# Troubleshooting IP Addressing

The tools covered herein and the skills you'll gain after learning how to use them will give you a huge advantage when taking the Cisco certification exam. Even more importantly, they'll give you a serious edge in the professional real world! Working through this chapter will hone your knowledge of IP addressing and networking, while refining the essential skills you've attained so far.

Because running into trouble now and then in networking is a given, being able to troubleshoot IP addressing is a vital skill.

Example 1

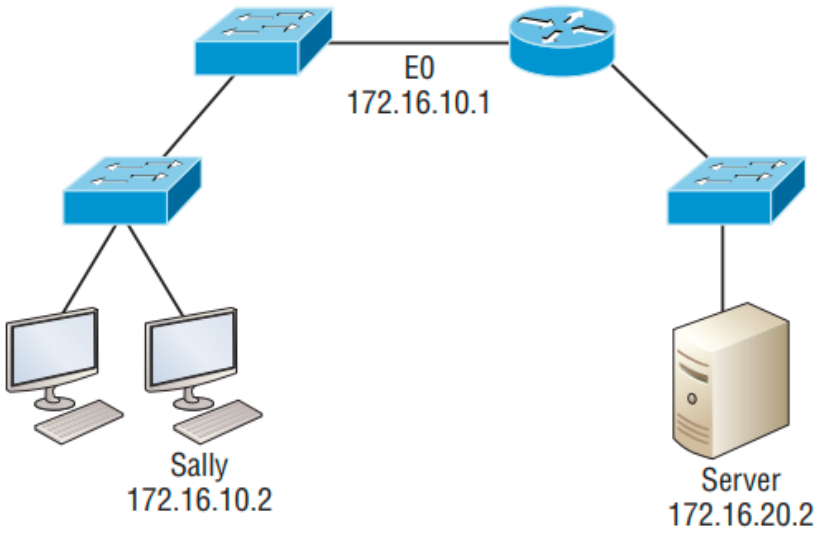



*Figure 1Basic IP troubleshooting*

Sally can't log in to the Windows server.

Her first step in troubleshooting would be to verify the network.

Let's walk through the Cisco Way of troubleshooting using a clear step-by-step approach. These steps are pretty simple—start by imagining you're at a customer host who's complaining they can't communicate to a server, which just happens to be on a remote network. In this scenario, here are the four troubleshooting steps Cisco recommends:

1. Open a Command window and ping 127.0.0.1. This is the diagnostic, or loopback, address, and if you get a successful ping, your IP stack is considered initialized. If it fails, then you have an IP stack failure and need to reinstall TCP/IP on the host:
   C:\>ping 127.0.0.1
   Pinging 127.0.0.1 with 32 bytes of data:
   Reply from 127.0.0.1: bytes=32 time
   Reply from 127.0.0.1: bytes=32 time
   Reply from 127.0.0.1: bytes=32 time
   Reply from 127.0.0.1: bytes=32 time
   Ping statistics for 127.0.0.1:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
   Approximate round trip times in milli-seconds:
   Minimum = 0ms, Maximum = 0ms, Average = 0ms
2. From the Command window, ping the IP address of the local host (we'll assume correct configuration here, but always check the IP configuration too!). If that's successful, your network interface card (NIC) is functioning. If it fails, there is a problem with the NIC. Just so you know, success here doesn't necessarily mean that a cable is plugged into the NIC, only that the IP protocol stack on the host can communicate to the NIC via the LAN driver:

   C:\>ping 172.16.10.2
   Pinging 172.16.10.2 with 32 bytes of data:
   Reply from 172.16.10.2: bytes=32 time
   Reply from 172.16.10.2: bytes=32 time

Reply from 172.16.10.2: bytes=32 time
Reply from 172.16.10.2: bytes=32 time
Ping statistics for 172.16.10.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms

