.

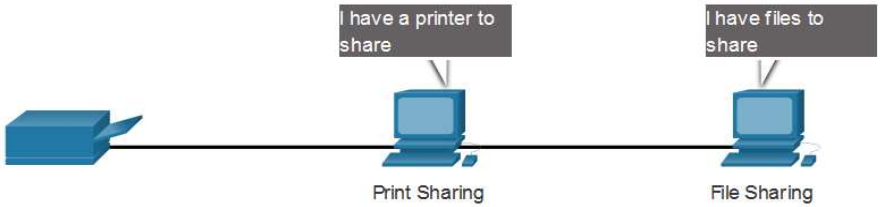
- Los servidores son computadoras que brindan información a los dispositivos finales:
  - servidores de correo
  - servidores web
  - servidor de archivos
- Los clientes son computadoras que envían solicitudes a los servidores para obtener información:
  - página web desde un servidor web
  - correo electrónico de un servidor de correo electrónico



Tipo	Descripción
Email	Servidor: ejecuta un servicio de correo electrónico. Los clientes utilizan el software para acceder al correo electrónico.
Web	El servidor web ejecuta el software del servidor web. Los clientes utilizan software de navegador para acceder a las páginas web.
Archivos	El servidor almacena archivos corporativos y de usuario. Los dispositivos cliente acceden a estos archivos.

Peer-to-Peer

Es posible que un dispositivo sea un cliente y un servidor en una red Peer-to-Peer. Este tipo de diseño de red solo se recomienda para redes muy pequeñas.

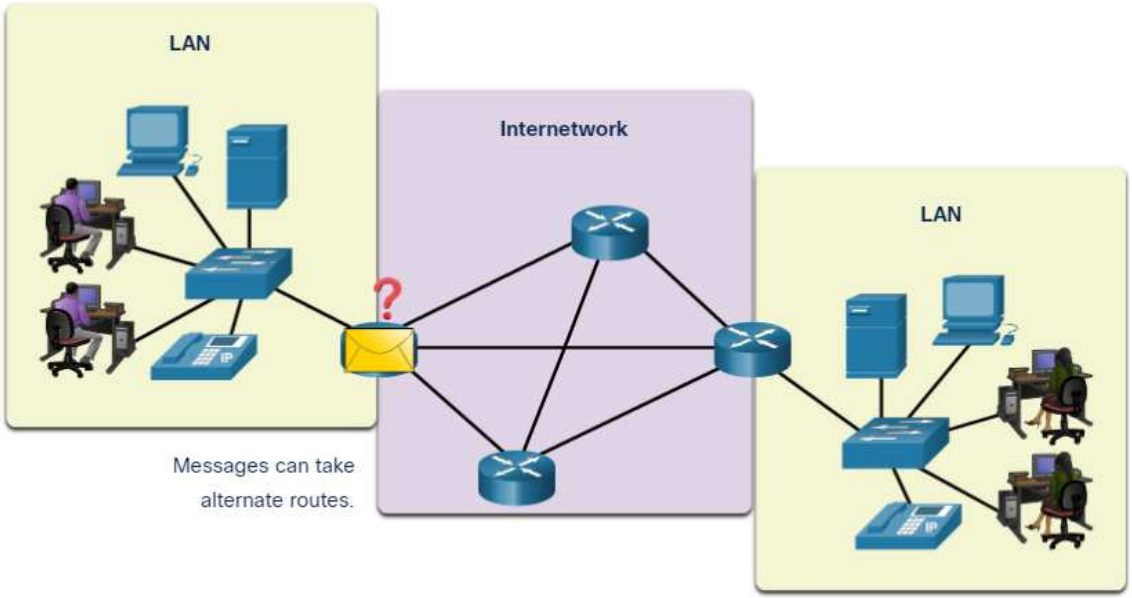


Advantages	Disadvantages
Facil de configurar	No hay administración centralizada
Menos compleja	Menos segura
Bajo coste	No es escalable
Se utiliza para tareas sencillas: transferir archivos y compartir impresoras	Bajo rendimiento

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

End Devices

Un dispositivo final es de donde se origina un mensaje o donde se recibe. Los datos que se originan en un dispositivo final, fluyen a través de la red y llegan a un dispositivo final.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Intermediary Network Devices

Un dispositivo intermedio interconecta los dispositivos finales. Los ejemplos incluyen conmutadores (switchs), puntos de acceso inalámbricos (wiereless access point), enrutadores (routers) y cortafuegos (firewall).

Gestionar los datos a medida que fluyen a través de una red también es función de un dispositivo intermedio, que incluye:

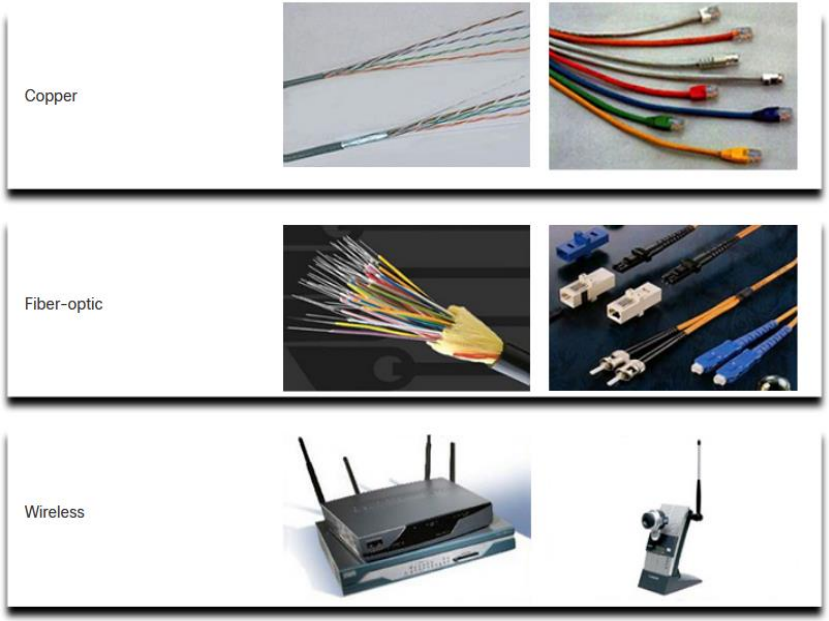
- Regenerar y retransmitir señales de datos.
- Mantener información sobre las rutas existentes en la red.
- Notificar a otros dispositivos sobre errores y fallas de comunicación.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Network Media

La comunicación a lo largo de una red se realiza a través de un medio que permite que un mensaje viaje desde el origen al destino.

Tipos de Medios	Descripción
Cables de alámbres de metal	Utilizan impulsos elécrtricos
Cables de fibras de plástico o vidrio (fiber-optic cable)	Usa pulsos de luz
Transmisión Inalambrica	Utiliza la modulación de frecuencias específicas de ondas electromagnéticas.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

1.3 Representaciones y topologías de red

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

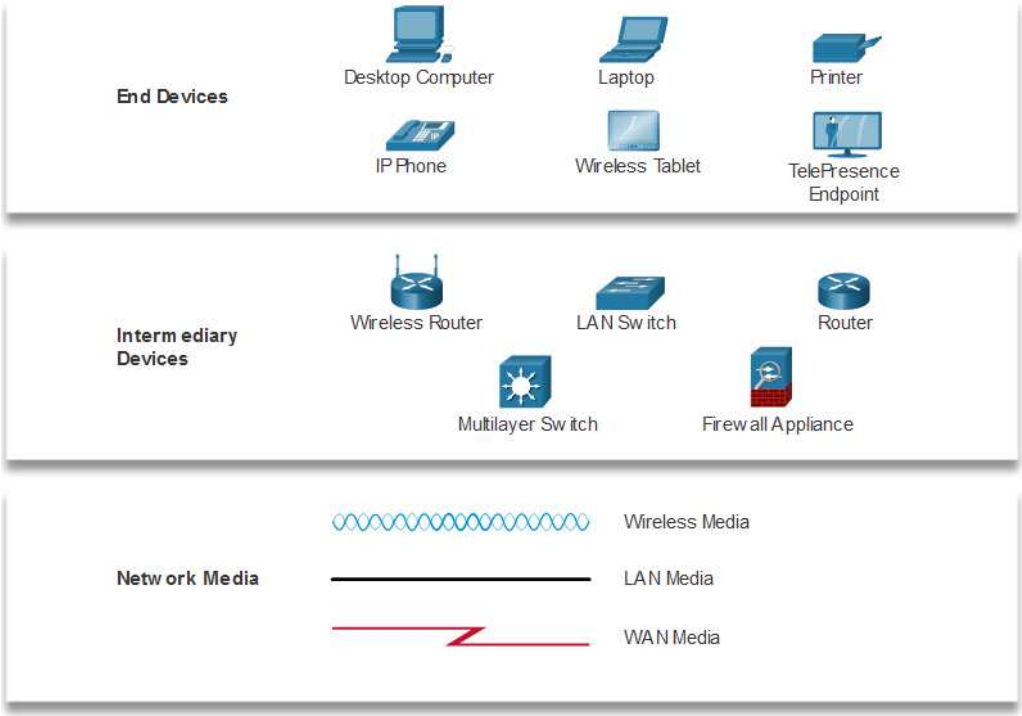
Network Representations

Los diagramas de red, a menudo llamados topologías se red, usan símbolos para representar los dispositivos dentro de la red.

Términos importantes

- Network Interface Card (NIC)
- Puerto físico
- Interface

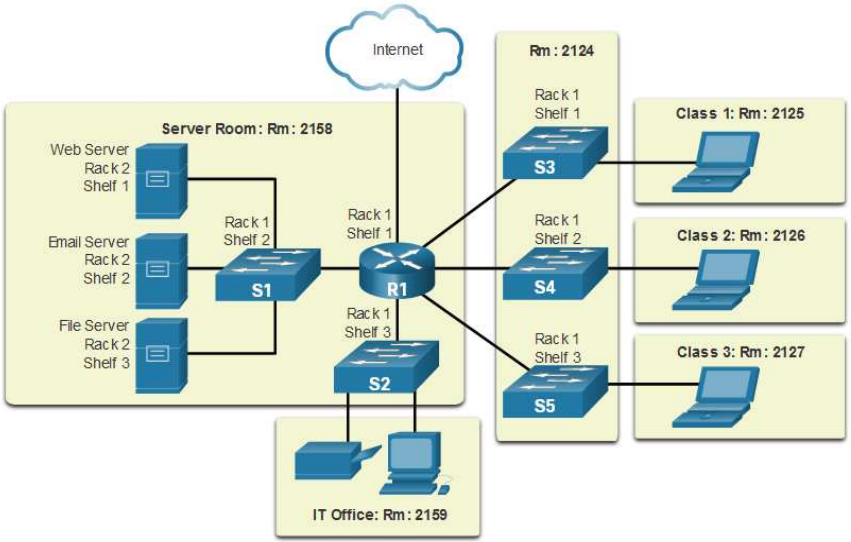
Nota: a menudo, los términos puerto e interfaz se intercambian indistintamente



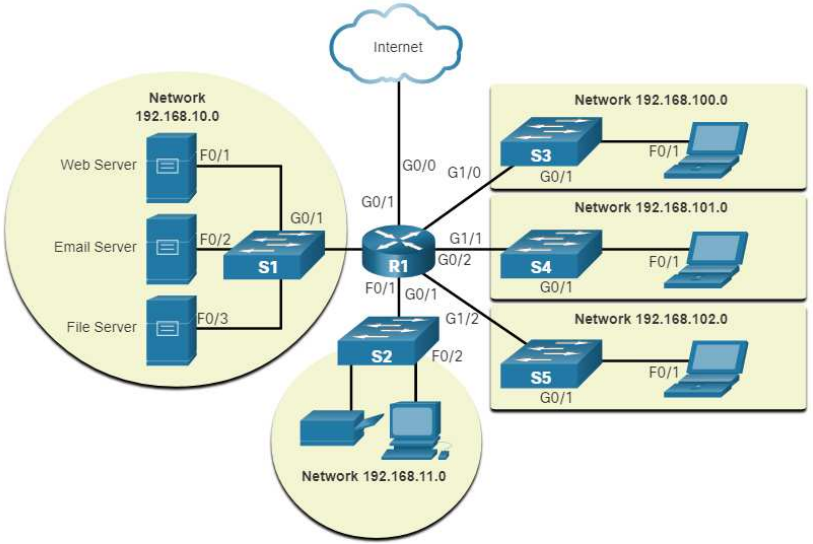
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Topology Diagrams

Los diagramas de topología física ilustran la ubicación física de los dispositivos intermediarios y la instalación de cables.



Los diagramas de topología lógica ilustran los dispositivos, los puertos y el esquema de direccionamiento de la red.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

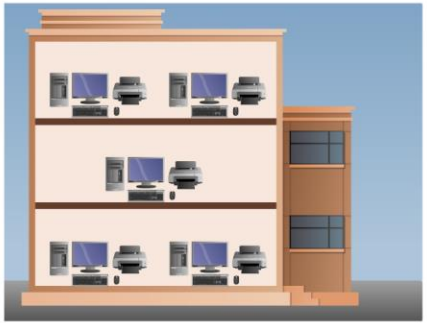
1.4 Tipos comunes de redes

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Networks of Many Sizes

Small Home

SOHO



Medium/Large

World Wide

- Redes domésticas pequeñas: conecte algunas computadoras entre sí y a Internet
- Small Office/Home Office – permite que la computadora dentro de una oficina doméstica o remota se conecte a una red corporativa
- Redes medianas a grandes: muchas ubicaciones con cientos o miles de computadoras interconectadas
- World Wide Networks: conecta cientos de millones de computadoras en todo el mundo, como Internet.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

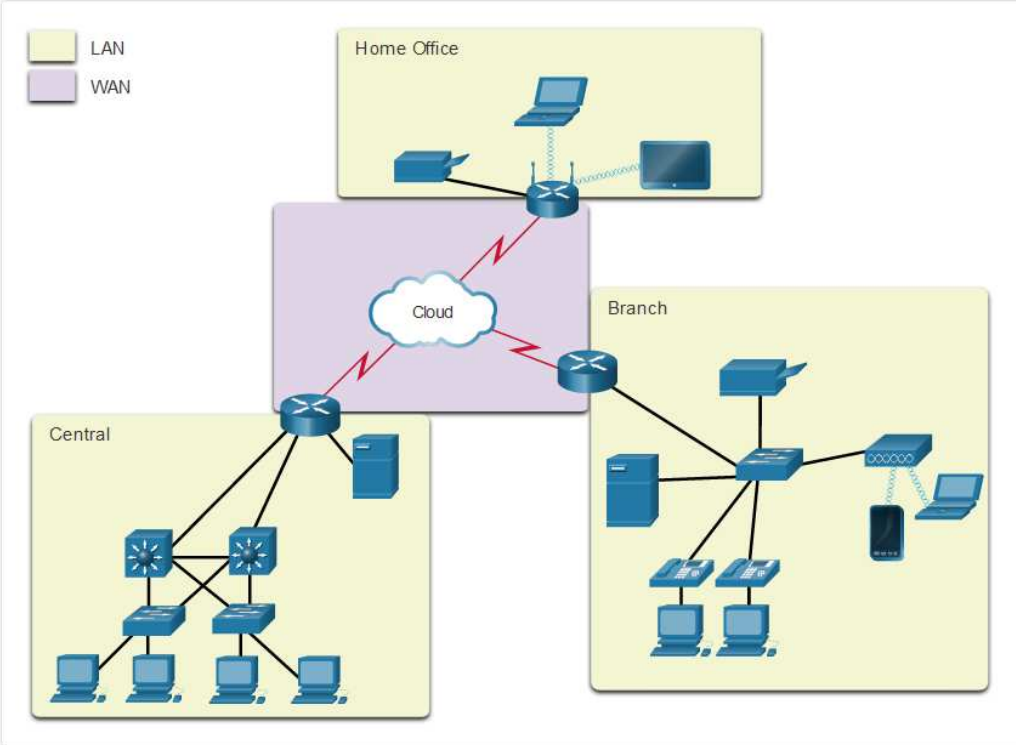
LANs and WANs

Las infraestructuras de red varían mucho en términos de:

- El tamaño del área cubierta
- Número de usuarios
- Número y tipo de servicios disponibles
- Área de responsabilidad

Los dos tipos de redes más comunes:

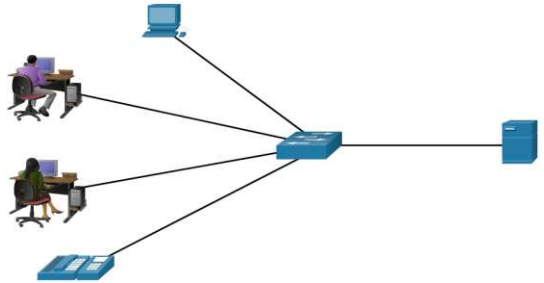
- Local Area Network (LAN)
- Wide Area Network (WAN).



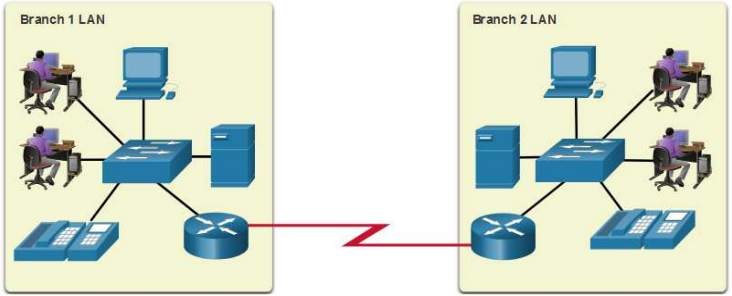
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

LANs and WANs (cont.)

Una LAN es una infraestructura de red que abarca un área geográfica pequeña.



Una WAN es una infraestructura de abarca una amplia área geográfica



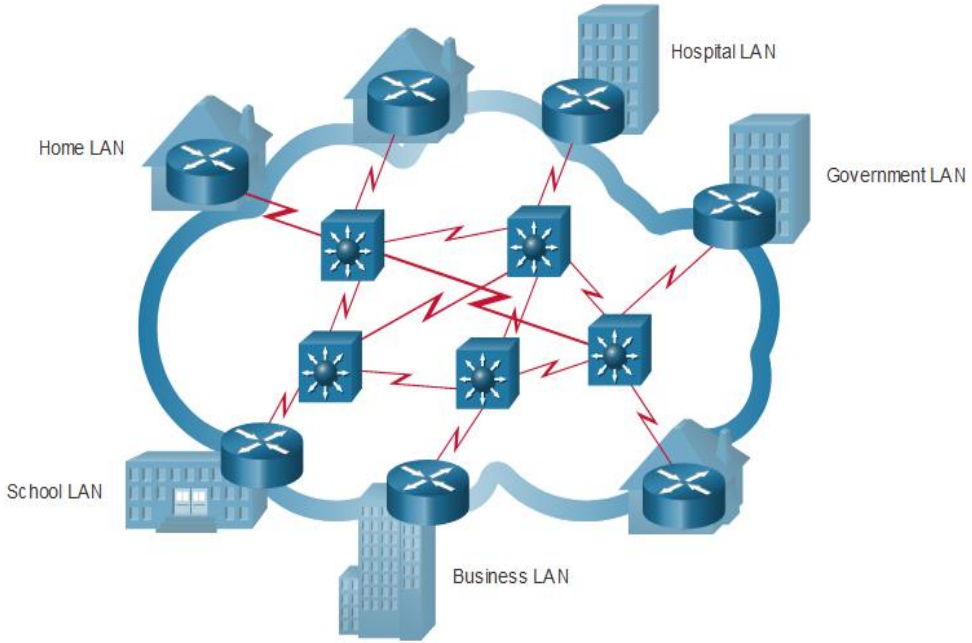
LAN	WAN
Interconecta los dispositivos en una área limitada.	Interconecta LANs en amplias áreas geográficas
Administrado po una solo organización o individuo	Tipicamente administrada por uno más proveoderes de servicios
Proporciona ancho de banda de al velocidad.	Normalmente proporcionan enlaces de menor velocidad entre las LAN.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

The Internet

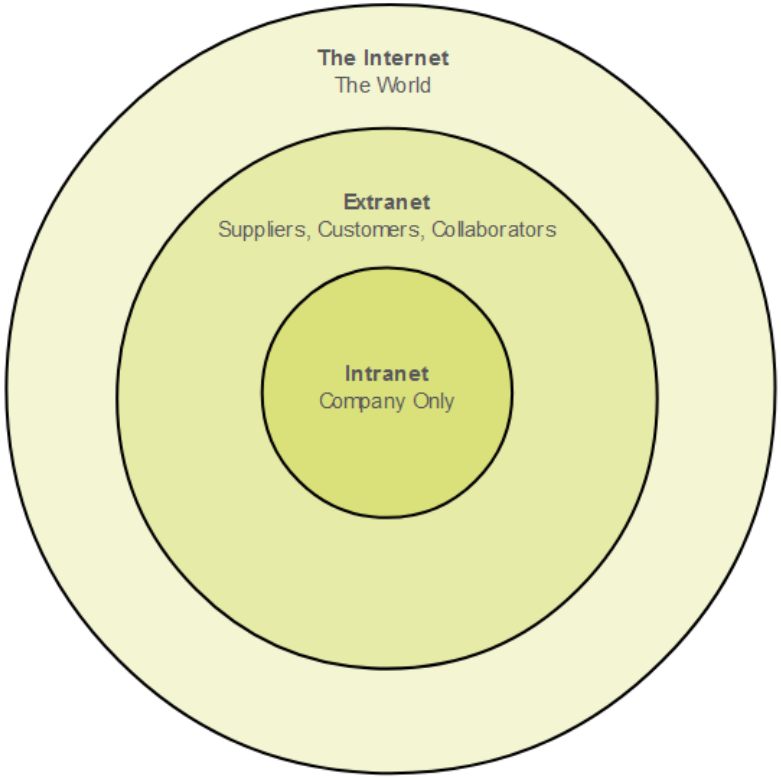
El internet es un conjunto mundial de in LANs y WANs interconectadas.

- LANs se conectan entres ellas mediante WANs.
- Las WANs transmintes mediante cables de cobre, fibra óptica y medios inálambricos,
- El internet no es propiedad de ningun grupo o individuo. Los siguientes grupos se desarrollaron para ayudar a mantener la estructura en Internet:
  - IETF
  - ICANN
  - IAB



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Intranets and Extranets



Una intranet es red privada de LAN y WAN internas a una organización que está destinada solo para los miembros de la organización u otras personas con autorización puedan acceder.

Una organización puede utilizar una extranet para proporcionar acceso seguro a su red para las personas que laboran en una organización diferente pero que necesitan acceder a su intranet.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

1.5 Conexiones de internet

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

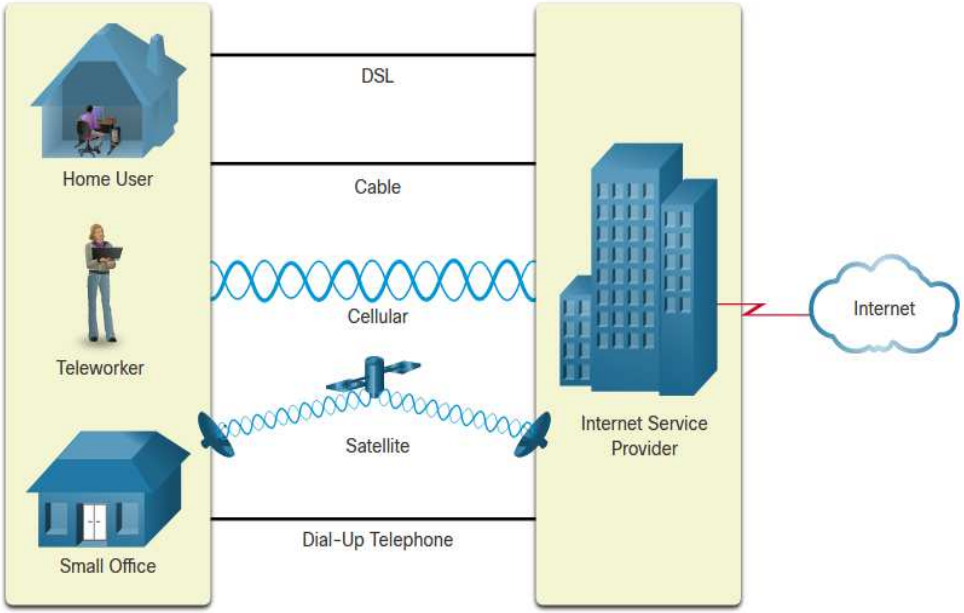
Tecnologías de Acceso a Internet

Existen muchas formas de conectar usuarios/organizaciones a internet

- Los servicios más populares para usuarios domésticos y oficinas pequeñas incluyen banda ancha, broadband digital subscriber line (DSL), servicios moviles e inalámbricos
- La organizaciones requieren de coneciones más rápidas para soportar teléfono IP, video conferencias, centros de almacenamiento de datos, etc.
- Las interconexiones de clase empresarial generalmente las proporcionan los proveedores de servicios (SP) y pueden incluir: DSL empresarial, líneas arrendadas y Metro Ethernet.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Home and Small Office Internet Connections



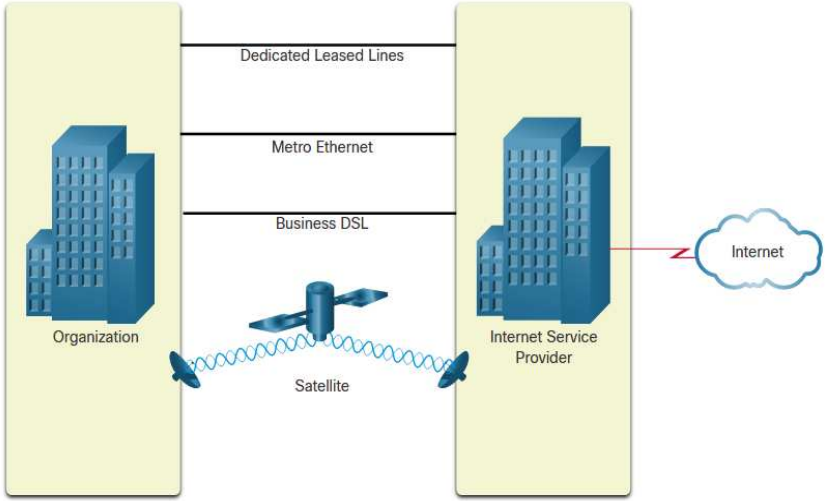
Connection	Description
Cable	Internet de gran ancho de banda, siempre activo, ofrecido prvedores de televisión por cable.
DSL	Interne de gran ancho de banda, siempre activo, se proporciona mediante linea telefónica.
Celular	Utiliza la red de telefonía celular para conectase a internet.
Satelite	Se utiliza en zonas rurales donde no se cuenta con provedores de internet.
Dial-up telefono	Bajo ancho de banda que requiere el uso de un módem.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Conexiones de internet empresariales

Las conexiones comerciales corporativas pueden requerir:

- Mayor ancho de banda
- Conexiones dedicadas
- Administración de servicios



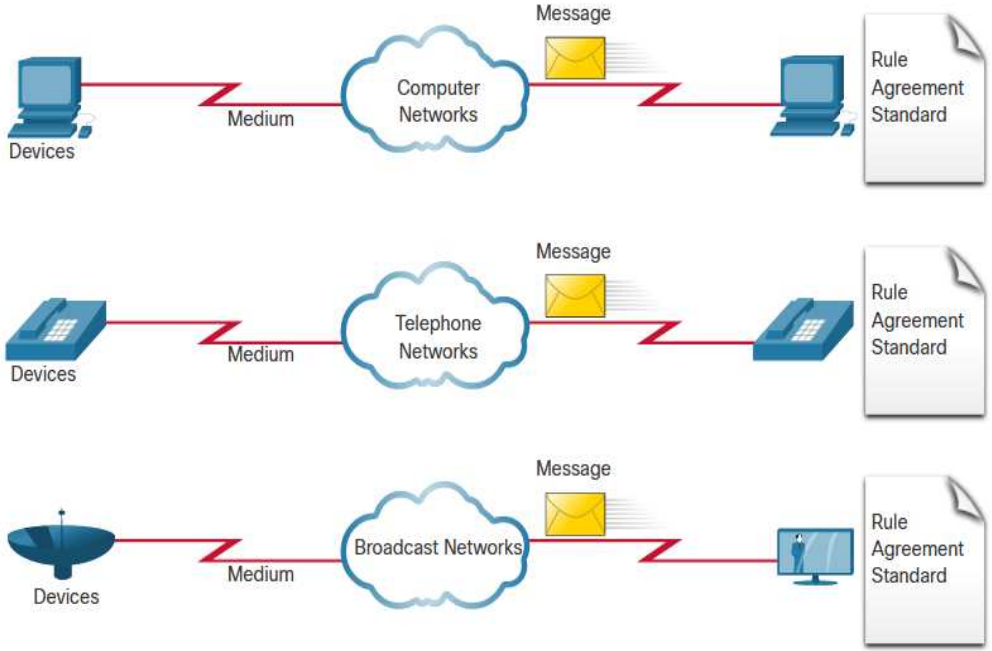
Tipo	Descripción
Linea dedicada	Circuitos resevados dentro de la red del proveedor de servicios que conectan oficinas distantes (redes privadas de voz y datos).
Ethernet WAN	Para extender la tecnología de acceso LAN a la WAN.
DSL	Business DSL está disponible en varios formatos incluyendo Symmetric Digital Subscriber Lines (SDSL).
Satellite	Proporciona una conexión cuando no existe una solución mediante cable.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Redes Convergentes

Antes de las redes convergentes, una organización requería de redes separadas para telefóno, video y datos. Cada una requería de diferentes tecnologías.

Cada una de las tecnologías utilizaría un conjunto diferente de reglas y estándares.



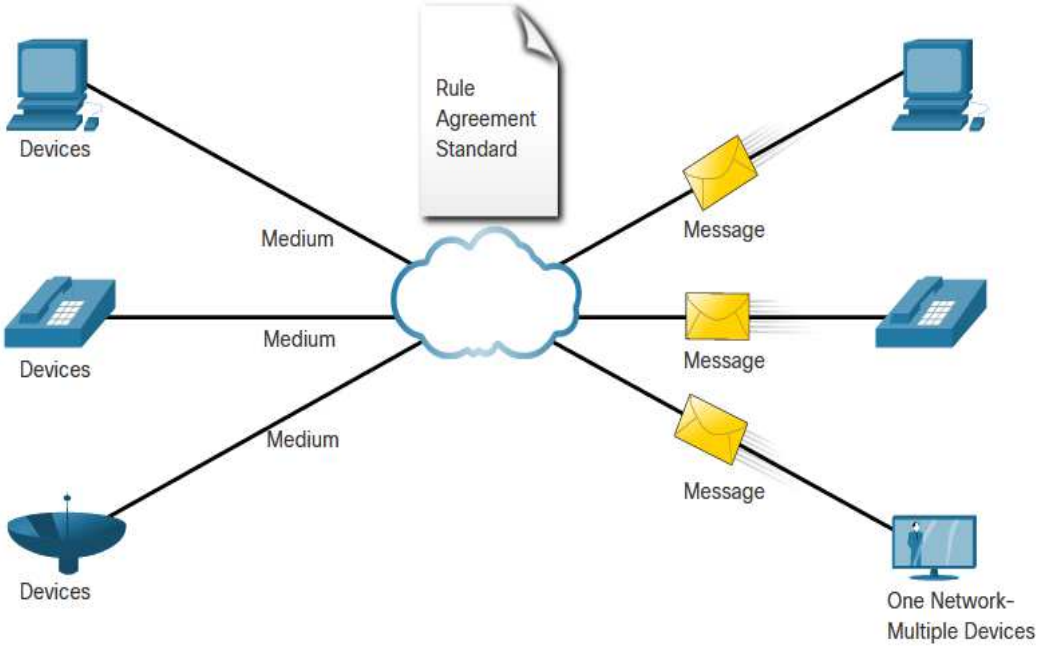
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

The Converging Network (Cont.)

Las redes de datos convergentes transportan múltiples servicios en un enlace que incluyen:

- Datos
- Voz
- Video

Las redes convergentes pueden entregar datos, voz y video a través de la misma infraestructura de red. La infraestructura de red utiliza el mismo conjunto de reglas y estándares.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Video – Descargar e Instalar Packet Tracer

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Video – Iniciando con Cisco Packet Tracer

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Actividad Packet Tracer – Network Representation

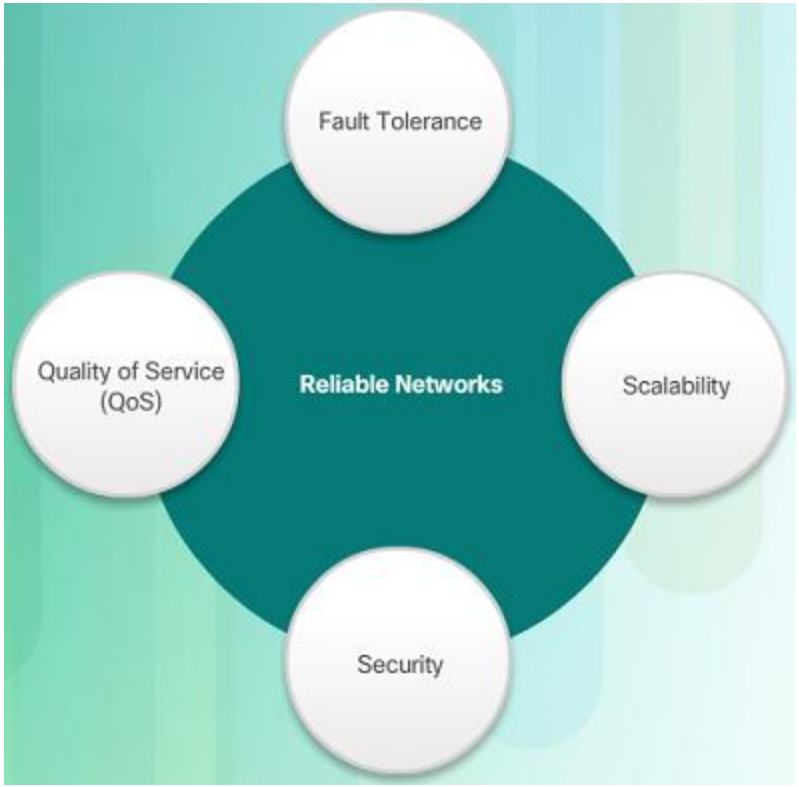
Note: Es importante que se entienda todo lo visto en está actividad.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

1.6 Redes confiables

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Reliable Network
Arquitectura de Red



La arquitectura de red se refiere a las tecnologías que admiten la infraestructura que mueve los datos a través de la red.

Hay cuatro características básicas que las arquitecturas subyacentes deben cumplir para satisfacer las expectativas del usuario:

- Tolerancia a fallos
- Escalabilidad
- Calidad de servicio (QoS)
- Seguridad

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

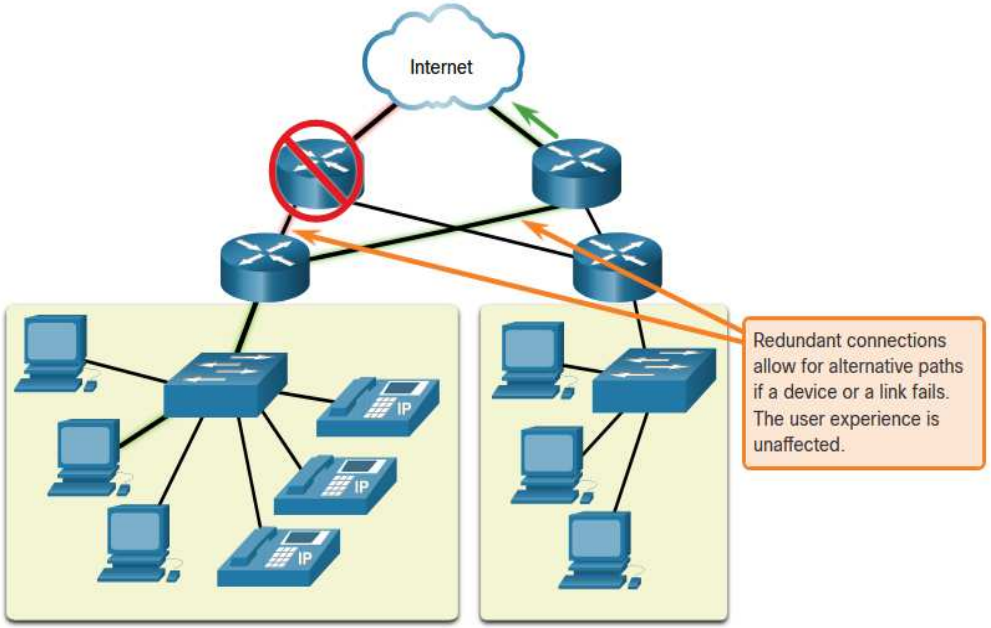
Tolerancia a fallas

Una red tolerante a fallas limita el impacto de una falla al minimizar la cantidad de dispositivos afectados. Se requieren múltiples rutas para la tolerancia a fallas.

Las redes confiables brindan redundancia al implementar una red de conmutación de paquetes:

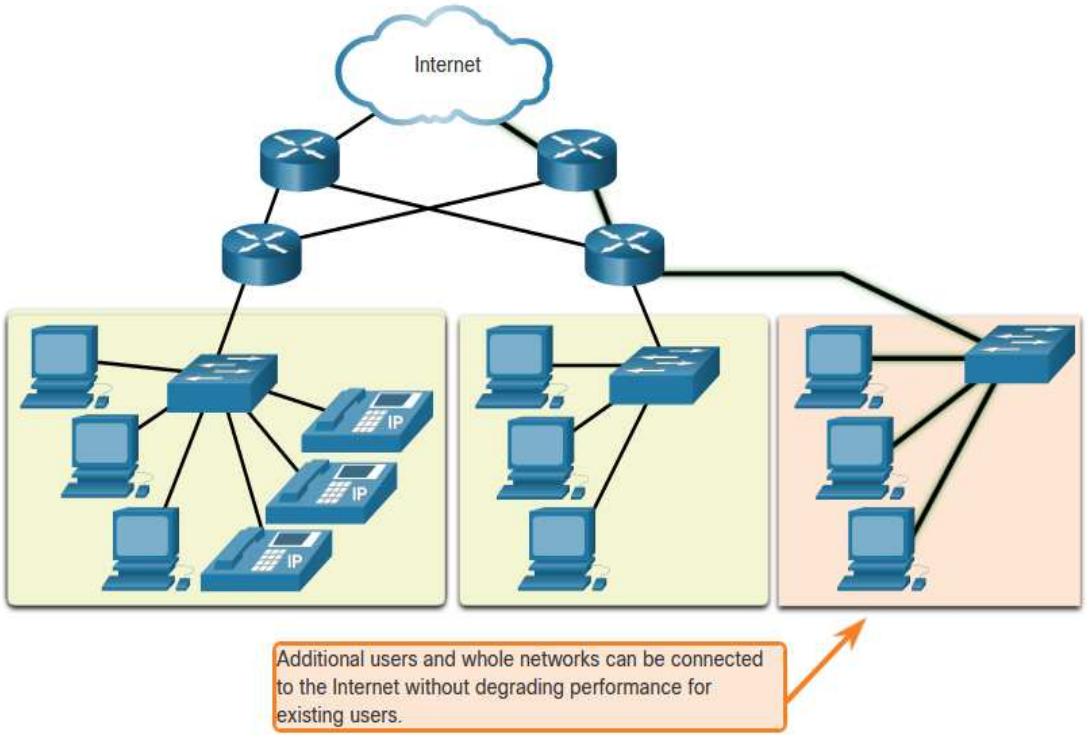
- La conmutación de paquetes divide el tráfico en paquetes que se enrutan a través de una red.
- En teoría, cada paquete podría tomar una ruta diferente hacia el destino.

Esto no es posible con redes de conmutación de circuitos que establecen circuitos dedicados.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Escalabilidad



Una red escalable puede expandirse rápida y fácilmente para admitir nuevos usuarios y aplicaciones sin afectar el rendimiento de los servicios para los usuarios existentes.

Los diseñadores de redes siguen estándares y protocolos aceptados para garantizar que las redes sean escalables.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

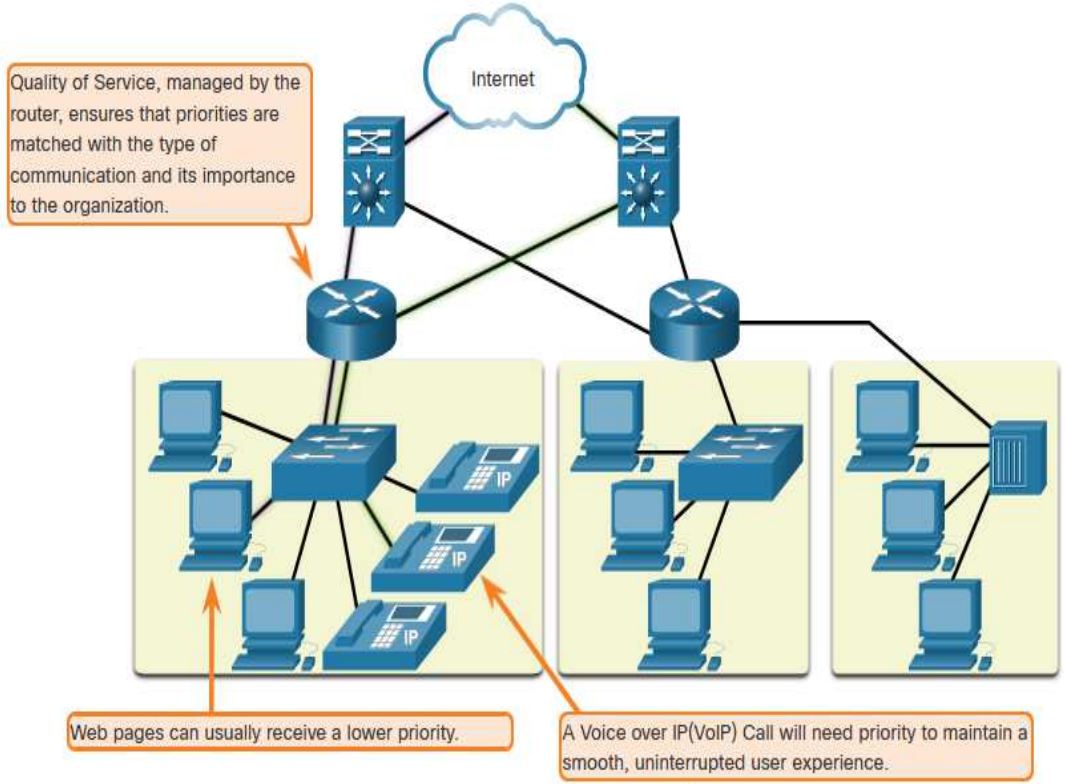
Quality of Service

Las transmisiones de voz y video en tiempo real requieren satisfacer mayores expectativas.

- ¿Alguna vez has visto un video en vivo con pausas constantes? Esto se produce cuando hay una mayor demanda de ancho de banda que el disponible y la calidad del servicio no está configurada.

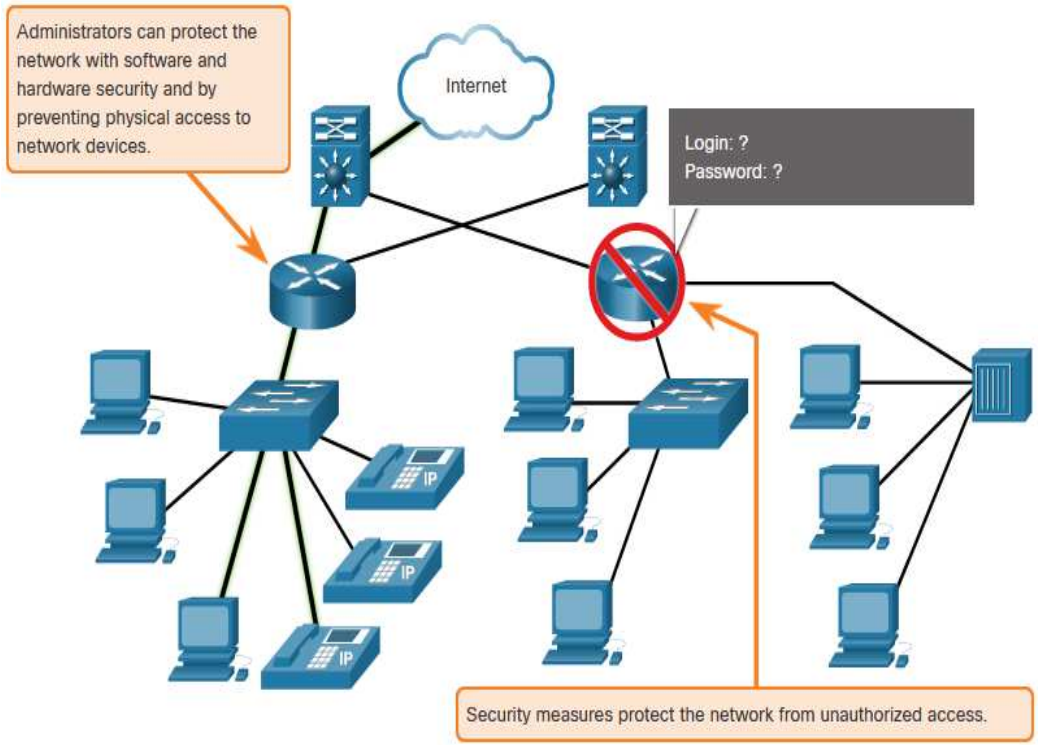
La calidad de servicio (QoS) es el mecanismo principal utilizado para garantizar la entrega confiable de contenido para todos los usuarios.

