Computer Networking: CS635

Individual Project

Brian Byrne

12/10/23

Table of Contents

Note:

Hello professor,

I used this same fake company for my previous class last semester. Operating Systems CS360. I really liked the idea of building off what I did with my last paper. Thank you for allowing this option for us. If you have any concerns regarding any changes needed to stay within the rules, please let me know and I will promptly make any corrections.

Thank you!

- Brian Byrne

Project Outline:

Hello, FloorsRUs is a flooring distributor in the greater Kansas City, Missouri greater area. This company sells flooring installation and flooring tools in both retail and online storefronts. Primarily service the flooring installers union members but looking to expand to service the general public moving into the future. A 100,000 square foot warehouse stores all inventory, running off paper records to keep track of product locations. Invoices are handed over to warehouse employees for picking and packing customer orders. Terminals are located next to all shipping stations in the back of the warehouse. Office Staff are equipped with desktop computers and laptops to complete their roles.

Currently, the company inventory tracking and order fulfillment systems run off paper transactions. There is no network system connecting the front office staff to the warehouse workers at the back of the facility. All communications take place over the phone or by the passing of paper documents that someone must physically relay back and forth. Many companies still utilize old school technology if any at all under the premise of, “Don’t fix what isn’t broken.” The current systems in place have worked for the past few decades but with business expanding, upgrades to networking, followed by upgrades to the overall process flows of the business due.

FloorsRUs has the option of upgrading to a few potential network infrastructures. We recommend FloorsRUs move to a distributed networking system, a cloud-based infrastructure style. We believe this option will be best served for expansion specifically to improve order-fulfillment timeframes and

increase the accuracy of inventory knowledge for the online storefront. Amongst a variety of other benefits and goals.

We will discuss these upgrades in detail throughout the rest of this text.

Distributed Network Requirements Analysis (Week 1)

Designing a distributed network involves considering various aspects to ensure that the organization's requirements are met efficiently. Below are five major areas of functionality with associated capacity, performance, connectivity, and security requirements, along with other considerations. These considerations are discussed in no order, focusing on the areas that have more applicable relevancy. Consider this list of topics to be a high-level arrangement of overall goals and benefits provided by the implementation of this project proposal.

Data Storage and Retrieval:

FloorsRUs needs to be able to move data across internal systems as well as move data to update the online storefront. FloorsRUs needs to eliminate the role of paper runners in the business. There is no need for any of the data transactions to be paper documents outside of shipping documents. Customers need to know what the business is selling immediately at the point where they are looking at the products online. For this reason, a good internet connection is essential. Any question on whether a product is even available for purchase will result in customers looking elsewhere and placing their product orders elsewhere. The latest prices need to be available, as well as whether the desired products are even in stock at all. A standard of anything less will result in lost sales.

Performance requirements need to be set in terms of server loads being able to handle increased customer demand. As customers visit the business-only storefront, the systems in place need to keep up. The business needs to be prepared to accept packet requests from the servers on a commercial scale. If this requirement isn't met, the website could be subjected to a server overload, resulting in a website outage and subsequent lost business.

These data transactions need to be reliable and free of inaccurate scrambling errors. Tanenbaum, p. 47, "Think about the bits of a packet traveling through the network. There is a chance that some of these bits will be damaged (inverted) due to fluke electrical noise, random wireless signals, hardware flaws, software bugs, and so on."

A cloud network has the massive benefit of being scalable, which will be discussed further in this document. FloorsRUs can simply meet the increased potential demand by adding more servers and resources to the network infrastructure on an as-needed basis. Subsequently, during slower parts of the year, resources could be pulled back and savings could be made by renting less server space.

Load Balancing:

In the domain of load balancing, the recommendation seeks to get the best results out of balancing server loads. If there are five servers in play in the network, the goal would be to 'balance' the load in such a way that not a single server is overloaded and crashes. If not all five servers are needed during slow times in the middle of the night, a couple of the servers could be turned off to avoid paying electric

bills for a resource not needed. There is a strong emphasis on this topic of creating an even distribution of workload amongst all servers involved in the task.