3. From the Command window, ping the default gateway (router). If the ping works, it means that the NIC is plugged into the network and can communicate on the local network. If it fails, you have a local physical network problem that could be anywhere from the NIC to the router:
   C:\>ping 172.16.10.1
   Pinging 172.16.10.1 with 32 bytes of data:
   Reply from 172.16.10.1: bytes=32 time
   Reply from 172.16.10.1: bytes=32 time
   Reply from 172.16.10.1: bytes=32 time
   Reply from 172.16.10.1: bytes=32 time
   Ping statistics for 172.16.10.1:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
   Approximate round trip times in milli-seconds:
   Minimum = 0ms, Maximum = 0ms, Average = 0ms
4. If steps 1 through 3 were successful, try to ping the remote server. If that works, then you know that you have IP communication between the local host and the remote server. You also know that the remote physical network is working:
   C:\>ping 172.16.20.2
   Pinging 172.16.20.2 with 32 bytes of data:
   Reply from 172.16.20.2: bytes=32 time
   Reply from 172.16.20.2: bytes=32 time
   Reply from 172.16.20.2: bytes=32 time
   Reply from 172.16.20.2: bytes=32 time
   Ping statistics for 172.16.20.2:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
   Approximate round trip times in milli-seconds:
   Minimum = 0ms, Maximum = 0ms, Average = 0ms

If the user still can't communicate with the server after steps 1 through 4 have been completed successfully, you probably have some type of name resolution problem and need to check your Domain Name System (DNS) settings. But if the ping to the remote server fails, then you know you have some type of remote physical network problem and need to go to the server and work through steps 1 through 3 until you find the snag.

## Verify IP Parameters for Operating Systems (OS)

Before we move on to determining IP address problems and how to fix them, let's mention some basic commands that you can use to help troubleshoot your network from a Windows PC, Cisco devices, as well as MAC and Linux hosts. Keep in mind that though these commands may do the same thing, they're implemented differently.

**ping** Uses ICMP echo request and replies to test if a node IP stack is initialized and alive on the network. **traceroute** Displays the list of routers on a path to a network destination by using TTL time-outs and ICMP error messages. This command won't work from a command prompt.

**tracert** Same function as traceroute, but it's a Microsoft Windows command and it won't work on a Cisco router.

**arp** -a Displays IP-to-MAC-address mappings on a Windows PC.

**show ip** arp Same function as arp -a, but displays the ARP table on a Cisco router. Like the commands traceroute and tracert, arp -a and show ip arp these aren't interchangeable through Windows and Cisco.

**ipconfig /all** Used only from a Windows command prompt; shows you the PC network configuration. **ifconfig** Used by MAC and Linux to get the IP address details of the local machine

**ipconfig getifaddr en0** Used to find your IP address if you are connected to a wireless network or use en1 if you are connected to an Ethernet for MAC or Linux.

**curl ifconfig.me** This command will display your global Internet IP address in Terminal for MAC or Linux.

**curl ipecho.net/plain ; echo** This command will display your global Internet IP address in Terminal for MAC or Linux.

Once you've gone through all these steps and, if necessary, used the appropriate commands, what do you do when you find a problem? How do you go about fixing an IP address configuration error? Time to cover the next step—determining and fixing the issue at hand!

## Determining IP Address Problems

It's common for a host, router, or other network device to be configured with the wrong IP address, subnet mask, or default gateway. Because this happens way too often, you've got to know how to find and fix IP address configuration errors.

A good way to start is to draw out the network and IP addressing scheme. If that's already been done, consider yourself lucky because though sensible, it's rarely done. Even if it is, it's usually outdated or inaccurate anyway. So, either way, it's a good idea to bite the bullet and start from scratch.

Once you have your network accurately drawn out, including the IP addressing scheme, you need to verify each host's IP address, mask, and default gateway address to establish the problem. Of course, this is assuming that you don't have a physical layer problem, or if you did, that you've already fixed it.

Example 2

Check out the example illustrated in Figure 2. A user in the sales department calls and tells you that she can't get to ServerA in the marketing department. You ask her if she can get to ServerB in the marketing department, but she doesn't know because she doesn't have rights to log on to that server. What do you do?

