



PROJECT REPORT

On

“Computer Networking”

SESSION 2017-18

BY:

VAISHNAVI ANAND

B.Tech (ECE), 2ND YEAR

UNDER THE GUIDANCE OF

MR.ANKIT PURI

Dy. SE (ELECTRONICS)



PLACEMENT CELL



SRMU/ T&P/ IPT/ 2016-'17

26/09/2017

ANKIT PURI / EE(ELECTRONICS)

ONGC LTD.
11 HIGH INFOCOM SERVICES
BANDRA
MUMBAI-400051
MAHARASHTRA
Dear Sir,

Sub. : Requisition for In-plant Training – Reg.

Greetings from SRM University!

SRM Engineering College was started in the year 1985-86. It has become a constituent of SRM University from 2003 – 04. We offer 27 undergraduate and 31 postgraduate degree programs in Engineering & Technology apart from Research Programs leading to Ph.D.

It is our endeavour to have effective industry-institute interaction whereby the students are exposed to the practical nuances through project Internship in organisation of repute like yours.

We request that the below mentioned student(s) may be accorded permission to do In-plant Training during DECEMBER TO JANUARY in your esteemed organisation.

STUDENT NAME	UNIV REG NO	DEGREE	DEPARTMENT	YR
1. VAISHNAVI ANAND	RA1611004010628	B.TECH.	ECE	II

We thank you in anticipation.



PLACEMENT OFFICER

SRM Nagar, Kattankulathur - 603 203, Kancheepuram District, Tamil Nadu, India. Ph: +91-44-27452767 (Direct), Fax: +91-44-27453903
Email: placementoffice@srmuniv.ac.in / srmplacement@yahoo.com, Website: srmuniv.ac.in

CERTIFICATE

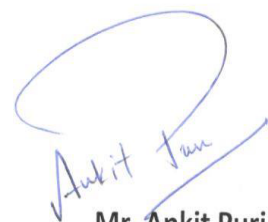
This is to certify that **Vaishnavi Anand**, a student of Shree Ramaswamy Memorial (SRM) Institute of Science and Technology has undergone project training in our organization for 4 weeks(1 Month) starting from 9th December 2017 to 8th January 2018.

She has successfully completed the training on "NETWORKING", under the guidance of **Mr. Ankit Puri**

During the training, she has worked on **Cisco Packet Tacer** a simulation software and covered various topics related to **computer networking**.

We have observed that her work has been excellent and appreciate his sincere learning. She has performed the project with energy and enthusiasm.

We wish her all the best for her future endeavors.



Mr. Ankit Puri

Dy SE (Electronics)



Oil and Natural Gas Corporation Limited
Skill Development Centre
 NBP Green Heights, 3rd Floor, Quadrant-4,
 Plot No. C-69, Bandra-Kurla Complex, Bandra (East), Mumbai – 400051
 Tel. 022 – 2627 5343 / 5051 /5308



No. MR/SDC-MUM/006/Winter Trg/2017-18

Dt. 22/11/2017

With reference to his/her application, the following student(s) is/are hereby permitted to undergo Winter Training during the below mentioned period at ONGC, Mumbai / Panvel:

Sl. No.	Name of the Student(s)	Course/ Discipline	Name of College/Institute/ University	Period of Training (DD/MM/YYYY)
1.	Vaishnavi Anand	B. Tech. (Electronics & communication Engg.)	SRM University, Tamilnadu	09/12/2017 to 08/01/2018

The Summer Training will be under the following terms and conditions:

1. ONGC will not provide any boarding and lodging facility to the student during the period of training.
2. No stipend will be paid to the student by ONGC for the period of the training.
3. The student will undergo the training at his/her own risk and ONGC will not be held responsible for any injury etc. caused to him during the period of the training.
4. The student will abide by all the rules and regulations of ONGC while inside its premises.
5. The training shall not incur any liability on ONGC for providing any job to the trainee.
6. **On completion of the period of the training, the student will have to submit a report (in soft and hard copy) to the Mentor.** On the basis of the report, the Mentor would issue a letter of completion in prescribed format (Annexure-B) to the trainee specifying the period of training and topic/subject on which the training was conducted
7. The trainee would submit the completion letter along with a copy of report (in soft copy) and copy of this letter to this office for issuing the Certificate of Completion. The soft copy of the report be mailed to SHAH_SB@ongc.co.in.
8. Mentor should ensure the regular attendance of the student during the training period.
9. The Mentor shall take care of the confidentiality of ONGC data/information.
10. The training period dates may slightly vary depending upon the availability of the mentor.

The student is hereby directed to report along with college ID card to **Mr Ankit Puri, EE (Elex), Infocom, RO, NBP Green Heights /11 High , ONGC, Mumbai**, for further guidance.

(S.B.SHAH)

SE (P),

For DGM-Head SDC

Distribution:

1. Vaishnavi Anand, Student of SRM University, Tamilnadu
2. Mr Ankit Puri, EE (Elex), Infocom, RO, NBP Green Heights/11 high, ONGC, Mumbai
3. In-charge Security, NBP Green Heights, ONGC, Mumbai
4. The HOD, SRM University, Tamilnadu

STUDENT'S DECLARATION

I Vaishnavi Anand, hereby declare that the work being presented in this report entitled "**Computer Networking**" submitted to **Shree Ramaswamy Memorial Institute of Science and Technology (SRM)** is an authentic record of my own work carried out under the guidance of **Mr. Ankit Puri**.


Dated: 08/01/2018



(Vaishnavi Anand)

Btech - ECE

This is to certify that the above statement made by the candidate is correct to the best of my knowledge.



Mr. ANKIT PURI

Dy SE (ELECTRONICS)

ACKNOWLEDGEMENT

I take this opportunity to express my profound sense of gratitude and appreciation to all those who helped me throughout the duration of this project.

I would like to thank **Mr. Ankit Puri, Dy.S.E (Elx)** for his encouragement, support and providing necessary facilities along with his guidance and expert supervision for this project.

I am truly thankful to the entire **Infocom team** for their support and timely help

LIST OF CONTENTS

CONTENTS

ABSTRACT	9
NETWORKING	9
About Oil and Natural Gas Corporation	10
Overview of the Company	10
History of the Company	10
Delhi is the Corporate Headquarters of ONGC	12
INFOCOM ACTIVITIES IN ONGC	14
Projects	14
IT Applications	14
Secirity System.....	14
VOIP Telephony	15
Wifi Access points.....	15
ADS – Active Directory Services	15
ANTIVIRUS SYSTEM	16
Tenable:	16
Algosec:.....	16
CYBER ARC (PIM)	17
Enterprise Vault	18
CPM – Central Policy Manager	18
PSM – Privileged Session Manager	19
PVWA – Privileged Vault Web Access	19
VOIP (Voice over Internet Protocol)	20
Working	20
VOIP Advantages	21
Proxy Server	23
DNS (Domain name System) Server	24
FIREWALL	25
DAOS folder.....	27
IT Network and Communication setup	28
ONSHORE CONNECTIVITY	28

LAN SETUP.....	29
WAN SETUP	29
OFFSHORE CONNECTIVITY	30
Application of ONGC	33
ONGC Reports.....	33
Email MAIL ID/Lotus Notes 8.5.3	33
WEBICE	33
INTERNET	33
INTRANET	34
IP MESSENGER.....	34
VIDEO CONFERENCING	34
OSI REFERENCE MODEL	35
Physical (Layer 1).....	36
Data Link (Layer 2)	36
Network (Layer 3)	36
Transport (Layer 4).....	36
Session (Layer 5)	37
Presentation (Layer 6)	37
Application (Layer 7)	37
IP ADDRESSING AND SUBNETTING	38
NETWORKING	41
VLAN	41
Simulation	41
STATIC ROUTING USING 2 ROUTERS	53
SIMULATION	54

ABSTRACT

NETWORKING

This report includes full-fledged networking system used at ONGC. IT communication between users within LAN and over WAN is discussed along with various servers used and their setup, the LAN connectivity given through L3 and L2 switches and the leased lines connectivity terminated at exchanges are described. It includes working of Network operation Centre and efficient usage of limited range of IPs done at ONGC and the brief overview of SCADA is also given.

The Aim of our project was to understand how the organization ONGC provides its IT applications through networks in Onshore as well as Offshore locations and how it provides connectivity to data as well as users at different ONGC offices.

ABOUT OIL AND NATURAL GAS CORPORATION

OVERVIEW OF THE COMPANY

Oil and Natural Gas Corporation Limited (ONGC) is an Indian multinational oil and gas company headquartered in Dehradun, Uttarakhand, India. It is a Public Sector Undertaking (PSU) of the Government of India, under the administrative control of the Ministry of Petroleum and Natural Gas. It is India's largest oil and gas exploration and production company. It produces around 69% of India's crude oil (equivalent to around 30% of the country's total demand) and around 62% of its natural gas.

On 31 March 2013, its market capitalisation was INR 2.6 trillion (US\$48.98 billion), making it India's second largest publicly traded company. In a government survey for FY 2011–12, it was ranked as the largest profit making PSU in India. ONGC has been ranked 357th in the Fortune Global 500 list of the world's biggest corporations for the year 2012. It is ranked 17th among the Top 250 Global Energy Companies by Platts.

ONGC was founded on 14 August 1956 by Government of India, which currently holds a 68.94% equity stake. It is involved in exploring for and exploiting hydrocarbons in 26 sedimentary basins of India, and owns and operates over 11,000 kilometres of pipelines in the country. Its international subsidiary ONGC Videsh currently has projects in 17 countries. ONGC has discovered 6 of the 7 commercially producing Indian Basins, in the last 50 years, adding over 7.1 billion tonnes of In-place Oil & Gas volume of hydrocarbons in Indian basins. Against a global decline of production from matured fields, ONGC has maintained production from its brownfields like Mumbai High, with the help of aggressive investments in various IOR (Improved Oil Recovery) and EOR (Enhanced Oil Recovery) schemes. ONGC has many matured fields with a current recovery factor of 25–33%.^[2] Its Reserve Replacement Ratio for between 2005 and 2013, has been more than one. During FY 2012–13, ONGC had to share the highest ever under-recovery of INR 494.2 million (an increase of INR 49.6 million over the previous financial year) towards the under-recoveries of Oil Marketing Companies (IOC, BPCL and HPCL).

