# Computer Networking: Case Study Analysis

**Technical Report** · September 2022

DOI: 10.13140/RG.2.2.10674.68806



**1 author:**

Chamoth Madushan Jayasekara
University of Plymouth
**35** PUBLICATIONS **6** CITATIONS

# Computer Networking:
# Case Study Analysis

*By: GPDCM Jayasekara*

## Case Overview

To understand the Local and Wide Area Network technologies, materials and protocols relate them to develop conceptual models, and to develop knowledge and skills relevant to the design, implementation, and configuration of network infrastructure.

| Description | Type I | Type II | Type III |
|---|---|---|---|
| Number of total students | >3000 | 3000> and >500 | <500 |
| Number of Labs | 4 Labs or higher (with 41 computer each) | 1 to 3 labs with 41 computers each | 1 or more labs with 10 computers |
| Admin PC/Laptops | 5 | 2 | 1 |
| WiFi | 6 or greater access points | 2 to 5 access points | No Wi-Fi |
| Cashed Engine | Yes mandatory | Yes optional | no |
| | | | |

Education Ministry of Sri Lanka has decided to expand the school network. In standardize approach all the schools will be given network connectivity with control access to Internet. Since the education ministry already have planned to provide laptops to high school students the network expansion is identified as a critical component. This will also provide access to educational content from the schools. By installing a local cache data system, which is provided by the Google larger schools will be able to save download content. The schools are divided into three categories. The following table gives you a detail of the categorizations and basic requirement for the Intended network solution for each category. You're supposed to Identified a possible? Network solution for each category to support the connectivity's. as given in the categorization table. Each group must also provide a detail specification. Required. By the ministry to proceed for procurement process. You are required from my detail addressing plan to connect these schools and build a comprehensive school network ("school net version 3'). the number of Schools to be connected is 6,000 and will be upgraded to total of 10,000 sites adding all public/private schools.

Your report must consist of the following.

a) Three different network layouts for each category.
b) List of key components(active) which sample specifications each network infrastructure.
c) A detail IP addressing plan if ISP has allocated the following address pool for this network Set up IPv6 address space is 2401:DD01: :/32.
d) Sample implementation for a school category one using simulator. Explaining the implementation details identified by you.
e) A possible Security setup for the entire network Identifying that all the connections go through a central ISP hosted facility.
f) The network management plan If the ministry is going to have a single control center at the ministry.
g) Group member contribution matrix (as Annexure A)
h) Group meeting minutes (as Annexure B)

To achieve a first class the presentation must demonstrate a thorough understanding of routing, IP addressing and switching architectures which should also be reflected accurately in the configurations and demonstrations. The network configurations must be of the specific architecture with the use of appropriate explanations and must address both operational and non-operational aspect of the network. You must justify all major network design and configuration choices and defend them at the end of the presentation highlighting your contribution for the group task.

## Acknowledgement

First, I would like to show my deepest gratitude & respect to Mr. Chamindra Attanayaka, for helping & guiding me throughout this research. The completion of this research report gives me much fascination, as it would not have been successful without the hard work, dedication & determination that has been put into this. I was able to provide with optimum commitment to the research. Thank you, dear sir for making this a success!

# Table of Contents

## List of Tables



## List of Figures

## Introduction

The project required us to come up with a island-wide network solution which would be implemented to connect 10,000 schools spread throughout the country. We have been allocated a total IPv6 IP block as 2401:DD01: :/32, under which all the schools will be supported. We have been asked to produce the network solutions for 3 different types of schools, with type 1 being a large school, type 2: a medium school and type 3: a small school. Explained below are our team's proposal for the project.

# Solutions

## Task a)

Shown below are the proposed network layouts for each type of school.

