

Configuración y gestión de dispositivos activos

Breve descripción:

Este componente formativo aborda aspectos generales y claves del direccionamiento IP y la verificación de dispositivos activos, como parte del proceso de la gestión de redes de datos. Con su estudio responsable de los temas, el aprendiz estará más y mejor capacitado para apropiar saberes en la configuración y gestión de dispositivos activos requeridos, de acuerdo con la arquitectura planteada en la fase de planeación.

Tabla de contenido

Introducción	1
1. Direccionamiento IP.....	3
1.1. Generalidades clave sobre las direcciones IP	4
1.2. Estructura de la dirección IP y clases de direccionamiento IP	6
1.3. Máscara de red y nombre de dominio	9
1.4. ¿Cómo se direcciona desde la máquina?	10
1.5. “Subnetting”	17
1.6. Matemática de red	19
1.7. IPv6.....	23
2. Verificación de dispositivos.....	25
Síntesis	35
Material complementario	36
Glosario	37
Referencias bibliográficas	39
Créditos	40

Introducción

Usted se ha comenzado el estudio del componente formativo “**Configuración y gestión de dispositivos activos**”. Su estudio responsable del mismo, enriquecerá su proceso formativo en **Gestión de redes de datos**. Ahora, diríjase al contenido del video que se propone a continuación, el cual le contextualizará sobre los temas que aquí desarrollarán. ¡Éxitos!

Video 1. Configuración y gestión de dispositivos activos



[Enlace de reproducción del video](#)

Síntesis del video: Configuración y gestión de dispositivos activos

Los sistemas informáticos aumentan su complejidad de acuerdo con la llegada de nuevas tecnologías, como lo es, por ejemplo, la red 5G: lo cual conduce, progresivamente, a la población mundial, a adquirir una cultura de conectividad en las tareas cotidianas.

Es así como adquirir conocimientos básicos sobre esquemas de redes y el direccionamiento IP es de vital importancia al implementar soluciones confiables en ecosistemas de interconexión de dispositivos en redes de datos.

En la actualidad, no solo se contempla la comunicación entre computadores; existen ecosistemas de redes de datos que incluyen dispositivos cableados e inalámbricos, los cuales integran diferentes dispositivos como “smartphones”, “tablets”, sistemas de vigilancia, electrodomésticos, entre otros.

Todos los dispositivos que se interconectan en una red necesitan una dirección IP para compartir información. Mediante una dirección IP se identifica de forma lógica y jerárquica a un dispositivo interconectado en red.

Las temáticas abordadas en este componente formativo, incluyen el estudio del direccionamiento IP que permite una correcta comunicación en ecosistemas de redes de datos que integren las últimas tecnologías.

1. Direccionamiento IP

Las conexiones de redes de datos implementan el protocolo TCP/IP; todos y cada uno de los “hosts”, es decir, cualquier computador o dispositivo conectado en red, conectados a Internet, están compuestos de una dirección IP (en IPv4 o IPv6) y una máscara de red que ayuda a determinar la red a la que pertenecen.

Estas direcciones IP van incrementando o cambiando debido a las nuevas tecnologías de comunicación, como la adaptación del protocolo IPv6.

Sobre los “hosts”, tenga en cuenta aspectos como estos:

- Cualquier “host” conectado a una red requiere, dentro de sus parámetros de comunicación, la configuración de la dirección IP.
- La dirección IP forma parte del protocolo IP (“Internet Protocol”), el cual indica el uso, formato, tipos y demás características del direccionamiento IP.
- La dirección IP corresponde a la identificación del dispositivo internamente en una red.
- Dentro de los límites de una red, la dirección IP debe ser única.

El siguiente video muestra cómo determinar o consultar una dirección IP en un equipo o dispositivo:

Video 2. Direccionamiento IP



[Enlace de reproducción del video](#)

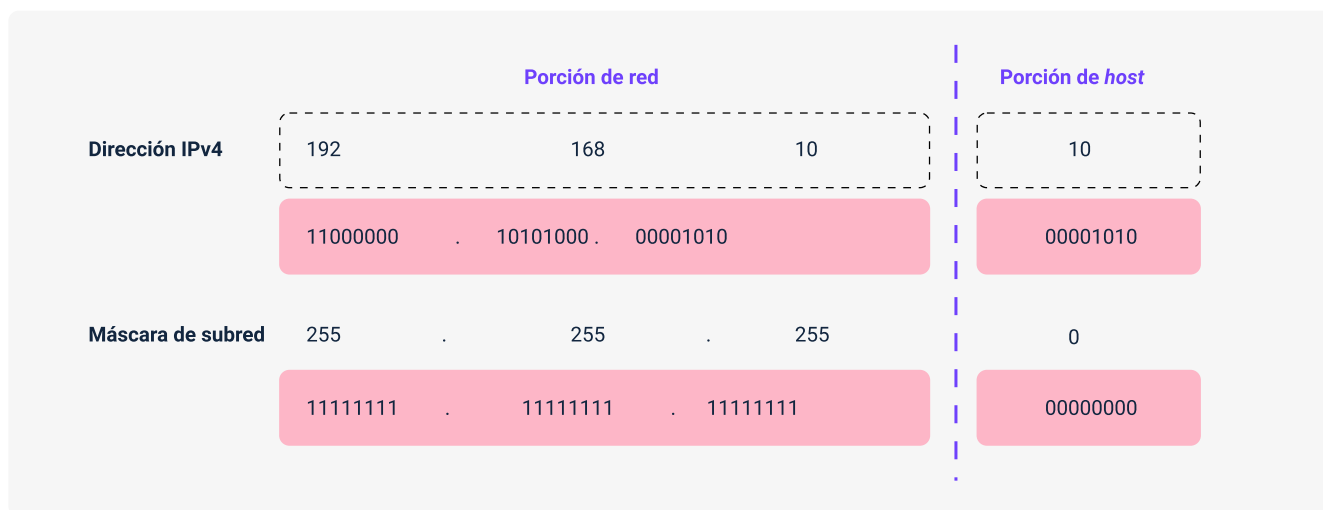
Síntesis del video: Direccionamiento IP

En este video, la instructora SENA ofrece el paso a paso, y otros elementos, sobre la determinación o consulta de la dirección IP en un equipo, provista por proveedores de internet para contar con conexión a la red de datos.

1.1. Generalidades clave sobre las direcciones IP

Las direcciones IP se dividen en dos grandes grupos, **IPv4** e **IPv6**. Estas direcciones son la identificación que cada uno de los “hosts” conectados en red tiene asociada para poder enviar y recibir datos; están compuestas por una porción de red y una porción de “host”.

Figura 1. Dirección IPv4



Comprenda, más y mejor, el concepto de dirección IP, haciendo su propia imagen mental de la siguiente analogía:

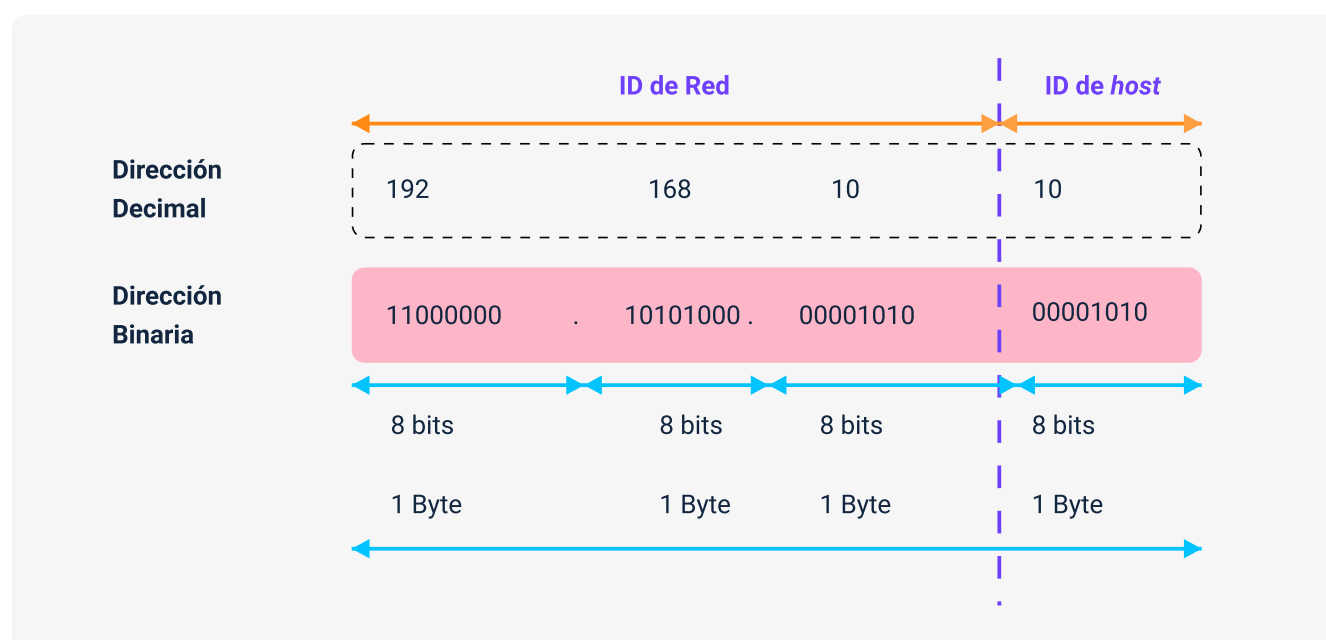
- Piense, por ejemplo, la dirección de una casa, la cual está comprendida por una estructura: Calle 1 con carrera 1 – 01. En esta dirección, se puede analizar que la parte de Calle 1 y Carrera 1 es un grupo en común para aquellas viviendas que coincidan, lo que vendría siendo la porción de red para la dirección IP; en ese mismo sentido, la nomenclatura del 01 (después del guion de la dirección), la cual representa una vivienda en específico de la Calle 1 con carrera 1. De ello se puede hacer analogía con la porción de “host” de la dirección IP.
- La misma dirección puede estar en otra ciudad y ahí es cuando entra en acción el concepto de la máscara de subred, que vendría siendo la ciudad para este ejemplo; por ende, con esa dirección IP (dirección de la casa) y máscara de subred (ciudad) se puede ubicar con facilidad, en un espacio, alguna

empresa de envíos para entregar algún pedido o, en este caso, entregar/recibir datos de información.

