

# Networking Nomad

## Network Sharing

Learning | Linux Journey

Nueva pestaña

linuxjourney.com/lesson/network-file-sharing

WhatsApp Webhttps://discord.com...SKZFLIXPinterestNotion – The all-in-...Nueva pestañaOtros marcadores

Network Sharing

1. File Sharing Overview

2. rsync

3. Simple HTTP Server

4. NFS

5. Samba

página de inicio

### 1. File Sharing Overview

You usually are not the only computer on your network, this is especially the case if you're working in a commercial environment. When we want to transfer data from one machine to another, sometimes it may be easier to connect a USB drive and manually copy them. But for the most part, if you're working with machines on the same network, the way to transfer data is through network file sharing.

In this course we'll go over a couple of different methods to copy data to and from different machines on your network. We'll discuss some simple file copies, then we'll talk about mounting entire directories on your machine that act as a separate drive.

One simple file sharing tool is the **scp** command. The scp command stands for secure copy, it works exactly the way the cp command does, but allows you to copy from one host over to another host on the same network. It works via ssh so all your actions are using the same authentication and security as ssh.

To copy a file over from local host to a remote host

```
$ scp myfile.txt username@remotehost.com:/remote/dir
```

To copy a file from a remote host to your local host

```
$ scp username@remotehost.com:/remote/directory/myfi
```

To copy over a directory from your local host to a remote host

```
$ scp -r mydir username@remotehost.com:/remote/direc
```

### Ceremonias

Try to copy a file over with scp from one machine to another.

### Examen

What command can you use to securely copy files from one host to another?

✓ ¡Respuesta correcta!

scp

Revisar respuesta

Continuar

Learning | Linux Journey

Nueva pestaña

linuxjourney.com/lesson/rsync

WhatsApp Webhttps://discord.com...SKZFLIXPinterestNotion – The all-in-...Nueva pestañaOtros marcadores

Network Sharing

1. File Sharing Overview

2. rsync

3. Simple HTTP Server

4. NFS

5. Samba

página de inicio

### 2. rsync

Another tool used to copy data from different hosts is rsync (short for remote synchronization). Rsync is very similar to scp, but it does have a major difference. Rsync uses a special algorithm that checks in advance if there is already data that you are copying to and will only copy over the differences. For example, let's say that you were copying over a file and your network got interrupted, therefore your copy stopped midway. Instead of re-copying everything from the beginning, rsync will only copy over the parts that didn't get copied.

It also verifies the integrity of a file you are copying over with checksums. These small optimizations allow greater file transfer flexibility and makes rsync ideal for directory synchronization remotely and locally, data backups, large data transfers and more.

Some commonly-used rsync options:

- v - verbose output
- r - recursive into directories
- h - human readable output
- z - compressed for easier transfer, great for slow connections

Copy/sync files on the same host

```
$ rsync -zvr /my/local/directory/one /my/local/direc
```

Copy/sync files to local host from a remote host

```
$ rsync /local/directory username@remotehost.com:/re
```

Copy/sync files to a remote host from a local host

### Ceremonias

Use rsync to sync a directory to another directory, be sure not to overwrite an important directory!

### Examen

What command would be useful for data backups?

✓ ¡Respuesta correcta!

rsync

Revisar respuesta

Continuar

Learning | Linux Journey

linuxjourney.com/lesson/nfs-network-file-share

WhatsApp Webhttps://discord.com...SKZFLIXPinterestNotion – The all-in-...Nueva pestañaOtros marcadores

Network Sharing

- 1. File Sharing Overview
- 2. rsync
- 3. Simple HTTP Server
- 4. NFS
- 5. Samba

página de inicio

## 4. NFS

The most standard network file share for Linux is NFS (Network File System). NFS allows a server to share directories and files with one or more clients over the network.

We won't get into the details of how to create an NFS server as it can get complex, however we will discuss setting up NFS clients.

### Setting up NFS client

```
$ sudo service nfsclient start
$ sudo mount server:/directory /mount_directory
```

### Automounting

Let's say you use the NFS server quite often and you want to keep it permanently mounted, normally you think you'd edit the `/etc/fstab` file, but you may not always get a connection to the server and that can cause issues on bootup. Instead what you want to do is setup automounting so that you can connect to the NFS server when you need to. This is done with the **automount** tool or in recent versions of Linux **amd**. When a file is accessed in a specified directory, automount will look up the remote server and automatically mount it.

## Ceremonias

Read the manpage for NFS to learn more.

## Examen

What tool is used to manage mount points automatically?

✓ ¡Respuesta correcta!

automount

Revisar respuesta

Continuar

Learning | Linux Journey

linuxjourney.com/lesson/samba

WhatsApp Webhttps://discord.com...SKZFLIXPinterestNotion – The all-in-...Nueva pestañaOtros marcadores

Network Sharing

- 1. File Sharing Overview
- 2. rsync
- 3. Simple HTTP Server
- 4. NFS
- 5. Samba

página de inicio

## 5. Samba

In the early days of computing, it became necessary for Windows machines to share files with Linux machines, thus the Server Message Block (SMB) protocol was born. SMB was used for sharing files between Windows operating systems (Mac also has file sharing with SMB) and then it was later cleaned up and optimized in the form of the Common Internet File System (CIFS) protocol.

