Networking Capstone Project

Rawan Amr Abdelsattar

2B

Content

Introduction

As a networking and cybersecurity specialized student, I was asked to propose a network design for WE School applying the knowledge and skills acquired through the whole year taking into considerations the best design practices and information systems infrastructure design industry standards and to come up with the optimal solutions to satisfy the requirements of WE School and its stakeholders and allow normal processes and operations.

In the next sections I am going to demonstrate my design in terms of soft and hard planning, covering all the necessary details. The report will mention in-depth technical details and will also include an executive summary for the c-level managers and the non-technical stakeholders concerned.

Network Purpose and Needs Assessment

1. Purpose

The main target of the school network is to enable 250 students and 20 staff to access online learning platforms simultaneously. High-speed internet is required for video classes, secure access to online resources.

2. User Requirements

As mentioned in the previous section, WE School's network serves 250 students and 20 staff. It is a must to consider while designing the network layout and the IP addressing scheme.

In addition to these numbers of users, a reasonable number should be added for further expansion or growth in the network to be considered to ensure the network's design resilience and network scalability.

3. Functional Requirements

WE School's Network should be able to handle user traffic to and from the internet. The network must be divided into departments. It should also enable communication between departments on a role-based basis. The network must also handle authentication requests

for the domain. Monitoring the network's system events, security events, and performance is necessary. The network should be capable of handling network and end devices that do not have power cables. Devices should receive network configuration as soon as they connect to the network. To improve network performance, broadcast storms should be eliminated. Also, devices should be connected to the internet as soon as they plug in the cable without delay.

4. Technical Requirements

To meet the functional requirements, technical requirements include the implementation of some networking concepts, protocols and network industry standards, the following are some of them: VLANs configuration, InterVLAN routing for VLAN communication, OSPF, Active Directory, SIEM solution implementation, PoE support, DHCP, RPVST+, PortFast and BPDUguard.

5. Design Considerations

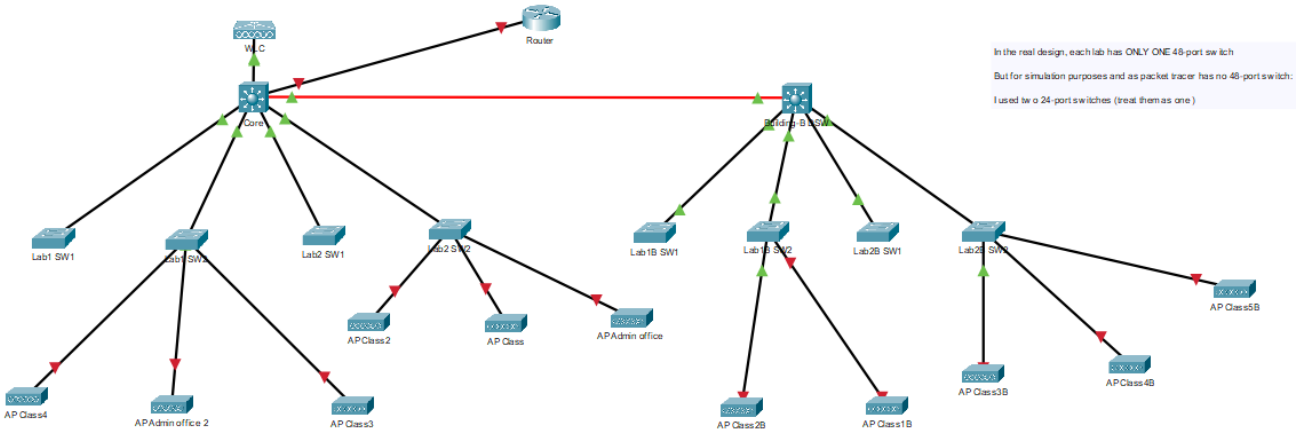
For WE School's network design some concepts are considered during each part of the report to ensure optimal network performance and satisfy stakeholders' needs.

These include high availability, security, scalability, flexibility, and cost-effectiveness.

Soft Planning

1. Logical Layout

As for the logical layout, provided below is a network diagram demonstrating the logical flow of data in the school's network:



Note: In the real-world design, each lab has ONLY ONE 48-port switch. But for simulation purposes and as packet tracer has no 48-port switch I used two 24-port switches (treat them as one)

2. IP Addressing Scheme

For the IP addressing scheme, the network will be divided into VLANs for each role of the roles of the different stakeholders where each VLAN lies in a separate subnet for isolation for security and to optimize the performance of the network. DHCP is configured on the Core Switch.