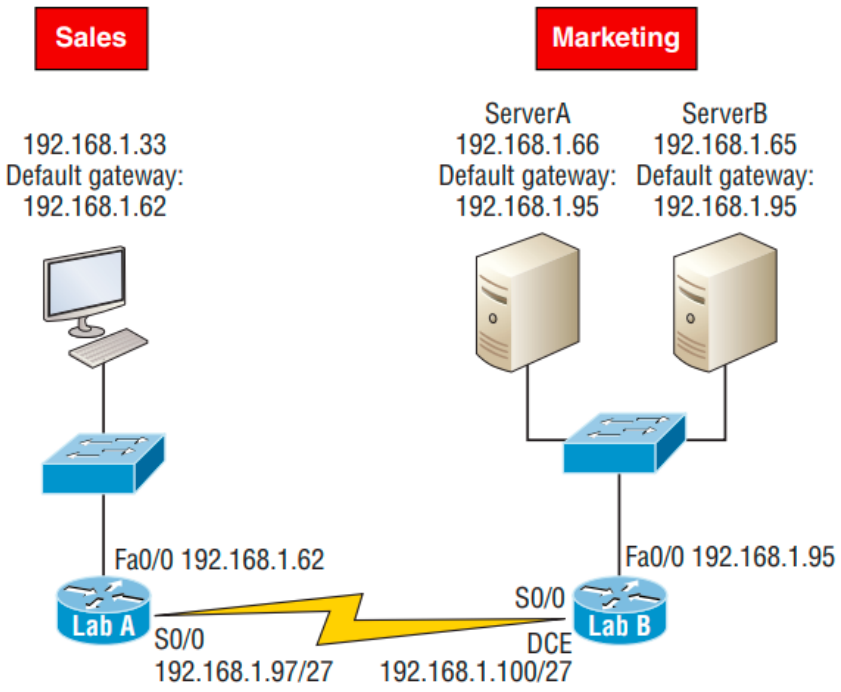



*Figure 2IP address problem 1*

First, guide your user through the four troubleshooting steps you learned in the preceding section. Let's say steps 1 through 3 work but step 4 fails. By looking at the figure, can you determine the problem?

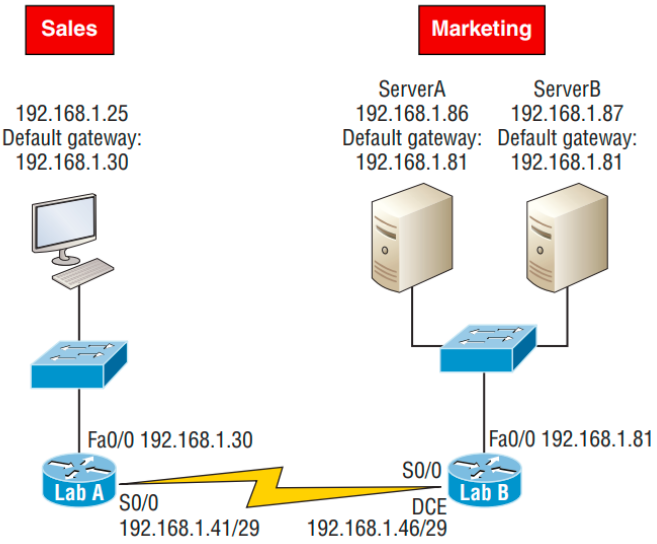
Look for clues in the network drawing. First, the WAN link between the Lab A router and the Lab B router shows the mask as a /27. You should already know that this mask is 255.255.255.224 and determine that all networks are using this mask. The network address is 192.168.1.0. What are your valid subnets and hosts? 256 – 224 = 32, so this makes our subnets 0, 32, 64, 96, 128, etc. So, by looking at the figure, you can see that subnet 32 is being used by the sales department. The WAN link is using subnet 96, and the marketing department is using subnet 64.

