Network Applications

The network applications that are part of the current network are IP phones, corporate computers, server farm, and video conferencing. The reason IP phones, and video conferencing are network applications is because it provides a way to communicate in the network. The corporate computers allow a way for security, software applications, and sharing and saving resources (Invision, 2022) that benefit the Memphis and Dallas offices.

The main component for the physical layer though is connecting the key components through cabling like fiber optic or twisted pair cabling. The components of the network at the data link layer are Network Interface Cards for the computers and switches (Skillset, 2016) as these handle MAC addresses by sending frames. Next layer 3 network layer are the routers in the organizational network diagram, as these will send packets by IP addressing. Also, the firewall in the network layer could help by filtering packets. The transport layer is using TCP and UDP, but in this case it would be TCP because this is a business, and they want to make sure their data is not lost, damaged, or out of order. This transport layer fits with the servers as TCP needs a server to operate controlling data flow between applications (Infoblox, 2024). The servers would also operate in the session layer by helping with hosting the session, managing, and finally shutting down the session for applications, so that the employees of the business can use the applications. The server also helps with the application and presentation layers as the presentation layer the server helps by converting data from EBCDIC-coded text file to an ASCII-coded file according to (Singla, 2021). The application layer the server helps by web browsing, email, and file transfer to function properly according to (Imperva, 2021).

A basic description of the key components to a nontechnical audience of layer one, is how your data is connected to your network devices usually by fiber optic cabling or twisted pair

cabling. The cabling converts digital data to electronic data, or in plain terms it describes the way devices (computers) are connected to one another (another computer). Next, the data link layer 2 of the OSI model is responsible for transferring data between devices in the same network (Staff, 2024). The switch in the network diagram is the component that completes this task, as it has a MAC address table of the local network that is connected to the ports on the device. Layer 3 of the OSI model helps find how to move data from your network to the destination network by finding the best path to do that. The router would be the device needed to complete this task in the network diagram. The firewall also functions at this layer because it can filter these packets based on rules of IP addresses. The servers in the network diagram provide hosting capabilities so that applications can be used, and information can be secured safely in a database. The servers help set up and connect with clients or end users on their devices by making the applications public on the internet. The servers then have to make data usable for the application layer by converting EBCDIC-coded text file to an ASCII-coded file. This makes the format and graphics for the application layer that end users can understand. The servers also give encryption so that data on the servers is safe from hackers. In the last layer the servers help by web hosting the applications so that the end user can see the data. Load balancing is also another function at this layer that helps with making the application run faster and have better efficiency so that it doesn't take as long for servers to process the data in a timely manner (What is Application layer? - Definition from WhatIs.com, 2024).

The applications that would not be accessible if the router of Dallas office went down would be the HR, email, accounting, and payroll. These would not be available to the Memphis office if the router were to go down. For the Memphis office if the router were to go down it would be the billing and operations applications that would be inaccessible to the Dallas office.

The risk of having one switch or router within the Memphis office is a single point of failure. There is no backup to mitigate the situation until it is fixed. This means the business is losing money every second it is down. The applications for the Memphis employees and users would be inaccessible to Dallas employees and end users as well.

For firewalls in the current network, it should be router than firewall. This is so then the router can connect its computers to the outside world and access other networks (Sophos, 2024). The router is also there to provide an external connection point, to connect to other networks (Hossain, 2024). The firewall should have a router between it and the internet in the network diagram and in the Memphis network as well. As soon as the router connects to the other network the firewall will apply rules to the traffic such as protocols and IP addresses to see if it allows or denies the traffic.

To summarize the project requirements the 1st layer of the OSI model is how your devices are connected which is usually fiber optic or twisted pair cabling for sending and receiving bits. The next layer, the data link layer, is the switch that uses a MAC address table to send data to the specific devices in the local area network. The third layer is the network layer that uses a router to send packets to networks outside of the local area network for Memphis and Dallas offices. The fourth layer uses TCP for complete data transfers between host and end systems using servers. The fifth layer also uses servers to set up, manage, and tear down a session between computers. The sixth layer encrypts, and decrypts data done by the servers and helps data translation so that the application layer can format and graphic data correctly for the user to understand. The final layer is the application layer that the user can interact with through the application.

Future Communication Needs

The network applications that are part of the current network are IP phones, corporate computers, server farm, and video conferencing. The risk of having one switch or router within the Memphis office is a single point of failure. There is no backup to mitigate the situation until it is fixed. This means the business is losing money every second it is down. The applications for the Memphis employees and users would be inaccessible to Dallas employees and end users as well. This will help offices communicate with one another in the case of a hardware malfunction or broken equipment such as routers and switches.