Con una política de QoS implementada, el enrutador puede administrar más fácilmente el flujo de tráfico de datos y voz.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Seguridad de la red



Exsiten dos tipos principales de seguridad de red que deben abordarse:

1. Seguridad de la infraestructura de red
   - Seguridad física de los dispositivos de red
   - Evitar el acceso no autorizado a los dispositivos
2. Seguridad de la información
   - Protección de la información o datos transmitidos por la red

Tres objetivos de la seguridad de la red:

1. Confidencialidad: solo los destinatarios previstos pueden leer los datos
2. Integridad: garantía de que los datos no se han alterado durante la transmisión.
3. Disponibilidad: garantía de acceso oportuno y confiable a los datos para usuarios autorizados

© All rights reserved. Cisco Confidential

1.7 Tendencias de la Red

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Tendencia recientes

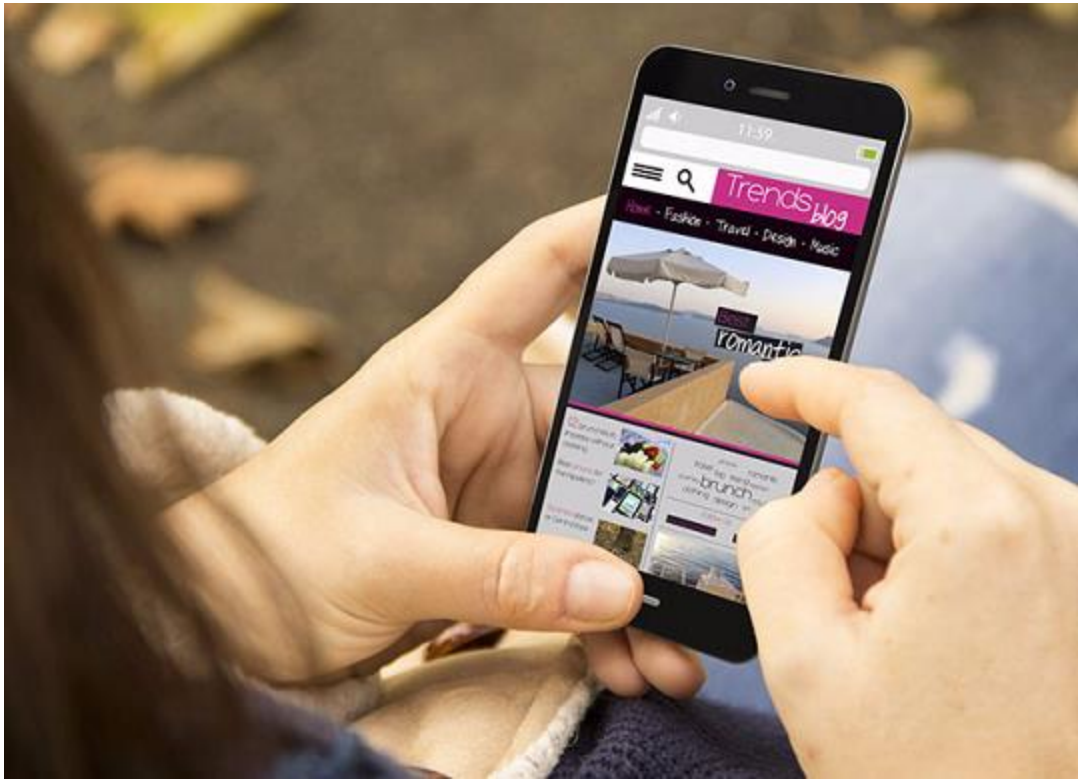
El papel de la red debe adaptarse y transformarse continuamente para poder mantenerse al día con las nuevas tecnologías y los dispositivos que llegan constantemente al mercado.

Algunas nuevas tendencias de redes que afectan a organizaciones y consumidores:

- LLeve su propio dispositivo (BYOD)
- Colaboración online
- Comunicaciones por video
- Computo en la nube

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Bring Your Own Device



Bring Your Own Device (BYOD) permite a los usuarios utilizar sus propios dispositivos dándoles más oportunidades y mayor flexibilidad.

Permite a los usuarios finales tener la libertad de utilizar herramientas personales para acceder a la información y comunicarse mediante sus:

- Laptops
- Netbooks
- Tabletas
- Teléfonos inteligentes
- Lectores electrónicos

BYOD significa cualquier dispositivo, con cualquier propiedad, utilizado en cualquier lugar.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Online Collaboration

Cisco Webex

- Colaborar y trabajar con otros a través de la red en proyectos conjuntos.
- Las herramientas de colaboración, incluido, brindan a los usuarios una forma de conectarse e interactuar instantáneamente.
- La colaboración es una prioridad muy alta para las empresas y la educación.
- Cisco Webex Teams es una herramienta de colaboración multifuncional.
  - enviar mensajes instantáneos
  - publicar imágenes
  - publicar videos y enlaces

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

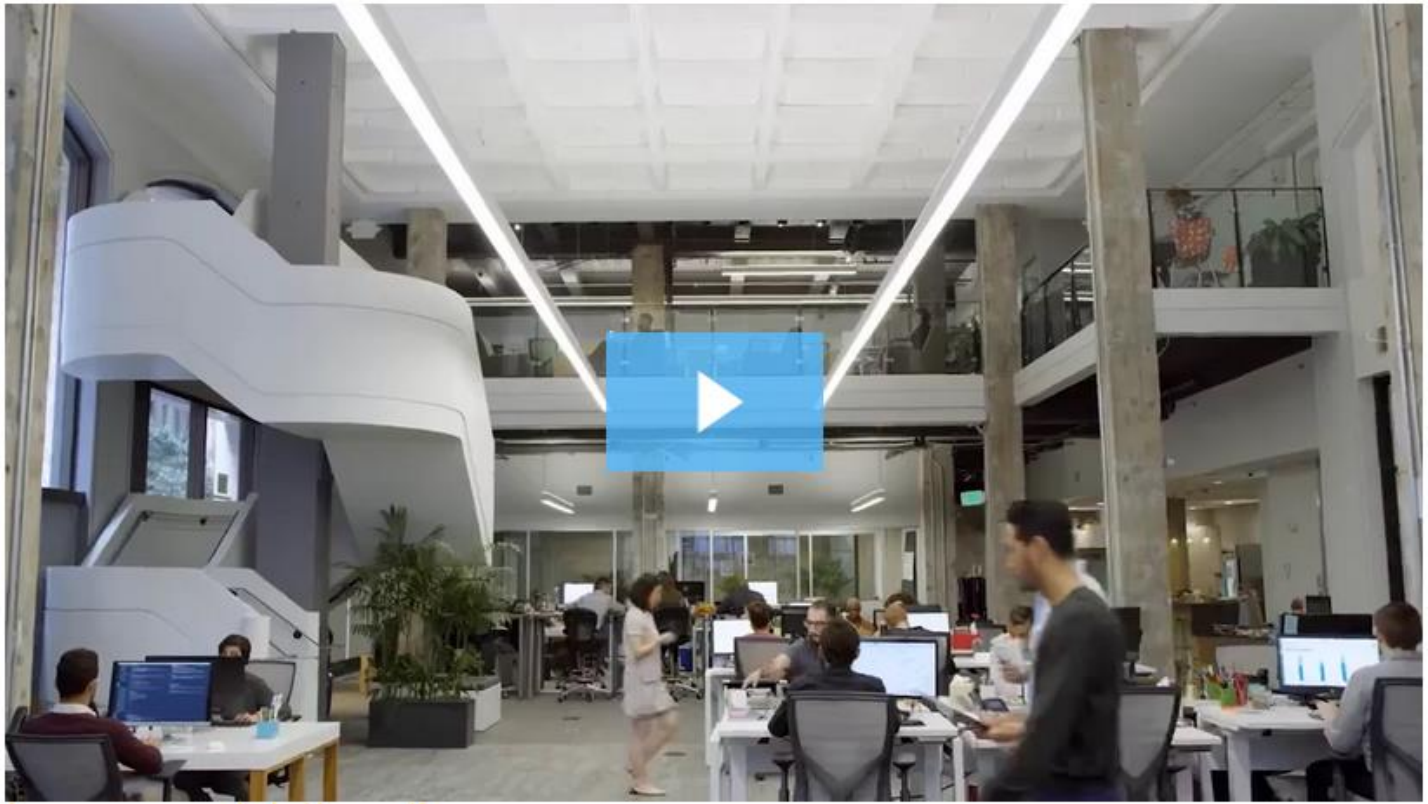
Comunicación en Video

- Las videollamadas se realizan a cualquier persona, independientemente de su ubicación.
- La videoconferencia es una herramienta poderosa para comunicarse con otros.
- El video se está convirtiendo en un requisito fundamental para una colaboración eficaz.

- Cisco TelePresence powers es una forma de trabajar donde todos, en todas partes.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Video – Cisco WebEx for Huddles



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Computo en la nube

La computación en la nube nos permite almacenar archivos personales o hacer copias de seguridad de nuestros datos en servidores a través de Internet.

- También se puede acceder a las aplicaciones utilizando la nube.
- Permite a las empresas realizar envíos a cualquier dispositivo en cualquier parte del mundo.

El computo en la nube es posible gracias a los centros de datos.

- Las empresas más pequeñas que no pueden costear sus propios centros de datos, alquilan servidores y servicios de almacenamiento en la nube de organizaciones de centros de datos más grandes.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

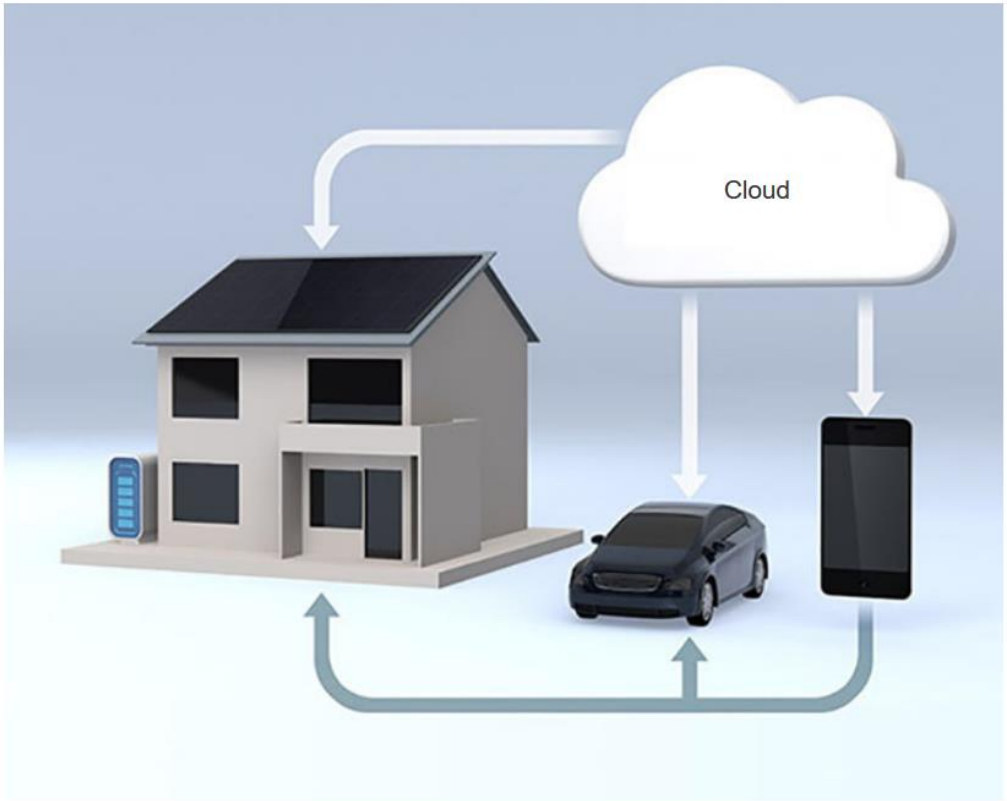
Computo en la nube (Cont.)

Cuatro tipos de nubes:

1. Nubes públicas
   - Disponible para el público en general a través de un modelo de pago por uso o de forma gratuita.
2. Nubes privadas
   - Destinado a una organización o entidad específica como el gobierno.
3. Nubes híbridas
   - Compuesto por dos o más tipos de nube, por ejemplo, parte personalizada y parte pública.
   - Cada parte sigue siendo un objeto distintivo, pero ambas están conectadas utilizando la misma arquitectura.
4. Nubes personalizadas
   - Creado para satisfacer las necesidades de una industria específica, como la atención médica o los medios.
   - Puede ser público o privado.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

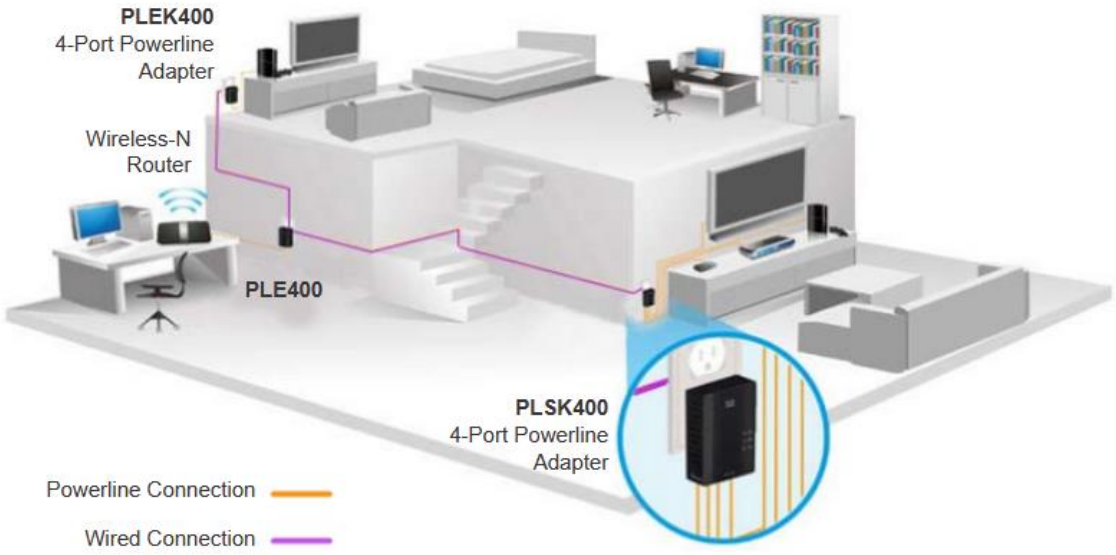
Tendencias tecnológicas en el hogar



- Los hogares inteligente son una tendencia creciente que permite que la tecnología se integre en los electrodomésticos de uso diario, lo que permite su interconexión con otros dispositivos.
- Los hornos pueden saber a qué hora cocinar una comida sincronizandose con su agenda electrónica para saber a qué hora llegará a casa.
  - Actualmente, se está desarrollando tecnología de hogar inteligente para todas las habitaciones de una casa.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Powerline Networking



- Mediante la redes eléctricas se puede permitir que los dispositivos se conecten a una LAN donde los cables de red de datos o las comunicaciones inalámbricas no son una opción viable.
- Con un adaptador de línea de alimentación estándar, los dispositivos se pueden conectar a la LAN siempre que haya una toma de corriente mediante el envío de datos en ciertas frecuencias.
- Las redes eléctricas son especialmente útiles cuando los puntos de acceso inalámbricos no pueden llegar a todos los dispositivos del hogar.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Banda ancha inalámbrica

Además de DSL y cable, la tecnología inalámbrica es otra opción que se utiliza para conectar hogares y pequeñas empresas a Internet.

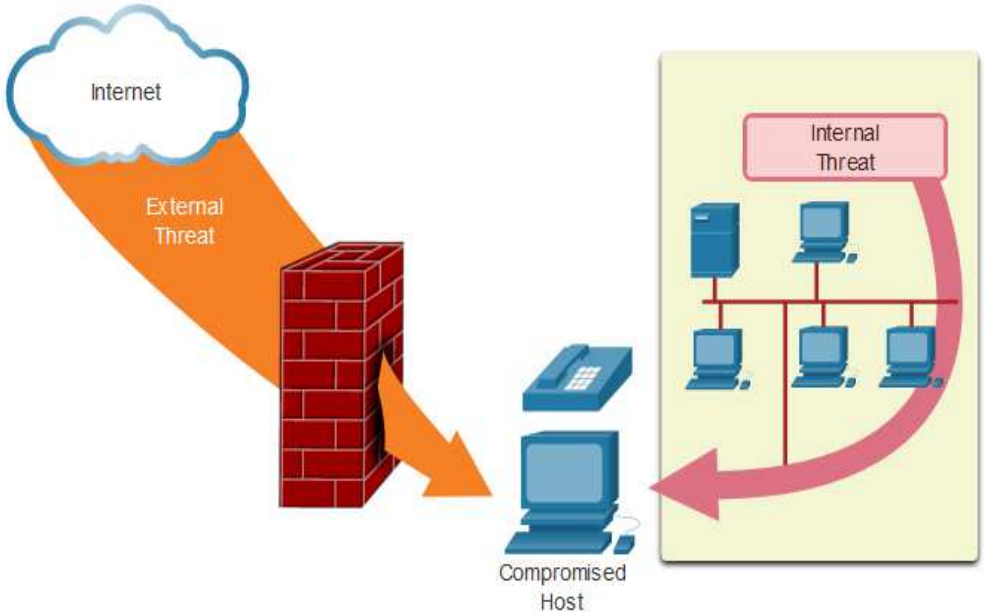
- Se usa comunmente en entornos rurales, un proveedor de servicios de Internet inalámbrico (WISP) es un ISP que conecta a los suscriptores a puntos de acceso o puntos de acceso designados.
- La banda ancha inalámbrica es otra solución para el hogar y las pequeñas empresas.
  - Utiliza la misma tecnología que utiliza un teléfono inteligente.
  - Se instala una antena fuera de la casa que proporciona conectividad inalámbrica o por cable para dispositivos en el hogar.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

1.8 Seguridad de la Red

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

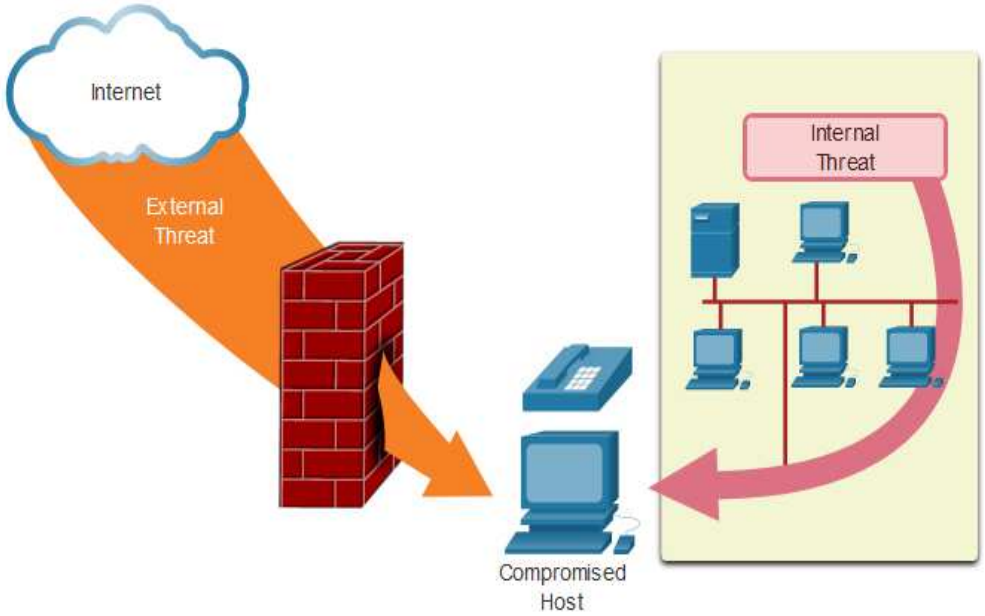
Amenazas de seguridad



- Sin importar el tamaño de la red, l a seguridad de la red es una parte integral de la red
- La seguridad de la red que se implemente debe tener en cuenta el entorno al mismo tiempo que protege los datos, pero al mismo tiempo debe garantizar la QoS de la red.
- Asegurar una red implica muchos protocolos, tecnologías, dispositivos, herramientas y técnicas para proteger los datos y mitigar las amenazas.
- Los fuentes de amenazas pueden ser externas o internas.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Amenazas de seguridad(Cont.)



Amenazas externas:

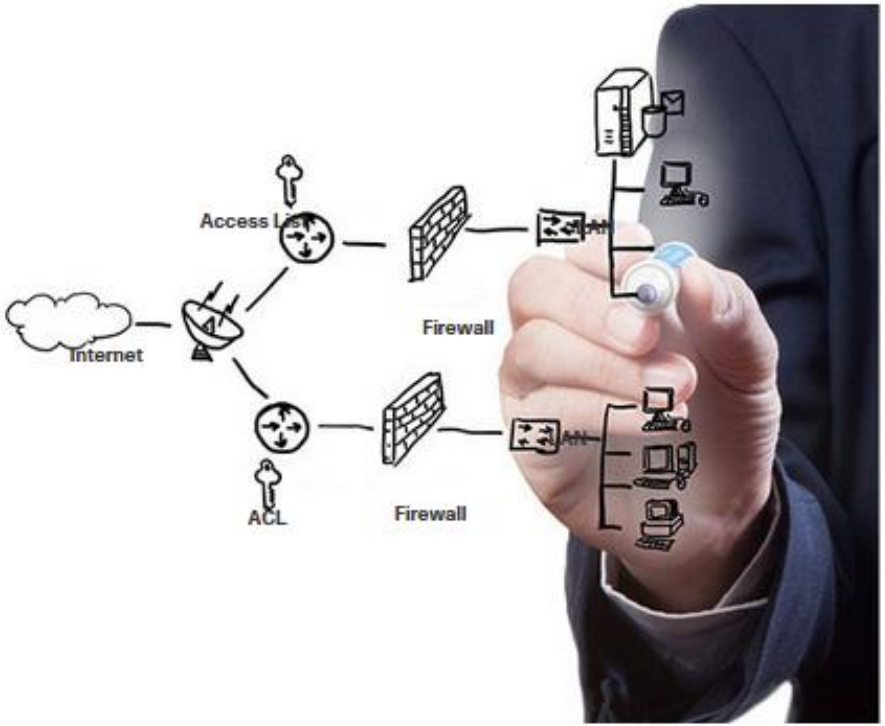
- Viruses, gusanos, y caballos de troya
- Spyware y adware
- Ataques de dias cero
- Threat Actor attacks
- Negación de servicio DoS
- Intercepción y robo de datos
- Robo de identidad

Amenazas internas:

- Dispositivos robados o perdidos
- Uso indebido accidental por parte de los empeados
- Empleados maliciosos

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Soluciones de Seguridad



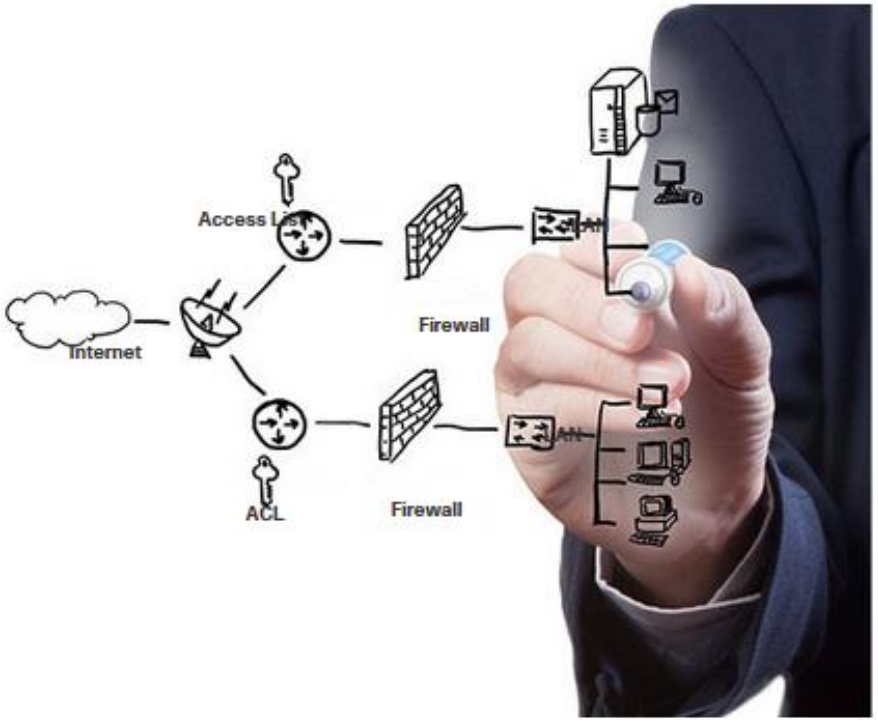
La seguridad debe implementarse en múltiples capas utilizando más de una solución de seguridad.

Componentes de seguridad de red para redes domésticas o de pequeñas oficinas:

- Se debe instalar software antivirus y antispyware en los dispositivos finales.
- El filtrado de firewall se utiliza para bloquear el acceso no autorizado a la red.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Solucione de Seguridad(Cont.)



En redes más grandes se tienen requisitos de seguridad adicionales:

- Sistema de firewall dedicado
- Listas de control de acceso (ACL)
- Sistemas de prevención de intrusiones (IPS)
- Redes privadas virtuales (VPN)

El estudio de la seguridad de la red comienza con una comprensión clara de la infraestructura de enrutamiento y conmutación subyacente.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

1.9 El profesional de IT

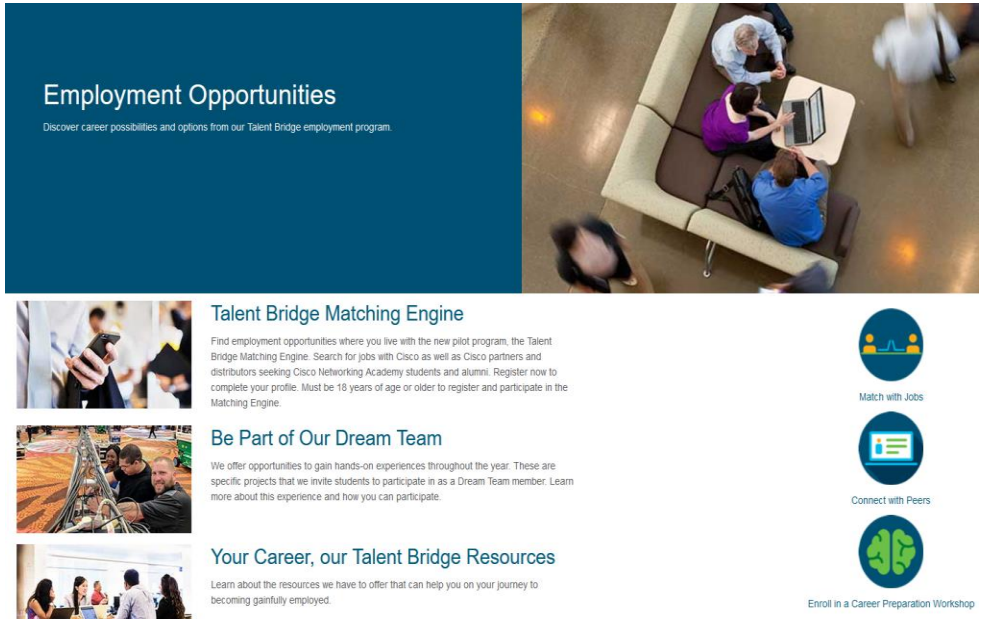
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

CCNA

La certificación Cisco Certified Network Associate (CCNA): demuestra que tiene conocimiento de las tecnologías fundamentales, lo cual garantiza que se mantenga actualizado con las habilidades necesarias para la adopción de tecnologías de próxima generación.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Redes de trabajo

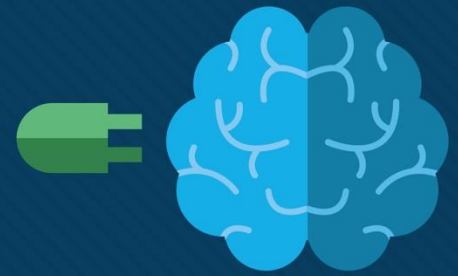


Oportunidades de empleo en www.netacad.com puede hacer clic en el menú Carreras y luego seleccionar Oportunidades de empleo.

Talent Bridge Matching Engine para encontrar oportunidades de empleo utilizando .

- Conecta socios y distribuidores de Cisco que busquen estudiantes y exalumnos de Cisco Networking Academy.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential



Módulo 2: Configuración básica de dispositivos finales y de conmutación

Introducción a Redes

Objetivos

Objectivo del modulo: Realizar la configuración inicial de un Switch y dispositivos finales, incluidas las contraseñas, la dirección IP y los parámetros de la puerta de enlace predeterminada.

Topic Title	Topic Objective
Cisco IOS	Como acceder al IOS de un dispositivo Cisco IOS para fines de configuración.
Navegación en el IOS	Como navegar entre los distintos modos para configurar un dispositivo
Estructura de los comandos	Comprender la estrutura de los comandos del software IOS
Configuración básica de dispositivos	Configurar un dispositivo Cisco usando CLI.
Guardar configuraciones	Salvar archivos de configuración mediante comandos IOS .
Puertos y Direcciones	Conocer como se comunican los dispositivos de una red
Configurar la direciones IP	Configurar la dirección IP de un host
Pruebas de conectividad	Verifcar conectividad entre dispositivos finales

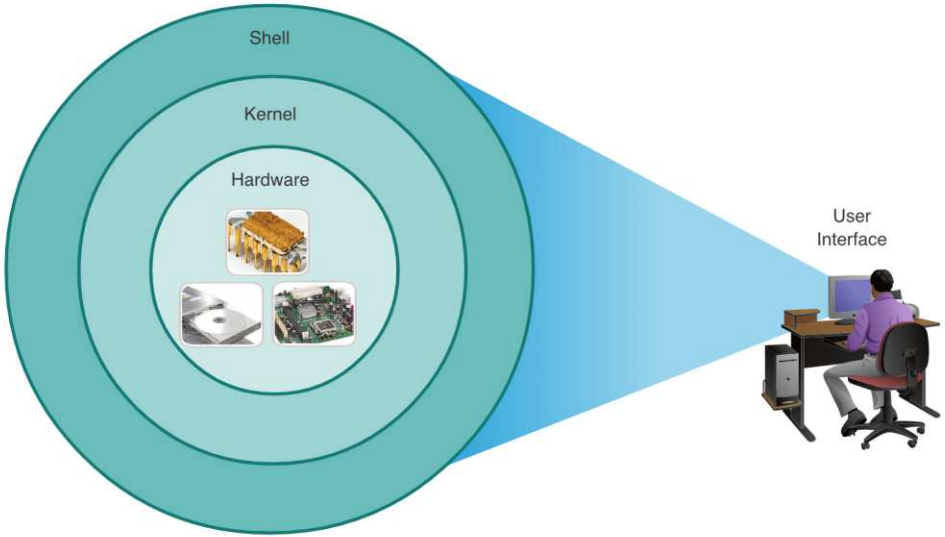
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

2.1 Acceso al Cisco IOS

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Sistemas Operativos

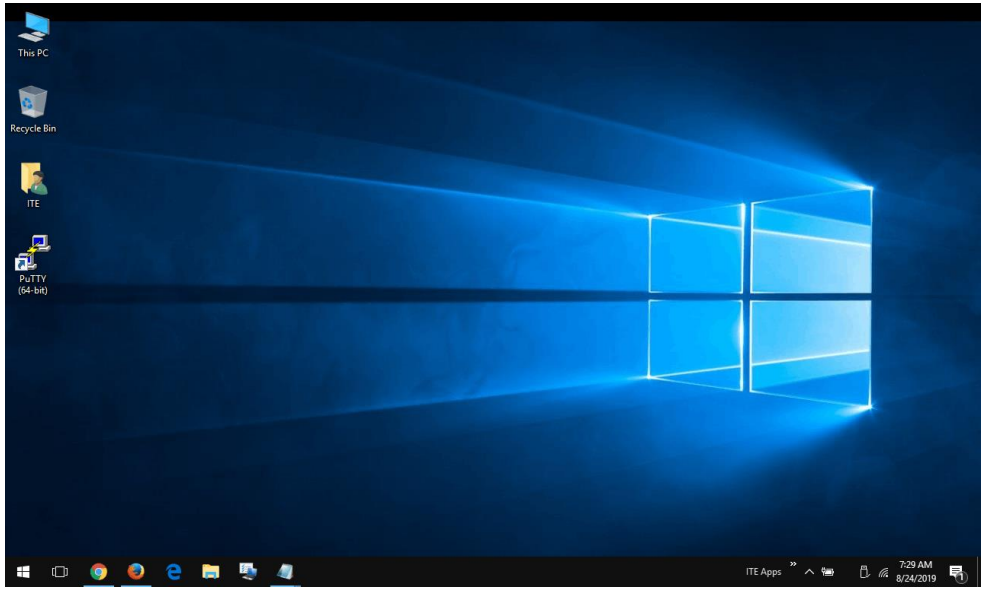
- **Shell** - Es la interfaz de usuario que permite a los usuarios ejecutar acciones específicas desde la computadora. Estas se pueden realizar a través de las interfaces CLI o GUI.
- **Kernel** - Comunica el hardware y el software de una computadora y administra cómo se utilizan los recursos de hardware para cumplir con los requisitos del software.
- **Hardware** - La parte física de una computadora, incluida la electrónica subyacente.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

GUI

- Una GUI permite al usuario interactuar con el sistema utilizando un entorno gráfico, menús y ventanas.
  - Es fácil de usar y requiere menos conocimiento de la estructura de comando subyacente que controla el sistema.
  - Ejemplos de GUIs: Windows, macOS, Linux KDE, Apple iOS y Android.
  - Las GUI pueden fallar, bloquearse o simplemente no funcionar como se especifica. Por estas razones, normalmente se accede a los dispositivos de red a través de una CLI.

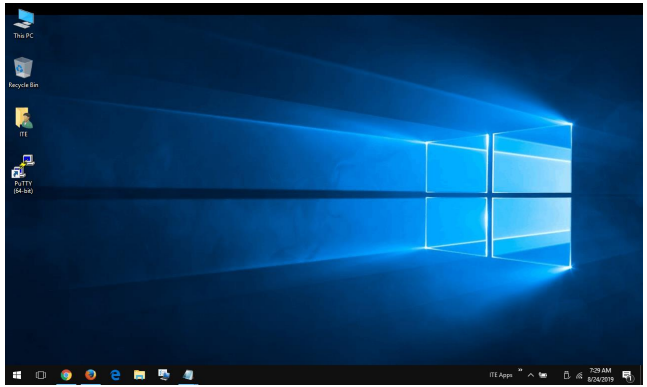


© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Purpose of an OS

El sistema operativo de una PC permite al usuario:

- Utilizar un mouse para hacer selecciones y ejecutar programas
- Ingresar texto y comandos basados en texto
- Ver la salida en un monitor



Un sistema operativo basado en CLI permite al usuario:

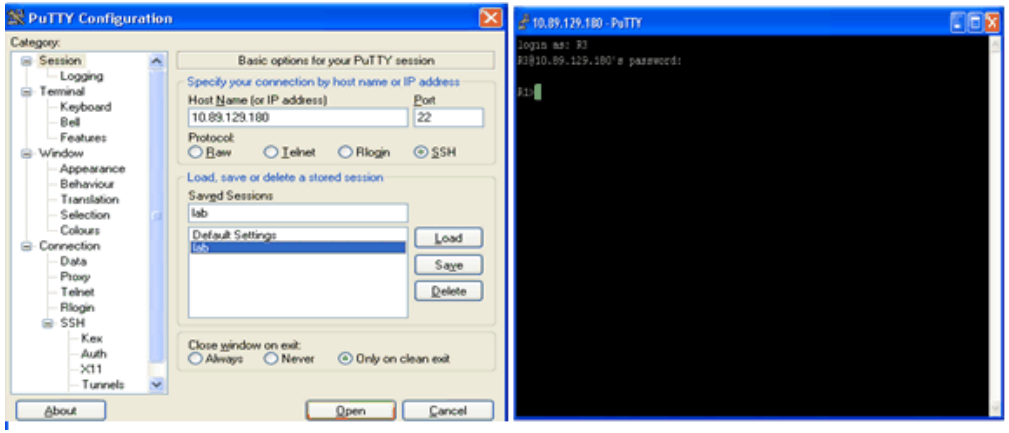
- Utilizar el teclado para ejecutar programas
- Ingresas comandos basados en texto
- Ver la salida en un monitor

```
analyst@secOps ~]$ ls
Desktop  Downloads  lab.support.files  second_drive
[analyst@secOps ~]$
```

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Método de Acceso

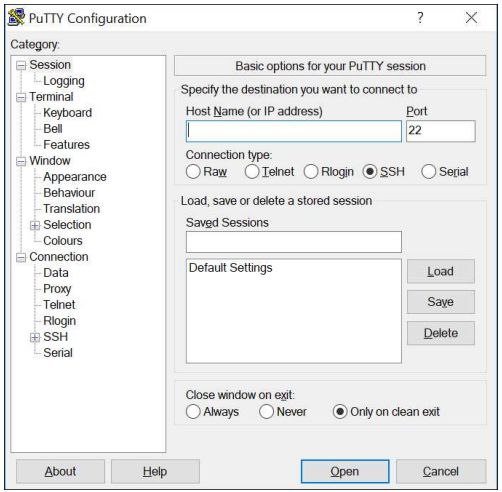
- **Console** – Un puerto de administración físico que se utiliza para acceder a un dispositivo con el fin de proporcionar mantenimiento, así como para realizar las configuraciones iniciales.
- **Secure Shell (SSH)** – Establece una conexión CLI remota segura a un dispositivo, a través de una interfaz virtual. (Nota: este es el método recomendado para conectarse de forma remota a un dispositivo).
- **Telnet** – Establece una conexión CLI remota insegura a un dispositivo a través de la red. (Nota: la autenticación de usuario, las contraseñas y los comandos se envían a través de la red en texto plano).

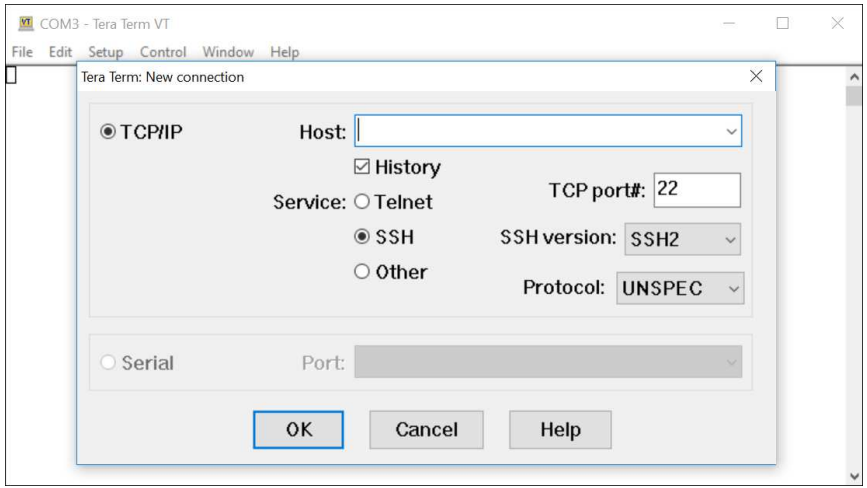


© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Terminal Emulation Programs

- Los programas de emulación de terminal se utilizan para conectarse a un dispositivo de red mediante un puerto de consola o mediante una conexión SSH / Telnet.
- Existen varios programas de emulación de terminal, como PuTTY, Tera Term y SecureCRT.





© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

2.2 Navegación IOS

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Modos primarios

Modo EXEC Usuario:

- Permite el acceso a un número limitado de comandos de monitoreo básicos
- Identificado por el indicador CLI que termina con el símbolo>

```
Router>

Switch>
```

Modo EXEC Privilegiado:

- Permite el acceso a todos los comandos y funciones.
- Identificado por el indicador CLI que termina con el símbolo #

```
Router#

Switch#
```

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Modos y submodos de configuración

Modo de configuración global:

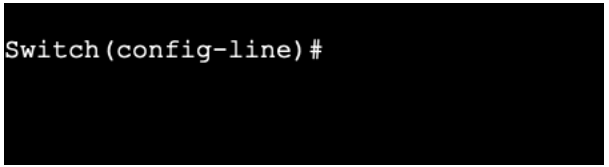
- Se utiliza para acceder a las opciones de configuración del dispositivo.

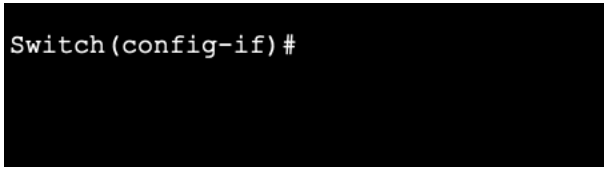
Modo de configuración Line :

- Se utiliza para configurar el acceso a la consola, SSH, Telnet o AUX

Interface Configuration Mode:

- Se utiliza para configurar un puerto de un switch/router





© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Video – IOS CLI Modos de Comando Principal (Sec. 2.2.3)

El video cubre:

- Modo EXEC Usuario
- Modo EXEC Privilegiado
- Modo de Configuración Global

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Navigación entre modos IOS

- **Modo EXEC Privilegiado:**
  - Para pasar del modo EXEC de usuario al modo EXEC privilegiado, utilice el comando **enabled**.

```
Switch> enable
Switch#
```

- **Modo de Configuración Global :**
  - Para entrar y salir del modo de configuración global, use el comando **configure terminal**. Para volver al modo EXEC privilegiado, use el comando **exit**

```
Switch(config)#
Switch(config)#exit
Switch#
```

- **Modo de Configuración Line :**
  - Para entrar y salir del modo de configuración de línea, use el comando de **line** seguido del tipo de línea de administración. Para volver al modo de configuración global, use el comando **exit**.

```
Switch(config)#line console 0
Switch(config-line)#exit
Switch(config)#
```

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Navigación entre modos IOS (Cont.)

Modos de Subconfiguración :

- Para salir de cualquier modo de subconfiguración y volver al modo de configuración global, use el comando **exit**. Para volver al modo EXEC privilegiado, use el comando final o la combinación de teclas **Ctrl + Z.**

```
Switch(config)#line console 0
Switch(config-line)#end
Switch#
```

- Para pasar directamente de un modo de subconfiguración a otro, escriba el comando del modo de subconfiguración deseado. En el ejemplo, el símbolo del sistema cambia de **(config-line)#** a **(config-if)#**.

```
Switch(config-line)#interface FastEthernet 0/1
Switch(config-if)#
```

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Video – Navigación entre modos IOS (Sec. 2.2.5)

Este video explica:

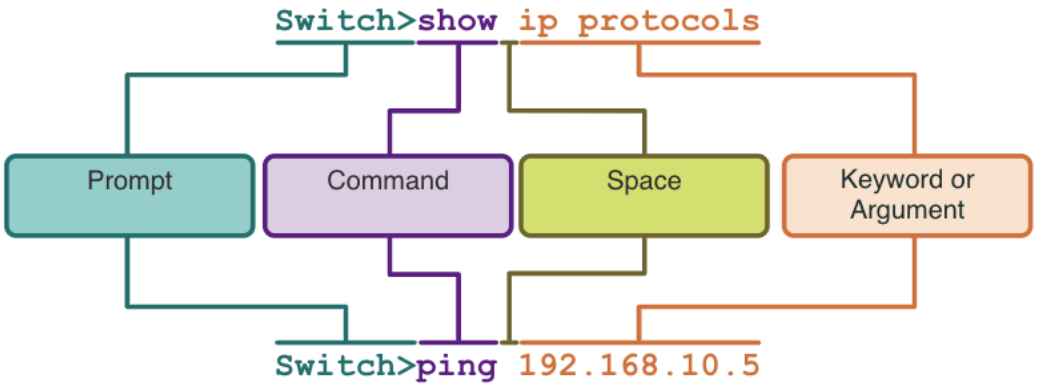
- enable
- disable
- configure terminal
- exit
- end
- Control + Z
- Comandos de modos de subconfiguración

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

2.3 La estructura de los comandos

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Estructura Básica de los Comandos IOS



- **Keyword** – Este es un parámetro específico definido en el sistema operativo (en la figura, **ip protocolos**).
- **Argument** - Es un parámetro no predefinido; es un valor o variable definida por el usuario (en la figura,**192.168.10.5**).

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

IOS Verificación de sintaxis de comandos

Un comando puede requerir uno o más argumentos. Para determinar las palabras clave y los argumentos necesarios para un comando, consulte la sintaxis del comando.

- El texto en negrita indica comandos y palabras clave que se ingresan literalment como se muestran.
- El texto en cursiva indica un argumento para el que el usuario debe proporciona el valor.

Convention	Description
negritas	El texto en negrita indica comandos y palabras clave que se deben ingresar literalmente como se muestran.
italicas	El texto en cursiva indica un argumento para el que el usuario debe proporciona el valor.
[x]	Indican un elemento opcional (palabra clave o argumento).
{x}	Indican un elemento requerido (palabra clave o argumento).
[x {y | z }]	Las llaves y las líneas verticales entre corchetes indican una opción requerida dentro de un elemento opcional. Los espacios se utilizan para delimitar claramente las partes del comando.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

IOS Verificación de sintaxis de comandos (Cont.)

- La sintaxis del comando proporciona el patrón o formato que se debe usar al ingresar un comando.

- El comando es **ping** y el argumento definido por el usuario es la dirección IP del dispositivo de destino. Por ejemplo, **ping 10.10.10.5**.

```
ping ip-address
```

- El comando es **traceroute** y el argumento definido por el usuario es la dirección IP del dispositivo de destino. Por ejemplo, **traceroute 192.168.254.254**.

```
traceroute ip-address
```

- Si un comando es complejo con varios argumentos, puede verlo representado así:

```
Switch(config-if)# switchport port-security aging { static | time time | type {absolute | inactivity}}
```

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

IOS Funciones de ayuda

El IOS tiene dos formas de ayuda disponibles: ayuda sensible al contexto y verificación de sintaxis de comandos.

