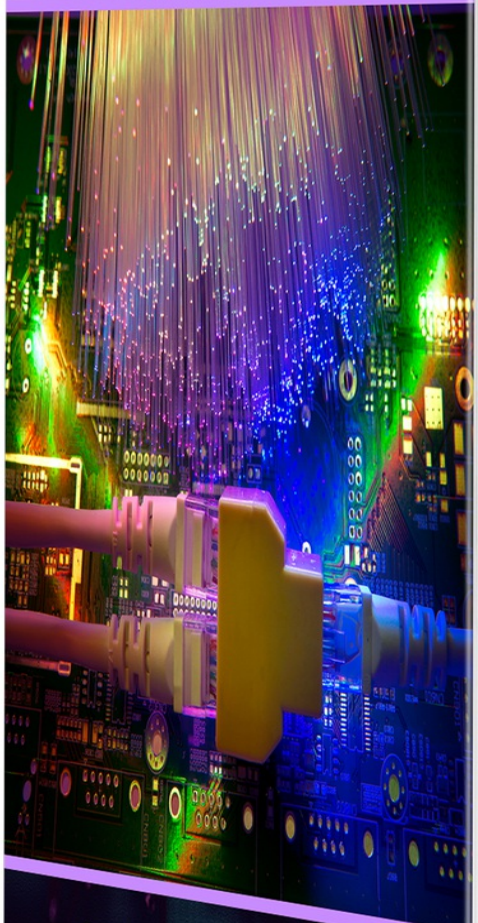
Cisco CCNA Command Guide

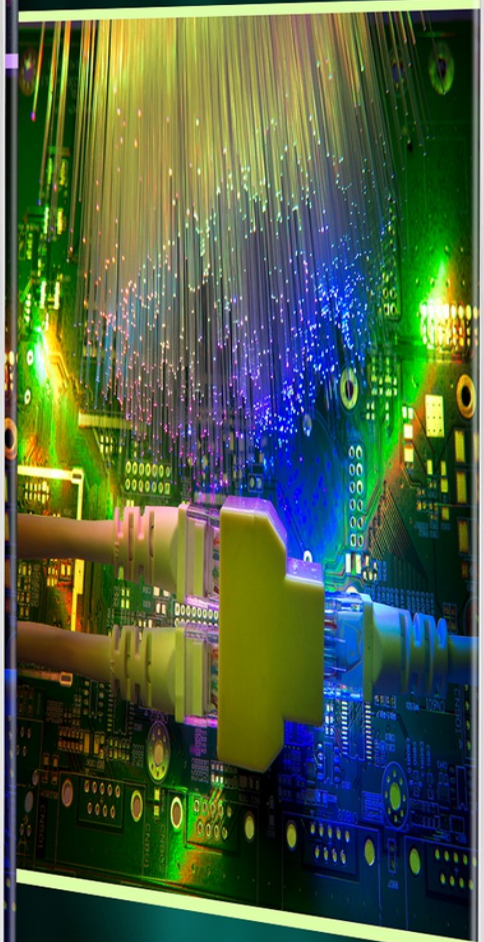
A Comprehensive Beginner's Guide from A-Z for CCNA and Computer Networking Users



STUART NICHOLAS

Cisco CCNA Command Guide

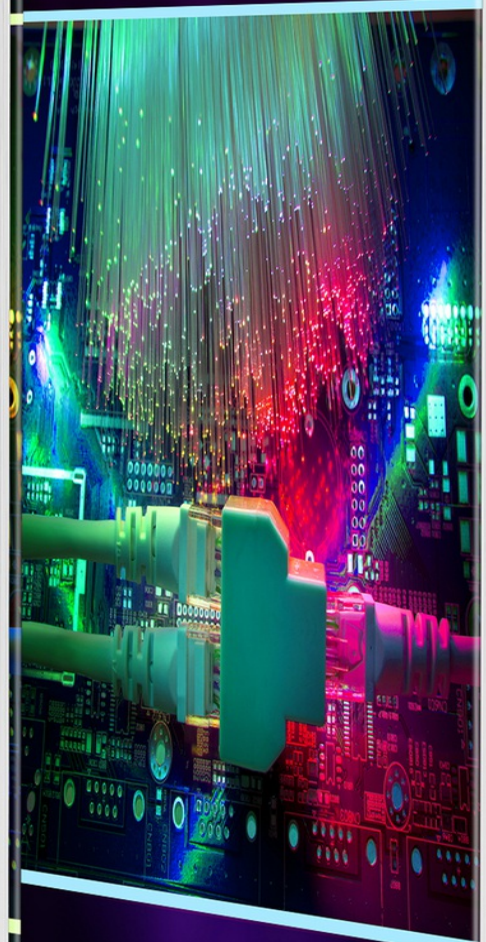
Tips and Tricks to Learn Cisco CCNA Command Guide



STUART NICHOLAS

Cisco CCNA Command Guide

Advanced Methods and Strategies to Learn CISCO CCNA



STUART NICHOLAS

CISCO CCNA COMMAND GUIDE

STUART NICHOLAS

Table of Contents

CISCO CCNA COMMAND GUIDE

Tips and Tricks to Learn Cisco CCNA Command Guide

CISCO CCNA COMMAND GUIDE
Advanced Methods and Strategies to Learn CISCO CCNA

CISCO CCNA COMMAND GUIDE

A Comprehensive Beginner's Guide from A-Z for CCNA and Computer Networking Users

STUART NICHOLAS

Introduction

In addition to a connection between two or more devices to share resources and exchange of information, a computer network enables the interaction of people, reduction of transportation costs, and the realization of distributed processing. To perform these activities, a computer network works with different complexities, because for each objective to be achieved, a network may have different equipment and ways of working. To help you understand these structures, in this chapter, you will study the first concepts about what makes up a computer network and how it works.

In this chapter, you will learn about conceptualizing protocol, Rate networks as its scope, recognize the different topologies of computer networks, and Compare the components as well as physical means used in a network.

With the evolution and the emergence of minicomputers in the 1960s, users had available terminals connected to these central computers, creating the first idea of computer networks. In the mid-1970s, the United States Department of Defense (DoD) has expanded its network used in research and military operations for universities. With this network, it was possible to share the physical environment and using multiple ways to connect two points without the need to use a telephone line connection, starting the ARPAnet.

The Beginning of Data Sharing

However, it was in the 1980s that was a great expansion of information technology and computer networks for home users because, with the advent of personal computers (PCs), home users have access to information technologies, which led to the need for connection between these importers computed. At that time, they originated the Bulletin boards (BBS), where users shared messages and files from your computer to other computers via telephone lines.

Then, in the 1990s, it was the union of these two ideas, the possibility of sharing data and information for users and companies using the physical environment, thus resulting in the internet.

The Internet Today

We are currently experiencing the second generation of the Internet, where certain information is not available in one physical location in the world. Today, information is available on the concept of clouds, i.e., the same information can be in several places in the world and still be changed location without users noticing this movement.

This book will help you to contribute to the evolution of the Internet, understanding and performing the deployment of such services.

Server Architecture and Peer

If you need to connect home computers or business, the way simpler to deploy a computer network is each component looks user folders from their computers to be accessed by others. These mannerisms, you are using the point to point architecture in which all computers on the network share and access data from other computers.

In architecture servers, there is a computer responsible for maintaining and provide information, called a server; computers accessing this information are called stations.

This architecture is widely used in enterprises and institutions that need to ensure the security and availability of information. Therefore, the centered data, it is much easier to perform backups (backup) or ensure the security of information against possible attacks.

The point to point architecture can be expanded to the internet where, through specific programs, you can share files with other users on the internet. Research peer to peer client.

Internet, Intranet, and Extranet

The intranet is where a company can use the same systems and servers that provide information to the internet, only back for the internal public, that is, a place that allows its employees to access restricted information from within the company, but with the same interface a site.

As we have seen, the Internet is a framework that enables information sharing among all global way. However, some information is not de- be public, especially in the business area.

Imagine companies having access to the purchase price of products from its current con-, or your personal data are available for all to access? To protect this information, it created the concept of the intranet.

Already the extranet is an evolution of the intranet; It is to share restricted information from a company with its customers or suppliers, making use of any means of protection as cryptographic cards or passwords. Thus, an undertaking client can access the system from a supplier, for example, ordering products online form.

Structure of Information Sharing

Internet	It is a framework that enables the sharing of data worldwide.
Intranet	It is a network that uses the same systems and servers internet; however, with the internal operation, usually on an enterprise level.
Extranet	It is a resource based on the intranet, typically used in enterprise-level, which allows data sharing restricted between company and customers.

Protocols of Communication

In our relationships in society, daily, use the protocol of good manners, how to respond "OK" or "more or less" when someone asks us "as you are?". This is the concept of protocol, preset messages, and responses that can be used both by individuals or computers to conduct communication.

In a computer network, we use communication protocols to define how the data will be transmitted.

We may use various protocols to establish a single communication:

- one for the definitions of which physical medium is used;
- another for what types of information to be exchanged;
- another to define how they will be dealt with communication errors.

In just one simple connection between two computers, they can be used multiple protocols as needed.

Classification of Networks

Computer networks are physically classified according to their type and scope. When we connect only two computers or devices, we have a link point-to-point, such as used during a telephone connection between two people.

Now, when we have more than two computers, we have a link type multipoint, as used in telephone meetings between several people. Regarding its geographical coverage, networks are classified in three ways:

- LAN (Local Area Network) - Known as local networks are limited to the same continuous physical space such as a room, a building, a company, a condo, or even an industrial complex.
- MAN (Metropolitan Area Network) - These are networks that span one or more nearby cities and share the same physical medium. Making a strategy with the telephone system, area code (DDD) represents a MAN network, and it has a metropolitan scope.
- WAN (Wide Area Network) - are networks of scattered connections over large geographical distances, such as the interconnection of the array of em- arrested in the capital with its subsidiaries inside or interconnection from one country to another.

These interconnections form the WAN may be the most varied possible connections between LAN and MAN networks.

Now it's your turn!

1. Noting the concepts of the intranet, extranet, and Internet, which companies use to structure the sharing sensitive information with its internal public?
2. Cite examples of the links multipoint type.

Physical Topologies

The physical topology of a network is how your devices or computers and a network are physically connected, with three possible structures (See the below Table):

Summary of Physical Topologies

bus	**Ring**	**Star**
Computers are connected to a single cable linearly.	The signal circulates between the computers connected in only one direction.	The signal is distributed to computers through a hub device.

Bus

In the bus topology, all computers are connected to a single cable. In this way, the network can be expanded easily as it is only necessary to extend the cable to insert a new computer on the network.

However, there is a big problem that virtually withdrew this topology strategy of use: if you have a break problem in any part of the cable, all computers will be without the network.

Ring

In the ring topology, the signal circulating between the computers in one direction (Figure below). This enables the network to be deterministic, i.e., after the computers know how long it takes to pass the signal from its neighbors, it is possible to know the total time a signal takes to go through all computers in the ring. However, if there are many stations in the network, it will be slower.

Star

The star networks require hub equipment (explained in more detail below) which distributes the signal between computers. Its disadvantage is the need for a unique cable for each computer, which increases the costs of deployment, but at the same time brings a great advantage in case of rupture of a cable, only one prospect computed will be out of network, not all as occurs in topologies and backslash ring. As a result, the star topology networks are the majority among the existing local networks today, using the Ethernet standard in its structure.

To Know More

The Ethernet standard refers to the physical and data-link connections to a network, such as electrical signals, access protocols in half and speed. These characteristics influence the definition of physical devices and cabling. The definition of this and other standards used in computer networks comes from the Institute of Electrical and Electronics Engineers - IEEE (Institute of Engineers Electrical and Electronics).

Media

A computer network requires necessarily a means of communication for the establishment of a connection. The means defining the communication to be used is the distance desired connection speed and whether or not mobility (Table below).

Communication for the Connection

wire rope	Mainly used in local area networks (LAN), as they are easy to handle. They have high costs and have good rates of speed. This medium is also used for wide area networks, using the existing structure of the telephone companies.
Radiofrequency	Also known by wireless (wireless), allows a point to point or multipoint connection of mobile devices in local networks through computers, phones, tablets, etc.
Optical fiber	means of communication that does not suffer electromagnetic interference extender, since it uses light as a means of transport. Optical fibers are used in networks that require high speeds and/or large distances because, with a single optical fiber, it is possible to pass a continuum net to another.

The use of means of communication for wireless multipoint networks is not restricted to local networks (LAN). They may have a metropolitan scope (MAN), making use of WiMAX or cellular technology.

The RF communication in computer networks is already used for decades, but only to peer connections, in which there is the need for an antenna, has a direct view to another. This medium is employed principally in regions where there is no infrastructure metal cables or optical fibers.

Now it's your turn!

1. Find out what is the physical topology of the network used in the institution where you study.
2. Knife a survey in your town of internet providers that provide a connection by radiofrequency.

Communication Components of a Computer Network

Data communication between distant points has two basic components, called DTE (Data Terminal Equipment) and DCE (Data Communications equipment).

The DTE or terminal transmission equipment is responsible for receiving and transmitting data. In a home network, the DTE would be our computer.

The DCE, or data communications equipment, is responsible for control communication. In a home network, the DCE would be our modem; their responsibility is to receive data from the DTE and DCE transmit to another.

This type of communication using modems is always necessary that the information to be transmitted/received must pass a digital means to an analog medium such as occurs in the use of elements of the public telephone network. Thus, in many WAN connections, the modem is still used.

The modem is the acronym of the modulator and demodulator words. It modulates (turns) and demodulates the analog signal to digital and digital to analog.

For communication in local area networks, the most commonly used components are:

- ***Network Adapter***

Also known as NIC (Network Interface Card), device pre- feel today on every computer to transmit and receive data from other computers.

This device has an identification number called a MAC address (Media Access Control), which is different on all network adapters and serves to computers on a network to identify who they are exchanging information.

- ***Concentrator***

In a multipoint network with bus star, the concentrator is responsible for gathering all the cables coming from the computers in a single device. There are several types of concentrators, among them the recognized are:

  - HUB: when you receive a message from a computer, it forwards this same message to every other computer networks.
  - Switch: It has a table with all MAC addresses of the devices connected to it. Thus, upon receiving a message from a computer, it verifies the destination MAC address and forwards it to the port where this computer is connected.
  - Router: This equipment makes it possible for computers or other devices operating with different physical media and different protocols to communicate through him. For this, when receiving a message from a computer, the router examines its contents and forwards it to the next rewriting device seeing the message so that the device according to understand.

Normally, the router is used to connect LAN to WAN networks using different physical media. The router is also able to choose which way a message should follow when there is more than one alternative.

IMPORTANT

The HUB is a device that allows only one active communication on the network, regardless of the number of computers. Already the Switch allows multiple communications are established at the same time, provided they are between different computers.

Chapter 1

Fundamentals of Computer Networks

As computers began to be used in businesses, schools, homes, etc., there was a need to connect them to each other to share information or data through a more secure and adequate method than soft floppy disks. Due to the above, it is essential to know the management of the networks, from the sharing of programs, printers, hard drives, scanners, servers, and so on.

After studying this chapter, you will be able to identify the types of networks that we can place on a computer, through its structure and characteristics, for the diagnosis and choice of the most convenient type of network, according to the user's needs.

Components

When the software component in a network is referred to, reference is made to the programs necessary to manage the devices that are interconnected by physical means (hardware). But it is important to emphasize that first, the physical components are required so that software or logic ones are installed on them. Software

Components, they are the programs or controllers required to establish communications between physical components, and enable interoperability between devices through communication protocols (see Communication protocols). An excellent example of these components is the network operating systems and the controllers of each of the physical components.

Operating Systems

The main functions performed by a network operating system are to create, share, store and retrieve files from the network, as well as transmit data through the network and its multiple connected computers.

As for the hardware, it is the necessary equipment and primary basis for the creation of a network. Within these teams, the most representative is the following:

- **Work stations:** Computers connected to the network that allows users to access all the resources of the network (database, printer, scanner, etc.).
- **Servers:** Servers are responsible for providing services to workstations connected to the network. Within these services are email, printers, and databases.
- **Repeaters:** Repeaters are devices that amplify the signal emitted by a segment from one network to another, to increase the reach of the same networks.
- **Bridges:** Bridges interconnect two different network segments. One of its main functions is to restrict the sending of information to equipment belonging to the same segment, allowing the passage of those that are directed to different segments and whose MAC address is within the bridge registration table.
- **Routers:** Routers enable the routing of information packets in a network and consist mainly of a routing table, where the routes to the different devices connected in the network are registered.
- **Brouters:** Brouters combine the functionality of a router and a bridge by increasing it. René Montesano Brand, Development of web applications, write SUA, Plan 2005, School of Accounting and Administration.
- **Hubs:** Hubs are electronic devices whose purpose is to increase the reach of a network and serve as a signal distribution point, by concentrating in them a link input cable to the network or main server with several output cables that link to the stations of work. There are several types of concentrators, from the simplest ones, which function as a common and current electrical extension, to the intelligent ones, which have a microprocessor and memory integrated and work with the SNMP communication protocol (simple network management protocol), which gives them the ability to detect collisions and control and diagnose the state of the network.
- **Switching hub or Ethernet switch:** They divide the network into several segments, limiting traffic to one or more of them, instead of

allowing packets to be broadcast across all ports. Within the switches, there is a circuit that works like a traffic light: it creates a series of address tables where each packet is examined and identifies to which segment of the network an address belongs and allows it to pass through it.

It is important to emphasize that, apparently, the previous devices seem the same, but it is not so; each one does and offers very specific functions; In addition, some devices include several of the functions of the hubs, such as router (router) and bridge (bridge) in the same device, for example.

In addition, for the correct installation of a network, inputs such as cables, RJ-45 connectors, jacks, punching pliers, gutters, covers, belts, cable testers, etc. are needed.

So, to choose the hardware components of a network, it is necessary to consider the needs that said network must cover. In this order, the questions to be answered are: what network topology? What is the scope of the network? What the number of machines and other peripherals that will connect to the network? What level of security should the network have? Will it be wired or wireless? What is the transmission speed? And so on.

Topologies

Topologies refer to the way a network is physically structured; that is, how each component of a network connects with the others. There are several topologies, each with decisive advantages and disadvantages for network performance.

To a large extent, the establishment of a topology depends on the following factors:

- Number of Computers
- Amount of wiring required
- Ease of installation
- Way and speed with which data travels on the network
- Easy to detect and repair faults that may occur etcetera

It may be that a network is formed by the union of more than one topology, which is known as hybrid topology, and requires software and hardware, as the central device (hub), bridges (bridges), routers (routers) or doors link (gateways).

When selecting the topology that will have a network, two important aspects should be considered:

1. The physical topology or actual arrangement of the network components.
2. The logical topology or architecture of the network: the way machines communicate within the network.

Network with Bus Topology

The bus or channel topology is distinguished by having the main cable to which all the devices that are going to integrate the network physically connect. The cable or channel propagates the signals in both directions so that all devices can see all the signals of the other devices. This feature can be advantageous if all devices are required to obtain that information, but it would also represent a disadvantage due to traffic: there is a possibility of collisions that would affect the network.

Advantage:

- Ease of incorporating or removing devices from the network.
- Less wiring is required than in other topologies.

Disadvantages:

- The wiring break causes all communication within the network to be broken.

Network with Ring Topology

It is characterized by sequentially connecting all devices (computers, printer, scanner, etc.) in a cable, forming a closed ring, in which each device or node is connected only to the two adjacent devices or nodes.

For the signal to circulating, each device or node must transfer the signal to the adjacent node.

It is possible to establish a network with double ring topology, consisting of two concentric rings, where each device in the network is connected to both rings, although these do not appear directly connected.

This topology is analogous to that of the ring, with the difference that, to increase the reliability and flexibility of the network, there is a second redundant ring that connects the same devices.

In a network with this topology, each device or node examines the information sent through the ring. If the information is not directed to that node, it is delivered to the next node in the ring, and the process is repeated until the signal reaches the destination node.

- **Advantage:** the main advantage in networks with ring topology is the stability with respect to the time it takes for the signals to reach their destination, without collisions.
- **Disadvantage:** its drawback is that the break in the connection of a device throws the entire network.

  The main advantage in networks with ring topology is the stability with respect to the time it takes for the signals to reach their destination without collisions, with the disadvantage that the break in the connection of a device throws the entire network.

Star Topology Network

It comprises a central device called a hub or hub, from which all the links to the other devices or nodes radiate. Through the hub, pass all the signals that circulate in the network, so its main function is to speed up the transmission of signals and avoid collisions.

Advantage:

- Happiness to incorporate or remove devices from the network.
- The breakdown of the wiring of a device only affects it.
- Some connection is easily detected.

Disadvantages:

- The amount of wiring required is greater than any topology.
- The acquisition of the hub increases the cost of installation.
- A failure in the hub affects the entire network.

Network with Hybrid Topologies

The channel, star, and ring can be combined to form hybrid topologies.

Physically, the hybrid ring-star topology consists of a star centralized in a hub, and logically it works like a ring.

The star-channel hybrid topology is a channel or bus that is physically wired like a star through hubs; that is to say, it results from the union of two or more networks with a star topology, connected by a central linear cable that uses the channel topology.

In this topology, the signal generated by one device is sent to the hub, which transmits it to the other hub connected in the channel, and from this hub, it reaches the destination device.

Hierarchical Star Topology Network

Through cascaded hubs, networks with different topologies are interconnected to form a hierarchical network.

Network Architecture

The architecture of a network is the standard that defines how the transmission of electrical signals is carried out. These architectures were created by the manufacturers of the network cards and the means or wiring required.

The most common architectures are Ethernet and token ring. Token Ring Architecture is applied in networks with ring-star topology; the wiring is arranged in the form of a star, but the signals travel in the form of a ring. When a computer transmits data to another, it must wait for permission called a token (witness).

This permit passes from device to device until it reaches one that requires a transmission. When this happens, the address of the sending device, the

address of the receiving device, and the data to be sent are incorporated into the token, and so it goes from device to device until it reaches its destination.

The Ethernet architecture can be used in networks with channel, star, and star-channel topologies. This architecture is based on the following premises:

1. All devices have the same right, possibility, or priority to transmit packets or groups of data.
2. To transmit, you must "listen" until the moment when no device is making a transmission, and then you can do it.
3. Check that while doing a transmission, no other device tries to transmit something, to avoid a collision.

Premises

There are several ways to establish a network; these depend on the selected topology and architecture, the possibility of growth or expansion and updating, and the speed that is required to make transmissions.

Installing a Wireless Network (WLAN)

To communicate different devices, each of them must have a wireless network card installed.

Each access point can serve 20 teams or more. The amount is limited for the use made of the band act; that is, the more devices are running simultaneously, the slower the transmission will be.

Communication Protocols

For data transmission to be successful, the sender and receiver must follow certain communication rules for the exchange of information, known as line protocols.

When different types of microcomputers are connected in a network, the protocol can become extremely complex. So, for the connections to work, the network protocols must conform to certain standards.

Originally, the protocols were relatively simple; for example, on which simple computer-terminal networks were supported, and that was contained in other computer application programs, such that, in addition to its main

processing function, the computer would be controlling the line transmission between it and the associated terminals, and other peripheral equipment.

IBM put into circulation the first set of business standards, which he called Systems Network Architecture(SNA, systems network architecture), but only operated with IBM's own team. As the networks became sophisticated, many computer accessories (equipment from different manufacturers) were incompatible.

To stop this situation, the concept of layer protocols was developed to separate all telecommunications functions to form a set of sub-functions by layers. In a short time, the International Standards Organization (ISO) defined a series of communications protocols called Open Systems Interconnection (OSI, open systems interconnection), whose purpose is to identify the functions provided by any network, taking up the concept of working in layers, with the idea of establishing global design standards for all telecommunications data protocols, so that all the equipment produced is compatible.

In this protocol scheme, each layer would develop a different and self-sufficient task but would be dependent on the sub-layers. Thus, complex tasks would comprise several layers, while simple ones only some. The simple function of each layer would imply simple implementation of circuitry and logistics and would be independent of the functions of other layers so that they could be changed, either the functions or the realization of a functional layer, with minimal impact on logistics and circuitry of the other layers.

Currently, most commonly used data transfer protocols employ an array of layer protocols. It is important to study this arrangement to get an accurate idea of the full range of functions necessary for successful data transfer. In this order, it is essential to consider the functions of each protocol layer established in the OSI model (in Spanish, ISA), which is not in itself a set of protocols but rather fulfills the function of carefully defining the division of the functional layers, with which it is expected to integrate all modern protocols.

The principle of the open systems interconnection model states that as long as the layers interact in a “paired” manner and the interface between the

function of a layer and its immediate upper and lower layer is not affected, how the function of that individual layer is carried out is not important.

This model subdivides data communication into seven “paired” layers that, in descending order, are as follows:

Physical layer (layer 1)

Send the data about the medium. It is a combination of material and logistics that converts the data bits required by the data link layer into electrical pulses, modem tones, optical signals, or any other entity that will transmit the data. It ensures that the data is sent over the link and presented at both ends of the data link layer in the standard form.

Regarding the format that the data must have to be handled by the protocols, the key is to use headers. Each protocol layer adds a header that contains information for its own use; thus, the entire message is longer than the one received from the highest layer (layer 7)

Data link layer (layer 2)

The datalink layer operates only within the individual links of a connection, handling the transmission of data so that the individual bits are sent over those links without error.

Network Layer (Layer 3)

It establishes the end-to-end connection through a real network and determines what permutation of individual links is used (routing functions).

Transport layer (layer 4)

The transport service is responsible for the end-to-end data relay in the communication session; In addition, it establishes the network connection that best suits the session requirements in terms of quality of service, data unit size, flow control, and data mail needs. You must also supply the network addresses to the network layer for the correct delivery of the message.

Session Layer (Layer 5)

The session protocol includes commands, for example, start, interrupt, resume, and end, to manage a communication (conversation) session between devices in an appropriate and orderly manner.

Presentation layer (layer 6)

Your task is to negotiate a mutually consistent technique for coding and scoring data (data syntax) and takes care of any necessary conversations between different code formats or data arrays so that the application layer receives the type it recognizes.

Application layer (layer 7)

It provides communication services to satisfy all types of data transfer between cooperating computers.

In reality, most OSI protocol layers exist only in software and can't be identified as physical elements; however, not all protocol layers demand to be instrumented within the same computer program or carried out by the same part of the team.

Another aspect of the ISO model is that it provides great possibilities and guarantees the development of very sophisticated networks. It may be that very complex functions are not needed; in this case, the model allows the use of null protocols.

For example, in a network that uses similar terminal devices, the syntax conversion possibilities of the presentation layer are unnecessary. In this way, it is avoided to implement functions that could increase the cost and volume of the administration.

Today, the network that connects thousands of networks and millions of users around the world is the Internet, a huge cooperative community without central ownership. In itself, the Internet is the conduit for transporting data between computers. Whoever has access to the Internet can exchange text, data files, and programs with any other user.

But this would not be possible if each computer connected to the Internet did not use the same set of rules and procedures (protocols) to control the synchronization and format of the data. In this order, the set of commands and synchronization specifications used by the Internet is called the transmission control protocol / Internet protocol or TCP / IP.

This protocol allows linking any type of computer regardless of the operating system used or the manufacturer, and the IP system allows networks to send an email, transfer files and interact with other computers, no matter where

they are located, as long as they have access to the Internet.

TCP / IP protocols include specifications that identify individual computers and exchange data between computers. They also include rules for various categories of application programs. In this way, programs that run on different types of computers can communicate with each other.

To understand the operation of TCP / IP protocols, the architecture they propose to communicate networks must be taken into account. Such architecture considers all networks to be the same when connected, regardless of their size, whether local or wide coverage.

Likewise, although TCP / IP software may appear different on different types of computers, it always looks the same to the network; however, all networks that exchange information must be connected to the same computer or processing equipment (equipped with communication devices); that is, routers or bridges. Based on this, Internet activity is understood as an activity of computers that communicate with other computers through the use of TCP / IP.

In addition, so that in a network two computers communicate with each other, both will be accurately identified, since the computer that originates a transaction will identify with a unique address the destination to which it is directed; Therefore, on the Internet, each computer has a numerical address consisting of four parts, known as the Internet protocol address or IP address. This address identifies both the network to which a computer belongs and itself within that network because it has routing information.

Most Important TCP / IP Services

FTP File Transfer (File Transfer Protocol): This protocol allows users to obtain or send files to other computers.

Remote access (telnet): It allows a user's direct access to another computer on the network. To establish telnet, you must set the address or name of the computer to which you want to connect. When accessed by this type of protocol, the remote computer generally asks for a username (user name, login, etc.) and a password (password). When you want to end the session, just close the protocol with the logout, logoff, exit, etc. commands.

Mail on computers (e-mail): Send or receive messages to different users on other computers.

Network File Systems (NFS): It causes a system to incorporate files to another computer in a more appropriate way than through an FTP. The NFS gives the impression that the hard drives of the remote computer are directly connected to the local computer. This creates a virtual disk in the local system. The above, apart from the economic benefits, allows users to work on several computers and share common files.

Remote printing: It allows access to printers connected to the network, for which print queues are created; the use of printers can be restricted, either by a password or to certain users. The benefit is to be able to share these resources.

Remote execution: It makes it run some specific program on some computers. It is useful when you have a large job that is not possible to run in a small system.

Most computers on the Internet (except those used exclusively for internal routing and switching) also have an address called a domain name system (DNS) address, which uses words instead of numbers to make them easier to handle directions to humans. DNS addresses consist of two parts: an individual name and a domain, which generally identifies the type of institution that occupies the address (for example, .com refers to commercial business).

Sometimes, this domain is divided into subdomains to specify more the address (even a domain can also identify the country in which the system is located; for example, .us refers to the USA).

When a computer is at the service of many users, each of them must also identify with a single account within the domain. The standard format includes the user name, separated from the DNS address by the @ symbol (at), which means “in”; for example, jhondoe@gmail.com.

Since the creation of the World Wide Web, the Web or www, in 1989, and the web examiners that developed from it, a world of possibilities has been opened for people to carry out activities through a PC since your home or office, thanks to the Internet.

Types of Networks

Next, the different types of real networks used for sending data will be reviewed, starting with simple point-to-point technology to WAN networks.

The point to point networks, involving nothing more interconnecting two teams, are relatively simple to establish and may employ either digital lines or analog modem lines. Whenever the protocols at both ends of the link match, the data terminal equipment (DTE) easily dialogue.

In its simplest form, a point-to-point network can be worked in asynchronous mode, character by character. This is a common method of connecting remote terminals to a computer. This technique considerably reduces the complexity and cost of the material and logistics needed at remote computer terminals.

This kind of connection does not match the ISO ideal since only computer terminals of this type, and a few manufacturers can be used with third-party computers, but a disadvantage of the ISO model is the volume of equipment and logistics indispensable in each transmission and reception device.

Local Networks (LAN network)

LAN networks (Local Area Network) are small, usually tens of meters; for example, those constituted by the PCs that we find in offices and homes. These types of networks connect a limited number of equipment (printers, PCs, scanners, faxes, etc.), and the connectivity between the elements is ensured through the same wiring. The most used protocol in these networks is the 10/100/1000 Mbit / s Ethernet.

Metropolitan Networks (MAN Network)

MAN (Metropolitan Area Network) networks are produced as an extension of LAN to the most geographically extensive areas and generally cover several kilometers. For example, a company with several branches in the same city would have several LANs in its buildings, and if it were connected through rented lines and equipment that would manage the exchange of information between the networks, it would together form a MAN.

The protocols and network equipment used in the MAN are adapted to work with several devices and a transmission capacity for equipment far superior to local area networks. The most used protocols in this type of networks are FDDI (fo), token ring (Fo), X25, and frame relay.

Wide or Global Networks (WAN NETWORK)

WAN networks (Wide Area Network) or distributed networks are the extensions of the concept of MAN or several regions or geographically remote areas. The most used protocols for these networks are TCP / IP. ATM and frame relay.

It is important to mention that the main functions of computer networks are very accessible in this computing medium, to share necessary and detailed information among users; On the other hand, in the structure of the topologies, it is necessary to know the type and its characteristics, to select the type of network that is most suitable for daily use.

Chapter 2

Basic Architecture of Computer Networking

In the globalized world in which we live, the use of technologies is essential, as they make our daily tasks easier. In this environment, where we need to interact with each other constantly, we rely on a variety of communication resources that interconnect various electronic devices and give us quick and accurate answers, meeting our desires.

This chapter is divided into six sections that present the main networking architecture knowledge required for CCNA.

Data Communication

As Forouzan (2006), data communication is the exchange of information between two devices through a communication medium such as a wire pair.

A basic data communication system consists of five elements:

1. Message: the information to be transmitted. It may consist of text, numbers, pictures, audio, and video - or any combination of these elements;
2. Transmitter: is the device that sends the data message. It can be a computer, a workstation, a phone, a video camera, among others;
3. Receiver: it is the device that receives the message. It can be a computer, a workstation, a phone, a video camera, etc .;
4. Medium: is the physical path through which travels a message addressed to the receiver;
5. Protocol: is a set of rules governing the communication of da-. It is an agreement between devices that communicate.

Streaming Data

According to Torres (2004), there are three types of data transmission:

1. Simplex: In this type of data transmission, one device is the transmitter, and the other is the receiver. Simplex data transmission is therefore unidirectional;
2. Half-duplex: This type of data transmission is bidirectional, but because they share the same communication channel, the devices do not transmit and receive data at the same time;
3. Full-duplex: it is true two-way communication. A and B may transmit and receive data at the same time.

History

As Morimoto (2008c), the networks have gone through a long process of evolution before they reach the standards currently used. The first computer networks were also created during the 60s, as a way to transfer information from one computer to another.

A brief timeline shows some important moments of developing computer networks, as can be seen below.

60 - The Beginning

From 1969 to 1972, it was created ARPANET, the embryo of the Internet we know today. The network went live in December 1969, initially with only four of us, who responded by SRI names, UCLA, UCSB and Utah and were hosted, respectively, at the Stanford Research Institute, the University of California, the University of Santa Barbara and the University of Utah, all of them in the US. They were linked by 50 kbps links created using dedicated phone lines, adapted for use as a data link (MORIMOTO, 2008b, [unpaged]).

The main ARPANET network characteristics were:

a) terminals "dumb" (without processor);

b) communication with a central computer;

c) consolidation of data communication principles;

d) modem appearance;

e) perception by the industry that the use of remote computers would be decisive in the following decades;

f) individual investment of each manufacturer to develop its own teleprocessing technology;

g) the huge growth of teleprocessing networks;

h) geographic expansion;

i) variety of applications;

j) the emergence of the need for users of an access system applied from other systems;

k) interconnection teleprocessing systems;

l) computer networking.

Project ARPA

In 1974, TCP / IP emerged, which became the vo definitive protocol for use on ARPANET and later the Internet. A network linking several universities allowed free traffic information, leading to the development of resources that we USA- today, such as e-mail, telnet, and FTP, that allowed connected users to exchange information, access other computers remotely, and share files. At the time, mainframes with good processing power were rare and incredibly expensive, so they ended up being com- shared between several researchers and technicians who could be located anywhere on the network (MORIMOTO, 2008b, [unpaged]).

The main features of this network were:

a) the early era of computer network technology;

b) distributing applications across multiple interconnected computers;

c) the teleprocessing systems continued to exist; however, each network computer had its own teleprocessing structure;

d) packet switching;

e) the division into several functional layers of the communication tasks

between different computer applications;

f) creating the basic concept of Computer Network Architecture;

g) creating transport protocols;

h) elaboration of mechanisms for flow control, reliability, and routing;

i) development and operation of the first application protocols:

- FTP - File Transfer Protocol;
- TELNET - Virtual Terminal;

j) interconnection American universities computers;

k) interconnection of computers in other countries;

l) opening a new market for companies specializing in the sale of telecommunications services: the provision of data communication services through the provision of a communication structure;

m) standardization of public packet networks from the development in 1976, the first version of Recommendation X.25

Network Concept

According to Sousa (1999), "computer network is a set of interconnected devices to exchange information and share resources such as recorded data files, printers, modems, software, and other equipment."

Classification of Networks

According to Dantas (2002), one of the features most used for classifying networks is their geographic coverage. Thus, it is conventionally divided the classification of local networks - LANs (Local Area Networks), metropolitan - MANs (Metropolitan Area Networks) and wide-area - WANs (Wide-Area Networks).

LAN

According to Das ([SD], p 246.) The local area network - LAN "is a fa- mobility communication that provides a high-speed connection between

processors, peripherals, communication terminals, and devices in general in a single building or campus."

LAN is the technology that has a good answer for inter-connecting devices with relatively small distances and with considerable bandwidth.

MAN

Metropolitan networks can be understood as those that provide the interconnection of local area networks in a metropolitan area of a given region.

WAN

When the distances involved in the interconnection of computers are superiors to a metropolitan area and may be geographically dispersed as large as the distance between continents, the correct approach is the geographically distributed network (WAN).

Topologies

Topology can be understood as how communication links and switching devices are interconnected, effectively providing signal transmission between network nodes. [...]

We can say that the physical topology of a local network comprises the physical linkages of the computational elements of the network, while the logical topology of the network refers to how the signal is effectively transmitted between one computer and another.

Bus

In this type of topology, all PCs are physically attached to the same cable, with it, any computer can use it as communication is being made.

Star

The star topology uses a peripheral hub, usually a hub, connecting all machines on the network.

Ring

In this topology, each computer, following a given direction, is connected to the neighbor computer, which in turn tam- well and connected to the neighbor and so on, forming a ring.

Broadcast Media

According to Tanembaum (1997), several physical media can be used for transmission of data. Each has its own niche in terms of bandwidth, delay, cost, and ease of installation and maintenance. The physical resources are grouped into guided media such as copper wire and fiber optics, and unguided media, such as radio waves and laser beams transmitted through the air.

Coaxial Cable

According to Tanembaum (1997), a coaxial cable consisting of a copper wire stretched in the central part, surrounded by an insulating material. The insulation is protected by a cylindrical conductor, usually a strong interknitted loop. The outer conductor is covered by a protective plastic layer.

Twisted Pair

According to Torres (2004), the twisted pair is the most used network cable type currently. There are basically two types of twisted pair: Unshielded, also called UTP (Unshielded Twisted Pair), and shielding, also called STP (Shielded Twisted Pair). The difference between them is precisely the existence in the shielded twisted pair, a mesh around the cable shielding it against electromagnetic interference.

Categories

According to Morimoto (2008a, [nonpaged]), there are cables of category 1 to category 7:

a) Categories 1 and 2: These two cable categories are no longer recognized by the TIA (Telecommunications Industry Association), which is responsible for defining the wiring patterns. They were used in the past in telephone installations, and category two cables came to be used in Arcnet networks 2.5 megabits and Token Ring 4 megabits but are not suitable for use in Ethernet networks.

b) Category 3: This was the first pair of wires twisted pattern developed especially for use in networks. The pattern signal is certified for up to 16 MHz, allowing its use in 10BASE-T standard, which is the

standard Ethernet network of 10 megabits for cable pair transitional Cado. Still existed a pattern of 100 megabits to Category 3 cable, 100BASE-T4, but it is rarely used and is not supported by all network cards.

c) Category 4: This category cable has a quality slightly superior and is certified for signal up to 20 MHz. They were used in Token Ring networks of 16 megabits and could also be used in Ethernet networks to replace the category three cables. But in practice, this is unusual. As the categories 1 and 2, the category 4 is no longer recognized by the TIA and cables are no longer manufactured, instead of Category 3 cable, which is still being used in telephone systems.

d) Category 5: the category five cables are the minimum requirement for 100BASE-TX and 1000BASE-T networks, which are, respectively, network standards 100 and 1000 megabits currently used. The Cat 5 cables follow much stricter manufacturing standards and support frequencies up to 100 MHz, which is a big jump from the cat ropes 3.

e) Category 6: this category of cable was originally developed for use in Gigabit Ethernet, but with development of the standard cable category five adoptions ended up being delayed because, although the cables category six offer superior quality, the range continues it is only 100 meters, so that, although the best quality cat six cables is always desirable, not just existing Tindo gain much in practice.

f) There are also cables category seven that may be used in the standard 100 gigabits, which is in the early stages of development.

As the cables category five are sufficient for both networks 100 megabits as 1000, they are the most common and cheaper, but the cables Category 6 and Category 6a are very popular and should replace them over the next few years. The cables are sold originally at 300 meters boxes, or 1000 feet (equivalent to 304.8 meters).

Optical Fiber

According to Torres (2001), "the optical fiber transmits information through light signals instead of electrical signals." The optical fiber is totally immune to noise; therefore, communication is faster.

According to Morimoto (2008c), natural successors of the twisted pair cables are fiber optic cables that support even higher speeds and allow for forward virtually unlimited distances with the use of repeaters. The fiber optic cables are used to create the backbone routers that connect the internet key. Without them, the large network would be much slower and much more expensive access.

According to Das (2002), the optical fibers used in networks are classified according to the way light travels in the cable, these being the monomode and multimode.

Singlemode

In a singlemode class, a single light signal is carried directly in the cable core. The signal can reach distances greater without repetition. This form of light traffic compared with the transmission fiber in the second class (Dantas, 2002).

Multimodal

The multimode fiber is characterized by a light beam that travels along its path, making different refractions in the walls of the cable core (Dantas, 2002).

OSI Model and Model TCP / IP

The OSI model attempts to explain the operation of the network, dividing it into seven layers [...]. Although it is only a theoretical model, which does not need necessarily to be followed to the letter by the network protocols, the OSI model is interesting because it serves as a cue to explain various theoretical aspects of network operation. There are books and courses devoted entirely to the subject, trying to explain everything detailed, sorting everything inside one of the layers, but actually understand the OSI model is not that hard.

The OSI Model

As Torres (2004), to facilitate the interconnection of importers computed systems, the ISO (International Standards Organization) has developed a reference model called OSI (Open Systems Interconnection), so that

manufacturers could create protocols from this template.

OSI Model Layers

According to Spurgeon (2000), the OSI reference model is the method to describe how interconnected sets of network hardware and software can be arranged to work concurrently in the networking world. Indeed, the OSI model provides a way to divide the task of the network arbitrarily into separate pieces, which are subject to the formal standardization process.

To do this, the OSI reference model describes seven layers of network functions, described below.

Layer	**description**
Physicist	This layer takes the frames sent over the link layer and transforms them into signals compatible with the environment where the data should be transmitted.
Data Link	The data link layer takes the received data packet network layer and transforms them into frames that will travel across the network by adding information such as the address of the source network adapter, the destination network adapter address, control data, the data itself and checking cyclic redundancy (CRC).
Network	It is responsible for addressing the packets by converting logical addresses into physical addresses so that the packages to arrive at their destination.
Transport	This layer is responsible for getting data sent by the session layer and divide them into packages to be transmitted to the network layer.
Session	The session layer allows two applications on different computers to establish a sessionCommunication.
Presentation	The presentation layer converts the data format received by the application layer into a common format to be used in the transmission of data.
Application	The application layer is the interface between the communication protocol and the application that requested or receive the information over the network.

The TCP / IP Model

According to Dantas (2002), the reference model is the best-known TCP / IP (Transmission Control Protocol / Internet Protocol). The TCP / IP model was designed in four layers.

Layer	**description**
network interface (network access)	This layer, network access, is the first TCP / IP model; its function is to support the network layer, attract the physical and logical access services to the physical environment.
	The level inter-network (Internet) is responsible for sending
Inter-network	datagrams from one computer to any
(Internet)	another computer, regardless of their locations
	on the network.
Transport	The transport layer is responsible for providing support to reliably application layer (or not), whether the services offered by the network interface layers and inter-network.
Application	The fourth layer of the TCP / IP is called the application layer. In this layer, the protocols are that support user applications.

Data Communication Protocol

According to Torres (2004), a protocol is the "language" used by devices on a network so that they can understand, that is, exchange information with each other. A protocol is a set of rules governing the communication data (Forouzan, 2006).

Types of Protocols

There are several types of protocols. Next, described are the main ones:

a) HTTP - HyperText Transfer Protocol - is mainly used for access SAR data on the World Wide Web This protocol allows the transfer of data in the form of simple text, hypertext, audio, video and many others (Forouzan, 2006).

b) SMTP - Simple Mail Transfer Protocol - This protocol is the default e-mail mechanism internet (Forouzan, 2006);

c) FTP - File Transfer Protocol - FTP file transfer protocol is the standard mechanism offered by the internet to copy a file from one host to another (Forouzan, 2006);

d) SNMP - Simple Network Management Protocol - is an Internet management protocol (Dantas, 2002);

e) DNS - Domain Name Server - this application protocol is fun- to identify IP addresses and maintain a table with the ways of the addresses of some networks on the Internet (Dantas, 2002);

f) TCP - Transmission Control Protocol - the feature of this protocol is to provide a reliable service between applications (Dantas, 2002);

g) UDP - User Datagram Protocol - is known for the characteristic of being an optimistic protocol, i.e., it sends all its packages, accredited ing they arrive smoothly and sequentially to the recipient (Dantas, 2002);

h) IP - Internet Protocol - is the main protocol inter-network level in the TCP / IP architecture (Dantas, 2002);

i) ICMP - Internet Control Message Protocol - this protocol is to ob- PURPOSE provides control messages in the communication between nodes in a network environment TCP / IP (Dantas, 2002);

j) ARP - Adress Resolution Protocol - the protocol that maps an IP address in its MAC address (Forouzan, 2006);

k) RARP - Reverse Resolution Protocol - the protocol that maps a MAC address to an IP address (Forouzan, 2006).

IP Addresses

As Morimoto (2006 [unpaged]), "the IP address is divided into two parts. The first identifies the network to which the computer is the connection, and the second identifies the host within the network. "

Classes Address

According to Morimoto (2006 [unpaged]), to improve the utilization of addresses available, developers - TPC / IP shared the IP address into five classes, called A, B, C, D, and E, and [that] the first three are used for addressing purposes, and the last two are reserved for future expansions. Each class reserves a different number of bytes for addressing the network.

In class A, only the first octet identifies the network; in class, B is used the first two octets, and class C has the first three octets reserved for the network, and only the latter reserved for the identification of hosts within the network.

What differentiates a class of addresses of the other is the value of the first octet. If a number between 1 and 126, have a Class A address A. If the value of the first octet is a number between 128 and 191, then we have a class B address, and finally, if the first octet is a number between 192 and 223, will have a class C address.

Network Active Elements

Hub

According to Torres (2004), the hubs are hubs devices, RESPONSIBLE for centralizing the distribution of data frames in physically connected star networks. Every hub is responsible for replicating repeater, in all its ports, the information received by the network machines.

Switch

According to Torres (2004), switches are bridges that contain multiple ports. They send data frames only to the destination port, unlike the hub, which transmits frames simultaneously to all ports. Thus, the switches can increase network performance.

Router

Routers that are bridges operate at the network layer of the OSI Model. They are responsible for deciding which way to go to interconnect different

networks.

Repeater

According to Gallo (2003), the function is to retrieve a signal repeater. Repeaters are also called concentrators and are used in local area networks, increasing its reach.

Bridge

The bridge (bridge) is an intelligent repeater. It operates on the bed of the link of the OSI model. That means it can read and analyze the data frames that are circulating on the network.

Internet, Intranet, and Extranet

Internet

According to Almeida and Rosa (2000), the internet is a set of interconnected computers networks among themselves, which are scattered all over the world. To - of the services available on the internet are standardized and use the same set of protocols (TCP / IP).

Intranet

According to Wikipedia, an intranet is a private computer network that [it] is based on the suite of Internet protocols. Consequently, all the concepts of the last apply also to an intranet, for example, the client-server paradigm. Briefly, the concept of Intranet can be interpreted as "a private version of the Internet" or a mini-internet confined by an organization.

Extranet

According to Wikipedia, the Extranet of a company is the portion of its computer network that uses the Internet to share part of its information system securely. Taken the term in its broadest sense, the concept is confused with the intranet. An extranet may also be seen as a part of the company that is extended to external users (outside the enterprise network), such as representatives and customers. Another common use of the Extra-net term occurs in the designation of the private part of a site where only registered users can browse previously authenticated by password.

Wireless Networks

A wireless network refers to a computer network without the need to use cables. [...] Their classification is based on the area of coverage: personal or short networks (WPAN), local area networks (WLAN), metropolitan area networks (WMAN), and geographically distributed networks or long-distance (WWAN).

WPAN

Wireless Personal Area Network (WPAN) or personal wireless network, normally [is] used to connect electronic devices physically near you, which you do not want to be detected at a distance (WIKIPEDIA). According to Torres (2004), the main equipment used in this network is Bluetooth and infrared.

Bluetooth

Bluetooth is an open standard for wireless communication, developed by the Bluetooth Special Interest Group - SIG, which includes several companies, including Sony, IBM, Intel, Toshiba, and Nokia.

Unlike Wi-Fi standard, which includes the 802.11b, 802.11a, and 802.11g, used in wireless networks, Bluetooth aims to replace the cables, allowing mobile phones, palmtops, mouses, headsets, etc., exchange data with each other and the PC without cables (MORIMOTO, 2007 [unpaged]).

Infra-Red

The infrared is used in wireless LANs, especially those where you need to connect notebooks.

There are two methods for data transmission using infrared light: direct transmission and diffuse transmission. [...] Indirect transmission, the transmitting and receiving devices have a small opening angle, [so they need to be aligned to transmit the data]. In diffuse transmission, infrared signals are sent in all directions.

WLAN

Wireless LAN or Wireless Local Area Network (WLAN) "is a local network that uses radio waves to make an Internet connection or from a network."

Radio

There are two basic modes of data transmission via radio on- (Figure Below).

The non-directional antennas located where the fingertips region of radio waves from the transmitting antenna can capture the transmitted data. [...] This system is widely used in buildings, to connect machines or networks together without cable. The directional transmission, using small satellite dishes, [...] only two networks can communicate. This system has a great advantage, only to transmit data to the receiver (no scattering radio waves to other antennas).

WMAN

Wireless Metropolitan Area Network (WMAN) means metropolitan wireless networks. They enable communication of two nodes distant (MAN) as if they were part of the same local network.

WAN

The Wide Area Network (WAN), wide area network, or long-distance network, also known as the geographically distributed network, is a computer network covering a large geographic area (generally you a country or continent).

Chapter 3

Basic of Ethernet

Ethernet is based on the LANs. The current LAN market is characterized by an unprecedented degree of standardization on the Ethernet. Through its enormous market share of the Ethernet standard relegated despite some disadvantages, all alternative technologies in niche applications.

1980: Digital Equipment Corporation, Intel, and Xerox issued under the name Ethernet Blue Book or DIX standard the first Ethernet standard, version 1.0. DIE ser defined as Thick Ethernet CSMA / CD 10 Mbit / s.

Ethernet is nothing more than a specification of the layers 1 and 2 of the OSI model. So this is not, this is a complete network protocol, but a subnet that can work in the other protocols, such as TCP / IP.

The main functions of ETHERNET are:

- Providing the bit transmission layer
    - Send and receive serial bit streams through the medium of
    - Detecting collisions
- Providing the data link layer
    - MAC sublayer:
        - ➢ The mechanism for access to the network (CSMA / CD)
        - ➢ Structure of the data frames
    - LLC sublayer:
        - ➢ Data Reliability
        - ➢ Providing data channels for overlaying applications

The Physical Implementations

The most important implementations in recent years were:

- Thick Ethernet (10Base5)
- Thin Ethernet (10Base2)
- Broadband Ethernet (10Broad36)
- Ethernet over twisted pair (10Base-T)
- Ethernet over fiber (10Base-F)
- Nearly Ethernet (100Base-T / 100Base-F)
- Gigabit Ethernet (1000Base-T)
- Wireless Ethernet

Implementations Based on Coaxial Cables

The original Ethernet was designed for a bus topology. The first implementations of the Ethernet (10Base5 Thick Ethernet or called) used a thick yellow coax cable.

Characteristics of the original Ethernet:

- 10 Mbit / s
- Baseband (baseband transmission)
- Max. 5 x 100 = 500 m
- Max. 100 transceivers per segment

Coaxial cable for Thick Ethernet has every 2.5 m on a marker to the correction te ensure positioning of the 10Base5 transceiver (or mouse). These transceivers are required to stations on the network to connect. They may only be placed every 2.5 m, to avoid signal reflections, which lead to a deterioration of the transmission quality.

This implementation form was quickly overtaken. After a short time, the rigid and thick yellow coax cable was replaced by a black, flexible, resulting in the

implementation of thin Ethernet (10Base2). The connection of the various stations is accomplished by T-shaped BNC connector pieces, whereby a maximum segment length of about 200 m is possible to apply.

Many bus technologies an important detail is to be noted for wiring: The terminating resistor (terminator) - a small and inexpensive component that must be installed on all ends of the coaxial cable used in Ethernet. A terminating resistor consists of a resistor that is connected to the central conductor of the cable to the shield. When an electrical signal reaches the termination resistor, it is neutralized newly. For the correct operation of a network of the terminating resistor is indispensable Lich, since electric signals of light are reflected at a mirror on the ends of a non-terminated cable as shown.

Implementations Based on Twisted-Pair Cables

The big problem with coaxial cables that communication ren only Halbduplexverfah- is possible. The bus structure used is not ideal when certain problems occur. To break through the limitation of the bus topology, Ethernet has moved to a topology that can be used in the well-twisted pair: where all stations are connected to one or more central hubs. In this way, a star topology can be created. The network can more easily be extended and controlled and troubleshooting easier. The maximum segment length between the subscriber and hub is 100m.

The twisted-pair variants have been further developed by 10Base-T (10 Mbit / s) over 100Base-T (100 Mbit / s) to 1000Base-T (1000 Mbit / s).

The MAU is designed for twisted pair and has four data pins: 2 for sending, 2 for the reception. This is the basis for full-duplex Ethernet. Basically, only point-to-point communication possible because each host is connected directly to a structural element must: a hub or switch.

Fast Ethernet

UTP1 cable, z. B. CAT52 UTP supports data rates up to 100 Mbit / s. The cable consists of 8 conductors, which are arranged in 4 pairs. The four pairs can be identified by the fact that the ladder is always fully colored, while the other conductor of the pair has the same color with white interruptions. Of the four pairs, 100Base-T 2 are merely used (pair 2: orange/white and orange,

as well as pair 3: green/white and green) at 10 /.

The IEEE specification for 10 / 100Base-T Ethernet determines that the one pair of pins 1 and 2 of the connector used to be connected, while the second pair with the pins 3 and 6 are connected. The remaining, unused pairs are connected to pins 4 and 5 and 7 and 8.

Pin code	**color**	**function**
1	green white	+ TD
2	green	-TD
3	orange / white	+ RD
4	blue	unused
5	Blue White	unused
6	orange	-RD
7	brown / white	unused
8th	brown	unused

The above table shows the pinout for 10 / 100Base-T. TD stands for Transmitted Data, RD for Received Data. The plus and minus signs indicate that the signal is sent over the wrong sign two data lines.

Straight cable, also called patch cables, are those in which at both ends of the cable pair 2 with pins 1 and 2 and pair 3 with pins 3 is connected and 6. This cable may be used to make connections between a patch panel or a PC and a hub/switch, or between the PC and the wall jack. Generally, these cables are used for the connection between a structural element and a terminal.

A crossover cable is required to connections between two PCs (connecting two check circuit devices) and to produce between a hub/switch and another Hub / Switch (connection structure of two elements). For producing across cable, the pairs used must be exchanged with each other: At one end of the cable pair, 2 is connected to pins 3 and 6 and pair 3 with the pins 1 and 2.

Current Ethernet ports dominate the so-called autocrossing. This

automatically detected, which cable is used and internally made, if necessary, the intersection.

As an extension of the 10-BaseT standard, the IEEE has defined the Fast Ethernet (100Base-T). Features of Fast Ethernet are:

- Data transmission at a speed of 100 Mbit / s
- Full-duplex operation
- Switched Ethernet

The Fast Ethernet has an auto-negotiation mechanism. This makes possible Ethernet interfaces that automatically / s switch between 10 and 100 Mbit.

When 10Base-T standard, each data bit is mapped into a physical bit. For a group-pe, So eight signals are sent over the wire from eight data bits. The data rate of 10 Mbit / s is a clock frequency of 10 MHz. At each clock pulse, a single bit is sent.

100Base-T is used the so-called 4B5B coding, in which each group of four bits into a 5-bit signal is converted. The individual bits are therefore not converted one to one into signals.

Data Stream: 0111010000100000

4-bit pattern: 0111 0100 0010 0000

5-bit code: 01111 01010 10100 11110

The clock frequency used is 125 MHz (5/4 x 100). Cat5 cables are approved for transmission speeds up to 125 MHz.

Gigabit Ethernet

Gigabit Ethernet aims at a data rate of 1000 Mbit / s. If for doing so. B. CAT5 Ethernet cable to be used, there is a problem, as they only support a clock frequency to 125 MHz. Therefore, should technology adapt?

First, with 1000Base-T two bits per clock pulse (00, 01, 10, and 11) encoding, to which four voltage levels are used.

In addition, in 1000Base-T, all four data line pairs are used for the Ethernet

cable. The four pairs are used here bidirectional: on all four pairs of data are transmitted and received.

So Gigabit Ethernet still uses the 100Base-T / Cat5 clock rate of 125 MHz. Since at each clock signal over each of the four data line pairs, 2 bits are processed, a data transmission rate of 1000 Mbit / s in total. This Modulation server is called as 4D PAM5 called and currently uses five different voltage levels. The fifth level is used for the failure mechanism. The table below shows the pin assignments for the Gigabit Ethernet. While BI is bidirectional; DA, DB, DC, and DD, respectively for data A, data B, data C and D.

Pin code	**color**	**function**
1	green white	+ BI_DA
2	green	-BI_DA
3	orange / white	+ BI_DB
4	blue	-BI_DB
5	Blue White	+ BI_DC
6	orange	-BI_DC
7	brown / white	+ BI_DD
8th	brown	-BI_DC

Implementations Based on Fiber Optic Cables

To allow longer segment distances, the fiber optic cable as a possible interface has been integrated imagine. The first glass fiber variants are known by the name 10Base-F and 100Base-F. In both be used for sending and receiving data separate optical fibers.

Gigabit Ethernet over fiber is designed for full-duplex operation with a data transfer rate of 1000 Mbit / s developed. There are two different versions of Gigabit Ethernet: 1000Base-SX and 1000Base-LX.

1000Base-SX used light pulses with a short wavelength, which are transmitted via a multimode fiber. 1000BASE-LX light pulses have a large

wavelength over a multi- or single-mode glass fiber transmitted. Recently, there are also 10 Gigabit Ethernet over fiber in different variants.

Wireless LAN

IEEE802.11

The IEEE defined under IEEE802.11 different standards for wireless LAN. The Radio connections in a wireless LAN, see the 2.4 GHz band (the so-called ISM3 band) or the 5 GHz band instead. For this, no licenses are required. A wireless LAN comparable applied the so-called spread spectrum (Spread Spectrum). This technique is specifically designed for fault-prone transmission channels. This is particularly the processing of importance because the frequency bands used (especially 2.4 GHz) and numerous other systems, eg. Bluetooth is used.

A wireless network is generally slower than a hard-wired. Its great advantage is flexibility.

As a physical implementation provides IEEE802.11 infrastructure and ad hoc configuration.