For communication needs to get better for the company soon the company should investigate using Microsoft Teams as this can help handle problems faster by jumping on a live call in the event of a crisis. All employees would have their own department chat rooms and instant messaging to give continuous updates to coworkers in the HR, accounting, and payroll departments that need to be improved upon in the organization. Microsoft teams would help by being a solution to all communication problems across the organization. Also, allowing security as according to (Houssier, 2023) Microsoft teams use "Transport Layer Security and other industry-standard technologies to prevent eavesdropping. TLS helps to encrypt data (including messages, files, meetings, and other content) both at rest and in transit." This would increase the security of IP phones, corporate computers, server farm, and video conferencing calls for the organization. Another added benefit is how simple Microsoft teams are to onboard new employees and offboard them by simply creating an email for the employee that correlates to the organizations name. You can then easily delete that account when the employee leaves the organization.

Network Architecture

To improve upon the communication across the company you would use Microsoft teams to help for security reasons, easy to use features such as live video conferencing, calling, and instant messaging all in one place, also the added benefit of easy onboarding and offboarding future employees. For the network architecture for the organization, you would want to use cloud native networking because this would help scale the company for the rapid increase in growth over each of the next two years. Cloud native networking according to (Cloud Native Networking, 2024) “can easily extend your network functions to new locations or regions.” Also, cloud native networking helps with efficiency by allowing you to update or upgrade a network function without affecting others in your organization (Cloud Native Networking, 2024). Finally, cloud native networking can help with Multitenancy for the organization. This means that resources can be fully utilized throughout the organization. Cloud native networking does this by sharing resources among multiple tenants, as you can reduce waste and improve cost efficiency according to (Cloud Native Networking, 2024). According to (Cloud Native Networking, 2024) you can separate these tenants and monitor network performance for each department and enforce policies for each department.

Physical Network Devices

The company will use switches, routers, and firewalls to connect to physical network devices. This gives the company the ability to reach other offices in different states to share important information between one another. The router will analyze, receive, and move data traffic between networks. The switch will help with the LAN topology as this will help route traffic locally to different departments. The firewall will help provide security as this will set up rules for what is accepted into the network.

Critical Traffic Patterns

The real-time transport protocol is currently being used for audio and voice data. RTP is not secure though for the network according to (What Is RTP? Understanding Network Protocols by Wirex Systems, 2023) there are vulnerabilities such as eavesdropping, hijacking, voice injection, and denial of service. This is due to RTP being a connectionless protocol meaning it doesn't need a connection between endpoints before data is transmitted (What Is RTP? Understanding Network Protocols by Wirex Systems, 2023). To make the data secure for the network we would want to upgrade it to Secure real-time transport protocol (SRTP). SRTP according to (RTP (Real-Time Transport Protocol) and SRTP (Secure RTP) - MDN Web Docs Glossary: Definitions of Web-Related Terms | MDN, 2024) "uses encryption and authentication to minimize the risk of denial-of-service attacks and security breaches."

The structured query language or MySQL protocol is secure for the network's security. However, upon further research it seems that PostgreSQL offers more flexibility in data types, scalability, concurrency, and data integrity (MySQL vs. PostgreSQL - Comparing Relational Database Management Systems (RDBMS) - AWS, 2024). The reason we should consider PostgreSQL over MySQL is due to the added security and extra capabilities such as define data types, index types, and functional languages (Smallcombe, 2023). PostgreSQL has become the go-to solution for complicated, high-volume data operations that MySQL wouldn't be able to handle (Smallcombe, 2023).

TCP is a much better protocol for security than user datagram protocol or UDP because TCP is a connection-oriented protocol that prioritizes reliability, while UDP is a connectionless protocol that prioritizes speed (Gorman, 2023). If we are using TCP, we should see protocol Internet Control Message Protocol (ICMP) being used too, for checking to see if a host is available as ICMP can according to (Fulin, 2021) "transmit control messages between hosts and routers to report whether hosts are reachable, and routes are available." This would benefit the

traffic of data between offices like Dallas and Memphis so that if one is not available the network would know and report back to the IT department. ICMP would help the network with network management and should be considered if the company is going to grow and have more offices around the United States. PostgreSQL should also be considered for the same reason as the database will better support a high volume of data operations than MySQL.

Patterns Across the Infrastructure

RTP is being used for audio and voice data for VoIP phones across the infrastructure. MySQL is being used for email as you can use automation from an application called Boomi to send emails directly from your MySQL database according to (How to Automate Email Sending from MySQL Databases, 2024). TCP is being used for the Human Resources department by sending data to other offices, like the Dallas office sending important data to the Memphis office. Secure Shell or SSH is being used to authenticate devices like computers being used by employees with credentials to log into the network.