- La ayuda contextual permite encontrar rápidamente respuestas a estas preguntas:
  - ¿Qué comandos están disponibles en cada modo de comando?
  - ¿Qué comandos comienzan con caracteres específicos o grupos de caracteres?
  - ¿Qué argumentos y palabras clave están disponibles para comandos particulares?

```
Router#ping ?
  WORD  Ping destination address or hostname
  ip    IP echo
  ipv6  IPv6 echo
```

- La comprobación de sintaxis del comando verifica que el usuario haya ingresado un comando válido.
  - Si el intérprete no puede entender el comando que se está ingresando, proporcionará retroalimentación describiendo lo que está mal.

```
Switch#interface fastEthernet 0/1
                  ^
% Invalid input detected at '^' marker.
```

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Video – Comprobador de sintaxis de comandos y ayuda contextual (Secc - 2.2.8)

Este video presenta:

- Uso del comando de ayuda en los modos de EXEC de usuario, EXEC privilegiado y de configuración global
- Como completar los comandos y argumentos con el comando de ayuda
- Uso del comprobador de sintaxis de comandos para corregir errores de sintaxis y comandos incompletos

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Hot Keys y Shortcuts

- La CLI del IOS proporciona teclas de acceso rápido y accesos directos para facilitar la configuración, la supervisión y la resolución de problemas.
- Los comandos y las palabras clave se pueden reducir al prefijo mínimo de caracteres que identifican una única selección. Por ejemplo, el comando **configure** puede acortarse a **conf** porque configure es el único comando que comienza con **conf**.

```
Router#con
% Ambiguous command: "con"
Router#con?
configure  connect
```

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

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Hot Keys y Shortcuts (Cont.)

- La siguiente tabla es una breve lista de keystrokes para mejorar la edición de la línea de comandos.

Keystroke	Descripción
Tab	Completa una entrada parcial dde nombre de comando.
Backspace	Borra el carácter a la izquierda del cursor.
Left Arrow or **Ctrl+B**	Mueve el cursor un carácter a la izquierda.
Right Arrow or **Ctrl+F**	Mueve el cursor un carácter a la derecha.
Up Arrow or **Ctrl+P**	Recupera los comandos en el búfer del historial, comenzando con los comandos más recientes.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Hot Keys and Shortcuts (Cont.)

- Cuando la salida de un comando produce más texto del que se puede mostrar en una pantalla de terminal, el IOS mostrará un mensaje "**--More--**". La siguiente tabla describe las keystrokes que se pueden utilizar cuando se muestra este mensaje.

Keystroke	Descripción
Enter	Muestra la siguiente línea.
Barra espaciadora	Muestra la siguiente pantalla.
Cualquier otra tecla	Finaliza la cadena de visualización, volviendo al modo EXEC privilegiado.

- La siguiente tabla enumera los comandos que se pueden usar para salir de una operación.

Keystroke	Descripción
Ctrl-C	Cuando está en cualquier modo de configuración, finaliza el modo de configuración y vuelve al modo EXEC privilegiado.
Ctrl-Z	Cuando está en cualquier modo de configuración, finaliza el modo de configuración y vuelve al modo EXEC privilegiado.
Ctrl-Shift-6	Secuencia de interrupción multiusos utilizada para abortar búsquedas de DNS, traceroutes, pings, etc.

Nota: para ver más funciones ver la sección 2.3.5.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Video – Hot Keys y Shortcuts (Secc 2.3.6)

Este video revisa lo siguente:

- Tab key (completado con tab)
- Acortamiento de comandoa
- Felhas Up and down
- CTRL + C
- CTRL + Z
- CTRL + Shift + 6
- CTRL + R

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Packet Tracer – Navegación del IOS (Secc 2.3.7)

En este Packet Tracer, se hace lo siguiente:

- Establecer conexiones básicas, acceder a la CLI y explorar la ayuda
- Explorae los modos EXEC
- Ajustar el reloj del dispositivo

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

2.4 Configuración básica

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Nombre del dispositivo

- El primer comando de configuración en cualquier dispositivo debería ser asignarle un nombre único de host.
- De forma predeterminada, a todos los dispositivos se les asigna un nombre predeterminado de fábrica. Por ejemplo, un Cisco IOS switch is "Switch."

- Directrices para nombrar dispositivos:
  - Empezar con una letra
  - No contiener espacios
  - Terminar con una letra o un dígito
  - Usar solo letras, dígitos y guiones
  - Tener menos de 64 caracteres de longitud

```
Switch# configure terminal
Switch(config)# hostname Sw-Floor-1
Sw-Floor-1(config)#
```

Nota: Para que el switch vuelva al indicador predeterminado, utilice el comando de configuración global **no hostname**.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Directrices para la contraseña

- El uso de contraseñas débiles o fáciles de adivinar es un problema de seguridad.
- Todos los dispositivos de red deben limitar el acceso administrativo asegurando EXEC privilegiado, EXEC de usuario y acceso remoto con contraseñas. Además, todas las contraseñas deben estar cifradas y deben proporcionarse notificaciones legales.
- Directrices para establecer contraseña:
  - Utilizar contraseñas que tengan más de ocho caracteres.
  - Utilizar una combinación de letras mayúsculas y minúsculas, números, caracteres especiales y / o secuencias numéricas.
  - Evite utilizar la misma contraseña para todos los dispositivos.
  - No usar palabras comunes porque son fáciles de adivinar.

Nota: La mayoría de las prácticas de laboratorio de este curso utilizan contraseñas simples como **cisco** o **class**. Estas contraseñas son débiles y fáciles de adivinar y deben evitarse en entornos de producción.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Configuración de contraseñas

Asegurar el acceso al modo EXEC de usuario:

- Ingresar al modo de configuración de la consola de línea usando el comando **line console 0** en el modo de configuración global.
- A continuación, especifique la contraseña del modo EXEC de usuario mediante el comando contraseña contraseña.
- Por último, habilite el acceso EXEC del usuario mediante el comando **login**.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# line console 0
Sw-Floor-1(config-line)# password cisco
Sw-Floor-1(config-line)# login
Sw-Floor-1(config-line)# end
Sw-Floor-1#
```

Asegurar el acceso al modo EXEC privilegiado:

- Primero ingrese al modo de configuración global.
- A continuación, utilice el comando **enable secret** password.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# enable secret class
Sw-Floor-1(config)# exit
Sw-Floor-1#
```

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Configuración de contraseñas (Cont.)

Asegurar el acceso a la línea VTY:

- Primero ingrese al modo de configuración line VTY usando el comando **line vty 0 15** en el modo de configuración global.
- A continuación, especifique la contraseña de VTY mediante el comando **password**
- Finalmente, habilite el acceso VTY usando el comando **login**

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# line vty 0 15
Sw-Floor-1(config-line)# password cisco
Sw-Floor-1(config-line)# login
Sw-Floor-1(config-line)# end
Sw-Floor-1#
```

- **Nota:** Las líneas VTY permiten el acceso remoto mediante Telnet o SSH al dispositivo. Muchos switches Cisco admiten hasta 16 líneas VTY numeradas del 0 al 15.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Cifrado de contraseñas

- Los archivos *startup-config* y r*unning-config* muestran la mayoría de las contraseñas en texto plano.
- Para cifrar todas las contraseñas de texto plano, utilice el comando de configuración global de cifrado de contraseñas del servicio.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# service password-encryption
Sw-Floor-1(config)# exit
Sw-Floor-1#
```

- Utilice el comando **show running-config** para verificar que las contraseñas del dispositivo estén ahora cifradas.

```
Sw-Floor-1# show running-config
!

!
line con 0
password 7 094F471A1A0A
login
!
Line vty 0 4
Password 7 03095A0F034F38435B49150A1819
Login
!
!
end
```

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Mensajes de banner

- Un mensaje es importante para advertir al personal no autorizado que no intente acceder al dispositivo.
- Para crear un mensaje de banner del día en un dispositivo de red, use el comando **banner motd #** *el mensaje del día* **#** en el modo de configuración global.

Nota: El "#" en la sintaxis del comando se denomina carácter delimitador. Se ingresa antes y después del mensaje.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# banner motd #Authorized Access Only!#
```

El banner se mostrará al intetar acceder al dispositivo.

```
Press RETURN to get started.



Authorized Access Only!

User Access Verification

Password:
```

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Video – Secure Administrative Access to a Switch (Secc 2.4.6)

Este video cubre:

- Acceso seguro al puerto de la consola
- Acceso seguro al terminal virtual para acceso remoto
- Cifrado de contraseñas
- Configuración del mensaje de banner
- Verificación de cambios de seguridad

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

2.5 Guadar configuraciones

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Archivos de configuración

- Hay dos archivos de sistema que almacenan la configuración del dispositivo:
  - **startup-config**: archivo de configuración guardado que se almacena en la NVRAM. Contiene todos los comandos que utilizará el dispositivo al iniciarse o reiniciarse. La memoria Flash no se borra cuando el dispositivo está apagado.
  - **running-config:** se almacena en la memoria de acceso aleatorio (RAM). Refleja la configuración actual. La modificación de una configuración en ejecución afecta el funcionamiento de un dispositivo Cisco de inmediato. La RAM es una memoria volátil. Pierde todo su contenido cuando el dispositivo se apaga o se reinicia.
  - Para guardar los cambios realizados en la configuración en ejecución en el archivo de configuración de inicio, use el comando del modo EXEC privilegiado **copy running-config startup-config**.

```
Router#show startup-config
Using 624 bytes
!
version 15.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
```

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

Current configuration : 624 bytes
!
version 15.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
```

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Modificar las configuraciones en ejecución

Si los cambios realizados en la configuración en ejecución no tienen el efecto deseado y la configuración en ejecución aún no se ha guardado, puede restaurar el dispositivo a su configuración anterior de las siguientes formas:

- Elimine los comandos modificados individualmente.
- Recargue el dispositivo usando el comando **reload** en el modo EXEC privilegiado. **Nota:** Esto hará que el dispositivo se desconecte brevemente, lo que provocará un tiempo de inactividad de la red.

```
Router# reload
Proceed with reload? [confirm]
Initializing Hardware ...
```

- Si los cambios no deseados se guardaron en startup-config, puede ser necesario borrar todas las configuraciones usando el comando **erase startup-config** en el modo EXEC privilegiado.
  - Después de borrar la configuración de inicio, vuelva a cargar el dispositivo para borrar el archivo de configuración en ejecución de la RAM.

```
Router# erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Router#
```

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Video – Modificar configuración en ejecución (Secc 2.5.3)

Se revisa lo siguient:

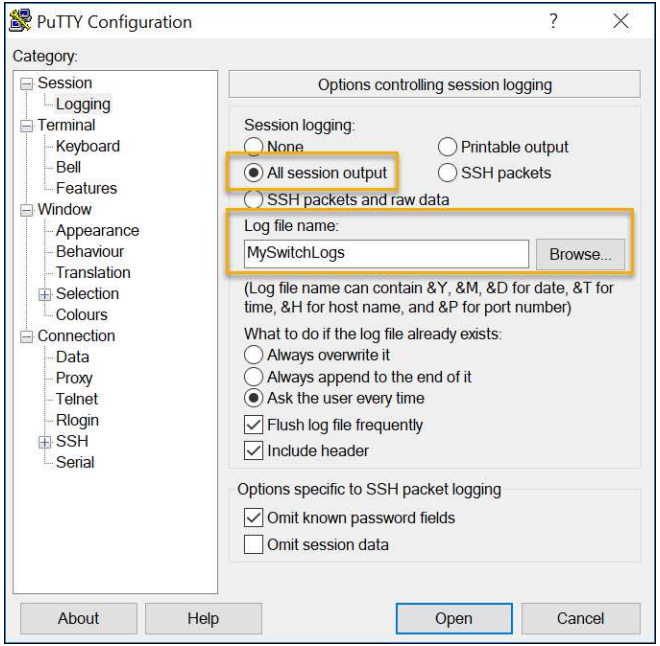
- Copiar el archivo running-config en el archivo startup-config
- Mostrar los archivos en el directorio flash o NVRAM
- Usar acortamiento de comandos
- Borrar el archivo de configuración de inicio
- Copiar el archivo start-config al archivo running-config

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Guardar la configuración en un archivo de texto

Los archivos de configuración también se pueden guardar y archivar en un documento de texto.

- **Step 1.** Abrir el Software de emulación de terminal. Por ejemplo: PuTTY o Tera Term, desde un dispositivo conectado a un Switch.
- **Step 2.** Habilite el inicio de sesión en el software del terminal y asigne un nombre y una ubicación de archivo para guardar el archivo de registro (log). La figura muestra seleccionada la opción **All session output,** con esto toda la salida del la sesión se guarda en el archivo seleccionado (i.e., MySwitchLogs).

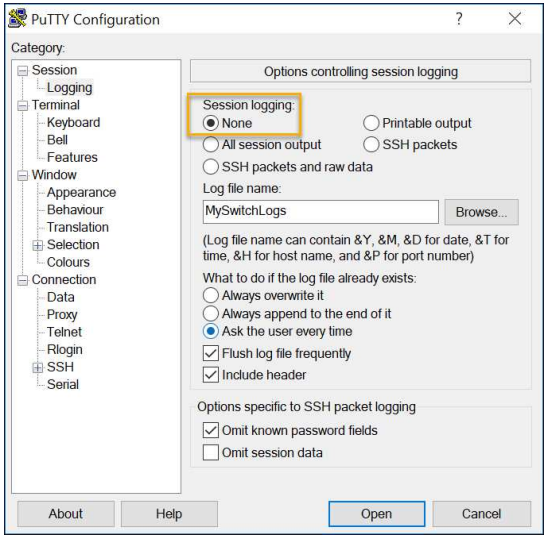


© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Guardar la configuración en un archivo de texto (Cont.)

- **Step 3.** Ejeturar el comandos **show running-config** o **show startup-config** en modo EXEC privilegiado. El texto que se muestra en la ventana del terminal se colocará en el archivo especificado.
- **Step 4.** Desactive el registro en el software del terminal. La figura muestra cómo deshabilitar el registro eligiendo la opción **None.**

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



Nota: El archivo de texto creado se puede utilizar como una bitácora de cómo está operando el dispositivo en ese momento. Es posible que sea necesario editar el archivo antes de que puedad ser utilizado para restaurar una configuración guardada.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Packet Tracer – Configuración inicial de dispositivos

En esta actividad de Packet Tracer, se realizará:

- Verificación de la configuración predeterminada del switch
- Configuración básica de conmutador
- Configurar banner MOTD
- Guardar archivos de configuración en NVRAM
- Configurar un segundo switch

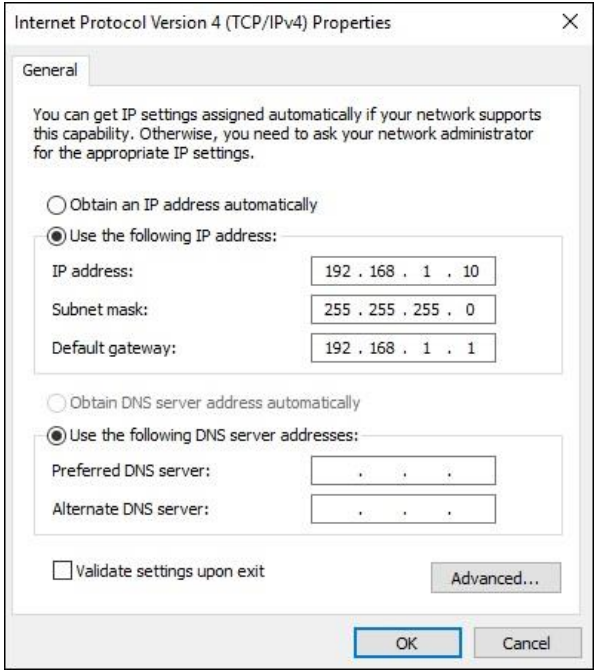
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

2.6 Puertos y Direcciones

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Dirección IP

- El uso de direcciones IP es el mecanismo principal que permite que los dispositivos se ubiquen entre sí y puedan establecer una comunicación de extremo a extremo en Internet.
- La estructura de una dirección IPv4 se denomina notación decimal con puntos y está representada por cuatro números decimales entre 0 y 255.
- Una máscara de subred IPv4 es un valor de 32 bits que diferencia porción de red de la dirección de la parte del host. Junto con la dirección IPv4, la máscara de subred determina a qué subred pertenece el dispositivo.
- La dirección de puerta de enlace predeterminada es la dirección IP del router que el host utilizará para acceder a redes remotas, incluida Internet.

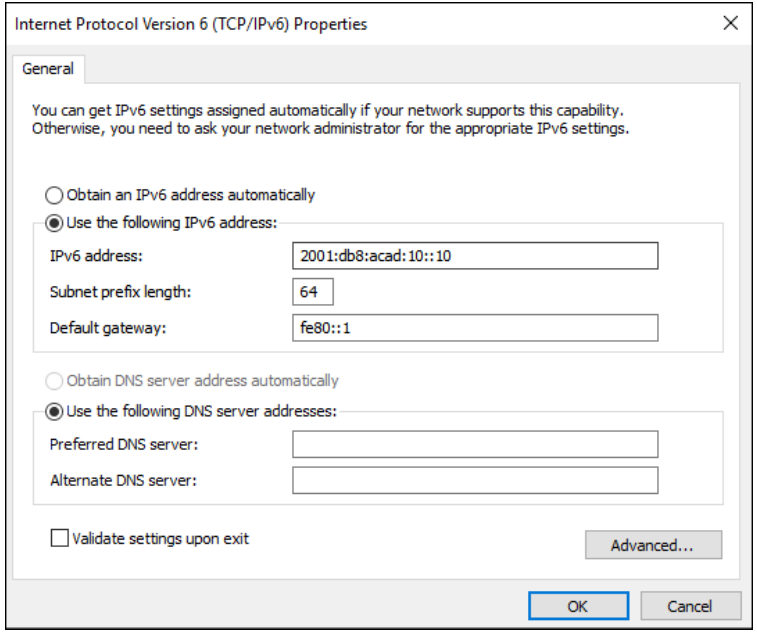


© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Direccion IP (Cont.)

- Las direcciones IPv6 tienen una longitud de 128 bits y están escritas como una cadena de valores hexadecimales. Cada cuatro bits está representado por un solo dígito hexadecimal; para un total de 32 valores hexadecimales. Los grupos de cuatro dígitos hexadecimales están separados por dos puntos ":".
- Las direcciones IPv6 no distinguen entre mayúsculas y minúsculas y se pueden escribir en minúsculas o mayúsculas.

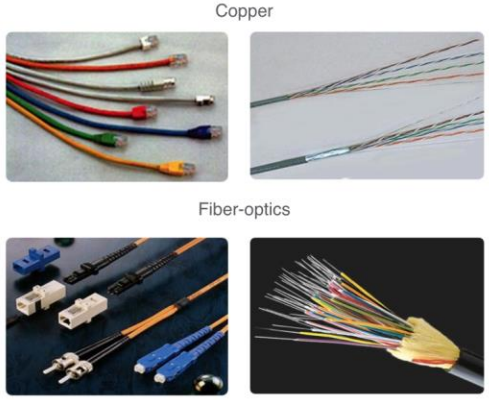
Nota: IP en este curso se refiere a los protocolos IPv4 e IPv6. IPv6 es la versión más reciente de IP y reemplazará al IPv4.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Interfaces y puertos

- Las comunicaciones de red dependen de las interfaces del dispositivo final, las interfaces del dispositivo de red y los cables que las conectan.
- Los tipos de medios de red incluyen cables de cobre de par trenzado, cables de fibra óptica, cables coaxiales o inalámbricos.
- Los diferentes tipos de medios de red tienen diferentes características y beneficios. Algunas de las diferencias entre varios tipos de medios incluyen:
  - Distancia a la que los medios pueden llevar una señal con éxito
  - Entorno en el que se instalarán los medios
  - Cantidad de datos y la velocidad a la que deben transmitirse
  - Costo de los medios e instalación



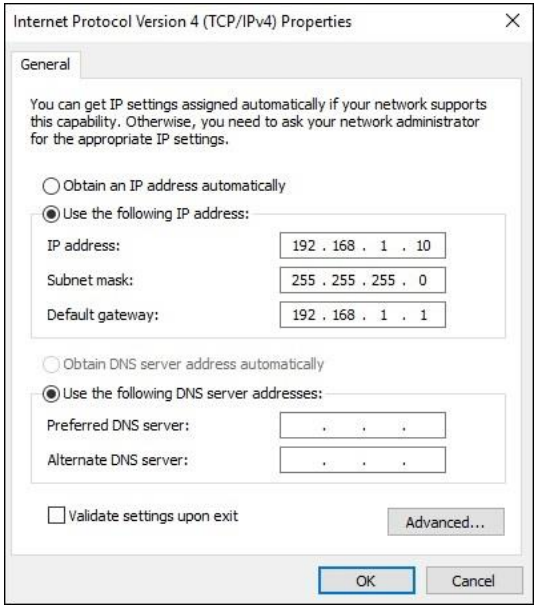
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

2.7 Configuración del direccionamiento IP

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Configuración Manual de Dispositivos Finales

- Los dispositivos finales en la red necesitan una dirección IP para comunicarse con otros dispositivos en la red.
- La información de la dirección IPv4 se puede ingresar en los dispositivos finales manualmente o automáticamente usando el Protocolo de configuración dinámica de host (DHCP).
- Para configurar manualmente una dirección IPv4 en una PC con Windows, abra el **Panel de control> Centro de redes compartidas> Cambiar la configuración del adaptador** y elija el adaptador. A continuación, haga clic con el botón derecho y seleccione Propiedades para mostrar las Propiedades de conexión de área local.
- A continuación, haga clic en **Propiedades** para abrir la ventana **Propiedades del Protocolo de Internet versión 4** (TCP / IPv4). Luego configure la dirección IPv4, la información de la máscara de subred y la puerta de enlace predeterminada.

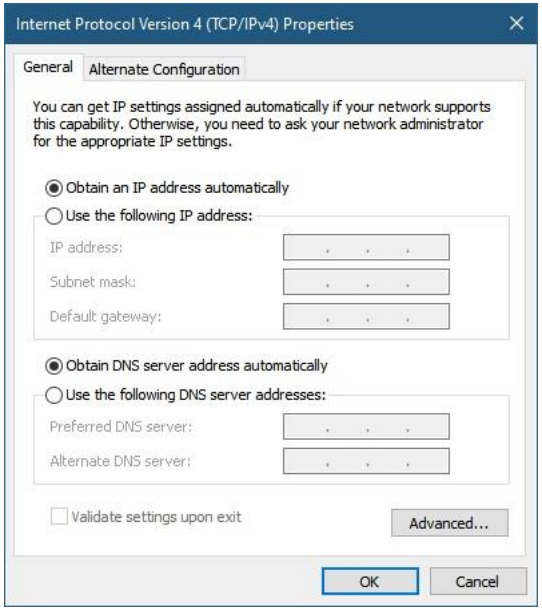


Note: IPv6 addressing and configuration options are similar to IPv4.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Configuración Automática de Dispositivos finales

- DHCP permite la configuración automática de direcciones IPv4 para cada dispositivo final que esté habilitado para DHCP.
- Los dispositivos finales suelen utilizar DHCP de forma predeterminada para la configuración automática de direcciones IPv4.
  - Para configurar DHCP en una PC con Windows, abra el **Panel de control> Centro de redes compartidas> Cambiar la configuración del adaptador** y elija el adaptador. A continuación, haga clic con el botón derecho y seleccione **Propiedades** para mostrar las **Propiedades de conexión de área local**.
  - Presionar **Propiedades** para abrir la ventana **Internet Protocol Version 4 (TCP/IPv4) Propertiee**, seleccionar **Obtener IP autonáticamente** y **Obtener dirección del servidor DNS automáticamente**.



Nota: IPv6 utiliza DHCPv6 y SLAAC (configuración automática de direcciones sin estado) para la asignación dinámica de direcciones.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Configuración de interfaces virtuales de Switch

Para acceder al conmutador de forma remota, se debe configurar una dirección IP y una máscara de subred en el SVI.

- Para configurar una SVI en un conmutador:
  - Ingrese el comando **interface vlan 1** en el modo de configuración global.
  - A continuación, asigne una dirección IPv4 mediante el comando **ip address** *ip-address subnet-mask*.
  - Finalmente, habilite la interfaz virtual usando el comando **no shutdown**

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip address 192.168.1.20 255.255.255.0
Switch(config-if)# no shutdown
```

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Packet Tracer – Implementación de conectividad básica (2.7.6)

En este Packet Tracer, aprenderá:

- Realice una configuración básica en dos Switchs
- Configurar PC
- Configurar la interfaz de administración del Switch

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

2.8 Verificar Conectividad

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Video – Test the Interface Assignment

El video cubre:

- Conecte un cable de consola desde la PC al Switch
- Utilice el programa de emulación de terminal y acepte los valores predeterminados para llevarlo a la línea de comandos
- Use enable para ingresar al modo EXEC privilegiado
- Utilice el modo de configuración global y el modo de configuración de interfaz para ingresar el comando no shutdown

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Video – Test End-to-End Connectivity

Este video cubrirá el uso del comando ping para probar la conectividad en ambos conmutadores y en ambas PC.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

2.9 Modulo Practica y Quiz

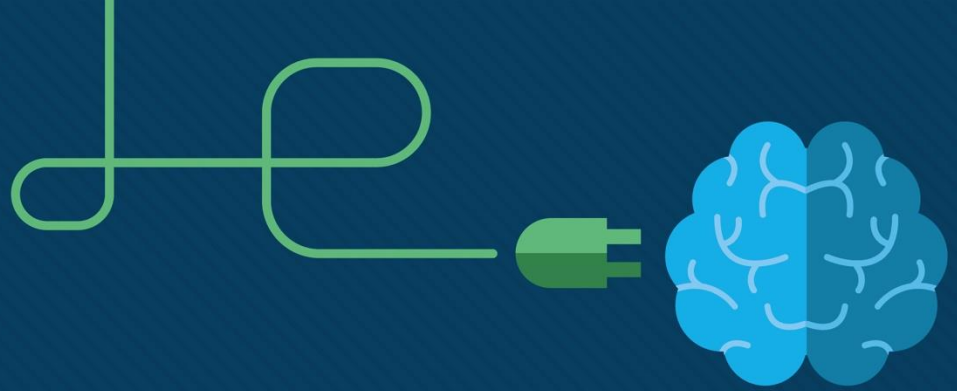
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Packet Tracer – Configuración básica del Switch y del dispositivo final (2.9.1)

En este Packet Tracer, praricará lo siguiente:

- Configurar nombres de host y direcciones IP en dos conmutadores
- Utilizar los comandos de Cisco IOS para especificar o limitar el acceso a las configuraciones del dispositivo
- Utilizar los comandos de IOS para guardar la configuración en ejecución
- Configurar dos dispositivos host con direcciones IP
- Verificar la conectividad entre los dos dispositivos finales de la PC

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential



Modulo 3: Protocolos y Modelos

Introduction to Networks 7.0 (ITN)

Objetivos

Modulo: Protocolos y Modelos

Objectivo: Explique cómo los protocolos de red permiten que los dispositivos accedan a los recursos de red locales y remotos.

Tema	Objetivo
Las reglas	Describir los tipos de reglas que son necesarias para comunicarse con éxito.
Protocolos	Explicar por qué los protocolos son necesarios en la comunicación de red.
Suites de Protocolos	Explicar el propósito de seguir un conjunto de protocolos.
Organizatciones de Estándares	Explicar el papel de las organizaciones de estándares para el establecimiento de protocolos y la interoperabilidad de redes.
Modelos de Referencia	Explicar el uso de los modelos TCP/IP y OSI para facilitar la estandarización en el proceso de comunicación.
Encapsulado de datos	Explicar cómo es que la encapsulación de datos permite que los datos se transmitan a través de la red.
Acceso a los datos	Explicar cómo los hosts en una red local acceden a los recursos locales.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

3.1 Las Reglas

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Las Reglas
Video – Devices in a Bubble (3.1.1)

- Este video explica los protocolos que utilizan los dispositivos para identificar su lugar en la red y comunicarse con otros dispositivos.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Fundamentos de la comunicación

Las redes pueden variar en tamaño y complejidad. No es suficiente tener una conexión, los dispositivos deben acordar "cómo" comunicarse.

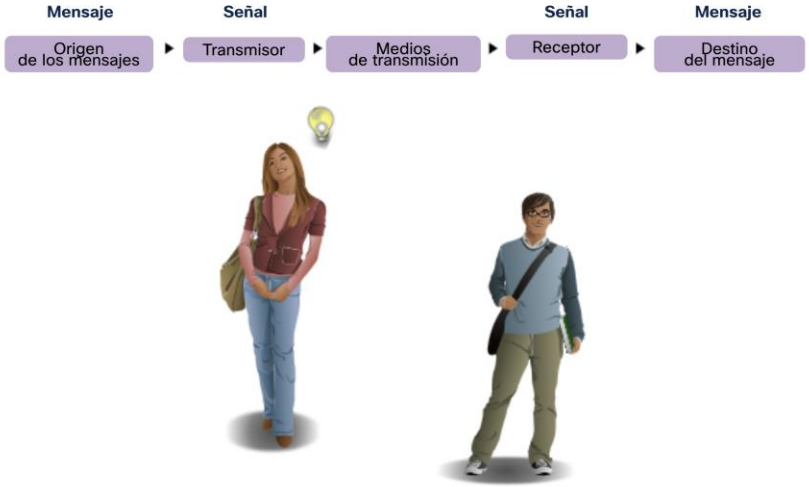
En cualquier comunicación podemos identificar tres elementos en cualquier:

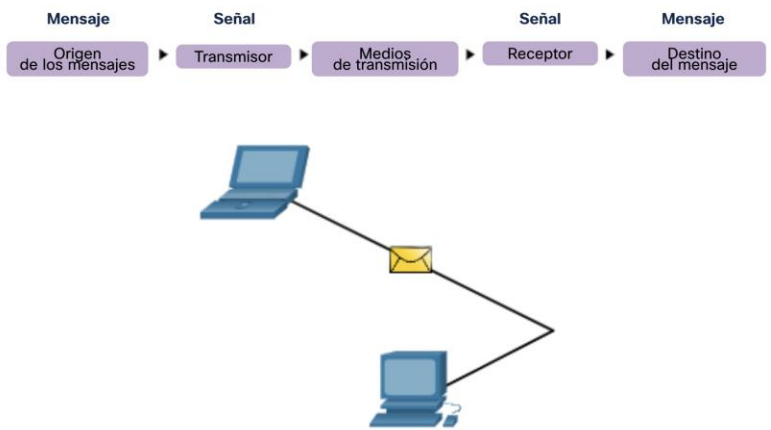
- Un origen/fuente (remitente).
- Un destino (receptor).
- Un canal (medio) que propocione la ruta de las comunicaciones.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Protocolos de Comunicación

- Todas las comunicaciones se rigen por protocolos.
- Los protocolos son las reglas que seguirán las comunicaciones.
- Estas reglas varian según el protocolo.





© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Establecimiento de Reglas

- Los individuos deben usar reglas o acuerdos establecidos para regir una conversación.
- El primer mensaje es difícil de leer porque no está redactadp correctamente. El segundo muestra el mensaje correctamente redactado

```
humanos comunicaciones las entre los gobiernan reglas. Es muydifícilcomprender
mensajes que no están correctamente formateados y quenosiguen las reglas y los
protocolos establecidos. La estructura de la gramática, el lenguaje, la puntuación y
la oración hace que la configuración humana sea comprensible para muchos individuos
diferentes.
```

