19141230

OXFORD BROOKES UNIVERSITY

LAB 1B

COMP7002 – MODERN COMPUTER SYSTEMS

Table of Contents

[Labelled Network Topology 2](#_Toc167030621)

[Equipment 4](#_Toc167030622)

[Subnetting 6](#_Toc167030623)

[Medical Departments Subnet 7](#_Toc167030624)

[Visitors Subnet 7](#_Toc167030625)

[Medical Equipment Subnet 8](#_Toc167030626)

[Server Subnet 9](#_Toc167030627)

[Modularity and Logic of the Network Design 9](#_Toc167030628)

[WAP Wireless Access Points for guest users 11](#_Toc167030629)

[Security 11](#_Toc167030630)

[Transmission Medium Speed 11](#_Toc167030631)

# Labelled Network Topology

***Figure 1*** *Logical Network Topology Diagram for a Hospital*

***A diagram of a computer network

Description automatically generated***

***Figure 2*** *Physical Network Topology Diagram for Both Floors in a Hospital*

A computer diagram with many different computer components

Description automatically generated with medium confidence

**Figure 2** Physical View of Main Wiring Closet

A computer server with green wires

Description automatically generated with medium confidence

# Equipment

**Table 1** *Networking Equipment*

|  |  |  |
| --- | --- | --- |
|  | **Room/s** | **Networking Equipment** |
| **GROUND FLOOR** | Reception | 2x PCs  IP phone  Wireless-Access-Point  Copper wall-mount  Straight-through cables |
| 6 GP Chambers | 6x PCs  6x IP phones  2x Copper wall-mounts  Straight-through cables |
| 2 Health Care Assistant Rooms | 2x PCs  2x IP phones  Copper wall-mount  Straight-through cables |
| Infrastructure Room | 2x copper patch panels  5x 2960 Department switches  3650 24 PS First floor distribution switch  3560 24 PS Ground floor distribution switch  4x Servers  Straight-through cables  4x Switch-Switch cross-over cables  Tablet  Home Gateway |
| **FIRST FLOOR** | 2 Operating Theatres | 2x IP phones  2x PCs  2x IoT – Temperature Monitors  2x IoT – LED Surgical Lights  Copper wall-mount  Straight-through cables |
| Scanning Room | IP phone  PC  IoT – Electromagnetic Siren  IoT – Electromagnetic Shielding Door  Copper wall-mount  Straight-through cables |
| Meeting Room | IP phone  PC  Wireless-Access-Point  IoT – Speaker  IoT – Webcam  Copper wall-mount  Straight-through cables |
| Remote Appointment/Diagnosis Room | IP Phone  PC  IoT – Webcam  IoT - Speaker  Copper wall-mount  Straight-through cables |
| Nurse Station | IP phone  6x PCs  Wireless-Access-Point  2x Copper wall mounts  Straight-through cables |
| Customer Cafeteria | IP phone  Wireless-Access-Point |

Subnetting

**Table 2** *IPv4 Address Subnetting for Hospital Network Users – (Class B prefix ‘LA’)*

A screenshot of a computer

Description automatically generated

**Table 3** *IPv4 Addresses*

A table with numbers and symbols

Description automatically generated

## Medical Departments Subnet

Assuming that the medical departments handling medical-related functions require regular communication between the same cluster of devices, a shared subnet would be appropriate for them. This segregation of sensitive data and devices from various parts of the network permits administrators to implement strict access controls and monitor the network traffic with more ease. Furthermore, this promotes scalability of the network infrastructure as subnetting reduces disrupting other areas of the network.

## Visitors Subnet

Creating a dedicated subnet for hospital visitors in the waiting area and cafeteria, isolates guest traffic from the internal hospital network. This can reduce network-wide threats by preventing unauthorised guest access to sensitive hospital resources and data. Similarly, subnetting helps in managing bandwidth usage, as administrators can decide which network resources will take priority to provide critical hospital services.

## Medical Equipment Subnet

**Image 1** *Hospital Gateway for Monitoring and Isolating Equipment A screenshot of a computer

Description automatically generated*

Additionally, a third subnet dedicated to IoT medical equipment/devices ensures that the high speed and low latency demands of these devices are met, without being disrupted by other network traffic, and vice versa. A Hospital Gateway was created to isolate and monitor sensitive IoT and medical equipment from general network traffic.

Image 1 displays the tablet’s interface which monitors the status of the hospital’s equipment. The live status information can be accessed through entering 141.130.64.1 on the tablet’s web browser URL, or, via selecting the tablet’s IoT Monitor app and using username and password “admin” to login.

Using the Hospital Gateway removes the limitation of expensive and time consuming cabling as these devices are networked wirelessly. To challenge some security threats, the PSK passphrase on the Hospital Gateway ensures that only authorised users/hosts are able to access the gateway and data transmitted over the network are maintained encrypted. This helps safeguard patient confidentiality and the integrity of data transmitted between IoT equipment and the gateway. Lastly, the Hospital Gateway implements DHCP which automatically assigns and provides IP addresses through TCP/IP and other communication parameters to end/client devices connected to the network. Manual assignment of IP addresses of IoT devices would be time-consuming and impractical in a dynamic hospital environment. DHCP accommodates flexibly changes in the network topology making it suitable to evolving network requirements.