Load balancing helps mitigate the classic Distributed Denial of Service (DDOS) attacks. Attackers have been known to spam specific servers with massive amounts of server packet requests, causing a near-immediate server crash. The machine gets too many requests at once, doesn't know what to do, and crashes. If more servers can be deployed quickly, these attacks become less damaging to specific servers, as this unexpected spike in load could be diverted to any available open server. It would not completely stop the problem, but in that scenario, it would take some extra time to figure out a solution. A distributed network allows for this kind of quick deployment.

Fault Tolerance:

Distributed networks provide various avenues of fault tolerance. One of the performance requirements is for the computer systems to always be live and operational. Network providers have regulated service level agreements as to the ratios of downtime to the business. The recommendation would be to include similar documents in the project plans discussing what these agreements would be for the business's network operations internally. These include limits to network downtime as well as speed to completing recovery solutions. Communication chains would be included so engineers know ahead of time who needs to be involved at what points in the process. One of the challenges in being effective in disaster recovery is knowing who maintains each piece of these complex systems for system access and general knowledge.

Distributed networks excel in this category with the use of backups of entire systems on different separate nodes in the network. Ideally, these backup servers would be in a far enough physical location where a natural disaster wouldn't knock both the main and backup servers out. If a tornado rips through the data center in Kansas, the plan would be to have a backup server in Colorado ready to roll and step into the process flow. General single points of failure would be mitigated by having multiple backups outside of the double layer. Any node in the distributed network could potentially house a backup copy. It's ok if many of these emergency backup copies are redundant; server space can be rented for reasonable rates.

Communication and Collaboration:

Communication and collaboration refer to internal processes moving along quickly and accurately. With most of the process flows moving from paper transactions to virtual data transfers, these activities need to move at a prompt speed. If the tasks take longer after the implementation of these systems, then the whole project would need to be re-evaluated. Customer data needs to be moved promptly after the point of sale from the front office staff to the back end of the warehouse. Warehouse employees need the data to pick the correct items off the warehouse shelves and print the required shipping labels. With a quality network arrangement, this information will flow at the speed of light, much faster than even the quickest speed-walking employee. These communications are built on networking protocols. According to Tanenbaum, p. 82, "Network software is built around protocols, which are rules by which processes communicate. Most networks support protocol hierarchies, with each layer providing services to the layer above it and insulating them from the details of the protocols used in the lower layers." These layers refer to the infamous OSI model.

When building the network plan, considerations for capacity requirements will be discussed, and those figures will be included in the end proposal. These requirements include the number of users, devices, frequency of use, and amount of network traffic expected during normal, slow, and peak operation times.

For security purposes, a VPN will be required to be used by all employees when accessing anything through an internet connection. This will ensure that all data is protected from being picked up by a malicious actor through 'man in the middle' packet sniffing operations. This is done by encrypting all data passing through the VPN, which is this mechanism's function. Other security measures to be implemented include password requirements and other access controls. Data access is only needed on an as-needed basis, with considerations made for employees' various roles in the organization. For a built-in implementation deep inside the software systems, we have protocol layering. According to Tanenbaum, p. 49, "This concept is a familiar one and is used throughout computer science, where it is variously known as information hiding, abstract data types, data encapsulation, and object-oriented programming. The fundamental idea is that a particular piece of software (or hardware) provides a service to its users but keeps the details of its internal state and algorithms hidden from them."

Scalability and Growth:

We have discussed this benefit of distributed networks at various points in the discussions above. According to Tanenbaum, p. 47, "When networks get large, new problems arise. Cities can have traffic jams and a shortage of telephone numbers, and it is easy to get lost. Not many people have these problems in their own neighborhood, but citywide they may be a big issue. Designs that continue to work well when the network gets large are said to be scalable." All the other topics lean heavily on this distributed system's scalability and growth options. As the company grows, the network should grow alongside it at a matching pace. Considerations should be made for unexpected spikes in server requests and slow times in the business where budgets could allocate fewer funds to operation while still being fully effective. It is much easier, quicker, and cheaper to rent more server space than it will ever be to purchase new hardware for company staff. Implementation via the wide market of web services allows for the growth of resources to be attained through the creation and execution of simple programming scripts. Further security measures would need to be considered for future additions to the distributed network.

