Small Scale Industry Network Design

[1]Rahul D. Mehta, [2]Suraj Kaneria
[1]Assistant Professor, [2]Network Engineer
[1]Electronics & Communication Engineering Department
[1]Government Engineering College - Rajkot, Rajkot, India

Abstract: Today's networks are customized and more of application specific instead of general purpose networks. Nowadays, small scale industry networks are also in huge demand due to plenty of start-up activities. Personalized requirements of small scale industry networks are quite different than that of gigantic networks. It demands scalability, cost effectiveness, ease of configuration, security, least response time and ease of maintenance. It is basically divided into major criteria, from network designer's point of view, like Client Requirements, Network Planning, Network Design, Hardware & Software Implementation and Testing. The paper explains in-depth study and implementation of each design aspects as well as of configuration. Moreover, monitoring as well as hardware and simulation based testing is carried out using variety of tools which in turn will provide a platform for the beginner to have a profound knowledge of professional approach to Small Scale Industry Network Design.

Index Terms **– Small Scale Industry, Network Design, Protocol, Packet tracer, GNS3, Wireshark, VLAN**

I. INTRODUCTION

In the success of any business, small scale to large scale, data networks play a paramount role. It helps connecting customers, support applications and services as well as manages resources to keep business flowing. In the race of providing simplified yet powerful solutions to the businesses, the networks have become too complex. Nowadays, scalability of the network is kept in centre of designing as well as with optimum availability and enhanced security.

Network design basics cover Network design overview, the benefits of a hierarchical network design and Network design methodology. Today's networks are expected to have quick response, round the clock functionality, automatic protection against potential threats as well as automatic load balancing mechanism. One can understand that, networks with all the functionality incorporated happen neither overnight nor by chance [1]. It takes network designers time and immense efforts over a time period to get tuned to the requirements to perform at the peak. Few authentic network designing steps, which are the abstract of designer's efforts, are as follows:

- Validate the goals and practical needs
- Decide the features and functionalities essential to meet the needs identified
- Carry out a network-readiness evaluation
- Construct a solution and location acceptance investigation map
- Generate a project map

Efficient network design focuses on following four elementary network design goals:

- **Scalability:** Accommodating new users, user groups and remote sites as well as facilitating novel applications without any adverse effect on the quality of the services delivered to the current group of users.
- **Availability:** Assurance of consistency and reliability in performance round the clock even in case of minor faults which don't affect the overall network performance.
- **Security:** Safeguarding the network using filters, devices and firewalls, against any type of potential thereat and security attacks frequently take place in a network.
- **Manageability:** Irrespective of initial design, network should be able to support staff and must be able to handle as well as maintain other networks. Complex network is quite difficult to handle and can't guarantee sustained efficient functionality.

To meet the elementary design goals, a network have to be built on architecture that works for both flexibility and growth. Hierarchical Network Design is the best way of achieving fundamental design goals. In the field of networking, a hierarchical design is implemented to set devices into multiple networks [2]. The networks are structured in a layered approach. The hierarchical design model consists of three basic layers: Core layer, Distribution layer, Access layer

Hierarchical networks have got plenty of advantages over the flat networks. The advantage of separating a flat network into tiny segments is: local traffic remains local. Only traffic intended for other networks is elevated to an upper layer. Layer 2 devices in a flat network provide slight chance to control broadcasts or to filter adverse traffic. As additional devices and applications are supplemented to a flat network, response times degrade until the network becomes impractical. Figures-1 and Figure-2 shows the arrangement of network devices in flat network design and hierarchical network design respectively.

