Internship

In

“NETWORKING”

At

“ CRISP, BHOPAL”

Department of Computer Science & Engineering (Cyber Security)

Approved by AICTE New Delhi & Govt. of MP Affiliated to Rajiv Gandhi Proudyogiki Vishwavidhyalaya, Bhopal

A report submitted in Partial fulfilment for the Award of the degree of

Bachelor of Technology

In

“Computer Science & Engineering (Cyber Security)”

August, 2023

Submitted to

RAJIV GANDHI PROUDYOGIKI VISHWAVIDHYALAYA, BHOPAL (M.P)

Submitted by

Honey Sharma (0126CY211027)

Under the guidance of: Asst. prof. Arani Tiwari

Phone No.-0755-2529015, 252901

Fax: 0755-2529472

E-mail: directoroct@\oriental.ac.in

Website: http://www.oriental.ac.in/oct-bhopal/

ORIENTAL COLLEGE OF TECHNOLOGY, BHOPAL

Approved by AICTE, New Delhi & Govt. of M.P. Affiliated to Rajiv Gandhi Proudyogiki Vishwavidyalaya, Bhopal Oriental Campus, Raisen Road, Bhopal-462021 (MP) INDIA

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING (CYBER SECURITY)

CANDIDATE'S DECLARATION

I hereby declare that the Industrial training/ internship report on **Networking : CISCO Switching, Routing, Wireless Networ**k which is being presented here for the partial fulfilment of the requirement of Degree of ***"Bachelor of Technology"*** has been carried out at **Oriental College Of Technology**. The technical information provided in this report is presented with due permission of the authorities from the training organization .

Honey Sharma

0126CY211027

ORIENTAL COLLEGE OF TECHNOLOGY, BHOPAL

Approved by AICTE, New Delhi & Govt. of M.P. Affiliated to Rajiv Gandhi Proudyogiki Vishwavidyalaya, Bhopal Oriental Campus, Raisen Road, Bhopal-462021 (MP) INDIA

CERTIFICATE OF INDUSTRY

This is to certify that **Mr. Honey Sharma** of "Computer Science & Engineering (Cyber Security)" Enrollment No. 0126CY211027 has **completed** his Industrial Training / Internship during the academic year 2023-2024 as partial fulfillment of the Bachelor of Engineering in "Computer Science & Engineering (Cyber Security)"

Industrial Guide:- Mr.Kapil Shrivastav
Designation:- (Head Cisco Instructor)

ORIENTAL COLLEGE OF TECHNOLOGY, BHOPAL

Approved by AICTE, New Delhi & Govt. of M.P. Affiliated to Rajiv Gandhi ProudyogikiVishwavidyalaya, Bhopal Oriental Campus, Raisen Road, Bhopal-462021 (MP) INDIA

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING (CYBER SECURITY)

CERTIFICATE OF INSTITUTE

This is to certify that **Mr. Honey Sharma** of B.Tech. Computer Science & Engineering (Cyber Security) Department Enrollment No. 0126CY211027 has **completed** his Industrial Training/Internship during the academic year 2022-2023 as partial fulfillment of the Bachelor of Technology in Computer Science & Engineering (Cyber Security).

Asst.Prof. Arani Tiwari
Supervisor

Prof. Roopali Soni
HOD (CSECY)

ACKNOWLEDGEMENT

First of all, I would like to thank **Mr. Kapil Shrivastava** (Head Cisco Instructor) for giving me this opportunity to do this internship under his supervision . I would like to thank our director, **Dr. Amita Mahor** (Oriental College of Technology) , for providing all facilities.

It is indeed with a great sense of pleasure and immense sense of gratitude that I acknowledge the help of these individuals. I would like to thank my head of department **Prof. Roopali Soni HOD (CSECY)** , for providing this wonderful internship program.

I would also like to thank my faculty coordinator **Asst.Prof.Arani Tiwari** for her support and advice to complete the internship as our T.G. and faculty coordinator. I am extremely grateful to my department, staff members, friends and my family who helps me in the successful completion of this internship. I also would like to thank all my friends who help me complete this internship/training , with their patience and openness and a enjoyable learning environment created.

Finally, I must express my very profound gratitude to my parents for providing me with unfailing support and continuous encouragement throughout my years of study leading to this very moment.

Honey Sharma

0126CY211027

List of tables

Learning Outcomes

- Basic understanding of Computer Networking Technology ,Network Protocols ,Networking Devices , Network Configuration Software.
- Basic Local Area Network (LAN) configuration techniques, Cisco routing ,Configuration Commands with the help of Network Simulation Software CISCO PACKET TRACER.
- Basic Network Device Security techniques, basic port security methods , remote access setup and security.
- Basic understanding Wireless Networks (IEEE 802.11) , wifi configuration on D-link hardwares.
- Wireless Network Security Techniques ,Types of filtering and security methods.

PO:-

- It provided the basic foundation to student for starting their career in computer networking .
- It made students capable of configuring a small LAN network.
- It made students capable of configuring wifi network and securing it .
- It was also helpful for those student who are planning for CCNA certification.

Table of Content

Abstract

Internship Programme on Networking: Cisco Switching ,Routing ,Wireless Network was organised by Department of Cyber Security form 14 August 2023 till 19 August 2023 ,in collaboration with CRISP Bhopal. In this 5-Days Programme students were benefited with basic knowledge in networking, Networking Fundamentals, Protocols, Devices, Connection and Configuration were the main verticals on which the programme was focused on.

Besides this student practised the basic network configuration in LAN with the help of Network Simulation Software (Cisco Packet Tracer).

At last to level up the knowledge of the student they were introduced to the real-world networking devices and the interfaces to configure them.

Wifi Networks, Port Security, Remote Access to any device are some advanced topics that were covered in the internship programme.

In conclusion, the 5-Days internship Programme by CRISP Bhopal was of great significance for students .As students of technical field, industry expect students to have the practical knowledge of networking to deal with the industry level challenges in the field of networking. The programme benefited the student with the practical knowledge of networking.

ABOUT ORANIZATION

Year of establishment - 1997

- Building spread over 2.5 Acres of Land
- Around 30 Labs equipped with latest machines and facilities.
- Conference Halls (4) - each having capacity for 100, 40, 40 & 20 persons.
- Around 250 motivated employees.
- About 500 delighted clients.
- Target Group : Government, Industries, Corporates, Academic Institutions, Multilateral Agencies, Developmental Organisations and the Civil Society.

Areas of Operation & milestones

- Training - Imparted training to 200,000 in : ○ a. Popular Technologies in - Industrial Automation, Manufacturing Technology & Information Technology. ○ b. Behavioral skills & Entrepreneurship development. ○ c. Vocational areas
- Software Application development & e-Governance to more than 50 clients from Governments and Private sector.
- Technical Consultancy ○ a. Engineering applications. ○ b. Established 30 skill development centres.
- Training cum Production Centre - serving around 100 industries.
- Awards received for Quality in delivery, Leadership and Perfection - 12 • Outreach : ○ National :
  - a. Headquarter – Bhopal
  - b. Academies – Bhopal, Indore, Vidisha, Jabalpur c. Skill Development Centres – 21 Districts of MP
- ○ International:
  - a. Training Centre at Addis Ababa in Ethiopia

Planning of Internship Programme

- **TIMING : 10:00 A.M. TO 1:00 P.M.**

- **DURATION : 14 AUGUST 2023 TO 19 AUGUST 2023**

- **VENUE : Crisp, 18, Shyamla Hills Rd, Krishna Nagar, TT Nagar, Bhopal, Madhya Pradesh 462013**

SWOT

Strengths:

- **Hands-On Experience**: You gained practical, hands-on experience in configuring routers, switches, and wireless networks, which is invaluable in the networking field.
- **Technical Skills**: Developed strong technical skills related to network setup, troubleshooting, and maintenance.
- **Problem-Solving:** Enhanced your problem-solving abilities by resolving real-time networking issues during the internship.
- **Industry Relevance**: Acquired skills and knowledge highly relevant to the constantly evolving field of networking.

Weaknesses:

- **Limited Scope**: As a basic networking internship, the exposure might have been limited to fundamental concepts, missing out on advanced or specialized areas.
- **Lack of Depth**: Due to the basic nature of the internship, there might be gaps in in-depth understanding of complex networking protocols and technologies.
- **Dependency on Supervision**: Reliance on supervisors for guidance and decision-making might have limited independent problem-solving opportunities.
- **Limited Exposure**: Might not have had exposure to a wide variety of networking scenarios or technologies.

Opportunities:

- **Further Education**: Use the foundational knowledge gained during the internship as a base to pursue further education or certifications in advanced networking technologies.
- **Specialization**: Explore specific areas within networking such as cybersecurity, cloud networking, or IoT, to broaden your skill set.
- **Networking Events**: Attend networking events, conferences, and workshops to expand your professional network and stay updated with industry trends.
- **Industry Demand**: Leverage the growing demand for networking professionals in various sectors, leading to potential job opportunities. **O Threats**:
- **Technological Advancements**: Rapid advancements in networking technologies might make certain skills obsolete, necessitating continuous learning and adaptation.
- **Competition**: High competition in the job market means staying updated with the latest trends and certifications is crucial to stand out.
- **Economic Factors**: Economic downturns or budget constraints in organizations might reduce opportunities for networking-related jobs.
- **Automation**: Automation in networking processes might reduce the demand for entry-level networking tasks, emphasizing the need for higher-level skills.

TOPICS

1. Networking

1.1 Network:

A computer network is a group of interconnected nodes or computing devices that exchange data and resources with each other. A network connection between these devices can be established using cable or wireless media. Once a connection is established, communication protocols -- such as TCP/IP, Simple Mail Transfer Protocol and Hypertext Transfer Protocol -- are used to exchange data between the networked devices.

The first example of a computer network was the Advanced Research Projects Agency Network. This packet-switched network was created in the late 1960s by ARPA, a U.S. Department of Defense agency.

A computer network can be as small as two laptops connected through an Ethernet cable or as complex as the internet, which is a global system of computer networks.

