IT Infrastructure Project: Kyle Stevens Hospital

Kyle M. Stevens

Liberty University

BMIS-520

Michael Hart

April 17, 2022

Table of Contents

[Section 1: Introduction 3](#_Toc101013480)

[Section 2: Carrier-Class Performance 4](#_Toc101013481)

[Section 3: Flexibility and Scalability 5](#_Toc101013482)

[Section 4: End-to-End Security 6](#_Toc101013483)

[Section 5: Operational Simplicity 6](#_Toc101013484)

[Section 6: Total Cost of Ownership 7](#_Toc101013485)

[Section 7: Design Explanation 8](#_Toc101013486)

[Section 8: Conclusion 8](#_Toc101013487)

[Section 9: Bibliography 10](#_Toc101013488)

[Section 10: Appendix 12](#_Toc101013489)

# Section 1: Introduction

A quick search on the largest hospitals in the world will show that the United States does not rank among the top ten (Goddard, *Top 10 largest hospitals in the world*). While this may sound optimistic, that the United States does not need hospitals as large as those in more populated countries, it could also mean that modern local hospitals are not equipped for the influx of patients, due to poor IT infrastructure. Kyle Stevens Hospital faces the problem of network latency and poor connectivity as a result of adding a new “Radiology Images” department. “Infrastructural inefficiencies and protocol overheads” cause latency by “more than one, and often, by more than two orders of magnitude (Chandrasekaran, Godfrey, Maggs, Singala, *The Internet at the Speed of Light*). For this reason, Kyle Stevens Hospital’s current network architecture must be updated to accommodate the increase workload of the hospital. An exploration of current hospital network architecture reveals five areas to consider when creating a hospital network: carrier-class performance, flexibility and scalability, end-to-end security, operational simplicity, and total cost of ownership (Juniper Networks, *Five Requirements of a Healthcare Network*). Kyle Stevens Hospital will need to incorporate all of these areas to better meet patient demands. Due to the critical nature of hospitals, “redundancy is an essential element in facilitating reliable and safe operations in health care delivery processes” (Tay, *Revisiting Redundancy in Hospitals – A Case-based Research Study*). Since Kyle Stevens Hospital is a growing hospital, future scalability must be considered as well. HIPAA laws require complete end-to-end security of all patient information; thus, security will be a top priority. Since the hospital is implementing a large network, it must be simple enough to implement and scale up when the time comes. Lastly, cost is a factor since implementation will be no small feat. Through the outlook of these areas, Kyle Stevens Hospital will set itself up for success.

# Section 2: Carrier-Class Performance

Even though technology enhances hospital’s services and abilities, “system outages and network downtime . . . can result in serious risk to patient safety (Juniper Networks, para. 5). A necessary component for redundancy is information backups. This can be solved through having multiple backups servers for patient records. These servers must continually be in sync. Syncing two large servers housing patient records raises two more areas to be considered: power and throughput. The issue of powering both serves can be addressed by implementing power sources, should one fail. The latter issue of throughput will need to be addressed via the network bandwidth. A proposed solution for improving bandwidth is to “utilize a forwarding identifier to indicate the compressor’s location, separating the header compression process from the packet forwarding process. In this way, context identifiers with an identical value are allowed to coexist in the same network, and flow table entries matching the compressed flows can be aggregated,” as discussed by Dong, Qin, Sun, Yan, Zhang, and Zheng (para.). The reason for this proposed forwarding identifier and proposed compression separation is because current convention has potential to limit processing capacity, as well as scalability. Since Kyle Stevens Hospital is looking ahead at future expansion, scalability is a prominent topic. By breaking down the information packets, these packets can be transferred more quickly, as well as the header packets providing an optimal route across which the information packets to be transferred. The benefits of this network design create two addresses for each network node: one to identify the node, one to locate the node. If the location of the node changes, its identity will remain unchanged, thereby transferring small packets across the network. This transfer of smaller packets means the same network can handle greater throughput. Locator/ID separation protocol (LISP) is the main protocol used for this type of network routing. LISP is especially useful for VLANs, where the network is comprised of many wireless devices. LISP allows the wireless devices to maintain the same IP address even when they’re location changes, because the endpoint identifier does not change, only the routing locator. Both duplicate servers and locator/ID separation protocol will increase the redundancy and carrier-class performance of Kyle Stevens Hospital.

