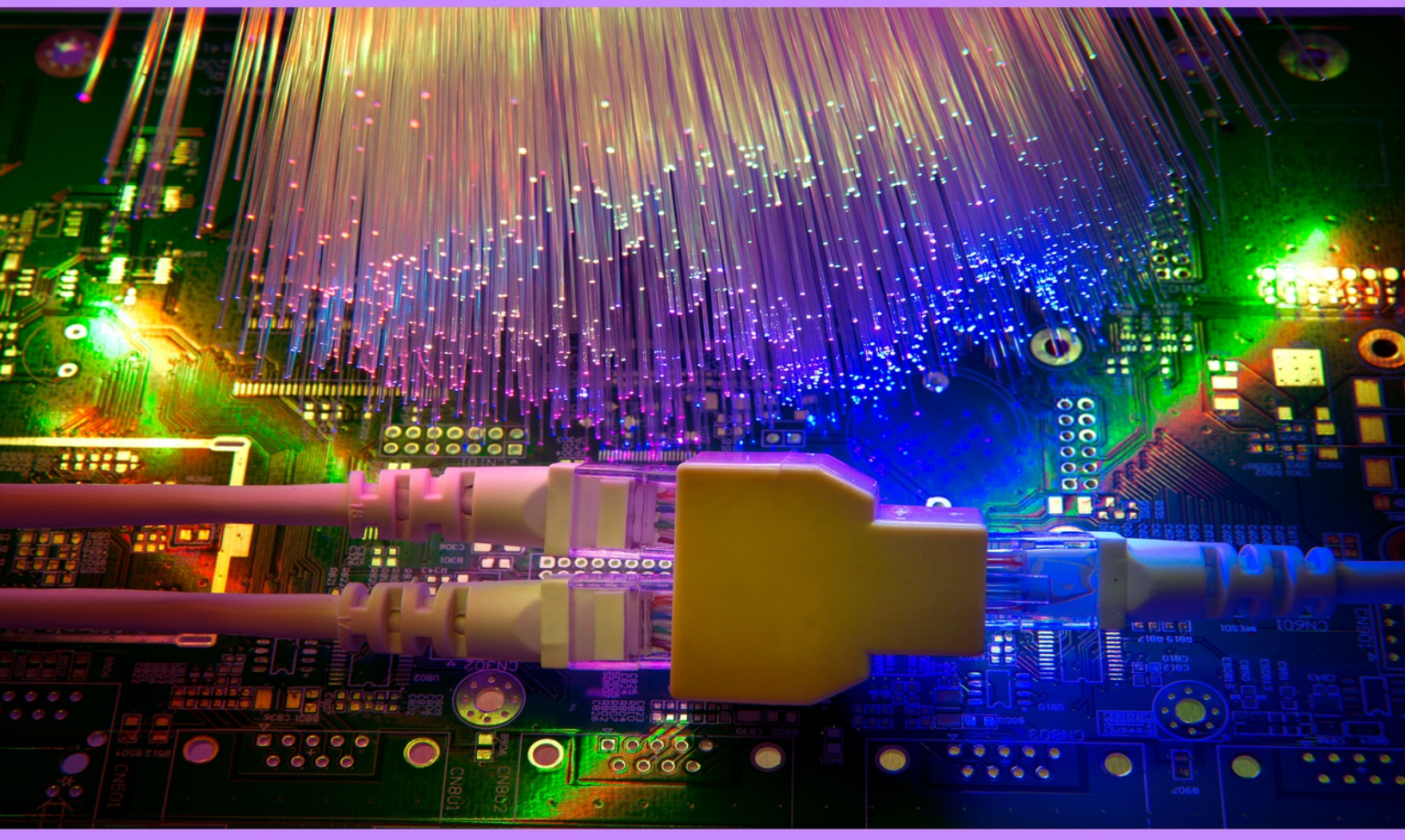
Cisco CCNA Command Guide

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



STUART NICHOLAS

https://t.me/learningnets

Cisco CCNA Command Guide

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

https://t.me/learningnets

Table of Contents

https://t.me/learningnets

https://t.me/learningnets

https://t.me/learningnets

© Copyright 2019 by __Stuart Nicholas_____ - All rights reserved.