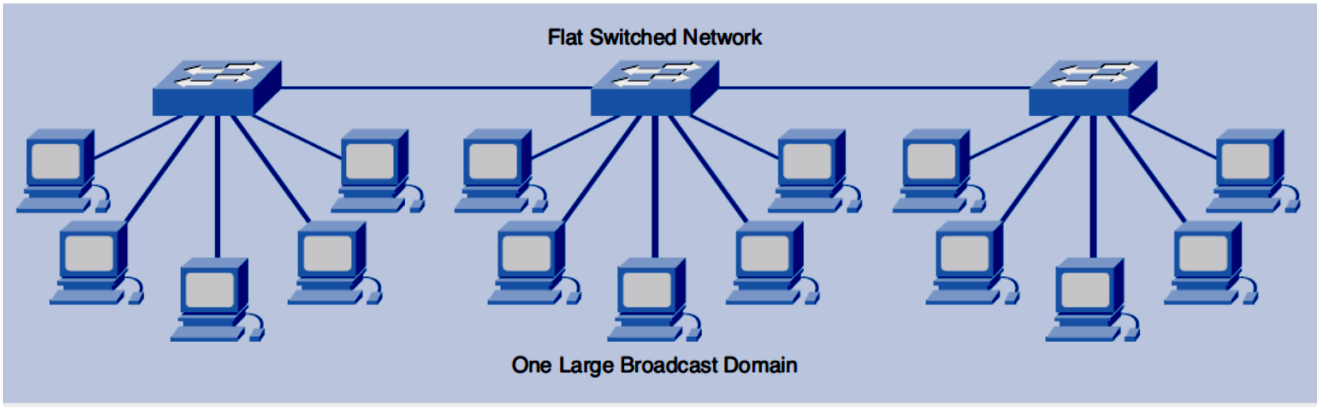

Figure 1: Flat Network

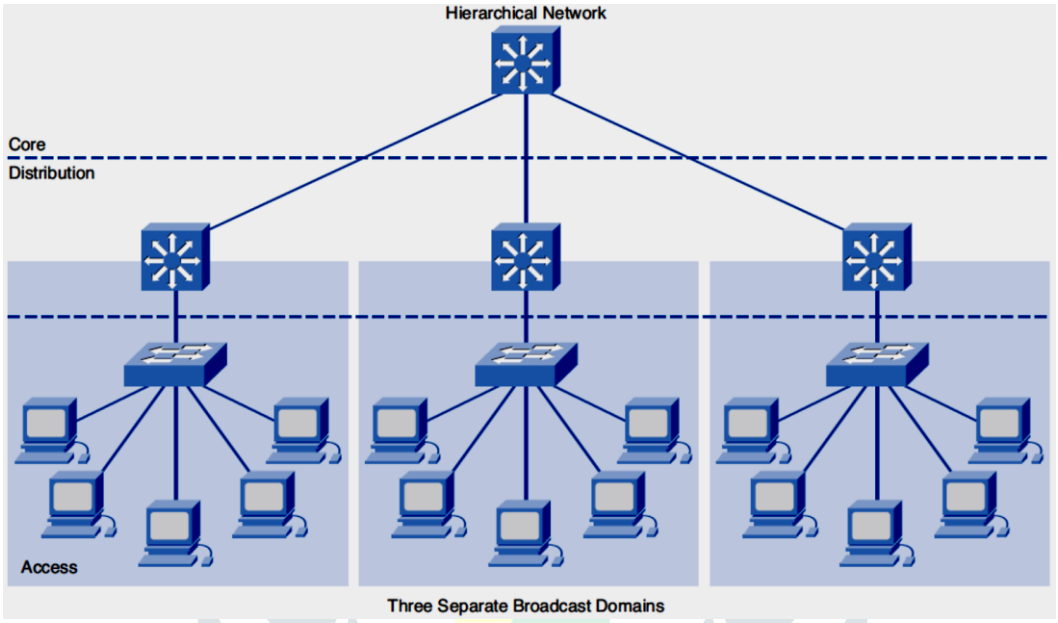

Figure 2: Hierarchical Network

II. LAYERED STRUCTURE

Layered architecture is the heart of the networking which gives a clear path of plan to execution. Each layer performs unique set of responsibilities as well as offers and obtains service to upper and from below layers respectively. Network device manufacturers implement functionality on core three-layered architecture in which network devices and links are clubbed according to three layers [3]: Core Layer, Distribution Layer and Access Layer.

