**Experimental Setup of an Enterprise Network**

{Word Count: 3194 words}

**Table of Contents**

[Introduction 5](#_Toc88165913)

[Background Study 5](#_Toc88165914)

[Networks and topology 6](#_Toc88165915)

[Experiment Methodology 9](#_Toc88165916)

[Results and Discussions 23](#_Toc88165917)

[Conclusion 24](#_Toc88165918)

[Reference List 26](#_Toc88165919)

**List of Figures**

[Figure 1: Experiment setup](#proposed_system_arch) 9

[Figure 2: Access Switch1 Configurations 11](#_Toc88150923)

[Figure 3: Access Switch2 Configuration 11](#_Toc88150924)

[Figure 4: Core Switch Configuration Pt1 12](#_Toc88150925)

[Figure 5: Core Switch Configuration Pt2 12](#_Toc88150926)

[Figure 6: Core Switch Configuration Pt3 13](#_Toc88150927)

[Figure 7: DHCP Relay Core\_SW1 14](#_Toc88150928)

[Figure 8: Dynamic IP Addressing in PC1 15](#_Toc88150929)

[Figure 9: Dynamic IP Addressing in PC2 15](#_Toc88150930)

[Figure 10: DNS Server Configuration 16](#_Toc88150931)

[Figure 11: Enterprise\_DNS1 17](#_Toc88150932)

[Figure 12: Enterprise DNS2 17](#_Toc88150933)

[Figure 13: DNS Query 18](#_Toc88150934)

[Figure 14: Syslog configuration of Net\_Infra\_Server 19](#_Toc88150935)

[Figure 15: Core\_SW1 configuration for remote syslogging 19](#_Toc88150936)

[Figure 16: Logs from Net\_Infra\_Server 20](#_Toc88150937)

[Figure 17: Syslog configuration of web server 20](#_Toc88150938)

[Figure 18: logs from Web browser 21](#_Toc88150939)

[Figure 19: Web Browser Client1 21](#_Toc88150940)

[Figure 20: We Browser Client2 22](#_Toc88150941)

[Figure 21: Web Browser Output on viewing the intranet site 22](#_Toc88150942)

**List of Tables**

[Table 1: Connectivity Details 11](#_Toc88151006)

[Table 2: IP Addressing 15](#_Toc88151007)

# Introduction

According to Shin, a computer network is a collection of wired and wireless links through which computers and other hardware devices exchange data or information. A computer network is an irreplaceable component of any industry running on digital technologies. It contains physical and virtual networks and protocols that connect all the users as well as the systems on a network (say, a Local Area Network) to a server or applications in the data centre or cloud to access network data. (Shin, 2021)

An Enterprise network span across the entities of an organisation like employees, departments, workgroups, trans-geographical facilities and expedites necessary communication among them. An Enterprise network can be any combination of PANs, LANs, and MAN/WAN connections etc., depending upon the diversity and size of the network. In an enterprise network, the various computing devices establish links via network elements such as switches, routers, Wi-Fi or other protocol based connections to share data, applications and services. Enterprise networks primarily rely on high-speed switching and routing devices to mediate data transfers between computers, applications, servers, services etc. An enterprise network also provides additional features like load balancing, firewalling, a service mesh for modern applications, helps eliminate operational siloes, ensure security and supports end-to-end network automation.

# Background Study

A network has computers located on or connected by network nodes, including personal computers, servers, networking hardware, or other general-purpose hosts, identified by network addresses and sometimes labelled using hostnames. Network addresses such as the Internet Protocol (IP) communication protocol serve to locate and identify the network nodes.

The need to increase the data rates in communication channels has propelled the research advancements in almost all the network technology areas. The researches, however, does not require revamping the entire system but certain only regions. According to Seifert and Edwards, this is achieved by separating the entirety of the network function into discrete partitions we call Layers. With layering and application of appropriate technology to each entity improves the performance without affecting the other layers. Thus, each architectural layer contains distinct, related functions. In addition, the function grouping makes each layer as independent of another as possible, with minimum information permeation between the layers. Some of the layers of a standard network are the physical, datalink, network, transport, session, presentation, and application layers. (Seifert and Edwards, 2008)

The functions provided by the Physical layer include line drivers, receivers, signal encoders, decoders etc. The physical layer serves the requests sent down from the data link layer. The services provided by the Data link layer allows direct communication between devices across the network's physical channel. For data delivery from the data link layer across multiple data links, a Network layer is responsible for it. The Transport layer provides error-free, guaranteed and sequenced message delivery across stations in a network. It also doubles as a shield against the vagaries of networks like misplaced or corrupted data packets to protect the higher layers. The Session layer manages Communication sessions between applications. For problems related to communication between network systems utilising different local data representation methods, the Presentation layer allows data exchange between systems using various formats while maintaining consistent semantics. And finally, the Application layer provides generic application functions, such as an e-mail utility, a file transfer capability and Application Program Interfaces (APIs), allowing communication between user applications across the network. (Seifert and Edwards, 2008).