## Server Subnet

Similarly, a subnet that isolates servers can mitigate security breaches and accelerates resolution times. Confining server-related problems to a dedicated subnet means that troubleshooting can be done efficiently, without affecting other parts of the network.

# Modularity and Logic of the Network Design

The hierarchical hospital network comprises of 3 different layers to optimise performance, ensure network availability and facilitate scalability. At the *Access Level Layer* switches (model 2960 24TT) serve the Nurse, Specialists (operating theatres and scanning room), Diagnosis and Business departments. The Specialists Department switch concerned with the Diagnosis room and Meeting room devices use the gigabit ports to connect end devices with it. These switches provide high bandwidth and minimal latency, enhancing the performance of video-calls (by using gigabit ports). Because of this, the networked equipment from the operating theatres and scanning rooms should not disrupt/delay communications in the first floor.

Coversely, the Ground Floor department utilises a cost-effective 3560 24PS switch, which provides fast ethernet connections to the GP chambers’, reception’s and health care assistants’ offices. The single switch handles the mixed traffic from the ground floor offices as these share similar networking requirements.

Separate subnets are assigned for the ground floor (141.130.1.0/24) and the first floor (141.130.2.0/24). This segmentations is combined with VLANs and Access Control Lists, to ensure secure and organised network management. Visitor Wi-Fi is provided via a Wireless Access Point connected to the Ground Floor switch and isolated in its own subnet (141.130.3.0/24) to prevent interference with internal hospital traffic.

In the physical view, the limitation of distance and disturbing cabling was dealt by inserting copper patch panels, where PC devices required access to fast. The copper patch panels in the main wiring closet connect with the copper wall mount connections of the ground and first floor rooms, allowing for organised cabling.

Fast gigabit physical guided media were used at the distribution points and e-diagnosis rooms as it required fast transmission of media.

For the IP telephones, copper straight through cables were used. Gigabit ports were used to network the Diagnosis department’s devices and Meeting room as these required fast media transmissions with minimal noise and collision.

At the *Distribution Level Layer* the 3650 24PS switch provides gigabit Ethernet for the cluster of departments on the first floor. This is necessary to ensure that the E-Diagnosis, Meeting, Scanning rooms and Operating theatres obtain superfast connectivity with minimal collisions and enhanced throughput. Consistent use of gigabit physical media (notably in the Diagnosis and Meeting rooms) ensures high bandwidth and fast communication, preventing delays in video calls and BOYD connections.

At the *Core* (or collapsed-core) Level Layer a switch provides centralised server access. It maintains the data received by both floors switches in its identical state and forwards it to the 2960 24TT switch, which identifies the destination address and sends the request to the designated server, relaying the information back to the client. There are four servers in total, – one for visitors, administration staff, medical teams and business/corporate staff –, this is to maintain the organisation’s data secure and organised based on the hospital’s various services.

The core-switch is adequate for handling the network traffic while providing secure connectivity to the servers. Switches are used to allow multiple devices connect to and share a single computer network. Additionally, three-tier hierarchical design optimises performance, network availability, and the ability to scaling network designs.

Due to similarities with the star topology it could be said that the network resembles a tree topology.

## WAP Wireless Access Points for guest users

WAPs are placed in the reception and the cafeteria to enable BOYD connection; a WEP Key, permits Wi-Fi access to guests through entering the correct password “abc0123456”.

Similarly, for staff members in the like in the nurse department a StaffGateway was created with password “0123456abc” to enable BOYD access for staff members.

## Security

By configuring the smart switches, suspicious arp requests (to find mac address, layer 2) from potential attackers will be rejected as a router would be assigned to reply to arp requests from sourcers attempting to find external posts.

The security of each host has been optimised through setting encrypted passwords for both global configuration mode (password cisco) and priviledge EXEC mode (password class).

***Table 2: Switch Passwords***

|  |  |
| --- | --- |
| **Console/User** | cisco |
| **Privileged EXEC Mode** | class |

# Transmission Medium Speed

Several Department-Department, Department-PC and PC-PC pings verified that a connection between host devices within the network was successfully established. There was zero losses and minimal latency (see images below).

The remote appointment/diagnosis room ensures high broadband and superfast by connecting it’s devices through the copper wall-mount that links the patch panel with the gigabit port of the diagnosis switch. This ensure’s that this particular department room functions comparably faster.

**Image 1** *PC-PC ping*

A screenshot of a computer program

Description automatically generated

**Image 2** *PC-Switch ping*

A screenshot of a computer program

Description automatically generated

**Image 3** *Switch-Switch ping*

A screenshot of a computer

Description automatically generated

Word Count: 1,153