HISTORY OF THE COMPANY

In 1955, Government of India decided to develop the oil and natural gas resources in the various regions of the country as part of Public Sector development. With this objective, an Oil and Natural Gas Directorate was set up in 1955 under the then Ministry of Natural Resources and Scientific Research. The department was constituted with a nucleus of geoscientists from the Geological survey of India.

Soon, after the formation of the Oil and Natural Gas Directorate, it became apparent that it would not be possible for the Directorate with limited financial and administrative powers to function efficiently. So in August, 1956, the Directorate was raised to the status of a commission with enhanced powers, although it continued to be under the government. In October 1959, the Commission was converted into a statutory body by an act of Parliament, which enhanced powers of the commission further. The main functions of the Oil and Natural Gas Commission subject to the provisions of the Act, were "to plan, promote, organize and implement programmes for development of Petroleum Resources and the production and sale of petroleum and petroleum products produced by it, and to perform such other functions as the Central Government may, from time to time, assign to it". The act further outlined the activities and steps to be taken by ONGC in fulfilling its mandate.

Since its inception, ONGC has been instrumental in transforming the country's limited upstream sector into a large viable playing field, with its activities spread throughout India and significantly in overseas territories. In the inland areas, ONGC not only found new resources in Assam but also established new oil province in Cambay basin (Gujarat), while adding new prolific areas in the Assam-Arakan Fold Belt and East coast basins (both inland and offshore).

ONGC went offshore in early 70's and discovered a giant oil field in the form of Bombay High, now known as Mumbai High. This discovery, along with subsequent discoveries of huge oil and gas fields in Western offshore changed the oil scenario of the country. Subsequently, over 5 billion tonnes of hydrocarbons, which were present in the country, were discovered. The most important contribution of ONGC, however, is its self-reliance and development of core competence in E&P activities at a globally competitive level.

The liberalized economic policy, adopted by the Government of India in July 1991, sought to deregulate and de-license the core sectors (including petroleum sector) with partial disinvestments of government equity in Public Sector Undertakings and other measures. As a consequence thereof, ONGC was re-organized as a limited Company under the Company's Act, 1956 in February 1994.

After the conversion of business of the erstwhile Oil & Natural Gas Commission to that of Oil & Natural Gas Corporation Limited in 1993, the Government disinvested 2 per cent of its shares through

competitive bidding. Subsequently, ONGC expanded its equity by another 2 per cent by offering shares to its employees.

Branches of ONGC

Delhi is the Corporate Headquarters of ONGC

Western region:-

- 11 High, Mumbai
- NBP Green Heights
- Priyadarshini, Mumbai
- Uran, Mumbai
- VasudharaBhavan, Mumbai
- Panvel, Mumbai
- Ankleshwar
- Ahmedabad-Asset
- Ahmedabad-IRS
- Mehsana
- Vadodara
- Cambay
- Hazira
- Goa
- Jodhpur

North Region:-

- Scope Minar, New Delhi
- DUB, ,New Delhi
- Dehradun-ONGC Academy
- Dehradun-Telbhavan

Southern Region:-

- Chennai
- Karaikal
- Rajahmundry
- Kakinada

Central Region

- Kolkata
- Bokaro

North Eastern Region:-

- Agartala
- Jorhat
- Nazira/Sibsagar
- Silchar

INFOCOM ACTIVITIES IN ONGC

Infocom in ONGC performs wide variety of operations & activities briefly brought out under:

PROJECTS

- VATMS (Vessel and Air Traffic Management System) West
- VATMS (Vessel and Air Traffic Management System) East
- Enterprise Wide Access Control System
- Up-gradation of the Onshore Microwave Project
- SCADA
- WAN Upgradation (Routers & Switches)

IT APPLICATIONS

- SAP
- ADS
- NOC
- DNS
- DHCP
- Proxy

SECURITY SYSTEM

- Firewall
- Web Sense
- Cyber-arc
- Antivirus
- Pravesh

VOIP TELEPHONY

- Cisco VOIP

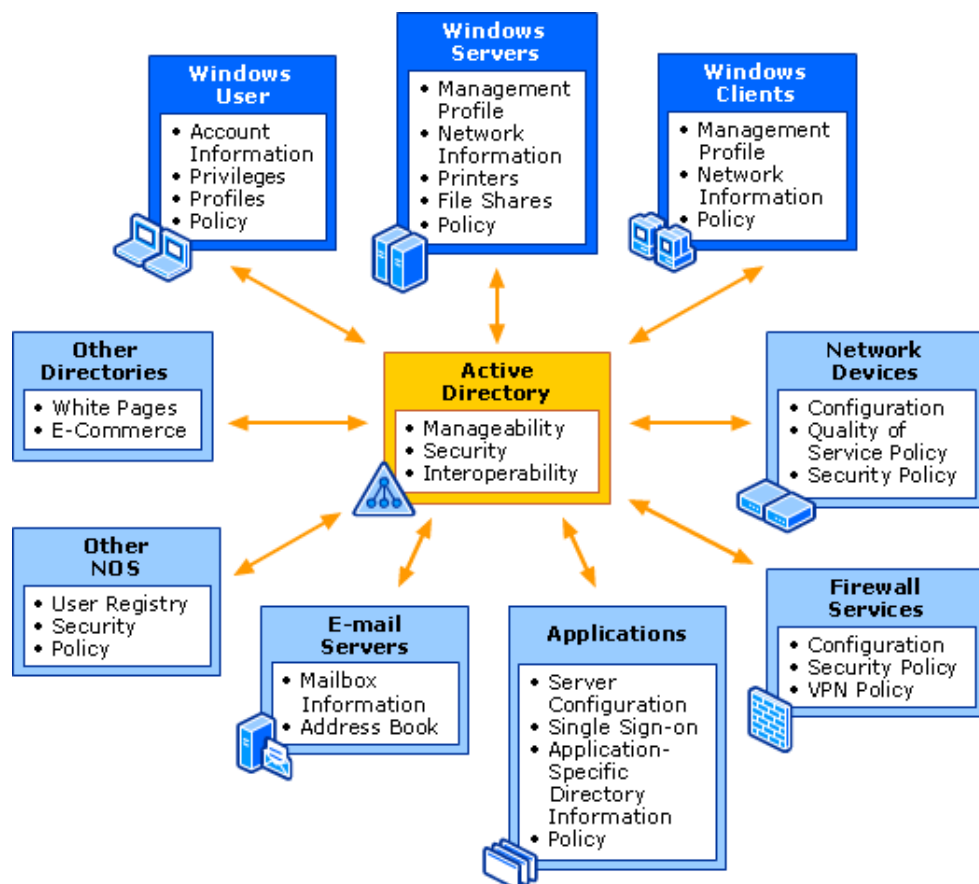
WIFI ACCESS POINTS

- Cisco Wifi Access Point

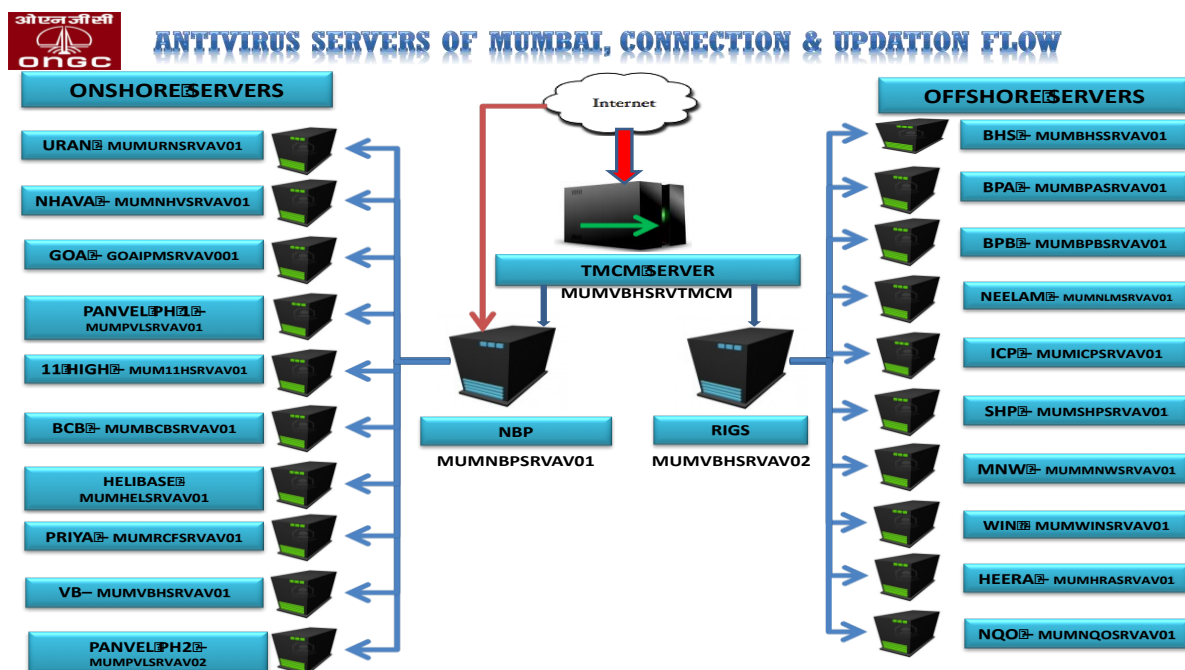
ADS – ACTIVE DIRECTORY SERVICES

Active Directory is a directory service Microsoft developed for Windows Domain networks. An ADS domain controller authenticates and authorizes all users and computers in a Windows domain type network assigning and enforcing security policies for all computers and installing or updating software.

