4CC523 - NETWORKING FUNDAMENTALS

Local Area Network Design

Network design proposal for Derwent College

Konstantinos Bazoukis
k.bazoukis@mc-class.gr

1. Introduction and Requirements of the Report

This report aims to cover a network installation for a new three-floor building at Derwent College - School of Computing. The main plan involves a LAN design that will be able to endure for the next five to seven years but will also be able to provide the means for any future upgrades.

The hardware of the network will consist of a number of dedicated servers and will also provide directory services and database services. The LAN will be resilient and secure with the ability to handle high traffic loads and support voice and video communications. Moreover, it will be cost effective and upgradable to cater for more users.

The school consists of 4 departments: The staff, general and administrative, where each member of both departments will have their own computer and connection to a printer and the servers, but the admin staff will be using a shared printer; The technicians, where all of its members will have their own computer and access to all networks but also access to a large and secure storeroom that exist in their area; And 6 Computing Laboratories.

Each department will be logically separated with the use of different subnets that will also provide the necessary isolation so that some departments will have limited access to others. A wireless network will also be available to provide access to the Internet to anyone from anywhere within the campus but will separate access from guests to lecturers and students by using proper security.

Remaining Sections

- Proposed Design
    1. Cabling and connectivity
    2. Logical Topology
    3. Device selection and placement
- IP Addressing
    1. IP addressing scheme
    2. Subnetting benefits
    3. IP address LAN allocation
- Summary
- References

2. Proposed Design

For the current plan, a two-tier collapsed core hierarchical network model is proposed because it offers the same benefits as a three-tier design such as modularity, which facilitates scalability, isolation through subnetting, which improves resiliency and reduced cost, as it provides the functions of the core and distribution layer in single device.

2.1 Cabling and connectivity

The whole network utilizes wired connectivity and offers restricted wireless connectivity for those who want to bring their own devices. While wireless connectivity is easier to setup, manage and maintain, it is not suggested in the enterprise area due to the many disadvantages that comes with it, such as high security risks and much slower speeds from wired ones due to wireless signals being affected from walls, floors or other electronics(Evans 2013).

In order to keep an organized and well-planned cabling system at the main distribution core, the network follows a structural cabling standard such as the EIA/TIA-568, where it suggests colored cables with appropriate labeling and patch panels for easy management. The cables travel from rack to rack via overhead cable pathways and with the use of vertical and horizontal cable managers at the sides of the racks end up to their corresponding device while keeping an organized cabling environment. This structured approach offers a reliable, scalable and manageable cabling infrastructure (Brocade, 2007).

The types of cables for the network are chosen based on the types of the devices that will be used for, as well as the layer that those devices exist in the hierarchical model. At the core layer, the cable of choice is the CAT6 STP straight-through that is made of copper, is shielded to protect from various interferences and supports 10GBase gigabit speeds within distances of 55 meters. For intermediary devices and hosts the cable of choice is the CAT5e UTP crossover which is widely used with fast ethernet connections but it also supports 1gigabit connections. Other alternatives are the CAT7 copper cable that supports 10GBase connections up to 100 meters and fiber optic cable that support various standards with different modes based on its wavelength, and distances up 40 kilometers. However, for the current plan these alternatives are cost-inefficient and redundant since that the chosen cables can already provide the required resiliency and scalability (Partsenidis, 2016).

The table below shows the categories of cables and the differences between them.

CABLE	DATA RATE	DISTANCE	APPLICATION
CAT5e	Up to 1Gbps	100 meters	Fast Ethernet (Hosts, Intermediary devices)
CAT6	Up to 10Gbps	55 meters	10Gigabit Ethernet Backbone - medium-sized campuses
CAT7	Up to 10Gbps	100 meters	10Gigabit Ethernet Backbone -large-sized campuses
Fiber Optic	Up to 10Gbps	40 kilometers (single mode)	10Gigabit Ethernet Large enterprises – industrial