## Type 1 Schools

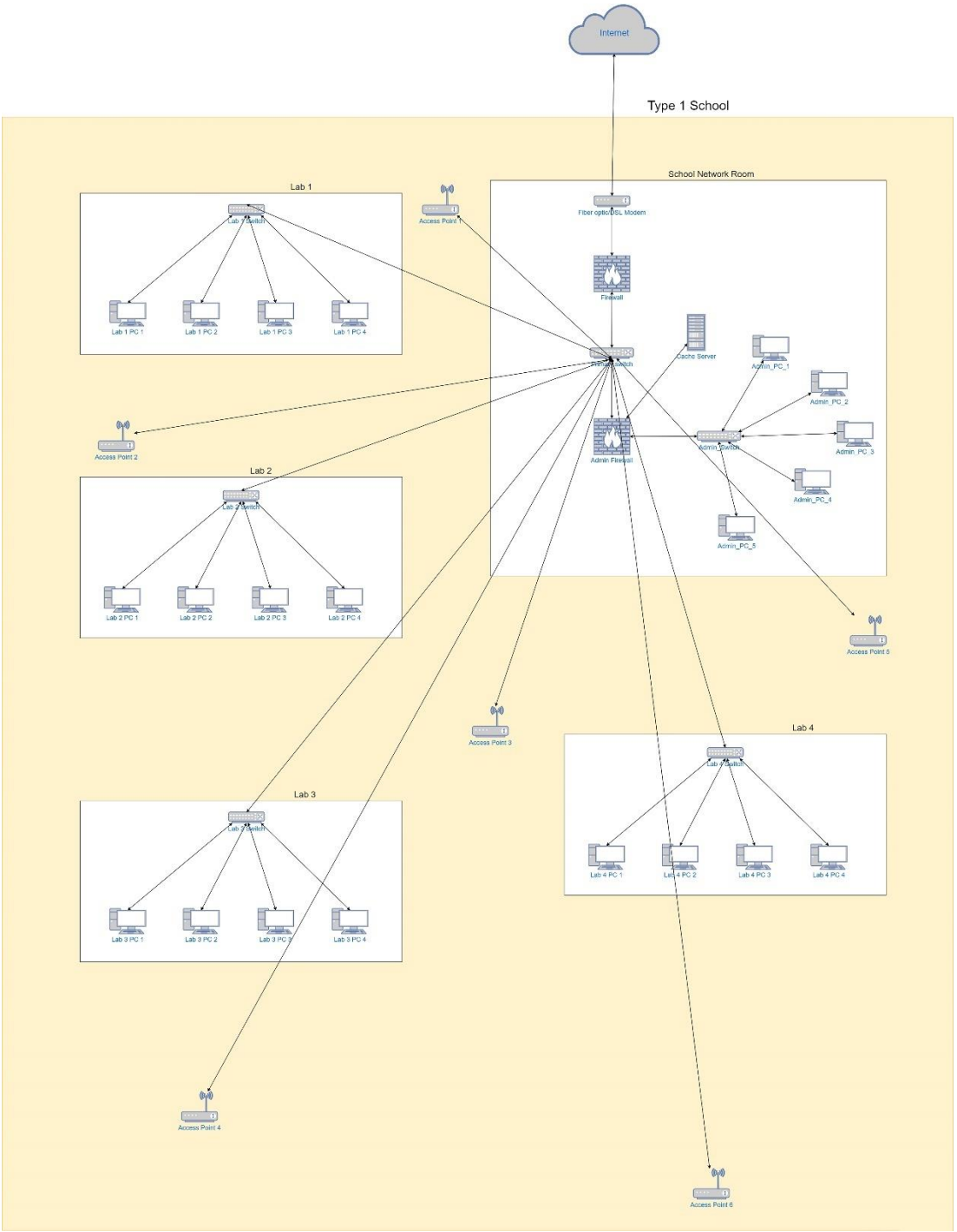


*Figure 1: Type 1 school network layout*

## Type 2 Schools

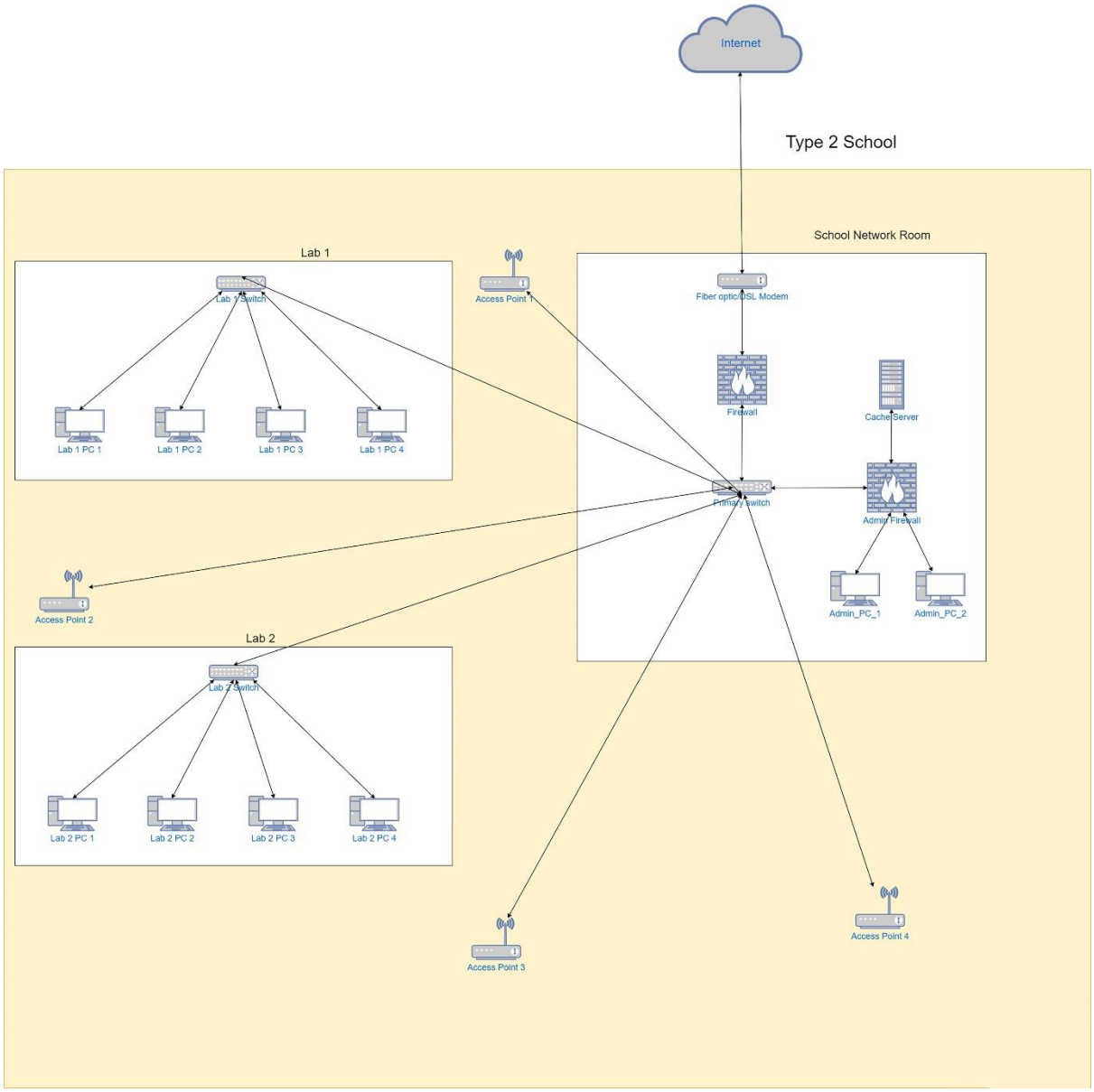


*Figure 2: Type 2 school network layout*

## Type 3 Schools

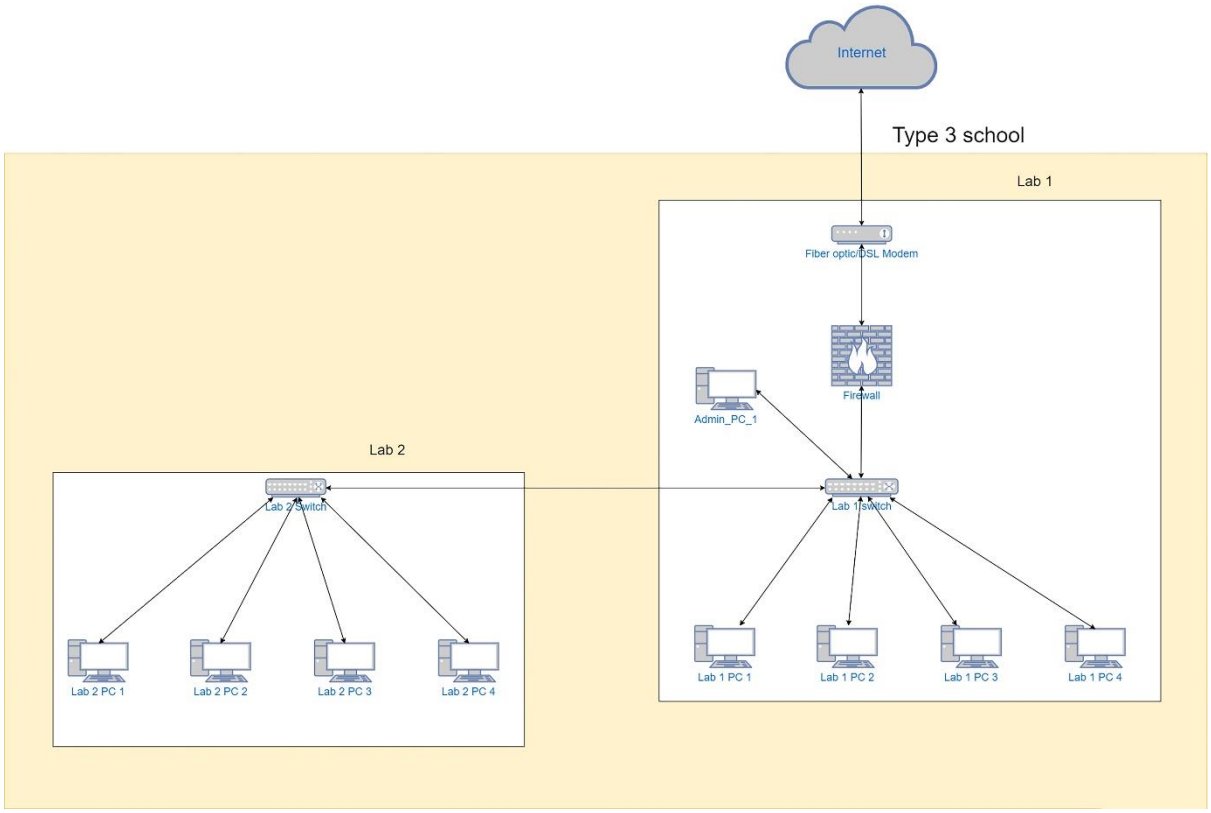


*Figure 3: Type 3 school network layout*

### Layout design assumptions, declarations, and justifications

- In all 3 layouts, the DSL/Fiber optic Modem on the top of the diagram represents an all-in-one modem-router combo solution. This is further explained under active components listings in task b).
- The layout has been simplified to keep it clean and neat. Please note that, for labs, in type 1 and 2 layout diagrams, the 4 lab PCs represent how the 41 lab PCs would be connected, and for type 3 layout diagrams, the 4 lab PCs represent how the 10 lab PCs would be connected.
- All school types have a firewall directly between the core switch and the modem used. This is to both help prevent any intruder attacks, and to regulate the internal traffic requests to sites. (Such as blocking access to certain sites like Facebook, Twitter, and even unauthorised VPN usage etc. from school network)

- For school types 1 and 2, given there is a server on-site which may contain some sensitive data, as well as to help further isolate the admin PCs from a would-be intruder who managed to connect via Wi-Fi or lab ethernet ports, another firewall/smart security appliance (i.e.: Cisco ASA 3 5500 series devices) has been placed. This will allow for further regulations with regards to network-level access control etc.
    - For school type 2, we have directly connected the 2 admin PCs to the firewall as well as the server. This is because in general, most network security appliances we looked at had 8 ethernet ports. Given there are only 2 admin PCs and 1 server, leaving 5 further ethernet slots for expansion, we believed this is a sufficient future-demand-tolerance approach.
        - Due to the same reason, for type 1 schools, we have placed a switch to connect all the admin PCs together. This is because, 5 admin PCs and 1 server would take up 6 ports overall, only leaving 2 more ports in the security appliance for future expansions. If the need arises to add more network-based items such as a common admin-level printer, a network-attached-storage and so on, this will very quickly fill up the remaining ports. This we felt was not sufficiently tolerant against potential future-demands. Therefore, we implemented a switch.