Samba is what we call the Linux utilities to work with CIFS on Linux. In addition to file sharing, you can also share resources like printers.

### Create a network share with Samba

Let's go through the basic steps to create a network share that a Windows machine can access:

### Install Samba

```
$ sudo apt update
$ sudo apt install samba
```

### Setup smb.conf

The configuration file for Samba is found at `/etc/samba/smb.conf`, this file should tell the system what directories should be shared, their access permissions, and more options. The default `smb.conf` comes with lots of commented code already and you can use those as an example to write your own configurations.

```
$ sudo vi /etc/samba/smb.conf
```

### Setup up a password for Samba

```
$ sudo smbpasswd -s -e username
```

## Ceremonias

Setup a Samba share, if you don't have one, open up `smb.conf` and familiarize yourself with the options in the config file.

## Examen

What is the latest protocol used for file transfer between Windows and Linux?

✓ ¡Respuesta correcta!

CIFS

Revisar respuesta

Return

Learning | Linux Journey

linuxjourney.com/lesson/network-basics

WhatsApp Webhttps://discord.com...SKZFlixPinterestNotion – The all-in-...Nueva pestañaOtros marcadores

Network Basics

1. Network Basics

2. OSI Model

3. TCP/IP Model

4. Network Addressing

5. Application Layer

6. Transport Layer

7. Network Layer

8. Link Layer

9. DHCP Overview

página de inicio

## 1. Network Basics

Let's look at a typical home network, you have a few different components.

- ISP - Your internet service provider, the company you pay to get Internet at your house.
- Router - The router allows each machine on your network to connect to the Internet. In most modern routers, you can connect via wireless or an Ethernet cable.
- WAN - Wide Area Network, this is what we call the network that encompasses everything between your router and a wider network such the Internet.
- WLAN - Wireless Local Area Network, this is the network between your router and any wireless devices you may have such as laptops.
- LAN - Local Area Network, this is the network between your router and any wired devices such as Desktop PCs.
- Hosts - Each machine on a network is known as a host.

The data and information that gets transmitted through networks are known as packets and by the end of the Networking Nomad section, you'll understand in detail how a packet travels to and from hosts.

Ceremonias

No exercises for this lesson.

Examen

What is the local area network known as?

✓ ¡Respuesta correcta!

LAN

Revisar respuesta

Continuar

Learning | Linux Journey

linuxjourney.com/lesson/osi-model

WhatsApp Webhttps://discord.com...SKZFlixPinterestNotion – The all-in-...Nueva pestañaOtros marcadores

Network Basics

1. Network Basics

2. OSI Model

3. TCP/IP Model

4. Network Addressing

5. Application Layer

6. Transport Layer

7. Network Layer

8. Link Layer

9. DHCP Overview

página de inicio

## 2. OSI Model

Before we can look at some practical networking stuff, we have to go over some boring jargon that you've probably heard of before. The OSI (Open Systems Interconnection) model is a theoretical model of networking. This model shows us how a packet traverses through a network in seven different layers. I won't get into specifics of this model, since most of these networking courses will be focused on the TCP/IP model, but it should be mentioned that such a theoretical networking model exists and has actually played a large part in the TCP/IP networking model that we use today.

Ceremonias

Read more about the OSI model:  
[https://en.wikipedia.org/wiki/OSI\\_model](https://en.wikipedia.org/wiki/OSI_model)

Examen

What is used as the theoretical model of networking?

✓ ¡Respuesta correcta!

OSI

Revisar respuesta

Continuar

Learning | Linux Journey

linuxjourney.com/lesson/tcp-ip-model

WhatsApp Webhttps://discord.com...SKZFLIXPinterestNotion – The all-in-...Nueva pestañaOtros marcadores

Network Basics

- 1. Network Basics
- 2. OSI Model
- 3. TCP/IP Model
- 4. Network Addressing
- 5. Application Layer
- 6. Transport Layer
- 7. Network Layer
- 8. Link Layer
- 9. DHCP Overview

página de inicio

### 3. TCP/IP Model

The OSI model gave birth to what eventually became the TCP/IP model and this model is actually what the Internet is based off of. It is the actual implementation of networking. The TCP/IP model uses the TCP/IP protocol suite, which we just commonly refer to as TCP/IP. These protocols work together to specify how data should be gathered, addressed, transmitted and routed through a network. Using the TCP/IP model, we can see how these protocols are used to show the breakdown of how a packet travels through the network.

#### Application Layer

The top layer of the TCP/IP model. It determines how your computer's programs (such as your web browser) interface with the transport layer services to view the data that gets sent or received.

This layer uses:

- HTTP (Hypertext Transfer Protocol) - used for the webpages on the Internet.
- SMTP (Simple Mail Transfer Protocol) - electronic mail (email) transmission

#### Transport Layer

How data will be transmitted, includes checking the correct ports, the integrity of the data, and basically delivering our packets.

This layer uses:

- TCP (Transmission Control Protocol) - reliable data delivery
- UDP (User Datagram Protocol) - unreliable data delivery

### Ceremonias

No exercises for this lesson.

