

INTERNATIONAL SCHOOL OF MANAGEMENT & TECHNOLOGY

**ASSIGNMENT COVER SHEET**

|  |  |  |  |
| --- | --- | --- | --- |
| STUDENT DETAILS | | | |
|  | | | |
| Student ID |  | **Reg No.** |  |
| Family Name | Shrestha | **Given Name** | Bisesh |
| Enrolment Year | 2019 | **Section** | N4 |
| Semester | 4th | **Email** | bisesh@ismt.edu.np |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| UNIT DETAILS | | | | |
| Unit Title |  | **Unit Code** | T/615/1639 | |
| Assessor Name | Anil Pande | **Issued Date** | 18 July 2021 | |
| Assignment Title | Network Management | | | |
| Assignment No | **1/1** | **Submission Date** | | 17 September, 2021 |
| Qualification | BTEC HND IN COMPUTING | **Campus** | | **ISMT** |





**STUDENT ASSESSMENT SUBMISSION AND DECLARATION**

When submitting evidence for assessment, each student must sign a declaration confirming that the work is their own.

|  |  |  |  |
| --- | --- | --- | --- |
| Student Name | Bisesh Shrestha | Assessor Name | Anil Pande |
| Issue Date | 18 July 2021 | Submission Date | 17 September, 2021 |
| Programme | Networking | | |
| Unit Name | Network Management | | |
| Assignment Title | Megatech Networking Management Solution | | |

**Plagiarism**

Plagiarism is a particular form of cheating. Plagiarism must be avoided at all costs and students who break the rules, however innocently, may be penalized. It is your responsibility to ensure that you understand correct referencing practices. As a university level student, you are expected to use appropriate references throughout and keep carefully detailed notes of all your sources of materials for material you have used in your work, including any material downloaded from the Internet. Please consult the relevant unit lecturer or your course tutor if you need any further advice.

**Student Declaration**

I certify that the assignment submission is entirely my own work and I fully understand the consequences of plagiarism. I understand that making a false declaration is a form of malpractice.



Pearson Education 2018  
Higher Education Qualifications

Contents

[Part 1: 5](#_Toc94295091)

[Introduction 7](#_Toc94295092)

[Network Management 7](#_Toc94295093)

[Network Management Concepts 7](#_Toc94295094)

[Network Management Principles 8](#_Toc94295095)

[Simple Network Management Protocol 9](#_Toc94295096)

[OSI Model 9](#_Toc94295097)

[TMN Model 9](#_Toc94295098)

[Basic Requirement of Planning on Network Design 10](#_Toc94295099)

[Types of network 10](#_Toc94295100)

[LAN(Local Area Network) 10](#_Toc94295101)

[PAN(Personal Area Network) 11](#_Toc94295102)

[MAN(Metropolitan Area Network) 11](#_Toc94295103)

[WAN(Wide Area Network) 12](#_Toc94295104)

[Network diagram 12](#_Toc94295105)

[Ip adding 13](#_Toc94295106)

[FOR VLAN 14](#_Toc94295107)

[Ping result for vlan 15](#_Toc94295108)

[Hostname for butwal router 16](#_Toc94295109)

[For enable password 16](#_Toc94295110)

[Testing 17](#_Toc94295111)

[For telnet 17](#_Toc94295112)

[From direct password 17](#_Toc94295113)

[From username and password 18](#_Toc94295114)

[For ssh 19](#_Toc94295115)

[Testing 19](#_Toc94295116)

[Normal user 20](#_Toc94295117)

[Testing 20](#_Toc94295118)

[For admin 21](#_Toc94295119)

[Testing 21](#_Toc94295120)

[Privilege for user 22](#_Toc94295121)

[Backup and restore 22](#_Toc94295122)

[Backup 22](#_Toc94295123)

[Restore 23](#_Toc94295124)

[Nm tools for network in design phase. 24](#_Toc94295125)

[TACACS+ 24](#_Toc94295126)

[Nagios XI 24](#_Toc94295127)

[Conclusion: 25](#_Toc94295128)

[Part 2: 25](#_Toc94295129)

[Introduction 26](#_Toc94295130)

[Presentation Slides on Network Protocol and Standards: 26](#_Toc94295131)

[Conclusion 42](#_Toc94295132)

[Part 3 43](#_Toc94295133)

[Introduction 43](#_Toc94295134)

[Tools 43](#_Toc94295135)

[**Nmap** : 43](#_Toc94295136)

[functions 43](#_Toc94295137)

[**Cacti** 44](#_Toc94295138)

[**Nagios** 45](#_Toc94295139)

[Methods 45](#_Toc94295140)

[Security audit: 45](#_Toc94295141)

[Security Compliance: 45](#_Toc94295142)

[Implementing Network Security: 45](#_Toc94295143)

[Network security threats, vulnerabilities and attacks: 46](#_Toc94295144)

[Security Threats: 46](#_Toc94295145)

[Security Vulnerabilities: 46](#_Toc94295146)

[Common Threats: 47](#_Toc94295147)

[Implementing Network security on network: 48](#_Toc94295148)

[Access Control 48](#_Toc94295149)

[Anti-Malware 49](#_Toc94295150)

[Behavioral Analytics 49](#_Toc94295151)

[Application Security 49](#_Toc94295152)

[Data Loss Prevention 49](#_Toc94295153)

[Firewalls 49](#_Toc94295154)

[Email Security 49](#_Toc94295155)

[Mobile and Wireless Security 49](#_Toc94295156)

[Intrusion Detection and Prevention 49](#_Toc94295157)

[Security Information and Event Management (SIEM) 49](#_Toc94295158)

[VPN 49](#_Toc94295159)

[Risk assessment: 49](#_Toc94295160)

[Risk assessment procedure: 50](#_Toc94295161)

[Identify the risks 50](#_Toc94295162)

[Risk Analysis: 51](#_Toc94295163)

[Risk Evaluation: 51](#_Toc94295164)

[Conducting a Risk Assessment on my network: 51](#_Toc94295165)

[Conclusion: 52](#_Toc94295166)

[Bibliography 53](#_Toc94295167)

# Part 1:

**Prepare a report covering the following topics:**

1. Conduct a detailed analysis of **Networking Management principles** and **concepts** covering devices needed to **implement a secure network**, **evaluate** the **importance** of Network Management.
2. **Produce a comprehensive design** of a network according to a given scenario and **Implement** a network design according to a predefined network specification.  
   **NOTE: Provide a comprehensive network configuration by providing screenshots of your work.**

**Report on:**

**Concept, principle of network management and plan, design, setup and configuration of a**

**network**

**Prepared by: Bisesh Shrestha**

# Introduction

This part comprises the important details which are focused on the idea around the Network Security Devices and Protocols where different devices such as Firewall, VPN Concentrator, etc. and protocols such as SSL, IPsec, DNSSEC related to Network Security got to be clarified. And, the examination with respect to the sole purpose and requirements of a secure network as per the situation where we too need to decide equipment and software to be utilized within the network.

# Network Management

In a business environment which employments organized system, there may be faults and performance issues with the network. Network management included utilizing various instruments and advances to oversee these errors. The objective of network management is to free the network from mistakes and make beyond any doubt the organize resources are accessible to correct users.

# Network Management Concepts

To guarantee quick and reliable progress on network management functions, ISO has gathered the management functions into five regions:

1. **Configuration management**

Configuration management means to oversee the arrangements of organize devices, it can be too utilized to gather device data, additionally, it is made up of processes required for network support and operations. Configuration management is both device setup and network arrangement. Devices can be arranged physically or remotely. Protocols such as DHCP and DNS are utilized in network management. Functions of configuration management incudes:

* Maintaining a database of device hardware and software
* Managing device software
* Log containing collection, backup, viewing, archiving, comparison of configured devices
* Detecting changes in hardware, software and configuration
* Change management using configuration change implementation

1. **Fault management**

Fault management is made up of recognizing, separation and the correction of abnormal operations in a network. Fault management can keep network, applications and services running at finest level. Error discovery gives an ability to distinguish faults. Fault management systems are tools made for the purpose of fault management. Its functions include:

* Error logs for maintaining and examine
* Acquire and fix error detection notifications
* Tracing and identification of faults
* Diagnostic tests
* Fixing faults

1. **Accounting management**

Accounting management is a collection of information including data about clients and their network resource usage. As well as the costs to be distinguished for the utilize of the resources. Accounting management incorporates functions such as:

* Informing users of cost relevant to the resources used
* Enable accounting limits to be set and tariff schedules to be linked
* Enable costs to be combined where multiple resources are invoked

1. **Security management**

The purpose of security management is to support the application of security policies by means of functions which include:

* Creation, deletion and control of security services and mechanisms
* Distribution of security-relevant information; and
* Reporting of security-relevant events.

1. **Performance management**

Network performance management is the made up of functions that empower, oversee and guarantee best performance levels of a computer network. Network performance management usually needs the performance and quality benefit level of each organize device and component to be frequently checked. The functions are:

* Gather statistical information
* Maintain and examine logs of system state histories
* Determine system performance under natural and artificial conditions
* Alter system modes of operation for the purpose of conducting performance
* Management activities

# Network Management Principles

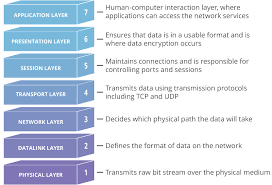
## Simple Network Management Protocol

Simple Network Management Protocol (SNMP) is an application-layer protocol utilized to oversee and screen organize devices and their functions. SNMP gives a common language for organize devices to relay management information inside single- and multivendor environments in a local area network (LAN) or wide area network (Wan). The most recent iteration of SNMP, version 3, includes security improvements that confirm and encrypt SNMP messages as well as ensure packets during transit.