2.2 Logical Topology

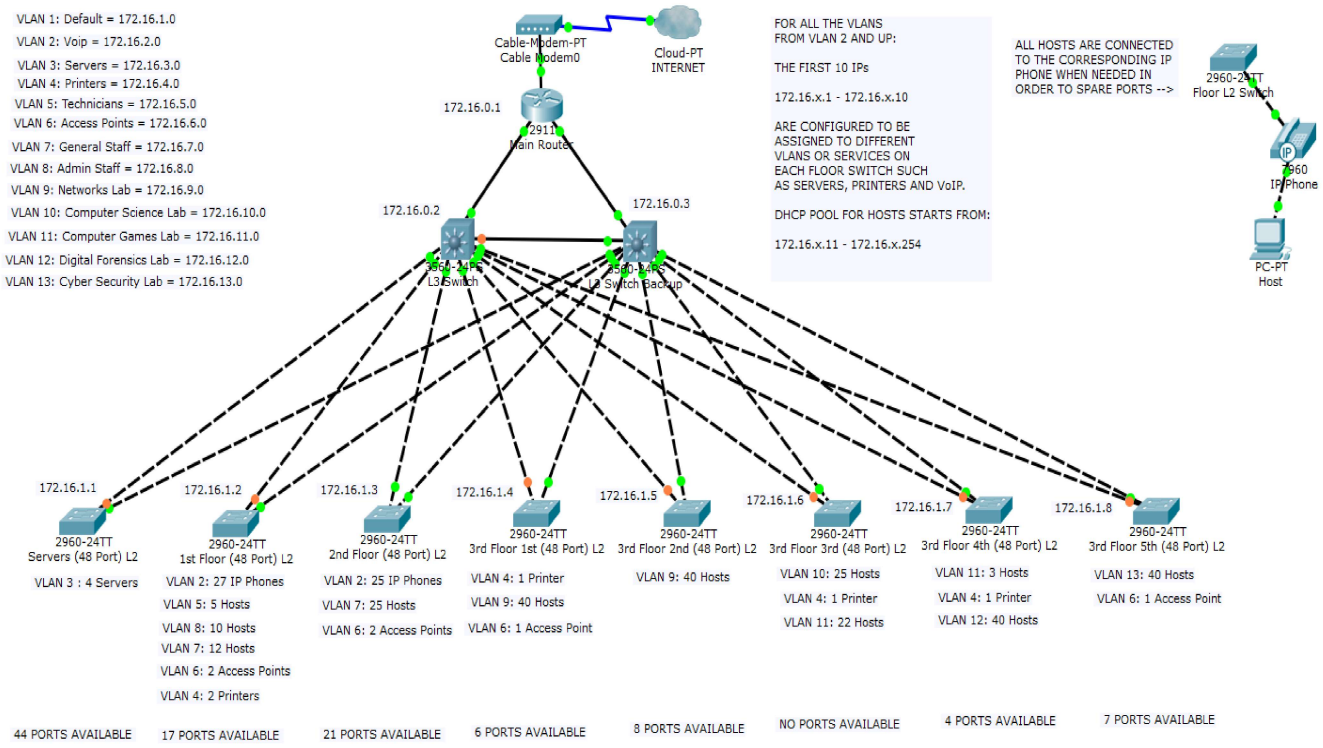

Figure 1 Logical topology Diagram

Figure 1 shows the IP addressing of the floor switches and the vlans that belong to each one of these.

