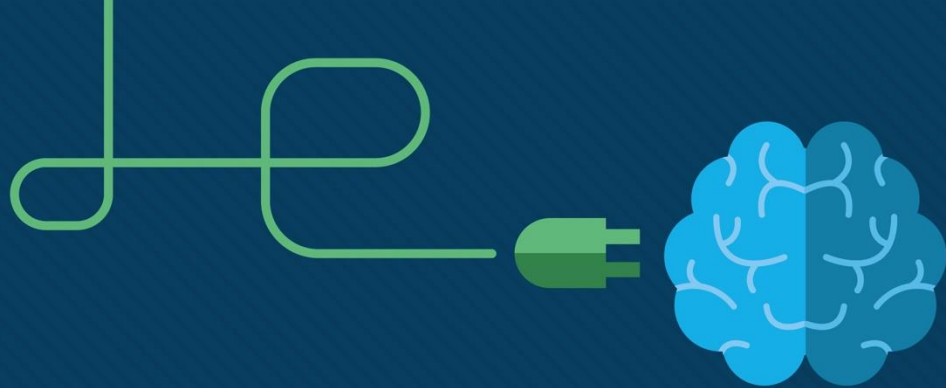




Capítulo 6: Redes aplicadas

IT Essentials v7.0



Capítulo 6: Secciones y objetivos

6.1 Conexión de un dispositivo a una red

- Configurar dispositivos para redes cableadas e inalámbricas.
 - Explicar la asignación de direcciones MAC e IP para las redes de computadoras.
 - Configurar una NIC para redes cableadas e inalámbricas.
 - Configurar las redes inalámbricas en una LAN pequeña.
 - Configurar los ajustes del firewall.
 - Configurar los dispositivos de IdC.

6.2 Solución de problemas de red

- Identificar y resolver problemas relacionados con redes.
 - Explicar los seis pasos del proceso de resolución de problemas de red.
 - Solucionar los problemas comunes y avanzados relacionados con las redes.

6.1 Conexión de un dispositivo a una red

Explicación en video: Asignación de direcciones MAC

Esta es una explicación en video sobre la asignación de direcciones MAC:

- Analogía de la comunicación
- Dirección MAC de la NIC
- Dirección física
- Asignado por el OUI y el proveedor
- Comunicación en la misma red
- Comunicación en otra red

Explicación en video: Asignación de direcciones IPv4

Esta es una explicación en video sobre la asignación de direcciones IPv4:

- Analogía de la comunicación
- Direcciones IPv4 frente a direcciones IPv6
- Decimal frente a binario frente a hexadecimal
- Máscaras de subred
- Porciones de red y de host de una dirección IPv4
- Ejemplo de asignación de direcciones IPv4

Explicación en video: Asignación de direcciones IPv6

Esta es una explicación de video sobre la asignación de direcciones IPv6:

- Segmentos hexadecimales
- Reglas de compresión de direcciones
- Porciones de red y de host de una dirección IPv6
- Ejemplo de asignación de direcciones IPv6

Asignación de direcciones de red

Dos direcciones de red



Formato de dirección MAC

Formato de dirección	Descripción
00-50-56-BE-D7-87	Dos dígitos hexadecimales separados por guiones
00:50:56:BE:D7:87	Dos dígitos hexadecimales separados por dos puntos
0050.56BE.D787	Cuatro dígitos hexadecimales separados por puntos

Formato de direcciones IPv4

32 bits en notación decimal punteada

192.168.200.8

Formatos de direcciones IPv6

128 bits en formato hexadecimal

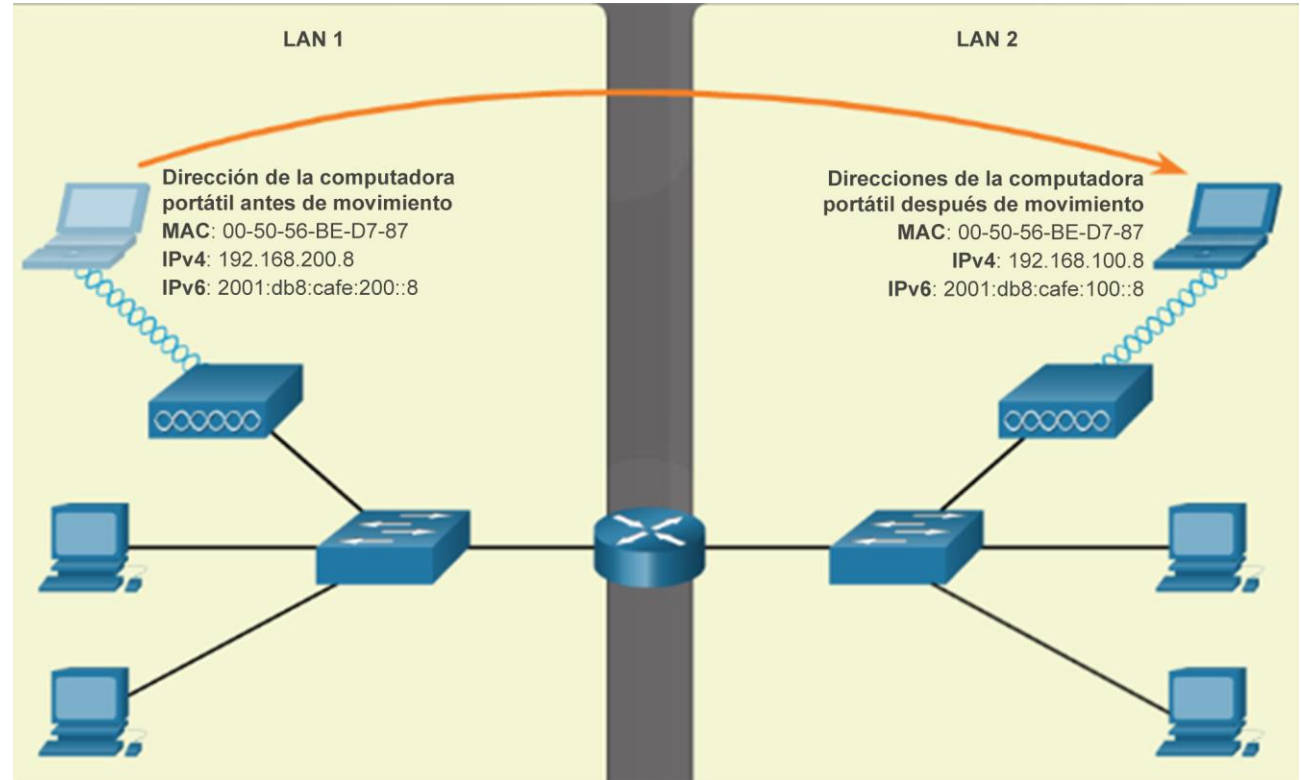
2001:0db8:cafe:0200:0000:0000:0000:0008

128 bits en formato comprimido

2001:db8:cafe:200::8

Dos direcciones de red (cont.)

- Cuando se traslada una computadora portátil a una red diferente, la dirección MAC permanece igual, pero las direcciones IPv4 e IPv6 cambian.
- Una dirección MAC es un número único que forma parte de la NIC.
- Las direcciones IP son asignadas por la empresa o el proveedor de Internet.