# Section 3: Flexibility and Scalability

Utilizing locator/ID separation protocol also promotes flexibility and scalability within Kyle Stevens Hospital. A major advantage of the LISP protocol is that it can be widely used for virtual local access networks (VLAN), where many of the connected devices are wireless. This is beneficial for scalability as it moves networks away from being Ethernet driven networks. While Ethernet networks are great for flexibility, they lack the scalability needed in growing hospital networks (Alezabi et al., para. 3). Scalability can also happen through various routing mechanisms: routing at the source, routing implicitly, aggregate granularity, and imposing routing restrictions (Cox et al., pt. 1). Routers aid in network scalability but can be costly, as well as necessitate complicated configuration and maintenance. However, for Kyle Stevens Hospital, routers prove a more viable option as most connected devices are wireless. This means that a relatively simple architecture and protocol should be implemented, as will be discussed later. The architecture of choice must contain the ability to either scale up or scale out. Scaling up refers to additional processing power and storage, while scaling out refers to adding more routers, switches, devices, etc. (Sundvall, p. 30). Kyle Stevens Hospital will take the approach of scaling out, adding more routers and switches when necessary. This will be the easiest and most flexible approach, as it will provide scalability for new departments when the time comes. Should Kyle Stevens Hospital choose to use a Cloud database server versus an on-premises, a network load balancer would benefit the hospital greatly for scaling out (www.aws.amazon.com/health/healthcare/solutions). During busy hours when many EHRs are needed at the same time, a network load balancer can increase the number of database servers to handle the load (Alankar et al., para. 2). This will allow greater flexibility and scalability withing Kyle Stevens Hospital.

# Section 4: End-to-End Security

With a proposed Cloud database, one might ask about the security of confidential EHR. This is a valid concern, as Kyle Stevens Hospital will not have access to the physical hardware. It provides many advantages, however, as the hospital will not have to power the large servers. All data in the Cloud can backed up over multiple regions and servers. This allows easy duplicates of secure data. In the case of one region going down, another region is already up and running to take its place. Cloud services also provide security groups with network and security protocols that each database must adhere to. Within these security groups, only authorized IP addresses can access data, all through a secure firewall. Cloud databases have a default encryption, but a custom encryption can also be created. “Data integrity is one of the most critical elements in any information system (Sun et al., pt. 2). Specific authorization both on client and server sides will permit only authorized users to access confidential data. Amazon Relational Database Service (RDS) is a great candidate for maintain HIPAA HER security compliance within a Cloud architecture (www.aws.amazon.com). A hybrid technique of key sharing and authentication techniques would be recommended for the best security. The hospital could also implement firewalls to block unauthorized traffic from accessing the entire system. In all, Cloud databases provide much of the needed security and compliance that Kyle Stevens Hospital will need to have performant database that maintains HIPAA security compliance.

# Section 5: Operational Simplicity

By utilizing Cloud services, Kyle Stevens Hospital will also be able to use a simple and robust architecture for storing and transmitting patient records. The term simple here means that the system is easy to implement, use, scale, and propagate. With a proposed VLAN network design, implementation will be simple because fewer Ethernet cables will need to be run to various devices. Having a Cloud database will also benefit the lack of needing to house and maintain local servers. VLANs “allow networks to be grouped logically rather than by physical location” (Fazio et al., ch. 3). This will also allow users only in specific groups to access certain resources, thus enhancing security. The primary protocol for VLANs is IEEE 802 1Q. Since it is such a widely used protocol, one can find many resources on its implementation and structure. To scale the hospital’s network, a new VLAN simply needs to be added. This means that the work involved is predominantly on the IT software side versus the hardware side, reducing overhead infrastructure. Kyle Stevens Hospital narrowed down the network topology to either a mesh or star topology, ultimately selecting the latter. The reason for choosing a star topology is the ease of integration and scalability. To add a new department, a new firewall, routers, and end devices will be added. This is a relatively small effort and can be implemented quickly. A well-defined routing table will make the addition seamless. A mesh network provides high redundancy by connecting every device to each other, but this might be difficult in a network with potentially many wireless devices. Mesh networks also complicate implementation and troubleshooting, both of which must be easy for Kyle Stevens Hospital.