1.2 Types of Networks:

There are mainly five types of Computer Networks

There are mainly five types of Computer Networks

- Personal Area Network (PAN)
- Local Area Network (LAN)
- Campus Area Network (CAN)
- Metropolitan Area Network (MAN)
- Wide Area Network (WAN)

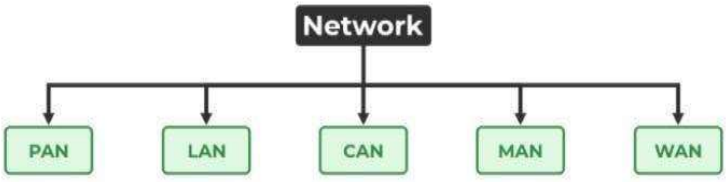


Fig.1.2.1

Personal Area Network (PAN)

PAN is the most basic type of computer network. This network is restrained to a single person, that is, communication between the computer devices is centered only on an individual's workspace. PAN offers a network range of 1 to 100 meters from person to device providing communication. Its transmission speed is very high with very easy maintenance and very low cost.

This uses Bluetooth, IrDA, and Zigbee as technology.
Examples of PAN are USB, computer, phone, tablet, printer, PDA, etc.

Fig.1.2.2

Local Area Network (LAN)

LAN is the most frequently used network. A LAN is a computer network that connects computers through a common communication path, **Local Area Network** contained within a limited area, that is, locally. A LAN encompasses two or more computers connected over a server. The two important technologies involved in this network are Ethernet and Wi-fi. It ranges up to 2km & transmission speed is very high with easy maintenance and low cost.
Examples of LAN are networking in a home, school, library, laboratory, college, office, etc.

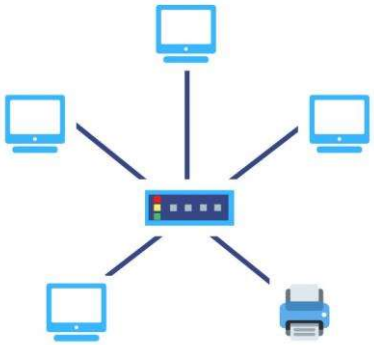


Fig.1.2.1

Campus Area Network (CAN)

CAN is bigger than a LAN but smaller than a MAN. This is a type of computer network that is usually used in places like a school or colleges. This network covers a limited geographical area that is, it spreads across several buildings within the campus. CAN mainly use Ethernet technology with a range from 1km to 5km. Its transmission speed is very high with a moderate maintenance cost and moderate cost.

Examples of CAN are networks that cover schools, colleges, buildings, etc.

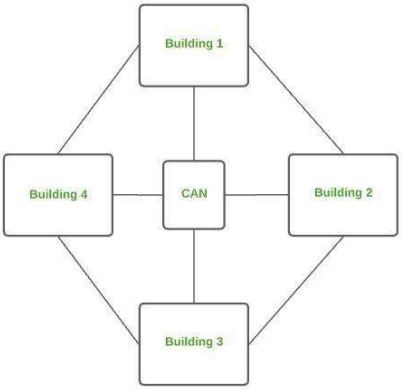


Fig.1.3.1

Metropolitan Area Network (MAN)

A MAN is larger than a LAN but smaller than a WAN. This is the type of computer network that connects computers over a geographical distance through a shared communication path over a city, town, or metropolitan area. This network mainly uses FDDI, CDDI, and ATM as the technology with a range from 5km to 50km. Its transmission speed is average. It is difficult to maintain and it comes with a high cost.

Examples of MAN are networking in towns, cities, a single large city, a large area within multiple buildings, etc.

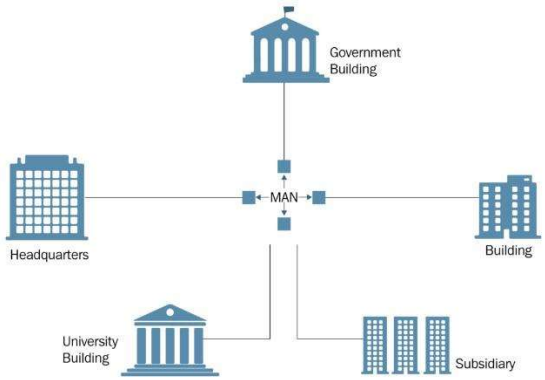


Fig.1.4.1

Wide Area Network (WAN)

WAN is a type of computer network that connects computers over a large geographical distance through a shared communication path. It is not restrained to a single location but extends over many locations. WAN can also be defined as a group of local area networks that communicate with each other with a range above 50km. Here we use Leased-Line & Dial-up technology. Its transmission speed is very low and it comes with very high maintenance and very high cost.

The most common example of WAN is the Internet.

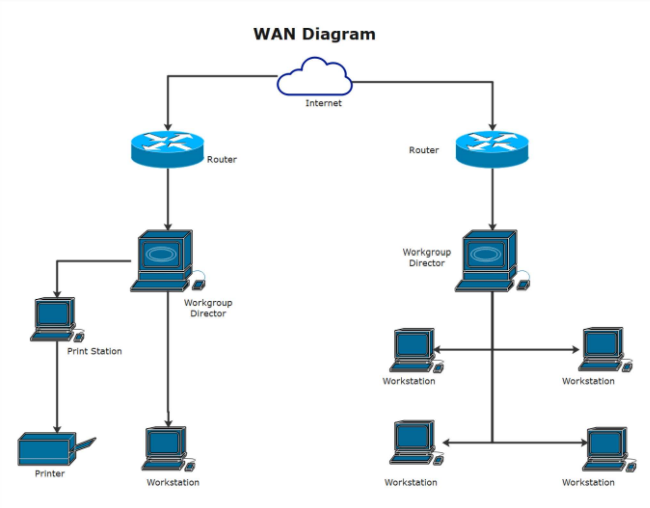


Fig.1.5.1

1.3 Topologies of Network:

The arrangement of a network that comprises nodes and connecting lines via sender and receiver is referred to as **Network Topology**. The various network topologies are:

- Point to Point Topology
- Mesh Topology
- Star Topology
- Bus Topology
- Ring Topology
- Tree Topology
- Hybrid Topology

Point to Point Topology

This is the kind of topology that relies upon two functions i.e. Transmit and Receive. It is a type of communication network between two communication nodes where there is one transmitter and on the other end, there is the receiver. It is a kind of communication medium which have two endpoints or end nodes. They provide high bandwidth

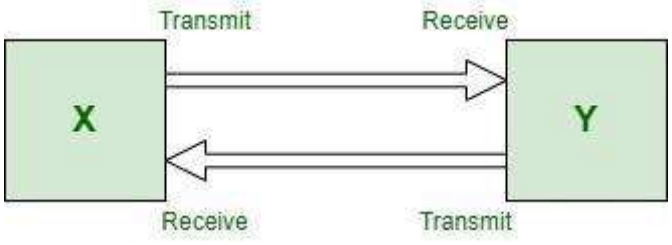


Fig.1.3.1

Mesh Topology

In a mesh topology, every device is connected to another device via a particular channel. In Mesh Topology, the protocols used are AHCP (Ad Hoc Configuration Protocols), DHCP (Dynamic Host Configuration Protocol), etc.

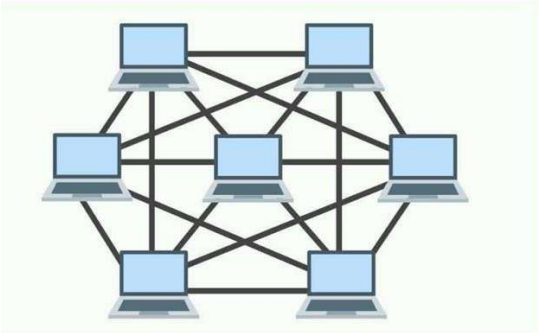


Fig.1.3.2

Star Topology

In Star Topology, all the devices are connected to a single hub through a cable. This hub is the central node and all other nodes are connected to the central node. The hub can be passive in nature i.e., not an intelligent hub such as broadcasting devices, at the same time the hub can be intelligent known as an active hub. Active hubs have repeaters in them. Coaxial cables or RJ-45 cables are used to connect the computers. In Star Topology, many popular Ethernet LAN protocols are used as CD(Collision Detection), CSMA (Carrier Sense Multiple Access), etc.

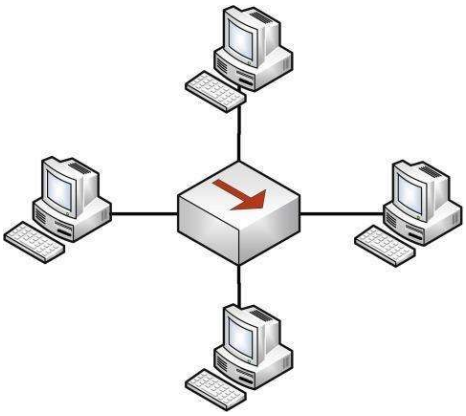


Fig.1.3.3

Bus Topology

Bus Topology is a network type in which every computer and network device is connected to a single cable. It is bi-directional. It is a multi-point connection and a non-robust topology because if the backbone fails the topology crashes. In Bus Topology, various MAC (Media Access Control) protocols are followed by LAN ethernet connections like TDMA, Pure Aloha, CDMA, Slotted Aloha, etc.

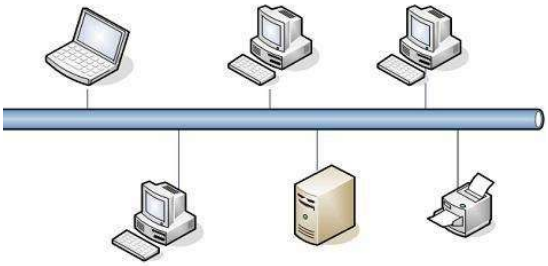


Fig.1.3.4

Ring Topology

In a Ring Topology, it forms a ring connecting devices with exactly two neighboring devices. A number of repeaters are used for Ring topology with a large number of nodes, because if someone wants to send some data to the last node in the ring topology with 100 nodes, then the data will have to pass through 99 nodes to reach the 100th node. Hence to prevent data loss repeaters are used in the network.
The data flows in one direction, i.e. it is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called Dual Ring Topology. In-Ring Topology, the Token Ring Passing protocol is used by the workstations to transmit the data.