1.2. Estructura de la dirección IP y clases de direccionamiento IP

La dirección IP corresponde a una dirección lógica de 32 “bits”, se trata del identificador de la conexión del dispositivo a la red, dicha dirección es única para cada dispositivo conectado a la red, ya que esta se asocia a la dirección de la tarjeta de red.

Figura 2. Identificador de conexión del dispositivo a la red



En la figura se muestra cómo cada grupo está formado por octetos, que corresponden a 8 “bits”; es así que una dirección IPv4 consta de 4 octetos que, en total, son 32 “bits”.

Las clases se definen en el protocolo IP, de manera tal que permitan optimizar el uso del enrutamiento de las unidades de información, denominadas datagramas, ya que, al no usar clases, los enrutadores deberían almacenar un alto flujo de información

en sus tablas de enrutamiento, lo cual no es eficiente para el funcionamiento de las redes de datos.

Para cubrir las necesidades de las diferentes organizaciones, se establecieron varias clases:

Figura 3. Rango de las clases

	Decimal punteado		Binario punteado
Clase A	0.0.0.0	0	0000000. 0000000. 0000000. 0000000
	127.255.255.255	0	1111111. 1111111. 1111111. 1111111
Clase B	128.0.0.0	10	000000. 00000000. 000000. 0000000
	191.255.255.255	10	1111111. 11111111. 1111111. 1111111
Clase C	192.0.0.0	110	0000000. 0000000. 0000000. 0000000
	223.255.255.255	110	1111111. 1111111. 1111111. 1111111
Clase D	224.0.0.0	1110	0000. 00000000. 00000000. 00000000
	239.255.255.255	1110	1111. 11111111. 11111111. 1111111

Las clases de direccionamiento, explicadas con más detalle, se muestran a continuación:

- **Clase A.** Este grupo de direcciones IP es el más grande del protocolo de Internet en su versión 4, donde el primer octeto empieza en 0 y termina en 127, el resto de los octetos están destinados para los “hosts”. Puede haber

un máximo de 128 (2^7) redes clase A. Cada red clase A puede contener un máximo de 16.777.216 (2^{24}) “hosts”.

- **Clase B.** Los octetos que se ocupan para este grupo son los dos primeros, empezando el primer octeto en el rango de 128 al 191 y los dos octetos restantes están disponibles para los “hosts”. La cantidad de redes de la clase B está compuesta por $2^{14} = 16.384$, puede contener un máximo de 65.536 (2^{16}) “hosts”.

Las direcciones IP, que se encargan de identificar los dispositivos conectados a una red en forma única, se pueden clasificar teniendo en cuenta el alcance y su función.

Las siguientes dos tablas, resumen la clasificación de las direcciones IP:

Tabla 1. Clasificación de las direcciones IP según alcance

Públicas	Privadas
Dirección IP visible por los dispositivos conectados a Internet.	Dirección IP visible únicamente por los dispositivos de su propia red.
Son usadas en servicios de web, DNS o correo electrónico.	Pueden ser usadas en diferentes redes internas.

Nota: adaptada de Ariganello (2020).

Tabla 2. Clasificación de las direcciones IP según su función

Públicas	Privadas
Dirección IP asignada a un dispositivo de forma fija y permanente.	Dirección IP asignada aleatoriamente. Para cada conexión a la red, la dirección IP es diferente.
Se usan para los servicios que deben ser alcanzados en forma constante como la web.	Se configuran de forma automática a través de servidores.

Nota: adaptada de Ariganello (2020).

Los servidores de Internet usan las direcciones IP públicas estáticas, con el objeto de que se encuentren siempre localizables por los usuarios que se conectan a Internet. Por otro lado, los “modems” que se conectan a internet usan direcciones IP públicas dinámicas.

1.3. Máscara de red y nombre de dominio

Cuando se conectan dos o más dispositivos mediante un “router”, este debe enrutar los paquetes que van dirigidos a cada dispositivo, es así que la máscara de red corresponde a una dirección IP que efectúa el enrutamiento interno de paquetes.

Para cada clase de red, según su tamaño, se tiene su correspondiente máscara de red:

Figura 4. Máscara de red según las clases

	Decimal punteado	Binario punteado
Clase A	255.0.0.0	11111111. 00000000. 00000000. 00000000
Clase B	255.255.0.0	11111111. 11111111. 00000000. 00000000
Clase C	255.255.255.0	11111111. 11111111. 11111111. 00000000

Como sugiere la figura, la máscara de red permite determinar la dirección de red a la cual pertenece un “host”, ya que indica qué porción de la dirección IP es de red y así mismo cuál porción corresponde a “host”. Realizando una operación denominada AND lógica entre la dirección IP del “host” y la máscara de red, se puede determinar la dirección de red.

Como la estructura de la dirección IP en formato decimal o binario es difícil de recordar, a fin de facilitar el acceso, se optó por asignar un nombre de dominio a cada dirección IP. Un ejemplo es el nombre de dominio asignado a la dirección de Google que es **www.google.com.co**, para no usar su correspondiente dirección IP expresada en forma decimal.

1.4. ¿Cómo se direcciona desde la máquina?

Cuando un “host” se comunica con uno o más “hosts” en la red, envía un conjunto de datos de origen a destino.

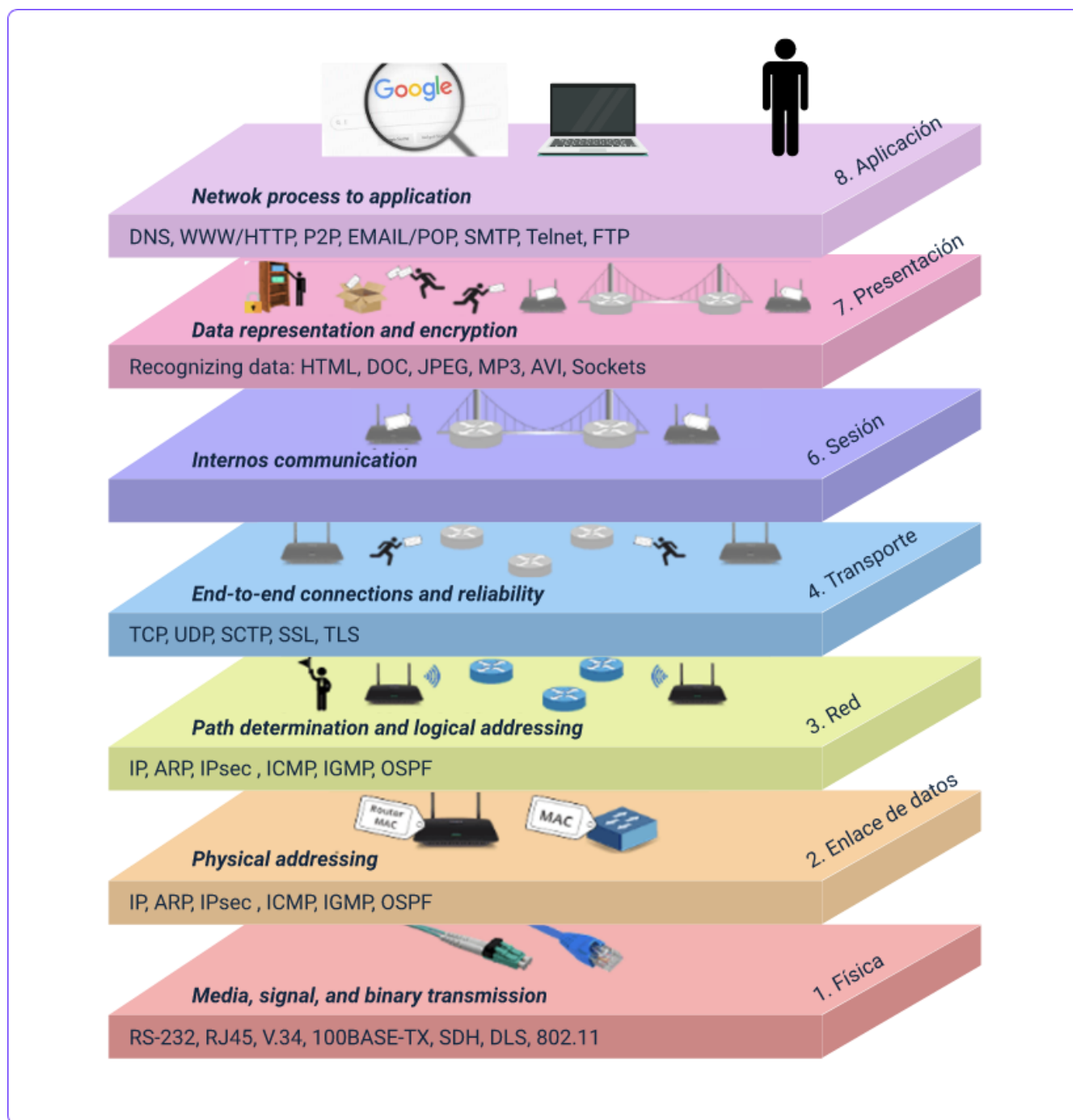
A continuación, se describe lo que sucede con los datos enviados:

- a. **Conversión a formato apropiado.** En la capa de aplicación, los datos son convertidos al formato de red apropiado.
- b. **División en segmentos numerados.** En la capa de transporte, los datos se dividen en segmentos numerados para el reensamblaje adecuado en el “host” destino.
- c. **Nominación del paquete.** En la capa de red, se ingresan las direcciones IP del “host” emisor y el “host” receptor. Por lo tanto, el nombre del paquete hace referencia a la unidad resultante.
- d. **Denominación de tramas.** En la capa de enlace de datos, se agregan las direcciones correspondientes a la MAC de los dos “hosts” y un respectivo número determinado para verificar si hay errores en el envío de la información durante las transmisiones posteriores, pasando a recibir la denominación de tramas.
- e. **Conversión a pulsos eléctricos u ondas.** En la capa física, las tramas se empaquetan mediante un flujo de “bits” adecuado para su conversión a pulsos eléctricos u ondas que se envían a los medios. Cuando los pulsos u ondas llegan al “host” receptor, el proceso se invierte, obteniendo en la capa de aplicación receptora los datos en su formato original.

Aunque son pulsos eléctricos lo que se transmite a través del medio físico, se hace referencia a los paquetes transmitidos porque son unidades de información con entidad propia.

El siguiente, es el modelo de capas OSI:

Figura 5. Modelo de capas OSI



Las siete capas del modelo de capas OSI, son:

- Física

- Enlace de datos
- Red
- Transporte
- Sesión
- Presentación
- Aplicación

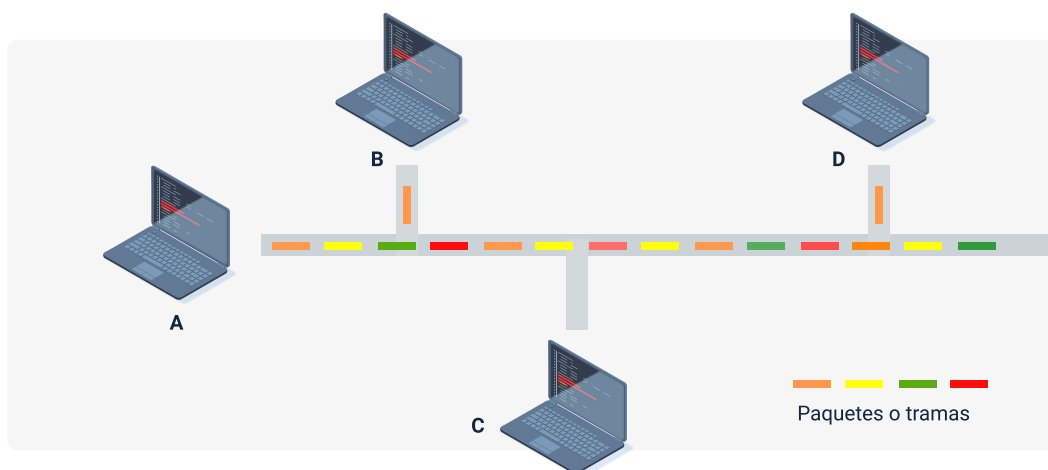
Comunicación entre “hosts” en red

Para establecer la comunicación en red TCP/IP, los dispositivos requieren tres datos sobre el “host” destino, al que se dirige el paquete de datos; estos son:

- Dirección IP.
- Máscara de subred.
- Dirección MAC (“Media Access Control”, Control de Acceso a Medios).

En el siguiente esquema, se muestra una red formada por varios “hosts” en una conexión directa de datos.

Figura 6. Interconexión de “hosts”



En la figura inmediatamente anterior, al “host” identificado como **C** se le configura la dirección IP 198.23.5.14. Este desea comunicarse con el “host” identificado como **D**, al cual se le configura la dirección IP 198.23.5.27. El conjunto de datos de origen a destino se integra en paquetes de datos, y la capa de red asigna las respectivas direcciones IP del “host” **C** (emisor) y del “host” **D** (destino), pasándose a la capa de enlace de datos, que desconoce la MAC (dirección física) del “host” **D**. Para realizar dicha consulta, el “host” **C** envía un mensaje a todas las máquinas interconectadas en red; esta petición es conocida como ARP (Protocolo de Resolución de Direcciones) y es de tipo “broadcast”, que son enviadas como difusión a todos los equipos en la red, consultando por la MAC correspondiente a la IP 198.23.5.27.

Para la petición ARP, solo el “host” **D** responde dicha petición, enviando como respuesta la dirección MAC. Es así que el “host” **C** incluye la dirección MAC de origen y destino a los paquetes ya en la capa física, y esta se encarga de transmitirlos al medio.

Comunicación entre “hosts” en dos redes

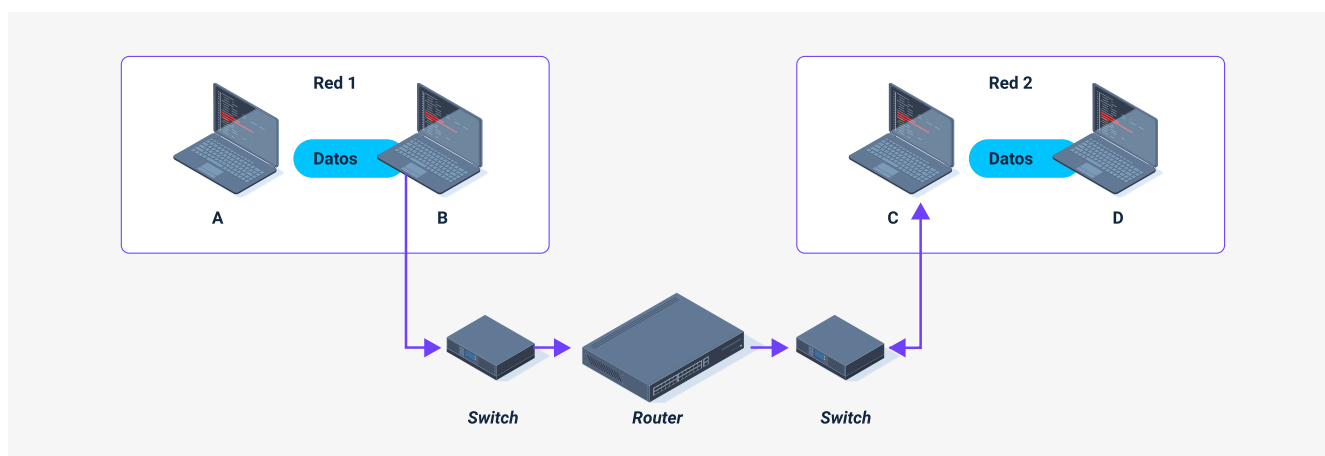
El “host” identificado como **D**, configurado con la dirección IP 190.200.23.5, no se ubica en la misma red que el “host” identificado como **A**, configurado con la dirección IP 200.23.5.14. El “host” **A** envía un mensaje “broadcast” consultando por la dirección MAC de **D**, pero no recibirá una respuesta. Por lo tanto, la comunicación entre ambos “hosts” se vuelve imposible. El dispositivo de red que se encarga de establecer dicha comunicación se conoce como “router”, el cual permite la conexión de dos o más redes, su principal función es enrutar o encaminar paquetes de datos al “host” de redes diferentes.

Cuando un paquete llega al “router”, este examina la dirección del “host” destino y lo envía hacia este, enrutando por una ruta predeterminada. Si la dirección IP destino pertenece a una de las redes que están interconectadas mediante el “router”, se envía el paquete directamente; si llegado el caso, no es así, el “router” envía el paquete al “router” más cercano a la dirección IP destino.

El enrutamiento se realiza a través de las tablas de enrutamiento que se configuran en el “router”, cada segmento de red interconectado en red a través de un “router” tiene su respectiva dirección IP que identifica de forma única el enlace a la red.

La interconexión de redes a través de enrutadores puede ser representada mediante el siguiente esquema:

Figura 7. Interconexión de redes a través de un “router”



Teniendo la conexión establecida entre las dos redes, el “host” emisor envía una petición ARP a fin de consultar la dirección MAC que pertenece a una IP asignada. Si no se tiene respuesta de los “hosts” conectados en su red, este envía los paquetes de datos a través de un “router” configurado para este tipo de envíos. Los paquetes se

envían mediante el “Gateway” (puerta de enlace) por defecto. Para que el “router” determine la dirección IP de la red a la que pertenece el “host” buscado, recurre a la máscara de red, en combinación con la dirección IP destino, realizando una operación conocida como AND binario.