Each layer of the model consists of a combination of Router, Switch and Links or all three. Some networks possibly merge the job of two layers into a single device or exclude a layer completely. The functionality of each layer is described below:

- **The Core Layer**

The middle layer gives an enhanced and concrete transport formation by sending activity at higher pace. The layer handles Access-list checking, Data encryption and Address translation.

- **The Distribution Layer**

The circulation layer is positioned between the get to and core layers and separates the core from whatever is left of the system. The layer utilizes access records and different channels. It handles Routing updates, Route summaries, VLAN traffic and Address aggregation. Unwanted traffic is prohibited to conserve resources and use of policies secures the network.

- **The Access Layer**

The passage control and movement of traffic are the key functionalities of Access layer. End clients get to network assets by method for the get to layer. Being a front end, it conserves the resources to obstruct unauthorized parties to gain access of the network resources.

III. SMALL SCALE INDUSTRY NETWORK DESIGN EXAMPLE

The network design depends on specific requirements of a network. Small scale industry network design criteria are quite different from medium and large size industry networks [1], [2], [4]. To make the difference clearer and to understand small scale industry network design, an example of a small scale company with all hardware and software requirements and specifications is discussed.

The company has got five functional departments: HR, Placement, Management, Technical and Student which are to be connected in a network. Common departmental requirements are as follows:

- Full Internet connectivity
- Security
- Automatic and Dynamic IP address allocation
- Access to FTP server

Total number of hosts per department and customized requirements of each department are as follows:

- HR – 5 hosts, HR host to HR host connectivity within HR department, only HR group member node can connect to HR node
- Technical – 20 hosts, only technical department should have access to remote access to network devices, should be able to ping other departments
- Management – 4 hosts, should not be able to communicate with other departments
- Placement department – 5 hosts, should be able to communicate to student department only
- Student department – 100 hosts, should not be able to communicate with other departments

Common requirements of a company as a solution provider as well as an administrator are as follows:

- Wireless access for guests and clients
- Should be able to monitor and measure incoming and outgoing traffic

To work out on customized requirement of each department and company as a whole, network scenario of the project is generated using GNS3 [5] tool before designing, as shown in Figure 3. The layout covers all the customized requirements and accommodates those at different standard layers of implementation model, named as Access Layer, Distribution Layer and Core Layer.

The simplified project scenario of overall customized network design is prepared in GNS3, a network simulator, to check feasibility, connectivity as well as complete hardware requirements and software and configurations. Hardware requirements, Hardware functionality, Protocols and Supporting software/Tools to provide required functionalities, are listed below in sequence:

A. Hardware / Components Required

- 2 SERIAL CABLES
- 28 FASTETHERNET CABLES
- 2 ROUTERS
- 4 SWITCHES(LAYER 2)
- 11 PCs
- 4 SERVERS
- 2 WIRELESS ROUTER

- Router is used to establish communication between public and private network, 2 routers are used, one as a functional router whereas other as a redundant one.
- Switches are used to divide the departments and to distribute router resources.
- Link redundancy is kept between switches to ensure reliable full connectivity in case of link failure.
- NAT (Network Address Translation) technology ensures the security by translating Private IP address into Public IP address.