# Section 6: Total Cost of Ownership

Lastly, Kyle Stevens Hospital is considering the total cost of implementing the new IT network. One factor to consider in terms of cost is whether a current solution already exists, or if one should be made. For example, the hospital can either create an on-premises database server or use a Cloud database. As previously discussed, a Cloud database will be more advantageous for cost savings, simplicity, and redundancy. While it still has an overhead cost, it will be cheaper than its alternative. The next major cost will be the hardware devices, routers, switches, ISPs, etc. A cost analysis will be conducted to determine the more economic hardware devices to use, while still maintaining data integrity and low latency. A key component of cost is sustainability (Jeong, para. 1). The network must be sustainable and scalable over time. These tie into a simple network as well. By selecting a software defined network (SDN), most of the network setup can be done via software, which reduces hardware costs. By creating a simple VLAN network utilizing a star network topology, the system administration will be simple and require less overhead that more complex designs.

# Section 7: Design Explanation

Kyle Stevens Hospital will utilize a Dynamic Host Configuration Protocol (DHCP), which is a network management protocol that dynamically assigns IP addresses and configuration parameters to each device on the network. By using DHCP, adding new devices to the network will be streamlined and made more efficient. The hospital will also utilize network address translation (NAT) within each unit to conserve IP addresses, as well as create a simple link to public IP addresses and the Internet. This means a more secure network system. To utilize DHCP, the hospital network will also contain a DNS server to automatically provide IP addressed for each network unit and domain. Each individual unit will also implement its own Internet server. This will provide faster Internet connectivity, as well as provide security for the hospital by decoupling Internet access among the hospital units.

# Section 8: Conclusion

Taking into account carrier-class performance, flexibility and scalability, end-to-end security, operational simplicity, and total cost of ownership, Kyle Stevens Hospital plans to implement a star network topology VLAN. This will provide the many advantages, including security, scalability, and simplicity (Mohammed et al., p.2). One benefit of the star network topology is that finding points of failure will be relatively easy to diagnose. This means less overhead IT cost as well. Each individual unit of the hospital will be routed behind its own firewall. This will permit only authorized traffic to pass through to the database servers and other units, increasing security. By using multiple routers and switches in each hospital unit, high redundancy and system throughput will be maintained. For the new Radiology Images application, a new VLAN will be created that will tie directly into the existing star topology network, an easy addition. Data from the local Radiology network devices will pas through a switch located within the VLAN. The VLAN encrypts the data using 802 1Q encryption (Berger et al., ch. 3.2). The switch will direct the data packets, using LISP to the router. The router, being an authorized network device, will be permitted to pass data through the first network firewall, to another router. The second router network is not connected directly to any hospital unit and will live on a private network. From there, data will pass through a second firewall. The reason for multiple firewalls and routers is for security of patient data. Each router will be private and only maintain connections to authorized network devices. After data is passed through the second firewall, it will move to a series of switches. Each switch is independent and will update two databases. In total, four databases will be used. This is for redundancy’s sake. Since these databases are Cloud databases, they will be stored in different geographical regions, increasing redundancy and security. With the hospital’s initiative of digitizing patient records, an off-premises database will save much need patient space, as well as easily store and transmit patient data. With the incorporation of this new star topology and Cloud architecture, Kyle Stevens Hospital will set itself up to better serve its local area.