Example: when a user logs into a computer that is a part of a windows domain, Active Directory checks the submitted password and determines whether the user is system administrator or normal user.



ANTIVIRUS SYSTEM



TENABLE:

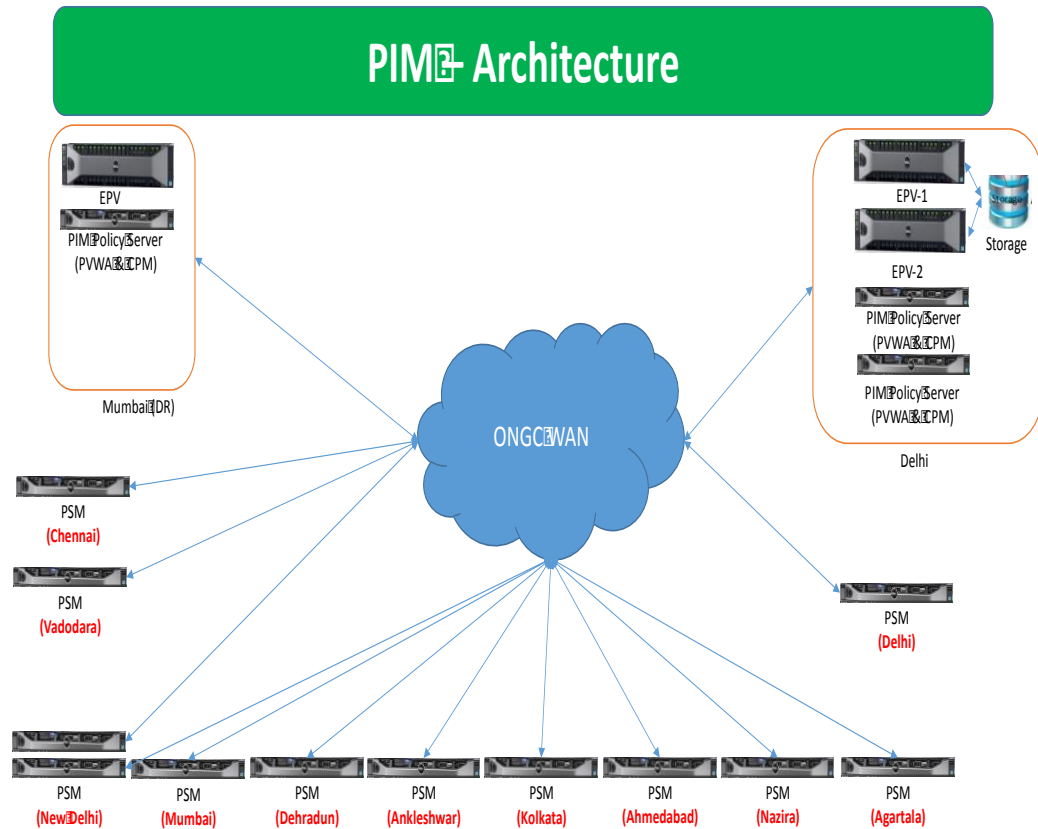
Security Center (SCCV) as a management console will be installed at DELHI and MUMBAI on DELL PowerEdge 630 servers which will provide ONGC with the most comprehensive security coverage across its network infrastructure. Security Center will collect with its Scanner which is combination of Nessus and Passive Vulnerability Scanner (PVS) which will again be running on the single DELL PowerEdge 630 located at Various ONGC locations.

ALGOSEC:

Algosec appliance installed Delhi and Mumbai which will be clustered for fault tolerance, ensuring availability if system components fail. For Disaster Recovery, AlgoSec appliances will

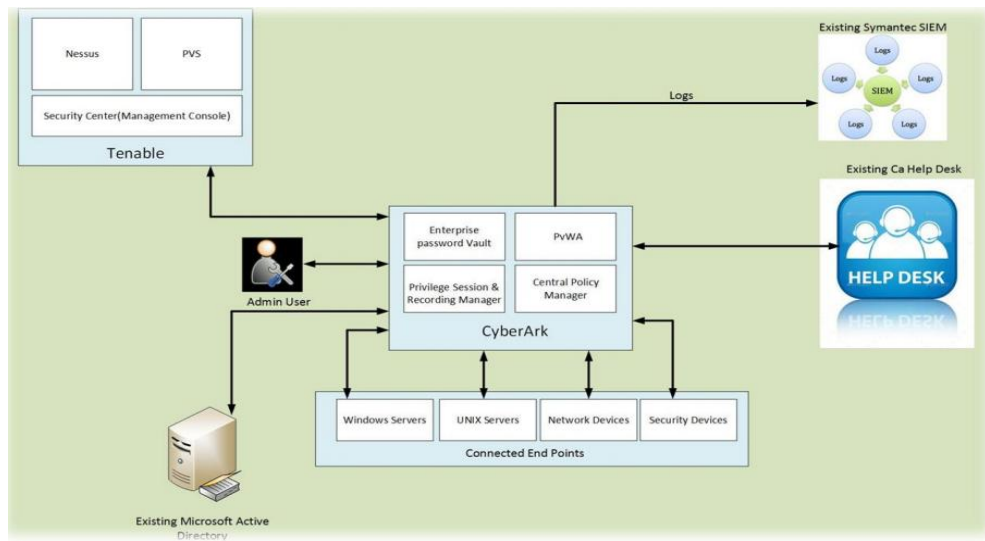
automatically synchronize data with offsite appliances to provide redundancy and ensure data preservation in the event of a failure at the primary site.

CYBER ARC (PIM)



- Control, manage, record and monitor privileged user accounts across critical IT resources
- Implementation of industry best practices such as process to on and off-board privileged users, least privilege for everything, strong authentication, manage passwords etc.
- Implement suitable workflows for Privileged Identity Management in the solution.

PIM[®] Integration



ENTERPRISE VAULT

- Enable PIM solution to securely store all the passwords for privileged accounts.
- Vault server also stores all the logs related to PIM solution including the video recordings of privileged sessions.

CPM – CENTRAL POLICY MANAGER

- Enable PIM solution to manage passwords of privileged accounts at the target system.
- As per the configured password policies in vault, CPM updates the passwords of privileged accounts at target and in the vault server.
- CPM also empowers PIM to verify privileged IDs at targets and reconcile those IDs into the PIM solution.

PSM – PRIVILEGED SESSION MANAGER

- Enable PIM solution to securely access target systems.
- A direct RDP of PSM server will be opened in user's browser once user accesses the target system using a privileged ID.
- PSM also records privileged sessions and transfers the recording to vault server.

PVWA – PRIVILEGED VAULT WEB ACCESS

- Provide a secured and centralized portal to access target systems using privileged IDs.
- PVWA will authenticate users based on their existing credentials stored in Active directory and authorize them based on their roles.
- PVWA will also enable PIM solution administrators to make configurations changes for existing integrated targets, integrate new targets, generating/viewing the reports, viewing the videos etc.

VOIP (VOICE OVER INTERNET PROTOCOL)

Voice over Internet Protocol (also **voice over IP**, **VoIP** or **IP telephony**) is a methodology and group of technologies for the delivery of voice communications and multimedia sessions over Internet Protocol(IP) networks, such as the Internet. The terms **Internet telephony**, **broadband telephony**, and **broadband phone service** specifically refer to the provisioning of communications services (voice, fax, SMS, voice-messaging) over the public Internet, rather than via the public switched telephone network (PSTN).

WORKING

A way is required to turn analog phone signals into digital signals that can be sent over the Internet. This function can either be included into the phone itself or in a separate box like an ATA .

VOIP Using an ATA

Ordinary Phone ---- ATA ---- Ethernet ---- Router ---- Internet ---- VOIP Service Provider

VOIP using an IP Phone

IP Phone ----- Ethernet ----- Router ---- Internet ---- VOIP Service Provider

VOIP connecting directly

It is also possible to bypass a VOIP Service Provider and directly connect to another VOIP user. However, if the VOIP devices are behind NAT routers, there may be problems with this approach.

IP Phone ----- Ethernet ----- Router ---- Internet ---- Router ---- Ethernet ---- IP Phone

VOIP ADVANTAGES

There are two major reasons to use VOIP

- Lower Cost
- Increased functionality

Lower Cost

In general phone service via VOIP costs less than equivalent service from traditional sources. This is largely a function of traditional phone services either being monopolies or government entities. There are also some cost savings due to using a single network to carry voice and data. This is especially true when users have existing under-utilized network capacity that they can use for VOIP without any additional costs.