This document is geared towards providing exact and reliable information in regards to the topic and issue covered. The publication is sold with the idea that the publisher is not required to render accounting, officially permitted or otherwise qualified services. If advice is necessary, legal or professional, a practiced individual in the profession should be ordered.

From a Declaration of Principles which was accepted and approved equally by a Committee of the American Bar Association and a Committee of Publishers and Associations.

In no way is it legal to reproduce, duplicate, or transmit any part of this document in either electronic means or in printed format. Recording of this publication is strictly prohibited, and any storage of this document is not allowed unless with written permission from the publisher. All rights reserved.

The information provided herein is truthful and consistent, in that any liability, in terms of inattention or otherwise, by any usage or abuse of any policies, processes, or directions contained within is the solitary and utter responsibility of the recipient reader. Under no circumstances will any legal responsibility or blame be held against the publisher for any reparation, damages, or monetary loss due to the information herein, either directly or indirectly.

Respective authors own all copyrights not held by the publisher.

The information herein is offered for informational purposes solely and is universal as so. The presentation of the information is without a contract or any type of guarantee assurance.

The trademarks that are used are without any consent, and the publication of the trademark is without permission or backing by the trademark owner. All trademarks and brands within this book are for clarifying purposes only and are owned by the owners themselves, not affiliated with this document.

https://t.me/learningnets

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

https://t.me/learningnets

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.

https://t.me/learningnets

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

https://t.me/learningnets

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

https://t.me/learningnets

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

https://t.me/learningnets

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

https://t.me/learningnets

	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:

https://t.me/learningnets

- ***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

https://t.me/learningnets

multiple communications are established at the same time, provided they are between different computers.

https://t.me/learningnets

Chapter One: 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,

https://t.me/learningnets

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.

https://t.me/learningnets

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.

https://t.me/learningnets

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.

https://t.me/learningnets

- **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

https://t.me/learningnets

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

https://t.me/learningnets

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

https://t.me/learningnets

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:

1. ***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)

2. ***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.

https://t.me/learningnets

3. ***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).

4. ***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.

5. ***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.

6. ***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.

7. ***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.

https://t.me/learningnets

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

https://t.me/learningnets

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

https://t.me/learningnets

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

https://t.me/learningnets

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.

https://t.me/learningnets

Chapter Two: 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

https://t.me/learningnets

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.

https://t.me/learningnets

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

https://t.me/learningnets

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.

https://t.me/learningnets

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.

1.7.2.1 Categories

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

https://t.me/learningnets

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).

https://t.me/learningnets

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

https://t.me/learningnets

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

https://t.me/learningnets

	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:

https://t.me/learningnets

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

https://t.me/learningnets

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

https://t.me/learningnets

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

https://t.me/learningnets

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

https://t.me/learningnets

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).

https://t.me/learningnets

Chapter Three: 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)

https://t.me/learningnets

- 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.

https://t.me/learningnets

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 100 m.