Next, you've got to establish what the valid host ranges are for each subnet. From what you've learned already, you should now be able to easily determine the subnet address, broadcast addresses, and valid host ranges. The valid hosts for the Sales LAN are 33 through 62, and the broadcast address is 63 because the next subnet is 64, right? For the Marketing LAN, the valid hosts are 65 through 94 (broadcast 95), and for the WAN link, 97 through 126 (broadcast 127). By closely examining the figure, you can determine that the default gateway on the Lab B router is incorrect. That address is the broadcast address for subnet 64, so there's no way it could be a valid host!

TIP: If you tried to configure that address on the Lab B router interface, you'd receive a bad mask error. Cisco routers don't let you type in subnet and broadcast addresses as valid hosts!

Example 3

A user in the Sales LAN can't get to ServerB. You have the user run through the four basic troubleshooting steps and find that the host can communicate to the local network but not to the remote network. Find and define the IP addressing problem.




If you went through the same steps used to solve the last problem, you can see that first, the WAN link again provides the subnet mask to use— /29, or 255.255.255.248. Assuming classful addressing, you need to determine what the valid subnets, broadcast addresses, and valid host ranges are to solve this problem.

The 248 mask is a block size of 8 (256 – 248 = 8), so the subnets both start and increment in multiples of 8. By looking at the figure, you see that the Sales LAN is in the 24 subnet, the WAN is in the 40 subnet, and the Marketing LAN is in the 80 subnet. Can you see the problem yet? The valid host range for the Sales LAN is 25–30, and the configuration appears correct. The valid host range for the WAN link is 41–46, and this also appears correct. The valid host range for the 80 subnet is 81–86, with a broadcast address of 87 because the next subnet is 88.

ServerB has been configured with the broadcast address of the subnet.

Okay, so now that you can figure out misconfigured IP addresses on hosts, what do you do if a host doesn't have an IP address and you need to assign one?

You need to scrutinize the other hosts on the LAN and figure out the network, mask, and default gateway.

Let's take a look at a couple of examples about how to find and apply valid IP addresses to hosts.

Example 5

*You need to assign a server and router IP addresses on a LAN. The subnet assigned on that segment is 192.168.20.24/29. The router needs to be assigned the first usable address and the server needs the last valid host ID. What is the IP address, mask, and default gateway assigned to the server?*

To answer this, you must know that a /29 is a 255.255.255.248 mask, which provides a block size of 8. The subnet is known as 24, the next subnet in a block of 8 is 32, so the broadcast address of the 24 subnet is 31 and the valid host range is 25–30.

Server IP address: 192.168.20.30

Server mask: 255.255.255.248

Default gateway: 192.168.20.25 (router's IP address)

Example 6

Look at the router's IP address on Ethernet0. What IP address, subnet mask, and valid host range could be assigned to the host?

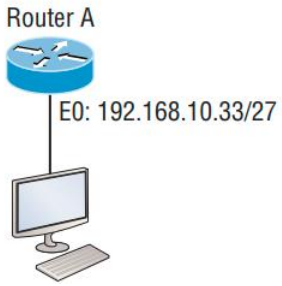



*Figure 3 Find the valid host #1.*

The IP address of the router's Ethernet0 is 192.168.10.33/27. As you already know, a /27 is a 224 mask with a block size of 32. The router's interface is in the 32 subnet. The next subnet is 64, so that makes the broadcast address of the 32 subnet 63 and the valid host range 33–62.

Host IP address: 192.168.10.34–62 (any address in the range except for 33, which is assigned to the router) Mask: 255.255.255.224 Default gateway: 192.168.10.33

Example 7

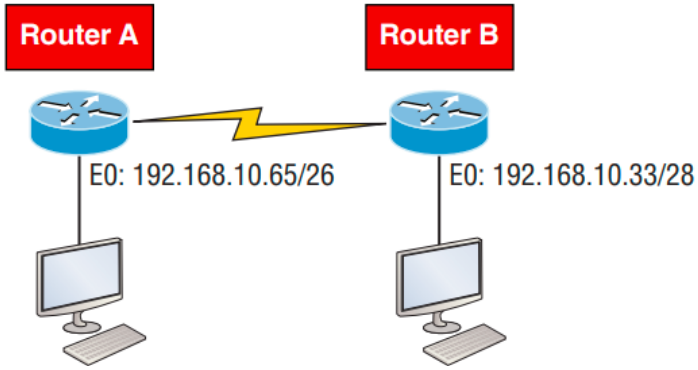



*Figure 4 Find the valid host #2.*

Figure 4 shows two routers with Ethernet configurations already assigned. What are the host addresses and subnet masks of HostA and HostB?