```
Las reglas gobiernan las comunicaciones entre los humanos. Es muy difícil comprender
mensajes que no están correctamente formateados y que no siguen las reglas y los
protocolos establecidos. La estructura de la gramática, el idioma, la puntuación y
la oración hacen que la configuración sea humanamente comprensible para muchos
individuos diferentes.
```

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Establecimiento de Reglas (Cont.)

Los protocolos deben tener en cuenta los siguientes requisitos:

- El remitentey un receptor deben estar identificados
- Lenguaje y gramática común
- Velocidad y tiempo de entrega
- Requisitos de confirmación o reconocimiento

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Requerimientos de los Protocolos de Red

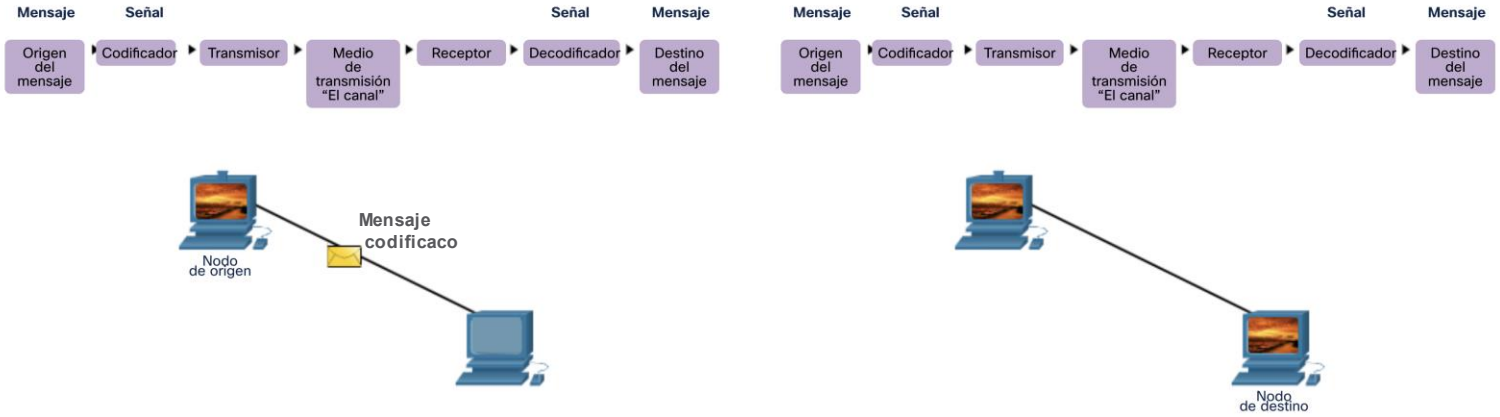
Los protocolos informáticos comunes deben estar de acuerdo e incluir los siguientes requisitos:

- Codificación de mensajes
- Formato y encapsulación de mensajes
- Tamaño del mensaje
- Sincronización de mensaje
- Opciones de entrega de mensajes

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Codificación de Mensajes

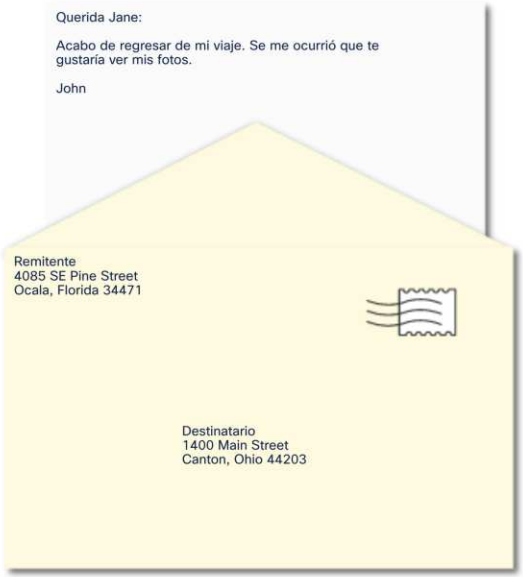
- La codificación es el proceso de convertir la información a una forma apropiada para su transmisión.
- La decodificación invierte el proceso para interpretar la información.

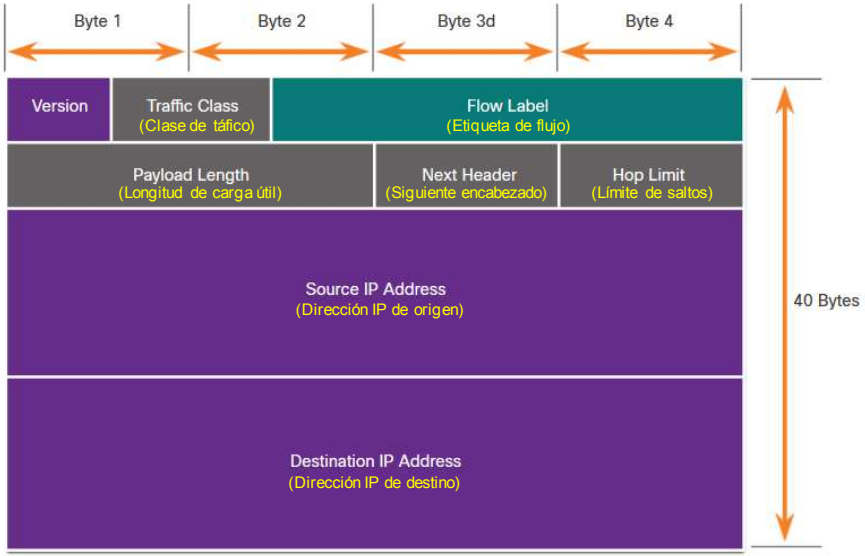


© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Formato y Encapsulación de Mensajes

- Cuando se envía un mensaje, se debe utilizar un formato o estructura específicos.
- Los formatos de mensaje dependen del tipo de mensaje y del canal que se utiliza para entregar el mensaje.

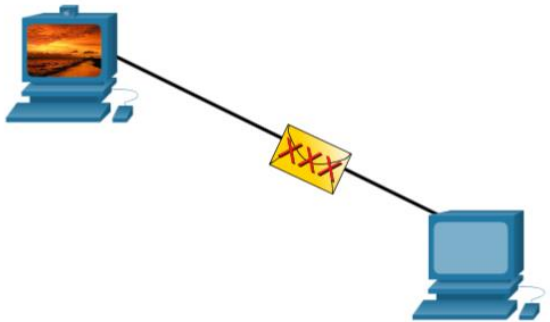


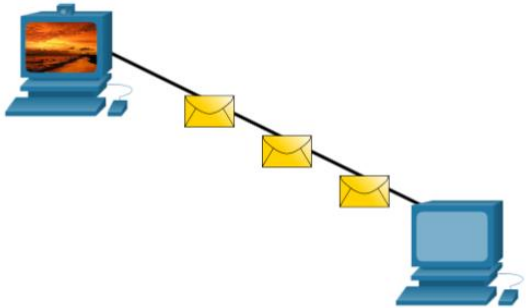


Tamaño de mensaje

La codificación entre hosts debe estar en un formato apropiado para el medio.

- Los mensajes enviados a través de la red se convierten en bits
- Los bits se codifican en un patrón de impulsos de luz, sonido o eléctricos.
- El host de destino debe decodificar las señales para interpretar el mensaje.





© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Sincronización del mensaje

La sincronización del mensaje consiste e lo siguiente:

Flow Control – Gestiona la velocidad de transmisión de datos, define cuánta información se puede enviar y que velocidad.

Response Timeout – Define cuánto tiempo debe esperar un dispositivo cuando no obtiene una respuesta del destino.

Método de Accesso - Determina cuándo se puede enviar un mensaje.

- Puede haber varias reglas que rigen cuestiones como las "colisiones". Esto ocurre cuando más de un dispositivo envía tráfico al mismo tiempo y los mensajes se corrompen.
- Algunos protocolos son proactivos e intentan prevenir colisiones; otros protocolos son reactivos y establecen un método de recuperación después de que ocurre la colisión.

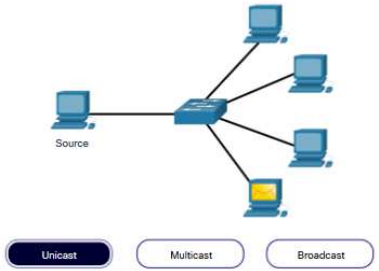
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

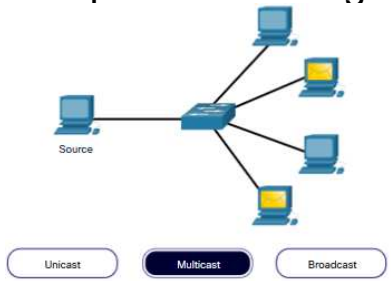
Message Delivery Options

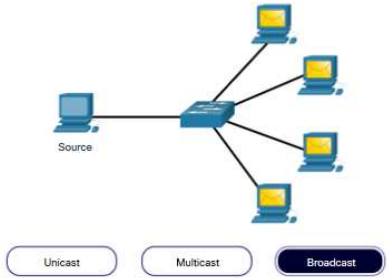
La entrega de mensajes puede utilizar uno de los siguientes métodos:

- **Unicast**: comunicación uno a uno
- **Multicast**: uno a muchos, normalmente no todos
- **Broadcast**: uno para todos

Nota: Broadcast se utilizan en redes IPv4, pero no son una opción para IPv6. Más adelante también veremos "**Anycast**" como una opción de entrega adicional para IPv6.



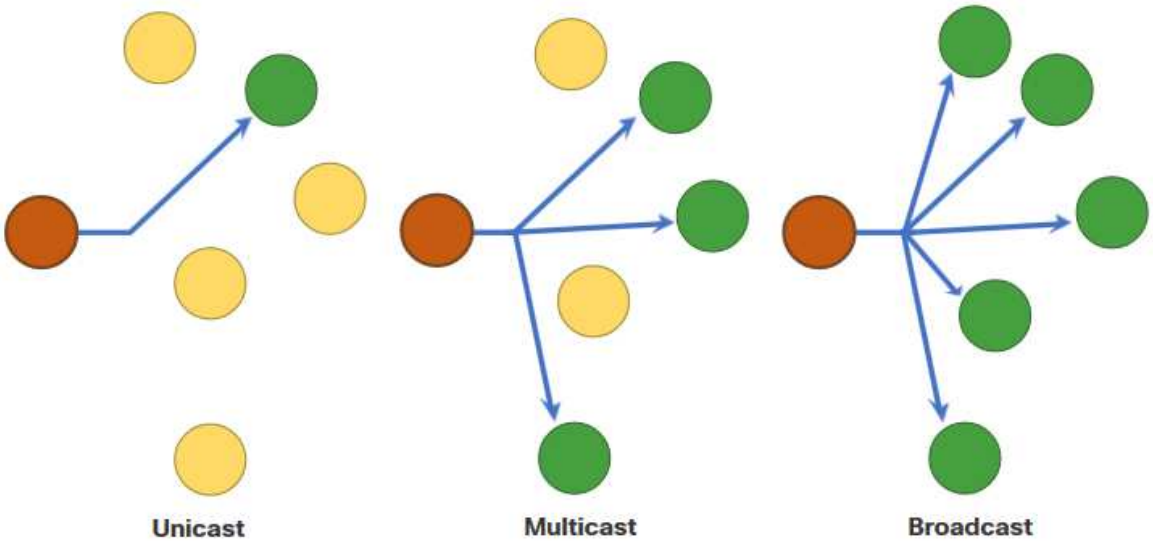




© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Una nota sobre el icono de nodo

- Los documentos pueden utilizar el icono de nodo, normalmente un círculo, para representar todos los dispositivos.
- La figura ilustra el uso del icono de nodo para las opciones de entrega.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

3.2 Protocolos

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Descripción general del protocolo de red

Los protocolos de red definen un conjunto común de reglas.

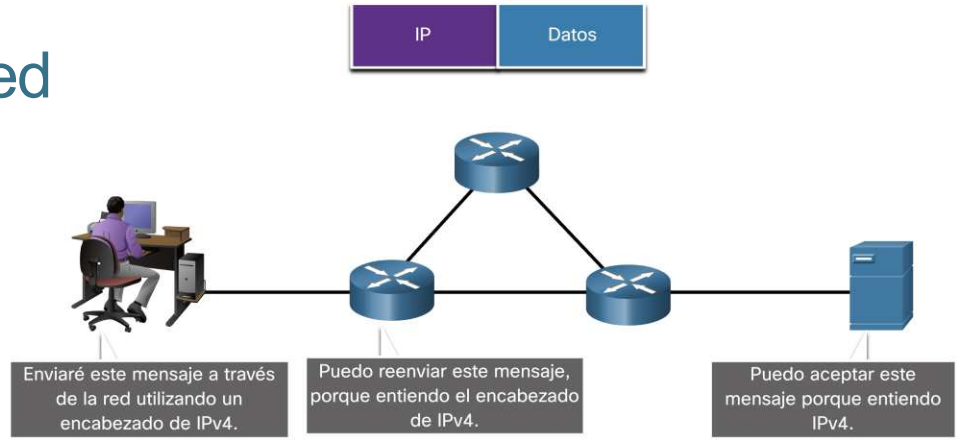
- Pueden ser implemetados en:
  - Software
  - Hardware
  - Ambos
- Cada protocolo tiene:
  - Función
  - Formato
  - Reglas

Tipo de Protocolo	Descripcion
Comunicación de redes	enable two or more devices to communicate over one or more networks
Seguridad de la red	secure data to provide authentication, data integrity, and data encryption
Enrutamiento	permitir que los routers intercambien y comparen información de ruta, con el fin de seleccionar la mejor ruta
Descubrimiento de servicios	para la detección automática de dispositivos o servicios

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Funciones de protocolos de red

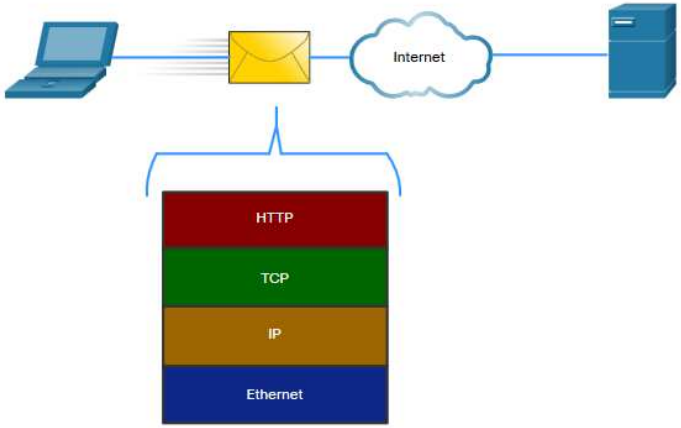
- Devices use agreed-upon protocols to communicate .
- Protocols may have may have one or functions.



Función	Descripción
Direccionamiento	Identificar el origen y el receptor
Fiabilidad	Garantizar la entrega
Control de Flujo	Asegurar que el fujo de los dato a un ritmo eficiente.
Secuenciación	Asignar etiquetas unicas a cada segmento de datos transmitido
Detección de errores	Determinar si los datos se corrompieron durante la transmisión
Interfaz de aplicación	Comunicaciones de proceso a proceso entre aplicaciones de red

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Interacción de protocolos



- Las redes requieren el uso de varios protocolos.
- Cada protocolo tiene su propia función y formato

Protocolo	Función
Hypertext Transfer Protocol (HTTP)	▪ Rige la forma en que interactúan un servidor y un cliente web ▪ Define contenido y formato
Transmission Control Protocol (TCP)	▪ Maneja las conversaciones individuales ▪ Proporciona entrega garantizada ▪ Gestiona el control de flujo
Internet Protocol (IP)	Entrega mensajes globalmente del remitente al receptor
Ethernet	Entrega mensajes de una NIC a otra NIC en la misma red de área local (LAN) Ethernet

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

3.3 Suites de protocolos

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Suites de protocolos de red

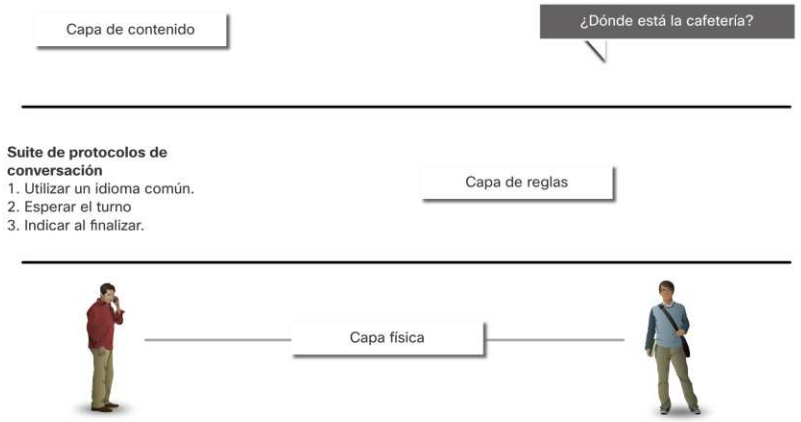
Los protocolos deben poder funcionar con otros protocolos.

Suite de protocolos:

- Un grupo de protocolos necesarios y interrelacionados para realizar una función de comunicación.
- Conjuntos de reglas que funcionan juntas para ayudar a resolver un problema.

Los protocolos se ven en términos de capas:

- Capas superiores
- Capas inferiores: se preocupan por mover datos y proporcionar servicios a las capas superiores



Las suites de protocolos son conjuntos de reglas que funcionan conjuntamente para ayudar a resolver un problema.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Evolución de los conjuntos de protocolos

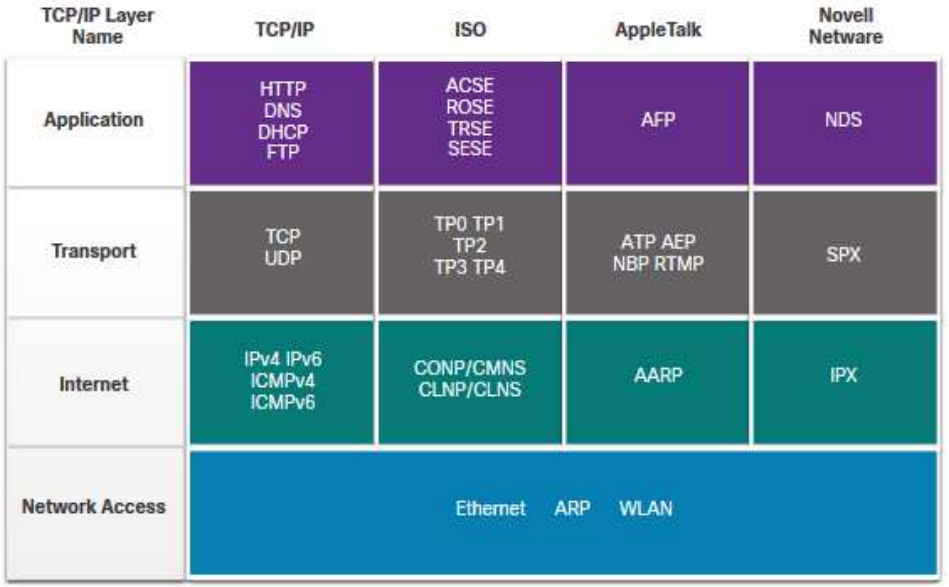
Existene muchos conjuntos de protocolos.

Internet Protocol Suite or TCP/IP - El conjunto de protocolos más común. Es mantenido por Internet Engineering Task Force (IETF)

Open Systems Interconnection (OSI) protocols- Desarrollado por la International Organization for Standardization (ISO) y la International Telecommunications Union (ITU)

AppleTalk-
Conjunto de protocolos propietario desarrollado por Apple Inc.

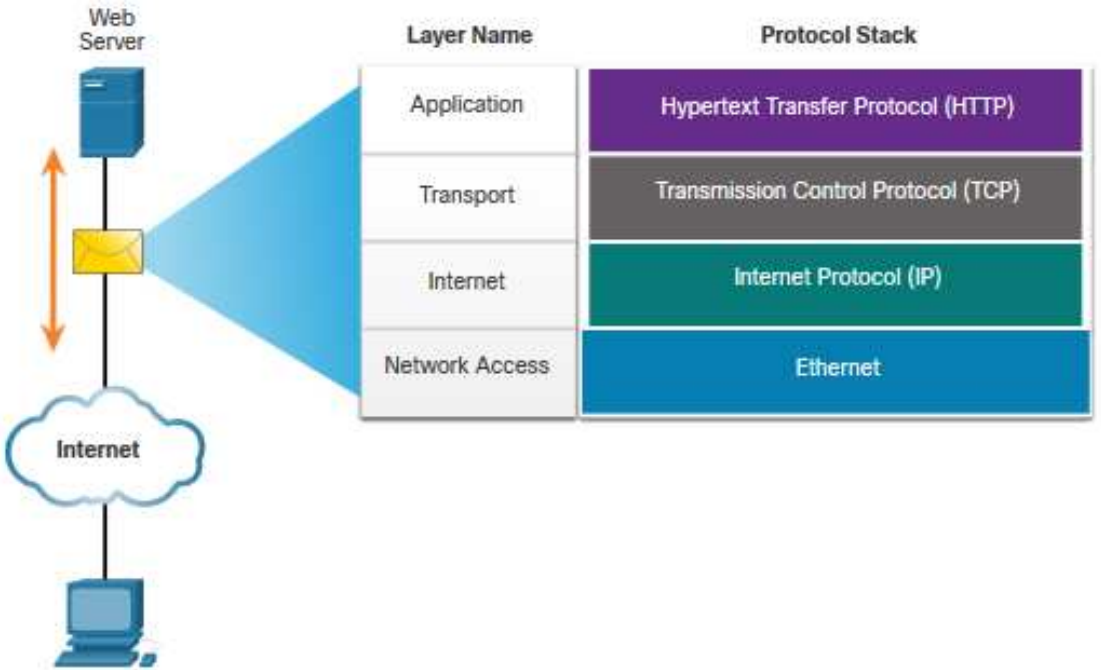
Novell NetWare - Conjunto de protocolos poprietario desarrollado por Novell Inc



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Ejemplo de protocolo TCP/IP

- Los protocolos TCP / IP operan en las capas de aplicación, transporte e Internet.
- Los protocolos LAN de capa de acceso a la red más comunes son Ethernet y WLAN (LAN inalámbrica).



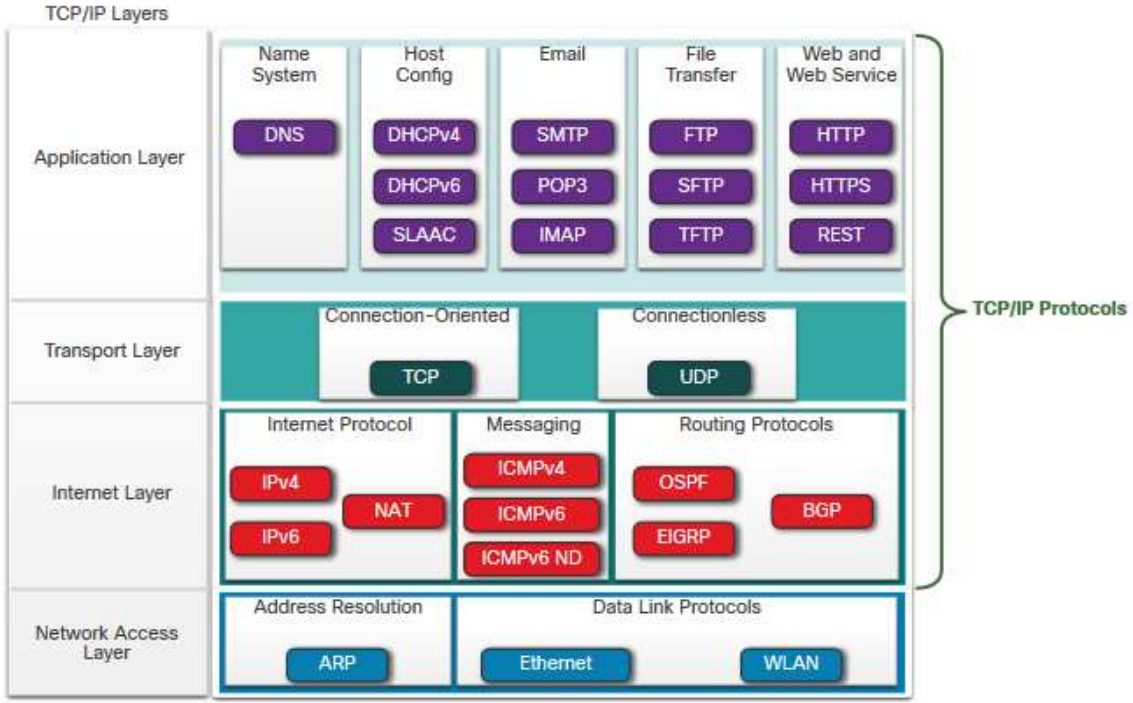
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Conjunto de protocolos TCP/IP

TCP / IP es el conjunto de muchos de protocolos que utiliza Internet

TCP / IP es:

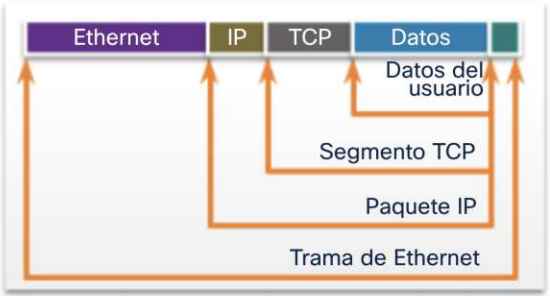
- Un conjunto de protocolos estándar abiertos que está disponible gratuitamente para el público y puede ser utilizado por cualquier proveedor.
- Un conjunto de protocolos basados en estándares respaldados por la industria de las redes y aprobados por una organización de estándares para garantizar la interoperabilidad.

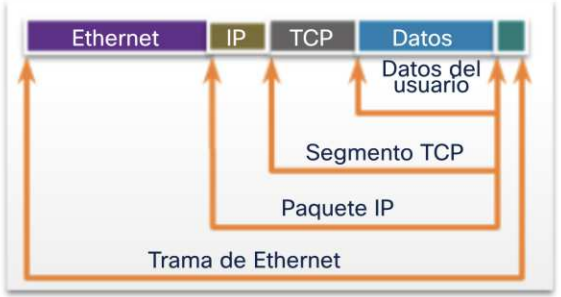


© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Proceso de comunicación TCP/IP

- Un servidor web encapsula y envia una página web a un cliente.
- Un cliente desencapsula la página web para el navegador web.





© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

3.4 Organizaciones de Estándares

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Estándares abiertos

Los estándares abiertos fomentan:

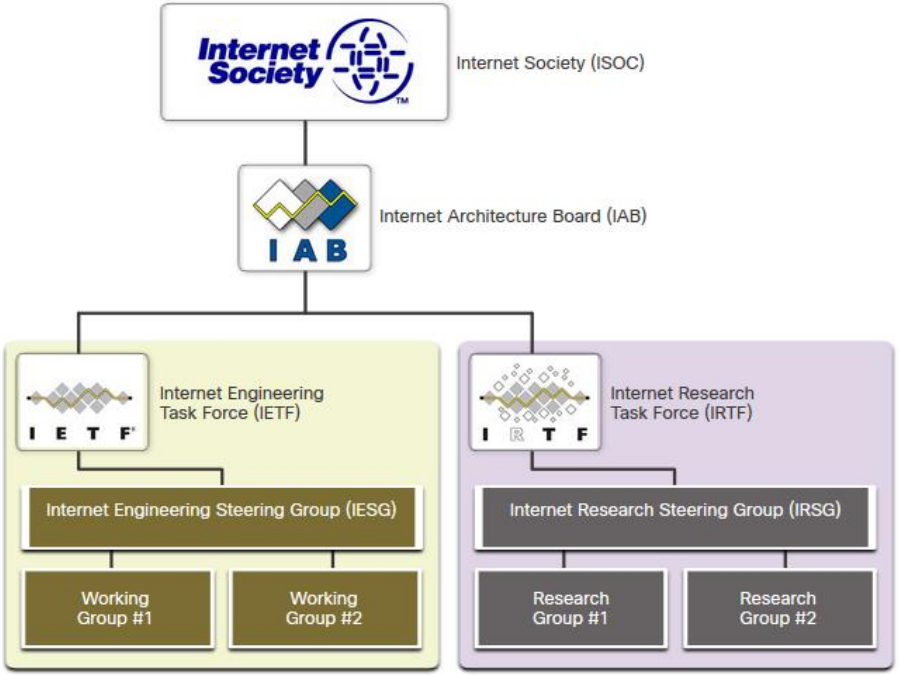
- Interoperabilidad
- Competencia
- innovación

Las organizaciones de normalización son:

- proveedor neutral
- organizaciones sin ánimo de lucro
- establecido para desarrollar y promover el concepto de estándares abiertos.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

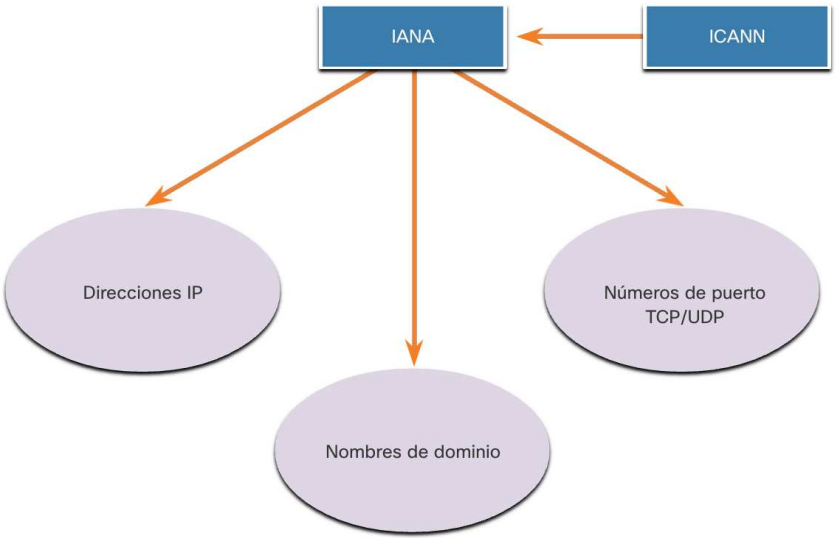
Estándares de Internet



- **Internet Society (ISOC)** - Promueve el desarrollo abierto y el desarrollo de internet
- **Internet Architecture Board (IAB)** - Responsable de la administración y desarrollo de estándares de internet
- **Internet Engineering Task Force (IETF)** - Desarrolla, actualiza y maintiene las tecnologías de internet y TCP/IP
- **Internet Research Task Force (IRTF)** - Se enfoca en la investigación a largo plazo relacionada con internet y TCP/IP

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Estándares de internet (Cont.)



Organizaciones de normalización involucradas en el desarrollo y soporte de TCP / IP

- **Internet Corporation for Assigned Names and Numbers (ICANN)** - Coordina la asignación de direcciones IP, la administración de nombres de dominio y la asignación de otra información
- **Internet Assigned Numbers Authority (IANA)** - supervisa y administra la asignación de direcciones IP, la administración de nombres de dominio y los identificadores de protocolo para ICANN

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Estándares electrónicos y de comunicaciones

- **Institute of Electrical and Electronics Engineers** (**IEEE**, pronunciado “I-triple-E”) - dedicado a crear estándares en potencia y energía, atención médica, telecomunicaciones y redes.
- **Electronic Industries Alliance (EIA)** - desarrolla estándares relacionados con cableado eléctrico, conectores y racks de 19 pulgadas utilizados para montar equipos de red.
- **Telecommunications Industry Association (TIA)** - desarrolla estándares de comunicación en equipos de radio, torres celulares, dispositivos de Voz sobre IP (VoIP), comunicaciones por satélite y más.
- **International Telecommunications Union-Telecommunication Standardization Sector (ITU-T)** - define los estándares para la compresión de video, la televisión por protocolo de Internet (IPTV) y las comunicaciones de banda ancha, como una línea de abonado digital (DSL)

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Lab – Investigación de estándares de redes

En este laboratorio, se realizará lo siguiente:

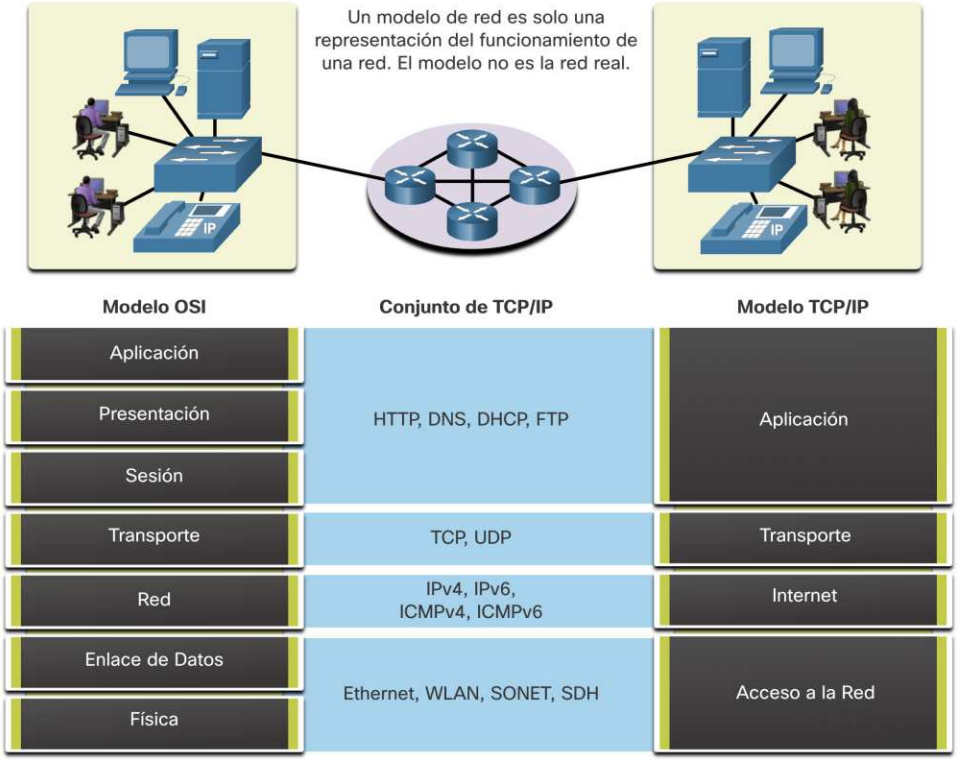
- Parte 1: Investigar sobre organizaciones de estándares de redes
- Parte 2: Reflexionar sobre la experiencia de Internet y las redes informáticas.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

3.5 Modelos de referencia

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Los beneficios de usar un modelo en capas



Los conceptos complejos, como el funcionamiento de una red, pueden resultar difíciles de explicar y comprender. Por esta razón, se utiliza un modelo en capas.

Los modelos de capas describen las operaciones de la red:

- Modelo de referencia de interconexión de sistemas abiertos (OSI)
- Modelo de referencia TCP / IP

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Los beneficios de usar un modelo en capas (Cont.)

Estos son los beneficios de utilizar un modelo en capas:

- Ayudar en el diseño de protocolos porque los protocolos que operan en una capa específica tienen información definida sobre la que actúan y una interfaz definida para las capas superior e inferior.
- Fomentar la competencia porque los productos de diferentes proveedores pueden operar juntos
- Evitar que los cambios de tecnología o capacidad en una capa afecten a otras capas
- Proporcionar un lenguaje común para describir las funciones y capacidades de la red.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

El model de referencia OSI

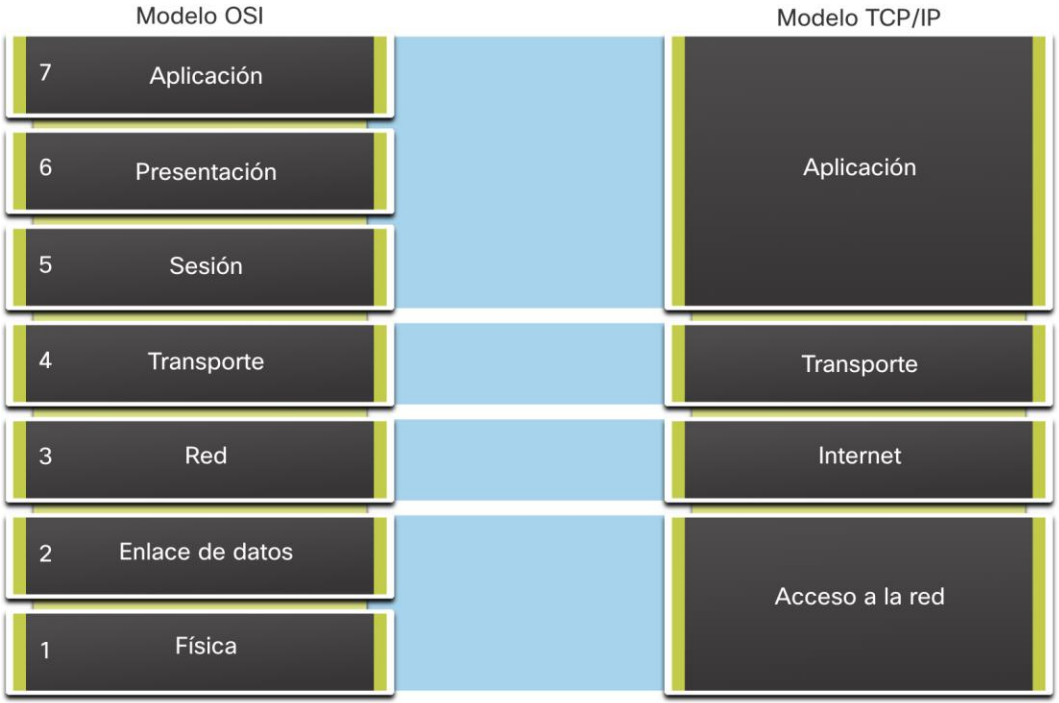
Capas del modelo OSI	Descripción
7 - Aplicación	Contiene protocolos utilizados para las comunicaciones de proceso a proceso.
6 - Presentación	Proporciona una representación común de los datos transferidos entre los servicios de la capa de aplicación.
5 - Sesión	Proporciona servicios a la capa de presentación y gestiona el intercambio de datos.
4 - Transporte	Define servicios para segmentar, transferir y reensamblar los datos para comunicaciones individuales.
3 - Red	Proporciona servicios para intercambiar los datos individuales a través de la red.
2 – Enlace de datos	Describe métodos para intercambiar tramas de datos a través de un medio común.
1 - Física	Describe los medios para activar, mantener y desactivar conexiones físicas.

El model de referencia TCP/IP

Capas del modelo TCP/IP	Description
Aplicación	Representa datos para el usuario, además de codificación y control de diálogo.
Transporte	Admite la comunicación entre distintos dispositivos a través de diversas redes.
Internet	Determina el mejor camino a través de una red.
Acceso a la red	Controla los dispositivos del hardware y los medios que forman la red.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

OSI and TCP/IP Model Comparison



- El modelo OSI divide la capa de acceso a la red y la capa de aplicación del modelo TCP / IP en varias capas.
- El conjunto de protocolos TCP / IP no especifica qué protocolos utilizar al transmitir a través de un medio físico.
- Las capas 1 y 2 de OSI analizan los procedimientos necesarios para acceder a los medios y los medios físicos para enviar datos a través de una red.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Packet Tracer – Investigar los modelos TCP / IP y OSI en acción

Esta actividad de simulación tiene como objetivo proporcionar una base para comprender el conjunto de protocolos TCP / IP y la relación con el modelo OSI. El modo de simulación le permite ver el contenido de los datos que se envían a través de la red en cada capa.

En este Packet Tracer, podrá:

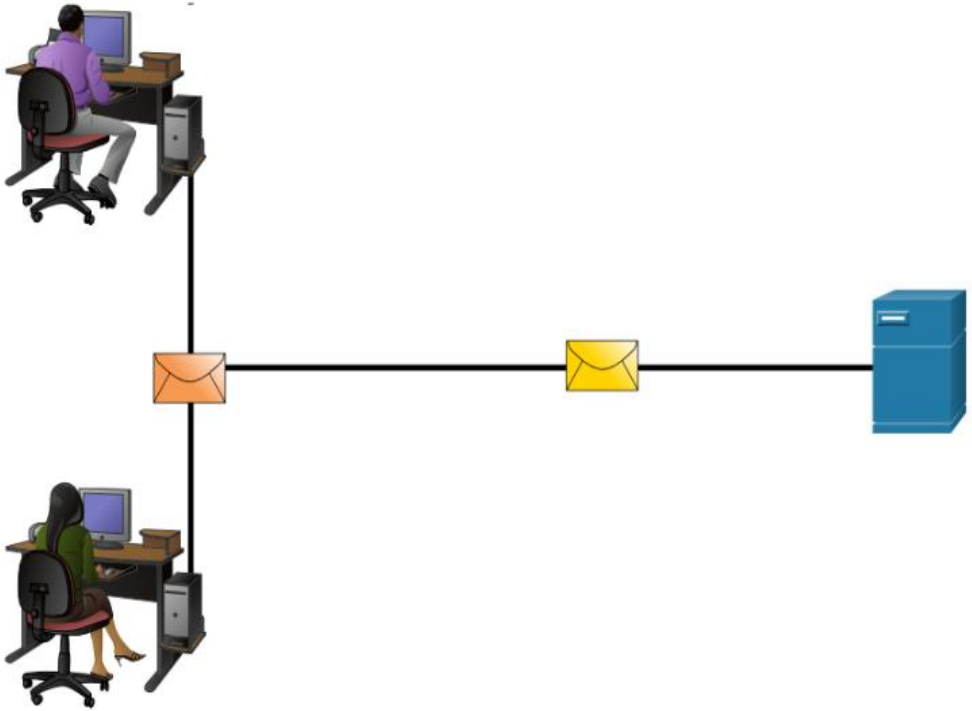
- Parte 1: examinar el tráfico web HTTP
- Parte 2: Mostrar elementos del conjunto de protocolos TCP / IP

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

3.6 Encapsulación de datos

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Segmentación de mensajes



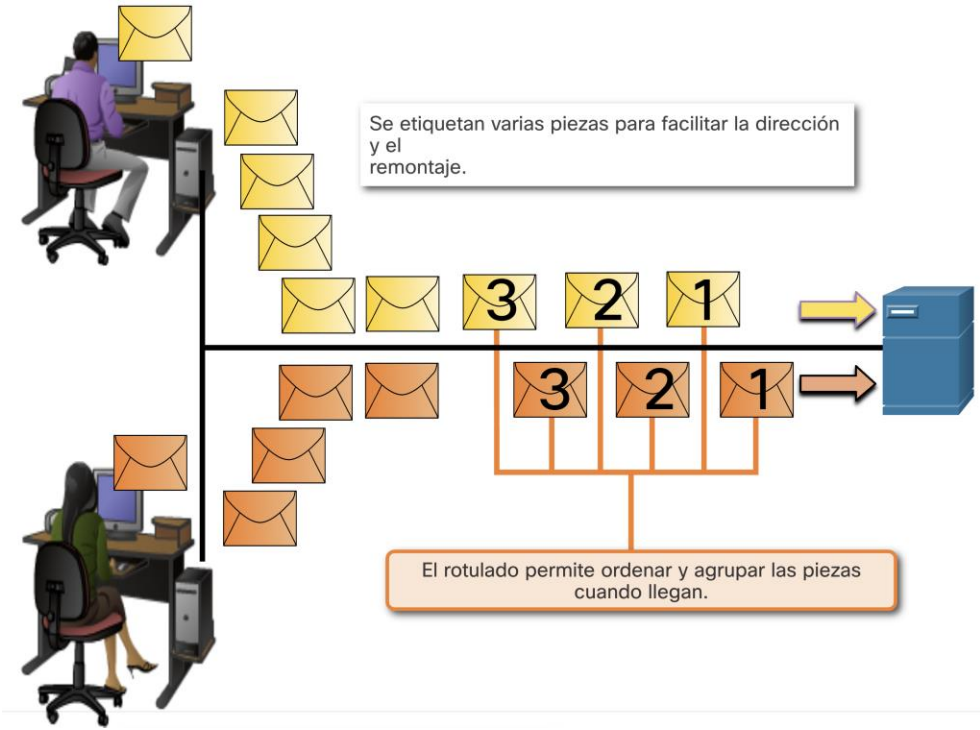
La **segmentación** es el proceso de dividir los mensajes en unidades más pequeñas. La **multiplexación** es el proceso de tomar múltiples flujos de datos segmentados e intercalarlos.

La segmentación de mensajes tiene dos ventajas principales:

- Aumenta la velocidad: se pueden enviar grandes cantidades de datos a través de la red sin inmovilizar un enlace de comunicaciones.
- Aumenta la eficiencia: solo los segmentos que no llegan al destino deben retransmitirse, no todo el flujo de datos.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Secuenciación

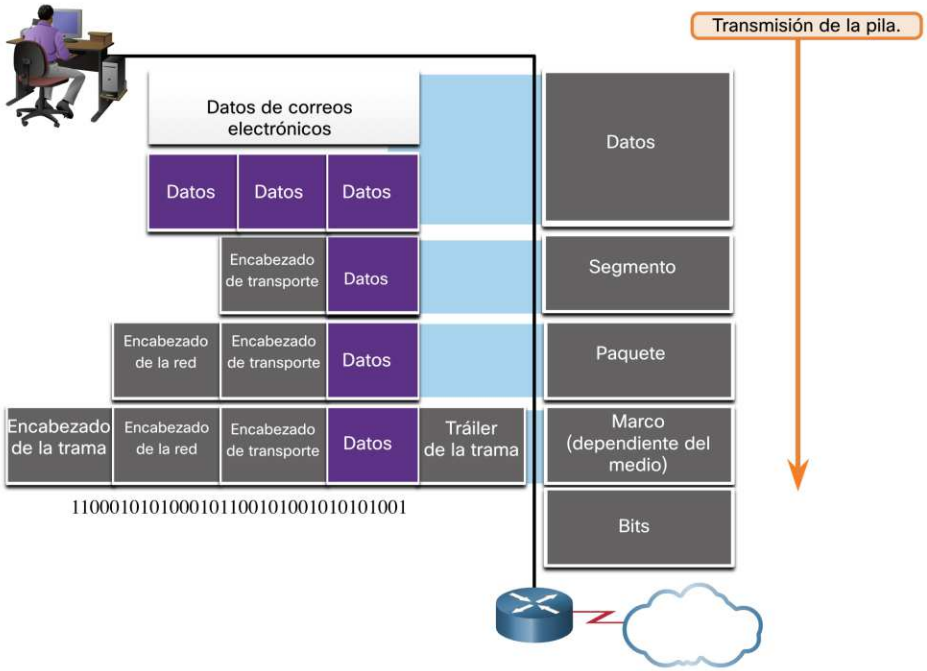


La **secuenciación** de mensajes es el proceso de numerar los segmentos para que el mensaje se pueda reensamblar en el destino.

TCP es el responsable de secuenciar los segmentos individuales.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Protocol Data Units



La **encapsulación** es el proceso en el que los protocolos agregan información a los datos.

En cada etapa del proceso, una PDU tiene un nombre diferente para reflejar sus nuevas funciones.

No existe una convención de nomenclatura universal para las PDU; en este curso, las PDU se nombran de acuerdo con los protocolos de la suite TCP / IP.

Las PDU que pasan por la pila son las siguientes:

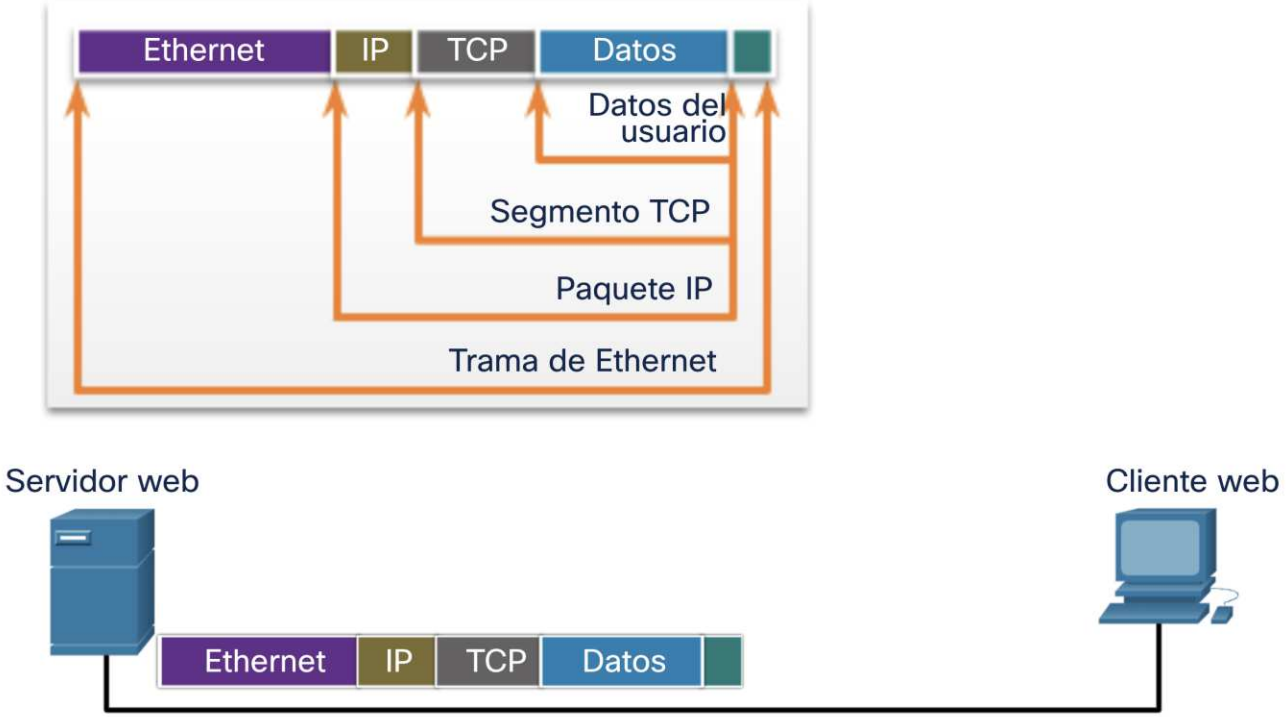
1. Datos (flujo de datos)
2. Segmento
3. Paquete
4. Trama/Marco
5. Bits (flujo de bits)

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Ejemplo de encapsulamiento

- La encapsulación es un proceso de arriba hacia abajo.

- El nivel superior realiza su proceso y luego lo pasa al siguiente nivel del modelo. Este proceso se repite en cada capa hasta que se envía como un flujo de bits.



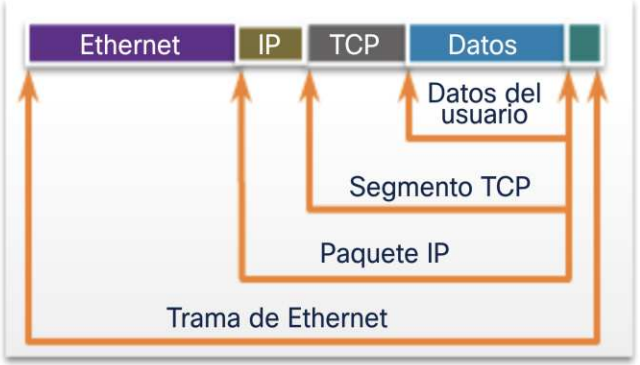
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Ejemplo de desencapsulamiento

Los datos se desencapsulan a medida que ascienden en la pila.

Cuando una capa completa su proceso, esa capa quita su encabezado y lo pasa al siguiente nivel para ser procesado. Esto se repite en cada capa hasta que es un flujo de datos que la aplicación puede procesar.

1. Recibido como bits (flujo de bits)
2. Trama
3. Paquete
4. Segmento
5. Datos (flujo de datos)



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

3.7 Acceso a los datos

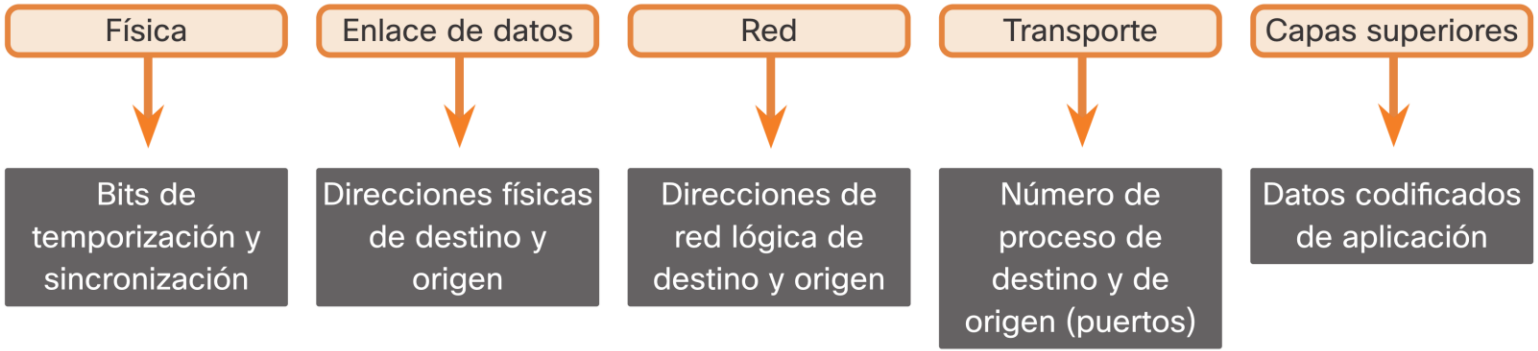
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Direcciones

Tanto el enlace de datos como las capas de red utilizan el direccionamiento para entregar datos desde el origen al destino.

Direcciones de origen y destino de la capa de red: responsable de entregar el paquete IP desde el origen original hasta el destino final.

Direcciones de origen y destino de la capa de enlace de datos: responsable de entregar la trama de enlace de datos desde una tarjeta de interfaz de red (NIC) a otra NIC en la misma red.



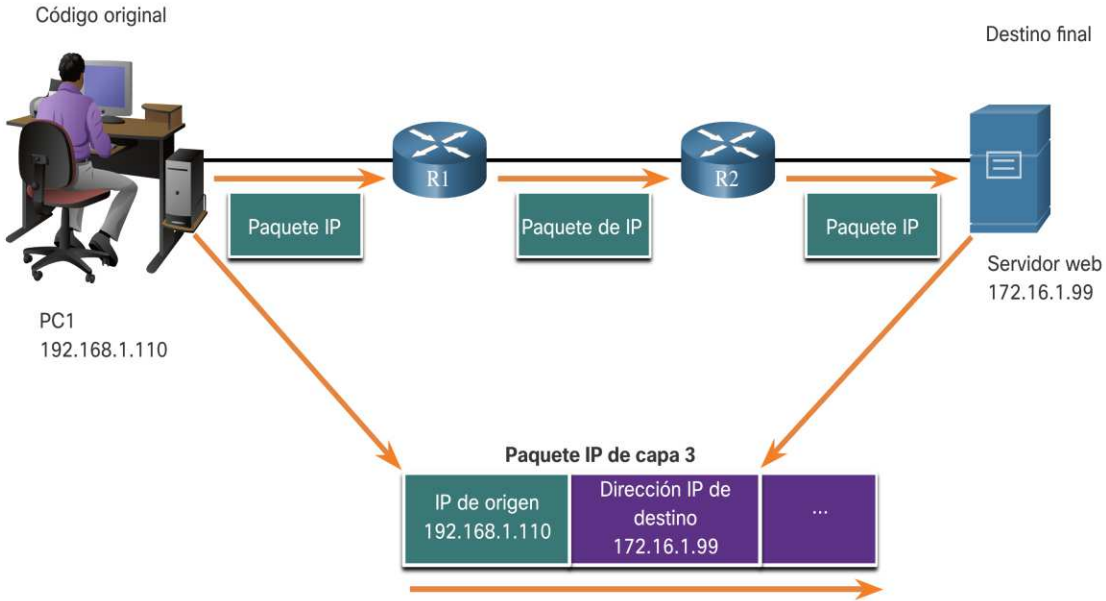
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Dirección lógica de capa 3

El paquete IP contiene dos direcciones IP:

- **Dirección IP de origen**: la dirección IP del dispositivo de envío, origen original del paquete.
- **Dirección IP de destino**: la dirección IP del dispositivo receptor, destino final del paquete.

Estas direcciones pueden estar en el mismo enlace o ser remotas.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Dirección lógica de capa 3 (Cont.)

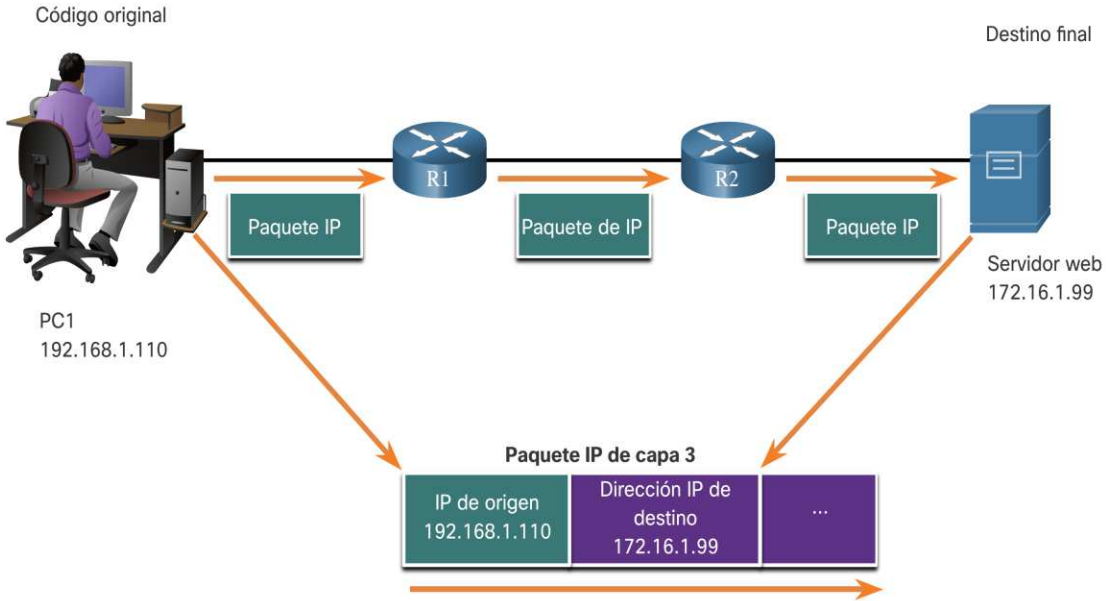
Una dirección IP contiene dos partes:

Porción de red (IPv4) o prefijo (IPv6)

- La parte más a la izquierda de la dirección indica el grupo de red del cual la dirección IP es miembro.
- Cada LAN o WAN tendrá la misma porción de red.

Porción de host (IPv4) o ID de interfaz (IPv6)

- La parte restante de la dirección identifica un dispositivo específico dentro del grupo.
- Esta porción es única para cada dispositivo de la red.

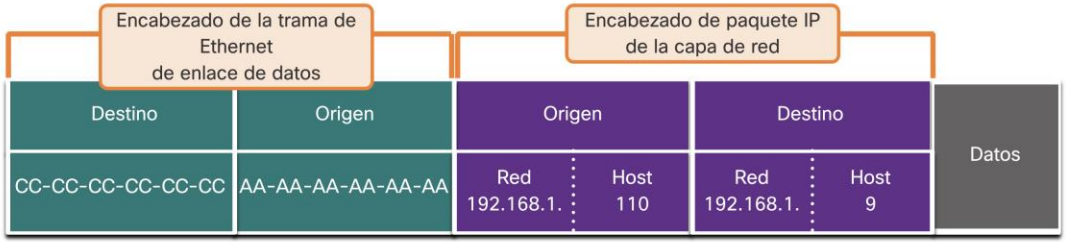


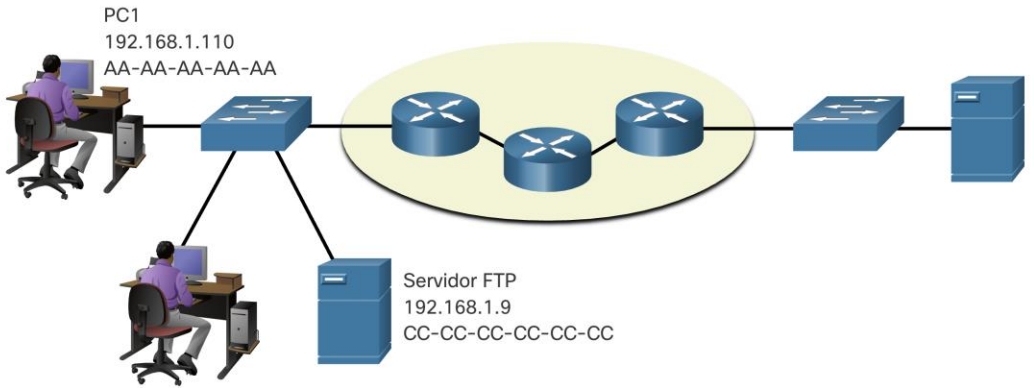
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Dispositivos en la misma red

Cuando los dispositivos están en la misma red, el origen y el destino tendrán el mismo número en la parte de red de la dirección.

- PC1 – 192.168.1.110
- FTP Server – 192.168.1.9





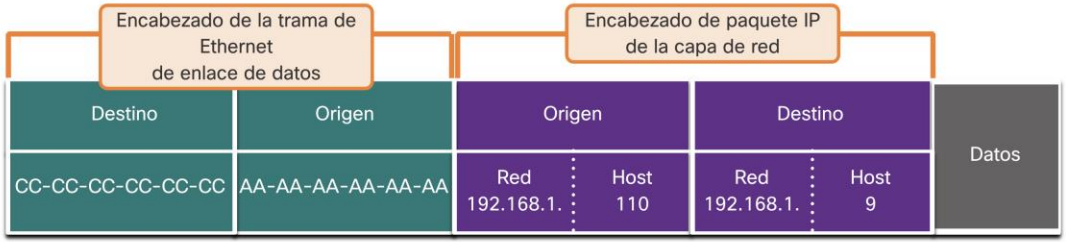
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

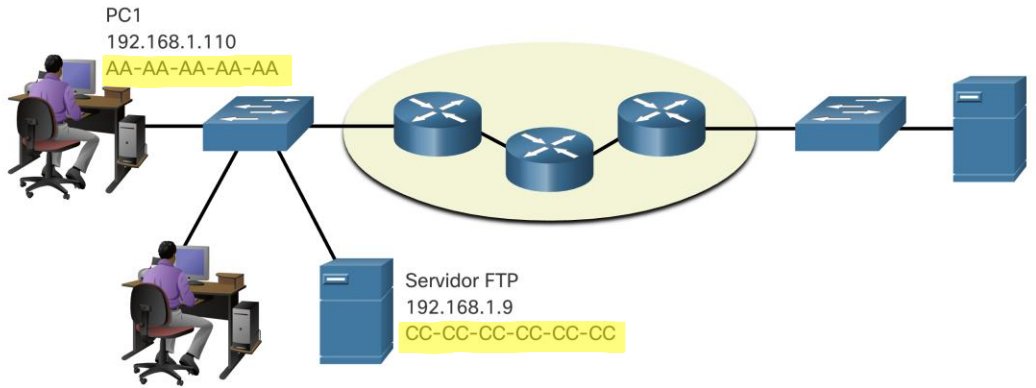
Rol de las direcciones de la capa de enlace de datos: la misma red IP

Cuando los dispositivos están en la misma red Ethernet, la trama de enlace de datos utilizará la dirección MAC real de la NIC de destino.

Las direcciones MAC están integradas físicamente en la NIC Ethernet y son direcciones locales.

- La dirección MAC de origen será la del originador en el enlace.
- La dirección MAC de destino siempre estará en el mismo enlace que la fuente, incluso si el destino final es remoto.

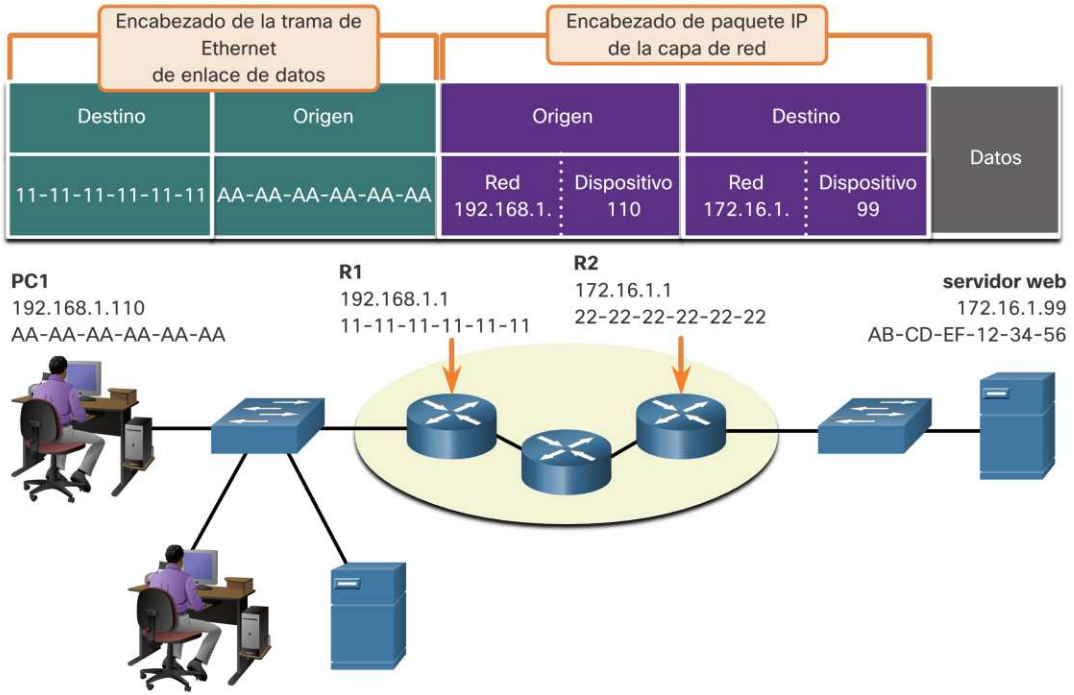




© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Dispositivos en una red remota

- ¿Qué sucede cuando el destino real (último) no está en la misma LAN y es remoto?
- ¿Qué sucede cuando la PC1 intenta acceder al servidor web?
- ¿Afecta esto a las capas de red y enlace de datos?

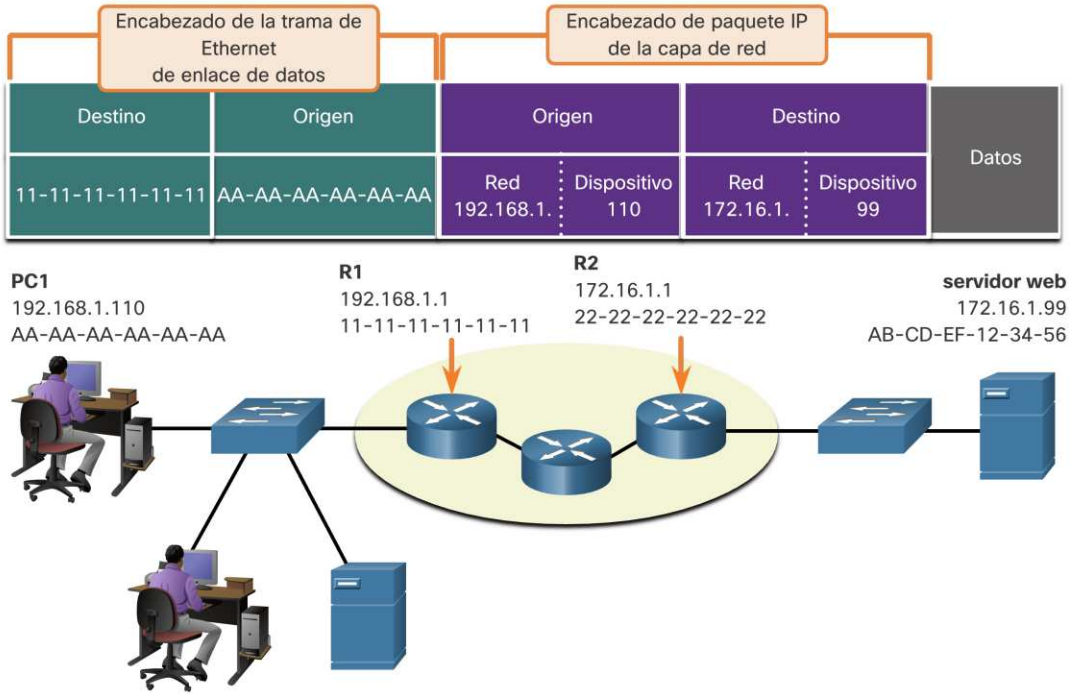


© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Rol de las direcciones de la capa de red

Cuando el origen y el destino tienen una porción de red diferente, esto significa que están en redes diferentes.

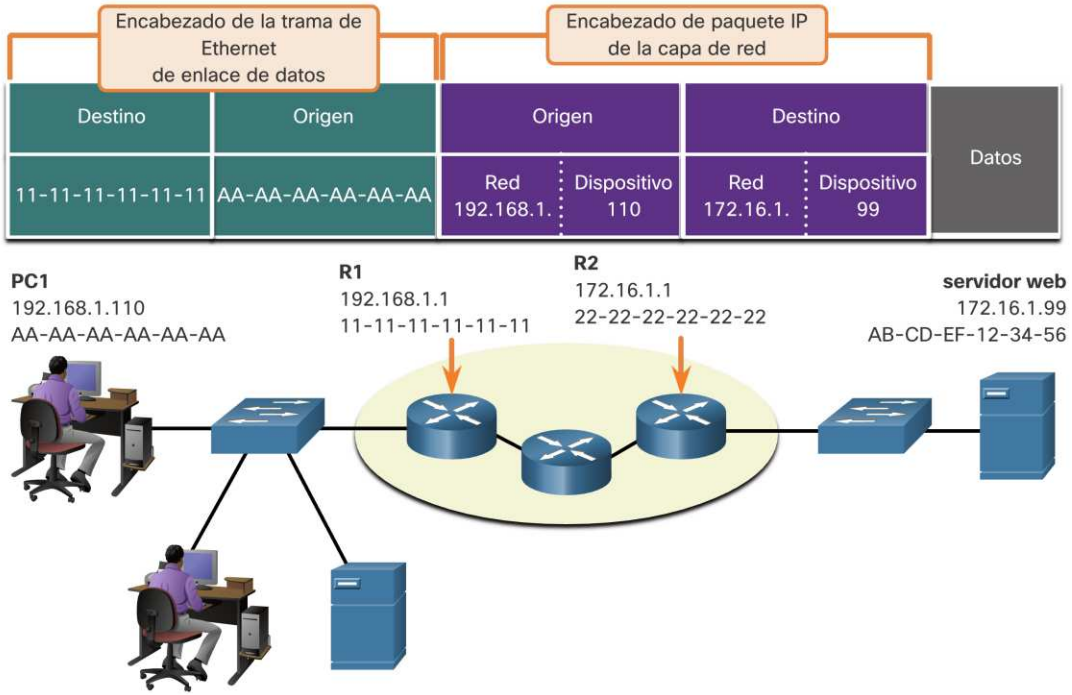
- PC1 - 192.168.1
- Servidor web - 172.16.1



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Rol de acceso a datos de las direcciones de capa de vínculo de datos: diferentes redes IP

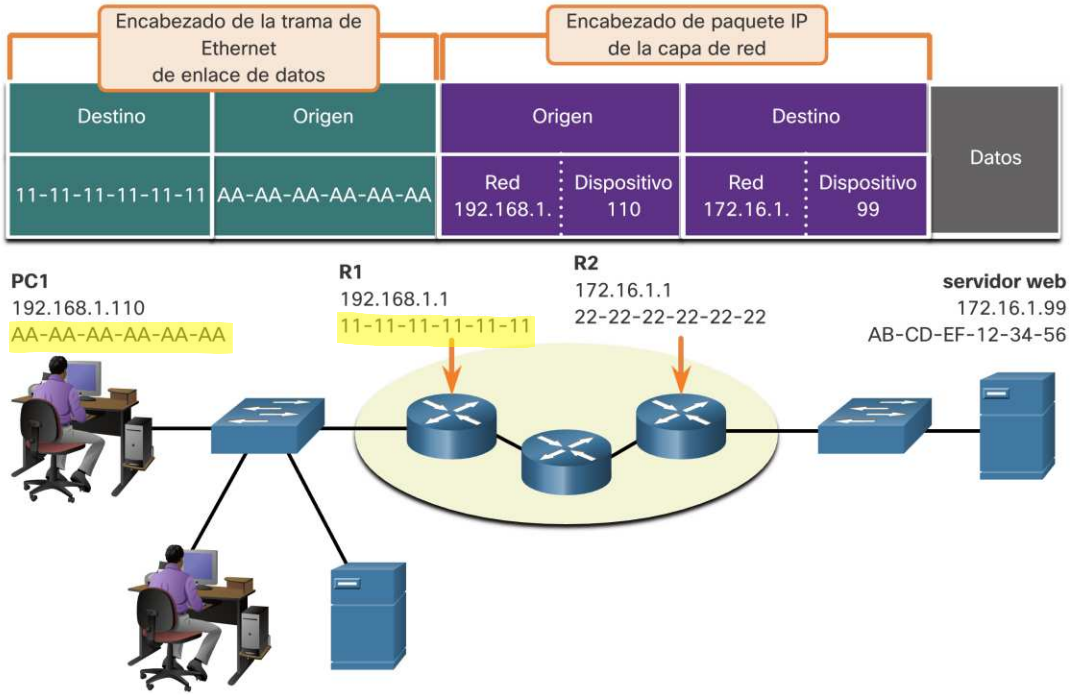
- Cuando el destino final es remoto, la Capa 3 proporcionará a la Capa 2 la dirección IP de la puerta de enlace predeterminada local (enrutador).
- La puerta de enlace predeterminada (DGW) es la dirección IP de la interfaz del enrutador que forma parte de esta LAN y será la "puerta de enlace" a todas las demás ubicaciones remotas.
- Todos los dispositivos de la LAN deben conocer esta dirección o su tráfico se limitará únicamente a la LAN.
- Una vez que la capa 2 en la PC1 se reenvía a la puerta de enlace predeterminada, este puede comenzar el proceso de enrutamiento para llevar la información al destino real.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Rol de acceso a datos de las direcciones de capa de vínculo de datos: diferentes redes IP (Cont.)

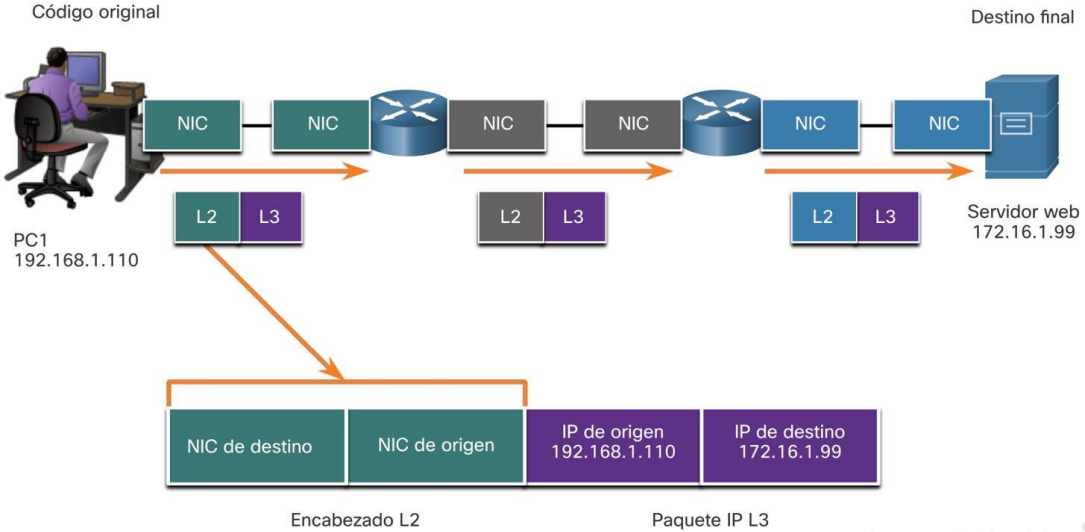
- El direccionamiento del enlace de datos es local, por lo que tendrá una fuente y un destino para cada enlace.
- El **direccionamiento MAC** para el primer segmento es:
  - **Fuente:** AA-AA-AA-AA-AA-AA (PC1) Envía el marco.
  - **Destino:** 11-11-11-11-11-11 (R1- MAC de puerta de enlace predeterminada) Recibe la trama.
- **Nota:** Si bien el direccionamiento local L2 cambiará de un enlace a otro o de un salto a otro, el direccionamiento L3 sigue siendo el mismo.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Direcciones de enlace de datos

- Dado que el direccionamiento del enlace de datos es un direccionamiento local, tendrá un origen y un destino para cada segmento o salto del viaje al destino.
- El direccionamiento MAC para el primer segmento es:
  - Fuente: (PC1 NIC) envía la trama
  - Destino: (primer enrutador: interfaz DGW) recibe la trama

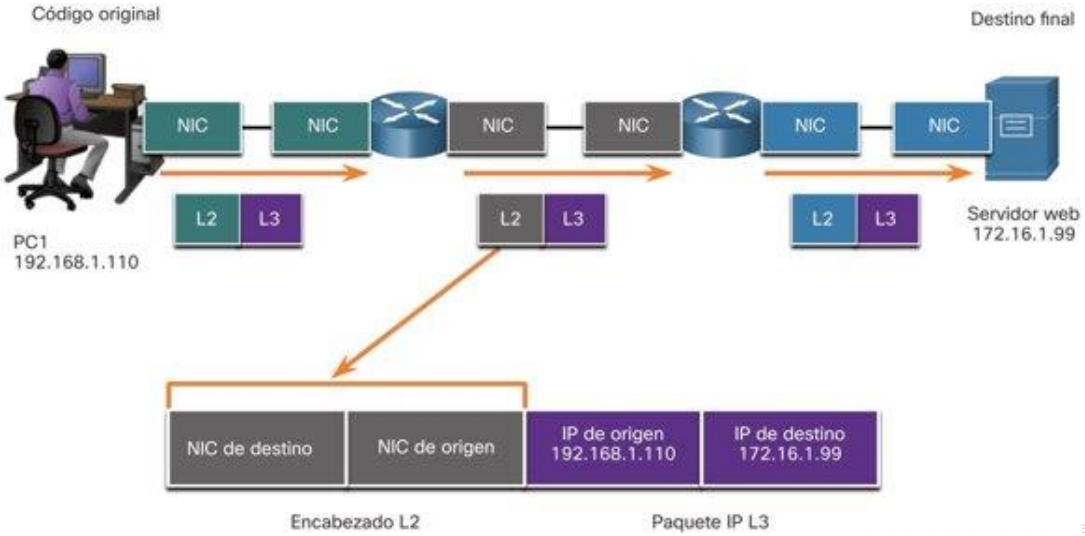


es. All rights reserved. Cisco Confidential

Direcciones de enlace de datos (Cont.)

El direccionamiento MAC para el segundo salto es:

- Fuente: (primer enrutador: interfaz de salida) envía la trama
- Destino: (segundo enrutador) recibe la tra

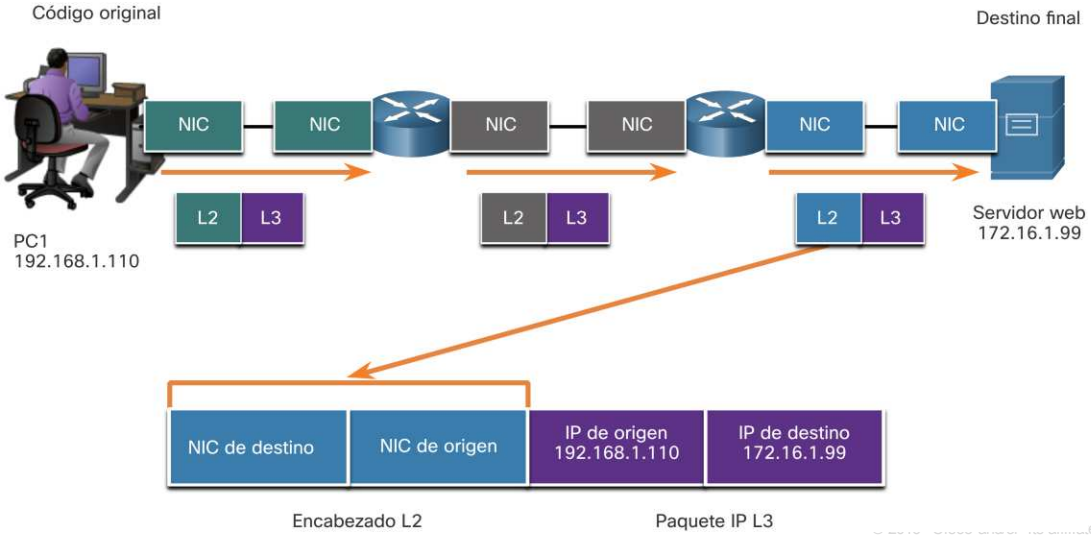


es. All rights reserved. Cisco Confidential

Direcciones de enlace de datos (Cont.)

El direccionamiento MAC para el último segmento es:

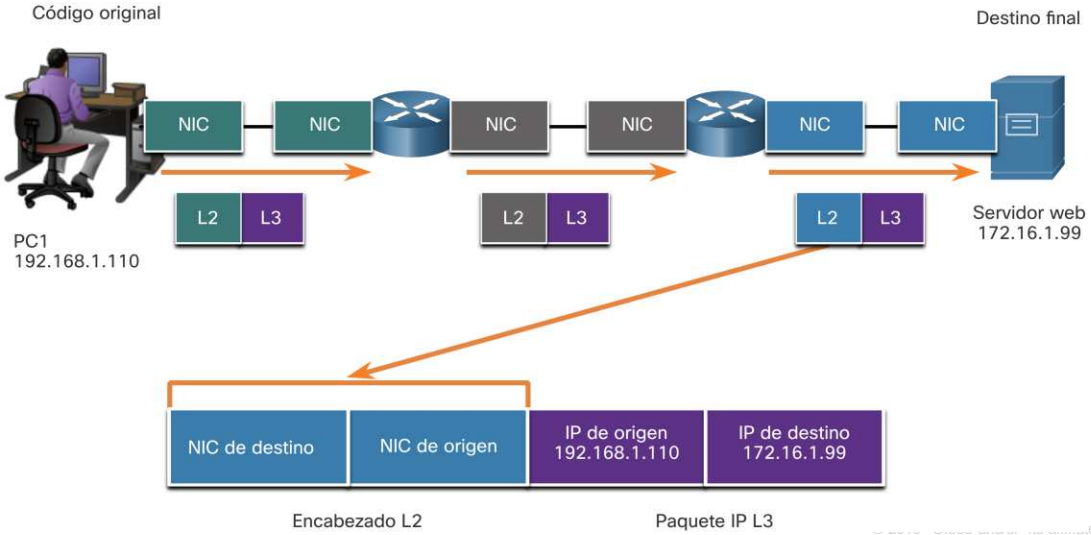
- Fuente: (segundo enrutador: interfaz de salida) envía la trama
- Destino: (NIC del servidor web) recibe el marco



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Direcciones de enlace de datos (Cont.)

- Observe que el paquete no se modifica, pero la trama se cambia, por lo tanto, el direccionamiento IP L3 no cambia de segmento a segmento como el direccionamiento MAC L2.
- El direccionamiento L3 sigue siendo el mismo, ya que es global y el destino final siempre es servidor web.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Lab – Instalar Wireshark

En esta actividad de aboratorio, hará lo siguiente:

- Descargue e instale Wireshark

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Lab – Uso de Wireshark para ver el tráfico de la red

En este laboratorio, hará lo siguiente:

- Parte 1: capturar y analizar datos ICMP locales en Wireshark
- Parte 2: capturar y analizar datos ICMP remotos en Wireshark

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

3.8 Practica de laboratorio y Cuestionario

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

¿Qué aprendí en este módulo?

Las reglas

- Los protocolos deben tener un remitente y un receptor.
- Los protocolos informáticos comunes incluyen estos requisitos: codificación, formato y encapsulación de mensajes, tamaño, tiempo y opciones de entrega.

Protocolos

- Para enviar un mensaje a través de la red se requiere el uso de varios protocolos.
- Cada protocolo de red tiene su propia función, formato y reglas para las comunicaciones.
- Suites de protocolo
- Un conjunto de protocolos es un grupo de protocolos interrelacionados.
- El conjunto de protocolos TCP / IP son los protocolos que se utilizan en la actualidad.

Organizaciones de estándares

- Los estándares abiertos fomentan la interoperabilidad, la competencia y la innovación.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

¿Qué aprendí en este módulo? (Cont.)

Modelos de referencia

- Los dos modelos utilizados en redes son el modelo TCP / IP y el modelo OSI.
- El modelo TCP / IP tiene 4 capas y el modelo OSI tiene 7 capas.

Encapsulación de datos

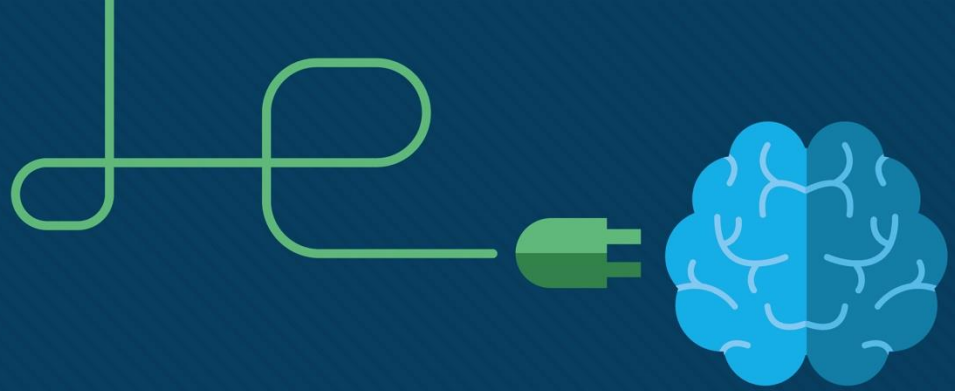
- La forma que toma un dato en cualquier capa se denomina unidad de datos de protocolo (PDU).
- Hay cinco PDU diferentes que se utilizan en el proceso de encapsulación de datos: datos, segmento, paquete, trama y bits

Acceso a los datos

- Las capas de red y enlace de datos proporcionarán direccionamiento para mover datos a través de la red.