# Networks and topology

Computer networks, from the inception of the term, are into four different types according to scope, Personal Area Networks (PANs), Local Area Networks (LANs), Metropolitan Area Networks (MANs) and Wide Area Networks (WANs). According to Shin, a PAN represents a small network with a few meters or less coverage, such as Bluetooth, Wi-Fi direct. Whereas a Local Area Network (LAN) covers an extended area than a PAN, usually stretches until the physical boundary of an entire organisation, company or institution. The size of a LAN hence depends upon the size of the organisation. An ethernet is a preferable form of LAN. A Metropolitan Area Network (MAN) is large enough to cover a city, and often interconnected LANs through land-based or wireless forms a MAN. Ethernet-based Metro-Ethernet is a good choice as a MAN platform. A true Wide Area Network (WAN) can cover a state, a nation, an international territory or smaller MANs. The internet itself, without any exclusive owner, is the best-known WAN connection. (Shin, 2021)

The physical network layout is called its topology and is a design approach used to interconnect network nodes. The physical structure of a network then means the connections and relations intermediary devices and hosts. (Shin, 2021)

Some elements of network topology are:

* Business locations (number of sites and degree of their distribution)
* Number of users
* Type and number of hosts
* Applications, and
* Security conditions

According to Shin, some popular network Topology layouts are,

a) Point to Point topology, where a direct connection between two nodes is established point-to-point,

b) Bus Topology, characterised by a half-duplex common line to which all the end nodes are directly connected and with two terminator devices situated at both ends,

c) Ring Topology, where nodes are attached to a backbone ring,

d) Star topology, in which host stations are connected to a central intermediary device,

e) Mesh topology, wherein all possible connections are directly linked, and

f) Tree topology, a hierarchical connection of nodes with the one on top becoming a root node, with the arrangement resembling a Christmas Tree.

Networks are also sometimes described according to their Server-Client relationship. A server in a network is the system providing services to the other systems in the network, and a client is a system using remote services from the server. Clients have limited computational and disk storage capacities, and they access respective services provided by the server through the Server-Client Channel. (Shin, 2021)

# **Components of an Enterprise Network and progressions**

Components - According to Seifert and Edwards, High-Port density bridges used in modern applications, called switches, often acts as the geographically central device which performs the bridging function among its ports and the environment where the switch operates. At the same time, for interconnectivity between networks, we use networking devices called routers to forward data packets between computers. An interconnection between the different networks, connected via the individual routers, makes up the Internetwork. A Layer 2 switch is associated with bridging between the nodes, while a Layer 3 switch functions as a router. Another type of switch called Virtual Switch or vSwitch is a software application that screens the data packet and intelligently directs the communication on a network. A Multi-layered switch (MLS) can perform all the traditional functions at layer 2 and 3 devices, sometimes at layer 4. (Seifert and Edwards, 2008). Secure networking is also one most rapidly developing fields in networking technology. As companies and industries have digitally transformed rapidly in the modern world, there is a high demand for appropriate infrastructure and security solutions. A recent development in secure networking is the development of Secure Access Service Edge or SASE. In SASE, all the existing services are integrated into commonality function sets to deliver multiple integrated secure networking solutions as a single service. (Wood, 2020)

Connectivity - Virtual LANs or VLANs are increasingly replacing traditional LANs in today's industrial setting and are not bound by conventional LAN limitations, like physical wiring devices. 5G or Fifth Generation mobile network characterised by high throughput, low latency, high reliability, increased scalability and energy-efficient mobile communication technology. According to Mitra and Agarwal, Heavy real-time control of machines using IoT and massive machine to machine communications will become possible due to 5G. (Mitra and Agrawal, 2015) Wi-Fi 6 is the new IEEE 802.11 standard in the WAN family targeting private, edge networks. According to Oughton et al., as a large proportion of global networks are in the Home or Office setting, they are most likely to use Wi-Fi as the form of wireless internet connectivity. (Oughton et al., 2021). According to Seifert and Edwards, the original intention for developing LAN bridges was to extend the LAN connectivity. But, now, due to the rapidly increasing advancements in wireless technologies, we find wireless networks and their applications applied globally across all settings, from home and office to large conglomerates. (Seifert and Edwards, 2008).