- As can be seen in the layouts, Type 3 network does not have an additional firewall in place to guard against intruders. This is primarily because, given there is no attached server, the potential of having a lot of highly sensitive data is low. Given there is no Wi-Fi, the only way an intruder can connect to this network without facing a firewall is through ethernet from a lab, which can be monitored by lab staff or academic staff. Given there is only 1 admin PC, with less than 500 students for the school, the potential security threat is low. Therefore, we did not feel that the very low risk justified additionally investing in very expensive firewall equipment and licenses.
- For all schools, there was no implementation of a DMZ as there are no specific servers that the schools are supposed to host which should be directly visible to the outside world. Therefore, all machines are directly behind a primary firewall. However, in type 1 and 2 school network layout designs, if port forwarding/routing needs to be done so that a lab-hosted server can be accessed from the outside world, that can still be done safely, provided that the lab-PCs do not contain any sensitive information.

**Task b)**

**Type 1 Schools**

- A modem and a router solution are required. Depending on Fiber optic connectivity availability in the school's location, we recommend opting for fiber-optic connectivity and modem/router. If it is not available, a high-speed DSL connection would have to suffice.
    - Recommended modem/router: Cisco ISR 927
        - This will also cover the firewall portion of the layout as this supports advanced filtering technologies with a full-scale firewall, and it even supports various VPN modes.
- Primary Switch: We recommend a fast, layer-3 (or managed) primary router as this is the central point through which all devices get relayed. If not sufficiently fast enough, this could become a major bottleneck point of the network.
    - Recommended primary switch: Cisco SG350XG – 24T
        - Has 24x 10 Gigabit (copper) ethernet ports. More than enough ports while leaving comfortable amount of room for future expansions.
- Admin firewall: We require a sufficiently fast firewall so that authorised users can quickly connect to the cache-engine and access data. It needs to have 8 RJ-45 ports.
    - Recommended Admin firewall: Cisco Firepower 1140
        - It has a throughput of 2.2Gbps and has 8 RJ-45 ports. Perfect for the problem at hand.
- Admin switch: We require a switch that has about 8-10 ports to allow for future expansions, while being sufficiently fast.
    - Recommended admin switch: Cisco SG350XG – 2F10
        - It has 10x 10 Gigabit (copper) Ethernet ports. If somehow even more expansions are needed, the switch is a stackable switch, therefore can easily add more switches to increase the number of ports.

