Auxiliar de Ciberseguridad

Año 2022

Guía 1

Aspectos Básicos de Networking

Edward Nova
Tutor

CONTENIDO

DENOMINACIÓN DEL MÓDULO DE APRENDIZAJE
Aspectos Básicos de Networking

COMPETENCIA FINAL DEL MÓDULO:
Al finalizar la cualificación la persona participante estará en capacidad de gestionar aplicaciones prácticas de sistemas de networking, bajo supervisión con cierto grado de autonomía.

RESULTADOS DE APRENDIZAJE

1. Administra distintos tipos de redes, para brindar acceso a dispositivos de usuarios finales.

2. Configura parámetros iniciales del switch con Cisco IOS, para manejar los aspectos básicos de comunicaciones, sus reglas, codificación, encapsulamiento y opciones de entrega.

3. Ejecuta comandos para identificar las direcciones de red y de enlaces de datos.

4. Diseña una red de entorno pequeño, para ser implementada.

- INTRODUCCIÓN A LOS ASPECTOS BÁSICOS DE REDES CISCO:

En la actualidad nos encontramos en un momento decisivo respecto del uso de la tecnología para extender y potenciar nuestra red humana. La globalización de Internet se ha producido más rápido de lo que cualquiera hubiera imaginado. El modo en que se producen las interacciones sociales, comerciales, políticas y personales cambia en forma continua para estar al día con la evolución de esta red global. En la próxima etapa de nuestro desarrollo, los innovadores usarán Internet como punto de inicio para sus esfuerzos, creando nuevos productos y servicios diseñados específicamente para aprovechar las capacidades de la red.

Mientras los desarrolladores empujan los límites de lo posible, las capacidades de las redes interconectadas que forman Internet tendrán una función cada vez más importante en el éxito de esos proyectos.

• CONCEPTOS BÁSICOS DE RED.

Una red es un conjunto de dispositivos físicos "hardware" y de programas "software", mediante el cual podemos comunicar computadoras para compartir recursos (discos, impresoras, programas, etc.) así como trabajo (tiempo de cálculo, procesamiento de datos, etc.). A cada una de las computadoras conectadas a la red se le denomina un nodo.

• LA COMUNICACIÓN EN UN MUNDO CENTRADO EN LA RED.

Entre todos los elementos esenciales para la existencia humana, la necesidad de interactuar está por debajo de la necesidad de sustentar la vida. La comunicación es casi tan importante para nosotros como el aire, el agua, los alimentos y un lugar para vivir. Los métodos que utilizamos para compartir ideas e información están en constante cambio y evolución. Mientras la red humana estuvo limitada a conversaciones cara a cara, el avance de los medios ha ampliado el alcance de nuestras comunicaciones. Desde la prensa escrita hasta la televisión, cada nuevo desarrollo ha mejorado la comunicación.

Al igual que con cada avance en la tecnología de comunicación, la creación e interconexión de redes de datos sólidas tiene un profundo efecto.

• LA RED COMO PLATAFORMA COTIDIANA.

La comunicación en nuestra vida cotidiana tiene diferentes formas y existe en muchos entornos. Tenemos diferentes expectativas según si estamos conversando por Internet o participando de una entrevista de trabajo. Cada situación tiene su comportamiento y estilo correspondiente.

Establecimiento de reglas Antes de comenzar a comunicarnos, establecemos reglas o acuerdos que rigen la conversación. Estas reglas o protocolos deben respetarse para que el mensaje se envíe y comprenda correctamente. Algunos de los protocolos que rigen con éxito las comunicaciones humanas son:

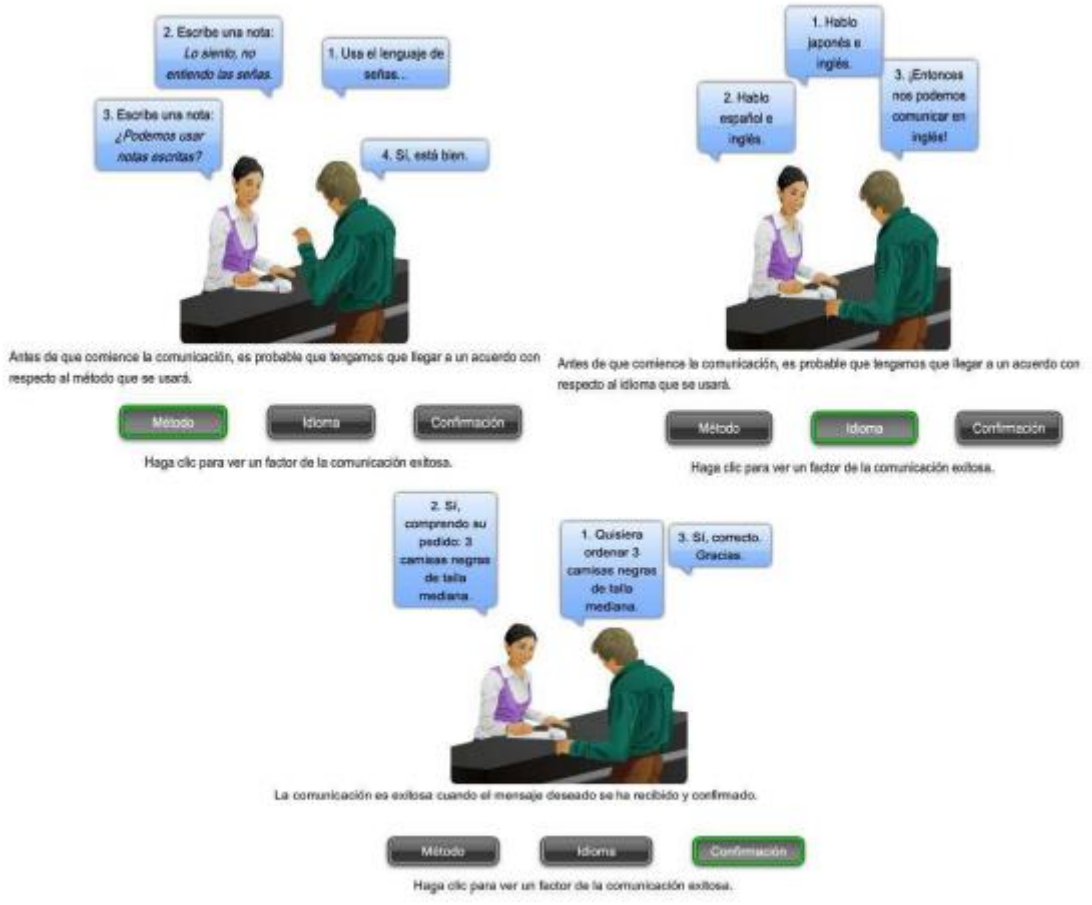
- emisor y receptor identificados,
- método de comunicación consensuado (cara a cara, teléfono, carta, fotografía),
- idioma y gramática comunes,
- velocidad y puntualidad en la entrega, y

- requisitos de confirmación o acuse de recibo.

Las reglas de comunicación pueden variar según el contexto. Si un mensaje transmite un hecho o concepto importante, se necesita una confirmación de que el mensaje se recibió y comprendió correctamente. Los mensajes menos importantes pueden no requerir acuse de recibo por parte del receptor.

Las técnicas utilizadas en las comunicaciones de red comparten estos fundamentos con las conversaciones humanas.

Se presuponen algunas reglas debido a que muchos de los protocolos de comunicación humana son implícitos y están arraigados en nuestra cultura. Al establecer las redes de datos, es necesario ser mucho más explícito sobre la forma en que se realizan y juzgan con éxito las comunicaciones.



• IMPACTO DE LAS REDES EN EL DIARIO VIVIR.

La privacidad en la red es un factor realmente importante que debemos tener en cuenta. Es fundamental en nuestras vidas y la mayoría de los usuarios de internet cada día son más conscientes de ello. La privacidad ha venido ganando importancia a medida que se ha extendido la toma de conciencia sobre las implicaciones de ser parte en redes sociales.

Sin embargo, su uso se ha extendido muy habitualmente antes de saber las implicancias de este y, en no pocas ocasiones, el aprendizaje ha llegado a través de traspiés, accidentes y fracasos.

En este contexto, se ha evidenciado la importancia de la seguridad y la privacidad online, que, aún ganará más importancia en el futuro. Cuidar de la privacidad es algo común a los intereses de cualquier usuario, pero especialmente importante y sensible cuando hablamos de menores edad, que aún tienen conductas despreocupadamente inconscientes de las consecuencias que puede tener su actividad digital.

Más allá de la industria o los reguladores, es elemental que los propios usuarios cuiden y se preocupen por la privacidad de sus datos. La información es propiedad del usuario y, por tanto, es el usuario el único con derecho a controlarlo. Es por eso que se tiene que exigir respecto absoluto a la privacidad del individuo como un valor universal ya que debemos tener garantizado que internet sea nuestro espacio de libertad y confianza.

- CONCEPTOS BÁSICOS DE RED.

Red de Computadoras

Una red es un conjunto de dispositivos físicos "hardware" y de programas "sofware", mediante el cual podemos comunicar computadoras para compartir recursos (discos, impresoras, programas, etc.) así como trabajo (tiempo de cálculo, procesamiento de datos, etc.). A cada una de las computadoras conectadas a la red se le denomina un nodo.

Los dispositivos físicos necesarios para construir una red son la tarjeta de comunicación instalada en cada una de las computadoras conectadas, el cableado que los une y los programas. Los programas de la red serán aquellos que establecen la comunicación entre las estaciones y los periféricos.

Las redes difieren entre sí por los servicios que pueden prestar a los usuarios, o por el tipo comunidad de usuarios atraídos por el servicio. Podemos dividir las redes de computadoras en las siguientes categorías principales, redes vinculadas a Internet que ofrecen las herramientas "Internet", redes fuera de líneas, proveedores de servicios comerciales, redes de conmutación (PSN).

El motivo para establecer una red de computadoras nos permite entender qué es una red y por qué esta puede ser de utilidad en una organización o institución tales como:

Compartir de programas y archivos

Las versiones de "software" para redes están disponibles con un ahorro en el precio comparativamente bajo a la compra de licencias de copias individuales. Los programas y sus archivos de datos se pueden guardar en un servidor de archivos al que pueden accesar muchos usuarios de la red a la misma vez.

Compartir de recursos de red

Entre los recursos de la red se incluyen las impresoras, los "Plotters" y los dispositivos de almacenamiento como torres opticas o de disco. De esta forma la red proporciona un enlace de comunicación que permite que los usuarios compartan estos dispositivos.

Compartir de base de datos

Un servidor de bases de datos es una aplicación ideal para una red. Una función de la red denominada bloqueo de registros permite que varios usuarios puedan accesar a la vez a un archivo sin corromper los datos. Con el bloqueo de registros se asegura que dos usuarios no pueden accesar al mismo registro simultáneamente.

Expansión económica de la Organización

Las redes proporcionan una forma económica de aumentar el número de computadoras de una organización o institución. A la red se pueden conectar estaciones de trabajo baratas sin disco que utilicen el disco fijo del servidor para el arranque y el almacenamiento.

Crear grupos de trabajo

Una red proporciona una forma de crear grupos de usuarios, dentro de una organización, que no necesariamente tienen qué encontrarse dentro de un mismo departamento. Los grupos de trabajo facilitan las nuevas estructuras corporativas en las que personas de distintos y lejanos departamentos pertenecen a un proyecto o a grupos especiales.

Correo electrónico(E-mail)

El correo electrónico permite que los ususarios puedan comunicarse fácilmente entre ellos. Los mensajes se dejan en <> para que los destinatarios los lean cuando estos quieran.

Programas de grupo y de flujo de trabajo

Los programas de grupo y de flujo de trabajo se han diseñado específicamente para las redes y aprovechan los sistemas de correo electrónico para ayudar a los usuarios a colaborar en proyectos, programación de tareas y el proceso de documentación al igual que el de aprobación de las etapas .

Centralizar las operaciones

Una red proporciona una forma de centralizar servidores y sus datos junto con otros recursos. Las actualizaciones del "hardware", las copias de seguridad del "software", el mantenimiento del sistema y la protección de éste resultan mucho más sencillas de manejar cuando los equipos están situados en solo lugar.

Mejorar las estructura corporativa

Las redes pueden cambiar la estructura de una organización y la forma en que se trabaja. Los usuarios que trabajan en un departamento específico o para una persona en específico ya no es necesario que se encuentren en la misma área física. Sus oficinas pueden encontrarse en donde su experiencia sea más necesaria. La red une los supervisores y compañeros de trabajo.

- LA RED COMO PLATAFORMA COTIDIANA.

Teléfonos móviles

Una manera común que utilizan las personas para conectarse es a través de sus teléfonos móviles. ¿Sabía que la mayoría de los teléfonos móviles pueden conectarse a diferentes tipos de redes simultáneamente? Repasemos algunas de las maneras en las que los teléfonos móviles, y los smartphones en particular, interactúan con las diversas tecnologías de red y aprendamos algo de terminología nueva en el proceso.

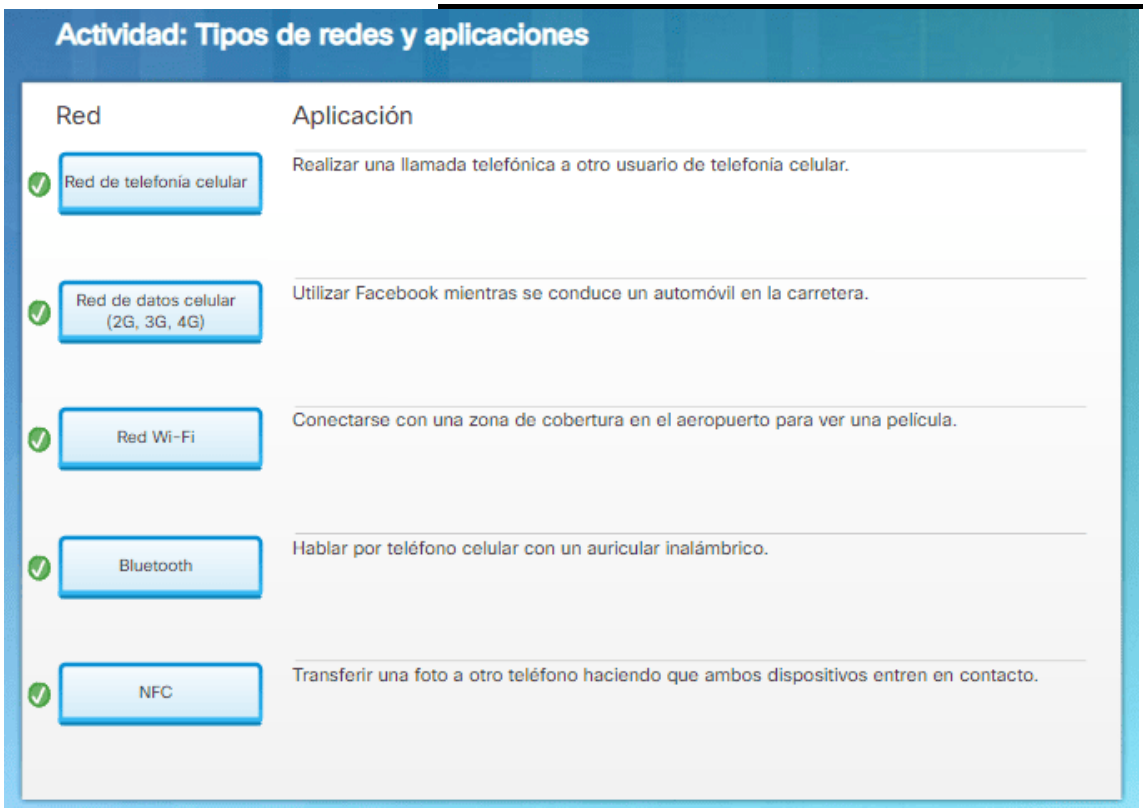
Los teléfonos móviles utilizan ondas de radio para transmitir señales de voz a las antenas montadas en las torres ubicadas en áreas geográficas específicas. Los teléfonos móviles se suelen denominar “teléfonos celulares” porque el área geográfica en la que una torre individual puede proporcionar una señal a un teléfono se denomina celda. Cuando se realiza una llamada telefónica, la señal de voz se transmite de una torre a otra hasta que llega a su destino. Este tipo de red se utiliza cuando usted realiza una llamada telefónica a otro teléfono móvil o a un teléfono fijo. También se utiliza para enviar mensajes de texto directamente desde el teléfono. El tipo más común de red de telefonía celular se denomina red GSM, que es la abreviatura del título “Sistema global para comunicaciones móviles (Global System for Mobile Communications)”.

Cómo enviar datos a través de redes de telefonía celular

El diseño de los primeros transmisores de radio para telefonía celular no permitía la transmisión eficiente de datos digitales, por lo que se implementaron mejoras para perfeccionar la manera en la que se envían los datos a través de las redes de telefonía celular. Las abreviaturas 3G, 4G y 4G-LTE se usan para describir las redes mejoradas de telefonía celular que están optimizadas para la transmisión rápida de datos. El letra “G” de estas designaciones representa la palabra “generación”, así que 3G es la tercera generación de la red celular. La mayoría de los teléfonos móviles y smartphones tienen un indicador que muestra cuándo hay una señal 3G o 4G disponible. Cuando el indicador no está encendido, el teléfono se conecta a través de la antigua red 2G que no ofrece grandes velocidades de transferencia de datos.

Diferentes tipos de redes

- Además de los transmisores y receptores GSM y 3G/4G, los smartphones realizan conexiones a distintos tipos de redes. Algunos ejemplos de otras redes que utilizan los smartphones son los siguientes:
- GPS: la red del Sistema de posicionamiento global utiliza satélites para transmitir señales que cubren todo el mundo. El smartphone puede recibir estas señales y calcular la ubicación del teléfono con una exactitud de 10 metros.
- Wi-Fi: los transmisores y receptores Wi-Fi ubicados dentro del smartphone permiten que el teléfono se conecte a redes locales y a Internet. Para recibir y enviar datos a través de una red Wi-Fi, el teléfono tiene que estar dentro del alcance de la señal proveniente de un punto de acceso a la red inalámbrica. Las redes Wi-Fi generalmente son privadas pero, a menudo, ofrecen zonas de cobertura para el acceso o público o de usuarios temporales. Una zona de cobertura es un área donde hay señales Wi-Fi disponibles. Las conexiones de red Wi-Fi en el teléfono son similares a las conexiones de red en una computadora portátil.
- Bluetooth: una tecnología inalámbrica de corto alcance y baja potencia que tiene como objetivo reemplazar a la conectividad cableada en el caso de accesorios como altavoces, auriculares y micrófonos. Dado que la tecnología Bluetooth se puede usar para transmitir datos y voz, se la puede utilizar para crear redes locales pequeñas.
- NFC: NFC es la sigla de Near Field Communications (o Transmisión de datos en proximidad). NFC es una tecnología de comunicación inalámbrica que permite intercambiar datos entre dispositivos que están muy cerca entre sí, generalmente menos de algunos centímetros.



- FUNCIONAMIENTO DE LAS REDES LOCALES Y NO LOCALES.

Red de Área Local. Una red de área local, red local o LAN (del inglés local area network) es la interconexión de varias Computadoras y Periféricos. Su extensión está limitada físicamente a un edificio o a un entorno de 200 metros, o con Repetidores podría llegar a la distancia de un campo de 1 kilómetro. Su aplicación más extendida es la interconexión de computadoras personales y estaciones de trabajo en oficinas, fábricas, etc., para compartir recursos e intercambiar Datos y Aplicaciones. En definitiva, permite una conexión entre dos o más equipos.

El término red local incluye tanto el Hardware como el Software necesario para la interconexión de los distintos dispositivos y el tratamiento de la información.

La función principal de este tipo de redes consiste básicamente en vincular los ordenadores entre sí y proporcionar acceso compartido a archivos, impresoras y otros servicios. Para ello, su arquitectura se clasifica como cliente-servidor o peer-to-peer.

En un tipo de red local cliente-servidor, distintos dispositivos se encuentran conectados a un servidor central, en el que se gestiona el acceso a los dispositivos, aplicaciones, el tráfico de la red y al almacenamiento de los archivos.

Red MAN (Metropolitan Area Network)

Las redes MAN (o redes de área metropolitana en castellano), son un tipo de red cuyo propósito es permitir el intercambio de datos en ciudades o pueblos. Se caracterizan por permitir conexiones de alta velocidad gracias al uso de fibra óptica y otros medios; además, permiten conexiones estables que no se ven afectadas por interferencias radioeléctricas.

Las redes MAN suelen usarse en sistemas de vigilancia.

Red WAN (Wide Area Network)

De trata de redes de cobertura amplia que permiten interconectar redes LAN y MAN con el fin de brindar una conectividad de mayor alcance.

Las redes WAN tienen la potencia suficiente para conectar países a través de redes de menor capacidad. Las empresas que proveen servicios de Internet, por ejemplo, utilizan WAN para que sus clientes puedan navegar.

Una red WAN generalmente se apoya en sistemas de telefonía para facilitar las interconexiones, pero también pueden usarse satélites u otros métodos.

Diferencias principales entre LAN, MAN, WAN

Al comparar los tipos de redes LAN, MAN y WAN se destacan diferencias que pueden ayudarnos a entender mejor en qué caso necesitaremos contratar los servicios de una u otra:

- Las redes LAN cubren áreas geográficas específicas de corto alcance; las MAN ofrecen conectividad a ciudades y pueblos; y las redes WAN conectan redes pequeñas y medianas entre sí para abarcar áreas más extensas.

- Las redes LAN ofrecen mayor velocidad en la transmisión de datos que las redes MAN y WAN.
- La disponibilidad de ancho de banda en las redes LAN es mayor que en MAN y WAN.
- Las redes LAN son de fácil mantenimiento en comparación con las redes MAN y WAN.
- Los fallos en la transmisión de datos y el ruido son mínimos en las redes LAN, ocasionales en las redes MAN y elevados en las redes WAN.

- TERMINOLOGÍAS Y CONCEPTOS DE COMPONENTES Y DISPOSITIVOS DE REDES.

Además de los smartphones y los dispositivos móviles, existen muchos otros componentes que pueden formar parte de una red de área local. Algunos ejemplos de componentes de red son las computadoras personales, los servidores, los dispositivos de red y el cableado. Estos componentes se pueden agrupar en cuatro categorías principales:

- Hosts
- Periféricos
- Dispositivos de red
- Medios de red

Los componentes de red que probablemente conozca más son los hosts y los periféricos compartidos. Recuerde que un host es cualquier dispositivo que envía y recibe mensajes directamente a través de la red.

Los periféricos compartidos no están conectados directamente a la red, sino a los hosts. Por lo tanto, el host es responsable de compartir el periférico a través de la red. Los hosts tienen software configurado a fin de permitir que los usuarios de la red utilicen los dispositivos periféricos conectados.

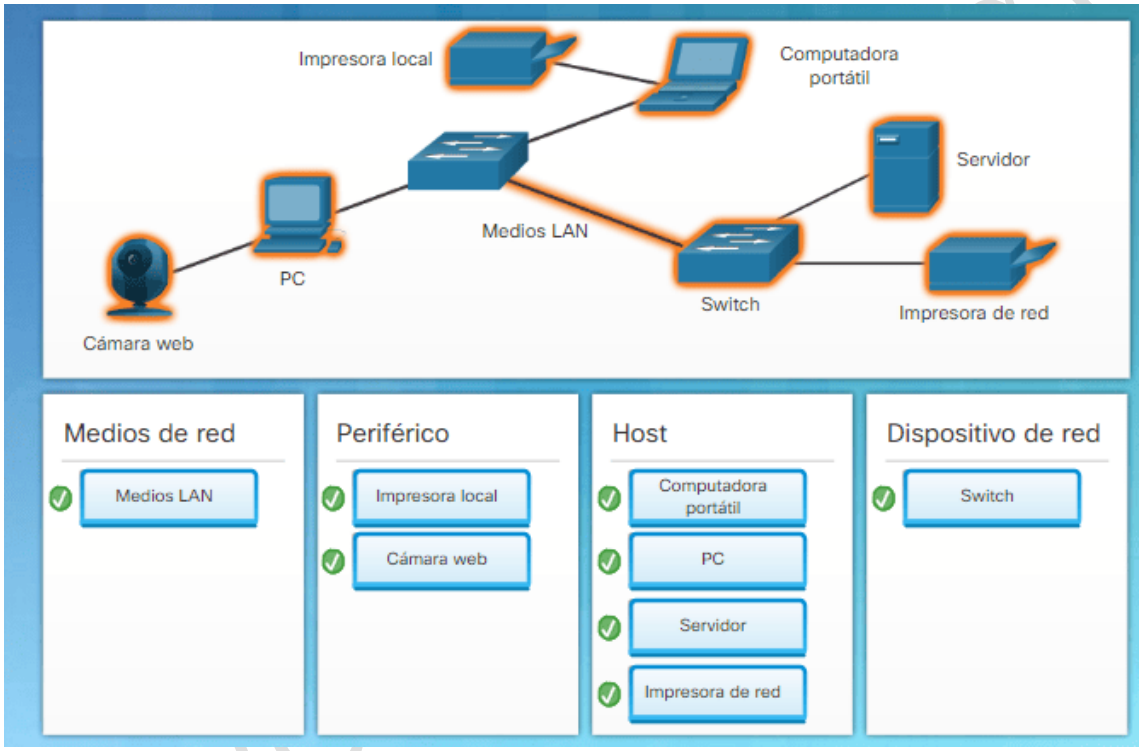
Los dispositivos de red, así como los medios de red, se utilizan para interconectar hosts. Los dispositivos de red a veces se denominan “dispositivos intermedios” porque se ubican generalmente en la ruta que siguen los mensajes entre un host de origen y uno de destino.

El término medios de red describe los cables y los conductores utilizados en las redes cableadas, junto con las ondas de radiofrecuencia utilizadas en las redes inalámbricas. Estas redes cableadas e inalámbricas proporcionan rutas por las que viajan que los mensajes entre los distintos componentes de red.

Algunos dispositivos pueden cumplir más de una función, según la manera en la que estén conectados. Por ejemplo: una impresora conectada directamente a un host (impresora

local) es un periférico. Una impresora que está conectada directamente a un dispositivo de red y participa en forma directa en las comunicaciones de red es un host.