In the most extreme case, users see VOIP phone calls (even international) as FREE. While there is a cost for their Internet service, using VOIP over this service may not involve any extra charges, so the users view the calls as free. There are a number of services that have sprung up to facilitate this type of "free" VOIP call. Examples are: Free World Dialup and Skype for a more complete list see:

VOIP Service Providers

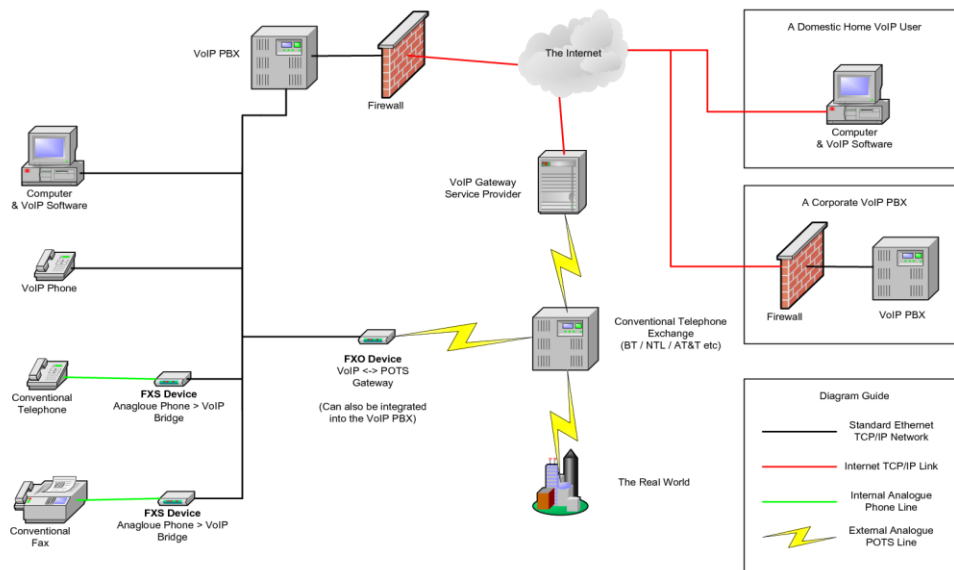
Friends and family overseas can call you for the lower price of a local call. Switch2Voip offers VoIP phone numbers in cities over 40 countries to add to your Switch2Voip VoIP account.

Increased Functionality

VOIP makes easy some things that are difficult to impossible with traditional phone networks.

- Incoming phone calls are automatically routed to your VOIP phone where ever you plug it into the network. Take your VOIP phone with you on a trip, and anywhere you connect it to the Internet, you can receive your incoming calls.
- Call center agents using VOIP phones can easily work from anywhere with a good Internet connection.

A Basic VoIP System



PROXY SERVER

In computer networks, a proxy server is a server that acts as an intermediary for requests from clients seeking resources from other servers. A client connects to proxy server, requesting a web page or other resource available from a different server. The proxy server evaluates the request as a way to simplify and control their complexity.

The proxy server evaluates the request according to its filtering rules. It is used for the following reasons:

1. It is mainly used to keep machines behind it anonymous, mainly for security.
2. To speed up access to resources (using caching). Web proxies are commonly used to cache web pages from a web server.
3. To apply access policy to network services or content, e.g. to block undesired sites.

Websense Proxy server is used in NBP green Heights, ONGC, Mumbai. Today, most proxies are web proxies, facilitating access to content on the World Wide Web.

DNS (DOMAIN NAME SYSTEM) SERVER

The **Domain Name System** (DNS) is a standard technology for managing the names of Web sites and other Internet domains. It allows us to type names into our Web browser like example.com and our computer to automatically find that address on the Internet. A DNS server is any computer registered to join the Domain Name System. A DNS server runs special-purpose networking software, features a public IP address, and it basically contains a database of network names and addresses for other Internet hosts.

DNS networking is based on the client / server architecture. Your Web browser functions as a **DNS client (also called DNS resolver)** and issues requests to your Internet provider's DNS servers when navigating between Web sites.

When a DNS server receives a request not in its database (such as a geographically far away or rarely visited Web site), it temporarily transforms from a server to a DNS client. The server automatically passes that request to another DNS server or up to the next higher level in the DNS hierarchy as needed. Eventually the request arrives at a server that has the matching name and IP address in its database (all the way to the root level if necessary), and the response flows back through the chain of DNS servers to your client.

FIREWALL

Nokia firewall is used in VasudharaBhawan, ONGC, Mumbai. A firewall can either be software-based or hardware-based and it tries to keep a network secure. Its primary objective is to **control the incoming and outgoing network traffic** by analyzing the data packets and determining whether it should be allowed through or not, based on ONGC's policies. A firewall builds a bridge between an internal network that is assumed to be secure and trusted, and another network, usually an external (inter)network, such as the Internet, that is not assumed to be secure and trusted.

A system designed to prevent unauthorized access to or from a private network. It is frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

NATting is done in firewall. **Network address translation (NAT)** is a technology whereby network address information in Internet Protocol (IP) datagram packet headers is modified while they are in transit across a traffic routing device for the purpose of remapping one IP address space into another.

Here NATting is done in **Load balancer** to divert the Traffic from Firewall.

MAIL SERVER SYSTEM

ONGC does its communication mostly over the mail. The employees use the mail service not only to communicate with each other but also with the people outside the organization like vendors, contractors, auditors etc.). Thus there is a requirement to give them a unique domain mail service for authenticity. For this purpose, ONGC has its own mail servers.

At ONGC it consists of one **primary Server**, one **secondary server** and a **Disaster recovery Server**. The system is such that we have one primary and one secondary server at Mumbai where in secondary stores **the replicated data** from primary server and the DR of Mumbai is at Delhi and similarly the DR of Delhi is at Mumbai. There is a backup server which Increments the data on (taking time to time back up) every time. **Robotic Tape Library** is used for taking incremental and full online backup on the tapes as per ONGC defined policies. This is to have a hardcopy of the data and in case of any crash of the EMC² storage the Tape Library can be used to restore the data.

70TB storage is given to the whole mail server system. **Interscan messaging security virtual appliance (IMSVa)** is provided scan incoming and outgoing mails, today **IMSVa 8.1.0** is in use, and earlier InterScan Messaging Security Suite (IMSS) was used.

ONGC uses licensed version of **IBM Lotus iNotes version 8.5.3** which provides single user unlimited mail box and an unlimited archiving space. An attachment of **25 mb data can be sent**. Archiving is done after every 90 days

DAOS FOLDER

According to this **DAOS concept** the attachments over 2 Mb are stored in a DAOS folder and users get the **link to the attachment saved** and the attachment in the DAOS folder can only be deleted when all the recipients of that particular mail delete it. This concept gives the **efficient usage of storage space**

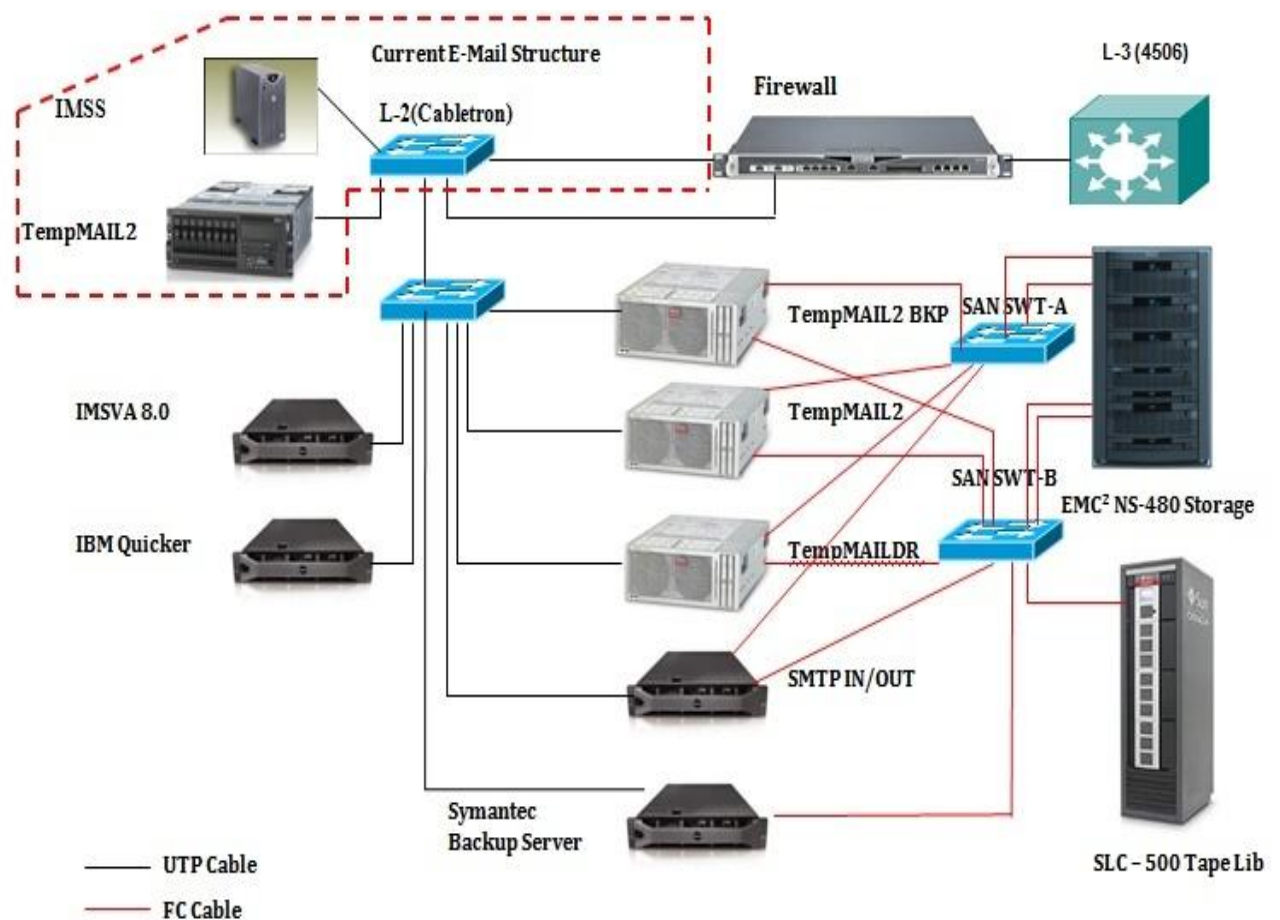


Figure : mail server setup

IT NETWORK AND COMMUNICATION SETUP

Mumbai region consists of

- | | |
|----|--------------------|
| 1. | Onshore Locations |
| 2. | Offshore locations |
| 3. | Goa |
| 4. | Hazira plant |
| 5. | Uran location |

Leased Lines (optical fiber) are used to connect these locations.