- Lab primary switch: Given the lab has 41 computers in each lab, the switch needs to be able to handle that number of computers.
    - Recommended lab switch: Cisco SG350XG – 48
        - It has 48x 10/100/1000 Megabit (copper) Ethernet ports so it can support all machines while being sufficiently fast for PCs. The switch is stackable, therefore if some more ports/expansions are needed later, it is easy to increase port counts.
- Access points: The network requirement states the need for 6 or more access points. However, it has not clearly stated whether all access points need to be under the same network (with AP-to-AP client roaming), or whether they would like to implement separate per-access-point Wi-Fi networks.
    - Recommended Access Point: Cisco Aironet 2800e AP
        - Has extended external antenna for better range per access point. Supports both deployment methods, where you can deploy all access points as 1 continuous network with client-roaming, or you can deploy as per-access-point networks.

**Type 2 Schools**

- The modem/router is required. We provide the same recommendation we have for type 1 school modems due to the same reasons.
    - Recommended modem/router: Cisco ISR 927
- Primary Switch: The primary switch recommendation requirements remain like Type 1 schools. However, due to the number of labs being limited to maximum 3 labs, and number of Wi-Fi access points being limited to maximum 5, we could see that having a stackable switch with 10 ports would be ideal for this deployment, as it allows for 2 more free ports for immediate expansions, and given that the switch is stackable, it provides an opportunity for future expansions as needed.
    - Recommended primary switch: Cisco SG350XG – 2F10
- Admin firewall: admin firewall recommendation requirements and the recommendation itself stays the same as for type 1 schools.
    - Recommended Admin firewall: Cisco Firepower 1140
- Lab switch: Lab switch requirements remain the same as for type 1 schools. Therefore, the recommendation is the same.
    - Recommended lab switch: Cisco SG350XG – 48
- Access points: The Access Point requirements remain the same as for type 1 schools. Therefore, the recommendation is the same.
    - Recommended Access Point: Cisco Aironet 2800e AP

**Type 3 Schools**

- The modem/router is required. We provide the same recommendation we have for type 1 and 2 school modems.
    - Recommended modem/router: Cisco ISR 927
- Primary Switch (lab 01 switch): This switch needs to be able to support the 10 lab PCs, where having around 100Mb/s connection is sufficient, while maintaining a high-speed connection to the other labs and being capable of operating at layer 3.
    - Recommended primary switch: Cisco SG350X – 24
        - This switch has 24x 10/100/1000 Megabit ethernet ports, while also having 2x 10 Gigabit ports to connect with other switches in other labs. Therefore, this switch is ideal for this scenario.
- Lab 2 (and normal labs) switch: The requirements state that each normal lab would have 10 lab PCs. Therefore, the ideal solution would have 10x 10/100/1000 Megabit speed ports in a stackable switch configuration. However, given this specific configuration is not available, we recommend the same switch used for the primary switch in Type 3 schools above.
    - Recommended lab switch: Cisco SG350X – 24

**Task c)**

According to the specs, this project has been allocated the IPv6 address space of 2401:DD01: :/32.

On the very first level, we need to create subnets/groupings at the level of schools. Meaning, each school should get its own realm of address space. Given that there will eventually be 10,000 schools added to the network, this would require us to use 14 bits more from the address space to provide each school with an address block. (As $2^{14}$ = 16,384. Which can cater for 10,000 addresses.)

Therefore, once this grouping is done, the per-school level IPv6 address space would be:

- 2401:DD01: :/46, where the range would be between
    - 2401:DD01:0000: :/46 - 2401:DD01: fffc: :/46
    - Incrementing per school as:
        - 2401:dd01:0000: :/46
        - 2401:dd01:0004: :/46
        - 2401:dd01:0008: :/46
        - 2401:dd01:000c: :/46

At this level, we can start to evaluate IPv6 addressing plan at school level.

**Type 1 schools**

Assuming the school being evaluated received the IP block space of 2401:dd01:0004: :/46.

At primary switch, it needs to divide the traffic into 3 separate subnets.

- Admin PCs + Server subnet
- Wi-Fi subnet
- Lab subnet

To allocate this, further 2 bits are required. Once past the primary switch, the address space would be: 2401:dd01:0004: :/48 - 2401:dd01:0007: :/48

With the 4 possible subnets being:

- 2401:dd01:0004: :/48 (Allocated for Wi-Fi subnetting)
- 2401:dd01:0005: :/48 (Allocated for Labs subnetting)
- 2401:dd01:0006: :/48 (Allocated for administrator subnetting)
- 2401:dd01:0007: :/48 (Unallocated address space for future expansions)

When we now evaluate the Wi-Fi subnet, assuming that the network requirement is that every access point manages its own subnet (this assumes that the network deployment requires isolation. This is not for network deployments with client roaming), given that type 1 schools can have 6 or greater number of access points, we will assume that these schools will not have more than 64 access points. Assuming for 64 access points, we would require 6 additional bits to cater to this requirement. Therefore, for each subnet revolving around an access point, it would have the address space of:

2401:dd01:0004:0000: :/54

With a range of address space as:

2401:dd01:0004:0000: :/54 - 2401:dd01:0004:fc00: :/54

With each subnet having an incremental address space as:

- 2401:dd01:0004:0000: :/54
- 2401:dd01:0004:0400: :/54
- 2401:dd01:0004:0800: :/54
- 2401:dd01:0004:0c00: :/54

This would conclude the Wi-Fi branch of the subnet tree for type 1 schools.

Considering the computer labs, given that the network requirement states that these schools will have 4 or more labs, if no school would have more than 16 labs per school, we will subnet for a maximum of 16 labs, which requires further 4 bits. This would allow each lab to have its own allocated IPv6 address space like: 2401:dd01:0005:0000: :/52

With a range of address space as:

2401:dd01:0005:0000: :/52 - 2401:dd01: 0005:f000: :/52

With each subnet having an incremental address space as:

- 2401:dd01:0005:0000: :/52
- 2401:dd01:0005:1000: :/52
- 2401:dd01:0005:2000: :/52
- 2401:dd01:0005:3000: :/52

This concludes the lab subnetting branch of the total subnetting tree for Type 1 schools.

