

Alex Lang and Daniel Otter

CS 4220

4/30/25

## Cisco Project Report

This project simulates a theoretical network for a local hospital in New Orleans, Louisiana, in need of a proper network with given specifications. This team has been instructed to include several services, make sure it is plenty secure, and follows all HIPAA regulations. To begin, the physical part of the network shows a map of the city the hospital is located in and an image of the hospital to which the network belongs. Once after clicking on the hospital, you can see the specified different areas of the hospital needed for its daily operations (several patient rooms, emergency rooms, radiology departments, offices, etc). When switching to the logical view, all the logic of the network is shown. In the top left, the 2 main networks are shown (guest network and the main network), both having a different purpose (one anyone can log into and the other for crucial hospital operations, image 1). The hospital's main network supports 3 different departments (facilities/maintenance, IT support, and the billing department, see image 2). Each of these departments have their own switches, as well as 2 PCs for their operations. All of these switches are connected to a singular Layer 3 switch so they're all connected together. Like these departments, all of the different rooms provided in the physical layer of this project also have their own switches and PCs. When it comes to data backups, there is a backup server implemented/configured to use a default gateway of 172.16.1.1 and a subnet mask of 255.255.255.0 with all of the PCs configured to send information to that default gateway when necessary (shown in image 3). Regarding firewalls/IDS, there is a TCP firewall added to the hospital main networks router as well as the PC connected to it (shown in image 4). As the main protocol that must be followed by this network is HIPAA, this network uses PHI (all information is encrypted, consistently monitored by the IT team/sys admins, and uses network segmentation). When it comes to the IP addressing, the public IP address is 203.0.113.1 and the internal IP address is 172.16.1.254, and then the private IP ranges from 172.16.(2-12.1-2). The range of 2-12 indicates which department is represented and can easily be extended when/if other departments need to be added (IP addressing is shown in image 5). Finally, for the network

segmentation, there are already 2 separate LANs, therefore it did not need to be further segmented using VLANs.

Images:

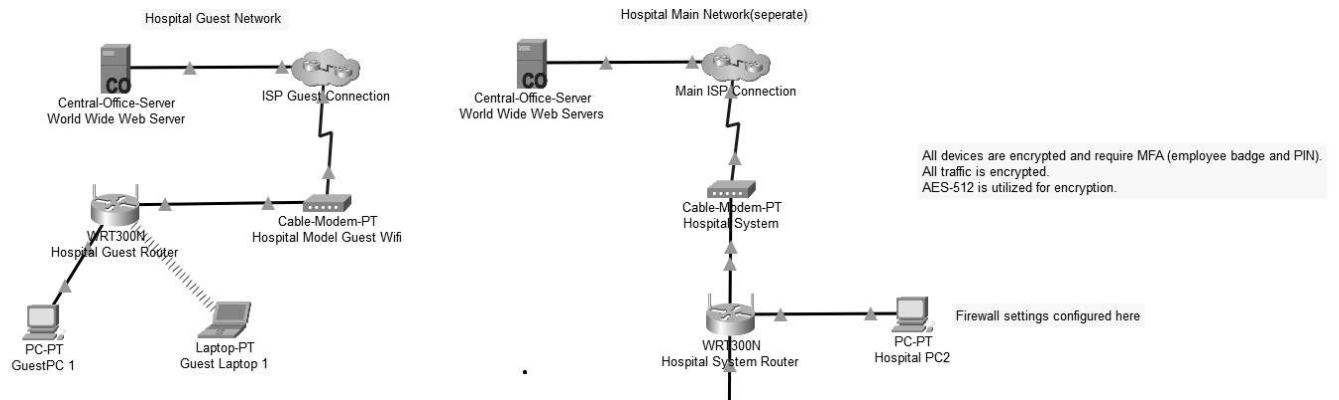


Image 1

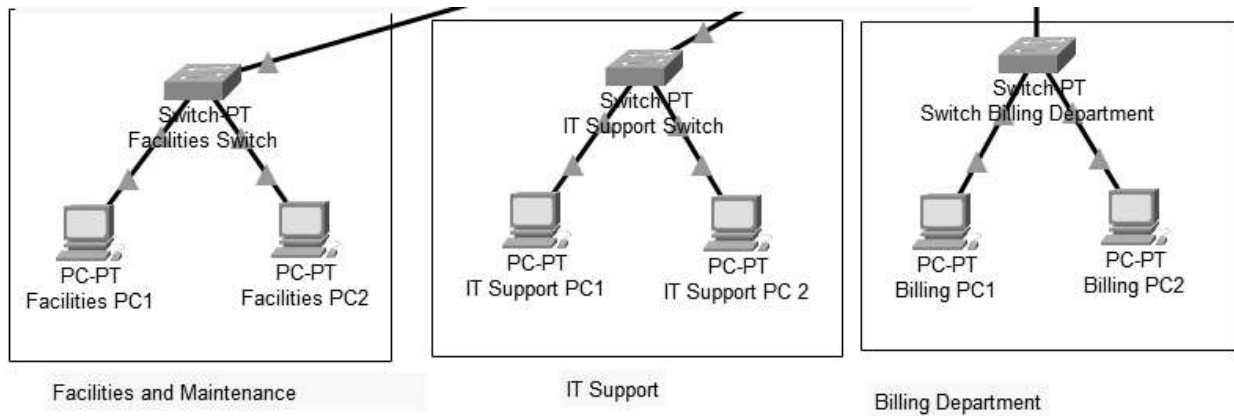


Image 2

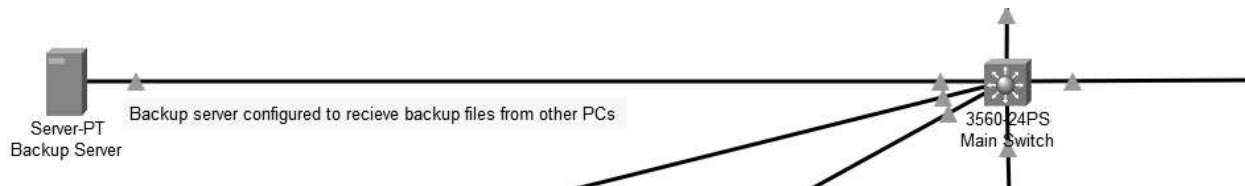


Image 3

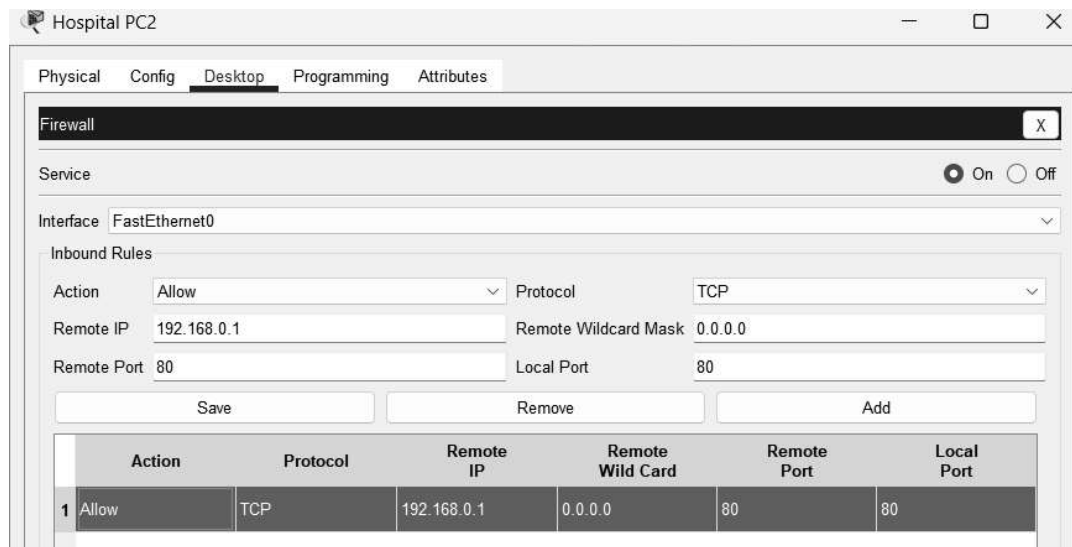
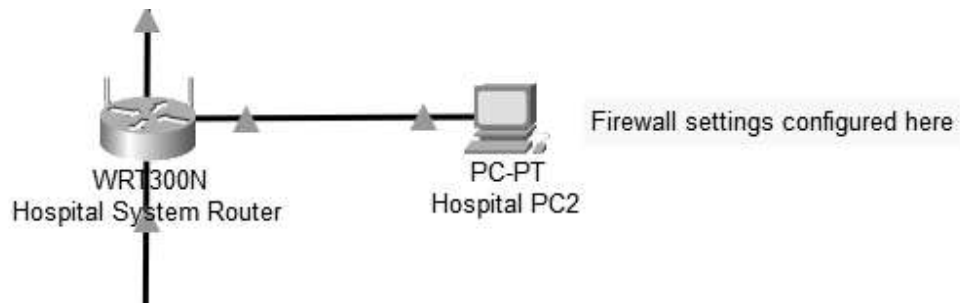