# Section 9: Bibliography

Alankar, B., Sharma, G., Kaur, H., Valverde, R., & Chang, V. (2020). Experimental Setup for Investigating the Efficient Load Balancing Algorithms on Virtual Cloud. *Sensors*, *20*(24), 7342. https://doi.org/10.3390/s20247342

Gentile, A. F., Fazio, P., & Miceli, G. (2021). A Survey on the Implementation and Management of Secure Virtual Private Networks (VPNs) and Virtual LANs (VLANs) in Static and Mobile Scenarios. *Telecom*, *2*(4), 430–445. https://doi.org/10.3390/telecom2040025

Goddard. (2021, July 16). *Top 10 largest hospitals in the world*. Healthcare Digital. Retrieved April 12, 2022, from https://healthcare-digital.com/top10/top-10-largest-hospitals-world-0

*Healthcare Solutions | Healthcare & Life Sciences | AWS*. (2022). Amazon Web Services, Inc. Retrieved April 12, 2022, from https://aws.amazon.com/health/healthcare/solutions/

Juniper Networks, Inc. (2018, August). *FIVE REQUIREMENTS OF A HEALTHCARE NETWORK* (No. 2000723–001-EN). https://www.juniper.net/content/dam/www/assets/white-papers/us/en/2021/five-requirements-of-a-healthcare-network.pdf

Kim, J. A., Park, D. G., & Jeong, J. (2019). Design and performance evaluation of cost-effective function-distributed mobility management scheme for software-defined smart factory networking. *Journal of Ambient Intelligence and Humanized Computing*, *11*(6), 2291–2307. https://doi.org/10.1007/s12652-019-01356-5

Mousa, A. H., Mohammed, N. T., & Mohammed, E. A. (2019). EFCNT: An evaluation framework for computer’s network topologies. *THE 7TH INTERNATIONAL CONFERENCE ON APPLIED SCIENCE AND TECHNOLOGY (ICAST 2019)*. https://doi.org/10.1063/1.5123126

Munther, M. N., Hashim, F., Abdul Latiff, N. A., Alezabi, K. A., & Liew, J. T. (2022). Scalable and secure SDN based ethernet architecture by suppressing broadcast traffic. *Egyptian Informatics Journal*, *23*(1), 113–126. https://doi.org/10.1016/j.eij.2021.08.001

Scarpati, J. (2013, August 21). *Cisco LISP (Location Identifier Separation Protocol)*. SearchNetworking. Retrieved April 12, 2022, from https://www.techtarget.com/searchnetworking/definition/Cisco-LISP-Cisco-Locator-ID-Separation-Protocol#:%7E:text=LISP%20(Location%20Identifier%20Separation%20Protocol)%20is%20a%20routing%20and%20addressing,its%20location%20in%20the%20network.

Stephens, B., Cox, A., Rixner, S., & Eugene Ng, T. (2018). *A Scalability Study of Enterprise Network Architectures*. Rice University. https://www.cs.uic.edu/~brents/docs/scalability.ancs11.pdf

Sun, J., Dong, P., Qin, Y., Zheng, T., Yan, X., & Zhang, Y. (2019). Improving bandwidth utilization by compressing small-payload traffic for vehicular networks. *International Journal of Distributed Sensor Networks*, *15*(4), 155014771984305. https://doi.org/10.1177/1550147719843050

Sun, Y., Zhang, J., Xiong, Y., & Zhu, G. (2014). Data Security and Privacy in Cloud Computing. *International Journal of Distributed Sensor Networks*, *10*(7), 190903. https://doi.org/10.1155/2014/190903

Sundvall, E. & Linköpings universitet. Institutionen för medicinsk teknik. (2013). *Scalability and Semantic Sustainability in Electronic Health Record Systems* (1499th ed.). Amsterdam University Press.