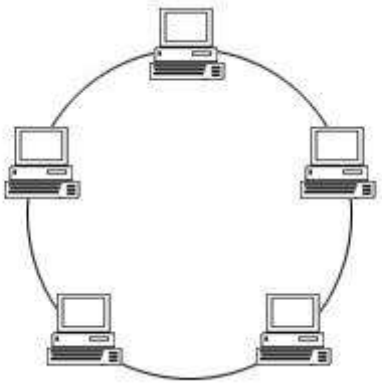


Fig.1.3.5

Tree Topology

This topology is the variation of the Star topology. This topology has a hierarchical flow of data. In Tree Topology, protocols like DHCP and SAC (Standard Automatic Configuration) are used.

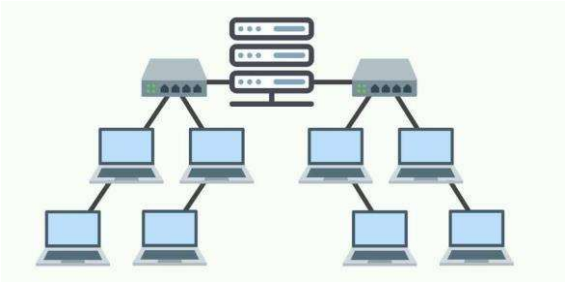


Fig.1.3.6

1.4 Networking Devices :

Network devices, also known as networking hardware, are physical devices that allow hardware on a computer network to communicate and interact with one another. For example Repeater, Hub, Bridge, Switch, Routers, Gateway, Brouter, and NIC, etc.

1. Repeater – A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted to extend the length to which the signal can be transmitted over the same network. An important point to be noted about repeaters is that they not only amplify the signal but also regenerate it. When the signal becomes weak, they copy it bit by bit and regenerate it at its star topology connectors connecting following the original strength. It is a 2-port device.

Fig.1.4.1

2. Hub – A hub is a basically multi-port repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices. In other words, the collision domain of all hosts connected through Hub remains one. Also, they do not have the intelligence to find out the best path for data packets which leads to inefficiencies and wastage.

Fig.1.4.2

3. Bridge – A bridge operates at the data link layer. A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of the source and destination. It is also used for interconnecting two LANs working on the same protocol. It has a single input and single output port, thus making it a 2 port device.

Fig.1.4.3

4. Switch – A switch is a multiport bridge with a buffer and a design that can boost its efficiency(a large number of ports imply less traffic) and performance. A switch is a data link layer device. The switch can perform error checking before forwarding data, which makes it very efficient as it does not forward packets that have errors and forward good packets selectively to the correct port only. In other words, the switch divides the collision domain of hosts, but the broadcast domain remains the same.

Fig.1.4.4

1.5 Networking Models and Protocol

OSI Model

Open System Interconnect is an open standard for all communication systems. OSI model is established by International Standard Organization (ISO). This model has seven layers:

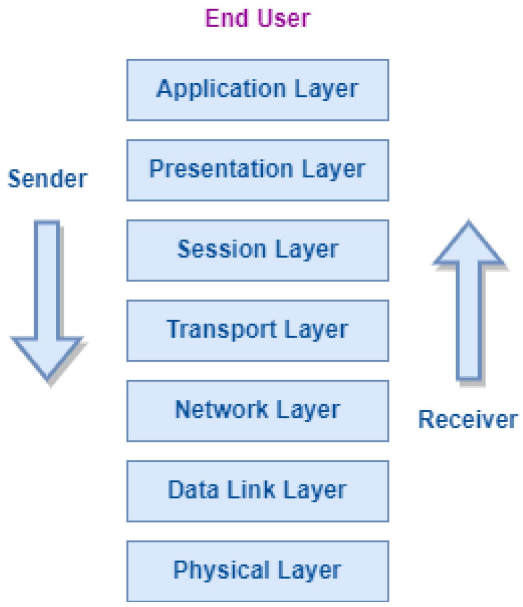


Fig.1.5.1

- **Application Layer**: This layer is responsible for providing interface to the application user. This layer encompasses protocols which directly interact with the user.
- **Presentation Layer**: This layer defines how data in the native format of remote host should be presented in the native format of host.
- **Session Layer**: This layer maintains sessions between remote hosts. For example, once user/password authentication is done, the remote host maintains this session for a while and does not ask for authentication again in that time span.
- **Transport Layer**: This layer is responsible for end-to-end delivery between hosts.
- **Network Layer**: This layer is responsible for address assignment and uniquely addressing hosts in a network.
- **Data Link Layer**: This layer is responsible for reading and writing data from and onto the line. Link errors are detected at this layer.
- **Physical Layer**: This layer defines the hardware, cabling wiring, power output, pulse rate etc.

Internet Model

Internet uses TCP/IP protocol suite, also known as Internet suite. This defines Internet Model which contains four layered architecture. OSI Model is general communication model but Internet Model is what the internet uses for all its communication.The internet is independent of its underlying network architecture so is its Model. This model has the following layers:

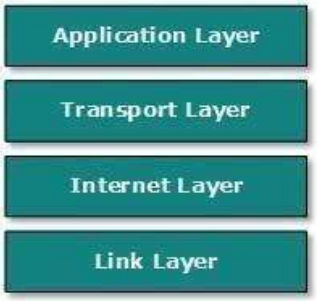


Fig.1.5.2

- **Application Layer**: This layer defines the protocol which enables user to interact with the network.For example, FTP, HTTP etc.
- **Transport Layer**: This layer defines how data should flow between hosts. Major protocol at this layer is Transmission Control Protocol (TCP). This layer ensures data delivered between hosts is in-order and is responsible for end-to-end delivery.
- **Internet Layer**: Internet Protocol (IP) works on this layer. This layer facilitates host addressing and recognition. This layer defines routing.
- **Link Layer**: This layer provides mechanism of sending and receiving actual data.Unlike its OSI Model counterpart, this layer is independent of underlying network architecture and hardware.

2. Cisco Switching

2.1 Switching:

A switch is a dedicated piece of computer hardware that facilitates the process of switching i.e., incoming data packets and transferring them to their destination. A switch works at the Data Link layer of the OSI Model. A switch primarily handles the incoming data packets from a source computer or network and decides the appropriate port through which the data packets will reach their target computer or network.

A switch decides the port through which a data packet shall pass with the help of its destination MAC(Media Access Control) Address. A switch does this effectively by maintaining a switching table, (also known as forwarding table).

Process of Switching

The switching process involves the following steps:

Frame Reception: The switch receives a data frame or packet from a computer connected to its ports.

- **MAC Address Extraction:** The switch reads the header of the data frame and collects the destination MAC Address from it.
- **MAC Address Table Lookup:** Once the switch has retrieved the MAC Address, it performs a lookup in its Switching table to find a port that leads to the MAC Address of the data frame.
- **Forwarding Decision and Switching Table Update:** If the switch matches the destination MAC Address of the frame to the MAC address in its switching table, it forwards the data frame to the respective port. However, if the destination MAC Address does not exist in its forwarding table, it

follows the flooding process, in which it sends the data frame to all its ports except the one it came from and records all the MAC Addresses to which the frame was delivered. This way, the switch finds the new MAC Address and updates its forwarding table.

- **Frame Transition:** Once the destination port is found, the switch sends the data frame to that port and forwards it to its target computer/network.

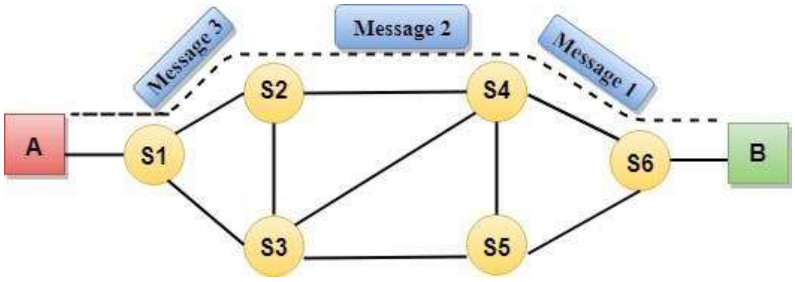


Fig.1.2.1

2.2 Switch Configuration:

Step 1: Inspect your hardware

Check the model number of your shiny new switch. Or, if you are using a spare, check the device hardware and its connected cables for any damages. If everything checks out, power on the switch and verify that all the indicator lights are in working order. Next, use a rollover cable to console into the switch from your computer. To do this, you will need to download and install Putty (or a similar, fun-named software tool). Run Putty and select the 9600 speed serial connection. You are now connected to the switch and ready to check the output of the following commands:

- show version
- show running-config
- show VLAN brief
- show VTP status
- (config)# IP domain-name routerfreak.com
- (config)# hostname Switch01
- (config)# interface VLAN1
- (config)# description Management VLAN
- (config)# IP address 192.168.101.1 255.255.255.0
- vtp [client | server | transparent]
- vtp domain name
- description *** DESCRIPTION ***
- switchport access vlan ###
- sswitchport mode access

- power inline consumption ###
- queue-set 2
- mls qos trust dscp
- storm-control multicast level 50.00
- no cdp enable
- spanning-tree portfast
- spanning-tree bpduguard enable
- Interface GigabitEthernet1/0/1
- description *** UPLINK ***
- switchport trunk encapsulation dot1q
- switchport mode trunk
- speed 1000
- duplex full
- Switch01(config)# crypto key generate rsa
- The name for the keys will be:
- Switch01.routerfreak.com
- How many bits in the modulus [512]: 1024
- % Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
- # line vty 0 4
- (config-line)# transport input ssh
- (config-line)# login local
- (config-line)# password routerfreak
- (config-line)# exit
- # line console 0
- (config-line)# logging synchronous
- (config-line)# login local
- Switch01# service password-encryption
- remote-computer# ssh 192.168..101.1
- Log in as: username
- Password:
- Switch01>en
- Password:
- Switch01#

For spare switches, make sure to delete the flash:vlan.dat file to erase the previous configuration.