Image 4

Internet IP Address: 203 . 0 . 113 . 1

Subnet Mask: 255 . 255 . 0 . 0

Default Gateway: 192 . 168 . 0 . 1

DNS 1: 0 . 0 . 0 . 0

DNS 2 (Optional): 0 . 0 . 0 . 0

DNS 3 (Optional): 0 . 0 . 0 . 0

Host Name:

Domain Name:

MTU: Size: 1500

---

IP Address: 172 . 16 . 1 . 254

Subnet Mask: 255.255.255.0

DHCP Server: ☒ Enabled ☐ Disabled DHCP Reservation

Start IP Address: 172.16.1. 100

Maximum number of Users: 50

IP Address Range: 172.16.1. 100 - 149

Client Lease Time: 0 minutes (0 means one day)

Static DNS 1: 0 . 0 . 0 . 0

Static DNS 2: 0 . 0 . 0 . 0

Static DNS 3: 0 . 0 . 0 . 0

WINS: 0 . 0 . 0 . 0

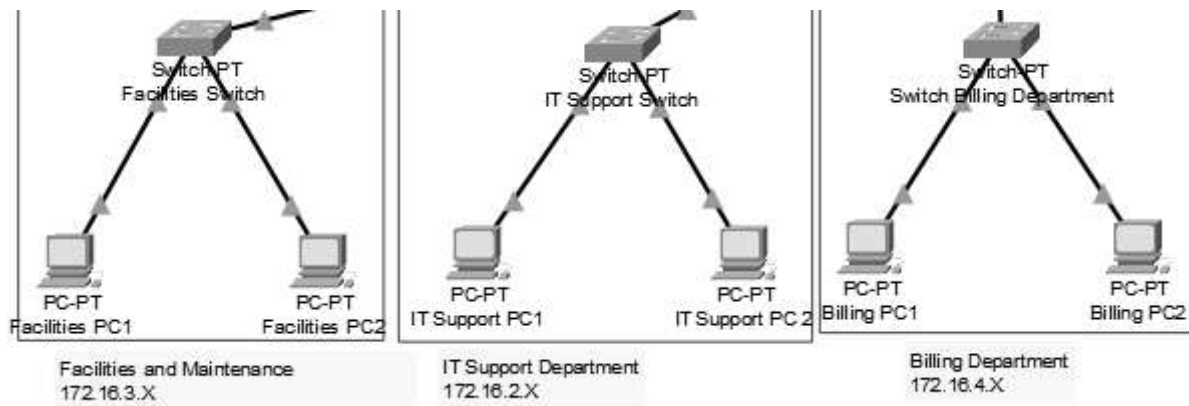


Image 5

References:

(OCR), O. for C. R. (2024, December 30). *Summary of the HIPAA security rule*. HHS.gov.  
<https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html>

Lincke, S. (2015). *Security planning*. New York, NY: Springer International.

Saunders, M. (2022, November 30). Security in Network Design: Key Considerations from a Network Architect's Perspective. *Cisco Blogs*. April 22, 2025,  
<https://blogs.cisco.com/learning/security-in-network-design-key-considerations-from-a-network-architect>

Cisco. (n.d.). *Getting started with Cisco Packet Tracer*. Cisco Networking Academy: Learn Cybersecurity, Python & More. <https://www.netacad.com/courses/getting-started-cisco-packet-tracer?courseLang=en-US>