S. B. JAIN INSTITUTE OF TECHNOLOGY, MANAGEMENT
& RESEARCH, NAGPUR.
(An Autonomous Institute, Affiliated to RTMNU, Nagpur)
DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING
Vision: To become a center for quality education in the field of Computer Science & Engineering and to create competent professionals.

Session 2021-22

Computer Networks

(BECSE309P)

LAB MANUAL

Year: III

Semester: VI

Computer Networks [BECSE310P]

Hardware and Software Requirement

Hardware Requirement

- Processor : Dual Core
- RAM : 1GB
- Hard Disk Drive :> 80 GB

Software Requirement

- Operating System: Windows
- UML Tool : Packet Tracer/ Omnet++

Institute Vision

Emerge as a leading Institute for developing competent and creative Professionals Mission.

Institute Mission

- Providing Quality Infrastructure and experienced faculty for academic excellence.
- Inculcating skills, knowledge and opportunities for competency and creativity.
- Aligning with Industries for knowledge sharing, research and development.

Vision

To become a center for quality education in the field of computer science & engineering and to create competent professionals.

Mission

- To provide academic ambience and latest software tools to prepare competent Software Engineers with strong theoretical and practical knowledge.
- To foster professionalism and strong work ethics in students for the betterment of Society.
- To provide adequate infrastructure as well as experienced & skilled faculty members.
- To encourage the spirit of entrepreneurship and adaptability in our students in view of the ever-changing scenario of the Software Industry.

Course Outcomes

C309P.1:-Use Network Related commands and configuration files in Linux OperatingSystem.

C309P.2:-Develop Network Application and its Programs.

C309P.3:-Analyze Network Traffic using network Monitoring Tools

C309P.4:-Setup and configure FTS, WLAN,HTTP server

GENERAL INSTRUCTIONS FOR STUDENTS

DO'S

- Students should enter into the Laboratory with prior permission.
- Students should come in proper uniform.
- Students should come with Practical note book to the laboratory.
- Students should maintain silence inside the laboratory.
- After completing the laboratory exercise, make sure to shut down the system and arrange chairs properly.

DONT'S

- Students bringing the bags inside the laboratory.
- Students using mobile phones inside the laboratory.
- Students using the computers in an improper way.
- Students scribbling on the desk and mishandling the chairs.
- Students making noise inside the laboratory.

List of Practicals

Sr. No.	Aim of Practical	Unit No.	CO Mapped
1	To understand and execute various networking commands	1	C310P.1
2	To determine the class of IP address	1	C310P.1
3	Configure different types of Network cables and Practically implement the cross-wired cable and straight through cable using clamping tool.	2 , 4	C310P.2,1
4	Installation and Use of network simulation in Packet Tracer/omnet++	3	C310P.2,1
5	Network design and implementation for small network using actual physical components with IP address scheme.	3	C310P.2,1
6	Study and Use of Different Networking Devices in Networks	3	C310P.3
7	Study and Implementation of Basic routing Protocols.	4	C310P.3
8	Configuration of DHCP server using packet tracer.	4	C310P.3
9	To implement Open shortest path first routing algorithm	5	C310P.4
10	Configure a Network using Distance Vector Routing protocol.	4	C310P.4
Practical number 16 to 19 based on Content beyond syllabus/Mini Project			
11	Installation of ftp server and client	4	C310P.4
12	To implement and configure Switch Port Security in Packet Tracer	5	C310P.4
13	Open Ended Practical	--	----

Practical No. 1

Aim: Execution of basic network command and network configuration commands.

INLAB AIM : Execution of basic network command and network configuration commands.

OBJECTIVES:

- To study and execute netwoking commands
- To study and execute network configuration commands
- To be able to access systems either directly or through services like mail and the web.

AIM: Execution of basic network command and network configuration commands.

INLAB

INLAB AIM : Execution of basic network command and network configuration commands.

OBJECTIVES:

- To study and execute netwoking commands
- To study and execute network configuration commands
- To be able to access systems either directly or through services like mail and the web.

THEORY:

A network consists of several computers connected together. The network can be as simple as a few computers connected in your home or office, or as complicated as a large university network or even the entire Internet. When a computer is part of a network, using this commands we can access to those systems either directly or through services like mail and the web.

1. Ping Command

ping IP Address sends an ICMP *ECHO_REQUEST* packet to the specified host. If the host responds, you get an ICMP packet back. "ping" an IP address is used to see if a machine is alive. If there is no response, there is something wrong.

