Official Cert Guide

Practice Tests

Flash Cards

Study Planner

Review Exercises

Cisco Certified Support Technician (CCST)

IT Support 100-140

Mark Smith, CCST
David Bayne, CCAI
John Pickard, CCAI

ciscopress.com

Cisco Certified Support Technician (CCST) IT Support 100-140 Official Cert Guide

Companion Website and Pearson Test Prep Access Code

Access interactive study tools on this book's companion website, including practice test software, review exercises, Key Term flash card application, a study planner, and more!

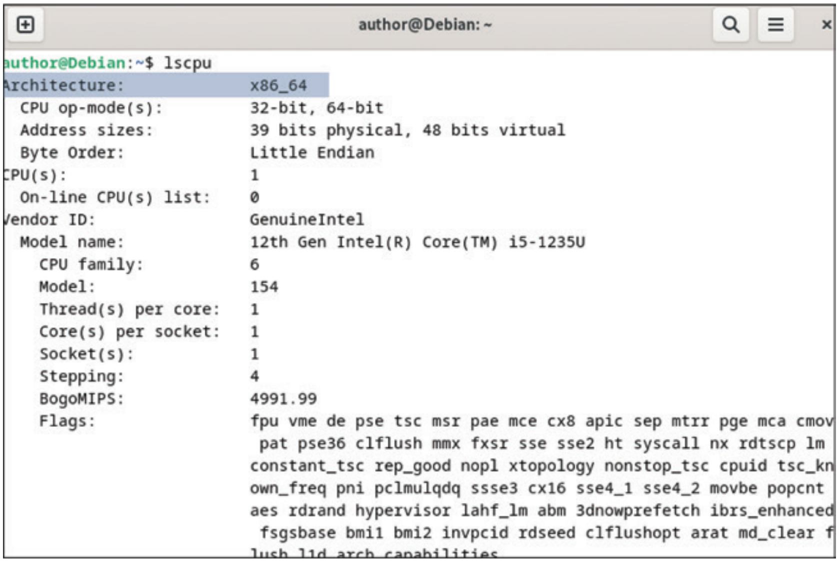
To access the companion website, simply follow these steps:

1. Go to www.ciscopress.com/register.
2. Enter the print book ISBN: **9780135403921**.
3. Answer the security question to validate your purchase.
4. Go to your account page.
5. Click on the **Registered Products** tab.
6. Under the book listing, click on the **Access Bonus Content** link.

Note that you must register your book by December 31, 2028 to access the available bonus content.

When you register your book, your Pearson Test Prep practice test access code will automatically be populated with the book listing under the Registered Products tab. You will need this code to access the practice test that comes with this book. You can redeem the code at **PearsonTestPrep.com**. Simply choose Pearson IT Certification as your product group and log into the site with the same credentials you used to register your book. Click the **Activate New Product** button and enter the access code. More detailed instructions on how to redeem your access code for both the online and desktop versions can be found on the companion website.

If you have any issues accessing the companion website or obtaining your Pearson Test Prep practice test access code, you can contact our support team by going to **pearsonitp.echelp.org.**



```
author@Debian:~$ lscpu
Architecture:             x86_64
  CPU op-mode(s):         32-bit, 64-bit
  Address sizes:          39 bits physical, 48 bits virtual
  Byte Order:             Little Endian
CPU(s):                   1
  On-line CPU(s) list:    0
Vendor ID:                GenuineIntel
  Model name:             12th Gen Intel(R) Core(TM) i5-1235U
    CPU family:           6
    Model:                154
    Thread(s) per core:   1
    Core(s) per socket:   1
    Socket(s):            1
    Stepping:             4
    BogoMIPS:             4991.99
    Flags:                fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov
                           pat pse36 clflush mmx fxsr sse sse2 ht syscall nx rdtscp lm
                          constant_tsc rep_good nopl xtopology nonstop_tsc cpuid tsc_kn
                          own_freq pni pclmulqdq ssse3 cx16 sse4_1 sse4_2 movbe popcnt
                          aes rdrand hypervisor lahf_lm abm 3dnowprefetch ibrs_enhanced
                           fsgsbase bmi1 bmi2 invpcid rdseed clflushopt arat md_clear f
                          lush l1d arch_capabilities
```