- La capa 3 proporcionará direccionamiento IP y la capa 2 proporcionará direccionamiento MAC.
- La forma en que estas capas manejan el direccionamiento dependerá de si la fuente y el destino están en la misma red o si el destino está en una red diferente de la fuente.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential


CISCO



Módulo 4: Capa física

Introducción a redes

Objetivos

Tema: Capa física

Objetivo: Explain how physical layer protocols, services, and network media support communications across data networks.

Tema	Objetivo
Propósito de la capa física	Describa el propósito y las funciones de la capa física en la red.
Características de la capa física	Describa las características de la capa física
Cableado de cobre	Identifique las características básicas del cableado de cobre.
Cableado UTP	Explique cómo se utiliza el cable UTP en las redes Ethernet.
Cableado de fibra óptica	Describir el cableado de fibra óptica y sus ventajas principales sobre otros medios.
Medios inalámbricos	Conecte dispositivos utilizando medios conectados por cable e inalámbricos.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

4.1 Propósito de capa física

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

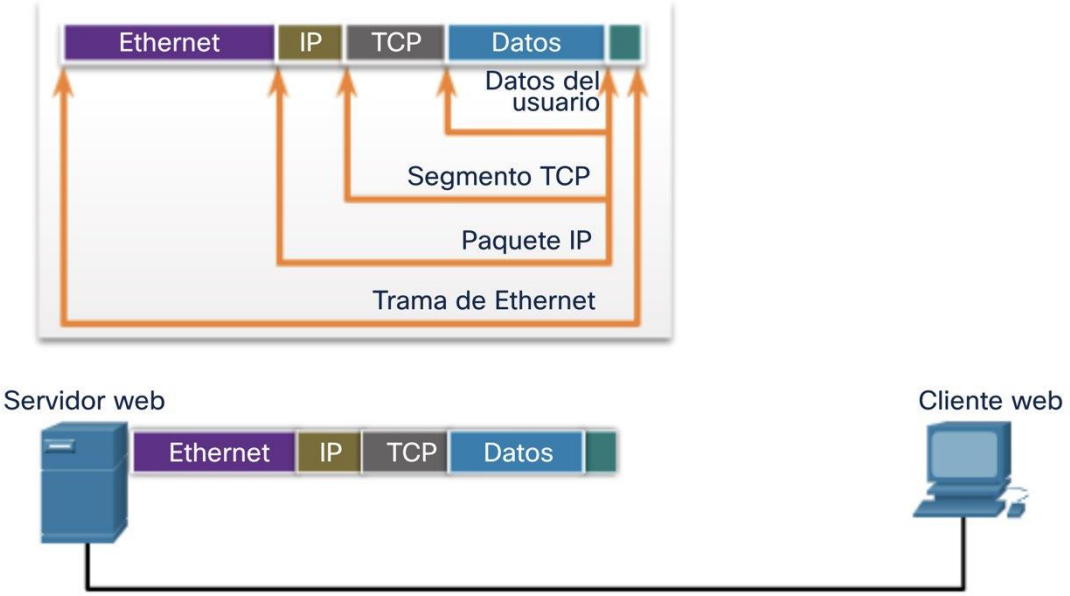
Conexión física

- Antes de que se pueda establecer una comunicación de red, se debe tener una conexión física a una red local.
- Esta conexión puede ser por cable o inalámbrica, según la configuración de la red.
- Esto generalmente aplica si se está considerando una oficina corporativa o un hogar.
- Una tarjeta de interfaz de red (NIC) que conecte un dispositivo a la red.
- Algunos dispositivos pueden tener solo una NIC, mientras que otros pueden tener varias (cableadas e inalámbricas, por ejemplo).
- No todas las conexiones físicas ofrecen el mismo nivel de rendimiento.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

La capa fisica

- Transporta bits a través de los medios de red.
- Acepta una trama completa de la capa de enlace de datos y la codifica como una serie de señales que se transmiten a los medios locales.
- Este es el último paso del proceso de encapsulación.
- El siguiente dispositivo en la ruta hacia el destino recibe los bits y vuelve a encapsular la trama, luego decide qué hacer con ella.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

4.2 Características de la capa física

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Características de la capa física
Physical Layer Standards

Los estándares TCP/IP se implementan en software, y los rige la IETF.

Los estándares de la capa física se implementan en hardware, y los rigen diversos organismos, incluidos los siguientes:

- ISO
- EIA/TIA
- ITU-T
- ANSI
- IEEE

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Componentes físicos

Los estándares de la capa física abordan tres áreas funcionales:

- Componentes físicos
- Codificación
- Señalización

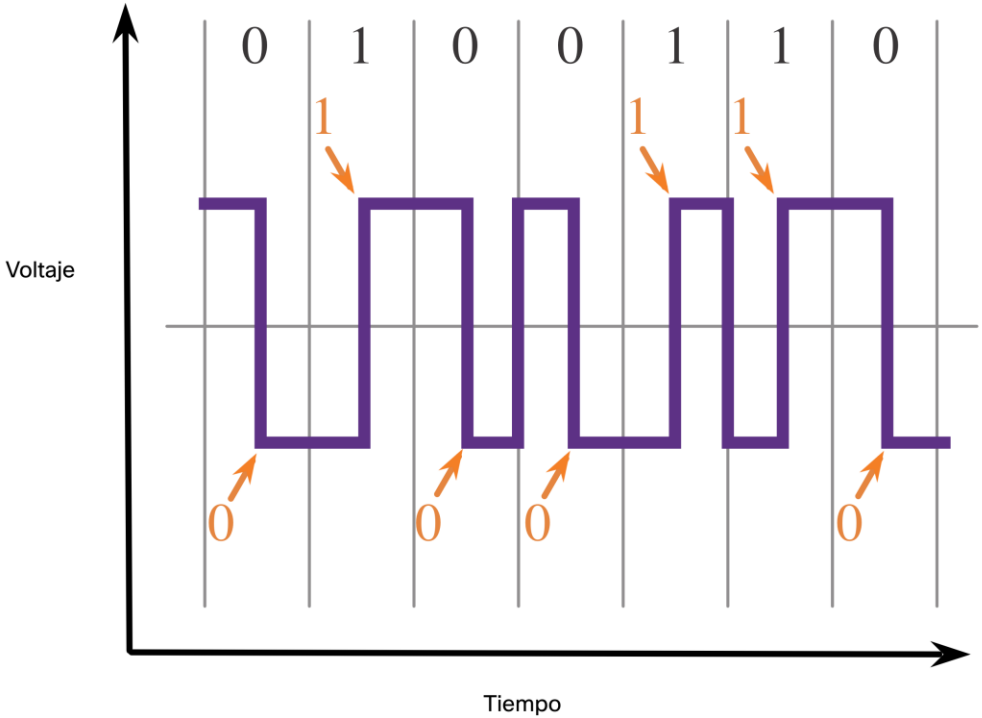
Los componentes físicos son los dispositivos de hardware, los medios y otros conectores que transportan las señales que representan los bits.

Los componentes de hardware, como las NIC, las interfaces y los conectores, los materiales de los cables y los diseños de los cables, se especifican en los estándares asociados con la capa física.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Codificacón

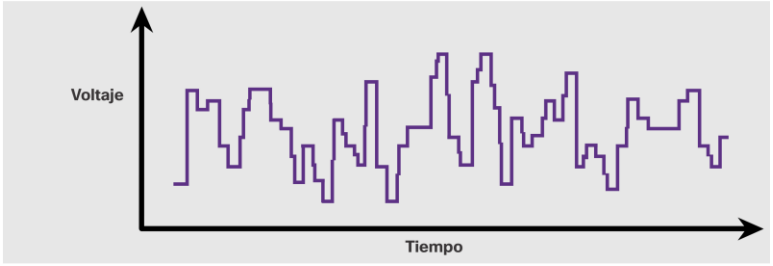
- La codificación convierte el flujo de bits en un formato reconocible por el siguiente dispositivo en la ruta de la red.
- Esta "codificación" proporciona patrones predecibles que pueden ser reconocidos.
- Los ejemplos de métodos de codificación incluyen Manchester (que se muestra en la figura), 4B / 5B y 8B / 10B.



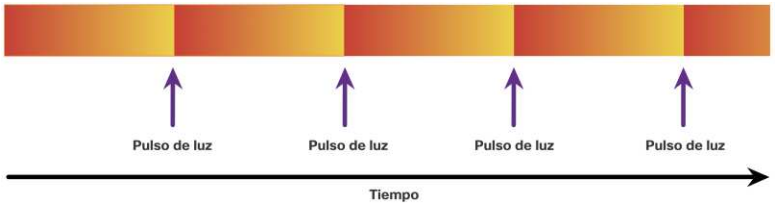
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Señalización

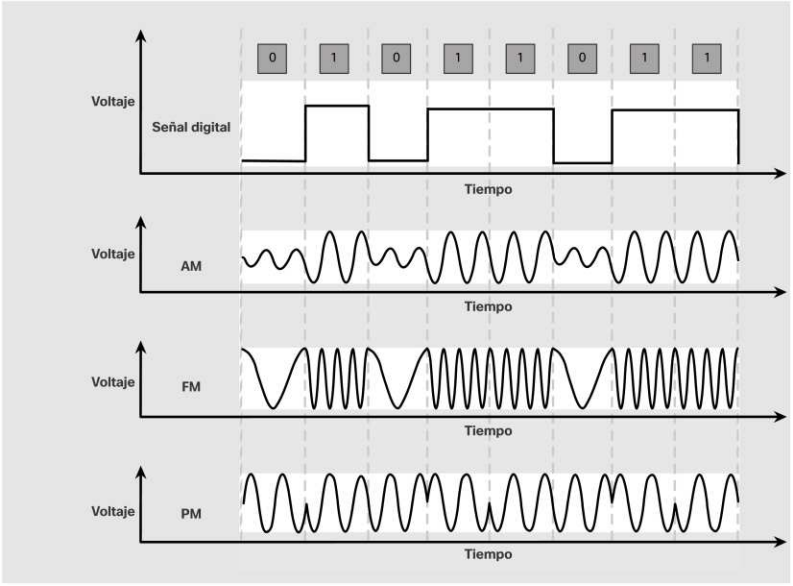
- El método de señalización es cómo se representan los valores de bit, "1" y "0" en el medio físico.
- El método de señalización variará según el tipo de medio utilizado.



Señalez eléctricas sobre cable de cobre



Pulsos de luz sobre cable Fibra Óptica



Señales de microndas sobre medios inalámbricos

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Ancho de banda

- El ancho de banda es la capacidad a la que un medio puede transportar datos.
- El ancho de banda digital mide la cantidad de datos que pueden fluir de un lugar a otro en un período de tiempo determinado; cuántos bits se pueden transmitir en un segundo.
- Las propiedades de los medios físicos, las tecnologías actuales y las leyes de la física juegan un papel en la determinación del ancho de banda disponible.

Unidad de ancho de banda	Abreviación	Equivalencia
Bits por segundo	bps	1 bps = unidad fundamental de ancho de banda
Kilobits por segundo	Kbps	1 Kbps = 1,000 bps = 10^3 bps
Megabits por segundo	Mbps	1 Mbps = 1,000,000 bps = 10^6 bps
Gigabits por segundo	Gbps	1 Gbps – 1,000,000,000 bps = 10^9 bps
Terabits por segundo	Tbps	1 Tbps = 1,000,000,000,000 bps = 10^{12} bps

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Terminología del ancho de banda

Latencia

- Cantidad de tiempo, incluidos los retrasos, para que los datos viajen de un punto determinado a otro

Rendimiento

- La medida de la transferencia de bits a través de los medios durante un período de tiempo determinado.

Goodput (Capacidad de transferencia útil)

- La medida de los datos utilizables transferidos durante un período de tiempo determinado.
- Goodput = rendimiento - sobrecarga de tráfico

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

4.3 Cableado de cobre

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Características de la capa física

El cableado de cobre es el tipo de cableado más comunmente utilizado en las redes en la actualidad. Es económico, fácil de instalar y tiene baja resistencia al flujo de corriente eléctrica.

Limitaciones:

- **Atenuación:** cuanto más tiempo tienen que viajar las señales eléctricas, más débiles se vuelven.
- La señal eléctrica es susceptible a la interferencia, que pueden distorsionar y corromper las señales de datos (Interferencia electromagnética (EMI) e Interferencia de radiofrecuencia (RFI) y Crosstalk).

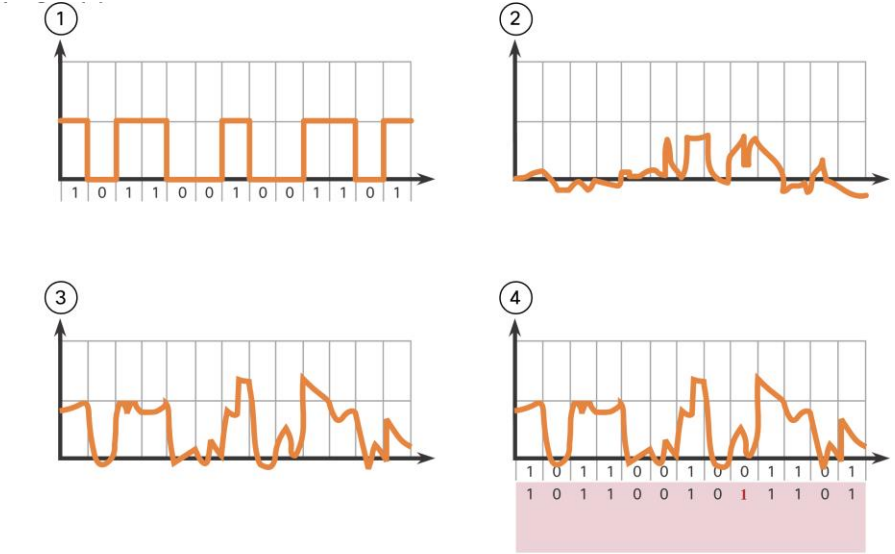
Mitigación:

- El estricto cumplimiento de los límites de longitud del cable mitigará la atenuación.
- Algunos tipos de cable de cobre mitigan las EMI y RFI mediante el uso de blindaje metálico y conexión a tierra.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Características de la capa física (Cont)

La señal eléctrica es susceptible a la interferencia, que pueden distorsionar y corromper las señales de datos (Interferencia electromagnética (EMI) e Interferencia de radiofrecuencia (RFI) y Crosstalk).



1. Se transmite una señal digital pura
2. En el medio, hay una señal de interferencia
3. La señal digital está dañada por la señal de interferencia.
4. El equipo receptor lee una señal cambiada. Observe que un bit 0 ahora se interpreta como un bit 1.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Tipos de cableado de cobre

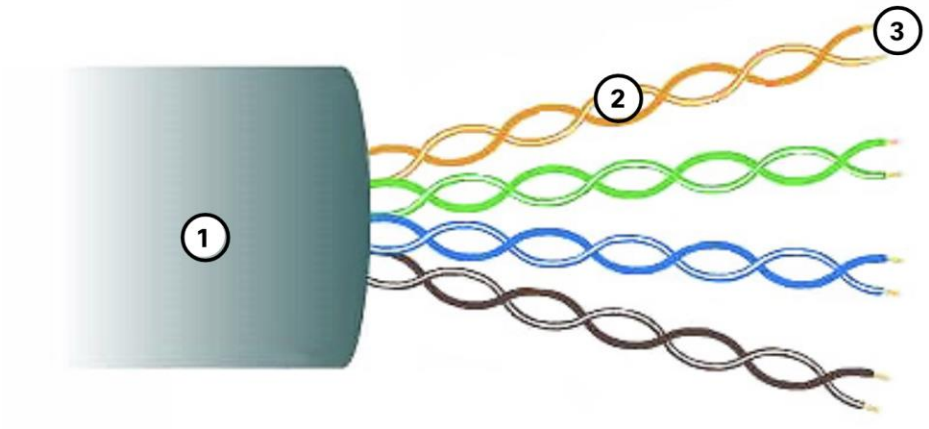
Cable de par trenzado no blindado (UTP)

Cable de par trenzado blindado (STP)

Cable coaxial

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Par trenzado no blindado (UTP)

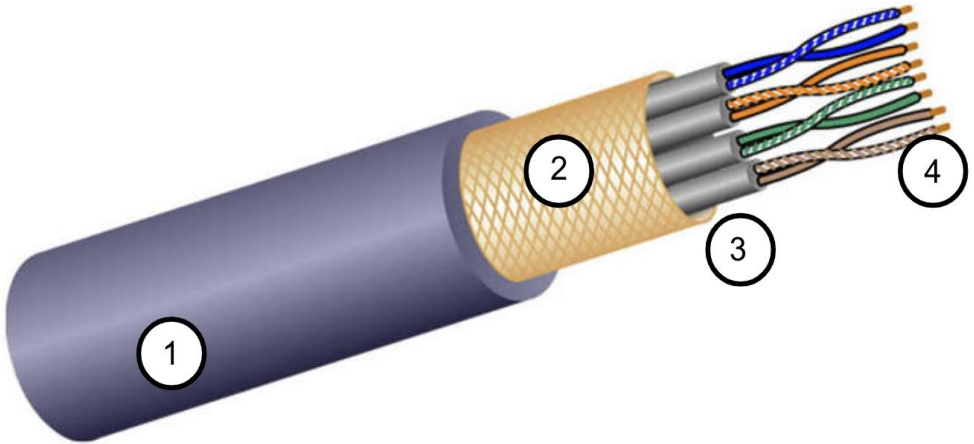


- UTP es el medio de red más común.
- Terminado con conectores RJ-45
- Interconecta hosts con dispositivos de red intermediarios.

- Características clave de UTP
  1. La cubierta exterior protege los cables de cobre de daños físicos.
  2. Los pares trenzados protegen la señal de interferencias.
  3. El aislamiento de plástico codificado por colores aísla eléctricamente los cables entre sí e identifica cada par.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Par trenzado blindado (STP)



- Mejor protección contra el ruido que UTP
- Más caro que UTP
- Más difícil de instalar que UTP
- Terminado con conectores RJ-45
- Interconecta hosts con dispositivos de red intermediarios

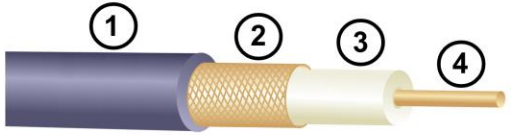
- Características clave de STP
  1. La cubierta exterior protege los cables de cobre de daños físicos.
  2. El blindaje trenzado o laminado proporciona protección EMI / RFI
  3. El blindaje de lámina para cada par de cables proporciona protección EMI / RFI

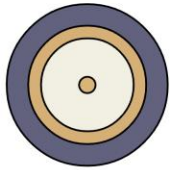
- El aislamiento de plástico codificado por colores aísla eléctricamente los cables entre sí e identifica cada par

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Cable Coaxial

- Consiste en lo siguiente:
  1. Cubierta exterior del cable para evitar daños físicos menores
  2. Una trenza de cobre tejida, o una hoja metálica, actúa como segundo cable en el circuito y como escudo para el conductor interno.
  3. Una capa de aislamiento de plástico flexible
  4. Se utiliza un conductor de cobre para transmitir las señales electrónicas.
- Hay diferentes tipos de conectores que se utilizan con cable coaxial.
- Usado comúnmente en las siguientes situaciones:
  - Instalaciones inalámbricas: conecta antenas a dispositivos inalámbricos
  - Instalaciones de Internet por cable: cableado en las instalaciones del cliente





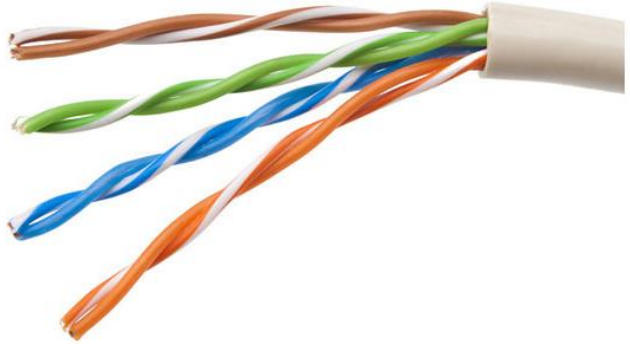
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

4.4 Cableado UTP

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Propiedades de cableado UTP

- TP tiene cuatro pares de cables de cobre codificados por colores trenzados y revestidos con una funda de plástico flexible. No se utiliza blindaje. UTP se basa en las siguientes propiedades para limitar el efecto de crosstalk:
  - **Anulación:** los hilos en cada par de cables se emparejan de tal forma que los campos magnéticos generados por cada uno se cancelan. Esto hace que también se anule cualquiere señal EMI / RFI externa.
  - **Variando el número de vueltas por par de hilos**: cada par está trenzado tiene diferente cantidad de vueltas, lo que ayuda a evitar la diafonía entre los hilos del cable.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

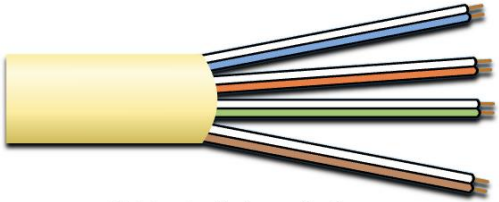
Conectores y estándares de cableado UTP

Los estándares para UTP están establecidos por TIA / EIA. TIA / EIA-568 estandariza elementos como:

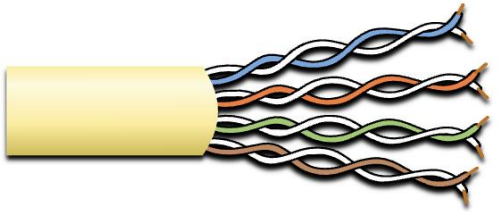
- Tipos de cable
- Longitudes de cable
- Conectores
- Terminación del cable
- Métodos de prueba

Los estándares eléctricos para cableado de cobre son establecidos por el IEEE, que clasifica el cable de acuerdo con su desempeño. Ejemplos incluyen:

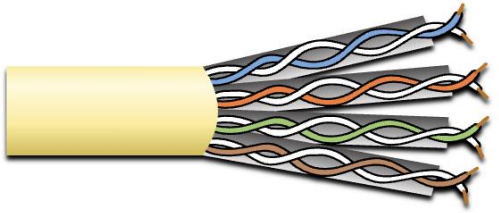
- Categoría 3
- Categoría 5 y 5e
- Categoría 6



Cable de Categoría 3
(UTP)



Cable de Categoría 5 o 5e
(UTP)



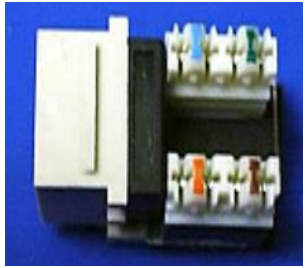
Cable de Categoría 6
(STP)

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Conectores y estándares de cableado UTP (Cont.)

Conector RJ-45

Cable UTP mal terminado

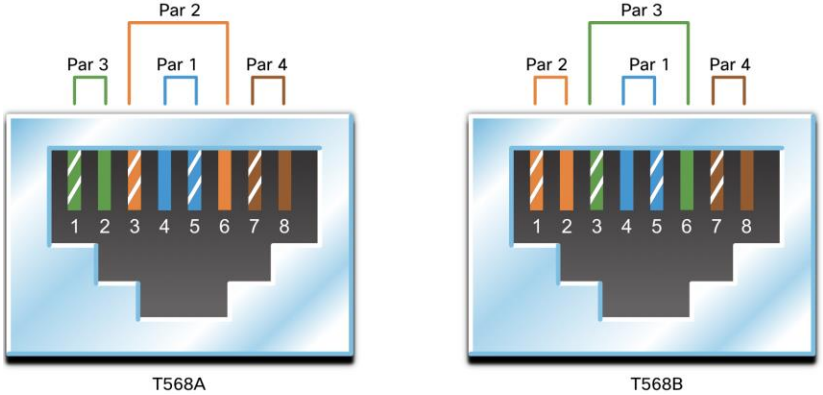


Socket RJ-45

Cable UTP correctamente terminado

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Cables UTP directos y cruzados



Tipo de cable	Estándar	Aplicación
Cable directo de Ethernet	Ambos extremos son T568A o T568B.	Conecta un host de red a un dispositivo de red como un switch o concentrador.
Cruzado Ethernet *	Un extremo T568A, otro extremo T568B.	Conecta dos hosts de red Conecta dos dispositivos intermediarios de red (switch a switch o router a router)
* Se considera descontinuado dado que la mayoría de las NIC utilizan Auto-MDIX para detectar el tipo de cable y la conexión completa		
Rollover	Propietario de Cisco	Conecta el puerto serial de una estación de trabajo al puerto de consola de un router utilizando un adaptador

4.5 Cableado de Fibra-Optica

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

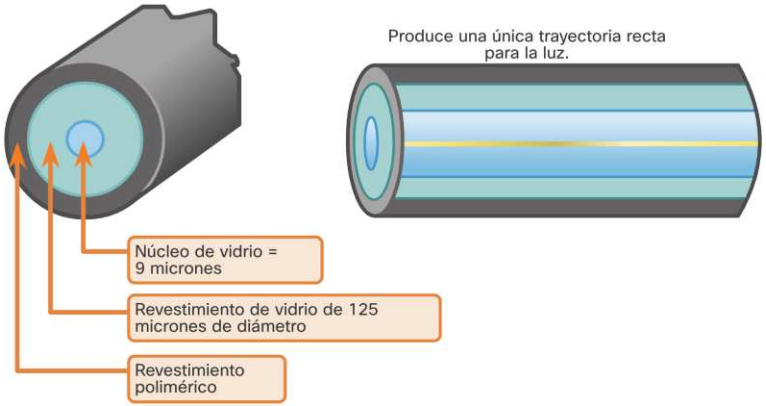
Propiedades del cableado de fibra óptica

- No es tan común como UTP debido al gasto involucrado
- Ideal para algunos escenarios de redes
- Transmite datos a distancias más largas con un ancho de banda mayor que cualquier otro medio de red
- Menos susceptible a la atenuación y completamente inmune a EMI / RFI
- Hecho de hebras flexibles y extremadamente delgadas de vidrio muy puro
- Utiliza un láser o LED para codificar bits como pulsos de luz
- El cable de fibra óptica actúa como una guía de ondas para transmitir luz entre los dos extremos con una mínima pérdida de señal.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

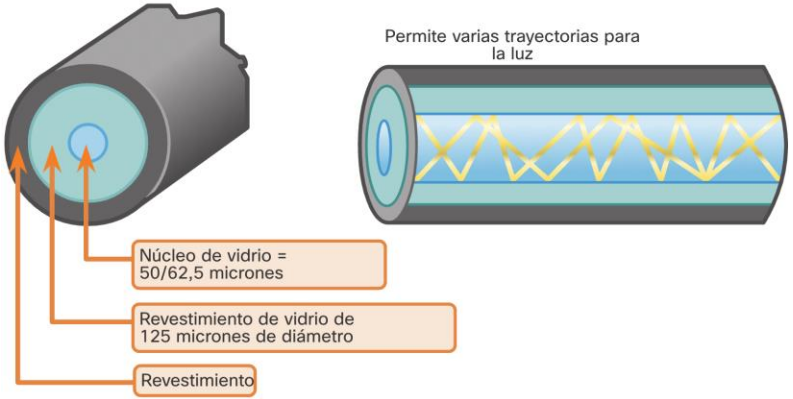
Types of Fiber Media

Fibra monomodo



- Núcleo muy pequeño
- Utiliza lasers costosos
- Transmisión a larga distancia

Fibra multimodo



- Núcleo más grande
- Usa LED, por lo que es menos costosa
- Los LEDs transmiten en diferentes ángulos
- Puede transmitir 10 Gbps a distancias de 550m

La dispersión se refiere a la extensión de los pulsos de luz con el tiempo. Una mayor dispersión significa una mayor pérdida de intensidad de la señal. MMF tiene una mayor dispersión que SMF, con una distancia máxima de cable para MMF es de 550 metros.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Uso del cableado de fibra óptica

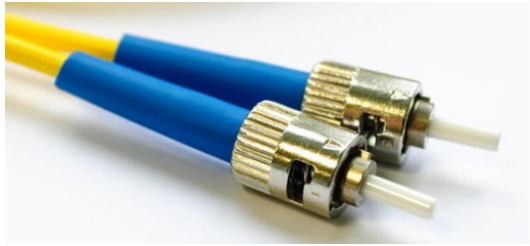
Tipos de cableado en fibra óptica:

- **Redes empresariales -** para aplicaciones de cableado backbone y dispositivos de infraestructura de interconexión
- **Fibra hasta el hogar (FTTH) -** para proporcionar servicios de banda ancha siempre activos a hogares y pequeñas empresas
- **Redes de larga distancia -** Utilizadas por proveedores de servicios para conectar países y ciudades
- **Redes de cable submarino -** se utilizan para proporcionar soluciones confiables de alta velocidad y alta capacidad capaces de sobrevivir en entornos submarinos hostiles a distancias transoceánicas.

En este curso, nos centraremos en el uso de la fibra óptica en el nivel de empresa.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

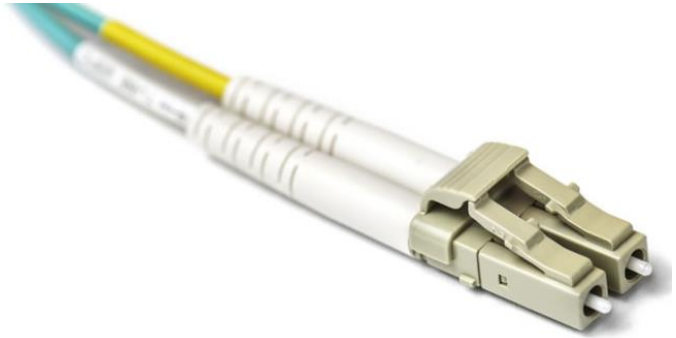
Conectores de fibra óptica



Conectores de punta directa (ST)

Conectores Lucent (LC) Conectores Simplex

Conectores subscritor (SC)



Conectores LC Multimodo Duplex

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Cables de conexión de fibra

Cablel de conexión multimodo SC-SC

Cable de conexión monomodo LC-LC

Cable de conexión multimodo ST-LC

Cable de conexión monomodo ST-SC

Una funda amarilla es para cables de fibra monomodo y naranja (o aguamarina) para cables de fibra multimodo.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Fibra versus Cobre

La fibra óptica se utiliza principalmente como cableado principal para conexiones punto a punto de alto tráfico entre instalaciones de distribución de datos y para la interconexión de edificios en campus de varios edificios.

Promblemas de implementación	UTP	Fibrá optica
Ancho de banda soportado	10 Mb/s - 10 Gb/s	10 Mb/s - 100 Gb/s
Distancia	Relativamente corto (1 - 100 metros)	Relativamente largo (1 - 100,000 metros)
Inmunidad a EMI y RFI	Baja	Alta (completamente inmune)
Inmunidad a peligros electricos	Baja	Alta (completamente inmune)
Costos medios de conectores	Más bajo	Más alto
Habilidades de instalación	Más bajo	Más alto
Precauciónes de seguridad	Más bajo	Más alto

4.6 Medios inalámbricos

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Propiedades de los medios inalámbricos

Transporta señales electromagnéticas que representan dígitos binarios utilizando frecuencias de radio o microondas. Esto proporciona la mejor opción de movilidad. El número de conexiones inalámbricas sigue aumentando.

Algunas de las limitaciones de la tecnología inalámbrica:

- **Área de cobertura**: la cobertura efectiva puede verse significativamente afectada por las características físicas de la ubicación de implementación.
- **Interferencia**: la tecnología inalámbrica es susceptible a interferencias y muchos dispositivos comunes pueden interrumpirla.
- **Seguridad**: la cobertura de comunicaciones inalámbricas no requiere acceso a una hebra física de medios, por lo que cualquiera puede obtener acceso a la transmisión.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Tipos de Medios inalámbrico

Los estándares de la industria de telecomunicaciones y IEEE para comunicaciones de datos inalámbricas cubren tanto el enlace de datos como las capas físicas.

En cada uno de estos estándares, las especificaciones de la capa física dictan:

- Métodos de codificación de datos a señales de radio
- Frecuencia y potencia de transmisión
- Requisitos de decodificación y recepción de señales
- Diseño y construcción de antenas

Estándares inalámbricos:

- **Wi-Fi (IEEE 802.11)**: tecnología de LAN inalámbrica (WLAN)
- **Bluetooth (IEEE 802.15)**: estándar de red de área personal inalámbrica (WPAN)
- **WiMAX (IEEE 802.16)**: utiliza una topología punto a multipunto para proporcionar acceso inalámbrico de banda ancha
- **Zigbee (IEEE 802.15.4)**: comunicaciones de baja velocidad de datos y bajo consumo de energía, principalmente para aplicaciones de Internet de las cosas (IoT)

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

LAN inalámbrica

En general, una LAN inalámbrica (WLAN) requiere los siguientes dispositivos:

- **Punto de acceso inalámbrico (AP)**: concentra las señales inalámbricas de los usuarios y los conecta a la infraestructura de red existente basada en cobre
- **Adaptadores NIC inalámbricos**: brindan capacidad de comunicaciones inalámbricas a los hosts de la red

Hay varios estándares de WLAN. Al comprar un equipo WLAN, asegúrese de la compatibilidad y la interoperabilidad.

Los administradores de red deben desarrollar y aplicar estrictas políticas y procesos de seguridad para proteger las WLAN de accesos no autorizados y daños.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Packet Tracer – Conectar una LAN inalámbrica y con cable

En esta actividad Packet Tracer, se hará lo siguiente:

- Conectarse a la nube
- Conectar un enrutador
- Conectar los dispositivos restantes
- Verificar conexiones

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Lab – Ver información para NIC cableado e inalámbrico

En esta actividad de laboratorio, completará los siguientes objetivos:

- Identificar y trabajar con NIC de PC
- Identificar y utilizar los iconos de red de la bandeja del sistema

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

4.7 Práctica del Modulo y Cuestionario

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

¿Qué aprendiste en este modulo?

- Antes de que pueda ocurrir cualquier comunicación de red, se debe establecer una conexión física a una red local, ya sea cableada o inalámbrica.
- La capa física consta de circuitos electrónicos, medios y conectores desarrollados por ingenieros.
- Los estándares de la capa física abordan tres áreas funcionales: componentes físicos, codificación y señalización.
- Los tres tipos de cableado de cobre son: UTP, STP y cable coaxial.
- El cableado UTP cumple con los estándares establecidos conjuntamente por TIA / EIA. Las características eléctricas del cableado de cobre están definidas por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE).
- Los principales tipos de cables que se obtienen mediante el uso de convenciones de cableado específicas son Ethernet directo y Ethernet cruzado.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

¿Qué aprendiste en este modulo?

- El cable de fibra óptica transmite datos a distancias más largas y con anchos de banda más altos que cualquier otro medio de red.
- Hay cuatro tipos de conectores de fibra óptica: ST, SC, LC y LC multimodo dúplex.
- Los cables de conexión de fibra óptica incluyen SC-SC multimodo, LC-LC monomodo, ST-LC multimodo y SC-ST monomodo.
- Los medios inalámbricos transportan señales electromagnéticas que representan los dígitos binarios de las comunicaciones de datos que utilizan frecuencias de radio o microondas. La tecnología inalámbrica tiene algunas limitaciones, que incluyen el área de cobertura, la interferencia, la seguridad y los problemas que ocurren con cualquier medio compartido.
- Los estándares inalámbricos incluyen los siguientes: Wi-Fi (IEEE 802.11), Bluetooth (IEEE 802.15), WiMAX (IEEE 802.16) y Zigbee (IEEE 802.15.4).
- La LAN inalámbrica (WLAN) requiere un AP inalámbrico y adaptadores NIC inalámbricos.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Packet Tracer – Conexión a la capa física

En está actividad de Packet Tracer, se realizará lo siguiente:

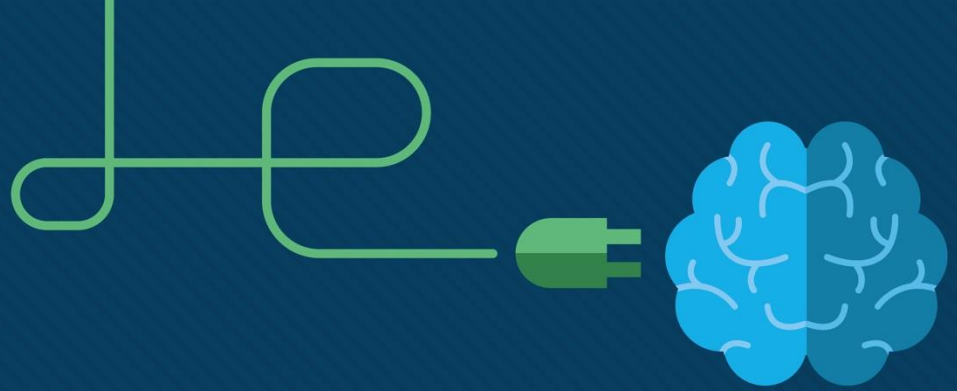
- Identificar las características físicas de los dispositivos de interconexión en red
- Seleccionar los módulos correctos para la conectividad
- Conectar dispositivos
- Comprobar conectividad

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

4.8 Resumen

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential


CISCO



Module 5: Sistemas numéricos

Introduction to Networks v7.0
(ITN)

Objetivos

Titulo: Sistemas númericos

Objectivo del modulo: Realizar cálculos y conversiones entre los sistemas decimal, binario, hexadecimal.

Titulo	Objectivo
Sistema binario	Realizar conversiones del sistema decimal y binario
Sistema hexadeciaml	Realizar conversiones del sistema decimal y hexadecimal

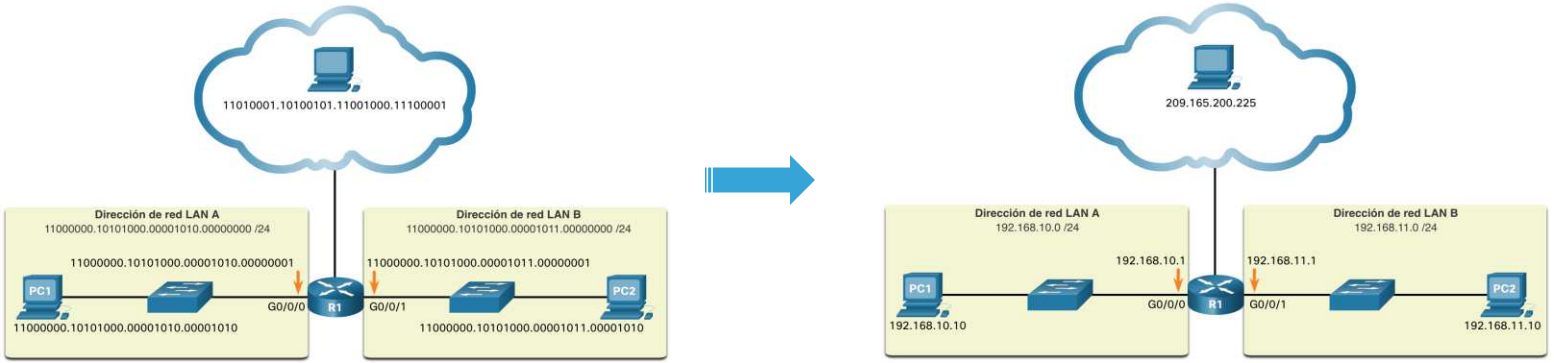
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

5.1 Sistema binario

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Direcciones binarias e IPv4

- El sistema de numeración binaria consta de unos y ceros, denominados bits
- El sistema de numeración decimal utiliza los dígitos del 0 al 9
- Hosts, servidores y equipos de red utilizan un direccionamiento binario para identificarse entre sí.
- Cada dirección está compuesta por una cadena de 32 bits, dividida en cuatro secciones llamadas octetos.
- Cada octeto contiene 8 bits (o 1 byte) separados por un punto.
- Para facilitar el uso por parte de las personas, esta notación con puntos se convierte en decimal con puntos.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Video – Conversión binario/decimal

Revisar video sección 5.1.2

Introduction to Networks -Sistema de numeración binaria

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Notación de posición binaria

- La notación posicional implica que un dígito representa valores diferentes dependiendo de la "posición" que ocupa dentro de la secuencia de números.
- El sistema de notación posicional decimal funciona como se muestra en las tablas siguientes.

Radix	10	10	10	10
Posición en número	3	2	1	0
Cálculo	(10^3)	(10^2)	(10^1)	(10^0)
Valor de la posición	1000	100	10	1

	Thousands	Hundreds	Tens	Ones
Valor de posición	1000	100	10	1
Número decimal (1234)	1	2	3	4
Calculo	1 x 1000	2 x 100	3 x 10	4 x 1
Sumarlos…	1000	+ 200	+ 30	+ 4
Resultado	**1,234**			

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Notación de posición binaria (Cont.)

El sistema de notación posicional binaria funciona como se muestra en las siguientes tablas.

Radix	2	2	2	2	2	2	2	2
Position in Number	7	6	5	4	3	2	1	0
Calculate	(2^7)	(2^6)	(2^5)	(2^4)	(2^3)	(2^2)	(2^1)	(2^0)
Position Value	128	64	32	16	8	4	2	1

Positional Value	128	64	32	16	8	4	2	1
Binary Number (11000000)	1	1	0	0	0	0	0	0
Calculate	1x128	1x64	0x32	0x16	0x8	0x4	0x2	0x1
Add Them Up…	128	+ 64	+ 0	+ 0	+ 0	+ 0	+ 0	+ 0
Result	**192**							

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Sistema binario

Conversión de binario a decimal

Convertir 11000000.10101000.00001011.00001010 a decimal.

Valor de posición	128	64	32	16	8	4	2	1	
Numero binario (11000000)	**1**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	
Cálculo	1x128	1x64	0x32	0x16	0x8	0x4	0x2	0x1	
Sumar…	128	+ 64	+ 0	+ 0	+ 0	+ 0	+ 0	+ 0	→ 192
Numero binario (10101000)	**1**	**0**	**1**	**0**	**1**	**0**	**0**	**0**	
Calculo	1x128	0x64	1x32	0x16	1x8	0x4	0x2	0x1	
Sumar…	128	+ 0	+ 32	+ 0	+ 8	+ 0	+ 0	+ 0	→ 168
Número binario(00001011)	**0**	**0**	**0**	**0**	**1**	**0**	**1**	**1**	
Cálculo	0x128	0x64	0x32	0x16	1x8	0x4	1x2	1x1	
sumar…	0	+ 0	+ 0	+ 0	+ 8	+ 0	+ 2	+ 1	→ 11
Número binario (00001010)	**0**	**0**	**0**	**0**	**1**	**0**	**1**	**0**	
Cálculo	0x128	0x64	0x32	0x16	1x8	0x4	1x2	0x1	
sumar…	0	+ 0	+ 0	+ 0	+ 8	+ 0	+ 2	+ 0	→ 10

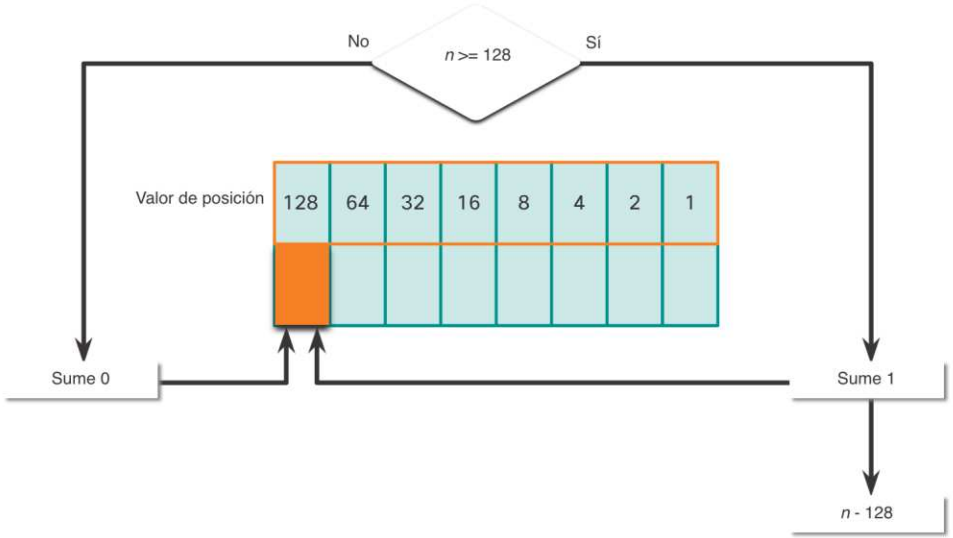
192.168.11.10

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Conversión decimal a binario

La tabla de valores posicionales binarios es útil para convertir una dirección IPv4 decimal con puntos en binaria.

- Comience en la posición 128 (el bit más significativo). ¿Es el número decimal del octeto (n) igual o mayor que 128?
- Si no, registre un 0 binario en el valor posicional 128 y pasar al valor posicional 64.
- En caso afirmativo, registre un 1 binario en el valor posicional 128, restar 128 del número decimal y pasar al valor posicional 64.
- Repita los pasos hasta el valor posicional 1.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Ejemplo de conversión decimal a binario

- Convertir 168 a binario

168 > 128
- Si, poner un 1 en la posición 128 y restar 128 (168-128=40)

¿40 > 64?
- No, poner 0 en la posición 64 y avanzar

¿40 > 32?
- Si, poner 1 en la posición 32 y restar 32 (40-32=8)

¿8 > 16?
- No, poner 0 en la posición 16 y avanzar

¿8 > 8?
- Es igual . poner 1 en la posición 8 y restar 8 (8-8=0)

No quedan valores. Poner 0 en las posiciones restantes

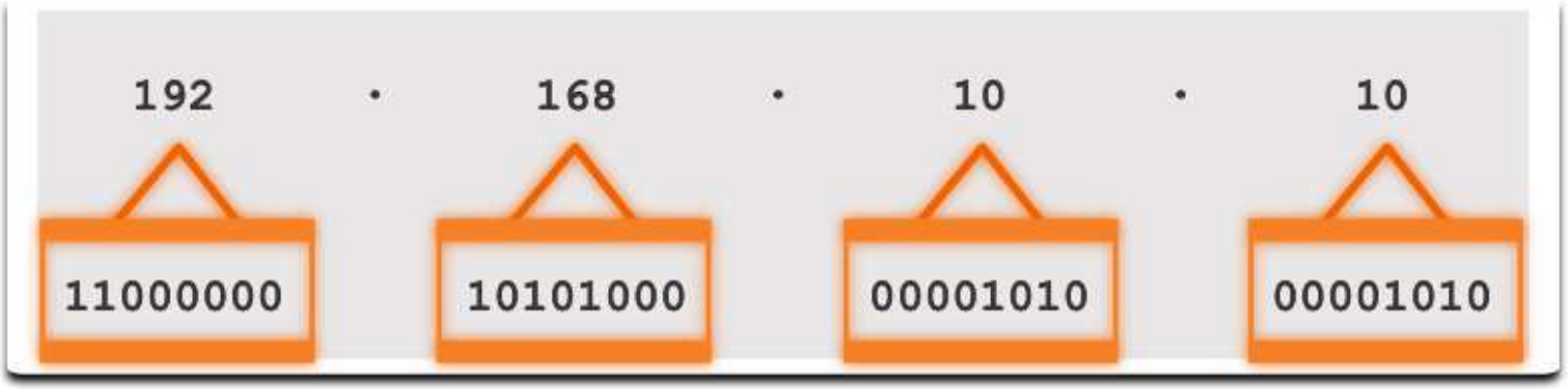
128	64	32	16	8	4	2	1