Finally considering the administration subnetting, we could see 2 main segments. 1 segment is the server segment, of which the resources will be accessed from multiple nodes of the school network, and the other segment being the administrators-only PCs and network appliances. Assuming that there might be requirements later to expand the server with multiple servers, or a storage area network etc., it would be logical to put servers and other accessible data nodes into 1 subnet, and further isolate administration computers on another subnet. This would mean primarily splitting the total administration subnet address space into 2 segments as:

- 2401:dd01:0006:0000: :/49
- 2401:dd01:0006:8000: :/49

However, given there is a large address space remaining, we recommend that some more address spaces be made to tolerate sudden expansion needs and break the total administration subnet address space into at least 4 segments as shown below.

- 2401:dd01:0006:0000: :/50 (For servers)
- 2401:dd01:0006:4000: :/50 (For administrator private subnet)
- 2401:dd01:0006:8000: :/50 (Unallocated)
- 2401:dd01:0006:c000: :/50 (Unallocated)

This concludes the administration subnetting branch of the total subnet tree for type 1 schools.

Special Note: The 2401:dd01:0007: :/48 address space has been completely left unallocated to tolerate a need for sudden further expansions beyond the above-mentioned tolerances.

| NO | Description | VLAN Name | VLAN ID | IP Block |
|---|---|---|---|---|
| 01 | Labs | | 1100-2700 | 2401:dd01:0005: :/48 |
| | Lab 1 | Lab1 | 1100 | 2401:dd01:0005:0000: :/52 |
| | … | … | … | … |
| | Lab 16 | Lab16 | 2700 | 2401:dd01:0005:f000: :/52 |
| | | | | |
| 02 | Administrator | | 2800-2900 | 2401:dd01:0006: :/48 |
| | Server Subnet | ServerSubNet | 2800 | 2401:dd01:0006:0000: :/49 |
| | Admin Subnet | AdminSubNet | 2900 | 2401:dd01:0006:8000: :/49 |
| | | | | |
| 03 | Wi-Fi Subnet | | 3000-9300 | 2401:dd01:0004: :/48 |
| | Access Point 1 | AP_1 | 3000 | 2401:dd01:0004:0000: :/54 |
| | Access Point 2 | AP_2 | 3100 | 2401:dd01:0004:0400: :/54 |
| | …. | …. | …. | …. |
| | …. | …. | …. | …. |
| | Access Point 64 | AP_64 | 9300 | 2401:dd01:0004: fc00: :/54 |

*Table 1 : Type 1 School Network Address Plan*

**Type 2 schools**

Assume that the school being evaluated received the IP block space of 2401:dd01:0008: :/46.

At primary switch, it needs to divide the traffic into 3 separate subnets just like Type 1 layout.

- Admin PCs + Server subnet
- Wi-Fi subnet
- Lab subnet

To allocate this, further 2 bits are required. Once past the primary switch, the address space would be:

2401:dd01:0008: :/48 - 2401:dd01:000b: :/48

With the 4 possible subnets being:

- 2401:dd01:0008: :/48 (Allocated for Wi-Fi subnetting)
- 2401:dd01:0009: :/48 (Allocated for Labs subnetting)
- 2401:dd01:000a: :/48 (Allocated for administrator subnetting)
- 2401:dd01:000b: :/48 (Unallocated address space for future expansions)

When considering the Wi-Fi subnetting: the network requirements have mentioned that it will have at most 5 separate access points. If these access points will require its own subnet, we would require 3 bits to allocate up to 8 subnets, which could handle the requirement, which would give the address space segment range as:

2401:dd01:0008:0000: :/51 - 2401:dd01:0008:e000: :/51

In which a case, the 5 Wi-Fi per-access point subnet address spaces would be:

- 2401:dd01:0008:0000: :/51
- 2401:dd01:0008:2000: :/51
- 2401:dd01:0008:4000: :/51
- 2401:dd01:0008:6000: :/51
- 2401:dd01:0008:8000: :/51

This concludes the Wi-Fi branch of the subnet tree for type 2 schools.

Considering the computer labs, given that the network requirement states that these schools will have no more than 3 labs, we must allocate up to 4 subnets for labs, taking 2 more bits. This would allow each lab to have its own allocated IPv6 address space, which would range as:

2401:dd01:0009:0000: :/50 - 2401:dd01:0009:c000: :/50

Which provides the 3 labs with the following address spaces:

- 2401:dd01:0009:0000: :/50
- 2401:dd01:0009:4000: :/50
- 2401:dd01:0009:8000: :/50

This concludes the lab subnetting branch of the total subnetting tree for Type 2 schools.

Finally considering the administration subnetting, the same requirements and reasonings from Type 1 school layouts are valid here. Therefore, just as in Type 1 layout, although only 2 segments are needed, we recommend having the administration subnetting address space be divided into 4, in the following manner.

- 2401:dd01:000a:0000: :/50 (For servers)
- 2401:dd01:000a:4000: :/50 (For administrator private subnet)
- 2401:dd01:000a:8000: :/50 (Unallocated)
- 2401:dd01:000a:c000: :/50 (Unallocated)

This concludes the administrative subnet address space allocations.