Para esto, el “router” realiza una operación interna, donde se combinan los “bits” de la dirección IP binario y la máscara de red binario. Tal combinación está detallada en la siguiente tabla:

Tabla 3. Operación AND binario

Combinación de “bits”	Resultado	Operación AND
1 1	1	Dirección IP binario “host” 11001000 . 00010111 . 00000101 . 00001110
1 0	0	Máscara de red binario 11111111 . 11111111 . 11111111 . 00000000
0 1	0	Dirección de red binario 11001000 . 00010111 . 00000101 . 00000000
0 0	0	Dirección de red decimal 200. 23. 5. 0

Realizada la operación AND, el “router” envía los paquetes de datos a la correspondiente red 2, a la que pertenece el “host” destino **D**. Luego, envía una petición “broadcast”, a fin de consultar la dirección MAC del “host” destino **D**.

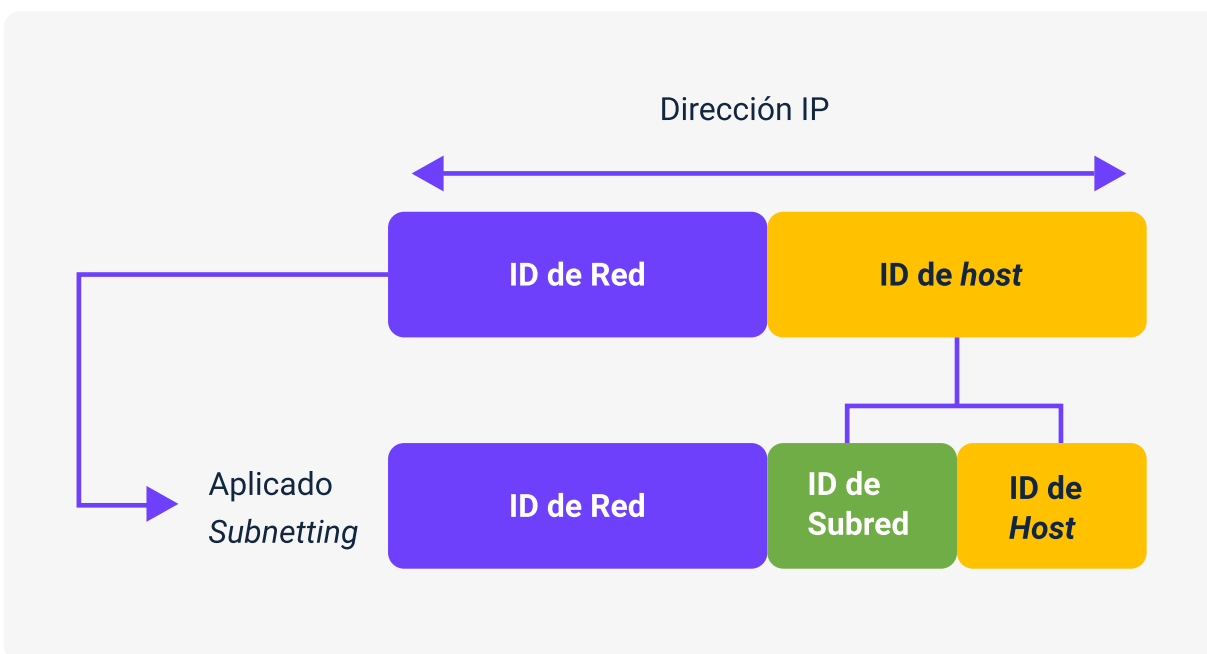
Al obtener la respuesta, el “router” enruta finalmente los paquetes de forma directa. Si se establece una comunicación en sentido contrario, de “host” **A** al “host” **D**, el proceso a realizar por el “router” es el mismo. En el primer proceso realizado, el “router” almacenó en su tabla de enrutamiento las direcciones MAC-IP del “host” **A** y del **D**, las cuales pueden ser usadas para posteriores envíos de datos.

1.5. “Subnetting”

Diseñar, implementar y administrar de forma eficaz el direccionamiento IP permite un uso eficiente de las direcciones IPv4 e IPv6. El “subnetting” consiste en la creación de múltiples redes, partiendo de una dirección IP de red. La estructura de la dirección IPv4 cuenta con dos niveles: ID de red y el ID de “host”. Los enrutadores reenvían paquetes según la porción de red de la dirección IP. Una vez que se encuentra la red, la parte de la dirección del “host” identifica el dispositivo de destino.

A medida que se expande la red y las organizaciones agregan cientos o miles de “hosts” a la red, la jerarquía de dos niveles se vuelve inadecuada. La subdivisión de red, mejor conocida como “subnetting”, agrega mayor cantidad de niveles a la jerarquía de la red, básicamente, creando tres niveles: red, subred y “host”.

Figura 8. Esquema “subnetting”



Como se sugiere en la figura inmediatamente anterior, la introducción de un nivel adicional a la jerarquía crea subgrupos adicionales dentro de una red IP, lo que facilita la entrega rápida de paquetes y proporciona un mayor filtrado, al contribuir a minimizar el tráfico local.

Algunos aspectos que, sobre el “subnetting” se debe tener en cuenta, son:

- Otra forma de realizar “subnetting” es aplicando el mecanismo VLSM (Máscara de subred de longitud variable).
- Así, se obtienen subredes de una longitud variable para las diferentes interfaces de conexión.
- El beneficio al crear diferentes identificadores de máscara de subred, es que se mejora la eficiencia del direccionamiento IP, optimizando recursos de direccionamiento IP, según convenga en el diseño de la red.

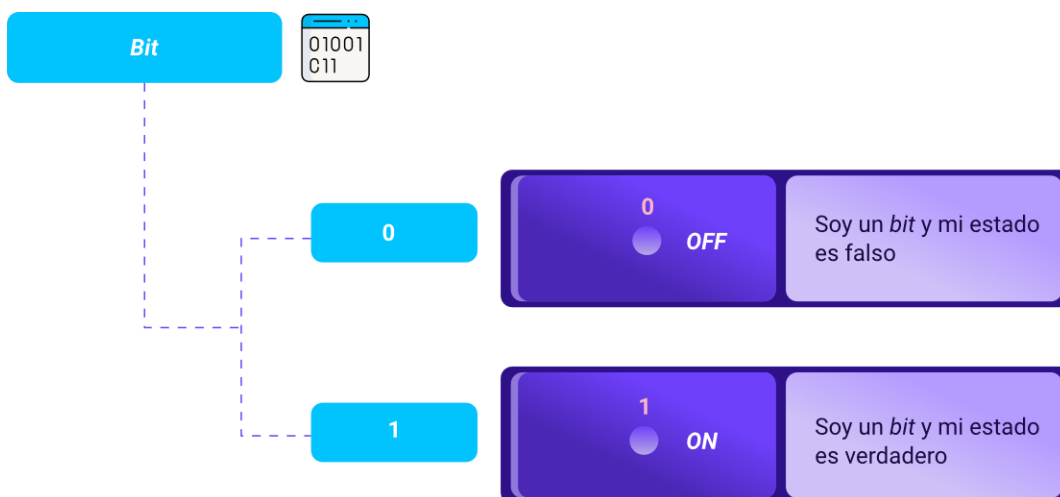
- Las superredes o “supernetting”, por otro lado, permiten a los enrutadores enrutar de manera más eficiente. En otras palabras, pueden manejar más tráfico con menos recursos.
- El enrutador ya no usa las clases para el direccionamiento, sino que envía la máscara de red contiguo a la dirección. Esto permite que los enrutadores realicen la agrupación por subredes.
- Este método, conocido como enrutamiento entre dominios sin capas (CIDR), permite a los enrutadores agrupar y jerarquizar subredes comunes para simplificar el tráfico.

1.6. Matemática de red

Las matemáticas permiten un entendimiento de las propiedades de la red, para acercarse al conocimiento y aplicación en ecosistemas de redes de datos. Para iniciar, se abordan los conceptos iniciales, que son un “bit” y un “byte” de información.

Algunos elementos que deben estar claramente comprendidos, en la matemática de red, son:

Figura 9. Elementos básicos en la matemática de red



- a. **Un “bit”.** Un “bit” está compuesto por los valores 0 y 1. (0 para falso y 1 para verdadero).
- b. **Valor 0.** El 0, indica que no hay comunicación. Cuando un “bit” se encuentra en cero, su estado es falso, apagado.
- c. **Valor 1.** El 1, indica que sí hay comunicación. Cuando un “bit” se encuentra en uno, su estado es verdadero, encendido.

Los computadores trabajan con grupos de 8 “bits”, los cuales se llaman “bytes”. El intervalo de valores de un “byte” está en el rango de 0 a 255. De esta manera, cuando se menciona que una dirección IPv4 está compuesta de 4 octetos, quiere decir que se compone de 4 “bytes”.

Binario a decimal

El sistema binario tiene como base el 2. Por esta razón, es ideal representar cada posición en potencias de 2. Las direcciones IPv4 se estructuran por cuatro “bytes”, punteados tanto en binario o decimal.

Por ejemplo:

Figura 10. Notación de dirección IPv4



En el sistema de numeración base 2, las posiciones en los números binarios de 8 “bits” se presentan así:

Tabla 4. Representación potencias de base 2

Potencia	Equivalencia
2^7	128
2^6	64
2^5	32
2^4	16
2^3	8
2^2	4
2^1	2
2^0	1

El sistema de numeración de base 2 puede ser expresado usando solo dos dígitos: 0 y 1. Al realizar la conversión de binario a decimal, se ubican los 8 “bits” en cada posición, iniciando por el MSB (“bit” más significativo), que equivale a 128, luego se procede a sumar las equivalencias que se encuentren en 1, para obtener el valor del octeto de binario a decimal.