Ethernet es la tecnología comúnmente utilizada en redes de área local. Desarrollada por Xerox PARC, Ethernet fue presentada comercialmente en el año 1980 por Digital Equipment Corporation (DEC), Intel y Xerox. Posteriormente, en 1983, Ethernet se estandarizó como IEEE 802.3. Los dispositivos acceden a la red LAN Ethernet con una Tarjeta de interfaz de red (NIC) Ethernet. Cada NIC Ethernet tiene una dirección única integrada en forma permanente en la tarjeta que se conoce como dirección de Control de acceso al medio (MAC).



- CÓMO IDENTIFICAR TODOS LOS ELEMENTOS DE UNA RED IDENTIFICADO COMO HOSTS.

NIC/MAU (Tarjeta de red)

"Network Interface Card" (Tarjeta de interfaz de red) o "Medium Access Unit" (Medio de unidad de acces). Cada computadora necesita el "hardware" para transmitir y recibir información. Es el dispositivo que conecta la computadora u otro equipo de red con el medio físico. La NIC es un tipo de tarjeta de expansión de la computadora y proporciona un puerto en la parte trasera de la PC al cual se conecta el cable de la red. Hoy en día cada vez son más los equipos que disponen de interfaz de red, principalmente Ethernet, incorporadas. A veces, es necesario, además de la tarjeta de red, un transceptor. Este es un dispositivo que se conecta al medio físico y a la tarjeta, bien porque no sea posible la conexión directa (10base 5) o porque el medio sea distinto del que utiliza la tarjeta.

Hubs (Concentradores)

Son equipos que permiten estructurar el cableado de las redes. La variedad de tipos y características de estos equipos es muy grande. En un principio eran solo concentradores de cableado, pero cada vez disponen de mayor número de capacidad de la red, gestión remota, etc. La tendencia es a incorporar más funciones en el concentrador. Existen concentradores para todo tipo de medios físicos.

Repetidores

Son equipos que actúan a nivel físico. Prolongan la longitud de la red uniendo dos segmentos y amplificando la señal, pero junto con ella amplifican también el ruido. La red sigue siendo una sola, con lo cual, siguen siendo válidas las limitaciones en cuanto al número de estaciones que pueden compartir el medio.

"Bridges" (Puentes)

Son equipos que unen dos redes actuando sobre los protocolos de bajo nivel, en el nivel de control de acceso al medio. Solo el tráfico de una red que va dirigido a la otra atraviesa el dispositivo. Esto permite a los administradores dividir las redes en segmentos lógicos, descargando de tráfico las interconexiones. Los bridges producen las señales, con lo cual no se transmite ruido a través de ellos.

"Routers" (Encaminadores)

Son equipos de interconexión de redes que actúan a nivel de los protocolos de red. Permite utilizar varios sistemas de interconexión mejorando el rendimiento de la transmisión entre redes. Su funcionamiento es más lento que los bridges pero su capacidad es mayor. Permiten, incluso, enlazar dos redes basadas en un protocolo, por medio de otra que utilice un protocolo diferente.

"Gateways"

Son equipos para interconectar redes con protocolos y arquitecturas completamente diferentes a todos los niveles de comunicación. La traducción de las unidades de información reduce mucho la velocidad de transmisión a través de estos equipos.

Servidores de terminales e impresoras

Son equipos que permiten la conexión a la red de equipos periféricos tanto para la entrada como para la salida de datos. Estos dispositivos se ofrecen en la red como recursos compartidos. Así un terminal conectado a uno de estos dispositivos puede establecer

sesiones contra varios ordenadores multiusuario disponibles en la red. Igualmente, cualquier sistema de la red puede imprimir en las impresoras conectadas a un servidor.

Modems

Son equipos que permiten a las computadoras comunicarse entre sí a través de líneas telefónicas; modulación y demodulación de señales electrónicas que pueden ser procesadas por computadoras. Los modems pueden ser externos (un dispositivo de comunicación) o interno (dispositivo de comunicación interno o tarjeta de circuitos que se inserta en una de las ranuras de expansión de la computadora).

El medio: constituido por el cableado y los conectores que enlazan los componentes de la red. Los medios físicos más utilizados son el Cable de par trenzado, Par de cable, Cable coaxial y La fibra óptica (cada vez en más uso esta última).

Concentradores de cableado: una LAN en bus usa solamente tarjetas de red en las estaciones y cableado coaxial para interconectarlas, además de los conectores, sin embargo este método complica el mantenimiento de la red ya que si falla alguna conexión toda la red deja de funcionar. Para impedir estos problemas las redes de área local usan concentradores de cableado para realizar las conexiones de las estaciones, en vez de distribuir las conexiones el concentrador las centraliza en un único dispositivo manteniendo indicadores luminosos de su estado e impidiendo que una de ellas pueda hacer fallar toda la red.

Existen dos tipos de concentradores de cableado:

1. Concentradores pasivos: actúan como un simple concentrador cuya función principal consiste en interconectar toda la Red.

2. Concentradores activos: además de su función básica de concentrador también amplifican y regeneran las señales recibidas antes de ser enviadas.

Los concentradores de cableado tienen dos tipos de conexiones: para las estaciones y para unirse a otros concentradores y así aumentar el tamaño de la Red. Los concentradores de cableado se clasifican dependiendo de la manera en que internamente realizan las conexiones y distribuyen los mensajes. A esta característica se le llama Topología lógica.

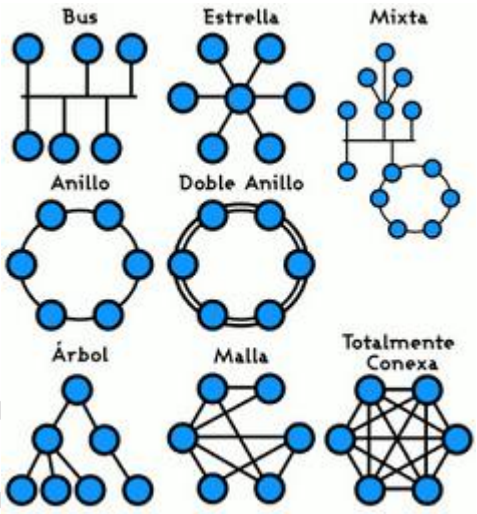
Existen dos tipos principales:

1. Concentradores con topología lógica en bus (HUB): estos dispositivos hacen que la red se comporte como un bus enviando las señales que les llegan por todas las salidas conectadas.

2. Concentradores con topología lógica en anillo (MAU): se comportan como si la red fuera un anillo enviando la señal que les llega por un puerto al siguiente.

- IDENTIFICACIÓN DE DIFERENTES TIPOS DE TOPOLOGÍAS Y SUS ELEMENTOS.

La topología de red define la estructura de una red. Una parte de la definición topológica es la Topología física, que es la disposición real de los Cables o medios. La otra parte es la Topología lógica, que define la forma en que los Hosts acceden a los medios para enviar datos. Las topologías más comúnmente usadas son las siguientes:



Topología de las redes

- LAS NUEVAS TENDENCIAS EN LAS REDES.

Extreme Networks ha recogido en un documento las principales tendencias que en opinión de la compañía definirán el mercado de networking en 2022, y las divide en diferentes apartados.

Networking/Cloud/entornos distribuidos

- Redes multicapa o 'multi-layered Networking'.

El concepto de red multicapa es un nuevo planteamiento de arquitectura que ha surgido en los últimos años, a medida que las redes se han hecho más complejas y distribuidas. En 2022 cogerá impulso este enfoque, que supera el concepto binario tradicional hardware/software, y que plantea contemplar la red de una manera integral y holística, incorporando también la nube y los entornos de conectividad remotos o distribuidos.

- SDN (o redes definidas por software).

SDN seguirá siendo una tecnología crucial debido al crecimiento de la computación en la nube, el aumento en el uso de dispositivos móviles y la necesidad de reducir costes de despliegue, configuración y gestión de red. SDN permite diseñar, desplegar y gestionar la red separando los planos de control y datos, eliminando la infraestructura subyacente

para aplicaciones y servicios de red y haciendo que el plano de control sea directamente programable. Con SDN es posible distribuir la capacidad de computación a sitios remotos, mover las funciones del centro de datos al extremo de la red y dar mejor soporte a nuevas tecnologías como cloud computing o IoT.

- Redes autónomas basadas en inteligencia artificial (IA).

En 2022 se avanzará en la aplicación de tecnologías de IA a la gestión de red, para acercarse a lo que se denomina "Redes Autónomas" y evolucionando desde una automatización básica hacia la red totalmente autónoma. Esta automatización reducirá la implementación manual y la intervención en áreas como la planificación, el aprovisionamiento, la prestación de servicios y las operaciones de red. Esta tendencia vendrá impulsada por la creciente complejidad de la red y la necesidad de realizar cambios en un entorno cambiante, que evoluciona muy rápidamente, muchas veces desbordando la capacidad de los departamentos de TI para llevar a cabo esos cambios de forma manual.

- Home Networking.

La tendencia aparecida con la pandemia de crecimiento del trabajo remoto y las oficinas domésticas seguirá consolidándose y creciendo, a pesar de la prevista vuelta al trabajo presencial. Los entornos de trabajo se han flexibilizado y distribuido. Esto planteará retos de gestión que los responsables de TI deberán abordar, e incrementará la demanda de soluciones de red más sencillas de gestionar, seguras y rápidas.

- Entornos cloud distribuidos.

La diferenciación entre nube pública, privada, híbrida y on-premise se difuminará cada vez más, de forma que los usuarios podrán disfrutar de las ventajas de ambos mundos. El planteamiento de Distributed Cloud permitirá obtener todo el potencial y flexibilidad de la nube utilizando servidores privados locales. La tecnología cloud y los datos asociados a estas plataformas residirán en las instalaciones del usuario, proporcionando computación local, control total y los beneficios operativos de la nube.

- Inteligencia Artificial aplicada a las operaciones de TI (AIOps).

Es otra tendencia tecnológica en alza que afectará a la gestión y soporte de infraestructuras de red. Se trata de utilizar la potencia de la IA como herramienta que ayude a facilitar, automatizar y reducir errores en la gestión y configuración de la red. Esta tecnología ayuda a interpretar los datos y entender mejor los procesos de negocio, para que los departamentos de TI puedan responder mejor a las alertas e incidencias, incluso antes de que se produzcan.

Tecnologías Wi-Fi

En este punto, la firma destaca que 2022 será un año de consolidación del estándar Wi-Fi6 para entornos corporativos. Por otro lado, se espera la puesta en producción del nuevo estándar WI-FI6E, que opera en la banda de frecuencia de 6 GHz. Esta banda ya está abierta en Estados Unidos y en algunos países europeos, aunque la directiva comunitaria

establecía el 1 de diciembre para su habilitación en toda la Unión Europea. Por otro lado, ya están apareciendo en el mercado los primeros dispositivos con soporte Wi-Fi6E.

Seguridad de red

En lo que respecta a la seguridad, Extreme Networks cree que las organizaciones van a seguir evaluando la implementación de tecnologías Zero Trust para protegerse contra los ataques sofisticados y complejos que se han registrado en 2021 y que tendrán continuidad previsiblemente en 2022. Probablemente este año se pueda conocer el resultado de esta estrategia de seguridad adoptada ya por muchas compañías y se puedan identificar las mejores prácticas de uso de esta estrategia.

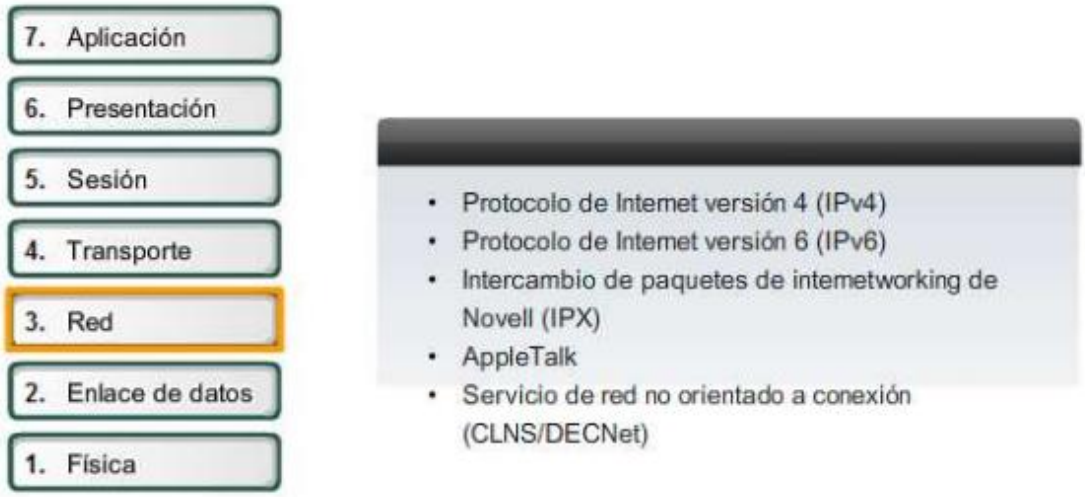
Por último, se habla cada vez más en el mercado de la utilización de las tecnologías de blockchain como mecanismos para proteger los datos personales y las infraestructuras en entornos de smart cities. A medida que las smart cities se acerquen al desarrollo completo, las tecnologías de blockchain se volverán mucho más frecuentes y se utilizarán para proteger la integridad de la información dentro de la infraestructura de la ciudad inteligente, y la información personal crítica. Blockchain también desempeñará un papel en la protección de las identidades digitales, así como en la protección frente a la "guerra cibernética" (ataques a la cadena de suministro o a infraestructuras críticas, securización de procesos electorales).

- PROTOCOLOS DE LA CAPA DE RED.

Los protocolos implementados en la capa de Red que llevan datos del usuario son:

- versión 4 del Protocolo de Internet (IPv4),
- versión 6 del Protocolo de Internet (IPv6),
- intetercambio Novell de paquetes de internetwork (IPX),
- AppleTalk, y
- servicio de red sin conexión (CLNS/DECNet).

El Protocolo de Internet (IPv4 y IPv6) es el protocolo de transporte de datos de la capa 3 más ampliamene utilizado y será el tema de este curso. Los demás protocolos no serán abordados en profundidad.



Como se muestra en la figura, los servicios de capa de Red implementados por el conjunto de protocolos TCP/IP son el Protocolo de Internet (IP). La versión 4 de IP (IPv4) es la versión de IP más ampliamente utilizada. Es el único protocolo de Capa 3 que se utiliza para llevar datos de usuario a través de Internet y es el tema de CCNA. Por lo tanto, será el ejemplo que usamos para protocolos de capa de Red en este curso.

La versión 6 de IP (IPv6) está desarrollada y se implementa en algunas áreas. IPv6 operará junto con el IPv4 y puede reemplazarlo en el futuro. Los servicios provistos por IP, así como también la estructura y el contenido del encabezado de los paquetes están especificados tanto por el protocolo IPv4 como por el IPv6. Estos servicios y estructura de paquetes se usan para encapsular datagramas UDP o segmentos TCP para su recorrido a través de una internetwork.

Las características de cada protocolo son diferentes. Comprender estas características le permitirá comprender la operación de los servicios descritos por este protocolo.

El Protocolo de Internet fue diseñado como un protocolo con bajo costo. Provee sólo las funciones necesarias para enviar un paquete desde un origen a un destino a través de un sistema interconectado de redes. El protocolo no fue diseñado para rastrear ni administrar el flujo de paquetes. Estas funciones son realizadas por otros protocolos en otras capas.

- CONFIGURACIÓN DEL PROTOCOLO TCP/IP EN UN HOST.

Configure aquí los ajustes relacionados con TCP/IP para la Tarjeta Ethernet.

Protocolo:
Muestra si se ha configurado la tarjeta de interface de red para el uso del protocolo TCP/IP.

Dirección IP:
Introduzca la Dirección IP de la tarjeta de interface de red.
Si se activa DHCP, aparece la Dirección IP adquirida del Servidor de DHCP.

Máscara de subred:
Introduzca la máscara de subred de la tarjeta de interface de red. Esto se utiliza para establecer como dirección de red una parte de la Dirección IP.
Si se activa DHCP, aparece la máscara adquirida del Servidor de DHCP.

Dirección gateway:
Introduzca la dirección de gateway por defecto predeterminada, que es el host/router que se utiliza para comunicarse con otras redes.
Si se activa DHCP, aparece la dirección adquirida del Servidor de DHCP.

Rango control acceso:
La función de Control de acceso limita el acceso (por ejemplo, para la impresión) a la tarjeta de interface de red de acuerdo con la Dirección IP de la estación de trabajo solicitante.
Para utilizar esta función, introduzca el rango de direcciones que permitían el acceso [Rango control acceso 1] en [Rango control acceso 5]. Puede establecerse un rango en cualquier cuadro. Puede especificarse un máximo de cinco rangos. Las direcciones que sobrepasen estos rangos tienen el acceso denegado.

- Cuando no especifique los cinco rangos, establezca [0.0.0.0]-[0.0.0.0] para los que no se utilizarán.
- Cuando se establecen los cinco rangos en [0.0.0.0]-[0.0.0.0], esta función se desactiva y todas las estaciones de trabajo tienen permitido el acceso.
- Los protocolos, como telnet y web, no están sujetos a esta limitación.

Arranque de red:
Seleccione "DHCP" para adquirir automáticamente los ajustes de red de un servidor DHCP; seleccione "NINGUNO" para configurar manualmente los ajustes de red.

WINS:
Seleccione si la resolución del nombre WINS para la tarjeta de interface de red está activada.
Cuando se active la resolución de nombre de WINS, introduzca las direcciones del servidor de WINS en [Servidor principal de WINS] y [Servidor secundario de WINS].

El nombre de dispositivo introducido en [Configuración] - [General] - [Nombre dispositivo] se registra en el servidor de WINS seleccionado. Puede especificar el dispositivo mediante el nombre incluso cuando la Dirección IP de la tarjeta de interface de red cambie en el entorno de DHCP.
Cuando no puede registrarse el nombre en el servidor de WINS, se transmite la solicitud de registro.

Servidor principal de WINS:
Introduzca la Dirección IP del Servidor principal de WINS.
Cuando una dirección del servidor de WINS se obtiene del servidor de DHCP, esa dirección se utiliza y la dirección especificada aquí se desactiva. Puede comprobar cuál es la dirección que realmente se utiliza verificando el log del sistema en [Info. Adminis.] - [Tarjeta Ethernet].

Servidor secundario de WINS:
Introduzca la Dirección IP del Servidor secundario de WINS.
El Servidor secundario de WINS se utiliza cuando el Servidor principal de WINS no está disponible para registrar el nombre del dispositivo.

Tipo de trama:
Muestra los tipos de trama que se están utilizando. Sólo podrá usar Ethernet II.

SNMP / LPR / RSH/RCP / DIPRINT / FTP / IPP:
Seleccione si cada protocolo se encuentra activado o desactivado en la tarjeta de interface de red.

Timeout IPP:
Cuando se imprime mediante el protocolo IPP, se produce un error timeout de impresión si durante el tiempo aquí indicado (de 30 a 65535 segundos) no se han enviado datos de impresión. El valor predeterminado de fábrica es "900 segundos".

- DISPOSITIVOS FINALES DE HOGAR.

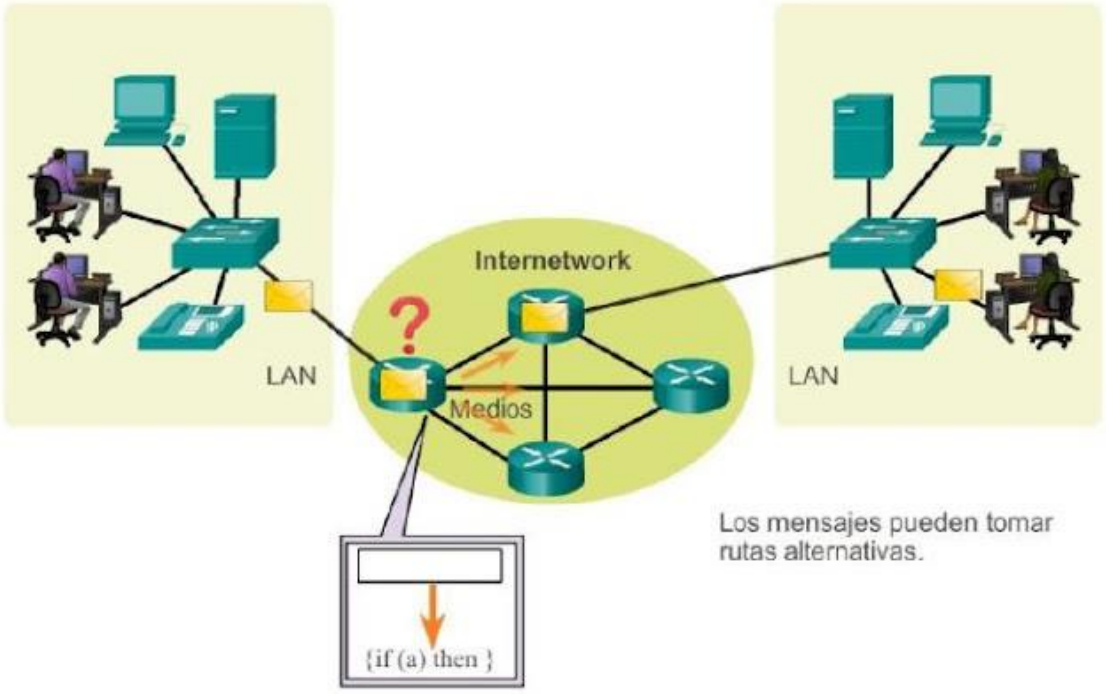
Los dispositivos de red con los que las personas están más familiarizadas se denominan “dispositivos finales” o “hosts”. Estos dispositivos forman la interfaz entre los usuarios y la red de comunicación subyacente.

Algunos ejemplos de dispositivos finales son:

- Computadoras (estaciones de trabajo, computadoras portátiles, servidores de archivos, servidores web)
- Impresoras de red
- Teléfonos VoIP
- Terminales de TelePresence
- Cámaras de seguridad

- Dispositivos portátiles móviles (como smartphones, tablet PC, PDA y lectores inalámbricos de tarjetas de débito y crédito, y escáneres de códigos de barras)

Un dispositivo host es el origen o el destino de un mensaje transmitido a través de la red, tal como se muestra en la animación. Para distinguir un host de otro, cada host en la red se identifica por una dirección. Cuando un host inicia la comunicación, utiliza la dirección del host de destino para especificar a dónde se debe enviar el mensaje.



Los datos se originan con un dispositivo final, fluyen por la red y llegan a un dispositivo final.

- IMPACTO DE APLICACIONES DE USO DIARIO.

La tecnología está revolucionando el mundo, se ha convertido en un apoyo importante para los humanos. Desarrollar aplicaciones móviles es, quizá, una forma de estar a la vanguardia de la demanda global en el marco de la tecnología e innovación. Kubo, con más de 10 años de experiencia en el mercado tecnológico lo consolidan como un aliado ideal para el desarrollo de aplicaciones móviles en los sistemas iOS y Android.

El equipo de trabajo de la compañía orienta al cliente en los procesos de creación, diseño y análisis de todo lo que implica desarrollar una plataforma virtual, de paso determinan cuáles son los puntos de riesgo, integración y pruebas del funcionamiento de la aplicación. Entre el número de empresas que han desarrollado aplicativos móviles con Kubo se encuentran Carvajal Tecnología y Herbalife, en lo que llevan operando, han implementado más de 150 proyectos para clientes en Colombia y el mundo.

Gunther Votteler, cofundador de Kubo S.A.S., habló sobre la importancia de la tecnología para el mundo y cómo la compañía está trabajando para ofrecerle a sus clientes los últimos avances tecnológicos y los que están por llegar.

- REDES SOCIALES DE USO DIARIO.

hoy en día internet está repleto de un infinito número de posibilidades para nuestro entretenimiento. Sin embargo, no hay ninguna duda de que algunas de las plataformas más populares y más utilizadas son las redes sociales.

¿Cuáles son las Redes Sociales más utilizadas?

Datos del 2021. Lideran el ranking de redes sociales más utilizadas Facebook (87%) y YouTube (68%), siendo esta última la que más seguidores jóvenes concentra (el 76% tiene entre 16 y 30 años). Instagram, en tercer lugar, es la que más seguidores ha ganado (de un 49% a un 54%). En cuarto y quinto lugar se mantiene Twitter con un 50% y Linkedin con un 57%.

De acuerdo con **The Global State of Digital,** elaborado por Hootsuite y We Are Social, se estima que **3.484 billones de personas utilizan las redes sociales,** esto representa 45 por ciento de la población mundial.

- E-LEARNING.

Aunque e-Learning no es un término castellano, su uso se ha generalizado de tal forma que es el más extendido a nivel mundial. Existen otros términos, que significan prácticamente lo mismo y a veces se usan como sinónimos, tales como: teleformación, formación on-line, enseñanza virtual, etc.

Podemos entender **e-Learning** como:

> Procesos de enseñanza-aprendizaje que se llevan a cabo a través de Internet, caracterizados por una separación física entre profesorado y estudiantes, pero con el predominio de una comunicación tanto síncrona como asíncrona, a través de la cual se lleva a cabo una interacción didáctica continuada. Además, el alumno pasa a ser el centro de la formación, al tener que autogestionar su aprendizaje, con ayuda de tutores y compañeros.

Características

Esta modalidad formativa a distancia a través de Internet o semipresencial (una parte de los procesos formativos se realizan de manera presencial), ha contribuido a que la formación llegue a un mayor número de personas. Entre las características más destacadas del e-Learning están:

- **Desaparecen las barreras espacio-temporales.** Los estudiantes pueden realizar un curso en su casa o lugar de trabajo, estando accesibles los contenidos cualquier día a cualquier hora. Pudiendo de esta forma optimizar al máximo el tiempo dedicado a la formación.
- **Formación flexible.** La diversidad de métodos y recursos empleados, facilita el que nos podamos adaptar a las características y necesidades de los estudiantes.
- **El alumno es el centro** de los procesos de enseñanza-aprendizaje y participa de manera activa en la construcción de sus conocimientos, teniendo capacidad para decidir el itinerario formativo más acorde con sus intereses.
- **El profesor**, pasa de ser un mero transmisor de contenidos a un tutor que orienta, guía, ayuda y facilita los procesos formativos.
- **Contenidos actualizados.** Las novedades y recursos relacionados con el tema de estudio se pueden introducir de manera rápida en los contenidos, de forma que las enseñanzas estén totalmente actualizadas.
- **Comunicación constante** entre los participantes, gracias a las herramientas que incorporan las plataformas e-Learning (foros, chat, correo-e, etc.).