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

https://t.me/learningnets

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

https://t.me/learningnets

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

https://t.me/learningnets

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

https://t.me/learningnets

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

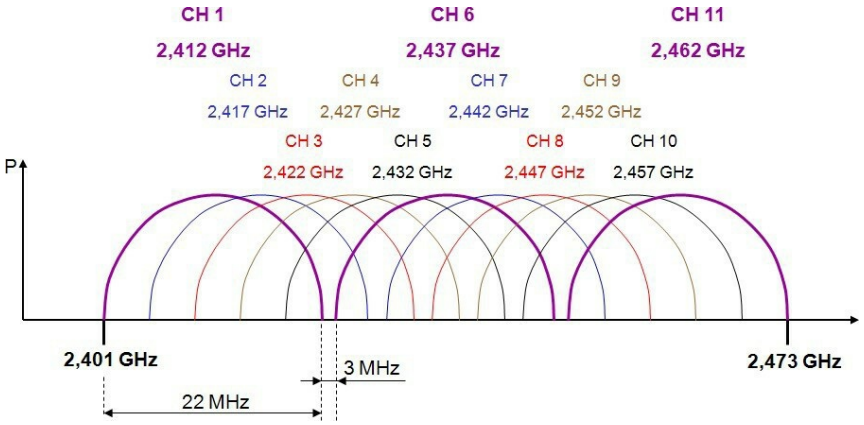
As part of the IEEE802.11 different standards are defined. These standards use different modulation techniques to the transmission speeds to optimize reindeer. The table below shows an overview of the various standards.

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.

https://t.me/learningnets

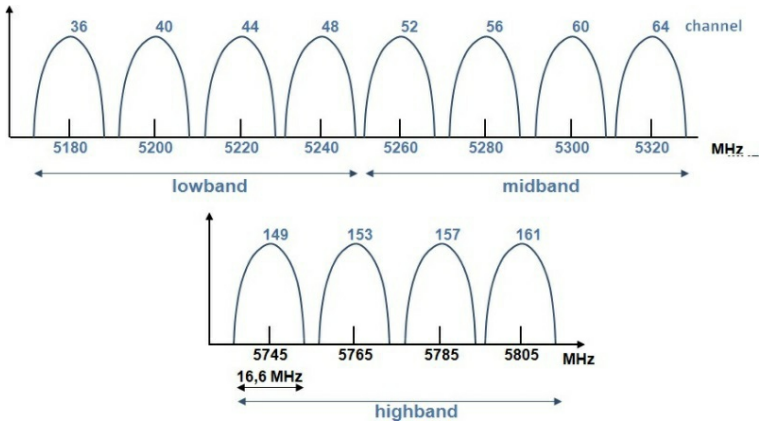


The ETSI defines a slightly larger frequency band with 13 channels wide, each with 22 MHz band. Therefore, generally, 4 to each other hardly-overlapping channels (namely 1, 5, 9, and 13) are used.

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.

https://t.me/learningnets

- 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.

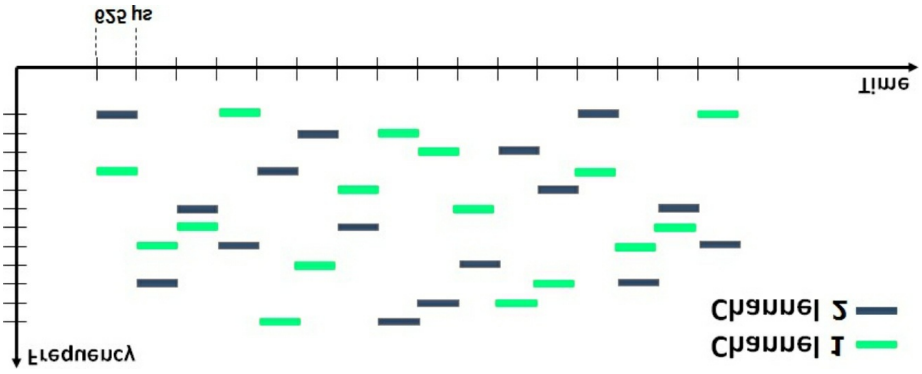
IEEE802.11n

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.