Just as in Type 1 layouts, this too have a totally unallocated address space at the primary switch as: 2401:dd01:000b: :/48, which can be used for further unplanned expansions if need-be.

| NO | Description | VLAN Name | VLAN ID | IP Block |
|---|---|---|---|---|
| 01 | Labs | | 1100-1300 | 2401:dd01:0009: :/48 |
| | Lab 1 | Lab1 | 1100 | 2401:dd01:0009:0000: :/50 |
| | Lab 2 | Lab2 | 1200 | 2401:dd01:0009:4000: :/50 |
| | Lab 3 | Lab3 | 1300 | 2401:dd01:0009:8000: :/50 |
| | | | | |
| 02 | Administrator | | 1500-1600 | 2401:dd01:000a: :/48 |
| | Server Subnet | ServerSubNet | 1500 | 2401:dd01:000a:0000: :/50 |
| | Admin Subnet | AdminSubNet | 1600 | 2401:dd01:000a:4000: :/50 |
| | | | | |
| 03 | Wi-Fi Subnet | | 2000-2400 | 2401:dd01:0008: :/48 |
| | Access Point 1 | AP_1 | 2000 | 2401:dd01:0008:0000: :/51 |
| | Access Point 2 | AP_2 | 2100 | 2401:dd01:0008:2000: :/51 |
| | Access Point 3 | AP_3 | 2200 | 2401:dd01:0008:4000: :/51 |
| | Access Point 4 | AP_4 | 2300 | 2401:dd01:0008:6000: :/51 |
| | Access Point 5 | AP_5 | 2400 | 2401:dd01:0008:8000: :/51 |

*Table 2 : Type 2 School Network Address Plan*

**Type 3 schools**

Assume that the school being evaluated received the IP block space of 2401:dd01:000c: :/46.

In type 3 schools, the primary switch doubles as the switch used for the 1st lab. In this layout, there are no Wi-Fi connections, and there are no cache-engines or servers. There is 1 admin PC connected. Assuming that there might be a need to keep two or more PCs as admin PCs together with other admin-only network devices, we will assume that this will still require an admin-subnet. The lab-subnet requirement exists as always. Although technically 2 segments would be sufficient to fulfill this request, we will break it down to 4 segments to allow for future unplanned expansions.

The address space after the primary switch would be the following range:

2401:dd01:000c: :/48 - 2401:dd01:000f: :/48

Which would be divided as follows:

- 2401:dd01:000c: :/48 (Allocated for Labs subnetting)
- 2401:dd01:000d: :/48(Allocated for Administrator subnetting)
- 2401:dd01:000e: :/48 (Unallocated)
- 2401:dd01:000f: :/48 (Unallocated)

Considering the lab subnetting allocations, the network requirement says that the school could have 1 or more labs. However, given the schools would have less than 500 students, it is logical that there would be no more than 8 labs in total in such a school, requiring us to use 3 more bits. Therefore, we can further divide the lab subnet address space into 8 segments, to give the following range: 2401:dd01:000c:0000: :/51 - 2401:dd01:000c:e000: :/51

With the addresses being:

- 2401:dd01:000c:0000: :/51
- 2401:dd01:000c:2000: :/51
- 2401:dd01:000c:4000: :/51
- 2401:dd01:000c:6000: :/51
- 2401:dd01:000c:8000: :/51
- 2401:dd01:000c:a000: :/51
- 2401:dd01:000c:c000: :/51
- 2401:dd01:000c:e000: :/51

This would conclude the lab subnetting branch of the subnet tree for Type 3 school layouts.

Considering the administrator subnetting address space, although currently it is only being used for only 1 purpose, to make the network tolerant against unplanned expansions, we would break that address space into 4 segments as well. Giving the address space of:

2401:dd01:000d:0000: :/50 - 2401:dd01:000d:c000: :/50

Where each segment would be listed as below.

- 2401:dd01:000a:0000: :/50 (For administrator private subnet)
- 2401:dd01:000a:4000: :/50 (Unallocated)
- 2401:dd01:000a:8000: :/50 (Unallocated)
- 2401:dd01:000a:c000: :/50 (Unallocated)

This concludes the administrator subnetting for type 3 schools.

For unexpected future expansions, we have kept in reserve, the 2 complete address spaces of:

- 2401:dd01:000e: :/48
- 2401:dd01:000f: :/48

| NO | Description | VLAN Name | VLAN ID | IP Block |
|---|---|---|---|---|
| 01 | Labs | | 1100-1400 | 2401:dd01:000c: :/48 |
| | Lab 1 | Lab1 | 1100 | 2401:dd01:000c:0000: :/51 |
| | Lab 2 | Lab2 | 1200 | 2401:dd01:000c:2000: :/51 |
| | Lab 3 | Lab3 | 1300 | 2401:dd01:000c:4000: :/51 |
| | Lab 4 | Lab4 | 1400 | 2401:dd01:000c:6000: :/51 |
| | | | | |
| 02 | Administrator | | 1500 | 2401:dd01:000d: :/48 |
| | Admin Subnet | AdminSubNet | 1500 | 2401:dd01:000a:0000: :/50 |

*Table 3 : Type 3 School Network Address Plan*

**Task d)**

All major considerations with regards to design of the networks have already been discussed under task a, b, & c.

With regards to Cisco Packet Tracer implementation specific details identified:

- We have used 2 lab computers to represent the 41 lab computers that are supposed to be present in the lab in the real-world scenario, to make the program run smoother and for the process to look neater.
- Cisco packet tracer has many hardware limitations. In example, it is missing 10 port and 48 port switches. In a full-scale simulation in cisco packet tracer where 41 computers were needed to be connected, the only available option would be to use 2x 24 port switches (such as the available 2960-24TT) in forced-stack configuration.
- VLAN map needed to be implemented as specified in the above tables.