Figure 3-7 *A Linux Terminal Showing the Results of the* lscpu *Command*

IP Addresses

IP addresses enable devices to communicate on networks. Part of OSI Layer 3, the TCP/IP Network layer, these are logical addresses that provide a way for devices to find one another on the network. There are two parts: network and host. The network portion allows the network devices such as routers to know which network segment contains the device, and the host portion identifies the specific device. Your network manager (which could be you!) will have divided the network into subnetworks for actual use. Most devices receive their IP addresses automatically via DHCP or similar methods, as discussed later in this chapter. No two devices can have the same public IP address.

There are two major variants of IP addresses in use: IPv4 and IPv6. A device can use one or both, a process called dual stacking. They each have network and host portions.

Key Topic

IPv4

IPv4 consists of 32 binary bits, written in **dotted decimal notation** as **decimal** numbers representing four **binary** octets (like bytes) separated by periods. While older, it is still extremely common, and you will see it in your everyday work as an IT support technician. Eventually, it will be replaced by IPv6, but that is expected to take decades.

Key Topic

Using a Subnet Mask

The network portion of an IPv4 address is defined by the **subnet mask**. This determines whether the destination host is on the local subnetwork or is on a remote network. It is easiest to see this in binary, where the subnet mask is compared against the IPv4 address. For instance, let's consider IP address 192.168.248.143. It translates to 11000000.10101000.111 11000.10001111 in binary. The decimals are here to make the binary easier to read, but the computer doesn't use them:

```
11000000.10101000.11111000.10001111 (192.168.248.143)
```

Now let's look at the subnet mask. If it has a subnet mask of 255.255.255.0, also written as /24, the binary for that would look like 11111111.11111111.11111111.00000000, where the ones represent the network and the zeros represent the host portion of the subnet mask:

```
11111111.11111111.11111111.00000000 (255.255.255.0)
```

Now, let's line these up together, and you can see where the network and host portions of the IPv4 address line up:

```
11000000.10101000.11111000.10001111

11111111.11111111.11111111.00000000
```

The system will combine them together in a process called ANDing; if both values are ones, the one is kept; if either value is zero, the value becomes zero. The network that this device belongs to, then, is easy to see. In this case, it is 11000000.10101000.11111000.00000000/24 (192.168.248.0/24) (because you always have to tell your readers what the subnet mask is).

Another way of saying this is: "Host 192.168.248.148/24 is on network 192.168.248.0/24."

Why is this information important? It tells us which other devices are also on the same network. Any other device on network 192.168.248.0/24 is local and can be connected to directly. Connecting to any device outside of the local network requires you to go through a gateway router (most often called a **default gateway**) because those hosts are not on the same network as this device. You need to ensure that your router's default gateway address is in the same subnet with your device. This default gateway is your network's egress point to the rest of the world; if it isn't configured correctly, your device can't get its packets out.

Key Topic

Public vs. Private IPv4

By using **private IPv4 addresses**, an organization can use as many IPv4 addresses as they need internally and needs only one public IPv4 address that everyone shares. This approach substantially reduces the need for public IPv4 addresses, which have largely been exhausted. Many organizations use this approach for security reasons as well, since devices using private IPv4 addresses are "invisible" to devices outside the organizational network without translation.

For this reason, it is not uncommon to have the same 192.168.x.x range at your home or small business and at your friend's house; each network uses the same IPv4 RFC 1918 private address range. You could get the same exact IPv4 address in these locations without it being an actual problem.

The IPv4 RFC 1918 private address ranges include

Class A: 10.0.0.0 to 10.255.255.255

Class B: 172.16.0.0 to 172.31.255.255

Class C: 192.168.0.0 to 192.168.255.255

Network Address Translation

A process called **Network Address Translation (NAT)** "translates" the private range into a public range before it goes onto the public Internet. This is generally done by a router at the network edge. The NAT router keeps track of which device has asked for which public service and automatically retranslates and reroutes packets appropriately.