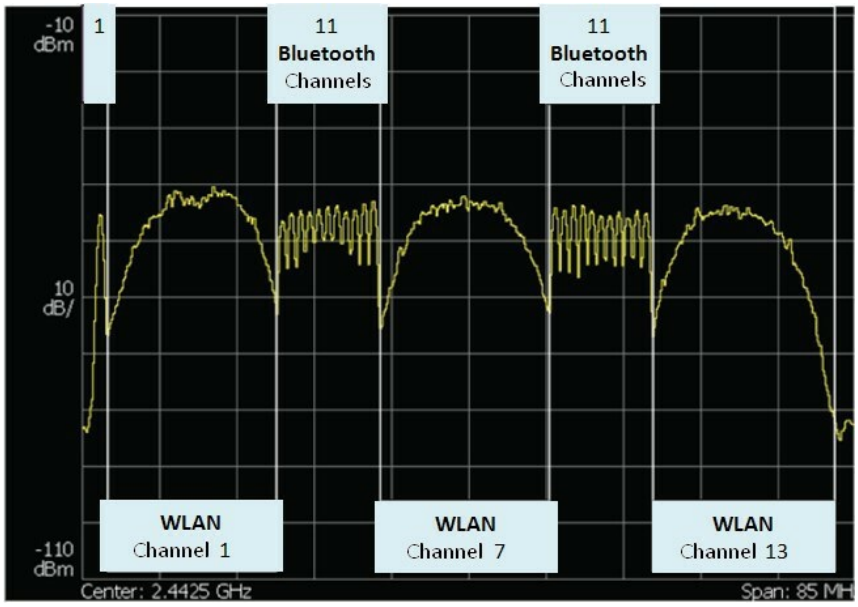


A big advantage of using Bluetooth in the industry is the easy coexistence with WLAN. If it occurs on a Bluetooth frequency interference by a wireless

https://t.me/learningnets

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

https://t.me/learningnets

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:

https://t.me/learningnets

- 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.

https://t.me/learningnets

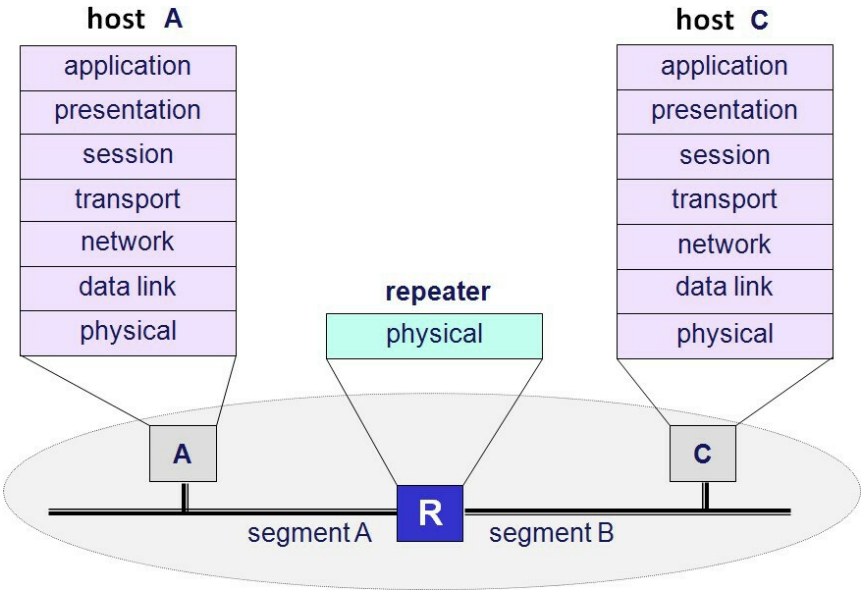
- PIFS (PCF InterFrame Spacing): This time is for polling an access point comparable uses (medium priority).
- DIFS (DCF InterFrame Spacing): This is the lowest priority for access to the medium and applies to a normal subscriber in the wireless segment.

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.



https://t.me/learningnets

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

https://t.me/learningnets

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

https://t.me/learningnets

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.