2.2.1 Physical Topology

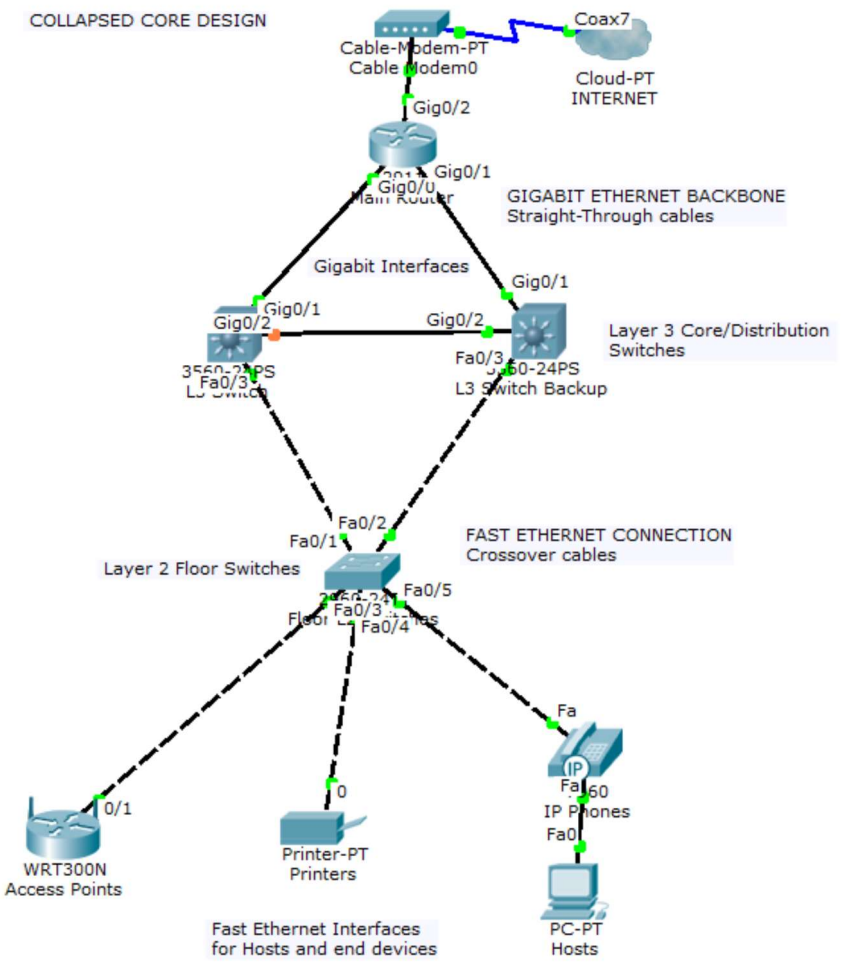

Figure 1.1 Physical topology Diagram

Figure 1.1 shows the main concept of the physical topology to be implemented throughout the network.