Step 2: Set up management IP

Unlike with that punny name you gave your home Wi-Fi network, when setting up the hostname for your switch you should probably stick to a more professional and standard naming convention. Follow any preset naming assignment your company is using and then assign an IP address on the management VLAN. Next, make sure your switch has a set hostname and domain name:

Step 3: Check VTP revision number

Hit the show vtp status command to reveal your Virtual Trunking Protocol (VTP) revision numbers. The VTP revision numbers determine which updates are to be used in a VTP domain. When you set a VTP domain name, the revision number is set to zero—after which each change to the VLAN database increases the revision number by one. Your switch will only process data from a neighboring switch coming from the same domain and if the revision number of the neighboring switch is higher than its own. This means that the switches will update their VLAN configuration based on the VTP information being sent by the switch with the highest revision number.

So, before you add your switch to the network, you're going to want to set its revision number to zero. To easily reset the domain back to zero, change the config mode to transparent:

Step 4: Configure access ports

You might already have a template ready for access port configuration, but in case you don't, here are some commands you should use: Step 5: Configure trunk ports

Enter the command sh int g0/1 capabilities and check the trunking protocol supported. If ISL is supported, you have to issue the switchport trunk encapsulation dot1q on the trunk port configuration. If not, simply type switchport mode trunk. It means there is no other encapsulation supported so there is no need for an encapsulation command. It only supports 802.1Q.

Step 6: Configure access ports

After already performing basic network switch configurations, it's time to generate RSA keys to be used during the SSH process, using the crypto commands shown here:

Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.

Step 7: Set up VTY line config

If you have not set the console line yet, you can easily input these values:

Set the enable password using the enable secret password command. Then, set the privilege exec password with username name privilege 15 secret password. Make sure that the password-encryption service is activated.

Verify SSH access by typing 'sh ip ssh' to confirm that the SSH is enabled. You can now try to log in from a remote machine to verify that you can ssh to your Cisco switch.

Finishing touches

You've made it through the learning process with (hopefully) minimum bumps and bruises, and you're just about ready to ride off. All that's left is to test your access, reload the switch, and ready the cables.

Once that's done, label your switch, rack it up, and go enjoy doing anything that doesn't involve switch configuration!

2.3 Switch Security:

SW1 Configurations enable
configure terminal spanning-tree portfast default
interface FastEthernet0/1 ip dhcp snooping limit rate 5
switchport mode access switchport port-security switchport
port-security maximum 4 switchport portsecurity mac-
address sticky switchport port-security
violation restrict switchport port-security mac-address
0010.11E8.3CBB
spanning-tree portfast
spanning-tree bpduguard enable

interface range FastEthernet0/2, FastEthernet0/10,FastEthernet0/24
ip dhcp snooping limit rate 5 switchport mode access switchport port-
security switchport port-security maximum 4 switchport portsecurity
mac-address sticky switchport port-security violation
restrict spanning-tree portfast
spanning-tree bpduguard enable

interface range FastEthernet0/3-9, FastEthernet0/11-23 switchport
access vlan 999
shutdown

interface range GigabitEthernet0/1-2
switchport trunk native vlan 100 ip
dhcp snooping trust switchport mode
trunk switchport nonegotiate vlan 100
name Native vlan 999 name
BlackHole SW-2 Configuration
enable configure terminal ip dhcp
snooping ip dhcp snooping vlan
10,20,99 spanning-tree portfast
default interface GigabitEthernet0/1
switchport trunk native vlan 100
switchport mode trunk
switchport nonegotiate

interface GigabitEthernet0/2 switchport trunk
native vlan 100 switchport mode
trunk switchport nonegotiate

vlan 100 name Native

3. Cisco Routing:

3.1 Router:

Cisco IP Routing Protocols provide the fundamental infrastructure for the delivery of advanced IP services across all Cisco networking products. Whether based on Internet Engineering Task Force (IETF) standards or Cisco innovations, Cisco offers the broadest portfolio of IP routing technologies. All share industry-leading scalability, availability, manageability, fast convergence, and high-performance capabilities.

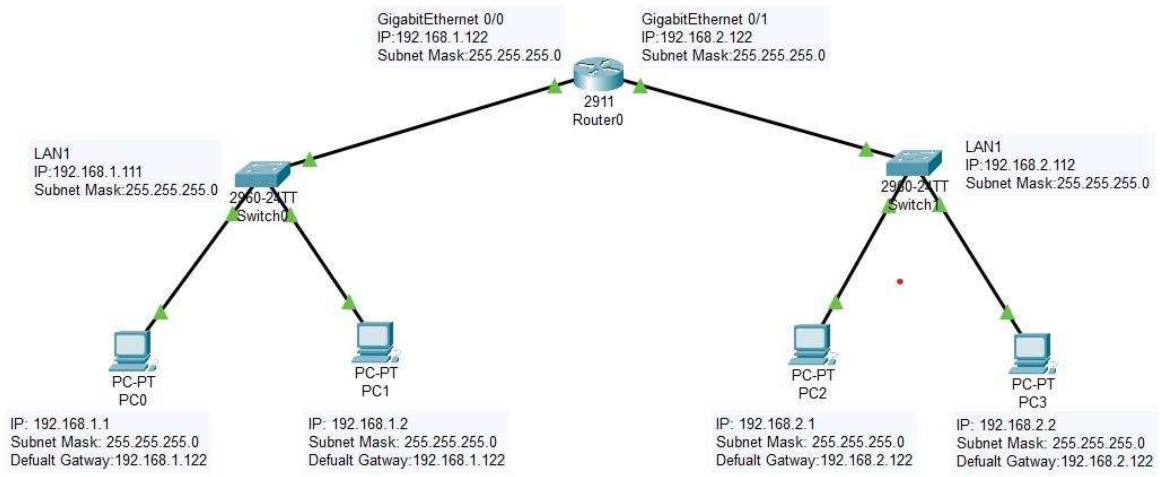


Fig 3.1.1

Router# show run
Building configuration...

Current configuration : 2525 bytes
!
version 12.4 service timestamps debug
datetime msec service timestamps log
datetime msec no service passwordencryption
!
hostname Router
!

```
boot-start-marker boot-end-marker
!
no logging buffered enable password
cisco
!
no aaa new-model
!
resource policy
! ip
cef !
!---
RSA
certifi
cate
genera
ted
after
you
enable
the  !--
- ip
http
secure
-server
comm
and.

crypto pki trustpoint TP-self-signed-2401602417  enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-2401602417  revocation-check
none
 rsakeypair TP-self-signed-2401602417

crypto pki certificate chain TP-self-signed-2401602417  certificate
self-signed 01
  30820248 308201B1 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 32343031 36303234 3137301E 170D3130 30353139 30393031
  31315A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D32 34303136
  30323431 3730819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
  8100CD35 A3A6E322 9B6005DA A0FF26C2 8A0DC5AF 27B38F3B DBF2BF58 D8F2655D
  31115681 EC8BC750 03FE3A25 0F79DC74 3A839496 CB9486F1 A1F5BF43 D92BA7AF
  3C72A57B D8D37799 50493588 A5A18F7F 27955AB0 AC36B560 3BE9F648 A4F6F41F
  B9E9C5E6 F9570DEB 5555FDED 9593BD00 5ABB30CD D3B9BDFA F570F987 651652CE
  3D310203 010001A3 70306E30 0F060355 1D130101 FF040530 030101FF 301B0603
  551D1104 14301282 10526F75 7465722E 70616D6D 692E636F 6D301F06 03551D23
  04183016 80146A0A C2100122 EFDA58AB C319820D 98256622 52C5301D 0603551D
```

0E041604 146A0AC2 100122EF DA58ABC3 19820D98 25662252 C5300D06 092A8648
86F70D01 01040500 03818100 83B0EC8C 6916178F 587E15D6 5485A043 E7BB258D
0C9A63F2 DA18793D CACC026E BC0B9B33 F8A27B34 5BD7DD7F FCECA34F 04662AEC
07FD7677 A90A8D1C 49042963 C2562FEC 4EFFF17C 360BF88A FEDC7CAA AE308F6C
A5756C4A F574F5F3 39CE14AE BAAEC655 D5920DD0 DA76E296 B246E36E 16CFBC5A
00974370 170BBDAD C1594013
quit

!--- Create a user account named ccpccp with all privileges.

username ccpccp privilege 15 password 0 cisco123
archive log config
hidekeys

!--- The LAN interface configured with a private IP address.

interface FastEthernet0/0 description
$ETH-LAN$
ip address 192.168.1.1 255.255.255.0

!--- Designate that traffic that originates from behind
!--- the interface is subject to Network Address Translation (NAT).

ip nat inside ip
virtual-reassembly duplex
auto
speed auto

!--- This is the LAN interface configured with a routable (public) IP address.

interface FastEthernet0/1 description
$ETH-WAN$ ip address 172.16.1.1
255.255.255.0

!--- Designate that this interface is the
!--- destination for traffic that has undergone NAT.

ip nat outside ip
virtual-reassembly duplex
auto
speed auto

```
!--- RIP version 2 routing is enabled.

router rip  version 2  network
192.168.1.0
 no auto-summary

!--- This is where the commands to enable HTTP and HTTPS are configured.

ip http server ip http authentication local
ip http secure-server


!--- This configuration is for dynamic NAT.
!--- Define a pool of outside IP addresses for NAT.

ip nat pool pool 10.10.10.1 10.10.10.100 netmask 255.255.255.0

!--- In order to enable NAT of the inside source address,  !---
specify that traffic from hosts that match access list 1  !--- are
NATed to the address pool named pool1.

ip nat inside source list 1 pool pool1


!--- Access list 1 permits only 192.168.1.0 network to be NATed.

access-list 1 remark CCP_ACL Category=2
access-list 1 permit 192.168.1.0 0.0.0.255


!--- This configuration is for static NAT
!--- In order to translate the packets between the real IP address 10.10.10.1 with TCP  !--- port 80
and the mapped IP address 172.16.1.1 with TCP port 500.

ip nat outside source static tcp 10.10.10.1 8080 172.16.1.1 80 extendable
!
! --- The default route is configured and points to 172.16.1.2.

ip route 0.0.0.0 0.0.0.0 172.16.1.2
!
control-plane
!
line con 0 line
aux 0
```

!--- Telnet enabled with password as cisco.

```
line vty 0 4
password cisco
transport input all
line vty 5 15
password cisco
transport input all
!
end
```

3.2 Router Devices:

The Router is a physical or virtual internetworking device that is designed to receive, analyse, and forward data packets between computer networks. A router examines a destination IP address of a given data packet, and it uses the headers and forward data packets between computer networks. A router examines a destination IP address of a given data packet, and it uses the headers and forwarding tables to decide the best way to transfer the packets. There are some popular companies that develop routers; such are **Cisco**, **3Com**, **HP, Juniper, D-Link, Nortel,** etc.