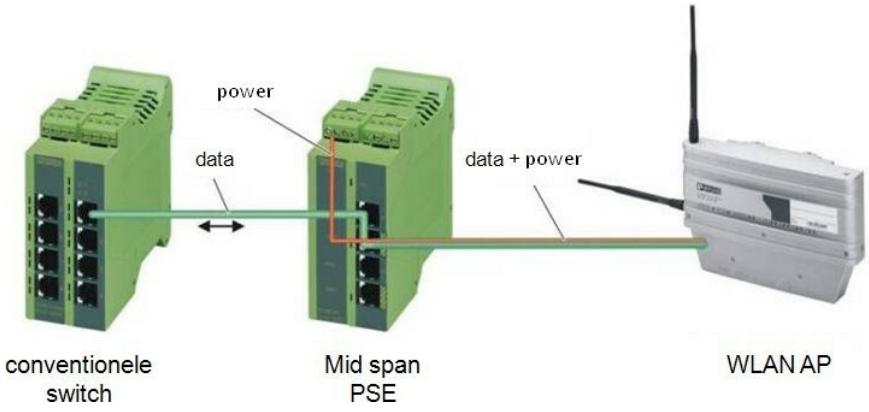
The protocol defines two basic components: the PSE (Power Sourcing Equipment) and the PD (Powered Device).

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

https://t.me/learningnets

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).

https://t.me/learningnets

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.

https://t.me/learningnets

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.

https://t.me/learningnets

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.

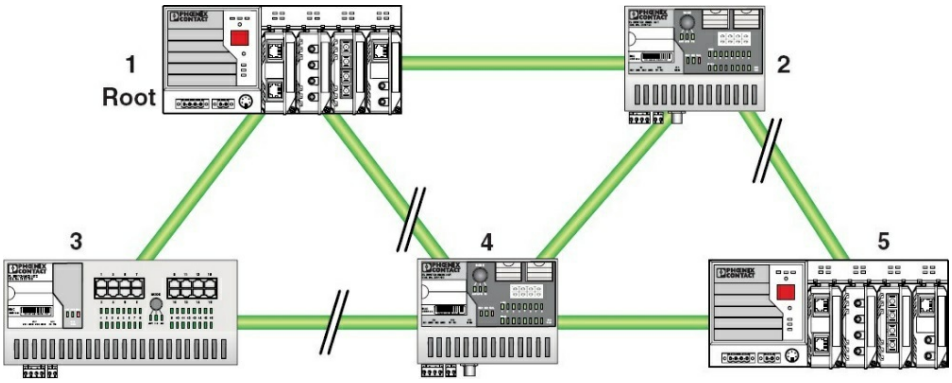
To use this protocol, it must be supported by the used switches. After an interruption of a segment, it can take up to 30 or 50 seconds until the alternative path is available to take. For control applications, such this delay time can not be acceptable, even for monitoring tasks 30 seconds very long.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

https://t.me/learningnets



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

https://t.me/learningnets

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.

https://t.me/learningnets

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.

https://t.me/learningnets

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

https://t.me/learningnets

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.

https://t.me/learningnets

Chapter Four: 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.