2. Traceroute

This network command will tell us where the package is going through (machines, switches, routers) and check that our network is working properly.

3. Host Command:

host command is used to map names to IP addresses.

4. Netstat

Network command identifies all TCP connections and UDP open on a machine. It allows to know the following information:

- Routing tables to meet our network interfaces and its outputs.
- Ethernet statistics that show sent and received packages and possible errors.
- To know the id of the process that is being used by the connection.

5. Whois

This network command is used to query data domains: to find out who owns the domain, when that domain expires, to view the configured logs, contact details, etc.

6. ssh command

Command to run terminals on remote machines safely. SSH allows any user to run a console just by registering and entering his credentials. So you can run the commands you want as if you were in local.

7. ifconfig

View network configuration, it displays the current network adapter configuration. It is handy to determine if you are getting transmit (TX) or receive (RX) errors.

8. nslookup:

If one know the IP address it will display hostname. To find all the IP addresses for a given domain name, the command nslookup is used. One must have a connection to the internet for this utility to be useful,

9. finger

View user information, displays a user's login name, real name, terminal name and write status. this is pretty old Unix command and rarely used nowadays.

10. telnet

Connects destination host via the telnet protocol, if telnet connection establishes on any port means connectivity between two hosts is working fine.

CODE:

OUTPUT:

CONCLUSION:

DISCUSSION AND VIVA VOCE:

1. Which command shows the response times at each host ?
2. Which command is used to map names to IP addresse ?
3. Which command shows connectivity between your machine and another machine on the network ?
4. Which command is used to measure the “speed” or latency time?

REFERENCE:

- *SRM University*
- *http://javarevisited.blogspot.in/2010/10/basic-networking-commands-in- linuxunix.html#axzz4y6Ylt1e0*
- *https://slackbook.org/html/basic-network-commands.html*

Practical No. 2

Aim: To determine the classes of IP address.

INLAB AIM: To determine the classes of IP address

OBJECTIVES:

- To study how to get started on learning about IP addresses
- To study and able to identify the class of an address

AIM: To determine the classes of IP address

INLAB AIM To determine the classes of IP address

OBJECTIVES:

- To study how to get started on learning about IP addresses
- To study and able to identify the class of an address

THEORY:

Classes of IP addresses

TCP/IP defines five classes of IP addresses: class A, B, C, D, and E. Each class has a range of valid IP addresses. The value of the first octet determines the class. IP addresses from the first three classes (A, B and C) can be used for host addresses. The other two classes are used for other purposes – class D for multicast and class E for experimental purposes.

The system of IP address classes was developed for the purpose of Internet IP addresses assignment. The classes created were based on the network size. For example, for the small number of networks with a very large number of hosts, the Class A was created. The Class C was created for numerous networks with small number of hosts.

Classes of IP addresses are:

Class	First octet value	Subnet mask
A	0-127	8
B	128-191	16
C	192-223	24
D	224-239	-
E	240-255	-

For the IP addresses from Class A, the first 8 bits (the first decimal number) represent the network part, while the remaining 24 bits represent the host part. For Class B, the first 16 bits (the first two numbers) represent the network part, while the remaining 16 bits represent the host part. For Class C, the first 24 bits represent the network part, while the remaining 8 bits represent the host part.

CODE:

OUTPUT:

CONCLUSION:

DISCUSSION AND VIVA VOCE:

1. What is the IP address and its format?
2. What are the different Classes of IP address and give the range of each class?
3. What is the subnet mask?
4. What is Default Gateway
5. What are Pvt. IP address?

REFERENCE:

- *https://study-ccna.com/classes-of-ip-addresses/*
- https://www.paessler.com/it-explained/ip-address
- https://www.geeksforgeeks.org/introduction-of-classful-ip-addressing/

Practical No. 3

Aim: Practically implement the cross-wired cable and straight through cable using clamping tool.

INLAB AIM : Practically implement the cross-wired cable and straight through cable using clamping tool.

OBJECTIVES:

- To make straight wire cable to connect pc to hub/switch/router
- To make cross cable for connecting same kind of devices

AIM: Practically implement the cross-wired cable and straight through cable using clamping tool.

INLAB

INLAB AIM : Practically implement the cross-wired cable and straight through cable using clamping tool.