2.2.2 Physical Topology - Firewalls

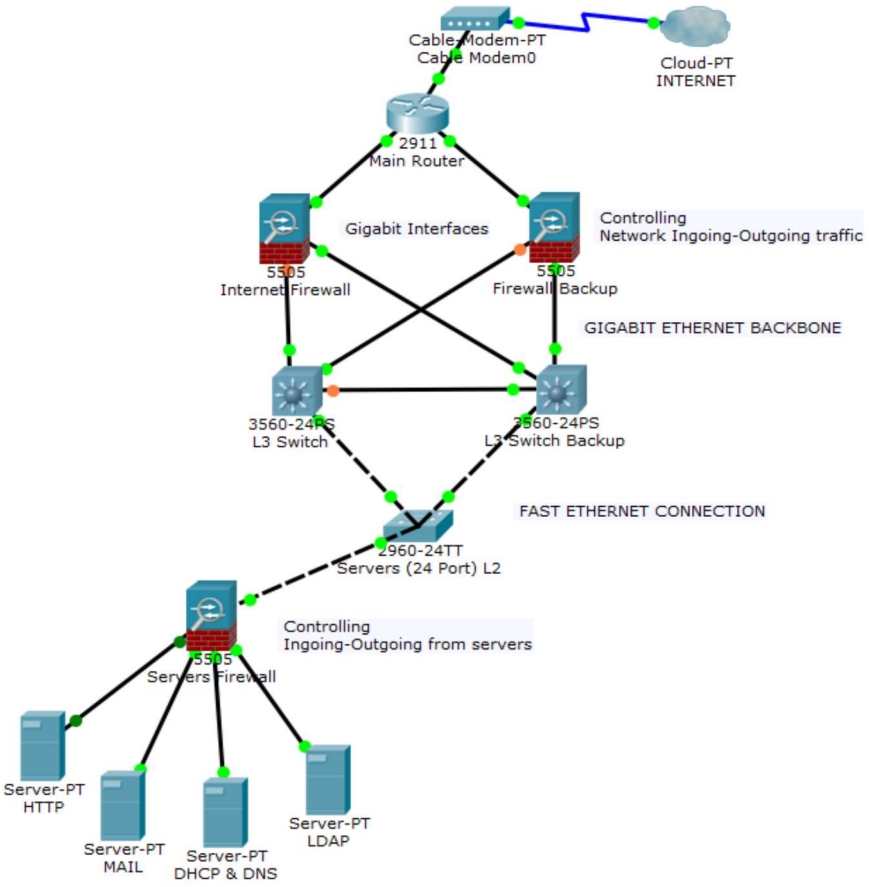

Figure 1.2 - Firewalls

Figure 1.2 shows the placement of firewalls for the servers as well as for accessing the Internet.

2.3 Device selection and placement

The devices are chosen based on the hierarchical model that is going to be implemented. At the core, a router operates as the default gateway and route the traffic in and outside of the network. At this point two firewalls control ingoing and outgoing traffic for security purposes as depicted in figure 1.2. Next, two, fixed configuration, fully managed, Layer 3 switches with 48 ports and stackable functionality, operate as backbone. Both switches and firewalls, are coupled for redundancy. The backbone of the network is placed at the large storeroom that exists in the technician's area depicted on figure 2 for security and protection reasons.

The chosen switches are the most optimal for this plan because they offer full configuration features such as, protection over DDNS attacks, Quality of Service and the ability to create Virtual LANs(vlans) but they are also stackable, which they could be a number of switches

operating as one. Alternative options were the modular switches, which offer the best flexibility but are the most expensive, standalone, which are configured individually, or unmanaged, which are not offering any configuration (Diedricks, 2014).

Next on the hierarchy are 8 L2 switches with 48 ports, that are placed on each floor based on the number of end devices, as well as 6 wireless access points, 2 for each floor. Specifically, 2 switches are placed on the technician's room, one for the servers and the other one for providing connection to all the other hosts and devices on the floor, including the two access points. Another one is used on the second floor at the large staff room as depicted in figure 3, that provides connection to all the hosts at this floor and the other two access points and the remaining 5 switches are placed on the third floor in a circular placement starting from the networks to the cyber security lab as depicted in figure 4 in order to connect all the hosts and devices as well as the remaining 2 access points.

The number of L2 switches is chosen and placed in such way because of the implementation of vlans which reduces the number of required switches compared to regular subnetting, as it allows each port to operate as a separate subnet. The number of 6 access points is chosen for increased availability at any place of the campus and they are placed on each floor at high positions at the aisles at the left and the right side of the stairs. The access points are configured with unique SSIDs and WPA2 security measurements so that every authorized person will be able to login to securely to their corresponding depart but guests will only have limited traffic-controlled access to the Internet.

The remaining devices in the topology are: the network printers in each department, one for each lab, one for the technicians and one shared for the admin staff. The IP phones that provide VoIP and exist at the staff's rooms, both admin and general, and the technician's departments. Lastly, there are the servers at the technician's area which are four, a HTTP, a MAIL, a DHCP & DNS, and a LDAP for directory services and a firewall to secure the servers.

