Enterprise Network Design and Implementation using Cisco Packet Tracer

Technical Report · December 2020

CITATIONS
0

READS
39,733

4 authors:

Aisha Muhammad
Middlesex University
6 PUBLICATIONS **3** CITATIONS
SEE PROFILE

Aisha Abdulrahman Abba
Middlesex University
5 PUBLICATIONS **3** CITATIONS
SEE PROFILE

Kashim Kyari Mohammed
13 PUBLICATIONS **4** CITATIONS
SEE PROFILE

Abuhuraira Abubakar
Middlesex University
1 PUBLICATION **0** CITATIONS
SEE PROFILE

MSc Cyber Security and Penetration Testing

CST4500: COMPUTER NETWORK AND INTERNETWORKING

IMPLEMENTATION OF A NETWORK DESIGN FOR MSS LTD. USING CISCO PACKET TRACER

Student Name	Student Number	Email Address
Abu Huraira Aliyu Abubakar		aa4784@live.mdx.ac.uk
Aisha Abdulrahman abba		aa4786@live.mdx.ac.uk
Aisha Muhammad		am3434@live.mdx.ac.uk
Kashim Mohammed		km1396@live.mdx.ac.uk

06/12/2020

1 INTRODUCTION

A computer network is a group of computer systems and other hardware computing devices connected through communication channels to enable communication between a wide range of users to share resources. The implementation of a corporate network scenario is completely network based. IT is a secure network that is mostly used in major organizations and other entities to ensure secure connectivity and exchange of their data, information, the building blocks of computer networks are specialized equipment such as hosts, routers, switches, and access points. A network is created when two or more of these devices are connected to exchange resources via a common convention known as protocols.

Local Area Network or LAN (Local Area Network) is a type of network that serves a local area and supplies networking capability to a group of computers near each other. A local area network can support as little as two or three users in the home office or several hundred users in the central office of a company. Homeowners and IT managers set up LANs such that network nodes can share services such as printers or network storage.

Many considerations must be considered to design and construct a well-secured network, such as the topology and location of hosts within the network, the choice of hardware and software technologies, and the careful configuration of each component. To ensure the design is done properly, all requirements necessary for the design are first defined before proceeding to the implementation.

Designing and Implement a computer network is a time-consuming, complex and intricate task, in which, many divisions of an organization are involved. Usually, factors like physical location to the analysis of user website access is taken into consideration during the design and implementation phase.

The group, as fresh graduates and new employees of NSP Ltd. Company, are required to advise on the Local Area Network requirements of a medium sized company, namely, MSS Ltd. The group is required to cover a network implementation design for MSS LTD, a three-floor medium sized company whose plan involves a LAN network design that would be able to endure any future upgrades. The company consists of 3 departments: Marketing, sales and general support equipped with workstations. All workstations will have access to the internet, intranet, and the email. The network will consist of dedicated servers and also provide database and data sharing services.

2 Devices and Technologies

This chapter gives an overview of the devices and configurations selected for the proposed design.

2.1 Devices

According to McQuerry (2008), the devices that transmit and/or receive data through a network segment are network devices. There are various devices used in the implementation of network design in accordance to the requirements.

2.1.1 Switch

A switch is used to connect several nodes of a network within multiple segments (Hucaby, 2014). This device works on the 2nd Layer of the OSI Model. Also, this device transmit data to the recipients except for broadcast traffic to devices with unknown ports. This device eliminates the remaining segments of a network from unintended procession of data and is imperative to network security and performance (Hucaby, 2014).

2.1.2 Router

Lucas (2009) stated that routers are interconnection network devices that send and receive packets between networks. This type of network device is based on Layer 3 IP addresses and selects the best path for data transmission in a network. This device, while on the 3rd Layer of the OSI Model, makes network address-based decisions.

2.1.3 Firewall

According to Sheth & Thakker (2011), a firewall, is considered as a single device, which imposes the access control policy amongst networks. Firewalls, usually a standalone device, is an application software based or network embedded device.

2.1.4 IP Phone

IP Telephone, very broadly speaking, is a telephone built to operate with an IP PBX. However, the prevalence of the SIP standard means that the IP PBX of today has invariably develop into a SIP-based PBX. This is excellent news for companies and end-users because it ensures the PBX providers cannot push you to lock in with their proprietary applications or hardware.