Con las posibilidades que nos brinda la plataforma de e-Learning que la Universidad pone al servicio de toda su comunidad, la relación que se establece entre alumnos y entre profesor-alumno es fluida, generándose un verdadero ambiente de enseñanza-aprendizaje, compartiendo dudas, ideas, temas de interés, etc. y contribuyendo a paliar algunos de los inconvenientes de la enseñanza a distancia tradicional, como era el sentimiento de aislamiento y soledad que el alumno experimentaba a lo largo del proceso.

De esta forma, el CFP pretende ser un servicio universitario de excelencia, basándose en un compromiso de mejora continua, ofreciendo una formación de calidad, moderna, a distancia, actualizada, flexible y personalizada.

- COMERCIO ELECTRÓNICO.

El comercio electrónico, también conocido como e-commerce, **tiene como principal característica la actividad económica que permite el** comercio de compra y vente de productos y servicios a partir de medios digitales, como, por ejemplo, páginas web, aplicaciones móviles y redes sociales.

Por medio de la internet, los clientes pueden acceder a diversas marcas, productos y servicios en todo momento, en cualquier lugar.

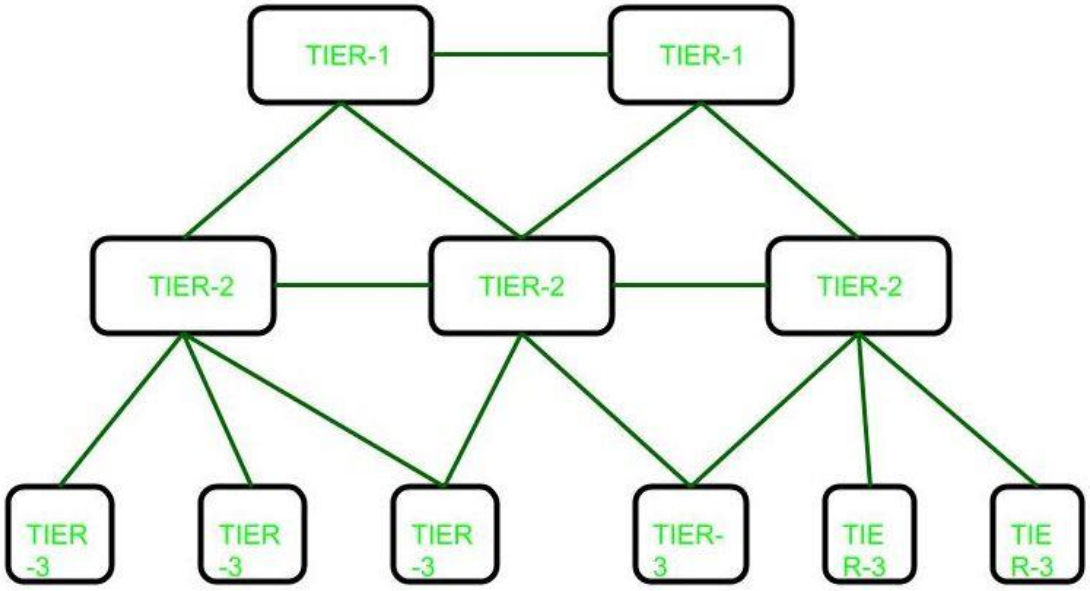
La relevancia de este tipo de comercio es tal que los negocios lo toman como parte de la estrategia de ventas gracias a su eficiencia.

Los establecimientos ya cuentan con páginas web y crean perfiles en redes sociales para conseguir llegar a un mayor rango de público.

- NIVELES DE ISP.

JERARQUÍA DEL PROVEEDOR DE SERVICIOS DE INTERNET (ISP)

El proveedor de servicios de Internet (ISP) es una empresa que proporciona conexión a Internet al usuario final, pero básicamente hay tres niveles de ISP. Hay 3 niveles de proveedor de servicios de Internet (ISP): ISP de nivel 1, ISP de nivel 2 e ISP de nivel 3.



Estos se explican a continuación.

- **ISP de nivel 1:**

  estos ISP están en la parte superior de la jerarquía y tienen un alcance global, no pagan por el tráfico de Internet a través de su red, en lugar de eso, los ISP de nivel inferior tienen que pagar un costo por pasar su tráfico de una ubicación geográfica a otra. que no está al alcance de esos ISP. Generalmente, los ISP en el mismo nivel se conectan entre sí y permiten que el tráfico pase libremente entre ellos. Estos ISP se denominan pares. Debido a este costo se ahorra. Construyen infraestructura, como los cables marítimos de Internet del Atlántico, para proporcionar tráfico a todos los demás proveedores de servicios de Internet, no a los usuarios finales.

  Ejemplos:
  algunos ejemplos de proveedores de Internet de nivel 1:

```
Cogent Communications,
Hibernia Networks,
AT&T
```

- **ISP de nivel 2:**

  estos ISP son proveedores de servicios que se conectan entre ISP de nivel 1 y nivel 3. Tienen alcance regional o nacional y se comportan como ISP de nivel 1 para los ISP de nivel 3.

Ejemplos:
ejemplos de ISP de nivel 2:

```
Vodafone,
Easynet,
BT
```

ISP de nivel 3:

estos ISP son los más cercanos a los usuarios finales y les ayudan a conectarse a Internet cobrando algo de dinero. Estos ISP trabajan en el modelo de compra. Estos ISP tienen que pagar algunos costos a los ISP de nivel 2 en función del tráfico generado.

Ejemplos:
ejemplos de ISP de nivel 3:

```
Comcast,
Deutsche Telekom,
Verizon Communications
```

- DISPOSITIVOS DE REDES.

Un **dispositivo de interconexión** de **redes** es un término ampliamente utilizado para cualquier hardware que conecte diferentes recursos de **red**. Los **dispositivos** clave que comprenden una **red** son conmutadores, enrutadores, brigde (**puentes**), repetidores y puertas de enlace.

Todos los **dispositivos** tienen características de alcance por separado, según los requisitos y escenarios de la red. Los siguientes son escenarios de **interconexión**:

- Una sola **LAN**
- Dos **LAN** conectadas entre sí (LAN-LAN)
- Una **LAN** conectada a una WAN (LAN-WAN)
- Dos **LAN** conectadas a través de una WAN (LAN-WAN-LAN)

Para entender los diversos **dispositivos de interconexión** de **redes**, creamos el siguiente glosario.

Repetidores

Se utilizan para extender la longitud de la **red**. Fueron creados para regenerar y amplificar señales débiles, extendiendo así la longitud de la red. La función básica de un repetidor es remodelar y reamplificar la señal de **datos** a su **nivel** original.

Las características importantes de estos equipos son las siguientes:

1. Conectar diferentes **segmentos de red** de una LAN
2. Reenviar cada paquete que recibe

3. Un repetidor es un regenerador, no un amplificador
4. Los repetidores operan en la **capa** física del **modelo OSI**

Hubs

Un **Hub** es básicamente un repetidor multipuerto, actúa como concentrador y conecta múltiples cables provenientes de diferentes conexiones. Los concentradores no pueden filtrar **datos**, por lo que los paquetes de **datos** se envían a todos los dispositivos conectados, el dominio de colisión de todos los hosts conectados a través de **Hub** sigue siendo uno.

Los **Hubs** no tienen inteligencia para encontrar la mejor ruta para los paquetes, las consecuencias: ineficiencia y desperdicio.

Bridge

Un **bridge** o un puente opera en la **capa** de **enlace de datos.** Es un repetidor con funcionalidad adicional de filtrado al leer las direcciones MAC de origen y **destino**. También se usa para interconectar dos LAN que funcionan en el mismo protocolo. Tiene un puerto de entrada y salida único, lo que lo convierte en un **dispositivo** de 2 **puertos**.

Switch o conmutador

El switch es un puente de múltiples **puertos**, es un **dispositivo** de capa de **enlace de datos.** El conmutador es muy eficiente, realiza una verificación de errores antes de reenviar paquetes. En otras palabras, el conmutador divide el dominio de colisión de los hosts, pero el dominio de difusión sigue siendo el mismo.

Router

Los enrutadores enlazan dos o más **redes** diferentes, estas pueden constar de varios tipos de **segmentos de red** LAN. Un **enrutador** recibe paquetes y selecciona la ruta óptima para reenviar el paquete a través de la red.

Los enrutadores crean una tabla de todas las direcciones de los **dispositivos**, llamada tabla de enrutamiento. Con ella, el enrutador envía una transmisión desde la fuente hacia el **destino** a través de la mejor ruta. Los enrutadores funcionan en el **nivel** de red del **modelo OSI.**

Gateway

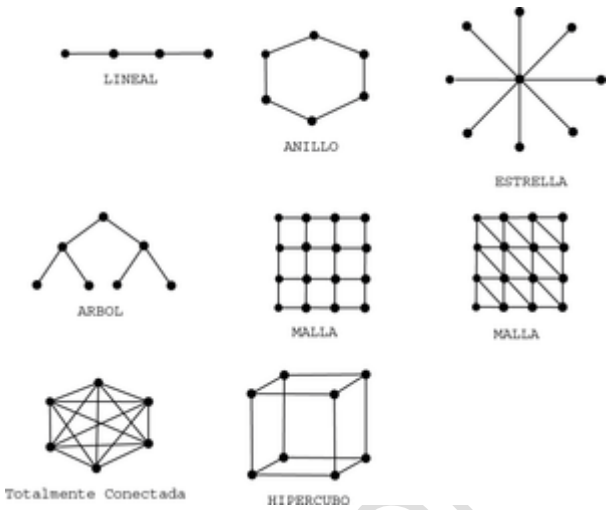
Las puertas de enlace son dispositivos de conexión multipropósito para crear uniones entre redes diferentes. Son capaces de convertir el formato de los paquetes de un entorno, a otro formato. Funcionan como agentes de mensajería que toman datos de un sistema, los interpretan y transfieren a otro sistema.

- TOPOLOGÍAS FÍSICAS Y LÓGICAS.

Topologías físicas

- Una Topología de bus circular usa un solo cable Backbone que debe terminarse en ambos extremos. Todos los Hosts se conectan directamente a este Backbone.

- La Topología de anillo conecta un Host con el siguiente y al último host con el primero. Esto crea un anillo físico de cable.
- La Topología en estrella conecta todos los cables con un punto central de concentración.
- Una Topología en estrella extendida conecta estrellas individuales entre sí mediante la conexión de Hubs o Switches. Esta topología puede extender el alcance y la cobertura de la red.



- Una Topología jerárquica es similar a una estrella extendida. Pero en lugar de conectar los HUBs o Switches entre sí, el sistema se conecta con un computador que controla el tráfico de la topología.
- La Topología de malla se implementa para proporcionar la mayor protección posible para evitar una interrupción del servicio. El uso de una topología de malla en los sistemas de control en red de una planta nuclear sería un ejemplo excelente. En esta topología, cada Host tiene sus propias conexiones con los demás hosts. Aunque Internet cuenta con múltiples rutas hacia cualquier ubicación, no adopta la Topología de malla completa.

Otras topologías de red

- La Topología de árbol tiene varias terminales conectadas de forma que la red se ramifica desde un Servidor base.

Topologías lógicas

La topología lógica de una red es la forma en que los Hosts se comunican a través del medio. Los dos tipos más comunes de topologías lógicas son Broadcast y transmisión de Tokens.

- La Topología broadcast simplemente significa que cada Host envía sus datos hacia todos los demás Hosts del medio de red. No existe una orden que las estaciones deban seguir para utilizar la red. Es por orden de llegada, es como funciona Ethernet.

- La Topología transmisión de tokens controla el acceso a la red mediante la transmisión de un Token electrónico a cada Host de forma secuencial. Cuando un host recibe el token, ese Host puede enviar datos a través de la red. Si el host no tiene ningún dato para enviar, transmite el token al siguiente host y el proceso se vuelve a repetir. Dos ejemplos de redes que utilizan la transmisión de tokens

son Token Ring y la Interfaz de datos distribuida por fibra (FDDI). Arcnet es una variación de Token Ring y FDDI. Arcnet es la transmisión de Tokensen una Topología de bus.

- DIRECCIONAMIENTO FÍSICO Y JERÁRQUICO.

Una de las principales funciones de la capa de red es proporcionar un mecanismo para direccionar hosts. A medida que crece la cantidad de hosts de la red, se requiere más planificación para administrar y direccionar la red.

División de Redes

En lugar de tener todos los hosts conectados en cualquier parte a una vasta red global, es más práctico y manejable agrupar los hosts en redes específicas. Históricamente, las redes basadas en IP tienen su raíz como una red grande. Como esta red creció, también lo hicieron los temas relacionados con su crecimiento. Para aliviar estos problemas, la red grande fue separada en redes más pequeñas que fueron interconectadas. Estas redes más pequeñas generalmente se llaman subredes.

Red y subred son términos utilizados indistintamente para referirse a cualquier sistema de red hecho posible por los protocolos de comunicación comunes compartidos del modelo TCP/IP.

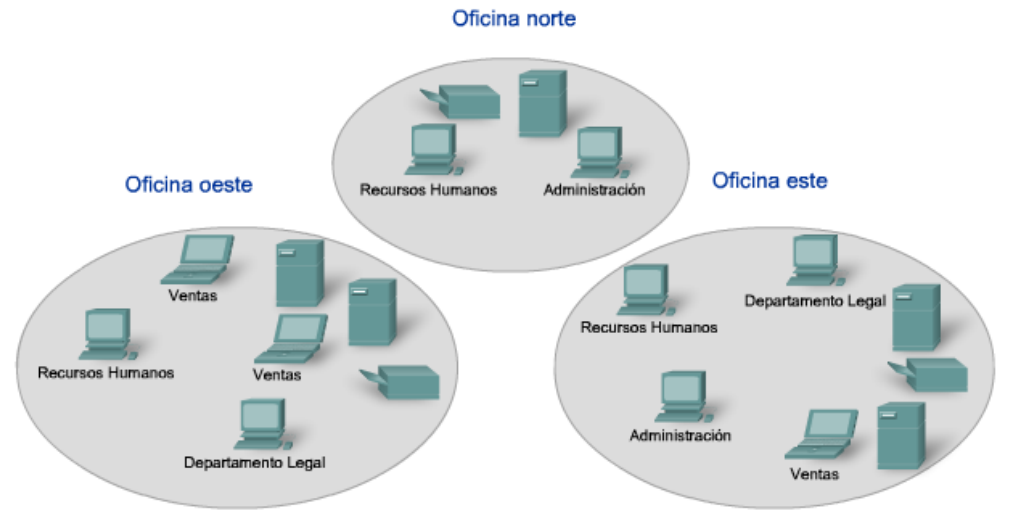
De manera similar, a medida que nuestras redes crecen, pueden volverse demasiado grandes para manejarlas como una única red. En ese punto, necesitamos dividir nuestra red. Cuando planeamos la división de la red, necesitamos agrupar aquellos hosts con factores comunes en la misma red.

Como se muestra en la figura, las redes pueden agruparse según factores que incluyen:

- Ubicación geográfica
- Propósito
- Propiedad

Agrupación de Hosts de Manera Geográfica

Podemos agrupar hosts de redes geográficamente. El agrupamiento de hosts en la misma ubicación, como cada construcción en un campo o cada piso de un edificio de niveles múltiples, en redes separadas puede mejorar la administración y operación de la red.

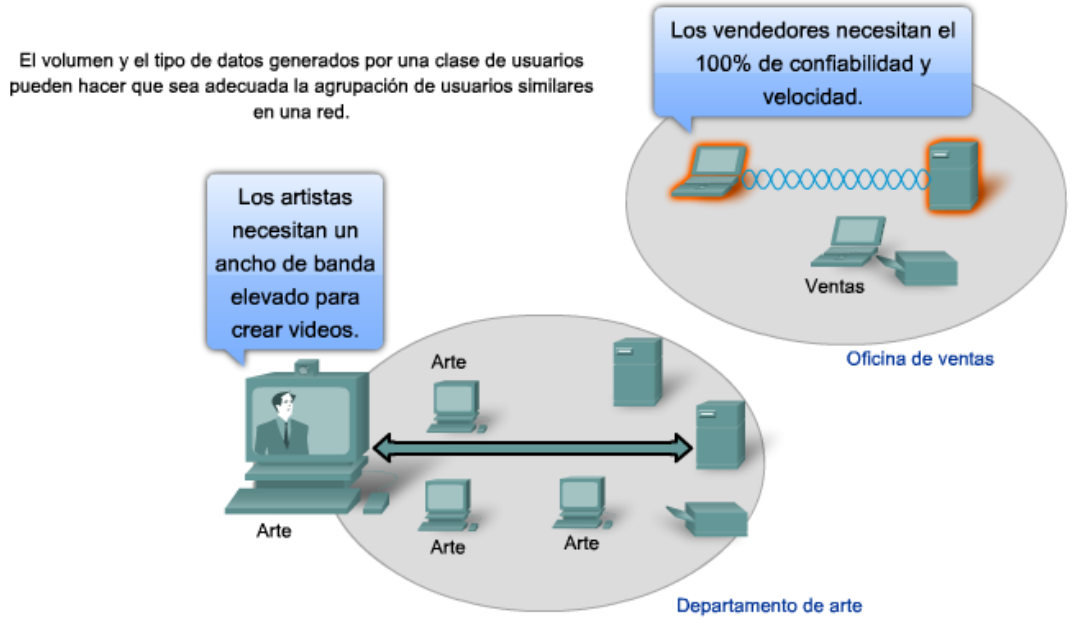


El simple hecho de conectar por cables la red física puede convertir la ubicación geográfica en un lugar lógico para realizar el inicio de la segmentación de una red.

Agrupación de Hosts para Propósitos Específicos

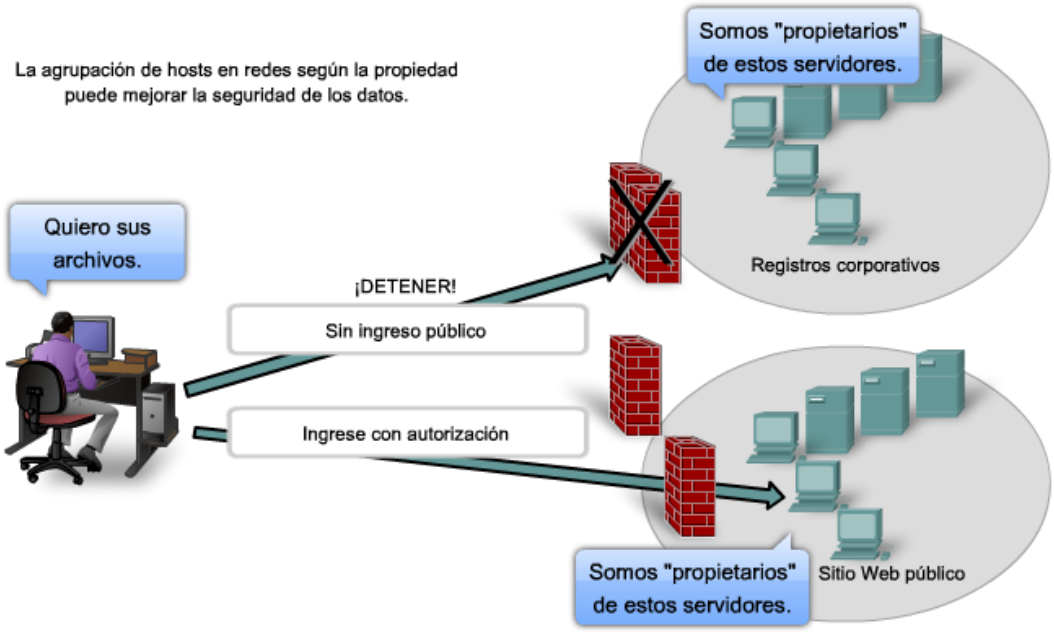
Los usuarios que tienen tareas similares usan generalmente software común, herramientas comunes y tienen patrones de tráfico común. A menudo podemos reducir el tráfico requerido por el uso de software y herramientas específicos, ubicando estos recursos de soporte en la red con los usuarios.

El volumen del tráfico de datos de la red generado por las diferentes aplicaciones puede variar significativamente. Dividir redes basadas en el uso facilita la ubicación efectiva de los recursos de la red así como también el acceso autorizado a esos recursos. Los profesionales en redes necesitan equilibrar el número de hosts en una red con la cantidad de tráfico generado por los usuarios. Por ejemplo, considere una empresa que emplea diseñadores gráficos que utilizan la red para compartir archivos multimedia muy grandes. Estos archivos consumen la mayoría del ancho de banda disponible durante gran parte del día laboral. La empresa también emplea vendedores que se conectan una vez al día para registrar sus transacciones de ventas, lo que genera un tráfico mínimo de red. En esta situación, el mejor uso de los recursos de la red sería crear varias redes pequeñas a las cuales unos pocos diseñadores tengan acceso y una red más grande para que usen todos los vendedores.



Agrupación de Hosts para Propiedad

Utilizar una base organizacional (compañía, departamento) para crear redes ayuda a controlar el acceso a los dispositivos y datos como también a la administración de las redes. En una red grande, es mucho más difícil definir y limitar la responsabilidad para el personal de la red. Dividir hosts en redes separadas provee un límite de cumplimiento y administración de seguridad de cada red.



Direccionamiento Jerárquico

Para poder dividir redes, necesitamos el direccionamiento jerárquico. Una dirección jerárquica identifica cada host de manera exclusiva. También tiene niveles que ayudan a reenviar paquetes a través de internetworks, lo que permite que una red se divida según esos niveles.

Para mantener las comunicaciones de datos entre redes por medio de internetworks, los esquemas de direccionamiento de capa de red son jerárquicos.

- PROTOCOLOS DE LA CAPA DE RED.

ORIENTACIÓN DE CONEXIÓN

Hay dos formas en las que el nivel de red puede funcionar internamente, pero independientemente de que la red funcione internamente con datagramas o con circuitos virtuales puede dar hacia el nivel de transporte un servicio orientado a conexión:

- Datagramas: Cada paquete se encamina independientemente, sin que el origen y el destino tengan que pasar por un establecimiento de comunicación previo.
- Circuitos virtuales: En una red de circuitos virtuales dos equipos que quieran comunicarse tienen que empezar por establecer una conexión. Durante este establecimiento de conexión, todos los routers que haya por el camino elegido reservarán recursos para ese circuito virtual específico.

TIPOS DE SERVICIOS

Hay dos tipos de servicio:

- Servicios orientados a la conexión: Sólo el primer paquete de cada mensaje tiene que llevar la dirección destino. Con este paquete se establece la ruta que deberán seguir todos los paquetes pertenecientes a esta conexión. Cuando llega un paquete que no es el primero se identifica a que conexión pertenece y se envía por el enlace de salida adecuado, según la información que se generó con el primer paquete y que permanece almacenada en cada conmutador o nodo.

Servicios No orientados a la conexión: Cada paquete debe llevar la dirección destino, y con cada uno, los nodos de la red deciden el camino que se debe seguir. Existen muchas técnicas para realizar esta decisión, como por ejemplo comparar el retardo que sufriría en ese momento el paquete que se pretende transmitir según el enlace que se escoja.

Encaminamiento

Las técnicas de encaminamiento suelen basarse en el estado de la red, que es dinámico, por lo que las decisiones tomadas respecto a los paquetes de la misma conexión pueden variar según el instante de manera que éstos pueden seguir distintas rutas. El problema, sin embargo, consiste en encontrar un camino óptimo entre un origen y un destino. La selección óptima de este camino puede tener diferentes criterios: velocidad, retardo, seguridad, regularidad, distancia, longitud media de las colas, costos de comunicación, etc. Los equipos encargados de esta labor se denominan encaminadores (router), aunque también realizan labores de encaminamiento los conmutadores (switch) "multicapa" o "de nivel 3", si bien estos últimos realizan también labores de nivel de enlace.

Algunos protocolos de la capa de red

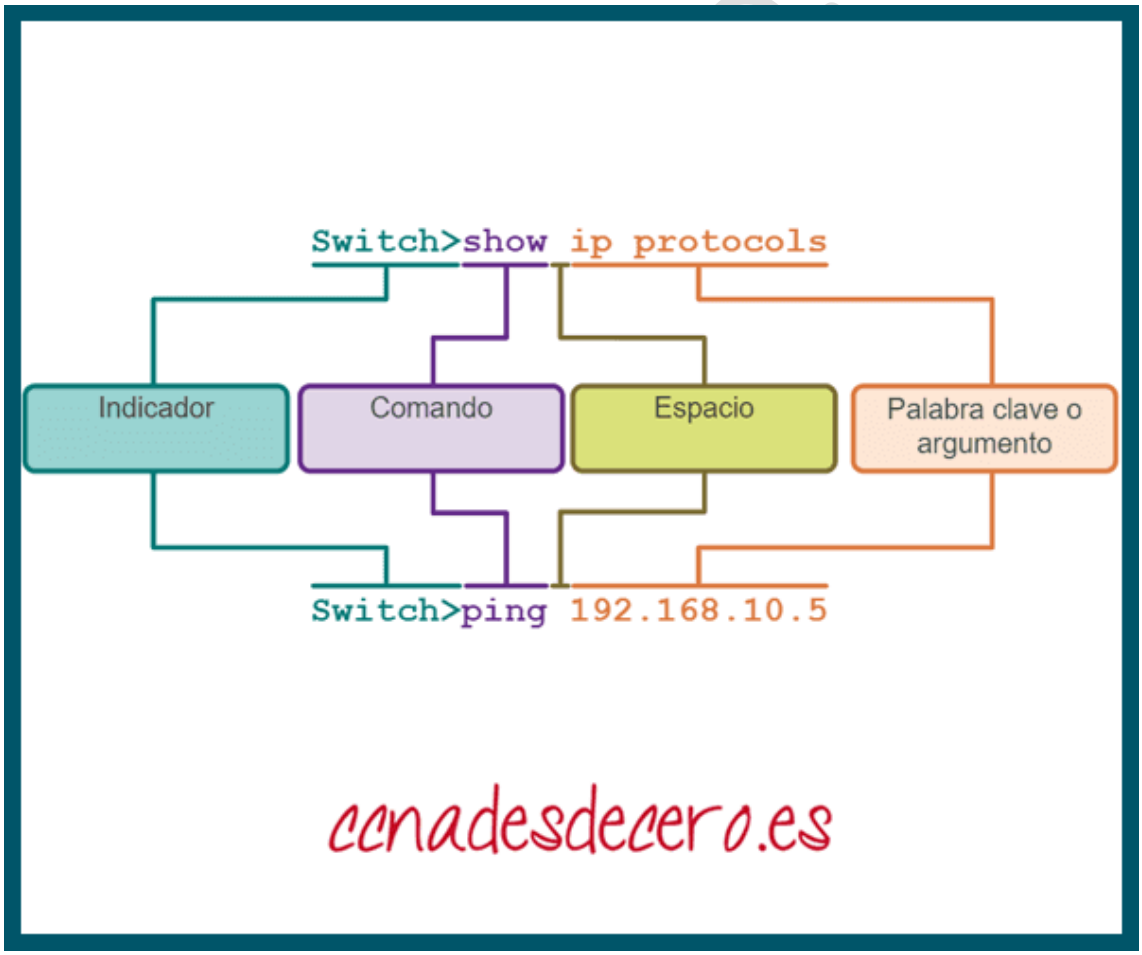
Algunos protocolos de la capa de red son:

- IP (IPv4, IPv6, IPsec)

- OSPF
- IS-IS
- ARP, RARP
- RIP
- ICMP, ICMPv6
- IGMP
- DHCP

- FUNCIONAMIENTO, ESTRUCTURA BÁSICA Y SINTAXIS DE LOS COMANDOS DEL CISCO IOS

Los dispositivos Cisco IOS admiten muchos comandos. Cada comando de IOS tiene una sintaxis o formato específico y puede ejecutarse solamente en el modo adecuado. La sintaxis general para un comando, que se muestra en la figura, es el comando seguido de cualquier palabra clave y argumento apropiados.