The infrastructure configuration, a wireless access point, is used to a wire-wireless LAN to connect to a wired. The Wireless Access Point acts as a Zen trail to route all wireless traffic. Wirelessly operating computers are received in an infrastructure mode, forming a Basic Service Set (BSS)-called te group. It may each be a maximum of 64 individual computers at the same time part of a BSS, as the capacity of the wireless access points 64 on clients is limited. The entire wireless network has been called a unique SSID (Service Set Identifier), also net- kName. This name refers only to the wireless network.

Under Ad-hoc or peer-to-peer wireless configuration is understood to be directly communicated with each participant with others. A real organization of the network is not possible, therefore. An ad-hoc wireless network consists of several devices which are equipped with a wireless adapter. These are connected directly via radio signals and thus form an independent wireless LAN.

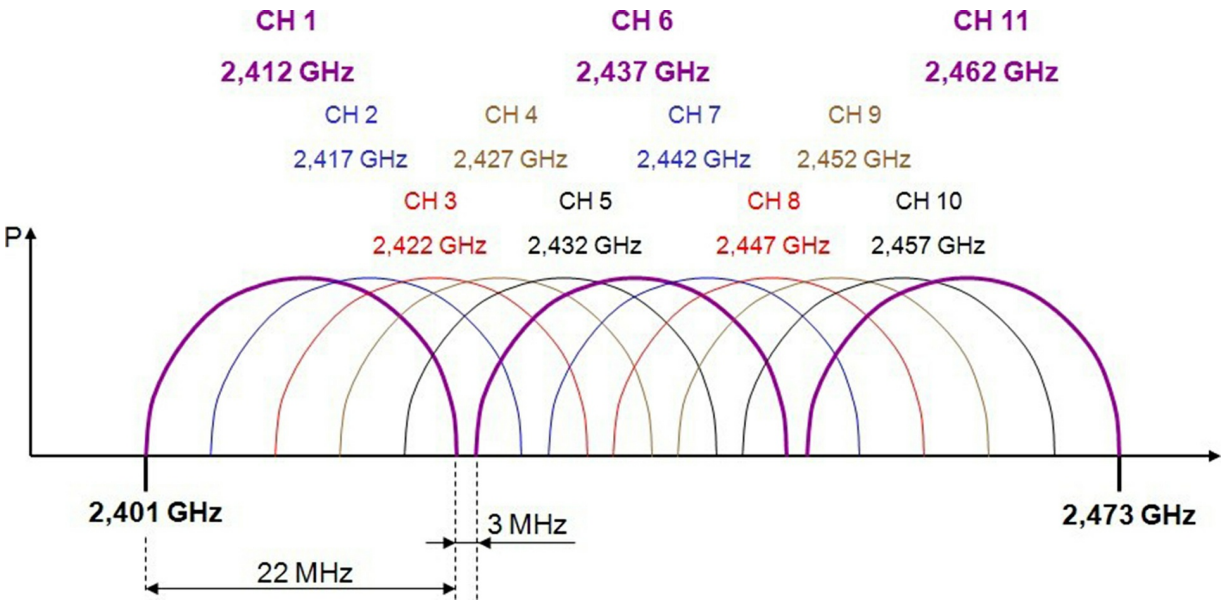
WLAN Standards

As part of the IEEE802.11 different standards are defined. These standards use different modulation techniques to the transmission speeds to optimize reindeer. The table below shows an overview of the various standards.

default	frequency band	transfer rate
IEEE802.11b	2.4 GHz	11 Mbit / s
IEEE802.11g	2.4 GHz	54 Mbit / s
IEEE802.11a	5 GHz	54 Mbit / s
IEEE802.11h	5 GHz	54 Mbit / s
IEEE802.11n	5 GHz and / or 2.4 GHz	600 Mbit / s

IEEE802.11b / g

IEEE802.11b / g using the 72 MHz wide portion of the 2.4 GHz band. Following the regulations of the FCC defined therein, 11 channels with a width of 22 MHz theoretically would be a bandwidth of these 11 channels of 242 Mbit / s (11x22 Mbit / s) possible. In practice, this value is not achieved by far, since the channels greatly overlap. The figure below shows that only three channels do not mutually overlap each other: Channel 1, 6, and 11.

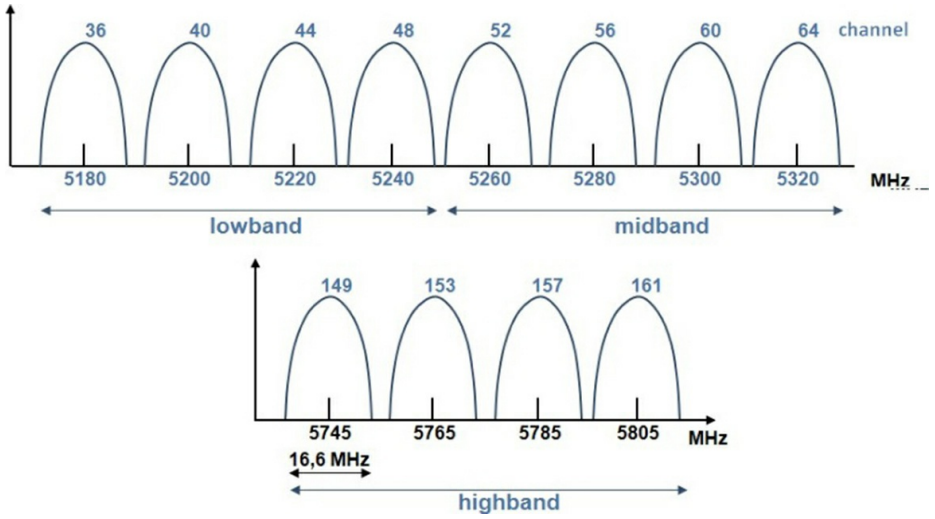


The ETSI defines a slightly larger frequency band with 13 channels wide, each with 22 MHz band. Therefore, generally, 4 to each other hardly-overlapping channels (namely 1, 5, 9, and 13) are used.

IEEE802.11b supports a maximum speed of 11 Mbit / s. With IEEE802.11b, a maximum speed of 54 Mbit / s is possible. A poor connection or distance to the access point, the speed is dynamically reduced.

IEEE802.11a / h

IEEE802.11a uses the entire 5-GHz band. By applying the OFDM (orthogonal Frequency Division Multiplexing), IEEE802.11a reaches a (theoretical) top speed of 54 Mbit / s. The figure below shows the different channels in the 5 GHz band. This means that on the two lowest bands of the 5 GHz UNII band 8, one other non-overlapping channels with a bandwidth of 20 MHz are available.



The use of the 5 GHz band is subject to fluctuations compared to the US numerous restrict-. Therefore IEEE802.11a has been adjusted, which led to IEEE802.11h.

- DCS (Dynamic Channel Selection): The AP will automatically search for another channel if it finds that another application already uses a particular channel.
- TPC (Transmit Power Control): The transmission power is not greater than necessary: If two participants have contact with each other, the AP controls the transmission power to the small most adequate value.

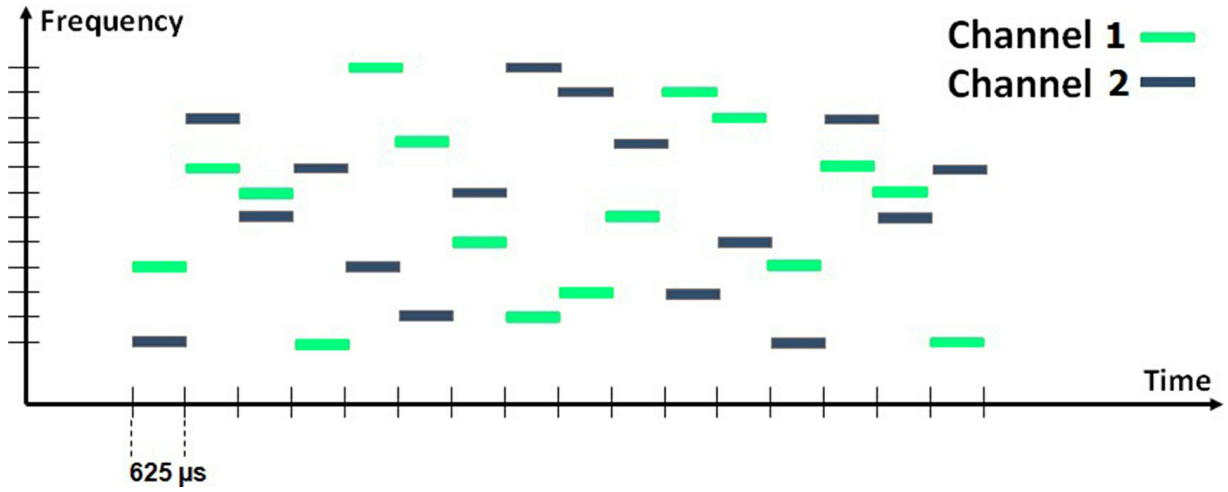
IEEE802.11n

This new standard uses the MIMO (Multiple Input - Multiple Output), which by use of multiple transmit and receive antennas data wirelessly at a speed of up to 600 Mbit / s can be transmitted if 4 channels with a bandwidth of each 40 MHz be used.

Bluetooth

The standard for the basic technology (the two lowest layers of the OSI model) is defined in the IEEE802.15.1. It also defined the Bluetooth SIG (Special Interest Group) different application profiles, including for serial communication and the transmission of Ethernet data frames.

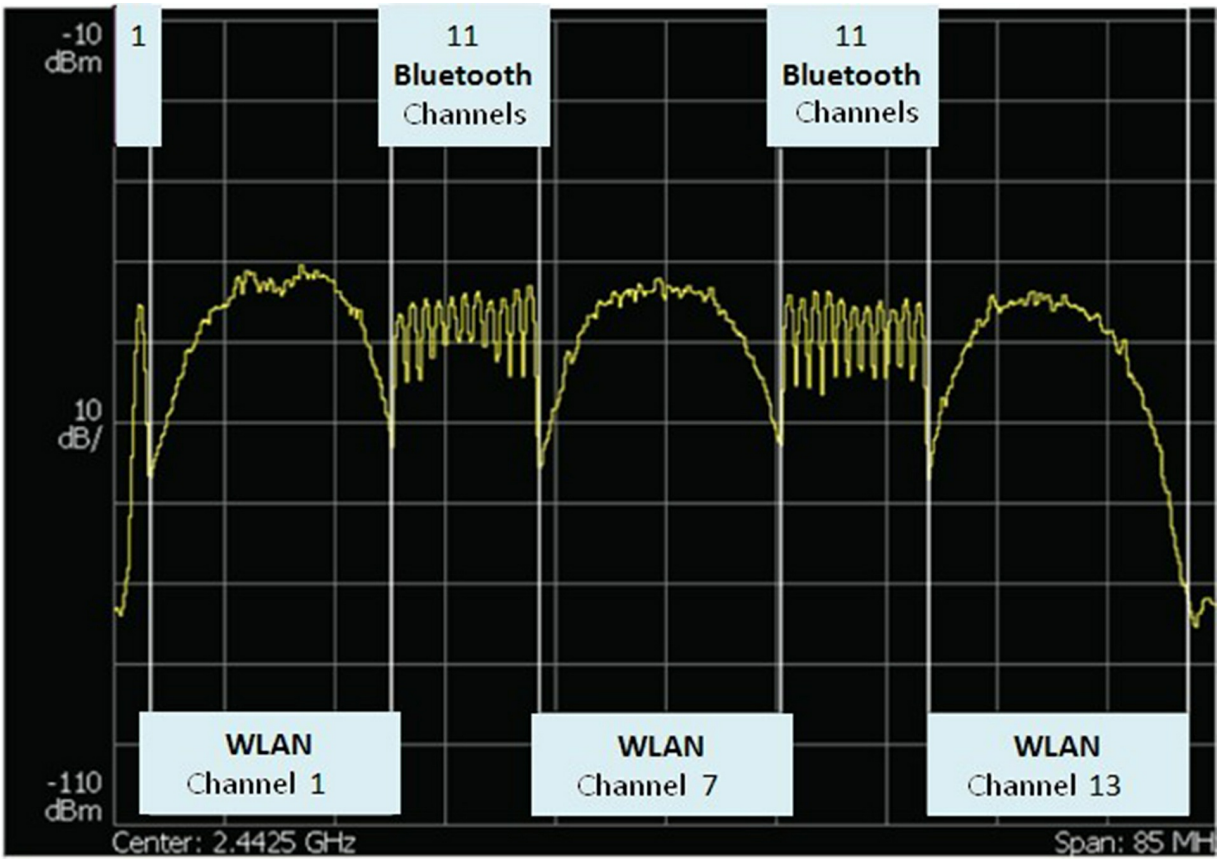
Bluetooth uses the license-free 2.4 GHz ISM band. In contrast to the wireless data to be transmitted will not be spread over a wider frequency band, but it is used for the so-called FHSS (Frequency Hopping Spread Spectrum). Here, the 2.4 GHz band is divided into 79 channels at 1 MHz. The figure below shows the operation of FHSS. There are carried out in 1600 frequency hops per second. Each data frame is in each case sent on a different frequency. In this way, different logical channels can be active together.



A big advantage of using Bluetooth in the industry is the easy coexistence with WLAN. If it occurs on a Bluetooth frequency interference by a wireless channel at the same frequency, Bluetooth can avoid these frequency (s). Since this phenomenon occurs frequently, Bluetooth has an automatic coexistence mechanism: Adaptive Frequency Hopping (AFH).

This mechanism allows Bluetooth to delete certain Bad frequencies temporarily from the list of frequencies used for hopping. The figure below

shows that activity in a crowded 2.4 GHz band with three and not mutually overlap- WLAN channels enough room for Bluetooth. The WLAN channel uses a static frequency band, Bluetooth, however, can be adapted and can choose from a sufficient number of frequencies to avoid interference.



The Data Link Layer

Messages are sent to the packet switching method. Packet switching is mainly used for communication between computers are plants in computer networks data is not transmitted in a continuous stream. Instead, the network system divides the data into small blocks, called packets, which are transmitted individually. Computer networks are, for this reason, also Packet switching network plans (Packet Switching Networks).

The reasons behind using the packages are:

- Transmitter and receiver must coordinate the transfer in the case of transmission errors. Much information is lost. If the data into smaller blocks divided, so the transmitter and receiver can easily

determine which blocks have been received correctly and which were not.

- Multiple computers share the underlying connection and hardware. A network needs to ensure that all computers have equal, direct access to a shared transmission path. A computer may one jointly used resources no longer monopolize, as it is necessary for the consignors to a single packet.

CSMA / CD

Ethernet CSMA / CD protocol used (Carrier Sense Multiple Access / Collision Detect). With CSMA / CD, two or more stations can create a common transmission medium groove- a data frame waiting to be sent must be a station on one idle period "means the inactivity of the bus, sends data in which no participant will then be sent a message, receive the other participants if a second participant simultaneous wants to send a message that a collision is detected the participant who realizes the first collision, sends an error frame (error frame).

A collision domain is a multi-segment configuration in the CSMA / CD protocol, is formed during the collision when two participants in the segment at the same time send a data frame.

A CSMA / CD shows flowchart will send a participant that data must first check the network for the presence of a carrier or a station; the counter sends data. If an active carrier is detected, the data is maintained with the consignors.

Becomes no active carrier is over a period of time greater or equal to the interframe gap, is detected, the station sending the message can begin. During transmission of the message of the participants must continue to check for collisions the medium. Therefore, a network interface must simultaneously send data and listen to the media. If a collision is detected, the transmission is immediately interrupted, and a 32-bit long jam signal transmitted. If the collision is very early detection, the preamble of the frame is first transmitted completely before the jamming signal is transmitted. This jam signal is necessary to ensure that the length of the collision is sufficiently large that all participants can see them. After sending the jamming signal from the user, it

waits a random amount of time before a new attempt is made. This is called the backoff.

Some other important definitions:

- InterFrame Gap: Ethernet stations need two frames between sending a certain inactive minimum time Idle Period stops. The inter-frame gap lasts as long as the transfer of 96 bits (9.6 microseconds at 10 Mbit / s, 960 ns at 100 Mbit / s, and 96 ns in Gigabit Ethernet.).
- Slot time: This parameter is defined as 512-bit times for 10 and 100 Mbit / s, while Gigabit Ethernet is the 4096-bit times. The transmission time for a satisfactory data frame must be a minimum amount to time slot one. The time that is required until all participants must detect a collision, more than one slot time, respectively.

The slot time is an important parameter:

- It specifies the minimum length of a data frame determined (64 bytes for 10 and 100 Mbit / s). Each frame that is smaller than 64 bytes is considered a collision fragment.
- Determines the maximum length of a collision domain to avoid late collisions.
- It ensures that any collisions within the 512-bit times of over-transfer time held the frame.

CSMA / CA

When wireless Ethernet CSMA / can not be used the wired Ethernet CD technology. This standard describes half-duplex radio signals: While DA sent ten, it can not be checked whether any conflicts exist. Remedy creates another technology: CSMA / CA. Instead, collisions to realize they are avoided: CA stands for Collision Avoidance.

The probability of collisions is shortly after a medium was occupied greatest. There are, therefore, defined waiting times and an access phase. The next figure shows some important parameters related to the waiting times for

access to the medium. All parameters are dependent on the time slot, which in turn is derived from the medium caused by the propagation delay. These parameters are:

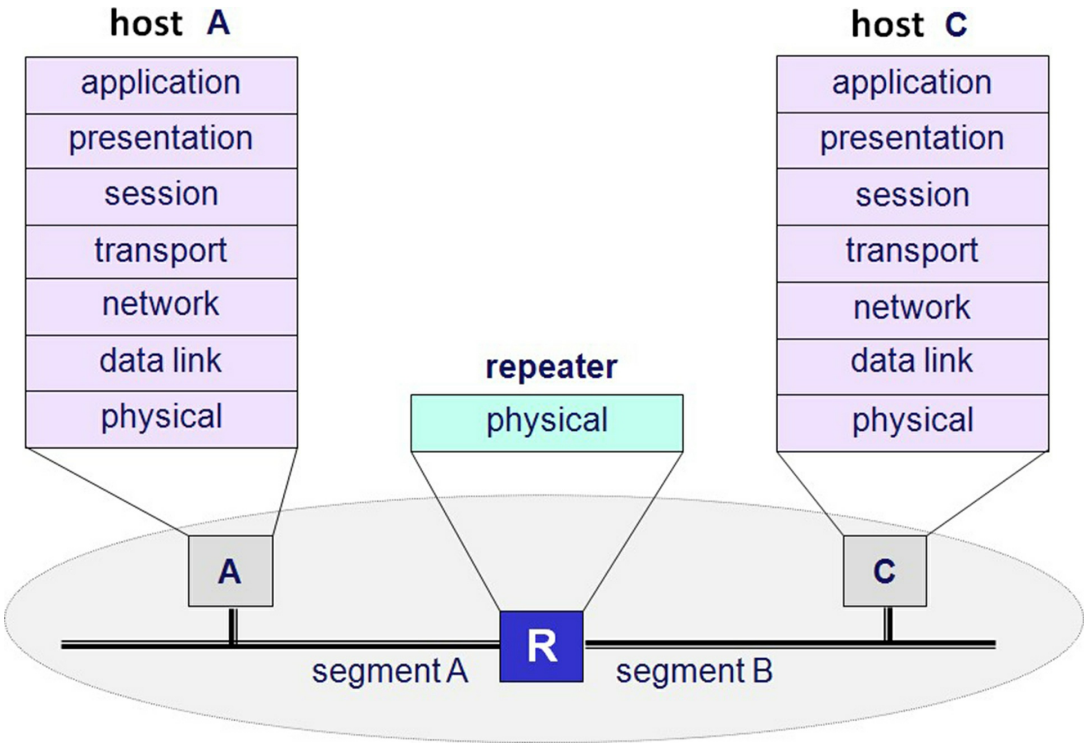
- SIFS (Short InterFrame Spacing): This is the shortest waiting time for access to the medium (the highest priority). The access point uses this waiting time for sending ACK messages.
- PIFS (PCF InterFrame Spacing): This time is for polling an access point comparable uses (medium priority).
- DIFS (DCF InterFrame Spacing): This is the lowest priority for access to the medium and applies to a normal subscriber in the wireless segment.

If the medium is busy, the system waits until the sending participants the transmission process has completed are then must wait DIFS respected. The access point has to comply with a higher priority and must, therefore, only the waiting time SIFS. If the medium is still free after the DIFS, the access phase starts in which each host that wants to send data, a random back-off timer starts. The participant whose backoff timer expires first can take the initiative to send data over the medium.

Structural Elements of the Ethernet

The Hub

The maximum segment length of a LAN is determined by the medium used and to those used access mechanism. To remove the restriction on the length, it was within a short time element with finding methods for coupling, and several segments started together. The first and easiest method here is the use of a repeater. A repeater is a signal amplifier that packets are regardless of their content transparent. With a repeater, two or more Ethernet segments can be connected together. As seen in the figure, a repeater coupling according to ISO / OSI, find definitions on the bit transmission layer instead.



The transmission media of the segments can be different. Thus, as a 10Base-T segment is coupled using a repeater to an optical fiber segment. Another important feature of a coupling with a repeater is that not only the data bits but also checks for collisions and signal errors are passed. Network segments, which are interconnected via a repeater, are therefore sensitive learning situations for fault: A in one of the segments occurring error is also continued in all the other segments. In modern local area networks based on Ethernet repeaters to interconnect segments of different media are used mainly. Thus, for example. B. backbone segments (fiber) always via optical repeaters to department segments with twisted-pair cabling connected.

A hub is actually a multiport repeater: He is an incoming signal to all ports On the other reindeer on, as shown in Figure above to see. All segments interconnected via a hub form a collision domain.

Hubs are available in many different versions. They differ in the number of ports supported media types and extensibility.

An important feature of modern hubs is the ability to network management. Hubs may comprise at least arrival ports or off, and detect faults around. To ask choices available, modern hub with an SNMP agent feature, which is managed by a management station.

The Switch

One of the ways LAN segments with higher intelligence to be connected with each other is to use a bridge. A bridge is more than just a medium for the WEI Pass on of data such as the repeater. A bridge examined before passing a packet from one segment to another, the MAC address, and decides, depending on whether the transport takes place in the other segment or not.

A bridge can have two network ports more. In this case, the designation is needed voltage switch. For each port, the MAC address table is maintained by software. This table is filled in, in which the switch's MAC addresses that the sender addresses the participants as waste use registered. Each address is maintained for a limited time in the table and then deleted when a certain time, the aging time has elapsed. In this way, prevents stations no longer recognized or inactive stations are addressed.

The use of a switch for coupling of segments in a local network has overall genüber the use of a repeater or hub some advantages. Thus, for example. B. not charged with the use of switch segments with frames that are addressed to other segments. This feature of the bridge, therefore, reduces the load per segment. Likewise, error situations will not be because the switch also checks the correct assembly of the frame. Finally, it is also prevented by the bridge that piston is passed between frames from one segment to another. Each port on a switch so concludes a collision domain. If each participant is connected directly to the port of a switch, though created many collision domains, but each of them contains only a single subscriber. Therefore, no collisions can occur. It will be discussed in more detail elsewhere on the switch.

802.1Q Tagged Frame

IEEE801.1Q describes four extra bytes, divided into two fields in an Ethernet frame, to enable new applications. One of these applications is the VLAN (see further below in this chapter).

Description of the additional fields:

- TYPE (TAG), 2 bytes: 8100h obtains the value to indicate that the frame in question is tagged and therefore contains an additional information field

- VLAN TPID, two bytes: VLAN Tag Protocol Identifier
    - User Priority, 3 bits: here the priority of the frames are also transmitted, the priority code (a number between 0 and 7) is described in IEEE802.1p
    - CFI: Canonical Format Indicator. 802.1Q is designed exclusively for Ethernet or Token Ring networks. This bit is 0 for Ethernet and one for Token Ring.
    - VLAN ID: ID of the VLAN, 4094 options
        - ➢ FFFF reserved
        - ➢ 0000 hci VLAN, frames prioritizing (Profinet IO)

Power over Ethernet

IEEE802.3af (Power over Ethernet) since June 2003 offers the possibility for simultaneous transmission of data and power over the same Ethernet cable.

PoE for wireless access points, Bluetooth access points, IP telephones (Voice over IP), IP cameras, RFID readers, touch screens, etc. have been developed. Even before the introduction of these standards, non-standardized systems were used which transfer a supply voltage of 24 or 48 V on the unused wires of the Ethernet cable run on the devices that can be restricted and controlled by the IEEE802.3af standard. Through the use of a separate PoE power supply is unnecessary. This is especially useful when the network device to be used in a place where power is difficult to realize a power socket.

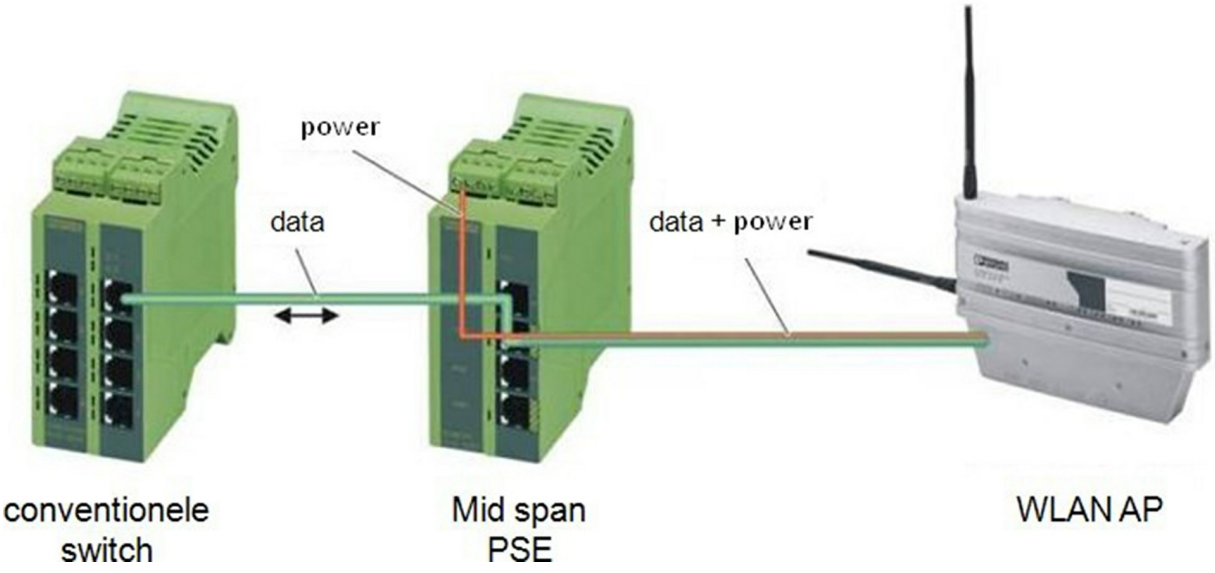
The protocol defines two basic components: the PSE (Power Sourcing Equipment) and the PD (Powered Device).

PSE

The device, which provides the supply voltage for the PoE available is called PSE (Power Sourcing Equipment). The provided by the PSE available nominal voltage is 48 V (44-57 V). Each port of a PSE must at 44 V to provide a current of 350 mA is available (15.4 W).

There are two different types:

- End Point PSE: a PoE switch replaces the standard Ethernet switch
- Mid clamping PSE: this device is inserted factory participants between the conventional switch and the network (only possible with alternative B, see below)



The figure above shows the integration of a mid-clamping PSE. It is only necessary for an additional module to enable PoE.

PD

Network stations that receive their power via the Ethernet cable, advertising the PD (Powered Device) called. To prevent damage from reverse polarity, PDs are equipped with reverse polarity protection. A PD, according to the standard, must Alternative A or B supported (see below).

The standard specifies that a PSE affords at least 15.4 W, and a PD at most 12.95 W may commence. The difference is necessary for covering losses in the twisted pair compensate. A 100 m long cable has an electrical resistance which provides a voltage drop along the line.

To protect equipment against unexpected stresses, is in preparing the conjunction, an identification process is performed:

If nothing is connected to the PSE, the port is idle.

- A device reports k with a resistance of 25Ω on.
- The PSE applies a voltage of 10.1 V and measures the current. If the current flow is less than the minimum current, the voltage supply is interrupted.
- To determine in detail the class (0 to 3), the PSE applies a voltage of 20.5 V. After determining the class, the PSE applies a voltage of 48 V. We distinguish the following performance categories:

  great 00.44 W and 12.95 W

  great 10.44 W up to 3.84 W

  great 23.84 W up to 6.49 W

  great 36.49 W and 12.95 W

Alternative A

Here, the voltage is transmitted via the data lines. The voltage is supplied via transformers with center available and to pins 1-2 and 3-6 connected so that it is invisible to the data stream. This method is suitable for 10/100 / 1000Base-T.

Alternative B

Here, the energy is transmitted via the data that are not used in a UTP cable for data transmission wires. The pairs 4-5 and 7-8 are used in parallel to the chip to minimize voltage drop along the line. Plus lies at pins 4 and 5 to pins 7 and 8.

This method can only be applied when the pairs 1 and 4 are available STE hen (certain industrial Ethernet cable contains only the pairs 2 and 3), and they are not used (at 1000Base-T; therefore, the application is not possible).

VLAN

A VLAN or Virtual Local Area Network is a group of participants in a larger network that forms a logical way, a separate network. In this way, multiple

logical groups can be created in a larger physical network. A VLAN form a separate broadcast domain. Data packets are only within a VLAN forwarded. All participants must be physically located in a common men network, and this network can be using VLANs then divided into logical segments. Some examples of the division into a network:

by department: one VLAN for the sales department, another for the engineering and another for automation

- by hierarchies: one VLAN for the management, another for the manager and WEI teres for workers
- to use: one VLAN for users who use e-mail services, another for multimedia users

Benefits of VLANs

The biggest advantage of VLANs is the segmentation of the network. Other benefits include improved security and the ability to network load balancing.

- Mobility of devices: devices can be implemented within the network easier to advertising. In a traditional network, cabling must be adjusted if a user moves from one subnet to another. Moving from one VLAN to another, however, does not require any changes in the wiring: It means only an adjustment be made to the switch. So a station in the sales department can be implemented at a network port of Engineering. For this, the port must the engineering VLANs are configured as a member; however, new cabling is unnecessary.
- Additional safety: devices of a VLAN can communicate only with other devices of the same VLAN. If it wants to communicate a device of the sales VLAN with the VLAN automation, it must link set in a router advertising the.
- Restriction of traffic on the network: In a traditional network can broadcast network congestion care. Devices often receive broadcast messages that they do not need. VLANs limit this problem as VLANs own broadcast domains form.

Trunking

Trunking (bundling) is exchanging different method VLANs to data between two switches provided. For this, only one port is needed per device. There are various methods for carrying out the metal trunking:

- ISL: Inter-Switch Link, a widely used proprietary protocol from Cisco
- 802.1Q: one of many switch manufacturers supported standard

When trunking a small piece of code (one day) added in which is recorded, from which VLAN the transmitted packet. Through this system, the benefits of VLAN remain. The VLANs remain separated, even if they are spread over separate switches. To still allow traffic between different VLANs, a router is needed.

Types VLANs

VLANs can be divided into two types: static and dynamic VLANs.

Static VLANs are port-based. The user belongs according to the port to which it connects his device, for one or another VLAN.

Benefits:

- easy to configure
- Everything happens in the switch, and the user hardly notices anything about it. Cons:
- If a user's PC to the wrong port connects, the administrators need tor a reconfiguration is performed.
- If at one belonging to a given VLAN port, a second switch is connected, include all computers that are connected to that switch automatically to this VLAN.

Dynamic VLANs: These are not based on the ports of a switch, but to the address of the user or the protocol used.

Advantage: No matter is a computer connected to which port, he is always on

the correct VLAN.

Disadvantage: The cost of this VLAN type is higher because special hardware is needed.

Network Redundancy

Under Network redundancy, the integration of hardware and software is meant to ensure that remains the failure of a single point of failure network. The communication system, the network is the heart of every modern automation project. To absorb network error, different protocols can be integrated into structural elements. There are three main groups:

1) STP / RSTP (Rapid) Spanning Tree Protocol. in meshed topologies that can be locked applies.
2) MRP: Media Redundancy Protocol, exclusively for ring topologies.
3) PRP: Parallel Redundancy Protocol

The Protocol of Spanning

The STP is a Layer-2 protocol that ensures a loop-free and closed LAN. It is based on a wound of Radia Perlman (an employee of Digital Equipment Corporation) corresponds algorithm. With spanning tree, it is possible networks with redundant paths build. In this way, an automatic backup network path can keep the advertising when an active path fails for any reason, is required without the need for closed loops in the network.

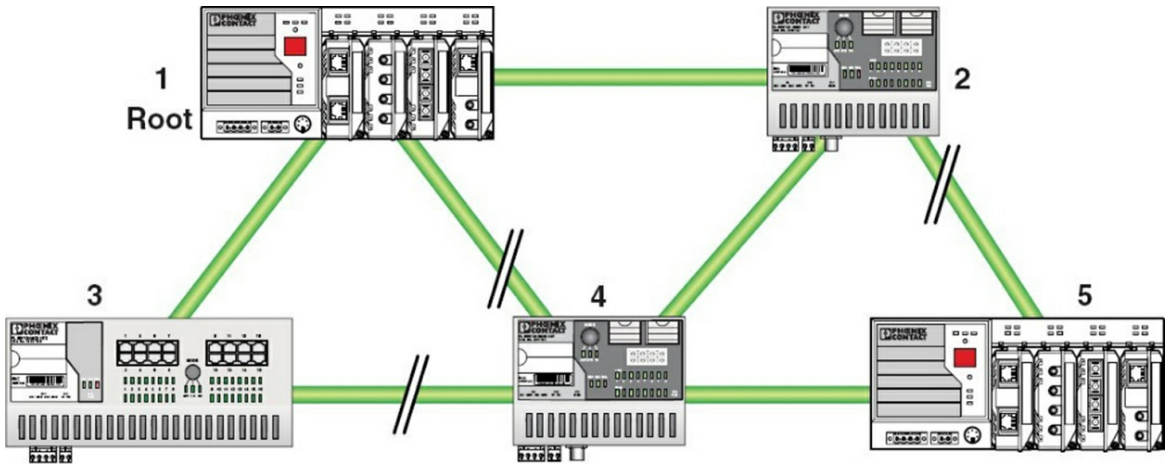
To use this protocol, it must be supported by the used switches. After an interruption of a segment, it can take up to 30 or 50 seconds until the alternative path is available to take. For control applications, such this delay time can not be acceptable, even for monitoring tasks 30 seconds very long. One advantage of STP is that it can be used not only for redundant ring structures.

The Rapid Spanning Tree Protocol

In response to the shortcomings of Spanning Tree Protocol, IEEE 2001 formulated the Rapid Spanning Tree Protocol (RSTP). This is described in IEEE802.1w. Since 2004, the STP is described in IEEE802.1d as

unnecessary, and it is recommended to use RSTP instead. Therefore, even IEEE802.1w standard 802.1d were included in the.

The switching time of RSTP is shorter than that of the STP (hence the name); it takes only 1 to 10 seconds instead of 30 to 50. Depending on the application, this switching time may already be fast enough.



The figure above shows a network with five different structural elements. It created various dene redundant connections. Thus impermissible loops may occur that will bring the network quickly into saturation. The RSTP converts this topology by switching off some ports into a tree structure. Here, one of the Structural elements is configured as root. From this root of all switches via a single path can be reached. If a network failure occurs, a new active path is created.

Enhancements to the RSTP

To meet the needs of automation, some manufacturers use proprietary extensions of the RSTP to achieve switching times under one second. In this way, the QoS is achieved for the redundant building automation networks.

Nearly ring Detection RSTP is an extension of Phoenix Contact. In case of failure of a network switch, switching times are achieved from 100 to 500 ms. Switching of max. 500 ms can be achieved for large automation networks with 1000 address entries in the switches. With fewer devices on the network, shorten times. This protocol is, however, only be used for 10 or 100 Mbit / s.

Bridge Protocol Data Units (BPDUs)

The tree structure is calculated using a specific algorithm, wherein a switch is configured as the root. Each switch has to have all the necessary information to determine the correct port rules. To ensure that each switch has sufficient and accurate information available, the switches exchange below the other information. For this purpose, special frames called Bridge Protocol Data Units (BPDUs) are used.

A bridge sends a BPDU, while the individual MAC address of the port as SA itself and as DA, the STP multicast address 01: 00 used: 80: C2: 00: 00th There are various working ten BPDUs:

- Configuration BPDU (CBPDU) for the calculation of the spanning tree
- Topology Change Notification BPDU (TCN) to notice of network changes
- Topology Change Notification Acknowledgment (TCA)
- To create a loop-free network, each port of a switch, a status assigned. Specifically, these are:
- ROOT: Port, which forms the path to the root switch
- DESIGNATED: active port which forms a path to lying in the hierarchy of the tree structure below Switch
- ALTERNATE: a port having a lower priority, an alternative path to the root

Multiple Spanning Tree Protocol (MSTP)

In an Ethernet environment with Virtual Local Area Networks (VLAN), Spanning Tree Protocol may also be used.

The originally defined in IEEE 802.1s and later recorded in IEEE 802.1q 2003 MSTP defines an extension of RSTP in combination with VLANs. Thereby the advantages of trains PVST (Per-VLAN Spanning Tree) defines its own spanning tree in which each VLAN, and the original IEEE 802.1Q, in which only a single spanning tree is built up across the network, combined with each other.

When MSTP different VLANs into logical instances (VLAN Groups, the same spanning-tree topology) are divided. When MSTP all spanning-tree information is summarized in a single BPDU to limit the number of BPDUs. Compatibility with RSTP switches is fully guaranteed.

Media Redundancy Protocol

MRP is part of the PROFINET standard. In MRP, a ring manager a port blocked, so as to obtain an active bus structure. In a network failure, the network is divided into two isolated network segments, which are again coupled to each other by releasing the blocked ports. The maximum guaranteed switching times are 200 ms.

Parallel Redundancy Protocol

In contrast to the technologies mentioned above, PRP provides no change in the active topology with a network error. This protocol works on two parallel networks. Each data frame is sent over both networks. The receiving node processes the first incoming message and discards the later inbound copy. PRP ensures for copying and discarding the messages. Also, PRP makes the second network for the higher layers of the communications stack invisible.

Important Supplements

LLDP

The IEEE802.1AB protocol (Link Layer Discovery Protocol, LLDP) is a standard that can be solved with the configuration problems for large LAN structures. The protocol defines a standard way for switches, routers, wireless access points, etc. to transmit information about themselves to other network participants and to store information about neighboring participants. LLDP is possible with all 802 media. It operates at the data link layer.

A switch that supports LLDP can other participants that also support this protocol, perform topology detection. Benefits:

- Improved detection of network failures
- Aid in the replacement of modules

- Better network configuration and better network management

LLDP information is used in engineering tools to graph network topologies.

EEE 802.1x

IEEE802.1X is a security standard for authentication on each individual port switches. The authentication takes place before the participant can access the network. The detection of an authorized subscriber, therefore, occurs at layer 2 of the OSI model, and that - depending on the hardware used - both in wireless and wire-bound in networks.

IEEE802.1X uses a protocol for exchanging information with participants/devices to permission to access the network via a port request. The Messages contain a user name and password. The switch performs an authenticated notification of itself but depends, in turn, a request to a RADIUS authentication server on the network. This server processes the request and notifies the switch which port to open for the participant.

As part of the protocol, there are three important players:

- The user or client, it is referred to in the report as SSupplicant ";
- The access hardware (a switch or access point) acts as Äuthenticator ";
- RADIUS infrastructure is the controlling authority: the Äuthentication Server. "

The 802-1X authentication is done via a flexible mechanism: the Extensible Authentication Protocol (EAP), are possible with the various forms of authentication. Thus, the authentication can be attributed to superiors, depending on the type of user in different ways: strong or weak. For example, the use of a combination of user name and password can be prescribed for students, while employees use a certificate. In the chapters on safety are covered in more detail on this point.

(Also called trunking or bundling) Aggregation with LACP IEEE 802.3ad Link Aggregation is the English name of a method for combining multiple physical network connections to a higher transmission speed target to be

expected. With link aggregation, a redundant path can be provided advertising to, so sensitive systems an additional fault tolerance is added. The technique is used in switches and network interface cards (NICs).

The IEEE 802.3ad standard currently describes the Link Aggregation. It offers the following advantages:

- Higher availability of the paths
- Increasing the capacity of a path
- Higher performance with existing hardware

The current LAN technologies see data rates before 10, 100, and 1000 Mbps. With link aggregation, if necessary, intermediate values can be achieved. By bundling of several 1000-Mbps paths and high-speed connections can be made.

Link aggregation is possible in several ways:

- The link between two switches
- The connection between the switch and terminal
- The connection between two terminals

The figure above shows, such as switches is connected via two 100 Mbps lines. If one of these compounds is omitted, assumes the other of the Link Aggregation Group.

The IEEE 802.3ad standard currently describes the Link Aggregation. In this method, one or more compounds to a so-called link-aggregation Ag Group can be bundled. A MAC client can use this group then as if it were a single compound (IEEE 802.3 standard, Edition 2000).

The IEEE802.3ad standard also describes the use of the LACP (Link Aggregation Control Protocol) to exchange simple way configuration information between the different systems. In this way, an automatic configuration is also possible Lich like surveillance of all link aggregation groups. The exchange of information happens over those described in the standard LACP frames.

Industrial Ethernet

In recent years, the Ethernet is turning more and more reasonable in industrial environments. The differences between office and industrial environments are great. The term Industrial Ethernet refers to the use of industrial products, to satisfy the specific requirements of the industry.

Chapter 4

TCP / IP

Transmission Control Protocol / Internet Protocol (TCP / IP) is a collection of standard protocols, which was to communicate over large networks, which consist of various interconnected via routers network segments developed.

TCP / IP is z. As usual, etc. connect the Internet, the collection of thousands, globally distributed networks, research centers, universities, libraries, businesses, private individuals.

In contrast, the intranet is a very general term. An intranet is not limited in its size: there are Intranet, which a few, but even those that include hundreds of networks. With the term Internet, however, the global or public Internet is called as the public internet.

This raises the question of how two different hosts that are connected to different networks with a large distance from each other to communicate.

The second part of the answer is a software aspect: to be active on every host needs a universal communication service. Although there are numerous software protocols for intranet, a family stands out among them particularly. This is known as the TCP / IP suite.

The TCP / IP family can be located perfectly in the OSI model. However, presenting the TCP / IP family, usually, a simplified, four-layer model is used: The DoD1- the model also ARPANET reference model or mostly just TCP / IP model named.

In this model are the Internet layer and the transport layer in the center, and advertising deals with the detail in this chapter. The application layer gathers and describes all protocols that use the TCP / IP protocol. This includes the HTTP protocol used on the Internet for surfing. The TCP / IP protocol is doing a universal communication service available that allows the surf order is possible over the Internet. The network layer then ensures the communication between host and router or between two routers on the LAN.

The Internet Protocol (IP)

The main features and functions of the IP protocol are:

- The protocol is responsible for routing through the Internet. A 32-bit IP address identifies each host.
- The IP protocol is connectionless. Every single IP packet can take a different path on the destination way to the destination host, and it does not establish a fixed physical connection.
- It is built up a universal data packet consists of a header and a DA Tenfold. The header contains, among other things, the sender and the Empfänge- address. The data packet is hardware-independent and is encapsulated in a local network before the transport again.
- The IP protocol does not check whether data has been sent correctly, and also has no confirmation or correction mechanisms: Send and hope.
- The IP header has a length of 20 bytes. When using the options field of the header up to 60 bytes can be great. The protocol generates a header checksum.

The Internet Protocol (IP) is (the OSI model layer 3) applies reasonable at the network layer. This layer is responsible for providing and transporting information across different networks. For this purpose, a uniform Addressing of need: the IP address.

As long as the information transfer takes place within the same network, the DIE function can be disregarded. The connection between different networks is made together by routers. If different networks into a larger whole connectedness to, then you have also any network at a unique address identifiable. Therefore, each network is assigned a unique network address. Based on this network address to each subscriber of the network will be assigned a unique address within half this network address space. The uniform addressing is based on this principle. The address is defined on the IP layer and IP address called.

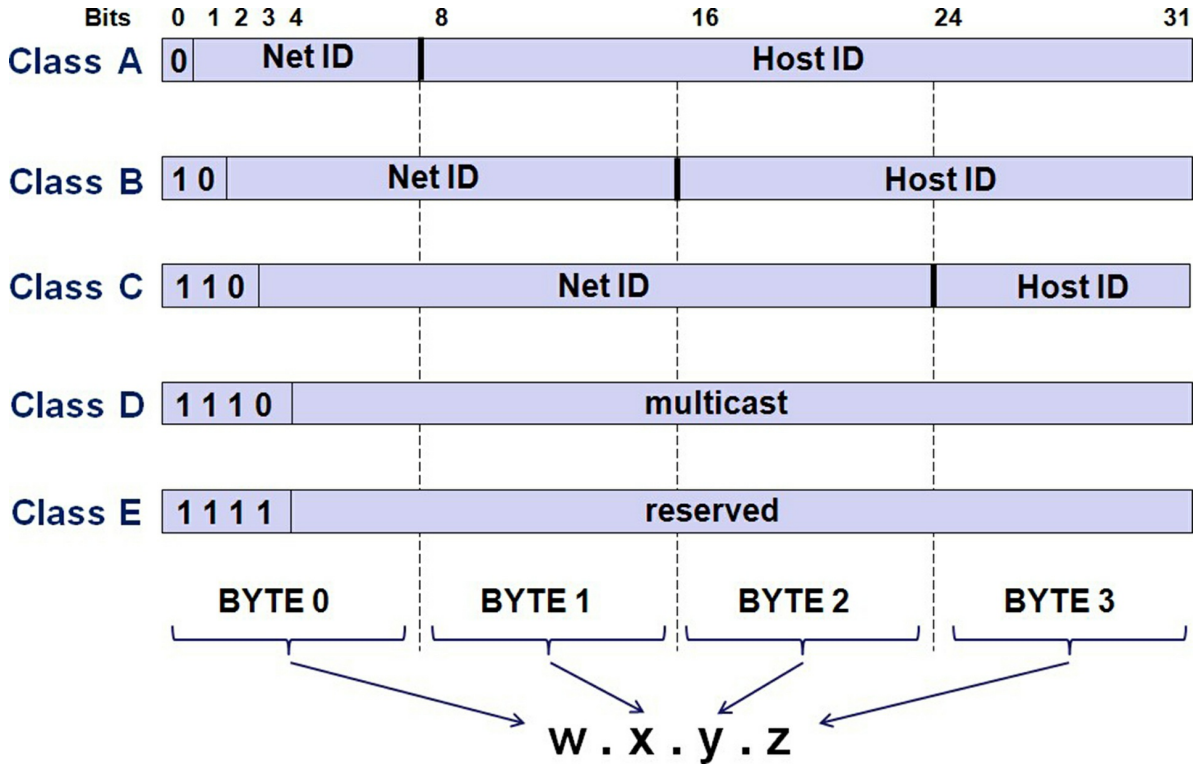
The IP Address

Generally, An IP address consists of 32 bits or 4 bytes, which are represented by 4 separated by a point decimal number.

Each network has a name (Net ID), and each network device is assigned a unique number (host ID) within this network.

Classification of IP Addresses

IP addresses are divided into different classes. The Figure below shows an overview.



The table below shows the characteristics of the classes A, B, and C. Class D was added to send multicast messages easily. Class E is still unused at present.

The number of bytes distinguishes the classes A, B, and C, respectively used for the Net ID one hand, and the host id other. The most significant bits of the IP address which class an IP address belongs to.

class A	Net ID	Byte 1, the first bit is 0, (0 xxxxxxx) 126 possible network addresses

	Host ID range example	Byte 2 Byte 3 + + byte 4 16777214 possible hosts per network 1 . n. n. n→ 126th n. n. n 90.15.167.2 (network name 90.0.0.0)
class B	Net ID Host ID range example	Byte 1, the first bits are 0, 1 (1 0 xxxxxx) + Byte 2 16,383 possible network addresses Byte 3 Byte 4 + 65,534 possible hosts per network 128th 0th n. n→ 191st 255th n. n 128.19.205.132 (network name 128.19.0.0)
class C	Net ID Host ID range example	Byte 1, the first bits are 1 1 0 (1 0 0 xxxxx) + Byte 2 Byte 3 + 2097152 possible network addresses byte 4 254 possible hosts per network 192nd 0th 0th n→ 223rd 255th 255th n 192.147.25.112 (network name 192.147.25.0)

The allocation of IP addresses from the IANA (Internet Assigned Numbers Authority).

IP Addresses for Private Networks

When assigning addresses, public and private (company) networks distinction to be. The Internet (the sum of all public networks) must each IP address to be unique. Routers connect corporate networks to the Internet. To prevent conflicts between private and public networks, several IP addresses defined within each class, which are not used on the Internet. These are described in RFC 1597 under (Reserved Address Space). A corporate network preferably has given a value from this range allocated as the network address.

Special IP Addresses

The table below shows an overview of the specific IP addresses.

Net ID	**Host ID**	**description**
all zeros	all zeros	The IP address of each computer is used at startup
Net ID	all zeros	Network address identifies a complete-ended

		network
Net ID	all ones	Broadcast address on the network
127	any	The IP address for testing networked system applications

Router and the Subnet Mask

Each ISP (Internet Service Provider) connects its network with at least one other network. Since each network has unique identification features, the information from one station can be sent to another. Here, routers ensure that the information is properly routed through the Internet. These routers perform so-called routing tables that can be found in those who are where certain IP addresses. The router receives an IP packet, and it compares the destination address with its routing tables. If a match is found, the router knows to which port that packet must be sent.

To simplify the routing and even better use of the existing classes has been created 1985, RFC 950 a possibility to create groups of addresses within the classes A, B, and C. To create multiple subnets within a class, the prefix (Net-ID) is extended by some bits, there arises an Extended Network Prefix. By using subnets, changes to the IP address per se nothing. However, the information is important for the router, which bits form the Net ID. To this end, the router uses a subnet mask. With this mask, the router filters network share from the IP address.

How is the Subnet Mask Composed?

The network share representing bits maintains the value of 1. The host share representing bits get set to 0.

Thereafter, it is converted into the decimal system.

For example, a Class C address is extended by four network bits. Then the sub is network mask:

11,111,111th 11,111,111th 11,111,111th 11110000

255th 255th 255th 240

Classless Inter-Domain Routing

Due to the success of the Internet is a lack of IP addresses is imminent. The increasing number of networks provides a strong increase in the number of routes, causing a problem for the routing tables globally.

There are two steps to solve this problem:

- IP addresses Restructuring
- Increase routing efficiency by a hierarchical route structure

CIDR (Classless Inter-Domain Routing) is a new form of addressing the Internet, which uses the IP addresses compared to classes A, B, and C efficiently. It is an evolution of Subnetting.

The Net ID is not restricted here more to 8, 16, or 24 bits. A CIDR address includes the 32-bit IP address and additional information about the number of bits that make up the Net ID. Thus, respectively. In the address 206.13.01.48/25 "/ 25" means that the first 25 bits define the network name, while the remaining bits identify the suffix B. the individual subscriber in the network.

CIDR code	**subnet mask**	**binary**	**number hosts**
/ 28	255255255240	11111111 11111111 11111111 11110000	16
/ 27	255255255224	11111111 11111111 11111111 11100000	32
/ 26	255255255192	11111111 11111111 11111111 11000000	64
/ 25	255255255128	11111111 11111111 11111111 10000000	128
/ 24	255.255.255.0	11111111 11111111 11111111 00000000	256
/ 23	255.255.254.0	11111111 11111111 11111110 00000000	512
/ 22	255.255.252.0	11111111 11111111 11111100 00000000	1024
/ 21	255.255.248.0	11111111 11111111 11111000 00000000	2048
/ 20	255.255.240.0	11111111 11111111 11110000 00000000	4096
/ 19	255.255.224.0	11111111 11111111 11100000 00000000	8192
/ 18	255.255.192.0	11111111 11111111 11000000 00000000	16384
/ 17	255.255.128.0	11111111 11111111 10000000 00000000	32768
/ 16	255.255.0.0	11111111 11111111 00000000 00000000	65536
/ 15	255.254.0.0	11111111 11111110 00000000 00000000	131072

/ 14	255.252.0.0	11111111 11111100 00000000 00000000	262144
/ 13	255.248.0.0	11111111 11111000 00000000 00000000	524288

The addressing of CIDR also allows the Summary of the Route (Route Aggregation "). This can represent table routing one parent Route numerous minor routes in a global. In this way, a complete hierarchical structural created structure associated with the allocation of compared telephone numbers in local networks advertising the can.

Examples

Show that the server with the IP addresses or 203.125.72.28/28 203.125.72.34/28 does not belong to the same network.

- The IP address of a host is 192.168.100.102/27.
    - Show that this host belongs to the network with the address 192.168.100.96/27.
    - Show that the broadcast address of this network is 192.168.100.127.
    - Show that the IP address of all participants of this network lies between 192168100126 and 192.168.100.97.
- A company network forms with different subnets.
    - The participants of the below IP addresses belong to particular sub-networks: 172.23.140.197, 172.23.139.78, and 172.23.136.45.
    - The participants with the IP address 172.23.126.120 172.23.127.92 and include hinge gen on the same subnet.
    - Show that the CIDR is within the corporate network / 23rd

The IP Packet

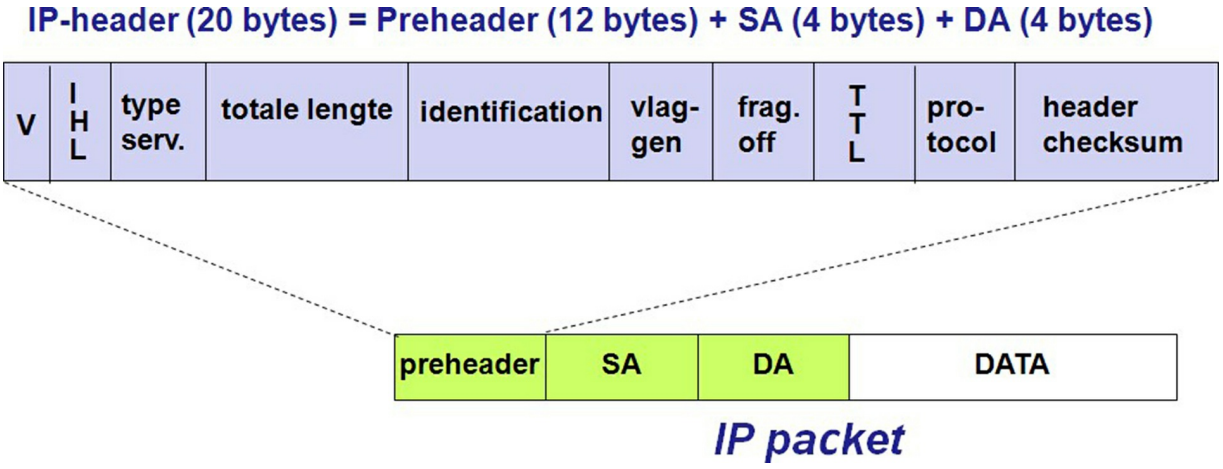
The information that needs to be transmitted is moved to the Internet layer from the transport layer. The information is packed by the internet layer

packs in the field of data and then includes the IP header. This IP packet is then passed layer for further processing of the mediation. Sending data to the protocol is done based on the IP packets.

If a router gets a packet of IPv4 that is too large for the network into which the packet is to be forwarded, the router separates the packet into several smaller packets that fit into the data frames of the subnet concerned. When these packets reach their final destination, the IPv4 protocol of the target host reassembles these packets in the original order. When splitting a package:

- Each package gets its own IP header.
- All part messages belonging to the same original message, save the original identification field. The flag more fragments flag indicates that there are more fragments. The last fragment of this flag is not set.
- The fragment offset field in there, at which point the fragment in question has the original message.

To give a clear idea of the functions of the IP protocol, the IP header is explained in more detail below. The figure below shows the various fields in the IP header. The header consists of a minimum of 20 bytes.



- Version (V): 4 bits field containing the IP version reflects.
- IHL: 4-bit wide field indicating the length of the header in bytes.
- Grade of Service: reserved / priority of the desired service

- Total length: Total length of the complete IP packet in bytes.
- ID: If an IP packet needs to be split, each sub-packet is assigned a unique ID, so that the recipient all packets correctly can be joined together again.
- Flags: The flags are used to monitor the fragmentation of the packets.
- Fragment Offset: When a data packet is divided, so the position of the fragment is recorded within the original packet here in an 8-bit unit.
- Time to Live (TTL): Each time an IP packet passes through a router, the value is reduced by the first If the value reaches zero, the router discards the packet concerned shall. In this way prevents a message remains indefinitely loading.
- Protocol: Reference is made to the next higher protocol.

01hICMP

06h TCP

11hUDP

- Header Checksum: Each router recomputes this checksum for the IP header.
- Source IP Address: IP address of the sending station.
- Destination IP Address: IP address of the receiving party.
- Options: additional network information in the IP header can be accommodated. If the option data does not end with a 32-bit word, the rest is filled with zeros.

IPv6

Generally, the most recent previously discussed in this chapter IP protocol has version number 4 (IPv4). However, a new version is necessary due to the huge success of the IP protocol. There is a clear lack of IP addresses. Also,

new features need to integrate multiple switches. Also, a new version of the IP protocol can also provide higher performance.

The introduction of IPv6 also brings a practical problem: How can the Internet accessible to the public, which so far is working on the basis of IPv4, switch to IPv6? The easiest way is the so-called dual-stack approach. Here is implemented in knots, both IPv6 and IPv4. These nodes can process; therefore, both IPv4 and IPv6 datagrams.

In the field of industrial automation is not working at the time on the integration of IPv6.

The following are some features of IPv6 are described briefly. There are, however, as far as possible, the characteristics that have made IPv4 so successful considered.

IP Address

IPv6 provides IP addresses before with a length of 128 bits. This creates extensive addressing. The 128 bits long addresses are recorded in 8 separate from each other by colons groups of 4 hexadecimal digits:

2000: 0000: 0000: 0FED: CBA9: 8765: 4321

2000 :: FED: CBA9: 8765: 4321

IPv4 addresses: 192.32.20.46

IPv6 header has been changed extensively. It is now used as a simpler basic header, which provides the ability to integrate optional headers and processing time header ensures to offer a substantial reduction of the router. Some IPv4 fields there are not more or available only as an option. The fields in the IPv6 header:

- To identify a 20-bit identification number to a packet in a data stream: flow label.
- Hop Limit: The maximum number of routers that can pass through a particular package.
- Next Header: Defines the type of the first optional header.

- Version field: This 4-bit field specifies the IP version number. For IPv6, this value is the sixth
- Payload Length: This 16-bit number is an unsigned integer value, specifying the number of bytes in the IPv6 datagram, which follows after the 40-byte standard header.
- Since the protocols of the transport layer (TCP and UDP) and link layer (z. B. ethernet) calculate the Internet checksum were the IPv6 developers, believe that in the Internet layer no checksum is needed

Transmission Control Protocol (TCP)

IP is a connectionless packet delivery protocol. TCP has, therefore, been a difficult task: About the unreliable IP packet services has various application programs a reliable data transmission service is provided applications for many check the reliability of a transmission system is an essential feature: The system must ensure that no data is lost, duplicated, or arrive in the wrong order.