### Examen

What is the top layer of the TCP/IP model?

✓ ¡Respuesta correcta!

ApplicationRevisar respuesta

Continuar

Learning | Linux Journey

linuxjourney.com/lesson/network-addressing

WhatsApp Webhttps://discord.com...SKZFLIXPinterestNotion – The all-in-...Nueva pestañaOtros marcadores

Network Basics

- 1. Network Basics
- 2. OSI Model
- 3. TCP/IP Model
- 4. Network Addressing
- 5. Application Layer
- 6. Transport Layer
- 7. Network Layer
- 8. Link Layer
- 9. DHCP Overview

página de inicio

### 4. Network Addressing

Before we jump into seeing how a packet moves across a network, we have to familiarize ourselves with some terminology. When you mail a letter, you must know who it is being sent to and where it is coming from. Packets need the same information, our hosts and other hosts are identified using MAC (media access control) addresses and IP addresses, to make it easier on us humans we use hostnames to identify a host.

#### MAC Addresses

A MAC address is a unique identifier used as a hardware address. This address will never change. When you want to get access to the Internet, your machine needs to have a device called a network interface card. This network adapter has its own hardware address that's used to identify your machine. A MAC address for an Ethernet device looks something like this 00:C4:B5:45:B2:43. MAC addresses are given to network adapters when they are manufactured. Each manufacturer has an organizationally unique identifier (OUI) to identify them as the manufacturer. This OUI is denoted by the first 3 bytes of the MAC address. For example, Dell has 00-14-22, so a network adapter from Dell could have a MAC address like: 00-14-22-34-B2-C2.

#### IP Addresses

An IP Address is used to identify a device on a network, they are hardware independent and can vary in syntax depending on if you are using IPv4 or IPv6 (more on this later). For now we'll assume you are using IPv4, so a typical IP address would look like: 10.24.12.4. IP addresses are used with the software side of networking. Anytime a system is connected to the Internet it should have an IP address. They can also

### Ceremonias

No exercises for this lesson.

### Examen

How many bytes are in an IPv4 address?

✓ ¡Respuesta correcta!

4Revisar respuesta

Continuar

Learning | Linux Journey

linuxjourney.com/lesson/application-layer

WhatsApp Webhttps://discord.com...SKZFLIXPinterestNotion – The all-in-...Nueva pestañaOtros marcadores

Network Basics

- 1. Network Basics
- 2. OSI Model
- 3. TCP/IP Model
- 4. Network Addressing
- 5. Application Layer
- 6. Transport Layer
- 7. Network Layer
- 8. Link Layer
- 9. DHCP Overview

página de inicio

## 5. Application Layer

Let's say I wanted to send an email to Patty. We'll go through each of the TCP/IP layers to see this in action.

Remember that packets are used to transmit data across networks, a packet consists of a header and payload. The header contains information about where the packet is going and where it came from. The payload is the actual data that is being transferred. As our packet traverses the network, each layer adds a bit of information to the header of the packet. Also keep in mind that different layers use a different term for our "packet". In the transport layer we essentially encapsulate our data in a segment and in the link layer we refer to this as a frame, but just know that packet can be used in regards to the same thing.

First we start off in the application layer. When we send our email through our email client, the application layer will encapsulate this data. The application layer talks to the transport layer through a specified port and through this port it sends its data. We want to send an email through the application layer protocol SMTP (simple mail transfer protocol). The data is sent through our transport protocol which opens a connection to this port (port 25 is used for SMTP), so we get this data sent through this port and that data is sent to the Transport layer to be encapsulated into segments.

### Ceremonias

No exercises for this lesson.

### Examen

What layer is used to present the packet data in a user friendly format?

✓ ¡Respuesta correcta!

ApplicationRevisar respuesta

Continuar

Learning | Linux Journey

linuxjourney.com/lesson/transport-layer

WhatsApp Webhttps://discord.com...SKZFLIXPinterestNotion – The all-in-...Nueva pestañaOtros marcadores

Network Basics

- 1. Network Basics
- 2. OSI Model
- 3. TCP/IP Model
- 4. Network Addressing
- 5. Application Layer
- 6. Transport Layer
- 7. Network Layer
- 8. Link Layer
- 9. DHCP Overview

página de inicio

## 6. Transport Layer

The transports layer helps us transfer our data in a way networks can read it. It breaks our data into chunks that will be transported and put back together in the correct order. These chunks are known as segments. Segments make it easier to transport data across networks.

### Ports

Even though we know where we are sending our data via IP addresses, they aren't specific enough to send our data to a certain processes or services. Services such as HTTP use a communication channel via ports. If we want to send webpage data, we need to send it over the HTTP port (port 80). In addition to forming segments, the transport layer will also attach the source and destination ports to the segment, so when the receiver gets the final packet it will know what port to use.

### UDP

There are two popular transport protocols UDP and TCP. We'll briefly discuss UDP and spend most of our time on TCP, since it's the most commonly used.

UDP is not a reliable method of transporting data, in fact it doesn't really care if you get all of your original data. This may sound terrible, but it does have its uses, such as for media streaming, it's ok if you lose some frames in return you get your data a little faster.