Zhao, Q., Sakurai, T., Yu, J., & Sun, L. (2016). Maximizing the stable throughput of high-priority traffic for wireless cyber-physical systems. *EURASIP Journal on Wireless Communications and Networking*, *2016*(1). https://doi.org/10.1186/s13638-016-0551-2

# Section 10: Appendix

Figure 1: Network Architecture of Kyle Stevens Hospital

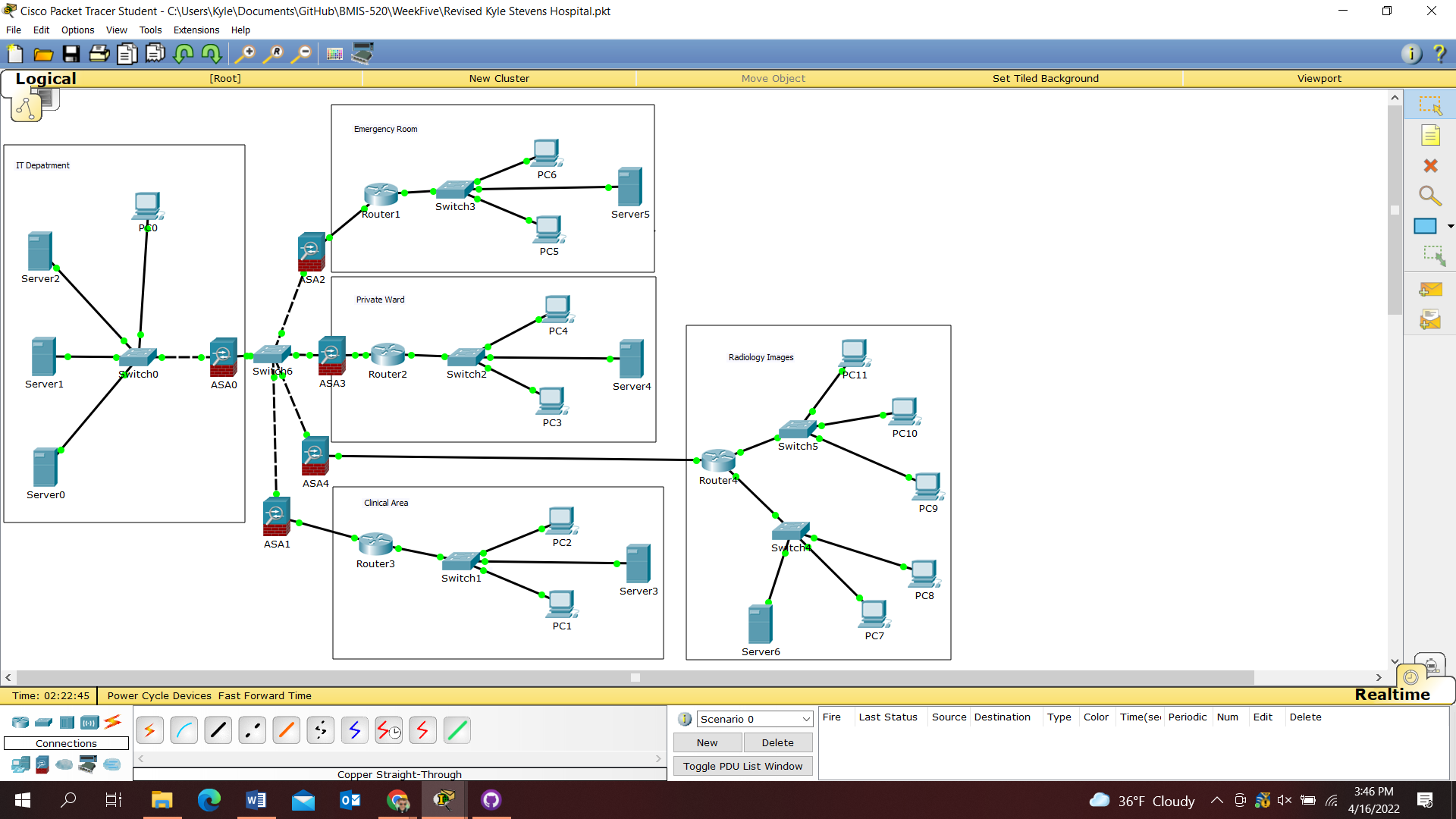


Figure 2: Configuration of Clinical Care DNS Server and PC1