End-to-End Transport Service

The TCP protocol is responsible for transferring information correctly through one or more power plants. The exchange of data with TCP is called a connection-oriented: It establishes a logical connection, used, and then stopped again. TCP is, therefore, an end-to-end protocol. The Figure below illustrates this relationship. TCP sees IP as a mechanism by which the TCP can exchange on a particular host data with a TCP on a second, remote host.

From the perspective of the TCP, the entire Internet is a communications system that can send messages and receive, without altering their content or to interpret.

Reliability is Guaranteed

TCP is a library of routines that can be used by applications when they want to add a reliable communication with another participant or host.

To ensure complete reliability, TCP uses a variety of techniques.

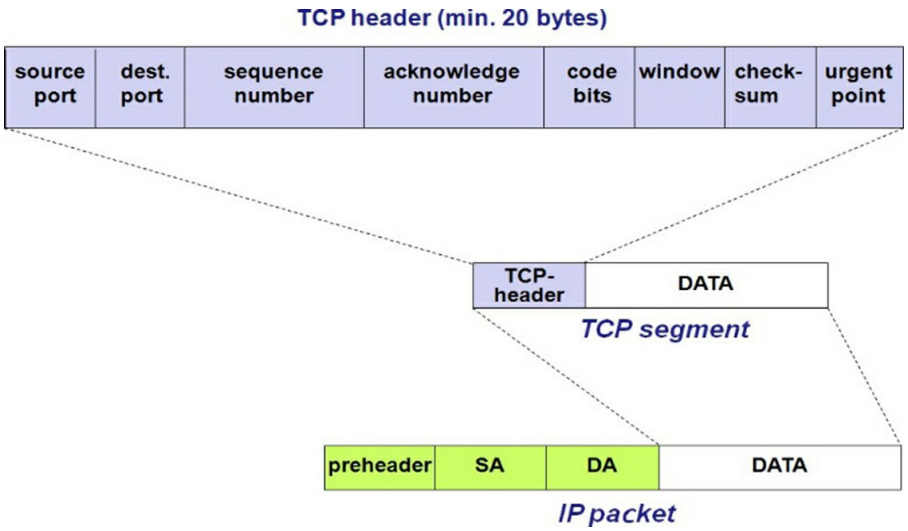
Resending datagrams: If TCP receives data, it sends an acknowledgment (Acknowledgement) back to the sender. Every time the TCP sends data, a timer is started. If the timer expires before the acknowledgment is received, the data is sent again (see also the next Figure).

Window mechanism for data stream control: When a connection is established, each of the two communication partner reserved connection of a buffer for incoming and outgoing data, and notifies the respective another end of the size of this buffer with. The available buffer size at any given time is called Window, shares the so-called Window Size Window Advertisement. The receiver sends along with each receipt a window advertisement. If the receiving application can read the data as fast as they are received, it transmits a positive Window Advertisement along with any confirmation. If the data but faster when the receiving end they can read, the receiver buffer is full at some point. The receiver then reports a window size of zero (SZERO window ").

Three-way handshake: To ensure that connections are established reliably and terminated, the TCP uses a three-way handshake is exchanged in which three messages. TCP uses the term synchronization segment (SYN segment) for messages in a three-way handshake used for stable connections. Called FIN segment messages are named for terminating a call in a three-way handshake.

The TCP Segment

The information to be transmitted is passed layer from the application layer to the transport. The transport layer packs the information in the data field and then adds the TCP header. This packet is then passed on for further processing to the Internet layer. The sending of data with the TCP protocol is done on the basis of TCP segments.



To give a clear idea of the functions of the TCP protocol, the TCP header is explained in more detail below. The Figure above shows the various fields in the TCP header. The header consists of 20 bytes.

- Source Port and Destination Port: TCP is accessible via different port numbers for the applications in upper layers. Ports are unique 16-bit addresses. The combination of a port having an Internet address according to the originally called socket as per ARPA definition 1971. The use of port numbers is important for establishing communication between different applications. It will be discussed further later in this chapter, even closer to it. The table below provides an overview of commonly used in automation ports.
- Sequence Number: The TCP each byte is assigned a number. The sequence number (SSE sequence Number ") is the number of first data byte in the TCP segment after the TCP header.
- Acknowledgment Number: This field contains the next number of sequences from the partner as the expected sequence number.
    - Header Length: Length of the TCP header in 32-bit words.
    - Code Bits: Various bits with which some states can be communicated.

- ➢ The RST bit with which the communication can be re-initialized;
- ➢ The SYN bit, with which the communication can be restarted;
- ➢ The FIN bit is indicating that communication can be terminated.

- Window: The Window field specifies the maximum amount of data bytes again, that can be sent prior to sending and receiving a confirmation.
- Checksum: a checksum of the TCP packet;
- Urgent Pointer: This value indicates where the urgency information starts loading in the data field. To urgent information to send a TCP packet must be the URG code bit set.

UDP

The protocol suite of the Internet, namely, also includes a connectionless transport protocol, UDP (User Data Protocol). With the UDP applications can send IP packets without having to establish a connection. Many client-server applications that include a request and a response using UDP instead of having to connect and later quit again. UDP is described in RFC 768 pixels.

UDP is almost a null protocol: The only services that it provides are a checksum for the data and multiplexing applications using port numbers. The UDP header is, therefore, much easier than that of the TCP.

A UDP segment consists of a header having a size of eight bytes followed by the data.

The header consists of:

- Source port (2 bytes): port number of the sender, if no port is used, the value is zero.
- Destination port (2 bytes): Port of the application for which the message is intended.

- Length (2 bytes): The length of the UDP header and the encapsulated data in bytes.
- Checksum (2 bytes)

A typical example of UDP is real-time audio. If this lost data packets, which is unfortunate, but does not affect the continued functioning of the application.

TCP and UDP Ports in the Automation

In this list, we give an overview of some commonly used in automation port numbers.

application	**Port number / Protocol**
FTP Data (File Transfer Protocol)	20 / TCP
FTP Control (File Transfer Protocol)	21 / TCP
SSH (Secure Shell)	22 / TCP, UDP
Telnet protocol	23 / TCP
BootP server	67 / UDP
DHCP server	67 / UDP
BootP client	68 / UDP
DHCP client	68 / UDP
TFTP (Trivial File Transfer Protocol)	69 / UDP
HTTP (Hypertext Transfer Protocol)	80 / TCP
NTP (Network Time Protocol)	123 / UDP
SNMP (Simple Network Management Protocol)	161 / TCP, UDP
SNMP TRAP (Simple Network Management Protocol Trap)	162 / TCP, UDP
HTTPS (Hypertext Transfer Protocol Secure)	443 / TCP

ISAKMP (Internet Security Association And Key Management Protocol)	500 / UDP
MODBUS	502 / TCP; UDP
IPsec NAT traversal	4500 / UDP
EtherNet / IP	2222 / TCP; UDP
PROFINET, such as connection establishment	0x8892 (34962) / UDP 0x8893 (34963) / UDP 0x8894 (34964) / UDP
IANA, free ports reserved for dynamic and / or Private Ports (Profinet Service)	0xC000 - 0xFFFF
DDI Device Driver Interface (especially for Diagnostic function Utilized protocol)	1962 / TCP
SOCOMM interface (engineering channel Control communication)	20547 / TCP

Communication Via TCP (UDP) / IP

Client-Server Model

A network (TCP / IP) provides a general communication infrastructure without specifying it, what services can be used. TCP / IP provides a Basic communications Service available, but the protocol software is not up able to contact a remote party or answer. Therefore, in every communication, two application programs must be used simultaneously: one starts communication, the other accepts it.

One significant problem is that the protocol software has no way an application program to communicate is that attempted to shoot a communication. Therefore base communication between two users on a model in which a purchase application is active (Request of interaction), while the other is passive (listening and possibly accept). Such a model is

currently generally employed in communication between two hosts via TCP / IP and is called a client-server model. A server application waits passively for contact, and the client application starts the communication active.

Features of the Client Software

- Client software is an application program that is temporary to the client if access to a remote computer is needed that also locally performs calculations and operations.
- It is started directly by the user and performed only for a single session.
- It runs locally on the PC of a user.
- She actively contacts the server.
- Can get to multiple servers if necessary access, but will point at any given time only to a server contact.
- Requires no special hardware or a complex control system.

Features of the Server Software

- Server software, however, can deal with several clients, a special application program that accurately represents a particular service available simultaneously.
- It is started automatically during system startup and remains active for many sessions.
- You are passively waiting for contact from any client.
- They often require powerful hardware and a sophisticated control system (depending on the application).

Endpoint and Internet Socket

The previous Figure shows a client-server communication via the TCP / IP stack. On a computer system, several clients and servers can be active simultaneously. Each application must be uniquely identifiable, and a computer to run applications on multiple presences, has only one physical connection to the Internet.

To this end, transport protocols give each communication service a unique name. TCP protocol used port numbers. Each server is assigned a specific protocol port number. About this port number, the server waits for communication requirements on the computer. When sending a request, the client reports the port number of the requested service. The TCP software on the server computer uses the destination port number in an incoming message to edit certain to which server the request must.

Endpoint

The term endpoint sometimes leads to confusion with the term socket. According to ARPANET originally defined in the socket, the combination of an IP address with the port number. This combination is now called the endpoint. Describes an endpoint, over which logical way an application is accessible in a network.

Internet Socket

The term socket is now a pure software concept. A socket provides for the MAP ping, linking an application with an endpoint. Thus, the term intervention arises net socket, also known as a network socket. An Internet socket or short socket is a bidirectional communication endpoint for a process-to-process connection and is determined by:

- The protocol
    - UDP: Datagram Sockets or connectionless sockets
    - TCP: Stream sockets or connection-oriented sockets
    - Basic IP packet (for example, ICMP.): Raw sockets
- Local IP address
- The port number of local protocol
- Remote IP address
- The port number of remote protocol

The Dynamic Server

Can work on a computer system with multiple applications at the same time, they say, it supports multitasking. A program with more than one thread of control (or short thread), process, or task is called a competing program.

Chapter 5

The Extension Protocols and its Network Applications

ARP

The IP address is virtual, which is processed via software. LAN or WAN hardware is unable to detect a connection between the net ID of a network and an IP address and or between a host and the IP address of a host ID. To transport an IP packet, the data must be encapsulated in a frame that can be delivered from the local hardware at the receiver. Therefore, this frame must contain the hardware address of the receiver and the sender.

Address Resolution Protocol (ARP)

Also, its MAC address to be known as the IP protocol wants to send a message via the Ethernet; it must in addition to the IP address of the recipient, corresponds to this end, the TCP / IP protocol suite maintains an Address Resolution Protocol (ARP). The ARP defines two basic components: a request and a response. A request message contains an IP address and asks the corresponding hardware address (MAC address) from. The answer contains the corresponding hardware address and the IP address for which the request was made.

To avoid having to provide for each packet to be sent first an ARP request, the ARP protocol stores all known information temporarily in a table.

ARP performs this table as a cache: a small table with some belonging together engine information each overwritten or after a certain period of time (several minutes) can be deleted.

The figure above shows the use of ARP in Wireshark. Wireshark is a packet sniffer and protocol analyzer, a program to collect and analyze data in a computer network.

The RARP protocol works the other way around: It sends a request, a request with a hardware address. Then, a reply, a reply with the requested IP address

is sent.

BootP and DHCP

Introduction

When starting hosts, some configurations must be made before the host can actively participate in the network traffic. Each host has an IP address, and the subnet mask applied reasonable, the IP address of the default gateway (this is the router that connects the local network to other networks, the Internet, etc.) and possibly data on the DNS server (see the further section in this chapter) below. This data statically defined in a host or as may be determined dynamically. This section is about how certain settings can be performed automatically at startup. This boot is also known under the name of bootstrapping.

BootP

The bootstrap protocol is the TCP / IP suite added to some dynamic Configuration before in a single step to unite. The BootP protocol sends out a broadcast request to obtain configuration information. A BOOTP server knows this message and responds with a BootP reply that contains all the necessary information. BootP uses IP packets, even though the participants do not already have IP addresses. As the destination address, a broadcast address is used, which consists exclusively of send inputs, the source address is all zeros. The BootP server can use the hardware address, send his answer to the configuration is simplified by BootP, but the problem remains that a BootP server receives its information from a database that is performed as before by an administrator must manually.

DHCP

For further automatic configuration has developed the IETF Dynamic Host Configuration Protocol (DHCP). DHCP is a protocol that can join a new network without manual intervention by an administrator a host. DHCP is a client-server protocol. The client is a new host, the requesting IP information one or more DHCP servers may exist that can assign these data per network.

For a new host is the DHCP protocol consists of four steps:

- DHCP Discover: A client sends an encapsulated in an IP packet UDP message using port 67 to search for a DHCP server. A broadcast destination address (255.255.255.255) and the source address (0.0.0.0) is used.
- DHCP offer: the response from a DHCP server to the client. This response contains an IP address, subnet mask, and release time for the IP address.
- DHCP request: The host selects the different address offers and responds to the selected server with a request that contains the configuration parameters.
- DHCP ACK: The server responds with an acknowledgment.

DHCP Relay Agent - DHCP Option 82

The DHCP Relay Agent is a bootstrap protocol in which DHCP packets between DHCP clients and servers can route to different IP networks. In other words, a DHCP server, a network can use a DHCP relay agent with which it is not directly connected.

A DHCP relay agent listens to the known bootpc of client ports (67) to broadcast packets from DHCP clients in the network. These packages are converted into unicast packets and forwarded to the configured DHCP server. Here, the DHCP Relay Agent transmits its own IP address in the giaddr field of these packets. The DHCP server can, therefore, send a unicast packet to the relay agent the answer. The relay agent then forwards the response as either broadcast or unicast packet on the network to the client.

The DHCP Option 82 is an information option of the DHCP Relay Agent. It was developed so that a DHCP relay agent can add a package to a DHCP server forward each network-specific information. The option uses an additional two information: Circuit ID and Remote ID.

About this information from the DHCP server receives information about the network in which the sending host is located information depends very much on the DHCP relay agent, and exist in Ethernet-based networks of the MAC addresses of the ports of the relay agents that shape the path to Endhost. With this information, you can specify where the assigned IP address is physically

located on the network. The DHCP server may also use this information in making decisions about how to assign a specific IP address.

ICMP

In IP communication service data packets can be lost, their delivery can be greatly delayed, or they can be delivered in the wrong order. IP is not a reliable communication service but tried to avoid mistakes and to report if necessary, the occurrence of problems. A typical example of error detection is the header checksum. Whenever a data packet is received, the checksum is controlled to ensure that the header is intact. If a checksum is detected errors, the message is deleted immediately. This can't be reported because the source address is deleted along with the message. However, other, less important term problems can be reported.

Internet Control Message Protocol

The TCP / IP protocol suite includes a protocol for sending error messages: the Internet Control Message Protocol (ICMP). So can be notified when a particular network device is unavailable, or that a particular host or router is unavailable. The computer users sometimes come directly in contact with the ICMP ping, especially when using the Network Diagnostics commands and traceroute.

ICMP has five errors and four informative messages. The five error messages ICMP are:

- Source Quench (source stop) is sent by a router if it forward temporarily; not enough free buffer has and therefore must reject incoming IP packets. This message is sent to the host, who created the IP packet. The sending host needs to adapt its transmission speed.
- Time Exceeded: is sent by a router if the Time to live field has reached zero.
- Destination Unreachable: is sent by a router if it determines that an IP packet can't reach its destination. The error message distinguishes between a situation in which an entire network is temporarily not connected to the Internet (because a particular

router is not functioning properly), and the event that a particular host is temporarily offline.

- Redirect: is sent by a router if it determines that the IP packet to another router would actually be sent to be able to achieve his goal.
- Fragmentation Required: is sent by a router if it determines that an IP packet is larger than the MTU (Maximum Transmission Unit) of the network.

In the ICMP, four informative messages are defined:

- Echo Request / Reply: An echo request can be sent to any host advertising. In response, an echo reply is sent; it contains the same data as the request.
- Address Mask Request / Reply: a host sends an address mask request at startup. A router responds with a message containing the correct subnet mask used on that network.

ICMP Message

The ICMP protocol is used to support the IP protocol. So it also uses IP packets to send messages. The figure below shows how an ICMP message to a data frame is encapsulated.

An ICMP error message is always processed in response to a specific IP packet and sent back to its source.

The various fields in the ICMP header are:

- TYPE:
- Code:
- checksum:
- Identifier:
- Sequence Number:

Check the Reachability of a Host

Many tools collect information over a network by sending test messages and waiting for the ICMP responses. One of the most important diagnostic tools is the ping command. This sends, after calling on the DOS level, ICMP IP packets to another subscriber to check whether this host is reachable over the network. The reasonable pinged host sends the packets immediately returns as an echo. Further, the command specifies the reaction rate and a static Summary of the percentage of packets that have not responded to the from. It can generate the IP address that is used as the hostname.

ping www.google.be ping 134.16.85.9

An overview of the numerous options for entering the command ping displayed without working.

Following Your Route

While the ping command only checks to see if a particular host is reachable, the command does tracert route to a specific host visible. The above figure shows how the command tracert all IP addresses of the routers, which receive the test packet and Send outputs.

Tracert first sends a test packet with a time-to-live value of 1. The first router decrements to 0, discards the message and sends the ICMP error message Time Exceeded. In this way, the IP address of the first router can be determined. Now a test packet with a time-to-live value of 2 is sent. The first router operation is valued by 1 and sends the message. The second router will set the TTL value to 0, in turn, rejects the message and sends the ICMP error

message. In this way, the IP address of the second router can be determined. This process will be continued as long as the last host reached.

IGMP

IGMP (Internet Group Management Protocol) is the protocol for IP multicast applications in TCP / IP networks. This standard is defined in RFC 1112th. In addition to a definition of address and host extensions for supporting multicasting by IP, hosts correspond to this keeps RFC also a definition of version 1 of IGMP. The IGMP Version 2 is defined in RFC 2236th. Both versions IGMP provide a protocol available to the information on the membership of a host on specific multicast groups exchanged and can be edited.

Multicast messages are sent to a single address (multicast IP address) but processed by multiple hosts. The group of participants who respond to a particular multicast IP address is called a multicast group. Some Important control features of multicasting:

Belonging to a group is dynamic: hosts can always leave the group or join a group.

- Hosts can subside- KISSING by sending IGMP messages multicast groups.
- Group size is not limited. The various participants can be distributed across multiple networks, provided that the intervening router IGMP sub base.
- Hosts can also send IP messages to a particular group if they are not part of this group.

IGMP Messages

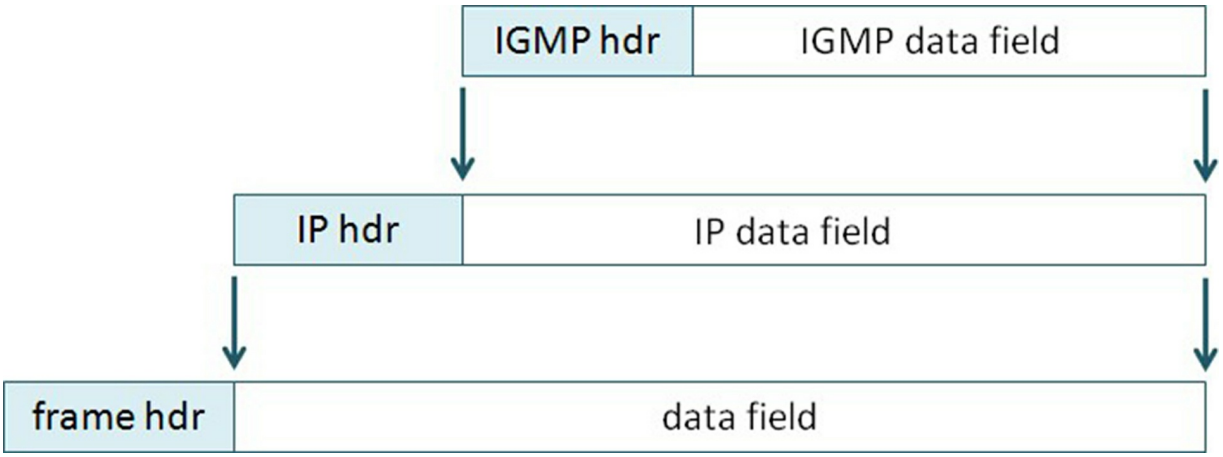
IGMP describes how the information on the membership status between routers and the various participants of multicast groups to be replaced. Examples of IGMP messages:

- Host Membership Report: When a host member of a multicast group is all, it sends a host membership report and informs all other members of the group. A router stores these reports,

ensuring the administration of the multicast group.

- Host Membership Query: is sent by routers to gather information about group members in a network periodically. All members of a group respond again with a membership report. Routers store all the information and ensure that multicast messages are not sent in networks where there are no group members.
- Leave group: is the last host that the factory segment leaves a group in a particular network, sent.

The IGMP protocol is used to support the IP protocol. So it also uses IP packets to send messages. The figure below shows how an IGMP message encapsulated in a data frame.



IGMP Snooping

A switch that connects a member of a multicast group with a router can read IGMP snooping IGMP messages and evaluate using. IGMP Snooping translates multicast IP addresses to multicast MAC addresses. In this way, a switch can store multicast MAC addresses in its multicast filter table and send as multicast messages only to the correct ports.

This ensures that multicast messages prevent a Network unnecessarily burden. This method is known under the name switches in dynamic multicasting, in contrast to the static multicasting, in which the groups must be manually configured in all switches and for all ports.

Multicast Addresses

Multicast IP addresses are addresses in the range between 224.0.0.0 and 239.255.255.255 (Class D). For private networks, it is generally recommended to use the range 239.xxx for multicast IP addresses.

The addresses in the range 224.0.0.1 to 224.0.0.255 include reserved for multicast applications within a network. The time-to-live value of such IP packets is set to 1, so they can not leave the network.

There are also multicast MAC addresses reserved. All addresses whose first byte is 01h, STE hen for multicasting are available. Addresses starting with 01: 00: 5E: 0 starts are multicast MAC addresses used for IP multicasting.

This transformation requires an explanation. The most significant bit of the second byte overall belongs to a multicast address to the identification code and is therefore not mapped with. Thus, the multicast IP address is 228.30.117.216 into the multicast MAC address 01: converted D8: 00: 5E: 1E: 75 miles. The multicast IP address 228158117216 is, however, in the multicast MAC address 01: converted D8: 00: 5E: 1E: 75 miles.

GMRP

IEEE 802.1p

Corporate networks are becoming ever larger and more complex. It is, therefore, important that the growing traffic can be managed efficiently. Here, the "Quality of convenience I represent an important tool with which it can be ensured that the most critical data is transmitted predictably. Using the IEEE 802.1p protocol kön- nen switches data on the network preferably be delivered. This will improve the predictability and reliability of improved traffic.

IEEE 802.1 defines a 3-bit field, which can be assigned to the data to be transmitted a priority from 0 to 7 within tagged Ethernet frames.

The IEEE 802.1 standard also provides for measures for filtering multicast packets so that they do not unnecessarily spread over Layer 2 networks. One of these measures is the GMRP (GARP Multicast Registration Protocol). GMRP and GARP are of the IEEE 802.1-defined industrial protocols.

The Function of the GMRP

GMRP processed multicast group addresses on Layer 2 (MAC layer). GMRP operates both the switches as well as the hosts. The host GMRP is used with IGMP. There it forms the IGMP packets Layer 3 data frames to the second layer.

A switch receives both the GMRP packets at layer 2 and the IGMP packets at Layer 3. The GMRP packets limit the switch traffic in the VLAN group to which the sending host belongs. If the switch the "GMRP join Message received, the port it was received on the multicast group in question is added. The switch forwards the subscription request to all other participants of the VLAN on, WOR among themselves the multicast source is located. If the source is a sends multicast message to the group, the switch those only to members of the corresponding group forwards.

The switch sends GMRP queries regularly. If a participant wants to stay in a group, he must answer these queries. Want a participant no longer listen to the group overall, it can be a leave message Send or simply not respond. If the switch from a particular host no response or receives leave a message, he strokes the operators concerned from the list.

DNS

There are two main ways to identify a host on the Internet: In addition to the previously mentioned IP address, there is also the possibility of a subscriber a hostname (a plain text names) allocated to facilitate the use in general.

Hostname, such as www.google.be (Search engine) or www.phoenixcontact.com read- sen easier to remember and, therefore, more user-friendly. A hostname has not enough information to be able to locate the host on the Internet. Since the application of preferring the hostname, the TCP / IP protocols, however, are based on IP address, must be a mapping between hostnames and IP addresses made. This is done by the Domain Name System (DNS), by Dr. Paul V. Mockapetris and Jon Postel was invented. In 1983 she presented the DNS architecture found in RFC882 and 883rd

In summary, DNS stands for:

- a distributed database that is implemented in a hierarchy of DNS servers;
- a protocol at the application layer, with the hosts and DNS servers, can communicate with each other to the conversion of IP addresses to hostnames and be able to make vice versa.

The DNS servers are often UNIX machines on which software such as Berkeley Internet Name Domain (BIND) or Microsoft DNS is running. The DNS protocol uses UDP and uses port 53rd

The Structure of Hostnames

With regard to the syntax of hostnames are always elements made of a series of the alphanumeric segment that is separated by points. Domain names have a hierarchical structure; the most significant part of the name is right. The leftmost segment is the name of individual hosts. Other segments in a domain name identify the group that owns the name. DNS does not specify how many segments a domain name is but gives values for the most significant segment before. The table below shows an overview of the different values of the test significantly segments.

Domain Name	Assigned to
com	commercial organizations
edu	educational institutions
gov	public bodies
mil	military
net	Network management facilities
org	other organizations
int	international organizations
Country codes	States such. U. be for U.S.A

SNMP

SNMPv1: The SNMP protocol defined in RFC 1157 1990th SNMP stands for Simple Network Management Protocol. This protocol describes a structured method for monitoring and managing specific network infrastructure. It was quickly applied extensively in commercial products and became the de facto standard for network management. SNMP is a simple protocol.

SNMPv2: The experience with the protocol led in 1993 to an improved version of SNMP, described in RFC 1441 and RFC 1452 (coexistence of v1 and v2), and eventually became the standard on the Internet.

SNMPv3: The third version of the standard Management Framework (SNMPv3) is based on the previous versions of SNMPv1 and SNMPv2. SNMPv3 is basically SNMPv2 supplemented by security and administration. Key features of SNMPv3 include:

- safety
    - Authentication and Privacy
    - Access control
- Administration
    - Management of user names and keys
    - Designation of participants
    - Policies

In a network, many interesting participants are active; the formations of important ones inform about the status may have to manage a network. Such participants can be hubs, switches, routers, printers and PCs. To be directly managed by SNMP, must on a node, an SNMP management process - a so-called SNMP agent -. Can fen lauryl. All computers to which are intended for use in the network will be able, as a number of hubs, switches, routers and peripherals. Each agent performs a local database where his condition is stated in the present and the past in variables that affect his work.

Network management is in place management stations: in practice, a normal computer on which special management software is running. On these

stations, run one or more processes that communicate over the network with agents by issuing orders and receive responses.

In this configuration, all intelligence sits in the management stations to the agents as simple as possible to keep and to minimize their impact on the devices on which they run. Many management stations have a graphical user interface, so the network administrator to inspect the state of the network and can take action if necessary.

Structure of SNMP

The SNMP consists of three main parts:

- MIB (Management Information Base (RFC1213)): description of all variables of a certain network element;
- SMI (Structure of Management Information (RFC 1155)): Structure for storing network information;
- SNMP: protocol for communication between the manager and a network device (RFC1157).

Most existing networks consist of elements from different manufacturers - hosts of one or more manufacturers, switches and routers from other companies, and printers from other manufacturers turn. To ensure that a management station. again by another manufacturer comes) with all these various components communicate can be to determine the nature of the information collected by these devices specified strictly.

It makes no sense if one asks Management station a router on the frequency of occurrence of lost packets when the router does not register the information. Therefore SNMP accurately describes the information that any type of agent available must provide and the format that has to use the agent to do so. Most of the SNMP model is to define customized who lead what information needs and how they are to be transmitted.

In short, it runs down to is that each device performs one or more variables (objects) that describe the state of the device. The totality of all possible objects in a network is in a data structure, the MIB (Management Information Base) is called.

The SNMP protocol itself now describes how the interaction between the Management and agents is established. To this end, five different Nachrich- be defined type.

MIB and SMI

Managed by the SNMP objects defined in the MIB and are shown in the above Figure to the FIN. For simplicity, these objects are divided into different groups. These categories provide a basis for the information that can operate a management station comparable needs.

- The group system offers managers the opportunity to find out how an overall is advised, who made it, the hardware and software it contains, where it is located, and what its job is. The timing of the recent boot is specified.
- In the interfaces, a group is about the network adapter. The group registered, how many packets and bytes sent and received on the network and discarded, how many broadcasts there, and how large the execution queue.
- The group IP addresses the IP traffic to and from the node. There is above all counters that register how many packets were discarded for various reasons. Also, there is static data about the fragmentation and Reassembly of datagrams. All this information is primarily for the management of routers is important.
- In the ICMP group is about IP error messages. There is a counter that records the number of each message type for each ICMP message.
- The TCP-group records the current number of open connections and the overall sent and received segments and various statistical data on a fault on the server.
- The UDP group counts the sent and received UDP datagrams, and REGI started how many of them were undeliverable because of an unknown port or for other reasons.

- The last group is used to collect statistical data on the work of the SNMP itself: how many messages were sent to what message it was, etc.

Each variable of each object in the MIB is characterized by an Object Identifier (OID) and its type:

- The OID describes a path in the MIB tree. The figure below shows the structure used in the SNMP MIB. The object sys Object ID, which belongs to the group system, is accessible via the OID 1.3.6.1.2.1.1.2.0.
- Object types are built using basic types that are defined in the SMI.

There are several MIBs. First, the global MIBs (z. B. MIB2 in RFC1213) have been described in RFCs. These MIBs must that is supported by all SNMP-incompatible device. Furthermore, there are also manufacturer-specific MIB objects.

SNMP Protocol

The SNMP normally operates so that the management station sends a request to an agent in which it requests information, or it prompts you to change its state to a certain way. Ideally, the agent responds only to the reasonably requested information or confirms that he has his condition changed as desired. The SNMP settles different messages which could be sent.

message	description
Get request	Queries the value of one or more variables
Get next request	Queries which the following current variable from
Get bulk request	Asks a piece of large group information from
Set request	Change one or more variables
Inform request	The message between different managers to describe the local MIB

In one particular case, the agent can take the initiative and send a message, namely when it detects the occurrence of a critical event. Managed nodes can fail and restart, and network segments can fail and go back into service, etc. Every relevant event is defined in a MIB module. When an agent determines that a relevant event has occurred, it reports this immediately all management stations in his configuration list. This message is called an SNMP trap. However, it is usually only the occurrence of an event. It is the task of the management station to carry out requests to get the details.

message	**description**
SNMP trap	Agent to the Manager reports an event

The table shows that SNMP messages the UDP protocol to use, and which ports here for use are for the next image.

HTTP and HTTPS

TLS / SSL

The Transport Layer Security (TLS), the successor to the Secure Sockets Layer (SSL), encryption is an encryption protocol that allows a secure data channel is created on an unsecured network such as the Internet.

Both protocols work a layer deeper than the application protocols, such as HTTP, SMTP, FTP, etc., but above the transport protocol TCP. They are part of protocol family TCP / IP. One of its main objectives is to back up client/server applications.

On the transmitter, the side encrypts the TLS layer data of the application and transmits it to the correct TCP port. At the receiver side, TLS reads the data from the correct TCP port, decrypts it and forwards it to the application. The through locks, the data is up to the recording layer.

TLS provides the following security features for client/server applications over TCP / IP:

- Authentication: This allows an application to verify the identity of another application with which it communicates.
- Privacy: Between the applications submitted, data is protected from access or misuse.
- Integrity: applications can determine if data has been modified in transit.

The techniques used are based on concepts such as public keys and certification skating.

If an application SSL / TLS uses a handshake process is started, first, in which the encryption algorithm and the agreed key to use and the server to be verified by the client. Following that procedure, all application data is encrypted.

HTTP

It defines the exact format of the requests (requests) of a web browser to the server and the format of the responses (responses) that can give to the Web server. Each request contains a URL pointing to a network component or a static object (eg., A Web page) points. The HTTP protocol uses port 80th

Each HTTP URL starts with "http: //".

HTTP is insecure and vulnerable to man-in-the-middle attacks and eavesdropping practices.

HTTPS

HTTPS (Hypertext Transfer Protocol Secure) is an extension of the HTTP protocol, which is used for the secure exchange of data. When using HTTPS, the data is encrypted form, making it impossible for an outsider to intercept the data. HTTPS is basically HTTP, with the addition of SSL / TLS is used to send the data to clauses scrambling system and to verify the server.

Each HTTPS URL begins with "https: //". The protocol uses TCP port 443rd

Review of Some Other Important Applications

FTP

FTP (File Transfer Protocol) is a protocol that allows the exchange is simplified files between different hosts. It allows the transmission of any files and create directories as well as rename or delete directories and files. The protocol hides the details of an individual computer system from the user, making it ideal for heterogeneous situations. The protocol can transfer files between any system.

TFTP

TFTP (Trivial File Transfer Protocol) is to provide a simplified FTP version that is often used by devices such as routers, switches, etc. with firmware and configurations.

NTP

NTP (Network Time Protocol) is a protocol that can synchronize with your computer in a network their internal clock with the other computers. NTP is based on the predictability of the network caused by the delay. The computer network is doing here- divided hierarchically, with the computer with the most accurate time as SStratum 0 "is referred to. The computer systems that bring about NTP directly from their time there are, by definition, SStratum 1. "

The protocol has some smart features. Thus, for. B. make an NTP client use of multiple NTP servers and decide for themselves which of the server works best. Using some decision criteria, an NTP client selects a server and synchronizes it with it. Small-time differences between server and client are resolved by the client, in which he leaves something to run faster or slower his watch. In this way, the time difference can be compensated without time jumps.

SSH

Secure Shell is located at the application layer of the TCP / IP protocol. SSH replaces old protocols such as Telnet and Rlogin by a secured variant. The protocol uses TCP port 22nd

SSH is a secure login on another computer and the execution of loading

missing possible on a computer at a different location within a shell. The encryption used makes it difficult for foreigners to read the original commands.

An important advantage of SSH is the ability to authenticate with an asymmetric encryption method. This allows SSH applications automatically be set once, without having to be stored in that code a password. The private key is to log on to any system that uses the corresponding public key, which is possible.

CLI (Command Line Interface)

Operating systems with a command-line interface (command-line interface), the user can place orders via text commands. When the execution of a command sen completed, the user can enter more commands. A command is the usual with <Enter> completed.

Known CLIs are command.com (DOS) or Bash (UNIX).

In addition to operating systems, other software programs can be used with a CLI loading such. As the FTP client and the Telnet client from Microsoft. Also, industrial switches are often operated via a CLI.

Chapter 6

The Switch

Generally, industrial switches can be initially divided into two different categories:

- Unmanaged switches
- Managed switches

In the first group of switches, no configurations can be made. This is also not necessary for the general operation of a switch.

The second group of switches can be configured via a web server, for example. Such an approach is of interest for the diagnosis of the network.

The above Figure shows the industrial switch FL SWITCH SFN 8GT Gigabit Switch from Phoenix Contact. Some typical technical features of such switches are:

- 10/100/1000 TX, auto-negotiation, auto-crossing
- Unmanaged, no configuration
- Mounting on DIN rails, alarm contact, redundant power supplies
- Temperature range: -25◦C to +60◦C

Technical Description of Industrial Switches

The technical description of a device from the Factory Line from Phoenix Contact all possible properties are shown a switch.

SMCS stands for Smart Managed Compact Switch. This switch corresponds to the IEEE802.3 standard and used for building automation networks based on Ethernet. He has eight RJ45 ports for connecting twisted pair cables. All ports support 10/100/1000 Mbit / s as well as auto-negotiation and auto crossing.

The switch is suitable not only for use as a standard Ethernet switch, especially for applications in the field Profinet RT and Ethernet / IP and supports necessary for this management function. Furthermore, the switch IGMP Snooping for Ethernet / IP.

Redundant network structures can the (Rapid) Spanning Tree Protocol or the Media Redundancy Protocol be constructed in accordance with. This ensures optimum operation of the network is guaranteed regardless of the comparable used topology.

Within complete network systems, information may be retrieved from the switch via SNMP. Configuration and diagnostics are possible via web server, SNMP, Telnet, or a V.24 interface (RS232).

The FL SWITCH SMCS 8GT is a store-and-forward switch. All data messages that reach the switch on a port are initially stored in a buffer and checked for validity. Corrupt data packets, i.e., those having a size of more than 1,522, or less than 64 bytes or packets with a checksum error occurs, must be discarded. Valid data packets are then forwarded via the correct port immediately. The transmission speed is set for each port through the connected network segment.

The switch dynamically learns all the addresses of the various network devices by extracting each incoming message, the source address. It can store up to 8000 addresses save in the address table. The aging time is 40 seconds (default) and is comparable changed. This time can be set via SNMP or Web-based management to a value between 10 and 825th. All addresses that were no longer needed after this time will be automatically deleted from the MAC address table.

The switch has a signaling contact. This signaling contact is closed floating and when properly function of the switch. With its help, the function of the switches is monitored. It is opened under the limited circumstances described below. At the restart, the switch performs a hardware self-test. If an error is detected, the alarm contact is opened. During normal operation, a watchdog device monitors the cyclical execution of the software program. If this watchdog body fails triggered cyclically by the software, the signaling contact is opened.

The user is optimized with the help of various status LEDs on the status of the switch informed. In this way, a local diagnosis without the use of additional tools is possible.

The SMCS switch supports autocrossing. Thus, it is not necessary more to distinguish between crossed and uncrossed twisted-pair Ethernet cables.

The SMCS switch supports auto-negotiation. In this case, the switch detects the parameters from a certain subnet on each port and configures the respective RJ45 port accordingly. The detected parameters are transmission speed (10, 100, or 1000 Mbit / s) and transmission mode (half or full-duplex). This automatic detection makes manual intervention by the user superfluous. The auto-negotiation function can be activated via the web-based management on or off.

(Are so if RD + and RD- reversed) with the use of twisted-pair cables with the wrong polarity, the switch reverses the polarity to automatically internally. This property is known as Auto Polarity Exchange.

The switch checks at predetermined times networks that are connected to each port sub. He uses link test signals as described in IEEE 802.3, to the connected TP / TX cable to check for short circuit and interruption.

The switch can receive in two different ways an IP address either via the BootP protocol or the serial V.24 interface. The factory, the assignment of the IP address on BootP, is set. There is a configuration software available to one to assign the IP address, if necessary, the switch easily. The mechanisms mechanism for assigning an IP address can be set interface via the Web-based management or V.24.

The switch in Smart Mode can be set using the MODE button on the front of the module. In Smart mode, the switch may be in a different mode shifted advertising to without using the management interfaces. In addition, the Smart mode, the factory settings can be restored.

The switch can be configured as a Profinet-IO device on the Web-based manage- or smart mode between operating modes Default (standard Ethernet switch) and Profinet IO or Ethernet / IP can be selected. If the switch is configured as a Profinet IO device, he can be recorded as such in the Profinet engineering software. In this way, a byte of diagnostic information that is

provided in the engineering software for each input of the switch.

The SMCS switch supports the LLDP protocol, according to IEEE802.1AB. The switch sends and receives management and connection information to/from adjacent (n) devices (s). Thus visually displayed on available tools network architectures and monitors advertising to. The Profinet engineering software uses this information to a network diagnosis visually represent.

The switch, according to different priorities, queues two different (traffic classes according to IEEE802.1D). Received data packets are assigned to one of these queues according to their priority. The priority is given in the VLAN tag of the Ethernet frames. So that the transmission of high-priority data is not hindered by large amounts of data with low priority is avoided. In the event of an overload, data is no longer assumed to be a low priority. This principle is applied, among others, Profinet RT and is their quality of service.

The switch can handle a VLAN tag according to IEEE 802.1Q. This day consists of four bytes and is in the Ethernet frame between the source address and type field. Three bits of the four bytes represent the priority. About the Web-Based Management, different VLANs per port can be set on the switch. In this way, different VLANs can structure within a network with such switches build. Within a physical network, so different logical networks can be created.

The switch supports Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP). STP is described in IEEE802.1d and allows the formation of a ring or mesh structures in the topology of a network made through the mesh structure kön- enables multiple communication paths between two devices. To prevent infinite loops and broadcast flooding, the switch cuts off some of the compounds. In the case of a cable break, the network after a specified time (20 to 50 s), the conjunction of switching on the switched-off ports restores. Powered-off ports can still receive data, but not send more. All active ports send data.

RSTP is a newer version of the STP and enabling switching times of 1 to 10 seconds. Also, the RSTP support ring and mesh structures. In the RSTP configuration, RSTP Fast Ring Detection can be activated.

The SMCS supports the Media Redundancy Protocol (MRP). This will pour

into a Ring topology after an error occurs, a recovery time of a maximum of 200 ms allows.

Via SNMP (Simple Network Management Protocol), the device can be monitored via the network. An SNMP management system provides the ability to read the device configuration data to diagnose and change it. It supports SNMP versions 1 and 2c. The following MIBs are supported: RFC1213, RMON MIB, Bridge MIB, If-MIB, Ether like MIB, Iana-Address-Family-MIB, IANA if Type MIB, P-Bridge-MIB, Q-Bridge MIB, SNMPv2 MIB, SNMP-FRAMEWORK-MIB, and its own SNMP objects from Phoenix Contact (FL-SWITCH-M-MIB).

A serial connection to the switch can be provided via a V.24 interface (RS232) manufacturing. The cable is connected to the COM port of the PC and the switch to a mini-DIN connector. In this connection, the serial communication is done via a program such as HyperTerminal. This interface IP address, subnetworks, and default gateway are set. The address for the automatic assignment of an IP used BootP can be turned on or off. The parameters can be through this interface to store, and it can restart the unit carried out by the advertising. Also, resetting the device to factory settings is possible.

Another interface provides management Web-based. This interface provides diagnostic and configuration capabilities at startup and during operation of the device, and if errors occur. And network and device information on the web-based management can be polled. With the web-based management can be (namely on the basis of a web browser) to query a general hand-known, all information from the device.

Technical data, installation data, local diagnostic information can be queried. Furthermore, all configuration parameters (IP configuration, SNMP configuration, software updates, and passwords) can be checked and can be changed under the item Switch station "various diagnostic information about the various ports and the signal contacts are monitored.

Each port can be individually enabled or disabled. For each port, all transmission parameters can be adjusted, and web-based management, static information can be queried about the data itself. Also, the Port Mirroring "can be activated. With this function, it is possible, all the data are sent via a

specific port or received to also send to a different port. This is important for error detection using a network sniffer.

Some common specifications:

- The device is mounted on a DIN rail.
- The protection class is IP20 (protected against solid objects with a size greater than 12 mm; no protection against water); 40050, IEC60529.
- Class 3, according to VDE 0106, IEC60536.
- Power supply: 24 V DC (18.5 V - 30.5 V), maximum cable cross-section. 2.5 mm2,
- The device can be redundantly powered.

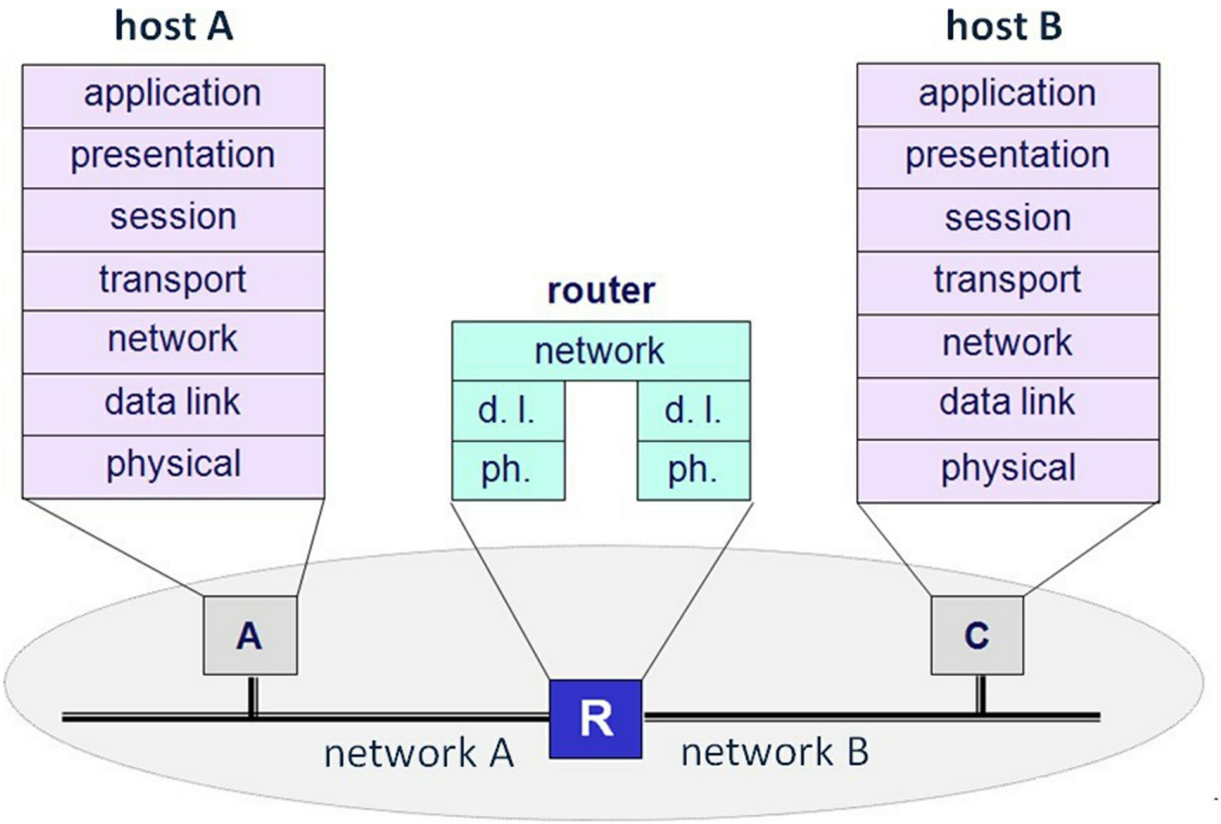
The grounding is done on the DIN rail on which the device is mounted on the current: 600 mA (15 W)

- Dimensions without configuration memory: 128 mm (W) x 110 mm (H) and 69 mm (T); Weight 650 g
- Operating temperature: 0 ◦C to 55 ◦C; Storage temperature: -40 ◦C to 85 ◦C
- Humidity: between 10 and 95% (non-condensing)
- Air pressure: mu in operation 80-108 kPa at 2000th NN; Storage 70-108 at 3000P. NN

Chapter 7

The Router

A router is a device that connects two or more different computer networks. As a corporate network to the Internet. The figure below shows that a router can be seen as an exchange of data packets that operate at layer 3 of the OSI model.



Message Routing

Different routers must process it, a message to be sent from one computer to another over a network. First, a transmitter sends the IP packet to a first router. To this end, the sender encapsulates the IP packet in a frame and adds a header, as is the physical network in which stations and routes are predetermined.

If the frame reaches the router, it removes the content and examines the IP

packet. The router needs to know which port the message must end. To determine the correct output port, the router looks up the destination address of the packet to be routed in the routing table when TCP / IP protocol is a routing table from a table of IP addresses and clustered IP addresses (subnet) and the respective next nodes (Next Hop).

If the destination address is found in the routing table and therefore can be routed, the router the output port sets where the thus found node. The reroute captured IP packet will be sent to the output port. The router encapsulates to the IP packet, again and again, adds a header as is the physical network that the two routers are connected to each other, predetermined. The above figure shows that an IP packet is always encapsulated in a frame that matches the respective physical network.

A router for each port has an IP address belonging to the network area of the Net-ID, to which the router is connected. Each port has its own MAC address.

A router is considered as a monitor. A data packet may not normally happen only limited by the TTL (time to live) of the packet number of routers before it reaches its final destination.

Router Types

There are many different types of routers. They can be based on their shapes, the connections, and the necessary additional functions (e.g., modem, firewall or switch) differ.

Further can be distinguished software and hardware router. Using special software is used as a conventional router, equipped with two network interface PC. A hardware router, however, is a separate device, actually a small, simple computer that has been specially developed for routing.

Commercial routers for home use are often combined with a switch, have a modem, and a wireless AP so that only a single device is required to connect to a small home network with the Internet.

There are also switches me router function on the market. The name Layer 3 Switch "is often used for these devices.

The remainder of this chapter focuses on industrial routers. In its simplest

form, such a router to a LAN and a WAN interface. Herewith an industrial network can be connected to a corporate network or the Internet. The industrial router can also optionally include a firewall so that they can be used as a full-fledged security module for the connection of industrial to corporate networks.

Layer 3 Switch

As already explained, the OSI model switches operate at layer 2, while the routers operate at layer 3. A Layer 3 switch, however, is a powerful device for routing in the network.

Layer 3 switches differ little from ordinary network routers. Both process the incoming packets and choose on the basis referred to in these addresses dynamically via the forwarding of these packets (routing). They have their origin in demand for routers that easily in large networks, for themselves leave as company intranets use.

The main difference between a Layer 3 switch and an ordinary routing is to build the hardware. In a Layer 3 switch, the hardware is one switch provided combined with a router to ensure better performance when routing in large LAN infrastructures. The Layer typically used for intranets 3 switches usually have no WAN ports and usually support no typical WAN applications.

Connecting a Private Network to the Internet

An automation network may be associated with an industrial router with a corporate network, or the Internet-based Ethernet for the automation network must be a Net-ID selected, preferably the RFC 1597 corresponds.

The below Figure shows an example. The router receives on the LAN side IP address of the selected address space for Net ID belongs. In general, this is the first or last free IP address of the network. The network interface, on the other hand, on the LAN side and a MAC address. The router acts on the network as the default gateway.

The network can through the WAN interface of the router connected to the Internet advertising. For this, get the router, usually via DHCP, assigned by the ISP (Internet Service Provider- of) a unique IP address on the Internet.

Each device on the network can now be configured as follows:

IP address 172.23.22.14

subnet Mask 255.255.0.0

default gateway 172.23.0.1

Each participant gets an IP address with the Net-ID, but the host ID is different for all participants the same for each participant.

If an application running on a networked PC application wants to initiate communication with a server on the Internet, the PC must first create an IP packet to the connection request. This IP packet is sent out via the default gateway to the Internet. For this purpose, the PC, the IP packet encapsulates in an Ethernet frame. The next figure shows the need for the creation of Ethernet frames data. The MAC address of the routers is requested via the ARP protocol.

Once the ARP reply has arrived at the router, it sends the IP packet through the WAN interface to another router on the Internet. Since the private network is disconnected from the Internet, the router replaces the source IP address of the PC with its own address on the WAN side. The private network is accessible only via these external IP address of the router over the Internet.

The server can then send a reply to the external IP address of the router. The router is now to determine at which PC this response must be sent on the task. In response, the server details are on the original sender. To solve this problem, the IP NAT has been developed.

IP NAT

NAT: IP Masquerading

Network Address Translation (NAT) is a protocol that enables networks with unregistered IP addresses (private networks, 1597 correspond to the RFC) advertising connected to the Internet. The router recorded as described above in each message that is sent from the private network to the Internet, always its external IP address as the source address.

Each answer word that is directed from the Internet to a PC on the private network goes to the external IP address of the router but contains as TCP destination port a port number from the NAT table of the router. In this way, the router for which end the respective message is intended white.

Practically speaking, NAT a protocol of a network translates an IP address into a valid in other network IP addresses. One network is called Inside, the other outside. Generally, a company translates its local internal IP addresses in one or multiple global external IP addresses and translates incoming messages from global IP addresses.

NAT makes it, therefore, possible that operation only a single global IP address used for its communication with the outside world, the Internet. This contributes to the safety concept, as all outgoing and incoming are subject to the news an address translation.

The below Figure shows the operation of the NAT protocol. Here, the NAT protocol is used dynamically. This use is also dynamic NAT.

Port Forwarding

The static use of the NAT protocol is known as port forwarding or port forwarding. If there is the private network server that must be accessed directly from the Internet, the endpoints of these servers can be static port numbers are assigned in the NAT table of the router to these servers from the Internet.

to achieve must be connected as the endpoint of the external IP address of the router with the port number of the NAT table. The router translates in for the special Server On outgoing messages from the endpoint to the correct endpoint of the server. This is an additional form of security. The exact IP data of the server must not be published, and any hackers know nothing about the architecture of the network are the servers in the. The next Figure shows the configuration for port forwarding or port forwarding.

1: 1 NAT

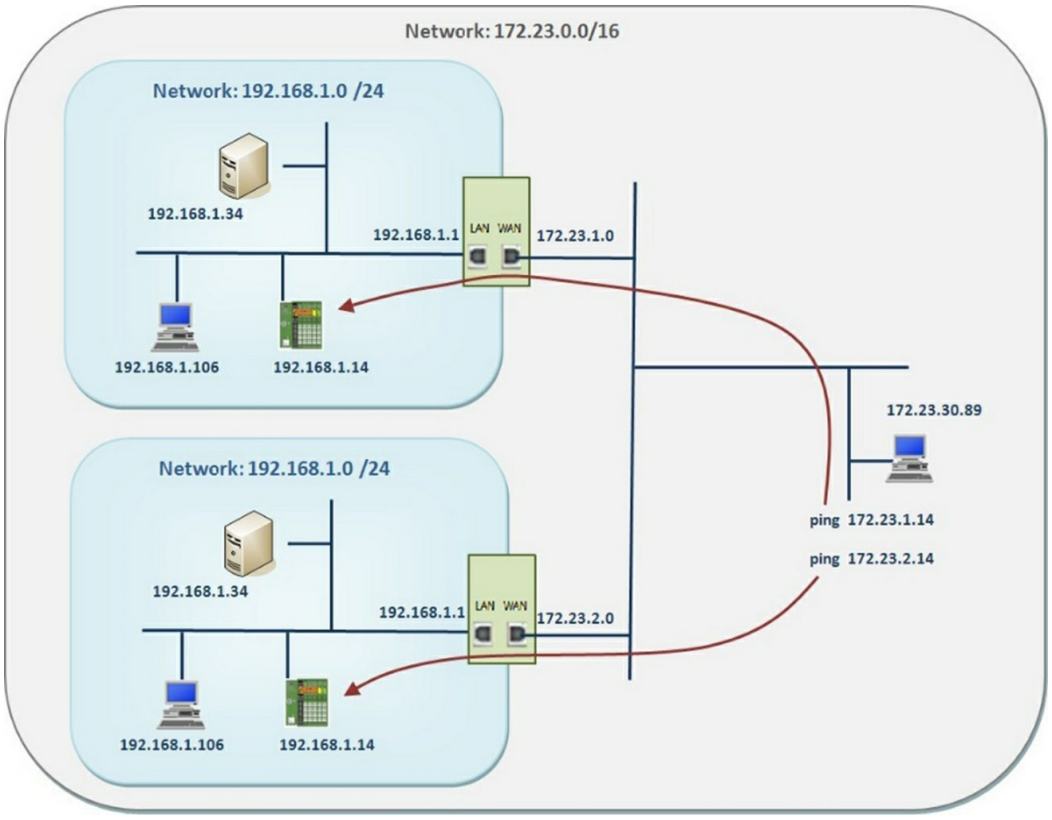
At 1: 1 NAT is an IP address translated to another without changing the TCP / UDP ports used.

If a router on the LAN side to the network 192.168.1.0/24 and via the WAN port is connected to the network 10.1.0.0/16 and has as external IP address 10.1.1.0/16, then using the 1: 1 NAT LAN nodes with the IP address 192.168.1.100 accessible on the WAN side through the IP address of 10.1.1.100.

1: 1 NAT offers interesting possibilities for the automation world:

- Different subnets can be connected together; in all subnet zen same IP address is used.
- No need additional routes are defined in the corporate network.
- An ARP demon on the mGuard processes the ARP request from the external network.
- Systems subnetworks can be addressed via the IP mapping directly from the corporate network. In this mapping, the host ID is retained; only the net ID is adjusted.

The below Figure illustrates the operation of 1: 1 NAT.



Conclusion

It's hard to talk about routers, switches, wireless connectivity, and other networking technologies without remembering Cisco. World leader in networking and internet device solutions, the company is also the fastest growing in the worldwide server market. In 2015, for example, while competitors were growing 6 percent, Cisco was up to 32 percent.

Given this fact, as well as about 85 percent of Internet data runs on US multinational solutions, it is not so complicated to understand the importance of IT professionals in getting Cisco certification.

With the high dollar, the increasing degree of difficulty of the tests (formulated by Pearson Vue), and the 3-year validity of certificates, many wonder if it's worth having an official Cisco qualification. If you are one of these people, we strongly recommend following this article to the end!

In the IT field, certification is a formal procedure in which a company ratifies that a particular professional has particular knowledge or skills. This seal reinforces its credibility with the market, a fact that invariably results in higher pay and a higher chance of career advancement.

For example, taking a Cisco Certified Network Associate (CCNA) certification means assuring the market that you have the necessary networking installation and support skills.

At the Cisco Expert level, a Cisco Certified Design Expert (CCDE) certification signals that you are an expert with the ability to design infrastructure solutions for large enterprise environments.

Some research shows that having IT certifications raises pay by about 30%. There is, however, a Forbes study that shows that, in some cases, these changes in your professional skills may even double your monthly earnings.

The point is that, no matter how good your home university, you will be introduced to the market with general knowledge about the most diverse technologies. The business world is pleased with this versatility but will also expect specialization in some routines.

After all, the learning curve required for a network professional to understand all the nuances of Cisco equipment takes time, something that organizations definitely don't have. This is why many CIOs prefer to pay higher salaries to those who already have certifications, rather than undergoing the extensive learning time of an employee not so familiar with specific technologies.

Cisco works with dozens of certifications at various levels, starting at entry-level, intermediate, specialist and expert, to the maximum degree of knowledge, called “architect.”

In addition to levels, certifications are also divided into “careers.” The most important are Routing and Switching, Security, Design, and Collaboration (collaboration - telephony, voice, and video over IP).

Imagine you have Cisco official recognition of all these areas, on many levels! Clearly, with such vast know-how in Cisco technologies, their possibilities for promotion are greatly expanded.

According to IDC, in the first quarter of 2017, Cisco took the lead in the Brazilian x86 blade server market, with 37.3% market share in the segment. With a universe of products spread across the world's top companies, can you assume the added value that Cisco certification can bring to your working life?

Know the most diverse network protocols (CCNA), troubleshoot local and wide area networks (CCNP), be able to plan and design a business strategy-bound IT infrastructure (CCAR)): Many doors open to those with these skills, especially since they are stamped by none other than Cisco itself!

Few segments change as fast as Information Technology. Thus, keeping up to date on databases, servers, network management tools, among other platforms, is essential to remain competitive in the market.

If you dream of living abroad and working for a large company abroad, Cisco certification is a must.