Tabla 5. Equivalencia binaria a decimal

Potencia	Equivalencia	Primer octeto	Operación	Decimal
2^7	128	1	128+64	192
2^6	64	1	128+64	192
2^5	32	0	128+64	192
2^4	16	0	128+64	192
2^3	8	0	128+64	192
2^2	4	0	128+64	192
2^1	2	0	128+64	192
2^0	1	0	128+64	192

Decimal a binario

El sistema binario tiene su correspondiente conversión al sistema decimal. Dado que las direcciones IPv4 se representan mediante el formato decimal punteado, solo es necesario analizar el proceso de conversión de valores binarios de 8 “bits” a valores decimales de 0 a 255, para cada agrupación de 8 “bits” (octeto) en una dirección IPv4.

En el siguiente video, se detallan los pasos respectivos para la conversión de direcciones IP decimales a direcciones IP binarias. Tenga en cuenta que, tal proceso se debe realizar para cada valor decimal a convertir, esto quiere decir que el proceso se debe realizar cuatro veces, a fin de convertir la dirección IPv4.

Video 3. Dirección IPv4



[Enlace de reproducción del video](#)

Síntesis del video: Dirección IPv4

En este video, la instructora SENA ofrece el paso a paso, y otros elementos, para ejecutar la conversión de direcciones IP decimales a direcciones IP binarias.

1.7. IPv6

Debido al crecimiento exponencial que tuvo la implementación del protocolo de Internet en su versión 4 y partiendo de que el diseño de este fue casi un experimento, sin llegar a imaginar el éxito comercial que iba a tener y que solo se dispone de 2^{32} direcciones, no se planteó que en pocos meses iba a quedar corto en espacio. Por tal motivo, se contempló la implementación de una nueva versión llamada IPv6.

Esta dispone de 2^{128} direcciones o, dicho de otra manera, 340 sextillones de direcciones. Esta versión fue trabajada por la organización de estandarización de los protocolos de Internet (“IETF, Internet Engineering Task Force”). El despliegue del direccionamiento IPv6 conserva una coexistencia ordenada con su antecesora versión

4; a medida que el ecosistema de las redes de datos se adapte, esta se irá desplazando a la nueva versión del protocolo de Internet.

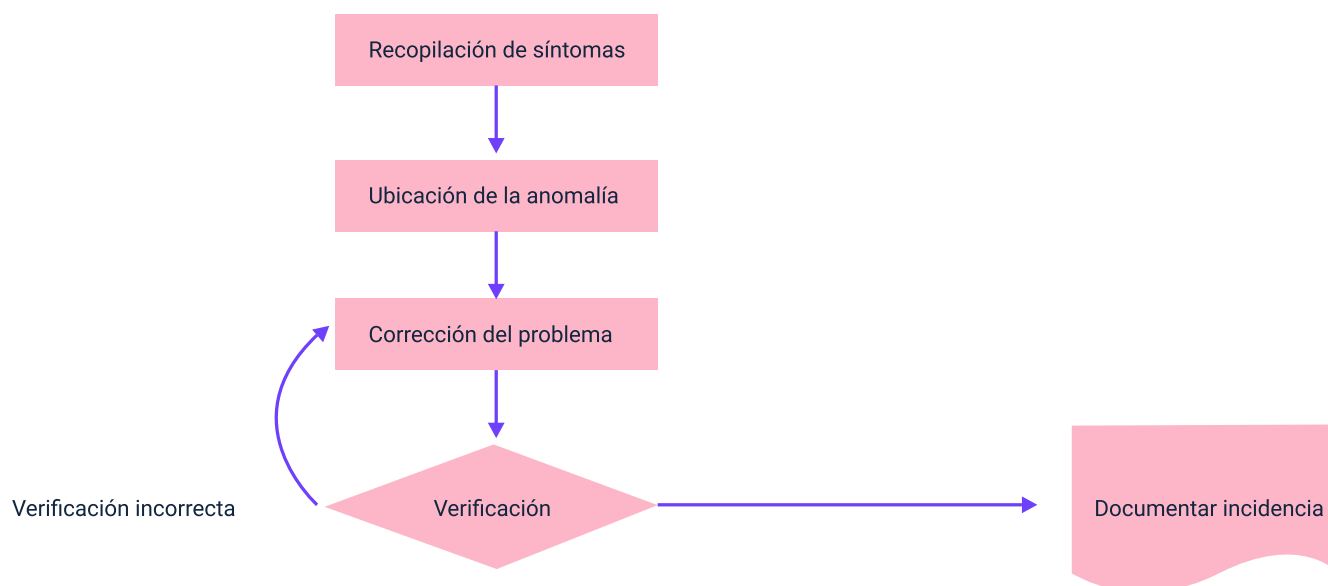
Por esta razón, es importante comprender cómo se implementa la versión 6 del Protocolo de Internet, ya que su aplicación se extiende incluyendo a usuarios domésticos, empresas, proveedores de contenido, proveedores de servicios de Internet y los entes de regulación de Internet.

2. Verificación de dispositivos

Para la verificación de dispositivos se debe establecer una distribución específica de las diferentes conexiones, mediante dominios o grupos de trabajo, configuraciones de las direcciones IP, recursos compartidos, gestión de cuentas de usuario y privilegios asociados, generalmente, bajo un sistema de archivo distribuido o directorio activo.

La implementación de diagramas de flujo para representar gráficamente los procedimientos sistemáticos, los métodos corporativos y las distintas técnicas a aplicar, es una manera idónea de documentar estos procesos.

Figura 11. Diagramación de anomalías



En esta figura inmediatamente anterior, el diagrama registra la anomalía así:

- **Entrada:** recopilación de síntomas
- **Acción:** ubicación de la anomalía
- **Acción:** corrección del problema
- **Decisión:** verificación

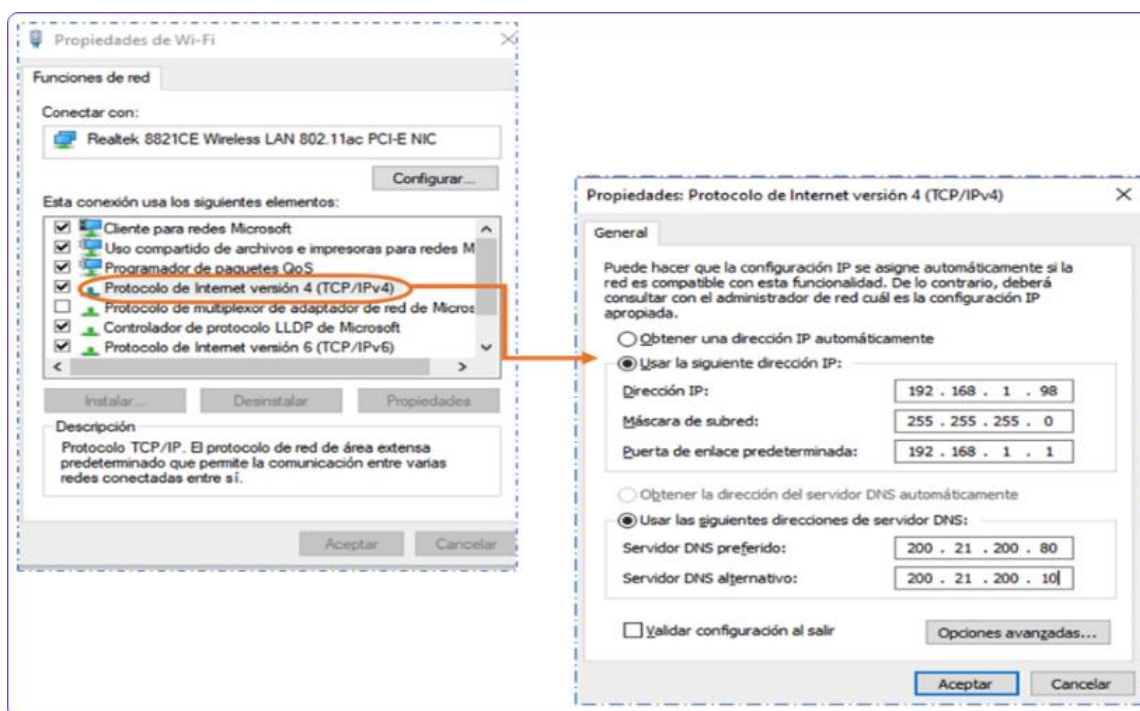
- Si la verificación es incorrecta: se retorna a la corrección del problema
- Si la verificación es correcta: se procede a documentar la incidencia

Configuración IPv4 / IPv6

Para que el terminal, es decir, el dispositivo final, se comuniquen a través de la red, debe configurarse con la información de direccionamiento IP correcta. El terminal debe configurarse con una dirección IP y una máscara de subred.

Esta información se configura desde la PC. Todos estos parámetros deben configurarse para que el terminal se conecte correctamente a la red. Esta información consta de la configuración de red de su PC. Además de la dirección IP y la información de la máscara de subred, se puede configurar la puerta de enlace predeterminada y la información del servidor DNS, como se muestra a continuación.