One of the most widely used protocols, SNMP is supported on an extensive range of hardware -- from conventional network equipment like routers, switches and wireless get to focuses to endpoints like printers, scanners and internet of things (IoT) devices. In addition to hardware, SNMP can be utilized to monitor services such as Dynamic Host Configuration Convention (DHCP). Software operators on these devices and services communicate with a network management system (NMS), too referred to as an SNMP manager, through SNMP to relay status data and setup changes.

## OSI Model

The Open Systems Interconnection model (OSI model) is a conceptual model that characterizes and standardizes the communication functions of a telecommunication or computing system without regard to its underlying internal structure and technology.



## TMN Model

The Telecommunications Management Network (TMN) system could be a model characterized by ITU-T for overseeing open systems in a communications network. It is referenced in ITU-T Proposal M.3010. It is imperative to understand that the TMN was created to supply a system for benefit suppliers to oversee their benefit delivery network; in any case, the same fundamental concepts can moreover be connected to standard enterprise systems. This system characterized four administration structures at distinctive levels of abstraction:

1. A functional architecture
2. An information architecture
3. A physical architecture
4. A logical layered architecture

# Basic Requirement of Planning on Network Design

Some of the basic requirements that are needed for successful Network Designs are listed below.

1. A detailed map of network
2. The required cabling structure and layout
3. The number, type, and location of all network devices
4. Complete IP addressing table along with device info
5. Network architecture details and processes

# Types of network

A computer network is a group of computers linked to each other that enables the computer to communicate with another computer and share their resources, data, and applications.

A computer network can be categorized by their size. A computer network is mainly of four types:

* LAN(Local Area Network)
* PAN(Personal Area Network)
* MAN(Metropolitan Area Network)
* WAN(Wide Area Network)

## LAN(Local Area Network)

* Local Area Network is a group of computers connected to each other in a small area such as building, office.
* LAN is used for connecting two or more personal computers through a communication medium such as twisted pair, coaxial cable, etc.
* It is less costly as it is built with inexpensive hardware such as hubs, network adapters, and ethernet cables.
* The data is transferred at an extremely faster rate in Local Area Network.
* Local Area Network provides higher security.



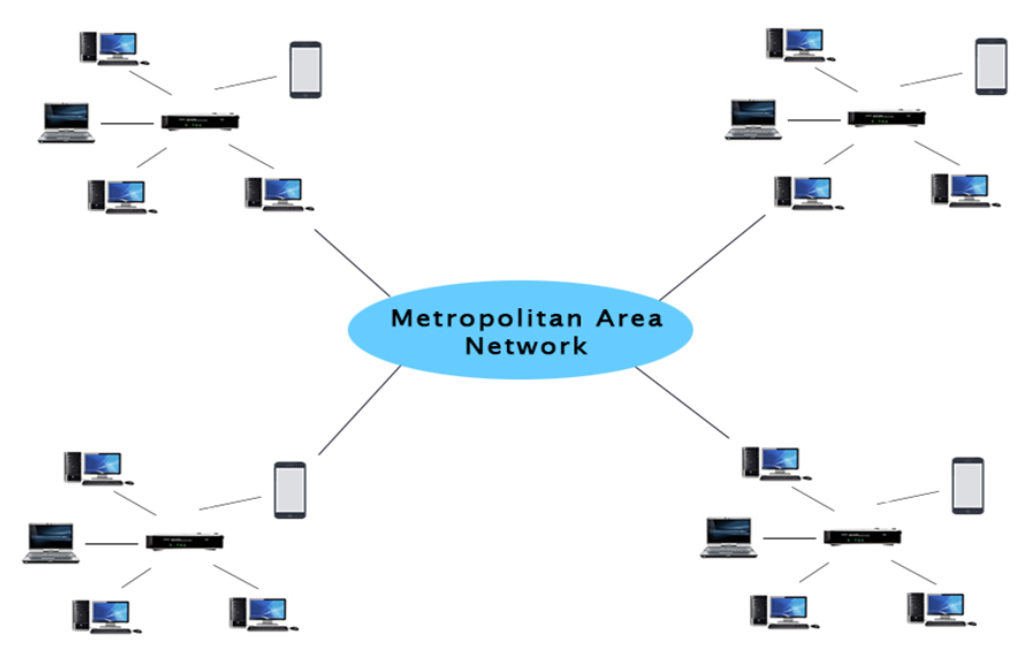
## PAN(Personal Area Network)

* Personal Area Network is a network arranged within an individual person, typically within a range of 10 meters.
* Personal Area Network is used for connecting the computer devices of personal use is known as Personal Area Network.
* Personal Area Network covers an area of 30 feet.
* Personal computer devices that are used to develop the personal area network are the laptop, mobile phones, media player and play stations.



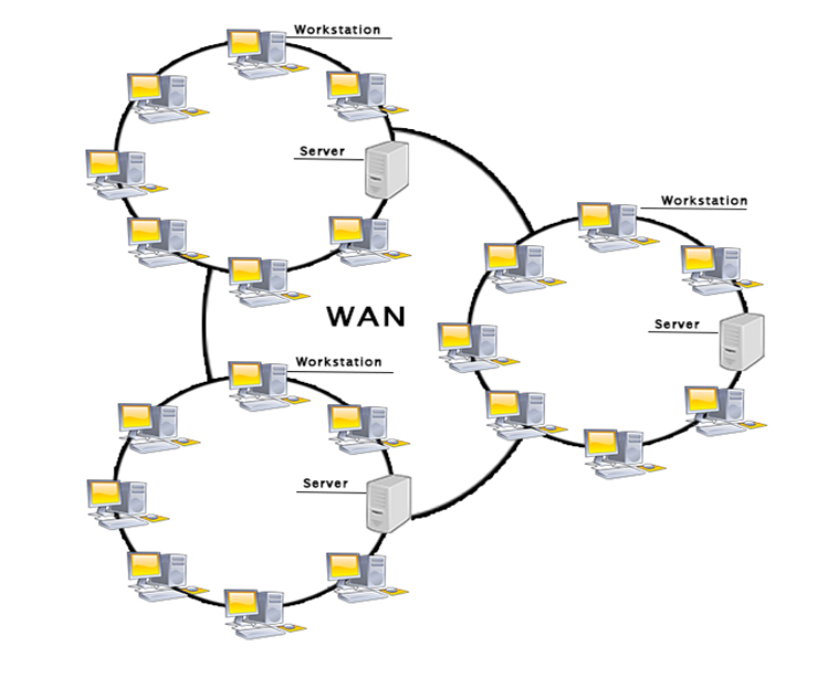
## MAN(Metropolitan Area Network)

* A metropolitan area network is a network that covers a larger geographic area by interconnecting a different LAN to form a larger network.
* Government agencies use MAN to connect to the citizens and private industries.
* In MAN, various LANs are connected to each other through a telephone exchange line.
* The most widely used protocols in MAN are RS-232, Frame Relay, ATM, ISDN, OC-3, ADSL, etc.
* It has a higher range than Local Area Network (LAN).



## WAN(Wide Area Network)

* A Wide Area Network is a network that extends over a large geographical area such as states or countries.
* A Wide Area Network is quite bigger network than the LAN.
* A Wide Area Network is not limited to a single location, but it spans over a large geographical area through a telephone line, fibre optic cable or satellite links.
* The internet is one of the biggest WAN in the world.
* A Wide Area Network is widely used in the field of Business, government, and education.



# Network diagram

“Netmax Technologies” has founded in the year of 2010 is a licensed of Internet Service Provider (ISP) in Nepal. Since the very beginning, focused on providing the fastest and the most stable connectivity to the customers. In a very short period of time, they have witnessed the high scale growth; making us one of the leading ISP of Nepal. This has only been possible due to dedicated team of executives and engineers.

In order to expansion the network, ISP has decided to open a western regional branch office on Butwal. I have recently been employed by “Netmax Technologies” on western region as “Network Administrator” and I have collected and eliciting requirements, planning, designing and implementing fully operational and functional managed network on Butwal.

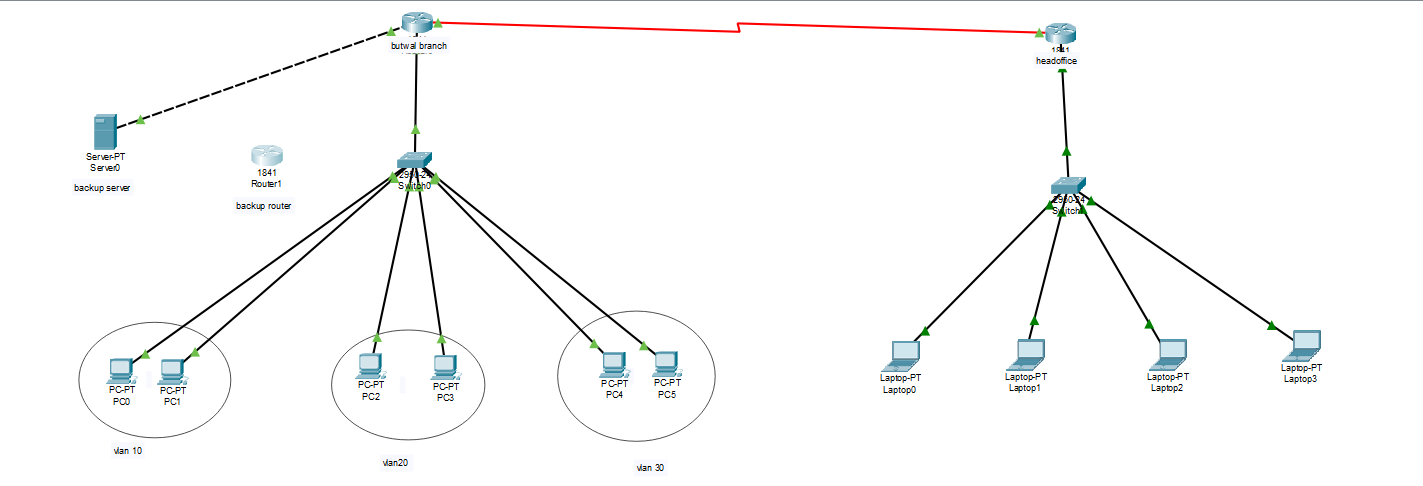
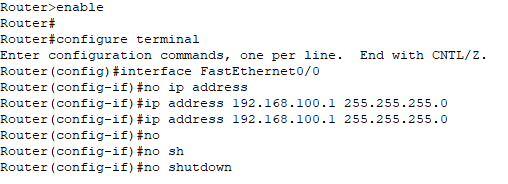