There are a lot of addresses available. IT support technicians need to know them in order to tell whether a device is using a private or public IP address, so you know to look at NAT translation as a possible cause of trouble.

IPv6

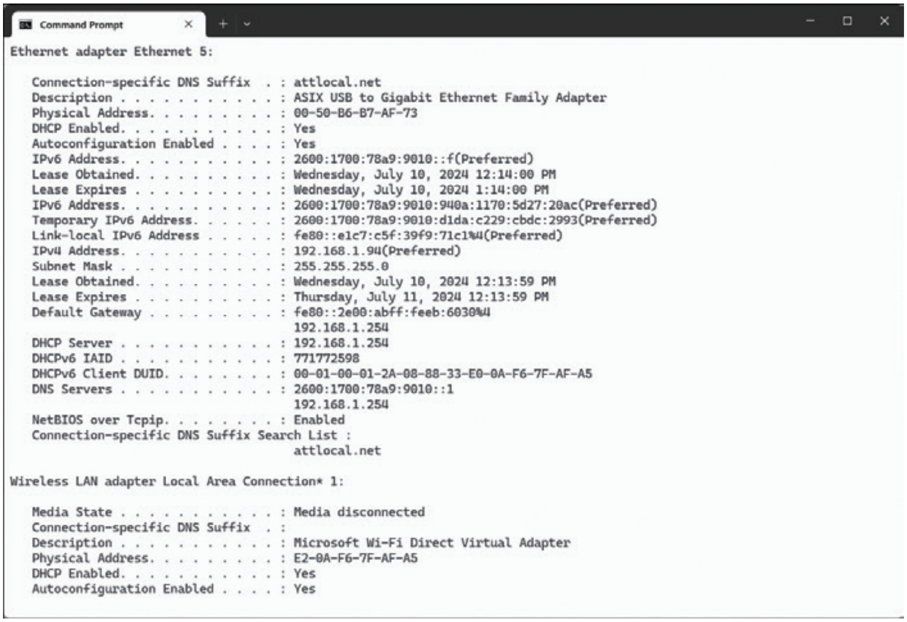
Key Topic

IPv6 is newer than IPv4. It consists of 128-bit addresses, written as eight groups of four **hexadecimal** (base 16) digits each, separated by colons and shortened where possible, because even in hexadecimal these numbers get long. For example, *2001:0db8:0000:0000:0000:8a2e:0370:7334* can be shortened to become *2001:db8::8a2e:370:7334*.

The rules for shortening IPv6 addresses are straightforward: (1) Remove leading zeros. If an octet has zeros at the beginning, just remove them. For instance, 00f0 becomes f0 without changing the value. But that's not the same as 00f, which *would* change the value. That also lets you shorten 0000 to just a single 0. (2) When you have long sequences of all zeros, replace all of them with a colon. In the example, three sequences are all zeros. All three sets are replaced with a double colon. Remember, though, you can only do this once (otherwise, you wouldn't know how many zeros were removed). That does mean that an address of :: or ::1 is valid (and is actually the loopback address). Compare the IPv6 address in the preceding example, and you'll see how it works in real life.

Finding your IPv4 or IPv6 address is simple and straightforward for most operating systems. For Windows, you will open a command prompt and type **ipconfig /all** to get full information for all your network interfaces. For Mac, you can find it in the System Settings under **Network**, then select **Wi-Fi** or **Ethernet**, then **Details** and scroll down. For Linux systems, open a terminal window and enter the command **ifconfig** or **ip addr** and press Enter. Note that **ifconfig** is deprecated on many Linux systems, so it is not always available.