2.1.5 Servers and Hosts

The host is a node that interacts in a user program, either as a server, a client, or both. The server is a type of host that provides services to other hosts. Usually, a server allows connections from clients who request a service feature (Jorge, 2019).

2.2 Technologies

This is known as entities for both material and irrelevant, created by the application of mental and physical effort to obtain some value. In this use, technology applies to instruments and devices that can be used to solve world problems.

2.2.1 Access Control Lists

The Access Control List is a policy used in filtering routing protocols, permit or deny traffic flows, and to redirect traffic based on the set policy. Also, this policy or rules is processed from top-to-down until it hits the first match. The access list is then processed only when a condition is met (Suman & Agrawal, 2016).

2.2.2 VLAN

Virtual Local Area Network (VLAN) is a standard of logically segmenting devices on a network that are physically dispersed (Froom et. Al., 2010). This standard allows network design to be flexible. Similarly, VLANs broadcast domain borders on the 2nd layer of the OSI Model. These broadcast Domains are device groups, that receive broadcast frames created by devices in the group (Kaluve et. Al., 2008).

2.2.3 STP

The Spanning Tree Protocol (STP) prevents uninvited loops while creating a redundancy path in a network (Saxena et. Al., 2017). Multiple active paths in a network is the major cause of loops. These allow duplication of messages while appearing on both ends of a switch. Similarly, this disrupts the forwarding algorithm on a switch and duplicate messages are sent. This protocol allows a LAN with redundancy to manage the loop period of ethernet frames (Saxena et. Al., 2017).

2.3 Cost Assessment

It must be considered the cost of physical network design and looking for best alternative design that can meet the budget. Hence, we should analyze the cost of circuit, internetworking devices, hardware, software, network management, test, and maintenance. These could be by two steps: request for proposal and selling the proposal to management.

3 Design and configuration

3.1 Requirements

3.1.1 FUNCTIONAL REQUIREMENTS

- The three departments, namely, Marketing, Sales and General Support, should have separate LAN with individual applications. However, these departments must share data.
- These departments should be able to run a telephony system with VoIP running both voice and data.
- The company should be able to run both voice and data over VLAN.
- The design should support email and communication
- The design should also support a database server
- The design should also accommodate the company's intranet

3.1.2 User Requirements

User Requirements	Description
Location and number of workstations	• Marketing department occupying the first floor with 20 workstations. • Sales department on the second floor with 30 workstations. • General support with 25 workstations on the last floor.
Availabilty	An uninterruptible network is required for user operations
Scalability	The network implemented should be scalable to endure any future expansions.
Affordability	MSS Ltd has a limited budget and network design and implemtation should be done within the said budget.

Affordability	MSS Ltd has a limited budget and network design and implemtation should be done within the said budget.
Security	The LAN should be secured with restricted access. The network should have the capability of filtering what enters and leaves the network.

3.1.3 Application Requirements

Application Requirements	Type	Level of importance
Email Client	Microsoft Outlook	Important
Web browser	Microsoft Edge	Important
Database	Microsoft Access	Critical

3.1.4 Hardware Requirements

Device	Type	Specification	Numbers	Location
Generic PCs	Hosts	CPU: Intel Core I5 RAM: 8GB 2666mHz DDR4 RAM: 128GB NvME SSD	75	First floor, Second floor, Third floor
Server	Application, Email, Database	CPU: Intel Xeon RAM: 64GB ECC ROM: 6TB x3 NvME SSD	3	Server room
IP Phone	VoIP	Name: Cisco IP Phone 7960 Cables: Cat 5E (8P8C Shielded Twisted Pair)	75	First floor, Second floor, Third floor
2811 router	Integrated services router	Dimensions (WxDxH) 43.8 cm x 41.7 cm x 4.5 cm. Weight. 6.4 kg. DRAM Memory. 512 MB (installed) DDR SDRAM. Flash Memory. 128 MB (installed)	4	First floor, Second floor, Third floor, Server room
5506-X ASA	Adaptive Security Appliance firewall	Users/nodes: Unlimited VLANs: 5; 30^4 Memory: 4 GB	1	Server room
3560-24PS multilayer switch	stackable access-layer switches	DRAM: 4 GB. Flash: 4GB. VLAN IDs. 4,094. switched virtual interfaces (SVIs): 1,000. Jumbo frame: 9198 bytes. Total routed ports: 208.	1	Server room
Cables	Copper Straight Through, Co-axial	8P8C STP with RJ45 connectors		As per requirement

