

## Troubleshooting Scenarios

17.7.1

### Duplex Operation and Mismatch Issues

Many common network problems can be identified and resolved with little effort. Now that you have the tools and the process for troubleshooting a network, this topic reviews some common networking issues that you are likely to find as a network administrator.

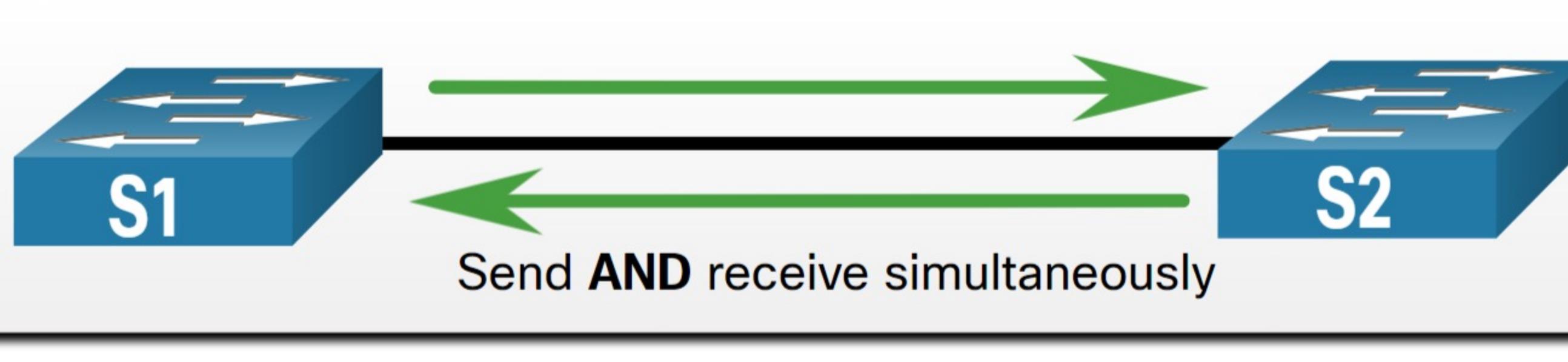
In data communications, **duplex** refers to the direction of data transmission between two devices.

There are two duplex communication modes:

- **Half-duplex** - Communication is restricted to the exchange of data in one direction at a time.
- **Full-duplex** - Communications is permitted to be sent and received simultaneously.

The figure illustrates how each duplex method operates.