Figure 3-8 shows a portion of the results of a Windows command prompt running the command **ipconfig /all**. Notice that the hostname is also available here.



```
Ethernet adapter Ethernet 5:

   Connection-specific DNS Suffix  . : attlocal.net
   Description . . . . . . . . . . . : ASIX USB to Gigabit Ethernet Family Adapter
   Physical Address. . . . . . . . . : 00-50-B6-B7-AF-73
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2600:1700:78a9:9010::f(Preferred)
   Lease Obtained. . . . . . . . . . : Wednesday, July 10, 2024 12:14:00 PM
   Lease Expires . . . . . . . . . . : Wednesday, July 10, 2024 1:14:00 PM
   IPv6 Address. . . . . . . . . . . : 2600:1700:78a9:9010:940a:1170:5d27:20ac(Preferred)
   Temporary IPv6 Address. . . . . . : 2600:1700:78a9:9010:d1da:c229:cbdc:2993(Preferred)
   Link-local IPv6 Address . . . . . : fe80::e1c7:c5f:39f9:71c1%4(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.94(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Wednesday, July 10, 2024 12:13:59 PM
   Lease Expires . . . . . . . . . . : Thursday, July 11, 2024 12:13:59 PM
   Default Gateway . . . . . . . . . : fe80::2e00:abff:feeb:6030%4
                                       192.168.1.254
   DHCP Server . . . . . . . . . . . : 192.168.1.254
   DHCPv6 IAID . . . . . . . . . . . : 771772598
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2A-08-88-33-E0-0A-F6-7F-AF-A5
   DNS Servers . . . . . . . . . . . : 2600:1700:78a9:9010::1
                                       192.168.1.254
   NetBIOS over Tcpip. . . . . . . . : Enabled
   Connection-specific DNS Suffix Search List :
                                       attlocal.net

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
   Physical Address. . . . . . . . . : E2-0A-F6-7F-AF-A5
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
```

Figure 3-8 *Running* ipconfig /all *on a Windows Command Line*

MAC Address

Key Topic

The media access control address, called a **MAC address**, is a physical address, represented by Layer 2 of the OSI model and the Network Access layer of the TCP/IP model. Each network interface has its own MAC address, which is used as an address within a network segment. Unlike an IP address, which can be used to identify a device outside of a network segment, a MAC address is used only within a particular network segment and is not routable. To reach a particular device, a packet is addressed with the MAC address as well as the IP address. If the device is in the local network, the MAC address is that of the device and is in the local network, and the packet is sent directly to that device. If the device is in a remote network, the MAC address is that of the default gateway with the remote device's IP address, and the default gateway will forward the packet to the destination.

In general, a MAC address is assigned by a manufacturer and is 48 bits, represented by six groups of two hexadecimal (base 16) digits, separated by hyphens, colons, or spaces. Because they are typically assigned by manufacturers, they are often referred to as *burned-in* or *physical* addresses. On a particular network segment, you cannot have two devices with the same MAC address, just like you cannot have two devices with the same IP address on an organizational network.

Figure 3-8 shows the MAC address for each interface, referring to it as a physical address. Note that Windows uses the hyphen to separate the octets. Other operating systems may use colons or spaces, but the meaning is the same. You can change MAC addresses if needed, but that is rare and unusual.

Because the MAC address is assigned by the manufacturer, you can generally tell the manufacturer of a device by its MAC address. This tip can help with troubleshooting of devices because it will help you determine if you have the correct network driver for a network device.