Estructura Básica Comandos de IOS

- **Palabra clave** – Es un parámetro específico definido en el sistema operativo (en la figura, **ip protocols**).
- **Argumento** – No está predefinido; es un valor o variable definido por el usuario (en la figura, **192.168.10.5**)

Después de introducir cada comando completo, incluyendo cualquier palabra clave y argumentos, pulsa la tecla **Intro** para enviar el comando al intérprete de comandos.

2. Comprobación de Sintaxis del Comando IOS

Un comando podría requerir uno o más argumentos. Para determinar cuáles son las palabras clave y los argumentos requeridos para un comando, consulta la sintaxis de comandos. La sintaxis proporciona el patrón o el formato que se debe utilizar cuando se introduce un comando.

Como se identifica en la tabla, el texto en negrita indica los comandos y las palabras clave que se ingresan como se muestra. El texto en cursiva indica los argumentos para los cuales el usuario proporciona el valor.

ⓘ

Convención	**Descripción**
negrita	El texto en negrita indica los comandos y palabras clave se introducen literalmente como se muestra.
CURSIVA	El texto en cursiva indica los argumentos para los que se suministran valores.
[x**]**	Los corchetes indican un elemento opcional (palabra clave o argumento).

Convención	Descripción
{x**}**	Los corchetes indican un elemento requerido (palabra clave o argumento).
[x **{**y	z **}]**	Los corchetes y las líneas verticales dentro de los corchetes indican una elección requerida dentro de un elemento opcional. Los espacios se utilizan para delinear claramente las partes del comando.

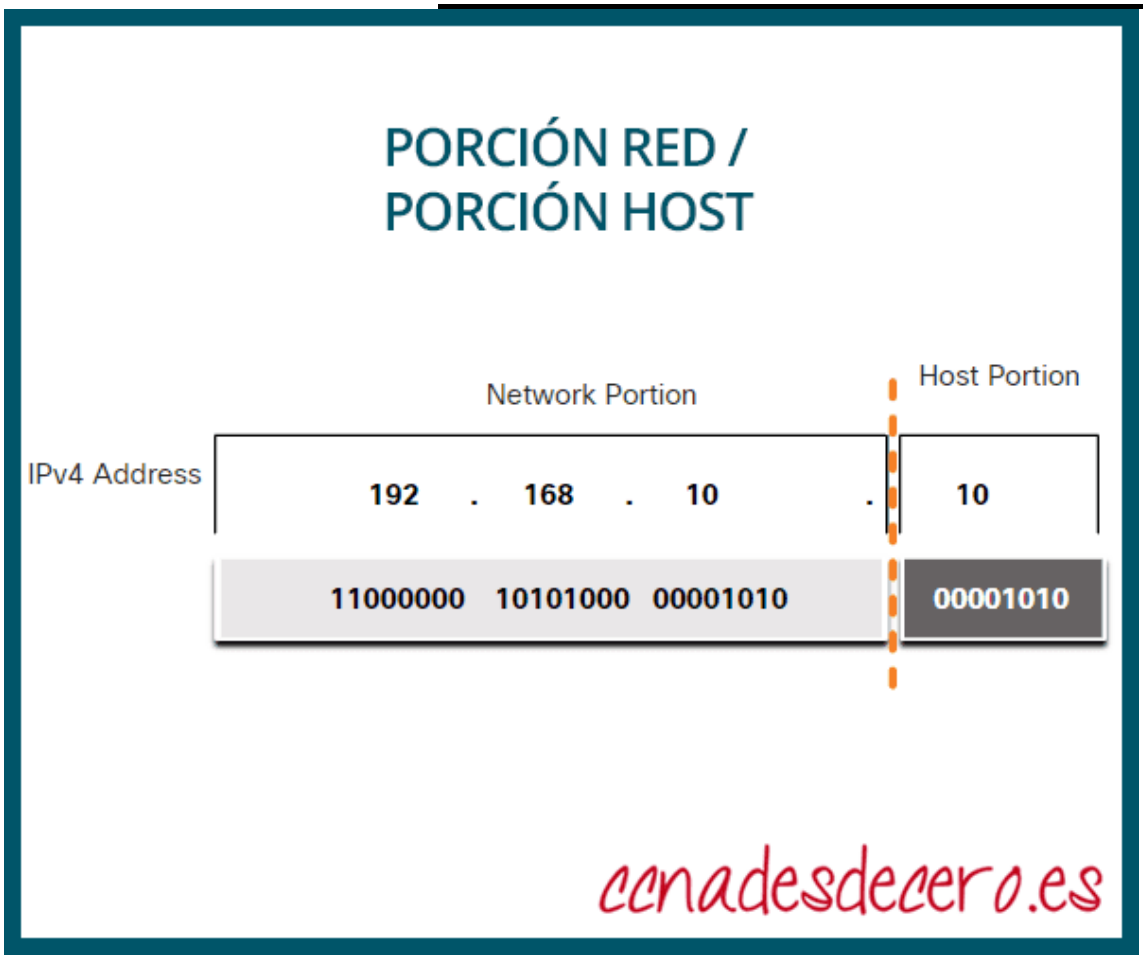
Por ejemplo, la sintaxis para usar el comando **description** es cadena de **description**. El argumento es un valor de cadena proporcionado por el usuario. El comando **description** suele utilizarse para identificar el propósito de una interfaz. Por ejemplo, al introducir el comando, **description Se conecta al interruptor de la oficina central**, describe dónde se encuentra el otro dispositivo al final de la conexión.

Los siguientes ejemplos muestran las convenciones utilizadas para documentar y utilizar los comandos del IOS:

- **ping** IP-ADDRESS – l 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**.
- **traceroute** 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**.

- DIRECCIONES DE RED IPV4.

Una dirección IPv4 es una dirección jerárquica de 32 bits que se compone de una porción de red y una porción de host. Al determinar la porción de red frente a la porción de host, debes mirar la secuencia de 32 bits, como se muestra en la imagen.



Porción de red y host IPv4

Los bits dentro de la porción de red de la dirección deben ser idénticos para todos los dispositivos que residen en la misma red. Los bits dentro de la porción de host de la dirección deben ser únicos para identificar un host específico dentro de una red. Si dos hosts tienen el mismo patrón de bits en la porción de red especificada de la secuencia de 32 bits, esos dos hosts residirán en la misma red.

Pero, ¿cómo saben los hosts qué porción de los 32 bits identifica la red y cuál identifica al host? Esa es la función de la máscara de subred.

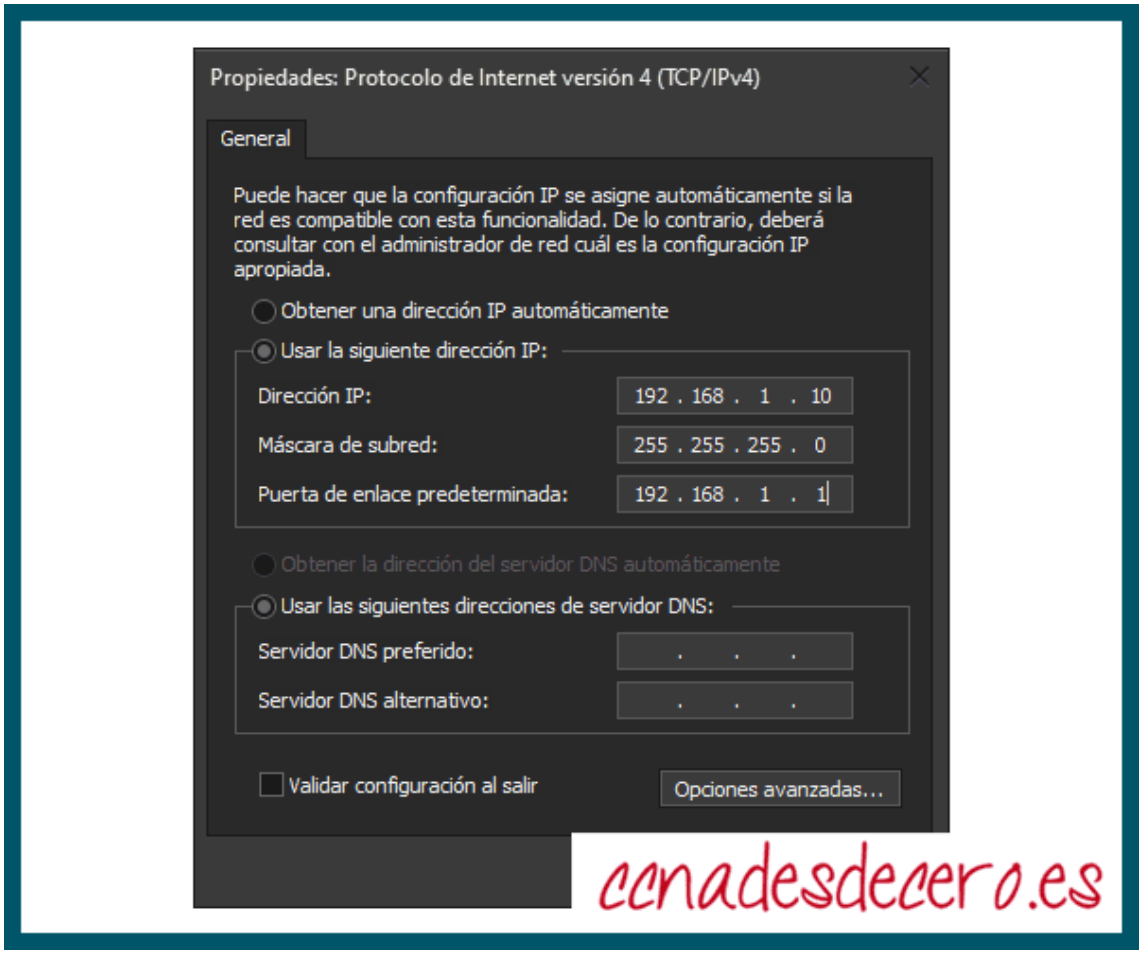
2. La Máscara de Subred

Como se muestra en la imagen, la asignación de una dirección IPv4 a un host requiere lo siguiente:

- **Dirección IPv4**: esta es la dirección IPv4 única del host.
- **Máscara de subred**: se usa para identificar la porción de red / host de la dirección IPv4.

Configuración de IPv4 en una computadora con Windows

ⓘ



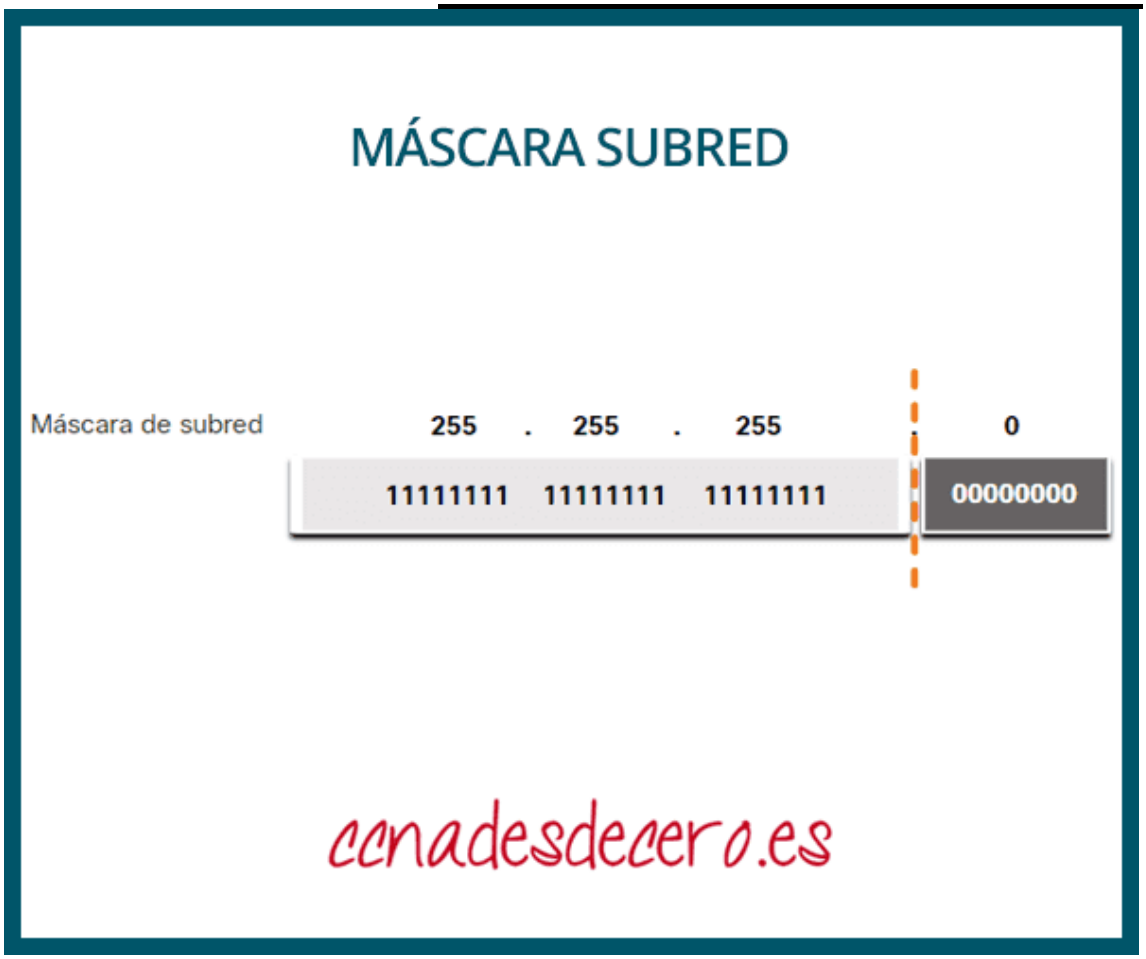
Ejemplo Dirección IP en PC

Nota: Se requiere una dirección IPv4 de puerta de enlace predeterminada para llegar a redes remotas y se requieren direcciones IPv4 del servidor DNS para traducir los nombres de dominio a direcciones IPv4.

La máscara de subred IPv4 se usa para diferenciar la porción de red de la porción de host de una dirección IPv4. Cuando se asigna una dirección IPv4 a un dispositivo, la máscara de subred se usa para determinar la dirección de red del dispositivo. La dirección de red representa todos los dispositivos en la misma red.

La siguiente imagen muestra la máscara de subred de 32 bits en formato decimal y binario punteado.

Máscara de subred

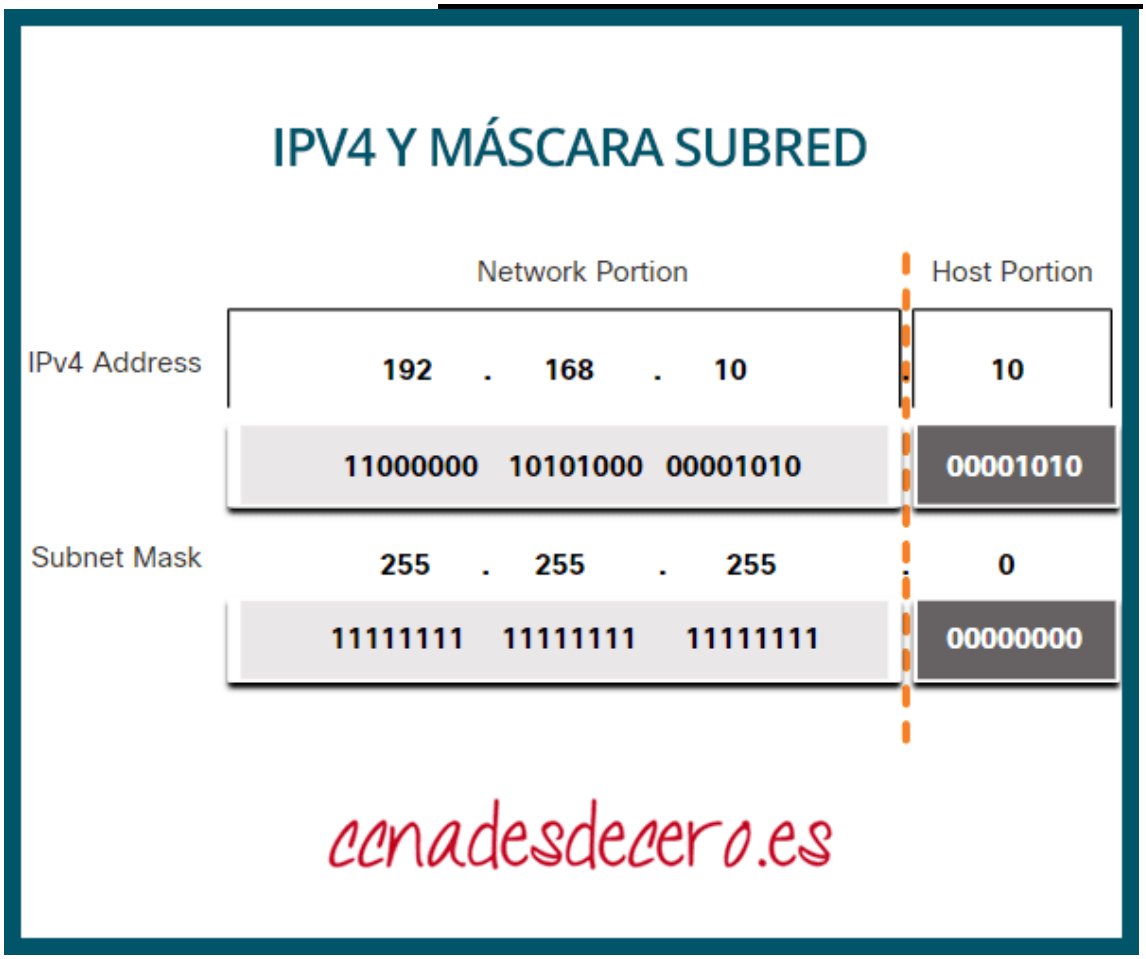


Máscara de subred

Observa cómo la máscara de subred es una secuencia consecutiva de 1 bits seguida de una secuencia consecutiva de 0 bits.

Para identificar las porciones de red y host de una dirección IPv4, la máscara de subred se compara con la dirección IPv4 bit por bit, de izquierda a derecha como se muestra en la imagen.

Asociar una dirección IPv4 con su máscara de subred

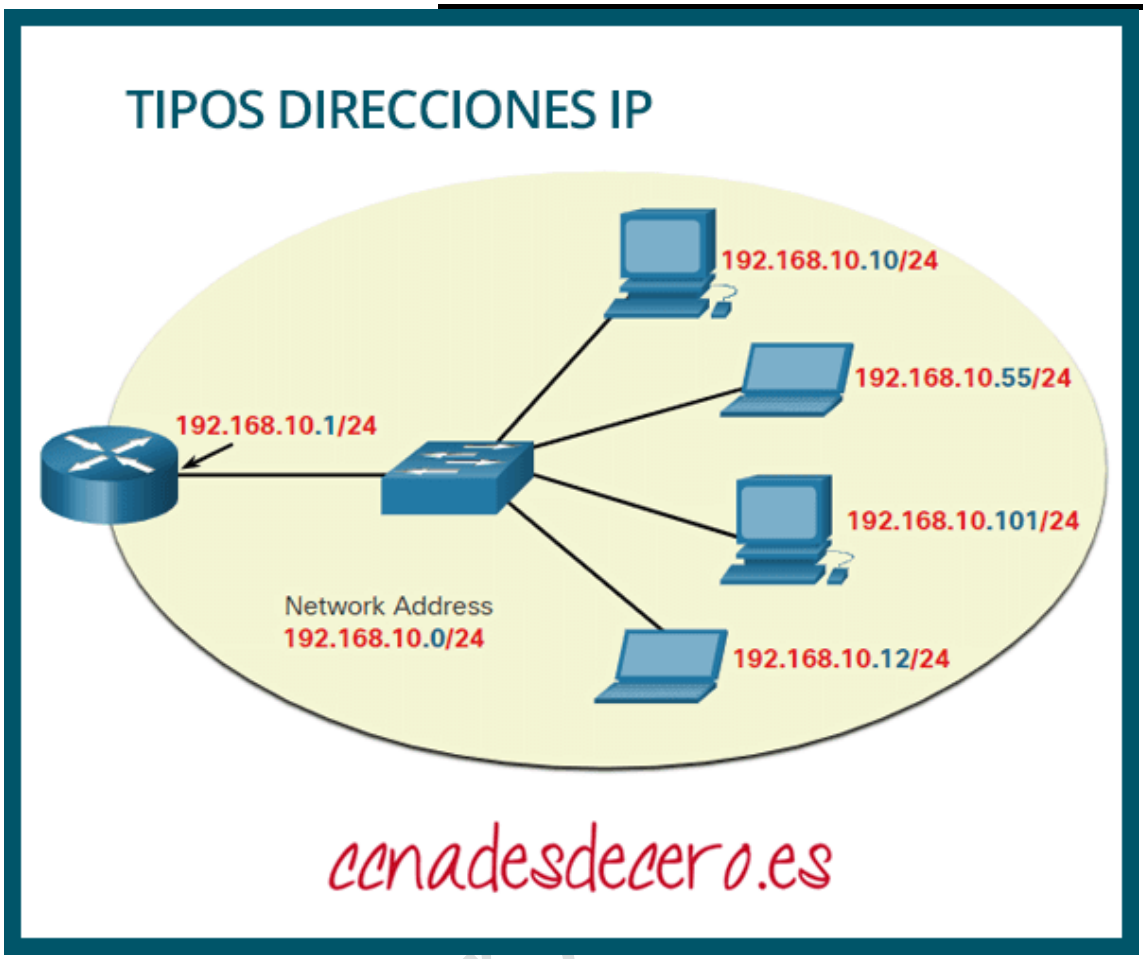


Asociar IPv4 con máscara de subred

Tenga en cuenta que la máscara de subred en realidad no contiene la porción de red o host de una dirección IPv4, solo le dice a la computadora dónde buscar la parte de la dirección IPv4 que es la porción de red y qué parte es la porción de host.

El proceso real utilizado para identificar la porción de red y la porción de host se llama **ANDing**.

Usando la topología en la imagen, se examinarán estos tres tipos de direcciones.



Tipos de direcciones IP

Dirección de red

Una dirección de red es una dirección que representa una red específica. Un dispositivo pertenece a esta red si cumple tres criterios:

- Tiene la misma máscara de subred que la dirección de red.
- Tiene los mismos bits de red que la dirección de red, como lo indica la máscara de subred.
- Se encuentra en el mismo dominio de difusión que otros hosts con la misma dirección de red.

Un host determina su dirección de red realizando una operación AND entre su dirección IPv4 y su máscara de subred.

Como se muestra en la tabla, la dirección de red tiene todos los 0 bits en la parte del host, según lo determinado por la máscara de subred. En este ejemplo, la dirección de red es 192.168.10.0/24. No se puede asignar una dirección de red a un dispositivo.

- DIRECCIONES DE RED IPV6 .

Descripción general de las direcciones IPv6

Las direcciones IPv6 se asignan a interfaces en lugar de a nodos, teniendo en cuenta que en un nodo puede haber más de una interfaz. Asimismo, se puede asignar más de una

IPv6 abarca tres clases de direcciones:

unidifusión

Identifica una interfaz de un solo nodo.

multidifusión

Identifica un grupo de interfaces, en general en nodos distintos. Los paquetes que se envían a una dirección multidifusión se dirigen a todos los miembros del grupo de multidifusión.

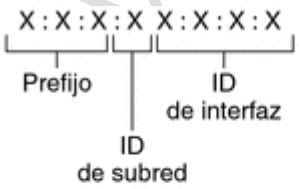
difusión por proximidad

Identifica un grupo de interfaces, en general en nodos distintos. Los paquetes que se envían a una dirección de difusión por proximidad de dirigen al nodo de miembros del grupo de difusión por proximidad que se encuentre más cerca del remitente.

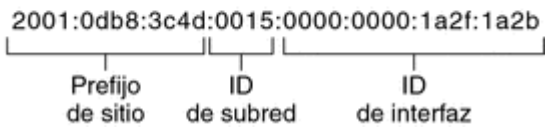
Partes de una dirección IPv6

Una dirección IPv6 tiene un tamaño de 128 bits y se compone de ocho campos de 16 bits, cada uno de ellos unido por dos puntos. Cada campo debe contener un número hexadecimal, a diferencia de la notación decimal con puntos de las direcciones IPv4. En la figura siguiente, las equis representan números hexadecimales.