Router A has an IP address of 192.168.10.65/26 and Router B has an IP address of 192.168.10.33/28. What are the host configurations? Router A Ethernet0 is in the 192.168.10.64 subnet and Router B Ethernet0 is in the 192.168.10.32 network.

Host A IP address: 192.168.10.66–126

Host A mask: 255.255.255.192

Host A default gateway: 192.168.10.65

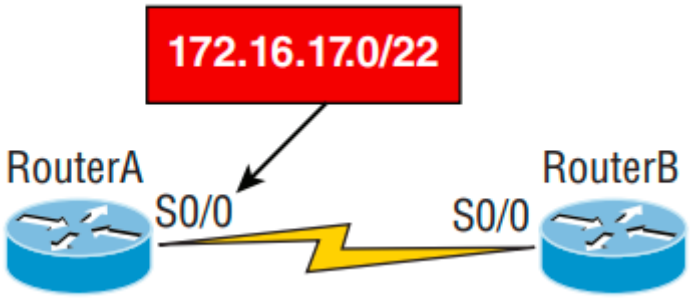
Host B IP address: 192.168.10.34–46

Host B mask: 255.255.255.240

Host B default gateway: 192.168.10.33

Example 8

Figure 5 shows two routers. You need to configure the S0/0 interface on RouterA. The IP address assigned to the serial link on RouterA is 172.16.17.0/22 (No, that is not a subnet address, but a valid host IP address on that interface—most people miss this one). Which IP address can be assigned to the router interface on RouterB?

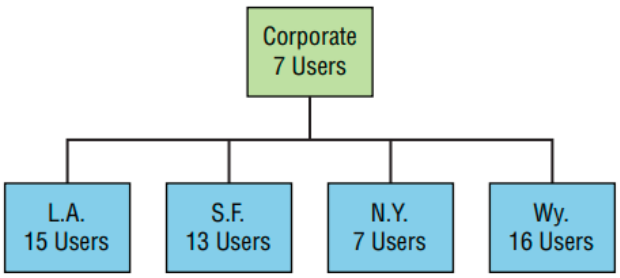



First, know that a /22 CIDR is 255.255.252.0, which makes a block size of 4 in the third octet. Since 17 is listed as the interface IP address, the available range is 16.1 through 19.254, so in this example, the IP address S0/0 on RouterB could be 172.16.18.255 since that's within the range.

*Figure 5 Find the valid host address #3*

Example 9

You need to find a classful network address that has one Class C network ID and you need to provide one usable subnet per city while allowing enough usable host addresses for each city specified in Figure 6. What is your mask?




Actually, this is probably the easiest thing you've done all day! You count 5 subnets needed, and the Wyoming office needs 16 users—always look for the network that needs the most hosts! What block size is needed for the Wyoming office? Your answer is 32. You can't use a block size of 16 because you always have to subtract 2. What mask provides you with a block size of 32? 224 is your answer because this provides 8 subnets, each with 30 hosts.

*Figure 6 Find the valid subnet mask*

Cisco Exam Essentials

**Describe the benefits of variable length subnet masks (VLSMs).**

VLSMs enable the creation of subnets of specific sizes and allow the division of a classless network into smaller networks that do not need to be equal in size. This makes use of the address space more efficient because many times IP addresses are wasted with classful subnetting.

**Understand the relationship between the subnet mask value and the resulting block size and the allowable IP addresses in each resulting subnet.**

The relationship between the classful network being subdivided and the subnet mask used determines the number of possible hosts or the block size. It also determines where each subnet begins and ends and which IP addresses cannot be assigned to a host within each subnet.