According to Salary Survey 2016 data from Certification Magazine, 61% of certified professionals reported that obtaining official qualification was a key factor in raising their salary and opening new career growth opportunities, including in other countries.

The first step is to understand your journey. Cisco certifications include the following identifications:

- Cisco Certified Entry Networking Technician (CCENT);
- Cisco Certified Technician (CCT);
- Cisco Certified Network Associate (CCNA);
- Cisco Certified Design Associate (CCDA);
- Cisco Certified Network Professional (CCNP);
- Cisco Certified Professional Designer (CCDP);
- Cisco Certified Internetwork Expert (CCIE);
- Cisco Certified Design Expert (CCDE);
- Cisco Certified Architect (CCAR).

So your initial step is to start with CCENT, also known as ICND-1. This certification is a prerequisite for associate-level qualifications such as CCNA and is indispensable for you to gain marketability as a network technician or help desk (earning above your peers who do not have this official recognition).

The exam (which is face to face) has between 45 and 55 questions to be solved in 90 minutes. The value of the investment currently circulates around the US $ 165.00 (ICND-1).

To take the ICND-1 test, it is highly recommended to take a specialized course. (Cisco official), which will cover all the content required by the company in the configuration of switches, routers, WAN network connections, Cisco Discovery Protocol (CDP), deployment of security features, among other key topics.

Passing this assessment is paramount to pursuing other certificates (such as ICND-2) and further advancing your certification portfolio.

Now that after completing this book, you know what to do next with your Cisco certification journey. Good luck!

References

http://www.ciscopress.com/store/ccna-200-301-portable-command-guide-9780135937822

https://www.mouser.com

https://dl.acm.org/citation.cfm?id=1207049

https://www.cisco.com/c/en/us/td/docs/ios/fundamentals/command/reference/

https://www.scribd.com/document/21011643/IP-Subnet-Cheatsheet

https://www.slideshare.net/minariyahi5/chapter-3-52210471

https://www.academia.edu/34123026/Introduction_to_TCP_IP

http://ijssst.info/Vol-17/No-33/paper13.pdf

https://www.academia.edu/35544352/CCNA_Routing_And_Switching_Portal_3rd_Edition

CISCO CCNA COMMAND GUIDE

Tips and Tricks to Learn Cisco CCNA Command Guide

STUART NICHOLAS

Introduction

Every company these days works on hiring new network administrators and engineers who can optimize and improve the existing systems. These employees also work toward reducing any costs that will eventually increase the productivity of other employees in the organization. If you are looking to improve your capabilities and want to become a routing and switching engineer, you should appear for the CCNA Routing and Switching examination.

This book is designed to guide you to help you understand what CCNA is and how it came about. We will also look at the different requirements you will need to fulfill to apply for the CCNA Routing and Switching examination. Apart from this, you will also gather some information on Cisco and the products offered by the company. It includes questions regarding the content of the exam, why you need a certification, what the different CCNA exams are, how to attain certification for each, and what exams can be taken to get the certification. You will learn more about the CCNA Routing and Switching examination and gather some information on the different topics covered in the examination. We will also look at the history of the examination. This will help you understand how Cisco made changes to the curriculum over time. You will notice that Cisco has done its best to incorporate the changes and developments in technology into the new curriculum.

If you follow the tips mentioned in this book, you can ensure that you will pass the examination in your first attempt. This book will answer all the questions you may have about CCNA Routing and Switching. This book also includes some tips that will help you ace the examination. It is important to remember that you cannot expect to clear the examination in your first attempt if you do not study ready for it. It is only when your concepts are strong that you can ensure that you ace the examination on the first attempt.

Having said that, it is okay if you do not clear the examination in your first attempt. All you need to do is use your experience to help you understand where you went wrong and correct your studying method. Once you clear the examination, you will attend interviews, and there are some employers who

like to throw trick questions at their candidates. This book also sheds some light on the different questions you can be asked during an interview for the role of a networking engineer or professional.

I wish you luck on your examination and hope you obtain the certification in your first attempt.

Chapter 1

An Introduction to Cisco

Cisco was founded in the year 1984 by two Stanford employees - Sandra Lerner and Leonard Bosack. The two graduated in the year 1981, and they worked at Stanford before they founded Cisco. They worked as Computer scientists at Stanford and used the router at Stanford to communicate with each other. Lerner and Bosack learned that they could communicate with one another using the router, and also expand the technology to include multiple systems to the network. This was when they realized that they could develop a large-scale, profitable business that would include router and networking services. That is when in the year 1984, the couple founded a company called Cisco Systems. It was only in the year 1986 that Cisco obtained the rights to the network and routing systems at Stanford. Cisco is what it is today because of the products and services that were offered by the business. These products and services are what made the company the largest leader in the industry. We will look at the different products and services offered by Cisco in the following chapter.

Facts about Cisco

As we read earlier, Cisco is a networking and IT brand that specializes in routers, switches, IoT, and cybersecurity. The logo of this company is in most offices on their conference hardware and telephone. Cisco is a very popular organization, but there is still some enigma around this brand that makes people want to learn more about it. This section covers some facts that you may not have known about Cisco.

Cisco Is Short For San Francisco

As mentioned earlier, the company was set up by two computer scientists Sandy Lerner and Leonard Bosack, in the year 1984. During the early years, the products and services offered by this company were always branded with the lowercase letters "cisco." The logo is just a few vertical lines, but these lines represent the Golden Gate Bridge.

Early Troubles at Stanford

Leonard Bosack and Sandy Lerner were employees at Stanford when they founded Cisco. When Lerner left Stanford, Bosack continued to work there with Krik Lougheed, a co-founder and co-worker at Cisco and developed the first router. This router was, however, a copy of the router used at Stanford, called "Blue Box." They used the multiple-protocol router software developed by the university in their Cisco IOS. This was an unlicensed copy of the software. When Stanford became aware of this in 1986, they forced Bosack and Lougheed to leave Stanford. The university also considered filing charges against the company since the founders stole intellectual property. Stanford, however, agreed to license two routers and the router software to Cisco in the year 1987.

Cisco Has 73,711 Employees Worldwide

Cisco was launched in the year 1984 on December 10th. The company was set up in California, and it went public in the year 1990. The employee count in the year 2016 was 73, 711, and the revenue of the company in that year was $12.6 billion.

Most Valuable Company in The World

Cisco is the most valuable company in the world. This company was at the apex in the year 2000 during the dot-com bubble. The price of each share was $80. This was not sustainable since the price of the stock was almost 250 times the earnings of the company, and when the bubble popped, the price of the stock reduced. The price of the stock never reached this value in the later years, but the market capital never reduced, and it is over $170 billion that trades at 18 times the earnings made by the company. Today, the world's most valuable company is Apple. This company has a market capital of $730 billion, and the shares are traded at 17 times the earnings made by the company.

Cybersecurity Is the Fastest Growing Business

Cisco has a cybersecurity company that it has set up, and this is the fastest growing business for Cisco. This unit increased Cisco's annual revenue by 14%, which made the returns $220 billion in the last year. This unit also accounted for about 10% of the product revenue. Cisco has begun to expand its business by acquiring other companies and investing in smaller companies. This company bundles its networking hardware and software with security products. This gives the company leverage against smaller

security companies like Fire Eye. Word has spread that Cisco is looking at acquiring this company.

Cisco Provides Free Training to Thousands Through the Academy Program

The Cisco Networking Academy, known as NetAcad, was launched in 1997. In that year, there were close to 64 educational institutions set up across seven states in the United States. Since its inception, the academy has spread to over 150 countries, and close to 2 million students have enrolled at over 10,000 academies in universities, technical schools, high schools, community-based organizations, and colleges.

The Cisco Networking Academy Program has numerous e-learning programs that help students improve their Internet technology skills that are essential in today's economy. This academy delivers online assessment, web-based content, hands-on lab, student performance tracking, preparation for industry-standard certification, and instructor support and training. Nigeria has over 30 Cisco Networking Academy centers, and this country has the highest female participation in the EMEAR (Europe, Middle East, Africa, and Russia) region. There are over 35,000 females trained since the inception of this academy. Nigeria has the largest number of women who signed up for the Cisco academy in the year 2016.

Cisco Made Cameras

In the year 2009, Cisco worked on expanding its presence across consumer electronics. It purchased Pure Digital Technologies for a mere $5Diva finished up this million. This company worked on developing and manufacturing Flip Video camcorders. Cisco, at that time, stated that they would connect cameras to the Internet. This would allow users to share, publish, and access the videos easily on the Internet. This fits Cisco's vision of visual networking.

This was very similar to what GoPro had mentioned a few years later. At that time, smartphones had come into existence, and they knocked out Flip video cameras and GoPro cameras out of the market. When these products were rendered obsolete, Cisco killed these products quietly in 2013.

Cisco Sold the Set-Top Box to Technicolor

In the year 2005, Cisco worked on improving the video streaming

technologies and acquired the company Scientific Atlanta for $6.9 billion. The technologies offered by Scientific Atlanta strengthened the video services that Cisco provided along with other collaboration products. These set-top boxes, however, were a dead weight since there was no way they could grow. Cisco then chose to sell the set-top box business in the year 2015 to Technicolor for $600 million. It is also for this reason that Cisco has reported set-top boxes over the last few quarters. In the last quarter of 2016, the revenue fell by 3%, but the revenue only dropped by 2% if you excluded the set-top box business.

Cisco is one of the best IT and Networking brands in the market. This company also takes pride in the fact that it has an equal number of male and female employees. It is also trying to bridge the gap in IT and networking skills across West Africa.

Chapter 2

Products and Services Offered by Cisco Networking Solutions

Networking

Cisco gives every company numerous choices for its networking needs. Some of these choices have been listed in the section below. Cisco designed the products mentioned below to meet the changing needs of companies and to improve data storage, access points, and servers that are used in the organization.

Any organization can be certain of the smooth flow of information and smooth business transactions if the network in the company is maintained well. There are numerous networking options that an organization can choose from. These options allow an organization now only to automate the network but also to decrease the cost of a Wide Area Network, thereby improving the business's ability to scale. These networking options also ensure that the network performs very well. These networks are built with enough detail that will help it to detect any imminent threat and protect the organization from any damages.

VPN Security Clients

A threat can occur through numerous attack vectors, and it is for this reason that every company must identify a way to secure active protection and connectivity for every endpoint in the network. On average, when others can detect threats in 100 days, Cisco can provide such details on threats in just 4.6 hours and process about 1.5 million malware per day.

Switching

It is important to find the right switch for your company. This is because data is extremely critical for the company in today's world. It is essential to select the right switch to avoid threats faced by the company - now and also in the future. Companies can always use Cisco products to simplify and manage their requirements for IoT, cloud, data center, and mobility.

Routing

Cisco's routing product, another networking product, can only be used for LAN, WAN, and cloud. It includes integrated security, application optimization, automated provisioning, and advanced analytics that deliver a complete and proven solution to your organizational requirements. A company can now automate all of its processes using these routers. These routers also offer application and intelligent path selection, which needs minimal control through customization and programming. A high performing router will always streamline any networking operation, thereby reducing the cost, increasing the speed, and the deployment of the network more agile. Regardless of whether the business is large or small, the Cisco Networking solutions will offer a wide range of products and services that can fit any business model.

Wireless

In today's digital world, one can access any network through a wireless mode. It is imperative that every business has a wireless network since, without that, it is hard for a business to communicate with its customers. It is also hard for an employee to work. If a business does not have the right network, its data is privy to attackers. By using Cisco Wireless Enterprise Technology and Mobility products, you can be assured to get the state-of-the-art access points and top of the line WAN and LAN connections. Cisco offers some of the best products and services in this area, and these products are designed to provide high-end security and performance. The best part of it all is that these can fit any small and medium-sized enterprises to large-scale businesses.

Wireless Controllers

As the world is geared up to go wireless, Cisco developed the Wireless Controllers to provide networking options that are secure. These networking options also allow the network to be segmented, thereby decreasing the number of threats. They are easy to access and can be enabled even on the cloud. A wireless controller was designed by Cisco to provide faster insights, troubleshoot any problems quickly, and deliver a personalized business. These are also designed to have easy upgrading without any interruptions.

Conferencing

WebEx and other conferencing tools are open platforms that enable companies to integrate different features into their workflow. They can

communicate with teams across the globe. These conferencing tools make it easier for companies to communicate, collaborate, and work together. You can communicate with someone in India or Australia in a matter of seconds, and these tools are encrypted. This will ensure that the work you share is safe. Cisco offers numerous such tools that allow companies to work seamlessly so they can share, create, and meet virtually.

Unified Communications

People from all over the world work together on a project, and they use different tools to collaborate. For example, they can use the web and video conferencing, IP telephones for Voice calling, mobility desktop sharing, voicemail, instant messaging, and more. Through the unified solutions offered by Cisco, a company can choose to integrate different tools to improve user experience. This will enable teams to work together effectively. The tools offer real-time communication methods to different companies anywhere in the world. Services like messaging, conferencing, and chat options are also included in these tools. Unified communications offer on-premise, partner-hosted solutions, or as a service, which is called UC SaaS from the cloud provider.

Advanced Malware Protection

There are multiple threats to a network, and hacking is one of the most common threats. Through advanced malware protection, Cisco offers companies products that will enable them to block malware and protect their data. These tools also offer global threat intelligence that will protect the network from any breaches. Since most companies cannot prevent threats alone, Cisco removes threats to the network and system by analyzing every file, quickly detecting any threats, containing and removing those threats from the system.

Web Security

There are many threats that hide in plain sight, even on legitimate websites. These threats come up in the form of advertisements or links. The clients and employees may threaten their data if they click on any of these links or advertisements. This will lead to some issues with data integrity. WSA Web Security Appliances, powered by Cisco Talos, protect you by automatically blocking risky sites.

Access Points

The need for security has increased since the growth of mobility and IoT devices. The Cisco Catalyst 910 access point exceeds the new W1-Fi 6 wireless standards and provides radio frequency excellence to high–density environments. These access points help to increase the productivity of employees since it allows data to be transmitted at high speed. This efficient data transmission will help businesses upgrade to new technologies in no time.

Business Collaborations (Collaboration Endpoints)

Cisco is the pioneer in networking and routing technology, and this enables the company to connect different businesses across the globe using this technology. Over time, Cisco has worked on developing numerous solutions that can enable teams from across the globe to work together towards a common goal. These tools enable employees to communicate with each other with less effort. These products include Cisco WebEx Board, Cisco Headset 500 Series, and Cisco WebEx Room Series. Choose the product that suits your company's needs, and you are good to go.

Interfaces and Modules

Cisco uses numerous modules and interfaces to deploy advanced networking capabilities. These help every business deliver a new service, which will lower the cost to the company.

Networking Management

Cisco uses leading products and services to reduce downtime and improve operational efficiency in businesses. Its products and services also manage the network of the enterprise. These products and services have been designed to fit an organization of any size and also provide access to numerous digital systems and processes. Through these products and services, Cisco provides opportunities to automate policy-based application profiles, which allow the IT team to respond quickly to new business opportunities.

Security

Since the world is data-driven, the safety of the consumer's data is of utmost priority. Cisco offers numerous solutions that have changed the face of data protection. Every company faces a major threat because of hacking and lack

of cybersecurity. Hackers have become smarter and dangerous over the years. With Cisco's integrated portfolio and industry threat intelligence, you get the scope, scale, and capability to keep up with the complexity of every kind of threat.

Advanced Email Security Protection

Most hackers rely on emails to hack a system. They send spam emails through which they can spread malware and other threats. Every business should maintain the right security solutions. This is the only way they can prevent any threats. Companies can use Cisco's email security to defend systems from compromising business emails, ransomware, and phishing. This product also enables companies to update their security every five minutes using Cisco Talos. This tool protects the system from any malware attachments or any malicious links that hackers send via emails. It is always essential that a business secures the data in the emails that are sent from one system to another, either within or outside the organization. Cisco's email security ensures that there is no loss of data and encrypts all the information in emails. This helps to safeguard sensitive information.

Outdoor and Industrial Access

An outdoor and industrial access product will allow you not only to access data anywhere but also access WiFi outdoors. It also helps people stay connected in numerous locations, which makes it easy for companies to continue their operations with ease. Since these access points are resistant to both extreme cold and heat, it makes it easier for businesses to transmit data through these access points.

Customer Collaborations

A consumer can acquire almost anything in today's digital world. With this comes the need for an organization to respond to all its customers' queries and issues and also provide them with a few personalized services. The mantra 'one size fits all' does not hold up in today's world, and it is for this reason that there are no contact centers any longer. Organizations now try to provide their customers with the right care, and this is no longer an exception but a rule. Cisco has developed products such as Cisco Packaged Contact Center Enterprise and Cisco Unified Contact Express to enable ease of service.

Product by Company Type

There are numerous medium-sized companies and new businesses that have been set up in the US in the recent past. One of the aims of Cisco is to empower these firms to do better in the market. This goes to show that the concept of 'one estimate doesn't fit all' works perfectly for Cisco. It is for this reason that Cisco has produced some items as per the wants of the organization, hence allowing organizations to work on personalizing their operations and help them stand out when compared to the other companies.

Services

Apart from the numerous products listed above, Cisco also provides companies, big or small, with the services necessary to install necessary hardware and software and also to train their employees to maintain that installed software. Cisco also works as an advisor and helps organizations and companies implement some IT solutions in their firm. It also helps a company optimize the performance of the company that improves both efficiency and productivity. Cisco also works on managing the assets of the company. It also takes care of the cloud services. Cisco also sends professionals to train employees to learn more about the digital shift in the market and also provides the necessary assistance that will help in the growth of the company.

Chapter 3

About CCNA Examination

CCNA or the Cisco Certified Network Associate is one of the many certifications offered by Cisco to networking professionals. This certification offers a wide variety of technical specialties that an IT professional must know. There are two levels of accreditations that any professional can obtain through Cisco: Cisco Certified Entry Level Technician (CCENT) or the Cisco Certified Technician (CCT) certification. The former is a certification for experts who have the necessary skills to configure and operate some network support stations. The latter is a certification that will enable a professional to identify, analyze, fix, and oversee any networking components used by an organization.

There are three specializations offered under the CCT certification:

1. CCT TelePresence
2. CCT Data Center
3. CCT Routing and Switching

The third certification is the most sought-after certification since the course material will focus on all the knowledge that a professional must know how to take care of any equipment developed by Cisco. This equipment includes routers, systems, and other network hardware and software. The course material will give the professional an idea on how to work with Cisco routers, switches, connected, and cabling parts. Every certification offered by Cisco will enable a professional to work as a network expert.

Cisco also offers associate-level qualifications to experts or professionals for video, voice, industrial, cloud, wireless, server provider, data center, routing, and switching. For example, many organizations use wireless products to ensure that they can connect different systems across the globe. The CCNA Wireless certification will enable the person writing it to learn more about wireless technologies and also understand how to troubleshoot any errors or configure a new wireless network.

The CCNA Security certification sheds some light on numerous security aspects that are important for any system security expert to know. When you pass this examination and obtain the certification, your employer will know that you have what it takes to identify any dangers to the system, limit any vulnerabilities in the network and also oversee any complex security frameworks.

The CCNA Routing and Switching examination are one of the most well-known associate-level programs offered by Cisco. The requirement for qualifying as a system expert increases since the systems continue to evolve. It is important for some individuals to learn more about how they can design, create, and troubleshoot any network issues that may arise.

The systems administration networks always plan video administrations, voice interchanges, and joint effort conditions. The different concepts and ideas covered in the CCNA Routing and Switching examination are significant and can be applied across different modules. The modules that you will need to prepare for while studying for the CCNA Routing and Switching certification are in line with the appointed assignments of systems administration experts. This program also helps you understand how you can plan and design a system. This also offers help as a specialized master.

When you clear the CCNA Routing and Switching certification, you will have a range of abilities and have amassed a lot of knowledge. As a CCNA associate, you should be able to:

- Learn the different network topologies and understand how you can protect the network
- Explain how the network works and understand how different devices can be connected to that network
- Investigate, build, design and check how a switch works with communication devices and VLAN
- Actualize an IP addressing service and scheme to meet any prerequisites
- Arrange, confirm and investigate routing and router activities on current Cisco gadgets
- Identify any dangers in security and depict or derive some strategies

to control or limit the risk

- Identify some countermeasures to address the risk
- Design and configure a Wide Local Area Network
- Setup and configure a WLAN and execute the right strategies to connect the devices to that network

Chapter 4

Frequently Asked Questions and Myths

FAQ

What changes have been made to the associate-level certification programs offered by Cisco?

Cisco declared on March 26, 2013, that it was planning to update or redesign the associate-level certification programs. This includes the CCNA and Cisco CCENT certifications. Cisco works on restructuring these courses to ensure that the course material is aligned with the changes in the technology in the routing and switching industry. The course material for these courses also includes advanced switching and routing technologies, including security, remote, and voice. This certification was previously called the CCNA Certification and has now been broken down into multiple segments, and one segment is the routing and switching certification.

Additionally, most associate-level examinations, including the CCNA Voice, CCNA SP Operations, CCNA Security, and CCNA Wireless examinations, consider the CCENT Certification as a prerequisite. You should visit the Cisco Learning Network to learn more about these associate-level certifications. This network will also help you learn more about the numerous changes that are made to the syllabus.

Are there changes being made to the CCNA Routing and Switching Exam?

Cisco has split the CCNA certification into the ICND1 and ICND2 examinations. Cisco has included the following topics in the syllabus for the certification: IPv6, investigating, and the most recent Cisco routing and switching technology and software. Cisco, as mentioned earlier, always includes newer concepts in the syllabus since improvements and advancements are being made in this industry. The exams 640-816 ICND2, 640-822, and 640-802 will now be replaced by the 200-101 ICND2, 100-101 ICND1, and 200-120 CCNA respectively.

Why have so many new topics been included in the CCNA and CCENT

Routing and Switching exams?

Numerous Cisco clients across the globe have affirmed that they require every employee with a Cisco certification, especially a CCNA certification, to have better abilities and knowledge. To accommodate this request, Cisco has moved a few subjects from the ICND2 certification to the ICND1 certification examination. If you pass the ICND1 test now, you will undoubtedly have better skills and more knowledge when compared to a student who passed the previous ICND1 examination. The new syllabus will now help you learn more about the different topics covered in this examination. Ensure that you clear this examination before you appear for the ICND2 examination. This addition made to the syllabus is indeed slightly difficult for most students to comprehend, but it is always a good idea to clear these examinations if you want to have the edge over your competition.

If I want to obtain the CCNA Routing and Switching Certification, what are the necessary requirements that I need to adhere to?

If you want to obtain the CCNA Routing and Switching Certification, you must clear the following exams:

- 200-125 CCNAX Composite Exam

OR

- 100-105 ICND1
- 200-105 ICND2

Is there a formal training course that I will need to attend to obtain the certification?

There is no necessity to attend any formal training if you want to appear for these examinations. That being said, it is always a good idea for you just take up a few instructor-led sessions while you are preparing for the examination. These sessions will give you the chance to learn more about the subject.

Where should I register to take up an instructor-led training course?

It is imperative to keep in mind that only those Learning Partners who are authorized by Cisco are allowed to provide instructor-led sessions. These sessions will always be given by those instructors who have been certified by

Cisco. You should visit the Learning Partner Locator on the Cisco site to identify the centers that are the closest to you.

Should I meet any prerequisites before I appear for the CCNA Routing and Switching certification examination?

Cisco has not laid out any prerequisites for the CCNA Routing and Switching examination. It is always a good idea to have some experience in this field before you appear for the examination.

What job roles can I apply for once I obtain the CCNA Routing and Switching Certification?

You can apply for the following jobs or roles when you obtain the certification:

- Network Analyst
- Network Support Engineer
- Network Specialist
- Network Engineer Associate
- Network Administrator

How soon must I recertify my certification?

As with every other certification offered by Cisco, the CCNA routing and switching certification are valid only for a specific period, which is three years. You must recertify yourself once the period is over. To learn more about the recertification process, read through chapter six.

Is there any self-study material that I can use to prepare for the certification?

You can use different self-study material available on the Cisco website to prepare for the examination. Some of these options are:

- E-learning courses
- Cisco Certification Practice Exams
- Cisco Learning Labs

- Cisco Press

Myths About CCNA

An issue with the Internet is that it gives some people the power to spread incorrect information about anything. The Internet also allows rumors and incorrect information to spread quickly. The fact is that the story is always exaggerated as it moves from one platform to the next, and the CCNA examinations are no exception to this. There are a few myths about the CCNA and CCNP examinations that have been covered in this section.

The questions you are asked in the exam are based on the survey that you fill out at the start of the exam.

Every student is required to complete a survey before he or she begins the test. This survey will ask the candidates about the different topics they are comfortable with and also talks about some technologies that they are comfortable with. It is difficult to rate yourself ISDN, Frame Relay, and other technologies since you are about to take an examination that covers those topics. Therefore, it is possible that you may worry about how the questions will impact your examination. The truth is that your answers to the questions in the survey do not matter. There are some forums and posts on the Internet, which will tell you that you must always rate yourself excellent on any topic that is being asked. This is because they believe that the questions asked from that topic will be easy for one to cover. If you lower the rating, the difficulty of the questions asked from that topic will increase. Cisco has debunked this myth, and you mustn't read too much into the questions asked in the survey. You should not worry too much when you are filling out the survey.

When you answer a question incorrectly, the exam will ask you questions from that topic until you get one answer right.

Cisco does not follow the pattern of adaptive testing in any of the certification examinations that it conducts. All the questions asked during the examination will be taken from a large question base. If you have appeared for the Novell examination or the GMAT, you will understand what I mean by adaptive testing. Therefore, CCNA examinations are not nerve-wracking.

Your answer will be marked wrong for the simulator questions if you include an extra command.

Both the CCNA and CCNP examinations use the simulator engine. This engine will only act like a router or a switch. Therefore, you can use some extra commands during the examination. You will be given instructions and information about the engine that you are using before the exam. Remember to relax and try to configure the switch the same way you did when you were practicing your labs.

Once you walk into the examination room with a combination of the required knowledge, the troubleshooting skills, theoretical and practical knowledge, and hands-on experience, you can pass your exam. Do not let what some people believe about the examination deter you from applying.

Things to Keep in Mind

CCNA is a comprehensive exam

Regardless of which CCNA certification you appear for, you will notice that the questions are spread across the different topics covered in the syllabus. You will see that the questions are not only based on TCP/IP topics but also cover questions on how routing protocols can be used to span trees. There is a lot to cover in the CCNA examination, and it is for this reason that the exam is deemed to be difficult. Instructors and experts state that every candidate should always focus on the ICND subjects if they wish to create a foundation for themselves. This means that you will need to understand everything in the material for those exams.

The CCNA exam is very quick

The CCNA examination is very quick in the sense that you only have ninety minutes to answer sixty questions. It is very difficult for anybody to answer those many questions in a short period, but if you are well prepared, you can zoom past the questions in no time. You must remember to focus on your training and experience. Most of the questions in the examination will focus on real-world problems.

The Cisco Networking Fundamentals

The CCNA Routing and Switching Certifications will teach you about the different fundamentals of Cisco networking if you are looking to work in that field. This certification focuses on foundational IP networking skills. It also teaches individuals how to troubleshoot any issues. A CCNA certification

will help you learn more about designing and configuring LAN switches, identify basic threats, configure IP routers, install and verify the basic IPv4 and IPv6 network, understand topologies, configure EIGRP, connect to a WAN, configure OSPF in IPv4 and IPv6, understand network issues and wide area of the technologies, understand device management and Cisco licensing. You will learn more about the course and some skills that will help you in your job. Your career will also improve once you obtain CCNA certification since this examination will ensure that you develop the necessary skills to perform effectively in your company. Numerous organizations accept this certificate since it will help you learn more about networking.

Exam Objectives

This section covers the objectives of the CCNA Routing and Switching examination.

Network fundamentals

This is the first module that is covered in the syllabus, and it includes fundamental topics like TCP/IP protocols, firewalls, etc. and others related to networks. Ipv4, Ipv6 address details are also included. Let us look at some of the topics covered in this module:

- Compare and contrast OSI and TCP/IP models
- Compare and contrast TCP and UDP protocols
- Describe the impact of infrastructure components in an enterprise network
    - Firewalls
    - Access points
    - Wireless controllers
- Describe the effects of cloud resources on enterprise network architecture
    - Traffic path to internal and external cloud services
    - Virtual services
    - Basic virtual network infrastructure

● Traffic path to internal and external cloud services

● Virtual services

● Compare and contrast collapsed core and three-tier architectures

● Configure and verify IPv6 address types

● Selection of the appropriate cabling type based on implementation requirements

● Compare and contrast Ipv4 address types

- Unicast
- Broadcast
- Multicast

● Comparison and contrast of network topologies

- Star
- Mesh
- Hybrid

● Configuration verification and troubleshooting Ipv6 addressing

● Compare and contrast of Ipv6 address types

- Global unicast
- Unique local
- Link-local
- Multicast
- Modified EUI 64
- Autoconfiguration
- Any cast

IP Addressing – Ipv4 and IPv6

● Identifying the addressing scheme for IPv6 to satisfy the addressing methods in the WAN or LAN environment

● Identifying the appropriate addressing scheme for IPv4 using summarization and VLSM to satisfy any addressing requirements in the WAN or LAN environment

● Describe the necessity and operation of using both public and private IP addresses for IPv4 addressing

● Describe the requirements to run IPv6 and IPv4 together as a dual-stack network

● Describe IPv6 addresses

IP Services

● Configure and verify DHCP (IOS ROUTER)

● Configure and verify ACLs in a network environment

● Configure and verify NAT for given network requirements

● Configure and verify NTP as a client

● Configure and Verify Syslog

● Describe the types, features, and applications of ACLs

● Recognize high availability (FHRP)

● Identify the basic operation of NAT

● Describe SNMP v2 and v3

Network devises Security

● Verify the network device security feature and configure it

● Verify the ACLs to limit the SSH and telnet access for a machine to a router

● Verify and configure the security features for a switch port

● Verify and configure the ACLs to filter any network

LAN Switching Technologies

You will learn more about different switching concepts in a network like inter-switch connectivity, STP protocols, configuring a network, and more. Some of the topics included in this module are:

● Configure and verify initial switch configuration including remote access management

● Determine the technology and media access control method for Ethernet networks

● Verify network status and switch operation using basic utilities such as PING, TELNET, and SSH

● Identify the basic switching concepts and operation of Cisco switches

● Identify enhanced switching technologies

● Configure and verify VLANs

● Configure and verify trunking on Cisco switches

● Configure and verify PVSTP operation

● Describe how VLANs create logically separate networks and the need for routing between them

● Troubleshoot interface and cable issues (collisions, errors, duplex, speed)

● Describe and verify switching concepts

● Configure and verify troubleshoot VLANs (normal/extended range) spanning multiple switches

● Describe the benefits of switch stacking and chassis aggregation

Routing Technologies

This module covers the basics of routing technology and also includes concepts about routing and the routing table. This module provides information on the types of routing like static and dynamic, routing protocols both interior and exterior, and some others like OSPFv2 for Ipv4. Some of

the topics included in this topic are:

● Describe the basic routing concepts

● Describe the boot process of Cisco IOS routers

● Differentiate methods of routing and routing protocols

● Configure and verify operation status of a device interface, both serial and Ethernet

● Configure and verify utilizing the CLI to set basic router configuration

● Configure and verify routing configuration for a static or default route given specific routing requirements

● Configure and verify OSPF (single area)

● Configure and verify EIGRP (single AS)

● Configure and verify interVLAN routing (Router on a stick)

● Configure SVI interfaces

● Manage Cisco IOS FILES

● Verify router configuration and network connectivity

● Interpret the components of a routing table

● Troubleshoot basic layer3 end to end connectivity issues

WAN Technologies

This module includes a detailed study of the PPP and MLPPP configuration and verification on WAN interfaces. It also talks about the PPPoE client-side interfaces that use local authentication. Options for WAN connectivity and basic QoS concepts are also included. Some of the topics included in this module are:

● Identify different WAN technologies

● Configuration and verification of PPP and MLPPP using local authentication on WAN interfaces

- ·Describe WAN connectivity options
    - MPLS
    - Metro Ethernet
    - Broadband PPPoE
    - Internet VPN
- Configure and verify a basic WAN serial connection
- Implement and troubleshoot PPPoE
- Configure and verify frame relay on Cisco routers
- Configure and Verify PPP connection between Cisco routers
- Describe WAN topology options
- Describe the basic QoS concepts
- Marking
- Device trust
- Prioritization
- Shaping
- Policing
- Congestion Management

Infrastructure Services

Topics in this module include DNS loop operation, client connectivity issue troubleshooting, DHCP configuration, and verification on routers, HSRP basics, etc. Some of the topics included in this module are:

- Description of DNS lookup operation
- Troubleshooting client connectivity issues involving DNS
- Configuration and verification of DHCP on router

- Server
- Relay
- Client
- TFTP, DNS, Gateway options

● Troubleshooting client and router-based DHCP connection issues

● Configuration verification and troubleshooting basic HSRP

- Priority
- Preemption
- Version

● Configuration verification and troubleshooting inside source NAT

- Static
- Pool
- PAT

● Configuration and verification of NTP operating in client or server mode

Infrastructure Security

The topics that are covered in this module include port security, mitigation techniques for common access layer threats, traffic filtering, etc. This module also covers some information on the configuration, verification, and troubleshooting of issues that may arise during device hardening. The topics included in this module are:

● Configuration, verification and troubleshooting port-security

- Static
- Dynamic
- Sticky
- Max MAC addresses

- Violation actions
- Err-disable recovery

● Description of common access layer threat mitigation techniques

- 802.1x
- DHCP snooping
- Non-Default native VLAN

● Configuration, verification, and troubleshooting of Ipv4 and Ipv6 access list for filtering traffic

- Standard
- Extended
- Named

● Verification of ACLS using APIC-EM Path Trace Analysis Tool

● Configuration, verification, and troubleshooting of basic device hardening

● Local authentication

● Secure password

● Access to device

- Source address
- Telnet/SSH

● Login banner

● Description of device security using AAA with TACAS+ and RADIUS

Infrastructure Management

This module covers the management of devices that are present in the network system. The module also covers the configuration and verification of the device monitoring protocols. It also provides information on how one can maintain the performance of the device. Some topics covered in this module are:

- ·Configuration and verification of device monitoring protocols
    - SNMPv2
    - SNMPv3
    - Syslog
- Troubleshooting network connectivity issues using ICMP echo-based IP SLA
- Configuration and verification of initial device configuration
- Performing device maintenance
    - Cisco IOS upgrades and recovery (SCP, FTP, TFTP, and MD5 verify)
    - Password recovery and configuration register
    - File system management
- · Using Cisco tools for troubleshooting and resolving problems
    - Ping and traceroute with extended option
    - Terminal monitor
    - Log events
    - Local SPAN
- Describing network programmability in enterprise network architecture
    - The function of a controller
    - Separation of control plane and data plane
    - Northbound and southbound APIs

Operation of IP Data Networks

Some of the topics included in this module are:

- (SDN) Awareness of programmable network architectures.
- Recognize the purpose and function of various network devices such as

Router, Switches Bridges and Hubs.

● Expanded VPN topics, DMVPN, site-to-site VPN, client VPN technologies.

● Increased focus on IPv6 routing protocols, configuration, and knowledge

● Knowledge of QoS concepts.

● Select the component required to meet a given network specification.

● Understanding of cloud resources deployed in enterprise network architecture.

● Describe the purpose of the networks

● Identify common applications and their impact on the network.

● Predict the data flow between two hosts across a network

● Identify appropriate media, ports, cables, and connection to connect the Cisco network device to another network device and host in a LAN

Chapter 5

The Process and Exams

A Cisco certification can take a professional in the networking industry a long way. There are numerous benefits that these certifications offer to both the company and the individual. If you want to improve your resume or are looking for a way to boost your career in the industry, you should complete at least one certification offered by Cisco. A novice or an expert can complete these certifications to improve their standing in the industry. There are different types of examinations provided by Cisco, and we will discuss them in detail in this chapter. It is always essential that you understand in what order you should complete those examinations.

1. The CCENT examination is the entry-level examination offered by Cisco.
2. The CCNA examination is the associate level certification.
3. The CCIP examination is the professional-level certification
4. CCIE is the expert level certification.

Every CCNA examination that you appear for will boost your IT career. This section will shed some light on the different examinations that you can appear for, and also help you understand how you can prepare for the examination.

Different Types of Examinations

There are different types of certifications that CCNA offers within the routing and switching domain, and you will need to pass the associate level examination before you appear for the CCIP or CCIE certifications. The exams listed below form the foundation of networking and security. We will look at the different examinations that you will need to appear for to obtain these certifications.

CCNA Cloud

Every organization is welcoming new changes in technology, and they have accepted the cloud services with open arms. These services allow them to work progressively. They can share their data across the Cloud with different teams sitting in different parts of the globe. At present, most organizations are using the SaaS model. As of 2018, over 78% of all the work was being handled on the Cloud. The CCNA Cloud certification is training programs that will help cloud administrators, cloud engineers, and network engineers develop their cloud skill set. It will also enable them to meet the changes in business and technology. With this certification, you will not only learn the basics of how to support and facilitate cloud solutions but will also learn how to troubleshoot any issues. You can learn all this from the only organization that provides the complete Cloud and Intercloud story. To obtain this certification, you must clear the following examinations:

210-451 CLDFND

This examination will test your understanding of Cloud Networks. You will be tested for your understanding of DC essentials, basics of UF, UC, Storage, Network Services and Virtualization, Windows Server, Hypervisors, Linux OS, remote connectivity/VPN solutions, and documentation of design, the framework fabrications, setups, and support strategies.

210-455 CLDADM

This examination will test your knowledge regarding the basics of the Cisco Cloud organization along with Cloud provisioning, remediation, monitoring, reporting, the charge-back formats, and the management.

- Perform Cloud management, checking and remediation

- The portrayal of detail reporting and charge-back

- Understanding the basics of Cloud framework administration

- Distinguishing the different features of the Cisco Cloud management software solution

- Providing Cloud-based on pre-designed templates

CCNA Collaboration

The CCNA Collaboration examination is designed for IP network engineers,

network engineers, IP telephony engineers, and collaboration engineers. The course material is intended for those professionals who want to learn and improve their skills of video engineering and collaboration on voice, data, and other versatile applications. This is also a job-oriented training that will help to improve your knowledge and also increase your value as a professional. It will provide you with the right attitude and skills to enable companies to perform better. To obtain this certification, you should complete the following examinations.

210-060 CICD

In this examination, you will learn more about Cisco Unified Communications. You will be tested on your knowledge of final-user and management interfaces, features of telephony and mobility along with the maintenance of UC solutions.

210-065 CIVND

In this examination, you will be tested for your skills and knowledge essential to implement different Cisco Video endpoints present in the United Cisco video frameworks. The examination will also check your aptitude to execute and resolve Cisco Unified Communication and Collaboration, Digital Media Player, and Telepresence in various Cisco business solution models.

CCNA Cyber Ops

Most organizations are now challenged with identifying or detecting breaches in security quickly. They also need to know how to react and remove these threats. They must have the right framework in place to achieve this. All the employees working in Security Operations Centers (SOC's) in the organization must monitor the security frameworks and protect the organizations by swiftly spotting and responding to any cybersecurity threats or potential breaches. This certification will help you understand how you can do this and also help you establish yourself in this field. Since July 2018, the United States Department of Defense (DoD) has affirmed the Cisco CCNA Cyber Ops Certification for the DoD 8570.01-M for the CSSP Analyst and CCSP Incident Responder groups. To obtain this certification, you must clear the following examinations:

210-250 SECFND

This test is one of the two prerequisite exams that are required for attaining the CCNA Cyber Ops certification and is necessary to secure the job of an entry-level Security Operations Center (SOC) Security Analyst. The SECFND exam tests your understanding of cyber security's primary principles and the fundamental skills essential to understanding the more progressive associate-level course materials required for the second prerequisite exam, 'Implementing Cisco Cyber Security Operations (SECOPS).'

210-255 SECOPS

This is the second exam that is essential for achieving the associate-level CCNA Cyber Ops certification, and it will prepare you for the role of an associate-level Security Operations Center (SOC) Security Analyst. This exam tests the knowledge and aptitude required for efficiently handling the different duties and obligations of an associate-level Security Analyst working in a Security Operations Center (SOC).

CCNA Data Center

Every data center is competent if it is maintained well by the employees in the company. The data center is the primary focus of every organization in today's digitized world since it is designed for quick execution of applications and reinforced by an exceptionally versatile framework. This certification will give you the required knowledge for installing, configuring, and maintaining the technology of a data center. You will also gain some footing in the concepts of infrastructure, data center, data center technologies, storage networking and unified computing, network virtualization, data center automation and orchestration, and Cisco Application Centric Infrastructure (ACI). To obtain this certification, you must complete the following examinations:

200-150 DCICN

In this exam, you will learn more about the physical infrastructure, networking, and storage networking concepts of the data center.

200-155 DCICT

This exam will test your fundamental knowledge about the physical infrastructure, networking concepts, automation, and storage networking

concepts related to a data center.

CCNA Industrial

The Cisco Certified Network Associate Industrial (CCNA Industrial) certification is designed for plant administrators, traditional network engineers, and control system engineers dealing with process control, assembling, and oil/gas ventures, who will be working along with industrial and IT networks. When you clear this certification, you will learn the different skills that are necessary for you to know to design, implement, and troubleshoot any issues that arise within a network. It will also provide information on how you can do this while using the best practices necessary for the connected networks present today.

This module consolidates both theoretical and practical knowledge through some practical lab work and exercises. This module will help you develop the skills necessary for working in the IT industry and also enhance your knowledge about the current infrastructures that different organizations incorporate in their functions. It will also provide information about the infrastructure that will support the future results of the business.

The prerequisites for this certification are Industrial Networking Specialist or CCENT or CCNA Routing and Switching or any other CCIE certification.

200 -601 IMINS2

This examination will test your understanding and knowledge about the concepts and techniques that you can find in an automated manufacturing environment. This exam will cover the Common Industrial Protocol (CIP) and ProfiNET industrial conventions. It will also test you on the fundamental design of the support network infrastructure to optimize the effectiveness of the Industrial Ethernet.

CCNA Security

The CCNA Security certification will help individuals garner the skills and knowledge that they will need to work as associate level representatives in the IT department of any organization. If you have this certification, you will be hired as a network professional since you will have the abilities required to develop a security infrastructure, perceive dangers and vulnerabilities to

networks, and alleviate any security breaches. The CCNA Security educational program emphasizes primary security technologies. It also provides information about the establishment, investigation, and vigilance of network instruments for maintaining the virtues, discretion, and the accessibility of information and instruments, as well as their competency of all the innovations that use Cisco security structure.

210-260 IINS

The CCNA Security examination will test your knowledge about the different aspects of security including security network infrastructure, your understanding of the fundamental concepts of security, verification of secure access, VPN encryption, firewalls, prevention of any breach and the endpoint security while using SIEM technology, Cloud and Virtual Network topology, BYOD, Identity Service Engine (ISE), 801.1 x Authentication and a other cyber-security related concepts.

This examination will help you validate your skills of designing, installing, monitoring, and troubleshooting any secure network which will help the service provider secure the data and also allow the data to be accessible to the devices connected to the network.

CCNA Service Provider

The CCNA SP or the Cisco Certified Network, Associate Service Provider certification, is specifically designed for specialists, network engineers, and planners. The objective of this certification is to help these specialists learn more about the recent developments and trends in technology within the Service Provider industry. You must obtain the following certifications to obtain this certification.

640-875 SPNGN1

This examination will test your basic knowledge and the basic skills needed to support the network of any service provider. To learn more about the exam, please refer to the following link: https://www.cisco.com/c/en/us/training-events/training-certifications/exams/current-list/spngn1.html

640-878 SPNGN2

This exam will test your aptitude and knowledge that is important for you to

know if you are going to execute, maintain, and support the network of any service provider. An applicant must get ready for this examination by taking up the Building Cisco Service Provider Next-Generation Networks, Part 2 (SPNGN2) course.

CCNA Wireless

Cisco has a wireless innovation department that has been placing a lot of demands on the network. These demands, in turn, affect the individuals working on networks. Every organization will require a set of professionals who can work on the network and ensure that the network has been configured properly. These individuals must also monitor the network and troubleshoot if necessary. You can improve your skills and enhance your knowledge of these networks when you prepare for the CCNA wireless certification.

Some prerequisites to apply for this certification are CCNA Routing and Switching certification, Cisco CCENT, and the CCIE certification. To obtain the CCNA Wireless certification, you must obtain the following certification.

200-355 WIFUND

This examination will test your knowledge about how to install, configure, and troubleshoot a small-sized network or a Wide Area Network.

The next few chapters will shed some light on the CCNA Routing and Switching examination.

Exam Preparation

Cisco is at the top when compared to different IT vendors. Cisco provides you with the required tools and material that will make it easy for you to earn your certification in the first attempt. Cisco constantly tries to improve the material that it creates for this certification to ensure that it provides readers with the latest information. From the Cisco Learning network to self-study materials as well as some exam dumps, you have different materials that you can use to clear your exam. This section lists some of the tools that you can use to prepare for the exam. These tools will help you strengthen your understanding of the numerous concepts you will be learning.

Self-Study Materials

The Cisco Learning Network provides numerous self-study material that you can use to obtain your certification. You should always enroll for the different courses available on the learning network like the Interconnecting Cisco Network Devices (parts one and two). You should also look at the labs that are conducted for these courses. The subjects and topics covered in these courses will help you learn all the concepts that you will need to cover in the composite examination. Numerous practice exams are available on the learning network that will help you gauge your knowledge. More information about these courses has been provided later in the book.

Training Videos and Webinars

You can always go through the different learning and training sessions that are provided on the Cisco learning web. These sessions will help you learn more in very little time. There are numerous resources available on the learning network that are covered in detail in this book.

Study Groups

It is always a good idea to join a study group when you decide to appear for the examination since you can ensure that you prepare well for the examination. You can always build your network. This group will also act as a support group since you will be studying with them to cover the different concepts in the syllabus.

Exam Dumps

An exam dump is as important, if not more important, as the study group you want to join or the study material that you want to read. These dumps will always contain all the questions that you can be asked in any certification examination, and it is for this reason that you should always go through the dump when you prepare for the exam. When you have understood the different topics covered in the syllabus, you can practice all the questions in the exam dump to strengthen your understanding. These dumps will also help you familiarize yourself with different questions.

Recertification

The CCNA Routing and Switching Certification have a validity period of three years. That being said, you can always extend the validity by earning a certification that is at a professional or expert level. For instance, you can

earn a CCIE certification that is valid for two years. You can easily extend the validity period of the routing and switching certification by obtaining the CCIE certification. You will learn more about how you can recertify yourself later in the book.

In simple words, it is important to remember that you can achieve a lot by earning any CCNA certification. Regardless of what experience you have, you can excel in your profession if you choose to earn different certifications that Cisco provides. You will always find a good job with a good salary if you obtain these certifications.

Chapter 6

Cisco Recertification

There are numerous benefits to obtaining a Cisco certification, and I am sure you are aware of how these certifications will benefit your career. There is, however, a drawback when it comes to these certifications – there is a validity period. These certifications are very different from other certifications in the sense that they expire. This is because the technology being used constantly changes and evolves. You cannot believe that technology will remain constant when innovations are happening every single day. There is always some new concept added to the syllabus every year by the Cisco team, and regardless of how painful it is, you must spend some time and update yourself with the changes that are taking place to the syllabus. If you think about this carefully, you will realize that this does make sense. Cisco constantly introduces new modules or adds information to the existing modules every year. It is for this reason that every Cisco certification expires in three years or less. To ensure that you are still certified in a specific module, you must recertify yourself in those modules. Let us take a look at the validity of each examination:

1. All CCIE certifications and Specialist certifications expire after two years.
2. The Entry, Associate, and Professional-level certifications expire in three years.
3. The Cisco Certified Architect has an expiry date of 5 years from the certification.

There are some charges applied to the recertification of a module, and you will need to bear those costs. You can also obtain recertification using other methods, and this chapter will provide further information about the same.

Certification Policy of Cisco

It isn't that good an idea to add expired certifications to your resume, but you can certainly mention them as an achievement. Since there are new

developments in the technological industry, Cisco ensures that it includes these changes into the course material for any certification that it provides. It is for this reason that they have set validity on their certifications. Cisco will make some changes to the syllabus over time, and when you recertify yourself, you can ensure that you update your knowledge and skills.

Entry-Level Certifications

If you want to renew an entry-level certificate, you'll either need to take the same exam once more or opt for a higher-level certification. For instance, if you've got a CCNA Routing and Switching Certification whose validity period is nearing expiration, you have the option to either sit for the CCNA Security examination or any other CCNA level certification exam. If you are not too keen on giving an associate-level examination, you can choose to give any other professional level examination. You can choose to clear any one of the CNNP-level exams, and a certification in any of these examinations can help you recertify your basic CCNA certifications. Alternatively, you can also choose to clear the CCIE examinations. There are no prerequisites to clearing the CCIE examinations, and it is for this reason that they are easy to do. A certification in this examination will automatically help you renew your certification.

To sum it all up, the following options are available if you want to rectify or renew your CCNA certifications:

1. Clear any of the present Associate-level exams except the ICNID exam
2. Clear any of the present 642-xxxx professional-level or any of the 300-xxxx professional-level exams
3. Clear any one of the existing 642-xxxx Cisco Specialist exams (this doesn't include Sales Specialist or Meeting Place Specialist, Implementing Cisco TelePresence Installations, Cisco Leading Virtual Classroom Instruction exams or any of the other 650-online exams)
4. Clear any of the existing CCIE written exams
5. Clear any of the existing CCDE written or practical exams

6. Clear the Cisco Certified Architect interview along with the Cisco Certified Architect board review for the renewal of your lower certifications
7. You merely have to choose one of the options, as mentioned earlier.

Professional-Level Certifications

As with entry-level certifications, even for professional-level certifications, you have got two choices - either take the same exam once more or choose a certification that is at a higher level. In this case, if you have a CCNP Routing and Switching certification whose validity period is expiring within a year, you can appear for the certification exam again or opt for a high-level examination. You can also choose to clear any other certification examination if you wish to renew the current certification that you have.

You should pass any of these options below if you want to recertify your Professional level Cisco certifications:

1. Clear any of the existing CCDE written or practical exams
2. Clear any of the existing CCIE written exams
3. Clear any of the existing 642-xxxx professional-level or any of the 300-xxxx professional-level exams
4. Clear the Cisco Certified Architect interview along with the Cisco Certified Architect board review for the renewal of your lower certifications

Expert-Level Certifications

Every Cisco certification has a validity period, including the expert level certifications. As mentioned earlier in this chapter, there is a constant change in technology, and since these certifications are all related to technology, they need to be updated too. You must reappear for the CCIE certification examination if you want to recertify your expert-level Cisco certifications.

To renew your expert-level certifications, you must clear any of the following exams.

1. Clear any of the existing CCDE written or practical exams
2. Clear any of the existing CCIE has written or lab exams
3. Clear the Cisco Certified Architect board review and the Cisco Certified Architect interview for the renewal of your lower certifications

This is all the information you need to learn about the recertification process that you will need to follow. You must recertify all your certifications before the validity of those certifications expires. You must also ensure that the time left on certification is not added to your certification upon clearing a higher-level exam. You can track the status of your certification on Cisco's website.

Chapter 7

About CCNA Routing and Switching

The CCNA Routing and Switching certification is a prominent certification that many networking professionals appear for. Since there is a constant advance in technology, a network engineer is expected to have the necessary skills to work on developing programmable network architectures. They can only develop this skillset if they have the capabilities and the knowledge that the CCNA Routing and Switching certification provides. Since most businesses now use a CLI-based interaction with their routing and switching framework, the networking professional needs to have a basic understanding of the interactions that take place within that framework. It is for this reason that Cisco developed the Routing and Switching certification, and the course material is constantly being updated to cater to the changing needs. The study material enables a networking professional to focus on and understand these changes. The course material of the routing and switching certification has been refreshed and updated to include the changes in technology:

1. Increased spotlight on IPv6 routing protocols, configuration, and knowledge
2. Awareness of programmable network (SDN) architectures and the partition of control plane and information plane
3. Understanding of cloud assets conveyed in enterprise network architectures
4. Knowledge of QoS concepts, including checking, forming and policing mechanisms to manage congestion of various types of traffic
5. Expanded VPN subjects to incorporate DMVPN, site-to-site VPN and customer VPN technologies

When you obtain the CCNA Routing and Switching certification, you can show your employers that you have the required skills to develop, design, implement, develop, and configure a network. They will also have the

confidence that you can troubleshoot any issues if they crop up. Having said that, you must ensure that you stay abreast of any developments or changes being made in the industry. This will give you an edge over your competitors. As read earlier, you will need to recertify yourself to ensure that your certification is valid. The previous chapter sheds some light on cisco recertification.

Before getting certified for CCNA Routing and Switching, it is important to pass the entry-level examination (CCENT). You can then choose to either take the one exam-path or the two exam-path to obtain the certification.

Cisco Certified Network Associate - Routing and Switching (CCNA Routing and Switching)

The CCNA Routing and Switching certification are one of the most sought-after certifications in the networking industry. If you want to obtain the certification, you can either appear for one exam or two exams. The former is the composite exam, while the latter is the ICND1 and ICND2 examination. You can appear for these examinations once you clear your CCENT examination. The cost of this examination is $150. The questions asked in the CCENT examination are often tricky, which makes this exam a little difficult to crack. It is for this reason that you should only purchase the material offered by Cisco. Like every other CCNA certification, the CCENT certification also covers different concepts. Therefore, you will need to read through the entire material and also test your level of understanding. If you do wish to study by yourself, you can do that, but experts suggest that you sign up for some online tutorial classes since these will help you understand the concepts better. Once you obtain this certification, you can obtain the CCNP (Cisco Certified Networking Professional) certification.

It is always a good idea to study for the CCNA Routing and Switching examination, and you can land a great job in the networking field. If you do not want to appear for two examinations, ICND1 and ICND2, you can sign up for the composite examination. You must remember that the syllabus covered in all three examinations is extensive. This will mean that you need to spend enough time preparing for the examination. You will learn later about the different reasons why you should appear for the CCNA Routing and Switching examination. We will also look at some tips you should keep in mind when you prepare for the examination.

Required Skills

You will be tested on the following in the IDND1 examination:

1. Knowledge and skills to test a small network
2. Installation of a network
3. How does the network function?
4. How to troubleshoot any issues?
5. LAN Switching technologies
6. IP routing technologies
7. IP services network device security
8. Network device security
9. Troubleshooting
10. IPv6 protocol

You will be tested on the following in the ICND2 examination:

1. How to design, develop, configure, work with and troubleshoot large networks
2. IP Routing technologies
3. LAN Switching technologies for large networks
4. WAN technologies
5. IP Services like Syslog, FHRP, and SNMP v2 and v3

Exams to Take

If you want to obtain the CCNA Routing and Switching Certification, you must take the Composite examination. This is a combined examination that is slightly difficult to clear. This is because the syllabus covered in this examination is vast, and it is impossible to understand every concept and remember them so you can answer the required number of questions to pass the examination. The different topics that are covered in the CCNA

Composite examination have been taken from the ICND1 and ICND2 examinations.

If you do not wish to appear for the composite examination, you can appear for the ICND1 and ICND2 examinations. You must always think carefully and plan your study route before you sign up for the examination. You can choose to give one examination instead of two, and there is a high probability of clearing the examination if you study for the required time. Remember that you must practice and work hard. You will need to clear the following papers if you choose to take up two examinations instead of one:

- Exam: Interconnecting Cisco Networking Devices Part 1 (ICND1)

- Exam: Interconnecting Cisco Networking Devices Part 2 (ICND2)

History about the Routing and Switching Certification

Cisco announced that it would begin the CCNA and CCNP certifications in the year 1998. At that time, the company only offered the routing and switching examination, so there was no separate routing and switching certification. The examination was simply called CCNA. It was also easier to appear for this examination since there were only two types of examinations, and one could obtain the CCNA certification by passing only one examination, which was CCNA. There was no CCENT examination at that time. The examination rules and requirements remained the same for the first three examination numbers.

Impressions About Old Exams and Books

As mentioned earlier, there were three examinations that one would need to clear to obtain the CCNA certification. If you counted the number of pages in each of the study material for these examinations, without counting the study tools and the overhead, the number of pages in the guidebook shared by Cisco Press were:

1. Examination 600-407: 500 pages
2. Examination 600-507: 650 pages
3. Examination 600-607: 750 pages

When you compare these texts to the new edition of the books for the CCNA

Routing and Switching certification examination, the latter has over 1600 pages. You will also notice that Cisco worked on revising the syllabus and the examination in the first few years. Some records suggest that there was a mere 16-month gap between the second and third editions of the CCNA examination. This is a very quick revision since Cisco now takes longer to revise either the CCNA or CCNP examinations. This does not come as a surprise since, in the past, they were working towards developing the latest syllabus.

Impressions About the Topics in the Past

If you look at the age of technology in the same way as the age of dogs, you can say that the CCNA certification is close to 130 years old. Continuing with that same line of thought, let us look at the technology that was included in the first three versions of the CCNA examination. For example, books:

1. All include information about the ISDN configuration
2. All include some information about Frame Relay since this concept was popular in the 1990s. Frame Relay is a topic that was removed in 2016 since it is no longer a popular method used
3. All include some information about VLAN trunking
4. All include information about the different protocols in the NetWare protocol suite, the Netware SAP filtering, and NetWare IPX Layer 3 protocol
5. None of these include information about the router-on-a-stick method or the 3-layer switching

The Fourth CCNA (2003): The Addition of the Two-Exam Path to CCNA

One of the biggest changes made to the CCNA Examination happened in the year 2003. The examination was still called CCNA, but the following changes were made to the curriculum:

1. Cisco broke the CCNA examination into two parts – the ICND (640-821) and INTRO (620-811)
2. The two parts combined to cover the same topics mentioned in the CCNA examination. This means that CCNA = INTRO +

ICND.

3. Cisco also offered a single examination for the students called CCNA (640-801). Students could choose to write this examination instead of the two parts.

Cisco offers some professional training courses, taught by the Cisco Learning Partners. The course offered was split into two courses as a pair of introductory courses to routing and switching called ICND and INTRO. The list of topics that they wanted to cover increased over the last few years, so the team had to accommodate these topics in two courses.