3.1.5 Network Requirements

- Network Interface Card (NIC) to connect the computer to the network cable.
- Network Circuits: category 5 unshielded twisted-pair (UTP) wire for a 10Base-T Ethernet and Connector RJ45.
- Switches 24-port
- Network Operating Systems (NOS): Linux for NOS server software, Windows OS for clients.
- IP Phone: Cisco IP Phone 7960

3.1.6 Functional Requirements

Functional Requirements	Description
Access to internet, intranet, and email.	Internet connectivity should be configured for all users accessing the network.
VoIP system	The VoIP system should be able to run both voice and data over the system.
Data sharing	Employees should be able to access the data of any departments database.

3.1.7 Estimated budget

BUDGET	PRICE PER UNIT	QUANTITY	TOTAL
Generic PC	20,000	75	Rs 1,500,000
Cisco IP Phone 7960	Rs 9,089	75	Rs 681,675
Cat 5E (8P8C Shielded Twisted Pair)	Rs 1,349	75	Rs 101,175
2950-24 switch	Rs 1,699	10	Rs 16,690
Cable-moderm	Rs 2,098	1	Rs 2,098
100ft coax cable	Rs 4,189	1	Rs 4,189
Dell poweredge R340 Server	Rs 97,902	3	Rs 293,706
2811 router	Rs 44,209	4	Rs 176, 836
5506-X ASA	Rs 42,569	1	Rs 42,569
3560-24PS multilayer switch	Rs 64,659	1	Rs 64,659
Serial DCE	Rs 236	3	Rs 708
			TOTAL
			Rs 2,884,305

This include the overall projecting cost for the hardware expenditure that is needed to build network Design.

4 IMPLEMENTATION

In this chapter, the knowledge gathered is applied into the commands and configuration of various devices.

4.1 Implementation plan

The propose implementation plan will follow the Cisco **PPDIOO** methodology:

- **Prepare(2 weeks) :** high level architecture design are created based on the given requirement of the network.
- **Plan (3 weeks):** the detailed environment of the network is laid out and structed.
- **Design(3 weeks):** this is beyond the basic architecture in need into the exact specification of a particular network, this will include building measurement and exactlly where all hardware will be placed.
- **Implement(4-5 weeks):** this is actual deployment and physical installation of the design and all required component.
- **Operate(2 months):** this is where the network is used and tested while its being seen to make sure there are no issues in the network architecture.
- **Optimize(continously):** this stage is ongoing and is used to practically manage the network, with the main goal of identifying and resolving issues before they affect the users.

4.2 Topology

Network Topology: Network topology is the configuration of the different elements (links, nodes, etc.) of the communication network. This is a topological structure of a network that can be presented either physically or logically.

4.2.1 Physical

Physical topology shows the configuration of various network components. It represents the spatial configuration of the equipment and cables in the context of a network. It concerns the basics of a network that lacks minute information such as data transmission and system sort. The pattern of layout of nodes (computers) and network cables depends on the ease of installation and network setup. It affects the cost and capability of the bandwidth depending on the system solution. This considers the location of nodes and the distance between them. Devices may be arranging to form a ring (Ring topology) or a linearly connected to a line called Bus topology.

4.2.2 Logical

A logical topology is a networking term that specifies the connection process configuration for all nodes within the network. It transfers data via Physical topology. It is independent of the spatial topology and the configuration of nodes. It involves the intricate specifics of the network, such as the type of devices chosen (switches, routers) and their efficiency, which influence the pace and speed of transmission of data packets. Logical topology guarantees maximal flow control that can be controlled within the network. However, the mesh network topology is implemented, which enables redundancy across the network.