The following table demonstrates the IP addressing scheme for the WE School's network:

VLAN		Network ID	IP Address Range		No. Of Usable Add.
No.	Name		First Usable	Last Usable	
10	Students	10.10.10.0 /23	10.10.10.1(gateway)	10.10.11.254	510
20	Staff	10.10.20.0 /25	10.10.20.1 (gateway)	10.10.20.126	126
30	Admin-Staff	10.10.30.0 /27	10.10.30.1 (gateway)	10.10.30.30	30
40	Guests	10.10.40.0 /24	10.10.40.1 (gateway)	10.10.40.254	254
50	IT-admins	10.10.50.0 /28	10.10.50.1 (gateway)	10.10.50.14	14
699	Native (mgmt)	10.10.60.0 /24	10.10.60.1 (gateway)	10.10.60.254	254

Device (Hostname)	IP Address
Core	**Int VLAN 699:** 10.10.60.2 **Int VLAN 10:** 10.10.10.2 **Int VLAN 20:** 10.10.20.2 **Int VLAN 30:** 10.10.30.2 **Int VLAN 40:** 10.10.40.2 **Int VLAN 50:** 10.10.50.2
DSW- Building-B	**Int VLAN 699:** 10.10.60.3
Lab1-SW	**Int VLAN 699:** 10.10.60.4
Lab2-SW	**Int VLAN 699:** 10.10.60.5
Lab1B-SW	**Int VLAN 699:** 10.10.60.6
Lab2B-SW	**Int VLAN 699:** 10.10.60.7
WLC	**Int VLAN 699:** 10.10.60.1

At least one port in each class, lab, workshop is for instructor devices and assigned to Staff VLAN. The rest of the ports in labs are assigned to the Students VLAN and the library's ports also. Ports in Admin offices are assigned to the Admin-Staff VLAN.

3. Network Segmentation

To apply adequate network segmentation within our network, a 3-tier network architecture is preferred. Network will be segmented into three layers which are: access layer, distribution layer and the core.

We have two buildings with 4 labs, 9 classes, 2 admin offices, a workshop, a library, and a control room. Each building will have a

distribution switch forming the distribution layer. Each lab will have an access switch forming the access layer and connected to the building's distribution switch. The control room in Building A will have a core switch connecting these distribution switches, along with other connections to the core switch.

This is visually demonstrated in the network's logical layout as shown in the previous sections.

In addition, the network will be further segmented into multiple VLANs to further apply security measures, improve the overall network's performance, and make management an easier task.

This is also demonstrated in the table in the **"Network's IP addressing scheme"** section.

4. Security Planning

To ensure the confidentiality, integrity and availability of the network, information security measures must be considered. This should be kept in mind starting from the design phase, it is often easier and more efficient to implement security measures and best practices during the implementation of the network design itself, as leaving it to the end may make things get more complex and may also require changes in the design or the layout of the network

and/or the configuration, and may cause problems that will be harder to troubleshoot.

To implement security in WE School's network, I suggest implementing the following solutions and practices:

- **Security Practices:** security must be considered through both the design and the implementation of the network:

  - native vlan is changed from default VLAN to vlan 699 and is NOT routable

  - strongly encrypted passwords for WLANs,

  - Portfast and BPDUGuard enabled on access ports

  - Switches and Router have a username-secret combination of "admin", "N3t@dmin2024" respectively for enable mode, console and vty lines.

  - An ACL is used to isolate guest VLAN from the other VLANs.

  - Training and effective communication of security policies to stakeholders to increase the level of awareness.

- **Network Firewall:** for Standard firewall capabilities like stateful inspection, Integrated intrusion prevention, Application awareness and control to see and block risky apps, Threat intelligence sources, Upgrade paths to include

future information feeds, Techniques to address evolving security threats.

- **Host-based Firewall:** to run on individual user devices and filter incoming and outgoing traffic. This can help secure the network from the spread of malware in case one machine is infected.

- **Antivirus or Anti-malware Software:** to ensure endpoint protection against malicious software.

- **Active Directory Domain Services AD DS:** to give the means to control access to network resources, apply security policies and for effective network management.

- **WSUS Server:** Windows Server Update Service, **WSUS**, plays a significant role in the network as it regularly searches for updates, downloads them, and pushes them to network devices. This ensures latest updates are automatically downloaded and improves network performance as it reduces network traffic and saves network bandwidth by downloading updates only once on the server instead of each individual device downloading its own copy of the update.

- **Simple SIEM Solution:** A Security Information and event management solution can be used to aggregate log and event data, threat intelligence, and security alerts to provide actionable insight on potential security events. Open-source solutions could be used to be cost-effective and do basic functions.

5. Budgeting

Item	Type	Item Count	Unit Price	Total
El Sewedy - CAT6 UTP Computer Cable - 305 m	Cabling	19	13,333 EGP	253327 EGP
Cisco C9105AXI-E	Access Point	11	18029.34 EGP	198322.74 EGP
Catalyst 9800-L	WLC	1	75648.20 EGP	75648.20 EGP
C9200L-48T-4G-E	Core Switch	2	126,750.83 EGP	253501.66 EGP
C1300-48FP-4G	Access Switch	4	82239.42 EGP	328957.68 EGP
Fortinet FG-40F	Firewall	1	30853.34 EGP	30853.34 EGP
Total Budget				1140610.62 EGP

The Rest of the Budget is reserved for purchasing a server, software solutions licenses, maintenance or future expansions.