Fig: network diagram

## Ip adding

At first I have to add ip to each and every devices using following steps shown in below:



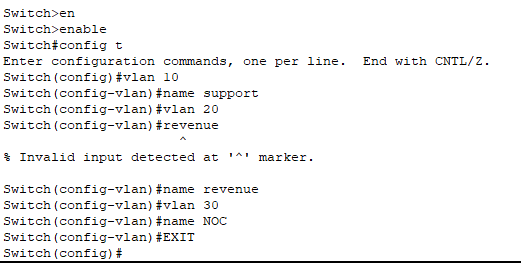
Remaining devices are given ip address as shown in table:

|  |  |  |  |
| --- | --- | --- | --- |
| DEVICES | INTERFACES | IP ADDRESS | SUBNET MASK |
| Head office | Serial0/0/0 | 192.168.2.2 | 255.255.255.0 |
| ROUTER(BUTWAL) | FastEthernet0/0 | 192.168.100.1 | 255.255.255.0 |
| Server | FastEthernet0/1 | 192.168.1.1 | 255.255.255.0 |
| Backup router | FastEthernet0/0 | 192.168.1.10 | 255.255.255.0 |
| Switch | N/A | N/A | N/A |
| PC-PT PC0 | FastEthernet0 | 192.168.100.2 | 255.255.255.0 |
| PC-PT PC1 | FastEthernet0 | 192.168.100.3 | 255.255.255.0 |
| PC-PT PC2 | FastEthernet0 | 192.168.100.4 | 255.255.255.0 |
| PC-PT PC3 | FastEthernet0 | 192.168.100.5 | 255.255.255.0 |
| PC-PT PC4 | FastEthernet0 | 192.168.100.6 | 255.255.255.0 |
| PC-PT PC5 | FastEthernet0 | 192.168.100.7 | 255.255.255.0 |

And then i have added vlan for those computer so that they cannot have access to another department.

## FOR VLAN

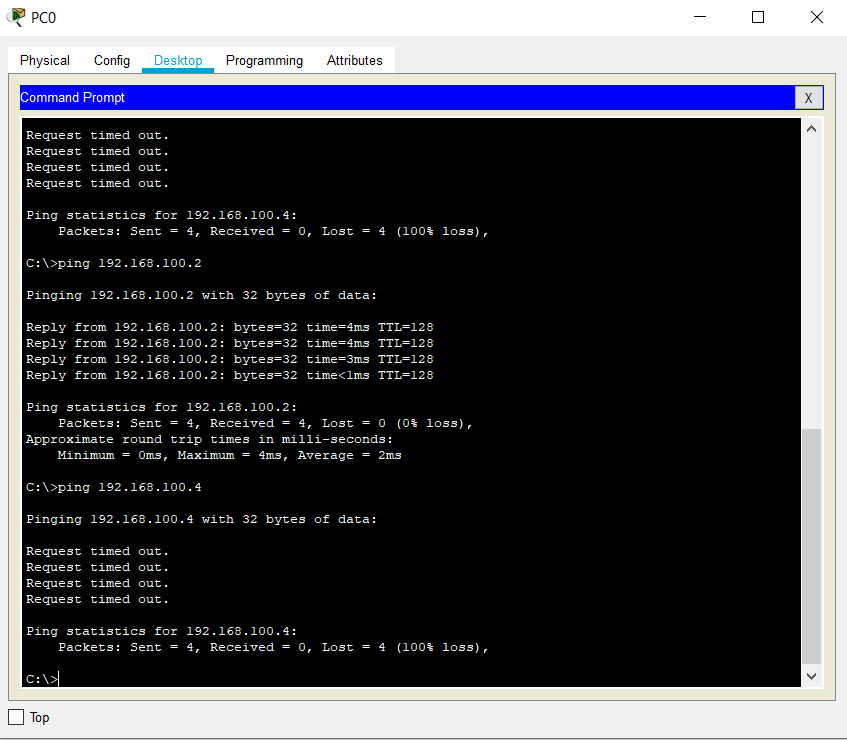
For vlan, I have used command as shown below:



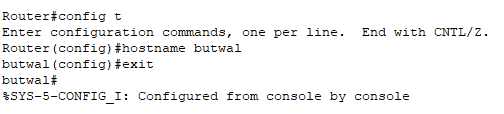
For vlan configuration



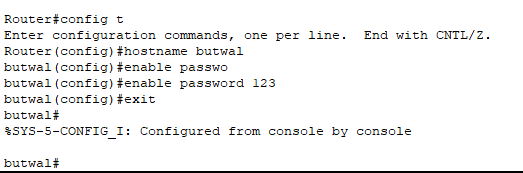
### Ping result for vlan



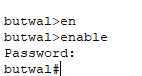
## Hostname for butwal router



## For enable password

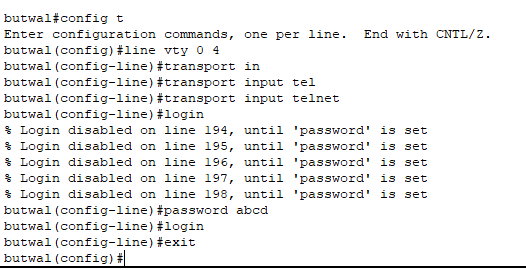


### Testing

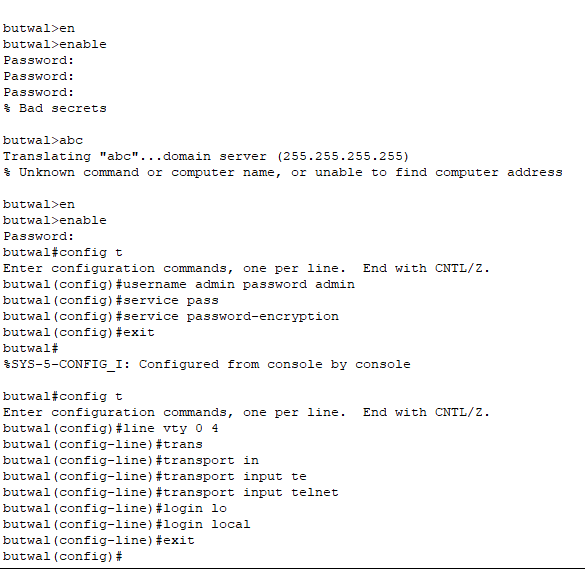


## For telnet

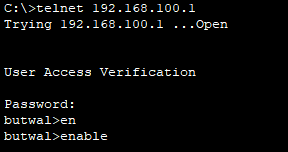
### From direct password

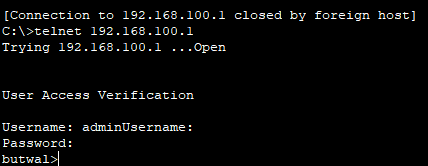


### From username and password

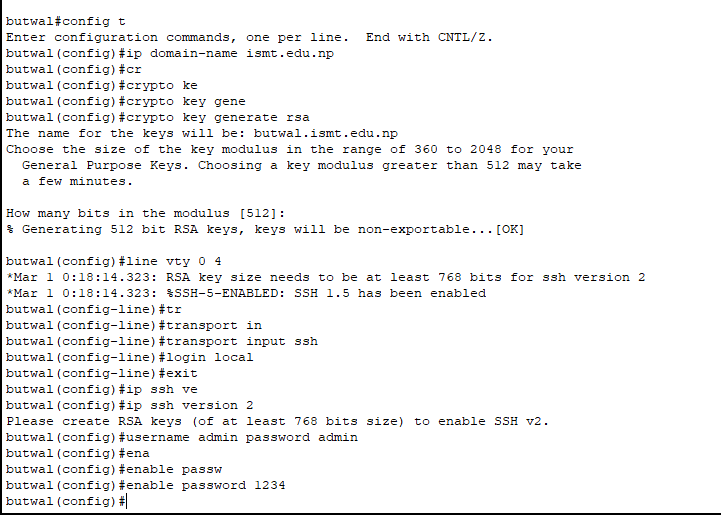


#### Testing of telnet

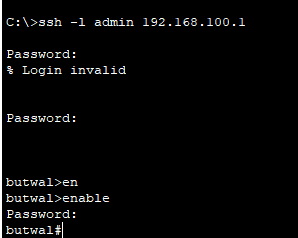




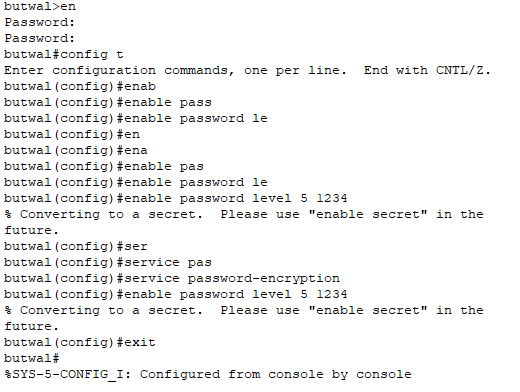
## For ssh



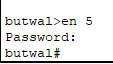
### Testing



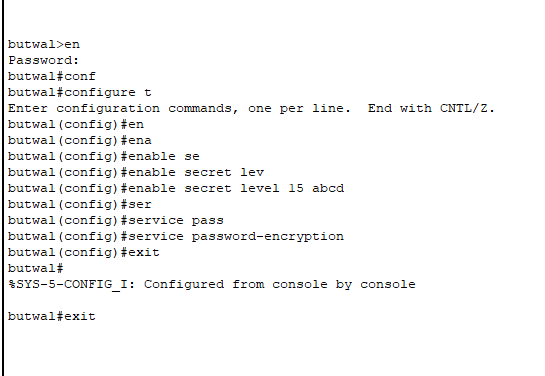
## Normal user



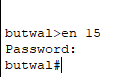
### Testing



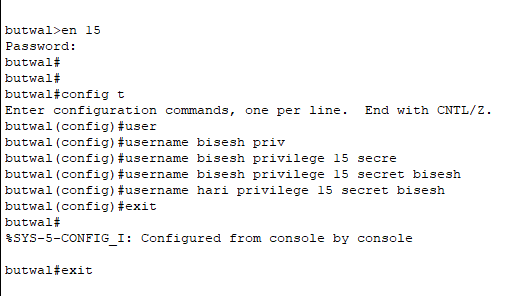
## For admin



### Testing

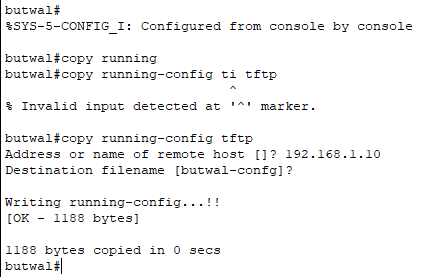


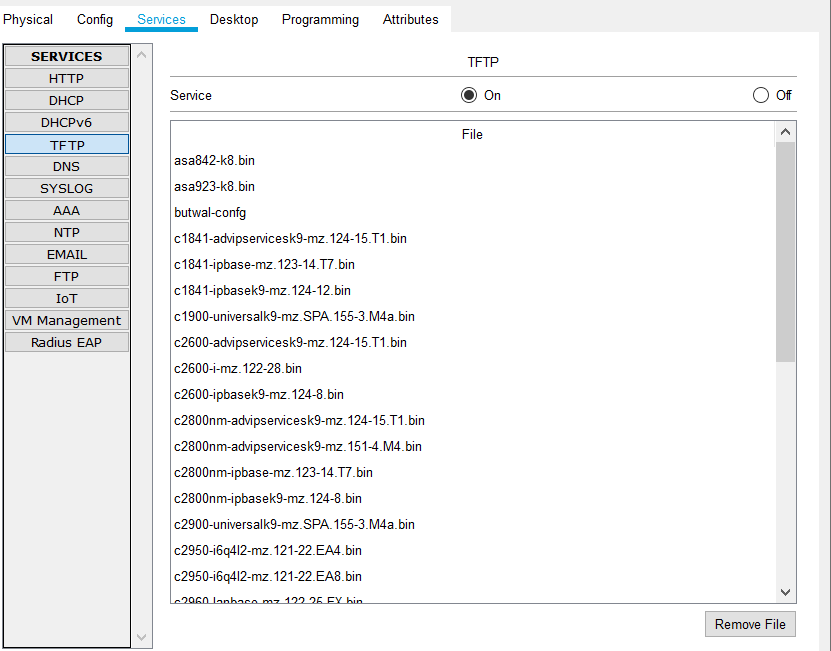
## Privilege for user



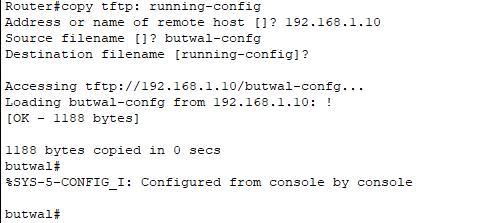
# Backup and restore

## Backup





## Restore



## Nm tools for network in design phase.

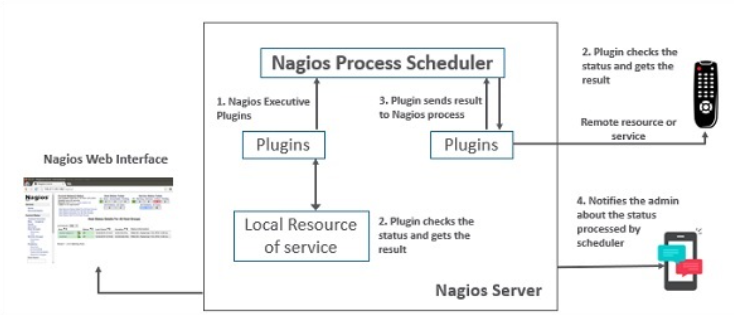
## TACACS+

TACACS+ (Terminal Access Control Server) is based on the UNIX client-server architecture, in which the client first asks the server for authentication, which the server either accepts or denies. The default port for Tacacs+ is 49 because it utilizes TCP as its transport protocol. The client is always the device seeking to connect to the server in order to obtain access to another device. As a result, it is also a more dependable transmission protocol. TACACS+ is a TCP-based access control protocol that lets a device communicate a user's login and password to an authentication server to see if access is granted. TACACS+ provides authorization and accounting functions in addition to authentication. TACACS+'s primary objective is to offer a centralized database against which authentication may be performed; but, as mentioned earlier, it also enables AAA. The server keeps track of authentication credentials (usernames and passwords), makes authorization decisions, and keeps track of accounting information. Client devices must employ a protocol to connect with servers in order to access their AAA services. For AAA, TACACSGUI is used, which is based on the previously stated TACACS+ daemon. With the AAA features, this tool can do a number of tasks, including LDAP, Open LDAP, One-Time Password, Local Database, and SMS authentication, as well as multi-vendor interoperability, which allows many other vendors to interact with Cisco.



## Nagios XI

Nagios XI is a good monitoring engine that makes use of the Nagios Core 4 monitoring engine to enable scalable and effective monitoring. The web interface's configuration wizard makes adding network devices to this utility straightforward. The dashboard, which offers an overview of hosts, services, and network devices, and Nagios' advanced graphs, which provide a concise summary of network issues and help in their resolution before significant disasters occur, make up the system. The main benefit of using Nagios is that it uses four status states to describe status: OK, WARNING, CRITICAL, and UNKNOWN, which allows for faster action when a problem arises because this status directs the alert to the specified person rather than the monitoring value or graph, which is ignored when it requires immediate attention. It also gives you a report on the state of numerous services, both critical and non-critical, as well as network device status.



The following diagram depicts the Nagios Architecture, which is built on a server/client approach.

A Nagios Server operating on a host, as well as server-side plug-ins, make up the architecture, and all of these components must be monitored. The plug-ins collect data from monitored components, transfer it to the server, and show it on the GUI. Here are the three primary Nagios categories:

Plug-ins: The user configures the plug-ins, which check a service and return a result to the Nagios server, allowing it to take appropriate actions.

Scheduler: It is a component of the Nagios Server-side that checks plug-ins at regular intervals and takes action based on the plug-ins.

GUI: The web interface part of the Nagios server which displays webpage generated by the Common Gateway Interface (CGI). With the help of GUI, all the configuration, state, alerts, and

MRTG graphs can be displayed.

This tool comprises various other features but for the project, the network devices monitoring is the major entity where we monitor the Port Status, Port Bandwidth and also, CPU Usage. For the design, SNMPv2 is enabled in all the three network devices and the routers are manually added in the Nagios XI server.

# Conclusion:

In this part, I have explained and examined about the analysis of network management principles and concepts as well as the devices required for implementing a secure network. I have evaluated the importance of the network management. Similarly, I have created a comprehensive network design based on a given scenario and implemented a network design based on a predefined network specification with comprehensive network configuration by providing screenshots.

# Part 2:

Produce a **Presentation** which **justifies** the Protocols and Standards concerned with Networking and Network Management. Your Presentation should cover at least following topics:

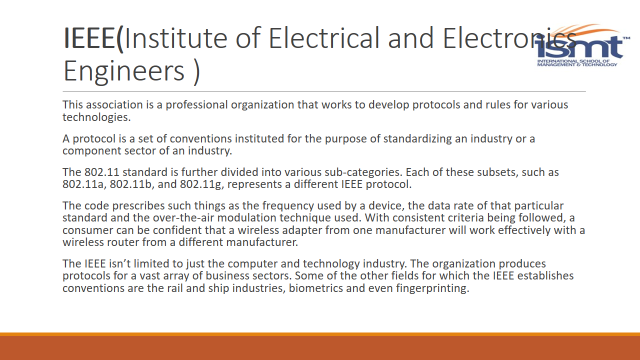
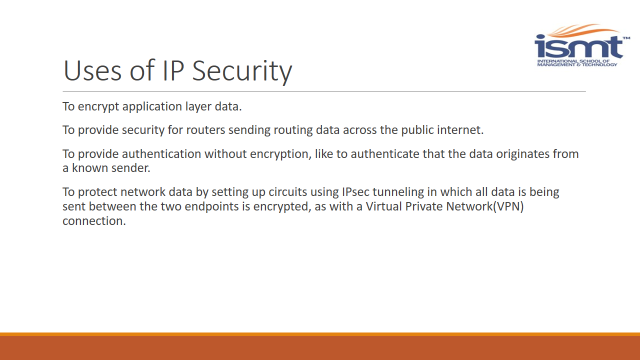
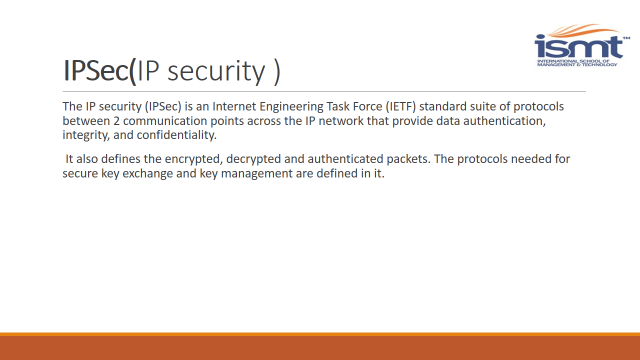
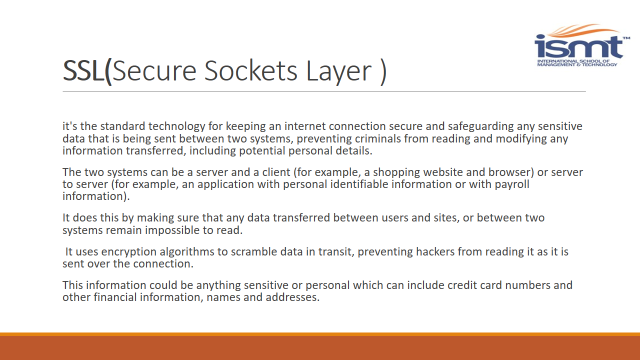
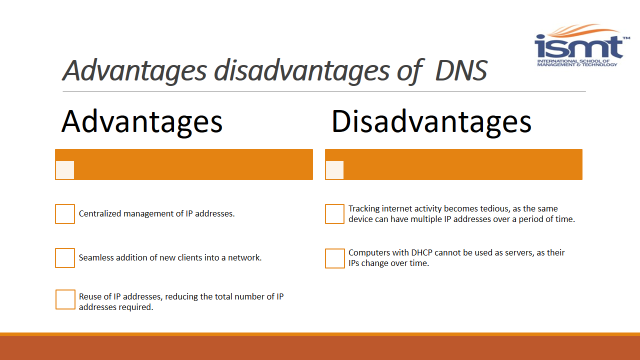
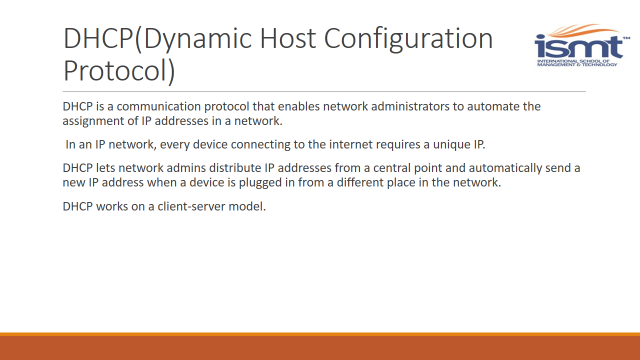
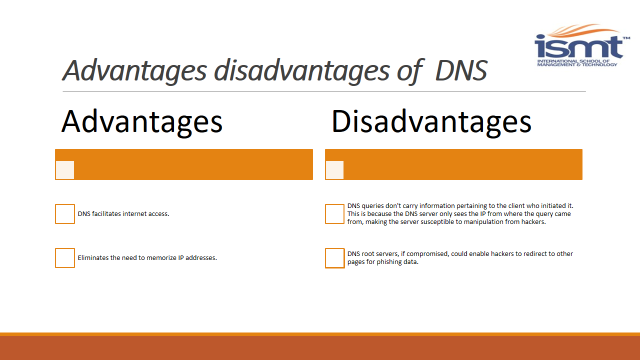
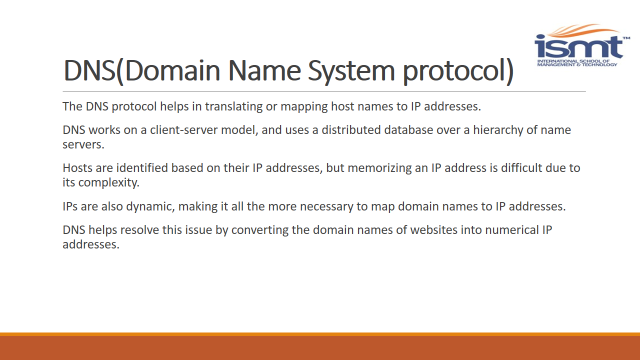
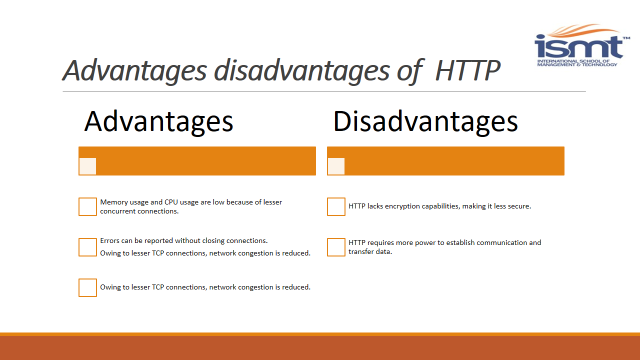
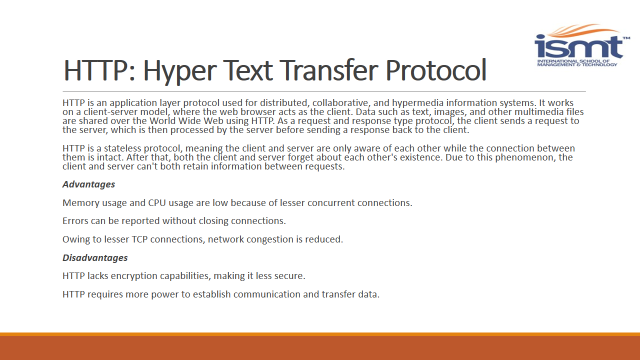
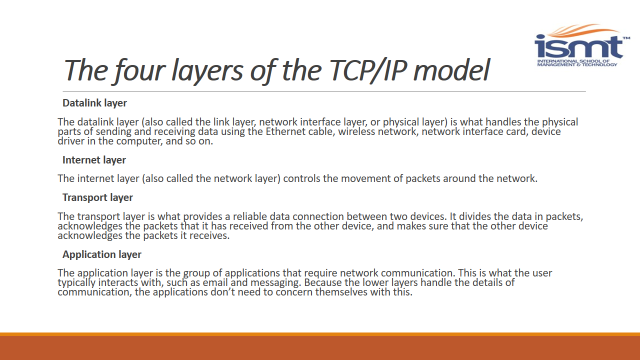
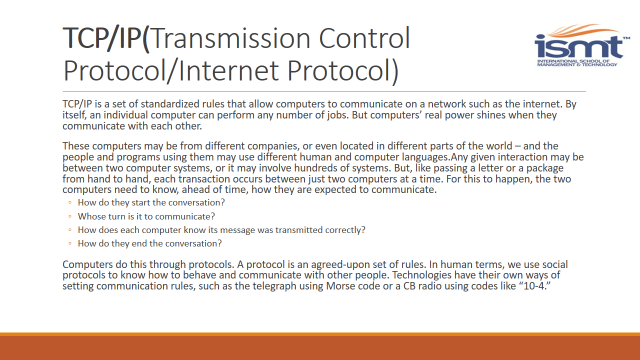
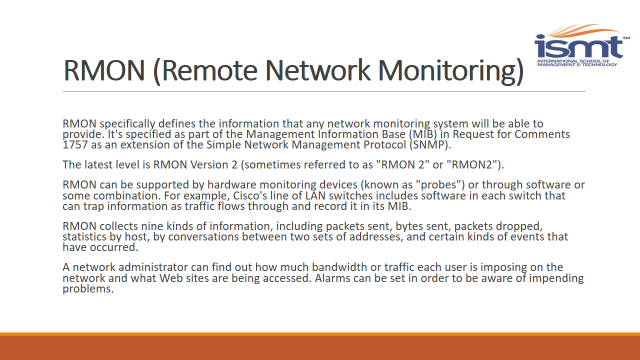
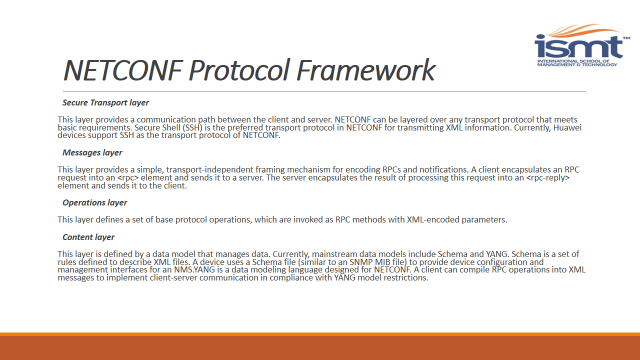
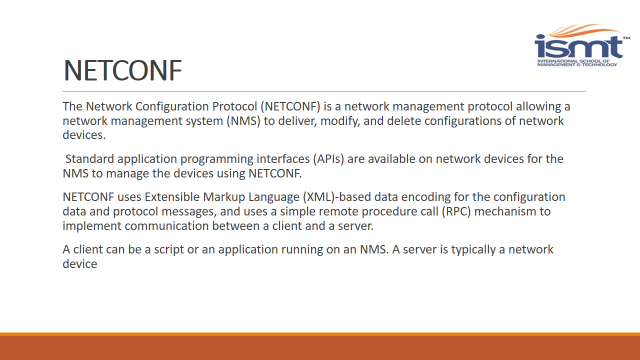
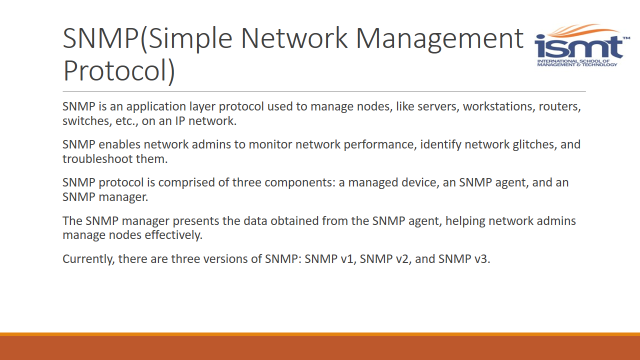
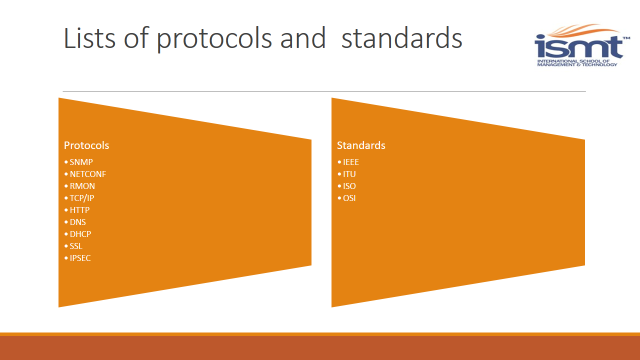
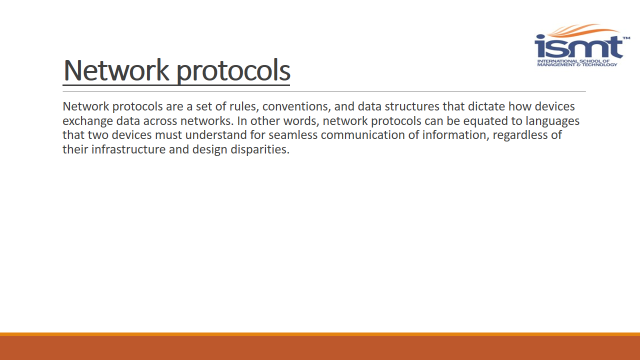
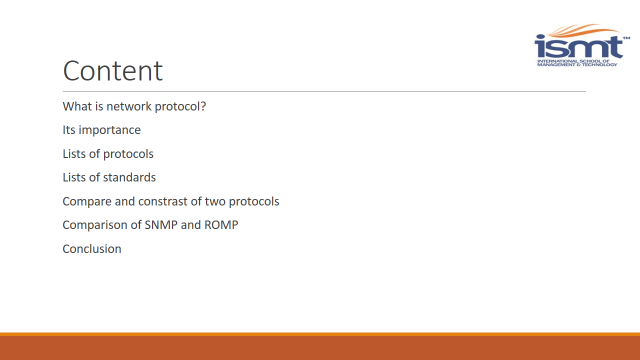
1. **Evaluate** the following Network **Protocols** and **Standards**: SNMP, NETCONF, RMON, TCP/IP, HTTP, DNS, DHCP, SSL, IPSec, IEEE, ITU, ISO, OSI including IANA and ICANN.
2. **Compare and contrast two Protocols**. Also, Compare and contrast SNMP and RMON.