**Describe the process of summarization or route aggregation and its relationship to subnetting.**

Summarization is the combining of subnets derived from a classful network for the purpose of advertising a single route to neighboring routers instead of multiple routes, reducing the size of routing tables and speeding the route process.

**Calculate the summary mask that will advertise a single network representing all subnets.**

The network address used to advertise the summary address is always the first network address in the block of subnets. The mask is the subnet mask value that yields the same block size.

**Remember the four diagnostic steps.**

The four simple steps that Cisco recommends for troubleshooting are ping the loopback address, ping the NIC, ping the default gateway, and ping the remote device.

**Identify and mitigate an IP addressing problem.**

Once you go through the four troubleshooting steps that Cisco recommends, you must be able to determine the IP addressing problem by drawing out the network and finding the valid and invalid hosts addressed in your network.

**Understand the troubleshooting tools that you can use from your host and a Cisco router.**

The ping 127.0.0.1 command tests your local IP stack, and tracert is a Windows command to track the path a packet takes through an internetwork to a destination. Cisco routers use the command traceroute, or just trace for short. Don't confuse the Windows and Cisco commands. Although they produce the same output, they don't work from the same prompts. The command ipconfig /all will display your PC network configuration from a DOS prompt, and arp -a (again from a DOS prompt) will display IP-to-MAC-address mapping on a Windows PC.

## Review Questions

1. On a VLSM network, which mask should you use on point-to-point WAN links in order to reduce the waste of IP addresses?
   - **A.** /27
   - **B.** /28
   - **C.** /29
   - **D.** /30
   - **E.** /31

2. If a host is configured with an incorrect default gateway and all the other computers and router are known to be configured correctly, which of the following statements is true?
   - **A.** Host A cannot communicate with the router.
   - **B.** Host A can communicate with other hosts in the same subnet.
   - **C.** With an incorrect gateway, Host A will not be able to communicate with the router or beyond the router but will be able to communicate within the subnet.
   - **D.** Host A can communicate with no other systems.

3. Which of the following troubleshooting steps, if completed successfully, also confirms that the other steps will succeed as well?
   - **A.** Ping a remote computer.
   - **B.** Ping the loopback address.
   - **C.** Ping the NIC.
   - **D.** Ping the default gateway.

4. When a ping to the local host IP address fails, what can you assume?
   - **A.** The IP address of the local host is incorrect.
   - **B.** The IP address of the remote host is incorrect.
   - **C.** The NIC is not functional.
   - **D.** The IP stack has failed to initialize.

5. When a ping to the local host IP address succeeds but a ping to the default gateway IP address fails, what can you rule out? (Choose all that apply.)
   - **A.** The IP address of the local host is incorrect.
   - **B.** The IP address of the gateway is incorrect.
   - **C.** The NIC is not functional.
   - **D.** The IP stack has failed to initialize.

6. What network service is the most likely problem if you can ping a computer by IP address but not by name?
   - **A.** DNS
   - **B.** DHCP
   - **C.** ARP
   - **D.** ICMP

7. When you issue the ping command, what protocol are you using?
   - **A.** DNS
   - **B.** DHCP
   - **C.** ARP
   - **D.** ICMP

8. Which of the following commands displays the networks traversed on a path to a network destination?
   - **A.** `ping`
   - **B.** `traceroute`
   - **C.** `pingroute`
   - **D.** `pathroute`

9. What command generated the output shown below?

```
Reply from 172.16.10.2: bytes=32 time
Reply from 172.16.10.2: bytes=32 time
Reply from 172.16.10.2: bytes=32 time
Reply from 172.16.10.2: bytes=32 time
```

   **A.** `traceroute`
   **B.** `show ip route`
   **C.** `ping`
   **D.** `pathping`

10. What switch must be added to the ipconfig command on a PC to verify DNS configuration?
   **A.** `/dns`
   **B.** `-dns`
   **C.** `/all`
   **D.** `showall`

*Source: CCNA Certification guide by Todd Lammle, 2020, John Wiley & Sons Inc.*