1	0	1	0	1	0	0	0

El número 168 se escribe en binario es 10101000

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Direcciones IPv4

- Los enrutadores y las computadoras solo entienden binario, mientras que los humanos utilizamos decimal. Es importante que comprenda a fondo estos dos sistemas de numeración y cómo se utilizan en las redes.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

5.2 Sistema Hexadecimal

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Hexadecimal y direcciones IPv6

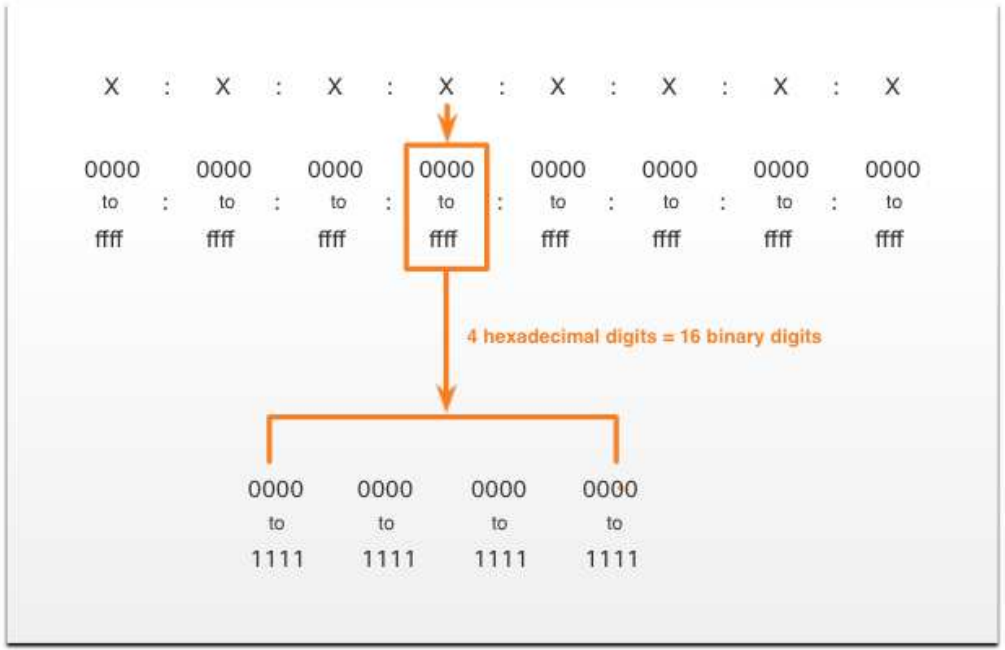
- Para comprender las direcciones IPv6, debe poder convertir hexadecimal a decimal y viceversa.
- El hexadecimal es un sistema de numeración de base dieciséis, utiliza los dígitos del 0 al 9 y las letras de la A a la F.
- Es más fácil expresar un valor como un solo dígito hexadecimal que como cuatro bits binarios.
- El hexadecimal se utiliza para representar direcciones IPv6 y direcciones MAC.

Decimal	Binary	Hexadecimal
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Hexadecimal y direcciones IPv6 (Cont.)

- Las direcciones IPv6 tienen una longitud de 128 bits. Cada 4 bits están representados por un solo dígito hexadecimal. Eso hace que la dirección IPv6 tenga un total de 32 valores hexadecimales.
- La figura muestra el método preferido para escribir una dirección IPv6, donde cada X representa cuatro valores hexadecimales.
- Cada grupo de cuatro caracteres hexadecimales se denomina hexteto.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Video – Conversión entre hexadecimal y decimal

Revisar video sección 5.2.2

Introduction to Networks -Sistema numérico hexadecimal

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Conversion decimal a hexadecimal

Siga los siguientes pasos para convertir números decimales en valores hexadecimales:

1. Convertir el número decimal en cadenas binarias de 8 bits.
2. Dividir las cadenas binarias en grupos de cuatro comenzando desde la posición más a la derecha.
3. Convertir cada cuatro números binarios en su dígito hexadecimal equivalente.

Por ejemplo, convertir 168 a hexadecimal:

- 168 en binario es 10101000.
- 10101000 en dos grupos de cuatro dígitos binarios es 1010 y 1000.
- 1010 en hexadecimal es A y 1000 es 8, por lo que 168 es A8 en hexadecimal.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Conversión de hexadecimal a decimal

Siga los siguientes pasaso para convertir números hexadecimales a valores decimales:

1. Conviertir el número hexadecimal en secuencias binarias de 4 bits.
2. Crear grupos binarios de 8 bits comenzando desde la posición más a la derecha.
3. Convertir cada grupo de 8 bits en su dígito decimal equivalente.

Por ejemplo, convertir D2 a decimal mediante el proceso de tres pasos:

1. D2 en secuencias binaria de 4 bits es 1101 y 0010.
2. 1101 y 0010 es 11010010 en un grupo de 8 bits.
3. 11010010 en binario es equivalente a 210 en decimal, entonces D2 es 210 es decimal

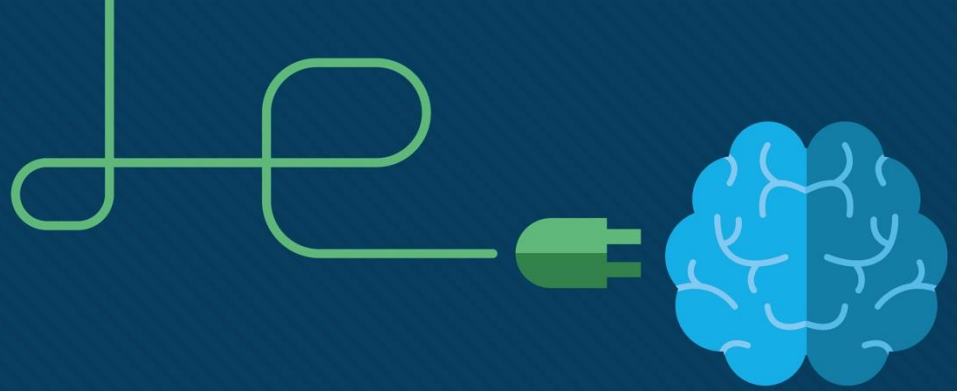
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

¿Qué aprendimos en este modulo?

- El sistema de numeración binario de base dos consta de los números 0 y 1, llamados bits.
- El sistema de numeración en base diez consta de números del 0 al 9.
- Los hosts, servidores y equipos de red utilizan el sistema binario para identificarse entre sí.
- El hexadecimal es un sistema de numeración de base dieciséis que consta de los números del 0 al 9 y las letras de la A a la F.
- El hexadecimal se utiliza para representar las direcciones IPv6 y direcciones MAC.
- Las direcciones IPv6 tienen una longitud de 128 bits y cada 4 bits está representado por un dígito hexadecimal para un total de 32 dígitos hexadecimales.
- Para convertir hexadecimal a decimal, primero debe convertir el hexadecimal a binario, luego convertir el binario a decimal.
- Para convertir decimal a hexadecimal, primero debe convertir el decimal a binario y luego el binario a hexadecimal.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential


CISCO



Módulo 6: Capa de enlace de datos

Objectivos

Modulo: Capa de enlace de datos

Objetivo: Explicar cómo el control de acceso a los medios en la capa de enlace de datos apoya la comunicación a través de las redes.

Tema	Objectivo
Propósito	Describir el propósito y la función de la capa de enlace de datos al preparar la comunicación para su transmisión en medios específicos.
Topologias	Comparar las características de los métodos de control de acceso a medios en topologías WAN y LAN.
Trama de enlace de datos	Describir las características y funciones de una trama de enlace de datos.

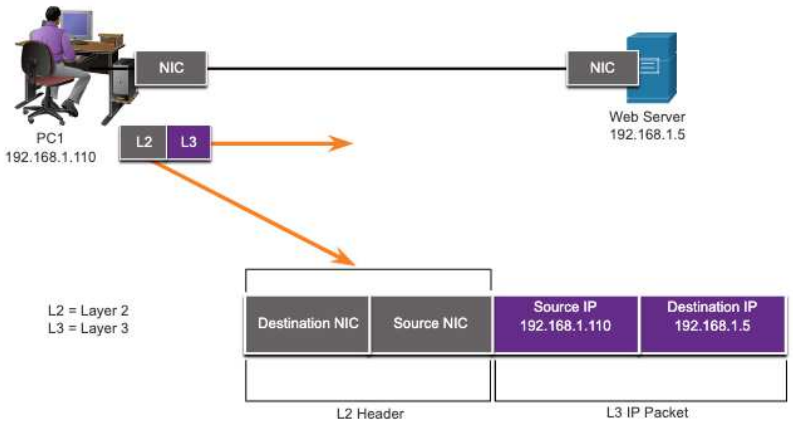
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

6.1 Proposito de la capa de enlace de datos

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

La capa de enlace de datos

- La capa de enlace de datos es responsable de las comunicaciones entre las tarjetas de interfaz de red del dispositivo final.
- Permite que los protocolos de la capa superior accedan a los medios de la capa física y encapsula los paquetes de la capa 3 (IPv4 e IPv6) en tramas de la capa 2.
- También realiza la detección de errores y rechazar los datos corruptos.



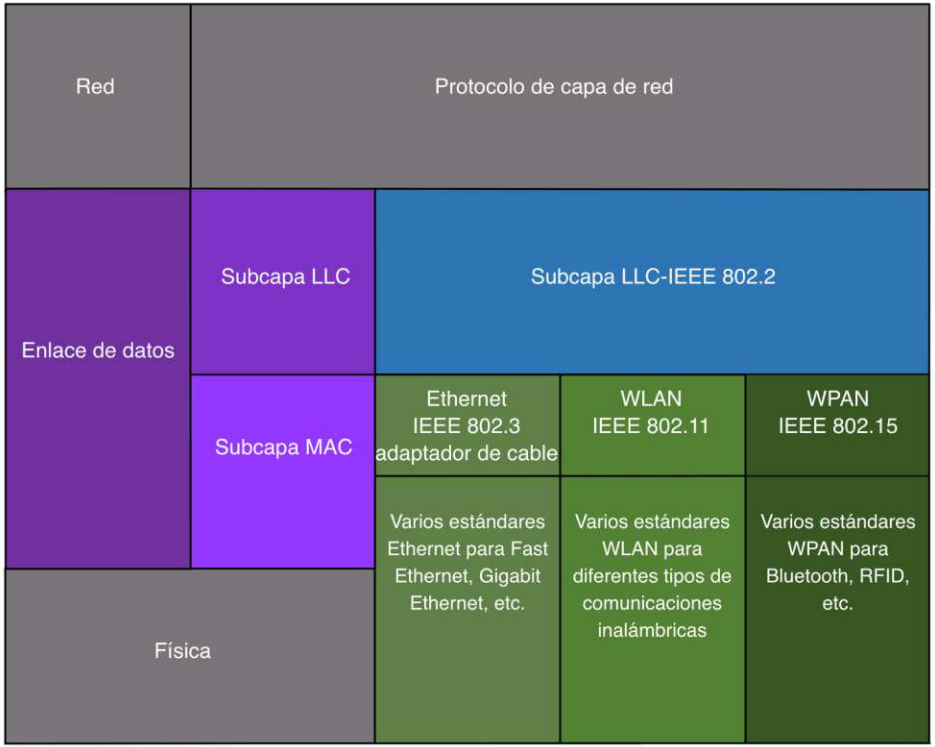
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

IEEE 802 LAN/MAN Sub-capas enlace de datos

Los estándares IEEE 802 LAN / MAN son específicos del tipo de red (Ethernet, WLAN, WPAN, etc.).

La capa de enlace de datos consta de dos subcapas. Control de enlace lógico (LLC) y control de acceso a medios (MAC).

- La subcapa LLC se comunica entre el software de red en las capas superiores y el hardware del dispositivo en las capas inferiores.
- La subcapa MAC es responsable de la encapsulación de datos y el control de acceso a los medios.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Provisión de acceso a los medios

Los paquetes intercambiados entre nodos pueden transitar a tráves de numerosas capas de enlace de datos y transiciones de medios.

En cada salto a lo largo de la ruta, un enrutador realiza cuatro funciones básicas de Capa 2:

- Acepta una trama del medio de red.
- Desencapsula la trama para exponer el paquete encapsulado.
- Vuelve a encapsular el paquete en una nueva trama.
- Reenvía la nueva trama en el medio del siguiente segmento de red.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Estándares de enlace de datos

Los protocolos de la capa de enlace de datos los definen las organizaciones de ingeniería:

- Institute for Electrical and Electronic Engineers (IEEE).
- International Telecommunications Union (ITU).
- International Organizations for Standardization (ISO).
- American National Standards Institute (ANSI).

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

6.2 Topologías

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Topologia lógica y física

La topología de una red es la disposición y relación de los dispositivos de red y las interconexiones entre ellos.

Hay dos tipos de topologías que se utilizan al describir redes:

- **Topología física**: muestra las conexiones físicas y cómo se interconectan los dispositivos.
- **Topología lógica:** identifica las conexiones virtuales entre dispositivos que utilizan interfaces de dispositivo y esquemas de direccionamiento IP.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Topologias WAN

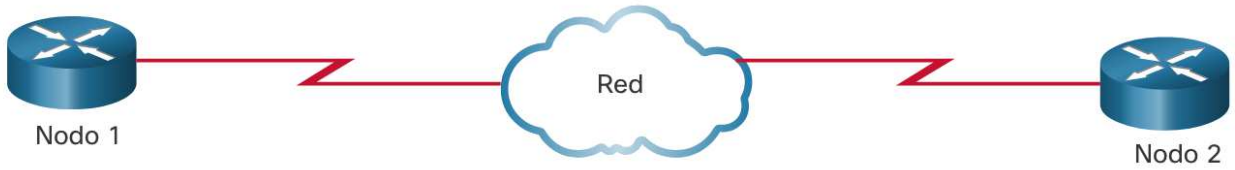
Hay tres topologías de WAN físicas comunes:

- **Punto a punto (Point-to-point)**: la topología WAN más simple y común. Consiste en un enlace permanente entre dos puntos finales.
- **Estrella (Hub and spoke)**: similar a una topología en estrella donde un sitio central interconecta los sitios de sucursales a través de enlaces punto a punto.
- **Malla (Mesh)**: proporciona alta disponibilidad, pero requiere que todos los sistemas finales estén conectados a todos los demás sistemas finales.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Topología Point-to-Point

- Las topologías físicas punto a punto conectan directamente dos nodos.
- Es posible que los nodos no compartan los medios con otros dispositivos.
- Debido a que todas las tramas de los medios solo pueden viajar hacia o desde los dos nodos, los protocolos WAN punto a punto pueden ser muy simples.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

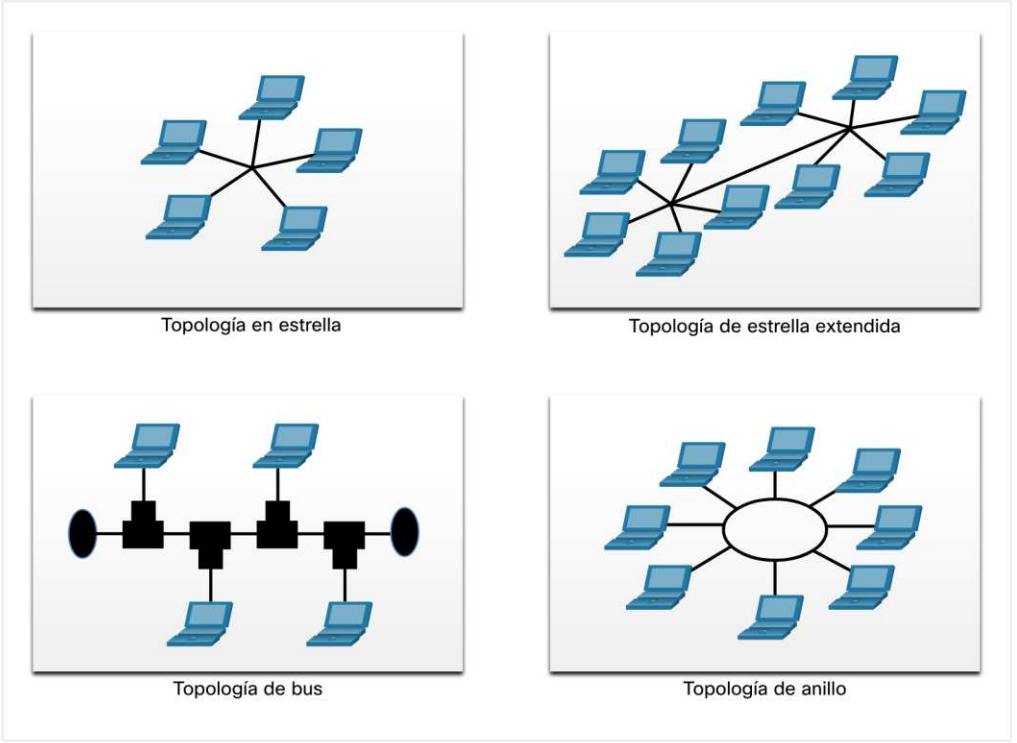
Topologias LAN

Los dispositivos finales en las LAN suelen estar interconectados mediante una topología en estrella o en estrella extendida. Las topologías en estrella y en estrella extendida son fáciles de instalar, muy escalables y de fácil matenimiento.

Las primeras tecnologías Ethernet y Token Ring heredado proporcionan dos topologías adicionales:

- **Bus**: todos los sistemas finales encadenados y terminados en cada extremo.
- **Anillo**: cada sistema final está conectado a sus respectivos vecinos para formar un anillo.

Topologías físicas



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Comunicación Half y Full Duplex

Half-duplex

- Solo permite que un dispositivo envíe o reciba a la vez en un medio compartido.
- Se utiliza en WLAN y topologías de bus heredadas con concentradores Ethernet.

Full-duplex

- Permite que ambos dispositivos transmitan y reciban simultáneamente en un medio compartido.
- Los conmutadores Ethernet funcionan en modo dúplex completo.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Métodos de control de acceso al medio

Basdo en contención

Todos los nodos funcionan en semidúplex, compitiendo por el uso del medio. Algunos ejemplos son:

- Acceso múltiple con detección de colisiones (CSMA / CD) como se usa en Ethernet de topología de bus heredada.
- Acceso múltiple con prevención de colisiones (CSMA / CA) como se usa en las LAN inalámbricas.

Controlado

- Acceso determinista donde cada nodo tiene su propio tiempo en el medio.
- Utilizado en redes heredadas como Token Ring y ARCNET

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Acceso badaso en contención – CSMA/CD

CSMA/CD

- Utilizado por LAN Ethernet heredadas.
- Funciona en modo semidúplex (half duplex).
- Utiliza un proceso de detección de colisiones para controlar cuándo un dispositivo puede enviar y qué sucede si varios dispositivos envían al mismo tiempo.

Proceso de detección de coliciones CSMA/CD:

- Los dispositivos que transmiten simultáneamente darán como resultado una colisión de señales en los medios compartidos.
- Los dispositivos detectan la colisión.
- Los dispositivos esperan un período de tiempo aleatorio y retransmiten datos.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Acceso basado en prevención – CSMA/CA

CSMA/CA

- Utilizado por WLAN IEEE 802.11.
- Funciona en modo half duplex.
- Utiliza un proceso de prevención de colisiones para controlar cuándo un dispositivo puede enviar y qué sucede si varios dispositivos envían al mismo tiempo.

Proceso de precvención de coliciones CSMA/CA:

- Al transmitir, los dispositivos también incluyen la duración de tiempo necesaria para la transmisión.
- Otros dispositivos en el medio compartido reciben la información de duración del tiempo y saben cuánto tiempo no estará disponible el medio.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

6.3 Trama de enlace de datos

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Trama/Frame

La capa de enlace de datos encapsula los datos con un encabezado y un avance para formar un marco.

Un marco de enlace de datos tiene tres partes:

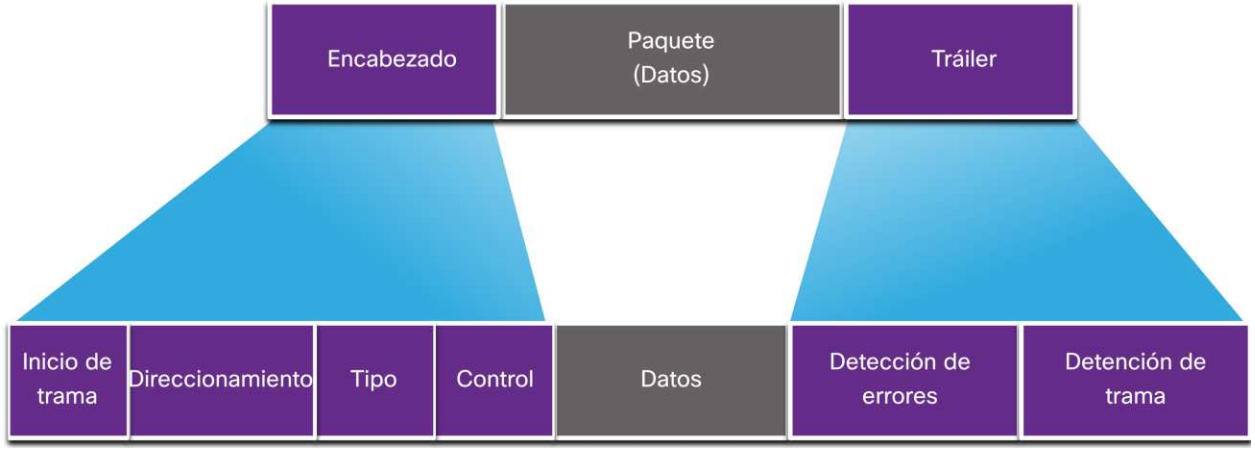
- Encabezado(header)
- Datos
- Tráiler

Los campos del encabezado y el final varían según el protocolo de la capa de enlace de datos.

La cantidad de información de control transportada en la trama varía según la información de control de acceso y la topología lógica.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Trama de enlace de datos
Campos de la trama

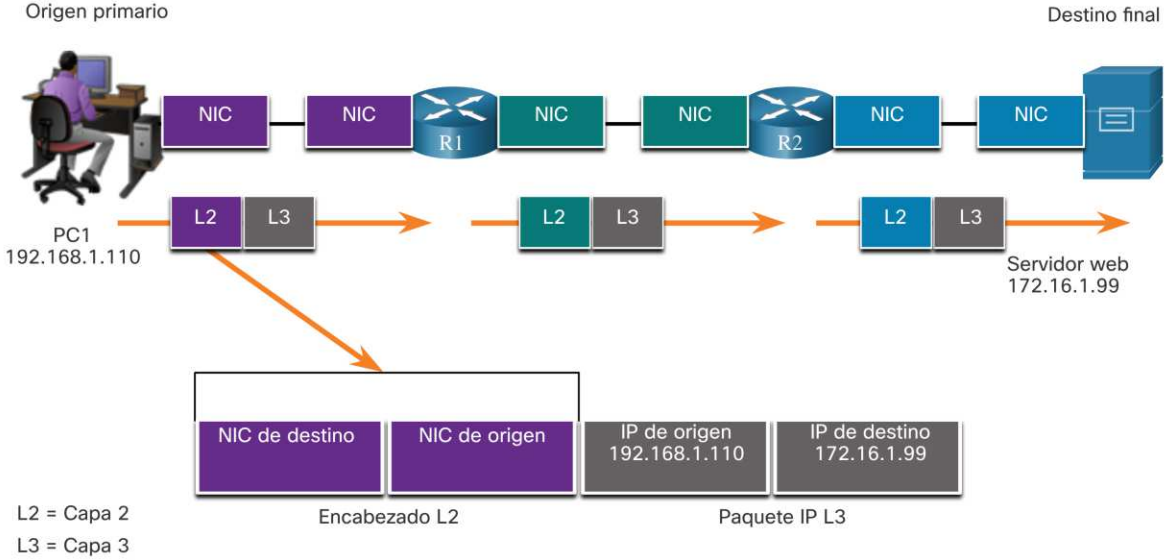


Campo	Descripción
Indicadores de Inicio y fin	Identifican el inicio y el final de una trama
Direccionamiento	lindican los nodos de origen ydestino
Tipo	Identifica el protocolo de capa 3
Control	Identifica los servicios de control de flujo (como QoS)
Datos	El contenido de la trama
Detección de errores	Información para determinar errores de transmisión

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Direcciones de capa 2

- También se conoce como dirección física.
- Contenido en el encabezado del marco.
- Se utiliza solo para la entrega local de un marco en el enlace.
- Actualizada por cada dispositivo que reenvía el marco.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Tramas LAN y WAN

La topología lógica y los medios físicos determinan el protocolo de enlace de datos utilizado:

- Ethernet
- 802.11 Wireless
- Point-to-Point (PPP)
- Control de enlace de datos de alto nive (High-Level Data Link Control HDLC)
- Frame-Relay

Cada protocolo realiza un control de acceso a los medios para topologías lógicas específicas.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

6.4 Práctica del modulo

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

¿Qué aprendimos en este modulo?

- La capa de enlace de datos del modelo OSI (Capa 2) prepara los datos de red para la red física.
- La capa de enlace de datos es responsable de las comunicaciones de la tarjeta de interfaz de red (NIC) a la tarjeta de interfaz de red.
- La capa de enlace de datos IEEE 802 LAN / MAN consta de las dos subcapas siguientes: LLC y MAC.
- Los dos tipos de topologías que se utilizan en las redes LAN y WAN son físicas y lógicas.
- Tres tipos comunes de topologías de WAN físicas son: punto a punto, concentrador y radio y malla.
- Las comunicaciones semidúplex intercambian datos en una dirección a la vez. El dúplex completo envía y recibe datos simultáneamente.
- En las redes de acceso múltiple basadas en contención, todos los nodos funcionan en semidúplex.

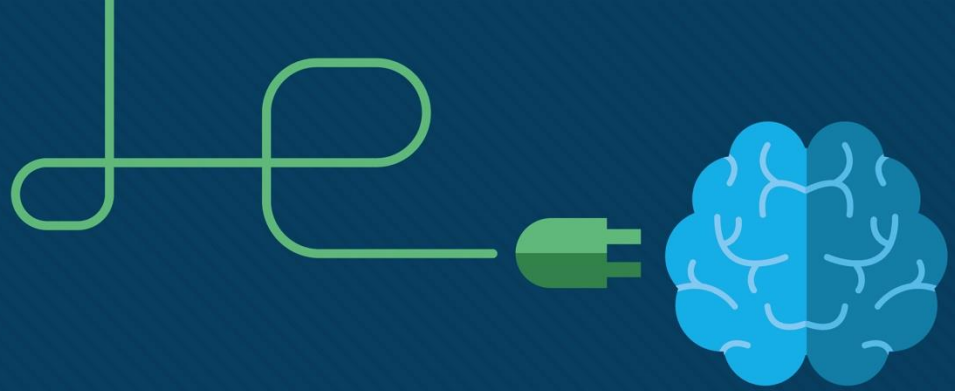
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

¿Qué aprendimos en este modulo?

- Ejemplos de métodos de acceso basados en contención incluyen: CSMA / CD para LAN Ethernet de topología de bus y CSMA / CA para WLAN.
- El marco de enlace de datos tiene tres partes básicas: encabezado, datos y avance.
- Los campos de tramas incluyen: banderas indicadoras de inicio y parada de tramas, direccionamiento, tipo, control, datos y detección de errores.
- Las direcciones de enlace de datos también se conocen como direcciones físicas.
- Las direcciones de enlace de datos solo se utilizan para la entrega local de enlaces de tramas.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential


CISCO



Modulo 7: Conmutación Ethernet

Introduction to Networks v7.0 (ITN)

Objectivos

Título: Conmutación thernet

Objetivo: Explicar como función una red de conmutación ethernet.

Tema	Objetivo
Trama Ethernet	Explicar cómo se relacionan las subcapas de Ethernet con los campos de la trama.
Ethernet MAC Address	Describir las direcciones Ethernet MAC.
Tabla de direcciones MAC	Explicar cómo un conmutador crea su tabla de direcciones MAC y reenvía tramas.
Velocidad de transmición y métodos de reenvio	Describir los métodos de reenvío de conmutadores y la configuración de puertos en conmutadores de capa 2.

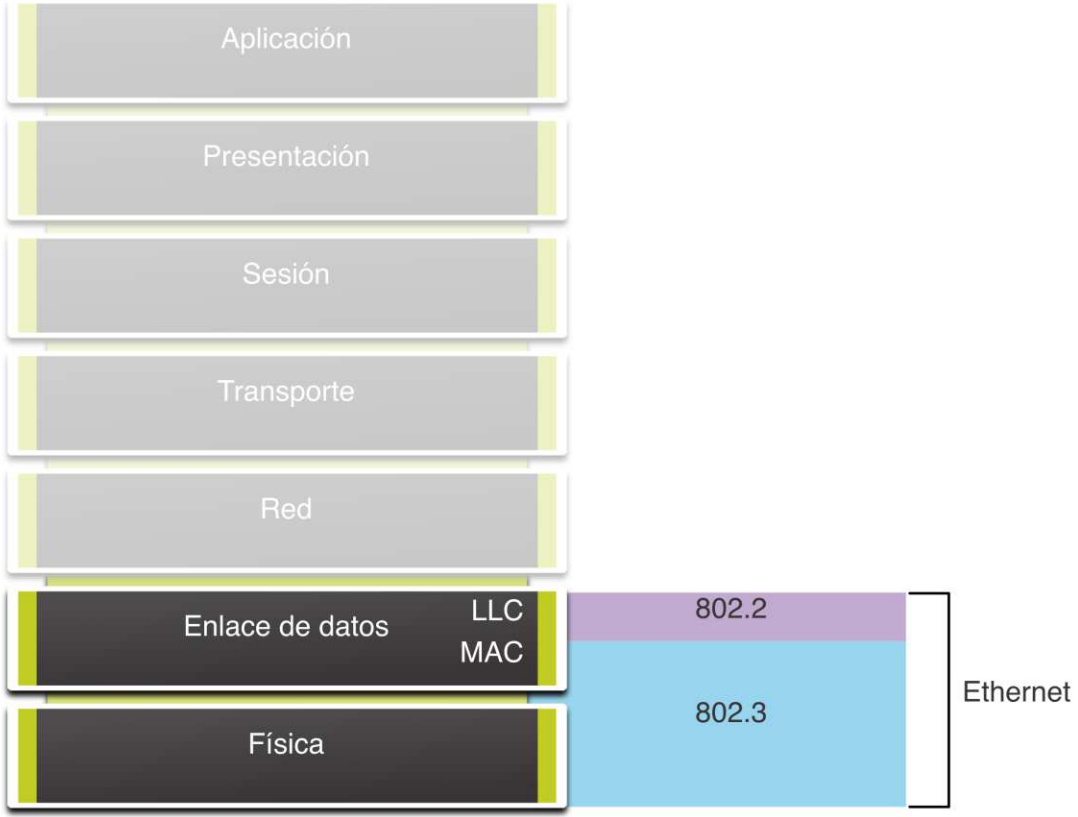
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

7.1 Trama Ethernet

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Encapsulado Ethernet

- Ethernet opera en la capa de enlace de datos y la capa física.
- Es una familia de tecnologías de redes definidas en los estándares IEEE 802.2 y 802.3.

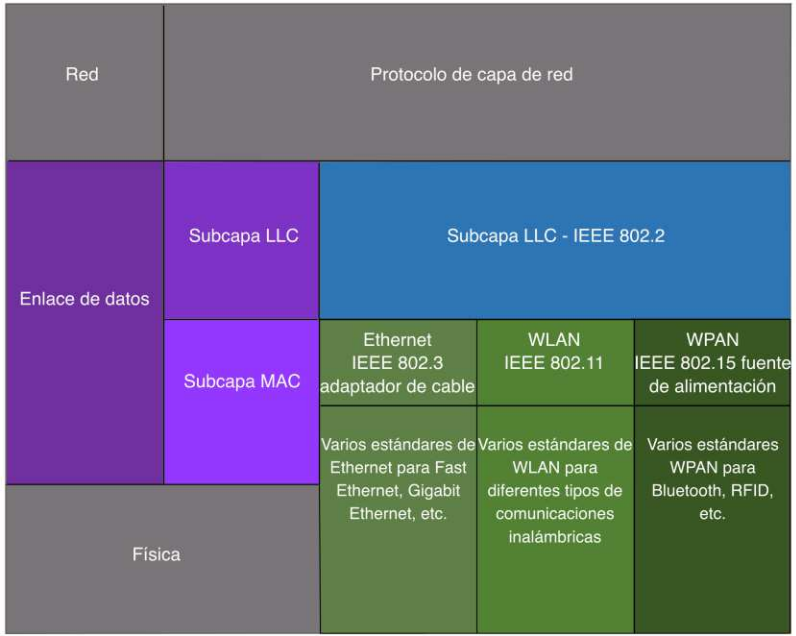


© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Sub-capas

Los estándares 802 LAN / MAN, incluida Ethernet, utilizan dos subcapas de la capa de enlace de datos para operar:

- Subcapa LLC: (IEEE 802.2) coloca información en la trama para identificar qué protocolo de capa de red se utiliza para la trama.
- Subcapa MAC: (IEEE 802.3, 802.11 u 802.15) Responsable de la encapsulación de datos y el control de acceso a los medios, y proporciona direccionamiento de la capa de enlace de datos.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Sub-capa MAC

La subcapa MAC es responsable de la encapsulación de datos y el acceso a los medios.

Encapsulado de datos

El encapsulado IEEE 802.3 incluye lo siguiente:

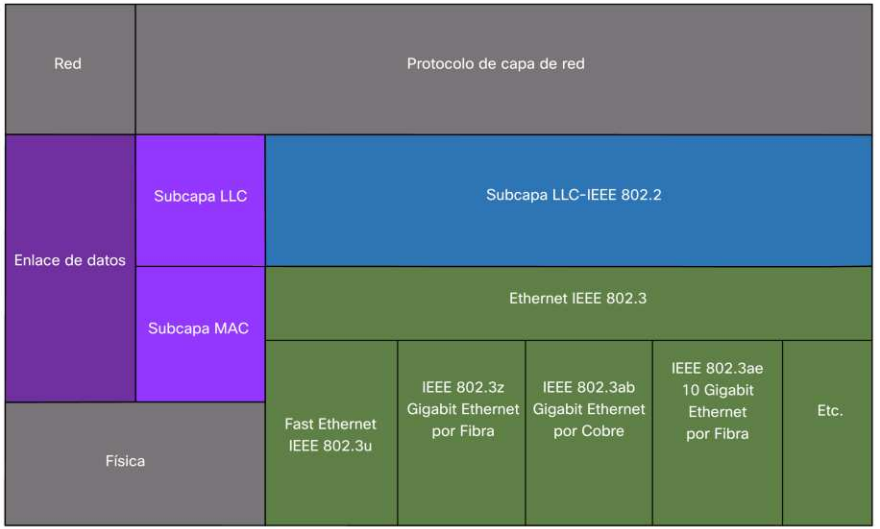
1. **Ethernet frame** - La estructura interna de la trama Ethernet.
2. **Ethernet Addressing** - La trama de Ethernet incluye una dirección MAC de origen y de destino para entregar la trama desde una NIC de Ethernet a otra en la misma LAN.
3. **Ethernet Error detection** - La trama de Ethernet incluye un tráiler de secuencia de verificación de tramas (FCS – Frame Check Sequence) que se utiliza para la detección de errores.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Sub-capa MAC

Acceso al medio

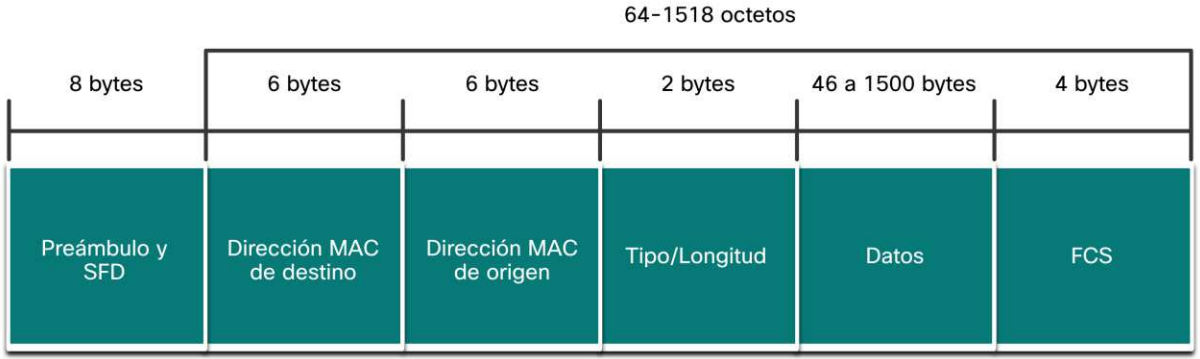
- La subcapa MAC IEEE 802.3 incluye las especificaciones para diferentes estándares de comunicaciones Ethernet en varios tipos de medios, incluidos cobre y fibra.
- Ethernet heredado que utiliza una topología de bus o concentradores es un medio semidúplex compartido. Ethernet sobre un medio semidúplex utiliza un método de acceso basado en contención, detección de acceso múltiple/colisión con detección de portadora (CSMA / CD).
- Las LAN Ethernet actuales utilizan conmutadores que funcionan en dúplex completo. Las comunicaciones full-duplex con conmutadores Ethernet no requieren control de acceso a través de CSMA/CD.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Campo de trama Ethernet

- El tamaño mínimo de la trama de Ethernet es de 64 bytes y el máximo es de 1518 bytes. El campo de preámbulo no se incluye al describir el tamaño de la trama.
- Cualquier trama de menos de 64 bytes de longitud se considera un "fragmento de colisión" o "trama runt" y se descarta automáticamente. Las tramas con más de 1500 bytes de datos se consideran "jumbo" o "tramas gigantes bebé".
- Si el tamaño de una trama transmitida es menor que el mínimo o mayor que el máximo, el dispositivo receptor descarta la trama. Es probable que los fotogramas descartados sean el resultado de colisiones u otras señales no deseadas. Se consideran inválidos. Las tramas gigantes suelen ser compatibles con la mayoría de los conmutadores y NIC Fast Ethernet y Gigabit Ethernet.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Lab – Utilizar Wireshark para examinar tramas (7.1.6)

Objetivos:

- Parte 1: Examinar los campos de encabezado en una trama de Ethernet II
- Parte 2: Utilizar Wireshark para capturar y analizar tramas de Ethernet

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

7.2 Direccion MAC

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

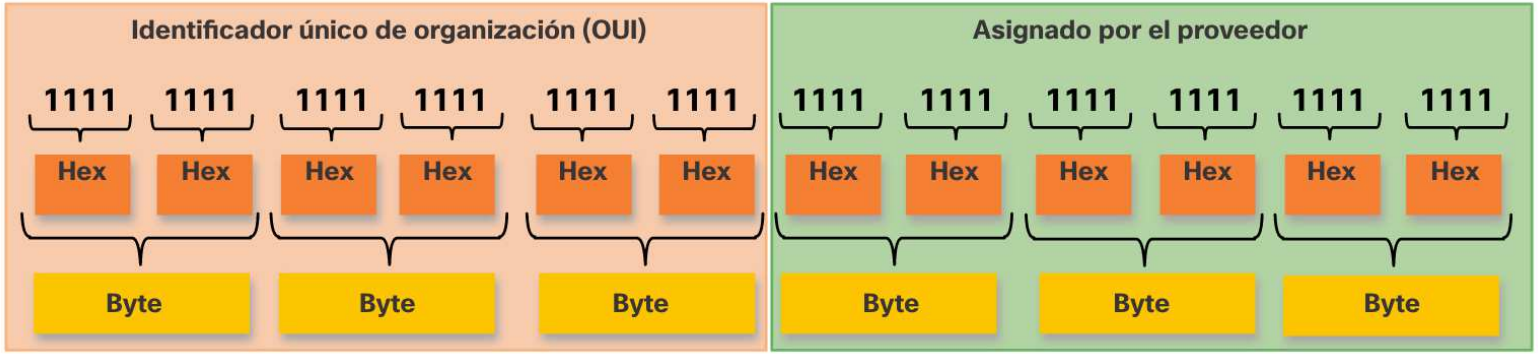
Direcciones MAC y Hexadecimal

- Una dirección MAC de Ethernet consta de un valor binario de 48 bits, expresado mediante 12 valores hexadecimales.
- Dado que 8 bits (un byte) es una agrupación binaria común, los binarios 00000000 a 11111111 se pueden representar en hexadecimal en el rango de 00 a FF,
- Cuando se usa hexadecimal, los ceros iniciales siempre se muestran para completar la representación de 8 bits. Por ejemplo, el valor binario 0000 1010 se representa en hexadecimal como 0A.
- Los números hexadecimales a menudo se representan precedidos por 0x (por ejemplo, 0x73) para distinguir entre valores decimales y hexadecimales.
- El hexadecimal también puede estar representado por un subíndice 16, o el número hexadecimal seguido de una H (por ejemplo, 73H).

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

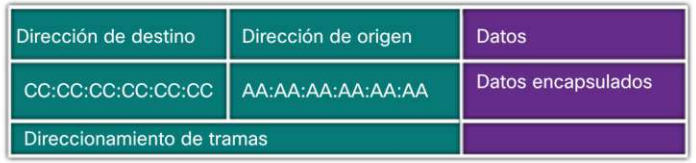
Direcciones MAC

- En una LAN, todos los dispositivos de red están conectados a los mismos medios compartidos. El direccionamiento MAC proporciona un método para la identificación de dispositivos en la capa de enlace de datos del modelo OSI.
- Una dirección MAC es una dirección de 48 bits expresada con 12 dígitos hexadecimales. Debido a que un byte equivale a 8 bits, también podemos decir que una dirección MAC tiene una longitud de 6 bytes.
- Todas las direcciones MAC deben ser únicas para el dispositivo/interfaz Ethernet. Para garantizar esto, los proveedores que venden dispositivos Ethernet deben registrarse con el IEEE para obtener un código hexadecimal de 24 bits o llamado identificador único organizacional (OUI).
- Una dirección MAC Ethernet consta de un código OUI de proveedor seguido de un valor asignado por proveedor.



Procesamiento de trama

- Cuando un dispositivo envía un mensaje a una red Ethernet, el encabezado de Ethernet incluye una dirección MAC de origen y una dirección MAC de destino.
- Cuando una NIC recibe una trama, examina la dirección MAC de destino para ver si coincide con la dirección MAC física que está almacenada en la RAM. Si no hay coincidencia, el dispositivo descarta el marco. Si hay una coincidencia, pasa la trama a las capas OSI, donde tiene lugar el proceso de desencapsulación.



- **Nota:** Las NIC de Ethernet también aceptarán tramas si la dirección MAC de destino es una transmisión o un grupo de multidifusión del que el host es miembro.
- Cualquier dispositivo que sea el origen o el destino de una trama Ethernet, tendrá una NIC Ethernet y, por lo tanto, una dirección MAC. Esto incluye estaciones de trabajo, servidores, impresoras, dispositivos móviles y enrutadores.

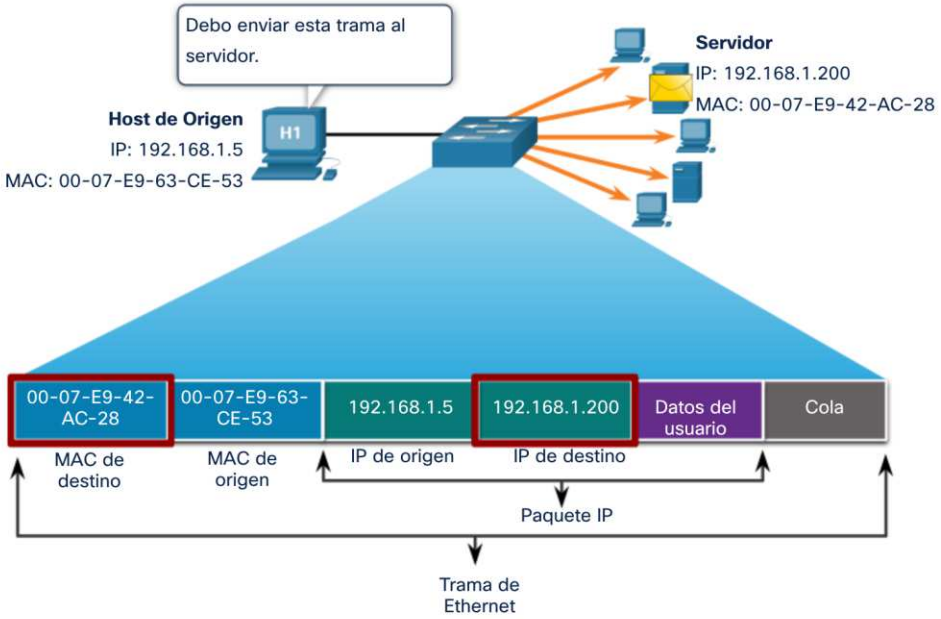
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Direccionamiento MAC
Unicast

En Ethernet, se utilizan diferentes direccinamiento MAC para comunicaciones de unicast, broadcast y multicast de capa 2.

- Una direccionamiento unicast MAC especifica una dirección que se utiliza cuando se envía una trama desde un único dispositivo de transmisión a un único dispositivo de destino
  - El proceso que utiliza un host de origen para determinar la dirección MAC de destino asociada con una dirección IPv4 se conoce como Protocolo de resolución de direcciones (ARP).
  - El proceso que utiliza un host de origen para determinar la dirección MAC de destino asociada con una dirección IPv6 se conoce como Descubrimiento de vecinos (ND).

Nota: La dirección MAC de origen debe ser siempre unidifusión.

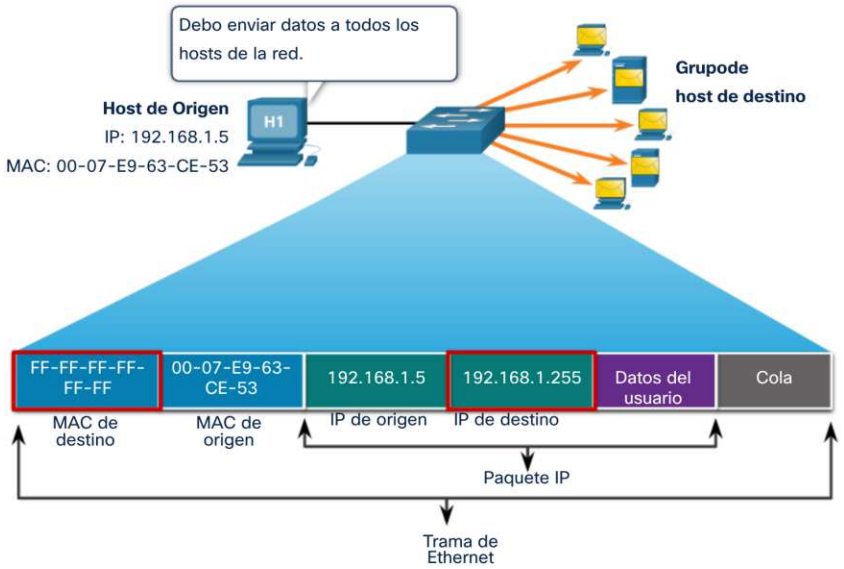


© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Direccionamiento MAC
Broadcast

Todos los dispositivos de la LAN Ethernet reciben y procesan una trama de transmisión Ethernet. Las características de una transmisión Ethernet son las siguientes:

- Tiene la MAC de destino de FF-FF-FF-FF-FF-FF en hexadecimal (48 bits).
- Se inunda todos los puertos del conmutador Ethernet, excepto el puerto de entrada. No es reenviado por un enrutador
- Si los datos encapsulados son un paquete de transmisión IPv4, esto significa que el paquete contiene una dirección IPv4 de destino que tiene todos unos (1) en la parte del host. Esta numeración en la dirección significa que todos los hosts de esa red local (dominio de transmisión) recibirán y procesarán el paquete.

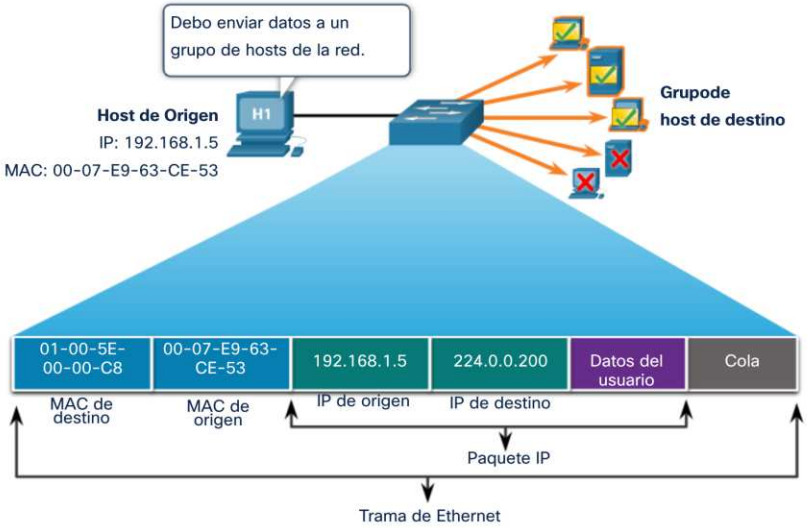


© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Direccionamiento MAC
Multicast

Una trama de multicast es recibida y procesada por un grupo de dispositivos que pertenecen al mismo grupo de multidifusión.

- Hay una dirección MAC de destino de 01-00-5E cuando los datos encapsulados son un paquete de multidifusión IPv4 y una dirección MAC de destino de 33-33 cuando los datos encapsulados son un paquete de multidifusión IPv6.
- Hay otras direcciones MAC de destino de multidifusión reservadas para cuando los datos encapsulados no son IP, como el Protocolo de árbol de expansión (STP).
- Se inunda todos los puertos del conmutador Ethernet, excepto el puerto de entrada, a menos que el conmutador esté configurado para espionaje de multidifusión. No es reenviado por un enrutador, a menos que el enrutador esté configurado para enrutar paquetes de multidifusión.
- Debido a que las direcciones de multidifusión representan un grupo de direcciones (a veces llamado grupo de hosts), solo se pueden usar como destino de un paquete. La fuente siempre será una dirección de unidifusión.
- Al igual que con las direcciones de difusión y unidifusión, la dirección IP de multidifusión requiere una dirección MAC de multidifusión correspondiente.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Lab – Ver las direcciones MAC del dispositivo de red (7.2.7)

En esta práctica de laboratorio se cumplirán los siguientes objetivos:

- Parte 1: Establecer la topología e inicializar los dispositivos
- Parte 2: Configurar los dispositivos y verificar la conectividad
- Parte 3: Mostrar, describir y analizar las direcciones MAC de Ethernet

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

7.3 Tabla de direcciones MAC

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Fundamentos de conmutación

- Un conmutador Ethernet de capa 2 utiliza direcciones MAC de capa 2 para tomar decisiones de reenvío. No tiene conocimiento de los datos (protocolo) que se transportan en la parte de datos de la trama, como un paquete IPv4, un mensaje ARP o un paquete ND IPv6. El conmutador toma sus decisiones de reenvío basándose únicamente en las direcciones MAC de Ethernet de capa 2.