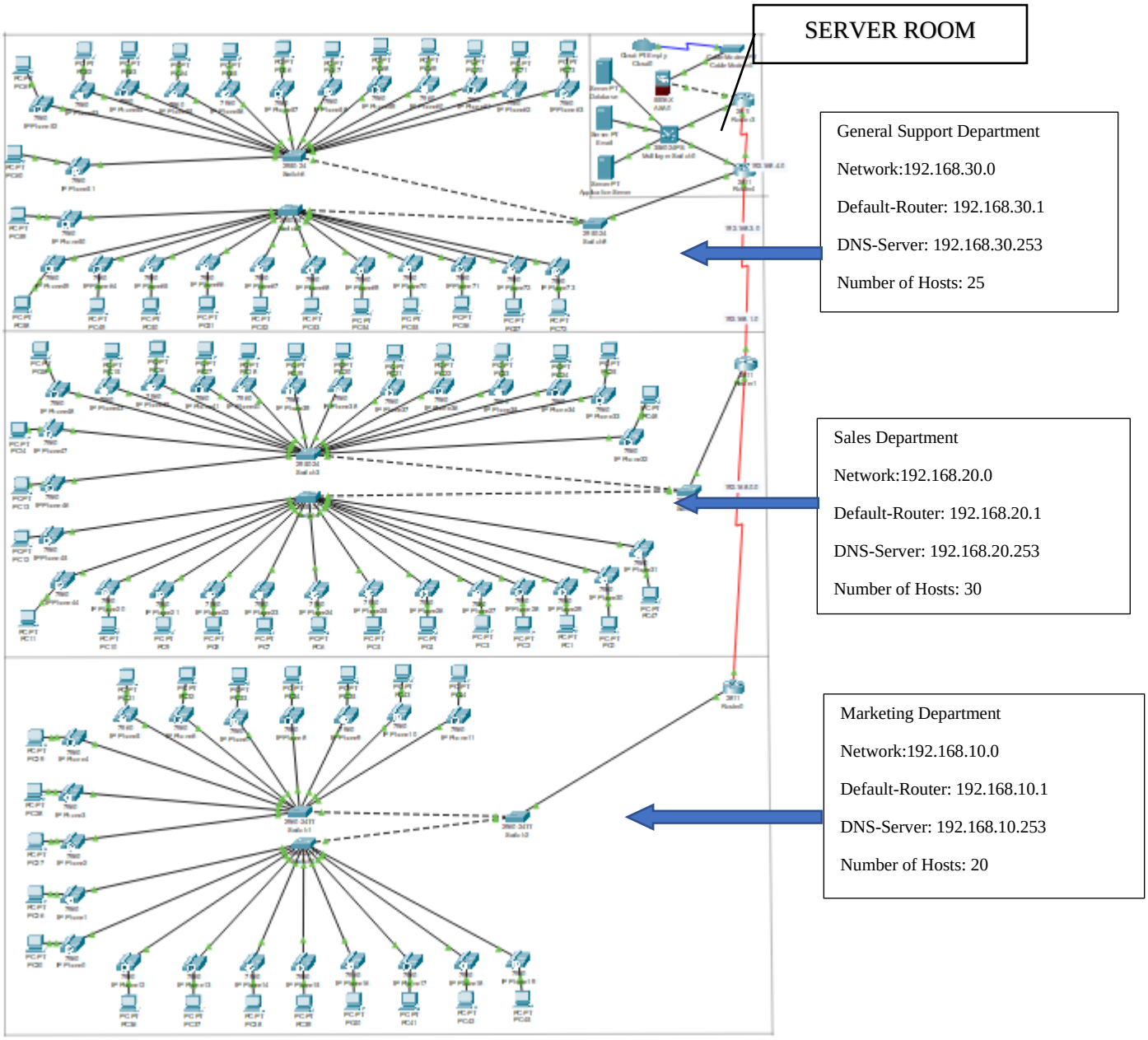

Figure 1 Logical Topology of MSS Ltd 's LAN

4.2.3 Difference between Physical and Logical Topology

Physical Topology	Logical Topology
Depicts the physical network structure.	Depicts the planning of the data transfer network
It can be arranged in the topologies of the star, ring, mesh, and bus.	It appears in the topologies of the bus and loop.