OBJECTIVES:

- To make straight wire cable to connect pc to hub/switch/router
- To make cross cable for connecting same kind of devices

THEORY:

Start by stripping off about 2 inches of the plas tic jacket off the end of the cable. Care should be taken to not nick or cut into the wires, which are inside. Doing so could alter the characteristics of your cable, or even worse render is useless. Check the wires, one more time for nicks or cuts. If there are any, just whack the whole end off, and start over.

Spread the wires apart, but be sure to hold onto the base of the jacket with your other hand. You do not want the wires to become untwisted down inside the jacket. Category 5 cable must only have 1/2 of an inch of 'untwisted' wireat the end; otherwise it will be 'out of spec'. At this point, you obviously have ALOT more than 1/2 of an inch of un-twisted wire.

You have 2 end jacks, which must be installed on your cable. If you are using a pre-made cable, with one of the ends whacked off, you only have one end to install - the crossed over end. Below are two diagrams, which show how you need to arrange the cables for each type of cable end. Decide at this point which end you are making and examine the associated picture below.

CODE:

OUTPUT:

CONCLUSION:

DISCUSSION AND VIVA VOCE:

6. Which are the diffrent types of cable?
7. What is cross over cable?
8. When to use fiber optics cables?
9. Which are the diffrent types of connector?
10. Which are the category 5 cables?

REFERENCE:

- *https://networkwolves.wordpress.com/.../types-of-network-communication-medium*
- http://cs-study.blogspot.in/2012/10/networking-cables-and-connections.html
- https://www.computerhope.com/issues/ch000639.html
- http://www.ace-edu.in/wp-content/

Practical No. 4

Aim: Installation and Use of network simulation in Packet Tracer.

INLAB AIM: Installation and Use of network simulation in Packet Tracer.

OBJECTIVES:

- To understand the installation and use of network simulator.
- To understand working of network simulatori.e. Packet Tracer.

AIM: Installation and Use of network simulation in Packet Tracer.

INLAB

INLAB AIM : Installation and Use of network simulation in Packet Tracer.

OBJECTIVES:

- To understand the installation and use of network simulator.
- To understand working of network simulatori.e. Packet Tracer.

THEORY:

Packet Tracer is virtual networking simulation software developed by Cisco, to learn and understand various concepts in computer networks. Networking devices appear in packet tracer as they look in reality and a student can interact with various networking devices, by customizing the configurations, by turning them on and off etc. Packet Tracer is teaching and learning software and a tool, easy to work with, thus after working with virtual environment, a student gains lot of confidence, when it comes to working in real-time environment. We can track the path of a packet, when it moves from source to destination, and also learn and understand, how to troubleshoot a network, when a packet doesn't reach the destination. Packet Tracer can be used to learn concepts more clearly by creating different scenarios. Since Networking is all about imagination and it's difficult to track movement of packets in a real-time environment, thus various networking concepts can be explained by creating a virtual environment, showing the moment of packets, exactly as it would happen in real-time. Packet tracer can be used to understand the working of various networking devices, their use, what makes them different and their appropriate use in a designing a network. Packet tracer is a user friendly tool, with various options, where a user can customize and design a network. Various tests can be run, to understand various network failures and how to troubleshoot them in real-time.

Packet creates a simulation environment where a student gets visualization experience. An instructor can set up an activity wizard to assess the students by giving them different grades. There is also a multi-user feature, where students at different physical locations can work together on the same project, assignment or lab. Packet tracer has both Logical and physical workspace to create customized scenario based labs and it has got both Real-time and simulation Modes to understand various networking concepts, the same way as it would have

happened in realtime. Packet trace also has got user friendly GUI and CLI interfaces, which are easy to work with and doesn't need any experience or expertise. Another most important feature of packet tracer is that it can support multiple languages and it is platform independent. It is an open-source software which can be downloaded free of cost from the internet. Packet tracer also helps to understand the concept of logical troubleshooting and it can also be used for case studies. There are integrated tutorials along with the software to understand use of various features of packet tracer. It also supports group and individual labs, homework, exams, games, problem solving etc.

OUTPUT:

CONCLUSION:

DISCUSSION AND VIVA VOCE:

1. What is the key advantage of using switches?
2. When does network congestion occur?
3. What is protocol?
4. What is MAC?
5. What is a Window in networking terms?