https://t.me/learningnets

- 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

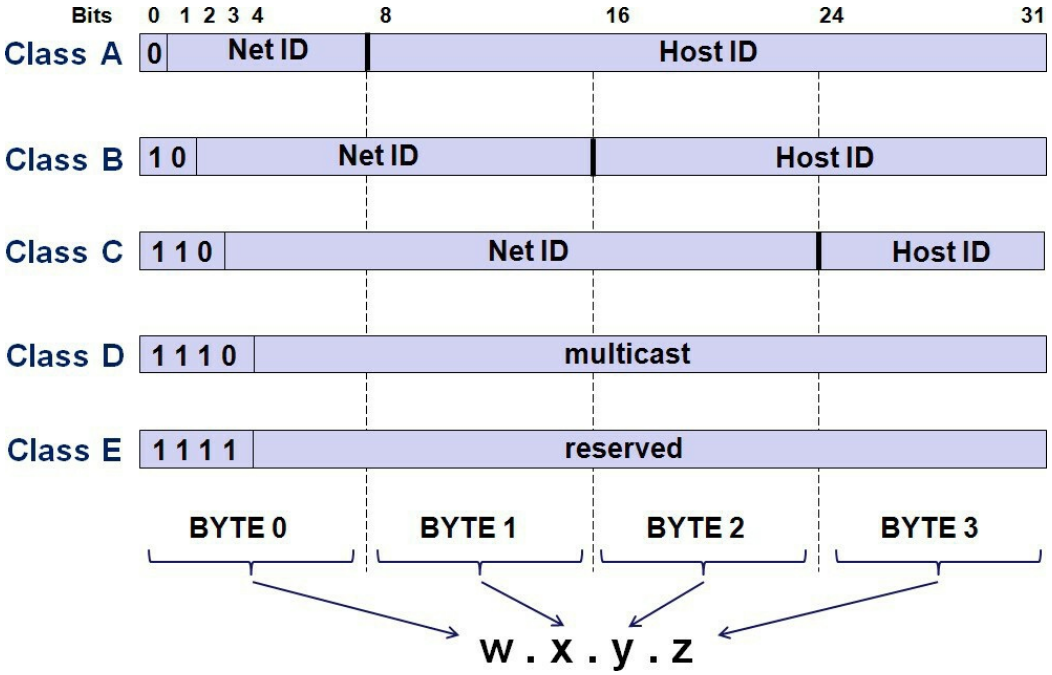
Generally, An IP address consists of 32 bits or 4 bytes, which are represented by 4 separated by a point decimal number.

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.

https://t.me/learningnets



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 Host ID range example	Byte 1, the first bit is 0, (0 xxxxxxx) 126 possible network addresses 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

https://t.me/learningnets

		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.

https://t.me/learningnets

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.

https://t.me/learningnets

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.

https://t.me/learningnets

- 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

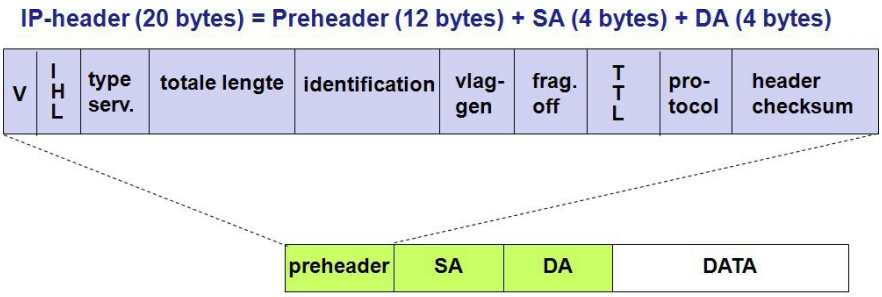
The information that needs to be transmitted is moved to the Internet layer from the transport layer. The information is packed by the internet layer packs in the field of data and then includes the IP header. This IP packet is then passed layer for further processing of the mediation. Sending data to 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.

https://t.me/learningnets



IP packet

- 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.

https://t.me/learningnets

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.

https://t.me/learningnets

- 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,

https://t.me/learningnets

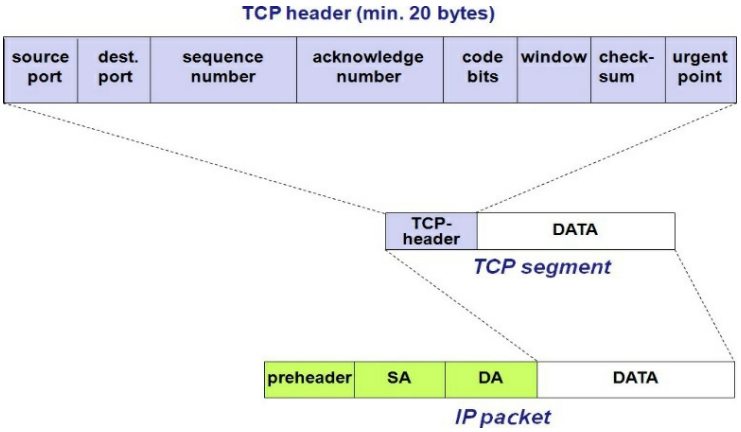
the data is sent again (see also the next Figure).