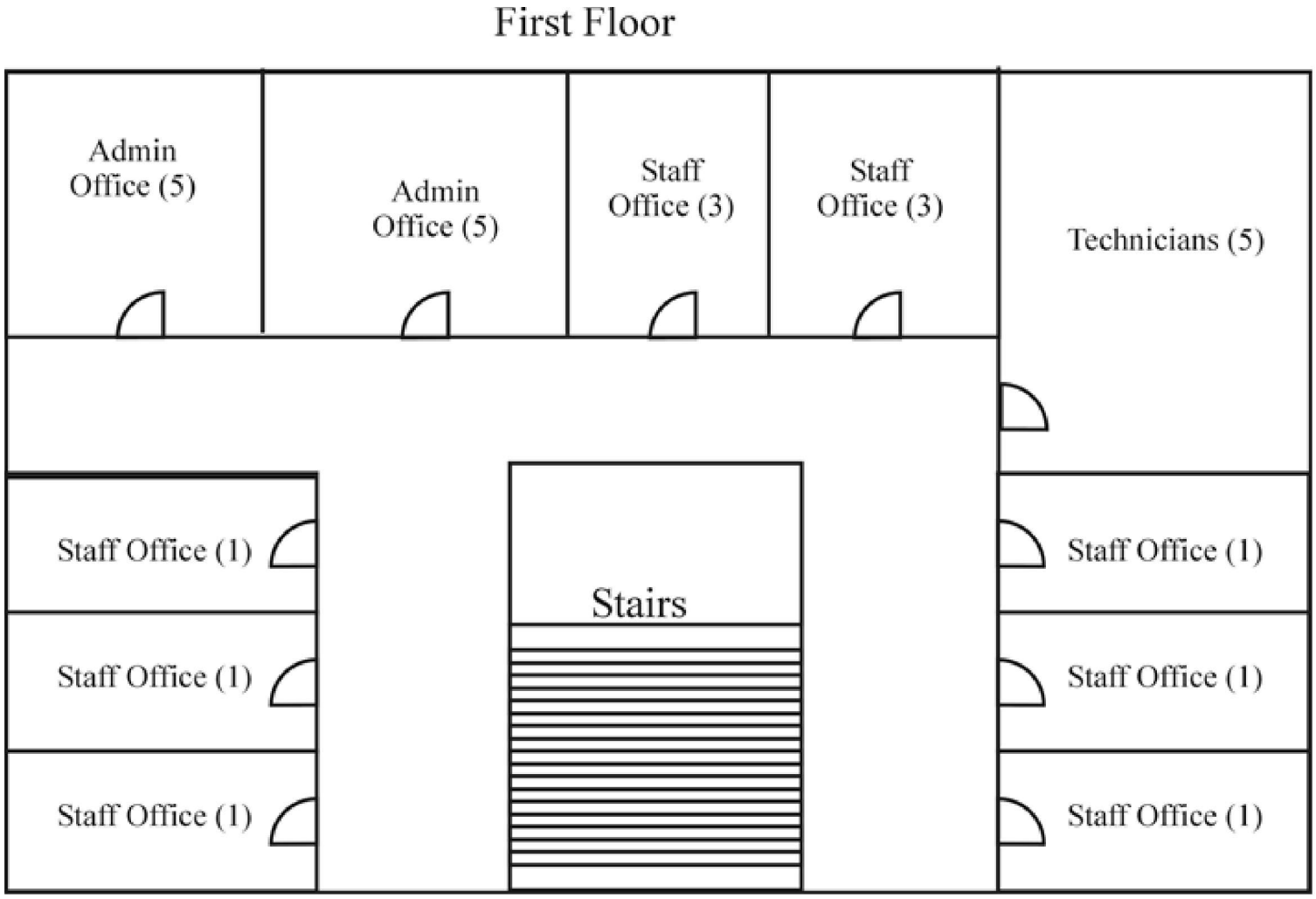

Figure 2 Physical topology diagram for first floor

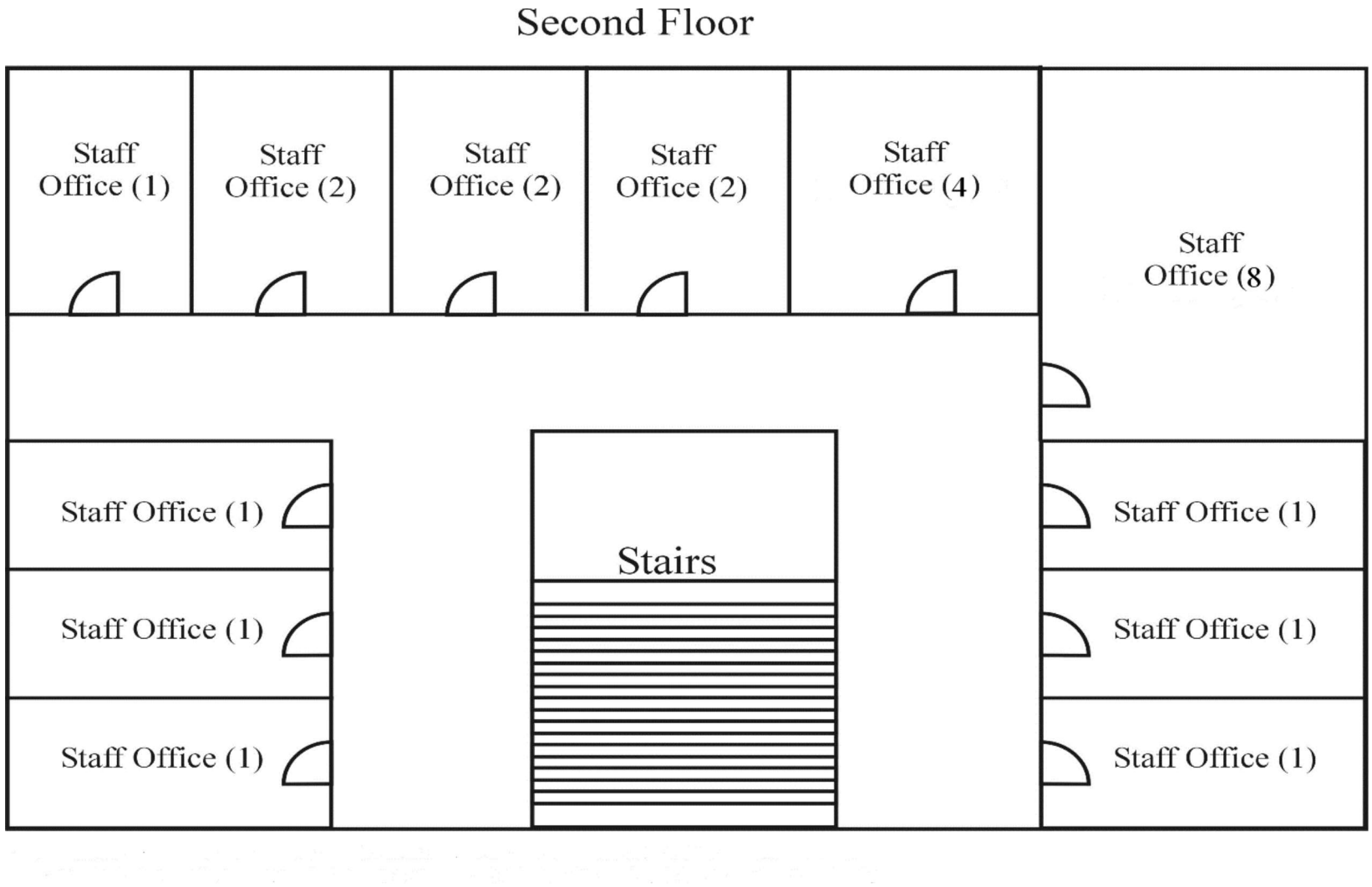

Figure 3 Physical topology diagram for second floor

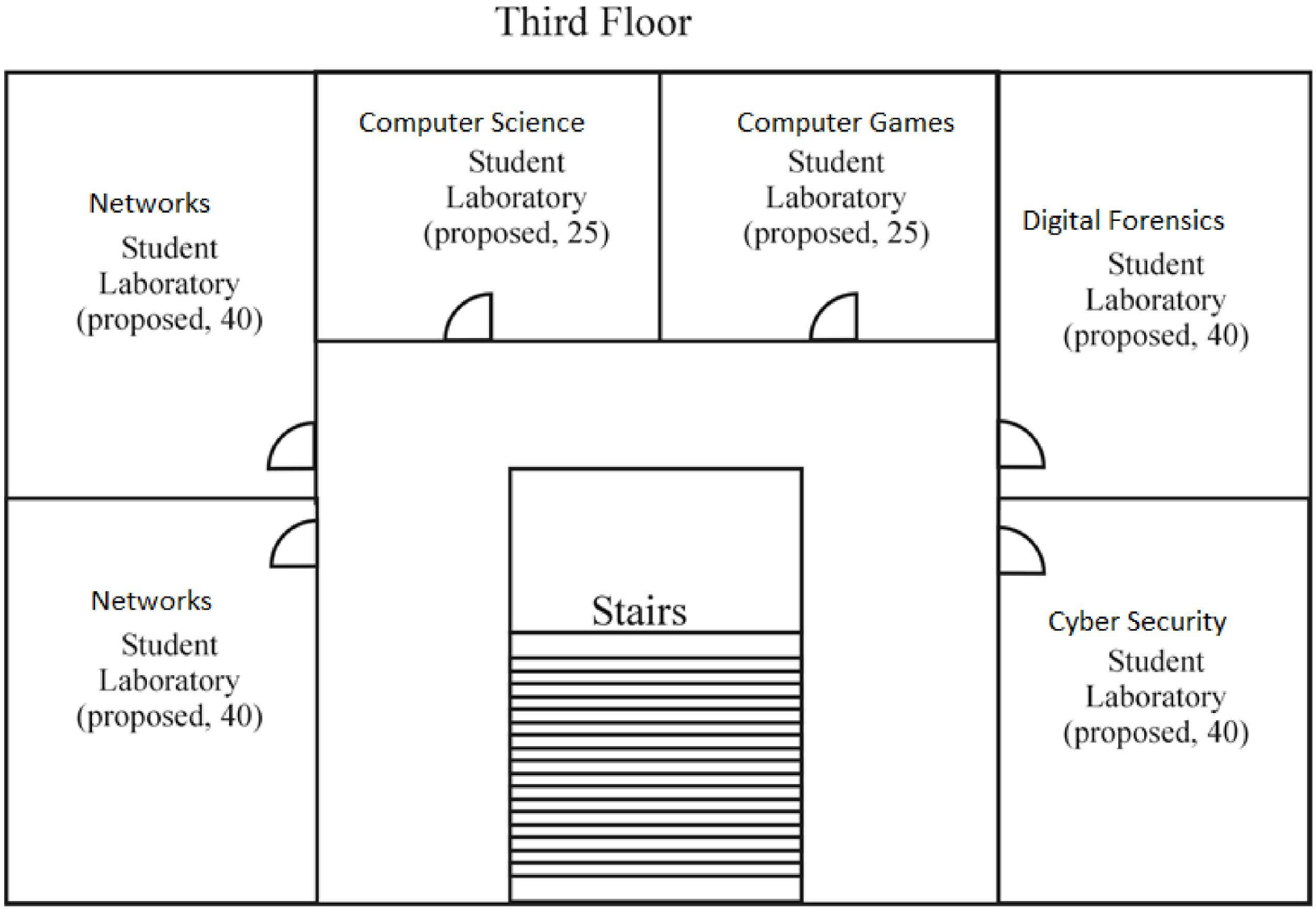

Figure 4 Physical topology diagram for third floor

3. IP Addressing

3.1 IP addressing scheme

The given IP address 172.16.0.0 with subnet mask 255.255.240.0 provides a total of 16 subnets with 4094 available hosts for each subnet. However, the number of these hosts is very large and redundant. In order to minimize the number of hosts the subnet mask is moved 4 bits and thus giving the IP 172.16.0.0 with subnet mask 255.255.255.0. With this subnet mask a total of 16 subnets is available but the number of hosts is reduced to 254 per subnet. At the table below the IP addressing of all the departments is depicted.