REFERENCE:

- https://www.computernetworkingnotes.com/ccna-study-guide/how-to-install-and-start-packet-tracer-in-ubuntu.html
- https://askubuntu.com/questions/864226/installing-cisco-packet-tracer-7-on-ubuntu-16-10
- https://www.computernetworkingnotes.com/ccna-study-guide/download-packet-tracer-for-windows-and-linux.html
- https://ipwithease.com/how-to-install-packet-tracer-on-windows-system/

Practical No. 5

Aim: Network design and implementation for small network using actual physical components with IP address scheme.

INLAB AIM : Network design and implementation for small network using actual physical components with IP address scheme.

OBJECTIVES:

- To understand Network design and implementation.
- To understand how physical components connects with IP address.

AIM: Network design and implementation for small network using actual physical components with IP address scheme.

INLAB

INLAB AIM : Network design and implementation for small network using actual physical components with IP address scheme.

OBJECTIVES:

- To understand Network design and implementation.
- To understand how physical components connects with IP address.

THEORY:

Designing the Network

The first phase in the life of a network--designing the network--involves making decisions about the type of network that best suits the needs of your organization. Some of the planning decisions you make will involve network hardware; for example:

- Number of host machines your network can support
- Type of network media to use: Ethernet, token ring, FDDI, and so on
- Network topology; that is, the physical layout and connections of the network hardware
- Types of hosts the network will support: standalone and dataless

Based on these factors, you can determine the size of your local-area network.

Factors Involved in Network Planning

After you have completed your hardware plan, you are ready to begin network planning, from the software perspective.

As part of the planning process you must:

1. Obtain a network number and, if applicable, register your network domain with the InterNIC.
2. Devise an IP addressing scheme for your hosts, after you receive your IP network number.
3. Create a list containing the IP addresses and host names of all machines that make up your network, which you can use as you build network databases.
4. Determine which name service to use on your network: NIS, NIS+, DNS, or the network databases in the local /etc directory.
5. Establish administrative subdivisions, if appropriate for your network.
6. Determine if your network is large enough to require routers, and, if appropriate, create a network topology that supports them.
7. Set up subnets, if appropriate, for your network.

The remainder of this chapter explains how to plan your network with these factors in mind.

Setting Up an IP Addressing Scheme

The number of machines you expect to support will affect several decisions you need to make at this stage of setting up a network for your site. Your organization might require a small network of several dozen standalone machines located on one floor of a single building. Alternatively, you might need to set up a network with more than 1000 hosts in several buildings. This arrangement can require you to further divide your network into subdivisions called subnets. The size of your prospective network will affect:

- Network class you apply for
- Network number you receive
- IP addressing scheme you use for your network

Obtaining a network number and then establishing an IP addressing scheme is one of the most important tasks of the planning phase of network administration.

CODE:

OUTPUT:

CONCLUSION:

DISCUSSION AND VIVA VOCE:

1. What is design of network?
2. How design of network implemented?
3. What indicates the starting and ending of network address?

REFERENCE:

- https://docs.oracle.com/cd/E19455-01/806-0916/6ja85398p/index.html
- https://www.ciscopress.com/articles/article.asp?p=2189637&seqNum=4
- https://librarytechnology.org/document/1236

Practical No. 6

Aim: Study and Use of Different Networking Devices in Networks.

INLAB AIM : Study and Use of Different Networking Devices in Networks.

OBJECTIVES:

- To understand different networking devices in networks.
- To understand in network simulation how to use and connect different networking devices.

AIM: Study and Use of Different Networking Devices in Networks.

INLAB

INLAB AIM : Study and Use of Different Networking Devices in Networks..

OBJECTIVES:

- To understand different networking devices in networks.
- To understand in network simulation how to use and connect different networking devices.

THEORY:
Procedure: Following should be done to understand this practical.