Hard planning

1. Physical Layout

For WE School's network, the physical layout (where every device is located) is as follows:

- The **Server**, **Router**, **firewall**, **core switch** and Building A's distribution switch are all placed in the main rack in the control room in building A.
- **Access switches** of each lab are in that lab's rack.
- An **Access point** is on classes' and Admin offices' ceiling.
- **Desktop computers** are placed in labs, one for the instructor in each class, one in the workshop, 4 in each admin office and 3 in the library.
- **Cabling** is discussed in the next sections.
- A **Printer** is placed in each admin office.
- A **smart screen** in each class, lab, and workshop.
- A Security **CCTV camera** is in each lab, workshop, and corridor (as a future upgrade, not currently available).

2. Control Room Location

The location of the control room is considered a design constraint as it has already been decided. It will be placed on the ground floor of building A.

3. Planning for cable runs

To plan for cable runs there are two main ways to run cable through the two buildings based on the type of room:

- **In labs:** raised floor for adequate cabling and to handle the dense of network cables along with power cables for Labs' desktop computers and other nodes

- **In classes, admin offices, workshop, library:** overhead cabling (placing cables over the ceiling floor tiles) can be acceptable and can be implemented using tools like cable pulling tools

4. Switches selections

The following table demonstrates the selection of switches and where they are going to be placed.

Switch Model	Room/Rack	Some Notes (or Features)
C9200L-48T-4G-E	• Building A Control Room • Building B Lab 1B	
C1300-48FP-4G	• Building A Lab 1, Lab2 • Building B Lab 1B, Lab 2B	

5. Router (Will be provided by WE company- using a dedicated Fiber Line)

As for the router, this is also considered a design constraint as it will be provided by the company “WE” so we should take into consideration that the other network devices should be compatible with the router. Also, some features and protocols may or may not be supported by that router, so reviewing its datasheet will be useful as well before making further decisions regarding them.

6. Wi-Fi Connections

In WE school’s network, Wireless connectivity is needed as students have their school tablets and may sometimes use their own laptops. Instructors and other staff need to use their own devices like mobile phones or laptops.

To provide wireless connectivity, an access points AP should be placed in each class/admin office, labs have wired connections to the workstations, so no APs are needed.

I recommend using a Wireless LAN Controller WLC since we have various APs throughout the two buildings to manage wireless network APs that allow wireless devices to connect to the network.

I also recommend using the 2.4GHz band as a better choice that will provide good coverage and good bandwidth since the distance

between rooms is relatively large on non-interfering channels to avoid interference as we have multiple access points in place.

The Design includes 5 WLANs for 5 VLANs which are Students, Staff, Admin-Staff, Guests, and IT-Admins:

VLAN	SSID	Passphrase
10	Students	stud@2024
20	Staff	staff@2024
30	Admin-Staff	adstaff@2024
40	Guests	guests@2024
50	IT-Admins	itadmins@2024

Note: passwords here are for demonstration purposes (to be used in pkt file only), more complex passphrases should be used in real world implementation.

7. Implementation Plan Timeline

Here is the implementation plan step by step within the three-month timeframe, I divided the implementation process into three phases forming the overall timeline:

- **Phase 1:** Planning and Purchasement
- **Phase 2:** Implementation
- **Phase 3:** Testing and Optimization

Next is the in-detail implementation plan timeline (can also be used as a checklist):

Phase	Week	Task	Detailed Checklist
Phase 1: Planning and Purchasement	Week 1	Planning	- Assess the building to ensure the already finished design is sufficient - Design the Active Directory structure for user and device management.
	Weeks 2-3	Purchasement	- Purchase network devices including switches, routers, access points, and PoE injectors, as necessary. - Procure licenses for required software solutions such as SIEM.
Phase 2: Implementation	Weeks 1-2	Installation	- Install network racks, cable trays, and run cables according to planned topology. - Physically install switches, routers, access points, and PoE injectors.
	Weeks 3-6	Configuration	- Configure VLANs, InterVLAN routing. - Set up Active Directory for user authentication and centralized management. - Deploy DHCP services for IP address assignment. - Enable PoE on switches for powering devices.

			- Configure RPVST+. - Implement PortFast and BPDUguard for enhanced network stability and security.
Phase 3: Testing and Optimization	Weeks 1-2	Network Testing	- Verify VLAN configurations, inter-VLAN communication. - Validate Active Directory integration and DHCP services. - Ensure PoE support and RPVST+ configuration is functioning correctly. - Test PortFast and BPDUguard configurations for network stability and security.
	Week 3	Network Optimization	- Tune configurations for optimal performance and address any identified issues - Document the final network configuration and topology. - Provide training for staff on network management and troubleshooting.