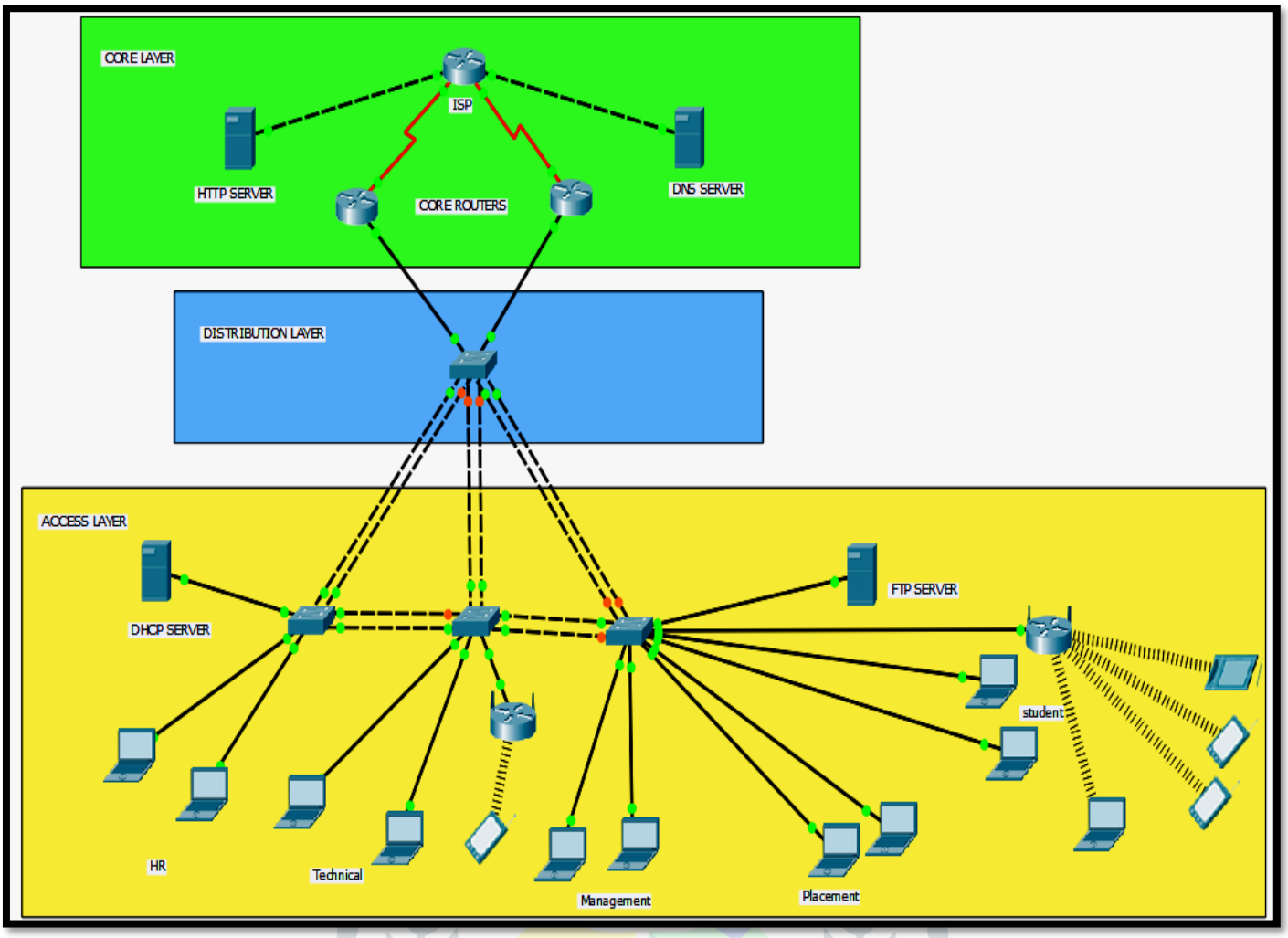

Figure 3: Project Scenario

B. Protocols Implemented

- IP (Internet Protocol)
- VLSM (Variable Length Subnet Mask)
- DHCP (Dynamic Host Configuration Protocol)
- VLAN (Virtual LAN)
- DTP (Dynamic Trunking Protocol)
- VTP (VLAN Trunking Protocol)
- Inter VLAN Routing
- Port-Fast
- Port Security
- ACL (Access Control Lists)
- PAT (Port Address Translation)
- Default Routing
- HSRP (Host Standby Router Protocol)
- SSH (Secure Shell)

Basic functionalities of each protocol are explained below [6], [7], [8]:

- **Internet Protocol (IP)**

IPv4 (Internet Protocol version 4) address is a 32 bits (4 bytes) long address. It is also known as Logical Address for a network interface. The IPv4 addresses are unique and universal. Each byte in IP address is separated by a dot and each byte is

identified by a decimal number in the range [0-255]. IP provides two main functions: Logical addressing of hosts and Routing of packets between networks. Network ID defines the network of IP address and Host ID defines the IP address for particular user.