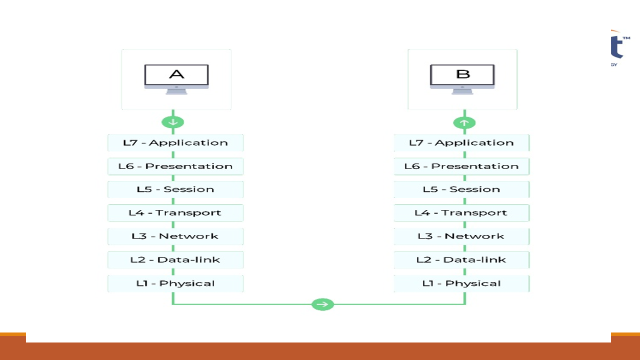
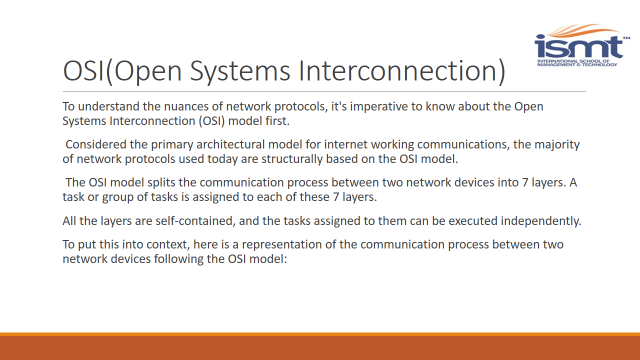
# Introduction

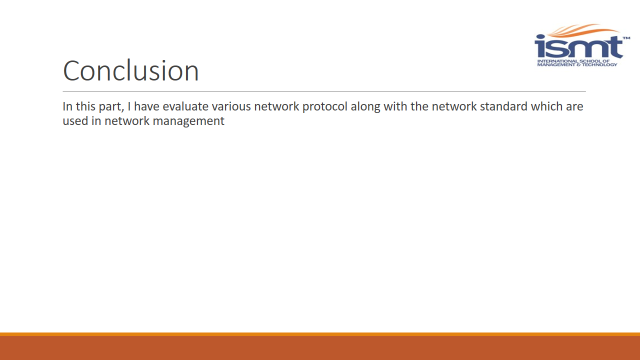
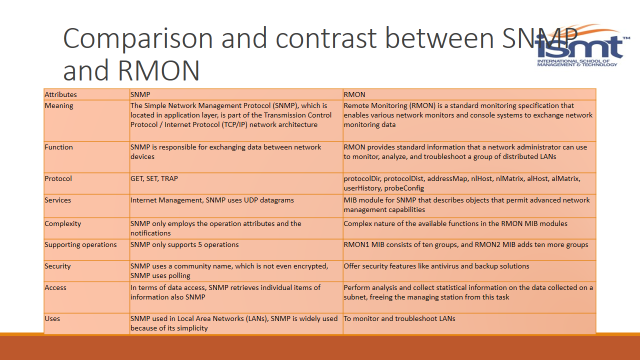
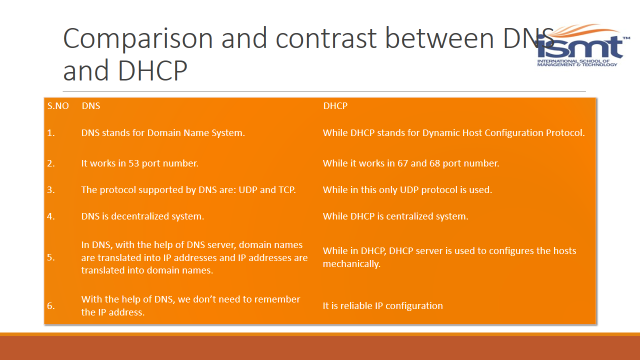
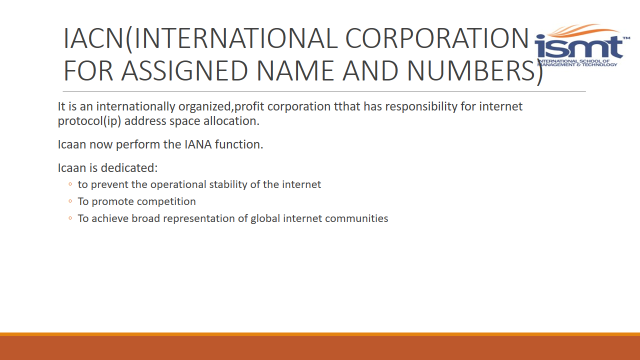
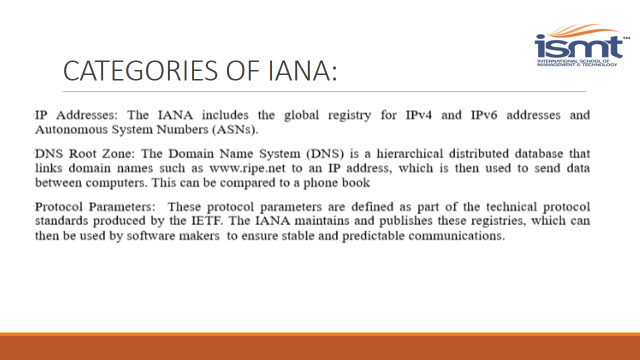
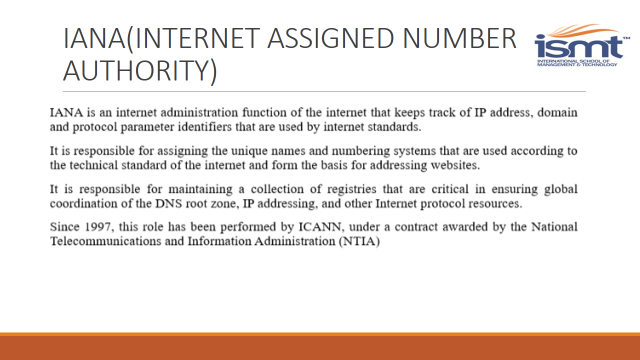
In this part, I am preparing the presentation on the network protocols and standards. In the presentation, I am including various protocols and standards such as SNMP, NETCONF, RMON,TCP/IP, HTTP, DNS, DHCP, SSL, IPsec, IEEE, ITU, ISO, OSI, IANA and ICANN with its features and application. Similarly, I am comparing and contrasting any two protocol and finally, I will compare and contrast between SNMP and RMON.

## Presentation Slides on Network Protocol and Standards:









Conclusion:

In this part, I have evaluated the Network Protocols and Standards such as SNMP, NETCONF,RMON, TCP/IP, HTTP, DNS, DHCP, SSL, IEEE, ITU, ISO, OSI, IANA, ICANN with its Features and its applications. Similarly, I have compared and contrast two protocol which are HTTP and HTTPs and lastly compared and contrast between SNMP and RMON.

# Part 3

Use **tools and methods** to manage a network, including Network Security and Risk Management.

1. **Use tools and methods** to manage a network and **Implement** network security on your Network. Also, **Conduct a Risk Assessment** on your network.

# Introduction

In this part, I am going to discuss about the different tools and methods that I have utilize in the network for appropriate network management. In arrange to oversee and monitor the network, I have implemented following network management tools such as SNMP, Syslog server, ACL and so on. Likewise, I’ll be implementing network security arrange to secure organize from various vulnerabilities. i am talking about approximately the hazard evaluation based on ISO 31000. Concurring to ISO 31000, Risk evaluation is the generally process of risk identification, risk analysis and risk evaluation. i will be conducting a hazard evaluation on our network with defending the significance of the network security within the network. In conclusion, I’ll be evaluating the significance of carrying-out a risk assessment on the network.