Control - The three A's (Triple-A or AAA) in networking stands for authentication, authorisation and accounting. The triple-A refers to the core mechanism which ensures data protection in the CIA (data Confidentiality, Data Integrity, and Data Availability) triad model. According to Shin, Data Confidentiality means that data should be read-only by the intended users. Data Integrity ensures that the original data in storage, in-process, or transit remains unchanged accidentally or via voluntary action of unauthorised personnel. Finally, Data availability means that Data/Information should be readily available to authorised users.

Authentication ensures that the identity of the engaging party must be validated such that the data is seen only by the intended users. Access control or authorisation permits the user to access specific resources. It is the process of denying or allowing access to network connectivity, data, or systems attached to the network. The accounting function provides the access and usage records of system resources belonging to a node in the network. The best practice is to keep logs of all the node activities. An added advantage of a log/record is its value in future analysis and auditing for resource utilisation and security controls. (Shin, 2021)

****Experiment Methodology****

The study aims to experimentally configure and set up an Enterprise network and simulate its network transactions using DHCP Server, Web server, DNS, and MySQL Server elements. The Enterprise Network shall consist of Layer 3 Enterprise switches, a DHCP server, DNS, Database System, Core Switch, Access Network, and client access via LAN in a two-layered architecture. The Experimental network subjected to this study is a Local Area Network (LAN) and focuses on the physical and data link layers.