- Un conmutador Ethernet examina su tabla de direcciones MAC para tomar una decisión de reenvío para cada trama, a diferencia de los concentradores Ethernet heredados que repiten bits en todos los puertos excepto el puerto de entrada.

- Cuando se enciende un interruptor, la tabla de direcciones MAC está vacía

Nota: La tabla de direcciones MAC a veces se denomina tabla de memoria direccionable de contenido (CAM).

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Switch, aprendiendo y reenviando

Examinar la dirección MAC de origen (aprender)

Cada trama que ingresa a un switch se verifica para obtener nueva información. Para ello se examina la dirección MAC de origen de la trama y el número de puerto donde la trama entró en el conmutador. Si la dirección MAC de origen no existe, se agrega a la tabla junto con el número de puerto entrante. Si la dirección MAC de origen existe, el conmutador actualiza el temporizador de actualización para esa entrada. De forma predeterminada, la mayoría de los conmutadores Ethernet mantienen una entrada en la tabla durante 5 minutos.

Nota: Si la dirección MAC de origen existe en la tabla pero en un puerto diferente, el switch lo trata como una nueva entrada. La entrada se reemplaza utilizando la misma dirección MAC pero con el número de puerto más actual.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Switch, aprendiendo y reenviando (Contd.)

Encuentre la dirección MAC de destino (reenvío)

Si la dirección MAC de destino es una dirección unicast, el switch buscará una coincidencia entre la dirección MAC de destino de la trama y una entrada en su tabla de direcciones MAC. Si la dirección MAC de destino está en la tabla, reenviará la trama por el puerto especificado. Si la dirección MAC de destino no está en la tabla, el switch reenviará la trama a todos los puertos excepto al puerto de entrada. Esto se denomina unicast desconocida.

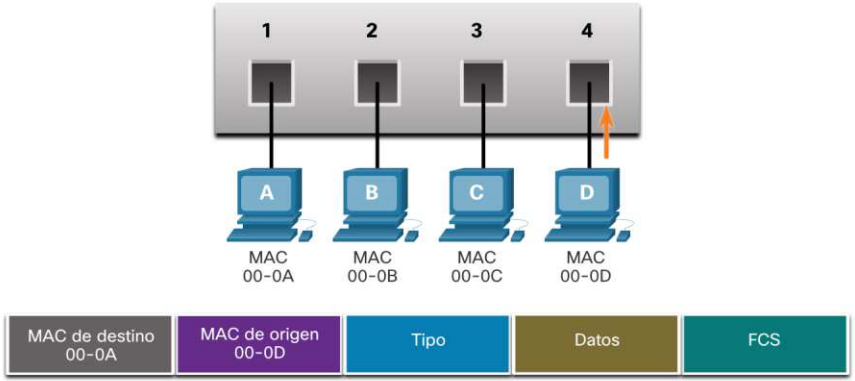
Nota: Si la dirección MAC de destino es broadcas o una multicast, la trama también se envía por todos los puertos excepto el puerto de entrada.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Filtrado de tramas

A medida que un conmutador recibe tramas de diferentes dispositivos, puede completar su tabla de direcciones MAC examinando la dirección MAC de origen de cada trama. Cuando la tabla de direcciones MAC del conmutador contiene la dirección MAC de destino, puede filtrar la trama y reenviar un solo puerto.

Tabla de direcciones MAC	
Puerto	**Dirección MAC**
1	00-0A
4	00-0D



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Video – Tablas de direcciones MAC en switches conectados (7.3.4)

Este video trata lo siguiente:

- Cómo los switches construyen tablas de direcciones MAC

- Cómo los conmutadores reenvían las tramas en función del contenido de sus tablas de direcciones MAC

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Video – Envío de una trama al gateway predeterminado(7.3.5)

Este video trata lo siguiente:

- Qué hace un conmutador cuando la dirección MAC de destino no aparece en la tabla de direcciones MAC del conmutador.

- Qué hace un conmutador cuando la dirección MAC de origen no aparece en la tabla de direcciones MAC del conmutador

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Lab – Visualización de la tabla de direcciones MAC del switch(7.3.7)

En este laboratorio, completará los siguientes objetivos:

- Parte 1: construir y configurar una red
- Parte 2: Examinar la tabla de direcciones MAC del conmutador

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

7.4 Velocidades y métodos de reenvio

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Métodos de reenvio en Switches Cisco (7.4.1)

Los conmutadores utilizan uno de los siguientes métodos de reenvío:

- **Store-and-forward switching** - Este método de reenvío recibe la trama completa y calcula el CRC. Si el CRC es válido, el conmutador busca la dirección de destino, que determina la interfaz de salida. Luego, la trama se reenvía por el puerto correcto.
- **Cut-through switching** - Este método de reenvío de tramas reenvía la trama antes de que se reciba por completo. Como mínimo, la dirección de destino de la trama debe leerse antes de que la trama pueda reenviarse.

- Una gran ventaja de la conmutación de **almacenamiento y envío** es que determina si una trama tiene errores antes de propagarla. Cuando se detecta un error en una trama, el conmutador descarta la trama. Descartar tramas con errores reduce la cantidad de ancho de banda consumido por datos corrompidos.
- La conmutación de **almacenamiento y reenvío** es necesaria para el análisis de la calidad de servicio (QoS) en redes convergentes donde es necesaria la clasificación de tramas para la priorización del tráfico. Por ejemplo, los flujos de datos de voz sobre IP (VoIP) deben tener prioridad sobre el tráfico de navegación web.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Switching por método de corte (7.4.2)

En la conmutación por corte, el conmutador actúa sobre los datos tan pronto como se reciben, incluso si la transmisión no está completa. El conmutador almacena en búfer el cual sea suficiente para leer la dirección MAC de destino, de modo que pueda determinar a qué puerto debe reenviar los datos. El conmutador no realiza ninguna comprobación de errores en el marco.

Hay dos variantes de conmutación por corte:

- **Fast-forward switching -** Ofrece el nivel más bajo de latencia al reenviar inmediatamente un paquete después de leer la dirección de destino. Debido a que la conmutación de **reenvio rápido** comienza a reenviar antes de que se haya recibido todo el paquete, puede haber ocasiones en las que los paquetes se transmitan con errores. La NIC de destino descarta el paquete defectuoso al recibirlo. La conmutación de avance rápido es el método típico de conmutación de corte directo.
- **Fragment-free switching** - Un compromiso entre la alta latencia y la alta integridad de la conmutación de almacenamiento y reenvío y la baja latencia y la integridad reducida de la conmutación de reenvio rápido, el switch almacena y realiza una verificación de errores en los primeros 64 bytes de la trama antes del reenvío. Debido a que la mayoría de los errores y colisiones de la red ocurren durante los primeros 64 bytes, esto asegura que no haya ocurrido una colisión antes de reenviar la trama.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Almacenamiento en búfer de memoria

Un conmutador Ethernet puede utilizar una técnica de almacenamiento en búfer para almacenar tramas antes de reenviarlas o cuando el puerto de destino está ocupado debido a la congestión.

Método	Descripciόm
Memoria basada en puerto	•Las tramas se almacenan en colas que se enlazan a puertos específicos de entrada y puertos de salida. •Una trama se transmite al puerto de salida sólo cuando todas las tramas en la cola se han transmitido correctamente. •Es posible que una sola trama retrase la transmisión de todas las tramas en memoria debido a un puerto de destino ocupado. •Esta demora se produce aunque las demás tramas se puedan transmitir a puertos de destino abiertos.
Memoria compartida	•Deposita todas las tramas en un búfer de memoria común compartido por todos los puertos y la cantidad de memoria intermedia requerida por un puerto es asignada dinámicamente. •Las tramas que están en el búfer se enlazan de forma dinámica al puerto de destino. que permite recibir un paquete en un puerto y, a continuación, transmitido en otro puerto, sin moverlo a una cola diferente.

- El almacenamiento en búfer de memoria compartida también da como resultado tramas más grandes resultando en menos tramas descartados. Esto es importante con la conmutación asimétrica que permite diferentes velocidades de datos en diferentes puertos. Por lo tanto, se puede dedicar más ancho de banda a ciertos puertos (por ejemplo, el puerto del servidor).

Configuración de dúplex y velocidad

Dos de las configuraciones más básicas de un conmutador son el ancho de banda ("velocidad") y la configuración dúplex para cada puerto de switch individual. Es fundamental que la configuración de ancho de banda y dúplex coincida entre el puerto del conmutador y los dispositivos conectados.

Hay dos tipos de configuraciones dúplex que se utilizan:

- **Full-duplex** - Ambos extremos de la conexión pueden enviar y recibir datos simultáneamente.
- **Half-duplex** - Solo uno de los extremos de la conexión puede enviar datos por vez.

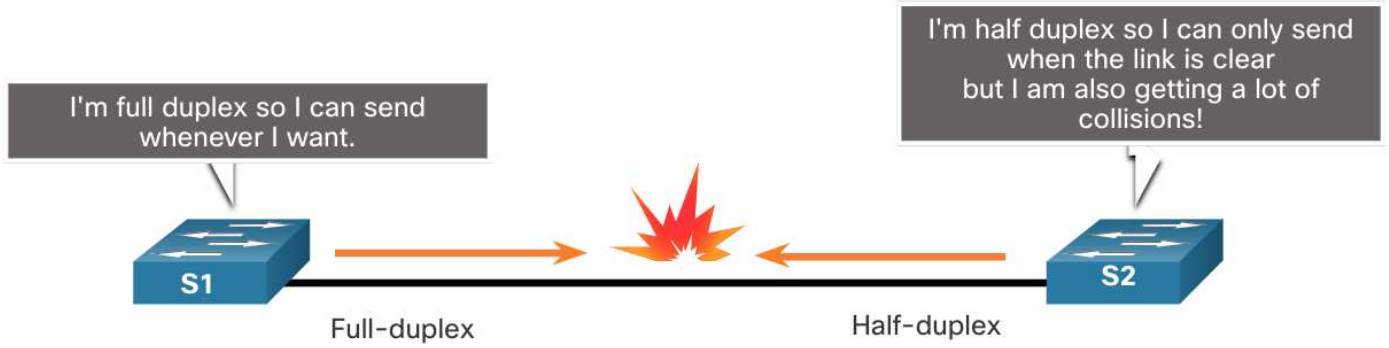
La autonegociación es una función opcional que se encuentra en la mayoría de los conmutadores Ethernet y NIC. Permite que dos dispositivos negocien automáticamente la mejor velocidad y capacidades dúplex.

Note: los puertos Gigabit Ethernet solo operan en full-duplex.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Configuración de dúplex y velocidad

- La falta de coincidencia dúplex es una de las causas más comunes de problemas de rendimiento en enlaces Ethernet de 10/100 Mbps. Ocurre cuando un puerto del enlace funciona en semidúplex mientras que el otro puerto funciona en dúplex completo.
- Esto puede ocurrir cuando se restablecen uno o ambos puertos en un enlace, y el proceso de negociación automática no da como resultado que ambos socios del enlace tengan la misma configuración.
- También puede ocurrir cuando los usuarios reconfiguran un lado de un enlace y se olvidan de reconfigurar el otro. Ambos lados de un enlace deben tener la negociación automática activada, o ambos lados deben tenerla desactivada. La mejor práctica es configurar ambos puertos de conmutador Ethernet como dúplex completo.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Auto-MDIX

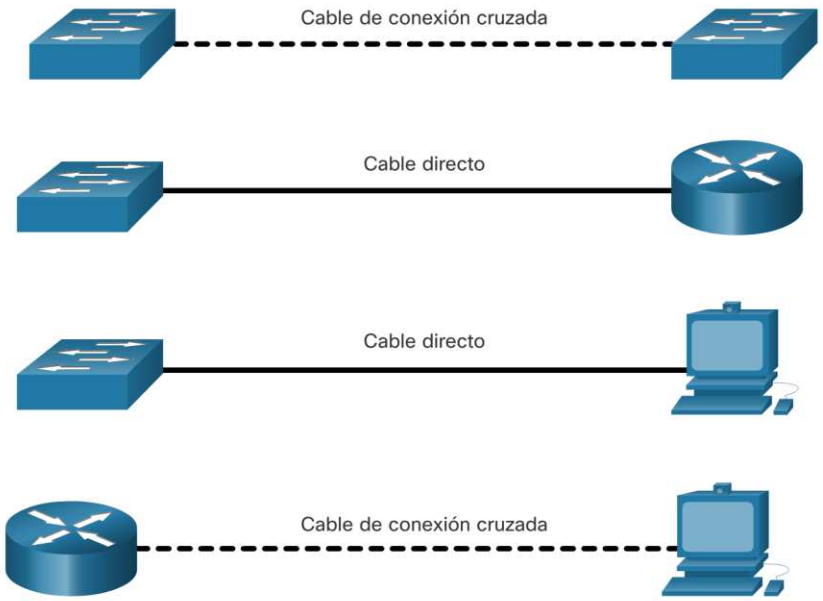
Las conexiones entre dispositivos requerían el uso de un cable cruzado o directo. El tipo de cable requerido dependía del tipo de dispositivos de interconexión.

Nota: Una conexión directa entre un enrutador y un host requiere una conexión cruzada.

- La mayoría de los dispositivos de conmutación ahora admiten la función de cruce automático de interfaz dependiente del medio (auto-MDIX). Cuando está habilitado, el conmutador detecta automáticamente el tipo de cable conectado al puerto y configura las interfaces en consecuencia.
- La función auto-MDIX está habilitada de forma predeterminada en los switches que ejecutan Cisco IOS versión 12.2 (18) SE o posterior. Sin embargo, la función podría deshabilitarse. Por esta razón, siempre debe usar el tipo de cable correcto y no confiar en la función auto-MDIX.
- Auto-MDIX se puede volver a habilitar usando el comando de configuración de interfaz automática mdix.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Interconexión entre dispositivos



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

7.5 Modulo de práctica y prueba

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

¿Qué aprendimos en este modulo?

- Ethernet opera en la capa de enlace de datos y la capa física. Los estándares de Ethernet definen tanto los protocolos de Capa 2 como las tecnologías de Capa 1.
- Ethernet utiliza las subcapas LLC y MAC de la capa de enlace de datos para operar.
- Los campos de la trama de Ethernet son: preámbulo y delimitador de trama inicial, dirección MAC de destino, dirección MAC de origen, EtherType, datos y FCS.
- El direccionamiento MAC proporciona un método para la identificación de dispositivos en la capa de enlace de datos del modelo OSI.
- Una dirección MAC de Ethernet es una dirección de 48 bits expresada con 12 dígitos hexadecimales o 6 bytes.
- Cuando un dispositivo envía un mensaje a una red Ethernet, el encabezado de Ethernet incluye las direcciones MAC de origen y destino. En Ethernet, se utilizan diferentes direcciones MAC para comunicaciones de unidifusión, difusión y multidifusión de capa 2.

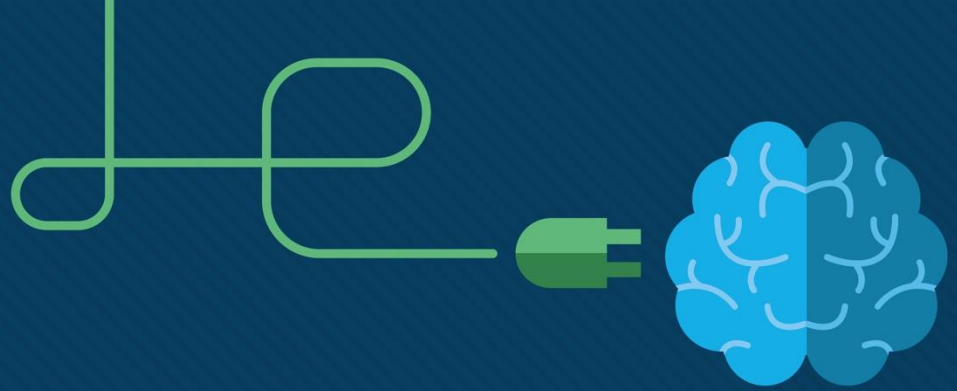
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

¿Qué aprendimos en este modulo? (Cont.)

- Un conmutador Ethernet de capa 2 toma sus decisiones de reenvío basándose únicamente en las direcciones MAC de Ethernet de capa 2.
- El conmutador crea dinámicamente la tabla de direcciones MAC examinando la dirección MAC de origen de las tramas recibidas en un puerto.
- El switch reenvía tramas buscando una coincidencia entre la dirección MAC de destino en la trama y una entrada en la tabla de direcciones MAC.
- Los conmutadores utilizan uno de los siguientes métodos de reenvío para conmutar datos entre puertos de red: conmutación de almacenamiento y reenvío o conmutación de corte. Dos variantes de conmutación **por corte** son de **reenvio rápido** y sin fragmentos.
- Dos métodos de almacenamiento en búfer de memoria son la memoria basada en puerto y la memoria compartida.
- Hay dos tipos de configuraciones dúplex que se utilizan para las comunicaciones en una red Ethernet: dúplex completo y semidúplex.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential


CISCO



Modulo 8: Capa de red

Introduction to Networks v7.0
(ITN)

Modulo 8: Temas

¿Qué aprenderemos en este modulo?

Titulo	Descripción
Características de la capa de red	Explicar cómo la capa de red usa protocolos IP para comunicaciones confiables.
Paquete IPv4	Explicar el papel de los principales campos en el encabezado de un paquete IPv4.
Paquete IPv6	Explicar el papel de los principales campos en el encabezado de un paquete IPv6.
Como enruta un host	Explain how network devices use routing tables to direct packets to a destination network.
Tablas de ruteo	Explicar cómo los dispositivos de red utilizan tablas de enrutamiento para dirigir paquetes a una red de destino.

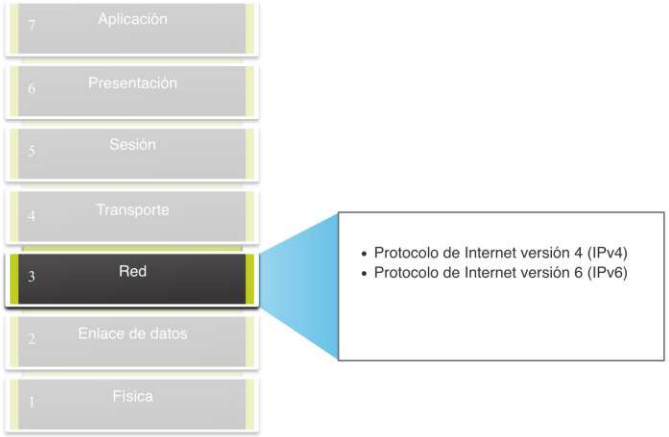
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

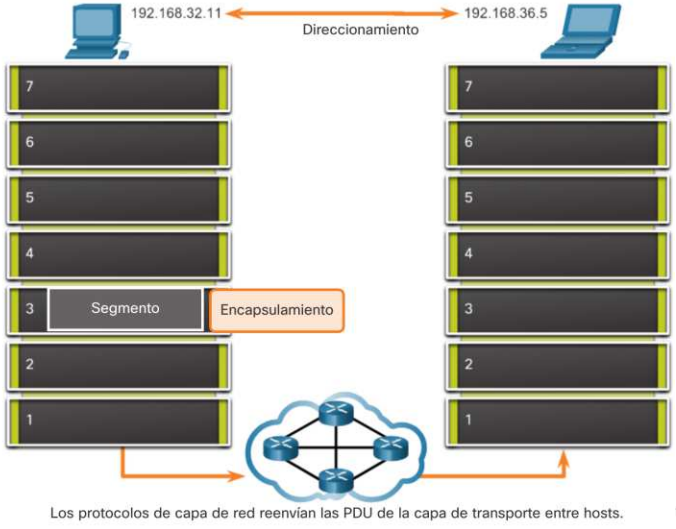
8.1 Características de la capa de Red

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

La capa de Red

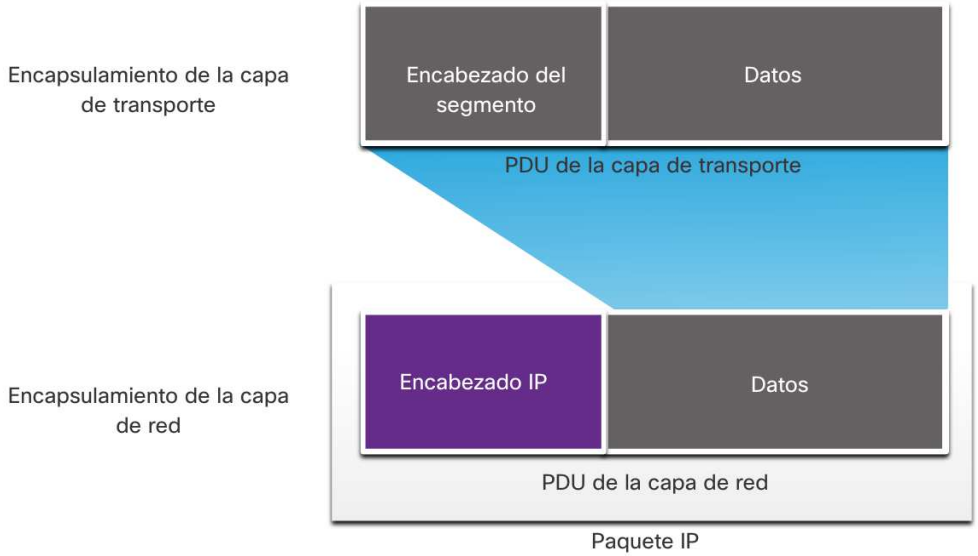
- Proporciona servicios para permitir que los dispositivos finales intercambien datos
- IP versión 4 (IPv4) e IP versión 6 (IPv6) son los principales protocolos de comunicación de la capa de red.
  - La capa de red realiza cuatro operaciones básicas:
  - Abordar los dispositivos finales
  - Encapsulamiento
  - Enrutamiento
  - Desencapsulamiento





Encapsulado IP

- IP encapsula el segmento de la capa de transporte.
- IP puede utilizar un paquete IPv4 o IPv6 y no afectar al segmento de la capa 4.
- El paquete IP será examinado por todos los dispositivos de capa 3 a medida que atraviesa la red.
- El direccionamiento IP no cambia de origen a destino.
- **Nota:** NAT cambiará el direccionamiento, pero se discutirá más adelante.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Caracterisicas de IP

IP está diseñado para tener una sobrecarga baja y puede describirse como:

- Sin conexión
- Mejor esfuerzo
- Independiente del medio

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Sin conexión

IP sin conexión

- IP no establece una conexión con el destino antes de enviar el paquete.
- No se necesita información de control (sincronizaciones, reconocimientos, etc.).
- El destino recibirá el paquete cuando llegue, pero no se envían notificaciones previas por IP.

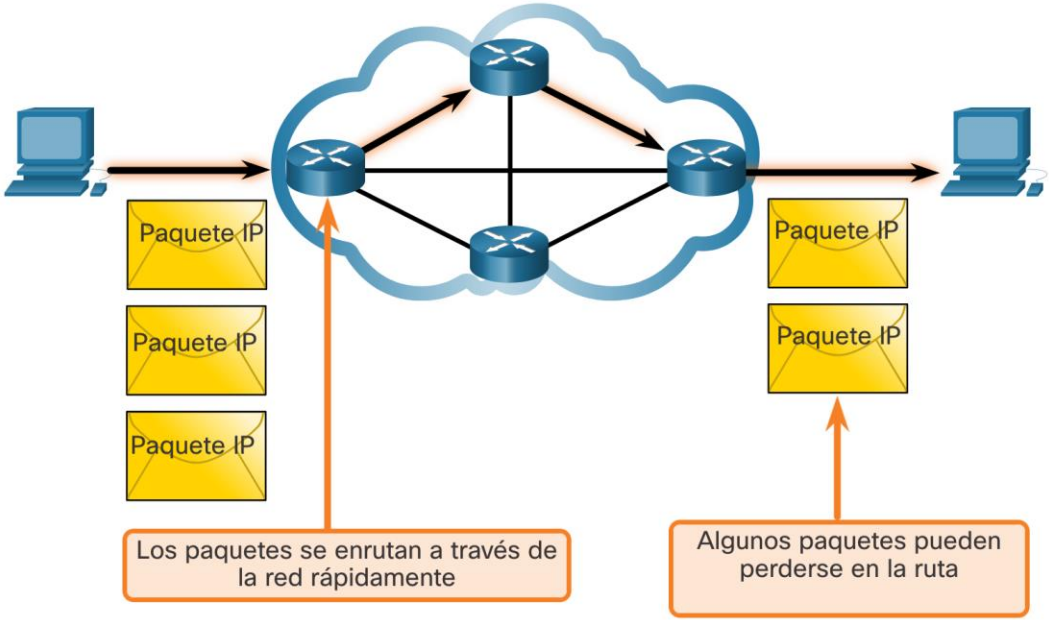
Si hay necesidad de tráfico orientado a la conexión, otro protocolo se encargará de esto (normalmente TCP en la capa de transporte).

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Mejor esfuerzo

IP es mejor esfuerzo

- IP no garantizará la entrega del paquete.
- IP reduce la sobrecarga ya que no existe un mecanismo para reenviar los datos que no se reciben.
- IP no espera confirmaciones.
- IP no sabe si el otro dispositivo está operativo o si recibió el paquete.

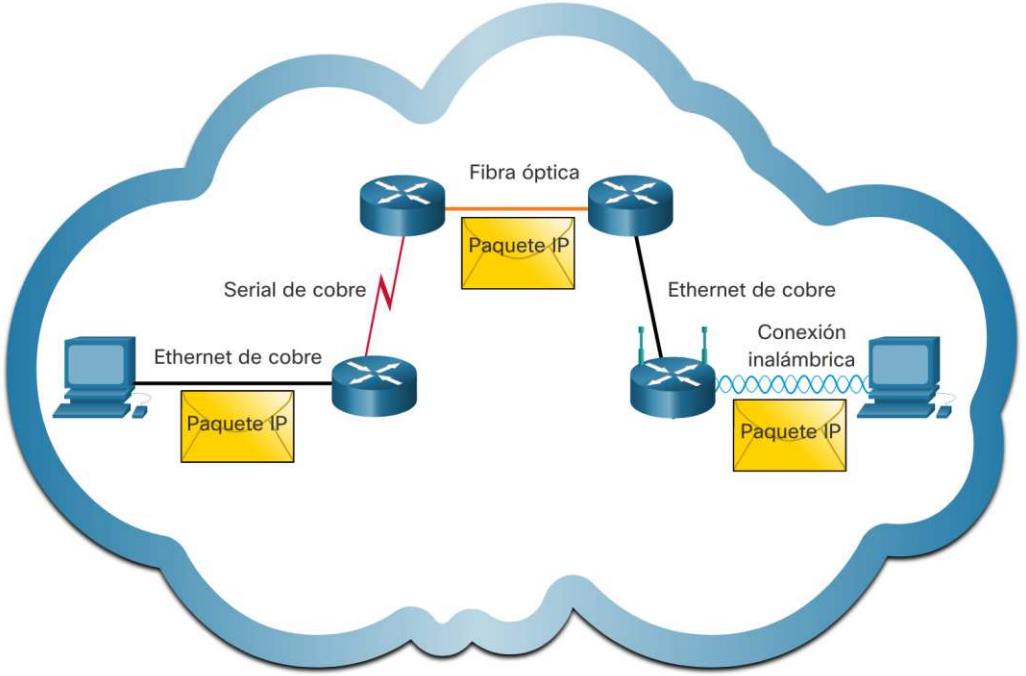


© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Independiente del medio

La IP no es confiable:

- No puede administrar ni reparar paquetes no entregados o corruptos.
- IP no puede retransmitir después de un error.
- IP no puede realinear paquetes fuera de secuencia.
- IP debe depender de otros protocolos para estas funciones.

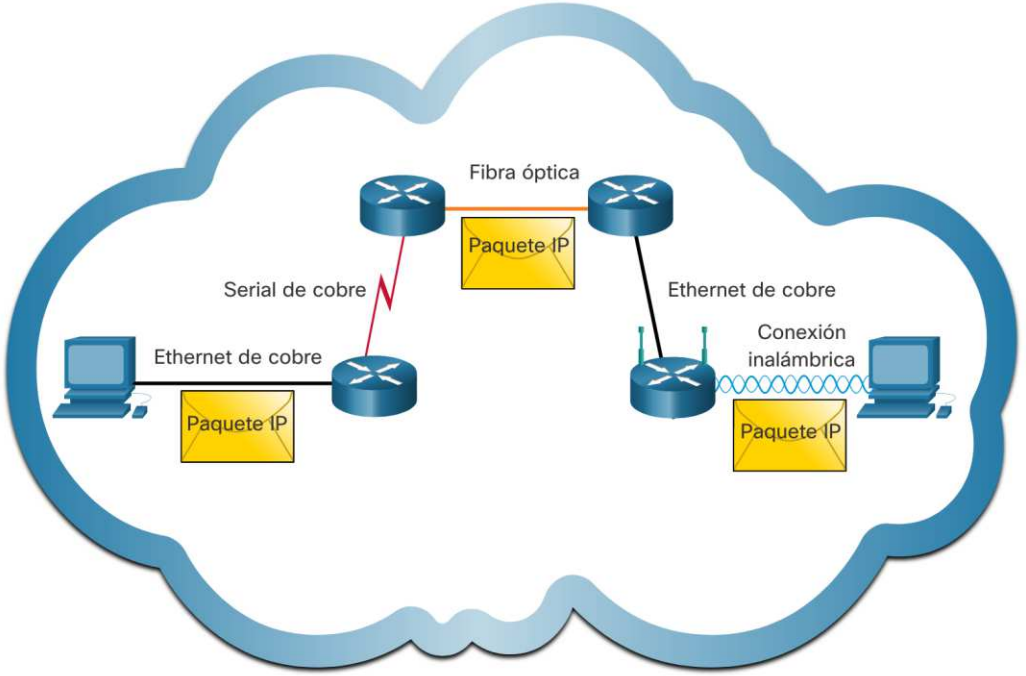


© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Independiente del medio

IP es independiente de los medios:

- IP no se preocupa por el tipo de trama requerida en la capa de enlace de datos o el tipo de medio en la capa física.
- IP se puede enviar a través de cualquier tipo de medio: cobre, fibra o inalámbrico.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Independiente del medio

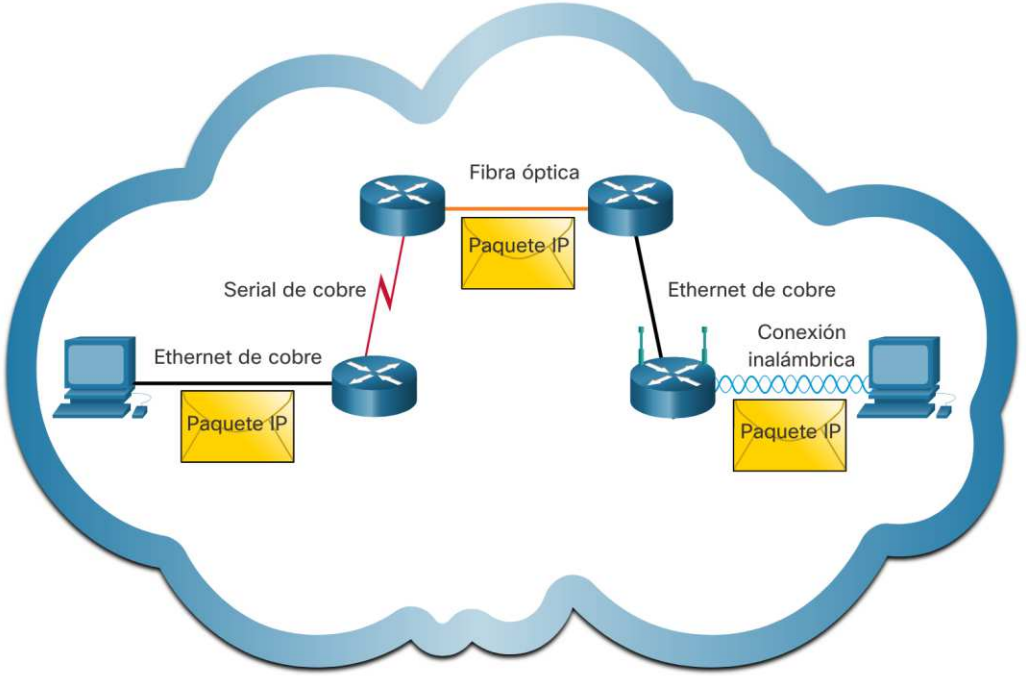
La capa de red establecerá el valor de Unidad de transmisión máxima (MTU).

- La capa de red recibe esto de la información de control enviada por la capa de enlace de datos.
- Luego, la red establece el tamaño de MTU.

La fragmentación es cuando la capa 3 divide el paquete IPv4 en unidades más pequeñas.

- Fragmentar provoca latencia.
- IPv6 no fragmenta los paquetes.

Ejemplo: el enrutador pasa de Ethernet a una WAN lenta con una MTU más pequeña



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

8.2 Paquete IPv4

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Encabezado IPv4

IPv4 es el protocolo de comunicación principal para la capa de red.

El encabezado de red tiene muchos propósitos:

- Asegura que el paquete se envíe en la dirección correcta (al destino).
- Contiene información para el procesamiento de la capa de red.
- La información del encabezado es utilizada por todos los dispositivos de capa 3 que manejan el paquete.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Paquete IPv4

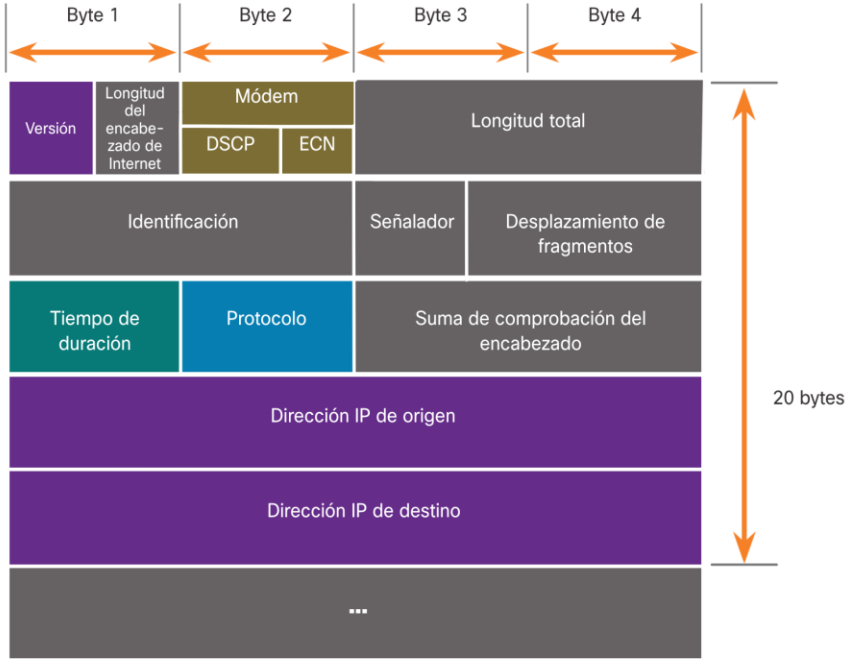
Las características del encabezado de red IPv4:

- Está en binario.
- Contiene varios campos de información

El diagrama se lee de izquierda a derecha, 4 bytes por línea

- Los dos campos más importantes son el origen y el destino.

Los protocolos pueden tener una o más funciones.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Campos del encabezado IPv4

Campos importantes en el encabezado de IPv4:

Function	Description
Version	Para diferencia v4 y v6, para este caso 4 bits = 0100
Differentiated Services	Usado para QoS: DiffServ - campo DS o IntServ - ToS o tipo de servicio más antiguo
Header Checksum	Para detectar integridad el encabezado de IPv4
Time to Live (TTL)	Recuento de saltos de capa 3. Cuando llegue a cero, el enrutador descartará el paquete.
Protocol	Protocolo de siguiente nivel de ID: ICMP, TCP, UDP, etc.
Source IPv4 Address	Dirección de origen (32 bit)
Destination IPV4 Address	Dirección de destino (32 bit)

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Video – Encabezados IPv4 en Wireshark (8.2.3)

Este video muestra lo siguiente:

- Paquetes IPv4 en Wireshark
- La información de control
- La diferencia entre paquetes

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

8.3 Paquetes IPv6

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Limitaciones de IPv4

IPv4 tiene tres limitaciones principales:

- Escases de direcciones IPv4: básicamente ya no hay direcciones IPv4.
- Falta de conectividad de un extremo a otro: para que IPv4 pudiera sobrevivir, se crearon direcciones privadas y NAT. Esto puso fin a las comunicaciones directas con direcciones públicas.
- Mayor complejidad de la red: NAT se pensó como una solución temporal y crea problemas en la red como un efecto secundario de la manipulación del direccionamiento de los encabezados de la red. NAT provoca problemas de latencia y resolución de problemas.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Información general IPv6

IPv6 fue desarrollado por Internet Engineering Task Force (IETF).

- IPv6 supera las limitaciones de IPv4.
- Mejoras que proporciona IPv6:
- Mayor espacio de direcciones: basado en una dirección de 128 bits, no en 32 bits
- Manejo de paquetes mejorado: encabezado simplificado con menos campos
- Elimina la necesidad de NAT: dado que hay una gran cantidad de direccionamiento, no es necesario utilizar el direccionamiento privado internamente y asignarse a una dirección pública compartida

Comparación del espacio de direcciones IPv4 e IPv6

Nombre del número	Notación científica	Cantidad de ceros
Mil	10^3	1000
1 millón	10^6	1 000000
1000 millones	10^9	1000000000
1 billón	10^12	1000000000000
1000 billones	10^15	1000000000000000
1 trillón	10^18	1000000000000000000
1000 trillones	10^21	1000000000000000000000
1 cuatrillón	10^24	1000000000000000000000000
1000 cuatrillones	10^27	1000000000000000000000000000
1 quintillón	10^30	1000000000000000000000000000000
1000 quintillones	10^33	1000000000000000000000000000000000
1 sextillón	10^36	1000000000000000000000000000000000000

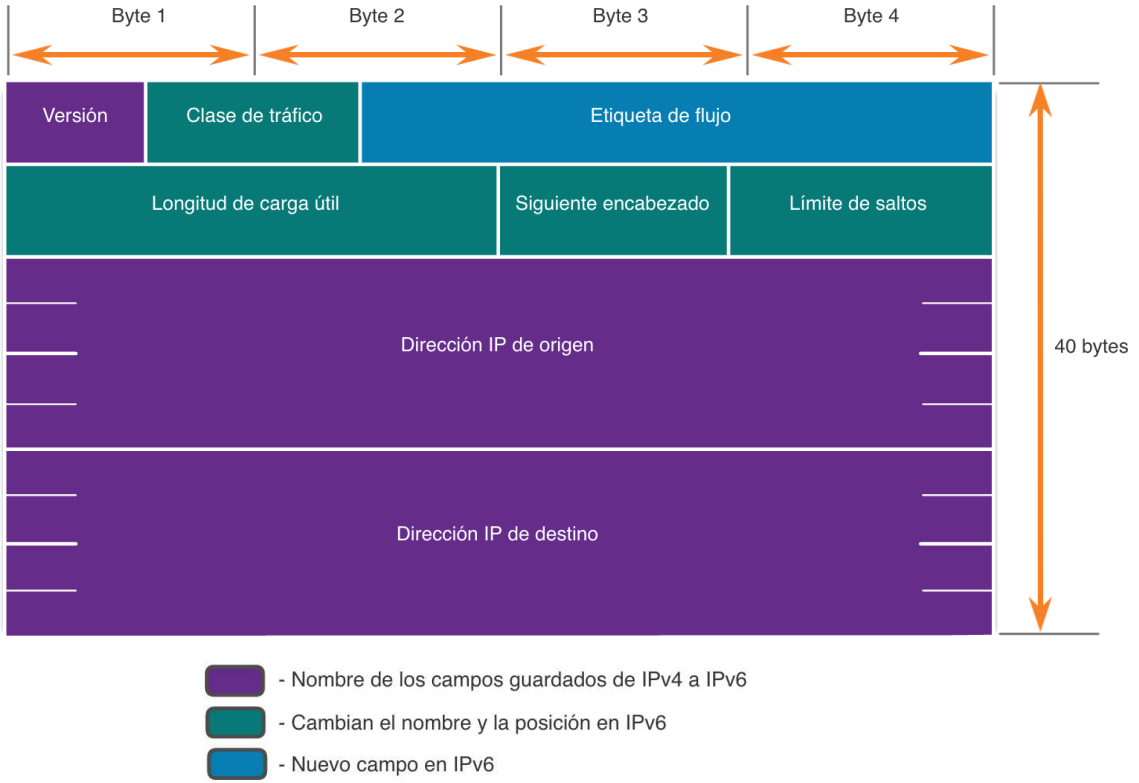
Hay 4000 millones de direcciones IPv4.

Hay 340 sextillones de direcciones IPv6.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Campos del encabezado de paquetes IPv6

- El encabezado de IPv6 está simplificado, pero no más pequeño.
- El encabezado se fija en 40 bytes u octetos de longitud.
- Se eliminaron varios campos de IPv4 para mejorar el rendimiento.
- Se eliminaron algunos campos de IPv4 para mejorar el rendimiento:
  - Señalador
  - Desplazamiento de fragmento
  - Suma de comprobación del encabezado



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Encabezado IPv6

Significant fields in the IPv4 header:

Function	Description
Version	Para diferencia v4 y v6, para este caso 4 bits = 0110
Traffic Class	Utilizado para QoS: Equivalente a DiffServ – DS
Etiqueta de flujo	Informa al dispositivo para manejar etiquetas de flujo idénticas de la misma manera, campo de 20 bits
Longitud de carga util	Este campo de 16 bits indica la longitud de la porción de datos o la carga útil del paquete IPv6
Siguiente encabezado	Protocolo de siguiente nivel de ID: ICMP, TCP, UDP, etc.
Limite de salto	Remplaza a TTL
Source IPv4 Address	Dirección de origen (128 bit)
Destination IPV4 Address	Direccion de destino (128)

Encabezado IPv6 (Cont.)

El paquete IPv6 también puede contener encabezados de extensión (EH).

Características de los encabezados EH:

- proporcionar información de capa de red opcional
- son opcionales
- se colocan entre el encabezado IPv6 y la carga útil
- puede usarse para fragmentación, seguridad, soporte de movilidad, etc.

Nota: a diferencia de IPv4, los enrutadores no fragmentan los paquetes IPv6.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Video – Encabezados IPv6 en Wireshark(8.3.5)

Este video trata lo siguiente:

- Paquetes de Ethernet IPv6 en Wireshark
- La información de control
- La diferencia entre paquetes

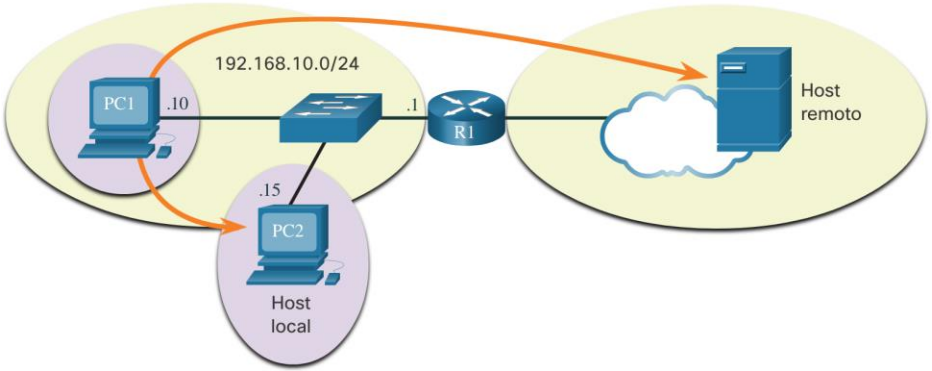
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

8.4 Como enrutan los host

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Decisión de reenvío de host

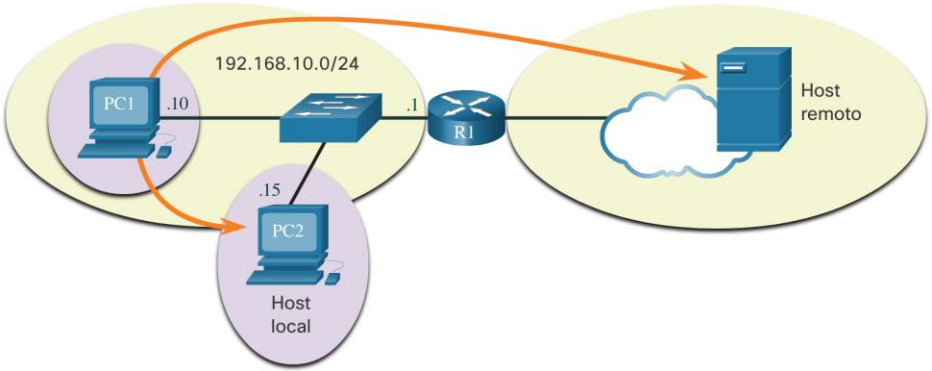
- Los paquetes siempre se crean en el origen.
- Cada dispositivo host crea su propia tabla de enrutamiento.
- Un host puede enviar paquetes a:
  - Sí mismo - 127.0.0.1 (IPv4), :: 1 (IPv6)
  - Hosts locales: el destino está en la misma LAN
  - Hosts remotos: los dispositivos no están en la misma LAN



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Decisión de reenvío de host (Cont.)

- El dispositivo de origen determina si el destino es local o remoto
- Método de determinación:
  - IPv4: el origen utiliza su propia dirección IP y máscara de subred, junto con la dirección IP de destino.
  - IPv6: la fuente utiliza la dirección de red y el prefijo anunciado por el enrutador local.
- El tráfico local se descarga de la interfaz del host para que lo maneje un dispositivo intermediario.
- El tráfico remoto se reenvía directamente a la puerta de enlace predeterminada en la LAN.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Puerta de enlace predeterminada

Un enrutador o conmutador de capa 3 puede ser una puerta de enlace predeterminada.

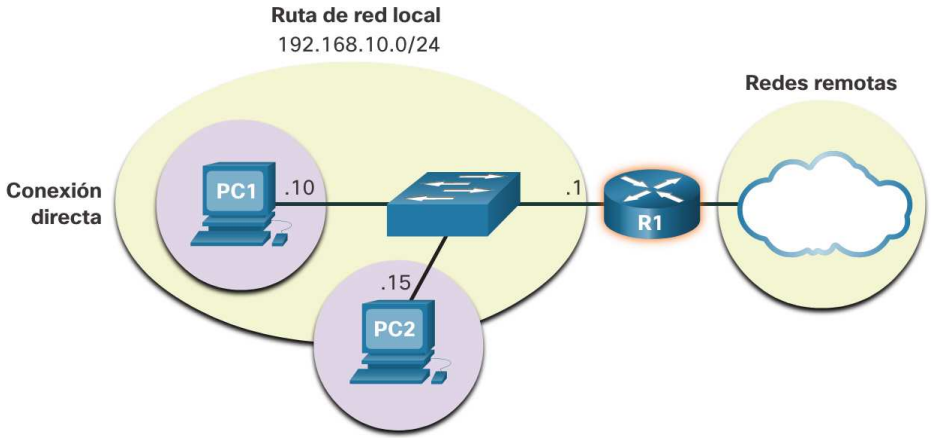
Características de una puerta de enlace predeterminada (DGW):

- Debe tener una dirección IP en el mismo rango que el resto de la LAN.
- Puede aceptar datos de la LAN y es capaz de reenviar el tráfico fuera de la LAN.
- Puede enrutarse a otras redes.
- Si un dispositivo no tiene una puerta de enlace predeterminada o una puerta de enlace predeterminada incorrecta, su tráfico no podrá salir de la LAN.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Un host enruta a la puerta de enlace predeterminada

- El host conocerá la puerta de enlace predeterminada (DGW) de forma estática o mediante DHCP en IPv4.
- IPv6 envía el DGW a través de una solicitud de enrutador (RS) o se puede configurar manualmente.
- Un DGW es una ruta estática que será una ruta de último recurso en la tabla de enrutamiento.
- Todos los dispositivos de la LAN necesitarán el DGW del enrutador si pretenden enviar tráfico de forma remota.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Tablas de enrutamiento de Host

- En Windows, **route print** o **netstat -r** para mostrar la tabla de enrutamiento de la PC
- Tres secciones mostradas por estos dos comandos:
  - Lista de interfaces: todas las interfaces potenciales y direccionamiento MAC
  - Tabla de enrutamiento IPv4
  - Tabla de enrutamiento IPv6

IPv4 Routing Table for PC1