FIGURA 3–2 FORMATO BÁSICO DE LAS DIRECCIONES IPV6



Ejemplo:



Los tres campos que están más a la izquierda (48 bits) contienen el prefijo de sitio. El prefijo describe la topología pública que el ISP o el RIR (Regional Internet Registry, Registro Regional de Internet) suelen asignar al sitio.

El campo siguiente lo ocupa el ID de subred de 16 bits que usted (u otro administrador) asigna al sitio. El ID de subred describe la topología privada, denominada también topología del sitio, porque es interna del sitio.

Los cuatro campos situados más a la derecha (64 bits) contienen el ID de interfaz, también denominado token. El ID de interfaz se configura automáticamente desde la dirección MAC de interfaz o manualmente en formato EUI-64.

Examine de nuevo la dirección de la figura Figura 3–2:

```
2001:0db8:3c4d:0015:0000:0000:1a2f:1a2b
```

En este ejemplo se muestran los 128 bits completos de una dirección IPv6. Los primeros 48 bits, 2001:0db8:3c4d, contienen el prefijo de sitio y representan la topología pública. Los siguientes 16 bits, 0015, contienen el ID de subred y representan la topología privada del sitio. Los 64 bits que están más a la derecha, 0000:0000:1a2f:1a2b, contienen el ID de interfaz.

Abreviación de direcciones IPv6

La mayoría de las direcciones IPv6 no llegan a alcanzar su tamaño máximo de 128 bits. Eso comporta la aparición de campos rellenados con ceros o que sólo contienen ceros.

La arquitectura de direcciones IPv6 permite utilizar la notación de dos puntos consecutivos (: :) para representar campos contiguos de 16 bits de ceros. Por ejemplo, la dirección IPv6 de la Figura 3–2 se puede abreviar reemplazando los dos campos contiguos de ceros del ID de interfaz por dos puntos. La dirección resultante es 2001:0db8:3c4d:0015::1a2f:1a2b. Otros campos de ceros pueden representarse como un único 0. Asimismo, puede omitir los ceros que aparezcan al inicio de un campo, como por ejemplo cambiar 0db8 por db8.

Así pues, la dirección `2001:0db8:3c4d:0015:0000:0000:1a2f:1a2b` se puede abreviar en `2001:db8:3c4d:15::1a2f:1a2b`.

La notación de los dos puntos consecutivos se puede emplear para reemplazar cualquier campo contiguo de ceros de la dirección IPv6. Por ejemplo, la dirección IPv6 `2001:0db8:3c4d:0015:0000:d234::3eee:0000` se puede contraer en `2001:db8:3c4d:15:0:d234:3eee::`.

PREFIJOS DE IPV6

Los campos que están más a la izquierda de una dirección IPv6 contienen el prefijo, que se emplea para enrutar paquetes de IPv6. Los prefijos de IPv6 tienen el formato siguiente:

prefijo/tamaño en bits

El tamaño del prefijo se expresa en notación CIDR (enrutamiento entre dominios sin clase). La notación CIDR consiste en una barra inclinada al final de la dirección,

seguida por el tamaño del prefijo en bits. Para obtener información sobre direcciones IP en formato CIDR, consulte Cómo diseñar un esquema de direcciones IPv4 CIDR.

El prefijo de sitio de una dirección IPv6 ocupa como máximo los 48 bits de la parte más a la izquierda de la dirección IPv6. Por ejemplo, el prefijo de sitio de la dirección IPv6 2001:db8:3c4d:0015:0000:0000:1a2f:1a2b/48 se ubica en los 48 bits que hay más a la izquierda, 2001:db8:3c4d. Utilice la representación siguiente, con ceros comprimidos, para representar este prefijo:

```
2001:db8:3c4d::/48
```

Nota –

`2001:db8::/32` es un prefijo especial de IPv6 que se emplea específicamente en ejemplos de documentación.

También se puede especificar un prefijo de subred, que define la topología interna de la red respecto a un enrutador. La dirección IPv6 de ejemplo tiene el siguiente prefijo de subred:

```
2001:db8:3c4d:15::/64
```

El prefijo de subred siempre contiene 64 bits. Estos bits incluyen 48 del prefijo de sitio, además de 16 bits para el ID de subred.

Los prefijos siguientes se han reservado para usos especiales:

`2002::/16`

Indica que sigue un prefijo de enrutamiento de 6to4.

`fe80::/10`

Indica que sigue una dirección local de vínculo.

`ff00::/8`

Indica que sigue una dirección multidifusión.

Direcciones unidifusión

IPv6 incluye dos clases de asignaciones de direcciones unidifusión:

- Dirección unidifusión global
- Dirección local de vínculo

El tipo de dirección unidifusión viene determinado por los bits contiguos que están más a la izquierda (orden superior) de la dirección, los cuales contienen el prefijo.

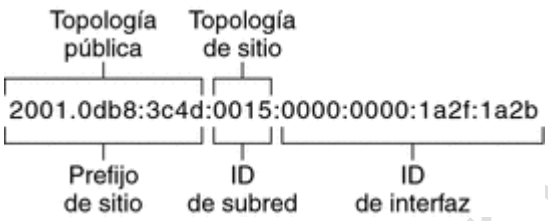
El formato de direcciones unidifusión se organiza conforme a la jerarquía siguiente:

- Topología pública
- Topología de sitio (privada)
- ID de interfaz

Dirección unidifusión global

La dirección unidifusión global es globalmente exclusiva de Internet. La dirección IPv6 de ejemplo que hay en Prefijos de IPv6 es de unidifusión global. En la figura siguiente se muestra el ámbito de la dirección unidifusión global, en comparación con las partes que componen la dirección IPv6.

Figura 3–3 Partes de la dirección unidifusión global



Topología pública

El prefijo de sitio define la topología pública de la red respecto a un enrutador. El ISP o el RIR proporcionan el prefijo de sitio a las empresas.

Topología de sitio y subredes IPv6

En IPv6, el ID de subred define una subred administrativa de la red y tiene un tamaño máximo de 16 bits. Un ID de subred se asigna como parte de la configuración de redes IPv6. El prefijo de subred define la topología de sitio respecto a un enrutador especificando el vínculo al que se ha asignado la subred.

Desde un punto de vista conceptual, las subredes IPv6 y las IPv4 son iguales en el sentido de que cada subred suele asociarse con solo vínculo de hardware. Sin embargo, los ID de subredes IPv6 se expresan en notación hexadecimal, en lugar de decimal con puntos.

ID de interfaz

El ID de interfaz identifica una interfaz de un determinado nodo. Un ID de interfaz debe ser exclusivo en la subred. Los hosts de IPv6 pueden aplicar el protocolo ND para generar automáticamente sus propios ID de interfaz. El protocolo ND genera de forma

automática el ID de interfaz, a partir de la dirección MAC o la dirección EUI-64 de la interfaz del host. Los ID de interfaz también se pueden asignar manualmente, lo cual es preferible en el caso de enrutadores de IPv6 y servidores habilitados para IPv6. Si desea obtener instrucciones sobre cómo crear manualmente direcciones EUI-3513, consulte RFC 3513 Internet Protocol Version 6 (IPv6) Addressing Architecture.

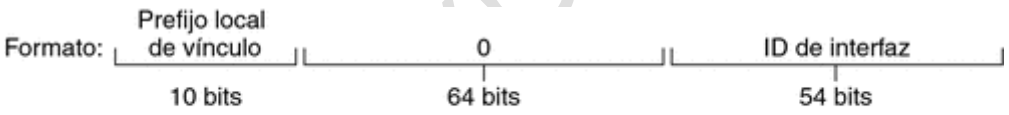
Direcciones unidifusión globales de transición

Por motivos de transición, el protocolo IPv6 incluye la posibilidad de incrustar una dirección IPv4 en una dirección IPv6. Esta clase de dirección IPv4 facilita la colocación en túneles de paquetes IPv6 en redes IPv4 ya configuradas. La dirección 6to4 es un ejemplo de dirección unidifusión global de transición. Para obtener más información sobre direcciones 6to4, consulte Túneles automáticos 6to4.

Dirección unidifusión local de vínculo

La dirección unidifusión local de vínculo sólo se puede utilizar en el vínculo de red local. Las direcciones locales de vínculo no son válidas ni se reconocen fuera del ámbito corporativo u organizativo. A continuación se muestra un ejemplo del formato que tienen las direcciones locales de vínculo.

Ejemplo 3–1 Partes de la dirección unidifusión local de vínculo



Ejemplo: fe80::123e:456d

Un **prefijo local de vínculo** presenta el formato siguiente:

`fe80::`*ID_interfaz*`/10`

A continuación se muestra una dirección local de vínculo:

```
fe80::23a1:b152
```

`fe80`

Representación hexadecimal del prefijo binario de 10 bits 1111111010. Este prefijo identifica el tipo de dirección IPv6 como dirección local de vínculo.

ID_interfaz

Dirección hexadecimal de la interfaz, que en general se deriva de la dirección MAC de 48 bits.

Al habilitar IPv6 durante la instalación de Oracle Solaris, la interfaz con el número más bajo del equipo local se configura con una dirección local de vínculo. Cada interfaz necesita por lo menos una dirección local de vínculo para identificar el nodo en los demás nodos del vínculo local. Así pues, las direcciones locales de vínculo deben configurarse manualmente para las interfaces adicionales de un nodo. Tras la configuración, el nodo utiliza sus direcciones locales de vínculo para la configuración automática de direcciones y el descubrimiento de vecinos.

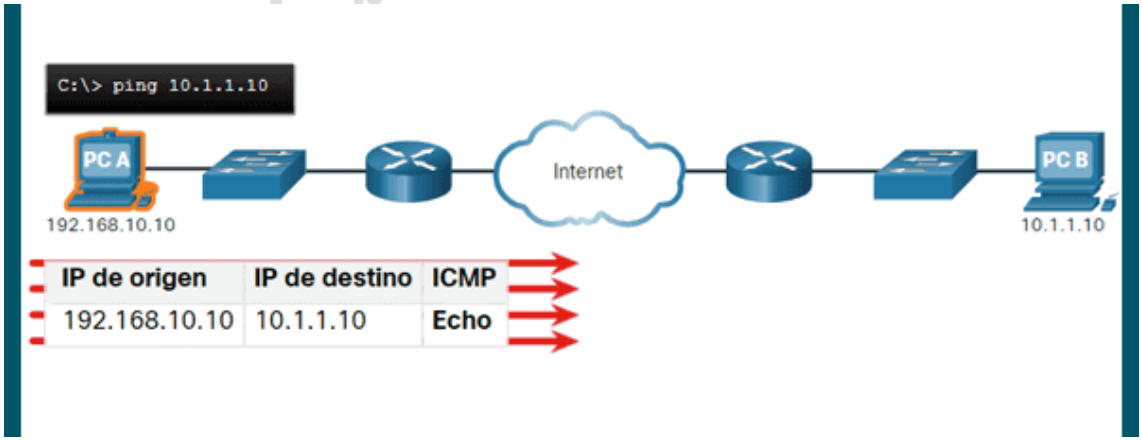
- VERIFICACIÓN DE CONECTIVIDAD.

El comando `ping` es la forma más efectiva de probar rápidamente la conectividad de Capa 3 entre una dirección IP de origen y de destino. El comando también muestra varias estadísticas de tiempo de ida y vuelta.

Específicamente, el comando `ping` utiliza los mensajes ECHO del Protocolo de mensajes de control de Internet (ICMP) (ICMP tipo 8) y de respuesta ECHO (ICMP tipo 0). El comando **ping** está disponible en la mayoría de los sistemas operativos, incluidos Windows, Linux, macOS y Cisco IOS.

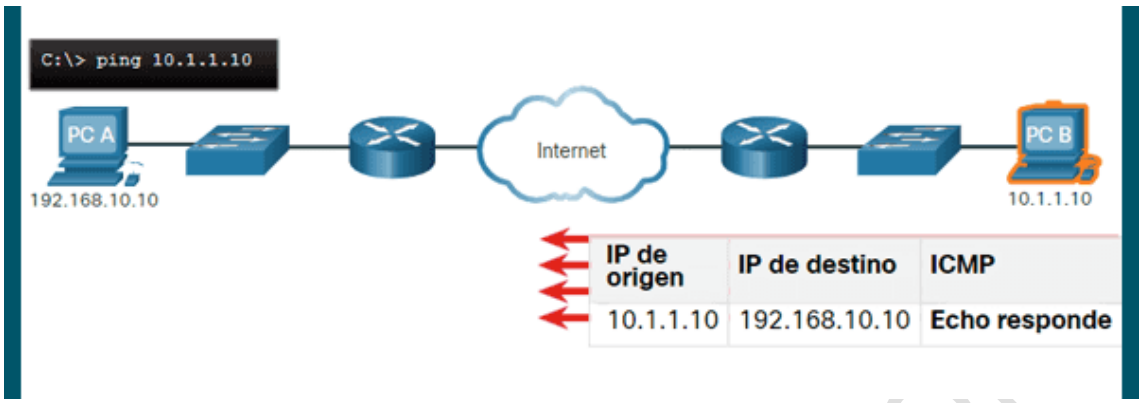
En un host con Windows 10, el comando **ping** envía cuatro mensajes de ECHO ICMP consecutivos y espera cuatro respuestas de ECHO ICMP consecutivas desde el destino.

Por ejemplo, suponga que la PC A hace ping a la PC B. Como se muestra en la imagen, el host de la PC A Windows envía cuatro mensajes de ECHO ICMP consecutivos a la PC B (es decir, 10.1.1.10).



Ejemplo comando Ping

El host de destino recibe y procesa los ECHOS ICMP. Como se muestra en la imagen, la PC B responde enviando cuatro mensajes de respuesta de ECHO ICMP a la PC A.



Respuesta de echo ICMP

Como se muestra en la salida del comando, la PC A ha recibido respuestas de ECHO de la PC-B verificando la conexión de red de Capa 3.

```
C:\Users\PC-A> ping 10.1.1.10
Pinging 10.1.1.10 with 32 bytes of data:
Reply from 10.1.1.10: bytes=32 time=47ms TTL=51
Reply from 10.1.1.10: bytes=32 time=60ms TTL=51
Reply from 10.1.1.10: bytes=32 time=53ms TTL=51
Reply from 10.1.1.10: bytes=32 time=50ms TTL=51
Ping statistics for 10.1.1.10:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 47ms, Maximum = 60ms, Average = 52ms
C:\Users\PC-A>
```

La salida valida la conectividad de Capa 3 entre la PC A y la PC B.

La salida del comando ping del Cisco IOS varía de un host de Windows. Por ejemplo, el ping de IOS envía cinco mensajes de ECHO ICMP, como se muestra en la salida.

```
R1# ping 10.1.1.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
R1#
```

Nota los caracteres **!!!!!** de salida. El comando ping IOS muestra un indicador para cada respuesta de ECHO ICMP recibida. La tabla enumera los caracteres de salida más comunes del comando ping .

Indicadores de ping en Cisco IOS

Elemento	Descripción
!	• El signo de exclamación indica la recepción exitosa de un mensaje de respuesta de ECHO. • Valida una conexión de Capa 3 entre el origen y el destino.
.	• Un punto significa que el tiempo expiró esperando un mensaje de respuesta de ECHO. • Esto indica que ocurrió un problema de conectividad en algún lugar a lo largo del camino.
U	• **U** mayúscula indica que un Router a lo largo de la ruta respondió con un mensaje de error ICMP tipo 3 «destino inalcanzable». • Las posibles razones incluyen que el Router no conoce la dirección hacia la red de destino o no pudo encontrar el host en la red de destino.

- USO DE COMANDOS DE VERIFICACIÓN.

Comandos para la verificación de la configuración

Los diversos comandos show se pueden utilizar para visualizar información sobre el sistema, examinar el contenido de los archivos de configuración del router y diagnosticar fallos. Tanto en el modo privilegiado como en el modo de usuario, el comando show ? muestra una lista de los comandos show disponibles. El número de comandos disponibles en modo privilegiado es mayor que en el modo de usuario.

A continuación, se presentan algunos de estos comandos que se podrán ejecutar en modo usuario o en modo privilegiado.

`show version`	Muestra información acerca de la versión del software CISCO IOS en uso en el router: Versión e información descriptiva del IOS; Versión de la ROM de bootstrap; Versión de la ROM de arranque; Tiempo de actividad del router; Último método de reinicio; Ubicación y nombre del archivo de imagen del sistema; Plataforma del router; Valores del registro de configuración.
`show flash:`	Muestra información acerca de la memoria flash y los archivos IOS que se encuentran almacenados en ella.
`show clock`	Muestra la hora fijada en el router.
`show arp`	Muestra la tabla ARP del router.
`show controllers serial <slot/puerto>`	Muestra información específica de la interfaz de hardware.
`show startup-config`	Muestra el archivo de configuración almacenado en la NVRAM.
`show running-config`	Muestra el contenido del archivo de configuración activo.
`show hosts`	Muestra la lista en caché de los nombres de dispositivos y sus direcciones.
`show users`	Muestra todos los usuarios conectados al router.
`show history`	Muestra un historial de los comandos introducidos.
`show interfaces`	Muestra las estadísticas completas de todas las interfaces del router.

`show ip interfaces brief`	Muestra la dirección IP y el estado de todas las interfaces.
`show interfaces <tipo> <slot/puerto>`	Muestra las estadísticas de una interfaz específica.
`show protocols`	Muestra el estado global y por interfaz de cualquier protocolo de capa 3 que haya sido configurado.

- NAVEGACIÓN CLI.

Existen varias herramientas de CISCO en formato GUI para no tener que tener un amplio conocimiento sobre el CLI de Cisco. Entre estas herramientas están:

- Asistente de red Cisco. Es una aplicación GUI basada en PC para la administración de redes optimizada para redes pequeñas y medianas. Es gratuito y se puede descargar aqui una vez logado en cisco.

- CiscoView. Proporciona una vista física del switch que se puede utilizar para estrablecer parámetros de configuración y para ver la información de funcionamiento y el estado del switch. No es gratuida y se puede descargar aquí.

- Administrador de dispositivos Cisco. Software basado en Web y en la memoria del switch.

- Administración de red SNMP. Puede administrar switches desde una estación de administración compatible con SNMP.

Los modos Interfaz de la línea de comando

Sintaxis de comando de la CLI del IOS de Cisco	
Cambia de modo EXEC usuario a modo EXEC privilegiado.	switch>**enable**
Si una contraseña ha sido configurada para modo EXEC privilegiado, se le solicitará que la ingrese ahora.	password:**Contraseña**
La petición de entrada # significa modo EXEC privilegiado.	switch#
Cambia de modo EXEC privilegiado a modo EXEC usuario.	switch#**disable**
La petición de entrada > significa modo EXEC usuario.	switch>

Los modos Interfaz de la línea de comando

Sintaxis de comando de la CLI del IOS de Cisco	
Cambia de modo EXEC privilegiado a modo de configuración global.	switch#**configure terminal**
La petición de entrada (config)# significa que el switch está en modo de configuración global.	switch(config)#
Cambia de modo de configuración global a modo de configuración de interfaz para la interfaz 0/1 fast ethernet.	switch(config)#**interface fastethernet 0/1**
La petición de entrada (config)# significa que el switch está en modo de configuración de interfaz.	switch(config-if)#
Cambia de modo de configuración de interfaz a modo de configuración global.	switch(config-if)#**exit**
La petición de entrada (config)# significa que el switch está en modo de configuración global.	switch(config)#
Cambia de modo de configuración global a modo EXEC privilegiado.	switch(config)#**exit**
La petición de entrada # significa que el switch está en modo EXEC privilegiado.	switch#

- CONFIGURACIÓN CLI.

El modo de configuración de la Junos OS CLI le permite configurar un dispositivo mediante instrucciones de configuración para establecer, administrar y supervisar las propiedades del dispositivo.

Descripción del modo de configuración de CLI

Puede configurar todas las Junos OS propiedades, incluidas las interfaces, la información general de enrutamiento, los protocolos de enrutamiento y el acceso de usuario, así como varias propiedades de hardware del sistema.

Como describe descripción de los modos, comandos y jerarquías de instrucciones de la CLI de Junos OS , una configuración de dispositivo se almacena como una jerarquía de instrucciones. En el modo de configuración, se crea un conjunto de instrucciones de

configuración para usar. Cuando termine de escribir las instrucciones de configuración y esté seguro de que están completas y correctas, las confirma, lo que activa la configuración en el dispositivo.

Puede crear la configuración de forma interactiva o crear un archivo de texto ASCII que contenga la configuración, cargarla en el dispositivo y confirmarla.

- Comandos del modo de configuración
- Instrucciones e identificadores de configuración
- Jerarquía de instrucciones de configuración

Comandos del modo de configuración

La siguiente tabla resume cada comando de modo de configuración de CLI. Los comandos se organizan alfabéticamente.

Tabla 1: Resumen de los comandos del modo de configuración

Comando	Descripción
`activate`	Quite la `inactive:` etiqueta de una instrucción. Las instrucciones o identificadores que se han activado surtan efecto cuando el siguiente problema es el `commit` comando.
`annotate`	Agregue comentarios a una configuración. Solo puede agregar comentarios en el nivel de jerarquía actual.
`commit`	Confirme el conjunto de cambios en la base de datos y hacer que los cambios surtan efecto operativo.
`copy`	Haga una copia de una instrucción existente en la configuración.
`deactivate`	Agregue la `inactive:` etiqueta a una instrucción, comentando efectivamente la instrucción o identificador desde la configuración. Las instrucciones o identificadores marcados como inactivos se ignoran cuando se emite el `commit` comando.
`delete`	Eliminar una instrucción o identificador. Todas las instrucciones e identificadores subordinados contenidos en la ruta de instrucción especificada se eliminan con ella.
`edit`	Moverse dentro de la jerarquía de instrucciones especificada. Si la instrucción no existe, se crea.

`exit`	Salga del nivel actual de la jerarquía de instrucciones, vuelva al nivel antes del último comando de edición o salga del modo de configuración. Los `quit` comandos y `exit` son equivalentes.
`extension`	Administre las configuraciones que contribuyen los paquetes de aplicaciones del SDK. Administrándolas mediante la visualización o eliminación de configuraciones definidas por el usuario que contribuyó con el paquete de aplicación de SDK denominado. El comando de extensión nunca elimina una configuración definida en cualquier paquete nativo Junos OS .
`help`	Muestra ayuda sobre las instrucciones de configuración disponibles.
`insert`	Inserte un identificador en una jerarquía existente.
`load`	Cargue una configuración desde un archivo de configuración ASCII o desde la entrada del terminal. La ubicación actual en la jerarquía de configuración se ignora cuando se produce la operación de carga.
`quit`	Salga del nivel actual de la jerarquía de instrucciones, vuelva al nivel antes del último comando de edición o salga del modo de configuración. Los `quit` comandos y `exit` son equivalentes.
`rename`	Cambie el nombre de una instrucción o identificador de configuración existente.
`replace`	Reemplace identificadores o valores en una configuración.
`rollback`	Vuelva a una configuración previamente confirmada. El software guarda las últimas 10 configuraciones confirmadas, incluido el número de reversión, la fecha, la hora y el nombre del usuario que emitió el `commit configuration` comando.
`run`	Ejecute un comando de CLI sin salir del modo de configuración.
`save`	Guarde la configuración en un archivo ASCII. Las instrucciones de configuración hasta el nivel actual de la jerarquía de instrucciones se guardan, junto con la jerarquía de instrucciones que la contiene. Esta acción permite guardar una sección de la configuración, a la vez que se especifica por completo la jerarquía de instrucciones.

`set`	Cree una jerarquía de instrucciones y establezca valores de identificador. Este comando es similar a `edit`, excepto que el nivel actual de la jerarquía no cambia.
`show`	Muestra la configuración actual.
`status`	Muestra los usuarios que editan actualmente la configuración.
`top`	Vuelva al nivel superior del modo de comando de configuración, que se indica en el `[edit]` banner.
`up`	Subir un nivel en la jerarquía de instrucciones.
`update`	Actualizar una base de datos privada.
`wildcard delete`	Eliminar una instrucción o identificador. Todas las instrucciones e identificadores subordinados contenidos en la ruta de instrucción especificada se eliminan con ella. Puede usar expresiones regulares para especificar un patrón. Según este patrón, el sistema operativo busca elementos que contienen estos patrones y los elimina.

Instrucciones e identificadores de configuración

Puede configurar las propiedades del dispositivo incluyendo las instrucciones correspondientes en la configuración. Por lo general, una instrucción se compone de una palabra clave definida por el sistema, que es texto fijo y un identificador opcional. Un identificador es un nombre de identificación que puede definir, como el nombre de una interfaz o un nombre de usuario, lo que le permite a usted y a la CLI diferenciarse entre una colección de instrucciones.

Tabla 2 enumera instrucciones de configuración de nivel superior. Consulte el Explorador de CLI para obtener información sobre cada instrucción de configuración.

Tabla 2: Instrucciones de nivel superior del modo de configuración

Declaración	Descripción
`access`	Configure el protocolo de autenticación de enlace de desafío (CHAP).
`accounting-options`	Configure la recopilación de datos de estadísticas contables para interfaces y filtros de firewall.

chassis	Configure las propiedades del chasis del enrutador, incluidas las condiciones que activan las alarmas y las propiedades de trama y concatenación SONET/SDH.
class-of-service	Configure parámetros de clase de servicio.
firewall	Configure filtros que seleccionen paquetes según su contenido.
forwarding-options	Configure opciones de reenvío, incluidas las opciones de muestreo de tráfico.
groups	Configure grupos de configuración.
interfaces	Configure información de interfaz, como encapsulación, interfaces, identificadores de canal virtual (VCIs) e identificadores de conexión de vínculo de datos (DLCIs).
policy-options	Configure políticas de enrutamiento, que le permiten filtrar y establecer propiedades en rutas entrantes y salientes.
protocols	Configure protocolos de enrutamiento, incluidos BGP, IS-IS, LDP, MPLS, OSPF, RIP y RSVP.
routing-instances	Configure una o más instancias de enrutamiento.
routing-options	Configure opciones de enrutamiento independientes del protocolo, como rutas estáticas, números de sistema autónomo, miembros de confederación y operaciones de rastreo global (depuración) para registrar.
security	Configure los servicios de seguridad IP (IPsec).
snmp	Configure cadenas de comunidad SNMP, interfaces, trampas y notificaciones.
system	Configure las propiedades de todo el sistema, incluyendo el nombre de host, el nombre de dominio, el servidor del sistema de nombres de dominio (DNS), los inicios de sesión y los permisos de usuario, las asignaciones entre nombres de host y direcciones y los procesos de software.