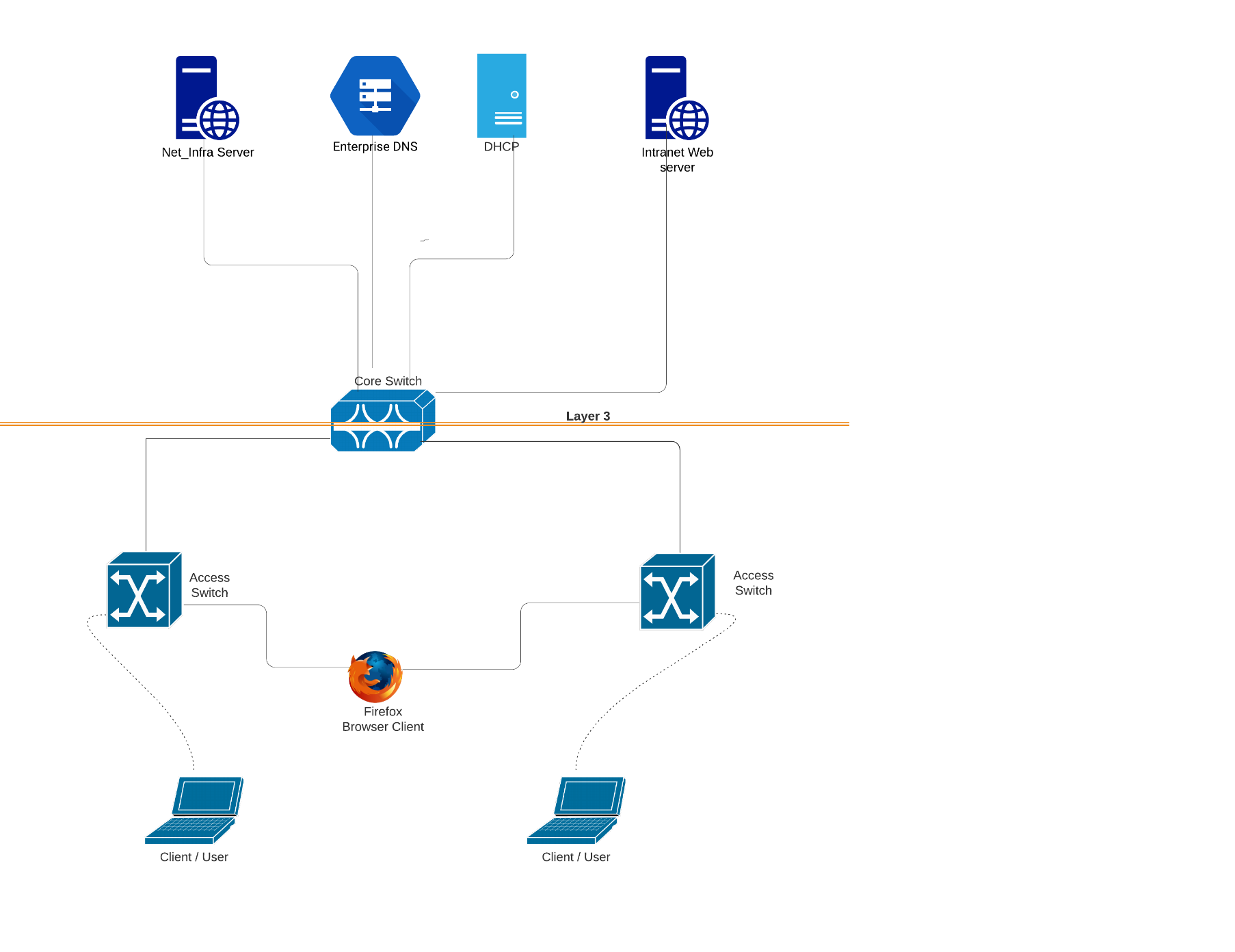


Figure 1. Proposed System architecture

Clients - A client is the system or computer part of the network using remote services provided by the server. A client provides the user with access to the network by making specific requests to the server. Clients then run programs to utilise the accessed data from the servers. Clients have limited computational and disk storage capacity compared to the server. The clients can access these services provided by the server through the Server-Client Channel and thus handle user interactions. The Client is also entirely dependent upon the server. It may get overloaded or fail in response to the Client-Server network. However, the function of preventing such a failure is executed by a specialised network manager. The clients are the highest priority nodes in a network. The Client/Server protocol employed in this study is Network File System or NFS. (Shin, 2021).

System Components 1) Collapsed Core Infrastructure- Core/Distribution Switch (Core\_SW1) & two Access Switches ( Ac\_SW1 & Ac\_SW2), two Virtual PC clients (PC1 & PC2) and one Firefox container (WebBrowserClient).

2) Servers - DNS (Enterprise\_DNS), DHCP (DHCP Server), Web Server(Intranet\_Web\_Server), and FTP/Syslog Server (Net\_Infra\_Server)

Access and Core Switches - According to DeCusatis, there are three, four, or more tiers such as access, aggregation and core switch layers in the traditional ethernet network hierarchy. Users access the terminal and connect to a network using the access switch or TOR switch. In contrast, a Core switch is a high-capacity switch positioned at the core or backbone of the network and is responsible for routing and forwarding data at the highest level. Data movement across each layer is called multi-tiering, and traffic movement across switches are called 'Hops'. Flat network architecture refers to removing tiers from the traditional arrangement such that only the access switches and core switches remain and the network collapses into a two-tier network. A flattened network that clusters multiple switches into one enormous (virtual) switch fabric can significantly reduce operating expenses and capital expenses. (DeCusatis, 2013)

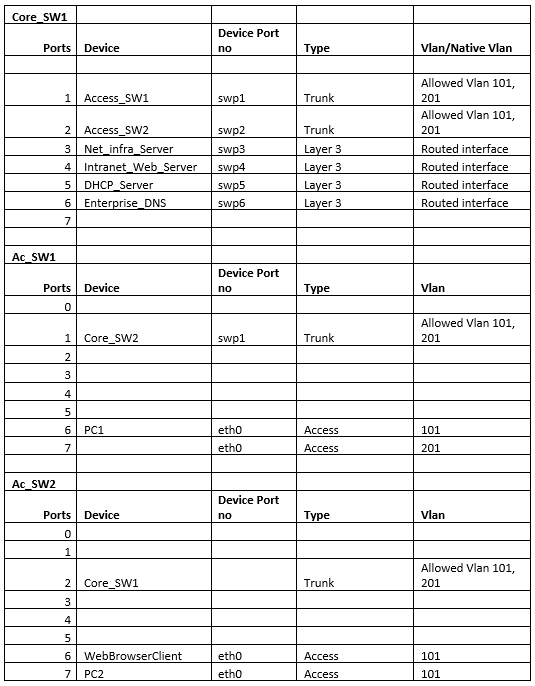
Layer 3 Switching application - According to Seifert and Edwards, Routers offers functionality beyond the capabilities of the data link layer bridge. State-of-the-art application-specific integrated circuits (ASICs) and reconfigurable ICs (FPGA) with low-cost logic have facilitated the fabrication of network layer routing engines at layer2 switch prices. High performance, cost-effectiveness, hardware-based internetworking, and the network-based protocols feature set characterises Layer-3 Switches. The primary application of a Layer 3 switch lies in implementing the fast path of flow in hardware. The switch architecture must be optimised to perform real-time functions on a packet-by-packet basis, and background tasks performed occasionally, indicating an integrated software implementation. (Seifert and Edwards, 2008),