#### Half-Duplex Communication



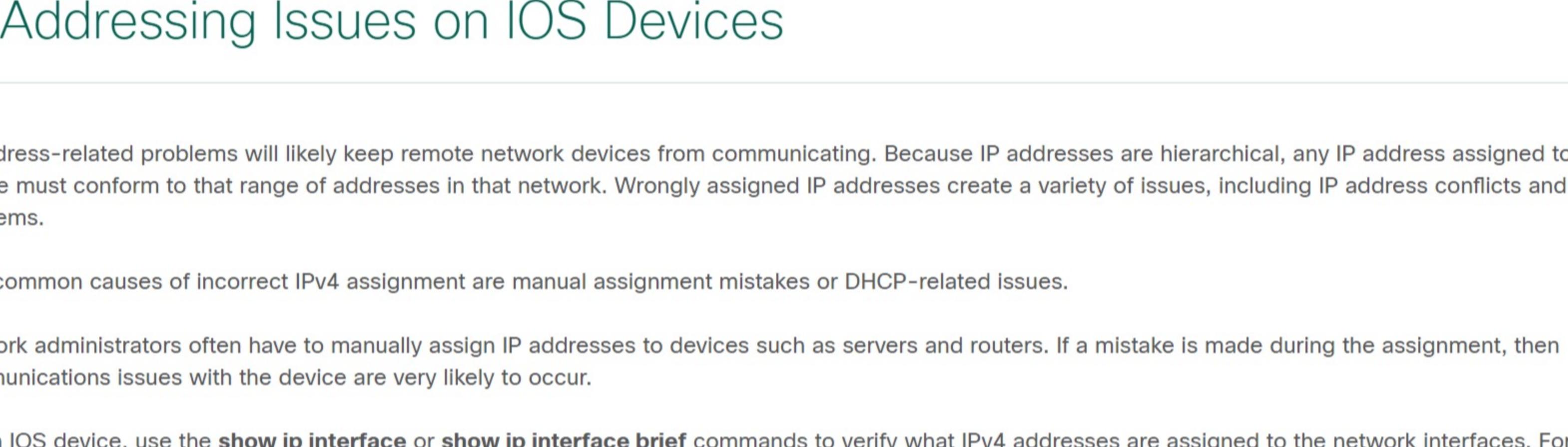
#### Full-Duplex Communication



Interconnecting Ethernet interfaces must operate in the same duplex mode for best communication performance and to avoid inefficiency and latency on the link.

The Ethernet autonegotiation feature facilitates configuration, minimizes problems, and maximizes link performance between two interconnecting Ethernet links. The connected devices first announce their supported capabilities and then choose the highest performance mode supported by both ends. For example, the switch and router in the figure have successfully autonegated full-duplex mode.

I can operate in full-duplex ...



If one of the two connected devices is operating in full-duplex and the other is operating in half-duplex, a duplex mismatch occurs. While data communication will occur through a link with a duplex mismatch, link performance will be very poor.

Duplex mismatches are typically caused by a misconfigured interface or in rare instances by a failed autonegotiation. Duplex mismatches may be difficult to troubleshoot as the communication between devices still occurs.

### IP Addressing Issues on IOS Devices

IP address-related problems will likely keep remote network devices from communicating. Because IP addresses are hierarchical, any IP address assigned to a network device must conform to that range of addresses in that network. Wrongly assigned IP addresses create a variety of issues, including IP address conflicts and routing problems.

Two common causes of incorrect IPv4 assignment are manual assignment mistakes or DHCP-related issues.

Network administrators often have to manually assign IP addresses to devices such as servers and routers. If a mistake is made during the assignment, then communications issues with the device are very likely to occur.

On an IOS device, use the `show ip interface` or `show ip interface brief` commands to verify what IPv4 addresses are assigned to the network interfaces. For example, issuing the `show ip interface brief` command as shown would validate the interface status on R1.

```
R1# show ip interface brief
Interface          IP-Address      OK? Method Status      Protocol
GigabitEthernet0/0/0 209.165.200.225 YES manual up        up
GigabitEthernet0/0/1 192.168.10.1  YES manual up        up
Serial0/1/0         unassigned     NO  unset down    down
Serial0/1/1         unassigned     NO  unset down    down
GigabitEthernet0     unassigned     YES unset administratively down down
R1#
```

### IP Addressing Issues on End Devices

In Windows-based machines, when the device cannot contact a DHCP server, Windows will automatically assign an address belonging to the 169.254.0.0/16 range. This feature is called Automatic Private IP Addressing (APIPA) and is designed to facilitate communication within the local network. Think of it as Windows saying, "I will use this address from the 169.254.0.0/16 range because I could not get any other address".

Often, a computer with an APIPA address will not be able to communicate with other devices in the network because those devices will most likely not belong to the 169.254.0.0/16 network. This situation indicates an automatic IPv4 address assignment problem that should be fixed.

Note: Other operating systems, such Linux and OS X, will not assign an IPv4 address to the network interface if communication with a DHCP server fails.

Most end devices are configured to rely on a DHCP server for automatic IPv4 address assignment. If the device is unable to communicate with the DHCP server, then the server cannot assign an IPv4 address for the specific network and the device will not be able to communicate.

To verify the IP addresses assigned to a Windows-based computer, use the `ipconfig` command, as shown in the output.

```
C:\Users\PC-A> ipconfig
Windows IP Configuration
(Output omitted)
Wireless LAN adapter Wi-Fi:
  Connection-specific DNS Suffix . :
  Link-local IPv6 Address . . . . . fe80::e4aa:2dd1%e2d:a75ek16
  IPv4 Address . . . . . 192.168.10.10
  Subnet Mask . . . . . 255.255.255.0
  Default Gateway . . . . . 192.168.10.1
  (Output omitted)
```

### Default Gateway Issues

The default gateway for an end device is the closest networking device that can forward traffic to other networks. If a device has an incorrect or non-existent default gateway address, it will not be able to communicate with devices in remote networks. Because the default gateway is the path to remote networks, its address must belong to the same network as the end device.