Loopback Interface and Localhost

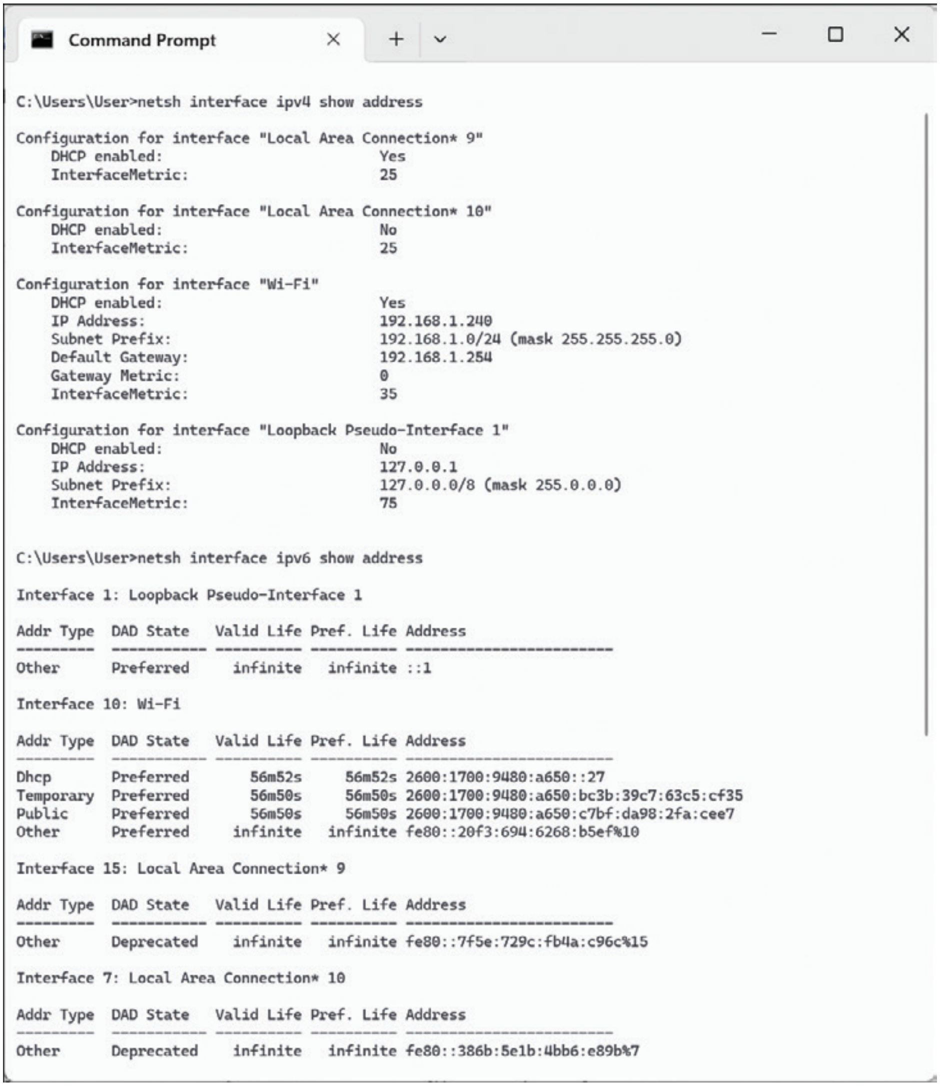
A **loopback** interface is a special software-only interface that mimics a physical interface. Most network-enabled devices have a loopback interface, and many operating systems enable a loopback interface by default, which is active regardless of whether there are any other active network connections. Because the loopback interface is virtual instead of physical, it is always on and can always be relied on to be active and thus addressable during troubleshooting.

The default IPv4 address for the loopback interface technically can be anywhere in the network 127.0.0.0/8, though traditionally you simply use 127.0.0.1, and many devices will only allow this address. This IPv4 address is named **localhost** by default.

The default IPv6 address for the loopback interface is ::1/128. Note that the /128 means that there is just one host on the network, and except for the one at the far right in binary, it is all zeros, as indicated by the double colon. As with all interfaces under IPv6, additional IPv6 addresses can be assigned to the loopback port as well.

To see your loopback interface in Windows, you will use the **netsh interface [ipv4 | ipv6] show address** command, which will show the IPv4 or IPv6 addresses of all interfaces, including the loopback interface. The loopback interface is listed as Loopback Pseudo-Interface.