Data Storage and Retrieval:

FloorsRUs needs to be able to move data across internal systems as well as move data to update the online storefront. FloorsRUs needs to eliminate the role of paper runner in the business. There is no need for any of the data transactions to be paper documents outside of shipping documents. Customers need to know what the business is selling immediately at the point where they are looking at the products online. Good internet connection for this reason is essential. Any question on whether a product is even available for purchase will result in customers looking elsewhere and placing their product orders elsewhere. The latest prices need to be available as well as if the products desired are even in stock at all. A standard of anything less will result in lost sales.

Performance requirements need to be set in terms of server loads being able to handle increased customer demand. As customers visit the business only storefront, the systems in place need to keep up. The business needs to be prepared to accept packet requests to the servers on a commercial scale. If this

requirement isn't met, the website could be subjected to a server overload resulting in a website outage and again subsequent lost business.

These data transactions need to be reliable, free of inaccurate scrambled errors. Tanenbaum pg. 47, "Think about the bits of a packet traveling through the network. There is a chance that some of these bits will be received damaged (inverted) due to fluke electrical noise, random wireless signals, hardware flaws, software bugs, and so on."

A cloud network has the massive benefit of being scalable, which will be discussed further in this document. FloorsRUs can simply meet the increased potential demand by adding more servers/resources to the network infrastructure on an as-needed basis. Subsequently during slower parts of the year, resources could be pulled back and savings could be made by renting less server space.

Load Balancing:

In the domain of load balancing, the recommendation seeks to get the best results out of balancing server loads. If there are five servers in play in the network, the goal would be to 'balance' the load in a way that not a single server is overloaded and crashes. If not all five servers are needed during slow times in the middle of the night, a couple of the servers could be turned off to avoid paying electric bills for a resource not needed. There is a strong emphasis on this topic on creating an even distribution of workload amongst all servers involved in the task.

Load balancing helps mitigate the classic Distributed Denial of Service (DDOS) attacks. Attackers have been known to spam specific servers with massive amounts of server packet requests causing a near immediate server crash. The machine gets too many requests at once, doesn't know what to do and crashes. If more servers can be deployed quickly, these attacks become less damaging to specific servers as this unexpected spike in load could be diverted to any available open server. Would not completely stop the problem but would in that scenario buy some extra time to figure out a solution. A distributed network allows for this kind of quick deployment.

Fault Tolerance:

Distributed networks provide various avenues of fault tolerance. One of the performance requirements is for the computer systems to be always live and operational. Network providers have regulated service level agreements as to the ratios of downtime to the business. The recommendation would be to include similar documents in the project plans discussing what these agreements would be for the business towards network operations internally. These include limits to network downtime as well as speed to completing recovery solutions. Communication chains would be included so engineers know ahead of time who needs to be involved at what points in the process. One of the challenges in being effective in disaster recovery is knowing who maintains each piece of these complex systems for system access and general knowledge.

Distributed networks excel in this category with the use of backups of entire systems on different separate nodes in the network. Ideally these backup servers would be located a far enough physical location where a natural disaster wouldn't knock both the main and backup servers out. If a tornado rips through the data center in Kansas, the plan would be to have a backup server in Colorado ready to roll and step into the process flow. General single points of failure would be mitigated by having multiple backups outside of the double layer. Any node in the distributed network could potentially house a

backup copy. It's ok if many of these emergency backup copies are redundant, server space can be rented for reasonable rates.

Communication and Collaboration:

Communication and Collaboration refers to internal processes moving along quickly and accurately. With most of the process flows moving from paper transactions to virtual data transfers, these activities need to move at a prompt speed. If the tasks take longer after implementation of these systems, then the whole project would need to be re-evaluated. Customer data needs to be moved promptly after the point of sale from the front office staff to the back end of the warehouse. Warehouse employees need the data to pick the correct items off the warehouse shelves and print the required shipping labels. With a quality network arrangement, this information will flow at the speed of light, much faster than even the quickest speed-walking employee. These communications are built off networking protocols. According to Tanenbaum pg. 82, "Network software is built around protocols, which are rules by which processes communicate. Most networks support protocol hierarchies, with each layer providing services to the layer above it and insulating them from the details of the protocols used in the lower layers." These layers are referring to the infamous OSI model.