The CCENT examination was still not prepared by the Cisco team at this point. The CCENT examination only came into existence in the fifth iteration. The course material included numerous topics that are still in the scope of the examinations conducted today. Let us look at some of the notable changes:

1. Removed the Novell NetWare IP Layer 3 protocol
2. Added information about VLAN
3. Added EIGRP and OSPF
4. Added VLSM and NAT
5. Added RSTP

The Fifth CCNA (2007): The Addition of CCENT

The next iteration of the CCNA examination maintained the same structure as the fourth iteration that we covered in the previous section. The CCNA examination still had a one exam-path and two exams-path approaches. Cisco also kept the idea that the content in the two parts will be the same as the content in the single CCNA examination. Some changes were made to the examinations in the year 2007:

1. The text names of the examinations in the two exam-path were changed to ICND1 and ICND2
2. Cisco also included the CCNET or Cisco Certified Entry

Network Technician examination to the syllabus

The change made to the course and the examination names did not impact the students who were taking the examination. The decision to add CCENT to the syllabus was a huge change. This examination will allow people to gather information on some parts of the CCNA examination and stop. When Cisco introduced CCENT to the course structure, it also came up with numerous prerequisites:

1. CCNA Routing and Switching Certification as a prerequisite
2. CCENT as a prerequisite
3. No exam is a prerequisite

The CCENT examination is also not simple since there are a lot of topics that the student will need to cover. The changes made to the syllabus were not topic changes but were changes made to the quality of information shared and the skills that the student developed. For example, this version of the examination included information about wireless LANs. Cisco then introduced the CCNA wireless examination and removed the topic of wireless LANs from the Routing and Switching certification. In this edition of the examination, there were many questions asked about wireless LANs. Some of the new topics included were:

1. Increased performance level to learn more about troubleshooting for some topics
2. Some topics on Wireless LANs
3. Introduction to the IPv6 protocol
4. Introduction to Internet access and VPNs
5. No information about the ISDN configuration

The Sixth CCNA (2013): a 5.5 Year Transition

The next change that was made to the routing and switching examination was when the sixth edition of the examination was released. This change was very interesting for the following reasons:

1. There was a 5.5-year gap between the previous edition and the current edition. The fifth edition was released in 2007 while the sixth edition was released in the fall of 2013
2. During the 5.5-year gap, Cisco also launched the CCNA and CCNP Wireless, Voice, and Security certifications. It also released a few other examinations and made changes to a few others. If you remember, in the year 2007, the only Cisco certification was the CCNA Routing and Switching track. Cisco spent some time and effort to improve the topics covered in the examination and also broaden the different options people could choose from

When there is a revision in the CCNA examination, the official certification guides are also revised. There was only one time, which was in the year 2013, that Cisco updated the study material but did not make any changes to the examination yet. The learning team wanted to include more tools into the market, and they wanted students to learn more about these tools, although they were not included in the examination. Apart from this exception, Cisco always ensures that the new certification guides for the CCNA routing and switching examination and CCENT examination were released when the exams were revised.

Another interesting change that was made to the examination was that Cisco decided to refer to the exams using a version number. Cisco had never represented the examinations it conducted using a reference or version number of any kind. The exam number was sufficient to help people understand the subject they cover. Cisco began to refer to some web pages and material as version 2.0 when the examinations were announced in the year 2013. In the year 2016, these examinations are referenced as version 3.0 across all web pages. If you are unsure of what the examination is about, you should only look at the examination number.

As for the content in the examination, the learning team decided to include troubleshooting as the main theme for these changes. These examinations required the students to develop some skills to troubleshoot any network that they have developed or configured. The mix of topics does always change over time, but the 2013 version had more emphasis on troubleshooting,

especially in the ICND2 examination. Some of the changes to the content include:

1. Added IOS licensing
2. Added FHRPs or First Hop Redundancy Protocols like HSRP
3. Added more IPv6 protocols including EIGRP, static routes and OSPF
4. Removed RIP

The Seventh CCNA (2016): The New CCNA R&S (Exam Version v3.0)

This is the latest change made to the CCNA routing and switching examination, and these changes represent the seventh version of the examination and the seventh number of the routing and switching examination. From the program perspective, you can note the following:

1. There was still a one exam-path and two exam-path to clear the CCNA examination
2. Every student is required to pass the CCENT examination to appear for the ICND1 100-105 examination
3. The new examination is called Version 3.0 on most web pages, but make sure to check the examination numbers if you are ever in doubt

    a. ICND1 100-105

    b. ICND2 200-105

    c. CCNA Routing and Switching 200-125

This version of the examination is the complete transition that Cisco has made wherein the course material focuses on whether a student can implement what they have learned and troubleshoot what they have configured. The topics included in the examination have also increased. From a larger perspective:

1. For most topics included in the examination, the student is

required to know how to troubleshoot any issues

2. New subject areas have been included in the examinations when compared to the earlier versions of the examination

Now that we are aware of how the examination changed over the years, let us look at the different products offered by Cisco and also look at some other information about the CCNA routing and switching examination.

Where to Register for the Examination

You are required to register for the exam on Pearson VUE regardless of whether you choose to take the ICND1 and ICND2 examinations or the composite examination. If you want to gather some more information about these examinations, please visit the website using the following link: www.vue.com.

Follow the steps given below if you have decided to clear the examination:

1. The first thing you must do is choose the exam that you want to appear for. If you want to take up the composite examination, you should choose the code 200-125. If you want to sign up for the ICND1 and ICND2 examinations, you should choose the codes 100-105 and 200-105.

2. After you have selected the examination that you want to appear form, you will need to visit the nearest examination center and register for that exam. Remember that you will need to pay for the exam in advance, and you can sit for the exam within a year since you have made the payment.

3. You can sit for the exam when you decide to give the exam or give yourself a six-week deadline before you sit for the exam. That being said, if you cannot appear for the exam on the day you have decided to sit for it, you must wait for five days before you sign up for the exam. If you know that you will be unable to sit for the exam, you should send Pearson VUE an email at least twenty-four hours before the examination. They will help you reschedule the examination at no cost.

4. Once you schedule the examination, Pearson VUE will send all the instructions to you via email, and will also provide some information about what you will need to do at the examination center. You will also be given information about the different items you will need to carry to the center.

5. You must always carry an original copy of the document or identification proof.

Always Use the Material Provided by Cisco Authorized Publishers

You must always purchase the course material from a well-known publisher. The best option would be to purchase this material from a publisher who has been authorized by Cisco. When you do this, you do not have to worry about having to look for new study material since the material that you will be purchasing will cover all the information that you will need to know for the examination. It is also a good idea to sign up for a course that is led by an instructor. This is because the trainer will guide you on how you should prepare for the examination. The trainer will also shed some light on the different material that you can study from, and also provide you with some links that you can use.

Differences between CCNA and CCNP

Both the CCNP and CCNA certifications are considered to be the most sought-after certifications in the IT industry. There are some differences between the two certifications based on the level or the experience of the individual.

CCNP and CCNA stand for Cisco Certified Network Professional and Cisco Certified Network Associate, respectively. An individual working in the IT industry is aware of these certifications since every organization values an employee with these certifications. Regardless of which certification you choose to appear for, you will need to appear for a written examination that you must clear. There is also a lab examination conducted which will test your skills. The individual's expertise is only assessed after five rounds of tests. Each round will define the individual's expertise.

The CCNA examination also ensures that you will have a good understanding

of buttoned and medium-range router systems, and can work with them easily. If you have this certification, and the necessary skills, your employer will know that you can install and activate the different systems in the network. In the same way, the CCNP certification will let employers know that you can work with and maintain area networks, like LAN and WAN, and can work with advanced solutions like voice, security, and wireless.

CCNA and CCNP Certification Training by Specialist

There are some prestigious positions that an individual can take up in the IT industry, and they are the network engineers or system engineers. An individual with either the CCNA or CCNP certification is eligible for these roles. The CCNA examination also teaches you about security threats, wireless ideas, and how systems can connect to the WAN or wide area network. You will also need to learn more about different protocols like SLIPFR, EIGRP, VLANs, ACLs, RIPv2, and so on. They need to know these protocols well.

You must be a certified CCNA expert before you can appear for the CCNP certification examination. You must also have at least a year's experience in the networking field if you wish to appear for the CCNP examination. You can look at different careers in the IT industry if you have a CCNA certification. Still, with a CCNP certification, you can improve your chances of being promoted or obtaining the best job in the industry. This is because there are very few individuals who are CCNP certified, and because of this, the demand for CCNP certified individuals is increasing.

You must remember that the Cisco products and systems are complex to deal with. Most organizations hire a team of individuals only to take care of these systems and products. Numerous organizations will be willing to hire you if you have a CCNP certification since you will have a good understanding of the products and systems. A CCNP certification will give you an edge over other individuals since you know how to install, organize, function, and even troubleshoot a complex Cisco network. It is for this reason that this certification is essential to obtain. The CCNP examination is only a two-hour examination, but it opens a wide range of prospects for you. This is the main difference between the CCNP and CCNA certification. Before you appear for the CCNP certification, you must ensure that you have a CCNA certification.

Strategic Tips

You will be awarded the CCNA Routing and Switching certification if you show some skill at implementing, designing, configuration, and troubleshooting different networks that you create based on the TCP/IP model. You must ensure that you always test your technical skills before you sit for the examination. A CCNA Routing and switching examination will improve your standing in any organization, and you may get a better role when compared to the one you are in now. This section lists some strategic tips you can use to clear the examination in your first attempt. You can stop worrying about any exam dumps.

1. Always spend some going over the flow of the syllabus before you start the examination. This flow, called the blueprint, can be found on the Cisco website: https://learningcontent.cisco.com/cln_storage/text/cln/marketing/e topics/200-125-ccna-v3.pdf

2. Never use only one source to obtain the material for the examination. Always try to use a combination of online training, videos, labs, and books.

3. It is important to remember to be honest with yourself when you talk about your understanding of the subjects. Always ensure that you know and understand a concept fully before you begin a practical assignment.

4. If you want to master troubleshooting concepts, you must learn some commands, and try to memorize them. To make it easier, you should note these commands down on a page in your book.

5. Never stick to only one workbook. You should try to look at different scenarios. As mentioned earlier, you should focus on learning more about network topologies.

6. As mentioned earlier, you must always focus on reviewing your concepts. This is because people only retain ten percent of the information that they read.

7. You should memorize the TCP/UDP services and port numbers. This will not only help you during the CCNA examination but will also help you during your job.

8. You should always try to look for new questions and complex questions on the Internet. Try to look at different forums and communities to collect these questions.

9. Always try to take the two-way examination. The single 200-125 CCNA examination will cost $295 while taking the 100-105 ICND1, and 200-105 ICND2 examinations will cost an additional $5 - so the total cost will come to $300.

10. You should take at least two practice examinations under examination conditions, and you should focus on the questions that you are uncertain about.

We will look at a few more tips to help you clear the examination later in the book.

Chapter 8

Why Should You Get A CCNA Routing and Switching Certification?

From what you have read earlier, you know that any Cisco certification will boost your career in the IT industry. You also know that you can apply for different roles in the same company or a different company. The examinations will help you create a sound foundation of technical knowledge. You will also develop the necessary skills to help you move ahead in this world. You will see that these examinations will bring in quantifiable results in the form of better pay and better increments. Let us now focus on the CCNA Routing and Switching Certification. There are multiple benefits of getting a CCNA Routing and Switching Certification. Since technology is constantly changing, the roles and responsibilities of a network engineer and administrator are also changing.

One of the best ways to prepare yourself for these changes is to appear for the CCNA Routing and Switching certification. Let us look at some of the reasons why you should obtain this certification.

A Certificate from the Networking Leader

If you remember from the first chapter, Cisco was one of the first companies to have established itself in the networking industry. In the previous chapter, we read that this company introduced the routing and switching certification. Cisco is one of the leading companies in the networking industry. Most companies use products and services developed by Cisco to develop and build network pathways. If you want to learn more about how to work on Cisco products, you should obtain this certification along with some other certifications offered by Cisco.

The Certification Is Globally Accepted

One of the best things about any CCNA certification is that it is recognized globally and is accepted in different countries in the world. So, the validity of a CCNA certification doesn't have any geographical constraints. Anybody working in the networking industry. If you have this certification, you are in a

position to negotiate higher pay and also obtain a better position in the organization. Currently, the number of CCNA jobs open on the market is steadily increasing, and they all require that the potential candidates have some CCNA certification as one of their criteria for job eligibility. All the knowledge you gain through the CCNA routing and switching certification will help you learn more about new modules and different methods of networking. The security courses and other information you learn while preparing for this examination will boost your career. Obtaining the first certification might seem rather complicated and also an uphill battle at times. Once you take this step, you can race through the other certifications since you will get the hang of it. After all, beginning well is half done, and this stands true for CCNA certification.

Your Networking Career Is Built on This Certification

Many networking employees and engineers are doing their best to obtain CCNA certifications ever since Cisco introduced them. There are different programs offered by Cisco. Studies conducted by IDC state that many networking companies look for different Cisco skills when they are hiring employees. Many employees include Cisco certifications along with other information on their resume. Employees must always have an idea of the different networks, infrastructure, and protocols that they need to use regularly. They need to know how they work together. When you obtain the Routing and Switching certification, you can obtain the expertise and knowledge that you will need to succeed in this industry. This knowledge will also help you troubleshoot any issues that occur within the network.

Ever since Cisco began to offer courses and certifications, people from the networking field, including administrators and engineers, have been working hard to complete these certifications. Many organizations also look for these certifications when they hire employees. As indicated by an ongoing report from the IDC (International Data Corporation), Cisco's abilities are among the most wanted for aptitudes while enlisting potential candidates. This need is constantly increasing by the day. The CCNA Routing and Switching examination will improve your knowledge and also validate it. You will be termed an expert in the networking industry. When you take up CCNA certification and successfully clear it, you can place yourself as a network administrator capable of troubleshooting network problems prevalent in networking areas. You will be able to create the infrastructure to back it.

When you hold the CCNA Routing and Switching certification, you will be considered before your other competitors. This certification will boost your career and give you better recognition in the networking field. When you hand your resume over to any company, you will be considered over other applicants who do not have this certification. Since you should recertify yourself in three years, you must recertify yourself. When you recertify yourself, you will learn about the latest developments in the field.

When you obtain the CCNA Routing and Switching certification, your career opportunities will increase. Based on a survey conducted by IDC, it was identified that seven out of ten organizations look for CCNA certifications when they are promoting or hiring an individual. You can move from the associate level to the expert level in the routing and switching certification. You can also improve processes in the company using the skills you develop as routing and switching expert in technologies like Collaboration, Cloud, Network Programmability, Data Center, Security, or Wireless. You can change the direction that your career will take if you have the routing and switching certification.

Certification Improves Your Learning

As mentioned earlier, the CCNA Routing and Switching examination will create a foundation for your networking knowledge. When you appear for these examinations, you can enhance your knowledge about networking. The CCNA examination gives you an efficient way to understand different concepts about networks. Regardless of whether you have years of experience under your belt in the field of networking or not, you will certainly need to keep up with the growing demand for specialized skills to keep up with your competition. There is indeed nothing that can substitute experience, but you need to stay abreast of the changes in technology. This is the only way you can maintain an edge over your competition. Before you choose to appear for all the examinations offered by Cisco, there are a few prerequisites that you need to clear. Only when you do this that you can appear for some of these examinations. The CCNA Routing and Switching certification are like the stepping-stone to move ahead in the Cisco Training courses.

Certification Prepares You for Network Evolution in the Digital Era

Since most businesses are now digitizing their processes, there is a rapid

change in the network tools and infrastructure. Many manual processes have been replaced with the software-driven network architecture that depends on analytics, automation, visualization, cloud service management, and whether the network is open and extensible. A survey conducted by IDC revealed that the role of a network architect and engineer is the most important role in the IT industry. Professionals who want to improve their standing in the industry should embrace this change and work towards improving their profiles.

Certification Keeps You Current on All the Latest Technology Changes

Cisco has brought about major changes to the network architecture that businesses use. Apart from this, Cisco also works on developing an IT landscape that is conducive to different developments in technology. These developments will have a huge impact on your job if you work in the networking industry. Cisco always ensures that it is aware of all the changes that are taking place in technology and the IT industry. The company does this to ensure that every student appearing for these examinations is aware of how the changes in technology will affect their role in the company. The company also wants students to learn how these changes will affect the certification. The CCNA Routing and Switching exam is not an exception to this. Cisco constantly revises the curriculum to ensure that students are aware of every small change made in the industry. The latest curriculum (for further details, please check the previous chapter) includes elements of QoS and also how they can be used, interactions of firewalls, wireless controllers and access points, and network functions. You will also learn more about IPv6 and basic network security. This means that you can keep up with any changes in the technology field by obtaining the CCNA routing and switching certification.

Certification Helps You Stand Out with Your Employer

You are not the only person who gains when you obtain this certification. This certification is also beneficial to organizations in the networking industry. Ask your potential employers, and they will tell you that they will prefer a certified professional any day. Therefore, if you want to stand out, you need to obtain this certification. When you obtain this certification, your employer will know that you have the necessary knowledge and skills to get the job done quickly and efficiently. Your employer will know that you want to excel in your career when you begin to prepare for the CCNA Routing and Switching examination. Managed will notice this kind of an initiative. Based

on a study conducted by IDC, close to eighty-two percent of leaders in digital transformation believe that people who have a certification help to accelerate innovation. Cisco certifications are credible, and many people do their best to obtain this certification. Many employers use the CCNA Routing and Switching Certification as a criterion to hire a candidate. It is always a good idea to have an additional qualification up your sleeve so you can have the edge over your competitors.

Certification Helps Increase Your Paycheck

The salary for a networking professional is very high since there are only a few professionals in this industry. You can most definitely expect an increment in your pay if you have the CCNA Routing and switching examination. As per a report by Robert Half Technology, in the 2018 Technology Salary Guide, CCNA routing and switching certification is one the most sought-after certifications in the industry. This salary guide showed that the salary could increase by ten percent or more if the candidate meets all the criteria. Most organizations also offer their employees a monetary reward for clearing the CCNA routing and switching certification. If you obtain the CCNA certification, that you can look for better career opportunities in the networking industry. The qualifications that you obtain will also lead to an increase in your salary. In every team, and employees given a role based on the different certifications they hold. If you have a CC any certification, you can climb up the corporate ladder pretty quickly. It is always a good idea to obtain this certification close to your appraisal cycle since this will ensure that you receive a higher increment.

Certification Helps You Learn from Your Peers

Professionals and individuals are doing their best to obtain more than one Cisco certification. Since many students appear for this examination, Cisco developed the learning network. This network is a community that enables students from across the globe to communicate with one another. It also aids in career development. There are a million professionals in this community. This community provides valuable support and also helps the members learn, study, and prepare for the certification examinations. If you are a member of the learning network, you can access a wealth of information, including training videos and material. You can also speak to your peers to clear your doubts or any other questions you may have about the industry.

Certification Gives You a Full Range of Training Options

There is no right way of learning when it comes to these certifications. There is numerous authorized learning partners comma, and each of these partners offers a variety of training options that will make it easier for you to understand the concepts covered in the routing and switching certification. You can either choose to enroll in an instructor-led training or a virtual classroom for the examination. You can also sign up for a hands-on lab session for both these examinations to stop the Cisco learning network also offers self-paced, E-learning, learning labs, and are there practice exams that will enable you to strengthen your concepts and prepare well for the certification. Cisco also provides numerous resources that you can use to prepare for the examination. This is school certifications that allow you to prepare for the examinations according to your convenience will stop you can choose to endure enroll yourself in a training program or a self-paced curriculum.

Don't Forget: There Is Value in Recertification

As mentioned earlier, Cisco routing and switching certification are valid only for three years. Having said that, you can recertify your certification at the end of 3 years. Cisco constantly monitors the industry and does its best to ensure that all the information included in the course material will keep the person writing the examination abreast of the changes in the industry. If you want to learn constantly and are happy to recertify yourself, you will learn more about the changes being made in the industry. We have covered recertification in the previous chapter in the book.

Secure Your Career through Routing and Switching

You must remember that digital transformation is changing the face of the world. It this is especially true in the case of every business in this industry since companies have to take advantage of these changes to maintain a competitive edge over other companies in the market. If you notice, every initiative that a company starts is a technology initiative point every ID professional is not only expected to improve different processes within the business but also know all the changes made in technology.

Businesses are doing better now since the development of the Internet of Things (IoT). IoT is constantly evolving. The importance of technology like mobility, big data, security, network design, cloud, application development,

and data center operations, systems, or services integration, as well as enterprise architecture, is increasing. You need to understand how this will affect your career or your growth in the company. Since there are numerous developments taking place every single day, managers want to hire people with certifications and the required knowledge. These certifications will let the company know that you have sufficient experience in the routing and switching industry. A recent study showed that there was a shortage of employees with critical IT skills. Managers who were a part of this study would be only willing to hire candidates or promote those employees who had Cisco certifications. When you obtain the CCNA routing and switching certification, you will gain a competitive edge over other applicants or employees.

Unique Way of Learning

The Cisco learning network is unique since this is not only a learning platform but also a social network platform that is used for learning. You can think of this platform as a better version of the Internet. This network offers students the option to share information across the globe with other professionals and students. You can also avail of a wide area of services like training, simulation labs, corporate internships, job listings, programs for mentorship and recruitment, and various other things.

Personal Gratification

Most networking professionals wonder whether you should appear for the Microsoft or Cisco examinations. The Cisco certification program does not include any broad frameworks, which makes it simpler for the applicant to understand the concepts and complete the modules. These certifications are also not very demanding, which allows you to appear or pursue other certifications that will stop if you are a certified CCNA routing and switching professional, you can move on to Obtaining the professional or expert level certification in this course. Apart from all the other benefits discussed in the chapter, you will also receive another benefit that cannot be quantified; this benefit is personal satisfaction. When you are certified, you will certainly feel a sense of personal satisfaction. If you are a networking professional, you would be quite proud to have the C CNA certification against your name. If you are in the networking field, you are quite lucky since there is a shortage of qualified professionals in the industry. With the ever-increasing innovations and developments in the industry, a greater number of people

must enter the industry. So, it is a good idea to cement your ground as a qualified professional in the networking industry by obtaining a CCNA certification.

The Changing Role of Core Network Engineers

Many businesses and organizations are now looking at adopting programmable network architecture. It is for this reason that most employees will need to develop the necessary skill set to understand, configure, design, and work with these architectures. Most companies are trying to get rid of CLI based interactions in the routing and switching infrastructure. They are now adopting a controller-based interaction that is driven by business and application policies. It is for this reason that Cisco updated its curriculum for the routing and switching certification in the year 2016 to ensure that every IT professional is aware of the changes in the industry. Those people who have not renewed their certification will need to pay attention to the following changes that were made to the syllabus:

1. Understanding of cloud resources deployed in enterprise network architectures
2. Awareness of programmable network (SDN) architectures and the separation of control plane and data plane
3. Increased focus on IPv6 routing protocols, configuration, and knowledge
4. Expanded VPN topics to include DMVPN, site-to-site VPN, and Client VPN technologies
5. Knowledge of QoS concepts, including marking, shaping, and policing mechanisms to manage congestion of various types of traffic

Cisco always ensures that the syllabus is updated regularly to cater to the changes in the networking and technology fields. The material will always need to include some new developments so professionals can stay abreast of the changes made. When you obtain the router and switching certification, you can prove to your current and future employers that you know what networking is and the different solutions you can use in that industry. Many

professionals do not renew their certificate or recertify themselves since they no longer require that certification. This is, however, a bad idea since you may lose out on future opportunities.

Chapter 9

Required Learning Material for Your CCNA Routing and Switching

You must have the right learning material to help you understand the concepts covered in the examination. This is the only way you can ensure that you are confident when you appear for the examination. This learning material should include all the information about the examination, including the various questions that one can be asked during the examination. This material should also include the exam code structure and some sample exam questions that one may be asked. You should keep the following factors in mind before you choose the right study material.

Factors to Consider

Look Out for Free Material

Every student will always look for the best resources when they are preparing for the examination. The same can be said for you when you appear for the CCNA routing and switching examination. You will want to rely on the expensive course material and books available on the Cisco learning network to learn for the examination. There are, however, numerous websites that offer free study material for the examination. Before you rush into making a purchase, you should conduct thorough the search to understand which material has the required information and can be purchased for a lower rate.

Your Peers are Your Greatest Resource

Your peers are not a great resource that you can Roach to learn more about the CC Annie routing and switching certification. You can always approach them and arrange a one on one session, so you are aware of which direction your career is going to take. You can also ask them to recommend some books and borrow their news before the examination. These notes can be very helpful when you prepare for the examination. It is always a good idea to ask someone who has already written the examination any questions and ask them for guidance.

Mix It Up

One of the best ways to learn something and also remember the concepts by committing them to memory is by engaging all your senses. You should always choose different ways of learning so that you are always on your toes, wanting to learn more first up this will make your learning experience fun. You can always choose a mix of video, audio, text, real-time data, and graphics to help you understand the different concepts covered in the examination. This will help you build a holistic approach of learning that will enable you to commit all your concepts the memory. You will be engaged in the subject when you mix things up.

Keep Yourself Updated

You must always be updated with the advancements made in technology in the routing industry. You should always stay abreast of the happenings and developments in the network industry. These study materials will only teach you a little bit about the networking industry. It is, therefore, important that you throw in some relevant information. In addition to studying the theoretical concepts.

Get Practical

You must always include some practical horses and tests as a part of your learning. If you are an employee of any organization or are a member of the Cisco learning network, you can obtain and appear for different practice tests that will help you prepare well for the examination. You cannot expect too easy examination simply with theoretical knowledge.

We will now look at how you can obtain the required information that will help you covered the concepts that you will need to learn to appear for the CCNA routing and switching certification.

The Cisco Official Study Material

The Cisco learning website will give you the link to the syllabus or material you will need to clear the CCNA Routing and Switching certification. You can obtain this information on the routing and switching tab on the Cisco website. In this tab, you will find a link to the two exam approaches: the one exam approach and the two-exam approach. The former is the CCNA composite exam, while the latter is the ICND1 and ICND2 examination. These sections have an examination kit that provides information about every

topic that you will need to cover to clear the examination. This kit will also shed some light on the topics that are easy to understand and also on the topics that are slightly difficult and more complicated.

As mentioned earlier, businesses are doing their best to migrate towards a control-based framework. This means that the role and the skills required for a network engineer are also changing rapidly. Most certifications offered by Cisco will provide this information. The CCNA routing and switching certification, however, will give you the foundation and the required knowledge about the technologies and how they impact the networks. Using this course material, you can ensure that your skills stay relevant even when there are changes in network technology.

This section will shed some light on the different study material and training program that you can use to understand the concepts covered in this certification.

Self-Study Materials

Interconnecting Cisco Networking Devices- Part 1

Cisco offers you an E-learning portal that is designed to assist you and enable you to learn to understand the concepts included in the routing and switching certification examination. This portal will include all the information about the ICND1 examination.

The course is structured in a way that will provide you a basic understanding of all the layers within the network that is used for code routing and switching. You will also gather information about various progressive technologies. Humorous topics have been included in the latest version of this examination, the version developed in the year 2016, to help you understand the interactions that take place in different network functions. You will also learn more about the interactions between wireless controllers, access points, and firewalls. Apart from this, you will also learn about the fundamentals of network security and some important protocols. This course will also introduce you to different configuration commands that will enable you to develop networks easily. You are also given a few lab exercises that will help you put your theoretical knowledge into practice.

This course is designed effectively. The material in this course will ensure

that you develop a basic understanding of the routing and switching certification. The content in this course is available in the form of text as well as an instructor-led session. This text is presented in a very easy format that you can understand. The course is often self-paced, but it ensures that you can interact with other students appearing for this examination. These different aspects ensure a hands-on learning experience while simultaneously increasing the efficiency and effectiveness of the course. This course will also make it easier for you to obtain feedback from your peers and instructors about your understanding of the course. There are some merit badges and leaderboards shown at the end of each week to motivate students to perform better.

When you complete this course, you will have gathered the required knowledge and skills to:

1. Define the fundamentals of networks and build basic LANs
2. Secure as well as manage network devices
3. Work on expanding networks that are small to medium-sized
4. Be able to describe the fundamentals of IPv6

This course is specifically designed for network specialists, network administrators, network support engineers, and some Cisco channel partners. You do not have to match any criterion. This means that there are no prerequisites for this course, but you will need to have some knowledge about the following topics will stop this knowledge will definitely come in handy while you are preparing for the course. The topics are fundamental computer literacy, essentials of PC operating system and navigation skills, primary Internet usage skills, and the basics of IP addressing systems. The associated certification of this course is CCNA Routing, and Switching and the associated exam is 100-1051 ICND1. English, Japanese, Chinese, and Spanish are the languages supported by this module. At present, the instructional videos are available in English and Spanish.

Cisco Learning Labs for ICND1

Cisco developed labs for each examination, and this set of labs was created to help students understand and improve their understanding of the different

concepts covered in this examination. These labs are powered by the Cisco IOS Software equipped with Layer 2 and Layer 3 features, are supported by CLI, and are accessible 24/7, so you can study and learn at your convenience. These labs will enable you to improve your understanding of all networks. You will be proficient in designing, configuring, managing, and troubleshooting any network issues that can arise. This product comes also comes with the discovery labs and challenge labs. The former provides you with guided learning so that you can learn different concepts while the latter will test your ability and understanding of the theoretical concepts. This means that you will need to spend some time on practical test sets so you can assess your knowledge. There are 45 different test sets or pieces that you will need to go through when you take this lab curriculum. These pieces are in line with the different concepts that you need to cover in this examination. When you clear this examination, you can appear for the second part of the examination. This will help you obtain the CCNA routing and switching certification.

Interconnecting Cisco Networking Devices- Part 2

The school also offers an E-learning portal for the second part of the examination. As with the first part of the examination, this learning portal is designed to help you prepare for the second part of the CCNA routing and switching certification examination. You will gather all the required information about the various topics covered in this examination.

This examination is an associate-level examination or course and is the second part of the CNA routing and switching certification. This course gives networking specialists and administrators the required skills and information to install, configure, operate, and troubleshoot networks in small enterprises. Some significant additions have been made to the curriculum in the year 2016. These have been discussed in detail in the previous chapters of the book. Some of the topics that have been included in this are:

1. Quality of Service (QoS) elements and their application
2. The interaction and impact of virtual and cloud services on the enterprise's network
3. An overview of programmability of network and associated controller types

4. Tools available to support any network architectures that are defined by the software

The course is structured similarly to the previous course. When you complete this course, you can:

1. Work with medium-sized LANs with various switches supporting VLANs, trunking and spanning tree
2. Solve problems related to IP connectivity
3. Understand the configuration and troubleshooting of EIGRP in an IPv4 system and the configuration of EIGRP for IPv6
4. Successfully understand the traits, functions and different aspects of WAN
5. Understand how device management can be executed by utilizing conventional and smart technology

You do not have to satisfy any prerequisites or criteria when you want to appear for the scores, but you must have some knowledge about the following topics:

- Fundamentals of networks
- Implementation of local area networks
- Implementation of Internet connectivity
- Management of devices
- Knowledge about securing network devices
- Implementation of IPv6 connectivity

The associated certification of this course is CCNA Routing, and Switching and the associated exam is 200-1051 ICND2. English, Japanese, Chinese, and Spanish are the languages supported by this module. At present, the instructional videos are available in English and Spanish.

Cisco Learning Labs for ICND2

Cisco developed labs for each examination, and this set of labs was created to help students understand and improve their understanding of the different concepts covered in this examination. These labs are powered by the Cisco IOS Software equipped with Layer 2 and Layer 3 features, are supported by CLI, and are accessible 24/7, so you can study and learn at your convenience. If you want to study on your own, the module and structure given in this course are easy to follow. It is the second part of the labs. You will learn more about how to configure, manage, and troubleshoot any issues in the network. Like the previous module, this module is also a combination of discovery and challenge labs. These will enable you to understand the topics better and also test your theoretical knowledge. These labs consist of 44 different pieces that you should go through. These pieces are aligned with the learning objectives of the second examination. When you hear this examination, you will obtain the CCNA routing and switching certification.

Certification Practice Exams

MeasureUp provides Cisco Certification Practice Exams to help test your level of understanding and skills. This website provides some information on different topics (these aren't the questions that might come in the final exam) that are related to various certification exams offered, such as Cisco CCENT, Cisco CCNA Routing, and Switching, Cisco CCNP ROUTE, Cisco CCNP SWITCH, and Cisco CCNA Security.

Apart from the study materials, Cisco also offers an extensive network of resources that include CCNA routing and switching study sessions, study material, access to different forums and blogs, and peer counseling.

Training

One of the best ways to prepare for the CCNA routing and switching certification is to enroll for the different training programs that are approved by Cisco. You can enroll for either the CCNAX course or enroll for the independent courses ICND1 and ICND2.

Interconnecting Cisco Networking Devices Part 1 (ICND1)

The ICND1 course will help you learn the basics of network layers, which are important for routing and switching. You will also learn more about the basics of routing and switching, which will create a base for some advanced technologies. The syllabus covered in this training module is the same as the

syllabus that is covered in the ICND1 course. Please refer to the previous section for more information about the ICND1 examination.

Interconnecting Cisco Networking Devices Part 2 (ICND2)

The syllabus or the content covered in this training module is the same as the course material you will need to prepare if you are writing the ICND2 examination. Please refer to the previous section for more information about the ICND2 examination. The difference between this training program and the self-paced learning is that the former has numerous lab exercises that you can work on to master the different training modules.

Enrollment

You can enroll for either the composite examination or the ICND1 and ICND2 examinations depending on which you choose to appear for in the following ways:

1. Choose an instructor-led training session, and enroll yourself into that session on the Cisco Learning Locator page.
2. Enroll for a private group training session on the Cisco Private Group Training.
3. Visit the Cisco Learning Network Store if you want to choose a self-paced e-learning program.
4. You should visit the Cisco Platinum Learning Library if you only want to access the digital library.

Interconnecting Cisco Networking Devices: Accelerated (CCNAX)

The CCNAX course is the perfect amalgamation of the courses ICND1 and ICND2. This course is a five-day training program. You will learn about the installation, management, operation, configuration, and the fundamentals of the Internet Protocol version 4 or IPv4 along with the Internet Protocol version 6 or IPv6 network. You will not only learn about these concepts but will also learn more about how to configure a LAN switch, how to work with an IP router, how do identify potential security breaches in a network, and connect to the Wen network. This combined course will give you the basic troubleshooting steps and tips that you can use if there are any errors in the network. These tips will also enable you to do well in the examination.

Some of the concepts included in this training program are:

1. Quality of Service (QoS) as well as their applications
2. The effect of virtual and cloud services on enterprise networks and their interaction
3. A detailed overview of the network programmability along with the corresponding tools and controller varieties that are available for supporting a Software-Defined Networking (SDN) architecture

This is not an exhaustive list of all the concepts that you will learn in this course. You will also learn about the functions and interactions of firewalls, the basics of network security, the IPv6 protocol, wireless controllers, the access points for wireless controllers, and more. This course is a combination of the ICND1 and ICND2 courses.

Cisco learning network offers instructor-led training that is spread over five days. This course also includes some lab practice. At the end of the course, you will learn to design, configure, implement, and troubleshoot a network. This course will ensure that you nor the basics of networking. Support engineers, associate network engineers, network specialists, and network administrators and analysts must appear for this course. You can either choose to take a private group training or instructor-led training depending on your interest. You can obtain further details about this course on Cisco's website in the following sections: "Cisco Learning Locator" and "Cisco Private Group Training," respectively.

Cisco Official Course Material for Purchase

You can access all the material required to prepare for the certification examination by just paying $750. Some topics can be downloaded for free, while others are sold at a lower price. You must ensure that you check the content and verify that the material is not repetitive.

Chapter 10

Exam Study Plan

Now that you are aware of what is included in the CCNA Routing and Switching examination let us look at how you can analyze where you stand concerning the curriculum. This book will help you understand everything you need to know about the examination, but this is not where it ends. You need to develop a study plan if you want to ensure that you ace the examination and clear it in your first attempt. This chapter will give you a four-week study plan that you can follow. Remember that you can clear your examination only if you follow the plan word for word.

When you choose to write the CCNA Routing and Switching examination, you must make some changes to your daily schedule since you need to spend some time studying for the examination. When you follow this study plan, you must complete at least two sections in the syllabus every week. Since there are numerous topics covered in each of these sections, you must spend at least four hours every day on the syllabus. If you have briefly read through the course material, you can identify the topics that will take you some time to master. You will also identify those topics where you will need to practice a little more.

If you choose to prepare for the routing and switching examination, you can undergo some training sessions provided by Cisco. You can find this training on the Global knowledge page. The instructors are people from the field who are well-read and know the concepts they are teaching. Most of the instructors are either recertifying themselves or taking the exam. They know exactly what one needs to do to clear the examination.

Week 1

Since subnetting and binary networks are the most difficult topics for most students, you will need to cover these during the first week of your study plan. It would be best if you also went through some active sessions and training to improve your understanding. During this week, you will need to cover the following topics:

- What networking is, building blocks of networks, types of networks, TCP/IP model and OSI reference
- Ethernet technologies like cabling, Cisco layer 3 model and a summary
- What subnetting is, IP addressing and subnetting, types, composition, and classes of IP addresses, private and public IP Addresses
- Basics of subnetting, subnet lengths, subnet masks, troubleshooting IP addresses, summarization of routes
- When you go through each of these topics, you must ensure that you have enough time. You must spend at least three hours every day to work on the topics mentioned in this section. Make sure that you do not revise the topics now. If you have finished the course material very early, you can move onto the next topics in the syllabus. If you want to master these topics, you can watch different videos on the Cisco learning page to help you understand the capacities of every gadget used in the network. If you have time, you can also complete some practice tests on those topics.

Week 2

Before you write the CCNA Routing and Switching examination, you must ensure that you clear the 640-840 examination. In this examination, you will need to cover a total of 76 subtopics. During the second week of your study plan, you should cover some of those 76 topics:

- Basics to enhanced gateway interior protocol routing and configuring the EIGRP, troubleshoot and verify the same, operations and configuration of OSPF
- Gather the information and verify the configuration, configure the router interfaces along with DHCP and DNS and take the CCNA Lab 1 at this point
- Restoring, backing up, erasing and saving the IOS and configuration file, use of password recovery through a Cisco router, Cisco discovery and protocol and use of Telnet via IOS

- Introduction to switches, IOS and Cisco routers, use of CLI, i.e., command-line interface, the basic configuration of switches and router

- Basics of IP routing, understanding the operations of the same, default, dynamic and static routing, routing metrics and administrative details and classifying routing protocols

- Routing loops and redistribution, default route and static lab, routing protocols of RIPv2 and RIPv1, configuring, troubleshooting and verifying the RIP

- Redistribution and summary routes for OSP and EIGRP. You should also take the labs for EGRP, OSP and RIP at this stage

Week 3

During this week, you should look at the protocols. You will need to cover the switching protocol and spanning tree, understanding the configuration and functioning for catalyst switch, STP, RSTP and Ether channels with Cisco additions, Rapid spanning and VLAN spanning, BPDU guard and filter, labs for Port and STP security, MAC addressing table, VLAN and VTP, types of VLANs and Ports, VLAN trunking and protocol, Cisco firewalls and Network security, VLAN configuration and routing, device management, secure communication and security for Layer 2.

Week 4

This is the last week of your study plan. You must push yourself hard during this week if you want to achieve your goals. Make sure that you cover every topic in the study material, and understand the content thoroughly. You can practice everything you learn using different mock and practice tests that are available on the Internet and in the Cisco learning press. Since this is the last leg of your preparation, you will need to complete the following topics: access-list and secure communication, switch port and remote access, standard and extended access list, network translation address, dynamic and static configuration of NAT, WAN and NAT troubleshooting, VPN and frame relay, IP services and IOS Netflow, NAT and WAN troubleshooting, PPP concepts and configuration, IPv6 and encryption.

The Cisco Learning press releases some guides and study material for every

examination version created. The content in these books will break the concept down into information that one can understand easily. These books will also provide some information that you may not have looked at in the beginning. It is also a good idea to go through some practice papers during this week and look for some discussion forums where people talk about some new questions they may have come across.

You are now ready to take the examination. All you need to do is stay calm and focus on what you know.

Chapter 11

Exam Tips

You now know what plan you should follow and also have an idea of the different topics that are covered in the CCNA Routing and Switching examination. This chapter will leave you with some tips that you can use to clear the CCNA Routing and Switching examination or any other CCNA certification that you appear for. Remember that you cannot expect to clear the exam by only studying the concepts. You also need to be smart about how you approach the examination. Experts have suggested the tips mentioned in this chapter.

Get to Know Your Exam

Remember, you need to know what you are signing up for if you want to succeed. Look at any actor as an example. They know they need to struggle and work hard to get to where they want to be. The same concept works for you too. When you sit for any examination without an idea of what will be thrown at you, you will not ace the examination. Numerous people are willing to share some knowledge about the examination through their experience. If you are wary about speaking to other people about your experience, you can visit the Cisco website to learn more about the examination. This book provides some links that you can use to learn more about the different topics that you should know well if you want to clear the examination. You will also obtain some links for study material, online tutors, and practice tests. If you are unsure of what you are doing with this examination, then this is the right book for you. It is the right place since you will learn all there is to know about the examination.

Organize a Study Space

You must ensure that you always set up a corner in your house that you will only use to study. Keep any distractions away. Make sure that you always focus on your studies when you begin preparing for the examination. Avoid sitting on the sofa or bed when you study since this will only make you sluggish. Make sure that you have enough place in your study area to spread your books around and study. Never keep any electronic items on your study

table, unless you need to use it while you study. You know how you can study and focus on the exam material, so make sure you do exactly that. If you are someone who needs complete silence when you study, you should work in a closed room with no disturbance. Some people may study better when they work with other people while some would like to listen to music while they study.

Obtain the Right Material

This book would have given you an overview of the different concepts you must cover when you prepare for the examination. The previous chapter also shed some light on the different topics you must cover every week. You must always obtain the right material to study from. You should always use the material provided by the Learning Press. There are separate books for each examination. You can also use the 31-days before the material for the last month. It is always important that you make notes so you can revise some concepts before the exam. You can also outline the flow of the chapter for future reference.

Join the Online Community

When it comes to any IT certification examination, there is a lot of material that you can source from the Internet. Numerous communities allow you to share your experiences with the world. Some people want to share some examination strategies in these communities. These forums will also help you learn more about people's successes and failures. Aside from the Cisco Learning Network, you can search Google for a forum for that specific certification. You can also view the CCNA page on Reddit since there are people from across the globe that share their experiences. You must ensure that you always stay away from some toxic people and posts. Numerous users only use these forums to vent their frustration, and this will discourage you.

Study Until it Feels Like Second Nature

When you study for the examination, you should know the concepts so well that if someone were to wake you up and ask you to define a concept, you should answer the question without a second thought. If you cannot learn the course material in this manner, the chances of you clearing the examination will decrease. Since the CCNA examination is comprehensive, there are some concepts that people overlook when they study for it. Remember that you cannot do this. You must cover every single note mentioned in the book, and

it is hard to do this. You must memorize Internet speed designations, port numbers, and understand different networking tools and more. Make sure that you study every single day. You can develop a study plan that will help you set some time out every day so you can study. You should remember everything you learn in the syllabus since you will come across these terms and concepts at work. A CCNA Certification is valuable since it will say a lot about your quality.

Create Your Own Custom Study Plan

As mentioned earlier, you must prepare your very own study plan. The previous chapter provided a four-week study plan that you can use to get started. It is always a good idea to create your own study plan since you know what plan will work for you, and how many hours you can spare every day to study for the examination. There is no need to write an elaborate plan. You must, however, consider the following when you develop your study plan:

1. Make sure you have the date set. You should choose the examination date before you begin preparing for the exam. To do this, you should create your profile and identify the time and location that will suit you

2. Decide the amount of time you can spare every day to prepare for the examination. You may have some other commitments, so you must find the right time to prepare for the examination. This is the only way you can complete all the topics in the material. Remember to give you enough time so you can practice every concept that you have learned

3. Take a look at the training material and courses, and see if you can afford it. If you can afford the certified study material and training videos, you can blindly follow the information in the two. If you are unable to purchase these materials and videos. One of the best ways to ensure that you pass the exam is to purchase the pre-study material and begin reading it. This will help you create a solid foundation and also help you develop the necessary skills based on the course you have chosen.

4. Identify the training method that will help you learn better. Some

people can work better in classroom sessions while others like to study alone. If you are someone who prefers online sessions, make sure you plan your study sessions accordingly. Since you know yourself better than anybody else, you should choose your study plan according to what works best for you.

5. Have you understood the subject you have chosen well? Do you know what the passing rate for this examination is? Make sure you use your experience to help you understand how to prepare for the exam. That being said, you should also take the questions, logic, and the length of the exam into account. When you rely only on your experiences, it can lead to bad results.

Get Practical and Theoretical Experience

If you want to pass the CCNA Examination, you must ensure that you have some practical experience. You cannot expect to pass with theoretical knowledge alone. Prepare for the exam in a way that you can use the theoretical concepts for troubleshooting or networking issues in the real world. When you are aware of the problem, you must also be able to list some alternative solutions to the problem. For instance, when IP is found to be unreliable, you have to determine some alternative troubleshooting for communication between the nodes.

Use Practice Drills and Flashcards

You may be wondering why I am asking you to use flashcards and practice drills. Many test-takers have stated that these methods did help them pass the examination. All you need to do is make a list of all the questions you struggled with during the mock exam. Note these questions down on flashcards and write the answer on the back of the flashcard. You will notice that you have a stack of cards that you can use for your review. You should try to review these cards at least twice a day. It may bore you, and there is a possibility that it may feel like overkill, but this habit will ensure that these answers become like second nature to you. If there are some answers where you will need to perform the process, you should take some time and practice those processes until you can complete the process with no external help. This will help to drill the concepts into your head, and will also help you remember the concepts during interviews.

Get Involved in an Exam Prep Course

If you are someone who prefers to study alone, you can choose to purchase the self-study material, but remember that this is not the best way to prepare for any examination. You must remember that you need to have a good understanding of the subject you want to appear for if you want to clear that examination. This is not the case only for CCNA examinations, but for any examinations that you write. Remember that the course material differs for each certification that you appear for, which means that you need to know the course material in and out before you sit for the examination. You must also understand that different bodies work together to develop the course material since they look at how different concepts can practically be applied. It is always a good idea to spend some time with a professional who has some idea about the course material when you prepare for the examination. You can ask the person for some help and also ask then any questions you may have about the material. This is what you get when you sign up for an exam preparation course on the Learning website. When you sign up for these courses, you can increase your chances of acing the test.

Revise

Like every other examination you write, you should take some time to go through the Cisco Press Books to refresh your memory. Make sure that you go through every single word in the book, and you pay attention to what you read. There are times when you will find that you have forgotten to learn a concept. During the last few days before the exam, you should ensure that you spend enough time revising and solving any practice question papers. If you want to obtain some additional information about the questions that can be asked, you can visit some online forums. Make sure that at this stage, you know the course material in and out.

Experts also suggest that you read the Cisco Press Books repeatedly so you can commit every word in the book to memory. Make sure you go through the entire book a day or two before the examination. It is essential to revise since you will re-learn the essential concepts that will create the foundation for the CCNA examination.

Take Practice Exams

One of the most effective ways to prepare for any examination is to take mock or practice exams before you appear for the actual exam. You should

always take these mock examinations under examination conditions. These tests will help you assess where you stand with respect to the subject material. You will also learn how the question paper can be structured and what kinds of questions you may be asked.

As mentioned earlier, you must give these examinations under examination conditions, which means you need to time yourself, so you know how long you take to answer the paper. When you do this, you will know where you need to focus and which section you must work on faster. It is important that you use the official training material and question databases to practice your knowledge. You should also purchase the official question bank for the examination you appear for. Remember to use these practice tests as a way to identify your weaknesses and strengths.

When you take the test, you will know what areas you do well in and which areas you do not understand fully. So, focus on the second section. Make sure you have the right question database to use since you will learn what the correct answer is. You will also know why other options are incorrect. This is an easier way to improve your understanding of this subject. Practice examinations always help you emulate how the actual exam will be.

As mentioned earlier in the book, you must ensure that you have theoretical and practical knowledge of any concept that you study in the CCNA course material. You cannot expect to clear the examination only because you know every concept, know how to define those concepts, and know the functions of those concepts. The CCNA examination is not easy, but you can definitely improve your chances of clearing that examination if you practice some fundamentals. There is different technology covered in this examination, including ISP, router/switch, PC, hub, and RJ-45 cords. First, understand these well before you learn more about WAN, WPS, and DNS. It is only when you understand these concepts fully that you will learn how to build that network. When you build a network, you can learn more about how to troubleshoot it if any issues come up during the transmission of data.

You should also work on building a network topography. In some examinations, you may be asked to design, build, and configure a network. You may also be asked to tear a network down. In these situations, you must know what the foundations of networking are. You need to work on building a lab if you want to clear the CCNA examination.

Give Yourself a Breather

You are allowed to kick back and relax a few days before the exam, and it is what the doctor recommends. You should revise your concepts, but should not stress about it. You must ensure that you remain calm and are composed. Most students are nervous and try to cram as much information as they can during the last few days, and this is a bad idea. You should make sure that you get sufficient sleep, do not skip meals, and study only when required. The last-minute studying will not help you at all, and it will hurt your ability to perform well on the scheduled exam date. Give yourself a breather for a few days and rest well before the exam.

Never Rush to Take the Exam

You must remember that it will take you a long time before you can fully prepare for the CCNA Routing and Switching examination. These tests will include some problems that will seem like second nature to you. That being said, if you do not know some terms in the syllabus or are overconfident, you will lose some marks in the examination. You must ensure that you spread the exams out well, so you have sufficient time to study. This will give you enough time to revise some concepts and also gauge if you can clear the examination with the amount of preparation that you have. You can take a less intensive route if you want to save more money. Remember that these tests have been designed to be unanswerable and tough if you have not spent sufficient time trying to understand the concepts covered in the syllabus.

Have an Exam Day Preparation Plan

The examination day has finally arrived, and you are most definitely going to be anxious like every other student who is taking this examination. That being said, you should stop worrying about how the exam is going to be and only focus on doing your best. You should ensure that you do not exhaust yourself. This section covers some simple tips that you should keep in mind.

Is your exam kit ready?

Always look at the examination website, and make sure that you have all the items that are listed on the website. The examiners are very strict, and they will ask you to leave the room if you do not have one or more of the required items with you. You must always read the exam or candidate guide and make a list of all the items that you must carry with you. Speak to the point of contact at the examination center to learn more about what you are required

for you to carry with you to the examination room.

Are you calm and well-rested?

This is an extremely important thing to keep in mind. Most students fail their examinations because they are either physically or mentally exhausted. Students believe that they should revise every concept they can right before the exam so they can remember it. To do this, they stay up all night or wake up early on the day of the exam. What they do not understand is that it is never a good idea to read the concepts at the very last minute since it will leave you feeling anxious. If you still want to do a final review, you should try to make a list of all the concepts that you fully understand and read them before. It is never a good idea to focus on those concepts that you do not have a clear understanding of since that will cause some anxiety and panic. Alternatively, you can create a glossary or a summary to cover all the essential and necessary information. Only focus on reading the glossary before the exam. Make sure that you eat something very light before the exam.

Did you make the necessary arrangements to be on time at the test site?

There is a strict policy when it comes to time. If you are late for the examination, you may not be allowed to sit for the examination. Try to leave at least an hour before the scheduled time if you use public transportation. If you own a vehicle, make sure that you identify the shortest route, and know exactly where you need to park your vehicle at the test center.

Clear your mind

You only have a little time to complete the examination. So, relax and take a deep breath before you begin answering the questions. Remember that you have put in the required time and effort to prepare for the examination. You will not be able to do well in the examination if you overthink or are nervous.

Be aware of the time

While answering the questions, you must ensure that you focus only on the question that you are working on and ignore everything else. It is always a good thing to do this since you can focus only on answering the questions correctly. That being said, you must also keep track of time. If you have ever written an exam under pressure, you know that the time flies very quickly. Therefore, you must ensure that you have enough time left to answer the

questions accurately.

Take your time reading the questions

Regardless of how much time you have left in the examination, you must ensure that you do not rush. When you do this, you can misread the question or even miss out on a question. You should always take some time out and read every question thoroughly, and also ensure that the answers you are writing are related to those questions. You should always ensure that you understand everything that is being asked in the question. This will ensure that you answer the question correctly. If you are answering a multiple-choice question, you must read every option well to ensure that you do not look at the options that were put in to distract you. You should also pay attention to terms like not, never, all, least, always and most. These words will always change the meaning of the sentences. When you see a question beginning with "Choose the best answer," ensure that you read the options carefully since more than one option can be the right answer. It is recommended that you go through the exam dump before you appear for the examination since you can learn more about the different types of questions you will come across during the examination.

Try to relax

You must always ensure that you remain calm and composed during the examination. Try stretching your muscles and take deep breaths. This will help you relax your mind. When you are calm, you can always focus better, and this will make it easier for you to answer any tough question. It is important to remember that the examination you are writing is difficult, so try to have some fun while writing the examination. Trust yourself, and know that you will do great in the exam if you have stuck to your study plan. Otherwise, you will have had enough practice for the next attempt.

Keep learning

You have given the examination and will now need to wait for five business days to go by before you receive your Certificate of Completion via email. You must understand that it is alright if you did not clear the examination. When you do not clear the examination, you are aware of the mistakes that you may have made either when you were preparing for the examination or during the examination. This means that you know what you are not supposed to do, and will be able to perform better the next time. This is an

accomplishment by itself. You must always motivate yourself to perform better since this will help you improve your chances of success. If you want to help your peers, you can share your experiences and prevent them from making the same mistakes that you did.

As mentioned earlier, the CCNA examination is comprehensive. This means that you will come across different questions from a variety of topics. These topics are all based on the concepts of TCP/IP, spanning trees, comprehensive routing protocols, and more. It is a little hard to pass the examination when you look at the course material. There are a ton of things you will need to study to ensure that you pass the examination. It is for this reason that most people recommend that you complete the ICND1 examination since this will give you a base or foundation. You must also go through every single topic mentioned in the book, so you can complete the examination in the stipulated time. You cannot waste time thinking about an answer. The duration is very short, and it can be stressful even for someone who has studied well for the examination. Your performance, however, is dependent on how well-prepared you are.

Make sure to keep yourself motivated and study hard for the examination. When you obtain a CCNA certification, you will open several doors.

Chapter 12

Frequently Asked Interview Questions and Answers

What is Routing?

Through routing, you can identify the path in which any information can be passed between the source and destination systems. The path is usually provided through a network layer that is created by the router.

What Purpose Does the Data Link serve?

There are two functions that the data link layer performs:

- Framing
- Verifying that the messages from the source reach the right device

What is the Difference between Physical Topology and Logical Topology?

The physical topology will provide the actual layout of the medium in the network while the logical topology refers to the path that the signal takes through the physical topology.

Why is it Important to Use a Switch?

When information is passed from a source to a destination, you need to use a switch to create a frame. The switch will receive signals, and it will use that signal to create a frame. When it does this, the switch can easily read the destination system's address and access that address. The switch can then send the frame to the correct port in the network to pass on the information. Every organization uses this method since this is the most effective way to transmit data. The switch will never broadcast the information sent to every other port in the network.

In What Situation Does Network Congestion Occur?

If numerous users are trying to access one network using the same

bandwidth, there will be some congestion in the network. For example, if you want to log onto a website on Black Friday to access the sales, you may find it difficult to find your product because the server of the store is down, considering there is too much traffic on that network. This situation, however, only occurs where there is no segmentation in a large network.

Define the Term 'Window' in Terms of Networking

The source and destination can only share a set of segments, called the window, on any network. Once the segments are shared between the source and the destination, a notification must be sent to the source, confirming that the destination has indeed received the segments.

How Do Hold-downs Work?

A hold-down will ensure that an update message does not reinstate any downed link. It does this by removing that link from that message. A triggered update is used to reset the hold-down timer.

How is the Router Hold-down Timer Reset Due to a Triggered Update?

A triggered update can reset the router's hold-down timer if the timer has expired. This happens when the router receives a processing task that was proportional to the number of links present in the Internetwork.

Is a Network Divided into Smaller Sections Using a Bridge?

A bridge cannot be used to break the network into smaller segments, but it can be used to filter a large network. It does this without shrinking the network.

How Many Types of Memories are used in a Cisco Router?

Every Cisco router will use the following memories:

1. The NVRAM is used to store the startup configuration file
2. The DRAM stores the configuration file during the execution
3. The Cisco IOS is stored in the flash memory during the execution process

How Does Cut-through LAN Switching Work?

In this type of switching, once a data frame is passed to a router, it is sent out immediately and forwarded to the next segment in the network. This is done once the destination address is read.

Which LAN Switching Method Does the Cisco Catalyst 5000 Use?

The Cisco Catalyst 5000 uses the store-and-forward method of switching. The data frame is only shared between the source and the destination once the switch checks the CRC and saves the frame within the buffer.

What is the Purpose of the LLC Sublayer?

Most application developers use the LLC or Logical Link Control sublayer to perform the following functions:

1. Error correction
2. Manage the flow of the network layer using the start and stop codes

What is the difference between IGRP and RIP?

RIP only looks at the hop count when it determines the route in which information should be passed through the network. IGRP not only looks at the hop count but also looks at the reliability, MTU, bandwidth, and other factors about the route before it selects the route to transmit the message.

What is BootP?

In most networks, there will be some diskless workstations. The Boot Program or BootP Protocol is used to start those workstations. Since there is no disk in the workstation, you cannot power it without a protocol or program. This workstation can also use the BootP program or protocol to identify its own and the server's IP Address.

What Does the Application Layer do in Networking?

The application layer is used to perform the following functions:

- Helps to synchronize any application on both the server and the client sides

- Supports the components that are directly associated with communication in an application
- If any applications span beyond the OSI reference model specification, the application layer is used to provide network services for those applications

What is the difference between the User Mode and Privileged Mode?

The network will use the user mode to perform a task that is performed by the system regularly using a Cisco router. These tasks include simple functions like checking the router status, checking the route status, view system information, or connect to remote devices. In the privileged mode, more functions can be performed, including making changes to the router, debugging or troubleshooting, and including some tests to validate the routes in a network.

Define 100BaseFX

Ethernet with a data speed of 100 is termed as 100BaseFX.

What Is the Transmission Medium in An Ethernet?

The main transmission medium in an Ethernet is a fiber optic cable.

What is MTU?

The maximum transmission unit or MTU is the largest size of the packet of data that can be shared across the network. This means that the packet of data does not have to be broken down further before it is sent across the network.

How Does Cut-through LAN Switching Work?

If you configure the network to use this type of switch, the data that is sent to the router will be forwarded or immediately sent to the next part of the network. The next segment is identified only when the router reads the destination address.

What is the Difference between the Hub, Router, and Switch?

Routers are used to transmit the packets of data along with the different networks. A switch is a tool or device that helps to filter packets or datagrams between various LAN segments. A switch can have either a single broadcast

domain or multiple collision domains. A switch is used to support packet protocols, and it works in the second and third data link layers. A hub has both multiple collision domains and a single domain. All the information that comes from one port will be sent out to another port.

Using a Cisco Router's Identifying Information, What Are the Things That You Can Access?

You can identify the interfaces and the hostname from the Cisco router's identifying information. The former is a fixed configuration that will refer to a router port while the latter will give you the name of the router.

Define Latency

When information or data is being sent from one device to another over a network, there is sometimes a delay. This delay or lapse is termed as latency.

What is the Number of Hops Used When the Network Uses RIP?

The network receives hops when information is being transferred. If the network receives more than fifteen hops, this will indicate that the route is out of service or unreachable. Therefore, the maximum number of hops that any network can receive is fifteen.

What are Packets?

A packet is a result of data encapsulation. The packets are data that have been encapsulated or wrapped between the different OSI layers under different protocols. They are also called datagrams.

Define Segments

A segment is a part of a data stream that moves from the top layers in OSI to the bottom layers, and towards the network. A segment is a logic unit that is found in the transport layer.