Technology dependencies - Use GNS3 and import the appliances in GNS3. A) Cumulus-Open source Switch, b) Networkers Toolkit- Web server, FTP server, DHCP server, Syslog Server, c) DNS- Domain Name server, and d) Firefox Container- Web browser

Switch connection and configuration - The first step in integrating a switch into a network is by powering it up and physically connecting it to the network. The connection is made via the computer's port running cables or a Secure Shell (SSH) for remote command-line access to the switch to make configuration changes. The former mode of switch connection is called Console connection. In the latter case, the switch is configured with an IP address, a hostname for the node and a connection protocol. Hence, the management interface must be configured to access before managing the switch or attempting to connect or configure.

In this study, for the Core Switch, we will be connecting and configuring the following devices: two trunk-type access switches at device port numbers swp1 and swp2 for the VLAN and four-layer-3 type switches, namely Net\_infra\_server, Intranet\_Web\_Server, DHCP-Server and Enterprise\_DNS at device port numbers swp3, swp4, swp5, and swp6 respectively for routing interface. (**Table 1**). For Access Switch 1, a trunk type device named Core\_SW2 needs to be connected at Device port number swp1 and the PC1 at device port number eth0. For Access Switch 2, a device named Core\_SW1 is connected at 2nd port, a 'WebBrowserClient' is connected at 6th port and the PC 2 at 7th port. (**Figures 2- 6**)

Table 1: Connectivity Details



Graphical user interface

Description automatically generated

Figure 2: Access Switch1 Configurations

Graphical user interface

Description automatically generated

Figure 3: Access Switch2 Configuration

Text

Description automatically generated

Figure 4: Core Switch Configuration Pt1

A screenshot of a computer

Description automatically generated

Figure 5: Core Switch Configuration Pt2

Graphical user interface

Description automatically generated

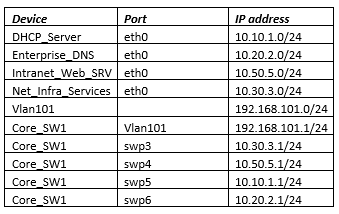
Figure 6: Core Switch Configuration Pt3

Configuring DHCP system - The Dynamic Host Configuration Protocol or the DHCP service hands out IP address configuration to the devices on the network, either via the servers in the network or the routers. The Four-step DHCP address acquisition process is:

1. DHCP Discover
2. DHCP Offer
3. DHCP Request
4. DHCP Ack or DHCP NAck

The IP addressing in this study relates to DHCP allotment to PC1 and PC2, the end clients in the network. (**Table 2**) (**Figures 7-9**)

Table 2: IP Addressing



The DHCP Relay of Core\_SW1 is given by:

Graphical user interface, text

Description automatically generated

Figure 7: DHCP Relay Core\_SW1

The following are the dynamic IP Address assignment in PC1 and PC2 respectively,

Text

Description automatically generated

Figure 8: Dynamic IP Addressing in PC1

Graphical user interface, text

Description automatically generated

Figure 9: Dynamic IP Addressing in PC2

Domain Name System (DNS) - A Domain name is an identification string representing a network domain, the area of influence under the network, or an Internet protocol used to access the internet like a PC. A DNS provides the mapping between the Domain name and the IP address. Any name needs to be registered in the DNS to become a Domain name. (Tetz, 2011)

**Figures 10-13** show the DNS configurations employed in this study, including a DNS server configuration named enterprise DNS 1 & 2 and a DNS Query.