```
C:\Users\PC1> netstat -r

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    192.168.10.1    192.168.10.10      25
        127.0.0.0        255.0.0.0         On-link         127.0.0.1     306
        127.0.0.1  255.255.255.255         On-link         127.0.0.1     306
  127.255.255.255  255.255.255.255         On-link         127.0.0.1     306
    192.168.10.0    255.255.255.0         On-link    192.168.10.10     281
   192.168.10.10  255.255.255.255         On-link    192.168.10.10     281
  192.168.10.255  255.255.255.255         On-link    192.168.10.10     281
        224.0.0.0        240.0.0.0         On-link         127.0.0.1     306
        224.0.0.0        240.0.0.0         On-link    192.168.10.10     281
  255.255.255.255  255.255.255.255         On-link         127.0.0.1     306
  255.255.255.255  255.255.255.255         On-link    192.168.10.10     281
```

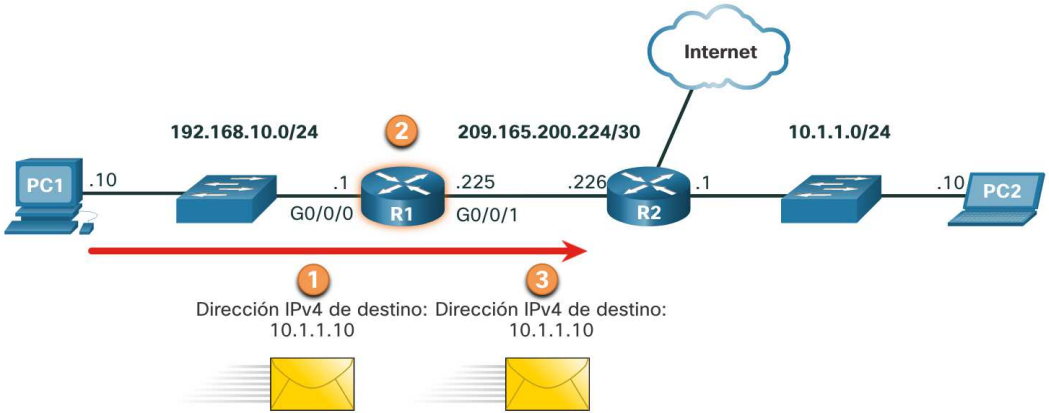
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

8.5 Introducción a enrutamiento

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Decisión de envío de paquetes del router

¿Qué sucede cuando llega un paquete a la interfaz de un router?



1. El paquete llega a la interfaz Gigabit Ethernet 0/0/0 del router R1. R1 desencapsula el encabezado Ethernet de Capa 2 y el remolque.
2. El router R1 examina la dirección IPv4 de destino del paquete y busca la mejor coincidencia en su tabla de enrutamiento IPv4. La entrada de ruta indica que este paquete se reenviará al router R2.
3. El router R1 encapsula el paquete en un nuevo encabezado Ethernet y remolque, y reenvía el paquete al siguiente router de salto R2.

Tabla de enrutamiento del R1

Route	Next Hop or Exit Interface
192.168.10.0 /24	G0/0/0
209.165.200.224/30	G0/0/1
10.1.1.0/24	**via R2**
Default Route 0.0.0.0/0	via R2

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Tabla de enrutamiento IP del router

Hay tres tipos de rutas en la tabla de enrutamiento de un enrutador:

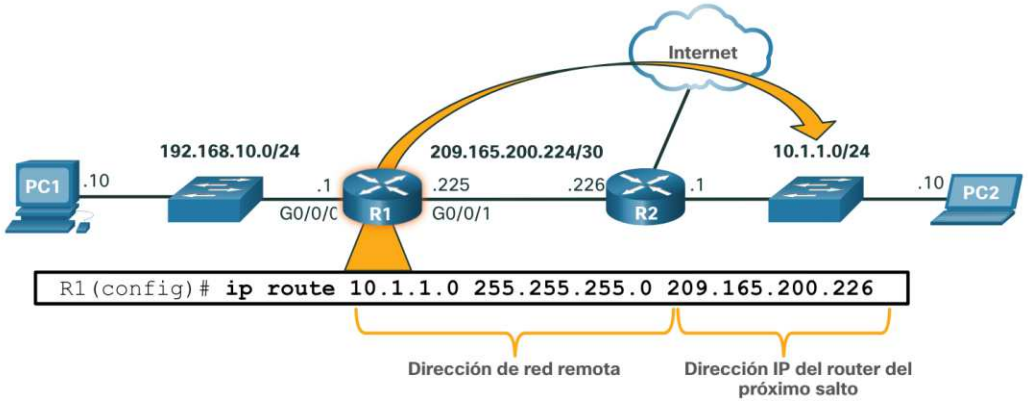
- **Directamente connectado** – el enrutador agrega automáticamente estas rutas, siempre que la interfaz esté activa y tenga direccionamiento.
- **Remote** – estas son las rutas que el enrutador no tiene una conexión directa y se pueden aprender:
  - Manualmente – con una ruta estática
  - Dinámicamente – mediante el uso de un protocolo de enrutamiento para que los enrutadores compartan su información entre sí
- **Ruta predeterminada** – a donde se reenvía todo el tráfico cuando no hay una coincidencia en la tabla de enrutamiento.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

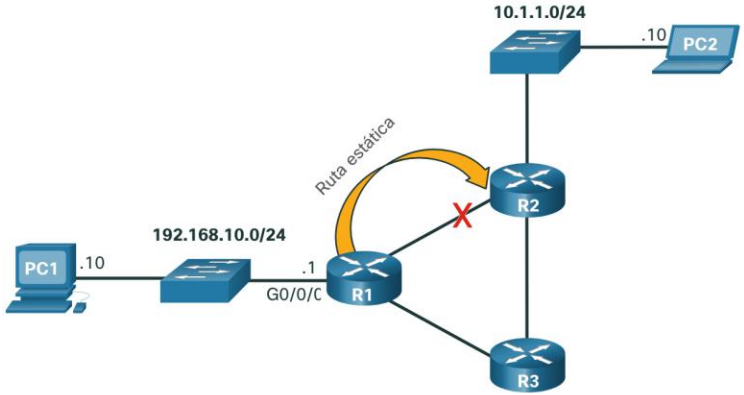
Ruta estática

Características de la ruta estática:

- Debe configurarse manualmente
- El administrador debe ajustarlo manualmente cuando haya un cambio en la topología
- Conveniente para redes pequeñas no redundantes
- A menudo se usa junto con un protocolo de enrutamiento dinámico para configurar una ruta predeterminada



R1 se configura manualmente con una ruta estática para llegar a la red 10.1.1.0/24. Si esta ruta cambia, R1 requerirá una nueva ruta estática.



Si la ruta desde R1 a R2 ya no está disponible, debería configurarse una nueva ruta estática a través de R3. Una ruta estática no se ajusta automáticamente para los cambios de topología.

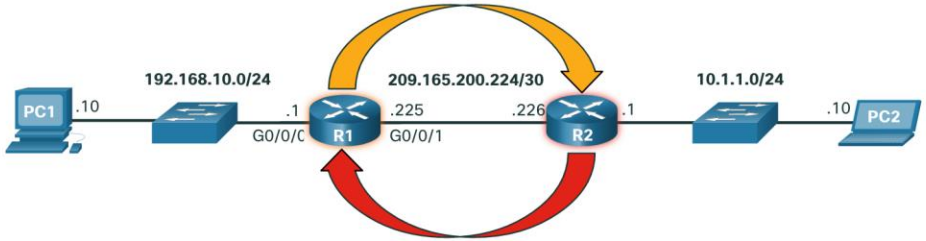
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Enrutamiento dinámico

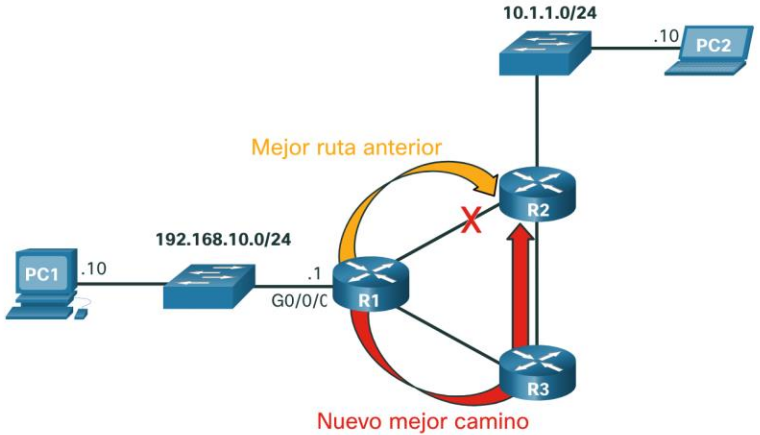
Rutas dinámicas automáticamente:

- Descubren redes remotas
- Mantienen la información actualizada
- Eligen el mejor camino hacia el destino.
- Encuentran nuevas y mejores rutas cuando haya un cambio de topología

El enrutamiento dinámico también puede compartir rutas estáticas predeterminadas con los otros enrutadores.



- R1 está utilizando el protocolo de enrutamiento OSPF para que R2 sepa acerca de la red 192.168.10.0/24.
- R2 está utilizando el protocolo de enrutamiento OSPF para que R1 sepa acerca de la red 10.1.1.0/24.



R1, R2 y R3 están utilizando el protocolo de enrutamiento dinámico OSPF. Si hay un cambio de topología de red, se pueden ajustar automáticamente para buscar una nueva mejor ruta.

Video – Tablas de enrutamiento de router IPv4 (8.5.5)

Este video explica la información en la tabla de enrutamiento del enrutador IPv4.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

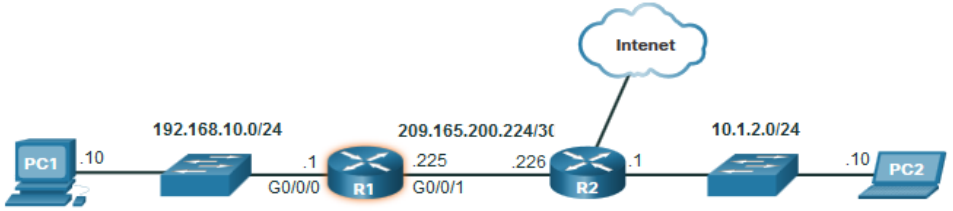
Introduction to an IPv4 Routing Table

El comando **show ip route** muestra la tabla de enrutamiento

- **L** - Dirección IP de la interfaz local conectada directamente
- **C** – Red directamente conectada
- **S** – a ruta estática fue configurada manualmente por un administrador
- **O** – OSPF
- **D** – EIGRP

Este comando muestra tipos de rutas:

- Conectado directamente: C y L
- Rutas remotas: O, D, etc.
- Rutas predeterminadas - S *




```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
Gateway of last resort is 209.165.200.226 to network 0.0.0.0
S*    0.0.0.0/0 [1/0] via 209.165.200.226, GigabitEthernet0/0/1
      10.0.0.0/24 is subnetted, 1 subnets
O        10.1.1.0 [110/2] via 209.165.200.226, 00:02:45, GigabitEthernet0/0/1
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected, GigabitEthernet0/0/0
L        192.168.10.1/32 is directly connected, GigabitEthernet0/0/0
      209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C        209.165.200.224/30 is directly connected, GigabitEthernet0/0/1
L        209.165.200.225/32 is directly connected, GigabitEthernet0/0/1
R1#
```

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

¿Qué aprendrió en este módulo?

- IP es sin conexión, mejor esfuerzo y es independiente de los medios.
- IP no garantiza la entrega de paquetes.
- El encabezado IPv4 consta de campos que contienen información del paquete.
- IPv6 supera la falta de conectividad de un extremo a otro de IPv4 y con una menor complejidad de la red.
- Un dispositivo determinará si un destino es él mismo, otro host local y un host remoto.
- Una puerta de enlace predeterminada es un enrutador que forma parte de la LAN y se utilizará como puerta a otras redes.
- La tabla de enrutamiento contiene una lista de todas las direcciones de red conocidas (prefijos) y dónde reenviar los paquetes.
- El enrutador utiliza la máscara de subred más larga o la coincidencia de prefijo.
- La tabla de enrutamiento tiene tres tipos de entradas de ruta: redes conectadas directamente, redes remotas y una ruta predeterminada.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential


CISCO