Define a Frame Relay

Frame relays are used to communicate between different frames while sending information. This is done by designing, creating, and maintaining a virtual circuit and using the WAN protocol. This protocol only operates at the Physical and Data Link layers and has a high-performance rating.

If you want to Route an IPX, How Do You Configure a Cisco Router?

If you want to enable IPX routing, you should use the command IPX routing. When you do this, you can ensure that every device and interface within that network will be configured. You can then make a change using the encapsulation method or network number.

List the Different IPX Access Lists

There are two types of access lists in Networking:

- Standard
- Extended

The standard access layer is only used to filter the IP address of either the source or the destination. The latter access list filters a network using the source and destination IP addresses, protocol, socket, and port.

What are the Benefits of VLANs?

VLANs will allow you to develop and create some collision domains using different groups on a network. You do not need to access the physical location of the router. You can use a VLAN to establish different networks. You can use different types of hardware, functions, protocols, and other means to establish the network. It is for this reason that most people choose to use VLANs to set up a network when compared to a LAN. In the latter, the collision domain is only connected to the physical location.

Define HDLC

High-Level Data Link Control or HDLC protocol is a Cisco protocol, and this is the default encapsulation that is operated in all Cisco routers.

Define Subnetting

Subnetting is a process of breaking a large network down into smaller networks. Since it is a part of the large network, every subnet will need to be assigned some identifiers or parameters that will indicate the subnet number.

List the Advantages of Using the Layered Model in the Networking Industry.

The advantages of the layered network are:

1. The network industry is allowed to progress faster since specialization is encouraged.

2. Administrators can always troubleshoot problems or issues in the network efficiently.

3. An administrator can make changes only to one layer if necessary. He or she can also ensure that this change does not affect the other layers in the network.

Why do Administrators Prefer the TCP to UDP?

UDP is an unreliable and unsequenced protocol when compared to TCP. This protocol cannot establish a virtual circuit or even obtain any acknowledgment.

What Standards Does the Presentation Layer Support?

Multiple standards are used or included in the presentation layer. This will ensure that all the data in the layer is presented or broken down correctly. These standards include TIFF, JPEG, and PICT for graphics and MPEG, QuickTime, and MIDI for audio or video files.

How can you configure a Router Remotely?

You may need to configure a router remotely if you do not have physical access to that router. The best way to do this is to use the Cisco AutoInstall Procedure. In this process, the router will need to be connected to a WAN or LAN through the interfaces.

What Does the Show Protocol Display?

You will find the following in a show protocol:

- The configured encapsulation method for every interface
- The address that is assigned to every interface
- The protocols that are routed on the configured router

How Can an IP Address be depicted?

An IP Address can be depicted in three ways:

- using Hexadecimal (for example 82 1E 10 A1)

- using Binary (for example 10000010.00111011.01110010.01110011)
- using Dotted-decimal (for example: 192.168.0.1)

Is There a Way to Switch to Privileged Mode, and What Should You Do to Switch to the User Mode?

Enter the command enable if you want to access the privileged mode in any network. Make sure you know why you are doing it. If you want to switch back to the user mode, open the command prompt and enter "disable."

What are the Benefits of LAN Switching?

The benefits of LAN switching are:

- LAN switching improves the media adaptation rate
- It allows the transmission of the data through a full-duplex
- It allows easy and efficient migration

How Can One Identify a Valid Host in any Subnet?

You can use the following equation to identify a valid host in the subnet: 256 – (subnet mask). You will find the valid host between that range.

What is Bandwidth?

The transmission capacity of every medium is called the bandwidth. This is used to measure the volume that any transmission channel can handle, and it is always measured in kilobytes per section.

Define DLCI

Data Link Control Identifiers or DLCI are assigned to identify every virtual circuit, and these identifiers are assigned to these circuits using a frame relay service provider. These circuits exist on the same network.

How is a Cisco Router Secured? What are the Different Passwords That Can be used?

A Cisco router can be protected by five passwords:

1. Virtual
2. Terminal
3. Auxiliary
4. Secret
5. Console

Why Do Most Administrators Use Segmenting When They Need to Manage a Large Network?

Network administrators often use network segmenting to improve the traffic in the network. It also ensures that every user has a high bandwidth. This ensures that the network performs better. It is important to segment the network, especially if it is a growing network.

What command should be Used If You Want to Delete Any Existing Configuration in a Router and Want to Reconfigure It?

a. erase startup-config
b. erase running-config
c. delete NVRAM
d. erase NVRAM

Correct Answer: A. erase startup-config

When You Look at the Commands Given Below, What is the Next Command that You Need to Use to Route the Traffic that is going to the Router?

Hostname: Branch Hostname: Remote

PH# 123-6000, 123-6001 PH# 123-8000, 123-8001

SPID1: 32055512360001 SPID1: 32055512380001

SPID2: 32055512360002 SPID2: 32055512380002

ISDN switch-type basic ni

username Remote password cisco

interface bri0

IP address 10.1.1.1 255.255.255.0

encapsulation PPP

PPP authentication chap

ISDN spid1 41055512360001

ISDN spid2 41055512360002

dialer map IP 10.1.1.2 name Remote 1238001

dialer-list one protocol IP permit

The answer is (config-if)# dialer-group 1

When you Configure a Router that Utilizes Both Logical and Physical Interfaces, What are the Factors that You Need to Consider When You Determine the OSPR Router ID?

A. The highest IP address of any interface.

B. The middle IP address of any logical interface.

C. The highest IP address of any physical interface.

D. The lowest IP address of any physical interface.

E. The highest IP address of any logical interface.

F. The lowest IP address of any interface.

G. The lowest IP address of any logical interface.

Correct Answer: C. The highest IP address of any physical interface.

Mention the Size of the IP Address.

An IP address has a size of 32 bits for IPv4 and 128s bit for IPv6.

What Does a Data Packet or a Datagram Consist Of?

A datagram or data packet consists of the following information:

- Sender information

- Receiver's information

- Information passed through the client

This packet also contains some information that will define the number of the packet and the order of that packet. When the data is sent through the network, the information is broken down into smaller packets of data. These packets also carry some configuration and data for that message.

What is DHCP?

DHCP or Dynamic Host Configuration Protocol can assign an IP Address to specific workstations and clients. This protocol can also be used to create static IP addresses for different machines like printers, servers, routers, and scanners.

What is the difference between Static and Dynamic IP Addressing?

The router will manually assign a static IP address to the network while the DHCP server can assign a dynamic IP address to the network.

What is the Range for a Private IPS?

For a private IPS, the ranges that can be selected are:

- Class A: 10.0.0.0 – 10.0.0.255

- Class B: 172.16.0.0 – 172.31.0.0

- Class C: 192.168.0.0 – 192.168.0.255

How Can You Access a Router?

You can access a router in the following way:

- Telnet (IP)

- AUX (Telephone)

- Console (Cable)

What is EIGRP?

EIGRP or Enhanced Interior Gateway Routing Protocol is a protocol that was designed and developed by Cisco. This protocol can be used by routers to share routes in the network with other routers connected to the same system. Unlike RIP, EIGRP can only send incremental updated. This will decrease the volume of data that can be transferred in the network.

What Does the EIGRP Protocol Consist Of?

EIGRP comprises of

1. Load

2. Bandwidth

3. Delay

4. MTU or Maximum Transmission Unit

5. Reliability

What is the Function of a Clock Rate?

You can use the clock rate to either enable the router equipment or DCE to improve communication.

What Command is used to Remove or Delete any Configuration Data in NVRAM?

If you want to delete any information in the NVRAM, you can use the command to erase startup coding.

State the Differences Between the UDP and TCP?

Different systems use different protocols, like TCP and UDP, to send files across the network.

TCP (Transmission Control Protocol)	UDP (User Datagram Protocol)
You can use TCP to retrieve the lost part of any file shared across a network since this is a connection-oriented protocol. A system can lose connection to network while a file is being transferred. This protocol will ensure	When you use a UDP, you cannot be certain if your files will be sent to the destination system since this is a connectionless protocol. You also cannot be certain if there will be no leak in the data.

that no data is lost during the transfer.	
The TCP protocol will ensure that the files are sent in the same order to the destination system.	Since this is a connectionless protocol, you cannot be certain if the message will reach the destination in the right order.
The data in this protocol will always be read by the network as a stream. This means that the packets of data are always connected in the form of a stream.	In UDP, the packets are always broken down and sent across the network to the destination system. It is impossible to ensure that the packet will fully arrive at the destination.
Example: World Wide Web, file transfer protocol, e-mail, etc.	Example: VOIP (Voice Over Internet Protocol), TFTP (Trivial File Transfer Protocol), etc.

What is the Difference between Full Duplex and Half Duplex?

The difference between a half-duplex and full-duplex is that in the former, the communication will only happen in one direction. In contrast, in the latter, communication happens in two directions.

What is the Process of Conversion in Data Encapsulation?

Data encapsulation includes the following steps:

- Layers one, two, and three: The first three layers in the network are the application, presentation, and session layers. The router and protocols will convert the input provided by the user in these layers into data that can be transmitted in the network.

- Layer Four: The fourth layer in the network is the transport layer, and the router and protocols will break the data down into smaller segments or chunks that can be passed through the network.

- Layer Five: The fifth layer is the network layer, and the router and protocols will convert the data into packets or datagrams. The router and protocol will also add a network header to the data.

- Layer Six: The sixth layer is the data link layer, where the datagrams or packets are all built into the frames.

- Layer Seven: The seventh layer is the physical layer, where the router and protocols convert the frames into bits.

If the Router IOS is Stuck, What Command Should You Use?

Use the following command if the IOS is stuck: Ctrl + Shift + F6 and X.

Define Route Poisoning

Routes in a network can become invalid or dead, and the router must prevent the movement of packets through those routes. When you poison the route, you can prevent the transmission of packets. This process is termed as route poisoning.

In the case of RIP, What Route Entry Will an Invalid or Dead Route be assigned?

If there is a RIP entry in the table, the network will assign sixteen hops to any dead or invalid routes. This makes that route unreachable.

Conclusion

The CCNA Routing and Switching certification are one of the most prestigious certifications that an individual in the IT industry can earn. This book sheds some light on this examination and also provides some information about the other examinations that are offered by Cisco. Since Cisco is a leading networking company, every certification offered by it is considered prestigious. Many employers expect their current or future employees to have a Cisco certification. This certification will give them the faith that the employee can function on a variety of tasks and cater to any issues that may occur in the network.

This book was written to guide you, and help you learn more about the CCNA Routing and Switching examination. This book leaves you with some tips that you can use to ace the exam. You can ensure that you clear the examination in your first attempt if you follow the instructions and tips mentioned in the book word for word.

Remember that the CCNA examination is a comprehensive examination. Therefore, you need to set aside some time to prepare for the exam because the syllabus covered is vast. You will need to create a study plan and ensure that you stick to that plan. It is only when you do this that your hard work will pay off. This certification will give you an edge over your competitors since it will tell organizations that you have the required capabilities to work with networks.

If you are an aspirant of this CCNA Certification, I'm sure that this guide will help you achieve your goals. Prepare well, and do not be disheartened if you do not clear the examination in your first attempt. Try again and ensure that you do not repeat the mistakes that you made in the past. This is the only way you can ensure that you ace the examination and obtain the certification.

References

https://www.cisco.com/c/en/us/products/index.html#~products-by-technology

https://www.cisco.com/c/en/us/solutions/collaboration/index.html#~stickynav=1

https://learningnetwork.cisco.com/community/certifications/ccna/ccna-exam/exam-topics

https://blog.certskills.com/ann2016-09/

https://www.cisco.com/c/en_dz/about/blog-africa/2017/8-things-you-didnt-know-about-Cisco.html

https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/associate/ccna-routing-switching.html#~stickynav=1

https://learningnetwork.cisco.com/community/certifications/ccna/icnd2/exam-topics

http://index-of.co.uk/Various/CCNA%20Routing%20and%20Switching%20Study%20Guide%20-%20Lammle,%20Todd.pdf

https://www.globalknowledge.com/us-en/training/certification-prep/brands/cisco/section/routing-and-switching/ccna-routing-and-switching/

https://www.cognitel.com/blog/ccna-certification/advantages-of-ccna-certification/

https://www.cisco.com/c/en/us/products/switches/virtual-networking/index.html#~tab-benefits

https://learningnetworkstore.cisco.com/on-demand-e-learning/interconnecting-cisco-networking-devices-part-1-icnd1-v3-0-elt-icnd1-v3-0-020196

https://www.cisco.com/c/en_au/products/hyperconverged-infrastructure/index.html

https://www.cisco.com/en/US/services/ps2827/ps2993/services_at_a_glance_sas_sasu.pdf

https://www.greycampus.com/blog/networking/10-reasons-to-get-a-ccna-certification

https://learningnetwork.cisco.com/community/learning_center/certification_exam_topics

https://www.bestvalueschools.com/faq/what-is-the-cisco-ccna-certification/

https://learningnetwork.cisco.com/community/certifications/ccna/ccna-exam/study-material

https://www.cisco.com/c/en_au/products/switches/data-center-switches/index.html#~stickynav=3

https://www.cisco.com/c/en_au/products/collaboration-endpoints/index.html#~stickynav=1

https://career.guru99.com/frequently-asked-ccna-interview-questions/

https://www.workitdaily.com/benefits-ccna-certified

https://www.greycampus.com/blog/networking/everything-you-wanted-to-know-about-ccna

http://blog.networkbulls.com/top-5-networking-concepts-to-prepare-for-ccna-routing-switching-examination

https://www.urbanpro.com/ccna-certification/top-10-tips-for-ccna-routing-and-switching

https://www.techrrival.com/prepare-cisco-ccna-200-125-exam/

https://www.certlibrary.com/blog/tips-passing-cisco-ccna-certification-exams/

https://www.workitdaily.com/benefits-ccna-certified

https://www.globalknowledge.com/us-en/training/certification-prep/brands/cisco/section/routing-and-switching/ccna-routing-and-switching/

https://www.braindumps.com/guide-4-weeks-study-plan-for-ccna-routing-and-switching-exam.htm

https://www.greycampus.com/blog/networking/everything-you-wanted-to-know-about-ccna

CISCO CCNA COMMAND GUIDE

Advanced Methods and Strategies to Learn CISCO CCNA

STUART NICHOLAS

Introduction

This book on CISCO CCNA is a command guide to assist you in your studies regarding CCNA certification. This book contains proven steps and strategies on how to prepare for the exam. You can use this guide for self-study and on-the-job training. You can use the commands, the hints to make your networking easier for you. The book is small and smart enough to be your pocket guide. Whenever you encounter a problem, you can use this book as a reference guide to tackle the problem and manage it effectively. Unlike some big heavy textbooks, this book is packed up with to-the-point commands to help you learn and prepare in a short time.

Your strategy to prepare for the CCNA exam might be different from that of the other students. You might work through your preparation in a different style. You might have been equipped with the basic skills unlike your peers. Your knowledge, skills, experience, and learning potential will affect how you study for the exam. I have kept all the possible variations in my view when I wrote this book. All the commands are explained in the text format, unlike tables that are hard to read and understand. The simple text format makes this book different from the other books, and it also helps the reader better understand the concepts behind the commands. It does not matter what your background is; the book will help you effectively learn Cisco CCNA. Students like to make sure they learn a topic by heart. To make it possible, they scan many books and notes and research on the internet. However, as the information is scattered over different mediums and platforms, they get extremely confused. This lands them in trouble while they are close to their exams. In this book, you will find all the relevant information neatly ordered. The topics are written coherently. I have added all the commands in a concise manner to help readers grasp the concept. These features will boost your confidence. Once you have a proper knowledge base, you can practice the commands to take the exam. A solid knowledge base will allow you to make out what topics you need to research in an in-depth manner.

The book is organized into chapters, explaining separate topics to make the reading process easy and fun. I have tried to keep the book as less jumbled up as I can. To achieve that purpose, I have used bullet points to explain each

command so you can better understand each of them. The chapters also contain troubleshooting commands to help you manage the errors that come along the way. I encourage you to move on to the first chapter and start the learning process.

Chapter One

Cisco Devices

The chapter walks you through the requisite information and commands needed to connect rollover cables to the switch or router. The chapter also spans around the determination of the terminal settings and setup of LAN connections. I have explained different categories in bullets to give you a clear understanding.

Cable Types

You must ensure that the cabling is properly done or you might trigger problems before you even start. See the following pattern.

- If your device A contains a computer COM port and device B contains the console of switch or router, you should use the rollover cable.
- If your device A contains computer NIC and device B contains the switch or hub, you should use the straight-through cable.
- If your device A contains computer NIC and device B also contains computer NIC, you should use the crossover cable.
- If your device A contains computer NIC and device B also contains computer NIC, you should use the rollover cable.
- If your device A contains a switch or hub port and device B contains Router's Ethernet port, you should use the straight-through cable.
- If your device A contains a switch or hub port and device B also contains a switch or hub port, you should use the crossover cable. Also, don't forget to check for the uplink button to defeat this.
- If your device A contains a router's Ethernet port and device B also contains a router's Ethernet port, you should use the crossover cable.

- If your device A contains a router's serial port and device B also contains a router's serial port, you should use the Cisco serial DCE/DTE cable.
- If your device A contains a computer NIC and device B contains the router's Ethernet port, you should use the crossover cable.

Different cables have different pinout systems. See the following patterns.

Crossover Cable: Pin 1 – Pin 3, Pin 2 – Pin 6, Pin 3 – Pin 1, Pin 4 – Pin 4, Pin 5 – Pin 5, Pin 6 – Pin 2, Pin 7 – Pin 7, Pin 8 – Pin 8

Straight-Through Cable: Pin 1 – Pin 1, Pin 2 – Pin 2, Pin 3 – Pin 3, Pin 4 – Pin 4, Pin 5 – Pin 5, Pin 6– Pin 6, Pin 7 – Pin 7, Pin 8 – Pin 8

Rollover Cable: Pin 1 – Pin 8, Pin 2 – Pin 7, Pin 3 – Pin 6, Pin 4 – Pin 5, Pin 5 – Pin 4, Pin 6 – Pin 3, Pin 7 – Pin 2, Pin 8 – Pin

LAN Connections

- If the connection or port is Ethernet, the port type will be RJ-45. You must connect it to an Ethernet hub or Ethernet switch through cable RJ-45.
- If the connection or port is TI/EI WAN, the port type will be RJ-48C/CA81A. You must connect it to EI or TI network through rollover cable.
- If the connection or port is a console, the port type will be 8-pin. You must connect it to a computer COM port through rollover cable.
- If the connection or port is AUX, the port type will be 8-pin. You must connect it to the Modem through cable RJ-45.
- If the connection or port is BRI U WAN, the port type will be RJ-49C/CA11A. You must connect it to an ISDN network exchange (PINX) through cable RJ-45.
- If the connection or port is BRI S/T, the port type will be RJ-48C/CA81A. You must connect it to an NTI device or private

integrated network exchange (PINX) through cable RJ-45.

The Difference Between 568A and 568B Cables

Two standards have been released by EIA/TIS group about the UTP wiring. These are dubbed as 568A and 568B. 568B is a bit newer and it is the standard. The difference between the two standards is due to the pin assignments and not based on the type of colors. The 568A standard is greatly compatible with the United States' Universal Service Order Codes (USOC) standards for the telephonic infrastructure and the voice connections. In both standards, the orange and blue pairs are at the center four pins therefore these colors tend to match closely with the 568A. It is best practice to use 568A for new installations and 568B for the existing installations. Now let us analyze the 568A and 568B standards.

568A Standard

- Pin 1 of white or green color will pair with 3. Its description is RecvData +.
- Pin 2 of green color will pair with 3. Its description is RecvData -.
- Pin 3 of white or orange color will pair with 2. Its description is TxData +.
- Pin 4 of blue color will pair with 1. Its description is 'Unused'.
- Pin 5 of white or green color will pair with 1. Its description is 'Unused'.
- Pin 6 of orange color will pair with 2. Its description is TxData .
- Pin 7 of white or brown color will pair with 4. Its description is Unused.
- Pin 8 of brown color will pair with 5. Its description is Unused.

568B Standard

- Pin 1 of white or orange color will pair with 2. Its description is TxData +.

- Pin 2 of orange color will pair with 2. Its description is TxData +.
- Pin 3 of white or green color will pair with 3. Its description is RecvData +.
- Pin 4 of blue color will pair with 1. Its description is Unused.
- Pin 5 of white or blue color will pair with 1. Its description is Unused.
- Pin 6 of green color will pair with 3. Its description is RecvData -.
- Pin 7 of white or brown color will pair with 4. Its description is Unused.
- Pin 8 of brown color will pair with 4. Its description is Unused.

The odd pin numbers always belong to the striped wires.

Command Line Interface

To enhance efficiency, Cisco IOS software has provided the users with some shortcuts to enter the most used commands.

- The command Router>enable is the same as Router>enab and Router>en. When you enter the short form of the commands, it is fine as long as you have no confusion.
- The command Router#configure terminal can be used interchangeably with Router#config t.
- You also can use the tab key to execute the commands. The command Router#sh + Tab key is the same as Router#show.

The question mark plays an important role in executing commands. You can use the question mark to see what you can do with the command and its parameters.

Question Mark

- The command Router#? will list all the commands that are

available in the present command mode.

- The command

  Router#c?

  clear clock

  will list all the available choices that tend to start with c.

- The command

  Router#c1?

  clear clock

  will list all the available choices that will start with cl.

- The command

  Router#clock ?

  set

will list all the available choices that reveal all the subcommands that are linked to this command. It also sets the date and time of the system.

- The command Router#c? set 20:40:00 17 August 2020 ? + Enter key will confirm that you have configured the data and time of the system.
- The command Router# will show there is no incomplete command message or error message and that the command was executed successfully.

Miscellaneous Commands

- There is an enable command you can use to move the user. The command Router>enable Router# will move the user to the privileged mode.
- The command Router#exit or Router>exit allows the user to log off on the system.
- The command Router(config-if)#exit Router(config)# will move

the user back to level one.

- The command Router(config)#exit Router# will also move the user back to level one.
- The command Router#disable Router> will move a user from the privileged mode to the user mode. It is known as the disable command.
- The command Router#logout has the same function to perform as exit. It is known as the logout command.
- The command Router#setup will take the user to the startup mode right at the command line. It is labeled as the setup mode and you will see an answer in the square brackets. If this is what you want, you should go on and press the Enter key. If you want to end the setup process at any point, you can enter Ctrl + C to shut down the interfaces and return to the user-mode Router>. The setup mode can never be used for the router's configuration as it only performs the basics. You can turn on the IGRP or RIPv1 but not the EIGRP or OSPF and you cannot make ACLs or enable the NAT.

Keyboard Usages

You can use different keyboard commands during the editing process. There will be many tasks that you will repeatedly be using. To make it possible, the Cisco IOS Software allows you to use different keyboard combinations to make the process highly efficient.

- You can use the carrot symbol ^ over the 6 key on the keyboard to locate the mistake you might have made while entering the command.
- You can enter ctrl + a on the keyboard to move the cursor from where it is to the start of the line.
- You can enter ctrl + b on the keyboard to move the cursor from where it is to the back by one word.
- You can enter ctrl + b or the left arrow on the keyboard to move

the cursor from where it is to back by one character.

- You can enter ctrl + e on the keyboard to move the cursor from where it is to the end of the line.
- You can enter Esc + f on the keyboard to move the cursor from where it is to a forward point by one word.
- You can enter Ctrl + f or the right arrow on the keyboard to move the cursor from where it is to a forward point by one character.
- You can enter $ that is above the 4 key on the keyboard to indicate that you have scrolled the line toward the left side.
- You can enter Router#terminal no editing to turn off the ability to use the keyboard shortcuts of the previous session.
- You can enter Router#terminal editing to re-enable the enhanced editing mode.

You can scroll through the history by the following commands.

- You can enter Ctrl + P or the up arrow on the keyboard to recall the commands that you have used in the past and that are a part of history. You will be able to use them in the backward sequence. You will see the most recent command.
- You can enter Ctrl + P or the up arrow on the keyboard to recall the commands that you have used in the past and that are a part of history. You will be able to use them in the backward sequence. You will see the most recent command.
- You can enter Ctrl + n or the down arrow on the keyboard to return the commands that you have used most recently.
- You can enter terminal history size *number* to set the total number of commands that reside in the buffer and that the router can recall. For example, Router#terminal history size 30 will recall the last 30 commands that are in the buffer. Similarly, the command Router#no terminal history size 25 will set the history

buffer coming back to the last ten commands. This is the default view of the command line. The history size command helps provide the function as that of the terminal history size command.

You can apply some show command to scan the information about the command line interface and the systems.

- The command Router#show version will display the requisite information about the present IOS.
- The command Router#show history will display all the commands you have used in the command line interface history.
- The command Router#flash version will display the requisite information about the flash memory of the system.

The last line of output from the show version tells us what the configuration register has been set up to.

Chapter Two

Commands for the Configuration of the Router

This chapter will walk you through the commands and information about the configuration of a router. You will learn how to set up the names, interfaces, passwords, host tables, and save the configurations. The router mode commands are as under.

Router Modes Commands

There are different router modes that you may experience while you are navigating through the command line. All the commands do not work in all modes. If you type something in a command and you know it is correct but you get an error instead, you should recheck if the mode you are working in is right.

- The command Router> reflects the user mode.
- The command Router# reflects the privileged mode.
- The command Router(config)# reflects the global configuration mode.
- The command Router(config-if)# reflects the interface mode.
- The command Router(config-subif# reflects the subinterface mode.
- The command Router(config-line)# reflects the line mode.
- The command Router(config-router)# reflects the router configuration mode.

Configuration of the Name of the Router

You can use this command both on switches and routers.

- The command Router(config)#hostname Cisco reflects the router configuration mode.

Global Configuration Mode

- The command Router> reflects that the limited view of the configuration mode cannot introduce any changes in the mode.
- The command Router# reflects that the user can see how the configuration process is going on and that they can make the changes they need.
- The command Router#config t will take you to the router configuration mode. Once you execute the command, you will see the following prompt Router(config)# which indicates that you are allowed to introduce the changes in the configuration of the system.

Commands for the Configuration of Passwords

You can use the following commands both on switches and routers. There is a variety of commands that you can use for the purpose.

- The command Router(config)#enable password cisco will allow you to set the enable password.
- The command Router(config)#enable secret class will allow you to set the enable secret password.
- The command Router(config-line)#login will allow you to enter the console-line mode. It will also fix the console-line mode passed to the console. It also enables the system to check the password at the login time.
- The command Router(config-line)#password console will allow you to enter the console-line mode. It will also fix the console-line mode passed to the console. It also enables the system to check the password at the login time.
- The command Router(config)#line con 0 will allow you to enter the console-line mode. It will also fix the console-line mode

passed to the console. It also enables the system to check the password at the login time.

- The command Router(config)#line vty 0 4 will allow you to pop into the vty mode for the five vty lines. This command will help you set the vty password to the telmet. You also can enable password checking at the time of login.
- The command Router(config-line)#login will enable the password checking at the time of login.
- The command Router(config-line)#password telmet will help you set the vty password to the telmet.
- The command Router(config)#line aux 0 will land you in the auxiliary line mode.
- The command Router(config-line)#password backdoor will help you to change the auxiliary line mode password into backdoor.

The enable secret password is usually encrypted by default. However, the enable password is usually not. The recommended practice should be that you must not use the enable password. You should only make use of the enable password to configure the router. If you do so, you will defeat the usage of encryption. Also, you cannot set the enable password and enable secret password to the same password. This will defeat the encryption.

Password Encryption Commands

- The command Router(config)# service password-encryption will help you set up and apply weak encryption to your passwords.
- The command Router(config)#no service password-encryption will block password encryption on your system.
- The command Router(config)#enable password cisco will set up the password to cisco.
- The command Router(config)#password cisco will continue with the passwords that you set up.

The show Commands

There are a bunch of show commands that allow you to see different statistics and numbers in the system.

- The command Router#show ? will let you see the show commands that are available in the system.
- The command Router#show interfaces will let you see the statistics for all the interfaces in the system.
- The command Router#show interface serial 0 will let you see the statistics for special interfaces such as Serial 0.
- The command Router#show clock will display the exact time on the device.
- The command Router#show users will let you see all the users have been connected to the device.
- The command Router#show history will let you see the history of different commands used the level of edit.
- The command Router#show controllers serial 0 will let you see the statistics of the interface hardware. These statistics will display if the rate of the clock is set and the cable is DTE or unattached.
- The command Router#show hosts will let you see the local host-to-IP addresses. You will see the names and the addresses of different hosts on the network to which you have been connected.
- The command Router#show version will let you see all the information related to the loaded version of the software concerned.
- The command Router#show running-config will let you see the configuration that is presently running inside the RAM.
- The command Router#show startup-config will let you see the configuration that is saved on the NVRAM.

- The command Router#show flash will let you see all the information that is related to the Flash memory.
- The command Router#show protocols will let you see the status of the configured layer that has 3 protocols.
- The command Router#show arp will let you see all the ARP table.

Interface Names

Remembering the names of the interfaces is one of the biggest problems that administrators might face. Each router has a different interface name. The market is replete with many Cisco devices that are being used in the production networks in the present day. Some administrators get confused due to these interface names. You can use the command router#show ip interface brief to see which type of interface is on your computer.

Router mode: 2501. The slot number or port location is on board. The port or slot type is Ethernet. The slot numbering range is labeled as an interface-type number. An example of this interface is ethernet0(e0).

Router mode: 2501. The slot number or port location is on board. The port or slot type can be Serial. The slot numbering range is labeled as an interface-type number. An example of this interface is serial0 (sO) & s1.

Router mode: 2514. The slot number or port location is on board. The port or slot type is Ethernet. The slot numbering range is labeled as an interface-type number. An example of this interface is e0 & e1.

Router mode: 1721. The slot number or port location is on board. The port or slot type is FastEthernet. The slot numbering range is labeled as an interface-type number. An example of this interface is fastethernet0() (fa0).

Router mode: 2514. The slot number or port location is slot 0. The port or slot type is WAC (WIN Interface Card) (Serial). The slot numbering range is labeled as an interface-type number. An example of this interface is s0 & s1.

Router mode: 1760. The slot number or port location is on board. The

port or slot type is Fast Ethernet. The slot numbering range is labeled as interface-type 0/port. An example of this interface is fa0/0.

Router mode: 1760. The slot number or port location is slot 0. The port or slot type is WIC/VIC (Voice Interface Card). The slot numbering range is labeled as interface-type 0/port. An example of this interface is s0/0 & s0/1 and v0/0 & v0/1.

Router mode: 1760. The slot number or port location is slot 1. The port or slot type is WIC/VIC. The slot numbering range is labeled as interface-type 1/port. An example of this interface is s1/0 & s1/1 and v1/0 & v1/1.

Router mode: 1760. The slot number or port location is slot 2. The port or slot type is VIC. The slot numbering range is labeled as interface-type 2/port. An example of this interface is v2/0 & v2/1.

Router mode: 1760. The slot number or port location is slot 3. The port or slot type is VIC. The slot numbering range is labeled as interface-type 3/port. An example of this interface is v3/0 & v3/1.

Router mode: 2610. The slot number or port location is on board. The port or slot type is Ethernet. The slot numbering range is labeled as interface-type 0/port. An example of this interface is e0/0.

Router mode: 2610. The slot number or port location is slot 0. The port or slot type is WIC (Serial). The slot numbering range is labeled as interface-type 0/port. An example of this interface is s0/0 & s0/1.

Router mode: 2611. The slot number or port location is on board. The port or slot type is Ethernet. The slot numbering range is labeled as interface-type 0/port. An example of this interface is e0/0 & e0/1.

Router mode: 2611. The slot number or port location is slot 0. The port or slot type is WIC (Serial). The slot numbering range is labeled as interface-type 0/port. An example of this interface is s0/0 & s0/1.

Router mode: 2620. The slot number or port location is on board. The port or slot type is FastEthernet. The slot numbering range is labeled as interface-type 0/port. An example of this interface is fa0/0.

Router mode: 2620. The slot number or port location is slot 0. The port or

slot type is WIC (Serial). The slot numbering range is labeled as interface-type 0/port. An example of this interface is s0/0 & s0/1.

Router mode: 2621. The slot number or port location is on board. The port or slot type is FastEthernet. The slot numbering range is labeled as interface-type 0/port. An example of this interface is fa0/0 & fa0/1.

Router mode: 2621. The slot number or port location is slot 0. The port or slot type is WIC (Serial). The slot numbering range is labeled as interface-type 0/port. An example of this interface is s0/0 & s0/1.

Router mode: 1841. The slot number or port location is on board. The port or slot type is FastEthernet. The slot numbering range is labeled as interface-type 0/port. An example of this interface is fa0/0 & fa0/1.

Router mode: 1841. The slot number or port location is slot 0. The port or slot type is HWIC/WIC/VWIC. The slot numbering range is labeled as interface-type 0/port. An example of this interface is s0/0/0& s0/0/1.

Router mode: 1841. The slot number or port location is slot 1. The port or slot type is HWIC/WIC/VWIC. The slot numbering range is labeled as interface-type 0/port. An example of this interface is s0/1/0& s0/1/1.

Router mode: 2801. The slot number or port location is on board. The port or slot type is FastEthernet. The slot numbering range is labeled as interface-type 0/port. An example of this interface is fa0/0& fa0/1.

Router mode: 2801. The slot number or port location is slot 0. The port or slot type is VIC/VWIC(voice only). The slot numbering range is labeled as interface-type 0/slot/port. An example of this interface is voice0/0/0& voice0/0/3.

Router mode: 2801. The slot number or port location is slot 1. The port or slot type is HWIC/WIC/VWIC. The slot numbering range is labeled as interface-type 0/slot/port. The examples of this interface are 0/1/0-0/1/3(this is single-wide HWIC) and 0/1/1-0/1/7 (this is double-wide HWIC).

Router mode: 2801. The slot number or port location is slot 2. The port or slot type is WIC/VIC/VWIC. The slot numbering range is labeled as interface-type 0/slot/port. An example of this interface is 0/2/0- 0/2/3.

Router mode: 2801. The slot number or port location is slot 3. The port or slot type is HWIC/WIC/VWIC. The slot numbering range is labeled as interface-type 0/slot/port. An example of this interface is 0/3/0- 0/3/3 for single-wide HWIC and o/3/0- 0/3/7 for double-wide HWIC.

Router mode: 2811. The slot number or port location is built into the front of the chassis. The port or slot type is USB. The slot numbering range is labeled as an interface-type port. An example of this interface is usb0& usb1.

Router mode: 2811. The slot number or port location is built into the back of the chassis. The port or slot type is FastEthernet Gigabit Ethernet. The slot numbering range is labeled as interface-type 0/port. An example of this interface is fa0/0& fa0/1 gi0/0& gi0/1.

Router mode: 2811. The slot number or port location is built into slot 0. The port or slot type is HWIC/HWIC-D/WIC/VWIC/VIC. The slot numbering range is labeled as interface-type 0/slot/port. An example of this interface is s0/0/0& s0/0/1 fa0/0/0& 0/0/1.

Router mode: 2811. The slot number or port location is built into slot 1. The port or slot type is HWIC/HWIC-D/WIC/VWIC/VIC. The slot numbering range is labeled as interface-type 0/slot/port. An example of this interface is s0/1/0& s0/1/1 fa0/1/0& 0/1/1.

Router mode: 2811. The slot number or port location is at NME slot. The port or slot type is NM/NME. The slot numbering range is labeled as interface-type 1/port. An example of this interface is gi1/0& gi1/1 s1/0& s1/1.

Navigation Through Interfaces

With the help of a few commands, you can easily navigate through the interfaces. Some commands are as under:

- The command Router(config)#int s0 will let you move to the S0 mode of the interface.
- The command Router(config-if)#exit will let you move from the S0 mode of the interface to E0 mode. After that you will reach

the following stage Router(config)#int e0.

- The command Router(config)#int e0 shows that you have entered the E0 interface. When you are done with a command, you will see Router(config-if)# that is a prompt and that does not change.

Configuring Interfaces

You can configure any kind of interface with the help of the following commands.

- The command Router(config)#int s0/0 will let you move from your current interface to the Serial 0/0 mode interface.
- The command Router(config-if)#clock rate 56000 will let you assign a set clock rate for the interface you are in.
- The command Router(config-if)#description Link to ISP will explain the optional descriptor of the link.
- The command Router(config-if)#no shut will let you turn on the interface.
- The command Router(config-if)#ip address 192.168.10.1 255.255.255.0 will let you assign the subnet mask and address to the interface.
- The command Router(config)#int fa0/0 will let you move from your current interface to the Fast Ethernet 0/0 mode interface.
- The command Router(config-if)#description Accounting LAN will let you view your link's optional descriptor.
- The command Router(config-if)#ip address 192.168.20.1 255.255.255.0 will let you assign subnet masks and addresses to your current interface.
- The command Router(config-if)#int fa0/0 will let you move from your current interface to the Fast Ethernet 0/0 mode interface.
- The command Router(config-if)#no shut will let you turn on the

interface.

You can use the clock rate command only on the serial interface that possesses a DCE cable that is plugged right into it. There ought to be a clock rate that is set on each serial link in between the routers. It is of least importance as to which router has been plugged with the DCE cable or which interface has got the cable plugged into it. The Serial 0 on the one router can be plugged into Serial 1 on some other router.

Some Miscellaneous Commands

- The command Router(config)#banner motd # You are inside a secure system. Unauthorized persons are not allowed. # is used to create banner messages and the character # is a delimiting character. The delimiting character must engulf the banner message that you want to convey. You can make it as long you want to. However, you should make sure that you do not include the # character in the body of the message or disrupt the command.

- The command Router(config)#clock timezone EST +5 will let you set the time zone that will be displayed on the interface.

- The command Router(config)#ip host (hostname) will let you assign the host's name to your IP address. After you have made the assignment, you can use the host's name instead of the IP address when you are trying to ping or Telnet to the address.

- The command Router(config)#no ip domain-lookup will let you turn off the domain in an effort to resolve any kind of unrecognized command to the name of the local host.

- Enter the command Router(config)#line con 0. Then enter the command Router(config-line)#nexec-timeout 0 0. It will let you set the time limit when your console will automatically log off. You can set the time to 0 0 (minutes seconds). This means that your console will never log off. This command works well for a lab because the console is not going to log out soon. Bad security is lethal in the real world.

- The command Router#copy run start will let you save your running-config to any kind of local NVRAM.
- The command Router#copy run tffp will let you save your running-config from a remote location to TFTP server.
- You can always have the option to erase the configurations from the system. The command Router#erase start will let you do that.

Basic Router Configuration

You can configure your router in a short time by pursuing the following steps.

- The command Router>en will allow you to enter the privileged mode from the basic user mode.
- You have to set the time first. The command Router#clock set 15:30:00 20 Oct 2020 will allow you to enter the privileged mode from the basic user mode.
- It is time to start the configuration mode. The command Router#config t will allow you to enter the global configuration mode.
- The command Router(config)#hostname Georgia will allow you to set the name of the router to Georgia. You can set the name of the router to other cities than Georgia.
- The next step is turning off the name resolution. The command Georgia(config)#no ip domain-lookup will allow you to turn off the name resolution on the unrecognized commands.
- Now you can create a banner for your router just like the one we created in the past section. The command Georgia(config)#banner motd # You have entered the Georgia router. There will be no entry for unauthorized users. # will allow you to set up the banner.
- Now you can set up the time zone. The command Georgia(config)#clock timezone EST +5 will allow you to set it

to the Eastern Standard Time (+5 to UTC).

- The next step in the router configuration is setting up the secret password on cisco. The command Georgia(config)#enable secret cisco allows you to enable the secret password on cisco. Moving forward you can set up encryption on your router password as well. The command Georgia(config)#service password-encryption will allow you to set up weak encryption on the password.
- The command Georgia(config)#line con 0 will allow you to enter the line console mode.
- The command Georgia(config-line)#logging will allow you to block unsolicited interruption to your commands.
- The command Georgia(config-line)#password class will allow you to set the password to class.
- The command Georgia(config-line)#login will allow you to turn on the password checking at the login.
- The command Georgia(config-line)#line aux 0 will allow you to shift to the system's line auxiliary mode.
- The next step once again is to set the password to class. The command Georgia(config-line)#password class will allow you to set the password to class.
- The command Georgia(config-line)#login will allow you to set up password checking at the point of login.
- This is the step toward setting up the global configuration mode. The command Georgia(config)#no service password-encryption will allow you to turn off any existing encryption on the password.
- The next step is to shift the system to Fast Ethernet mode. The command Georgia(config)#int fa 0/0 will allow you to shift to Fast Ethernet 0/0 mode.
- Now you can set up a locally significant description on the

interface. The command Georgia(config-if)#desc Engineering LAN will allow you to set up your interface's locally significant description.

- The command Georgia(config-if)#ip address (write the address number here) will allow you to assign an IP address to your interface. It also assigns a subnet mask to your interface as well.
- The command Georgia(config-if)#no shut will allow you to turn on your interface.
- The command Georgia(config-if)#int s0/0 will allow you to move toward the Serial 0/0 mode.
- The command Georgia(config-if)#desc Link to Belfast Router will set up your interface's local description.
- The command Georgia(config-if)#ip address (address number) will assign your IP address and also the subnet mask to your interface.
- The command Georgia(config-if)#clock rate 5000 will allow you to set the clock rate.
- The next command Georgia(config-if)#no shut will switch on your interface.
- The command Georgia(config-if)#exit will allow you to come back to the global configuration mode.
- The command Georgia(config-if)#clock rate 5000 will allow you to set the clock rate.
- The command Georgia(config)#ip host belfast (address number) will allow you to set the local host's name to the IP address.
- The command Georgia(config)#exit will take you back toward the privileged mode.
- The command Georgia#copy run start will take your configurations to the NVRAM.

Chapter Three

Networking and Routing Concepts

This chapter will walk you through the basic concepts of networking and routing in cisco. The administrative distance is an important aspect in networking and routing. There are some default administrative distances (AD) in the world of cisco, which are as under:

- The administrative distance for the connected interface is 0.
- The administrative distance for the static route is 1.
- The administrative distance for the internal EIGRP is 90.
- The administrative distance for the EIGRP summary route is 5.
- The administrative distance for the external border gateway protocol (eBGP) is 20.
- The administrative distance for the internal BGP(iBGP) is 200.
- The administrative distance for the external EIGRP is 170.
- The administrative distance for the Interior Gateway Routing Protocol (IGRP) is 100.
- The administrative distance for the Intermediate System-to-Intermediate System (IS-IS) Protocol is 115.
- The administrative distance for the RIP is 120.
- The administrative distance for the unknown is 255.

Change the Default Settings of the Administrative Distance

You can use some commands to change the OSPF route's administrative distance from the default settings with the help of the following commands.

- The command Georgia(config)#router ospf 1 will let you kick off the process of OSPF routing.

- The command Georgia(config-router)#distance 85 will let you change the OSPF distance from 110 to 85.
- The command Georgia(config-router)#distance 85 192.168.10.2 0.0.0.0 will let you apply the administrative distance of 85 to the OSPF routes that you receive from 192.169.10.2. This newly assigned administrative distance will be locally significant, and other routers will use the default administrative distance.
- The command Georgia(config-router)#distance 103 172.16.10.2 0.0.0.0 will let you change the OSPF distance from 110 to 103 for all the routes that come through 182.16.10.2.
- The command Georgia(config-router)#distance 85 172.16.20.0 0.0.0.255 2 will let you change the distance from 110 to 85 for all the routes that match ACL 2.
- The command Georgia(config-router)#exit will bring you back to the mode of global configuration.
- The command Georgia(config)#access-list 2 permit 192.168.30.0 0.0.0.255 will let you create the ACL that will help you understand which route will have an administrative distance of 85. You can use a named ACL and replace its number with the ACL name that is usually in command.

Permanent Keywords

The command Georgia(config)#ip route 192.168.50.0 255.255.255.0 serial0/0/0/0 permanent will let you create a static route that you cannot remove from the table even if you have shut down the interface. In the absence of a permanent keyword in the static route statement, the static route will stand removed, if your interface that is specified in the command moves down. An interface that is down will trigger the directly connected network and the associated static routes to get deleted from the table. When the interface is back up, the routes will definitely be returned. When you have added a permanent keyword to a static route statement, you will keep the static routes in the table even if the interface goes down. The interface remains down but the routes remain in the table. Its benefit is that when the interface gets back up, little need is usually left for the reprocessing of the static routes. This saves time and also the power that is usually consumed on

processing.

IPv6 Address Assignment to Interface

You can use a bunch of commands for the assignment of different types of Ipv6 addresses to your interface.

- The command Georgia(config)#ipv6 unicast-routing will allow you to turn on the forwarding of the IPv6 unicast datagrams on a global scale across the router.
- The command Georgia(config)#interface gigabitetehernet0/0 will allow you to shift on to the configuration mode of your interface.
- The command Georgia(config-if)#ipv6 enable will allow you to kick off an IPv6 link-local address's automatic configuration process. It also enables the processing of IPv6 processing on your interface. The link-local address can be used to communicate with the nodes present on the same link.
- The command Georgia(config-if)#ipv6 address autoconfig will allow the router to configure itself automatically with the help of a link-local address. It does this with the help of a stateless auto configuration process.
- The command Georgia(config-if)#ipv6 address 2001::1/64 will allow you to configure a kind of global IPv6 address on your interface. It also lets you start the IPv6 processing on your interface. If you happen to add the global IPv6 address to your interface before you enter the ipv6 enable command, you will see witness the creation of a link-local address. In the end, the IPv6 will stand enabled on your interface.
- The command Georgia(config-if)#ipv6 unnumbered type/number will specify the unnumbered interface. It will enable IPv6 processing on your interface. The global IPv6 address of your interface that is usually specified by type/number will only be used as a source address for the packets that are sent from your interface.

Chapter Four

Deciphering RIP, IGRP & EIGRP

This chapter will walk you through the commands and information that are concerned with the optional and mandatory commands for the configuration of the Routing Information Protocol (RIP). I will also explain the commands that are linked to the configuration of RIP Version 2 (RIP-2).

First of all, I will explain how you can turn and off the ip classless.

- The command Georgia(config)#ip classless will direct IOS to process the packets that are destined for the unknown subnet toward the top supernet route. Usually, you do not have to enable this command in cisco as it is enabled by default in interfaces.
- The command Georgia(config)#no ip classless will undo what you have done with the help of the previous command.

RIP Routing

- The command Georgia(config)#router rip will help you to enable RIP.
- The command Georgia(config-router)#network w.x.y.z is usually a network number of a directly connected network that you are looking forward to advertise.

If you happen to advertise a subnet, there will be no error message, because the router will convert that subnet into a classful address.

The above mentioned commands are mandatory. What you will see next will be the optional commands.

- The command Georgia(config)#no router rip will let you switch off the RIP routing process.
- The command Georgia(config-router)#no network w.w.w.w will let you remove the network mentioned in the command from the

RIP process. This is easy and fun. You can simply name the network in the command and do away with it in no time.

- The command Georgia(config-router)#passive-interface s0/0 will let you lock the RIP updates so that they cannot be sent out of your interface.
- The command Georgia(config-router)#ip split-horizon will let you enable the split.
- The command Georgia(config-router)#no ip split-horizon will let you turn off your split horizon. The split horizon is usually on by default settings.
- The command Georgia(config-router)#neighbor x.x.x.x will let you define a neighbor to share your information.
- The command Georgia(config-router#timera basic 30 90 180 270 360 will let you change the timers of your RIP. You can update the timer at 30 seconds. The timer will turn invalid in 90 seconds and the hold-down timer is at 180. The flush timer is at 270 and the sleep timer is at 360 seconds.
- The command Georgia(config-router)#default-information originate will let you generate some default routes in the RIP.

RIP Version 2 Commands

- The command Georgia(config-router)#version 2 will let you tune the system as such that the RIP will only send and receive the RIP-2 packets in a global setting.
- The command Georgia(config-if)#ip rip send version 1 will let you send only the RIP-1 packets.
- The command Georgia(config-if)#ip rip send version 2 will let you send only the RIP-2 packets.
- The command Georgia(config-if)#ip rip send version 1 2 will let you send only the RIP-1 packets and RIP-2 packets.
- The command Georgia(config-if)#ip rip receive version 1 will let

you receive only the RIP-1 packets.

- The command Georgia(config-if)#ip rip receive version 2 will let you receive only the RIP-2 packets.
- The command Georgia(config-if)#ip rip receive version 1 2 will let you receive only the RIP-1 packets and RIP-2 packets.

Troubleshooting Problems

The commands that you can use to troubleshoot problems are as under:

- The command Georgia#debug ip rip will let you see the entire RIP activity. The results will be displayed in real time.
- The command Georgia#show ip rip database will let you see the contents of the database of RIP.

Mandatory Commands for RIP Version 2

- The command Georgia(config)#router rip will let you switch on the RIP routing process. You can use the same command for RIP Version as well.
- The command Georgia(config-router)#version 2 will let you switch on Version 2 of your routing process. Version 1 is default.
- The command Georgia(config-router)#network y.y.y.y will let you advertise the network that has been mentioned.

Optional Commands for RIP Version 2

- The command Georgia(config-router)#no version 2 will let you change the version back to the previous one that is RIP-1
- The command Georgia(config-router)#version 1 will let you change the RIP routing back to RIP-1.
- The command Georgia(config-router)#no auto-summary will let you summarize different networks. The RIP-2 summarizes different networks at the boundary namely classful. The command tends to turn off the autosummarization process.

- The command Georgia(config-router)#auto-summary will let you enable the autosummarization process again at the boundary namely classful.

IGRP

In the following section, I will give the details of different mandatory and optional commands that are related to Interior Gateway Routing Protocol (IGRP).

- The command Georgia(config)#router igrp will enable the routing process related to IGRP. IGRP routing uses autonomous system. The process ought to match other routers that will share the routing updates to make sure that the communication takes place.
- The command Georgia(config-router)#network x.x.x.x will let you advertise the network. The x.x.x.x is the name of the network that is directly connected and that you are looking forward to advertise.

You only have to advertise the classful network. You are not required to advertise a subnet. If you advertise a subnet, you will see no error message, because the router is likely to automatically convert the subnet into the address of a classful network.

Mandatory Commands for IGRP

There are few mandatory commands for IGRP routing. They are listed as under:

- The command Georgia(config)#no router igrp (enter number here) will let you disable the entire process of IGRP routing.
- The command Georgia(config-router)#no network x.x.x.x will let you remove the named network from the process of IGRP routing.
- The command Georgia(config-router)#bandwidth a will set up the bandwidth of the interface to a kilobit so that IGRP is

allowed to make an improved routing decision.

- The command Georgia(config-router)#variance a will let the IGRP take on the unequal-cost routes.

The bandwidth command is also used for metric calculations. It will not change the performance of the interface.

Troubleshooting

You can use two commands to troubleshoot if an issue pops up in the middle of the operations.

- The command Georgia#debug ip igrp events will let you see the IGRP events in the real time.
- The command Georgia#debug ip igrp transactions will let you see the IGRP updates that exist in between the routers.

EIGRP

This section will explain how to configure EIGRP, verify EIGRP, autosummarize EIGRP, and troubleshoot EIGRP.

Configuring EIGRP

- The command Georgia(config)#router eigrp 100 will turn on process 100 of EIGRP, an autonomous system (AS) number. This can be a number in between 1 and 65535. All the routers in AS ought to use a similar AS number.
- The command Georgia(config-router)#network 10.0.0.0 will specify which network must advertise in EIGRP.
- The command Georgia(config-router)#eigrp log-neighbor-changes will log any kind of changes that happen to one of the EGRIP neighbors.
- The command Georgia(config-router)#no network 10.0.0.0 will allow you to remove the same network from EIGRP process.
- The command Georgia(config-router)#bandwidth a will allow

you to set up the bandwidth of your interface to a kilobit. This allows the EIGRP to make an improved and beneficial routing decision. You only can use the bandwidth command to perform the metric calculations. This usually does not change the performance of your interface.

Auto-summarization

- The command Georgia(config-router)#no auto-summary will allow you to switch off the feature of auto-summarization. You will be able to summarize the networks, by default, at the boundary of the classful. The command Georgia(config-router)#int fa 0/0 is also a part of the auto-summarization process.
- The command Georgia(config-if)#ip summary-address eigrp 100 10.10.0.0 255.255.0.0 will allow you to enable the manual summarization process on your interface. This will be for the given mask and address.

EIGRP offers the facility to summarize different networks automatically at the boundary namely classful. If a network is poorly designed and is packed up with discontinuous subnets, it could create connectivity problems, especially if you leave the summarization feature open. There may be two routers that advertise the same network. However, the original intention can be the advertising of two different networks. In this situation, you should switch off the feature of auto-summarization and use the ip summary-address in its place. You can manually summarize what you have to do.

Verifying EIGRP

- The command Georgia#show ip eigrp neighbors will allow you to see the neighbor table.
- The command Georgia#show ip eigrp neighbors detail will allow you to see the contents of the same table.
- The command Georgia#show ip eigrp topology will allow you to see the table for topology.
- The command Georgia#show ip eigrp int 100 will allow you to

see the data regarding running process 100 of interfaces.

- The command Georgia#show ip eigrp s 0/0 will allow you to see the information for a particular interface.
- The command Georgia#show ip eigrp interfaces will allow you to see the data that pertains to each interface.
- The command Georgia#show ip eigrp traffic will allow you to see the type of packets sent or received and the numbers.

Troubleshooting

You can use the following commands to troubleshoot a problem that pops up along the way.

- The command Georgia#debug eigrp fam will allow you to see the actions/events that are related to the DUAL FSM.
- The command Georgia#debug eigrp neighbor will allow you to see the actions/events that are connected to EIGRP neighbors.
- The command Georgia#debug eigrp packet will allow you to see the actions/events that are connected to the packets of EIGRP.

RIP Next Generation

In this section, I will explain how you can implement RIPng on your routers.

- The command Georgia(config)#ipv6 unicast-routing will allow you to enable to spread the IPv6 unicast datagrams across the router globally.
- The command Georgia(config)#interface serial0/0/0 will allow you to shift to the interface's configuration mode.
- The command Georgia(config-if)#ipv6 tip tower enable will allow you to create the process named tower. It also enables the RIPng on your interface. The RIPng processes are shorter and smarter than the processes of RIPv1 and RIPv2. In RIPng, you do not have to create RIP routing processes with the help of the router rip command. Also, you do not have to use the network

command for the specification of your interfaces on which you will run RIP. In RIPng, these processes are created and done away with automatically on your interface. All it takes is the ipv rip name enable command. The name of the process should not be misspelled. If you misspell it, you will create a second process that carries the misspelled name. The name of the routing process need not match between the neighboring routers.

- The command Georgia(config)#ipv6 router rip tower will allow you to create a process named tower. It also takes you to the configuration mode of the router.
- The command Georgia(config-router)#maximum-paths 2 will allow you to define how many equal-cost routes there will be that are supported by RIPng. The number of paths may range between 1 and 64. The default number here is 64.
- The command Georgia(config-if)#ipv6 rip tower default-information originate will reveal the default route and other RIPng routes.
- The command Georgia(config-if)#ipv6 rip tower default-information only will reveal the default route. One difference is that this command will hide the other RIPng routes.

Troubleshooting RIPng

When you are using the debug command for RIPng, it is likely to affect the router performance adversely. It may even trigger a reboot in the router. Therefore, you should always stay cautious when you are using this command. You must never leave the debugging process open. You may use it long enough to collect the information and once you have harvested the information, you must immediately disable it with the undebug command. I will continue to use the router name Georgia in the following example as well. Here is the rundown of the commands for troubleshooting in RIPng.

- The command Georgia#clear ipv6 rip will help you to delete the routes from the IPv6 RIP table. It will also delete the routes from the IPv6 table as well.

- The command Georgia#clear ipv6 route * will let you delete all the routes that exist in the IPv6 routing table.
- The command Georgia#clear ipv6 route 2001:db8:c18:3: :/64 will let you clear a specific route from the IPv6 table.
- The command Georgia#clear ipv6 interface will let you see the status of all the interfaces that have been configured for IPv6.
- The command Georgia#clear ipv6 routing will let you see the debug messages related to the updates of the IPv6 routing table and the routing cache updates.
- The command Georgia#clear ipv6 traffic will let you reset the IPv6 traffic counters.
- The command Georgia#clear ipv6 packet will let you see the debug messages that are for the IPv6 packets.
- The command Georgia#clear ipv6 rip will let you see the debug messages for the transactions regarding IPv6 RIP routing.
- The command Georgia#show ipv6 route rip will let you see the present routes for RIPng in the IPv6 table.
- The command Georgia#show ipv6 route will let you see the present status of the IPv6 table.
- The command Georgia#show ipv6 rip next-hops will let you see the processes of RIPng. It also displays the next-hop processes that are running under each major process.
- The command Georgia#show ipv6 tip database will let you see the database of the RIPng processes. Even if more than two processes are running in the system, this command will show all the databases.
- The command Georgia#show ipv6 rip will let you see the information about the present process.
- The command Georgia#show ipv6 protocols will let you see the protocols and the present state of all the IPv6 protocol processes.

- The command Georgia#show ipv6 neighbors will let you see the IPv6 neighbor discovery information.
- The command Georgia#show ipv6 traffic will let you see the statistics that are related to IPv6 traffic.
- The command Georgia#show ipv6 route summary will let you see the short form of the IPv6 table.
- The command Georgia#show ipv6 routers will let you see the advertisement data for the IPv6 router.

IPv6 Ping

If you are looking forward to diagnosing the basic connectivity in a network with the help of IPv6, you may enter the Ping command that can be seen below.

Georgia#ping ipv6 2001:db8: :3/64

In the next section, I will shed light on the characters that you will see and their meaning and understand how to read the symbols.

- The character ! means that there is an indication of some replies.
- The character. means that a network has an error that timed out while the network was waiting for a reply.
- The character ? means that there is some kind of unknown error.
- The character @ means that there is some kind of unknown reason.
- The character T means that the time has already been exceeded.
- The character R means that there is a serious problem with the parameter.
- The character P means that the port is already unreachable.
- The character N means that the network has been unreachable and is beyond scope.
- The character H means that the host of the network is not

reachable.

- The character B means that there is a packet that is too big.
- The character A means that the network is administratively unreachable. It also means that a kind of access control list (ACL) tends to block the network traffic.

Chapter Five

Open Shortest Path Protocol (OSPF)

This chapter will walk you through the commands related to the Open Shortest Path First (OSPF). You will navigate through the commands regarding the configuration of single-area OSPF, the use of wildcard masks in OSPF areas, and the configuration of single-area OSPF such as cost metrics and loopback interfaces, timers, authentication, and propagation of default tone. You will also learn about the commands to verify OSPF and the troubleshooting of issues that pop up along the way.

Mandatory Commands for OSPF

- The command Georgia(config)#router ospf 123 will allow you to turn on the OSPF process number 123. The process ID can be anywhere between 1-65535. Its ID is not in any way linked to OSPF area.

- The command Georgia(Config)#network 172.16.10.0 0.0.0.255 area 0 will allow you to advertise the interfaces. OSPF does not advertise networks however it does advertise interfaces. It will use a wildcard mask that will determine which interface it has to advertise. The interfaces that belong to the address 172.16.10.x will be placed into Area 0. The process ID number of a router need not match the process ID number of other routers. Unlike Enhanced IGRP (EIGRP) and Interior Gateway Routing Protocol (IGRP), matching the number across the existing routers does not ensure adjacencies' formation.

