12.1.7 Common Ports

Click one of the buttons to take you to that part of the video.

Common Ports 0:00-2:26

To effectively manage a network-to-Linux system you need to understand the concept of IP ports. You might be asking, 'What in the world is an IP port?'

In essence, a port, in terms of the IP protocol, is a logical connection that's created by either the TCP protocol or the UDP protocol for some upper layer application. Now, ports essentially allow a single host with a single IP address to provide multiple network services. Each service uses the same IP address, but operates using a different TCP or UDP port number.

For example, let's suppose we have a network server running here and it has a single IP address assigned to it, '10.0.0.1'. Now on this server, we're going to assume it's a Linux server, we could configure multiple network services.

For example, we could install a web server and we could install an FTP server--both of these services run at the same time on the same server hardware on the same operating system.

Now each of these services, the web server and the FTP server, will listen for network requests coming in on the very same network interface, which has the only one IP address assigned to it, 10.0.0.1.

In this configuration, each of these services has exactly the same IP address, 10.0.0.1. So when that request comes in on the network for a particular network resource, how does the Linux operating system tell whether that request is supposed to go over here to the web server or over here to the FTP server?

Here's how it works. The web server runs on a different port than the FTP server does. The web server runs on port 80, but the FTP server on the same system runs on ports 20 and 21.

Therefore, any network request that's coming in on the network from a client, say this one right here, that's addressed to port 80 on this IP address, 10.0.0.1, when that request arrives, the operating system knows that it goes through the web service because that's the service that's listening on port 80 for requests.

Port Overview 2:11-3:14

Let's suppose this other system down here sends a network request to the same IP address, 10.0.0.1, but this one is being sent to port 20 or 21. Those are the ports that are used by the FTP service. So when that request arrives, the operating system knows that it goes over here through the FTP service because that's the service that's listening for requests on those ports.

Now before we go on, understand that FTP is somewhat unique in the respect that it uses two ports. Most network services don't do this, they use just one port. There are a limited number that use two and there are even a more limited number that use three different ports, which we'll talk about in just a second. Most other services just use one port.

Well-Known Ports 3:15-7:57

In light of this, you need to be familiar with the various categories that are used to organize IP ports. Now a port number can range from a value of 0 up to a maximum value of 65,535.

The way these ports are used is regulated by the Internet Corporation for Assigned Names and Numbers, which we affectionately just call ICANN. ICANN lumps all of these available IP ports into three different categories.

The first one is our well-known ports. Well-known ports are reserved for specific services. Just remember if you see well-known, we're talking about reserved ports. Well-known ports begin at 0 and end at 1,023. Some of the more frequently used well-known ports are listed here.

As we just talked about, port 20 and 21 are used by the FTP service; port 22 is reserved for the Secure Shell protocol, SSH, to establish remote connections over a network. Port 23 is reserved for Telnet, which performs a similar function as SSH, just without any security involved.

Port 25 is used by the Simple Mail Transfer protocol. This protocol is used by your email clients to send an email from your client to the mail server and it's also used to send messages between email servers on the internet.

Port 53 is used by the DNS protocol to resolve hostnames into IP addresses. As we talked about a second ago, port 80 is used by web servers, which use the HTTP protocol.

Port 110 is reserved for the POP3 protocol, which is used to download email messages from an email server to an email client application. Port 123 is used by the Network Time protocol, NTP. This is used to synchronize time between multiple systems over a network connection.

Ports 137, 138 and 139 are used by Microsoft's NetBIOS protocol. They're also used by the SMB protocol, which is implemented on Linux to make it compatible with Microsoft systems. That's why they use the same port numbers.

Port 143 is used by the IMAP protocol which functions in a similar manner to POP3. It allows you to download email messages and send email messages for that matter. It allows you to download email messages from an email server to your email client.

Ports 161 and 162 are used by the Simple Network Management protocol. This is used to monitor systems on the network to see what their status is and how well they're functioning basically.

Port 389 is used by the Lightweight Directory Access protocol, or LDAP. This is used to communicate with an LDAP directory service. Port 443 is used by web servers as well, but it's a special port that's used for secure communications between a web browser and a web server.

This is done using the HTTPS protocol. Regular HTTP transmits data insecurely, clear text--anybody can read it who grabs ahold of the packets being transmitted. HTTPS uses the TLS protocol to encrypt that data so that even if you capture it, you can't read it.

Port 465 is used by the SMTPS protocol, this is the Simple Mail Transfer Protocol Secure. It basically is the same thing as the Simple Mail Transfer protocol, except that it's encrypted. By default, SMTP sends your emails unencrypted so anybody who wants to can read them.

Using port 465 in the SMTPS protocol, we encrypt the data so that even if somebody does get ahold of it, they can't read it. Port 514 is used by the syslog daemon to send log messages remotely over the network to a log server.

Port 636 is used for the Lightweight Directory Access protocol. But it's a secure connection. Port 389 up here transmits data between the LDAP client and the LDAP service insecurely. All the data is sent clear text, including passwords and usernames, which isn't good. So what we usually do is encrypt that data using port 636 and the LDAPS protocol.

Likewise, port 993 is reserved for the secure version of the IMAP protocol. It's also used to download email messages from a mail server to your mail client but it does so with encryptions so that nobody can read it as the data's being transferred.

Same thing for port 995. It's reserved for the POP3S protocol, which is also a secure version of the POP3 protocol that also allows you to download email messages from an email server to an email client, encrypting the data as it's being transmitted.

Registered Ports 7:58-8:35

Now in addition to our well-known ports, we also have a category of ports that are called registered ports. ICANN has reserved ports 1,024 through 49,151 for special implementations. Basically, an organization can create their own network service and then apply for a registered port number to be assigned to it.

For example, a software company could write a new network application and then apply for a specific port to be reserved for use with their particular network application. This prevents anybody else from using that same port.

Dynamic Ports 8:36-10:00

Finally, we have the free for all range called dynamic ports. These are also called private ports. They range from port 49,152 all the way to the end, 65,535. These are available for use by any network service. They're frequently used by network services that need to establish a temporary connection.

For example, let's suppose we have a client system here that needs to communicate with the server system over here. Using dynamic ports, these two systems will negotiate with each other and say, "Hey, we need to set up a port that we can talk together on."

They know by default that they can't use a registered port and they can't use a well-known port. So each system will take a look at what ports are currently in use and which ports are currently available on both sides and they'll talk with each other and negotiate which port they want to use.

For example, they may determine that, "Hey, neither one of us are using 49,153. Let's go ahead and use it." Then the client and server will use that port during the communication session. Then after that session is complete, the port is closed and it's no longer in use.

That's why we call them dynamic ports. They're allocated when the connection is set up, but once the session is done, the connection is broken and the ports are unallocated and then it can be used by another communication session if they're needed.

Summary 10:01-10:11

That's how ports work on a Linux system. In this lesson, we talked about the three different categories of ports. We talked about the well-known ports that have specific numbers assigned to them. We also talked about registered ports, and then we ended this lesson by talking about dynamic ports.