The address of the default gateway can be manually set or obtained from a DHCP server. Similar to IPv4 addressing issues, default gateway problems can be related to misconfiguration (in the case of manual assignment) or DHCP problems (if automatic assignment is in use).

To solve misconfigured default gateway issues, ensure that the device has the correct default gateway configured. If the default address was manually set but is incorrect, simply replace it with the proper address. If the default gateway address was automatically set, ensure the device can communicate with the DHCP server. It is also important to verify that the proper IPv4 address and subnet mask were configured on the interface of the router and that the interface is active.

To verify the default gateway on Windows-based computers, use the `ipconfig` command as shown.

```
C:\Users\PC-B> ipconfig
Windows IP Configuration
(Output omitted)
Wireless LAN adapter Wi-Fi:
  Connection-specific DNS Suffix . :
  Link-local IPv6 Address . . . . . fe80::e4aa:2dd1%e2d:a75ek16
  IPv4 Address . . . . . 192.168.10.10
  Subnet Mask . . . . . 255.255.255.0
  Default Gateway . . . . . 192.168.10.1
  (Output omitted)
```

On a router, use the `show ip route` command to list the routing table and verify that the default gateway, known as a default route, has been set. This route is used when the destination address of the packet does not match any other routes in its routing table.

For example, the output verifies that R1 has a default gateway (i.e., Gateway of last resort) configured pointing to IP address 209.165.200.226.

```
R1# show ip route | begin Gateway
Gateway of last resort is 209.165.200.226 to network 0.0.0.0
O*E2 0.0.0.0/0 [110/1] via 209.165.200.226, 02:19:58, GigabitEthernet0/0/0
  0.0.0.0/32 is subnetted, 1 subnets
  O 192.168.10.0/24 via 209.165.200.226, 02:05:42, GigabitEthernet0/0/0
    192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
    C 192.168.10.0/32 is directly connected, GigabitEthernet0/0/1
    L 192.168.10.0/32 is directly connected, GigabitEthernet0/0/1
  209.165.200.226/32 is subnetted, 1 subnets
  C 209.165.200.224/32 is directly connected, GigabitEthernet0/0/0
  L 209.165.200.225/32 is directly connected, GigabitEthernet0/0/0
  O 209.165.200.228/30
  [110/2] via 209.165.200.226, 02:07:19, GigabitEthernet0/0/0
R1#
```

The first highlighted line basically states that the gateway to any (i.e., 0.0.0.0) should be sent to IP address 209.165.200.226. The second highlighted displays how R1 learned about the default gateway. In this case, R1 received the information from another OSPF-enabled router.

### Troubleshooting DNS Issues

Domain Name System (DNS) defines an automated service that matches names, such as [www.cisco.com](http://www.cisco.com), with the IP address. Although DNS resolution is not crucial to device communication, it is very important to the end user.

It is common for users to mistakenly relate the operation of an internet link to the availability of the DNS. User complaints such as "the network is down" or "the internet is down" are often caused by an unreachable DNS server. While packet routing and all other network services are still operational, DNS failures often lead the user to the wrong conclusion: if a user types in a domain name such as [www.cisco.com](http://www.cisco.com) in a web browser and the DNS server is unreachable, the name will not be translated into an IP address and the website will not display.

DNS server addresses can be manually or automatically assigned. Network administrators are often responsible for manually assigning DNS server addresses on servers and other devices, while DHCP is used to automatically assign DNS server addresses to clients.

Although it is common for companies and organizations to maintain their own DNS servers, any reachable DNS server can be used to resolve names. Small office and home offices (SOHO) users often rely on the DNS server maintained by their ISP for name resolution. ISP-maintained DNS servers are assigned to SOHO customers via DHCP. Additionally, Google maintains a public DNS server that can be used by anyone and it is very useful for testing. The IPv4 address of Google's public DNS server is 8.8.8.8 and 2001:4860:4860:8888 for its IPv6 DNS address.