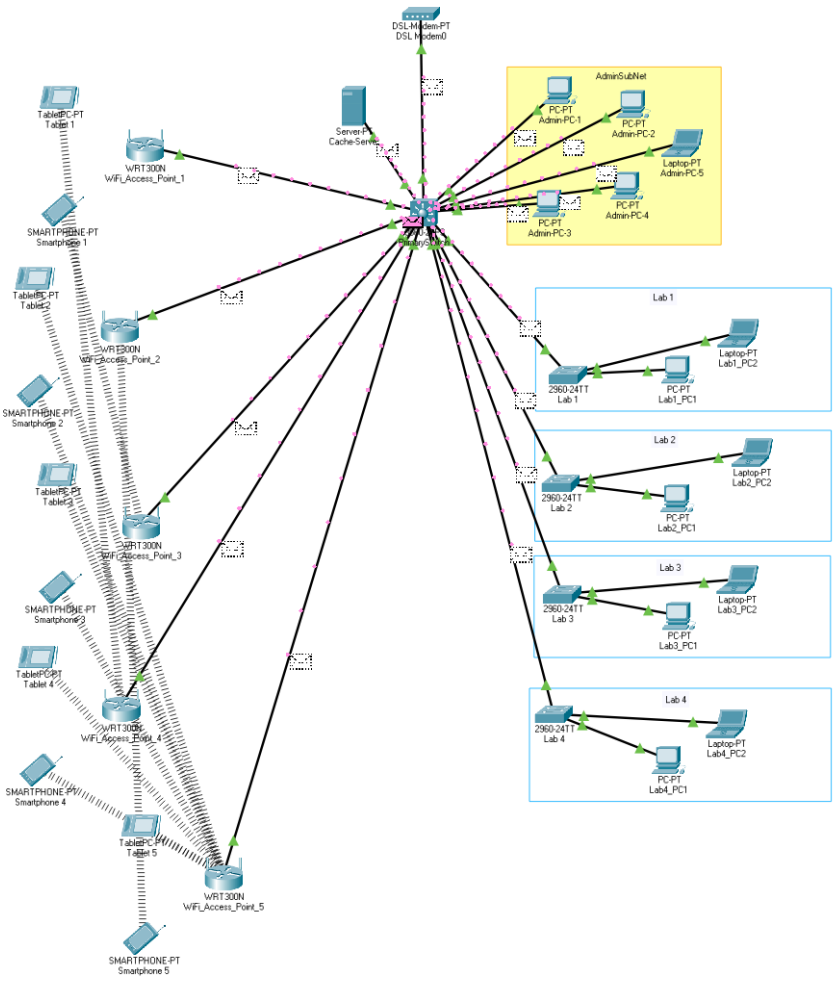


*Figure 4: Type 1 School Implemented on CPT*

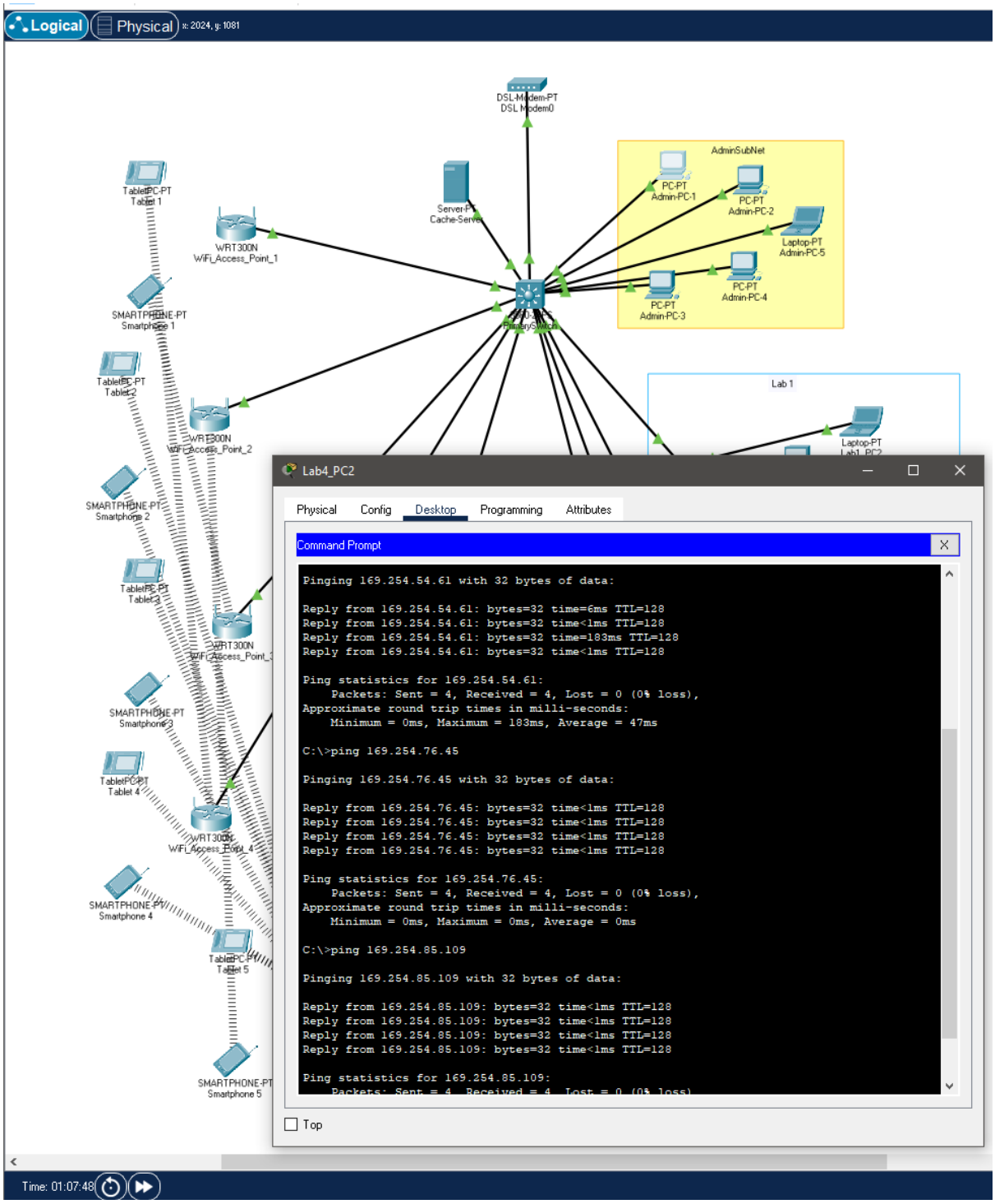


*Figure 5: ping tests to multiple nodes and cache server*

**Task e)**

If we are to assume that all the connections finally go through a central ISP hosted facility, multiple security concerns arise.

**Identified issues.**

First and foremost, the risk for data confidentiality occurs. Given that all the data goes through unsafe channels, and ends up at 1 center, someone who is at the center could launch either an active or a passive attack, such as a man-in-the-middle attack or a simple eavesdropping attack, respectively. The risk of a full-network-wide malware propagation and infection is also extremely high, especially considering the scenario where the malware was injected at the ISP host facility. There is also a major risk of network availability being lost if the ISP host facility goes down. To add to potential issues, given it is an ISP hosted facility, where many different services also run, sometimes on the same servers, there is also a risk of remote eavesdropping or reverse terminal and similar scenarios.