JERARQUÍA DE INSTRUCCIONES DE CONFIGURACIÓN

La Junos OS configuración consta de una jerarquía de instrucciones. Hay dos tipos de instrucciones:

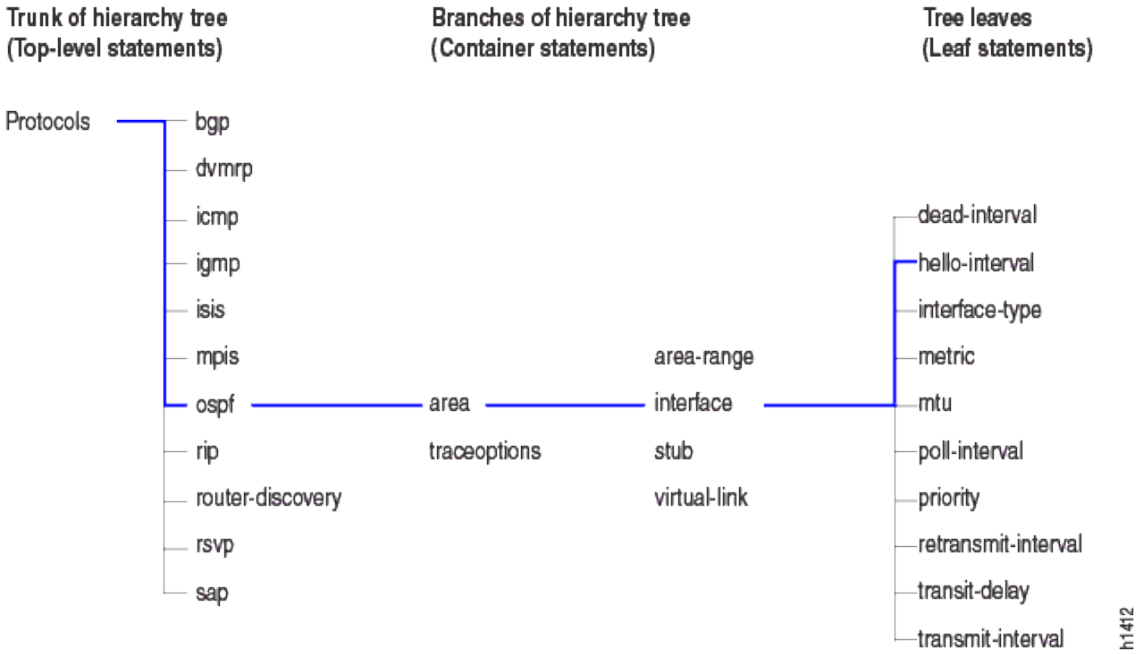
- Instrucciones de contenedor, que son sucursales que pueden contener otras instrucciones (incluidas instrucciones de contenedor adicionales o instrucciones leaf). Las instrucciones de contenedor en la parte superior de la jerarquía se consideran el troncal del árbol jerárquico.

- Instrucciones Leaf (contenidas por instrucciones contenedoras), que no contienen otras instrucciones.

Las instrucciones container y leaf forman la jerarquía de configuración. Cada instrucción en el nivel superior de la jerarquía de configuración reside en el troncal de un árbol jerárquico. Estas instrucciones de nivel superior son instrucciones contenedoras, que contienen otras instrucciones que forman las ramas de árbol. Las instrucciones leaf son las hojas del árbol de jerarquía. Una jerarquía individual de instrucciones, que comienza en el tronco del árbol jerárquico, se denomina ruta de instrucción.

En la siguiente ilustración se muestra el árbol de jerarquía, que ilustra una ruta de instrucción para la parte de la jerarquía de configuración de protocolo responsable de configurar la hello-interval instrucción en una interfaz en un área OSPF.

Figura 1: Jerarquía de instrucciones en modo de configuración



La protocols instrucción es una instrucción de nivel superior en el troncal del árbol de configuración. Las ospfinstrucciones , areay son interface todas instrucciones de contenedor subordinadas de una instrucción superior (son ramas del árbol de jerarquía).

La hello-interval instrucción es una hoja en el árbol, que en este caso contiene un valor de datos, a saber, la longitud del hello-interval, en segundos.

En el siguiente ejemplo de configuración se muestra la jerarquía de instrucciones como se muestra en Figura 1:

`[edit protocols ospf area area-number interface interface-name]`

El comando muestra la configuración de la siguiente manera:

content_copy zoom_out_map

```
protocols {
    ospf {
        area 0.0.0.0 {
            interface so-0/0/0 {
                hello-interval 5;
            }
            interface so-0/0/1 {
                hello-interval 5;
            }
        }
    }
}
```

La CLI indenta cada nivel de la jerarquía para indicar la posición relativa de cada instrucción en la jerarquía. Además, en general, establece cada nivel con llaves, utilizando una llave abierta al principio de cada nivel jerárquico y una llave de cierre al final. Si la instrucción en un nivel de jerarquía está vacía, las llaves no se imprimen.

Cada instrucción leaf termina con un punto y coma. Si la jerarquía no se extiende hasta una instrucción leaf, la última instrucción de la jerarquía termina con un punto y coma.

La jerarquía de configuración también puede contener "oneliners" en el nivel más bajo de la jerarquía. Los oneliners eliminan un nivel de llaves en la sintaxis y muestran la instrucción container, sus identificadores, la instrucción child o leaf y sus atributos en una sola línea.

Por ejemplo, `dynamic-profile dynamic-profile-name aggregate-clients;` es un oneliner porque la `dynamic-profile` instrucción, su identificador *dynamic-profile-name*y la instrucción `aggregate-clients` leaf aparecen en una sola línea cuando se ejecuta el show comando en modo de configuración:

content_copy zoom_out_map

```
[edit forwarding-options]
user@host# show
dhcp-relay {
    dynamic-profile dynamic-profile-name aggregate-clients;
}
```

- ESQUEMATIZACIÓN DE DIRECCIONAMIENTO IPV4 E IPV6.

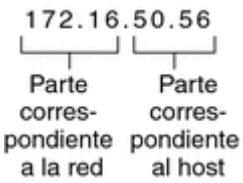
Cada red basada en IPv4 debe contar con:

- Un número de red exclusivo asignado por un ISP, un IR o, para las redes más antiguas, registrado por la IANA. Si tiene previsto utilizar direcciones privadas, los números de red que cree deben ser exclusivos en su organización.
- Direcciones IPv4 exclusivas para las interfaces de cada sistema en la red.
- Una máscara de red.

La dirección IPv4 es un número de 32 bits que identifica de forma exclusiva una interfaz de red en un sistema, tal como se explica en Aplicación de las direcciones IP a las interfaces de red. Una dirección IPv4 se escribe en dígitos decimales, y se divide en cuatro campos de 8 bits separados por puntos. Cada campo de 8 bits representa un byte de la dirección IPv4. Este modo de representar los bytes de una dirección IPv4 se denomina normalmente **formato de decimales con puntos**.

La figura siguiente muestra los componentes de una dirección IPv4, 172.16.50.56.

FIGURA 2–1 FORMATO DE DIRECCIONES IPV4



172.16

Número de red IPv4 registrada. En la notación IPv4 basada en clases, este número también define la clase de red IP (la clase B en este ejemplo), que registra la IANA.

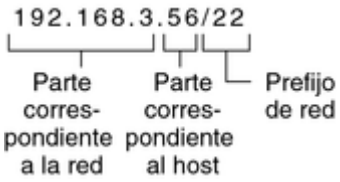
50.56

Parte del host de la dirección IPv4. La parte del host identifica de forma exclusiva una interfaz en un sistema de una red. Para cada interfaz de una red local, la parte de la red de la dirección es la misma, pero la parte del host debe ser diferente.

Si tiene previsto crear una subred de una red IPv4 basada en clases, debe definir una máscara de subred o **máscara de red**, tal como se describe en Base de datos netmasks.

El ejemplo siguiente muestra la dirección de formato CIDR 192.168.3.56/22

FIGURA 2–2 DIRECCIÓN IPV4 DE FORMATO CIDR



192.168.3

Parte de la red, que se compone del número de red IPv4 que se recibe de un ISP o un IR.

56

Parte del host, que se asigna a una interfaz de un sistema.

/22

Prefijo de la red, que define cuántos bits de la dirección componen el número de red. El prefijo de la red también proporciona la máscara de subred para la dirección IP. Los prefijos de red también los asigna el ISP o el IR.

Una red basada en Oracle Solaris puede combinar direcciones IPv4 estándar, direcciones IPv4 con formato CIDR, direcciones DHCP, direcciones IPv6 y direcciones IPv4 privadas.

CREACIÓN DEL ESQUEMA DE NUMERACIÓN DE IPV6

A menos que la red IPv6 que se proponga sea totalmente nueva, la topología de IPv4 ya configurada sirve de base para el esquema de numeración de IPv6.

CREACIÓN DE UN ESQUEMA DE NUMERACIÓN PARA SUBREDES

Inicie el esquema de numeración asignando las subredes IPv4 ya configuradas a subredes IPv6 equivalentes. Por ejemplo, fíjese en las subredes de la Figura 4–1. Las subredes 1–4 utilizan la designación de redes privadas IPv4 de RFC 1918 para los primeros 16 bits de sus direcciones, además de los dígitos 1–4 para indicar la subred. A modo de ejemplo, suponga que el prefijo de IPv6 2001:db8:3c4d/48 se ha asignado al sitio.

La tabla siguiente muestra la asignación de prefijos de IPv4 privados a prefijos de IPv6.

Prefijo de subred IPv4	**Prefijo de subred IPv6 equivalente**
192.168.1.0/24	2001:db8:3c4d:1::/64

Prefijo de subred IPv4	Prefijo de subred IPv6 equivalente
192.168.2.0/24	2001:db8:3c4d:2::/64
192.168.3.0/24	2001:db8:3c4d:3::/64
192.168.4.0/24	2001:db8:3c4d:4::/64

CREACIÓN DE UN PLAN DE DIRECCIONES IPV6 PARA NODOS

En la mayoría de los hosts, la configuración automática sin estado de direcciones IPv6 para sus interfaces constituye una estrategia válida y eficaz. Cuando el host recibe el prefijo de sitio del enrutador más próximo, el protocolo ND genera de forma automática direcciones IPv6 para cada interfaz del host.

Los servidores necesitan direcciones IPv6 estables. Si no configura manualmente las direcciones IPv6 de un servidor, siempre que se reemplaza una tarjeta NIC del servidor se configura automáticamente una dirección IPv6. Al crear direcciones para servidores debe tenerse en cuenta lo siguiente:

- Proporcione a los servidores unos ID de interfaz descriptivos y estables. Un método consiste en aplicar un sistema de numeración consecutiva a los ID de interfaz. Por ejemplo, la interfaz interna del servidor LDAP que aparece en la Figura 4–1 podría ser 2001:db8:3c4d:2::2.
- Si habitualmente no cambia la numeración de la red IPv4, es buena idea utilizar como ID de interfaz las direcciones IPv4 ya creadas de los enrutadores y servidores. En la Figura 4–1, suponga que la interfaz del enrutador 1 con la DMZ tiene la dirección IPv4 123.456.789.111. La dirección IPv4 puede convertirse a hexadecimal y aplicar el resultado como ID de interfaz. El nuevo ID de interfaz será ::7bc8:156F.

  Este planteamiento se utiliza sólo si se es el propietario de la dirección IPv4 registrada, en lugar de haber obtenido la dirección de un ISP. Si utiliza una dirección IPv4 proporcionada por un ISP, se crea una dependencia que puede causar problemas en caso de cambiar los ISP.

Debido al número limitado de direcciones IPv4, antes un diseñador de redes debía tener en cuenta si iba a utilizar direcciones registradas globales y direcciones RFC 1918 privadas. No obstante, el concepto de direcciones IPv4 globales y privadas no es aplicable a las direcciones IPv6 . Puede utilizar direcciones unidifusión globales, que incluyen el prefijo de sitio, en todos los vínculos de la red, incluida la DMZ pública.

- ASIGNACIÓN DE DIRECCIONAMIENTO IPV4 E IPV6.

IPV4

El protocolo de internet versión 4 fue el primero de implementarse a gran escala definido como un direccionamiento que consta de 32 bits y tiene un espacio de más de 4 millones de direcciones únicas, cada dirección se encuentra dividida en dos partes, la primera parte correspondiente a las direcciones de red y la segunda a las direcciones de los hosts locales. Cada parte se divide en 2 grupos de ocho bits, cada bit tiene un valor binario que va desde 0 que es el mínimo hasta 255 que es el máximo del octeto es decir todos son 1, este conjunto de valores es representado por una notación decimal separadas por puntos. (Rodriguez A, Tejada Z, & Villao Q, 2014)

Fases de Agotamiento de IPv4

Aunque este protocolo contenga bastantes direcciones, la IANA ente que proporciona el direccionamiento IP ha pronunciado el desgaste de este protocolo el cual se encuentra en su fase de agotamiento en la región de LACNIC, el agotamiento se refiere a la etapa de reservas donde las designaciones de este protocolo son limitadas en tamaño y periodicidad definidas por políticas que proveen una mejor administración al agotamiento gradual del direccionamiento IPv4. Las fases que comprenden la finalización este protocolo comenzaron en el año 2013 en el manejo de

Fuente: http://stats.labs.lacnic.net/REGISTRO/index-es.html Autor: Lacnic.net

IPV6

El Protocolo de Internet versión 6 (IPv6) fue diseñado en 1990 por Steve Deering de Xerox PARC y Craig Mudge con el fin de reemplazar al Protocolo versión 4 (IPv4) que en la actualidad está implementado a nivel mundial, pero con un límite en la cantidad de direcciones de red.

Estructura de la cabecera IPv6

Según (Amelines Sarria, 2017) la cabecera de Ipv6 consta de los campos siguientes:

o Versión (4bits): Es la versión del IP que es igual a 6.

o Clase de tráfico: Longitud de 8bits, prioridad de paquetes.

o Etiqueta de flujo: Longitud de 20bits, utilizado para el manejo de calidad de servicio (QoS).

o Longitud de la carga útil: 16bits, representa el tamaño del paquete. Gráfico 6 Cabecera de IPv6

Características de las subdivisiones de direcciones IPv6

Local

Útil para redes temporales. Se empleada en un enlace sencillo y no puede ser enrutada. Se utiliza en mecanismos de autoconfiguración, descubrimiento de vecinos y en redes sin ruteadores puede utilizar sin un prefijo global. Sitio Local Dentro de la dirección contiene información de subred. Son enrutadas dentro de un sitio, pero los ruteadores no pueden enviarlas fuera de éste. Se utiliza sin un prefijo global.

Agregable Global

Son direcciones IPv6 empleadas para el tráfico de IPv6 genéricos en el internet de IPv6, son equivalentes a las direcciones unicast utilizadas para comunicarse a través del internet de IPv4. Su estructura admite una incorporación estricta de prefijos de enrutamiento para limitar el tamaño de la tabla de enrutamiento global de internet.

Loopback Todos los dispositivos tienen una dirección loopback, que es utilizada por el mismo nodo. En IPv6 se representa en el formato comprimido ::1.

Sin- Especificar

Indica la ausencia de una dirección unicast sin ser asignada a una interfaz, usada para propósitos especiales. Es representada en el formato comprimido ::

Compatible con IPv4

Para crear automáticamente túneles IPv4 es utilizada por los mecanismos de transición en computadores y ruteadores, de esta forma se entregan paquetes IPv6 sobre redes IPv4.

Asignada Multicast

Está definida y reservada por el REC 2373 para la operación del protocolo IPv6.

Nodo Solicitado

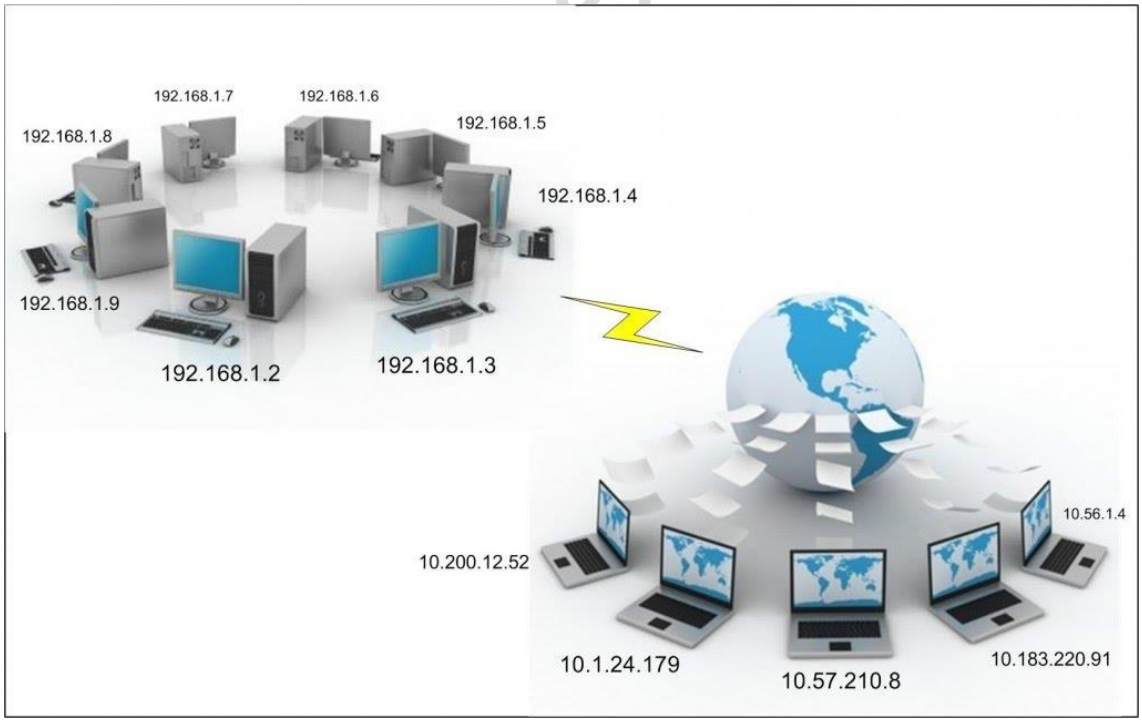
Multicast

Es un tipo de direcciones a la que se le debe unir cada nodo por cada dirección unicast y anycast

Uno de los principales parámetros que es necesario configurar en cualquier dispositivo conectado a una red es su **dirección IP**. La dirección IP es el identificador del dispositivo dentro de una red y debe ser único dentro de los límites de dicha red. El uso, formato, tipos y demás características del direccionamiento IP están incluidos en lo que se conoce como **protocolo IP** (*Internet Protocol*).

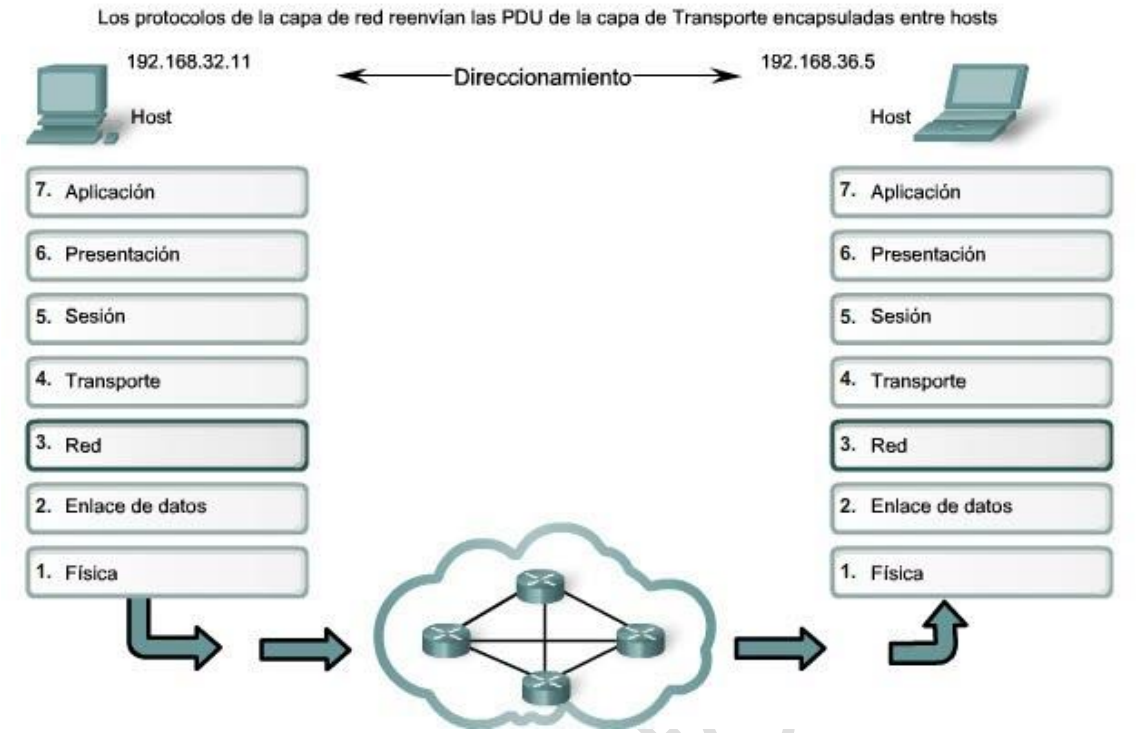
El direccionamiento IP proporciona un mecanismo para la asignación de identificadores a cada dispositivo conectado a una red. Antes de dar información más técnica, exponemos los principales conceptos:

- Todos los dispositivos conectados a una red que utilice los protocolos TCP/IP (en la práctica todas las redes lo hacen) DEBEN tener una dirección IP asignada.
- Una dirección IP es un NÚMERO, que sirve para identificar de forma única a un dispositivo dentro de la red.
- La ASIGNACIÓN de la dirección IP a un dispositivo se puede hacer de dos formas:
    - Estática. En este caso, alguien (yo, mi amigo informático, el administrador de la red, etc) debe configurar manualmente todos los parámetros de red, incluyendo la dirección IP.
    - Dinámica. En este caso, en la red donde se conecta el dispositivo debe haber un equipo que se encargue de asignar de forma automática (sin nuestra intervención) una dirección IP válida.
- En cuanto a su alcance podemos distinguir dos tipos de direcciones:
    - Direcciones públicas. Son las direcciones asignadas a dispositivos conectados a Internet y cuya dirección IP debe ser única para toda la Red. Hay organismos que se encargan de gestionar dichas asignaciones.
    - Direcciones privadas. Son direcciones asignadas a dispositivos dentro de una red que no tiene "visibilidad" con Internet. Los dispositivos que tienen asignada una dirección privada no pueden acceder a Internet con su dirección y necesitan un dispositivo que les "preste" una dirección pública.



- PROTOCOLOS DE COMUNICACIÓN DE CAPAS INFERIORES. CONCEPTOS.

Introducción



La capa de red, o Capa 3 de OSI, provee servicios para intercambiar secciones de datos individuales a través de la red entre dispositivos finales identificados. Para realizar este transporte de extremo a extremo la Capa 3 utiliza cuatro procesos básicos:

- Direccionamiento
- Encapsulación
- Enrutamiento
- Desencapsulación

Direccionamiento

Primero, la capa de red debe proporcionar un mecanismo para direccionar estos dispositivos finales. Si las secciones individuales de datos deben dirigirse a un dispositivo final, este dispositivo debe tener una dirección única. En una red IPv4, cuando se agrega esta dirección a un dispositivo, al dispositivo se lo denomina host.

Encapsulación

Segundo, la capa de red debe proporcionar encapsulación. Los dispositivos no deben ser identificados sólo con una dirección; las secciones individuales, las PDU de la capa de red, deben, además, contener estas direcciones. Durante el proceso de encapsulación, la Capa 3 recibe la PDU de la Capa 4 y agrega un encabezado o etiqueta de Capa 3 para

crear la PDU de la Capa 3. Cuando nos referimos a la capa de red, denominamos paquete a esta PDU. Cuando se crea un paquete, el encabezado debe contener, entre otra información, la dirección del host hacia el cual se lo está enviando. A esta dirección se la conoce como dirección de destino. El encabezado de la Capa 3 también contiene la dirección del host de origen. A esta dirección se la denomina dirección de origen.

Después de que la capa de red completa el proceso de encapsulación, el paquete se envía a la capa de enlace de datos a fin de prepararse para el transporte a través de los medios.

Enrutamiento

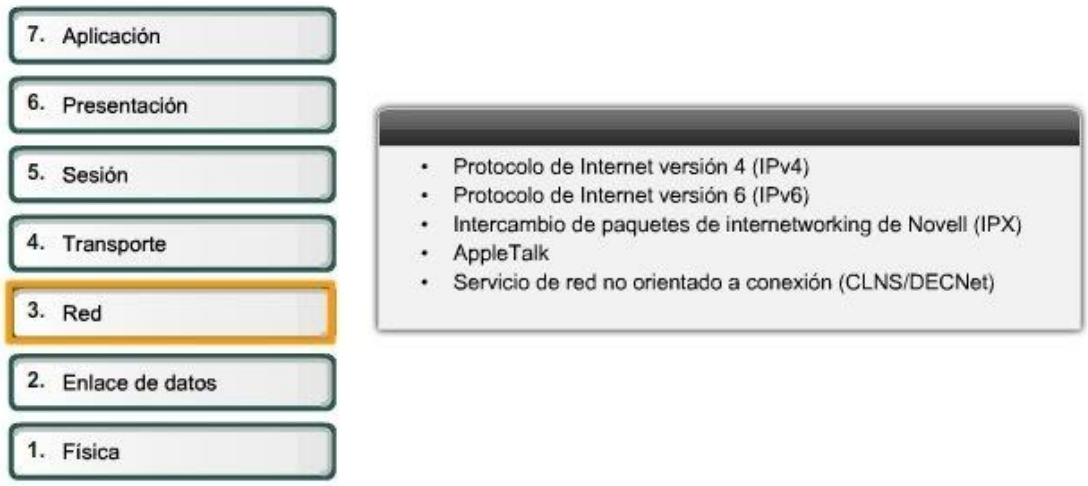
Luego, la capa de red debe proporcionar los servicios para dirigir estos paquetes a su host de destino. Los host de origen y destino no siempre están conectados a la misma red. En realidad, el paquete podría recorrer muchas redes diferentes. A lo largo de la ruta, cada paquete debe ser guiado a través de la red para que llegue a su destino final. Los dispositivos intermediarios que conectan las redes son los routers. La función del router es seleccionar las rutas y dirigir paquetes hacia su destino. Este proceso se conoce como enrutamiento.

