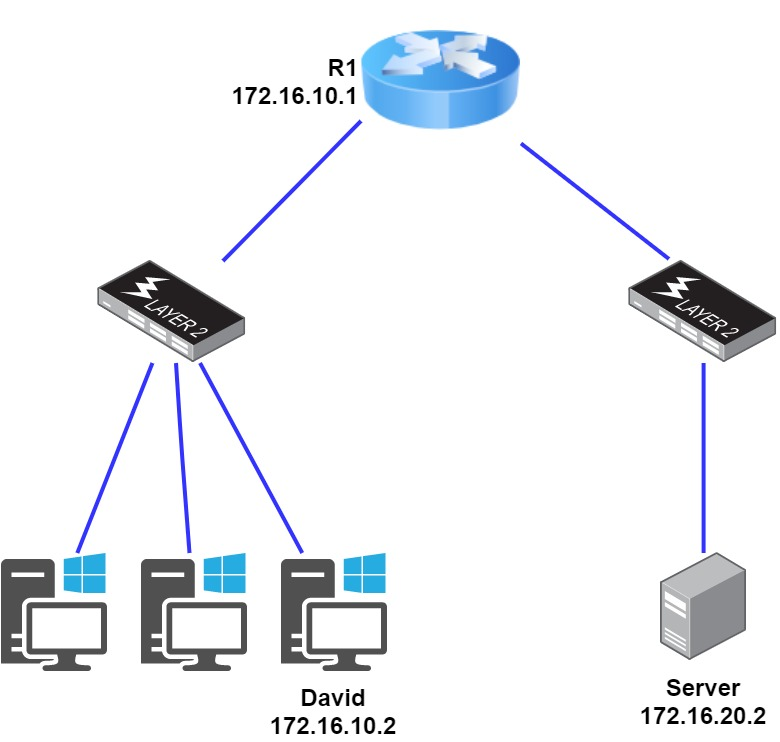
**Troubleshooting IP Addressing (Optional)**

**Troubleshooting IP Addressing**

Troubleshooting IP addressing is obviously an important skill because running into trouble somewhere along the way is pretty much a sure thing, and it’s going to happen to you.

Let’s use the below figure as an example of basic IP trouble— David can’t log in to the Windows server.

***Basic IP troubleshooting***

Let’s get started by going over the basic troubleshooting steps.

1. Open a command prompt window on David’s host, and ping 127.0.0.1.

**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<1ms TTL=128

Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

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

This is the diagnostic(tanılama), or loopback address, and if you get a successful ping, your IP stack is considered to be initialized. If it fails, then you have an IP stack failure and need to reinstall TCP/IP on the host.

**💡Tips:**

* If you ping the loopback address and receive an **“unable to contact IP driver, error code 2”** message, you need to reinstall the TCP/IP protocol suite on the host.

1. Now, from the same command prompt window, ping the IP address of the localhost.

**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<1ms TTL=128

Reply from 172.16.10.2: bytes=32 time<1ms TTL=128

Reply from 172.16.10.2: bytes=32 time<1ms TTL=128

Reply from 172.16.10.2: bytes=32 time<1ms TTL=128

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

If that’s successful, your network interface card (NIC) is functioning. If it fails, there is a problem with the NIC.

1. From the command prompt window, ping the default gateway (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<1ms TTL=128

Reply from 172.16.10.1: bytes=32 time<1ms TTL=128

Reply from 172.16.10.1: bytes=32 time<1ms TTL=128

Reply from 172.16.10.1: bytes=32 time<1ms TTL=128

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

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.