Graphical user interface, text, application

Description automatically generated

Figure 10: DNS Server Configuration

A screenshot of a computer

Description automatically generated with medium confidence

Figure 11: Enterprise\_DNS1

Graphical user interface, text, application

Description automatically generated

Figure 12: Enterprise DNS2

Graphical user interface, application

Description automatically generated

Figure 13: DNS Query

Server Configuration - Server network configuration tasks include installing and configuring application servers, installing and configuring access managers, enabling protocols, configuring the SQL server browser service, exposing or hiding SQL server database engine on the network, etc. System Logging Protocol or Syslog is a standard protocol used for sending system logs and event messages to a specific server in the network. It collects device logs from several different machines in a central administrative system.

The study uses the following server configurations – Syslog configuration using Net Infra Server, remote Syslog for Core SW, log reads from Net Infra Server, Syslog configuration of Web Server, and log reads from it, and presentation of Web Browser clients for PC1 and PC2. (**Figures 14-20**).

Graphical user interface, application

Description automatically generated

Figure 14: Syslog configuration of Net\_Infra\_Server

Graphical user interface, text

Description automatically generated

Figure 15: Core\_SW1 configuration for remote Syslog

Text

Description automatically generated

Figure 16: Logs from Net\_Infra\_Server

Graphical user interface, application

Description automatically generated

Figure 17: Syslog configuration of web server

Text

Description automatically generated

Figure 18: logs from Web server

A screenshot of a computer

Description automatically generated

Figure 19: Web Browser Client1

Graphical user interface

Description automatically generated

Figure 20: Web Browser Client2

# Results and Discussions

The setup in the experiment section mimics a typical enterprise server switching configuration layout. The network contains layer-3 switching and has elements like DHCP Server, Web Server, DNS, and a MySQL server Database system to simulate the network transaction between these elements.

The following figure is the Web browser output obtained from viewing the intranet site:

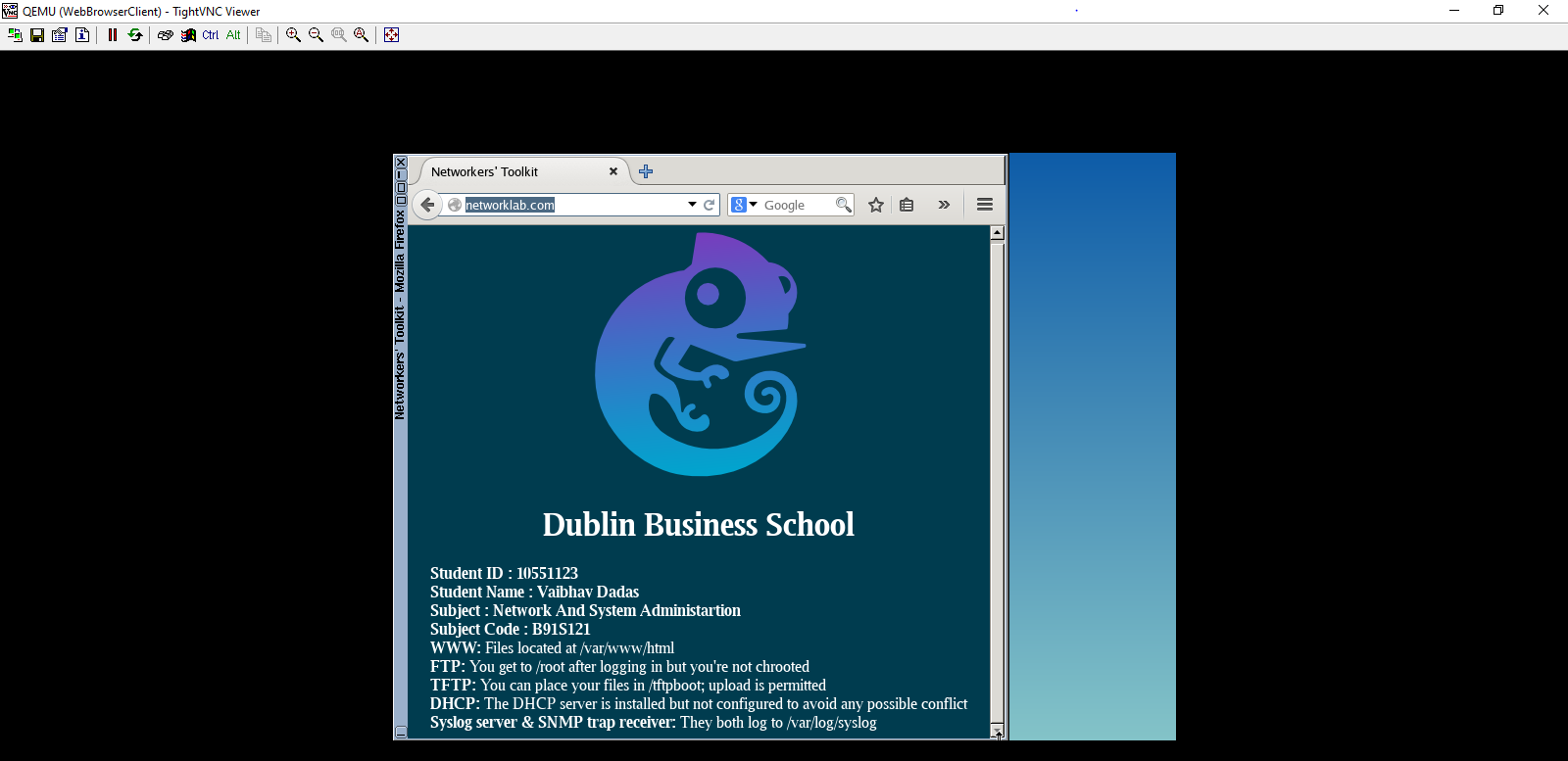


Figure 21: Web Browser Output on viewing the intranet site

A layer-3 switch is essentially a router built over a layer-2 switch that acts as a bridge. Flattening the network, i.e., clustering a large number of switches into a single large virtual fabric, significantly reduces both capital and operational expenses. By eliminating dedicated storage, clustering and managing adapters and their respective switches and eliminating traditional networking tiers have resulted in the reduction of capital expense. Employing a single console to manage the resultant convergent switch fabric also results in reduced operational costs. While traditional networks use several tools to manage their networks, servers, and storage, a common model for management, provisioning, configuration, severe reporting, and network traffic management will optimise the network performance and support the IT infrastructure. Flattened and converged data centres may also require new routing and switching architectures to improve the scalability, resilience and capacity of large layer-2 networks and domains. As the data handled through Enterprise networks are critical, their confidentiality and data integrity must be protected while maximising data availability and utility. (DeCusatis, 2013)

# Conclusion

A wide variety of networking devices exists, from smartphones to laptops, which are accessible to almost everyone in the world. The trend is to get information directly from the internet using high-speed connections regardless of where they are. The desire to access data and data irrespective of geographical locations is the driving force behind wireless technologies and cloud computing. The observation is doubly valid for industries and enterprises where the users or employers might require instant access to information and data. The advancements in technologies like the Internet of Things (IoT) has heralded this change into wireless digital technologies.

Every enterprise needs a unique network tailor-made to meet their requirements and support their workflow, production and management processes. In today's world, it is not a matter of choosing whether one needs an enterprise network or not, but it's about choosing the most suitable network to meet one's demand and expectations. The right enterprise network can increase efficiency by collaborating inside and outside their offices, companies or institutions. Furthermore, a well-implemented enterprise network guarantees security and connectivity to an organisation's connectivity and applications. Therefore, it is crucial in increasing productivity and minimising costs in any industry.

# Reference List

DeCusatis, C. (2013). *Chapter 1 - Transforming the Data Center Network*. [online] ScienceDirect. Available at: https://www.sciencedirect.com/science/article/pii/B9780124016736000015 [Accessed 18 Nov. 2021].

Mitra, R.N. and Agrawal, D.P. (2015). 5G mobile technology: A survey. *ICT Express*, 1(3), pp.132–137.

Oughton, E.J., Lehr, W., Katsaros, K., Selinis, I., Bubley, D. and Kusuma, J. (2021). Revisiting Wireless Internet Connectivity: 5G vs Wi-Fi 6. *Telecommunications Policy*, 45(5), p.102127.

Seifert, R. and Edwards, J. (2008). *The all-new switch book : the complete guide to LAN switching technology*. Indianapolis, In: Wiley Pub.

Shin, B. (2021). *A Practical introduction to enterprise network and security management*. 2nd ed. Boca Raton: Auerbach.

Tetz, E. (2011). *Cisco Networking All-in-One For Dummies*. Chichester: John Wiley And Sons.

Wood, M. (2020). How SASE is defining the future of network security. *Network Security*, 2020(12), pp.6–8.