ONGC Onshore locations are connected using lease lines (30nos) of different bandwidth as required

Line communication is required for basic 3 purposes:

- | | |
|----|-----------|
| 1. | Telephone |
| 2. | FAX |
| 3. | IP phone |

ONSHORE CONNECTIVITY

The desktops in the offices of ONGC are connected by LAN technology while the different offices of ONGC are connected by WAN technology. There are three routers in Vasudhara Bhawan. 1 is for onshore connectivity, 2 is for offshore connectivity, 3rd is for rigs connectivity.

LAN SETUP

All offices in Mumbai are connected and even rigs and platforms at offshore are connected through WAN network. All the computers interconnected to each other using layer2 and layer3 switches.

There are eight floors at VB and at each floor there are layer2 switches in LAN racks and on the seventh floor there are layer3 switches. Each floor is then divided into two wings A and B. In each wing there are L2 switches as per requirement of number of nodes needed. All the L2 switches at each floor are connected to the L3 switch on the 7th floor through **vertical backbone cabling** e.g. L2 switches in wing A are connected to L3 in wing A and similarly for wing B. The L2 switches in each floors are connected to each other by the **UTP cables**, thus if a certain L2 to L3 connection fails than it can take the other path. On the 7th floor the L3 switches are connected to each other by **horizontal cabling**. The L3 switches are connected to the router.

WAN SETUP

Wide Area Network combines multiple LANs that are geographically separate. ONGC connects the different LANs using **leased lines**, **radio links** and **Integrated Services Digital Network (ISDN)**.

All onshore offices are connected over Lease Lines and offshore platforms and rigs are connected using Satcom like Kuban and Cband connectivity.

Leased line- Leased Lines are the service contract between a provider and a customer where a provider agrees to deliver a telecommunication line connecting two or more locations in exchange for a monthly rent. It does not have a telephone number, each side of the line being permanently connected to each other. Leased lines can be used for telephone, data or internet services. ONGC has rented lease lines of 2 Mb, 4 Mb, 6 Mb and 8 Mb according to the usage of data transmission.

Radio links- They are widely used for point-to-point communications because their small wavelength allows conveniently-sized antennas to direct them in narrow beams, which can be pointed directly at the receiving antenna. Another advantage is that the high frequency of microwaves gives the microwave band a very large information-carrying capacity; the microwave band has a very high bandwidth. A disadvantage is that radio links are limited to line of sight propagation; they cannot pass

around hills or mountains as lower frequency radio waves can. It is used between Trombay and Nhava as they lie within line of sight (LOS) and also Helibase and VB.

ISDN- Integrated Services Digital Network (ISDN) is a set of communication standards for simultaneous digital transmission of voice, video, data, and other network services over the traditional circuits of the public switched telephone network. The key feature of ISDN is that it integrates speech and data on the same lines, adding features that were not available in the classic telephone system. ISDN is used in ONGC only when the lease lines are down otherwise it isn't used much.

OFFSHORE CONNECTIVITY

There are many electromagnetic spectrum bands. ONGC uses C and Ku band for connecting onshore with offshore.

C-BAND: C band uplink is 4 GHz and downlink is 8 GHz. It is used for official purpose. C band is used for critical data. It is a 2.4 m antenna. It is mission critical. SCADA finds useful purposes by using C band.

Advantages:

- Less disturbance from heavy rain fade
- Cheaper Bandwidth

Disadvantages:

- Needs a larger satellite dish (diameters of minimum 2-3m)
- Powerful (=expensive) RF unit
- More expensive hardware
- Possible Interference from microwave links

Ku-Band: The uplink of Ku band is 12 GHz and downlink is 18 GHz. Video Conferencing, internet etc., used for secondary purposes. It is a redundancy of C-band. It is a 1.2m antenna. No fading occurs since many antennae can be used in a given region. It may break down during rains but its failure does not bother much, as it is used for non-critical applications in the company.

Advantages:

- No interference from microwave links and other technologies
- Operates with a smaller satellite dish (diameters from 0.9m) and cheaper and more easy installation
- Needs less power and cheaper RF unit

Disadvantages:

- More expensive capacity
- Sensitive to heavy rain fade (significant attenuation of the signal) / possibly can be managed by appropriate dish size or transmitter power.

Both can be used as an alternate for each other. If C-band is down, K-band automatically takes the traffic which was earlier given to C-band. Vice-versa is not true. If K-band is down, its traffic is not automatically handled by C-band. C-band has to be manually configured to take the traffic of K-band.

C band applications- SCADA, SAP and WEBICE

Ku band applications- Video Conferencing, and non-critical traffic like Intranet, Internet, IP Messenger, ONGC reports and email

The routers at various locations of Mumbai are used to direct the network traffic to appropriate network (ONGC network here). All are directly connected to **VASUDHARA BHAVAN Office** which serves as the main hub for C band and **11HIGH Office** serves as the main hub for Ku band.

APPLICATION OF ONGC

ONGC REPORTS

ONGC Reports provides information regarding the overall activities of the organization on a global level including detailed Financial Results and other Performance **REPORTS**. The ONGC Reports Server is kept in Delhi.

EMAIL MAIL ID/LOTUS NOTES 8.5.3

Lotus Notes provides integrated collaboration functionality, including email, calendaring, and contacts management, to do tracking, instant messaging, an office productivity suite, and access to other Lotus Domino applications and databases.

WEBICE

is ONGC Employee portal based on SAP or ERP System. It contains information of all the Employees which are stored in the system in a separate Database. Through Web ice, an employee can undergo his financial, personal claims and other useful transactions which are available to them. The system was developed to make the employee transactions paperless. The WEBICE Server is also kept in Delhi.

INTERNET

It is a network of networks that consists of millions of private, public, academic, business, and government networks, of local to global scope, that are linked by a broad array of electronic, wireless and optical networking technologies.

INTRANET

An intranet is a computer network that uses Internet Protocol technology to share information, operational systems, or computing services within an organization. Every Location in ONGC has a separate INTRANET page which is maintained by INFOCOM of that location

IP MESSENGER

IP Messenger is a tool which allows users to send messages, files and folders across the LAN and WAN Network. It is the easiest and fastest way of communication employed in ONGC. Every specific user is identified through an IP Address allocated to them by the DHCP Server.

VIDEO CONFERENCING

Video conferencing is the conduct of a conference by a set of telecommunication technologies which allow two or more locations to communicate by simultaneous two-way video and audio transmissions.

OSI REFERENCE MODEL

Layer 7	Application
Layer 6	Presentation
Layer 5	Session
Layer 4	Transport
Layer 3	Network
Layer 2	Data link
Layer 1	Physical

The OSI reference model:

- Defines the process for connecting two layers together, promoting interoperability between vendors
- Separates a complex function into simpler components
- Allows vendors to compartmentalize their design efforts to fit a modular design, which eases implementations and simplifies troubleshooting
- Provides a teaching tool to help network administrators understand the communication process used between networking components

PHYSICAL (LAYER 1)

OSI Model, Layer 1 conveys the bit stream - electrical impulse, light or radio signal — through the network at the electrical and mechanical level. It provides the hardware means of sending and receiving data on a carrier, including defining cables, cards and physical aspects. Fast Ethernet, RS232, and ATM are protocols with physical layer components.

Layer 1 Physical examples include Ethernet, FDDI, B8ZS, V.35, V.24, and RJ45.

DATA LINK (LAYER 2)

At OSI Model, Layer 2, data packets are encoded and decoded into bits. It furnishes protocol knowledge and management and handles errors in the physical layer, flow control and frame synchronization. The data link layer is divided into two sub layers: The Media Access Control (MAC) layer and the Logical Link Control (LLC) layer. The MAC sub layer controls how a computer on the network gains access to the data and permission to transmit it. The LLC layer controls frame synchronization, flow control and error checking.

Layer 2 data link examples include PPP, FDDI, ATM, IEEE 802.5/ 802.2, IEEE 802.3/802.2, HDLC, and FRAME RELAY.

NETWORK (LAYER 3)

Layer 3 provides switching and routing technologies, creating logical paths, known as virtual circuits, for transmitting data from node to node. Routing and forwarding are functions of this layer, as well as addressing, internetworking, error handling, congestion control and packet sequencing.

Layer 3 network examples include AppleTalk DDP, IP, and IPX.

TRANSPORT (LAYER 4)

OSI Model, Layer 4, provides transparent transfer of data between end systems, or hosts, and is responsible for end-to-end error recovery and flow control. It ensures complete data transfer.

Layer 4 transport examples include SPX, TCP, and UDP.

SESSION (LAYER 5)

This layer establishes, manages and terminates connections between applications. The session layer sets up, coordinates, and terminates conversations, exchanges, and dialogues between the applications at each end. It deals with session and connection coordination.

Layer 5 session examples include NFS, NETBIOS NAMES, RPC, SQL.

PRESENTATION (LAYER 6)

This layer provides independence from differences in data representation (e.g., encryption) by translating from application to network format, and vice versa. The presentation layer works to transform data into the form that the application layer can accept. This layer formats and encrypts data to be sent across a network, providing freedom from compatibility problems. It is sometimes called the syntax layer.

Layer 6 presentation examples include ENCRYPTION, ASCII, EBCDIC, TIFF, GIF, PICT, JPEG, MPEG, AND MIDI.

APPLICATION (LAYER 7)

OSI Model, Layer 7, supports application and end-user processes. Communication partners are identified, quality of service is identified, user authentication and privacy are considered, and any constraints on data syntax are identified. Everything at this layer is application-specific. This layer provides application services for file transfers, e-mail, and other network software services. Telnet and FTP are applications that exist entirely in the application level. Tiered application architectures are part of this layer.