Figura 12. Direccionamiento de dispositivos finales

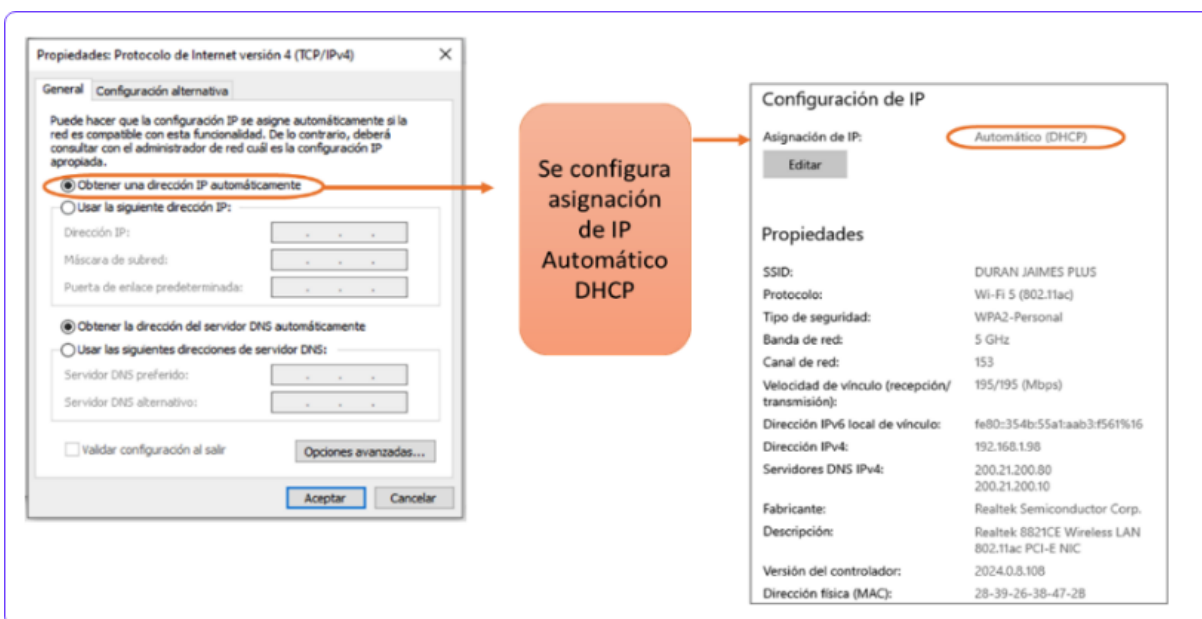


Como se muestra en la imagen anterior, la dirección de puerta de enlace predeterminada, o “Gateway”, es la dirección IP de la interfaz del enrutador utilizada para permitir que los paquetes salgan de la red local. El “Gateway” es asignado normalmente por el administrador de la red, lo cual direcciona la salida del tráfico en la red cuando este debe enrutarse a otra red.

El servidor DNS es la dirección IP que corresponde a un servidor conocido como DNS (Sistema de Nombres de Dominio). Este sistema asocia direcciones IP en red con nombres de dominio, o también conocidos como páginas web, como **www.google.com** o **www.sena.edu.co**.

La información de la dirección IP se puede ingresar en la PC manualmente o usando el Protocolo de configuración dinámica de “host” (DHCP). Se puede utilizar DHCP para configurar automáticamente la información IP de su terminal. DHCP es una tecnología utilizada en la mayoría de las redes comerciales.

Figura 13. Direccionamiento dinámico

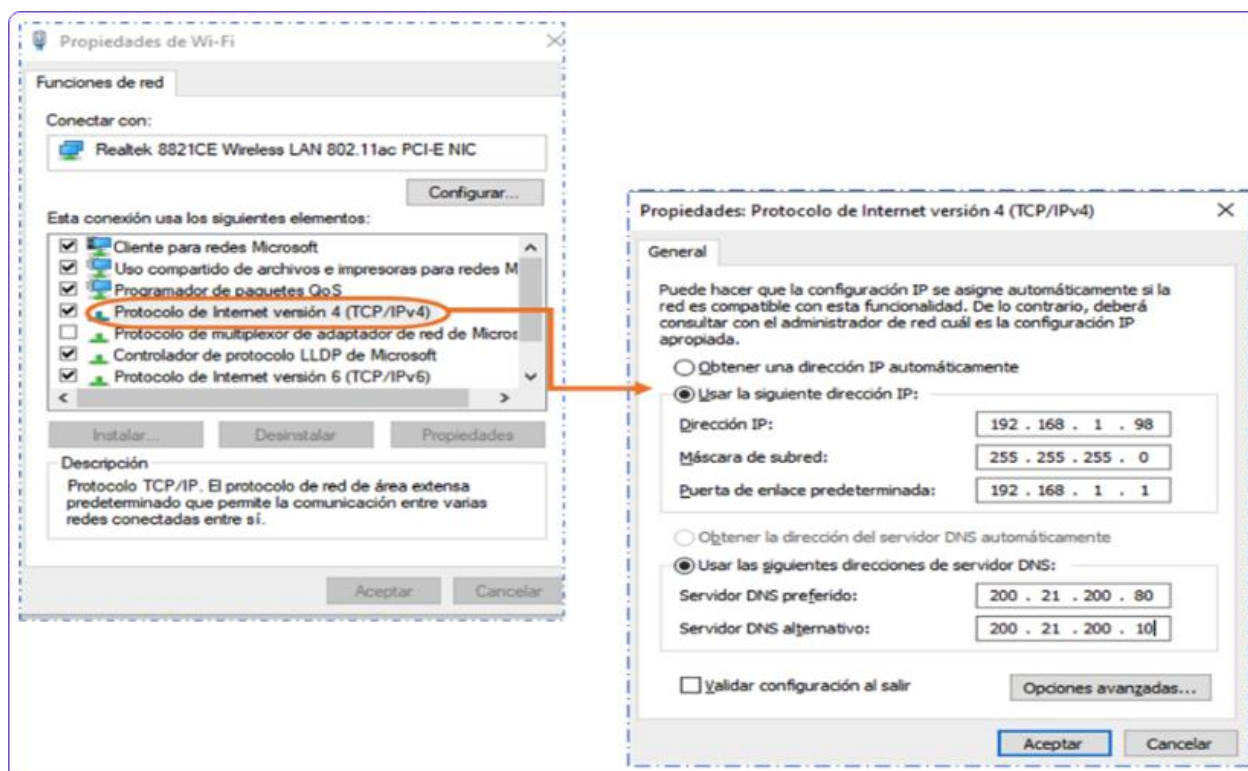


DHCP permite configurar automáticamente la dirección IPv4 de cada terminal en una red habilitada para DHCP. Imagínese cuánto tiempo tomaría si tuviera que ingresar manualmente su dirección IP, máscara de subred, puerta de enlace predeterminada y servidor DNS, cada vez que se conecta a la red. Multiplique esto por cada usuario y cada dispositivo en su red, para encontrar el problema.

DHCP es un ejemplo de la mejor tecnología. Uno de los principales objetivos de la tecnología es facilitar el trabajo que debe realizarse. Con DHCP, los usuarios finales pueden ingresar a un área cubierta por una red específica y recibir rápidamente la información IPv4 necesaria para conectar un cable Ethernet o habilitar una conexión inalámbrica y comunicarse correctamente a través de la red.

La figura siguiente, muestra el proceso de asignación de direcciones dinámicas:

Figura 14. Direccionamiento IPv6



La imagen inmediatamente anterior, muestra los procesos para configuración con el protocolo IPv6. Tal proceso se hace de manera similar a la del protocolo IPv4 y tiene las mismas dos opciones planteadas anteriormente.

Plano de control IPv4/IPv6

Se asume, implícitamente, que el plano de control de enrutamiento reside y se ejecuta, completamente, en un procesador de enrutamiento dentro del “router”. Por lo tanto, el plano de control de enrutamiento de toda la red está descentralizado, con diferentes partes (por ejemplo, de un algoritmo de enrutamiento) que se ejecutan en diferentes “routers” e interactúan enviando mensajes de control entre sí.

De hecho, los “routers” de Internet y los algoritmos de enrutamiento operan exactamente de esta manera. Además, los proveedores de “switches” y “routers” agrupan su plano de datos de “hardware” y el plano de control de “software” en plataformas cerradas (pero interoperables), en un producto integrado verticalmente.

Son varios los investigadores (como Caesar 2005, Casado 2009, McKeown 2008) quienes, recientemente, han comenzado a explorar nuevos controles de arquitecturas de plano en las que parte del plano de control se implementa en los “routers”. La medición (informe local del estado del enlace, instalación y mantenimiento de la tabla de reenvío) junto con el plano de datos, y parte del plano de control, se puede implementar de forma externa al enrutador (por ej; en un servidor centralizado, que podría realizar el cálculo de ruta).

Para el tipo de plano de control, es importante considerar dos enfoques:

a. Algoritmos de ruteo tradicional: implementados en los “routers”.