1. Repeater: Functioning at Physical Layer.Arepeater is an electronic device that receives a signal and retransmits it at a higher level and/or higher power, or onto the other side of an obstruction, so that the signal can cover longer distances. Repeater have two ports ,so cannot be use to connect for more than two devices
2. Hub: An Ethernet hub, active hub, network hub, repeater hub, hub or concentrator is a device for connecting multiple twisted pair or fiber optic Ethernet devices together and making them act as a single network segment. Hubs work at the physical layer (layer 1) of the OSI model. The device is a form of multiport repeater. Repeater hubs also participate in collisiondetection, forwarding a jam signal to all ports if it detects a collision.
3. Switch: Anetwork switch or switching hub is a computer networking device that connects network segments.The term commonly refers to a network bridge that processes and routes dataat the data link layer (layer 2) of the OSI model. Switches that additionally process data at thenetwork layer (layer 3 and above) are often referred to as Layer 3 switches or multilayer switches.
4. Bridge: A network bridge connects multiple network segments at the data link layer (Layer 2) of the OSI model. In Ethernet networks, the term bridge formally means a device that behavesaccording to the IEEE 802.1D standard. A bridge and switch are very much alike; a switch beinga bridge with numerous ports. Switch or Layer 2 switch is often used interchangeably with
bridge .Bridges can analyze incoming data packets to determine if the bridge is able to send the given packet to another segment of the network.
5. Router: A router is an electronic device that interconnects two or more computer networks, and selectively interchanges packets of data between them. Each data packet contains address information that a router can use to determine if the source and destination are on the same network, or if the data packet must be transferred from one network to another. Where multiple routers are used in a large collection of interconnected networks, the routers exchange information about target system addresses, so that each router can build up a table showing the preferred paths between any two systems on the interconnected networks.
6. GateWay: In a communications network, a network node equipped for interfacing with another network that uses different protocols. • A gateway may contain devices such as protocol translators, impedance matchingdevices, rate converters, fault isolators, or signal translators as necessary to providesystem interoperability. It also requires the establishment of mutually acceptableadministrative procedures between both networks. • A protocol translation/mapping gateway interconnects networks with different networkprotocol technologies by performing the required protocol conversions.

Task:

OUTPUT:

CONCLUSION:

DISCUSSION AND VIVA VOCE:

1. What is the difference between Hub and Switch?
2. What are the advantages and disadvantages of Switch?
3. What happens when central hub fails in the Network?
4. What are the advantages and disadvantages of Bridge?

REFERENCE:

- https://www.elprocus.com/what-are-network-devices-and-their-types/#:~:text=The%20network%20device%20is%20one,modem%2C%20repeater%20%26%20access%20point. http://www.differencebetween.info/different-types-of-network-topologies
- https://www.geeksforgeeks.org/network-devices-hub-repeater-bridge-switch-router-gateways/
- https://www.tutorialspoint.com/communication_technologies/communication_technologies_network_devices.htm

Practical No. 7

Aim: Study and Implementation of Basic routing Protocols.

INLAB AIM : Study and Implementation of Basic routing Protocols.

OBJECTIVES:

- To understand routing protocols methods in computer networks.
- To understand the Implementation of Basic routing Protocols.

AIM: Study and Implementation of Basic routing Protocols.

INLAB AIM: Study and Implementation of Basic routing Protocols.

OBJECTIVES:

- To understand routing protocols methods in computer networks.
- To understand the Implementation of Basic routing Protocols.

THEORY:

Routing protocols are mechansims by which routing information is exchanged between routers so that routing decisions can be made. In the Internet, there are three types of routing protocols commonly used. They are: distance vector, link state, and path vector.the basic concepts and fundamentals behind each of these three types of protocols in a generic framework. Routing protocols, being distributed mechanisms, can face pitfalls during a transient period such as looping. Thus, we also discuss such issues and how various efforts are made to address them. Steps to translate these protocols to actual routing protocol specifications on the Internet

IGRP

The networking community began to realize the limitations of the RIP protocol (which we will see later in the chapter), and something had to be done. Many years ago, the Internet Engineering Task Force (IETF) had not yet formalized the specifications for OSPF, so Cisco had the option of waiting for the specifications, or continuing to develop their own protocol. They chose to implement their own protocol, which turned out to be Interior Gateway Routing Protocol (IGRP).

The alternative to distance-vector routing is Shortest Path First (SPF) routing, which we will discuss in great detail in the section on Open Shortest Path First (OSPF). This is a link-state technology in which each router contains an identical database.

Routing Updates

When a router using EIGRP comes online, the first thing it will do is try to find all its neighbors. It will then try to form an association with them. Once this association is formed, the router and its neighbors will advertise their entire routing tables to each other. But, after this initial synchronization, only updates will be transmitted between neighbors, not the entire

routing table.

RTP

EIGRP uses Reliable Transport Protocol (RTP) to communicate with neighbors. When communicating with neighbors, EIGRP will first send out information to its neighbors using the multicast address of 224.0.0.10. EIGRP will keep a list of neighbors who have replied to the message. If a reply is not sent back from one of its neighbors, then EIGRP will start using unicasts to talk to the neighbor. After 16 attempts, if there is no response back, the neighbor will be considered dead and removed from the router's list of neighbors.