Performance Issues

If no changes are made to MySQL swapping out for PostgreSQL, then the network will continue to slow down due to MySQL limitations. Also, in some cases it will not work due to account limitations for customer's email. Example would be customer goes to use email application but can no longer use it due to the data cap the customer has reached within the time limit, which will take an hour until the customer can use the email application. This also would mean the service the customer is paying for is unavailable for an hour to that customer due to data limitations. This is bad for a company trying to grow and support more and more customers and may very well leave customers looking for a new company provider, so that they can have closer to one hundred percent availability. **Security Issues**

For security we must get rid of RTP because this is not a secure protocol. An example of this going bad for a growing organization would be data breaches constantly, as there is no encryption method being used and outsider threats could easily use snooping to get the credentials or other valuable information because of the RTP. This would also lead to fines for data breaches, customers leaving for better security at another company that offers the same service, and a loss of revenue.

Performance Issue Resolve

According to (MySQL :: MySQL Restrictions and Limitations :: 12.5 Limits on Table Column Count and Row Size, 2019) MySQL has data limit of 4096 columns per table, but the effective maximum may be less for a given table. PostgreSQL according to (PostgreSQL Maximum Table Size, 2018) has a data limit of about 32 terabytes. Next is using ICMP as this would help with troubleshooting performance issues in the network. An example would be the Dallas office trying to send data from the human resources department over to the Memphis office to their human resources department. However, every time they try to Dallas never receives them. We don't know where the issue is due to not knowing what the error message is saying, and we don't know which office to start looking at because it could be the firewall for Memphis is blocking it or misconfigured router for the Dallas office, or the Memphis office. If we have ICMP on the network, we can troubleshoot this issue by sending ICMP ping command to each router to see if they receive the packets. When one does not work, we can enter the configuration commands on the router to fix the routing for the packets to pass through so that the human resources departments can continue to operate and complete daily tasks. Without

ICMP on the network these mistakes could take longer leading to longer downtimes for an office to complete daily tasks and communicate with the other departments.

Security Issue Resolve

If we use SRTP this would encrypt data of valuable information and help keep customers with the company, as well as save the company money from fines because we are trying to protect customers' data. We could also lose less customers leading to a higher number of customers because they could trust us more. Using SRTP helps according to (Sinch - TLS/SRTP: Secure Real-Time Transport Protocol Explained, 2024) by improving in the areas RTP was vulnerable in such as eavesdropping, tampering, and replay attacks.

Network Management Tool

Datadog is a network management tool to use the organization as it grows. This is because this network management can help with faster root cause analysis for the organization. As it has a dashboard providing a view of system health, consolidate network performance data alongside application performance metrics and logs according to (Datadog, 2021). This would help with having the separate offices in separate states, as we need to have a dashboard show and provide the IT department with relevant data to find the root cause of the issue faster to have more uptime for the business so that it can make more money.

Security Devices

We must be able to protect our employee’s computers from malicious attacks such as viruses, ransomware, worms, trojans, and adware. To have a line of defense against these for all four offices we should be using antivirus as this can help protect against all these attacks by installing antivirus on all systems connected to the network. Antivirus software can help protect against these attacks according to (EC-Council, 2022) by detecting and preventing malicious files from

being installed on the organizations systems. Also, we can keep this updated to always have the latest software to stop the newest attacks. Another security device to implement would be network segmentation as this would help mitigate attacks to the network by splitting it into smaller networks. This limits the chances of an attacker gaining access to devices without authenticating first, reducing the attack surface for the organization (Palo Alto Networks, 2024). Network segmentation would also help if there was an attack that got into the network by making that attack only subject to that network as it would limit the spread to another network (Palo Alto Networks, 2024). We could do this by physical or logical separation from the network.

Changes To Existing Devices

The existing devices for the network would need to be assigned their own IP addressing for the specific network for the department they are in. An example of this would be the accounting office getting an address of 192.2.1.1 and the other in HR department getting the IP address of 192.168.2.1. So, all devices would need to be changed from their original IP address to the new IP address of the network segmentation. To integrate the antivirus software into these computers for the organization this would be done by simply downloading and updating the software to the newest version to stop the most updated attacks.

Challenges

Challenges when trying to implement the future network of the organization could be employees having to change their processes and user behavior. For the technology could be advanced or require knowledge not used before by the organization. This could also lead to employee dissatisfaction as they are required to learn more about these processes and how they work in order to do their job. To mitigate this challenge faced by the company the ideal solution would

be to provide step by step instructions in a learning program from the company or a third-party service so that the installation of the new security and devices can go smoother and not lead to

Overall Risk

The overall risk of the new network would be security policies as there is not a clear definition for them, and potential to add in new technologies that could stop future attacks. As the organization is making improvements in a lot of areas there are still areas such as security policies that need to be addressed further. Overall, the network is in a much better environment to support the organization as a whole and its employees. By not keeping security standards up to date you risk the chances of being attacked. This could be a data breach that would lead the company to financial loss and lastly leave your company with a bad reputation. This would in all have a bad outcome for your business and potentially, one that could no longer be in business depending on the amount of financial loss and bad reputation from that data breach.