When it is compared with the IP address of a computer, a wildcard mask will identify how addresses will be matched for the placement into a particular area.

A zero (0) inside a wildcard mask means checking the corresponding bit inside the address to have an exact match. A one (1) inside a wildcard means ignorance of the corresponding bit for the address. Here are some uses of

wildcard masks for OSPF.

- The command Georgia(config-router)#network 72.16.10.1 0.0.0.0 area 0 will allow you to put an interface that has an address 172.16.10.1 in Area 0.
- The command Georgia(config-router)#network 72.16.10.0 0.0.255.255 area 0 will allow you to put your interface that has an address 172.16.x.x in Area 0.
- The command Georgia(config-router)#network 0.0.0.0 255.255.255.255 area 0 will allow you to put your interface with any address in Area 0.

Optional Commands for OSPF

The first commands on the line are for loopback interfaces.

- The command Georgia(config)#interface 1o0 will allow you to shift from your current interface to the virtual interface that is Loopback 0.
- The command Georgia(config-if)#ip address 192.168.100.1 255.255.255.255 will allow you to assign an IP address to your interface. You can choose any IP address that fulfills your requirements. The loopback interfaces always remain up and up. They do not go down unless you manually shut them down, which is why loopback interfaces are considered wonderful for using OSPF router ID.

The following commands will help you modify the OSPF cost metrics.

- The command Georgia(config)#int s 0/0 will allow you to modify the metrics.
- The command Georgia(config-if)#bandwidth 256 will allow you to change the bandwidth of the network. You can change it to 128. OSPF will also recalculate the cost of the link.
- The command Georgia(config-if)#ip ospf cost 1690 will allow you to change the cost figure to the value of 1690. The link's cost

is generally determined by the division of the reference bandwidth by interface bandwidth. The default bandwidth can be a number from 1-10,000,000. It is generally measured in kilobits. The cost is a number between 1-65,535.

Authentication

- The command Georgia(config)#router ospf 456 will allow you to kick off the authentication process.
- The next command on the line is Georgia(config-router)#area 0 authentication will allow you to turn on the process of simple authentication. You can send in the password in clear text.
- The command Georgia(config-router)#exit will allow you to exit the authentication process.
- The next command to enter in the interface is Georgia(config)#int fa0/0.
- The command Georgia(config-if)#ip ospf authentication-key jasmine will allow you to set the password for your authentication process to jasmine. You can choose any other word to set the password. You can also make it more complex so that it defies any cracking attempts.

MD5 Authentication

- The command Georgia(config)#router ospf 456 will allow you to kick off the process of authentication using MD5.
- The command Georgia(config-router)#area 0 authentication message-digest will allow you to enable the authentication process with MD5 password encryption.
- The command Georgia(config-router)#exit will allow you to exit the process at any time.
- The next command on the line is Georgia(config-router)#int fa 0/0.
- The command Georgia(config-if)#ip ospf message-digest-key 1

md5 jasmine will allow you to encrypt the password that you have filled in the interface. In the command 1 is the key-id. This value remains the same. The key and password must remain the same for any neighboring router.

Timers

- The command Georgia(config-if)#ip ospf hello-interval timer 30 will allow you to change the Hello interval to 30 seconds. You can change the timing as per your custom requirements.
- The command Georgia(config-if)#ip ospf dead-interval 90 will allow you to change the dead interval to 90 seconds. You can fill it in with any other amount of seconds.

Default Route

- The command Georgia(config)#ip route 0.0.0.0 0.0.0.0 s0/0 will allow you to create a default route in the system. After you have entered the abovementioned command, you can fill in the system with the following command Georgia(config)#router ospf 1 to further the process of creating default routes.
- The command Georgia(config-router)#default-information-originate will allow you to set the default route so that it can be propagated across the OSPF routers.

OSPF Configuration Verification

- The command Georgia#show ip protocol will allow you to see the parameters for different protocols that are running on the routers.
- The command Georgia#show ip route will allow you to see the full IP routing tables.
- The command Georgia#show ip ospf will allow you to see the basic information of the network.
- The command Georgia#show ip ospf interface will allow you to see the information about OSPF because the same is related to all

the interfaces that exist on the system.

- The command Georgia#show ip ospf int fa 0/0 will allow you to see the OSPF information for the interface titled fa 0/0.
- The command Georgia#show ip ospf neighbor will allow you to see the list of all the OSPF neighbors and their respective states.
- The command Georgia#show ip ospf neighbor detail will allow you to see all the neighbors' detailed lists in the network system.
- The command Georgia#show ip ospf database will allow you to see the contents of the OSPF database.

Troubleshooting Process

- The command Georgia#clear ip route * will allow you to clear the routing table. It forces the users to rebuild the table. In that way, the problem is automatically killed.
- The command Georgia#clear ip route x.x.x.x will allow you to clear a specific route to the network x.x.x.x.
- The command Georgia#clear ip ospf counters will allow you to clear and reset the OSPF counters.
- The command Georgia#clear ip ospf process will allow you to reset the OSPF process. This forces the OSPF to recreate the neighbors, routing tables and databases. This is how the problem is tackled and erased completely from the system.
- The command Georgia#debug ip ospf events will allow you to see OSPF events in the system. This is how you can correct any problem that pops up along the way.
- The command Georgia#debug ip ospf packets will allow you to see the OSPF packets.
- The command Georgia#debug ip ospf adj will allow you to see different states of OSPF.

Chapter Six

Open Shortest Path Protocol (OSPF) Single Area and Multiarea Configuration

This chapter will walk you through the configuration processes of single area OSPF and multiarea OSPF. I will explain each configuration process by neatly stating the step-by-step commands.

Single Area OSPF Configuration

The configuration of a single area OSPF system comprises the following steps.

- The command Router>en is the first step to kick off the configuration process.
- The command Router#config t is the second step. It will land you in the configuration mode.
- The command Router(config)#no ip domain-lookup will allow you to turn off the DNS queries so that the spelling mistakes will never allow you to slow down.
- The command Router(config)#hostname Georgia will allow you to set up the name of the host.
- The command Georgia(config)#line con 0 is the next step on the line.
- The command Georgia(config-line)#logging sync will allow you to list the commands that are interrupted by the console messages and append them to a new line.
- The command Georgia(config-line)#exit will is the next step on the line.
- The command Georgia(config)#int fa 0/0 will allow you to set up Fast Ethernet.

- The command Georgia(config-if)#ip add 172.16.10.1 255.255.255.0 will allow you to set up the system's IP address.
- The command Georgia(config-if)#no shut is the step for the configuration.
- The command Georgia(config-if)#int s0/0 is the next step.
- The command Georgia(config-if)#ip add 172.16.20.1 255.255.255.0 will allow you to set up and add another IP address for the system.
- The command Georgia(config-if)#clock rate 56000 will allow you to set up and connect the DCE cable to your interface.
- The next command to enter the system is Georgia(config-if)#no shut.
- The command Georgia(config-if)#exit will allow you to exit the previous state.
- The command Georgia(config)#route ospf 1 will allow you to turn on the OSPF process 1.
- The command Georgia(config-router)#net 172.16.10.0.0.0.255 area 0 will allow you to pair up any interface that has an address of 172.10.10.x with area 0.
- The command Georgia(config-router)#net 172.16.20.0.0.0.255 area 0 will allow you to pair up any interface that has an address of 172.16.10.x with area 0.
- The command Georgia(config-router)#Ctrl + Z is the second last command to apply for the configuration process.
- The command Georgia#copy run start will finish the configuration process.

Multi-area OSPF

OSPF uses different types of messages. A few of them are given as under. Each OSPF packet is packed up inside an IP header.

- The first type of OSPF messages is named Hello. The message is used to discover the neighbors and it also builds the adjacencies that are between them.
- The second type of OSPF messages is named Database description (DBD). The message is used to check for the synchronization of the database between the routers.
- The third type of OSPF messages is named Link-state request (LSR). The message is used to request specific link-state advertisements (LSAs) from a different router.
- The fourth type of OSPF messages is named Link-state update(LSU). The message is used to send off the specifically requested LSAs.
- The fifth type of OSPF messages is named Link-state acknowledgment (LSAck). The message is used to acknowledge the different types of packets.

LSA Types

In the next section, I will explain the different types of LSA that the OSPF uses. LSAs are considered as the building blocks of the OSPF link-state database (LSDB). LSAs act as database records. They describe the topology of the OSPF network area.

- The first type of LSA is Router LSA. It describes the router link state to area. It remains flooded in a single area.
- The second type of LSA is Network LSA. Designated routers generate this type. It is also flooded in a single area.
- The third type of LSA is Summary LSA. This type is used by area Border Router (ABR). It is also used to harvest information that is collected from one area. It also summarizes it for a different area.
- The fourth type of LSA is ASBR summary LSA. It tends to inform the OSPF domain on how to approach the ASBR.
- The fifth type of LSA is Autonomous system LSA. Its

description is that ASBR generates it. These types of LSAs describe the routes to the destinations that are generally external to the systems that operate autonomously.

- The sixth type of LSA is Group membership LSA. Its description is that it is used in multicast OSPF apps. Multicast apps or MOSPF apps have been deprecated.
- The seventh type of LSA is NSSA external link entry LSA. Its description is it is used in the special types of areas are known as not-so-stubby-area (NSSA). It tends to advertise the external routes in the NSSA.
- The eighth type of LSA is Link-local LSA for OSPFv3. Its description is that it yields information about the link-local addresses in addition to displaying a list of IPv6 addresses on the link. It is generally not supported by Cisco.
- The ninth type of LSA is Opaque LSA. This LSA is reserved for future usage.
- The tenth type of LSA is Opaque LSA. This LSA is reserved for future usage.
- The eleventh type of LSA is Opaque LSA. This LSA is reserved for future usage.

OSPF Configuration

There are a few steps involved in the configuration process of OSPF. The steps are given below.

- The command Georgia(config)#router ospf 555 will allow you to initiate the OSPF process 555. The ID can be a positive integer between 1 and 65,535. The process ID is never related to the OSPF area. The process ID distinguishes one process from another one inside of the device.
- The command Georgia(config-router)#network 172.16.10.0 0.0.0.0255 area 0 will allow you to use the wildcard mask to determine which interfaces you can advertise. Any interface that

has an address of 172.16.10.x will run the OSPF. It can also be put into area 0.

- The command Georgia(config-router)#log-adjacency-changes detail will allow you to configure routers to some syslog messages whenever there is some change of state inside the OSPF neighbors.

You can use different wildcard masks with OSPF areas. When you compare it with an IP address, a wildcard mask will help you locate what addresses will be matched up to run the OSPF and also be placed inside a particular area.

- The zero(0) in the wildcard mask means checking the corresponding bit within the address to make a perfect match.
- The one(1) in the wildcard mask means ignorance of the corresponding bit within the address.

The following commands will do the trick for you.

- The command Georgia(config-router)# network 172.16.0.1 0.0.0.0 area 0 will allow you to confirm that any interface that possesses the address 172.16.10.1 will run OSPF and will also be placed inside area 0.
- The command Georgia(config-router)# network 172.16.0.0 0.0.255.255 area 0 will allow you to confirm that any interface that possesses the address 172.16.y.y will run OSPF and will also be placed inside area 0.
- The command Georgia(config-router)# network 0.0.0.0 255.255.255.255 area 0 will allow you to confirm that any interface that any possesses address type will run OSPF and will also be placed inside area 0.

Multiarea OSPF Configuration

Georgia Router:

- The command Router> enable will allow you to shift to the

privileged mode.

- The command Router#configure terminal will allow you to shift to the global configuration mode.
- The command Router(config)#hostname Georgia will allow you to set up the name of the router.
- The command Georgia(config)#interface loopback0 will allow you to enter the mode of the loopback interface.
- The command Georgia(config-if)#ip address (enter ip address here) will allow you to assign the IP address and the netmask to the network.
- The command Georgia(config-if)#description Router ID will allow you to set up a locally significant description.
- The command Georgia(config-if)#exit will allow you to shift back to the global configuration mode.
- The command Georgia(config)#ip route 0.0.0.0 0.0.0.0 10.1.0.2 fastethernet0/1 will allow you to create a default route. If you use the next-hop address and exit interface on a Fast Ethernet interface, you will be able to prevent the recursive look-ups within the routing table.
- The command Georgia(config)#ip route 11.0.0.0 0.0.0.0 null0 will allow you to create a kind of static route to the null interface. This example shows you the routes that represent some remote simulated destination.
- The command Georgia(config)#ip route 12.0.0.0 0.0.0.0 null0 will allow you to create a kind of static route to the null interface. This example shows you the routes that represent some remote simulated destination.
- The command Georgia(config)#ip route 13.0.0.0 0.0.0.0 null0 will allow you to create a kind of static route to the null interface. This example shows you the routes that represent some remote simulated destination.

- The command Georgia(config)#router ospf1 will allow you to kick off OSPF 1.
- The command Georgia(config-router)#network 172.16.0.0 0.0.255.255 area 0 will ensure that the interface with the IP address 172.16.y.y will operate OSPF it will also be put in area 0.
- The command Georgia(config-router)#default-information originate will allow you to set up the default route that must be propagated to the OSPF routers.
- The command Georgia(config-router)#redistribute static will allow you to redistribute the OSPF process's static routes. This will turn the router into Georgia because the static routes are usually not a part of OSPF. The definition of Georgia is a router that usually sits in between OSPF and the static routing process.
- The command Georgia(config-router)#exit will take you back to the global configuration mode.
- The command Georgia(config)#exit will allow you to get back to the privileged mode.
- The command Georgia#copy running-config startup-config will allow you to save your network configuration to NVRAM.

Georgia1 Router:

- The command Router> enable will allow you to shift to the privileged mode.
- The command Router#configure terminal will allow you to shift to the global configuration mode.
- The command Router(config)#hostname Georgia1 will allow you to set up the name of the router.
- The command Georgia1(config)#interface loopback0 will allow you to enter the mode of the loopback interface.
- The command Georgia1(config-if)#ip address (enter ip address

here) will allow you to assign the IP address and the netmask to the network.

- The command Georgia1(config-if)#description Router ID will allow you to set up a locally significant description.
- The command Georgia1(config-if)#exit will allow you to shift back to the global configuration mode.
- The command Georgia1(config-if)#interface fastethernet0/1 will allow you to shift back to the interface configuration mode.
- The command Georgia1(config-if)#ip ospf priority 200 will set up the priority for BDR and DR election processes. The router is likely to win and become the DR.
- The command Georgia1(config-if)#no shutdown will allow you to shift back to the interface mode.
- The command Georgia1(config-if)#exit will allow you to reenter the global configuration mode.
- The command Georgia1(config)#router ospf1 will allow you to kick off OSPF 1.
- The command Georgia1(config)#ip route 0.0.0.0 0.0.0.0 10.1.0.2 fastethernet0/1 will allow you to create a default route. If you use next-hop address and exit interface on a Fast Ethernet interface, you will be able to prevent the recursive look-ups within the routing table.
- The command Georgia1(config-router)#network 172.16.1.0 0.0.0.255 area 0 will ensure that the interface that has the IP address 172.16.1.y will operate OSPF and it will also be put in area 0.
- The command Georgia1(config-router)#network 172.16.51.1 0.0.0.0 area 51 will ensure that the interface that has the IP address 172.16.51.1 will operate OSPF and it will also be put in area 51.
- The command Georgia1(config-router)#exit will take you back

to the global configuration mode.

- The command Georgia1(config)#exit will allow you to get back to the privileged mode.
- The command Georgia1#copy running-config startup-config will allow you to save your network configuration to NVRAM.

Georgia2 router:

- The command Router> enable will allow you to shift to the privileged mode.
- The command Router#configure terminal will allow you to shift to the global configuration mode.
- The command Router(config)#hostname Georgia2 will allow you to set up the name of the router.
- The command Georgia2(config)#interface loopback0 will allow you to enter the mode of the loopback interface.
- The command Georgia2(config-if)#ip address (enter ip address here) will allow you to assign the IP address and the netmask to the network.
- The command Georgia2(config-if)#description Router ID will allow you to set up a locally significant description.
- The command Georgia2(config-if)#exit will allow you to shift back to the global configuration mode.
- The command Georgia2(config-if)#interface fastethernet0/0 will allow you to shift back to the interface configuration mode.
- The command Georgia2(config-if)#ip ospf priority 100 will set up the priority for BDR and DR election processes. The router is likely to win and become the DR.
- The command Georgia2(config-if)#no shutdown will allow you to shift back to the interface mode.

- The command Georgia2(config-if)#exit will allow you to reenter the global configuration mode.
- The command Georgia2(config)#router ospf1 will allow you to kick off OSPF 1.
- The command Georgia2(config)#ip route 0.0.0.0 0.0.0.0 10.1.0.2 fastethernet0/1 will help you create a default route. If you use next-hop address and exit interface on a Fast Ethernet interface, you will be able to prevent the recursive look-ups within the routing table.
- The command Georgia2(config-router)#network 172.16.1.0 0.0.0.255 area 0 will ensure that the interface that has the IP address 172.16.1.y will operate OSPF and it will also be put in area 0.
- The command Georgia2(config-router)#network 172.16.10.14 0.0.0.3 area 1 will ensure that the interface with the IP address 172.16.10.4—7 will operate OSPF it will also be put in area 1.
- The command Georgia2(config-router)#area 1 stub will allow you to make area 1 stub area. The LSA type 4 and 5s are usually blocked. They are generally not sent into area 1. Usually, a default route is placed into the stub area. It points to Georgia1.
- The command Georgia2(config-router)#exit will take you back to the global configuration mode.
- The command Georgia2(config)#exit will allow you to get back to the privileged mode.
- The command Georgia2#copy running-config startup-config will allow you to save your network configuration to NVRAM.

GeorgiaInt Router:

- The command Router> enable will allow you to shift to the privileged mode.
- The command Router#configure terminal will allow you to shift

to the global configuration mode.

- The command Router(config)#hostname GeorgiaInt will allow you to set up the name of the router.
- The command GeorgiaInt(config)#interface loopback0 will allow you to enter the mode of loopback interface.
- The command GeorgiaInt(config-if)#ip address (enter ip address here) will allow you to assign the IP address and the netmask to the network.
- The command GeorgiaInt(config-if)#description Router ID will allow you to set up a description that is locally significant.
- The command GeorgiaInt(config-if)#exit will allow you to shift back to the global configuration mode.
- The command GeorgiaInt(config-if)#exit will allow you to reenter the global configuration mode.
- The command GeorgiaInt(config)#router ospf1 will allow you to kick off OSPF 1.
- The command GeorgiaInt(config-router)#network 172.16.0.0 0.0.255.255 area 1 will ensure that the interface that has the IP address 172.16.y.y will operate OSPF and it will also be put in area 0.
- The command GeorgiaInt(config-router)#area 1 stub will allow you to make area 1 stub area.
- The command GeorgiaInt(config-router)#exit will take you back to the global configuration mode.
- The command GeorgiaInt(config)#exit will allow you to get back to the privileged mode.
- The command GeorgiaInt#copy running-config startup-config will allow you to save your network configuration to NVRAM.

Loopback Interfaces

- The command Georgia(config)#interface loopback0 will allow you to create a type of virtual interface named Loopback 0. It then shifts the router to the configuration mode of the interface.
- The command Georgia(config-if)#ip address (Ip address) will allow you to assign an IP address to your interface. The loopback interfaces are all the time up. They do not go down unless you shut them down manually. This is why loopback interfaces are great for usage as OSPF router ID.

Router ID

- The command Georgia(config)#router ospf 1 will allow you to kick off process 1.
- The command Georgia(config-router)#router-id 10.1.1.1 will allow you to set up the router ID and fix it to 10.1.1.1. If you use the command on the OSPF router process that is active already, the new router ID will be used at the next reload. It will also be used for the manual restart of the OSPF process.
- The command Georgia(config-router)#no router-id 10.1.1.1 will allow you to remove your static router ID from the process of configuration. If you use the command on the ODPF router process that is active already, the old router ID will be used at the upcoming reload or at the manual restart of the OSPF process.

If you want to choose the router ID at the point of the initialization of the OSPF process, the router will use the following criteria in a particular order.

- You should use the router ID that is specified in the command regarding the router-id ip address.
- You should use the highest IP address among the active loopback interfaces that present are on the router.
- You should use the highest IP address among the active nonloopback interfaces that are present on the router.

DR/BDR Elections

- The command Georgia(config)#interface fastethernet0/0 will allow you to enter into the interface's configuration mode.
- The command Georgia(config-if)#ip ospf priority 100 will allow you to change the priority of the ospf interface to 100. You can set the priority at any figure between 0 and 255. The priority of 0 will make the router ineligible to create a designated router (DR). The highest priority will win the election and become the DR. The one that comes at the second slot will win the position of BDR. If all the routers on a network have the same priority, there will be a tie. You can break up a tie by the highest router ID. The default setting for the priorities is set at 1.

Passive Interfaces

- The command Georgia(config)#router ospf 1 will allow you to kick off the OSPF process 1.
- The command Georgia(config-router)#network 172.16.10.0 0.0.0.255 area 0 will allow you to put the interface with the address 172.16.10.y into area 0.
- The command Georgia(config-router)#passive-interface fastethernet0/0 will disable the process of sending OSPF packets on your interface.
- The command Georgia(config-router)#passive-interface default will disable the process of sending OSPF packets on all the interfaces in the system.
- The command Georgia(config-router)#no passive-interface serial 0/0/1 will enable the process of sending OSPF packets to interface serial0/0/1. That’s how it allows the neighbor adjacencies to formulate.

Cost Metrics

- The command Georgia(config)#interface will land you in the mode of configuration of your interface.
- The command Georgia(config-if)#bandwidth 256 will let you

change the bandwidth of your network. If you change it, the OSPF will allow you to recalculate the link cost.

Configuration: OSPF Single Area

In the following section, I will show network topology for single-area OSPF. I will state all the relevant commands to single-area OSPF.

Georgia1 router:

- The command Georgia1(config)#router ospf1 will allow you to kick off OSPF 1.
- The command Georgia1(config-router)#network 172.16.10.0 0.0.255.255 area 0 will ensure that the interface that has the IP address 172.16.y.y will operate OSPF and it will also be put in area 0.
- The command Georgia1(config-router)#network 172.16.20.0 0.0.255.255 area 0 will ensure that the interface that has the IP address 172.16.y.y will operate OSPF and it will also be put in area 0.
- The command Georgia1(config-router)#<CTRL> z will take you back to the network system's privileged mode.
- The command Georgia1#copy running-config startup-config will allow you to save your network configuration to NVRAM.

Georgia2:

- The command Georgia1(config)#router ospf1 will allow you to kick off OSPF 1.
- The command Georgia1(config-router)#network 172.16.10.0. 0.0.255.255 area 0 will ensure that the interface that has the IP address 172.16.y.y will operate OSPF and it will also be put in area 0.
- The command Georgia1(config-router)#<CTRL> z will take you back to the network system's privileged mode.

- The command Georgia1#copy running-config startup-config will allow you to save your network configuration to NVRAM.

Georgia3:

- The command Georgia1(config)#router ospf1 will allow you to kick off OSPF 1.
- The command Georgia1(config-router)#network 172.16.40.2 0.0.0.0 area 0 will ensure that the interface that has the IP address 172.16.40.2 will operate OSPF and it will also be put in area 0.
- The command Georgia1(config-router)#network 172.16.50.1 0.0.0.0 area 0 will ensure that the interface that has the IP address 172.16.50.1 will operate OSPF and it will also be put in area 0.
- The command Georgia1(config-router)#<CTRL> z will take you back to the network system's privileged mode.
- The command Georgia1#copy running-config startup-config will allow you to save your network configuration to NVRAM.

OSPF Single Area Configuration

I will use three routers and set up the commands accordingly.

Georgia:

- The command Georgia(config)#router ospf1 will allow you to initiate the OSPF 1 process.
- The command Georgia(config-router)#network 172.16.10.0 0.0.0.255 area 0 will ensure that the interface that has the IP address 172.16.10.y will operate OSPF and it will also be put in area 0.
- The command Georgia(config-router)#network 172.16.20.0 0.0.0.255 area 0 will ensure that the interface with the IP address 172.16.20.y will operate OSPF it will also be put in area 0.
- The command Georgia(config)#<CTRL> z will allow you to get back to the privileged mode.

- The command Georgia#copy running-config startup-config will allow you to save your network configuration to NVRAM.

Georgia1:

- The command Georgia1(config)#router ospf1 will allow you to initiate the OSPF 1 process.
- The command Georgia1(config-router)#network 172.16.0.0 0.0.255.255 area 0 will ensure that the interface with the IP address 172.16.y.y will operate OSPF and it will also be put in area 0.
- The command Georgia1(config)#<CTRL> z will allow you to get back to the privileged mode.
- The command Georgia1#copy running-config startup-config will allow you to save your network configuration to NVRAM.

Georgia3:

- The command Georgia3(config)#router ospf1 will allow you to initiate the OSPF 1 process.
- The command Georgia3(config-router)#network 172.16.40.2 0.0.0.0 area 0 will ensure that the interface with the IP address 172.16.40.2 will operate OSPF and it will also be put in area 0.
- The command Georgia3(config)#<CTRL> z will allow you to get back to the privileged mode.
- The command Georgia3#copy running-config startup-config will allow you to save your network configuration to NVRAM.

Chapter Seven

Open Shortest Path Protocol (OSPF) Area and Network Types

This chapter will walk you through the OSPF area types and network types. You will learn the commands for different areas and networks related to OSPF.

OSPF Special Area Types

In this section, I will explain the different areas of OSPF. Generally, they are four in total. Stub areas, totally stubby area, totally NSSA and not-so-stubby areas (NSSAs) are the four major categories discussed in this section.

Stub Areas

- The command ABR (config)#router ospf 1 will kick off the OSPF process 1.
- The command ABR (config-router)#network 172.16.10.0 0.0.0.255 area 0 will allow you to confirm that any interface that possesses the address 172.16.10.y will run OSPF and will also be placed inside area 0.
- The command ABR (config-router)#network 172.16.20.0 0.0.0.255 area 51 will allow you to confirm that any interface that possesses the address 172.16.20.y will run OSPF and will also be placed inside area 51.
- The command ABR (config-router)#area 51 stub will allow you to label area 51 as the stub area.
- The command ABR (config-router)#area 51 default-cost 10 will explain the cost of the default router sent into the stub area. The default value is 1. This is considered an optional command and you can use it at will.
- The command ABR (config)#router ospf 1 will allow you to kick

off the OSPF process 1.

- The command Internal(config-router)#network 172.16.20.0 0.0.0.255 area 51 will allow you to confirm that any interface that possesses the address 172.16.20.y will run OSPF and will also be placed inside area 51.
- The command Internal(config-router)#area 51 stub will label area 51 as the stub area. That's how the shift in area is made possible. All the routers inside the stub area ought to be configured with area x stub command.

Totally Stubby Areas

- The command ABR (config)#router ospf 1 will kick off the OSPF process 1.
- The command ABR (config-router)#network 172.16.10.0 0.0.0.255 area 0 will allow you to confirm that any interface that possesses the address 172.16.10.y will run OSPF and will also be placed inside area 0.
- The command ABR (config-router)#network 172.16.20.0 0.0.0.255 area 51 will allow you to confirm that any interface that possesses the address 172.16.20.y will run OSPF and will also be placed inside area 51.
- The command ABR (config-router)#area 51 stub no-summary will allow you to label area 51 as the totally stub area.
- The command ABR (config)#router ospf 1 will allow you to kick off the OSPF process 1.
- The command ABR (config-router)#network 172.16.20.0 0.0.0.255 area 51 will allow you to confirm that any interface that possesses the address 172.16.20.y will run OSPF and will also be placed inside area 51.
- The command ABR (config-router)#area 51 stub will label area 51 as the stub area. That's how the shift in area is made possible. As all the internal routers in the particular area are configured

with area x nssa command, the ABR router is configured with area x nssa no-summary command

Not-So-Stubby Areas

- The command ABR (config)#router ospf 1 will kick off the OSPF process 1.
- The command ABR (config-router)#network 172.16.10.0 0.0.0.255 area 0 will allow you to confirm that any interface that possesses the address 172.16.10.y will run OSPF and will also be placed inside area 0.
- The command ABR (config-router)#network 172.16.20.0 0.0.0.255 area 1 will allow you to confirm that any interface that possesses the address 172.16.20.y will run OSPF and will also be placed inside area 1.
- The command ABR (config-router)#area 1 nssa will allow you to label area 1 as the no-so-stubby-area.
- The command Internal(config)#router ospf 1 will allow you to initiate the OSPF process 1.
- The command Internal(config-router)#network 172.16.20.0 0.0.0.255 area 1 will allow you to confirm that any interface that possesses the address 172.16.20.y will run OSPF and will also be placed inside area 1.
- The command Internal(config-router)#area 1 nssa will label area 1 as the not-so-stubby-area.

Totally NSSA

- The command ABR (config)#router ospf 1 will kick off the OSPF process 1.
- The command ABR (config-router)#network 172.16.10.0 0.0.0.255 area 0 will allow you to confirm that any interface that possesses the address 172.16.10.y will run OSPF and will also be placed inside area 0.

- The command ABR (config-router)#network 172.16.20.0 0.0.0.255 area 11 will allow you to confirm that any interface that possesses the address 172.16.20.y will run OSPF and will also be placed inside area 11.
- The command ABR (config-router)#area 11 nssa no-summary will allow you to label area 11 as the totally nssa.
- The command Internal(config)#router ospf 1 will allow you to kick off the OSPF process 1.
- The command Internal(config-router)#network 172.16.20.0 0.0.0.255 area 11 will allow you to confirm that any interface that possesses the address 172.16.20.y will run OSPF and will also be placed inside area 11.
- The command Internal(config-router)#area 11 nssa will label area 11 as NSSA. As all the internal routers in the particular area are configured with area x nssa command, the ABR router is configured with area x nssa no-summary command.

OSPF Network Types

The OSPF network types ought to be described as a Cisco proprietary or as RFC complaint.

Full-Mesh Frame Relay: NBMA for Physical Interfaces

- The command Georgia(config)#router ospf 1 will let you start the OSPF process 1.
- The command Georgia(config-router)#neighbor 10.1.1.2 will let you identify the neighboring router.
- The command Georgia(config-router)#exit will let you get back to the network system's mode of global configuration.
- The command Georgia(config)#interface serial0/0/0 will let you switch to the mode of interface configuration.
- The command Georgia(config-if)#encapsulation frame-relay will let you enable the frame relay on your interface.

- The command Georgia(config-if)#ip address (ip address) will let you assign a particular IP address as well as a netmask to your interface.
- The command Georgia(config-if)#ip ospf network non-broadcast will let you define the OSPF nonbroadcast network type. This is known as the default on the physical interfaces.
- The command Georgia(config-if)#frame-relay map ip 10.1.1.2.100 will let you map out a remote IP address to the data-link connection identifier (DLCI) 100.
- The command Georgia(config-if)#frame-relay map ip 10.1.1.3 200 will let you map out a remote IP address to DLCI 200. When you are using the neighbor command, it will allow for the OSPF router to trade routing information in the absence of multicasts. Instead, you can use unicasts to the IP address that is manually entered.

Broadcast on the Physical Interfaces

- The command Georgia(config)#interface serial0/0/0 will let you switch to the mode of interface configuration.
- The command Georgia(config-if)#encapsulation frame-relay will let you enable the frame relay on your interface.
- The command Georgia(config-if)#ip address (ip address) will let you assign a particular IP address as well as a netmask to your interface.
- The command Georgia(config-if)#ip ospf network non-broadcast will let you define the OSPF nonbroadcast network type. This is known as the default on the physical interfaces.
- The command Georgia(config-if)#frame-relay map ip 10.1.1.2.100 will let you map out a remote IP address to the data-link connection identifier (DLCI) 100.
- The command Georgia(config-if)#frame-relay map ip 10.1.1.3 200 will let you map out a remote IP address to DLCI 200. When

you are using the neighbor command, it will allow for the OSPF router to trade routing information in the absence of multicasts. Instead, you can use unicasts to the IP address that is manually entered.

- The command Georgia(config-if)#no shutdown will let you enable your interface.
- The command Georgia(config-if)#network 10.1.1.0 0.0.0.255 area 0 will let you confirm that any interface that possesses the address 10.1.1.y will run OSPF and will also be placed inside area 0.

Point-to-Multipoint Networks

- The command Georgia(config)#interface serial0/0/0 will let you switch to the mode of interface configuration.
- The command Georgia(config-if)#encapsulation frame-relay will let you enable the frame relay on your interface.
- The command Georgia(config-if)#ip address (ip address) will let you assign a particular IP address as well as a netmask to your interface.
- The command Georgia(config-if)#ip ospf network point-to-multipoint will let you change the type of the network to point-to-multipoint network.
- The command Georgia(config-if)#exit will take you back to the mode of global configuration.
- The command Georgia(config)#router ospf 1 will let you start the OSPF process 1.
- The command Georgia(config-if)#network 10.1.1.0 0.0.0.255 area 0 will let you confirm that any interface that possesses the address 10.1.1.y will run OSPF and will also be placed inside area 0.
- The command Georgia(config-if)#neighbor 10.1.1.2 will let you detect the neighbor router.

- The command Georgia(config-if)#exit will take you back to the mode of global configuration.
- The command Georgia(config)#interface serial0/0/0 will let you switch to the mode of interface configuration.
- The command Georgia(config-if)#ip ospf network point-to-multipoint non-broadcast will let you create and enter a point-to-multipoint network mode that is non-broadcast as well. The point-to-multipoint non-broadcast mode is a kind of Cisco extension to RFC-compliant mode. The neighbors in the network ought to be manually defined in this specific mode. The BDRs/DR will not be used in this specific mode. The point-to-multipoint non-broadcast mode can be used in some special cases in which neighbors are not supposed to be discovered automatically.

Point-to-Point Networks

- The command Georgia(config)#interface serial0/0/0 will let you switch to the mode of interface configuration.
- The command Georgia(config-if)#encapsulation frame-relay will let you enable the frame relay on your interface.
- The command Georgia(config-if)#no shutdown will let you enable your interface.
- The command Georgia(config)#interface serial0/0/0.300 point-to-point will let you create a subinterface 300 and make it onwards a point-to-point network. This is a kind of default mode.
- The command Georgia(config-subif)#ip address (ip address) will let you assign a particular IP address as well as a netmask to your interface.
- The command Georgia(config-subif)#frame-relay interface-dlci 300 will let you map out and assign the DLCI 300 to your subinterface.
- The command Georgia(config-subif)#interface serial0/0/0.400

point-to-point will let you define and create subinterfaces 400 and make them point-to-point networks.

- The command Georgia(config-subif)#ip address (ip address) will let you assign a particular IP address as well as a netmask to your interface.
- The command Georgia(config-subif)#frame-relay interface-dlci 400 will let you map out and assign DLCI 400 to your subinterface.
- The command Georgia(config-subif)#exit will take you back to the mode of interface configuration.
- The command Georgia(config-if)#exit will take you back to the mode of global configuration.

OSPF and NBMA Topology

The broadcast mode of OSPF will have partial or full mesh NBMA preferred topology. The subnet address will remain the same while the hello timer will be 10 seconds. The adjacency will be automatic, DR/BDR elected and the network will be cisco.

The nonbroadcast mode of OSPF will have partial or full mesh NBMA preferred topology. The subnet address will remain the same while the hello timer will be 30 seconds. The adjacency will be manual configuration and DR/BDR elected, and the network will be RFC.

The point-to-multipoint mode of OSPF will have partial or star mesh NBMA preferred topology. The subnet address will remain the same while the hello timer will be 30 seconds. The adjacency will be automatic, DR/BDR elected and the network will be RFC.

The point-to-point multipoint nonbroadcast mode of OSPF will have partial or full mesh NBMA preferred topology. The subnet address will remain the same while the hello timer will be 30 seconds. The adjacency will be manual configuration and DR/BDR elected, and the network will be cisco.

The point-to-point mode of OSPF will have partial or full mesh NBMA preferred topology. The subnet address will be different for all the interfaces

while the hello timer will be 10 seconds. The adjacency will be automatic, DR/BDR elected and the network will be cisco.

OSPF and NBMA Networks

In the following section, I will explain how you can configure OSPF on the NBMA network by using the following commands. In the network, there will be four routers that will be connected to a frame relay. Each router will have a set of commands to run the network effectively.

Georgia1 Router:

- The command Georgia1(config)#interface serial0/0/0 will allow you to enter the configuration mode.
- The command Georgia1(config-if)#encapsulation frame-relay will allow you to enable the Frame Relay Encapsulation on the network.
- The command Georgia1(config-if)#ip address (enter ip address here) will allow you to assign a particular IP address and netmask to the system.
- The command Georgia1(config-if)#frame-relay map ip (enter ip address here) 50 will allow you to map out a remote IP address to the local DLCI 50.
- The command Georgia1(config-if)#frame-relay map ip (enter ip address here) 51 will allow you to map out a remote IP address to the local DLCI 51.
- The command Georgia1(config-if)#frame-relay map ip (enter ip address here) 52 will allow you to map out a remote IP address to the local DLCI 52.
- The command Georgia1(config-if)#ip ospf priority 10 will allow you to change your OSPF interface priority into 10.
- The command Georgia1(config-if)#no shutdown will allow you to enable your interface on the network.
- The command Georgia1(config-if)#exit will allow you to shift

back to the global configuration mode.

- The command Georgia1(config)#router ospf1 will allow you to kick off OSPF 1.
- The command Georgia1(config-router)#network 172.16.0.0 0.0.255.255 area 0 will ensure that the interface that has the IP address 172.16.y.y will operate OSPF and it will also be put in area 0.
- The command Georgia1(config-router)#neighbor 172.16.2.2 will allow you to identify the neighbor to Georgia1. In this case the neighbor is Georgia2.
- The command Georgia1(config-router)#neighbor 172.16.2.3 will allow you to identify the neighbor to Georgia1. In this case the neighbor is Georgia3.
- The command Georgia1(config-router)#neighbor 172.16.2.4 will allow you to identify the neighbor to Georgia1. In this case the neighbor is Georgia4.
- The command Georgia1(config-router)#exit will take you back to the global configuration mode.
- The command Georgia1(config)#exit will allow you to get back to the privileged mode.
- The command Georgia1#copy running-config startup-config will allow you to save your network configuration to NVRAM.

Georgia2 Router:

- The command Georgia2(config)#interface serial0/0/0 will allow you to enter the configuration mode.
- The command Georgia2(config-if)#encapsulation frame-relay will allow you to enable the Frame Relay Encapsulation on the network.
- The command Georgia2(config-if)#ip address (enter ip address here) will allow you to assign a particular IP address and

netmask to the system.

- The command Georgia2(config-if)#frame-relay map ip (enter ip address here) 50 will allow you to map out a remote IP address to the local DLCI 50.
- The command Georgia2(config-if)#frame-relay map ip (enter ip address here) 150 will allow you to map out a remote IP address to the local DLCI 150.
- The command Georgia2(config-if)#frame-relay map ip (enter ip address here) 150 will allow you to map out a remote IP address to the local DLCI 150.
- The command Georgia2(config-if)#ip ospf priority 0 will allow you to change your OSPF interface priority into 0.
- The command Georgia2(config-if)#no shutdown will allow you to enable your interface on the network.
- The command Georgia2(config-if)#exit will allow you to shift back to the global configuration mode.
- The command Georgia2(config)#router ospf1 will allow you to kick off OSPF 1.
- The command Georgia2(config-router)#network 172.16.0.0 0.0.255.255 area 0 will ensure that the interface that has the IP address 172.16.y.y will operate OSPF and it will also be put in area 0.
- The command Georgia2(config-router)#exit will take you back to the global configuration mode.
- The command Georgia2(config)#exit will allow you to get back to the privileged mode.
- The command Georgia2#copy running-config startup-config will allow you to save your network configuration to NVRAM.

Georgia3 router:

- The command Georgia3(config)#interface serial0/0/0 will allow you to enter the configuration mode.
- The command Georgia3(config-if)#encapsulation frame-relay will allow you to enable the Frame Relay Encapsulation on the network.
- The command Georgia3(config-if)#ip address (enter ip address here) will allow you to assign a particular IP address and netmask to the system.
- The command Georgia3(config-if)#frame-relay map ip 172.16.2.1 151 will allow you to map out a remote IP address to the local DLCI 151.
- The command Georgia3(config-if)#frame-relay map ip 172.16.2.2 151 will allow you to map out a remote IP address to the local DLCI 151.
- The command Georgia3(config-if)#frame-relay map ip 172.16.2.1 151 will allow you to map out a remote IP address to the local DLCI 151.
- The command Georgia3(config-if)#ip ospf priority 0 will allow you to change your OSPF interface priority into 0.
- The command Georgia3(config-if)#no shutdown will allow you to enable your interface on the network.
- The command Georgia3(config-if)#exit will allow you to shift back to the global configuration mode.
- The command Georgia3(config)#router ospf1 will allow you to kick off OSPF 1.
- The command Georgia3(config-router)#network 172.16.0.0 0.0.255.255 area 0 will ensure that the interface that has the IP address 172.16.y.y will operate OSPF and it will also be put in area 0.
- The command Georgia3(config-if)#ip ospf priority 0 will allow you to change your OSPF interface priority into 0.

- The command Georgia3(config-router)#exit will take you back to the global configuration mode.
- The command Georgia3(config)#exit will allow you to get back to the privileged mode.
- The command Georgia3#copy running-config startup-config will allow you to save your network configuration to NVRAM.

Georgia4 router:

- The command Georgia4(config)#interface serial0/0/0 will allow you to enter the configuration mode.
- The command Georgia4(config-if)#encapsulation frame-relay will allow you to enable the Frame Relay Encapsulation on the network.
- The command Georgia4(config-if)#ip address (enter ip address here) will allow you to assign a particular IP address and netmask to the system.
- The command Georgia4(config-if)#frame-relay map ip 172.16.2.1 152 will allow you to map out a remote IP address to the local DLCI 152.
- The command Georgia4(config-if)#frame-relay map ip 172.16.2.2 152 will allow you to map out a remote IP address to the local DLCI 152.
- The command Georgia4(config-if)#frame-relay map ip 172.16.2.3 152 will allow you to map out a remote IP address to the local DLCI 152.
- The command Georgia4(config-if)#ip ospf priority 0 will allow you to change your OSPF interface priority into 0.
- The command Georgia3(config-if)#no shutdown will allow you to enable your interface on the network.
- The command Georgia4(config-if)#exit will allow you to shift back to the global configuration mode.

- The command Georgia4(config)#router ospf1 will allow you to kick off OSPF 1.
- The command Georgia4(config-router)#network 172.16.0.0 0.0.255.255 area 0 will ensure that the interface that has the IP address 172.16.y.y will operate OSPF and it will also be put in area 0.
- The command Georgia4(config-router)#exit will take you back to the global configuration mode.
- The command Georgia4(config)#exit will allow you to get back to the privileged mode.
- The command Georgia4#copy running-config startup-config will allow you to save your network configuration to NVRAM.

OSPF and Broadcast Networks

Just like the NBMA network, we will use four routers to build a broadcast network. I will explain in detail the commands that are required to build and configure the network system.

Georgia 1:

- The command Georgia1(config)#interface serial0/0/0 will allow you to enter the configuration mode.
- The command Georgia1(config-if)#encapsulation frame-relay will allow you to enable the Frame Relay Encapsulation on the network.
- The command Georgia1(config-if)#ip address (enter ip address here) will allow you to assign a particular IP address and netmask to the system.
- The command Georgia1(config-if)#ip ospf network broadcast will allow you to switch your network's type from default nonbroadcast to the broadcast.
- The command Georgia1(config-if)#ip ospf priority 10 will allow you to change your OSPF interface priority into 10 for DR and

BDR election process.

- The command Georgia1(config-if)#frame-relay map ip 172.16.2.1 50 will allow you to map out a remote IP address to the local DLCI 50.
- The command Georgia1(config-if)#frame-relay map ip 172.16.2.1 51 will allow you to map out a remote IP address to the local DLCI 51.
- The command Georgia1(config-if)#frame-relay map ip 172.16.2.1 52 will allow you to map out a remote IP address to the local DLCI 52.
- The command Georgia1(config-if)#no shut will allow you to enable your interface on the network.
- The command Georgia1(config-if)#exit will allow you to shift back to the global configuration mode.
- The command Georgia1(config)#router ospf1 will allow you to kick off OSPF 1.
- The command Georgia1(config-router)#network 172.16.0.0 0.0.255.255 area 0 will ensure that the interface that has the IP address 172.16.y.y will operate OSPF and it will also be put in area 0.
- The command Georgia1(config-router)#exit will take you back to the global configuration mode.
- The command Georgia1(config)#exit will allow you to get back to the privileged mode.
- The command Georgia1#copy running-config startup-config will allow you to save your network configuration to NVRAM.

Georgia2 router:

- The command Georgia2(config)#interface serial0/0/0 will allow you to enter the configuration mode.

- The command Georgia2(config-if)#encapsulation frame-relay will allow you to enable the Frame Relay Encapsulation on the network.
- The command Georgia2(config-if)#ip address (enter ip address here) will allow you to assign a particular IP address and netmask to the system.
- The command Georgia2(config-if)#ip ospf network broadcast will allow you to switch your network's type from default nonbroadcast to the broadcast.
- The command Georgia1(config-if)#ip ospf priority 0 will allow you to change your OSPF interface priority into 0 for DR and BDR election process.
- The command Georgia2(config-if)#frame-relay map ip 172.16.2.1 150 will allow you to map out a remote IP address to the local DLCI 150.
- The command Georgia2(config-if)#frame-relay map ip 172.16.2.2 150 will allow you to map out a remote IP address to the local DLCI 150.
- The command Georgia2(config-if)#frame-relay map ip 172.16.2.3 150 will allow you to map out a remote IP address to the local DLCI 150.
- The command Georgia2(config-if)#no shut will enable your interface on the network.
- The command Georgia2(config-if)#exit will allow you to shift back to the global configuration mode.
- The command Georgia2(config)#router ospf1 will allow you to kick off OSPF 1.
- The command Georgia2(config-router)#network 172.16.0.0 0.0.255.255 area 0 will ensure that the interface that has the IP address 172.16.y.y will operate OSPF and it will also be put in area 0.

- The command Georgia2(config-router)#exit will take you back to the global configuration mode.
- The command Georgia2(config)#exit will allow you to get back to the privileged mode.
- The command Georgia2#copy running-config startup-config will allow you to save your network configuration to NVRAM.

Georgia3 router:

- The command Georgia3(config)#interface serial0/0/0 will allow you to enter the configuration mode.
- The command Georgia3(config-if)#encapsulation frame-relay will allow you to enable the Frame Relay Encapsulation on the network.
- The command Georgia3(config-if)#ip address (enter ip address here) will allow you to assign a particular IP address and netmask to the system.
- The command Georgia3(config-if)#ip ospf network broadcast will allow you to switch your network's type from default nonbroadcast to the broadcast.
- The command Georgia3(config-if)#ip ospf priority 0 will allow you to change your OSPF interface priority into 0 for DR and BDR election process.
- The command Georgia3(config-if)#frame-relay map ip 172.16.2.1 151 will allow you to map out a remote IP address to the local DLCI 151.
- The command Georgia3(config-if)#frame-relay map ip 172.16.2.2 151 will allow you to map out a remote IP address to the local DLCI 151.
- The command Georgia3(config-if)#frame-relay map ip 172.16.2.4 151 will allow you to map out a remote IP address to the local DLCI 151.

- The command Georgia3(config-if)#no shut will allow you to enable your interface on the network.
- The command Georgia3(config-if)#exit will allow you to shift back to the global configuration mode.
- The command Georgia3(config)#router ospf1 will allow you to kick off OSPF 1.
- The command Georgia3(config-router)#network 172.16.0.0 0.0.255.255 area 0 will ensure that the interface that has the IP address 172.16.y.y will operate OSPF and it will also be put in area 0.
- The command Georgia3(config-router)#exit will take you back to the global configuration mode.
- The command Georgia3(config)#exit will allow you to get back to the privileged mode.
- The command Georgia3#copy running-config startup-config will allow you to save your network configuration to NVRAM.

Georgia4 router:

- The command Georgia4(config)#interface serial0/0/0 will allow you to enter the configuration mode.
- The command Georgia4(config-if)#encapsulation frame-relay will allow you to enable the Frame Relay Encapsulation on the network.
- The command Georgia4(config-if)#ip address (enter ip address here) will allow you to assign a particular IP address and netmask to the system.
- The command Georgia4(config-if)#ip ospf network broadcast will allow you to switch your network's type from default nonbroadcast to the broadcast.
- The command Georgia4(config-if)#ip ospf priority 0 will allow you to change your OSPF interface priority into 0 for DR and

BDR election process.

- The command Georgia4(config-if)#frame-relay map ip 172.16.2.1 152 will allow you to map out a remote IP address to the local DLCI 152.
- The command Georgia4(config-if)#frame-relay map ip 172.16.2.2 152 will allow you to map out a remote IP address to the local DLCI 152.
- The command Georgia4(config-if)#frame-relay map ip 172.16.2.3 152 will allow you to map out a remote IP address to the local DLCI 152.
- The command Georgia4(config-if)#no shut will allow you to enable your interface on the network.
- The command Georgia4(config-if)#exit will allow you to shift back to the global configuration mode.
- The command Georgia4(config)#router ospf1 will allow you to kick off OSPF 1.
- The command Georgia4(config-router)#network 172.16.0.0 0.0.255.255 area 0 will ensure that the interface that has the IP address 172.16.y.y will operate OSPF and it will also be put in area 0.
- The command Georgia4(config-router)#exit will take you back to the global configuration mode.
- The command Georgia4(config)#exit will allow you to get back to the privileged mode.
- The command Georgia4#copy running-config startup-config will allow you to save your network configuration to NVRAM.

OSPF and Point-to-Multipoint Networks

Georgia1 router:

- The command Georgia1(config)#interface serial0/0/0 will allow

you to enter the interface's configuration mode.

- The command Georgia1(config-if)#encapsulation frame-relay will allow you to enable the Frame Relay Encapsulation on the network.
- The command Georgia1(config-if)#ip address (enter ip address here) will allow you to assign a particular IP address and netmask to the system.
- The command Georgia1(config-if)#ip ospf network point-to-multipoint will allow you to switch your network’s type from default nonbroadcast to point-to-multipoint.
- The command Georgia1(config-if)#frame-relay map ip 172.16.2.2 50 will allow you to map out a remote IP address to the local DLCI 50.
- The command Georgia1(config-if)#frame-relay map ip 172.16.2.3 51 will allow you to map out a remote IP address to the local DLCI 51.
- The command Georgia1(config-if)#frame-relay map ip 172.16.2.4 52 will allow you to map out a remote IP address to the local DLCI 52.
- The command Georgia1(config-if)#no shutdown will allow you to enable your interface on the network.
- The command Georgia1(config-if)#exit will allow you to shift back to the global configuration mode.
- The command Georgia1(config)#router ospf1 will allow you to kick off OSPF 1.
- The command Georgia1(config-router)#network 172.16.0.0 0.0.255.255 area 0 will ensure that the interface that has the IP address 172.16.y.y will operate OSPF and it will also be put in area 0.
- The command Georgia1(config-router)#exit will take you back to the global configuration mode.

- The command Georgia1(config)#exit will allow you to get back to the privileged mode.
- The command Georgia1#copy running-config startup-config will allow you to save your network configuration to NVRAM.

Georgia2 router:

- The command Georgia2(config)#interface serial0/0/0 will allow you to enter the interface's configuration mode.
- The command Georgia2(config-if)#encapsulation frame-relay will allow you to enable the Frame Relay Encapsulation on the network.
- The command Georgia2(config-if)#ip address (enter ip address here) will allow you to assign a particular IP address and netmask to the system.
- The command Georgia2(config-if)#ip ospf network point-to-multipoint will allow you to switch your network's type from default nonbroadcast to point-to-multipoint.
- The command Georgia2(config-if)#frame-relay map ip 172.16.2.1 150 will allow you to map out a remote IP address to the local DLCI 150.
- The command Georgia2(config-if)#frame-relay map ip 172.16.2.3 150 will allow you to map out a remote IP address to the local DLCI 150.
- The command Georgia2(config-if)#frame-relay map ip 172.16.2.4 150 will allow you to map out a remote IP address to the local DLCI 150.
- The command Georgia2(config-if)#no shutdown will allow you to enable your interface on the network.
- The command Georgia2(config-if)#exit will allow you to shift back to the global configuration mode.
- The command Georgia2(config)#router ospf1 will allow you to

kick off OSPF 1.

- The command Georgia2(config-router)#network 172.16.0.0 0.0.255.255 area 0 will ensure that the interface that has the IP address 172.16.y.y will operate OSPF and it will also be put in area 0.
- The command Georgia2(config-router)#exit will take you back to the global configuration mode.
- The command Georgia2(config)#exit will allow you to get back to the privileged mode.
- The command Georgia2#copy running-config startup-config will allow you to save your network configuration to NVRAM.

Georgia3 router:

- The command Georgia3(config)#interface serial0/0/0 will allow you to enter the interface's configuration mode.
- The command Georgia3(config-if)#encapsulation frame-relay will allow you to enable the Frame Relay Encapsulation on the network.
- The command Georgia3(config-if)#ip address (enter ip address here) will allow you to assign a particular IP address and netmask to the system.
- The command Georgia3(config-if)#ip ospf network point-to-multipoint will allow you to switch your network’s type from default nonbroadcast to point-to-multipoint.
- The command Georgia3(config-if)#frame-relay map ip 172.16.2.1 151 will allow you to map out a remote IP address to the local DLCI 151.
- The command Georgia3(config-if)#frame-relay map ip 172.16.2.2 151 will allow you to map out a remote IP address to the local DLCI 151.
- The command Georgia3(config-if)#frame-relay map ip

172.16.2.4 151 will allow you to map out a remote IP address to the local DLCI 151.

- The command Georgia3(config-if)#no shutdown will allow you to enable your interface on the network.
- The command Georgia3(config-if)#exit will allow you to shift back to the global configuration mode.
- The command Georgia3(config)#router ospf1 will allow you to kick off OSPF 1.
- The command Georgia3(config-router)#network 172.16.0.0 0.0.255.255 area 0 will ensure that the interface that has the IP address 172.16.y.y will operate OSPF and it will also be put in area 0.
- The command Georgia3(config-router)#exit will take you back to the global configuration mode.
- The command Georgia3(config)#exit will allow you to get back to the privileged mode.
- The command Georgia3#copy running-config startup-config will allow you to save your network configuration to NVRAM.

Georgia4 router:

- The command Georgia4(config)#interface serial0/0/0 will allow you to enter the interface's configuration mode.
- The command Georgia4(config-if)#encapsulation frame-relay will allow you to enable the Frame Relay Encapsulation on the network.
- The command Georgia4(config-if)#ip address (enter ip address here) will allow you to assign a particular IP address and netmask to the system.
- The command Georgia4(config-if)#ip ospf network point-to-multipoint will allow you to switch your network’s type from default nonbroadcast to point-to-multipoint.

- The command Georgia4(config-if)#frame-relay map ip 172.16.2.2 152 will allow you to map out a remote IP address to the local DLCI 152.
- The command Georgia4(config-if)#frame-relay map ip 172.16.2.2 152 will allow you to map out a remote IP address to the local DLCI 152.
- The command Georgia4(config-if)#frame-relay map ip 172.16.2.2 152 will allow you to map out a remote IP address to the local DLCI 152.
- The command Georgia4(config-if)#no shutdown will allow you to enable your interface on the network.
- The command Georgia4(config-if)#exit will allow you to shift back to the global configuration mode.
- The command Georgia4(config)#router ospf1 will allow you to kick off OSPF 1.
- The command Georgia4(config-router)#network 172.16.0.0. 0.0.255.255 area 0 will ensure that the interface that has the IP address 172.16.y.y will operate OSPF and it will also be put in area 0.
- The command Georgia4(config-router)#exit will take you back to the global configuration mode.
- The command Georgia4(config)#exit will allow you to get back to the privileged mode.
- The command Georgia4#copy running-config startup-config will allow you to save your network configuration to NVRAM.

OSPF and Point-to-Point Networks By Using Subinterfaces

The following section is packed up with commands to build a four router network of OSPF and point-to-point networks. There will be commands for four routers in the following example. You can build and configure the network by using the following commands.

Georgia1 router:

- The command Georgia1(config)#interface serial0/0/0 will allow you to enter the interface's configuration mode.
- The command Georgia1(config-if)#encapsulation frame-relay will allow you to enable the Frame Relay Encapsulation on the network.
- The command Georgia1(config-if)#no shutdown will allow you to start your interface.
- The command Georgia1(config-if)#interface serial 0/0/0.50 point-to-point will allow you to make a subinterface.
- The command Georgia1(config-subif)#description Link to Georgia2 will allow you to create a locally significant interface description.
- The command Georgia1(config-subif)#ip address (enter ip address here) will allow you to assign a particular IP address and netmask to the system.
- The command Georgia1(config-subif)#frame-relay interface-dlci 50 will allow you to assign a DLCI to subinterface.
- The command Georgia1(config-subif)#exit will allow you to shift back to the interface configuration mode.
- The command Georgia1(config-if)#interface serial 0/0/0.51 point-to-point will allow you to make a subinterface.
- The command Georgia1(config-subif)#description Link to Georgia3 will allow you to create a locally significant interface description.
- The command Georgia1(config-subif)#ip address (enter ip address here) will allow you to assign a particular IP address and netmask to the system.
- The command Georgia1(config-subif)#frame-relay interface-dlci 51 will allow you to assign a DLCI to subinterface.

- The command Georgia1(config-subif)#exit will allow you to shift back to the interface configuration mode.
- The command Georgia1(config-if)#interface serial 0/0/0.52 point-to-point will allow you to make a subinterface.
- The command Georgia1(config-subif)#description Link to Georgia4 will allow you to create a locally significant interface description.
- The command Georgia1(config-subif)#ip address (enter ip address here) will allow you to assign a particular IP address and netmask to the system.
- The command Georgia1(config-subif)#frame-relay interface-dlci 52 will allow you to assign a DLCI to subinterface.
- The command Georgia1(config-subif)#exit will allow you to shift back to the interface configuration mode.
- The command Georgia1(config-if)#exit will allow you to shift back to the global configuration mode.
- The command Georgia1(config)#router ospf1 will allow you to kick off OSPF 1.
- The command Georgia1(config-router)#network 172.16.0.0 0.0.255.255 area 0 will ensure that the interface that has the IP address 172.16.y.y will operate OSPF and it will also be put in area 0.
- The command Georgia1(config-router)#exit will take you back to the global configuration mode.
- The command Georgia1(config)#exit will allow you to get back to the privileged mode.
- The command Georgia1#copy running-config startup-config will allow you to save your network configuration to NVRAM.