Layer 7 application examples include WWW BROWSERS, NFS, SNMP, TELNET, HTTP, and FTP

IP ADDRESSING AND SUBNETTING

- IP Address: A logical numeric address that is assigned to every single computer, printer, switch, router or any other device that is part of a TCP/IP-based network
- Subnet: A separate and identifiable portion of an organization's network, typically arranged on one floor, building or geographical location
- Subnet Mask: A 32-bit number used to differentiate the network component of an IP address by dividing the IP address into a network address and host address
- Network Interface Card (NIC): A computer hardware component that allows a computer to connect to a network

A subnet, is a logical organization of connected network devices.

Each device on each subnet has an address that logically associates it with the others on the same subnet. This also prevents devices on one subnet from getting confused with hosts on the other subnet.

In terms of IP addressing and subnets, these devices are referred to as hosts.

Any one of the numbers between the dots can be between 0 and 255, so example IP addresses include:

- 205.112.45.60
- 34.243.44.155

These numbers can also be written in binary form by taking each of the decimal values separated by dots and converting to binary. So a number like 205.112.45.60 could be written as:

11001101.01110000.00101101.00111100

Each of these binary components is referred to as an octet.

Each IP address belongs to a class of IP addresses depending on the number in the first octet. These classes are:

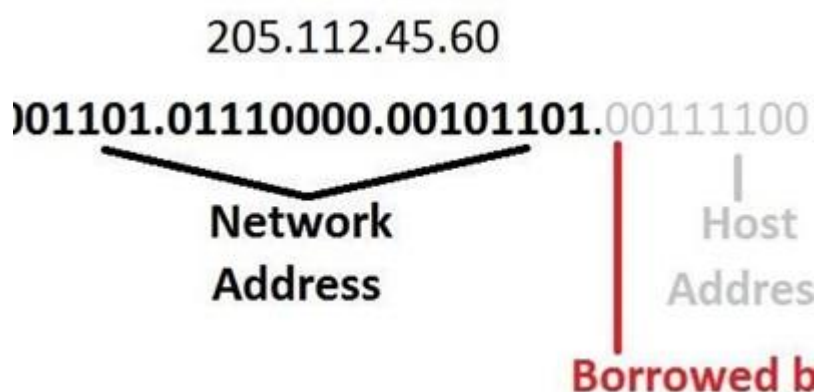
First Octet value	Class	Example IP address
0 - 126	Class A	34.126.35.125
128 - 191	Class B	134.23.45.123
192 - 223	Class C	212.11.123.3
224 - 239	Class D	225.2.3.40
240 - 255	Class E	245.192.1.123

Notice that the number 127 is not included. That's because it is used in a special, self-reflecting number called a loopback address.

The network and host components of class IP addresses are:

Class	Address components	Network/ Host
Class A	Network.Host.Host.Host	34.126.35.125
Class B	Network. Network.Host.Host	134.23.45.123
Class C	Network. Network Network.Host	212.11.123.3
Class D	Not Defined	Not Defined
Class E	Not Defined	Not Defined

We create a subnet by logically grabbing the last bit from the network component of the address and using it to determine the number of subnets required. In the following example, a Class C address normally has 24 bits for the network address and eight for the host, but we are going to borrow the left-most bit of the host address and declare it as identifying the subnet.



If the bit is a 0, then that will be one subnet; if the bit is a 1 that would be the second subnet. Of course, with only one borrowed bit we can only have two possible subnets. By the same token, that also reduces the number of hosts we can have on the network to 127 (but actually 125 useable addresses given all zeros and all ones are not recommended addresses), down from 255.

Private IP addresses allow network administrators to extend the size of their networks. A network could have one public IP address that all traffic on the Internet sees, and hundreds - or even thousands - of hosts with private IP addresses on the company subnet.

Anyone can use a private IP address on the understanding that all traffic using these addresses must remain local. It would not be possible, for example, to have an email message associated with a private IP address to move across the Internet, but it is quite reasonable to have the same private IP address work well in the company network.

The private IP addresses that you can assign for a private network can be from the following three blocks of the IP address space:

- 10.0.0.1 to 10.255.255.255: Provides a single Class A network of addresses
- 172.16.0.1 to 172.31.255.254: Provides 16 contiguous Class B network addresses
- 192.168.0.1 to 192.168.255.254: Provides up to 216 Class C network addresses

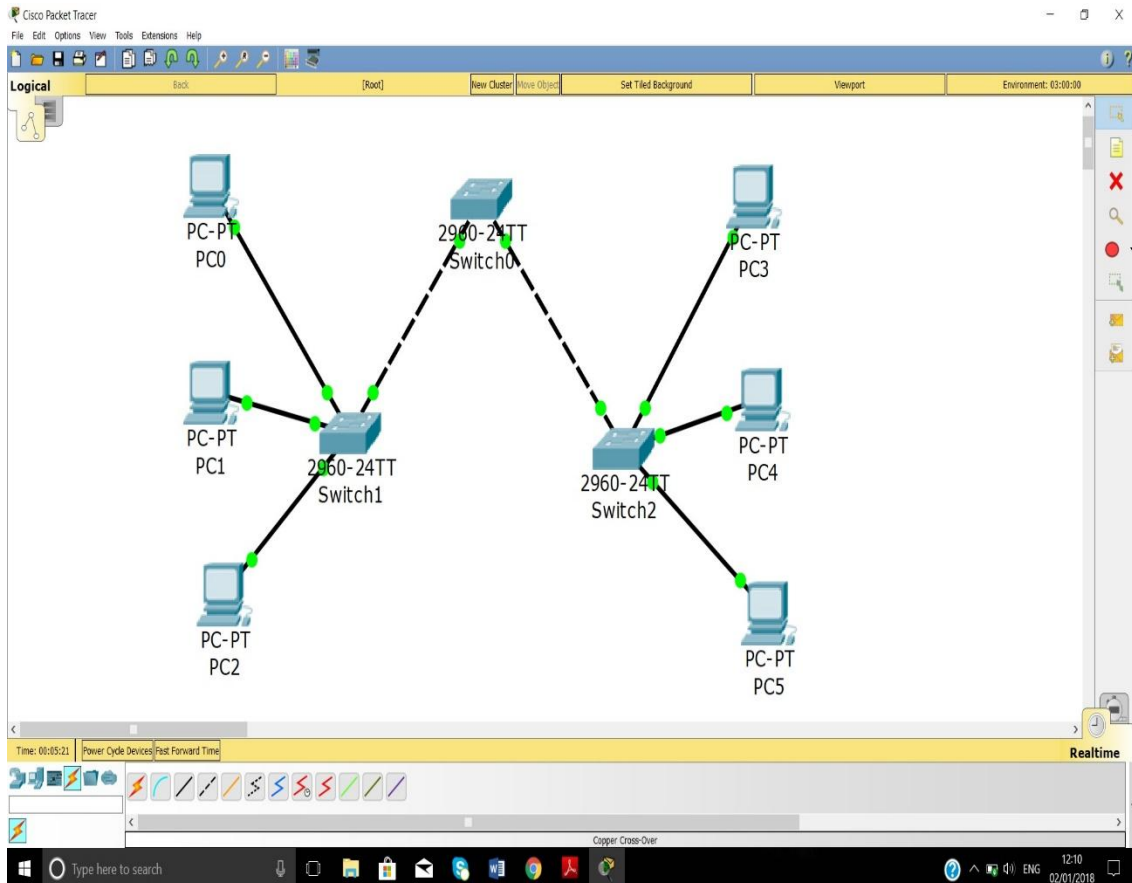
NETWORKING

VLAN

A **virtual LAN (VLAN)** is any broadcast domain that is partitioned and isolated in a computer network at the data link layer (OSI layer 2). LAN is the abbreviation for local area network and in this context virtual refers to a physical object recreated and altered by additional logic. VLANs work by applying tags to network packets and handling these tags in networking systems – creating the appearance and functionality of network traffic that is physically on a single network but acts as if it is split between separate networks. In this way, VLANs can keep network applications separate despite being connected to the same physical network, and without requiring multiple sets of cabling and networking devices to be deployed.

SIMULATION

Step 1: Cabling a network



Step 2: Re-enable the user ports on S1 and S2.

```
switch_A>en
switch_A#config t
Enter configuration commands, one per line. End with CNTL/Z.
switch_A(config)#interface range fa0/6, fa0/11, fa0/18
switch_A(config-if-range)#switchport mode access
switch_A(config-if-range)#no shutdown
```

```
switch2>en
switch2#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch2(config)#interface range fa0/6, fa0/11, fa0/18
Switch2(config-if-range)#switchport mode access
Switch2(config-if-range)#no shutdown
```

Step 3: Configure VLANs on the Switch0, 1 and 2

```
Switch1>en
Switch1#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch1(config)#vlan 10
Switch1(config-vlan)#name faculty/staff
Switch1(config-vlan)#vlan 20
Switch1(config-vlan)#name students
Switch1(config-vlan)#vlan 30
Switch1(config-vlan)#name guest
Switch1(config-vlan)#vlan 99
Switch1(config-vlan)#name management
Switch1(config-vlan)#end
```

Step 4: Assign switch ports to VLANs on S1 and S2

```
Switch2(config)#interface range fa0/6-10
Switch2(config-if-range)#switchport access vlan 30
Switch2(config-if-range)#interface range fa0/11-17
Switch2(config-if-range)#switchport access vlan 10
Switch2(config-if-range)#interface range fa0/18-24
Switch2(config-if-range)#switchport access vlan 20
Switch2(config-if-range)#end
```

Step 5: Configure trunking and the native VLAN for the trunking ports on all switches.

```
S0(config)#interface range fa0/1-5
S0(config-if-range)#switchport mode trunk
S0(config-if-range)#switchport trunk native vlan 99
S0(config-if-range)#no shutdown
S0(config-if-range)#end
```

```
S1(config)# interface range fa0/1-5
S1(config-if-range)#switchport mode trunk
S1(config-if-range)#switchport trunk native vlan 99
S1(config-if-range)#no shutdown
S1(config-if-range)#end
```

```
S2(config)# interface range fa0/1-5
S2(config-if-range)#switchport mode trunk
S2(config-if-range)#switchport trunk native vlan 99
S2(config-if-range)#no shutdown
S2(config-if-range)#end
```

Step 6: Verify that the switches can communicate.