### TCP

TCP provides a reliable connection-oriented stream of data. TCP uses ports to send data to and from hosts. An application opens up a connection from one port on its host to another port on a remote host. In order to establish the

### Ceremonias

No exercises for this lesson.

### Examen

What is a reliable transport protocol?

✓ ¡Respuesta correcta!

tcpRevisar respuesta

Continuar

Learning | Linux Journey

linuxjourney.com/lesson/network-layer

WhatsApp Webhttps://discord.com...SKZFLIXPinterestNotion – The all-in-...Nueva pestañaOtros marcadores

Network Basics

- 1. Network Basics
- 2. OSI Model
- 3. TCP/IP Model
- 4. Network Addressing
- 5. Application Layer
- 6. Transport Layer
- 7. Network Layer
- 8. Link Layer
- 9. DHCP Overview

página de inicio

## 7. Network Layer

The Network layer determines the routing of our packets from our source host to a destination host. Fortunately in our example, our packet is only traveling within the same network, but the Internet is made up of many networks. These smaller networks that make up the Internet are known as subnets. All subnets connect to each other in some way, which is why we are able to get to [www.google.com](http://www.google.com) even though it's on its own network. I won't go into detail as we have a whole course dedicated to subnets, but for now in regards to our Network layer, know that the IP addresses define the rules to travel to different subnets.

In the network layer, it receives the segment coming from the transport layer and encapsulates this segment in an IP packet then attaches the IP address of the source host and the IP address of the destination host to the packet header. So at this point, our packet has information about where it is going and where it came from. Now it sends our packet to the physical hardware layer.

### Ceremonias

No exercises for this lesson.

### Examen

What are smaller networks that make up the Internet called?

✓ ¡Respuesta correcta!

subnets

Revisar respuesta

Continuar

Learning | Linux Journey

linuxjourney.com/lesson/link-layer

WhatsApp Webhttps://discord.com...SKZFLIXPinterestNotion – The all-in-...Nueva pestañaOtros marcadores

Network Basics

- 1. Network Basics
- 2. OSI Model
- 3. TCP/IP Model
- 4. Network Addressing
- 5. Application Layer
- 6. Transport Layer
- 7. Network Layer
- 8. Link Layer
- 9. DHCP Overview

página de inicio

## 8. Link Layer

At the bottom of the TCP/IP model sits the Link Layer. This layer is the hardware specific layer.

In the link layer, our packet is encapsulated once more into something called a frame. The frame header attaches the source and destination MAC addresses of our hosts, checksums and packet separators so that the receiver can tell when a packet ends.

Fortunately we are on the same network, so our packet won't have to travel too far. First, the link layer attaches my source MAC address to the frame header, but it needs to know Patty's MAC address as well. How does it know that and how do I find it since it's not on the Internet? We use ARP!

### ARP (Address Resolution Protocol)

ARP finds the MAC address associated with an IP address. ARP is used within the same network. If Patty was not on the same network, we would use a routing system to determine the next router that would receive the packet and once we were on the same network, we could use ARP.

Once we are on the same network, systems first use the ARP look-up table that stores information about what IP addresses are associated with what MAC address. If the value is not there, then ARP is used. Then the system will send a broadcast message to the network using the ARP protocol to find out which host has IP 10.10.10.14. A broadcast message is a special message that is sent to all hosts on a network (aptly named for sending a broadcast). Any machine with the requested IP address will reply with an ARP packet containing the IP address and the MAC address.

Now that we have all the necessary data we need, IP address

### Ceremonias

No exercises for this lesson.

### Examen

What is used to find the MAC address on the same network?

✓ ¡Respuesta correcta!

ARP

Revisar respuesta

Continuar



Learning | Linux Journey

linuxjourney.com/lesson/dhcp-overview

WhatsApp Webhttps://discord.com...SKZFLIXPinterestNotion – The all-in-...Nueva pestañaOtros marcadores

Network Basics

- 1. Network Basics
- 2. OSI Model
- 3. TCP/IP Model
- 4. Network Addressing
- 5. Application Layer
- 6. Transport Layer
- 7. Network Layer
- 8. Link Layer
- 9. DHCP Overview

## 9. DHCP Overview

An important networking concept that we did not go over yet is DHCP (Dynamic Host Configuration Protocol)

DHCP assigns IP addresses, subnet masks and gateways to our machines. For example, let's say you have a cell phone and you want to get a cell phone number to start talking to people. You have to call up your phone carrier and they will give you a number. As long as you pay your bills you can keep using your phone. DHCP is the phone carrier in this case, it gives you an IP address so that you can talk to other IP addresses. You are also leased an IP address, these last for a certain period of time, then will get renewed depending on how you have your lease settings.

DHCP is great for many reasons, it allows a network administrator to not worry about assigning IP addresses and it also prevents them from setting up duplicate IP addresses. Every physical network should have its own DHCP server so that a host can request an IP address. In a regular home setting, the router usually acts as the DHCP server.