In order to connect a LAN to the Internet, a router first needs to communicate with a modem. There are two primary ways to do this:

- *Wireless router:* A wireless router uses an Ethernet cable to connect to a modem. It distributes data by converting packets from binary code into radio signals, then wirelessly broadcasts them using antennae. Wireless routers do not establish LANs; instead, they create WLANs (wireless local area networks), which connect multiple devices using wireless communication.

- *Wired router:* Like a wireless router, a wired router also uses an Ethernet cable to connect to a modem. It then uses separate cables to connect to one or more devices within the network, create a LAN, and link the devices within that network to the Internet.

Fig 3.2.1

4. Wireless Network

4.1. IEEE 802.11:

IEEE 802.11 standard, popularly known as WiFi, lays down the architecture and specifications of wireless LANs (WLANs). WiFi or WLAN uses high-frequency radio waves instead of cables for connecting the devices in LAN. Users connected by WLANs can move around within the area of network coverage.

IEEE 802.11 standard, popularly known as **WiFi**, lays down the architecture and specifications of wireless **LANs** (**WLANs**). WiFi or WLAN uses high frequency radio waves for connecting the nodes.

There are several standards of IEEE 802.11 WLANs. The prominent among them are 802.11, 802.11a, 802.11b, 802.11g, 802.11n and 802.11p. All the standards use carrier-sense multiple access with collision avoidance (CSMA/CA). Also, they have support for both centralised base station based as well as ad hoc networks.

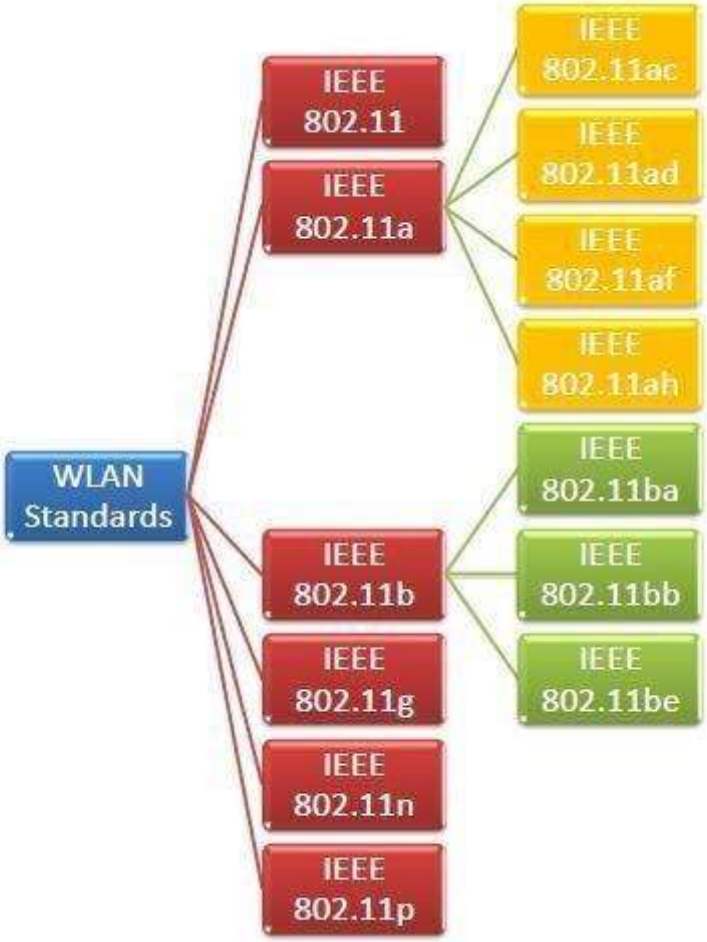


Fig 4.1.1

4.2 Wireless Network Evolution:

The evolution of wireless networks has been a significant and ongoing process that has transformed the way we communicate and access information. Here's a brief overview of the key stages in the evolution of wireless networks:

First Generation (1G):

1G networks were introduced in the 1980s.

They were analog cellular networks primarily for voice communication.

Low data rates and limited coverage.

Second Generation (2G):

2G networks emerged in the early 1990s.

Digital technology improved call quality and added some data services (like SMS).

GSM (Global System for Mobile Communications) and CDMA (Code Division Multiple Access) were common 2G technologies.

Third Generation (3G):

3G networks were introduced around the early 2000s.

Provided higher data rates, enabling internet access and video calling.

Technologies like UMTS (Universal Mobile Telecommunications System) and EV-DO (Evolution-Data Optimized) were used.

Fourth Generation (4G):

4G networks began deployment in the late 2000s.

Significantly faster data rates, making it possible for mobile broadband, streaming video, and mobile apps.

LTE (Long-Term Evolution) and WiMAX were the primary 4G technologies.

Fifth Generation (5G):

5G is the current generation of wireless networks, with deployment starting around 2019.

Offers much higher data rates, low latency, and massive device connectivity.

Utilizes advanced technologies like mmWave and sub-6 GHz spectrum for improved performance.

Expected to support applications like autonomous vehicles, IoT (Internet of Things), and augmented reality.

Beyond 5G (B5G) and 6G:

Beyond 5G (B5G) and 6G networks are still in the research and development phase.
Expected to provide even faster data rates, lower latency, and improved connectivity.

Envisioned to support emerging technologies such as holographic communication, advanced AI, and more.

Wireless Technologies in Other Sectors:

Wireless networks have also evolved in other sectors, such as Wi-Fi and Bluetooth in the consumer space.

Industrial sectors have developed specialized wireless networks for applications like IoT and Industrial IoT (IIoT).

Security and Standardization:

With each generation, wireless networks have improved security features to protect user data and privacy.

Standardization bodies like 3GPP (3rd Generation Partnership Project) and IEEE (Institute of Electrical and Electronics Engineers) play a crucial role in defining wireless network standards.

Challenges and Considerations:

The evolution of wireless networks brings challenges like spectrum allocation, infrastructure deployment, and cybersecurity.

Environmental concerns, such as energy consumption and electronic waste, are also important considerations.

Wireless network evolution continues to be a dynamic field, with ongoing research and development aimed at enhancing performance, expanding coverage, and enabling new applications that drive technological progress and change the way we live and work.

4.3 Wireless Network Configuration

Configuration

Configure the Access Point

You can configure the AP with the use of any of these:

- GUI
- Command-line interface (CLI), after you establish a Telnet session
- The console port

Note: In order to connect to the AP through the console port, connect a nine-pin, straight-through DB-9 serial cable to the RS-232 serial port on the AP and to the COM port on a computer. Set up a terminal emulator in order to communicate with the AP. Use these settings for the terminal emulator connection:

- 9600 baud
- 8 data bits
- No parity
- 1 stop bit
- No flow control

Note: These settings are the default settings. If you cannot access the device after you set the terminal program to the settings, the problem can be that the device is not set to the defaults. Try different settings, and start with the baud rate. For more information on the console cable specifications, refer to the *Connecting to the 1200 and 1230AG Series Access Points Locally* section of Configuring the Access Point for the First Time.

This document explains how to configure the AP with the use of the GUI.

There are two ways to access the AP with the use of the GUI:

- Assign an IP address to the device before you connect through the GUI.
- Obtain an IP address with the use of DHCP.

The different models of Aironet APs exhibit different default IP address behaviors. When you connect an Aironet 350, 1130AG, 1200, or 1240AG series AP with a default configuration to your LAN network, the AP

requests an IP address from your DHCP server. If the AP does not receive an address, it continues to send requests indefinitely.

When you connect an Aironet 1100 series AP with a default configuration to your LAN, the AP makes several attempts to get an IP address from the DHCP server. If the AP does not receive an address, it assigns itself the IP address 10.0.0.1 for 5 minutes. During this 5-minute period, you can browse to the default IP address and configure a static address. If after the 5 minutes the AP is not reconfigured, the AP discards the 10.0.0.1 address and requests an address from the DHCP server. If the AP does not receive an address, it sends requests indefinitely. If you miss the 5-minute window to browse to the AP at 10.0.0.1, you can power cycle the AP in order to repeat the process.

The network in this document uses a 1200 series AP. A login through the console configures the AP with a static IP address of 10.0.0.1. For information on how to assign IP addresses to the AP, refer to the *Obtaining and Assigning an IP Address* section of Configuring the Access Point for the First Time.

Step-by-Step Instructions

After configuration of the IP address, you can access the AP through the browser in order to configure the AP to accept client association requests from the client adapter.

Complete these steps:

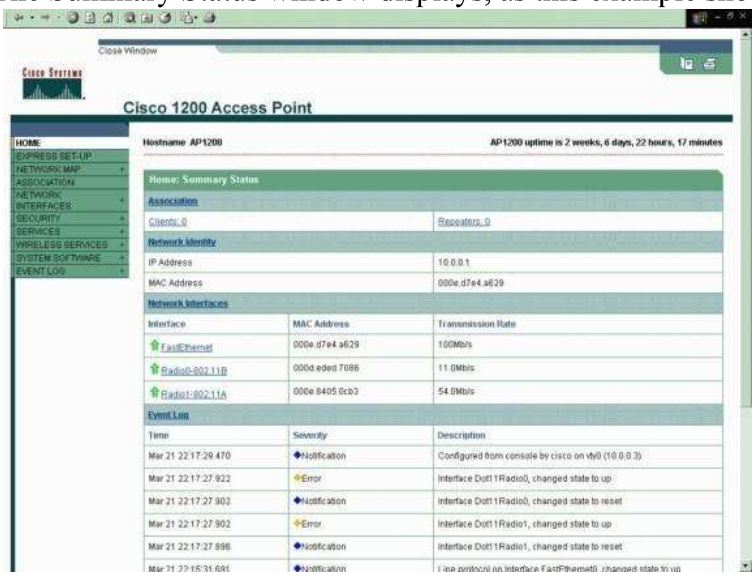
1. In order to access the AP with the GUI and get the Summary Status window, complete these steps:

   a. Open a web browser and enter **10.0.0.1** in the address line.

   b. Press **Tab** in order to bypass the Username field and advance to the Password field. The Enter Network Password window displays.