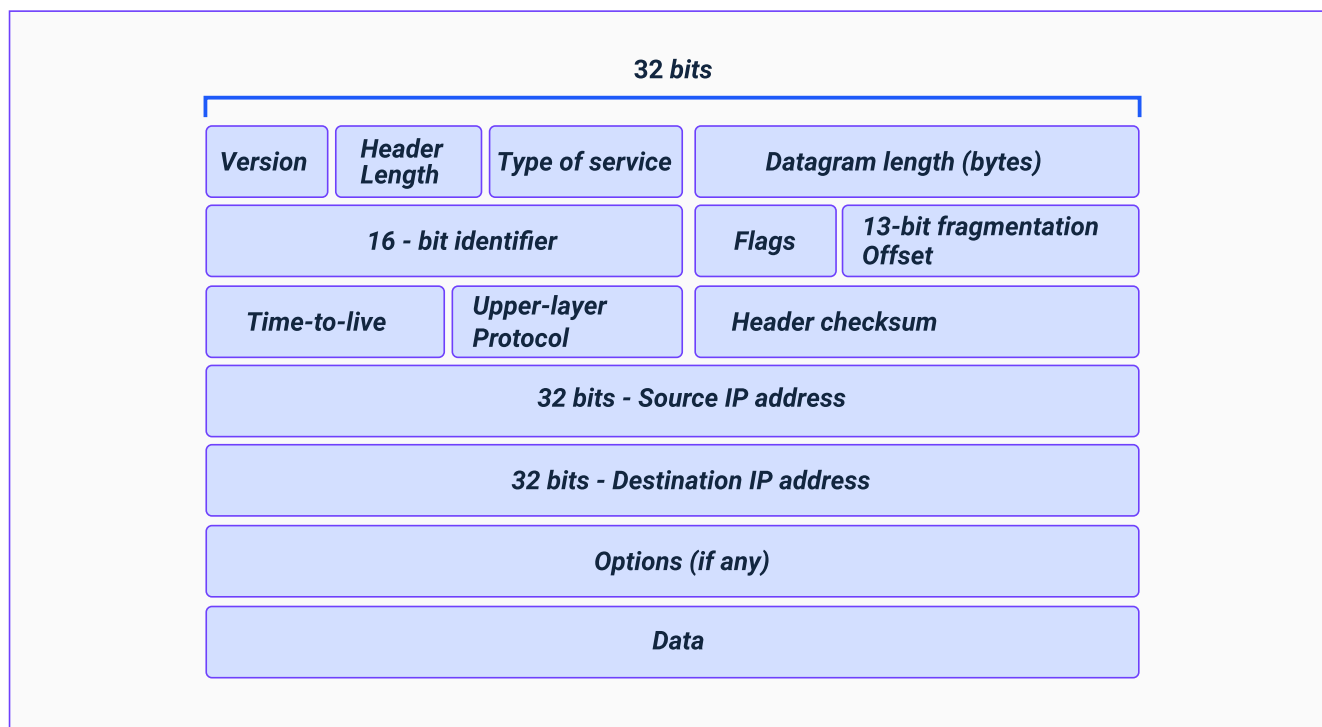
- b. **“Software Defined Networking” (SDN)**: implementado en los servidores remotos.

Plano de datos IPv4/IPv6

El reenvío de paquetes es una de las funciones de la capa de red que mueve los paquetes desde la entrada del “router” hasta la salida correspondiente. Funciona localmente y es una característica de todos los “routers”.

En una red de datos, existe un flujo constante de información que se envía de un extremo a otro. Los datagramas IP son las unidades principales que contienen la información de Internet. Un datagrama se estructura con toda la información necesaria sobre direcciones, enrutamiento, prioridad, entre otros.

Figura 15. Estructura datagrama



Nota: tomada de Kurose y Ross (2013).

El siguiente enlace, conduce hasta el video denominado **Configurar IPv6**

Windows – Linux; donde se lleva a cabo una configuración de IPv6 en el sistema Linux.

Preste atención a la información allí contenida y aprópiase tanto de los conceptos como de las acciones que se ejecutan para tal fin:

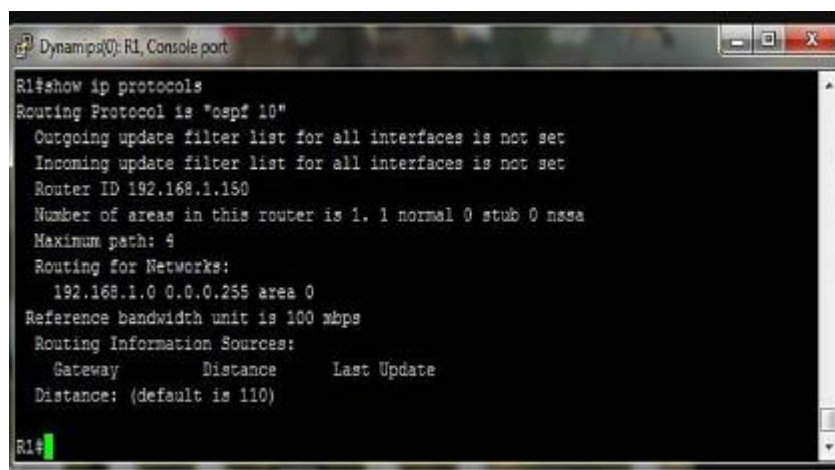
https://www.youtube.com/watch?v=F9RDmrCp_K8

Verificación de problemas protocolo RIP y OSPF para IPv6

El uso de comandos necesarios para la resolución de problemas en los protocolos RIP y OSPF toma importancia tanto para IPv4 como para IPv6, ya que las posibles causas son las mismas en ambos.

El proceso de depuración de errores se logra con la implementación de los comandos adecuados, como son:

- a. **“Show IP Route”**. Muestra contenido de una tabla de enrutamiento IP.



```
Dynamips(U): R1, Console port
R1#show ip protocols
Routing Protocol is "ospf 10"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 192.168.1.150
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.1.0 0.0.0.255 area 0
  Reference bandwidth unit is 100 mbps
  Routing Information Sources:
    Gateway         Distance      Last Update
  Distance: (default is 110)
```

- b. **“Show IP Protocols”**. Muestra los parámetros de un protocolo en particular.

```
Dynamips(U): R1, Console port
R1#show ip protocols
Routing Protocol is "ospf 10"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 192.168.1.150
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.1.0 0.0.0.255 area 0
  Reference bandwidth unit is 100 mbps
  Routing Information Sources:
    Gateway         Distance      Last Update
  Distance: (default is 110)
```

c. “Debug IP RIP”. Depura anuncios RIP y actualizaciones.

```
Router# debug ip rip
RIP: received update from 10.89.80.28 on Ethernet0
  10.89.95.0 in 1 hops
  10.89.81.0 in 1 hops
  10.89.66.0 in 2 hops
  172.31.0.0 in 16 hops (inaccessible)
  0.0.0.0 in 7 hop
RIP: sending update to 255.255.255.255 via Ethernet0 (10.89.64.31)
  subnet 10.89.94.0, metric 1
  172.31.0.0 in 16 hops (inaccessible)
RIP: sending update to 255.255.255.255 via Serial1 (10.89.94.31)
  subnet 10.89.64.0, metric 1
  subnet 10.89.66.0, metric 3
  172.31.0.0 in 16 hops (inaccessible)
  default 0.0.0.0, metric 8
```

El OSPF (“Open Shortest Path First”), por su parte, es un protocolo de enrutamiento de estado de enlace desarrollado para reemplazar el protocolo de enrutamiento por vector de distancia RIP. En los primeros días de la tecnología de redes e Internet, RIP era un protocolo de enrutamiento aceptado.

Sin embargo, el hecho de que el protocolo RIP se base en el número de saltos como única métrica para determinar la mejor ruta, se convierte rápidamente en un problema. El uso de conteos de saltos no es apropiado para redes grandes, con muchas rutas, a diferentes velocidades. OSPF tiene ventajas significativas sobre RIP, ya que proporciona una convergencia y escalabilidad más rápidas para implementaciones de

red mucho más grandes. OSPF es un protocolo de enrutamiento sin clases, que utiliza el concepto de zonas para lograr escalabilidad.

Explore el contenido del video que se muestra en el siguiente enlace y asimile con propiedad los conceptos y acciones del protocolo OSPF:

<https://www.youtube.com/watch?v=wK24zn66Dbs>

Servicios para IPv6

Los servicios de red con soporte IPv6 son de alta importancia para este mundo de transición, debido al cambio que se avecina en todo el mundo y, especialmente, en Colombia, donde el liderazgo lo lleva el ministerio de las TIC.

Algunos de los servicios que se van a tratar son:

- Servicio web con HTTP y HTTPS.
- DNS.
- SSH.
- DHCP.
- Telefonía IP.
- Servicio de base de datos.
- Enrutamiento BGP.
- Enrutamiento OSPF.