From S1, ping the management address on both S2 and S3.
S1#ping 172.17.99.12
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.99.12, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/9 ms
S1#ping 172.17.99.13
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.99.13, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms

Step 7: Ping several hosts from PC2.

Ping from host PC2 to host PC1 (172.17.10.21). Is the ping attempt successful? _____ no
Ping from host PC2 to the switch VLAN 99 IP address 172.17.99.12. Is the ping attempt successful?
_____ no
Because these hosts are on different subnets and in different VLANs, they cannot communicate without
a
Layer 3 device to route between the separate subnetworks.
Ping from host PC2 to host PC5. Is the ping attempt successful? _____ yes
Because PC2 is in the same VLAN and the same subnet as PC5, the ping is successful

Step 8: Move PC1 into the same VLAN as PC2.

S2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#interface fastethernet 0/11
S2(config-if)#switchport access vlan 20
S2(config-if)#end

Ping from host PC2 to host PC1. Is the ping attempt successful? _____ no

Step 11: Change the IP address and network on PC1.

Change the IP address on PC1 to 172.17.20.22. The subnet mask and default gateway can remain the same. Once again, ping from host PC2 to host PC1, using the newly assigned IP address.
Is the ping attempt successful? _____yes

Running configurations

Switch 0

```

switch_A>enable
switch_A#sh runn
switch_A#sh running-config
Building configuration...

Current configuration: 1912 bytes
!
Version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname switch_A
!
!
!
!
!
spanning-tree mode pvst
!
interface FastEthernet0/1
switchport trunk native vlan 99
switchport mode trunk
!
interface FastEthernet0/2
switchport trunk native vlan 99
switchport mode trunk
!
interface FastEthernet0/3
switchport trunk native vlan 99
switchport mode trunk
!
interface FastEthernet0/4
switchport trunk native vlan 99
switchport mode trunk
!
interface FastEthernet0/5
switchport trunk native vlan 99
switchport mode trunk
!
interface FastEthernet0/6
switchport access vlan 30
switchport mode access
!
interface FastEthernet0/7
switchport access vlan 30
!
interface FastEthernet0/8
switchport access vlan 30
!

```

```
interface FastEthernet0/9
switchport access vlan 30
!
interface FastEthernet0/10
switchport access vlan 30
!
interface FastEthernet0/11
switchport access vlan 20
switchport mode access
!
interface FastEthernet0/12
switchport access vlan 10
!
interface FastEthernet0/13
switchport access vlan 10
!
interface FastEthernet0/14
switchport access vlan 10
!
interface FastEthernet0/15
switchport access vlan 10
!
interface FastEthernet0/16
switchport access vlan 10
!
interface FastEthernet0/17
switchport access vlan 10
!
interface FastEthernet0/18
switchport access vlan 20
switchport mode access
!
interface FastEthernet0/19
switchport access vlan 20
!
interface FastEthernet0/20
switchport access vlan 20
!
interface FastEthernet0/21
switchport access vlan 20
!
interface FastEthernet0/22
switchport access vlan 20
!
interface FastEthernet0/23
switchport access vlan 20
!
interface FastEthernet0/24
switchport access vlan 20
!
```

```

interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
shutdown
!
!
!
!
line con 0
!
line vty 0 4
login
line vty 5 15
login
!
!
!
end

```

Switch 1

```

switch_A>enable
switch_A#sh runn
switch_A#sh running-config
Building configuration...

```

Current configuration : 1912 bytes

```

!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname switch_A
!
!
!
!
spanning-tree mode pvst
!
interface FastEthernet0/1
switchport trunk native vlan 99
switchport mode trunk
!
interface FastEthernet0/2
switchport trunk native vlan 99

```

```
switchport mode trunk
!
interface FastEthernet0/3
switchport trunk native vlan 99
switchport mode trunk
!
interface FastEthernet0/4
switchport trunk native vlan 99
switchport mode trunk
!
interface FastEthernet0/5
switchport trunk native vlan 99
switchport mode trunk
!
interface FastEthernet0/6
switchport access vlan 30
switchport mode access
!
interface FastEthernet0/7
switchport access vlan 30
!
interface FastEthernet0/8
switchport access vlan 30
!
interface FastEthernet0/9
switchport access vlan 30
!
interface FastEthernet0/10
switchport access vlan 30
!
interface FastEthernet0/11
switchport access vlan 20
switchport mode access
!
interface FastEthernet0/12
switchport access vlan 10
!
interface FastEthernet0/13
switchport access vlan 10
!
interface FastEthernet0/14
switchport access vlan 10
!
interface FastEthernet0/15
switchport access vlan 10
!
interface FastEthernet0/16
switchport access vlan 10
!
interface FastEthernet0/17
```



```
switchport access vlan 10
!
interface FastEthernet0/18
switchport access vlan 20
switchport mode access
!
interface FastEthernet0/19
switchport access vlan 20
!
interface FastEthernet0/20
switchport access vlan 20
!
interface FastEthernet0/21
switchport access vlan 20
!
interface FastEthernet0/22
switchport access vlan 20
!
interface FastEthernet0/23
switchport access vlan 20
!
interface FastEthernet0/24
switchport access vlan 20
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
shutdown
!
!
!
!
line con 0
!
line vty 0 4
login
line vty 5 15
login
!
!
!
End
```

Switch 2

```

Switch>en
Switch#sh runn
Building configuration...

Current configuration : 1630 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
!
!
!
!
spanning-tree mode pvst
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
switchport access vlan 30
switchport mode access
!
interface FastEthernet0/7
switchport access vlan 30
!
interface FastEthernet0/8
switchport access vlan 30
!
interface FastEthernet0/9
switchport access vlan 30
!
interface FastEthernet0/10
switchport access vlan 30
!
interface FastEthernet0/11
switchport access vlan 10
switchport mode access
!
interface FastEthernet0/12

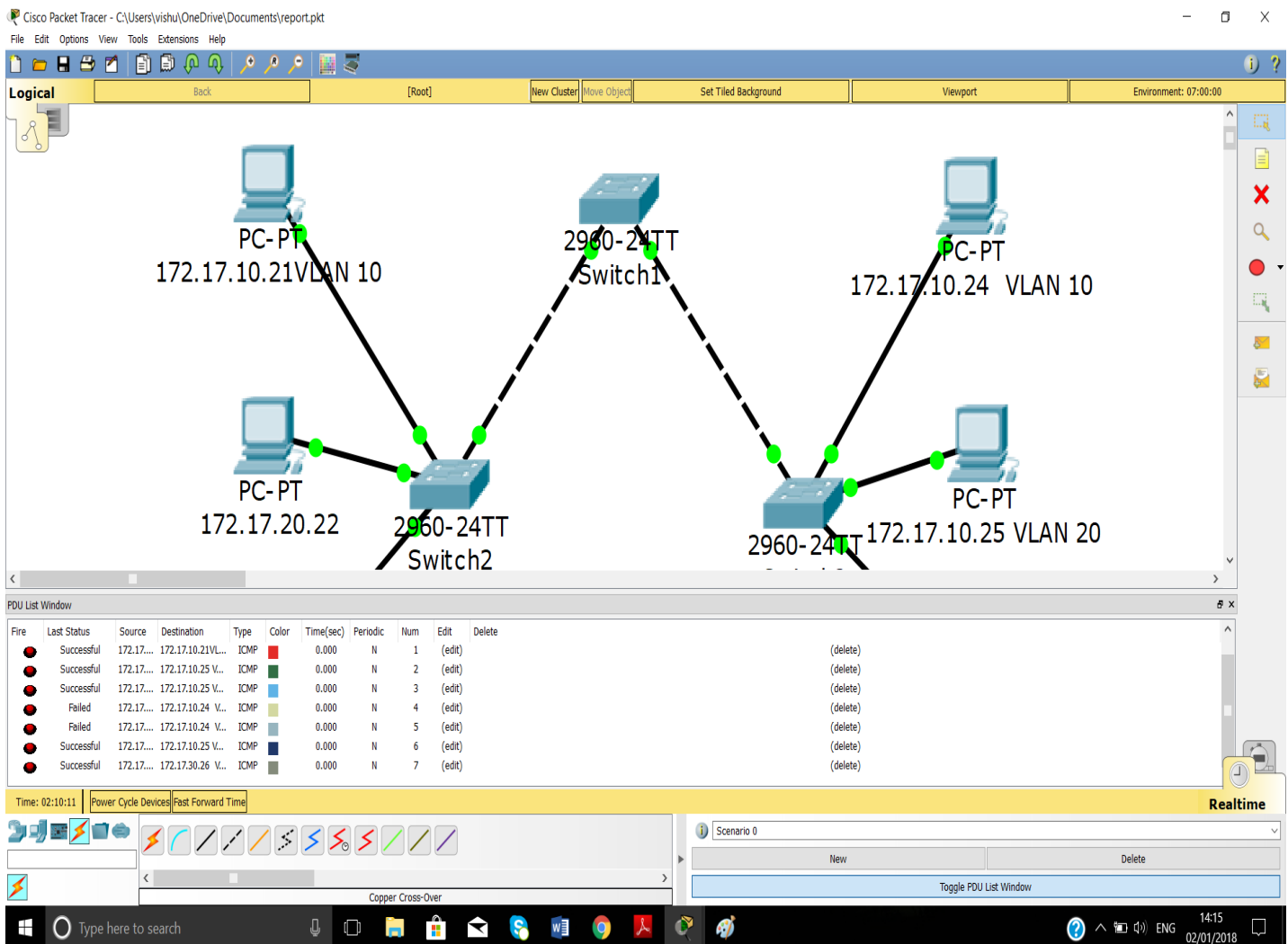
```

```
switchport access vlan 10
!
interface FastEthernet0/13
switchport access vlan 10
!
interface FastEthernet0/14
switchport access vlan 10
!
interface FastEthernet0/15
switchport access vlan 10
!
interface FastEthernet0/16
switchport access vlan 10
!
interface FastEthernet0/17
switchport access vlan 10
!
interface FastEthernet0/18
switchport access vlan 20
switchport mode access
!
interface FastEthernet0/19
switchport access vlan 20
!
interface FastEthernet0/20
switchport access vlan 20
!
interface FastEthernet0/21
switchport access vlan 20
!
interface FastEthernet0/22
switchport access vlan 20
!
interface FastEthernet0/23
switchport access vlan 20
!
interface FastEthernet0/24
switchport access vlan 20
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
shutdown
!
!
!
!
```

```

line con 0
!
line vty 0 4
login
line vty 5 15
login
!
!
!
end