Visualización de las direcciones

Use el switch /all con el comando `ipconfig` para ver la dirección MAC (física).

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

Windows IP Configuration

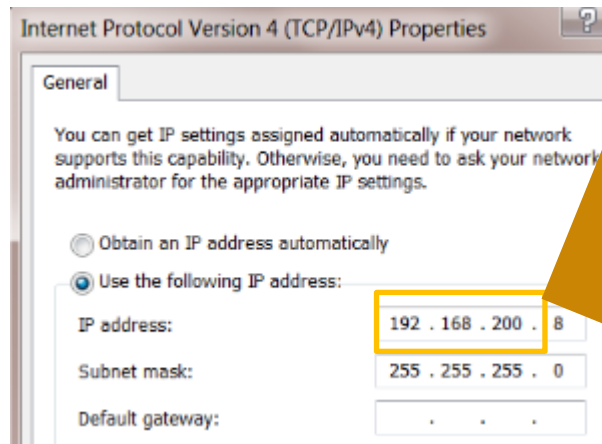
```
Host Name . . . . . : ITEuser
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
```

Ethernet adapter Local Area Connection:

```
Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) PRO/1000 MT Network Connection
Physical Address. . . . . : 00-50-56-BE-D7-87
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
IPv6 Address. . . . . : 2001:db8:cafe:200::8(Preferred)
Link-local IPv6 Address . . . . . : fe80::8cbf:a682:d2e0:98a%11(Preferred)
IPv4 Address. . . . . : 192.168.200.8(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 2001:db8:cafe:200::1
                            192.168.200.1
```

Formato de direcciones IPv4

- Dos partes de una dirección IP:
 - Red
 - Host
- La máscara de subred define la parte de red de la dirección.



La porción de red de la dirección proviene de la máscara de subred.

	Porción de red	Porción de host
192.168.200.8	11000000.10101000.11001000	00001000
255.255.255.0	11111111.11111111.11111111	00000000
192.168.200.0	11000000.10101000.11001000	00000000

Formato de direcciones IPv6

■ Reglas:

- Omitir ceros iniciales: 0db8 puede ser db8
- Omita todos segmentos en 0: use dos puntos dobles (::)

```
2001 : 0DB8 : 0000 : 1111 : 0000 : 0000 : 0000 : 0200  
FE80 : 0000 : 0000 : 0000 : 0123 : 4567 : 89AB : CDEF  
FF02 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0001
```

Completamente expandida	2001:0db8:0000:1111:0000:0000:0000:0200
Sin ceros iniciales	2001:db8:0:1111:0:0:0:200
Comprimido	2001:db8:0:1111::200

Completamente expandida	fe80:0000:0000:0000:0123:4567:89ab:cdef
Sin ceros iniciales	fe80:0:0:0:123:4567:89ab:cdef
Comprimido	fe80::123:4567:89ab:cdef

Completamente expandida	ff02:0000:0000:0000:0000:0000:0000:0001
Sin ceros iniciales	ff02:0:0:0:0:0:0:1
Comprimido	ff02::1

Asignación de direcciones de red

Asignación de direcciones estáticas

- Información de direcciones estáticas necesaria para la comunicación con otras redes e Internet:
 - Dirección IP
 - Máscara de subred
 - Puerta de enlace predeterminada (dirección del router para que la información pueda enviarse a otras redes)
 - Servidor DNS (convierte los nombres de dominio o las URL en direcciones IP para facilitar la accesibilidad o los sitios web y dispositivos remotos)

Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

☐ Obtain an IP address automatically

☒ Use the following IP address:

IP address: 192 . 168 . 200 . 8

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 200 . 1

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 200 . 10

Alternate DNS server: . . .

Internet Protocol Version 6 (TCP/IPv6) Properties

General

You can get IPv6 settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IPv6 settings.

☐ Obtain an IPv6 address automatically

☒ Use the following IPv6 address:

IPv6 address: 2001:db8:cafe:200::8

Subnet prefix length: 64

Default gateway: 2001:db8:cafe:200::1

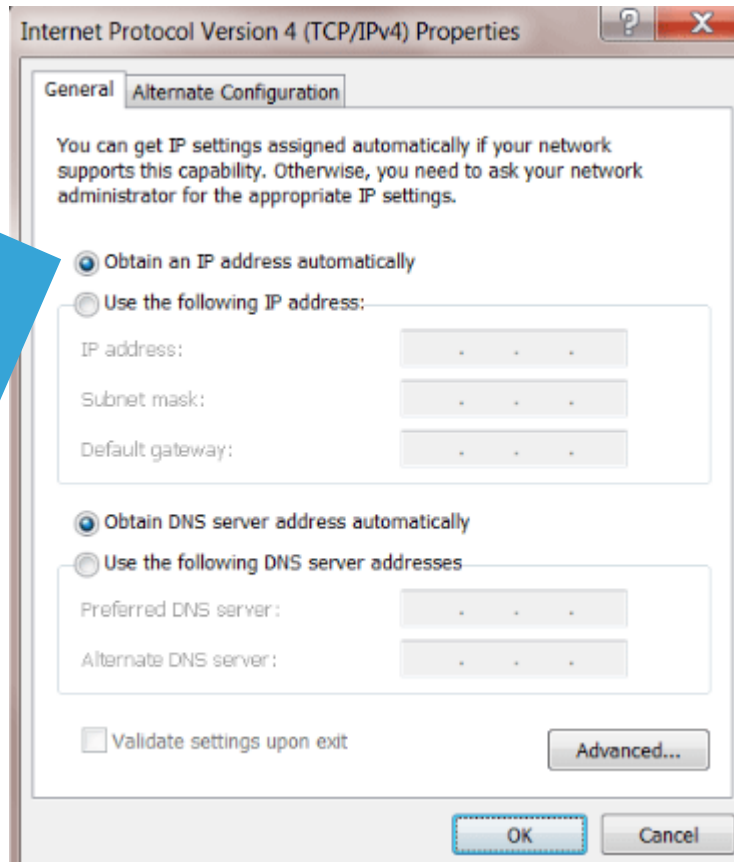
☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

Preferred DNS server: 2001:4860:4860::8888

Alternate DNS server:

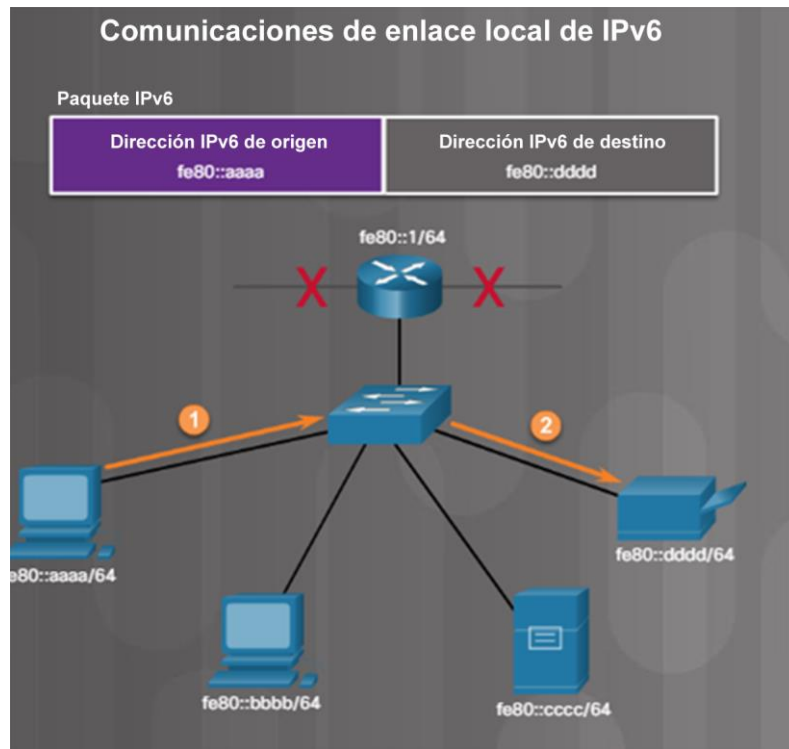
Asignación de direcciones dinámicas



- La información de asignación de direcciones IP proviene de un servidor DHCP

Direcciones IPv4 e IPv6 con vínculos locales

- Se usa el dispositivo IPv4 si el dispositivo no puede obtener una dirección IP IPv4.
- El dispositivo IPv6 siempre debe tener una dirección IP IPv6 dinámica o configurada manualmente con un vínculo local.



Packet Tracer: Agregar computadoras a una red existente

En esta actividad del Packet Tracer, configurará las computadoras para utilizar DHCP, configurar las direcciones estáticas, utilizará el comando ipconfig para recuperar la información IPv4 del host y utilizará un ping para verificar la conectividad.

Configurar un diseño de red de NIC

- Componentes de la red
- Diseño de la red



Configuración de una NIC

Selección de una NIC



Ethernet
por cable



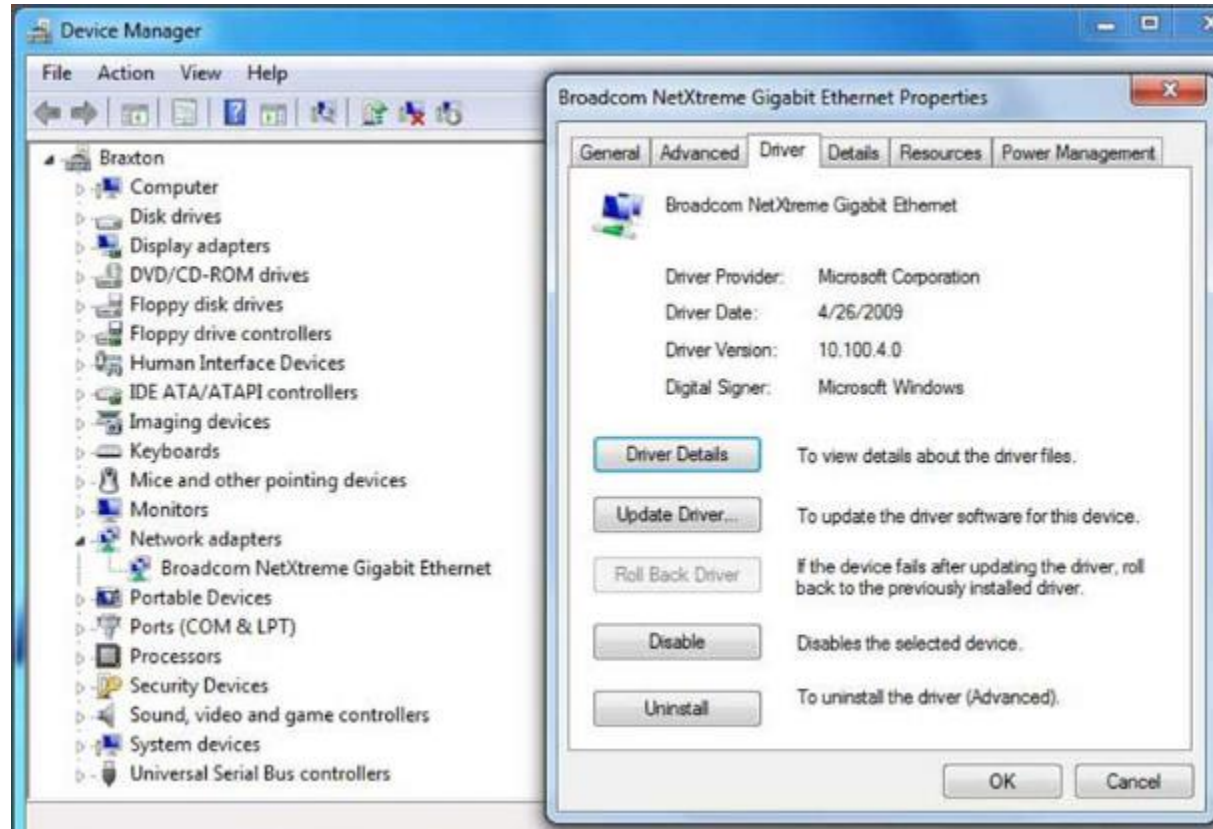
Ethernet
inalámbrica



Ethernet
inalámbrica

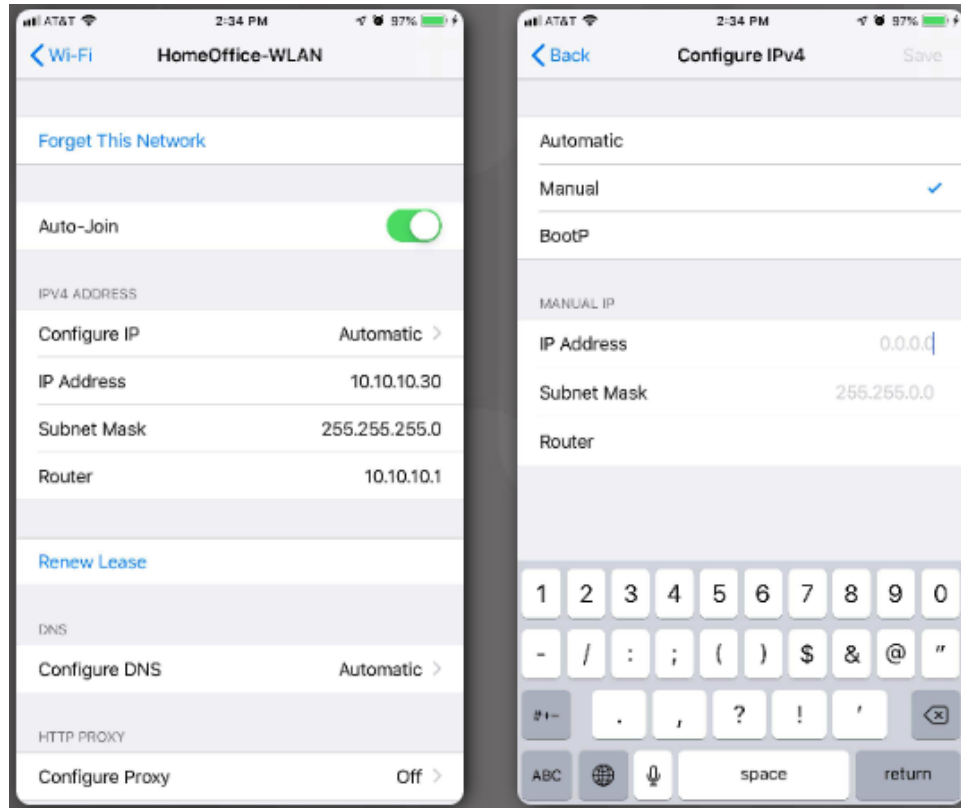
Instalación y actualización de una NIC

- Si se instala una NIC inalámbrica, asegúrese de que la antena esté posicionada para lograr un alcance óptimo.
- Use el **Administrador de dispositivos** para ver los detalles del controlador:
 - Expanda la categoría de *Adaptadores de red*
 - Haga clic con el botón secundario en la NIC específica > *Propiedades* o *Actualizar controlador*