- **VLSM (Variable Length Subnet Mask)**

A Variable Length Subnet Mask (VLSM) is a need based IP addressing resource allocation mechanism instead of common IP assignment rules. It is known as 'subnetting a subnet' that is used to enhance effectiveness of IP addressing scheme. The example in this paper uses 192.168.1.0/24 as a mother network to create sub-networks.

- **Dynamic Host Control Protocol (DHCP)**

Basically there are major two ways of assigning IP addresses, Static which is administratively assigned and Dynamic which is automatically assigned. Unlike its predecessor BOOTP, DHCP permits a host to get an IP address progressively without the system director by setting up an individual profile for every gadget. DHCP server consists of range of IP addresses. As soon as host becomes alive, DHCP server is contacted for an address. The DHCP server selects an address and assigns it to that host on lease. Mobility is the most powerful feature of DHCP server.

- **VLAN (Virtual LAN)**

Virtual LANs (or VLANs) segregates Layer-2 switch into several broadcast domains. Each VLAN holds individual broadcast domain (i.e. IP subnet). Communication from one VLAN will never be conveyed to the ports having a place with another VLAN. Broadcast Control, Enhanced Security, Flexibility and Scalability are the major benefits of using VLAN.

- **Dynamic Trunking Protocol (DTP)**

Negotiation of Trunking on a link between two VLAN aware switches is done by the Dynamic Trunking Protocol (DTP). In OSI model, DTP works at Layer 2.

- **VLAN Trunking Protocol (VTP)**

VLAN database management is done across switches in large switching networks. VLAN Trunking Protocol (VTP) provides the functionality such that VLAN database is managed throughout the network quite easily.

- **Inter VLAN Routing**

Single huge network is divided into many broadcast domains by means of VLAN. Forwarding of traffic outside VLAN environment is not automatically done by VLAN enabled switches. Inter VALN routing provides this functionality by means of Layer- 3 device like Router.

- **Port Fast**

Port Fast makes a switch or trunk port to go into the scattering over tree sending state promptly, skipping the tuning in and learning states.

- **Port security**

Port security is a layer two activity control. It allows design to do single change to the ports to sanction just a pre-determined number of source MAC addresses in the port.

- **Access Control List (ACL)**

Organization directors must make sense of how to limit undesirable access to the system while permitting inward clients fitting access to fundamental administrations. In spite of the fact that security instruments, for example, passwords, physical security gadgets and callback hardware are useful, they frequently do not have the adaptability of fundamental movement shifting and the particular controls most chairmen lean toward. For instance, a system manager needs to permit client's access to the Internet, yet not to allow outer clients telnet access into the LAN. Routers give fundamental activity shifting abilities, for example, blocking Internet movement with Access Control Lists (ACLs). An ACL is a consecutive rundown of allow or deny proclamations that apply to locations or upper-layer conventions. Govern to utilize when no particular course can be resolved. There are mainly two types of ACL: Standard and Extended

- **Port Address Translation (PAT)**

Port Address Interpretation (PAT) is a capability that allows variety of clients within a private system to utilize a trivial number of IP locations. It's essential ability is to distribute a solitary IP open address among different customers who require to making use of the Internet liberally. It is an extension of network address translation (NAT).

- **Default Routing Protocol**

When there is no route found to the destination through routing protocol tables, there is always a default route to the next hop is available. All the routing, in this case, will be done through default routing using default routing protocol. Only sub-router can use default routing.

- **HSRP (Hot Standby Routing Protocol)**

Hot Standby Router Protocol (HSRP) built up the preventive Hot Standby Router Protocol (HSRP) to allow multiple switches or multilayer modifications to take on the outer shell of a private entrance way. This is distinguished by relegating a virtual IP and MAC deliver to all switches taking an interest in a HSRP gathering. Routers within the same HSRP assemble must be allocated a similar gathering number, which can go from 0 to 255.