The way DHCP gets all your dynamic host information is:

1. DHCP DISCOVER - This message is broadcasted to search for a DHCP server.
2. DHCP OFFER - The DHCP server in the network replies with an offer message. The offer contains a packet with DHCP lease time, subnet mask, IP address, etc.
3. DHCP REQUEST - The client sends out another broadcast to let all DHCP servers know which offer it accepted.
4. DHCP ACK - Acknowledgement is sent by the server.

DHCP gets more involved than this, but this is the gist of it.

### Ceremonias

No exercises for this lesson.

### Examen

What are the steps in a DHCP request?

✓ ¡Respuesta correcta!

Discover, Offer, Request, ACK

Revisar respuesta

Return

## Network Basics

Learning | Linux Journey

linuxjourney.com/lesson/network-basics

WhatsApp Webhttps://discord.com...SKZFLIXPinterestNotion – The all-in-...Nueva pestañaOtros marcadores

Network Basics

- 1. Network Basics
- 2. OSI Model
- 3. TCP/IP Model
- 4. Network Addressing
- 5. Application Layer
- 6. Transport Layer
- 7. Network Layer
- 8. Link Layer
- 9. DHCP Overview

página de inicio

## 1. Network Basics

Let's look at a typical home network, you have a few different components.

- ISP - Your internet service provider, the company you pay to get Internet at your house.
- Router - The router allows each machine on your network to connect to the Internet. In most modern routers, you can connect via wireless or an Ethernet cable.
- WAN - Wide Area Network, this is what we call the network that encompasses everything between your router and a wider network such the Internet.
- WLAN - Wireless Local Area Network, this is the network between your router and any wireless devices you may have such as laptops.
- LAN - Local Area Network, this is the network between your router and any wired devices such as Desktop PCs.
- Hosts - Each machine on a network is known as a host.

The data and information that gets transmitted through networks are known as packets and by the end of the Networking Nomad section, you'll understand in detail how a packet travels to and from hosts.

### Ceremonias

No exercises for this lesson.

### Examen

What is the local area network known as?

✓ ¡Respuesta correcta!

LAN

Revisar respuesta

Continuar

Learning | Linux Journey

linuxjourney.com/lesson/osi-model

WhatsApp Webhttps://discord.com...SKZFLIXPinterestNotion – The all-in-...Nueva pestañaOtros marcadores

Network Basics

- 1. Network Basics
- 2. OSI Model
- 3. TCP/IP Model
- 4. Network Addressing
- 5. Application Layer
- 6. Transport Layer
- 7. Network Layer
- 8. Link Layer
- 9. DHCP Overview

página de inicio

## 2. OSI Model

Before we can look at some practical networking stuff, we have to go over some boring jargon that you've probably heard of before. The OSI (Open Systems Interconnection) model is a theoretical model of networking. This model shows us how a packet traverses through a network in seven different layers. I won't get into specifics of this model, since most of these networking courses will be focused on the TCP/IP model, but it should be mentioned that such a theoretical networking model exists and has actually played a large part in the TCP/IP networking model that we use today.

### Ceremonias

Read more about the OSI model:  
[https://en.wikipedia.org/wiki/OSI\\_model](https://en.wikipedia.org/wiki/OSI_model)

### Examen

What is used as the theoretical model of networking?

✓ ¡Respuesta correcta!

OSI

Revisar respuesta

Continuar

Learning | Linux Journey

linuxjourney.com/lesson/tcp-ip-model

WhatsApp Webhttps://discord.com...SKZFLIXPinterestNotion – The all-in-...Nueva pestañaOtros marcadores

Network Basics

- 1. Network Basics
- 2. OSI Model
- 3. TCP/IP Model
- 4. Network Addressing
- 5. Application Layer
- 6. Transport Layer
- 7. Network Layer
- 8. Link Layer
- 9. DHCP Overview

página de inicio

## 3. TCP/IP Model

The OSI model gave birth to what eventually became the TCP/IP model and this model is actually what the Internet is based off of. It is the actual implementation of networking. The TCP/IP model uses the TCP/IP protocol suite, which we just commonly refer to as TCP/IP. These protocols work together to specify how data should be gathered, addressed, transmitted and routed through a network. Using the TCP/IP model, we can see how these protocols are used to show the breakdown of how a packet travels through the network.

### Application Layer

The top layer of the TCP/IP model. It determines how your computer's programs (such as your web browser) interface with the transport layer services to view the data that gets sent or received.

This layer uses:

- HTTP (Hypertext Transfer Protocol) - used for the webpages on the Internet.
- SMTP (Simple Mail Transfer Protocol) - electronic mail (email) transmission

### Transport Layer

How data will be transmitted, includes checking the correct ports, the integrity of the data, and basically delivering our packets.

This layer uses:

- TCP (Transmission Control Protocol) - reliable data delivery
- UDP (User Datagram Protocol) - unreliable data delivery

### Ceremonias

No exercises for this lesson.

### Examen

What is the top layer of the TCP/IP model?

✓ ¡Respuesta correcta!