Configuración de una NIC

Configuración de una NIC



- Los dispositivos inalámbricos, incluidos los smartphones, también necesitan direcciones IP para participar en una red inalámbrica.

Configuración de una NIC

ICMP

Opciones del comando ping del switch

- El protocolo de mensajes de control de Internet (ICMP) se usa para probar la conectividad y enviar mensajes de control y de error.
- El comando **ping** es parte de ICMP.

```
C:\> ping cisco.com

Pinging e144.dscb.akamaiedge.net [23.200.16.170] with 32 bytes of data:
Reply from 23.200.16.170: bytes=32 time=25ms TTL=54
Reply from 23.200.16.170: bytes=32 time=26ms TTL=54
Reply from 23.200.16.170: bytes=32 time=25ms TTL=54
Reply from 23.200.16.170: bytes=32 time=25ms TTL=54

Ping statistics for 23.200.16.170:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 25ms, Maximum = 26ms, Average = 25ms
```

```
C:\> ping /?
```

```
Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
          [-r count] [-s count] [[-j host-list] | [-k host-list]]
          [-w timeout] [-R] [-S srcaddr] [-4] [-6] target_name
```

Options:

-t	Ping the specified host until stopped. To see statistics and continue - type Control-Break; To stop - type Control-C.
-a	Resolve addresses to hostnames.
-n count	Number of echo requests to send.
-l size	Send buffer size.
-f	Set Don't Fragment flag in packet (IPv4-only).
-i TTL	Time To Live.
-v TOS	Type Of Service (IPv4-only. This setting has been deprecated and has no effect on the type of service field in the IP Header).
-r count	Record route for count hops (IPv4-only).
-s count	Timestamp for count hops (IPv4-only).
-j host-list	Loose source route along host-list (IPv4-only).
-k host-list	Strict source route along host-list (IPv4-only).
-w timeout	Timeout in milliseconds to wait for each reply.
-R	Use routing header to test reverse route also (IPv6-only).
-S srcaddr	Source address to use.
-4	Force using IPv4.
-6	Force using IPv6.

Práctica de laboratorio: Configuración de una NIC para usar DHCP en Windows

En esta práctica de laboratorio, configurará una NIC Ethernet para utilizar DHCP a fin de obtener una dirección IP y probar la conectividad entre dos computadoras.

Explicación en video: Configuración de una red cableada e inalámbrica

Esta es una explicación en video sobre la configuración de una red cableada e inalámbrica:

- Conectar cables
- Página web del router inalámbrico
- Cambiar contraseña
- Configuración de WAN
- Configuración de LAN
- Configuración inalámbrica
- Conectarse a la red inalámbrica

Conexión de dispositivos cableados a Internet

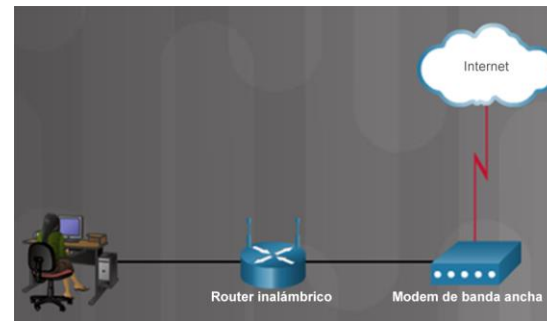
Para conectar un dispositivo de red cableada de oficina pequeña o doméstica:

1. Conecte el cable al dispositivo.
2. Conecte el otro extremo del cable al switch (puerto amarillo).
3. Conecte el cable entre el router inalámbrico (puerto azul) y el módem de banda ancha.



Al módem

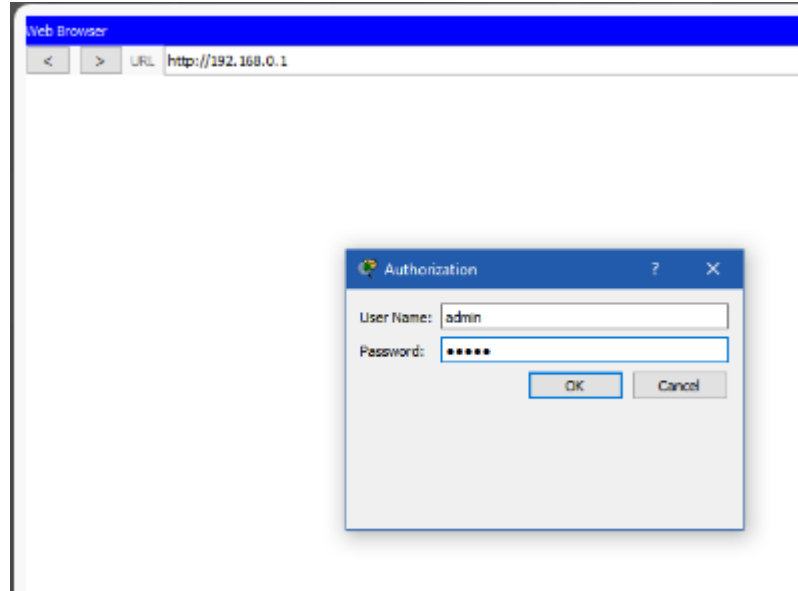
A la PC



Configuración de una red cableada e inalámbrica

Inicio de sesión en el router

- Abra un navegador e ingrese la dirección IP predeterminada del router.
- Cambie de inmediato los nombres de usuario y las contraseñas predeterminadas.



Configuración de una red cableada e inalámbrica

Configuración básica de red

1. Inicie sesión en el router.
2. Cambie la contraseña predeterminada.
3. Inicie sesión con la contraseña nueva.
4. Establezca el rango de direcciones DHCP.
5. Renueve las direcciones IP en los dispositivos (use los comandos **ipconfig/release** e **ipconfig/renew**).
6. Cambie la dirección IP predeterminada e inicie sesión con la nueva dirección IP.

Web Browser

URL: <http://192.168.0.1/index.asp> Go Stop

Wireless-N Broadband Router Firmware Version: v0.93.3

Setup Wireless Security Access Restrictions Applications & Gaming Administration Status

Basic Setup DDNS MAC Address Clone Advanced Routing

Internet Setup

Internet Connection type: Automatic Configuration - DHCP

Optional Settings (required by some internet service providers)

Host Name:

Domain Name:

MTU: Size: 1500

Network Setup

Router IP: 10.10.10.1

Subnet Mask: 255.255.255.0

DHCP Server: ☒ Enabled ☐ Disabled DHCP Reservation

Start IP Address: 192.168.0.100

Help...