- **Secure Shell (SSH)**

SSH is a system convention that furnishes executives with a safe approach to get to a remote PC. SSH too refers to the group of utilities that employ the protocol. Secure Shell offers strong authentication and protected encrypted information interchanges between PCs interfacing above an uncertain system.

C. Tools used

- Graphical Network Simulator – 3 (GNS3) [5], Cisco Packet Tracer (CPT) [11] and Wireshark [12] are used as an emulation tool, designing tool and traffic analyzing tool respectively.

IV. IMPLEMENTATION

- **Hardware Implementation**

- Firstly, the core routers are connected to the ISP router by serial cables for point to point connection. This gives Internet connectivity to the core routers.
- Both core routers are connected further to a Distribution switch. Distribution layer switch allocates the core layer resources to the access layer.
- Three switches of access layer are connected to distribution layer switch as shown in Figure-3.
- End devices are connected to the access layer switches.

- **Software implementation**

IP addressing

- DHCP server is configured manually so that all end devices can get IP address from DHCP server.
- HR department's IP addresses are configured manually.
- This network contains subnetting and VLSM concepts for efficient use of IP addresses.
- IP scheme used in this network
    - Mother network : 192.168.1.0/24
    - HR department : 192.168.1.0/28
    - Management department : 192.168.1.16/29
    - Placement department : 192.168.1.24/29
    - Technical department : 192.168.1.32/27
    - Student department : 192.168.1.128/25

VLAN (Virtual LAN)

- VLAN concept is used to accommodate five departments with three switches only.
- VLAN is used for dividing physical broadcast domain into logical one to make different departments on each switch.
    - HR department : VLAN 50
    - Management department : VLAN 20
    - Placement department : VLAN 30
    - Technical department : VLAN 10
    - Student department : VLAN 40
- By implementing VLANs we cannot communicate in between departments. So, to make them communicate we have used the concept of Inter VLAN routing.

DTP (Dynamic Trunking Protocol)

- Links between switches must be trunk in order to forward multiple VLANs data.
- DTP provides the service to form trunk dynamically between switches.

❖ Note: Links between Core routers and distributer switch are configured as a trunk manually. It cannot be performed dynamically.

VTP (VLAN Trunking Protocol)

- It propagates and creates the information of VLAN automatically with all other switches.
- The switch which belong to HR department acts as server for VTP and all other switches act as client.

PORT-FAST

- It skips the 30 seconds of listening and learning stages of an access port when end devices are connected to it.

Inter VLAN Routing

- It can be performed through router by configuring sub-interfaces.
- Both core routers perform the Inter VLAN routing

Default routing

- It gives the default route towards the ISP network from the core routers.

PAT (Port Address Translation)

- It provides the translation of IP addresses from the private network to the public network.
- It translates all private IPs into single public IP
- PAT tries to use the real source port number of the internal host to form a unique registered IP address and port number combination.

SSH (Secure Shell)

- It is remote access protocol from which we can get the access of the device remotely.
- It uses RSA algorithm to secure the connection. Hence encrypting data as well as password.

- **Redundancy**

HSRP (Hot Standby Redundancy Protocol)

- It is first hop redundancy protocol. So, we have used this in core routers so that when main core router fails, backup router will take its place and route the traffic from it without disturbing the network topology.
- When main core router comes online backup router will go on standby mode and all traffic will go through main core router.

Link Redundancy

- Used in between the switches.
- When one link fails the backup link will become active.

- **Security**

ACL (Access Control List)

- An extended access-list is a regimented register of statements that can refute or allow packets based on source as well as destination IP address, port numbers and upper-layer protocols. Model access list can reject or sanction packets by source address only and authorize or disallow complete TCP/IP protocol suite.

PAT (Port Address Translation)

- By translating private IP into public IP we hide the real source address of data. Hence, it also provides the security to the network.