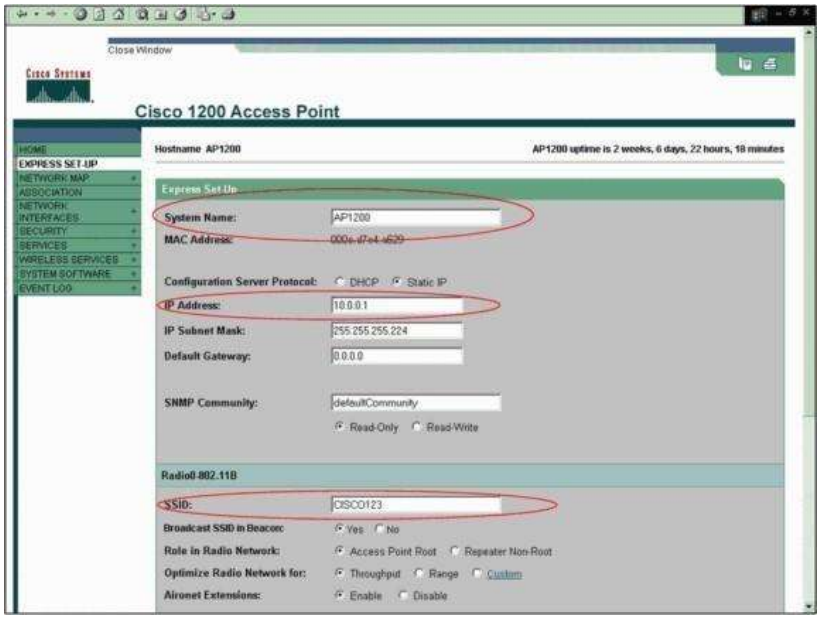
   c. Enter the case-sensitive password **Cisco**, and press **Enter**.

   The Summary Status window displays, as this example shows:



2. Click Express Setup in the menu on the left.

   The Express Setup window displays. You can use this window to configure some of the basic parameters that are necessary to establish a wireless connection. Use the Express Setup window on the AP 1200 in order to configure the acceptance of wireless client associations. Here is an example of the window:



3. Enter the configuration parameters in the appropriate fields in the Express Setup window. The configuration parameters include these parameters:

    a. The host name of the AP

    b. IP address configuration of the AP, if the address is a static IP

    c. Default gateway

    d. Simple Network Management Protocol (SNMP) community string

    e. Role in the radio network

    f. SSID

    This example configures these parameters:

    g. IP address: **10.0.0.1**

    h. Host name: **AP1200**

    i. SSID: **CISCO123**

    Note: SSIDs are unique identifiers that identify a WLAN network. Wireless devices use SSIDs to establish and maintain wireless connectivity. SSIDs are case-sensitive and can contain up to 32 alphanumeric characters. Do not use any spaces or special characters in an SSID.

    Note: The other parameters are left with the default values.

4. Click **Apply** in order to save your settings.
5. Complete these steps in order to set up the radio settings:

    a. Click **Network Interfaces** in the menu on the left in order to browse to the Network Interfaces Summary page.

    b. Select the radio interface that you want to use.

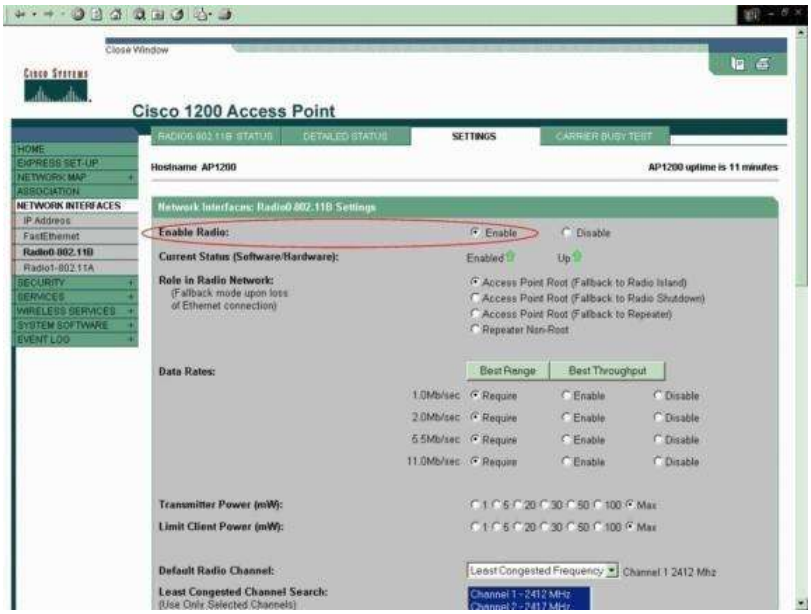
    This example uses interface Radio0-802.11B. The action allows you to browse to the Network Interfaces: Radio Status page.

    c. Click the **Settings** tab in order to browse to the Settings page for the radio interface.

    d. Click **Enable** in order to enable the radio.

e. Leave all the other settings on the page with the default values.

f. Scroll down and click **Apply** at the bottom of the page in order to save the settings.



6. In order to configure the SSID and open authentication with WEP encryption, complete these steps:

   a. Choose **Security > SSID Manager** in the menu on the left. The SSID Manager page displays.

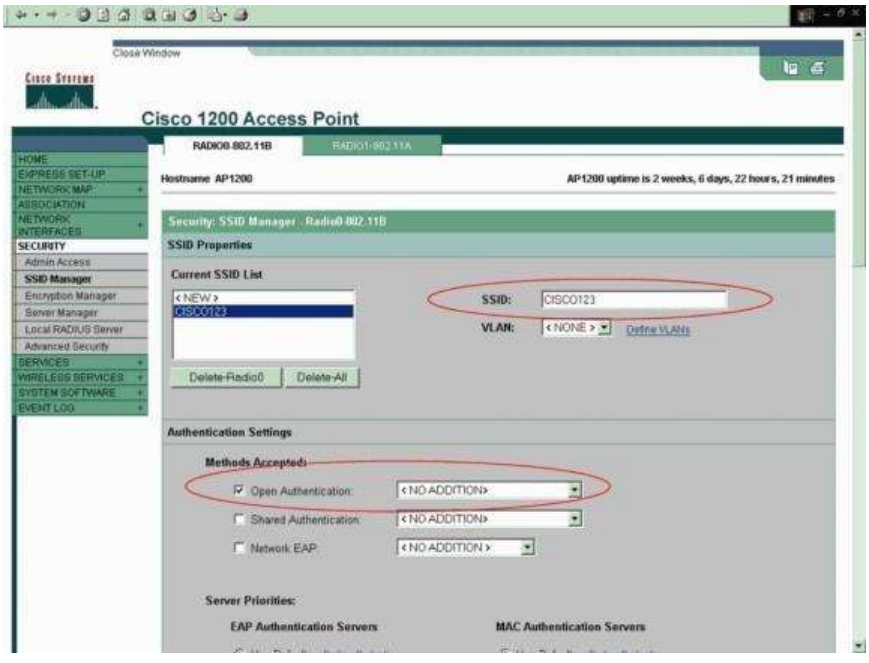
   b. Select the SSID that you created in Step 3 from the Current SSID List menu.

      This example uses CISCO123 as the SSID.

   c. Under Authentication Settings, choose **Open Authentication**.

   d. Leave all other parameters with their default values.

   e. Click **Apply** at the bottom of the page.



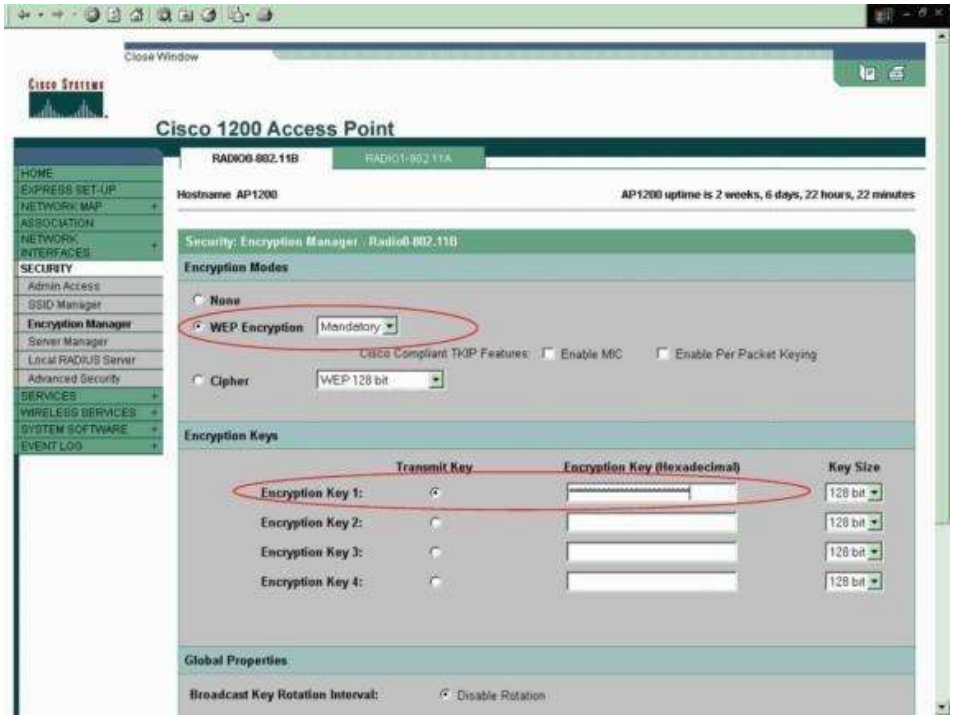
7. In order to configure the WEP keys, complete these steps:

a. Choose **Security > Encryption Manager**.

b. Click **WEP Encryption** under Encryption Modes, and choose **Mandatory** from the dropdown menu.

c. Enter the encryption key for WEP in the Encryption Keys area.