Figure 3-9 shows **netsh interface ipv4 show address** and **netsh interface ipv6 show address** being run, clipped showing the loopback interfaces.



```
C:\Users\User>netsh interface ipv4 show address

Configuration for interface "Local Area Connection* 9"
    DHCP enabled:                         Yes
    InterfaceMetric:                      25

Configuration for interface "Local Area Connection* 10"
    DHCP enabled:                         No
    InterfaceMetric:                      25

Configuration for interface "Wi-Fi"
    DHCP enabled:                         Yes
    IP Address:                           192.168.1.240
    Subnet Prefix:                        192.168.1.0/24 (mask 255.255.255.0)
    Default Gateway:                      192.168.1.254
    Gateway Metric:                       0
    InterfaceMetric:                      35

Configuration for interface "Loopback Pseudo-Interface 1"
    DHCP enabled:                         No
    IP Address:                           127.0.0.1
    Subnet Prefix:                        127.0.0.0/8 (mask 255.0.0.0)
    InterfaceMetric:                      75


C:\Users\User>netsh interface ipv6 show address

Interface 1: Loopback Pseudo-Interface 1

Addr Type  DAD State   Valid Life Pref. Life Address
---------  ----------- ---------- ---------- ------------------------
Other      Preferred     infinite   infinite ::1

Interface 10: Wi-Fi

Addr Type  DAD State   Valid Life Pref. Life Address
---------  ----------- ---------- ---------- ------------------------
Dhcp       Preferred       56m52s     56m52s 2600:1700:9480:a650::27
Temporary  Preferred       56m50s     56m50s 2600:1700:9480:a650:bc3b:39c7:63c5:cf35
Public     Preferred       56m50s     56m50s 2600:1700:9480:a650:c7bf:da98:2fa:cee7
Other      Preferred     infinite   infinite fe80::20f3:694:6268:b5ef%10

Interface 15: Local Area Connection* 9

Addr Type  DAD State   Valid Life Pref. Life Address
---------  ----------- ---------- ---------- ------------------------
Other      Deprecated    infinite   infinite fe80::7f5e:729c:fb4a:c96c%15

Interface 7: Local Area Connection* 10

Addr Type  DAD State   Valid Life Pref. Life Address
---------  ----------- ---------- ---------- ------------------------
Other      Deprecated    infinite   infinite fe80::386b:5e1b:4bb6:e89b%7
```

Figure 3-9 *A Command Prompt Running the* **netsh interface ipv4 show** *Address and* **netsh interface ipv6 show** *Address Commands*

Basic End-Device Network Connectivity

Modern devices are connected to one another to facilitate communication. While there are many methods to do this, building and campus networks can be divided into a handful of large groups: local area networks (LANs) and wireless local area networks (WLANs). Regardless of size, the key point is that they are in a single, limited area—defined by a campus or building. If connection is made beyond that, the term wide area network (WAN) or metropolitan area network (MAN) is used. A WAN or MAN will connect multiple LAN networks together.

LAN vs. WLAN

Devices are connected in many ways, but the main difference is important: wired versus wireless. That is the focus of the following sections.

LAN

Key Topic

A **local area network (LAN)** refers to a collection of devices connected in one physical location, such as a building, office, or home, and overseen by one central administrative organization—like you, the IT support technician. LANs can be small or large and may have several segments.

These segments can be connected via copper cabling, usually Category 5, 6, or 7, or via fiber-optic cabling, and are interconnected using network switches.

LANs are connected to WANs using routers. In home and small business networks, they often use network devices containing both routers and switches, and many of these also contain wireless access points.

Standard icons describe each of these devices, as shown in the following figures. Figure 3-10 shows a standard network router icon. Figure 3-11 shows a standard network switch icon.

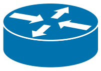


Figure 3-10 *The Standard Icon for a Router*

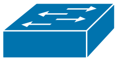


Figure 3-11 *The Standard Icon for a Workgroup Switch*

WLAN

Key Topic

A **wireless local area network (WLAN)** refers to a segment of a LAN connected by Wi-Fi or other wireless connection. Wi-Fi connections are radio based, but some other types of WLAN are optical, usually infrared. The most important characteristic is that they connect devices to a LAN via a wireless access point, either as a dedicated device called a wireless bridge or via a combined gateway device. Many home and small business networks use combined wireless and wired network devices.

The **service set identifier (SSID)** is the name by which your WLAN is known. Often this is the same as the overall network name, but that isn't required. Most home and small business networks use the default SSID configured by their ISP.

Many individuals and most large organizations will customize their SSID. You may use up to 32 alphanumeric characters to customize the SSID, and these names are case sensitive. Spaces and special characters are permitted but discouraged in an SSID name due to potential incompatibilities with some devices. Hiding your SSID is possible but does not provide any security advantages.

You should secure your SSID with the strongest encryption available. As of this writing, that is WPA2 and WPA3. Avoid the oldest, WEP and WPA, unless you absolutely must. In that case, you should put devices that require the older WEP and WPA encryption into their own