1. If steps 1 through 3 were successful, try to ping the remote server.

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<1ms TTL=128

Reply from 172.16.20.2: bytes=32 time<1ms TTL=128

Reply from 172.16.20.2: bytes=32 time<1ms TTL=128

Reply from 172.16.20.2: bytes=32 time<1ms TTL=128

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

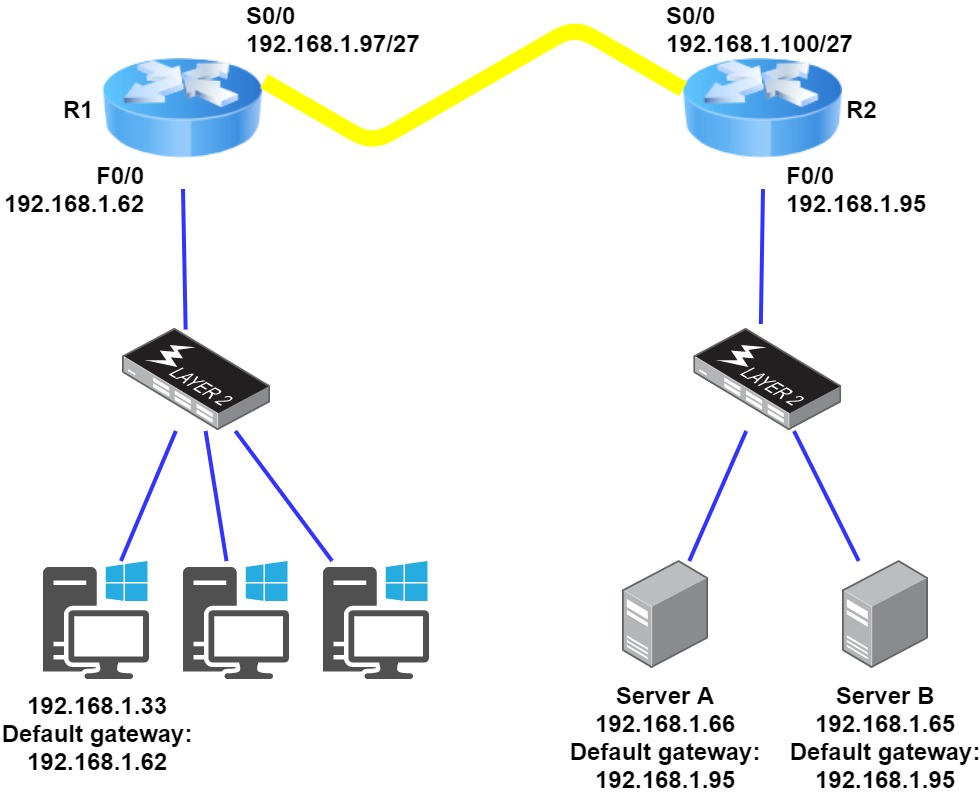
If that works, then you know that you have IP communication between the local host and the remote server. You also know that the remote physical network is working.

If the user still can’t communicate with the server after steps 1 through 4 are successful, 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.

**Determining IP Address Problems-1**

It’s common for a host, router, or other [network devices](https://lms.clarusway.com/mod/resource/view.php?id=13690) to be configured with the wrong IP address, subnet mask, or default gateway. Because this happens way too often, in this example you will learn how to both determine and fix IP address configuration errors.

After you’ve worked through the four basic steps of troubleshooting and determined there’s a problem, you obviously then need to find and fix it. 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 determine the problem. Let’s check out the below example illustration. A user calls and tells you that he can’t get to Server A. You ask him if he can get to Server B in the marketing department, but he doesn’t know because he doesn’t have the rights to log on to that server.



**IP address problem**

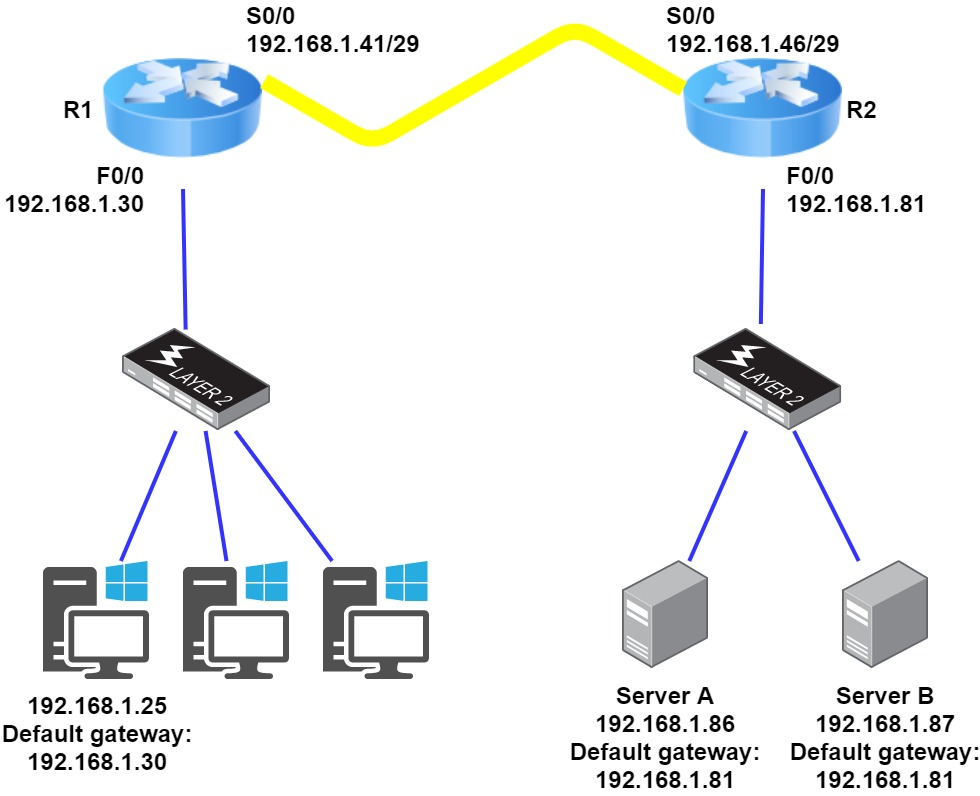
You ask the client to go through the four troubleshooting steps that you learned about in the preceding(önceki) section. Steps 1 through 3 work, but step 4 fails. First, the WAN link between the R1 and the R2 shows the mask as a /27. You should already know that this mask is 255.255.255.224 and then determine that all networks are using this mask. The network address is 192.168.1.0. What are our valid subnets and hosts?