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

https://t.me/learningnets

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

https://t.me/learningnets

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

https://t.me/learningnets

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 col)	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 proto- col)	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

https://t.me/learningnets

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

https://t.me/learningnets

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.

https://t.me/learningnets

Chapter Five: 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.

4.2 BootP and DHCP

https://t.me/learningnets

4.2.1 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

https://t.me/learningnets

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

https://t.me/learningnets

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

https://t.me/learningnets

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.

https://t.me/learningnets

```
H:\PIH\personeel\henk.capoen>ping 192.168.1.1

Pingen naar 192.168.1.1 met 32 byte gegevens:

Antwoord van 192.168.1.1: bytes=32 tijd=3 ms TTL=64
Antwoord van 192.168.1.1: bytes=32 tijd=4 ms TTL=64
Antwoord van 192.168.1.1: bytes=32 tijd=3 ms TTL=64
Antwoord van 192.168.1.1: bytes=32 tijd=4 ms TTL=64

Ping-statistieken voor 192.168.1.1:
    Pakketten: verzonden = 4, ontvangen = 4, verloren = 0
    (0% verlies).De gemiddelde tijd voor het uitvoeren van één bewerking in mill
iseconden:
    Minimum = 3ms, Maximum = 4ms, Gemiddelde = 3ms
```

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:

https://t.me/learningnets

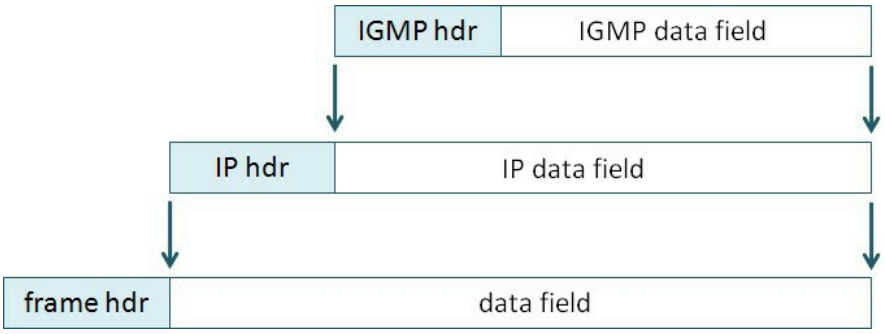
- Belonging to a group is dynamic: hosts can always leave the group or join a group.
- Hosts can subside- KISSING by sending IGMP messages multicast groups.
- Group size is not limited. The various participants can be distributed across multiple networks, provided that the intervening router IGMP sub 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.



https://t.me/learningnets

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

https://t.me/learningnets

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

https://t.me/learningnets

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

https://t.me/learningnets

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

https://t.me/learningnets

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

https://t.me/learningnets

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:

https://t.me/learningnets

- 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

https://t.me/learningnets

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

https://t.me/learningnets

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. "

https://t.me/learningnets

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.

https://t.me/learningnets

Chapter Six: 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

https://t.me/learningnets

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

https://t.me/learningnets

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

https://t.me/learningnets

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

https://t.me/learningnets

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)