```



STATIC ROUTING USING 2 ROUTERS

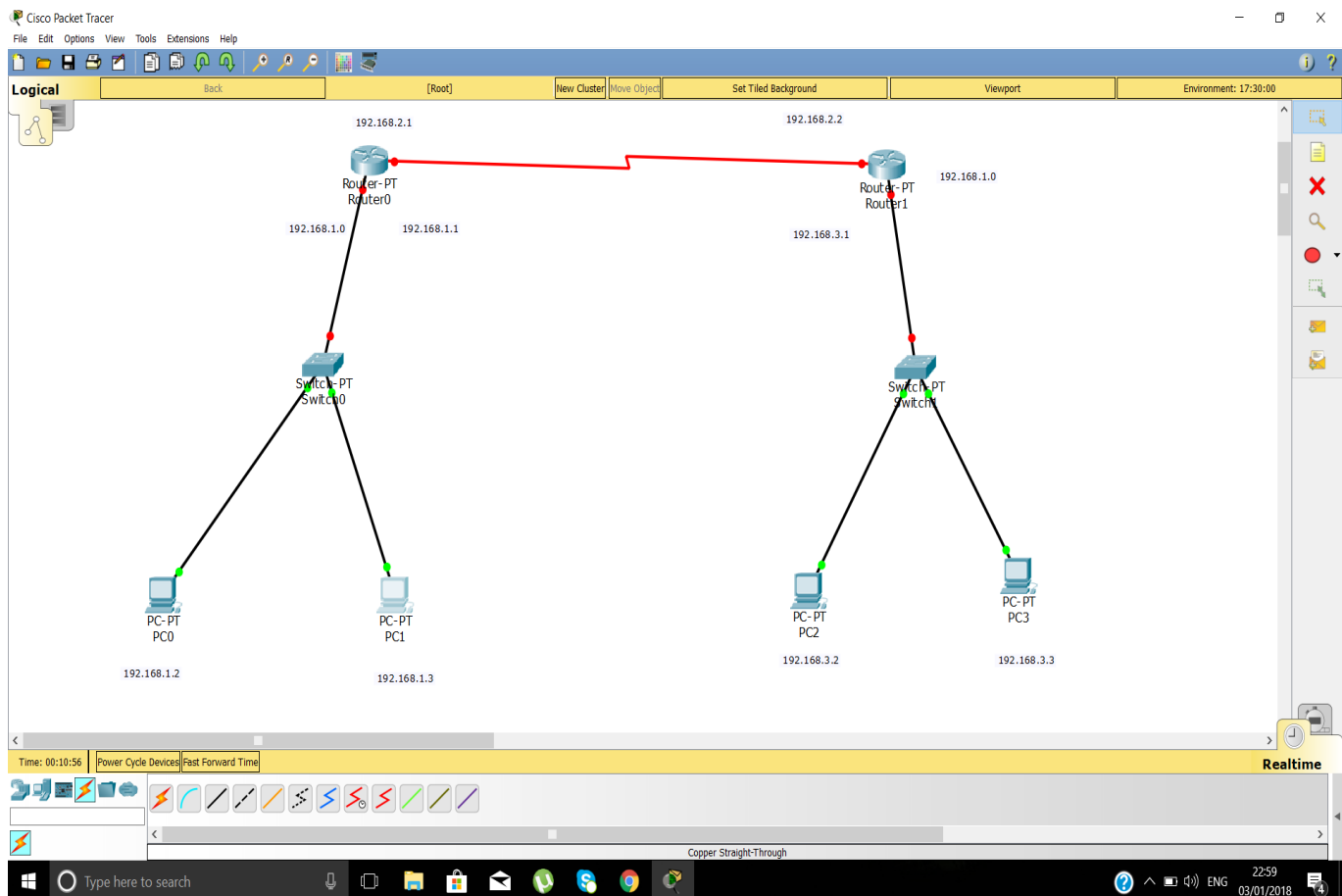
Static routing is a form of routing that occurs when a router uses a manually-configured routing entry, rather than information from a dynamic routing traffic.^[1] In many cases, static routes are manually configured by a network administrator by adding in entries into a routing table, though this may not always be the case.^[2] Unlike dynamic routing, static routes are fixed and do not change if the network is changed or reconfigured. Static routing and dynamic routing are not mutually exclusive. Both dynamic routing and static routing are usually used on a router to maximise routing efficiency and to provide backups in the event that dynamic routing information fails to be exchanged. Static routing can also be used in stub networks, or to provide a gateway of last resort.

Static routing may have the following uses:

- Static routing can be used to define an exit point from a router when no other routes are available or necessary. This is called a **default route**.
- Static routing can be used for small networks that require only one or two routes. This is often more efficient since a link is not being wasted by exchanging dynamic routing information.
- Static routing is often used as a complement to dynamic routing to provide a failsafe backup in the event that a dynamic route is unavailable.
- Static routing is often used to help transfer routing information from one routing protocol to another (routing redistribution).

SIMULATION

Step1:Cabling the setup



Step 2: Configure ip address to routers go to global configuration mode in R1 and R2 configure connected interfaces

In Router 1

Interface Fastethernet0/0 in global configuration mode

```
R1(config)#interface fastethernet 0/0
R1(config-if)#ip address 10.0.0.1 255.0.0.0
R1(config-if)#no shutdown
R1(config-if)#exit
```

Interface Serial 2/0

```
R1(config)#interface serial 2/0
R1(config-if)#ip address 20.0.0.1 255.0.0.0
R1(config-if)#clock rate 64000
R1(config-if)#encapsulation ppp
R1(config-if)#no shutdown
R1(config-if)#exit
```

In Router 2

Interface Fastethernet 0/0

```
R2(config)#interface fastethernet 0/0
R2(config-if)#ip address 30.0.0.1 255.0.0.0
R2(config-if)#no shutdown
R2(config-if)#exit
```

Interface Serial 2/0

```
R2(config)#interface serial 2/0
R2(config-if)#ip address 20.0.0.2 255.0.0.0
R2(config-if)#encapsulation ppp
R2(config-if)#no shutdown
R2(config-if)#exit
```

Step 3 : Assign ip address for both Pc's with appropriate ip and subnetmask and default gateway

Double Click the PC Icon . Move to config tab and **configure** default gateway

Then Click on FastEthernet and apply ip address and subnetmask

Step 4: Now configure both router with static route

```
R1(config)#ip route Destination Network| Destination N/W SubnetMask |Next Hop Address
```

In [Router](#) R1, Just give this command, In this case Destination is 30.0.0.0 and its subnet mask is 255.0.0.0 next hop address is 20.0.0.2

```
R1(config)#ip route 30.0.0.0 255.0.0.0 20.0.0.2
```

In [Router](#) R2

```
R2(config)#ip route 10.0.0.0 255.0.0.0 20.0.0.1
```

Step 5: Double click PC move to desktop then command prompt give the command ping 30.0.0.10 in PC 0 you will get [reply](#) from 30.0.0.10

Router 0

```
Router>en
```

```
Router#sh runn
```

```
Building configuration...
```

```
Current configuration : 796 bytes
```

```
!
```

```
version 12.2
```

```
no service timestamps log datetime msec
```

```
no service timestamps debug datetime msec
```

```
no service password-encryption
```

```
!
```

```
hostname Router
```

```
!
```



```
!
!  
!  
!  
!  
!  
!  
!  
  
ip cef  
no ipv6 cef  
  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
  
interface FastEthernet0/0  
ip address 192.168.1.1 255.255.255.0  
duplex auto  
speed auto  
!  
  
interface FastEthernet1/0  
no ip address
```

```
interface FastEthernet0/0
ip address 192.168.1.1 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet1/0
no ip address
```

```
duplex auto
speed auto
shutdown
!
interface Serial2/0
ip address 192.168.2.1 255.255.255.0
clock rate 64000
!
interface Serial3/0
no ip address
clock rate 2000000
shutdown
!
interface FastEthernet4/0
no ip address
shutdown
!
interface FastEthernet5/0
no ip address
shutdown
!
ip classless
ip route 192.168.3.0 255.255.255.0 192.168.2.2
!
ip flow-export version 9
!
!
!
!
!
!
!
line con 0
!
```

```
line aux 0
!  
line vty 0 4  
login  
!  
!  
!  
end
```

Router 1

```
Router>en  
Router#sh runn  
Building configuration...  
  
Current configuration : 730 bytes  
!  
version 12.2  
no service timestamps log datetime msec  
no service timestamps debug datetime msec  
no service password-encryption  
!  
hostname Router  
!  
!  
!  
!  
!  
!  
!  
!  
ip cef  
no ipv6 cef  
!
```



```
shutdown
!
interface FastEthernet4/0
no ip address
shutdown
!
interface FastEthernet5/0
no ip address
shutdown
!
ip classless
!
ip flow-export version 9
!
!
!
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
login
!
!
!
end
```