ASes

EIGRP uses AS numbers to determine which updates will be processed by each router. For EIGRP updates to be processed, two systems must share the same AS number. This helps cut down on the amount of updates being processed by each router. They will only process updates with the correct AS number.

CODE:

OUTPUT:

CONCLUSION:

DISCUSSION AND VIVA VOCE:

1)what is routing Protocols?

2)Which are the diffrent types of routing protocols?

3)What is RIP?

4)Explain the working of IGRP?

5)How RIP work?

REFERENCE:

- https://www.sciencedirect.com/topics/computer-science/routing-protocol
- https://www.computernetworkingnotes.com/ccna-study-guide/basic-routing-concepts-and-protocols-explained.html
- https://www.ciscopress.com/articles/article.asp?p=2180210&seqNum=7

Practical No. 8

Aim: Configuration of DHCP server using packet tracer.

INLAB AIM : Configuration of DHCP server using packet tracer.

OBJECTIVES:

- To understand DHCP Server.
- To understand the working and simulation of DHCP server using packet tracer.

AIM: Configuration of DHCP server using packet tracer.

INLAB

INLAB AIM : Configuration of DHCP server using packet tracer.

OBJECTIVES:

- To understand DHCP Server.
- To understand the working and simulation of DHCP server using packet tracer.

THEORY:

A DHCP Server is a network server that automatically provides and assigns IP addresses, default gateways and other network parameters to client devices. It relies on the standard protocol known as Dynamic Host Configuration Protocol or DHCP to respond to broadcast queries by clients.

A DHCP server automatically sends the required network parameters for clients to properly communicate on the network. Without it, the network administrator has to manually set up every client that joins the network, which can be cumbersome, especially in large networks. DHCP servers usually assign each client with a unique dynamic IP address, which changes when the client's lease for that IP address has expired.

When to use a router/switch as your DHCP Server

There are many enterprise companies who are still using DHCP for IPv4 on their routers/switches. This is typically done by the network administrator who needs to get a DHCP capability up and running quickly but does not have access to a DHCP server. Most routers/switches have the ability to provide the following DHCP server support:

- a DHCP client and obtain an interface IPv4 address from an upstream DHCP service
- a DHCP relay and forward UDP DHCP messages from clients on a LAN to and from a DHCP server
- a DHCP server whereby the router/switch services DHCP requests directly. However, there are limitations to using a router/switch as a DHCP server
- Running a DHCP server on a router/switch consumes resources on the network device. These DHCP packets are handled in software (not hardware accelerated forwarding). The resources required make this practice not suitable for a network with a large number (> 150) of DHCP clients.

- Does not support dynamic DNS. The router/switch DHCP server cannot create an entry into DNS on behalf of the client based on the IPv4 address that was leased to the client.
- No ability to e asilymanage the scope and see the current DHCP bindings and leases across multiple routers. Administrator must log into the switch/router individually to get information about DHCP bindings.
- No high availability or redundancy of the DHCP bindings. This could cause problems if the current DHCP server and default gateway fails.
- It is more difficult to configure DHCP options on router/switch platform.
- The DHCP service running on a router/switch is not integrated with IP address management (IPAM) for address tracking and scope utilization or security forensics.

OUTPUT:

CONCLUSION:

DISCUSSION AND VIVA VOCE:

1. What do you mean by DHCP Server?
2. How DHCP Server works?
3. What is the difference between BOOTP and DHCP?
4. What are the advantages of DHCP Server?

REFERENCE:

- https://www.infoblox.com/glossary/dhcp-server/
- https://www.efficientip.com/what-is-dhcp-and-why-is-it-important/
- https://docs.microsoft.com/en-us/windows-server/networking/technologies/dhcp/dhcp-top

Practical No. 9

Aim: To implement Open shortest path first routing algorithm.

INLAB AIM : To implement Open shortest path first routing algorithm.

OBJECTIVES:

- To understand Open shortest path first routing algorithm.
- To understand the working and simulation Open shortest path first routing algorithm.

AIM: To implement Open shortest path first routing algorithm.

INLAB

INLAB AIM : To implement Open shortest path first routing algorithm.

OBJECTIVES:

- To understand Open shortest path first routing algorithm.
- To understand the working and simulation Open shortest path first routing algorithm.