The WEP encryption keys can be 40 bits or 128 bits in length. This example uses the 128bit WEP encryption key **1234567890abcdef1234567890**.



d. Click **Apply** in order to save the settings.

Configure the Wireless Client Adapter

Before configuration of the client adapter, you must install the client adapter and client adapter software components on the PC or laptop. For instructions on how to install the drivers and utilities for the client adapter, refer to Installing the Client Adapter.

Step-by-Step Instructions

After installation of the client adapter on the machine, you can configure it. This section explains how to configure the client adapter.

Complete these steps:

1. Create a profile on the ADU for the client adapter.

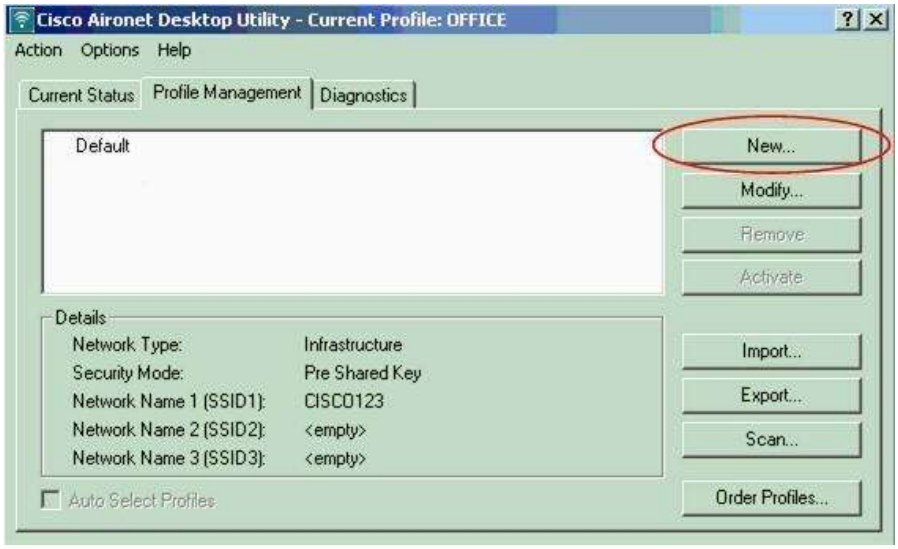
   The profile defines the configuration settings that the client adapter uses in order to connect to the wireless network. You can configure a maximum of 16 different profiles on the ADU. You can switch between the different configured profiles on the basis of your requirement. Profiles enable you to use your client adapter in different locations, each of which requires different configuration settings. For example, you may want to set up profiles to use your client adapter at the office, at home, and in public areas, such as airports or hot spots.

   In order to create a new profile, complete these steps:

   a. Click the **Profile Management** tab on the ADU.

   b. Click **New**.

      Here is an example:



2. When the Profile Management (General) window displays, complete these steps in order to set the Profile Name, Client Name, and SSID:

    a. Enter the name of the profile in the Profile Name field.

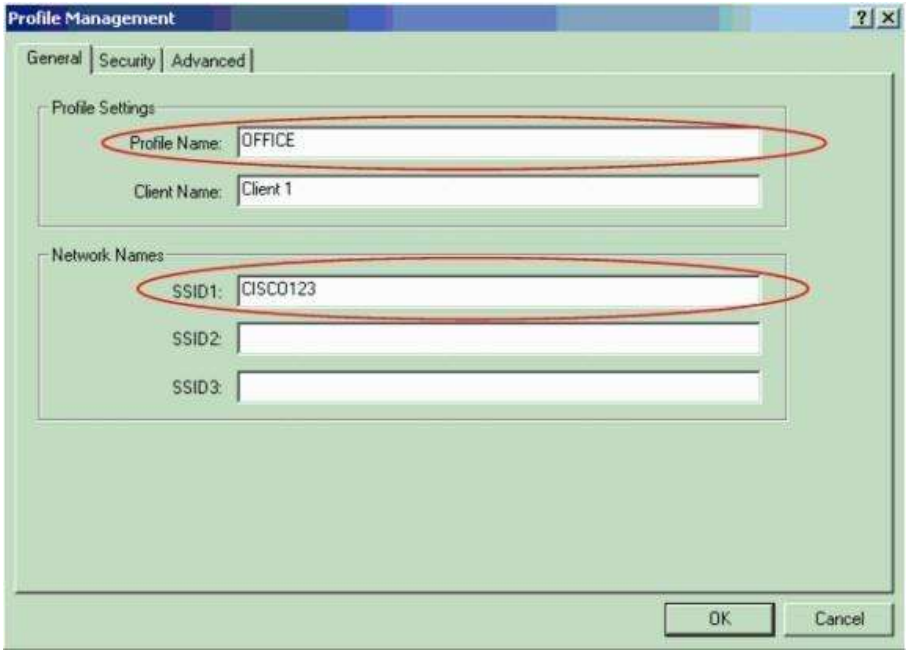
    This example uses **OFFICE** as the Profile Name.

    b. Enter the name of the client in the Client Name field.

    The client name is used to identify the wireless client in the WLAN network. This configuration uses the name **Client 1** for the first client.

    c. Under Network Names, enter the SSID that is to be used for this Profile.

    The SSID is the same as the SSID that you configured in the AP. The SSID in this example is **CISCO123**.



3. Complete these steps in order to set up the Security Options:

    a. Click the **Security** tab at the top of the window.

    b. Click **Pre-Shared Key (Static WEP)** under Set Security Options.

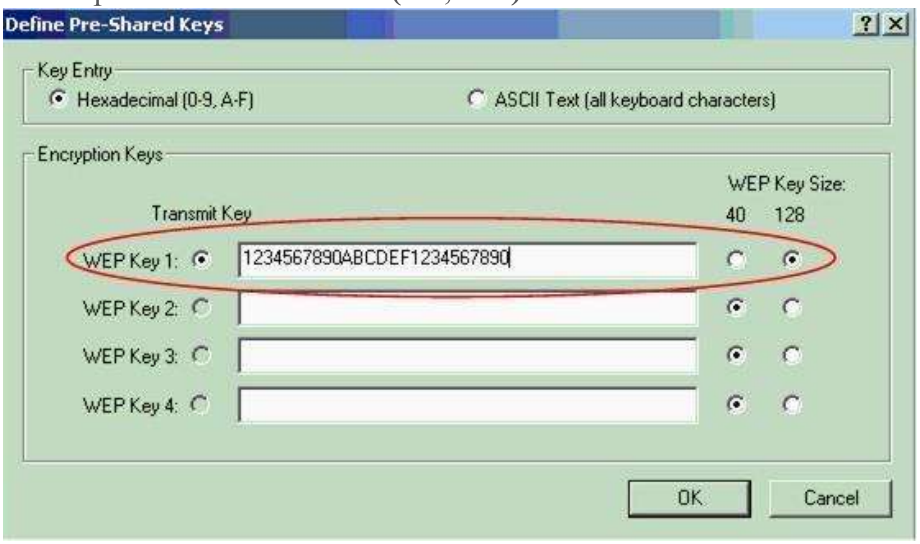
    Here is an example:

c. Click **Configure**.

The Define Pre-Shared Keys window appears.

d. Click one of buttons in the Key Entry area in order to choose a key entry type.

This example uses **Hexadecimal (0-9, A-F)**.



e. Under Encryption Keys, enter the WEP key that is to be used for encryption of the data packets.

This example uses the WEP key **1234567890abcdef1234567890**. See the example in Step d.

Note: Use the same WEP key as the one you configured in the AP.

4. Click **OK** in order to save the WEP key.
5. Complete these steps in order to set the authentication method to Open:

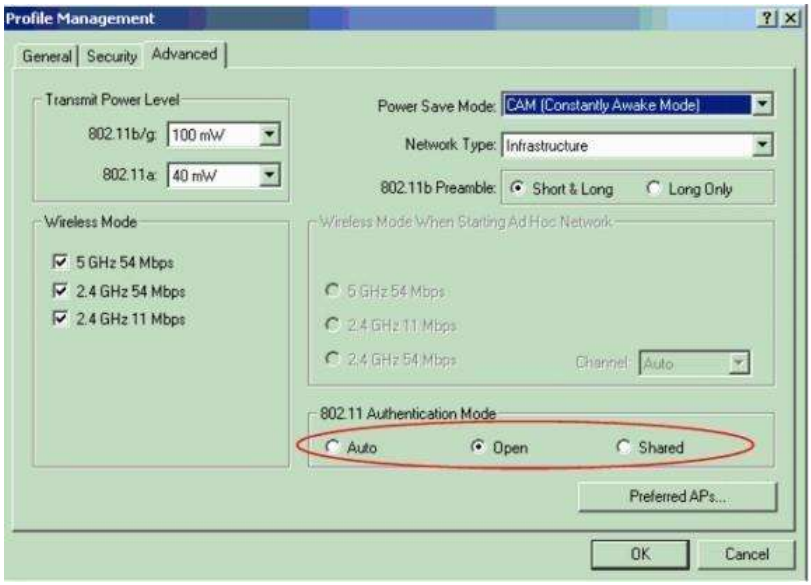
a. Click the **Advanced** tab at the top of the Profile Management window.

b. Be sure that **Open** is selected under 802.11 Authentication Mode.