Durante el enrutamiento a través de una internetwork, el paquete puede recorrer muchos dispositivos intermediarios. A cada ruta que toma un paquete para llegar al próximo dispositivo se la llama salto. A medida que se reenvía el paquete, su contenido (la unidad de datos del protocolo [PDU] de la capa de transporte) permanece intacto hasta que llega al host de destino.

Desencapsulación

Finalmente, el paquete llega al host de destino y es procesado en la Capa 3. El host examina la dirección de destino para verificar que el paquete fue direccionado a este dispositivo. Si la dirección es correcta, el paquete es desencapsulado por la capa de red y la PDU de la Capa 4 contenida en el paquete pasa hasta el servicio adecuado en la capa de Transporte.

Protocolos de la capa de red



- ESTÁNDARES DE COLORES TIA/568A.

Norma 658A

En un cable cruzado lo que hacemos es cambiar el orden de los dos pares que transmiten los datos. El cable cruzado se usa para: Conectar un ordenador con otro, que actúa como servidor, sin necesidad de un concentrador. Conectar dos estaciones de trabajo aisladas. Conectar concentradores entre sí. O bien si queremos conectar dos concentradores directamente, utilizando cualquier otro puerto.

¿Cuál es el propósito de la norma EIA/TIA 568A?

El estándar de cableado estructurado TIA / EIA definen la forma de diseñar, construir y administrar
un sistema de cableado que es estructurado, lo que significa que el sistema está diseñado en bloques
que tienen características de rendimiento muy específicos. Los bloques se integran de una manera
jerárquica para crear un sistema de comunicación unificado. Por ejemplo, el grupo de trabajo LAN
representan un bloque con los requerimientos de menor rendimiento que el bloque de red

troncal,
que requiere un cable de alto rendimiento de fibra óptica en la mayoría de los casos.

El alcance según la norma EIA/TIA 568A

La norma EIA/TIA 568A específica los requerimientos mínimos para el cableado de establecimientos comerciales de oficinas. Se hacen recomendaciones para:

- La topología
- La distancia máxima de los cables
- El rendimiento de los componentes

La toma y los conectores de telecomunicaciones

Se pretende que el cableado de telecomunicaciones especificado soporte varios tipos de edificios y aplicaciones de usuario. Se asume que los edificios tienen las siguientes características:

- Una distancia entre ellos de hasta 3 km
- Un espacio de oficinas de hasta 1, 000,000 m2
- Una población de hasta 50,000 usuarios individuales

Las aplicaciones que emplean los sistemas de cableado de telecomunicaciones incluyen, pero no están limitadas a:

- Voz
- Datos
- Texto
- Vídeo
- Imágenes

La vida útil de los sistemas de cableado de telecomunicaciones especificados por esta norma debe ser mayor de 10 años.

- ESTÁNDARES DE COLORES TIA/568B.

NORMA EIA/TIA 568B

Esta surge de la revisión de la EIA/TIA 568A. La TIA/EIA-568-B intenta definir estándares que permitirán el diseño e implementación de sistemas de cableado estructurado para edificios comerciales y entre edificios en entornos de campus.

Esta norma se subdivida en:

• ANSI/TIA/EIA-568-B1: Cableado genérico de Telecomunicaciones en Edificios Comerciales. (Requisitos y recomendaciones en estructura, configuración, interfaces, instalación, parámetros de desempeño y verificación)

• TIA/EIA 568-B2: Requerimientos generales para componentes de par tranzado balanceados

• TIA/EIA 568-B3: Componentes de cableado, Fibra óptica (cable, conectores, hardware de conexión, cordones, jumpers y equipo de prueba)

Norma de Colores 568A y 568B

ANSI/EIA/TIA-568A y 568B

La Asociación de la Industria de las Telecomunicaciones **(TIA)** y la Asociación de Industrias de Electrónica (EIA), son asociaciones industriales que desarrollan y publican una serie de estándares sobre el cableado estructurado para voy y datos para las **LAN**.

La norma **TIA 568A y 568B,** especifica un sistema de cableado de telecomunicaciones genérico para edificios comerciales que soportará un ambiente multiproducto y multifrabricante.

Estas normas son un estándar a la hora de hacer las conexiones. Los dos extremos del cable **(UTP CATEGORÍA 5, 6)** que llevarán conectores **RJ45** con un cierto orden de colores especificado por la norma.

El estándar también define los tipos de cables, las distancias, los conectores, las terminaciones de cables, sus rendimientos, los requisitos de instalación de cable y los métodos de pruebas de los cables instalados.

568-A Norma que Regula Los Sistemas de Cableado Estructurado

En resumen el propósito de la norma EIA/TIA 568¬A se describe en el documento de la siguiente forma:

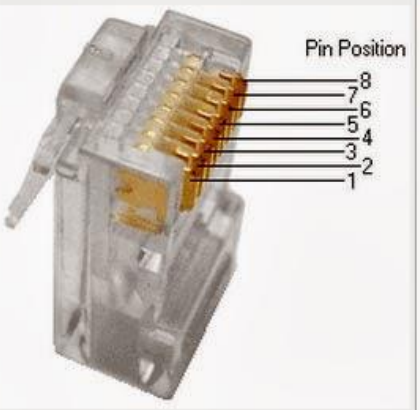
Esta norma especifica un sistema de cableado de telecomunicaciones genérico para edificios, la norma recomienda la instalación de sistemas de cableado durante la construcción o renovación de edificios pues es significativamente menos costosa que cuando el edificio está ocupado.

Código de Colores para Conectores RJ45

Las normas T568A y T568B, dictan como se deben armar los conectores RJ45, estas dos normas se diferencian por el orden de los colores de los pares a seguir. Si bien el uso de la norma T568B para cableado recto es mas utilizada, también en algunos casos se usa la

norma T568A, es por ello necesario conocer el código de colores que rigen ambas normas, la siguiente figura muestra el orden de los colores según los pines de un conector RJ45.

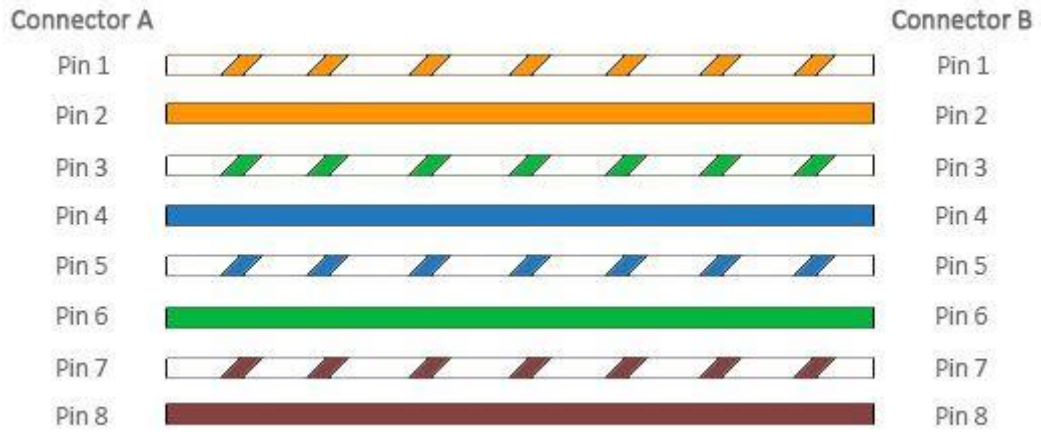
Conexión RJ45 Normas T568A y T568B

Pin	Cable	Color, T568A	Color, T568B	RJ45 pines
1	positivo	blanco/verde rayado	blanco/naranja rayado	
2	negativo	verde entero	naranja entero	
3	positivo	blanco/naranja rayado	blanco/verde rayado	
4	negativo	azul entero	azul entero	
5	positivo	blanco/azul rayado	blanco/azul rayado	
6	negativo	naranja entero	verde entero	
7	positivo	blanco/marrón rayado	blanco/marrón rayado	
8	negativo	marrón entero	marrón entero	

• TIPOS DE CABLES: DIRECTO, CRUZADO.

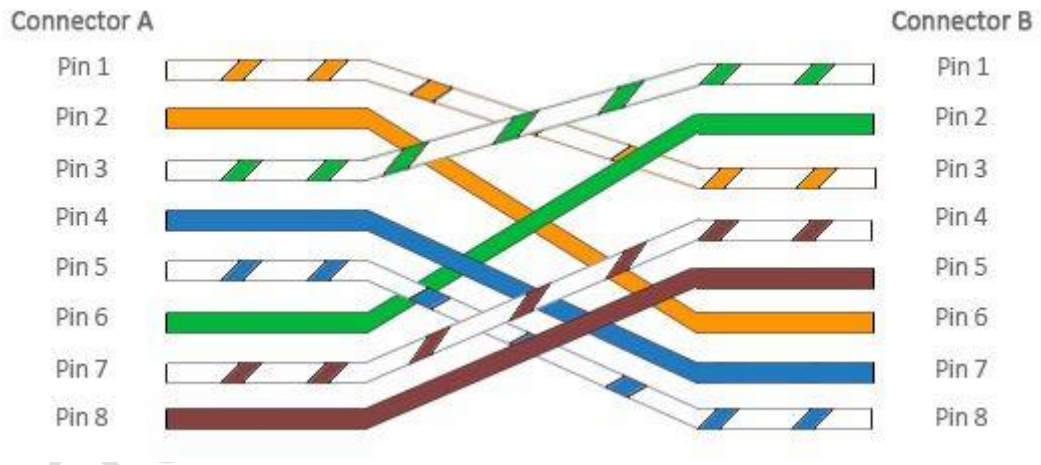
¿ Qué es el cable directo ?

Los colores de un cable de red directo no cambian su dirección. Ambos extremos utilizan el mismo estándar de cableado (T-586-A o T-568-B). Así, el Pin 1 del conector A se dirige al Pin 1 del conector B, el Pin 2 al Pin 2. Estos cables **se utilizan para conectar ordenadores a switches, hubs o routers**.



¿ Qué es el cable cruzado ?

Los colores de un cable de red cruzado cambian su dirección de un extremo a otro. Este cable utiliza diferentes estándares de cableado en cada uno de sus extremos. En una punta se utiliza el estándar T-568-A y en la otra el estándar T-568-B. Ambos conectores tendrán una disposición de cable de colores diferente. Los cable cruzados **se utilizan para conectar dispositivos del mismo tipo**, por ejemplo, dos ordenadores, dos routers o dos switches.



¿ Cuando usar cada tipo de cable ?

En general, un cable cruzado se usa para conectar dos dispositivos del mismo tipo, como por ejemplo un PC a otro PC o un switch a otro switch. Y el cable directo conecta dos dispositivos diferentes entre sí, como por ejemplo un PC a un switch. Vamos a ver diferentes configuraciones:

PC a PC

Los PCs utilizan dos canales, uno de transmisión (TX) y otro de recepción (RX). Si tenemos dos ordenadores conectados entre sí intentando transmitir por el canal TX, sus

señales chocarían y no se conseguiría ninguna transmisión en el canal RX. Por ello, **necesitamos un cable cruzado** para la conexión de dos equipos del mismo tipo. Dado que este tipo de cable se cruza, los datos enviados por el cable TX del PC 1 se recibirá por el cable RX del PC 2.

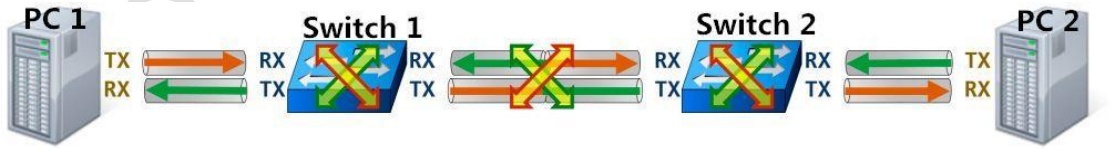
PC a PC a través de switch

Los switches están diseñados para realizar el cruce de transmisiones internamente. El PC 1 envía sus datos a través del cable TX y el switch los recibe por su canal RX; este los transmite por su canal TX al PC 2 que los recibe por su cable RX. El mismo proceso sucede de igual forma en la dirección opuesta, del PC 2 al PC 1. En este caso, **necesitamos un cable directo** ya que es el switch el que se encarga de cruzar los canales.

PC a switch y de switch a PC

Los dos switch cruzarían el cable por separado, originando así la transmisión cruzada entre los switches. Como hemos dicho anteriormente, dos dispositivos iguales necesitan un cable cruzado para realizar la conexión. Por lo tanto, para este caso necesitamos:

- Cuando el PC 1 se conecta al Switch 1, **necesitamos un cable directo**.
- Cuando el Switch 1 se conecta al Switch2, **necesitamos un cable cruzado**.
- Cuando el Switch 2 se conecta al PC 2, **necesitamos un cable directo**.



• TRANSPUESTO.

Configuración de pines del cable transpuesto

El patrón en el que los cables de color de un cable de red codificado están fijados a un conector se llama "Configuración de pines". Los hilos de un cable de red transpuesto están fijados a los conectores del cable en un patrón que es el opuesto en cada extremo del mismo. Esto significa que la secuencia de los cables en un conector se refleja (invertidos) en el otro conector.

Significado de la configuración de pines del transpuesto

Tener los cables que están conectados en una secuencia de espejo permite la comunicación entre los puertos idénticos sin necesidad de conmutación interna.

Uso del cable transpuesto

Un cable transpuesto es más comúnmente utilizado para la conexión de un equipo al puerto de consola del enrutador. Esto se hace generalmente mediante la conexión del conector RJ45 del cable transpuesto al enrutador y conectando el otro extremo a un DB9 o DB25. Este adaptador es compatible con el puerto COM de una computadora.

- LOS CONCEPTOS DE PROTOCOLOS, NORMAS Y ESTÁNDARES QUE REGULAN LAS CONEXIONES A INTERNET:

• DEFINICIONES.

La **interconexión de sistemas** o redes de computadoras son la base de las comunicaciones hoy en día y están diseñadas bajo múltiples **protocolos de comunicación**. Por ejemplo, existen muchos protocolos al establecer una conexión a internet y según el tipo que se necesite establecer, dichos protocolos van a variar. Además, la **comunicación** a internet no es el único tipo de **comunicación** cuando hablamos de **transmisión de datos** e intercambio de mensajes en redes. En todos los casos, los protocolos de red definen las características de la conexión.

Un protocolo es un conjunto de reglas: los **protocolos de red** son estándares y políticas formales, conformados por restricciones, procedimientos y formatos que definen el intercambio de **paquetes** de información para lograr la comunicación entre dos **servidores** o más dispositivos a través de una red.

Los **protocolos de red** incluyen mecanismos para que los dispositivos se identifiquen y establezcan conexiones entre sí, así como reglas de formato que especifican cómo se forman los **paquetes** y los datos en los mensajes enviados y recibidos. Algunos

protocolos admiten el reconocimiento de mensajes y la compresión de datos diseñados para una comunicación de red confiable de alto rendimiento.

Tipos de protocolos de red

Los protocolos para la **transmisión de datos** en internet más importantes son TCP (Protocolo de Control de Transmisión) e IP (**Protocolo de Internet)**. De manera conjunta (TCP/IP) podemos enlazar los dispositivos que acceden a la red, algunos otros **protocolos de comunicación** asociados a internet son POP, SMTP y HTTP.

Estos los utilizamos prácticamente todos los días, aunque la mayoría de los usuarios no lo sepan ni conozcan su funcionamiento. Estos protocolos permiten la **transmisión de datos** desde nuestros dispositivos para navegar a través de los sitios, enviar correos electrónicos, escuchar música online, etc.

Existen varios tipos de protocolos de red:

- Protocolos de comunicación de red: protocolos de comunicación de **paquetes** básicos como TCP / IP y HTTP.
- Protocolos de seguridad de red: implementan la seguridad en las comunicaciones de red entre **servidores**, incluye HTTPS, SSL y SFTP.
- Protocolos de gestión de red: proporcionan mantenimiento y gobierno de red, incluyen SNMP e ICMP.

Un grupo de protocolos de red que trabajan juntos en los niveles superior e inferior comúnmente se les denomina FAMILIA DE PROTOCOLOS.

El modelo OSI (Open System Interconnection) organiza conceptualmente a las familias de protocolos de red en **capas de red** específicas. Este Sistema de Interconexión Abierto tiene por objetivo establecer un contexto en el cual basar las arquitecturas de comunicación entre diferentes sistemas.

A continuación listamos algunos de los protocolos de red más conocidos, según las capas del modelo OSI:

Protocolos de la capa 1 - Capa física

- USB: Universal Serial Bus
- Ethernet: Ethernet physical layer
- DSL: Digital subscriber line
- Etherloop: Combinación de Ethernet and DSL
- Infrared: Infrared radiation
- Frame Relay

- SDH: Jerarquía digital síncrona
- SONET: Red óptica sincronizada

Protocolos de la capa 2 - Enlace de datos

- DCAP: Protocolo de acceso del cliente de la conmutación de la transmisión de datos
- FDDI: Interfaz de distribución de datos en fibra
- HDLC: Control de enlace de datos de alto nivel
- LAPD: Protocolo de acceso de enlace para los canales
- PPP: Protocolo punto a punto
- STP (Spanning Tree Protocol): protocolo del árbol esparcido
- VTP VLAN: trunking virtual protocol para LAN virtual
- MPLS: Conmutación multiprotocolo de la etiqueta

Protocolos de la capa 3 - Red

- ARP: Protocolo de resolución de direcciones
- BGP: Protocolo de frontera de entrada
- ICMP: Protocolo de mensaje de control de Internet
- IPv4: Protocolo de internet versión 4
- IPv6: Protocolo de internet versión 6
- IPX: Red interna del intercambio del paquete
- OSPF: Abrir la trayectoria más corta primero
- RARP: Protocolo de resolución de direcciones inverso

Protocolos de la capa 4 - Transporte

- IL: Convertido originalmente como capa de transporte para 9P
- SPX: Intercambio ordenado del paquete
- SCTP: Protocolo de la transmisión del control de la corriente
- TCP: Protocolo del control de la transmisión

- UDP: Protocolo de datagramas de usuario
- iSCSI: Interfaz de sistema de computadora pequeña de Internet iSCSI
- DCCP: Protocolo de control de congestión de datagramas

Protocolos de la capa 5 - Sesión

- NFS: Red de sistema de archivos
- SMB: Bloque del mensaje del **servidor**
- RPC: Llamada a procedimiento remoto
- SDP: Protocolo directo de sockets
- SMB: Bloque de mensajes del servidor
- SMPP: Mensaje corto punto a punto

Protocolos de la capa 6- Presentación

- TLS: Seguridad de la capa de transporte
- SSL: Capa de conexión segura
- XDR: Extenal data representation
- MIME: Multipurpose Internet Mail Extensions

Protocolos de la capa 7 - Aplicación

- DHCP: Protocolo de configuración dinámica de host
- DNS: Domain Name System
- HTTP: Protocolo de transferencia de hipertexto
- HTTPS: Protocolo de transferencia de hipertexto seguro
- POP3: Protocolo de oficina de correo
- SMTP: protocolo de transferencia simple de correo
- Telnet: Protocolo de telecomunicaciones de red

• TIPOS DE MEDIO DE COBRE:

Los medios de red o medios de transmisión constituyen el soporte físico a través del cual los dispositivos pueden comunicarse en una red de datos. Podemos distinguir dos tipos

de medios: guiados y no guiados. En cualquiera de los dos la transmisión se realiza por medio de ondas electromagnéticas.

Los medios guiados conducen o guían las ondas a través de un camino físico, ejemplos de estos medios son el cable coaxial, la fibra óptica y el cable par trenzado.

Los medios no guiados proporcionan un soporte para que las ondas se transmitan, pero no las dirigen; como ejemplo de ellos tenemos el aire y el vacío.

La naturaleza del medio junto con la de la señal que se transmite a través de él constituyen los factores determinantes de las características y la calidad de la transmisión.

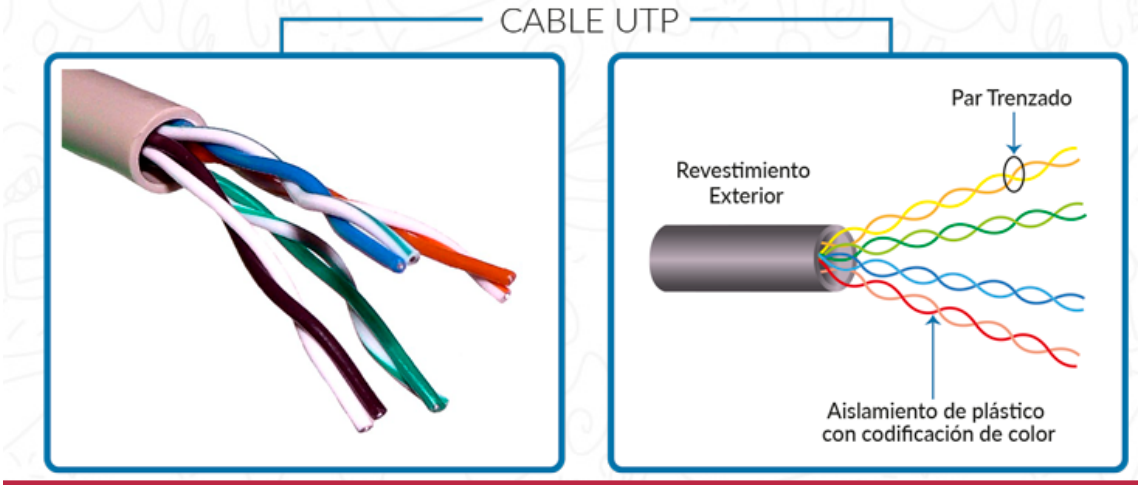
Actualmente son los medios más utilizados en las redes de datos debido a que son económicos y fáciles de instalar y tienen una baja resistencia a la corriente eléctrica. Los datos que viajan por los medios de cobre son transmitidos como pulsos eléctricos. Sin embargo tienen como desventaja que se ven limitados por la distancia y la interferencia en las señales.

Actualmente los medios de cobre más utilizados en las redes de datos son: Cable de par trenzado no blindado (UTPCable de par trenzado no blindado.), Cable Par trenzado blindado, y cable coaxial.

CABLES UTP, CABLES STP.

Es el medio más común utilizado en las redes de datos; consta de una funda plástica, que contiene un conjunto de 8 cables de colores trenzados entre sí de a dos en dos.

Los colores de los cables internos según es estándar son: Verde, Blanco – Verde, Azul, Blanco – Azul, Naranja, Blanco – Naranja, Café, y Blanco – Café. Estos colores identifican los pares individuales con sus hilos y sirven de ayuda para la terminación de cables. El cable UTP por lo general se termina con conectores RJ-45 y se utiliza para interconectar hosts de red con dispositivos intermedios de red.

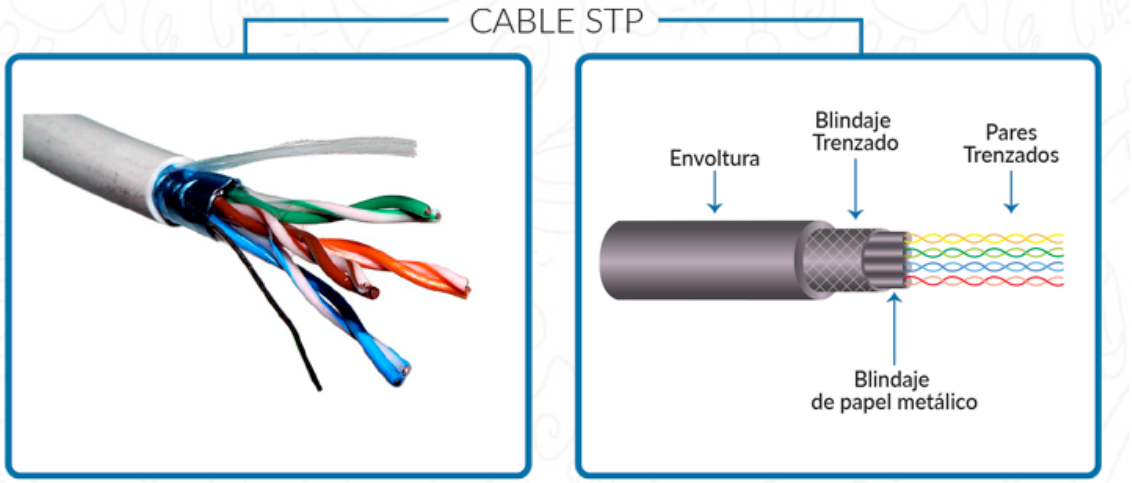


Cable STP

Este cable brinda mayor protección contra interferencias y ruido causado por fuentes eléctricas externas, sin embargo es más costoso y difícil de manipular que el cable UTP.

Dentro de sus características se destaca que utiliza un conector RJ45, posee un revestimiento plástico y un blindaje trenzado que cubren los hilos de cobre, que a su vez están protegidos por un blindaje metálico.