THEORY:

The OSPF (Open Shortest Path First) protocol is one of a family of IP Routing protocols, and is an Interior Gateway Protocol (IGP) for the Internet, used to distribute IP routing information throughout a single Autonomous System (AS) in an IP network.

The OSPF protocol is a link-state routing protocol, which means that the routers exchange topology information with their nearest neighbors. The topology information is flooded throughout the AS, so that every router within the AS has a complete picture of the topology of the AS. This picture is then used to calculate end-to-end paths through the AS, normally using a variant of the Dijkstra algorithm. Therefore, in a link-state routing protocol, the next hop address to which data is forwarded is determined by choosing the best end-to-end path to the eventual destination.

The main advantage of a link state routing protocol like OSPF is that the complete knowledge of topology allows routers to calculate routes that satisfy particular criteria. This can be useful for traffic engineering purposes, where routes can be constrained to meet particular quality of service requirements. The main disadvantage of a link state routing protocol is that it does not scale well as more routers are added to the routing domain. Increasing the number of routers increases the size and frequency of the topology updates, and also the length of time it takes to calculate end-to-end routes. This lack of scalability means that a link state routing protocol is unsuitable for routing across the Internet at large, which is the reason why IGPs only route traffic within a single AS.

Each OSPF router distributes information about its local state (usable interfaces and reachable neighbors, and the cost of using each interface) to other routers using a Link State Advertisement (LSA) message. Each router uses the received messages to build up an identical database that describes the topology of the AS.

From this database, each router calculates its own routing table using a Shortest Path First (SPF) or Dijkstra algorithm. This routing table contains all the destinations the routing protocol knows about, associated with a next hop IP address and outgoing interface.

- The protocol recalculates routes when network topology changes, using the Dijkstra algorithm, and minimises the routing protocol traffic that it generates.
- It provides support for multiple paths of equal cost.
- It provides a multi-level hierarchy (two-level for OSPF) called "area routing," so that information about the topology within a defined area of the AS is hidden from routers outside this area. This enables an additional level of routing protection and a reduction in routing protocol traffic.
- All protocol exchanges can be authenticated so that only trusted routers can join in the routing exchanges for the AS.

OUTPUT:

CONCLUSION:

DISCUSSION AND VIVA VOCE:

5. What do you mean by OSPF?
6. How Open shortest path first routing algorithm works?
7. What is the diffrence between OSPF and BGP?
8. What are the advantages of Open shortest path first routing algorithm?

REFERENCE:

- https://www.metaswitch.com/knowledge-center/reference/what-is-open-shortest-path-first-ospf#:~:text=The%20OSPF%20(Open%20Shortest%20Path,AS)%20in%20an%20IP%20network.
- https://www.geeksforgeeks.org/open-shortest-path-first-ospf-protocol-states/
- https://www.cisco.com/c/en/us/products/ios-nx-os-software/open-shortest-path-first-ospf/index.html

Practical No. 10

Aim: Configure a network using Distance Vector Routing protocol.

INLAB AIM : Configure a network using Distance Vector Routing protocol.

OBJECTIVES:

- To understand Netwok layer services.
- To understand how packets are transmitted using Distance Vector Routing.

AIM: Configure a network using Distance Vector Routing protocol.

INLAB

INLAB AIM : Configure a network using Distance Vector Routing protocol.

OBJECTIVES:

- To understand Netwok layer services.
- To understand how packets are transmitted using Distance Vector Routing.

THEORY:

Distance vector routing is a simple distributed routing protocol. Distance vector routing allows routers to automatically discover the destinations reachable inside the network as well as the shortest path to reach each of these destinations. The shortest path is computed based on metrics or costs that are associated to each link. We use l.costto represent the metric that has been configured for link l on a router.

Each router maintains a routing table. The routing table R can be modelled as a data structure that stores, for each known destination address d, the following attributes :

- R[d].link is the outgoing link that the router uses to forward packets towards destination d
- R[d].cost is the sum of the metrics of the links that compose the shortest path to reach destination d
- R[d].time is the timestamp of the last distance vector containing destination d

A router that uses distance vector routing regularly sends its distance vector over all its interfaces. The distance vector is a summary of the router's routing table that indicates the distance towards each known destination

Task:

OUTPUT:

CONCLUSION:

DISCUSSION AND VIVA VOCE:

1. What do you mean by routing?
2. Which protocol is used by distance vector routing?
3. How routing table is calculated and updated?
4. What are the common characteristics of distance vector routing protocol?