Configuración de una red cableada e inalámbrica

Configuración inalámbrica básica

2.

- 1. Vea los valores predeterminados de WLAN.
- 2. Cambie el modo de red.
- 3. Configure el SSID.
- 4. Configure el canal.
- 5. Configure el modo de seguridad
- 6. Configure la contraseña.

Basic Wireless Settings

Network Mode: Mixed

Network Name (SSID):

Radio Band:

Wide Channel:

3.

Network Name (SSID): OfficeNet

4.

Standard Channel: 1 - 2.412GHz

1 - 2.412GHz

2 - 2.417GHz

3 - 2.422GHz

4 - 2.427GHz

5 - 2.432GHz

5.

Security Mode: WPA2 Personal

Encryption: AES

Passphrase:

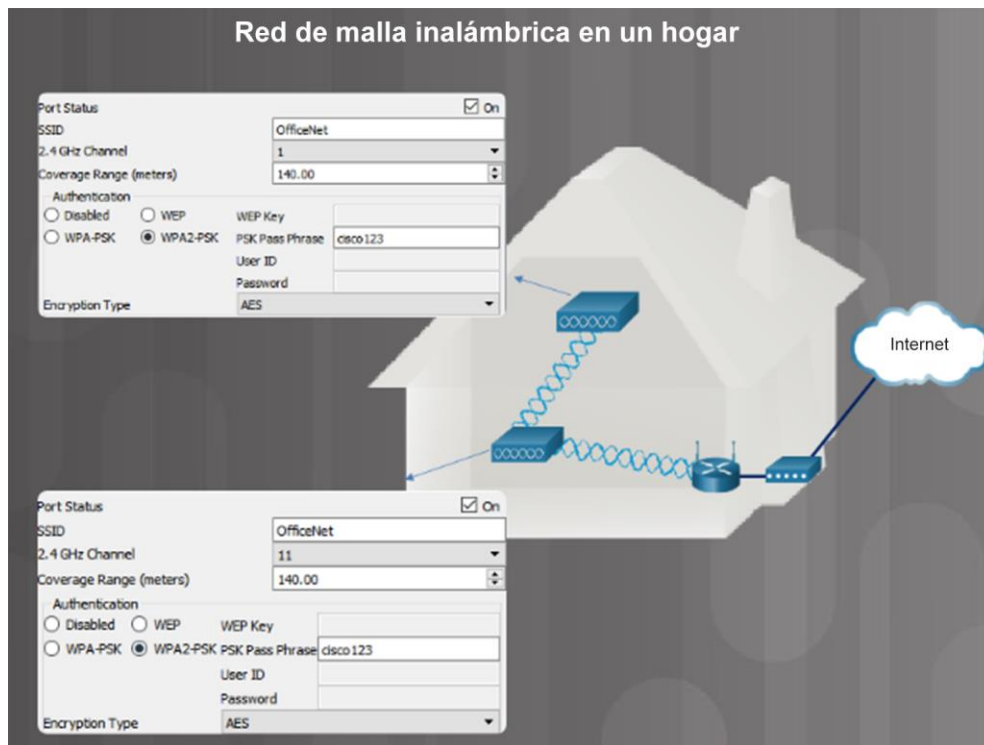
Key Renewal: 3600 seconds

6.

Passphrase: cisco123

Configuración de una red cableada e inalámbrica

Configuración de una red de malla inalámbrica



Configuración de una red cableada e inalámbrica

NAT para IPv4

- El proceso que se usa para convertir las direcciones IPv4 privadas en direcciones IPv4 públicas enrutables de Internet se denomina traducción de direcciones de red (NAT, Network Address Translation).



Configuración de una red cableada e inalámbrica

Calidad de servicio

- La configuración de calidad de servicio (QoS) permite la priorización de tipos de tráfico específicos.

BásicoAdvanced

CancelarAplicar

Inicio avanzado

Configuración

Configuración de Internet

Configuración inalámbrica

Configuración de LAN

Configuración de QoS

Almacenamiento

Seguridad

Administración

Configuración avanzada

Configuración de QoS

#	Política de QoS	Prioridad	Descripción
1	Teléfono IP	Alto	Aplicaciones del teléfono IP
2	Counter Strike	Alto	Juegos en línea Counter Strike
3	Netflix	Alto	Transmisión de video en línea de Netflix
4	FTP	Medio	Aplicaciones FTP
5	WWW	Medio	Aplicaciones WWW
6	Gnutella	Bajo	Aplicaciones de Gnutella
7	SMTP	Medio	Aplicaciones SMTP

EditarEliminarEliminar todos

Agregar regla de prioridad

Packet Tracer: conexión a una red inalámbrica

Durante esta actividad de Packet Tracer, configurará un router inalámbrico y un punto de acceso para que admitan clientes inalámbricos y enruten los paquetes IP. También actualizará algunas de las configuraciones predeterminadas.

Práctica de laboratorio: configuración de una red inalámbrica

En esta práctica de laboratorio, hará una configuración básica de un router inalámbrico y conectará una PC al router de manera inalámbrica.

Explicación en video: Configuración de Firewalls

Esta es una explicación en video sobre la Configuración de Firewalls:

- Configuración de DMZ en la LAN
- Reglas de Firewalls

Configuración de Firewalls

UPnP

- Plug and Play universal (UPnP) no es seguro y es un riesgo de seguridad.
- UPnP permite que los dispositivos se agreguen de forma dinámica a una red inalámbrica sin intervención ni configuración.

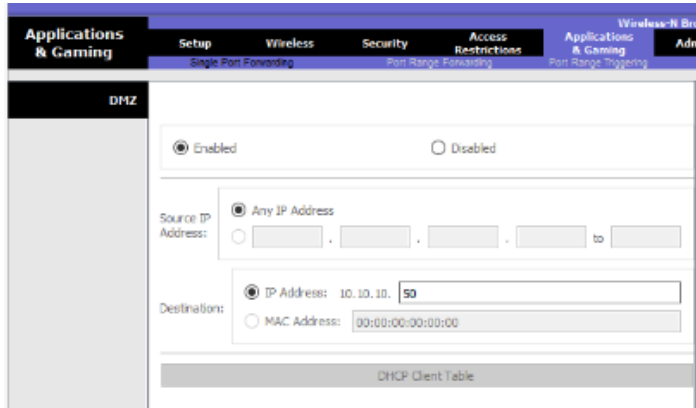
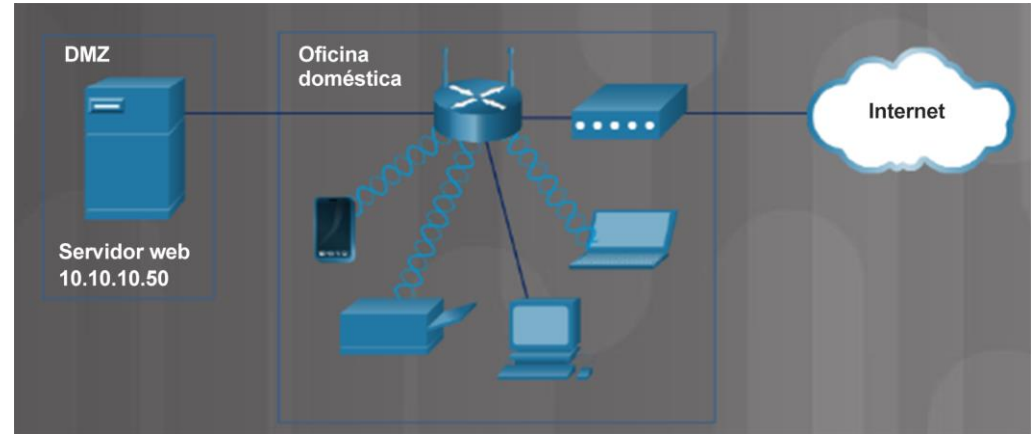
The screenshot displays the UPnP configuration page. On the left, a vertical grey bar contains the label 'Upnp'. The main content area is white and contains the following settings:

- Allowed Remote Ip Address:** A section with two radio button options. The first is 'Any Ip Address'. The second is a numeric IP address field showing '0 . 0 . 0 . 0' followed by 'to' and another '0'.
- Remote Management Port:** A text field containing the value '8080'.
- Upnp:** A section with two radio button options: 'Enabled' (selected) and 'Disabled'.
- Allow Users to Configure:** A section with two radio button options: 'Enabled' (selected) and 'Disabled'.
- Allow Users to Disable Internet Access:** A section with two radio button options: 'Enabled' and 'Disabled' (selected).

Configuración de Firewalls

DMZ

- Una zona desmilitarizada (DMZ, demilitarized zone) es una red que proporciona servicios a una red no confiable.
- Una DMZ suele contener servidores.
- Algunos routers inalámbricos admiten la creación de una DMZ.



Reenvío a puerto asignado

- El reenvío a puerto asignado permite el tráfico a los puertos específicos.
- La activación de puertos permite una apertura temporal en el firewall para permitir datos en puertos específicos de entrada o en un rango de puertos para una aplicación o un juego.

Web Browser

URL <http://10.10.10.1/SingleForward.asp>

Wireless-N Broadband Router

Applications & Gaming Setup Wireless Security Access Restrictions Applications & Gaming Admin

Single Port Forwarding Port Range Forwarding Port Range Forwarding

Single Port

Application Name

None

None

None

None

None

Web Server

External Port	Internal Port	Protocol	To IP Address	Enabled
---	---	---	10.10.10. 0	☐
---	---	---	10.10.10. 0	☐
---	---	---	10.10.10. 0	☐
---	---	---	10.10.10. 0	☐
---	---	---	10.10.10. 0	☐
80	80	TCP	10.10.10. 50	☐
0	0	Both	10.10.10. 0	☐
0	0	Both	10.10.10. 0	☐

Configuración de Firewalls

Filtrado de direcciones MAC

- El filtrado de direcciones MAC se usa para especificar las direcciones MAC que se permiten en la red inalámbrica.

Las direcciones MAC aún no se ingresaron en la lista de filtro de direcciones MAC en la configuración del router inalámbrico de la izquierda.

Wireless Setup Wireless Security Access Restrictions Applications & Gaming

Wireless MAC filter

☒ Enabled ☐ Disabled

☐ Prevent PCs listed below from accessing the wireless network

☒ Permit PCs listed below to access wireless network

Wireless Client List

MAC 01:	00:00:00:00:00:00	MAC 26:	00:00:00:00:00:00
MAC 02:	00:00:00:00:00:00	MAC 27:	00:00:00:00:00:00
MAC 03:	00:00:00:00:00:00	MAC 28:	00:00:00:00:00:00
MAC 04:	00:00:00:00:00:00	MAC 29:	00:00:00:00:00:00
MAC 05:	00:00:00:00:00:00	MAC 30:	00:00:00:00:00:00
MAC 06:	00:00:00:00:00:00	MAC 31:	00:00:00:00:00:00
MAC 07:	00:00:00:00:00:00	MAC 32:	00:00:00:00:00:00
MAC 08:	00:00:00:00:00:00	MAC 33:	00:00:00:00:00:00
MAC 09:	00:00:00:00:00:00	MAC 34:	00:00:00:00:00:00
MAC 10:	00:00:00:00:00:00	MAC 35:	00:00:00:00:00:00

Configuración de Firewalls

Lista blanca y lista negra

- **Listas blancas:** permiten que los usuarios, como los niños o los empleados, accedan a direcciones IP específicas.
- **Listas negras:** bloquean sitios web conocidos

The screenshot shows the 'Access Restrictions' configuration page for an 'Internet Access Policy'. The left sidebar contains a tree view with 'Internet Setup' selected. The main content area is divided into sections: 'Access Policy' (showing '10' and buttons for 'Delete This Entry' and 'Summary'), 'Enter Policy Name' (with 'Whitelist' entered), 'Status' (radio buttons for 'Enabled' and 'Disabled', with 'Enabled' selected), 'Edit List' (with a note 'This Policy applies only to PCs on the List.'), 'Access Restriction' (radio buttons for 'Deny' and 'Allow', with 'Allow' selected), 'Schedule' (checkboxes for 'EveryDay', 'Sun', 'Mon', 'Tue', 'Wed', 'Thu', 'Fri', 'Sat', with 'EveryDay' checked), 'Times' (radio buttons for '24 Hours' and a time range, with '24 Hours' selected), and 'Website Blocking by URL Address' (input fields for 'URL 1' through 'URL 4' and 'Keyword 1' through 'Keyword 3').

Packet Tracer: configuración de ajustes del Firewalls

En esta actividad de Packet Tracer, configurará un router inalámbrico para:

- Confiar en el filtrado MAC para mejorar la seguridad
- Permitir el acceso a un servidor en la DMZ
- Desactivar la DMZ y configurar el soporte para el reenvío a puerto único asignado

Práctica de laboratorio: Configuración de ajustes del Firewall

En esta práctica de laboratorio, configurará los ajustes del firewalls para usar filtrado de direcciones MAC, una DMZ y reenvío a puerto asignado en un router inalámbrico a fin de administrar las conexiones y el tráfico del router inalámbrico.