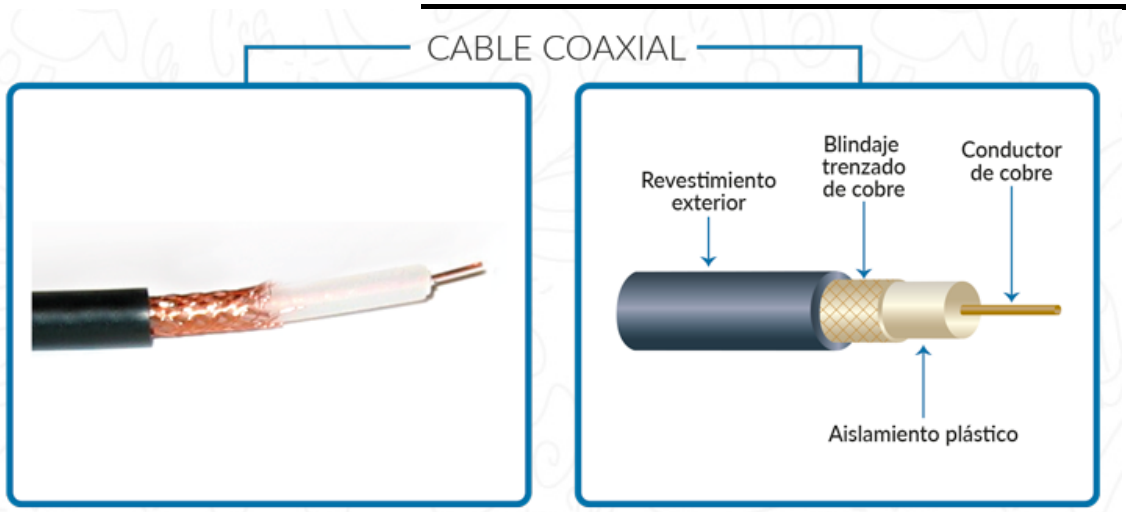
Actualmente este cable está tomando fuerza para las conexiones que funcionan a velocidades de 10GB para Ethernet.



CABLES SCTP, COAXIAL.

Creado en la década de los años 30, es un cable que transporta señales eléctricas de alta frecuencia. Consta de un conductor de cobre central llamado núcleo que se utiliza para trasportar la información, y un conductor exterior de aspecto tubular llamado malla que sirve como blindaje para el núcleo, protegiendo asi las señales de interferencia electromagnética externa.

Actualmente es utilizado en las redes de televisión por cable y para conectar algunas antenas a los dispositivos inalámbricos. Permite el uso de diferentes tipos de conectores como. BNC, Tipo N, y Tipo F.



- ESTÁNDARES DE COLORES DE LOS CABLES DE PAR TRENZADOS.

Estándares

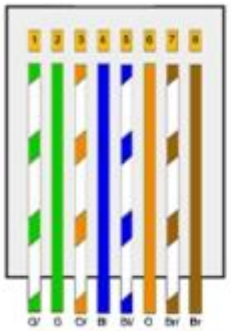
Los estándares de cableado estructurado definen varios tipos de conexiones que se pueden utilizar a la hora de ensamblar el cable de par trenzado con el conector RJ-45, tanto en conectores macho como hembra. De todas ellas, las que más se utilizan son la ANSI/EIA/TIA-568A y ANSI/EIA/TIA- 568B. El instalador debe decidir qué norma resulta más recomendable seguir, sobre todo si ya existe cableado anterior que se quiere reutilizar. Hay que tener en cuenta que no es aconsejable utilizar las dos normas a la vez al realizar el cableado de un edificio, ya que puede dar lugar a problemas de instalación y mantenimiento. La norma ANSI/EIA/TIA-568A se suele utilizar en Estados Unidos, mientas que la norma ANSI/EIA/TIA-568B se usa en Europa.

Según el estándar ANSI/EIA/TIA-568A, la forma de engastar un cable en un conector RJ-45 macho sigue el orden especificado en la siguiente tabla:

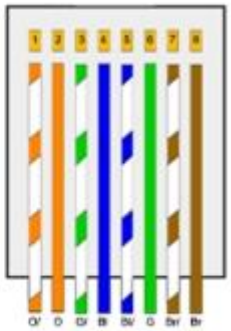
Pin nº	Par nº	Color
1	3	Blanco verde
2	3	Verde
3	2	Blanco naranja
4	1	Azul
5	1	Blanco azul
6	2	Naranja
7	4	Blanco Marrón
8	4	Marrón

Según el estándar **ANSI/EIA/TIA-568B**, la forma de engastar un cable en un conector RJ-45 macho es:

Pin nº	Par nº	Color
1	2	Blanco naranja
2	2	Naranja
3	3	Blanco verde
4	1	Azul
5	1	Blanco azul
6	3	Verde
7	4	Blanco Marrón
8	4	Marrón



568A



568B

- MODELOS DE REFERENCIA, OSI Y TCP/IP Y LOS BENEFICIOS DEL USO DE DICHOS MODELO:

Modelo de capas en una red

El **modelo de capas de una red** surgió como respuesta al problema de que cada fabricante implementaba su propia solución de red y muchas veces era incompatible con el hardware de otros fabricantes.

El modelo de capas es una abstracción de una red en la que segmentamos o dividimos una conexión en capas independientes una de otra para descomponer el sistema en partes

más pequeñas, más fáciles de analizar y de resolver. Cada capa recibe los datos de la capa superior o inferior, los procesa y se los devuelve a la siguiente capa.

Modelo OSI

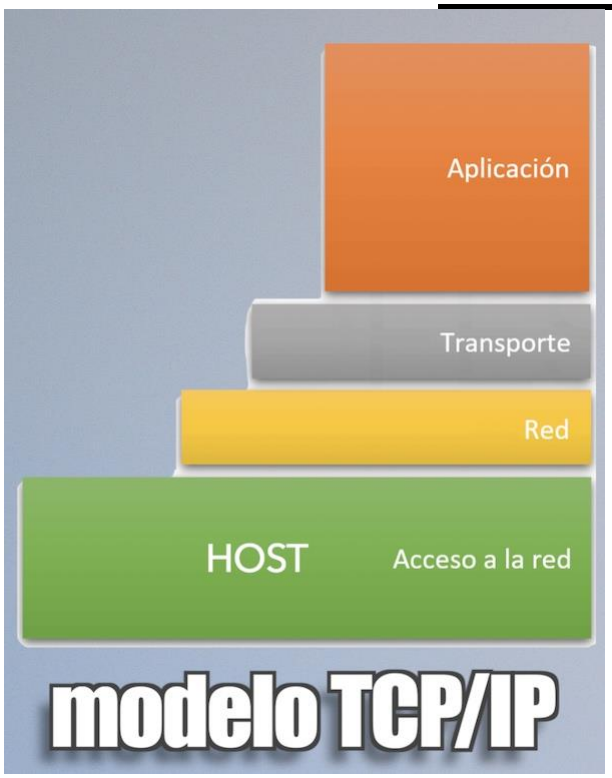
El **modelo OSI consta de 7 capas** o niveles que van desde el más bajo que es la capa fisca del hardware hasta la capa 7 que serían las aplicaciones .

En el video que tienes un poco más abajo tienes descrito el modelo OSI explicando cada una de sus capas con ejemplos sencillos para hacerlo más entendible.

El modelo de capas OSI es el referente, pero a la hora de la verdad utilizamos un modelo con un número menor de capas para hacerlo más sencillo y flexible.

Modelo TCP/IP

Como el modelo de capas OSI no tenía los protocolos bien desarrollados y su implementación era muy cara y complicada surgió el **modelo de capas TCP/IP**.

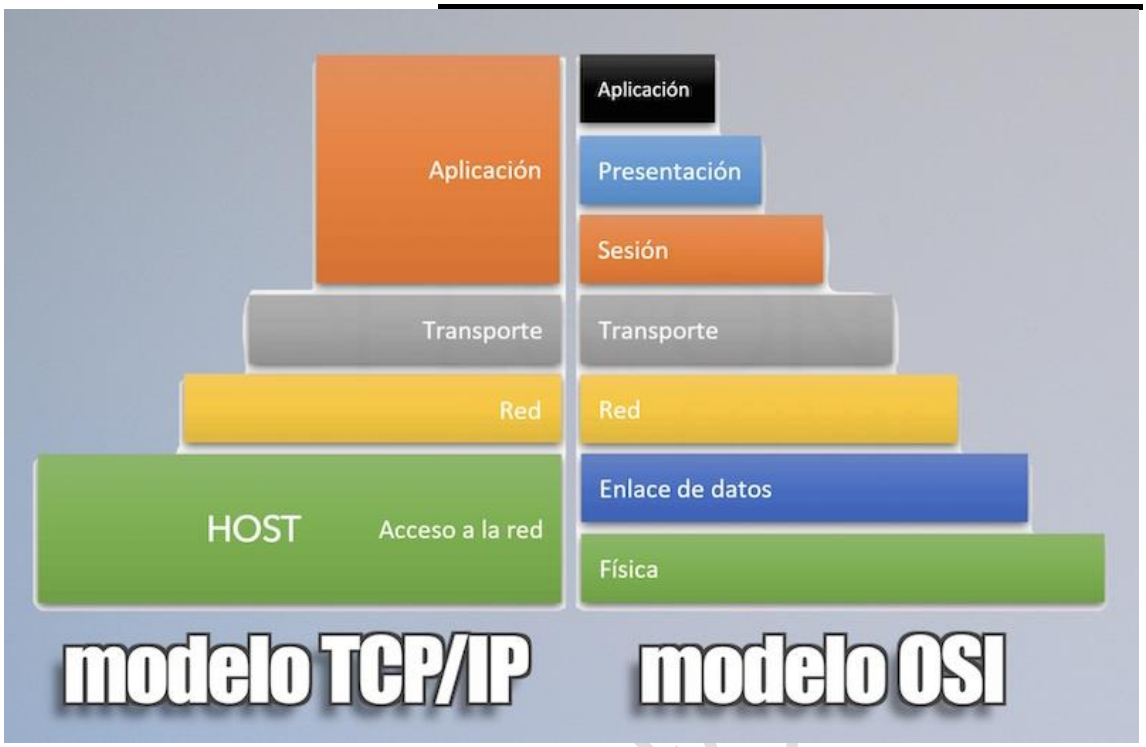


El modelo TCP/IP consta de tan solo 4 capas, agrupamos varias capas del modelo OSI en una sola. La capa 1 y 2 la englobamos en una única **capa llamada "Host"** y la capa 5 y 6 las agrupamos en la capa 7 de aplicación.

Como la capa 2 de enlace se encarga de realizarla el hardware, juntamos la capa 1 y 2 en una sola que llamamos host-red. Esta capa es la encargada de transmitir, recibir y verificar la integridad de los datos.

Las tareas de sesión y presentación las puede realizar las capas inferiores o superiores, por lo que la capa 7 de aplicación es la encargada de realizar las funciones de las 3 capas. Paradójicamente aunque a la capa de aplicación le correspondería el número 4 se le respeta el número de orden del modelo OSI y se le sigue designando como capa 7.

En esta imagen vemos la comparativa entre el modelo TCP/IP frente al OSI.



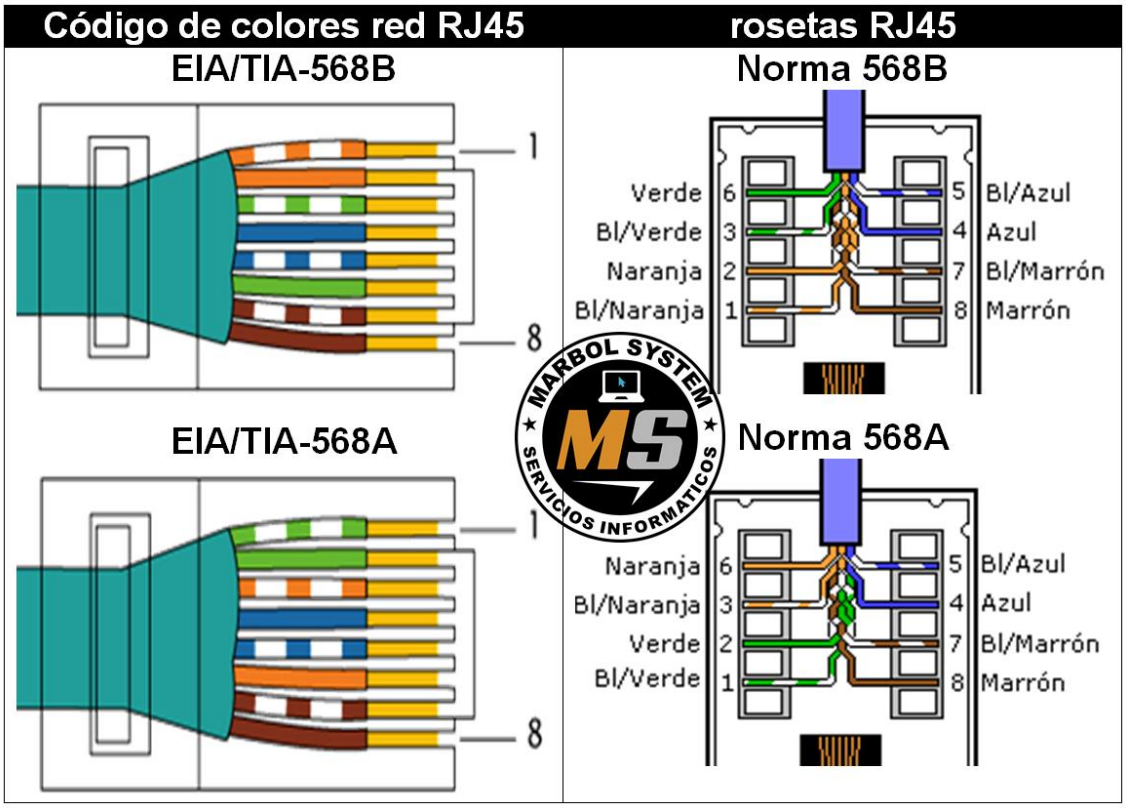
Modelo híbrido

A la hora de la verdad utilizamos un **modelo de capas híbrido** en el que la capa 1 del modelo TCP/IP lo dejamos como estaba en el modelo OSI, con 2 niveles: físco y enlace.

También podríamos verlo como que en el modelo OSI agrupamos las 3 últimas capas en una sola. Es decir, el modelo híbrido podríamos considerarlo como el modelo OSI con 2

capas menos (la 5 y 6) o como el modelo TCP/IP con una capa más (la 1 y 2 separadas). Da igual, es lo mismo, es como ver el vaso medio lleno o medio vacío, el resultado es el mismo.

• IDENTIFICAR LOS ESTÁNDARES DE COLORES TIA/568 A Y B.

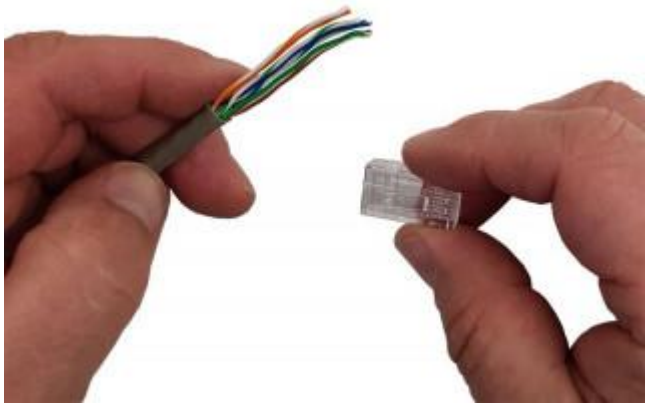


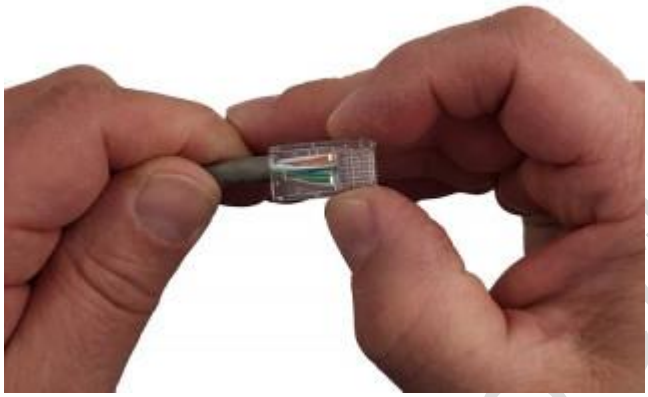
• MANEJAR EL USO DE RJ-45.

¡Usa los enchufes RJ45 para conectarte!

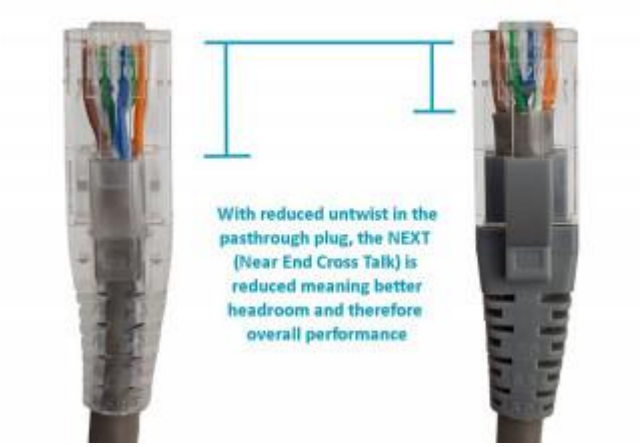
En lo que respecta a sus cables de red, no puede conectarse realmente sin conectores RJ45. El conector RJ45 (Jack-45 registrado para ser precisos...) es el pequeño conector al final del cable que se conecta a su televisor, computadora, enrutador, etc. 8 posiciones de las que consta cada enchufe, cada una separada aproximadamente 1 mm. Luego se insertan cables individuales en estas posiciones. Hay una variedad de conectores disponibles, siendo el más frecuente el moderno conector Ethernet RJ45.

Al mantener los giros lo más cerca posible del punto de terminación, disminuye significativamente la diafonía y aumenta notablemente el rendimiento. Esto, a su vez, mejora la capacidad de margen general del enlace, proporcionando al usuario final el mejor ancho de banda posible.






Wires Can Enter The
Wrong Channel Slot



• HACER LOS DIFERENTES TIPOS DE CABLES SEGÚN EL ESTÁNDAR SOLICITADO.

1. Pelar el cable con cuidado

El primer paso consiste en pelar unos 3 cm. la cubierta de plástico del cable de red en uno de sus extremos. A la hora de hacer esta operación, hay que tener cuidado y no dañar los pares internos del cable

2. Separar los cables y estirarlos

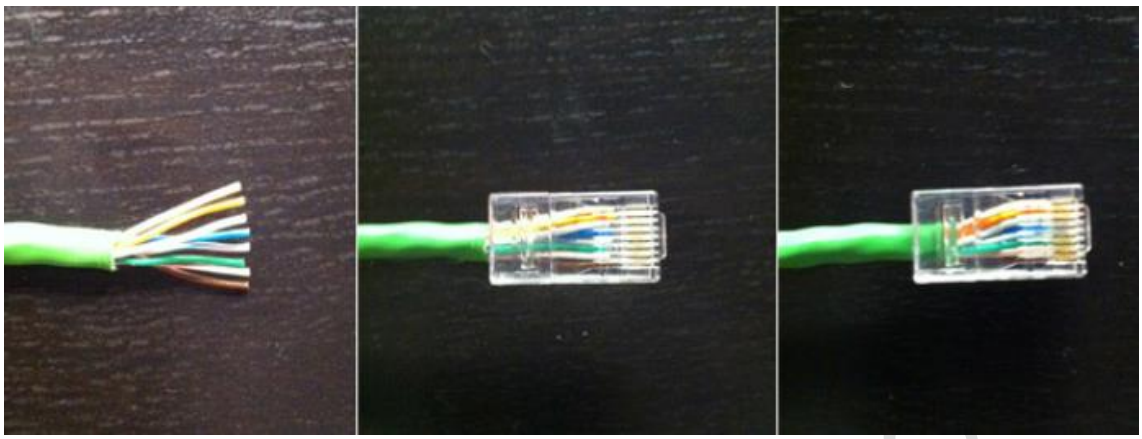
Tenemos que **"destrenzarlos" y estirarlos** lo máximo posible, evitando curvas o ángulos

3. Ordenar los cables

Es importante que los cables queden bien ordenados para que después no haya problemas.

4. Cortarlos e introducirlos con cuidado en la clavija RJ-45

Para introducir los cables en el RJ-45, es importante primero cortar la parte sobrante de los cables. La idea es que sólo nos queden como1.5cm de pares al aire-



5. Fijar con la crimpadora

Introducimos la clavija RJ-45 en el hueco de la crimpadora y **apretamos moderadamente** (no muy flojo pero tampoco sin pasarse). Sonará un pequeño "clic". Eso significa que la clavija RJ-45 ya está fija y bien colocada en su sitio.

6. Repetir con el otro extremo y comprobar

- PDU DE LAS CAPAS.

PDU Significa "Unidad de datos de protocolo". Una PDU es un bloque específico de información transferida a través de un red. A menudo se usa en referencia a la Modelo OSI, ya que describe los diferentes tipos de datos que se transfieren desde cada capa. La PDU para cada capa del modelo OSI se enumera a continuación.

• MANEJO DE DIFERENTES PROTOCOLOS ESTÁNDARES DE LA INDUSTRIA

1. Capa física - cruda los bits (1 o 0) transmitido físicamente a través de hardware
2. Capa de enlace de datos: un marco (o serie de bits)
3. Capa de red - a paquete que contiene la dirección de origen y destino
4. Capa de transporte: un segmento que incluye un TCP encabezado y datra
5. Capa de sesión: los datos pasados a la conexión de red
6. Capa de presentación: los datos formateados para la presentación
7. Capa de aplicación: los datos recibidos o transmitidos por un software solicitud

Los temas de este módulo continúan en la guía 2

- Fuente
- https://nebul4ck.files.wordpress.com/2015/08/ccna-exploration-4-0-c2b7-aspectos-basicos-de-networking.pdf
- https://sites.google.com/site/605bredesdecomputadoras/home/2
- https://humanbranding.com.pe/el-impacto-del-internet-en-la-vida-diaria-ab/
- https://www.angelfire.com/pro/edcanj/Redes.htm
- https://www.cisacad.net/networking-essentials-capitulo-2-las-redes-en-nuestra-vida-cotidiana/
- https://www.ecured.cu/Red_de_%C3%A1rea_local_(LAN)
- https://www.muyinteresante.es/tecnologia/articulo/que-es-una-red-local-y-para-que-sirve-501612389487#:~:text=La%20funci%C3%B3n%20principal%20de%20este,o%20peer%2Dto%2Dpeer.
- https://empresas.blogthinkbig.com/tipos-de-redes-lan-man-wan/#:~:text=Las%20redes%20LAN%20cubren%20%C3%A1reas,las%20redes%20MAN%20y%20WAN.
- https://www.ituser.es/actualidad/2021/12/seis-tendencias-que-marcaran-la-evolucion-de-las-redes-corporativas-en-2022#:~:text=%2D%20Redes%20multicapa%20o%20'multi%2Dlayered%20Networking'.&text=En%202022%20coger%C3%A1%20impulso%20este,de%20conectividad%20remotos%20o%20distribuidos.
- https://sites.google.com/site/investigacionesitlm/3-capas-inferiores-del-modelo-osi-y-tcp-ip/3-1-2-protocolos-de-la-capa-de-red
- https://www.ibm.com/docs/es/i/7.1?topic=pc-configuring-tcpip-windows-operating-systems
- https://manuals.ricoh.com/online/RICOH/wsmhlp/m003/es/rt0402.html
- http://www.ingenieriasystems.com/2016/06/Dispositivos-finales-y-dispositivos-de-red-intermediarios-CCNA1-V5-CISCO-C1.html
- https://www.larepublica.co/empresas/las-aplicaciones-generan-cambios-tanto-en-la-vida-de-las-personas-como-en-las-empresas-2879115
- https://www.iebschool.com/blog/medios-sociales-mas-utilizadas-redes-sociales/
- https://cfp.us.es/e-learning-definicion-y-caracteristicas
- https://rockcontent.com/es/blog/comercio-electronico/
- https://es.acervolima.com/jerarquia-del-proveedor-de-servicios-de-internet-isp/
- https://www.ecured.cu/Capa_de_red
- http://cidecame.uaeh.edu.mx/lcc/mapa/PROYECTO/libro35/211_servicios_y_protocolos_de_la_capa_fsica.html
- https://ccnadesdecero.es/estructura-de-comandos/
- https://ccnadesdecero.es/redes-direccionamiento-ipv4/
- https://docs.oracle.com/cd/E19957-01/820-2981/ipv6-overview-10/index.html#:~:text=Una%20direcci%C3%B3n%20IPv6%20tiene%20un,las%20equis%20representan%20n%C3%BAmeros%20hexadecimales.
- https://sites.google.com/site/redeslocalesyglobales/4-configuracion-de-red/2-configuracion-de-routers/3-configuracion-del-router/1-comandos-basicos-para-la-configuracion-de-un-router/ddf
- https://sites.google.com/site/cursosciscoccna/cisco-3/2-conceptos-basicos-y-configuracion-de-switch/2-3-configuracion-de-la-administracioin-de-switches/2-3-1-navegacion-por-los-modos-del-cli
- https://www.juniper.net/documentation/mx/es/software/junos/cli/topics/topic-map/cli-configuration.html#:~:text=propiedades%20del%20dispositivo.-,Descripci%C3%B3n%20del%20modo%20de%20configuraci%C3%B3n%20de%20CLI,propiedades%20de%20hardware%20del%20sistema.
- https://docs.oracle.com/cd/E19957-01/820-2981/ipplan-5/index.html

- https://docs.oracle.com/cd/E19957-01/820-2981/ipv6-planning-21/index.html
- https://1library.co/article/asignaciones-direccionamiento-ip-an%C3%A1lisis-evoluci%C3%B3n-ipv-basado-experiencias.q2nkl9pq
- https://elcapored.jimdofree.com/normas-568a-568b/
- https://www.gruponst.es/cable-directo-cruzado/#:~:text=En%20general%2C%20un%20cable%20cruzado,un%20PC%20a%20un%20switch.
- https://techlandia.com/utiliza-cable-transpuesto-hechos_506345/
- https://www.kionetworks.com/blog/data-center/protocolos-de-comunicaci%C3%B3n-de-redes
- http://contenidos.sucerman.com/nivel3/redes/unidad2/leccion1.html
- https://sites.google.com/site/redeslocalesyglobales/2-aspectos-fisicos/3-medios-de-transmision/medios-de-transmision-guiados/cable-de-par-trenzado/estandares-y-tipos-de-cable
- https://naseros.com/2021/01/15/modelo-de-capas-osi-y-tcp-ip/
- https://www.dintek.com.tw/es/index.php/Articles/Using-dintek-s-rj45-plugs-to-get-connected.html
- https://www.xatakamovil.com/conectividad/cables-de-red-guia-para-montar-nuestro-propio-cable
- https://techlib.net/definition/pdu.html