REFERENCE:

- http://cnp3book.info.ucl.ac.be/principles/dv.html
- http://www.ciscopress.com/articles/article.asp?p=24090&seqNum=3
- https://www.youtube.com/watch?v=_SxlpxqIs-s
- http://nptel.ac.in/courses/106105080/pdf/M7L2.pdf

Practical No. 11

Aim: Implementation of FTP Server and FTP Client.

INLAB AIM : Implementation of FTP Server and FTP Client.

OBJECTIVES:

- To understand FTP server and client.
- To implement the working FTP server and client.

AIM: Implementation of FTP Server and FTP Client.

INLAB

OBJECTIVES:

- To understand FTP server and client.
- To implement FTP server and client.

THEORY:

FTP is a commonly used protocol for exchanging files over any network that supports the TCP/IP protocol (such as the Internet or an intranet). There are two computers involved in an FTP transfer: a server and a client. The FTP server, running FTP server software, listens on the network for connection requests from other computers. The client computer, running FTP client software, initiates a connection to the server. Once connected, the client can do a number of file manipulation operations such as uploading files to the server, download files from the server, rename or delete files on the server and so on. Virtually every computer platform supports the FTP protocol. This allows any computer connected to a TCP/IP based network to manipulate files on another computer on that network regardless of which operating systems are involved (if the computers permit FTP access). There are many existing FTP client and server programs, and many of these are free.

OUTPUT:

CONCLUSION:

DISCUSSION AND VIVA VOCE:

1) What is FTP server?
2) How can we connect from FTP client to FTPserver?
3) which are the commands use to connect FTPserver?

4) 4)What is TCP/IP?

5) At which layar of OSI model FTP work?

REFERENCE:

- SRM University
- https://cseweb.ucsd.edu/classes/fa10/cse123/lectures/123-fa10-l12.pdf
- http://nptel.ac.in/courses/106105080/pdf/M7L1.pdf

Practical No. 12

Aim: To implement and configure Switch Port Security in Packet Tracer.

INLAB AIM : To implement and configure Switch Port Security in Packet Tracer.

OBJECTIVES:

- To understand Switch Port Security.
- To understand the working and simulation of Switch Port Security.

AIM: To implement and configure Switch Port Security in Packet Tracer.

INLAB

INLAB AIM : To implement and configure Switch Port Security in Packet Tracer.

OBJECTIVES:

- To understand Switch Port Security.
- To understand the working and simulation of Switch Port Security.

THEORY:

The switchport security feature (Port Security) is an important piece of the network switch security puzzle; it provides the ability to limit what addresses will be allowed to send traffic on individual switchports within the switched network.

Once an organization decides to utilize the switchport security feature on their networks, it is important to carefully plan before any configuration is put in place. While the switchport security feature is very useful if used correctly, it can easily be misconfigured; this misconfiguration can cause service interruption and ongoing headaches for an organization. The planning of the configuration includes determining which violation mode and operation mode to use based on the goals of the organization, as well as determining which switchports should be enabled with the feature. This article takes a look at how the switchport security feature is configured by extending on the concepts that were covered in Switchport Security Concepts.

Switchport Security Configuration

By default, the switchport security feature is disabled on all switchports and must be enabled. Table 1 shows the steps required to enable the switchport security feature on an interface (This can cause some confusion, but when using Cisco IOS, switchport configuration is performed while in interface configuration mode. The terms interface and switchport are interchangeable).

Enter privileged mode	router>**enable**
Enter global configuration mode	router#**configure terminal**
Enter interface configuration mode	router(config)#**interface** *interface*
Enable the switchport security feature	router(config-if)#**switchport port-security**

Without configuring any other specific parameters, the switchport security feature will only permit one MAC address to be learned per switchport (dynamically) and use the shutdown violation mode; this means that if a second MAC address is seen on the switchport the port will be shutdown and put into the err-disabled state.

OUTPUT:

CONCLUSION:

DISCUSSION AND VIVA VOCE:

1. What do you mean by Switch Port Security?
2. How Switch Port Security works?
3. What are the advantages of Switch Port Security?

REFERENCE:

- https://www.pluralsight.com/blog/it-ops/switchport-security-configuration#:~:text=Overview,switchports%20within%20the%20switched%20network.
- https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25ew/configuration/guide/conf/port_sec.html
- https://www.computernetworkingnotes.com/ccna-study-guide/switchport-port-security-explained-with-examples.html

Practical No. 13

Open Ended Practical