When building the network plan, considerations for capacity requirements will be discussed and those figures will be included in the end proposal. These requirements include number of users, devices, frequency of use, and amount of network traffic expected during normal, slow, and peak operation times.

For security purposes, a VPN will be required to be used by all employees when accessing anything through an internet connection. This will ensure that all data is protected from being picked up by a malicious actor through 'man in the middle' packet sniffing operations. This is done by encrypting all data passing through the VPN which is this mechanisms function. Other security measures to be implemented include password requirements and other access controls. Data access is only needed on an as-needed basis with considerations made for employee's various roles in the organization. For a built-in implementation deep inside the software systems we have protocol layering. According to Tanenbaum pg. 49, "This concept is a familiar one and is used throughout computer science, where it is variously known as information hiding, abstract data types, data encapsulation, and object-oriented programming. The fundamental idea is that a particular piece of software (or hardware) provides a service to its users but keeps the details of its internal state and algorithms hidden from them."

Scalability and Growth:

We have discussed this benefit of distributed networks at various points in the discussions above. According to Tanenbaum pg. 47, "When networks get large, new problems arise. Cities can have traffic jams, a shortage of telephone numbers, and it is easy to get lost. Not many people have these problems in their own neighborhood, but citywide they may be a big issue. Designs that continue to work well when the network gets large are said to be scalable." All the other topics lean heavily on this distributed systems scalability and growth options. As the company grows, the network should grow alongside at a matching pace. Considerations should be made for unexpected spikes in server requests and slow times in the business where budgets could allocate fewer funds to operation while still being fully effective. It is much easier, quicker, and cheaper to rent more server space than it will ever be to purchase new hardware for company staff. Implementation via the wide market of web services allows for growth of

resources to be attained through the creation and execution of simple programming scripts. Further security measures would need to be considered for future additions to the distributed network that fall outside of the high-level scope of this proposal.

Communication Protocols Analysis and Recommendations (Week 2)

There are many protocols that regulate distributed networks in terms of communication and the movement of data. These standards provide worldwide standardization for the setup of these networks so developers can expect the mechanisms to behave in a consistent manner. For the purposes of the company upgrades for FloorsRUs, we will focus on the OSI networking model and the TCP/IP protocols that regulate the transport layer (Layer 4) of the OSI model.

The OSI model describes, at a high level, how the worldwide internet operates. It consists of 7 layers that form a stack that data moves through from top to bottom and bottom to top depending on which side of the transfer we are starting with (sender vs. receiver). The layers listed in order starting from the top are: physical layer, data link layer, network layer, transport layer, session layer, presentation layer, and application layer. We will discuss each layer individually as it relates to the big picture of the model in its entirety. We will start with data being received by the network hardware. If we are talking about the 'sender' role in this relationship, the stack is flipped. The model doesn't dictate specific technologies or protocols but is used as a reference model to describe the conceptual design of standard network infrastructure. A good network setup will be the backbone for the online storefront FloorsRUs plans on expanding with.

Physical Layer:

The first layer of the model refers to the physical transmission of raw bits over a physical medium. It includes packets being received by the physical hardware (modems, routers, and cables). Defines characteristics such as voltage layers and data rates. The physical layer receives the signals and converts them into data packets, passing data to the data link layer.

Data Link Layer:

The second layer of the stack talks about reliability over the physical links. Handles logical addressing, error detection, and flow control. Checks for errors and removes hardware addresses, passing data to the network layer.

Network Layer:

The third layer focuses on routing the data packets between different networks. Ensures the data is sent to the correct destination, sending data through to the transport layer.

Transport Layer:

The fourth layer reassembles the data packets as received from the network layer, passing data on through to the session layer. Adds sequence numbers for the reassembly of the packets.

Session Layer:

The fifth layer manages the communication session, passing data on through to the presentation layer.