Configuración de dispositivos de IdC

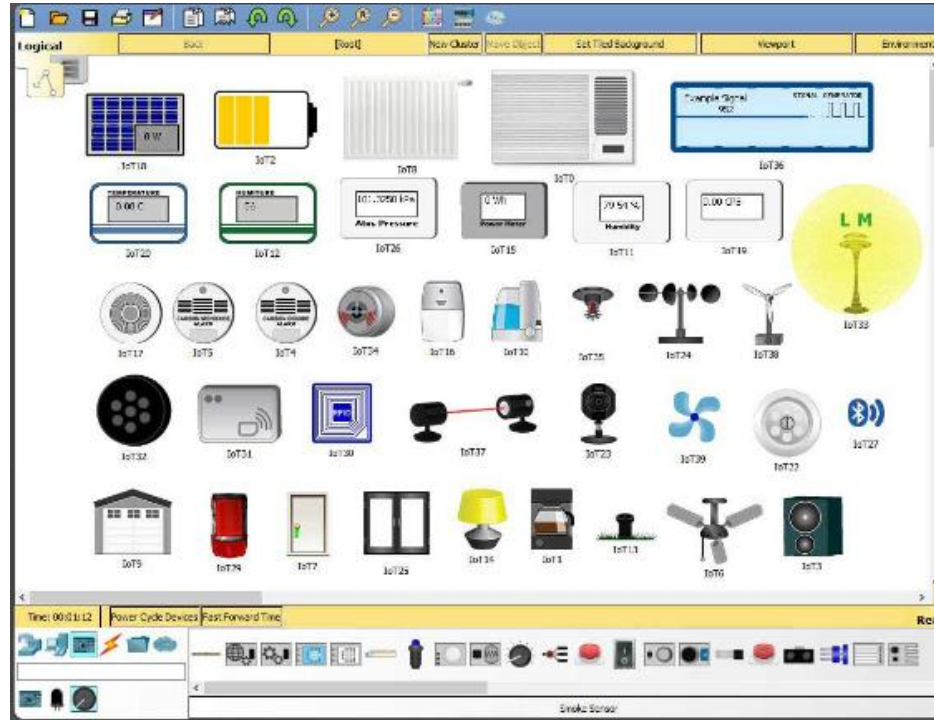
Internet de las cosas

- Internet de las cosas (IdC) puede conectarse a una red preexistente o a una red propia.
- Un hogar inteligente contiene dispositivos de IdC.



Configuración de dispositivos de IdC

Dispositivos de IdC en Packet Tracer

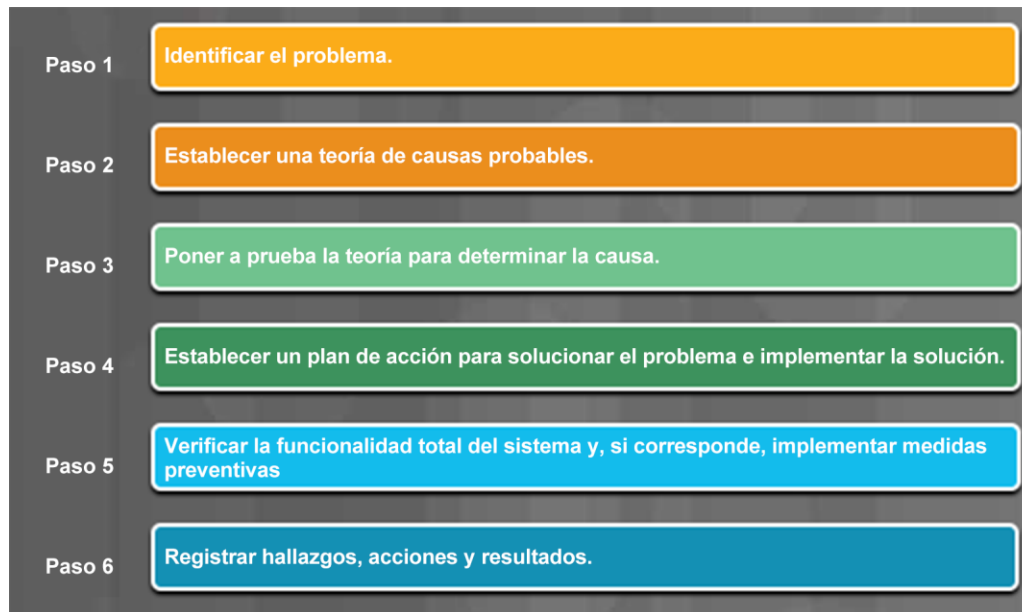


Packet Tracer: configuración de los dispositivos de IdC

En esta actividad, acaba de instalar varios dispositivos de Internet de las cosas en toda la casa y desea configurarlos como un sistema de seguridad doméstica. Configuraré la puerta de enlace residencial para utilizar un sensor de movimiento, probará y restablecerá las características de seguridad, y configurará el aire acondicionado.

6.2 Proceso de resolución de problemas de red

El proceso de solución de problemas



Los seis pasos para solucionar problemas en una red: paso 1

Paso 1. Identificar el problema.

Preguntas abiertas	• ¿Qué problemas tiene con su dispositivo? • ¿Qué software se instaló en su dispositivo recientemente? • ¿Qué hacía cuando se identificó el problema? • ¿Qué mensaje de error recibió? • ¿Qué tipo de conexión de red utiliza el dispositivo?
Preguntas cerradas	• ¿Alguien más utilizó su dispositivo recientemente? • ¿Puede ver las impresoras o los archivos compartidos? • ¿Cambió la contraseña recientemente? • ¿Puede acceder a Internet? • ¿Está conectado a la red en este momento? • ¿Alguien más tiene este problema? • ¿Hubo algún cambio en el entorno o la infraestructura en la red?

Los problemas de red pueden ser simples o complejos, y pueden ser el resultado de una combinación de problemas de hardware, software y conectividad. Como técnico, debe desarrollar un método lógico y coherente para diagnosticar problemas de red mediante la eliminación de un problema por vez.

Por ejemplo, para evaluar el problema, determine cuántos dispositivos de la red lo tienen. Si hay un problema con un dispositivo, comience con ese dispositivo. Si el problema es con todos los dispositivos, inicie el proceso de solución de problemas en el dispositivo de sala de red donde se conectan todos los dispositivos.

El primer paso del proceso de solución de problemas consiste en identificar el problema. Utilice la lista de preguntas abiertas y cerradas como punto de partida para recopilar información del cliente.

Los seis pasos para solucionar problemas en una red: paso 2

Paso 2. Establecer una teoría de causas probables.

Causas comunes de los problemas de red

- Conexiones de cables flojas.
- La NIC no se instaló correctamente.
- El ISP no funciona.
- Baja intensidad de señal inalámbrica.
- La dirección IP no es válida.
- Problema del servidor DNS
- Problema en el servidor DHCP.

Después de hablar con el cliente, puede establecer una teoría de causas probables. La lista anterior brinda algunas causas probables comunes de los problemas de red.

Los seis pasos para solucionar problemas de una red: paso 3

Paso 3. Poner a prueba la teoría para determinar la causa.

Pasos comunes para determinar la causa

- Verificar que todos los cables estén conectados en las ubicaciones correctas.
- Desconectar y volver a conectar los cables y los conectores.
- Reiniciar la PC o el dispositivo de red.
- Iniciar sesión con un usuario diferente.
- Reparar o volver a habilitar la conexión de red.
- Comunicarse con el administrador de red.
- Hacer ping al gateway predeterminado del dispositivo.
- Acceder a una página web remota, como <http://www.cisco.com>.

Una vez que haya elaborado algunas teorías sobre el problema, ponga a prueba dichas teorías para determinar la causa del problema. La lista anterior muestra algunos procedimientos rápidos que puede utilizar para determinar la causa exacta del problema o, incluso, resolverlo. Si el problema se corrige con un procedimiento rápido, puede verificar la funcionalidad total del sistema. Si el problema no se corrige con un procedimiento rápido, quizá deba continuar investigando el problema para establecer la causa exacta.