The architecture can be updated on a need-based basics.	No intervention and coercion are involved here.
This has a noteworthy influence on the cost, bandwidth and scalability capability of the network depending on the preference and availability of equipment.	This has a huge effect on the speed and distribution of data packets. It controls the flow control and the organized distribution of data packets.
This is the real path associated with the transmission.	This represents the high- level of data flow.
Physical network link.	The data route taken by the network

4.3 Addressing

4.3.1 IP Address Table

DEPARTMENT	NO OF DEVICES	NETWORK ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS	SUBNET MASK
MARKETING	40	192.168.10.0	192.168.10.1	192.168.10.254	192.168.10.255	255.255.255.0
SALES	60	192.168.20.0	192.168.20.1	192.168.20.254	192.168.20.255	255.255.255.0
GENERAL SUPPORT	50	192.168.30.0	192.168.30.1	192.168.30.254	192.168.30.255	255.255.255.0

4.3.2 DHCP

DHCP is a network server that dynamically assign default gateways, IP addresses and other parameters of network to client's computers. This relies on the standard protocol also known as Dynamic Host Configuration Protocol or DHCP to respond to client broadcast queries. The DHCP server automatically sends the proper network parameters for clients to interact correctly on the network. Without DHCP the network administrator must manually set up any client that enters the network, which can be tedious, particularly in large networks.

4.3.3 RIP

RIP is a standard transport layer protocol, intended to be used on a lesser scale. Networks, RIP was one of the first genuine network architectures for a distance vector, It is supported by a variety of systems. Each network which is 16 hops away or more is declared inaccessible by RIP, with a higher network length of 15 hops. A metric of 16 hops in RIP is known to be a poison route or an infinity metric. If several paths exist for a specified route, RIP can load that balancing among these paths (by default, up to 4) unless the metric (hopcount) is equivalent (Gani *et al.*, 2011).

5 CONCLUSION

In this article, an MSS LTD (MSS LTD) that uses networking topology applied with principles such as VLANs in multiple area networks using Cisco Packet Tracer. VLANs have been used for logical MSS LTD and with the aid of router and transfer setups, data packets have been routed from one system to another. The procedures include a specification and method for MSS LTD using VLANs to end IP network connections for next generation network infrastructure implementations.

The MSS LTD network architecture offers a substructure for all infrastructure frameworks, such as network stability, wireless networking, and operating performance. Also, network foundation services such as switching, multicast routing and high availability for MSS LTD are supported.

This chapter presents a summary of configurations on network devices and hosts. The firewall and Switches were configured on the primary switch in the rack, and within the failover cluster's main unit. Similarly, all PCs and Servers were assigned IP addresses using the DHCP pool and hostnames were grouped numerically, for address management i.e., PC001 to PC100 belongs to the first floor. An NTP Server was setup to have a synchronization time within the network and all the hosts were added to MSS Ltd's domain.

VLANs were created to accommodate VOIP phones on the main switch within every network i.e, VTP server, and numbers assigned on the router. Network interfaces that are used to connect end devices were added to VLANs and setup as access ports. Also, the BDPUGuard Spanning Tree Protocol (STP) features were configured on these access ports.

REFERENCE

1. Froom, R., Sivasubramanian, B. and Frahim, E., 2010. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide: Foundation learning for SWITCH 642-813. Cisco press.
2. Gani, A. *et al.* (2011) 'Intelligent routing information protocol using full triggered update mechanism', *International Journal of Physical Sciences*, 6(11), pp. 2750–2761. doi: 10.5897/IJPS11.282.
3. Sheth, C. and Thakker, R., 2011, February. Performance evaluation and comparative analysis of network firewalls. In 2011 International Conference on Devices and Communications (ICDeCom) (pp. 1-5). IEEE.
4. Lucas, M.W., 2009. Cisco Routers for the Desperate: Router Management, the Easy Way. No Starch Press.
5. Hucaby, D., 2014. CCNP Routing and Switching SWITCH 300-115 Official Cert Guide: Exam 38 Cert Guide. Cisco Press.
6. McQuerry, S., 2008. Interconnecting Cisco Network Devices: Part 2 (ICND2). Cisco Press.
7. Kaluve, S.S., Foo, I., Murthy, S., Ponnapalli, R. and Manam, R., Cisco Technology Inc, 2008. *Method to distribute IEEE 802.1 X authenticated users among multiple broadcast domains*. U.S. Patent 7,447,166.
8. Suman, S. and Agrawal, E.A., 2016. IP traffic management with access control list using cisco packet tracer. Int. J. Sci. Eng. Technol. Res, 5(5), pp.2278-7798.
9. Saxena, A., Mellacheruvu, R. and Deshpande, P., Cisco Technology Inc, 2017. Spanning tree protocol (STP) optimization techniques. U.S. Patent 9,655,232.