**Tools and Methods used to manage network:**

A network monitoring tool enables to:

* Auto discover devices connected to network.
* View live and historic performance data for a range of devices and applications.
* Configure alerts to notify of unusual activity.
* Generate graphs and reports to analyze network activity in greater depth.

# Tools

## **Nmap** :

Nmap ("Network Mapper") is a free and open source (license) utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. It was designed to rapidly scan large networks, but works fine against single hosts. Nmap runs on all major computer operating systems, and official binary packages are available for Linux, Windows, and Mac OS X. In addition to the classic command-line Nmap executable, the Nmap suite includes an advanced GUI and results viewer (Zenmap), a flexible data transfer, redirection, and debugging tool (Ncat), a utility for comparing scan results (Ndiff), and a packet generation and response analysis tool (Nping).

### functions

**Flexible**: Supports dozens of advanced techniques for mapping out networks filled with IP filters, firewalls, routers, and other obstacles. This includes many port scanning mechanisms (both TCP & UDP), OS detection, version detection, ping sweeps, and more. See the documentation page.

**Powerful**: Nmap has been used to scan huge networks of literally hundreds of thousands of machines.

**Portable**: Most operating systems are supported, including Linux, Microsoft Windows, FreeBSD, OpenBSD, Solaris, IRIX, Mac OS X, HP-UX, NetBSD, Sun OS, Amiga, and more.

**Easy**: While Nmap offers a rich set of advanced features for power users, you can start out as simply as "nmap -v -A targethost". Both traditional command line and graphical (GUI) versions are available to suit your preference. Binaries are available for those who do not wish to compile Nmap from source.

**Free**: The primary goals of the Nmap Project is to help make the Internet a little more secure and to provide administrators/auditors/hackers with an advanced tool for exploring their networks. Nmap is available for free download, and also comes with full source code that you may modify and redistribute under the terms of the license.

**Well** **Documented**: Significant effort has been put into comprehensive and up-to-date man pages, whitepapers, tutorials, and even a whole book! Find them in multiple languages here.

**Supported**: While Nmap comes with no warranty, it is well supported by a vibrant community of developers and users. Most of this interaction occurs on the Nmap mailing lists. Most bug reports and questions should be sent to the nmap-dev list, but only after you read the guidelines. We recommend that all users subscribe to the low-traffic Nmap-hackers announcement list. You can also find Nmap on Facebook and Twitter. For real-time chat, join the #Nmap channel on Freenode or EFNet.

**Acclaimed**: Nmap has won numerous awards, including "Information Security Product of the Year" by Linux Journal, Info World and Codetalker Digest. It has been featured in hundreds of magazine articles, several movies, dozens of books, and one comic book series. Visit the press page for further details.

**Popular**: Thousands of people download Nmap every day, and it is included with many operating systems (Redhat Linux, Debian Linux, Gentoo, FreeBSD, OpenBSD, etc). It is among the top ten (out of 30,000) programs at the Freshmeat.Net repository. This is important because it lends Nmap its vibrant development and user support communities.

## **Cacti**

It is a graphing solution that acts as an addition to RRD Tool and is used by many network administrators to collect performance data in LANs. Cacti comes with Simple Network Management Protocol (SNMP) support on Windows and Linux to create graphs of traffic data. Cacti typically works by using data sourced from user-created scripts that ping hosts on a network. The values returned by the scripts are stored in a MySQL database, and this data is used to generate graphs. This sounds complicated, but Cacti has templates to help speed the process along. We can also create a graph or data source template that can be used for future monitoring activity.

Below is a list of the components that comprise the Cacti monitoring system:

* Apache HTTP Server: A web server responsible for accepting HTTP requests.
* MySQL database: Multi-Threaded, Multi-user, SQL database management system.
* RRDTool: Round Robin Database - RRD is a system to store and display time-series
* Data like network traffic, temperatures, etc.
* php scripting: PHP is a widely-used general-purpose scripting language that is
* Suited, e.g., for Web development. PHP can be embedded into HTML.
* Perl Scripting: Perl is a high-level programming language that is stable and is a
* Cross- platform programming language.
* Cacti Monitoring Tool: Cacti is a complete network graphing solution
* designed to harness the power of RRD Tool&#39;s data storage and graphing
* Functionality.
* Cacti Plug-In Architecture: This provides the ability to add features to Cacti.
* Cacti Thresholding Plug In: This enables the ability to send e-mails based on
* Preset thresholds.

## **Nagios**

Nagios monitors your entire IT infrastructure to ensure systems, applications, services, and business processes are functioning properly. In the event of a failure, Nagios can alert technical staff of the problem, allowing them to begin remediation processes before outages affect business processes, end-users, or customers. With Nagios you’ll never be left having to explain why an unseen infrastructure outage hurt your organization’s bottom line.

Methods:

### Security audit:

The method of evaluation of the security system in arrange to confirm the systems secure operation and helps for the superior execution of the software. Security audits will help within the security of sensitive data, distinguishing proof of security escape clauses, make unused security arrangements and screen the effectiveness of security methodologies. These reviews are one of three primary sorts of security diagnostics, along with vulnerability evaluations and penetration testing. Security audits degree the execution of an information systems against a set of criteria. A helplessness evaluation may be a comprehensive study of a data system, looking for potential security vulnerabilities. Penetration testing may be a covert method in which a security master test to confirm in the event that a system can withstand a particular assault. It incorporates analyzing and distinguishing the current issues, as well as performs the essential steps to resolve the situation.

### Security Compliance:

Security compliance is both legal and operational concerns for the organization. The value of information resources has expanded essentially as a result of expanded dependence on information technology (IT), and keeping up repeatable, standardized operations requires a solid control compliance system. IT is essentially capable for giving a stage for conducting business. As a result, risk management for data resources by means of security controls has ended up a major issue. Security compliance makes a difference to maintain a strategic distance from fines and punishments, ensure trade notoriety, and improve data management capabilities, support access control and responsibility.

### Implementing Network Security:

When we talk about security, the primary step is that how we characterize network security. network security is the assurance of systems, their applications or administrations against unauthorized get to that prevents form modification, disclosure or destruction of information. It too guarantees that the network is performing correctly with no harmful side impacts. This is as a matter of fact, a really wide definition, but a general definition superior plans network administrators to bargain with unused sorts of attacks. Each organization characterizes its own security approach that describes the level of access, which is permitted or denied. So it is vital for any organization to form such a security mechanism that's wide in scope and makes a difference to deal with unused sorts of attack.

# Network security threats, vulnerabilities and attacks:

## Security Threats:

When talking about threat it can be any person or event that can cause the damage of data or network. Threats can also be natural for example wind, lightning, flooding or can be accidental, such as accidentally deletion of file.

## Security Vulnerabilities:

Vulnerabilities defined as the weakness in any organize that can be exploited by a threat. Recently nearly in all regions network technologies have been connected, such as banking, tax, E-Commerce. These applications are comprising of different network devices and computers and it is exceptionally vital to secure these applications and gadgets from malicious hackers so that chances to misuse the vulnerabilities may decrease. There are different hardware and software tools accessible within the advertise to ensure against these attacks, such as firewalls, Intrusion Detection Systems (IDS), antivirus software and vulnerability scanning software.

The impact of these threats and vulnerabilities points to the problems that result in disclosure, modification or denial of service. Below are some common threats to a network:

* **Unauthorized Access:**
  + Use strong passwords, contains at least 10 characters, contains at least one alpha, one numeric and one special character and use passwords that cannot contain dictionary words.
  + Use hardware and software firewall.
  + Use protection software against Trojan, spyware, viruses and other malwares.
  + Carefully handle emails, usually viruses, spyware and other malware are distributed through emails that have an e-mail attachment
* **Inappropriate Access of resources**: Unauthorized access occurs when a user tries to access are source that is not permitted for it. This may occur because administrators not properly assigned the resources. It may also occur when privileges are not enough for a user. Company which have different departments and users, some users have inappropriate access to any network resources, mostly because the users are not from the same department or may be such users who are from outside the company. For example, access to the accounts department data is inappropriate by the administrators for the users which belong to some other department. In this case, administrators need to grant more access rights than a user needed.
* **Disclosure of Data**: In any organization, some information, which is either stored in a computer in the network or transmitted, may require some level of confidentiality. Illegal access occurs when someone who is not authorized for that tries to read the data. It mostly happens because our information is not encrypted. There are different encryption schemes that are used today; we will discuss them in detail in next chapters.
* **Unauthorized Modification**: Unauthorized modification of data is attack on data integrity. Any changing in data or software can create big problems; possibly can corrupt databases, spreadsheets or some other important applications. Any miner-unauthorized change in software can damage the whole operating system or all applications, which are related to that software and perhaps need to reinstall the software with all related applications. Unauthorized as well as authorized users can make this. Any change in the data or in application can divert the information to some other destinations. Any outsider or hacker who can make some changes and again send to the destination can use this information.

# Common Threats:

The need for you to guard your business against cyber-attacks has never been more crucial as network security risks are continually on the rise. In any case of whether your company’s data and information are put away on a difficult drive or sent through e-mails, being attentive of network security dangers, knowing how to avoid them, and contracting a managed IT security supplier can assist you ease any possible information breaches.

**Most Common Network Security Risks**

Here are some five most common network security threats:

* 1. Phishing

This type of online fraud is planned to take sensitive data, such as credit card numbers and passwords. Phishing attacks imitate trustworthy banking institutions, websites, and individual contacts, which come within the shape of quick phishing e-mails or messages designed to see legitimate. Once you tap the URL or reply to the messages, you're provoked to enter your money related details or utilize your credentials, which at that point sends your information to the malicious source.

* 1. Computer Viruses

These are pieces of software planned to spread from one computer device to another. Generally they are downloaded from specific websites or sent as email connections with the expectation of infecting your computer as well as other computers on your contact list through systems on your network. They can disable your security settings, send spam, take and degenerate information from your computer, and indeed erase each single thing on your difficult drive.