Application

Revisar respuesta

Continuar



Learning | Linux Journey

linuxjourney.com/lesson/network-addressing

WhatsApp Webhttps://discord.com...SKZFLIXPinterestNotion – The all-in-...Nueva pestañaOtros marcadores

Network Basics

- 1. Network Basics
- 2. OSI Model
- 3. TCP/IP Model
- 4. Network Addressing
- 5. Application Layer
- 6. Transport Layer
- 7. Network Layer
- 8. Link Layer
- 9. DHCP Overview

página de inicio

## 4. Network Addressing

Before we jump into seeing how a packet moves across a network, we have to familiarize ourselves with some terminology. When you mail a letter, you must know who it is being sent to and where it is coming from. Packets need the same information, our hosts and other hosts are identified using MAC (media access control) addresses and IP addresses, to make it easier on us humans we use hostnames to identify a host.

### MAC Addresses

A MAC address is a unique identifier used as a hardware address. This address will never change. When you want to get access to the Internet, your machine needs to have a device called a network interface card. This network adapter has its own hardware address that's used to identify your machine. A MAC address for an Ethernet device looks something like this 00:C4:B5:45:B2:43. MAC addresses are given to network adapters when they are manufactured. Each manufacturer has an organizationally unique identifier (OUI) to identify them as the manufacturer. This OUI is denoted by the first 3 bytes of the MAC address. For example, Dell has 00-14-22, so a network adapter from Dell could have a MAC address like: 00-14-22-34-B2-C2.

### IP Addresses

An IP Address is used to identify a device on a network, they are hardware independent and can vary in syntax depending on if you are using IPv4 or IPv6 (more on this later). For now we'll assume you are using IPv4, so a typical IP address would look like: 10.24.12.4. IP addresses are used with the software side of networking. Anytime a system is connected to the Internet it should have an IP address. They can also

### Ceremonias

No exercises for this lesson.

### Examen

How many bytes are in an IPv4 address?

Revisar respuesta

Continuar

Learning | Linux Journey

linuxjourney.com/lesson/application-layer

WhatsApp Webhttps://discord.com...SKZFLIXPinterestNotion – The all-in-...Nueva pestañaOtros marcadores

Network Basics

- 1. Network Basics
- 2. OSI Model
- 3. TCP/IP Model
- 4. Network Addressing
- 5. Application Layer
- 6. Transport Layer
- 7. Network Layer
- 8. Link Layer
- 9. DHCP Overview

página de inicio

## 5. Application Layer

Let's say I wanted to send an email to Patty. We'll go through each of the TCP/IP layers to see this in action.

Remember that packets are used to transmit data across networks, a packet consists of a header and payload. The header contains information about where the packet is going and where it came from. The payload is the actual data that is being transferred. As our packet traverses the network, each layer adds a bit of information to the header of the packet. Also keep in mind that different layers use a different term for our "packet". In the transport layer we essentially encapsulate our data in a segment and in the link layer we refer to this as a frame, but just know that packet can be used in regards to the same thing.

First we start off in the application layer. When we send our email through our email client, the application layer will encapsulate this data. The application layer talks to the transport layer through a specified port and through this port it sends its data. We want to send an email through the application layer protocol SMTP (simple mail transfer protocol). The data is sent through our transport protocol which opens a connection to this port (port 25 is used for SMTP), so we get this data sent through this port and that data is sent to the Transport layer to be encapsulated into segments.

### Ceremonias

No exercises for this lesson.

### Examen

What layer is used to present the packet data in a user friendly format?

✓ ¡Respuesta correcta!

Application

Revisar respuesta

Continuar

Learning | Linux Journey

linuxjourney.com/lesson/transport-layer

WhatsApp Webhttps://discord.com...SKZFLIXPinterestNotion – The all-in-...Nueva pestañaOtros marcadores

Network Basics

- 1. Network Basics
- 2. OSI Model
- 3. TCP/IP Model
- 4. Network Addressing
- 5. Application Layer
- 6. Transport Layer
- 7. Network Layer
- 8. Link Layer
- 9. DHCP Overview

página de inicio

## 6. Transport Layer

The transports layer helps us transfer our data in a way networks can read it. It breaks our data into chunks that will be transported and put back together in the correct order. These chunks are known as segments. Segments make it easier to transport data across networks.

### Ports

Even though we know where we are sending our data via IP addresses, they aren't specific enough to send our data to a certain processes or services. Services such as HTTP use a communication channel via ports. If we want to send webpage data, we need to send it over the HTTP port (port 80). In addition to forming segments, the transport layer will also attach the source and destination ports to the segment, so when the receiver gets the final packet it will know what port to use.

### UDP

There are two popular transport protocols UDP and TCP. We'll briefly discuss UDP and spend most of our time on TCP, since it's the most commonly used.

UDP is not a reliable method of transporting data, in fact it doesn't really care if you get all of your original data. This may sound terrible, but it does have its uses, such as for media streaming, it's ok if you lose some frames in return you get your data a little faster.

### TCP

TCP provides a reliable connection-oriented stream of data. TCP uses ports to send data to and from hosts. An application opens up a connection from one port on its host to another port on a remote host. In order to establish the

### Ceremonias

No exercises for this lesson.

### Examen

What is a reliable transport protocol?