Georgia 2:

- The command Georgia2(config)#interface serial0/0/0 will allow you to enter the interface's configuration mode.
- The command Georgia2(config-if)#encapsulation frame-relay will allow you to enable the Frame Relay Encapsulation on the network.
- The command Georgia2(config-if)#no shutdown will allow you to start your interface.
- The command Georgia2(config-if)#interface serial 0/0/0.150 point-to-point will allow you to make a subinterface.
- The command Georgia2(config-subif)#description Link to Georgia1 will allow you to create a locally significant interface description.
- The command Georgia2(config-subif)#ip address (enter ip address here) will allow you to assign a particular IP address and netmask to the system.
- The command Georgia2(config-subif)#frame-relay interface-dlci 150 will allow you to assign a DLCI to subinterface.
- The command Georgia2(config-subif)#exit will allow you to shift back to the interface configuration mode.
- The command Georgia2(config)#exit will allow you to shift back to the global configuration mode.
- The command Georgia2(config)#router ospf1 will allow you to kick off OSPF 1.
- The command Georgia2(config-router)#network 172.16.0.0 0.0.255.255 area 0 will ensure that the interface that has the IP address 172.16.y.y will operate OSPF and it will also be put in area 0.
- The command Georgia2(config-router)#exit will take you back to the global configuration mode.
- The command Georgia2(config)#exit will allow you to get back

to the privileged mode.

- The command Georgia2#copy running-config startup-config will allow you to save your network configuration to NVRAM.

Georgia3 router:

- The command Georgia3(config)#interface serial0/0/0 will allow you to enter the interface's configuration mode.
- The command Georgia3(config-if)#encapsulation frame-relay will allow you to enable the Frame Relay Encapsulation on the network.
- The command Georgia3(config-if)#no shutdown will allow you to start your interface.
- The command Georgia3(config-if)#interface serial 0/0/0.151 point-to-point will allow you to make a subinterface.
- The command Georgia3(config-subif)#ip address (enter ip address here) will allow you to assign a particular IP address and netmask to the system.
- The command Georgia3(config-subif)#frame-relay interface-dlci 151 will allow you to assign a DLCI to subinterface.
- The command Georgia3(config-subif)#exit will allow you to shift back to the interface configuration mode.
- The command Georgia3(config)#exit will allow you to shift back to the global configuration mode.
- The command Georgia3(config)#router ospf1 will allow you to kick off OSPF 1.
- The command Georgia3(config-router)#network 172.16.0.0 0.0.255.255 area 0 will ensure that the interface that has the IP address 172.16.y.y will operate OSPF and it will also be put in area 0.
- The command Georgia3(config-router)#exit will take you back

to the global configuration mode.

- The command Georgia3(config)#exit will allow you to get back to the privileged mode.
- The command Georgia3#copy running-config startup-config will allow you to save your network configuration to NVRAM.

Georgia4:

- The command Georgia2(config)#interface serial0/0/0 will allow you to enter the interface's configuration mode.
- The command Georgia2(config-if)#encapsulation frame-relay will allow you to enable the Frame Relay Encapsulation on the network.
- The command Georgia2(config-if)#no shutdown will allow you to start your interface.
- The command Georgia2(config-if)#interface serial 0/0/0.150 point-to-point will allow you to make a subinterface.
- The command Georgia2(config-subif)#description Link to Georgia1 will allow you to create a locally significant interface description.
- The command Georgia2(config-subif)#ip address (enter ip address here) will allow you to assign a particular IP address and netmask to the system.
- The command Georgia2(config-subif)#frame-relay interface-dlci 150 will allow you to assign a DLCI to subinterface.
- The command Georgia2(config-subif)#exit will allow you to shift back to the interface configuration mode.
- The command Georgia2(config)#exit will allow you to shift back to the global configuration mode.
- The command Georgia2(config)#router ospf1 will allow you to kick off OSPF 1.

- The command Georgia2(config-router)#network 172.16.0.0 0.0.255.255 area 0 will ensure that the interface that has the IP address 172.16.y.y will operate OSPF and it will also be put in area 0.
- The command Georgia2(config-router)#exit will take you back to the global configuration mode.
- The command Georgia2(config)#exit will allow you to get back to the privileged mode.
- The command Georgia2#copy running-config startup-config will allow you to save your network configuration to NVRAM.

OSPF for IPv6 on Interface

- The command Georgia(config)#ipv6 unicast-routing will let you enable the globally spread of IPv6 unicast datagrams across the router.
- The command Georgia(config)#interface fastethernet0/0 will let you switch to the mode for interface configuration.
- The command Georgia(config-if)#ipv6 address 2001:db8:0:1: :/64 will let you configure the global IPv6 address across the interface and it also enables the IPv6 processing across the interface.
- The command Georgia(config-if)#ipv6 ospf 1 area 0 will let you enable the OSPFv3 process 1 across the interface. It also places the interface into area 0.
- The command Georgia(config-if)#ipv6 ospf priority 50 will let you assign a certain priority number to your interface, which you can use in the designated router election. You can set the priority number between 1 and 255. If you do not assign any number, the default digit 1 will be automatically set. The router with priority set up to 0 is not eligible to become a DR(BDR) or DR.
- The command Georgia(config-if)#ipv6 ospf cost 50 will allow you to assign the cost value 50 to the interface. The cost values

may be any integer between 1 and 65,535.

- The command Georgia(config)#ospfv3 1 ipv6 will enable the OSPFv3 instance with 1. The address family will be IPv6 and area will be 0.
- The command Georgia(config)#ospfv3 1 ipv4 will enable the OSPFv3 instance with 1. The address family will be IPv4 and area will be 0.

OSPFv3 Address Families

- The command Georgia(config)#router ospfv3 1 will enable the router configuration mode of OSPFv3 for IPv6 and IPv4 address families.
- The command Georgia(config-router)#address-family ipv6 unicast will enable the router configuration mode of OSPFv3 for IPv6 address family. You will be able to notice a prompt change in the interface.

OSPFv3 for IPv4

- The command Georgia(config)#router ospfv3 1 will enable the router configuration mode of OSPFv3 for IPv6 and IPv4 address families.
- The command Georgia(config-router)#address-family ipv4 unicast will enable the router configuration mode of OSPFv3 for IPv4 address family. You will be able to notice a prompt change in the interface.

OSPFv3 for IPv6

Georgia3 Router:

- The command Georgia3(config)#ipv6 unicast-routing will let you enable the globally spread of IPv6 unicast datagrams across the router.
- The command Georgia3(config)#interface fastethernet0/0 will let you switch to the mode for interface configuration.

- The command Georgia3(config-if)#ipv6 address 2001:db8:0:1::3/64 will let you configure the global IPv6 address across the interface and it also enables the IPv6 processing across the interface.
- The command Georgia3(config-if)#ipv6 ospf 1 area 1 will let you enable the OSPFv3 process across the interface. It also places the interface into area 1.
- The command Georgia3(config-if)#no shutdown will let you enable the interface of your network.
- The command Georgia3(config-if)#interface loopback0 will let you shift to the interface configuration mode.
- The command Georgia3(config-if)#ipv6 address 2001:db8:0:1::1/64 will let you configure the global IPv6 address across the interface and it also enables the IPv6 processing across the interface.
- The command Georgia3(config-if)#ipv6 ospf 1 area 1 will let you enable the OSPFv3 process across the interface. It also places the interface into area 1.
- The command Georgia3(config-rtr)#router-id 3.3.3.3 will let you set up a router ID that is manually configured.
- The command Georgia3(config-if)#exit will take you back to the global configuration mode.
- The command Georgia3(config)#exit will allow you to get back to the privileged mode.
- The command Georgia3#copy running-config startup-config will allow you to save your network configuration to NVRAM.

Georgia2 router:

- The command Georgia2(config)#ipv6 unicast-routing will let you enable the globally spread of IPv6 unicast datagrams across the router.

- The command Georgia2(config)#interface fastethernet0/0 will let you switch to the mode for interface configuration.
- The command Georgia2(config-if)#ipv6 address 2001:db8:0:1::2/64 will let you configure the global IPv6 address across the interface and it also enables the IPv6 processing across the interface.
- The command Georgia2(config-if)#ipv6 ospf 1 area 1 will let you enable the OSPFv3 process across the interface. It also places the interface into area 1.
- The command Georgia2(config-if)#no shutdown will let you enable the interface of your network.
- The command Georgia2(config-if)#interface loopback0 will let you shift to the interface configuration mode.
- The command Georgia2(config-if)#ipv6 address 2001:db8:0:1::1/64 will let you configure the global IPv6 address across the interface and it also enables the IPv6 processing across the interface.
- The command Georgia2(config-if)#ipv6 ospf 1 area 1 will let you enable the OSPFv3 process across the interface. It also places the interface into area 1.
- The command Georgia2(config-rtr)#router-id 2.2.2.2 will let you set up a router ID that is manually configured.
- The command Georgia2(config-if)#exit will take you back to the global configuration mode.
- The command Georgia2(config)#exit will allow you to get back to the privileged mode.
- The command Georgia2#copy running-config startup-config will allow you to save your network configuration to NVRAM.

Georgia1 Router:

- The command Georgia1(config)#ipv6 unicast-routing will let

you enable the globally spread of IPv6 unicast datagrams across the router.

- The command Georgia1(config)#interface fastethernet0/0 will let you switch to the mode for interface configuration.
- The command Georgia1(config-if)#ipv6 address 2001:db8:0:1: :1/64 will let you configure the global IPv6 address across the interface and it also enables the IPv6 processing across the interface.
- The command Georgia1(config-if)#ipv6 ospf 1 area 1 will let you enable the OSPFv3 process across the interface. It also places the interface into area 1.
- The command Georgia1(config-if)#no shutdown will let you enable the interface of your network.
- The command Georgia1(config)#interface serial0/0 will let you switch to the mode for interface configuration.
- The command Georgia1(config-if)#ipv6 address 2001:db8:0:1: :1/64 will let you configure the global IPv6 address across the interface and it also enables the IPv6 processing across the interface.
- The command Georgia1(config-if)#ipv6 ospf 1 area 0 will let you enable the OSPFv3 process across the interface. It also places the interface into area 0.
- The command Georgia1(config-if)#clock rate 56000 will let you set up and assign the clock rate to your interface.
- The command Georgia1(config-if)#no shutdown will let you enable the interface of your network.
- The command Georgia1(config-if)#exit will take you back to the global configuration mode.
- The command Georgia2(config)#ipv6 router ospf 1 will allow you to shift to OSPFv3 configuration mode.

- The command Georgia2(config-rtr)#router-id 1.1.1.1 will let you set up a router ID that is manually configured.
- The command Georgia1(config-if)#exit will take you back to the global configuration mode.
- The command Georgia1(config)#exit will allow you to get back to the privileged mode.
- The command Georgia1#copy running-config startup-config will allow you to save your network configuration to NVRAM.

Georgia4 Router:

- The command Georgia4(config)#ipv6 unicast-routing will let you enable the globally spread of IPv6 unicast datagrams across the router.
- The command Georgia4(config)#interface serial0/0 will let you switch to the mode for interface configuration.
- The command Georgia4(config-if)#ipv6 address 2001:db8:0:1: :2/64 will let you configure the global IPv6 address across the interface and it also enables the IPv6 processing across the interface.
- The command Georgia4(config-if)#ipv6 ospf 1 area 0 will let you enable the OSPFv3 process across the interface. It also places the interface into area 0.
- The command Georgia4(config-if)#no shutdown will let you enable the interface of your network.
- The command Georgia4(config-if)#no shutdown will let you enable the interface of your network.
- The command Georgia4(config-if)#exit will take you back to the global configuration mode.
- The command Georgia4(config)#ipv6 router ospf 1 will allow you to shift to OSPFv3 configuration mode.

- The command Georgia4(config-rtr)#router-id 4.4.4.4 will let you set up a router ID that is manually configured.
- The command Georgia4(config-if)#exit will take you back to the global configuration mode.
- The command Georgia4(config)#exit will allow you to get back to the privileged mode.
- The command Georgia4#copy running-config startup-config will allow you to save your network configuration to NVRAM.

Verifying OSPF Configuration

- The command Georgia#show ip protocol will allow you to see all the parameters for all the protocols that have been running on a router.
- The command Georgia#show ip route will allow you to see the full IP routing table.
- The command Georgia#show ip route ospf will allow you to see OSPF routes inside the routing table.
- The command Georgia#show ip route ospfv3 will allow you to see the routes for the OSPFv3 routes inside the routing table.
- The command Georgia#show ip ospf will allow you to see the basic information on OSPF's routing processes.
- The command Georgia#show ip ospf border-routers will allow you to see the information about the boundary and borders.
- The command Georgia#show ip ospf database will allow you to see the contents of the OSPF database.
- The command Georgia#show ip ospf database asbr-summary will allow you to see the LSAs of type 4.
- The command Georgia#show ip ospf database external will allow you to see the LSAs of type 5.
- The command Georgia#show ip ospf database nssa-external will

allow you to see the external link states of NSSA.

- The command Georgia#show ip ospf database network will allow you to see the network LSAs.
- The command Georgia#show ip ospf database router self-origin will allow you to see the LSAs you have generated locally.
- The command Georgia#show ip ospf database summary will allow you to see a summary of the database of OSPF.
- The command Georgia#show ip ospf interface will allow you to see the OSPF information as it tends to relate to different interfaces.
- The command Georgia#show ip ospf interface fastethernet0/0 will allow you to see the information about the interface namely fastethernet 0/0 of OSPF.
- The command Georgia#show ip ospf neighbor will allow you to see the information about OSPF neighbors and their current states.
- The command Georgia#show ip ospf neighbor detail will allow you to see the list of the neighbors with all the relevant information.
- The command Georgia#show ipv6 interface will allow you to see the information about the current status of interfaces that are configured for IPv6.
- The command Georgia#show ipv6 interface brief will allow you to see brief details of the interfaces that have been configured for IPv6.
- The command Georgia#show ipv6 neighbors will allow you to see the information about the IPv6 neighbor discovery cache.
- The command Georgia#show ipv6 ospf will allow you to see the information about the routing process of OSPFv4.
- The command Georgia#show ipv6 ospf border-routers will allow

you to see the information about the routing table entries of internal OSPF.

- The command Georgia#show ipv6 ospf database will allow you to see the information about the database of OSPFv3.
- The command Georgia#show ipv6 ospf database-summary will allow you to see the information about each type of LSA's existence for all areas in the database.
- The command Georgia#show ipv6 ospf interface will allow you to see the information about the interface linked to OSPFv3.
- The command Georgia#show ipv6 ospf neighbor will allow you to see the information about the neighbors of OSPFv3.
- The command Georgia#show ipv6 ospf virtual-links will allow you to see the information about the present state and the parameters of the virtual links for OSPFv3.
- The command Georgia#show ipv6 protocols will allow you to see the information about the current state and the parameters of the routing protocol processes of IPv6.
- The command Georgia#show ipv6 route will allow you to see the information about the routing table for IPv6.
- The command Georgia#show ipv6 route summary will allow you to see the summarized information about the routing table for IPv6.
- The command Georgia#show ipv6 routers will allow you to see the information about the router advertisement for IPv6. The information that pops up on the display is usually collected from the other routers.
- The command Georgia#show ipv6 traffic will allow you to see the information about the traffic on IPv6.
- The command Georgia#show ip ospf virtual-links will allow you to see the information about all the virtual links in the system.

- The command Georgia#show ospfv3 database will allow you to see the information about the database of OSPFv3.
- The command Georgia#show ospfv3 neighbor will allow you to see the information on the neighbors of OSPFv3. The information is displayed in a per-interface style to help the reader understand better.

Troubleshooting OSPF

- The command Georgia#clear ip route * will clear away the complete touting table. It will also force the user to rebuild the same.
- The command Georgia#clear ip route x.x.x.x will clear away the specific route for the network namely x.x.x.x. It can have a different name.
- The command Georgia#clear ipv6 route * will clear away all the routes for the IPv6 routing tables.
- The command Georgia#clear ipv6 traffic will help you reset the traffic counters for IPv6.
- The command Georgia#clear ip ospf counters will help you reset the OSPF counters.
- The command Georgia#clear ip ospf process will help you reset the entire process of OSPF. It also forces the OSPF to recreate the neighbors, the routing table and the database.
- The command Georgia#clear ip ospf 3 process will help you reset the process 3 of OSPF. It also forces the OSPF to recreate the neighbors, the routing table and the database.
- The command Georgia#clear ipv6 ospf process will help you reset the entire process of OSPF. It also forces the OSPF to recreate the neighbors, the routing table and the database.
- The command Georgia#clear ipv6 ospf 3 process will help you reset the process 3 of OSPFv3. It also forces the OSPF to

recreate the neighbors, the routing table and the database.

- The command Georgia#debug ipv6 ospf events will help you see all the events of OSPF.
- The command Georgia#debug ip ospf adj will help you see the debug messages that are related to the OSPF adjacency processes.
- The command Georgia#debug ipv6 ospf adj will help you see the debug messages that are related to the OSPF adjacency processes.
- The command Georgia#debug ipv6 packet will help you see the debug messages that are related to the IPv6 packets.
- The command Georgia#debug ip ospf packets will help you see all the OSPF packets.
- The command Georgia#debug ipv6 routing will let you see debug messages that are related to the IPv6 route cache updates and routing table updates.
- The command Georgia#undebug all will let you switch off the debugging commands.

Chapter Eight

Configuration of Switch

This chapter will walk you through the commands and information that are related to the configuration of switch. I will shed light on the hostnames, passwords, duplex and speed settings, interface descriptions and port security and I will explain each command and its purpose. The first on the line is the help command.

- The command switch>? will allow you to get help about different aspects of switches. The symbol ? works in the same manner as it does in a router.

Command Modes

- The command switch>enable lets you enter the user mode in the same way you do in a router.
- The command switch# will allow you to enter the privileged mode in the same way as you do in a router.
- The command switch>disable will allow you to leave the privileged mode in the same way as you do in a router.
- The command switch>exit will allow you to leave the user mode in the same way as you do in a router.

Command Verification

- The command switch#show version will allow you to see the information about the hardware and the software.
- The command switch#show interfaces will let you see the information about the configuration of interfaces and the status of the lines such as admin down, up/up and up/down.
- The command switch#show flash: will allow you to see the information about the flash memory. This feature is only

available for the 2900/2950 series only.

- The command switch#show vlan will allow you to see the information about the present configuration of VLAN.
- The command switch#show mac-address-table will allow you to see the information about the forwarding table of the present MAC address.
- The command switch#show post will allow you to see the information about the POST that is switch passed.
- The command switch#show controllers ethernet-controller will allow you to see the information about the Ethernet controller.
- The command switch#show start will allow you to see the information about the present level of configuration in NVRAM.
- The command switch#show running-config will allow you to see the information about the present configuration style in NVRAM.
- The command switch#show interface vlan1 will allow you to see the information about the settings of the virtual interfaces such as VLAN1 and the default interfaces such as VLAN on the system's switch.

Resetting Configuration

The following settings are for the 1900 series switches.

- The command 1900switch#delete vtp will allow you to remove the information about VLAN Trunking Protocol.
- The command 1900switch#delete nvram will allow you to reset the switch along the lines of the default settings.
- The command 1900switch>en will allow you to get back to the privileged mode.
- The command 1900switch#reload will allow you to restart your switch.

The following settings are for the 2900/2950 series switches.

- The command switch#delete flash:vlan.dat will allow you to delete the VLAN database from the system's flash memory.
- The command Switch#erase startup-config will allow you to delete all the files from the NVRAM.
- The command Switch#reload will allow you to restart the switch.

Setting Hostnames

For 1900 series switches:

- The command #config t will allow you to start the process of setting up the hostnames.
- The command (config)#hostname AustinSwitch will allow you to set up the name of the switch. The method is the same as for the router. The interface will appear like the following: AustinSwitch(config)#.

For 2900/2950 series switches:

- The first command is Swtich#config t.
- The command Switch(config)#hostname AustinSwitch will allow you to set up the name of the switch. The method is the same as for the router. you will see the following in the next line: 2900Switch(config)#.

Setting passwords for 1900 Series Switches:

- The command AustinSwitch(config)#enable password level1 python will allow you to set up the user mode password to python.
- The command AustinSwitch(config)#enable password level15 python1 will allow you to set up the enable mode password to python1.
- The command AustinSwitch(config)#enable secret python2 will

allow you to set up the enable secret password to python2.

Setting passwords in 2900/2950 series:

- The command AustinSwitch(config)#enable password python1 will allow you to set up the enable mode password to python1.
- The command AustinSwitch(config)#enable secret password python1 will allow you to set up the encrypted secret password to python1.
- The command AustinSwitch(config)#line con 0 will allow you to enter the line console mode on the network.
- The command AustinSwitch(config-line)#login will allow you to set up and enable the passwords' checking process.
- The command AustinSwitch(config-line)#password python1 will allow you to set up the password to python1.
- The command AustinSwitch(config-line)#exit will allow you to exit the console.
- The command AustinSwitch(config-line)#line aux 0 will allow you to enter the line auxiliary mode.
- The command AustinSwitch(config-line)#login will allow you to set up and enable the checking of passwords.
- The command AustinSwitch(config-line)#password python1 will allow you to set up the enable mode password to python1.
- The command AustinSwitch(config-line)#exit will allow you to exit the line auxiliary mode.
- The command AustinSwitch(config-line)#line vty 0 4 will allow you to enter the line vty mode for all the virtual ports.
- The command AustinSwitch(config-line)#login will allow you to set up and enable the checking of the passwords.
- The command AustinSwitch(config-line)#exit will allow you to

exit the line vty mode.

Setting IP Addresses

- The command AustinSwitch(config)#ip address (write ip address here) will allow you to set up the system's IP address and the mask to enable remote access to switch.

For 2900/2950 series:

- The command AustinSwitch(config)#ip address (write ip address here) will allow you to set up the system's IP address and the mask to enable remote access to switch.

Interface Descriptions

- The command AustinSwitch(config-if)#description Finance VLAN will allow you to set up and add the description for your interfaces.

For 2900/2950 series switches:

- The command AustinSwitch(config-if)#int fa0/1 will allow you to enter the interface mode.
- The command AustinSwitch(config-if)#description Finance VLAN will allow you to set up and add the description for your interfaces.

Duplex Settings

- The command AustinSwitch(config)#int e0/1 will allow you to use e0/1 on the 2900/2950 series.
- The command AustinSwitch(config-if)#duplex full will allow you to force the full-duplex operation on your network.
- The command AustinSwitch(config-if)#duplex half will allow you to force the half-duplex operation on your network.
- The command AustinSwitch(config-if)#duplex auto will allow

you to force the auto-duplex configuration on your network.

Duplex Settings for 2900/2950 series:

- The command AustinSwitch(config)#int fa0/1 will allow you to start the process.
- The command AustinSwitch(config-if)#speed 10 will allow you to force the 10-Mbps operation.
- The command AustinSwitch(config-if)#speed 100 will allow you to force the 100-Mbps operation.
- The command AustinSwitch(config-if)#speed auto will allow you to force the enabling of autospeed configuration.

Web-based Interface for Configuration Setting

- The command AustinSwitch(config)#ip http server will allow you to turn on the HTTP service on your network.
- The command AustinSwitch(config)#ip http port 80 will allow you to set the port for HTTP. You will have to turn off the port security reasons unless you have to use it to do some work.

MAC Address Management

- The command AustinSwitch#show mac-address-table will allow you to see the forwarding table for the present MAC address on the network system.
- The command AustinSwitch#clear mac-address-table will allow you to erase the entries of the forwarding table for the present MAC address on the network system.
- The command AustinSwitch#clear mac-address-table dynamic will allow you to delete only the dynamic entries from the forwarding table for the present MAC address on the network system.

Configuring Static MAC Addresses

- The command AustinSwitch(config)#mac-address-table permanent x.x.x e0/1 will allow you to set up the permanent address in the present MAC address table for your interface e 0/1.
- The command AustinSwitch#clear mac-address-table perm will allow you to delete all the permanent entries that you have made in the table.

For 2900/2950 series

- The command AustinSwitch(config)#mac-address-table static x.x.x fa0/1 vlan 1 will allow you to set up the permanent address in the present MAC address table for your interface fa0/1 in VLAN 1.
- The command AustinSwitch(config)#no mac-address-table permanent x.x.x e0/1 will allow you to erase the permanent address in the present MAC address table for your interface e 0/1.

Port Security

- The command AustinSwitch(config-if)#port secure will allow you to set up security for the interface you are working in.
- The command AustinSwitch(config-if)#port secure max-mac-count 1 will allow you one MAC address in the table for the given interface.

For 2900 series:

- The command AustinSwitch(config)#int fa0/1 will allow you to set up the interface for working.
- The command AustinSwitch(config-if)#port security will allow you to set up the mode for security.
- The command AustinSwitch(config-if)#port secure max-mac-count 1 will allow you to set up only one mac address for the given interface.

- The command AustinSwitch(config-if)#port security action shutdown will allow you to shut down the port if it witnesses any kind of violation in the system.

For 2950 series:

- The command AustinSwitch(config)#int fa0/1 will allow you to set up the interface to start working in.
- The command AustinSwitch(config-if)#switchport port-security is the next command on the line.
- The command AustinSwitch(config-if)#switchport port-security mac-address sticky will allow you to initiate the process of conversion of MAC addresses to secure and sticky addresses. The MAC address that is learned first will be accepted on the port.
- The command AustinSwitch(config-if)#switchport port-security maximum 1 will allow you to give one address for the interface.
- The command AustinSwitch(config-if)#switchport port-security violation shutdown will allow the port to shut down when it witnesses some kind of violation in the network system.

Port Security Violation

- The command AustinSwitch#show mac-address-table security will allow you to see the MAC address table that is packed up with the maximum security information.
- The command AustinSwitch#show port security will allow you to see the MAC address table that is packed up with the maximum security information.

2900 Switch Configuration

- The command switch>en will allow you to enter the privileged mode of the system network.
- The command switch#config t will allow you to enter the global

configuration mode in the network.

- The command switch(config)#no ip domain-lookup will turn off the DNS queries so that the spelling mistakes will keep you from slowing down in the midst of the process.
- The command switch(config)#hostname AustinSwitch will allow you to set up the name of the host. You can choose the name you like for the system.
- The command AustinSwitch(config)#enable secret python1 will allow you to set up the secret password to python1.
- The command AustinSwitch(config)#line con 0 will allow you to enter the line console.
- The command AustinSwitch(config-line)#logging synchronous will allow you to append different commands to the new line. The router information will not interrupt the sequence.
- The command AustinSwitch(config-line)#login will allow the user to log in the console before he or she can use it.
- The command AustinSwitch(config-line)#password python2 will allow you to set up the password to python2.
- The command AustinSwitch(config-line)#exec-timeout 0 0 will allow the console not to log out of the system.
- The command AustinSwitch(config-line)#exit will allow you to switch back to the global configuration mode.
- The command AustinSwitch(config)#line aux 0 will allow you to switch to the line auxiliary mode in a network system.
- The command AustinSwitch(config-line)#password python2 will allow you to change and set up the password to python2.
- The command AustinSwitch(config-line)#exit will allow you to switch back to the global configuration mode.
- The command AustinSwitch(config)#line vty 0 15 will allow you

to switch back to the configuration mode for all the 16 vty ports at the same time.

- The command AustinSwitch(config-line)#login will allow you to log in on the system to use the vty ports.
- The command AustinSwitch(config-line)#password python2 will allow you to change and set up the password to python2.
- The command AustinSwitch(config-line)#exit will allow you to switch back to the global configuration mode.
- The command AustinSwitch(config)#ip default-gateway 192.168.1.1 will allow you to set up the gateway to default.
- The command AustinSwitch(config)#int vlan 1 will allow you to switch back to the virtual interface VLAN 1.
- The command AustinSwitch(config-if)#ip add (enter ip address here) will allow you to set up the switch's IP address.
- The command AustinSwitch(config-if)#no shut will allow you to switch on the virtual interface.
- The command AustinSwitch(config-if)#int fa 0/1 will allow you to switch back to the interface fa 0/1.
- The command AustinSwitch(config-if)#desc Link to Router will allow you to set up the local description.
- The command AustinSwitch(config-if)#int fa 0/4 will allow you to switch back to the interface fa 0/4.
- The command AustinSwitch(config-if)#desc Link to Workstation A will allow you to set up the interface's local description.
- The command AustinSwitch(config-if)#port security will allow you to activate the system's port security.
- The command AustinSwitch(config-if)#port security max-mac-count 1 will allow you to include one MAC address into the MAC table.

- The command AustinSwitch(config-if)#port security action shutdown will allow you to turn off the port if multiple MAC addresses are reported in the system.
- The command AustinSwitch(config-if)#int fa 0/8 will allow you to switch back to the interface fa 0/8.
- The command AustinSwitch(config-if)#desc Link to Workstation B will allow you to set up the interface's local description.
- The command AustinSwitch(config-if)#port security will allow you to activate the system's port security.
- The command AustinSwitch(config-if)#port security max-mac-count 1 will allow you to include one MAC address into the MAC table.
- The command AustinSwitch(config-if)#port security action shutdown will allow you to turn off the port if multiple MAC addresses are reported in the system.
- The command AustinSwitch(config-if)#port security action shutdown will allow you to turn off the port if multiple MAC addresses are reported in the system.
- The command AustinSwitch(config-if)#exit will allow you to switch back to the global configuration mode.
- The command AustinSwitch(config)#exit will allow you to switch back to the privileged mode.
- The command AustinSwitch#copy run start will allow you to save the configurations to NVRAM.

Spanning Tree Protocol

In this section, I will explain the concept of spanning-tree verification and the troubleshooting process.

Verifying Spanning-Tree Protocol

- The command AustinSwitch#show spanning-tree brief will allow you to see the spanning-tree table for the switch.

- The command AustinSwitch#show spanning-tree will allow you to see the spanning-tree table for the switch.
- The command AustinSwitch#show spanning-tree int fa 0/17will allow you to see the information on spanning-tree for the port fa 0/17.
- The command AustinSwitch#show spanning-tree vlan y will allow you to see the information about the spanning-tree for a particular VLAN.
- The command AustinSwitch#show spanning-tree {all} will allow you to see the information about the changes in the topology in spanning-tree.

Changing Spanning-tree Priority of the Switch

- The command AustinSwitch(config)#spanning-tree priority 15 will allow you to set the priority at will. The number at the end of the command can be any in between 1 and 65535. A lower number indicates a better chance of electing the root bridge. The default number for the priority is 32768.
- The command AustinSwitch(config)#spanning-tree vlan 1 priority 15 will allow you to set the priority at will. The number at the end of the command can be any in between 1 and 65535. A lower number indicates a better chance of electing the root bridge. The default number for the priority is 32768.
- The command AustinSwitch#spanning-tree vlan y root will allow you to shift the switch to root switch for VLAN y by dropping he priority to 24576 or less than the present root bridge.

Changing the Spanning Tree Cost

- The first command on the line is AustinSwitch#config t.
- The command AustinSwitch(config)#int fa 0/1 will allow you to start the interface.
- The command AustinSwitch(config)#spanning-tree cost y will

allow you to set up the cost for the spanning tree to the specified value of y.

Changing Spanning Tree

- The command AustinSwitch(config)#int fa 0/1 will allow you to start the interface.
- The command AustinSwitch(config)#spanning-tree portfast will allow you to force the port to shift back to the forwarding state, without transitioning through the learning states, the blocking, and the listening processes. You can save about 50 seconds of the wait time by going through this process. This is the best command on the access ports that you will never be able to hook up to some other switch.

Portfast BPDU Guard Command

- The command AustinSwitch#config t will allow you to start the configuration mode.
- The command AustinSwitch(config)#spanning-tree portfast bpduguard will allow you to enable the BPDU Guard for your network system's interfaces.
- The command AustinSwitch(config)#errdiable recovery cause bpduguard will allow the port to get re-enabled after setting up a recovery timer.
- The command AustinSwitch(config)#errdiable recovery interval 500 will allow the port to get re-enabled after setting up a recovery timer to 500 seconds. The default timer is 300 seconds.
- The command AustinSwitch(config)#show spanning-tree summary totals will allow you to verify whether the BPDU Guard remains enabled or not.
- The command AustinSwitch#show errdisable recovery will allow you to see the information about the errdisable recovery timer.

Configuration of EtherChannel

- The command AustinSwitch#config t will allow you to start the configuration mode.
- The command AustinSwitch(config)#int fa 0/11 will allow you to start the interface.
- The command AustinSwitch(config-if)channel-group y mode on will allow you to start the mode for channel groups. In the command, y is the total number of channel groups. It must watch the other interfaces.
- The command AustinSwitch(config)#int fa 0/12 will allow you to start the interface.
- The command AustinSwitch(config-if)channel-group y mode on will allow you to start the mode for channel groups. In the command, y is the total number of channel groups. It must watch the other interfaces.

Verification

- The command AustinSwitch#show etherchannel y detail will allow you to see comprehensive information about the ether channel.
- The command AustinSwitch#show etherchannel y port will allow you to see comprehensive information about the EtherChannel port.
- The command AustinSwitch#show etherchannel y port-channel will allow you to see comprehensive information about the port channel.
- The command AustinSwitch#show etherchannel y summary will allow you to see the one-line summary information about per channel-groups.

The EtherChannel may combine about two to eight parallel links of Ethernet. The 1900 switches need 9.00.03 or the later Enterprise Edition software, the 2900 switches need the IOS 11.2(8)SA or later versions and the 2950

switches need the IOS 12.0(5.2)WC(1). You can set up the auto mode, the desirable mode and the on mode.

The auto mode tells the switch to wait for the other switches to kick off the EtherChannel negotiations. If the auto mode is set on both sides, the EtherChannel will never be able to form. Both sides will keep waiting for the other side to initiate negotiations. The desirable mode tells the switch that it is willing to turn the EtherChannel on. The on mode tells the switch that it wants to form the Ether Channel.

Chapter Nine

VLAN

This chapter will walk you through the commands and information about the display of VLAN info, the creation of static VLANs, the assigning of the ports to the VLANs, and the assigning of the ports by using the range command.

Displaying VLANs

- The command AustinSwitch#show vlan will allow you to see the information about VLAN.
- The command AustinSwitch#show vlan-membership will allow you to see the information about VLAN ports.
- The command AustinSwitch#show vlan 2 will allow you to see the information about VLAN 2.

For 2900/2950 series:

- The command AustinSwitch#show vlan will allow you to see the information about VLAN status.
- The command AustinSwitch#show vlan brief will allow you to see the summarized information about VLAN.
- The command AustinSwitch#show vlan id 2 will allow you to see the information about VLAN 2 only
- The command AustinSwitch#show vlan name Mark will allow you to see the information about VLAN that is named Mark.

Static VLANs

- The command AustinSwitch#config t will allow you to start the configuration mode.
- The command AustinSwitch(config)#vlan 2 name John will

allow you to create the VLAN 2 named John.

- The command AustinSwitch(config)#vlan 3 name John1 will allow you to create the VLAN 3 named John1.

For 2900 Series Switch:

- The command AustinSwitch#vlan database will allow you to enter the database mode.
- The command AustinSwitch(config)#vlan 2 name John will allow you to create the VLAN 2 named John.
- The command AustinSwitch(config)#vlan 3 name John1 will allow you to create the VLAN 3 named John1.
- The command AustinSwitch(vlan)#exit will allow you to apply the changes and then exit VLAN database mode.

For 2950 Series:

- The command AustinSwitch#config t will allow you to start the configuration mode.
- The command AustinSwitch(config)#vlan 10 will allow you to create VLAN 10. Also, you will enter the configuration mode for VLAN to have further definitions.
- The command AustinSwitch(config-vlan)#name John1 will allow you to name the vlan John1.
- The command AustinSwitch(config-vlan)#exit will allow you to exit and switch back to the global configuration mode.
- The command AustinSwitch(config)#vlan 20 will allow you to create VLAN 20. Also, you will enter the configuration mode for VLAN to have further definitions.
- The command AustinSwitch(config-vlan)#name John5 will allow you to name the vlan John5.
- The command AustinSwitch(config-vlan)#exit will allow you to

exit and switch back to the global configuration mode.

Port Assigning to VLANS

- The command AustinSwitch#config t will allow you to start the configuration mode.
- The command AustinSwitch(config)#int e0/2 will allow you to shift to the interface mode.
- The command AustinSwitch(config-if)#vlan static 2 will allow you to assign the port to VLAN 2.
- The command AustinSwitch(config)#int e0/3 will allow you to shift to the interface mode.
- The command AustinSwitch(config-if)#vlan static 3 will allow you to assign the port to VLAN 3.
- The command AustinSwitch(config-if)#exit will allow you to exit the interface mode.
- At the end you will see the following: AustinSwitch(config-if)#.

For 2900/2950 Series:

- The command AustinSwitch#config t will allow you to start the configuration mode.
- The command AustinSwitch(config)#int fa0/2 will allow you to shift to the interface mode.
- The command AustinSwitch(config-if)#switchport mode access will allow you to turn the switchport mode to access.
- The command AustinSwitch(config-if)#switchport access vlan 2 will allow you to assign the port to VLAN 2.
- The command AustinSwitch(config)#int fa0/3 will allow you to shift to the interface mode.
- The command AustinSwitch(config-if)#switchport mode access will allow you to turn the switchport mode to access.

- The command AustinSwitch(config-if)#switchport access vlan 3 will allow you to assign the port to VLAN 3.
- The command AustinSwitch(config-if)#exit will allow you to exit the interface mode.
- At the end you will see the following: AustinSwitch(config-if)#.

Saving VLAN Configurations

- The command AustinSwitch#copy run start will allow you to save the running-config the NVRAM.

Erasing VLAN Configurations

- The command AustinSwitch#delete vtp will allow you to erase the VLAN information from switch and it also resets the VTP parameters to the default factory settings.

You also can use the following commands.

- The command AustinSwitch(config)#inf fa 0/2 will allow you to start the interface mode.
- The command AustinSwitch(config-if)#no vlan static 2 will allow you to erase the interface from VLAN2 and then places it back in the default VLAN 1.
- The command AustinSwitch(config-if)#exit will allow you to exit the interface mode.
- The command AustinSwitch(config-if)#no vlan 2 name John1 will allow you only to erase VLAN2 from the system's database.
- At the end you will see the following: AustinSwitch(config-if)#.

For 2900 series:

- The command AustinSwitch#config t will allow you to start the configuration mode.
- The command AustinSwitch(config)#inf fa 0/3 will allow you to

start the interface mode.

- The command AustinSwitch(config-if)#no switchport access vlan 3 will allow you to erase the port from VLAN 3 and then places it back in the default VLAN 1.
- The command AustinSwitch(config-if)#exit will allow you to exit the interface mode.
- The command AustinSwitch(config)#exit will allow you to exit.
- The command AustinSwitch#vlan database will allow you to enter only the VLAN database of the system.
- The command AustinSwitch(vlan)#no vlan 3 will allow you only to erase VLAN 3 from the system's database.
- The command AustinSwitch(vlan)#exit will allow you to apply the changes and then exit the database mode.

Troubleshooting Process

- The command AustinSwitch#show vlan will allow you to see the information about the full VLAN database.
- The command AustinSwitch#show vlan brief will allow you to see the information about the database in a summarized manner.
- The command AustinSwitch#show vlan interfaces will allow you to see the information about the interfaces. This includes the information about the duplex settings and the speed as well.
- The command AustinSwitch#debug sw-vlan packets will allow you to see the information about the VLAN packets that a router received but it cannot support it.

VLAN Configuration Process

- The command switch>en will allow you to enter the privileged mode.
- The command switch#config t will allow you to enter the mode

of global configuration.

- The command switch(config)# hostname AustinSwitch will allow you to set up the name for the host.
- The command AustinSwitch(config)#no ip domain-lookup will allow you to switch off the DNS entries checking on spelling mistakes.
- The command AustinSwitch(config)#enable secret jasmine will allow you to set up the secret password to jasmine.
- The command AustinSwitch(config)#line con 0 will allow you to enter the console mode.
- The command AustinSwitch(config-line)#logging synchronous will ensure that the informational lines do not meddle with the command that you have entered.
- The command AustinSwitch(config-line)#password john1 will allow you to set up the password to john1.
- The command AustinSwitch(config-line)#exit will allow you to get back t the global configuration mode.
- The command AustinSwitch(config)#line vty 0 15 will allow you to enter the 16 vty modes. You will the same commands being applied to all lines.
- The command AustinSwitch(config-line)#login synchronous will allow you to challenge remote users to enter a password.
- The command AustinSwitch(config-line)#password john1 will allow you to set up the password to john1.
- The command AustinSwitch(config-line)#exit will allow you to get back t the global configuration mode.
- The command AustinSwitch(config)#ip default-gateway 192.168.1.1 will allow you to set up the switch's default gateway.
- The command AustinSwitch(config)#int vlan1 will allow you to

enter the virtual interface VLAN1.

- The command AustinSwitch(config-if)#ip address 192.168.1.2 255.255.255.0 will allow you to set up your switch's IP address.
- The command AustinSwitch(config-if)#no shut will allow you to switch on the interface you are working in.
- The command AustinSwitch(config-if)#exit will allow you to get back to the global configuration mode.
- The command AustinSwitch#vlan database will allow you to enter into the VLAN database.
- The command AustinSwitch(vlan)# 10 name Rose will allow you to create VLAN 10.
- The command AustinSwitch(vlan)# 20 name Rosemary will allow you to create VLAN 20.
- The command AustinSwitch(vlan)# 30 name Jasmine will allow you to create VLAN 30.
- The command AustinSwitch(vlan)#exit will allow you to apply the information you have entered and exit the system.
- The command Austinswitch#config t will allow you to enter the mode of global configuration.
- The command Austinswitch(config)#int fa0/2 will allow you to switch back to the interface mode.
- The command Austinswitch(config-if)#switchport mode access will allow you to set up the switchport mode to give access.
- The command Austinswitch(config-if)#switchport access vlan 10 will allow you to assign the port to VLAN 10.
- The command Austinswitch(config)#int fa0/3 will allow you to switch back to the interface mode.
- The command Austinswitch(config-if)#switchport mode access will allow you to set up the switchport mode to give access.

- The command Austinswitch(config-if)#switchport access vlan 10 will allow you to assign the port to VLAN 10.
- The command Austinswitch(config)#int fa0/4 will allow you to switch back to the interface mode.
- The command Austinswitch(config-if)#switchport mode access will allow you to set up the switchport mode to give access.
- The command Austinswitch(config-if)#switchport access vlan 10 will allow you to assign the port to VLAN 10.
- The command Austinswitch(config)#int fa0/5 will allow you to switch back to the interface mode.
- The command Austinswitch(config-if)#switchport mode access will allow you to set up the switchport mode to give access.
- The command Austinswitch(config-if)#switchport access vlan 20 will allow you to assign the port to VLAN 20.
- The command Austinswitch(config)#int fa0/6 will allow you to switch back to the interface mode.
- The command Austinswitch(config-if)#switchport mode access will allow you to set up the switchport mode to give access.
- The command Austinswitch(config-if)#switchport access vlan 20 will allow you to assign the port to VLAN 20.
- The command Austinswitch(config)#int fa0/7 will allow you to switch back to the interface mode.
- The command Austinswitch(config-if)#switchport mode access will allow you to set up the switchport mode to give access.
- The command Austinswitch(config-if)#switchport access vlan 20 will allow you to assign the port to VLAN 20.
- The command Austinswitch(config)#int fa0/8 will allow you to switch back to the interface mode.
- The command Austinswitch(config-if)#switchport mode access

will allow you to set up the switchport mode to give access.

- The command Austinswitch(config-if)#switchport access vlan 10 will allow you to assign the port to VLAN 10.
- The command Austinswitch(config)#int fa0/9 will allow you to switch back to the interface mode.
- The command Austinswitch(config-if)#switchport mode access will allow you to set up the switchport mode to give access.
- The command Austinswitch(config-if)#switchport access vlan 30 will allow you to assign the port to VLAN 30.
- The command Austinswitch(config)#int fa0/10 will allow you to switch back to the interface mode.
- The command Austinswitch(config-if)#switchport mode access will allow you to set up the switchport mode to give access.
- The command Austinswitch(config-if)#switchport access vlan 30 will allow you to assign the port to VLAN 30.
- The command Austinswitch(config)#int fa0/11 will allow you to switch back to the interface mode.
- The command Austinswitch(config-if)#switchport mode access will allow you to set up the switchport mode to give access.
- The command Austinswitch(config-if)#switchport access vlan 30 will allow you to assign the port to VLAN 30.
- The command Austinswitch(config)#int fa0/12 will allow you to switch back to the interface mode.
- The command Austinswitch(config-if)#switchport mode access will allow you to set up the switchport mode to give access.
- The command Austinswitch(config-if)#switchport access vlan 30 will allow you to assign the port to VLAN 30.
- The command Austinswitch(config)#(enter the following keys on the keyboard: ctrl + z) will allow you to get back to the

privileged mode.

- The command Austinswitch#copy run start will allow you to save the settings to NVRAM.

VTP Configuration

For 1900 series:

- The command Austinswitch1900(config)#vtp client will allow you to turn the switch to the mode namely VTP client.
- The command Austinswitch1900(config)#vtp server will allow you to turn the switch to mode namely default VTP server.
- The command Austinswitch1900(config)#vtp transparent will allow you to turn the switch to the mode namely VTP transparent.
- The command Austinswitch1900(config)#vtp domain SNAP will allow you to change the domain from the default to CNAP.
- The command Austinswitch1900(config)#vtp password john will allow you to change the password.

For 2900 series:

- The command Austinswitch2900#vlan database will allow you to initiate the mode namely VLAN database.
- The command Austinswitch2900(vlan)#vtp client will allow you to turn the switch to mode namely client.
- The command Austinswitch2900(vlan)#vtp server will allow you to turn the switch to mode namely server.
- The command Austinswitch2900(vlan)#vtp transparent will allow you to turn the switch to the mode namely VTP transparent.
- The command Austinswitch2900(vlan)#vtp domain academy will allow you to change the domain to academy.

- The command Austinswitch2900(vlan)#vtp password john1 will allow you to change the password to john1.
- The command Austinswitch2900(vlan)#vtp v2-mode will allow you to turn the switch to the mode namely version 2 or v2.
- The command Austinswitch2900(vlan)#vtp pruning will allow you to turn on VTP pruning.
- The command Austinswitch2900(vlan)#vtp transparent will allow you to turn the switch to the mode namely VTP transparent.
- The command Austinswitch2900(vlan)#exit will allow you to implement the changes and then exit the mode.

For 2950 series

- The command Austinswitch2950#config t will allow you to enter the global configuration mode.
- The command Austinswitch2950(config)#vtp mode client will allow you to turn the switch to the mode namely VTP client.
- The command Austinswitch2950(config)#vtp server will allow you to turn the switch to mode namely default VTP server.
- The command Austinswitch2950(config)#vtp mode transparent will allow you to turn the switch to the mode namely VTP transparent.
- The command Austinswitch2950(config)#vtp domain academy will allow you to change the domain from the default to academy.
- The command Austinswitch2950(config)#vtp password john will allow you to change the password to john.
- The command Austinswitch2950(config)#vtp v2-mode will allow you to turn the switch to the mode namely version 2 or v2.
- The command Austinswitch2950(condig)#vtp pruning will allow

you to turn on VTP pruning.

Configuration for 2900 Series

- The command switch>en will allow you to enter the privileged mode.
- The command switch>config t will allow you to enter the configuration mode.
- The command switch(config)#hostname AustinSwitch2900 will allow you to set up the host name.
- The command AustinSwitch2900(config)#no ip domain-lookup will allow you to turn off the DNS resolution to avoid the waiting time to the DNS lookup for the spelling errors.
- The command AustinSwitch2900(config)#line con 0 will allow you to enter the line mode.
- The command AustinSwitch2900(config-line)#logging synchronous will allow you to append the command line to a new line. There will be no interruption from the information items.
- The command AustinSwitch2900(config-line)#exec-timeout 0 0 will allow you to stop the console session from getting timed out.
- The command AustinSwitch2900(config-line)#exit will allow you to line mode.
- The command AustinSwitch2900(config)#enable secret john will allow you to set up the secret password to the word john.
- The command AustinSwitch2900(config)#exit will allow you to exit the session.
- The command AustinSwitch2900#vlan database will allow you to enter the database mode.
- The command AustinSwitch2900(vlan)#vlan 10 name Rose will allow you to create a VLAN 10 named Rose.

- The command AustinSwitch2900(vlan)#vlan 20 name Rose1 will allow you to create a VLAN 10 named Rose1.
- The command AustinSwitch2900(vlan)#vlan 30 name Rose2 will allow you to create a VLAN 10 named Rose2.
- The command AustinSwitch2900(vlan)#vtp server will allow you to turn your switch into the VTP server.
- The command AustinSwitch2900(vlan)#vtp domain academy will allow you to assign the domain name academy to the server.
- The command AustinSwitch2900(vlan)#exit will allow you to exit the VTP server mode after applying all the system's necessary changes.
- The command AustinSwitch2900#config t will allow you to enter the configuration mode once again.
- The command AustinSwitch2900(config)#int vlan1 will allow you to initiate vlan1.
- The command AustinSwitch2900(config-if)#ip add (enter ip address here) will allow you to enter and add the ip address to the network.
- The command AustinSwitch2900(config-if)#no shutdown is the next command on the line.
- The last command is AustinSwitch2900(config-if)#exit. It will exit the configuration mode.
- The command AustinSwitch2900(config)#ip default-gateway 192.168.1.1 will allow you to set the ip default-gateway.
- The command AustinSwitch2900(config)#int fa 0/1 will allow you to initiate the interface.
- The command AustinSwitch2900(config-if)#desc Trunk Link to Corp Router will allow you to link the system to the CORP router.

- The command AustinSwitch2900(config-if)#switchport mode trunk will allow you to create trunk link.
- The command AustinSwitch2900(config-if)#switchport trunk encapsulation dotiq will allow you to set up the encapsulation to the DotIQ.
- The command AustinSwitch2900(config-if)#int fa 0/2 will allow you to initiate the interface.
- The command AustinSwitch2900(config-if)#switchport access vlan 10 will allow you to assign VLAN 10 a separate port.
- The command AustinSwitch2900(config-if)#spanning-tree portfast will allow you to transition the port to the forwarding state inside the Spanning Tree Protocol (STP).
- The command AustinSwitch2900(config-if)#int fa 0/3 will allow you to initiate the interface.
- The command AustinSwitch2900(config-if)#switchport access vlan 10 will allow you to assign VLAN 10 a separate port.
- The command AustinSwitch2900(config-if)#spanning-tree portfast will allow you to transition the port to the forwarding state inside the Spanning Tree Protocol (STP).
- The command AustinSwitch2900(config-if)#int fa 0/4 will allow you to initiate the interface.
- The command AustinSwitch2900(config-if)#switchport access vlan 10 will allow you to assign VLAN 10 a separate port.
- The command AustinSwitch2900(config-if)#spanning-tree portfast will allow you to transition the port to the forwarding state inside the Spanning Tree Protocol (STP).
- The command AustinSwitch2900(config-if)#int fa 0/5 will allow you to initiate the interface.
- The command AustinSwitch2900(config-if)#switchport access vlan 20 will allow you to assign VLAN 20 a separate port.

- The command AustinSwitch2900(config-if)#spanning-tree portfast will allow you to transition the port to the forwarding state inside the Spanning Tree Protocol (STP).
- The command AustinSwitch2900(config-if)#int fa 0/6 will allow you to initiate the interface.
- The command AustinSwitch2900(config-if)#switchport access vlan 20 will allow you to assign VLAN 20 a separate port.
- The command AustinSwitch2900(config-if)#spanning-tree portfast will allow you to transition the port to the forwarding state inside the Spanning Tree Protocol (STP).
- The command AustinSwitch2900(config-if)#int fa0/7 will allow you to initiate the interface.
- The command AustinSwitch2900(config-if)#switchport access vlan 20 will allow you to assign VLAN 20 a separate port.
- The command AustinSwitch2900(config-if)#spanning-tree portfast will allow you to transition the port to the forwarding state inside the Spanning Tree Protocol (STP).
- The command AustinSwitch2900(config-if)#int fa0/8 will allow you to initiate the interface.
- The command AustinSwitch2900(config-if)#switchport access vlan 20 will allow you to assign VLAN 20 a separate port.
- The command AustinSwitch2900(config-if)#spanning-tree portfast will allow you to transition the port to the forwarding state inside the Spanning Tree Protocol (STP).
- The command AustinSwitch2900(config-if)#int fa0/8 will allow you to initiate the interface.
- The command AustinSwitch2900(config-if)#switchport access vlan 20 will allow you to assign VLAN 20 a separate port.
- The command AustinSwitch2900(config-if)#spanning-tree portfast will allow you to transition the port to the forwarding

state inside the Spanning Tree Protocol (STP).

- The command AustinSwitch2900(config-if)#int fa0/9 will allow you to initiate the interface.
- The command AustinSwitch2900(config-if)#switchport access vlan 20 will allow you to assign VLAN 20 a separate port.
- The command AustinSwitch2900(config-if)#spanning-tree portfast will allow you to transition the port to the forwarding state inside the Spanning Tree Protocol (STP).
- The command AustinSwitch2900(config-if)#int fa0/10 will allow you to initiate the interface.
- The command AustinSwitch2900(config-if)#switchport access vlan 30 will allow you to assign VLAN 30 a separate port.
- The command AustinSwitch2900(config-if)#spanning-tree portfast will allow you to transition the port to the forwarding state inside the Spanning Tree Protocol (STP).
- The command AustinSwitch2900(config-if)#int fa0/11 will allow you to initiate the interface.
- The command AustinSwitch2900(config-if)#switchport access vlan 30 will allow you to assign VLAN 30 a separate port.
- The command AustinSwitch2900(config-if)#spanning-tree portfast will allow you to transition the port to the forwarding state inside the Spanning Tree Protocol (STP).
- The command AustinSwitch2900(config-if)#int fa0/12 will allow you to initiate the interface.
- The command AustinSwitch2900(config-if)#switchport access vlan 30 will allow you to assign VLAN 30 a separate port.
- The command AustinSwitch2900(config-if)#spanning-tree portfast will allow you to transition the port to the forwarding state inside the Spanning Tree Protocol (STP).

- Now enter the following command AustinSwitch2900(config-if)# (enter Ctrl + Z on the keyboard).
- The command AustinSwitch2900#copy run start will allow you to save the configuration of the system to NVRAM.

Configuration for 2950 Series

- The command switch>en will allow you to enter the privileged mode.
- The command switch>config t will allow you to enter the configuration mode.
- The command switch(config)#hostname AustinSwitch2950 will allow you to set up the host name.
- The command AustinSwitch2950(config)#no ip domain-lookup will allow you to turn off the DNS resolution to avoid the waiting time to the DNS lookup for the spelling errors.
- The command AustinSwitch2950(config)#line con 0 will allow you to enter the line mode.
- The command AustinSwitch2950(config-line)#logging synchronous will allow you to append the command line to a new line. There will be no interruption from the information items.
- The command AustinSwitch2950(config-line)#exec-timeout 0 0 will allow you to stop the console session from getting timed out.
- The command AustinSwitch2950(config-line)#exit will allow you to line mode.
- The command AustinSwitch2950(config)#enable secret john will allow you to set up the secret password to the word john.
- The command AustinSwitch2950(config)#vlan 10 will allow you to create a VLAN 10.
- The command AustinSwitch2950(config-vlan)#name Rose will

allow you to name the vlan Rose.

- The command AustinSwitch2950(config-vlan)#vlan 20 will allow you to create a VLAN 20.
- The command AustinSwitch2950(config-vlan)#name Rose1 will allow you to name the vlan Rose1.
- The command AustinSwitch2950(config-vlan)#vlan 30 will allow you to create a VLAN 30.
- The command AustinSwitch2950(config-vlan)#vlan 30 name Rose2 will allow you to name the vlan Rose2.
- The command AustinSwitch2950(config-vlan)#exit will allow you to vlan mode.
- The command AustinSwitch2950(config)#vtp server will allow you to convert your switch into the VTP server.
- The command AustinSwitch2950(config)#vtp domain academy will allow you to assign the domain name academy to the server.
- The command AustinSwitch2950(config)#int vlan1 will allow you to initiate vlan1.
- The command AustinSwitch2950(config-if)#ip add (enter ip address here) will allow you to enter and add the ip address to the network.
- The command AustinSwitch2950(config-if)#no shutdown is the next command on the line.
- The last command is AustinSwitch2900(config-if)#exit. It will exit the configuration mode.
- The command AustinSwitch2950(config)#ip default-gateway 192.168.1.1 will allow you to set the ip default-gateway.
- The command AustinSwitch2950(config)#int fa 0/1 will allow you to initiate the interface.
- The command AustinSwitch2950(config-if)#desc Trunk Link to

Corp Router will allow you to link the system to the CORP router.

- The command AustinSwitch2950(config-if)#switchport mode trunk will allow you to create trunk link.
- The command AustinSwitch2950(config-if)#int range fa 0/2 - 4 will allow you to initiate the interface.
- The command AustinSwitch2950(config-if-range)#switchport access vlan 10 will allow you to assign VLAN 10 a separate port.
- The command AustinSwitch2950(config-if-range)#spanning-tree portfast will allow you to transition the port to the forwarding state inside the Spanning Tree Protocol (STP).
- The command AustinSwitch2950(config-if-range)#int range fa 0/5 - 6 will allow you to initiate the interface.
- The command AustinSwitch2950(config-if-range)#switchport access vlan 20 will allow you to assign VLAN 20 a separate port.
- The command AustinSwitch2950(config-if-range)#spanning-tree portfast will allow you to transition the port to the forwarding state inside the Spanning Tree Protocol (STP).
- The command AustinSwitch2950(config-if-range)#int range fa 0/9 - 12 will allow you to initiate the interface.
- The command AustinSwitch2950(config-if-range)#switchport access vlan 10 will allow you to assign VLAN 10 a separate port.
- The command AustinSwitch2950(config-if-range)#spanning-tree portfast will allow you to transition the port to the forwarding state inside the Spanning Tree Protocol (STP).
- Now enter the following command AustinSwitch2900(config-if)# (enter Ctrl + Z on the keyboard).
- The command AustinSwitch2900#copy run start will allow you to save the configuration of the system to NVRAM.

Conclusion

Now that you have made it to the end of the book, I hope you are better prepared for your next exam. The book has equipped you with the technicalities of the subject. I recommend that you give it a second read to clear the concepts in a better way. I also recommend that you keep the books as a pocketbook to use it on the go. You can also use it to note down references whenever you are stuck on a command. The next step is to practice what you have learned. Memorizing the commands is not easy. It takes determination, sweat and the will to read them again and again, and memorize the commands.

I hope you have found the book highly useful and effective for your learning program. I do not claim that you will learn everything in the first go. Instead, I encourage you to read it at least twice to have a clear picture of all the commands that I have given in the book. I hope that with commitment, you will be able to understand the subject in a better way.

References

Empson, S. (2006). CCNA Self-Study CCNA Portable Command Guide. https://www.pdfdrive.com/ccna-self-study-ccna-portable-command-guide-shinra-inc-main-page-d3667445.html

Empson, S., Gargano, P., & Roth, H. (2015). CCNP Routing and Switching Portable Command Guide. https://www.pdfdrive.com/ccnp-routing-and-switching-portable-command-guide-d56814104.html

OSPF part I. (n.d.). CCNA Blog | Tips and Tutorials. https://www.ccnablog.com/ospf-part-1/

Cisco certified network associate (CCNA). (2020, November 4). Welcome to Computer Institute, The technology training School. https://www.trainus.com/ccna.asp

Cisco CCNA training certification course in Lahore Pakistan - CCNA training course in Lahore. (n.d.). Student Shelter In Computers. https://www.stscomps.com/cisco.htm