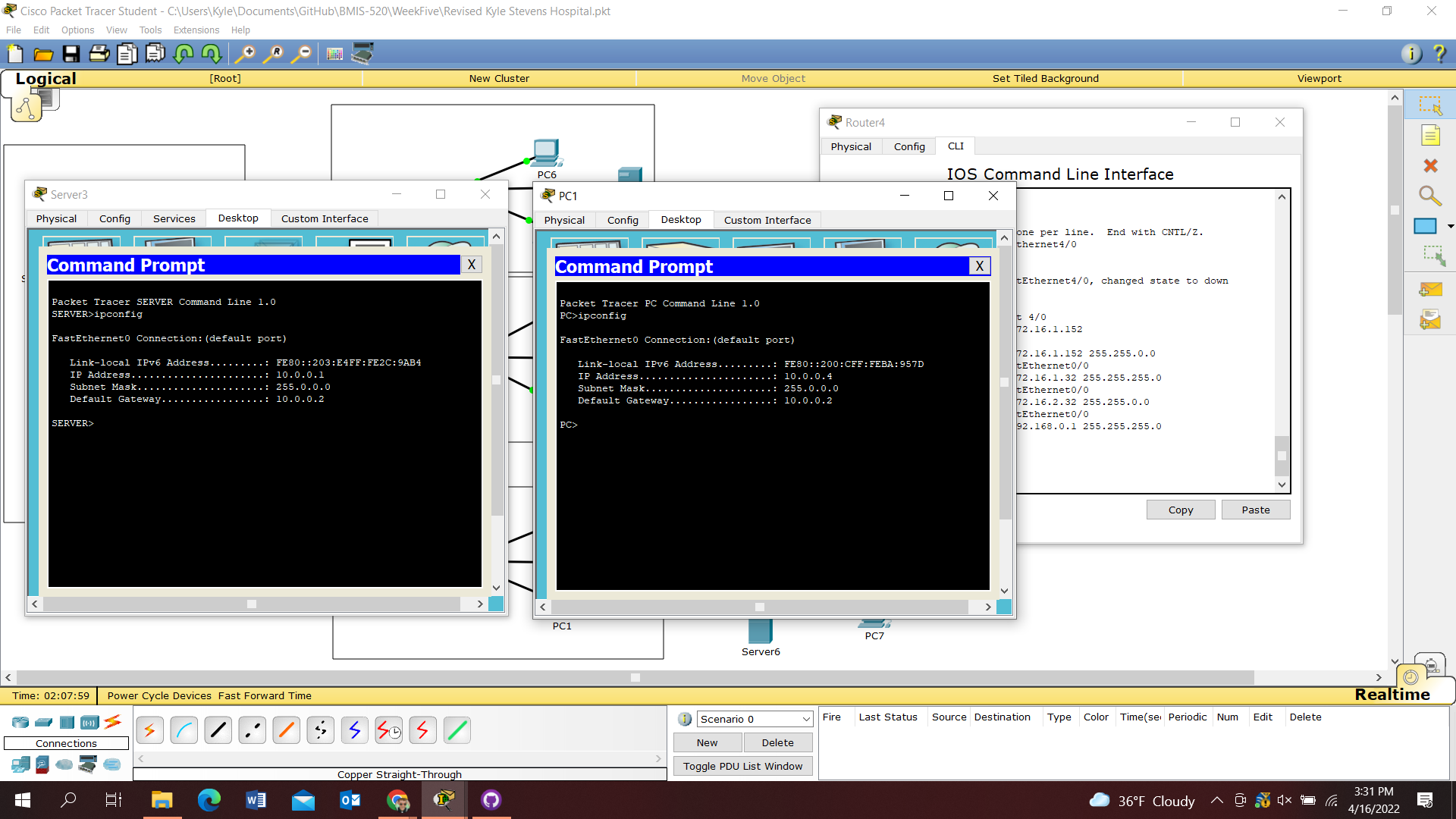


Figure 3: PC5 pinging PC6 in same subnetwork

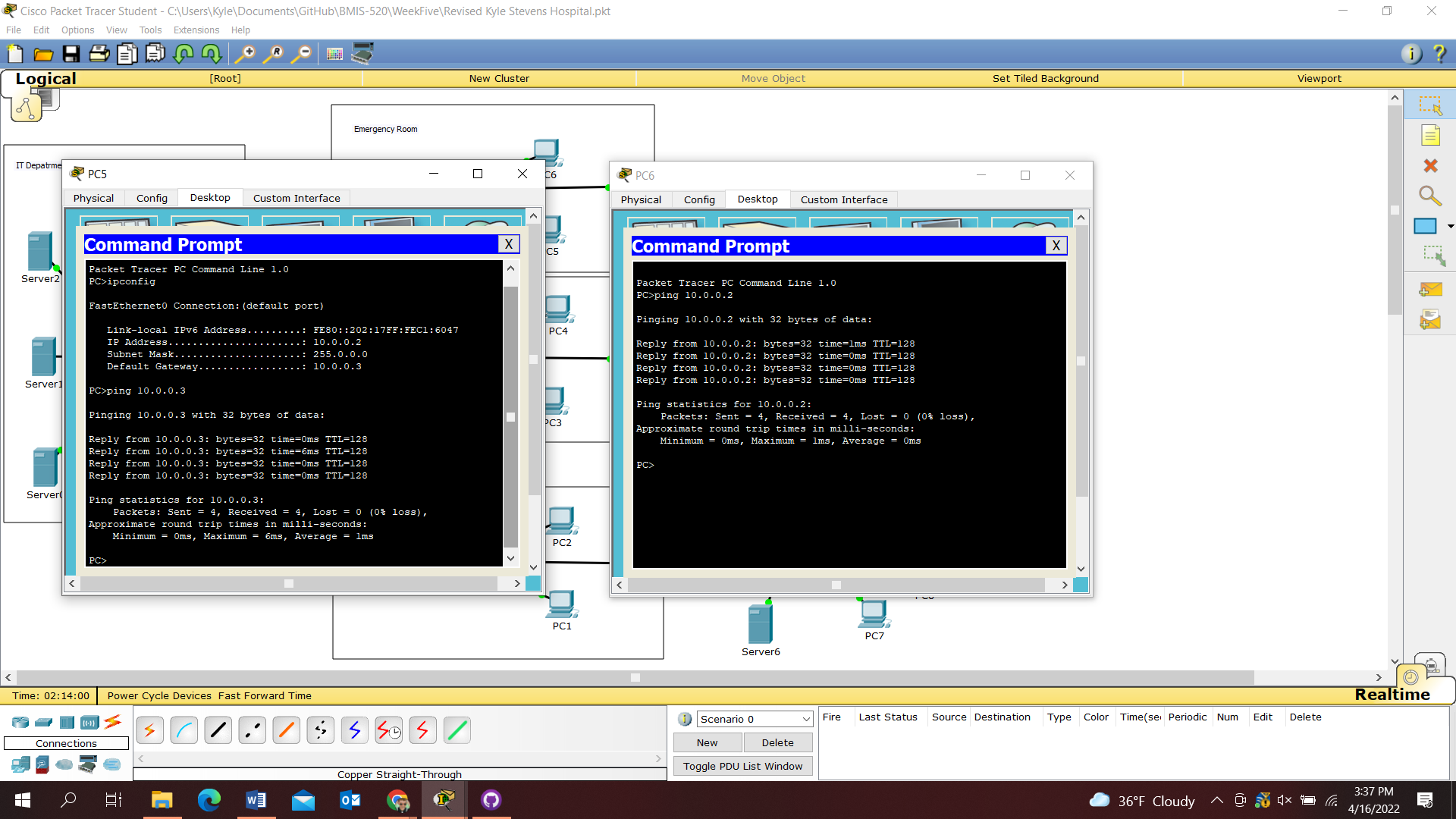


Figure 4: PC3 pinging PC6 from the Private Ward subnetwork