✓ ¡Respuesta correcta!

tcp

Revisar respuesta

Continuar

Learning | Linux Journey

linuxjourney.com/lesson/network-layer

WhatsApp Webhttps://discord.com...SKZFLIXPinterestNotion – The all-in-...Nueva pestañaOtros marcadores

Network Basics

- 1. Network Basics
- 2. OSI Model
- 3. TCP/IP Model
- 4. Network Addressing
- 5. Application Layer
- 6. Transport Layer
- 7. Network Layer
- 8. Link Layer
- 9. DHCP Overview

página de inicio

## 7. Network Layer

The Network layer determines the routing of our packets from our source host to a destination host. Fortunately in our example, our packet is only traveling within the same network, but the Internet is made up of many networks. These smaller networks that make up the Internet are known as subnets. All subnets connect to each other in some way, which is why we are able to get to www.google.com even though it's on its own network. I won't go into detail as we have a whole course dedicated to subnets, but for now in regards to our Network layer, know that the IP addresses define the rules to travel to different subnets.

In the network layer, it receives the segment coming from the transport layer and encapsulates this segment in an IP packet then attaches the IP address of the source host and the IP address of the destination host to the packet header. So at this point, our packet has information about where it is going and where it came from. Now it sends our packet to the physical hardware layer.

### Ceremonias

No exercises for this lesson.

### Examen

What are smaller networks that make up the Internet called?

✓ ¡Respuesta correcta!

Subnets

Revisar respuesta

Continuar

Learning | Linux Journey

linuxjourney.com/lesson/link-layer

WhatsApp Webhttps://discord.com...SKZFLIXPinterestNotion – The all-in-...Nueva pestañaOtros marcadores

Network Basics

- 1. Network Basics
- 2. OSI Model
- 3. TCP/IP Model
- 4. Network Addressing
- 5. Application Layer
- 6. Transport Layer
- 7. Network Layer
- 8. Link Layer**
- 9. DHCP Overview

página de inicio

## 8. Link Layer

At the bottom of the TCP/IP model sits the Link Layer. This layer is the hardware specific layer.

In the link layer, our packet is encapsulated once more into something called a frame. The frame header attaches the source and destination MAC addresses of our hosts, checksums and packet separators so that the receiver can tell when a packet ends.

Fortunately we are on the same network, so our packet won't have to travel too far. First, the link layer attaches my source MAC address to the frame header, but it needs to know Patty's MAC address as well. How does it know that and how do I find it since it's not on the Internet? We use ARP!

### ARP (Address Resolution Protocol)

ARP finds the MAC address associated with an IP address. ARP is used within the same network. If Patty was not on the same network, we would use a routing system to determine the next router that would receive the packet and once we were on the same network, we could use ARP.

Once we are on the same network, systems first use the ARP look-up table that stores information about what IP addresses are associated with what MAC address. If the value is not there, then ARP is used. Then the system will send a broadcast message to the network using the ARP protocol to find out which host has IP 10.10.1.4. A broadcast message is a special message that is sent to all hosts on a network (aptly named for sending a broadcast). Any machine with the requested IP address will reply with an ARP packet containing the IP address and the MAC address.

Now that we have all the necessary data we need, IP address

### Ceremonias

No exercises for this lesson.

### Examen

What is used to find the MAC address on the same network?

✓ ¡Respuesta correcta!

arp

Revisar respuesta

Continuar

Learning | Linux Journey

linuxjourney.com/lesson/dhcp-overview

WhatsApp Webhttps://discord.com...SKZFLIXPinterestNotion – The all-in-...Nueva pestañaOtros marcadores

Network Basics

- 1. Network Basics
- 2. OSI Model
- 3. TCP/IP Model
- 4. Network Addressing
- 5. Application Layer
- 6. Transport Layer
- 7. Network Layer
- 8. Link Layer
- 9. DHCP Overview**

página de inicio

## 9. DHCP Overview

An important networking concept that we did not go over yet is DHCP (Dynamic Host Configuration Protocol)

DHCP assigns IP addresses, subnet masks and gateways to our machines. For example, let's say you have a cell phone and you want to get a cell phone number to start talking to people. You have to call up your phone carrier and they will give you a number. As long as your pay your bills you can keep using your phone. DHCP is the phone carrier in this case, it gives you an IP address so that you can talk to other IP addresses. You are also leased an IP address, these last for a certain period of time, then will get renewed depending on how you have your lease settings.

DHCP is great for many reasons, it allows a network administrator to not worry about assigning IP addresses and it also prevents them from setting up duplicate IP addresses. Every physical network should have its own DHCP server so that a host can request an IP address. In a regular home setting, the router usually acts as the DHCP server.

The way DHCP gets all your dynamic host information is:

1. DHCP DISCOVER - This message is broadcasted to search for a DHCP server.
2. DHCP OFFER - The DHCP server in the network replies with an offer message. The offer contains a packet with DHCP lease time, subnet mask, IP address, etc.
3. DHCP REQUEST - The client sends out another broadcast to let all DHCP servers know which offer it accepted.
4. DHCP ACK - Acknowledgement is sent by the server.

DHCP gets more involved than this, but this is the gist of it.

### Ceremonias

No exercises for this lesson.

### Examen

What are the steps in a DHCP request?

✓ ¡Respuesta correcta!