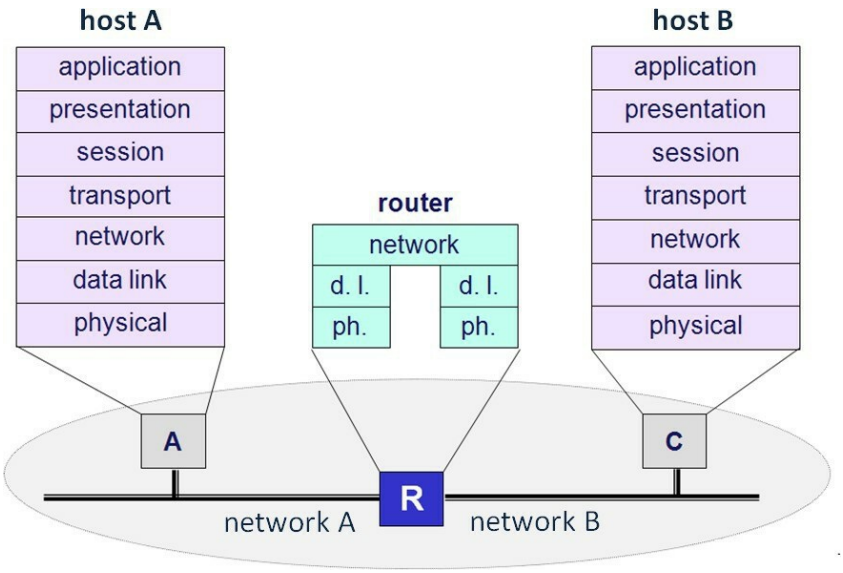
https://t.me/learningnets

- 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

https://t.me/learningnets

Chapter Seven: 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

https://t.me/learningnets

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

https://t.me/learningnets

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

https://t.me/learningnets

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.

https://t.me/learningnets

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.

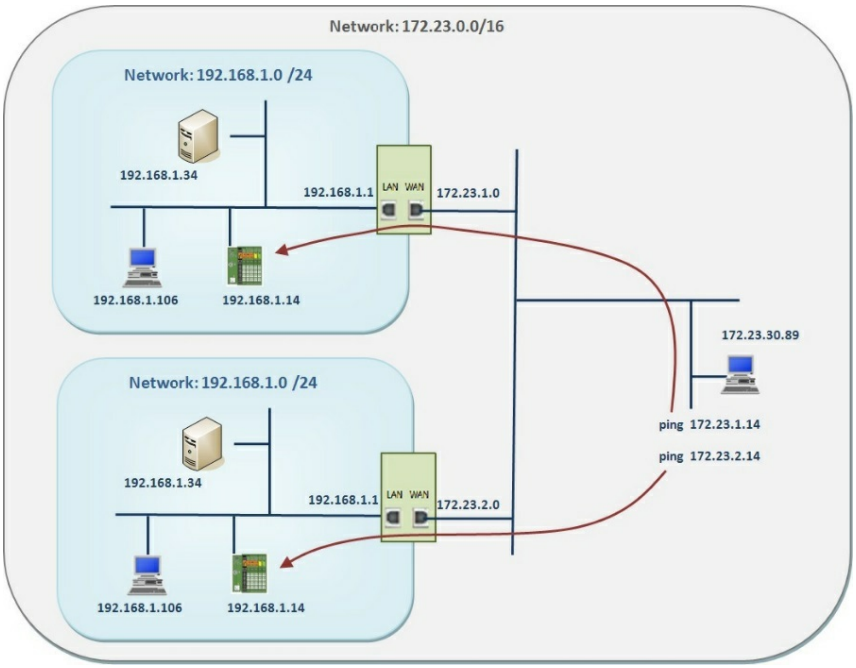
If a router on the LAN side to the network 192.168.1.0/24 and via the WAN port is connected to the network 10.1.0.0/16 and has as external IP address 10.1.1.0/16, then using the 1: 1 NAT LAN nodes with the IP address 192.168.1.100 accessible on the WAN side through the IP address of 10.1.1.100.

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.

https://t.me/learningnets



https://t.me/learningnets

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

https://t.me/learningnets

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);

https://t.me/learningnets

- 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!

https://t.me/learningnets

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

https://t.me/learningnets