**Solutions.**

1) To protect against data getting caught in an active or passive attack, it is recommended that a technology such as IPsec be used. For this scenario, implementing IPsec at ESP (Encapsulating Security Payload) mode is sufficient to minimize overhead, as school-level traffic would not contain sensitive information in the packet headers such as source or destination. However, if security requirements do demand it, IPsec under tunnel mode can be implemented.
    - Implementation: The modems we have recommended for all 3 layouts fully support end-node VPN deployments. Therefore, the hardware already included in the layouts would be sufficient to provide this needed element of security once configured. (However, it is crucial to figure out if the ISP hosted facility also supports this feature.)

2) To protect against the whole network becoming infested with malware if a single or multiple nodes become compromised, it is extremely important to deploy Intrusion Detection and Prevention Systems (IDPS) on the network.
    - Implementation:
        i. The modems we have recommended for all 3 layouts fully support advanced filtering features in its built-in firewall system. But this system on its own is not sufficient to protect against more complex malware attacks. Therefore, for Type 3 schools where no sensitive/important data is being stored, the modem-alone solution with proper configurations may be sufficient. However, for Type 1 and 2 schools, another solution may be needed.
        ii. For type 1 and 2 solutions, a complete security solution is recommended. A system such as a Cisco ASA 5506-X which supports FirePOWER services would serve as a great solution for this problem. This should be placed between the modem and the primary (core) switch of the school to ensure no external threats would reach the internal networks.
3) To protect against data unavailability, this needs to be negotiated with the ISP host. The network deployment team must ensure that suitable number of fall-back/fail-over options have also been rented out under contract from ISP, and that the network traffic is being handled through some system which is connected in real time with another site's server which is available to automatically take over in case a disaster in the main site occurs. This implementation needs to occur from ISP side, so we need to make sure the contract that will be signed with the host facility includes these features. (Similar to a stretched cluster setup with witnesses in VMWare VCenter etc.)
4) To protect against false authentication, physical monitoring of school network nodes should be done, specially if some suspicious behaviour is noted. Additionally, roles need to be implemented to restrict certain clearance levels from accessing certain functions or requesting certain sites etc. Any physical security challenge (such as passwords, pins etc.) must be complex to protect against dictionary or brute force attacks.
5) To protect against loss of integrity during transport: an IPsec implementation in tunnelling mode should provide sufficient security against this matter. The protocol's inherit ability to clearly authenticate its source and the message clearly achieves the desired security. Implementation of this has been explained under "Solutions 1)".

**Task f)**

**Summary of proposal requirements**

If the whole network is to be monitored and managed through a single control center at the ministry, it needs to have a certain set of objectives to achieve through this deployment, added benefits to the system and the network, as well as an inherit support with how the school system had been managed over the years (divided by Geographical boundaries or by educational zones/divisions etc.) so that the computer systems can be easily managed and integrated with currently gathered data on other management facilities.

**Potential added features/benefits:**

- Ability to unicast, multicast or broadcast certain messages to schools.
- Ability to group schools and manage them according to the standard educational zones and divisions as schools had been managed for the past decades in Sri Lanka.
- Ability to quickly note (if) broken school networks/systems and quickly respond.

**Content of plan:**

- Fault management and tolerance:
    - Detect any network going under (breaking down)
    - Log the failures, and events leading up to failure.
    - Dispatch repair teams to investigate and correct failures.
- Performance monitoring:
    - To monitor network usage levels from schools, log against date of month/week, and time of day to collect statistical data on usage.
    - Remote internal network health testing
- Security management:
    - Remote control and shutdowns of compromised networks
    - Communicate within the network of any potential malware propagation through utilizing an IDPS (Intrusion Detection and Prevention System).
    - Remote reconfigurations of firewalls of networks to adapt them to latest & complex threats.
- Configuration management:
    - Remotely configure internal networks
    - Remotely configure IDS, IPS, Firewalls and other hardware/software.
    - Track which devices are on the managed network.

## Bibliography

Chennai Cisco, 2019. *How to Configure Ip address to PC and Routers in Packet Tracer.* [Online]
Available at: https://www.chennaicisco.com/2013/10/how-to-configure-ip-address-to-pc-and.html
[Accessed 24 04 2021].

CISCO, 2021. *Cisco 350X Series Stackable Managed Switches.* [Online]
Available at: https://www.cisco.com/c/en/us/products/switches/350x-series-stackable-managed-switches/compare-model.html
[Accessed 27 04 2021].

CISCO, 2021. *Cisco 900 Series Integrated Services Routers.* [Online]
Available at: https://www.cisco.com/c/en/us/products/routers/900-series-integrated-services-routers-isr/index.html?ccid=cc001532
[Accessed 26 04 2021].

CISCO, 2021. *Cisco Firepower 1000 Series.* [Online]
Available at: https://www.cisco.com/c/en/us/products/security/firepower-1000-series/index.html?ccid=cc001536
[Accessed 26 04 2021].

CISCO, 2021. *Compare the 2800 Series models.* [Online]
Available at: https://www.cisco.com/c/en/us/products/wireless/aironet-2800-series-access-points/index.html?ccid=cc001530#~benefits
[Accessed 27 04 2021].

ComputerNetworkingNotes, 2014. *Basic Switch Configuration Guide with Examples.* [Online]
Available at: https://www.computernetworkingnotes.com/ccna-study-guide/basic-switch-configuration-guide-with-examples.html
[Accessed 19 04 2021].

## About Author

**Personal Quote**

*"You'll never get what you want if you don't pursue it. If you don't ask, you'll always get a no. If you don't move forward, you remain stationary."*

## Who Is GPDCM Jayasekara?

"My name is GPDCM Jayasekara, I consider myself an optimistic & creative individual who has passion in the field of computer networks & automation & hope to create a difference in the industry. I am a smart and diligent collaborator who enjoys exceeding targets. I am also enthusiastic and willing to learn new things that would challenge me both personally and academically, which would help me be a better version of myself.

## Personal Objective

To carve a niche for myself as a professional in the computer network industry with a reputed and well-managed organization where my potential is utilized to the fullest, thereby leading to the growth of both the organization as well as my career in the organization. Further, I'm interested in pursuing higher studies in computer security in which I can help improve my knowledge for the betterment of the organization and our society.

# END REPORT