256 – 224 = 32,

so this makes our subnets 0, 32, 64, 96, 128, and so on. So, by looking at the figure, you can see that subnet 32 is being used by the clients, the WAN link is using subnet 96, and the servers are using subnet 64. Now you have to determine what the valid host ranges are for each subnet. The valid hosts for the Sales LAN are 33 through 62—the broadcast address is 63 because the next subnet is 64. For the servers, the valid hosts are 65 through 94 (broadcast 95), and for the WAN link, 97 through 126 (broadcast 127). By looking at the figure, you can determine that the default gateway on the Lab\_B router is incorrect. That address is the broadcast address of the 64 subnet, so there’s no way it could be a valid host.

**Determining IP Address Problems-2**

The below figure shows a network problem. A user can’t get to Server B. 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.

***IP address problem***

If you use the same steps used to solve the last problem, you can see first that the WAN link again provides the subnet mask to use— /29, or 255.255.255.248. 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 user is in the 24 subnet, the WAN is in the 40 subnet, and the servers are in the 80 subnet. Can you see the problem yet? The valid host range for the user's 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. Server B has been configured with the broadcast address of the subnet. 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? What you need to do is look at other hosts on the LAN and figure out the network, mask, and default gateway.

Let’s take a look at a couple of examples of how to find and apply valid IP addresses to hosts. You need to assign a server and router IP address on a LAN. The subnet assigned on that segment is 192.168.1.24/29, and the router needs to be assigned the first usable address and the server the last valid host ID. What are the IP address, mask, and default gateway assigned to the server?

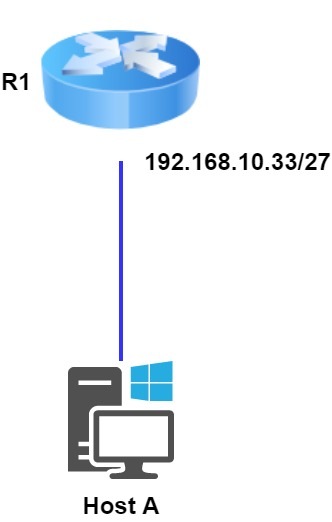
To answer this, you must know that a /29 is a 255.255.255.248 mask, which provides a block size of 8. The subnet is known as 24, the next subnet in a block of 8 is 32, so the broadcast address of the 24 subnet is 31, which makes the valid host range 25–30:

Server IP address: 192.168.1.30

Server mask: 255.255.255.248

Default gateway: 192.168.1.25 (router’s IP address)

**Determining IP Address Problems-3**



**Invalid Host**

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

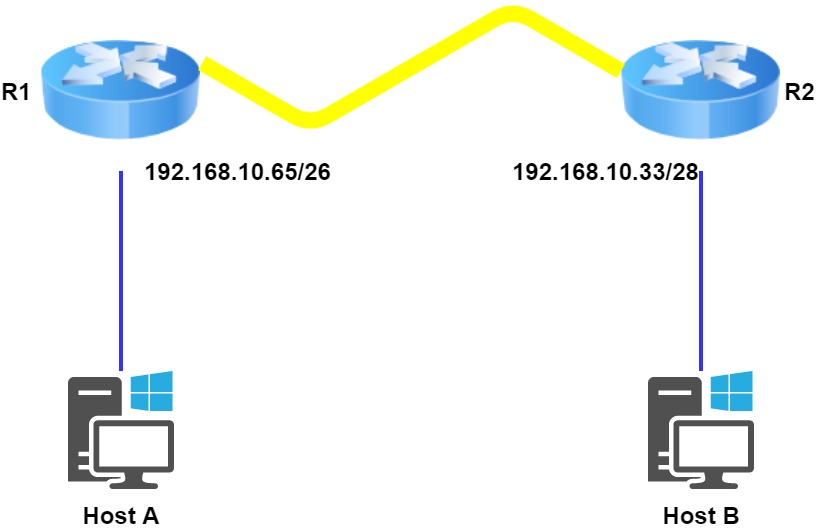
The IP address of the router’s Ethernet0 is 192.168.10.33/27. As you already know, a /27 is a 224 mask with a block size of 32. The router’s interface is in the 32 subnet. The next subnet is 64, so that makes the broadcast address of the 32 subnet 63 and the valid host range 33–62:

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

The below figure shows two routers with Ethernet configurations already assigned. What are the host addresses and subnet masks of hosts A and B?

***Invalid Host***

Router 1 has an IP address of 192.168.10.65/26 and Router 2 has an IP address of 192.168.10.33/28. What are the host configurations?

Router 1 Ethernet0 is in the 192.168.10.64 subnet, and Router 2 Ethernet0 is in the 192.168.10.32 network:

HostA IP address: 192.168.10.66–126

HostA mask: 255.255.255.192

HostA default gateway: 192.168.10.65

HostB IP address: 192.168.10.34–46

HostB mask: 255.255.255.240

HostB default gateway: 192.168.10.33