“Cisco Packet Tracer”

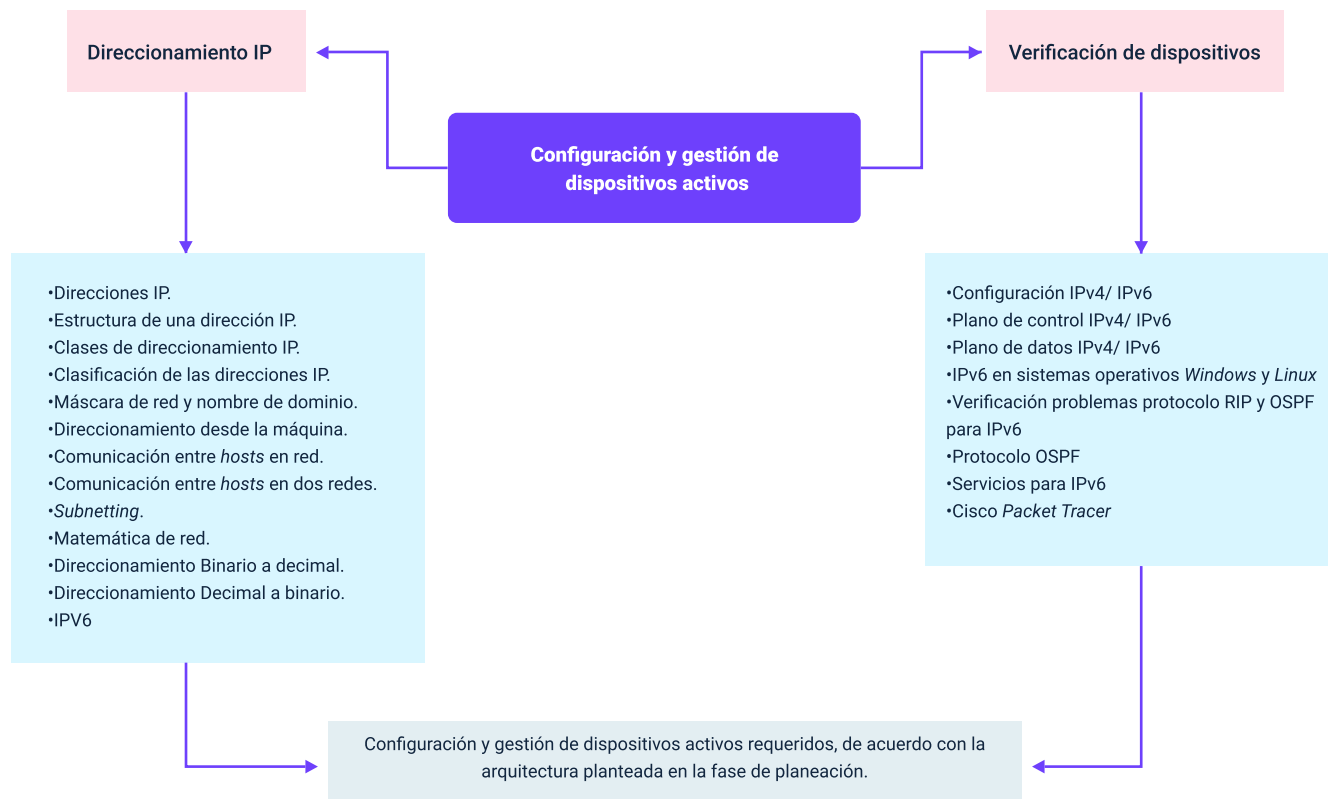
La herramienta “Packet Tracer” de Cisco, corresponde a un “software” de simulación de redes, que permite hacer pruebas con diferentes dispositivos de red, pudiendo llevar un caso real al mundo de la simulación, donde se obtienen resultados

favorables en cada una de las fases de una topología de red, comenzando por la planeación hasta la verificación de sus transmisiones.

Esta herramienta se utilizará en la mayor parte de los laboratorios propuestos de esta **Tecnología en gestión de redes de datos**.

Síntesis

Ha llegado al final de este componente formativo. En este punto, se presenta un mapa general de los contenidos estudiados, el cual usted debe analizar y, entonces, desarrollar su propia síntesis de los temas y conceptos trabajados. ¡Adelante!



El mapa de contenidos y conceptos del componente formativo muestra el enfoque de los temas hacia las generales y aspectos claves del direccionamiento IP y la verificación de dispositivos activos, como parte del proceso de la gestión de redes de datos.

Material complementario

Tema	Referencia	Tipo de material	Enlace del recurso
1. Direccionamiento IP	Ariganello, E. (2020). REDES CISCO Guía de estudio para la certificación CCNA 200–301. Editorial Ra-Ma.	Documento	https://aprenderedes.com/wp-content/uploads/2020/04/CCNA-200-301-indice.pdf
1. Direccionamiento IP	Cortés, A. (s. f.). Introducción a redes. Capítulo 8: Direccionamiento IP. Cisco Networking Academy.	Documento	https://silo.tips/download/introduccion-a-redes-ing-anibal-coto-cortes
2. Verificación de dispositivos	Tárrega, J. (2020, 5 abril). Configurar IPv6 Windows - Linux [Video]. YouTube.	Video	https://www.youtube.com/watch?v=F9RDmrCp_K8
2. Verificación de dispositivos	Lopez, M. [Guerreros de la Red Mic hely Lopez]. (2018, 26 mayo). ¿Qué es? ¿Cómo funciona? Protocolo de Routing de Redes OSPF (Open Shortest Path First) Cisco, Huawei [Video]. YouTube.	Video	https://www.youtube.com/watch?v=wK24zn66Dbs

Glosario

Datagrama: hace referencia a un paquete de datos que se transmite como un bloque de información mediante la capa de red.

Dirección IP: corresponde a un grupo de valores numéricos que identifican de manera lógica y a su vez jerárquica a la conexión en red de un “host”.

Estación de trabajo: es una forma de referirse a **computadora en red**.

“Host”: hace referencia a los computadores u otro dispositivo que está conectado en red.

LAN: “Local Area Network”, corresponde a la Red de Área Local. Es una red de datos con alcance reducido a un área como la de una oficina, una casa o un edificio.

Modelo OSI: modelo de estandarización internacional establecido por ISO e UITT, permite desarrollar estándares para redes de datos, los cuales facilitan la interoperabilidad de equipos desarrollados por diferentes fabricantes.

Paquete: indica una pequeña agrupación de información de longitud variable, que generalmente tiene de 256 a 2,000 “bytes” de longitud.

Protocolo: reglas de comunicación para el funcionamiento de la red. Los protocolos especifican cómo se formatean y envían las solicitudes, los mensajes y otras señales a través de la red.

“Router”: es un dispositivo de “hardware” que permite la interconexión de “hosts” en redes de datos.

Servidor: dispositivo conectado a la red que permite dar asistencia, brindando información u otros servicios solicitados por los clientes en la red.

Sistema operativo: corresponde al “software” que gestiona las características de “hardware”. Se encarga de establecer una interfaz de comunicación con el usuario e interviene en el almacenamiento de los datos en los dispositivos.

“Switch”: es un dispositivo de “hardware” que se utiliza para interconectar varios “hosts” a través de la red de datos.

WAN: “Wide Area Network”, corresponde a la Red de Área Amplia, que sobrepasa extensas regiones geográficas.

Referencias bibliográficas

Ariganello, E. (2020). REDES CISCO Guía de estudio para la certificación CCNA 200–301 (Spanish Edition). Editorial Ra-Ma. https://www-alphaeditorialcloud-com.bdigital.sena.edu.co/auth/ip?intended_url=https://www-alphaeditorialcloud-com.bdigital.sena.edu.co/library/publication/redes-cisco-guia-de-estudio-para-la-certificacion-ccna-200-301

Cisco Networking Academy. (2013). Principios básicos de enrutamiento y switching. CCNA1 V5.
https://julioestrepo.files.wordpress.com/2015/03/pdf_ccna1_v5.pdf

Guevara, L. (2018). Tutoría y Orientación. Universidad Nacional de Educación Enrique Guzmán y Valle.
<https://repositorio.une.edu.pe/bitstream/handle/20.500.14039/3448/MONOGRAF%c3%8dA%20-%20GUEVARA%20FLORES%20-.pdf?sequence=1&isAllowed=y>

Kurose, J. y Ross, K. (2013). Computer networking. A top-down approach. Pearson.
https://www.ucg.ac.me/skladiste/blog_44233/objava_64433/fajlovi/Computer%20Networking%20-%20A%20Top%20Down%20Approach,%207th,%20converted.pdf

Mora, P. (2016). Equipos de interconexión y servicios de red. Elearning S.L.

Vilás, P. (2014). Supernetting o sumarización de rutas. Estribancus.
<http://pvilas.com/2014/12/supernetting-o-sumarizacion-de-rutas.html>

Créditos

Nombre	Cargo	Regional y Centro de Formación
Claudia Patricia Aristizábal	Responsable del Ecosistema	Dirección General
Rafael Neftalí Lizcano Reyes	Responsable de Línea de Producción	Centro Industrial del Diseño y la Manufactura - Regional Santander
Cinthia Rocío Trejos Chacón	Experto Temático	Centro de la Industria, la Empresa y los Servicios - Regional Norte de Santander
Fabian Leonardo Correa Díaz	Diseñador Instruccional	Centro Industrial del Diseño y la Manufactura - Regional Santander
Carlos Eduardo Garavito Parada	Animador y Productor Multimedia	Centro Industrial del Diseño y la Manufactura - Regional Santander
Wilson Andrés Arenales Cáceres	Storyboard e ilustración	Centro Industrial del Diseño y la Manufactura - Regional Santander
Daniela Muñoz Bedoya	Locución	Centro Industrial del Diseño y la Manufactura - Regional Santander
Carlos Julián Ramírez Benítez	Diseñador de Contenidos Digitales	Centro Industrial del Diseño y la Manufactura - Regional Santander
Andrea Paola Botello De la Rosa	Desarrollador “Full-stack”	Centro Industrial del Diseño y la Manufactura - Regional Santander
Emilsen Alfonso Bautista	Actividad didáctica	Centro Industrial del Diseño y la Manufactura - Regional Santander
Daniel Ricardo Mutis Gómez	Evaluador para Contenidos Inclusivos y Accesibles	Centro Industrial del Diseño y la Manufactura - Regional Santander

Nombre	Cargo	Regional y Centro de Formación
Zuleidy María Ruíz Torres	Validador de Recursos Educativos Digitales	Centro Industrial del Diseño y la Manufactura - Regional Santander
Luis Gabriel Urueta Álvarez	Validador de Recursos Educativos Digitales	Centro Industrial del Diseño y la Manufactura - Regional Santander