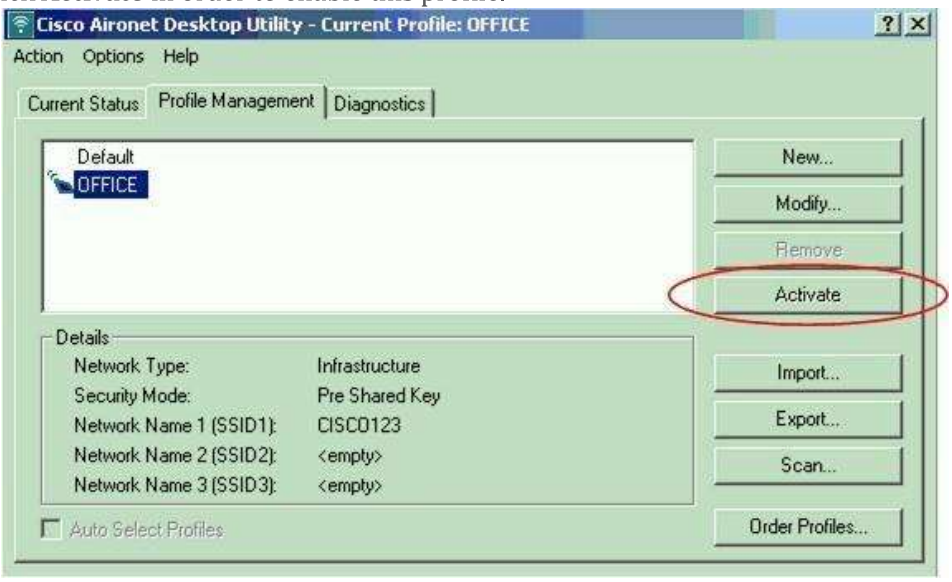
Note: Open authentication is usually enabled by default.

c. Leave all the other settings with the default values.

d. Click **OK**.



6. Click **Activate** in order to enable this profile.



Note: You can use these same Step-by-Step Instructions in order to create a completely new profile. In an alternate method to create a profile, the client adapter scans the RF environment in order to check for available networks and then creates a profile on the basis of the scan results. For more information on this method, refer to the *Creating a New Profile* section of Using the Profile Manager.

You can use the same procedure in order to configure the other two client adapters. You can use the same SSID on the other adapters. The only difference is the client name and the IP address that is statically given to the adapter.

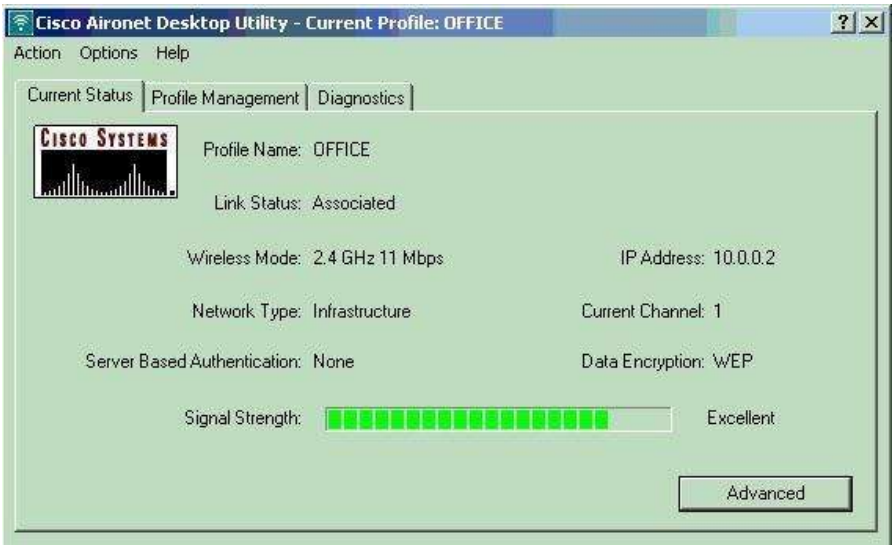
Note: This example assumes that the client adapter IP address is configured manually and is in the same subnetwork as the AP.

Verify

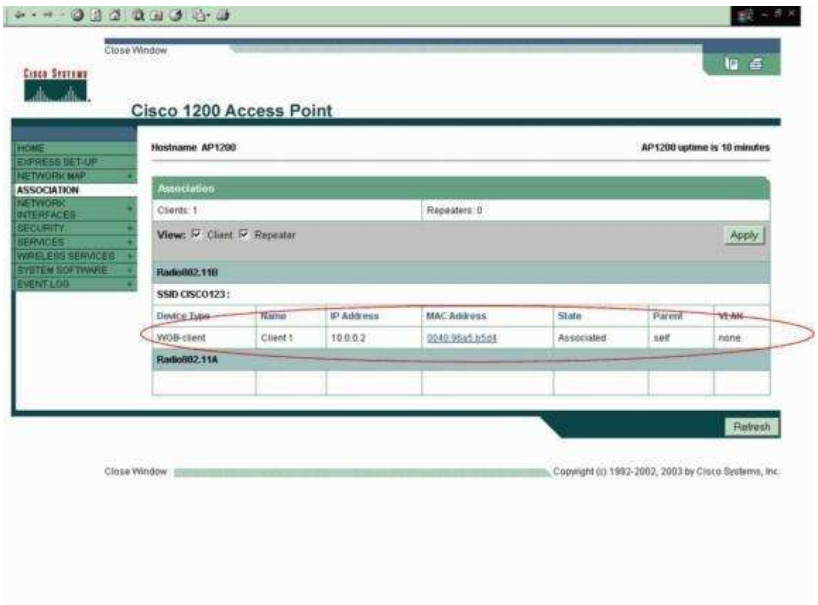
This section explains how to confirm that your configuration works properly.

When you have completed the configurations and activated the profile, the client adapter connects to the AP. In order to check the status of the client connection, click the **Current Status** tab at the top of the ADU window.

This example illustrates a successful connection to the AP. You can see that the client uses Channel 1 for communication and uses WEP for encryption. Also, since only open authentication is used, the Server Based Authentication field shows None:



As another method to verify the client connection on the AP, click **Association** in the menu on the left side of the AP home page. Here is an example:



Troubleshoot

If 802.1x authentication is used, and a Cisco Catalyst 2950 or 3750 Switch is present in the network, an 802.1X client might fail to authenticate. This error message is displayed:

Jul 21 14:14:52.782 EDT: %RADIUS-3-ALLDEADSERVER: Group rad_eap: No active radius servers found. Id 254

Conclusion:

During my internship in basic networking, where I focused on Routing, Switching, and Wireless Networking, I had the opportunity to delve into the fundamental aspects of networking technologies and their practical applications. This experience has been immensely valuable, providing me with hands-on skills and a deeper understanding of the critical components that form the backbone of modern communication systems.

Key Learnings:

Practical Application of Concepts: Through real-world projects, I applied theoretical knowledge to configure routers, switches, and wireless networks. This practical experience enhanced my problemsolving abilities and technical proficiency.

Teamwork and Communication: Collaborating with colleagues and clients improved my communication skills and taught me the importance of effective teamwork in resolving networking issues efficiently.

Troubleshooting Skills: I honed my troubleshooting skills by diagnosing and rectifying network problems. This experience significantly enhanced my ability to identify and address issues promptly.

Personal Growth:

This internship not only expanded my technical skill set but also nurtured my ability to adapt to new challenges and work under pressure. The exposure to different networking scenarios broadened my perspective and deepened my passion for the field of networking.

Professional Development:

I am now equipped with a solid foundation in basic networking principles, making me well-prepared for further education and certification programs. This internship has reinforced my career aspirations, motivating me to explore specialized areas within networking and pursue certifications to enhance my expertise.

Looking Ahead:

As I reflect on my internship experience, I am excited about the prospects that lie ahead. I am keen to leverage the knowledge and skills gained during this internship to contribute meaningfully to the rapidly evolving world of networking. I am also committed to staying updated with the latest industry trends and advancements to remain competitive and relevant in this dynamic field.

In conclusion, I am deeply grateful for the opportunity to have been a part of this internship program. I express my sincere appreciation to my mentors, colleagues, and the entire organization for their guidance,

support, and encouragement throughout this enriching journey. This internship has been a stepping stone towards my professional growth, and I am enthusiastic about applying my learnings to future endeavors in the field of networking.

References:-

1. Cisco Official Documentation: • Cisco's official website (https://www.cisco.com/) offers a wealth of resources, including whitepapers, case studies, and technical documentation. • Cisco Learning Network (https://learningnetwork.cisco.com/) is a valuable resource for certification exam preparation and networking knowledge.

2. Books: • "CCNA Routing and Switching Complete Study Guide" by Todd Lammle • "CCNA Routing and Switching Portable Command Guide" by Scott Empson • "Cisco Networking All-in-One For Dummies" by Edward Tetz .

3. Research Papers and Journals: • IEEE Xplore (https://ieeexplore.ieee.org/) is a great repository for research papers on networking and related topics. • ACM Digital Library (https://dl.acm.org/) contains papers on computer networking and communication.

4. Online Courses and Tutorials: • Greeks of Greeks • Java Tutorials • Google.com • Chat gpt.Ai.

5. Networking Magazines: • "Network World" (https://www.networkworld.com/) • "Cisco Focus" (https://www.cisco.com/c/en/us/solutions/enterprise networks/focus.html)

Self-assessment of Industrial Training by the student

1. Name of Student: __Honey Sharma
2. Name and address of __Cisco Academy CRISP_____
   Sponsoring Industry _Shyamla Hills Rd, Krishna Nagar,Bhopal,M.P
3. Guide from Industry __Kapil Shrivastava___
   (with designation) __Cisco Head Instructor_____
4. Date of commencement 14 August 2023
   of Industrial Training
5. Number of days present _____5____days out of ____5_____days.

6. I hereby declare that, I have learnt following skills during my Industrial Training:

Sr.	Description	Weightage (%)
1	Learning new Techniques – Software, Hardware, Process etc.	10%
2	Network Configuration and Management	12%
3	Network Security and Wireless Networking	10%
4	Network Troubleshooting	9%
5	Virtualization of Networking	8%
6	Research and Development	15%
7	Network Planning and Scalability	9%
8	Collaboration and Teamwork	8%
9	Documentation	9%
10	Any other (Specify)	-
	Total	100

Date: Signature of Student

Place: OCT Bhopal **Name of Student: Honey Sharma**