Cisco offers OpenDNS which provides secure DNS service by filtering phishing and some malware sites. You can change your DNS address to 208.67.222.222 and 208.67.220.220 in the Preferred DNS server and Alternate DNS server fields. Advanced features such as web content filtering and security are available to families and businesses.

Use the `ipconfig /all` as shown to verify which DNS server is in use by the Windows computer.

```
C:\Users\PC-A> ipconfig /all
Windows IP Configuration
(Output omitted)
Wireless LAN adapter Wi-Fi:
  Connection-specific DNS Suffix . :
  Description . . . . . Intel(R) Dual Band Wireless-AC 8265
  Physical Address . . . . . F8-94-C2-E4-C5-0A
  DHCP Enabled. . . . . Yes
  Autoconfiguration Enabled . . . . Yes
  Link-local IPv6 Address . . . . . fe80::e4aa:2dd1%e2d:a75ek16(PREFERRED)
  IPv4 Address . . . . . 192.168.10.10(Preferred)
  Subnet Mask . . . . . 255.255.255.0
  Lease Obtained. . . . . August 17, 2019 1:20:17 PM
  Lease Expires . . . . . August 18, 2019 1:20:18 PM
  Default Gateway . . . . . 192.168.10.10(Preferred)
  DHCPv6 T1D1 . . . . . 2019-08-17T01:20:09Z
  DHCPv6 Client DUID. . . . . 00-01-00-01-21-F1-76-75-54-E1-AD-DE-DA-9A
  DNS Servers . . . . . 208.67.222.222
  NetBIOS over Tcpip. . . . . Enabled
  (Output omitted)
```

The nslookup command is another useful DNS troubleshooting tool for PCs. With nslookup a user can manually place DNS queries and analyze the DNS response. The nslookup command shows the output for a query for [www.cisco.com](http://www.cisco.com). Notice you can also enter an IP address and nslookup will resolve the name.

Note: It is not always possible to type an IP address in nslookup and receive the domain name. One of the most common reasons for this is that most websites run on servers that support multiple sites.

```
C:\Users\PC-A> nslookup
```

Default Server: Home-Net

Address: 192.168.1.1

> cisco.com

Server: Home-Net

Address: 192.168.1.1

Non-authoritative answer:

Name: cisco.com

Addresses: 208.67.222.222

72.169.4.185

> 8.8.8.8

Server: Home-Net

Address: 192.168.1.1

Name: dns.google

Address: 8.8.8.8

> 208.67.222.222

Server: Home-Net

Address: 192.168.1.1

Name: resolver1.opendns.com

Address: 208.67.222.222

>

### Packet Tracer – Troubleshoot Connectivity Issues

The objective of this Packet Tracer activity is to troubleshoot and resolve connectivity issues, if possible. Otherwise, the issues should be clearly documented and so they can be escalated.

Troubleshoot Connectivity Issues

Troubleshoot Connectivity Issues

17.7.6

### Lab – Troubleshoot Connectivity Issues

#### Skills Practice Opportunity

You have the opportunity to practice the following skills:

- Part 1: Identify the Problem
- Part 2: Implement Network Changes
- Part 3: Verify Full Functionality
- Part 4: Document Findings and Configuration Changes

You can practice these skills using the Packet Tracer or lab equipment, if available.

Packet Tracer - Physical Mode (PTPM)

Troubleshoot Connectivity Issues - Physical Mode

Troubleshoot Connectivity Issues - Physical Mode

Lab Equipment

Troubleshoot Connectivity Issues

17.7.7

17.7.8

17.7.9

17.7.10

17.7.11

17.7.12

17.7.13

17.7.14

17.7.15

17.7.16

17.7.17

17.7.18

17.7.19

17.7.20

17.7.21

17.7.22

17.7.23

17.7.24

17.7.25

17.7.26

17.7.27

17.7.28

17.7.29

17.7.30