Los seis pasos para solucionar problemas de una red: paso 4

Paso 4. Establecer un plan de acción para solucionar el problema e implementar la solución.

Si no logró solucionar el problema en el paso anterior, deberá realizar una investigación más exhaustiva para implementar la solución.

- Registros de reparaciones del servicio de asistencia técnica.
- Otros técnicos.
- Sitios web de preguntas frecuentes de los fabricantes.
- Sitios web técnicos.
- Grupos de noticias.
- Manuales de computadoras.
- Manuales de dispositivos.
- Foros en línea.
- Búsquedas en Internet.

Luego de determinar la causa exacta del problema, defina un plan de acción para resolverlo e implementar la solución. La lista anterior muestra algunos orígenes para que pueda utilizar para recopilar información adicional y resolver un problema.

Los seis pasos para solucionar problemas de una red: paso 5

Paso 5. Verificar la funcionalidad total del sistema y, si corresponde, implementar medidas preventivas.

Verificar la funcionalidad total del sistema y, si corresponde, implementar medidas preventivas

- Utilice el comando **ipconfig /all** para visualizar la información de las direcciones IP de todos los adaptadores de red.
- Utilice el comando **ping** para revisar la conectividad de red. Esto envía un paquete a la dirección especificada y muestra la información de respuesta.
- Verifique que el dispositivo pueda acceder a los recursos autorizados, como los servidores de correo electrónico de la empresa y a Internet.
- Investigue los comandos adicionales o solicite ayuda a un supervisor con otras utilidades de prueba.

Una vez que haya corregido el problema, verifique la funcionalidad total y, si corresponde, implemente medidas preventivas. La lista anterior muestra algunos pasos para verificar la solución.

Los seis pasos para solucionar problemas de una red: paso 6

Paso 6. Registrar hallazgos, acciones y resultados.

Registrar hallazgos, acciones y resultados.

- Analizar la solución implementada con el cliente.
- Solicitarle al cliente que verifique que se haya solucionado el problema.
- Proporcionarle todos los documentos pertinentes al cliente.
- Registrar los pasos que siguió para resolver el problema en la solicitud de trabajo y en el registro diario del técnico.
- Registrar todos los componentes utilizados en la reparación.
- Registrar el tiempo que le llevó resolver el problema.

En el último paso del proceso de solución de problemas, documente los hallazgos, las acciones y los resultados, como se muestra en la lista anterior.

Problemas y soluciones comunes para redes

Identificar del problema

Las luces LED de la NIC no están encendidas.

El usuario no puede utilizar Shell seguro (SSH) para acceder a un dispositivo remoto.

El dispositivo no detecta el router inalámbrico.

Una computadora con Windows tiene una dirección IPv4 169.254.x.x.

Un dispositivo remoto no responde a una solicitud de PIN.

Un usuario puede acceder a la red local, pero no puede acceder a Internet.

La red funciona completamente pero el dispositivo inalámbrico no puede conectarse a la red.

Los recursos locales, como los archivos compartidos o las impresoras, no están disponibles.

Las luces LED de la NIC no están encendidas.

Causas probables

- El cable de red está desconectado o está dañado.
- La NIC está dañada.

Soluciones posibles

- Reemplace la conexión de red o vuelva a conectarla a la computadora.
- Reemplace la NIC.

Ver PDF

Problemas y soluciones avanzados para las conexiones de red

Identificar el problema

Un dispositivo se puede conectar a un dispositivo de red mediante la dirección IP, pero no mediante el nombre de host.

El dispositivo no obtiene o renueva la dirección IP en la red.

Se muestra un mensaje de conflicto de dirección IP al conectar un dispositivo nuevo a la red.

Un dispositivo tiene acceso a la red, pero no a Internet.

Los usuarios experimentan velocidades bajas de transferencia, potencia débil de la señal y conectividad intermitente en la red inalámbrica.

Un dispositivo se puede conectar a un dispositivo de red mediante la dirección IP, pero no mediante el nombre de host.

Causas probables	Soluciones posibles
El nombre de host es incorrecto.	Volver a ingresar el nombre de host.
La configuración del DNS es incorrecta.	Volver a ingresar la dirección IP del servidor DNS.
El servidor DNS no funciona.	Reiniciar el servidor DNS.

Ver PDF

Problemas y soluciones de red

Problemas y soluciones avanzados para las conexiones de FTP e Internet segura

Identificar el problema

Un usuario no puede acceder al servidor FTP.

El software de cliente FTP no encuentra el servidor FTP.

Un dispositivo no puede acceder a un sitio HTTPS específico.

Un usuario no puede acceder al servidor FTP.

Causas probables	Soluciones posibles
El firewall en el router bloquea el FTP.	Asegurarse de que los puertos 20 y 21 estén permitidos a través del firewall saliente del router.
El firewall de Windows bloquea el FTP.	Asegurarse de que los puertos 20 y 21 estén permitidos a través del firewall saliente de Windows.
Se alcanzó la cantidad máxima de usuarios.	Aumentar la cantidad máxima de usuarios de FTP en el servidor FTP simultáneamente.

Ver PDF

Problemas y soluciones avanzados con herramientas de red

Identificar el problema

Un dispositivo de una red no puede hacer ping a un dispositivo de otra red.

La computadora no se puede conectar a una computadora remota mediante Telnet.

El comando nslookup indica que "no se puede encontrar el nombre del servidor para la dirección {dirección IP}: tiempo de espera agotado" (donde dice dirección IP...

El comando ipconfig /release o ipconfig /renew genera el mensaje "No se puede realizar ninguna operación..."

El comando ipconfig /release o ipconfig /renew genera el siguiente mensaje: "Error en la operación. No hay ningún adaptador..."

Un dispositivo de una red no puede hacer ping a un dispositivo de otra red.

Causas probables	Soluciones posibles
Hay un enlace roto entre las dos redes.	Utilizar tracert para ubicar el enlace que no funciona y repararlo.
Se bloquea el protocolo de mensajes de control de Internet (ICMP) en el router.	Configurar el router para que acepte las solicitudes de eco y las respuestas de eco de ICMP.
ICMP se bloquea en los firewalls de Windows.	Configurar el firewall de Windows para que acepte las solicitudes de eco y las respuestas de eco de

Ver PDF

Práctica de laboratorio: Solución de problemas de red

En esta práctica de laboratorio, deberá diagnosticar las causas de los problemas de red y resolverlos.

6.3 Resumen del capítulo

Capítulo 6: Resumen de redes aplicadas

6.1 Conexión de un dispositivo a una red

- Configurar dispositivos para redes cableadas e inalámbricas.
 - Explicar la asignación de direcciones MAC e IP para las redes de computadoras.
 - Configurar una NIC para redes cableadas e inalámbricas.
 - Configurar las redes inalámbricas en una LAN pequeña.
 - Configurar los ajustes del Firewall.
 - Configurar los dispositivos de IdC.

6.2 Solución de problemas de red

- Identificar y resolver problemas relacionados con redes.
 - Explicar los seis pasos del proceso de resolución de problemas de red.
 - Solucionar los problemas comunes y avanzados relacionados con las redes.