Discover, Offer, Request, ACK

Revisar respuesta

Return

# **Subnetting**

Learning | Linux Journey

linuxjourney.com/lesson/ipv4

WhatsApp Webhttps://discord.com...SKZFLIXPinterestNotion – The all-in-...Nueva pestañaOtros marcadores

Subnetting

- 1. IPv4
- 2. Subnets
- 3. Subnet Math
- 4. Subnetting Cheats
- 5. CIDR
- 6. NAT
- 7. IPv6

página de inicio

## 1. IPv4

So we know that network hosts have a unique address they can be found at. These addresses are known as IP addresses. An IPv4 address looks something like this:

204.23.124.23

This address actually contains two parts, the network portion that tells us know network it's on and the host portion that tells us which host on that network it is. For this course we will mostly be discussing IPv4 addresses, which are what you commonly will see when referring to IP addresses.

An IP address is separated into octets by the periods. So there are 4 octets in an IPv4 address. If you know a bit of computer science, an octet is 8 bits and 8 bits actually equal 1 byte, so we also refer to an IPv4 address as having 4 bytes. We use bits frequently when dealing with subnets and IP addresses.

You can view your IP address with the ifconfig -a command:

```
pete@icebox:~$ ifconfig -a
eth0      Link encap:Ethernet  HWaddr 1d:3a:32:24:4d:ce
          inet addr:192.168.1.129  Bcast:192.168.1.255
          inet6 addr: fd60::21c:29ff:fe63:5cdc/64 Scope
```

As you can see my IPv4 address is: 192.168.1.129

## Ceremonias

Find your IP address with ifconfig.

## Examen

How many bytes are in an IPv4 address?

✓ ¡Respuesta correcta!

4

Revisar respuesta

Continuar

Learning | Linux Journey

linuxjourney.com/lesson/subnets

WhatsApp Webhttps://discord.com...SKZFLIXPinterestNotion – The all-in-...Nueva pestañaOtros marcadores

Subnetting

- 1. IPv4
- 2. Subnets
- 3. Subnet Math
- 4. Subnetting Cheats
- 5. CIDR
- 6. NAT
- 7. IPv6

página de inicio

## 2. Subnets

How can I tell if I'm on the same network as Patty? Well we can just look at the subnet short for subnetwork. A subnet is a group of hosts with IP addresses that are similar in a certain way. These hosts usually are in a proximate location from each other and you can easily send data to and from hosts on the same subnet. Think about it as sending mail in the same zip code, it's a lot easier than sending mail to a different state.

For example, all hosts with an IP address that starts with 123.45.67 would be on the same subnet. My host has an IP of 123.45.67.8 and Patty's has an IP of 123.45.67.9. The common numbers are my network prefix and the 8 and 9 are our hosts, therefore my network is the same as Patty's. A subnet is divided into a network prefix, such as 123.45.67.0 and a subnet mask.

### Subnet Masks

Subnet masks determine what part of your IP address is the network portion and what part is the host portion.

A typical subnet mask can look something like this:

255.255.255.0

The 255 portion is actually our mask. To make this a little easier to understand, remember how we refer to each octet as 8 bits? In computer science a bit is denoted by a 0 or a 1 in binary form. When binary numbers are used, 1 means on and 0 means off. So what does 8 0's or 1's equal?

Punch into Google "binary to decimal calculator" and convert 1111111 into a decimal form. What do you get? 255! So an octet ranges from 0 to 255. So if we had a subnet mask of 255.255.255.0, and an IP address of 192.168.1.0, how many

## Ceremonias

Use ifconfig to view your subnet mask.

## Examen

True or false, a subnet consists of a subnet mask and network prefix.

✓ ¡Respuesta correcta!

true

Revisar respuesta

Continuar

Learning | Linux Journey

linuxjourney.com/lesson/subnet-math

WhatsApp Webhttps://discord.com...SKZFLIXPinterestNotion – The all-in-...Nueva pestañaOtros marcadores

Subnetting

1. IPv4

2. Subnets

3. Subnet Math

4. Subnetting Cheats

5. CIDR

6. NAT

7. IPv6

página de inicio

### 3. Subnet Math

Ok, we know that subnet masks are important to figure out how many hosts we can have on our subnet. So how many hosts would that be?

Let's say I have an IP address of **192.168.1.0** and a subnet mask of **255.255.255.0**, now let's line up these numbers in binary form. For now use an online calculator to convert these values from decimal to binary.

192.168.1.165 = 11000000.10101000.00000001.10100101

255.255.255.0 = 11111111.11111111.11111111.00000000

The IP address is masked by our subnet mask, when you see a 1, it is masked and we pretend like we don't see it. So the only possible hosts we can have are from the 00000000 region. Remember 11111111 in binary form equals 255, we also account 0 as a host number, so there are 256 possible options. However, it may look like we have 256 possible options, but we actually subtract 2 hosts because we have to account for the broadcast address and the subnet address, leaving us with 254 possible hosts on our subnet. So we know that we can have hosts with IP addresses ranging from 192.168.1.1 - 192.168.1.254.

Ceremonias

No exercises for this lesson.

Examen

What is the binary equivalent of 255?

✓ ¡Respuesta correcta!

11111111

Revisar respuesta

Continuar