Department	Number of hosts	Network Address	Broadcast address	First Usable Address	Last Usable Address	Subnet mask
Guest wireless access	**200**	**172.16.6.0**	**172.16.6.255**	**172.16.6.1**	**172.16.6.254**	**255.255.255.0**
Networks labs	**200**	**172.16.9.0**	**172.16.9.255**	**172.16.9.1**	**172.16.9.254**	**255.255.255.0**
General staff offices	**200**	**172.16.7.0**	**172.16.7.255**	**172.16.7.1**	**172.16.7.254**	**255.255.255.0**
Digital forensics lab	**180**	**172.16.13.0**	**172.16.13.255**	**172.16.13.1**	**172.16.13.254**	**255.255.255.0**
Cyber security lab	**220**	**172.16.12.0**	**172.16.12.255**	**172.16.12.1**	**172.16.12.254**	**255.255.255.0**
Admin	**150**	**172.16.8.0**	**172.16.8.255**	**172.16.8.1**	**172.16.8.254**	**255.255.255.0**
Computer games lab	**170**	**172.16.11.0**	**172.16.11.255**	**172.16.11.1**	**172.16.11.254**	**255.255.255.0**
Computer science lab	**190**	**172.16.10.0**	**172.16.10.255**	**172.16.10.1**	**172.16.10.254**	**255.255.255.0**
Technicians	**130**	**172.16.5.0**	**172.16.5.255**	**172.16.5.1**	**172.16.5.254**	**255.255.255.0**

3.2 Subnetting benefits

By moving the bits on the given IP, the number of available hosts is reduced and the number of broadcast packets that will be sent. This provides network performance and speed because it limits the traffic to a single subnet but also increases security. Even more flexibility is provided by using vlans because compared to basic subnetting implementation, the number of the switches needed is limited to individual ports. This implementation increases security even more but also keeps costs lower because the number of switches is reduced.

3.3 IP address LAN allocation

In the current IP allocation scheme, all the devices belong to separate vlans. The first one begins with the IP address 172.16.1.0 which is assigned dynamically via DHCP servers to the L2 floor switches and each port of these switches has a separate vlan from numbers 5 and up. The vlans 2-4 with the IPs 172.16.2.0 – 172.16.4.0 are assigned to the voIP, servers and printers respectively as depicted in figure 1. All the vlans are configured accordingly with the right ports so that they can get IPs from the DHCP server and have as first usable IP for hosts the 172.16.x.11. The reason for this configuration is to allow each vlan in any floor switch to assign an IP from 2 to 10 for accessing the servers, the printers and voIP services and the first IP 172.16.x.1 in each vlan, as the default gateway.

4. Summary

The proposed design analyzed in this report provides the necessary means to cover for the requirements of the campus. The collapsed core design, combined with the appropriate structural cabling and connectivity, provides a Gigabit network that is cost-effective and resilient for the next five to seven years but also easily upgradable with the use of stackable L3 switches. Moreover, the LAN is secure logically, as a combination of firewalls, vlans and secure wireless access points is implemented but also physically with the backbone installed in a secured area. Finally, with the chosen IP addressing scheme and the wireless availability on each floor, scalability and availability is also ensured.

5. References

Brocade (2007). 'Best Practices Guide: Cabling the Data Center', *Brocade.com* [Online]. Available from: https://www.brocade.com/content/dam/common/documents/content-types/product-design-guide/cabling-best-practices-ga-bp-036-02.pdf [Accessed: 7 APR 2017].

Diedricks, I. (2014). 'Understanding the different types of Ethernet Switches', *blogs.cisco.com* [Online]. Available from: http://blogs.cisco.com/smallbusiness/understanding-the-different-types-of-ethernet-switches [Accessed: 7 APR 2017].

Evans, S. (2013). 'Wired vs wireless in the enterprise', *computerweekly.com* [Online]. Available from: http://www.computerweekly.com/feature/Wired-vs-wireless-in-the-enterprise [Accessed: 7 APR 2017].

Partsenidis, C. (2016). 'Essential network cabling tips for your infrastructure', *searchnetworking.techtarget.com* [Online]. Available from: http://searchnetworking.techtarget.com/tutorial/Ten-cabling-tips-in-10-minutes [Accessed: 7 APR 2017].