* 1. Malware/Ransom ware

Malware is a malicious software mostly used by criminals to hold your system, steal your confidential data, or install damaging programs in your device without your knowledge. It spreads spyware, Trojans, and worms through pop-up ads, infected files, bogus websites, or e-mail messages.

On the other hand, ransomware is a type of malware where the cyber-criminals lock your device through a bad app or phishing e-mails then request a ransom to unlock the device. It can hinder you from running applications, encrypting your files, and even from completely using your device.

* 1. Rogue Security Software

This is malicious software that deceives users by making them believe that their security measures are not up-to-the-minute or their computer has a virus. They then offer to help you install or update the user’s security settings by asking you to pay for a tool or download their program to help do away with the alleged viruses. This can lead to the installation of actual malware in your device.

* 1. Denial-Of-Service Attack

A denial-of-service attempts to hinder legitimate users from accessing services or information from a website. It happens when malicious attackers overload a website with traffic. It is carried out by one computer and its internet connection, which may enable the intruder to access your credentials. A distributed denial-of-service is similar to the denial-of-service but is harder to overcome. This is because it is launched from different computers that are distributed all over the globe. The network from these compromised computers is called a botnet.

# Implementing Network security on network:

No network is safe in an environment where hackers continuously find ways to exploit the system. A threat can cause problems at any moment. A foolproof network security system will ensure these problems won’t occur.

Here are some of the must-have network security tools that help you protect your internal systems from intrusions.

## Access Control

Access control in network security allows you to improve defense by limiting user access and resources to certain parts of the network for which they are responsible.

## Anti-Malware

Anti-malware is one of the security essentials that identifies viruses, worms, Trojans, etc., and prevents them from infecting the network.

## Behavioral Analytics

Security personnel establish guidelines for what is considered as normal behavior for customers as well as users. Behavioral analytics software keeps an eye on any suspected activity to identify abnormal behavior.

## Application Security

Application security helps establish security guidelines for applications that are relevant to network security. This process blocks any suspicious application from entering the system as well as for closing gaps in security coverage.

## Data Loss Prevention

Humans are considered the weakest security link. Data loss prevention (DLP) technologies protect staff and anyone who uses the network from misusing and possibly compromising sensitive data.

## Firewalls

Firewalls are an important part of the network security system as they act as a barrier between the network trusted zone and everything beyond it.

## Email Security

Phishing allows intruders to access an insecure network illegally. Email security blocks phishing attempts and outbound messages carrying sensitive data.

## Mobile and Wireless Security

Mobile and wireless devices are vulnerable to possible network breaches and therefore require extra scrutiny.

## Intrusion Detection and Prevention

Intrusion detection and prevention systems AKA intrusion detection system analyze network traffic/packets to identify different types of attacks and respond quickly. Intrusion detection systems create a database of known attack methods to identify patterns and thwart any similar incidents in the future.

## Security Information and Event Management (SIEM)

SIEM collects data from various network tools. This information helps in identifying and responding to threats accordingly.

## VPN

A virtual private network authenticates safer communication between a network and a device.

# Risk assessment:

Risk assessment is a term that is utilized to describe the overall prepare or strategy where we identify hazards and risk factors that have the potential to cause harm, analyze and evaluate the risk associated with that risk (hazard investigation and risk evaluation), decide appropriate ways to dispose of the hazard or control the chance when the risk can’t be eliminated (Risk Assessment: OSH Answers, n.d.). A risk assessment is the examination process that's utilized to recognize circumstances, processes, and other factor within the organization that will harm to the individuals. After we have made the identification, we will got to analyze and assess the chance. At that point we have to be have the assurance for the elimination of the risk. Moreover, we choose to take measure step to successfully eliminate or control the harm.

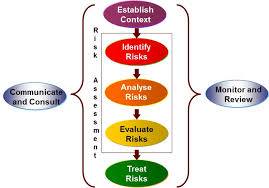
Here are some of the importance of risk assessment:

* Create awareness of hazards and risk.
* Identify who may be at risk (e.g., employees, cleaners, visitors, contractors, the public, etc.).
* Determine whether a control program is required for a particular hazard.
* Determine if existing control measures are adequate or if more should be done.
* Prevent injuries or illnesses, especially when done at the design or planning stage.
* Prioritize hazards and control measures.
* Meet legal requirement where applicable.

# Risk assessment procedure:

According to ISO 31000, Risk assessment is the overall process of risk identification, risk analysis

and risk evaluation.



## Identify the risks

The first step to creating your risk assessment plan is determining what hazards your employees and your business face, including:

* Natural disasters (flooding, tornadoes, hurricanes, earthquakes, fire, etc.)
* Biological hazards (pandemic diseases, foodborne illnesses, etc.)
* Workplace accidents (slips and trips, transportation accidents, structural failure, mechanical breakdowns, etc.)
* Intentional acts (labor strikes, demonstrations, bomb threats, robbery, arson, etc.)
* Technological hazards (lost Internet connection, power outage, etc.)
* Chemical hazards (asbestos, cleaning fluids, etc.)
* Mental hazards (excess workload, bullying, etc.)
* Interruptions in the supply chain

# Risk Analysis:

Risk analysis is the process of creating an understanding of the risk. Risk analysis is utilized to help evaluate dangers and make decision about whether dangers ought to be treated as well as the foremost appropriate risk treatment methodologies and strategies. Risk analysis considers the cause and sources of risk, as well as the positive and negative results of those dangers and probability that those results can occur. Risk is analyzed by deciding results and their probability, and other attributes of the risk. Hazard examination can be embraced with shifting degrees of detail, depending on the risk, the purpose of the analysis, and the data, information and resources available. Analysis can be qualitative, semi-quantitative or quantitative, or a combination of these, depending on the circumstances

## Risk Evaluation:

Risk evaluation involves comparing the level of risk found during the analysis process with risk criteria established when the context was considered. The need for treatment can be determined based on this comparison. The goal of risk evaluation is to help in making decisions, based on the outcomes of risk analysis, about which risks need to be treatment and the priority for treatment implementation (Risk Evaluation, 2009, p. 18). In some circumstances, the risk evaluation can lead to a decision to conduct further analysis. The risk evaluation can also lead to a decision not to treat the risk in any-way other than maintaining existing controls. This decision will be influenced by the organization risk attitude and the risk criteria that have been established. The result of the risk evaluation should be recorded, communicated and then validated at the appropriate organizational levels.

# Conducting a Risk Assessment on my network:

I have used ISO 31000 risk management methodology to conduct the risk assessment, which are given below:

Worldwide Organization for the standardization released any updated on the risk management methodologies. It can be applied to attain any sort of objective at any organizational level and in any area. It helps in decision-making and can be connected to any sorts of exercises. Risk management is a part of governance and authority, and it is basic to how an organization is managed at all levels, according to the Universal Organization for Standardization. The risk assessment methodologies include deciding whether or not a risk management procedure is effective. It makes a difference to create the strategy that empowers the creation, security of the value and as well as helps to achieve the success and goals whereas minimizing dangers and threats.

These methods or strategies includes the improvement of exercises in arrange to avoid risk and achieve absolute output. It empowers involvement of areas and work of all the activities. This approach moreover energizes partner support and the utilize of dependable data and information. Another risk management strategy or method is to decide whether or not the risk management methods and approaches are energetic or relevant. It is profitable to be able of managing changes in risk or changing expectations. This method moreover incorporates an approach that promotes organizational improvement on a continuous basis.

The methods also include determining whether or not the risk management strategy is customized. This method includes the organization or the company accommodates the human and the cultural factors, it also addresses the respond to the context and last developing the approach that risk management framework that meets the organizational needs. The methods include developing and implementing an iterative risk management process, as well as planning and establishing a risk management process. The other method is to discuss all of the risks with stakeholders and obtain feedback from them. Determining the overall scope of the organization is risk management processes, as well as conducting regular risk assessments. Furthermore, assessing the risks that could influence the organization’s ability to achieve its goals.

# Conclusion:

This part of the analysis ultimately deals with network security and risk evaluations, where we analyzed different network security instruments and approaches utilizing both arrange security and risk assessments. At first, at the side the network security implementation that demonstrates network vulnerabilities and dangers, the apparatuses and approaches utilized to control the network are discussed. The attacks are moreover talked about with potential security arrangements to protect the network from attacks with network performance monitoring.

# Bibliography

<https://www.manageengine.com/network-monitoring/network-management.html>

<https://www.cisco.com/en/US/technologies/tk869/tk769/technologies_white_paper0900aecd806c0d88.html>

<https://searchnetworking.techtarget.com/definition/fault-management>

<https://www.creanord.com/echonews/fcaps-series-accounting-management-for-carrier-ethernet.html>

<https://www.techopedia.com/definition/29972/network-performance-management>

<http://ceit.aut.ac.ir/~siabi/NSM/3-%20Network%20Management%20Principles%20and%20Practice%20-%202nd%20Edition%20(2010)_2.pdf>

<https://www.avast.com/c-what-is-tcp-ip>

<https://searchnetworking.techtarget.com/definition/SNMP>

[https://www.dpstele.com/ /v1-v2c-v3-difference.php](https://www.dpstele.com/snmp/v1-v2c-v3-difference.php)

<https://en.wikipedia.org/wiki/OSI_model>

https://nmap.org

https://www.websecurity.digicert.com/security-topics/what-is-ssl-tls-https

<https://searchmobilecomputing.techtarget.com/definition/RMON>

<https://www.howtonetwork.org/tshoot/module-1/an-overview-of-network-management-models/>

<https://www.oreilly.com/library/view/top-down-network-design/9781587140051/ch09.html>

<https://www.ibm.com/support/knowledgecenter/en/POWER5/iphae_p5/networkmanagement.htm>

<https://info.support.huawei.com/info-finder/encyclopedia/en/NETCONF.html>

<https://www.manageengine.com/network-monitoring/network-protocols.html>

<https://www.essentialtech.com.au/blog/5-most-common-network-security-risks>

<https://www.eccouncil.org/network-security/>