References

Datadog. (2021). *Real Time Business Intelligence | Datadog*. Datadog. https://www.datadoghq.com/solutions/real-time-business-intelligence/

EC-Council. (2022, March 24). *Five Ways to Defend Against Network Security Threats*. Cybersecurity Exchange. https://www.eccouncil.org/cybersecurity-exchange/network-security/how-to-prevent-network-security-attacks/

Palo Alto Networks. (2024). *What Is Network Segmentation?* Palo Alto Networks. https://www.paloaltonetworks.com/cyberpedia/what-is-network-segmentation

What Is RTP? Understanding Network Protocols By Wirex Systems. (2023, March 26). WireX. https://wirexsystems.com/resource/protocols/rtp/

RTP (Real-time Transport Protocol) and SRTP (Secure RTP) - MDN Web Docs Glossary: Definitions of Web-related terms | MDN. (2024). Developer.mozilla.org. https://developer.mozilla.org/en-US/docs/Glossary/RTP

Gorman, B. (2023, February 23). *TCP vs UDP: What's the Difference and Which Protocol Is Better?* TCP vs UDP: What's the Difference and Which Protocol Is Better? https://www.avast.com/c-tcp-vs-udp-difference

MySQL vs. PostgreSQL - Comparing Relational Database Management Systems (RDBMS) - AWS. (n.d.). Amazon Web Services, Inc. https://aws.amazon.com/compare/the-difference-between-mysql-vs-postgresql/

Smallcombe, M. (2023, September 20). *PostgreSQL vs MySQL: The Critical Differences*. Integrate.io. https://www.integrate.io/blog/postgresql-vs-mysql-which-one-is-better-for-your-use-case/

Fulin, X. (2021, November 23). *What Is ICMP? How Does ICMP Work?* Huawei. https://info.support.huawei.com/info-finder/encyclopedia/en/ICMP.html

How to automate email sending from MySQL databases. (2024, April 19). Eyer.ai. https://eyer.ai/blog/how-to-automate-email-sending-from-mysql-databases/

MySQL :: MySQL Restrictions and Limitations :: 12.5 Limits on Table Column Count and Row Size. (2019). Mysql.com. https://dev.mysql.com/doc/mysql-reslimits-excerpt/5.7/en/column-count-limit.html

PostgreSQL Maximum Table Size. (2018). EDB. https://www.enterprisedb.com/blog/postgresql-maximum-table-size

Sinch - TLS/SRTP: Secure Real-Time Transport Protocol Explained. (2024, September 11). Sinch. https://sinch.com/glossary/tlssrtp/

What is Application layer? - Definition from WhatIs.com. (2024). SearchNetworking. https://www.techtarget.com/searchnetworking/definition/Application-layer

Cloudflare. (2024). What is the network layer? | Network vs. Internet layer | Cloudflare. *Cloudflare*. https://www.cloudflare.com/learning/network-layer/what-is-the-network-layer/

HOSSAIN, M. S. (2024, May 21). *Extending Your Network — TryHackMe - MD SAKHAWAT HOSSAIN - Medium*. Medium. https://medium.com/@MrBadasss/extending-your-network-tryhackme-205d2b9e0aaa

Invision. (2022, June 14). *6 Reasons a Computer Network is Good for Business*. Invision. https://invisionkc.com/6-reasons-a-computer-network-is-good-for-business/

Staff, C. (2024). *What Is a Data Link Layer?* Coursera. https://www.coursera.org/articles/data-link-layer

Skillset. (2016). *Which layer of the OSI model does the Network Interface Card (NIC) medium work on? - Skillset*. Skillset.com. https://www.skillset.com/questions/which-layer-of-the-osi-model-does-the-network-medium-work-on

Infoblox. (2024). *What is Layer 4 of the OSI Model: Transport Layer? | DDI (Secure DNS, DHCP, IPAM)*. Infoblox. https://www.infoblox.com/glossary/layer-4-of-the-osi-model-transport-layer/

Imperva. (2021). *What Is OSI Model | 7 Layers Explained*. Imperva. https://www.imperva.com/learn/application-security/osi-model/

Sophos. (2024). *Firewalls Explained | How to Corporate Firewalls Work?* Www.sophos.com. https://www.sophos.com/en-us/cybersecurity-explained/firewall

Houssier, E. (2023, February 28). *Microsoft Teams Security: Is Your Data Secure?* Powell Software. https://powell-software.com/resources/blog/microsoft-teams-security/

Nile. (2024). *What Is Network Scalability? How to Optimize for Growth*. Nile. https://nilesecure.com/network-design/network-scalability

Cloud Native Networking. (2024, May 5). Tigera - Creator of Calico. https://www.tigera.io/learn/guides/cloud-native-security/cloud-native-networking/