Port Security

- It allows only specific MAC address on a port which is predefined by network administrator. So that unauthorized device cannot connect to that particular port. If any unauthorized device connects to that port, the port goes into error disabled mode [9], [10].

V. APPLICATIONS

The example of small scale industry network design helps in understanding network design aspects from Idea to Implementation. Following are the direct and indirect knowledge gaining benefits of the study.

- Insight to fundamentals of networking and data communication, understanding of flow of data communication, introduction to various networks and basic networking devices.
- Hands on IP address strategies and IP assignment, understanding and implementation of various routing protocols.
- In-depth study and analysis of complex network behaviour, Emulation of various protocols and connecting simulated network to real world.
- Applications and Tools study for remote access, packet capturing, traffic management and security

VI. CONCLUSION

The paper covers in-depth survey of small scale industry network design from Idea to Implementation. The designing example is selected such a way that it is identical to real life industry requirement which in turn helps gaining insight about lots of fundamentals as well as core aspects of designing for efficient network configuration. Network design goals and importance of hierarchical design are proved to be the most important parameters to achieve optimized performance for small and customized design. Also, extensive study of hardware and software level implementation is carried out. Adequate use of various protocols, applications and tools has been done for network implementation, monitoring and maintenance. In a nutshell, the paper covers each and every aspect of Small Scale Industry Design that a beginner is expected to learn and a professional is expected to implement.

VII. ACKNOWLEDGEMENT

We would like to specially acknowledge Ms. Shweta Adroja for her contribution in terms of suggestions and technical assistance throughout the paper writing exercise.

REFERENCES

[1] S. Kenneth, *Designing and Supporting Computer Networks, CCNA Discovery Learning Guide*. .
[2] K. Stewart, A. Adams, A. Reid, and J. Lorenz, *Designing and Supporting Computer Networks, CCNA Discovery Learning Guide*. 2008.
[3] "Cisco Three Layer / Three-tier Hierarchical Network Model." [Online]. Available: http://www.omnisecu.com/cisco-certified-network-associate-ccna/three-tier-hierarchical-network-model.php. [Accessed: 06-Feb-2019].
[4] "Enterprise Campus 3.0 Architecture: Overview and Framework - Cisco." [Online]. Available: https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Campus/campover.html. [Accessed: 06-Feb-2019].
[5] J. C. Neumann, *The book of GNS3 : build virtual network labs using Cisco, Juniper, and more*. No Starch Press, 2015.
[6] J. Steinberg, T. Speed, C. Fernando, and A. Pande, *SSL VPN : understanding, evaluating, and planning secure, web-based remote access*. Packt Pub, 2005.
[7] "What is SSL VPN (Secure Sockets Layer virtual private network)? - Definition from WhatIs.com." [Online]. Available: https://searchsecurity.techtarget.com/definition/SSL-VPN. [Accessed: 06-Feb-2019].
[8] "Configuring IP Access Lists - Cisco." [Online]. Available: https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/23602-confaccesslists.html. [Accessed: 06-Feb-2019].
[9] "Cisco IOS IP Configuration Guide, Release 12.2 - Configuring IP Addressing [Cisco IOS Software Releases 12.2 Mainline] - Cisco." [Online]. Available: https://www.cisco.com/c/en/us/td/docs/ios/12_2/ip/configuration/guide/fipr_c/1cfipadr.html. [Accessed: 06-Feb-2019].
[10] "IP Addressing: DHCP Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches) - Configuring the Cisco IOS DHCP Server [Cisco IOS XE 3SE] - Cisco." [Online]. Available: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_dhcp/configuration/xe-3se/3850/dhcp-xe-3se-3850-book/config-dhcp-server.html. [Accessed: 06-Feb-2019].
[11] "Download The Packet Tracer Simulator Tool & Find Courses | Networking Academy." [Online]. Available: https://www.netacad.com/courses/packet-tracer. [Accessed: 06-Feb-2019].
[12] "Wireshark · Go Deep." [Online]. Available: https://www.wireshark.org/. [Accessed: 06-Feb-2019].