Presentation Layer:

The sixth layer modifies the data from the session layer into a format that can be understood by the application layer. This format is specific to the application in use.

Application Layer:

The seventh and final layer presents the data from the presentation layer to the user or application to complete the process flow. Original data is now open for full functional use. The stack is complete.

Each layer in the OSI goes through encapsulation processes to ensure data is properly formatted, addressed, and secured as it moves through the model. Each layer performs its own roles independently from the other layers as it adds and removes information from the data. The logical process flow of steps allows developers and network engineers the unique ability to troubleshoot any issues in a step-by-step logical manner. Each layer has its own checks that confirm a successful movement onto the next layer. By checking these confirmation messages, developers can isolate and easily identify any issues to the last successful message as data is pushed through the system. Avoids potential wild goose chases as the model allows for confidence that there is a solid starting point.

TCP/IP Networking Protocol:

The TCP/IP protocol is a suite of communication protocols that form the backbone of the modern internet and many other large private networks. These protocols create a standard set of rules for how devices on a distributed network communicate with each other. The name comes from the two main protocols of the suite (Transmission Control Protocol and Internet Protocol). The suite regulates the transport model for the OSI model as described above. According to Tanenbaum pg. 60, “The TCP/IP model did not originally clearly distinguish between services, interfaces, and protocols, although people have tried to retrofit it after the fact to make it more OSI-like.” The recommendation is to implement the network for FloorsRUs to match these protocols to make implementation into the World Wide Web much smoother. These protocols are considered the industry standard.

IP (Internet Protocol):

IP protocol is responsible for addressing and routing data packets so they travel across networks and arrive at the correct destination. There are two versions (IPv4 and IPv6) with the difference being the length of the destination addresses. IPv4 has 32-bit addresses while IPv6 has 128-bit addresses. While IPv4 is still used for some parts of the internet, the recommendation would be to implement IPv6 as a form of future proofing the network setup.

TCP (Transmission Control Protocol):

TCP provides reliable, connection-oriented communication between devices. It breaks down data into smaller packets, ensures the delivery of these packets in the correct order. It also handles retransmission

in the event that some packets get lost along the way. According to Tanenbaum pg. 558 “TCP service is obtained by both the sender and the receiver creating endpoints, called sockets, as discussed in Sec. 6.1.3. Each socket has a socket number (address) consisting of the IP address of the host and a 16-bit number local to that host, called a port. A port is the TCP name for a TSAP. For TCP service to be obtained, a connection must be explicitly established between a socket on one machine and a socket on another machine.”

Advantages:

Universal Adoption:

TCP/IP is universally adopted as the standard protocol suite for networking. The widespread acceptance brings interoperability among diverse systems and devices.

Scalability:

The rules laid out by TCP/IP have built-in scalability. The same rules apply for networks of all sizes. From large global networks to small home networks, TCP/IP handles communication demands effectively.

Versatility and Ease of Integration:

TCP/IP supports various network services and applications. From simple file transfers to complex web-based interactions, these protocols have answers for all setups. Developers can expect specific behaviors to occur and write their code with assumptions in mind, creating a ‘plug and play’ mindset. This follows the programming pillar of abstraction.

Open Architecture:

TCP/IP is built on open architecture; the specifications of the protocols are publicly available. This fosters innovation as developers are able to conform their code to the rules in mind. This also brings interoperability between different companies' hardware and software.

Disadvantages:

Overhead:

Reliability of TCP/IP comes with a level of overhead. The control mechanisms involving error checking and the sequencing of data packets can lead to increased latency. Even if the handle time for each interaction may only increase slightly, the effects on the overall network could be sizable. For real-time applications where low latency is critical for success, this is a severe drawback.

Complexity:

Even though the specifications of TCP/IP are easy to find, there are multiple layers of protocols in the suite. Configuring and managing these layers can be difficult, particularly for someone without in-depth networking knowledge. Implementing a network to match TCP/IP standards involves a substantial learning curve.

Security Considerations:

The TCP/IP does not have security considerations built into the protocols. Additional protocols are required to ensure that network interactions are secure from a wide variety of security vulnerabilities. This requires additional knowledge that must be attained by developers and network engineers as well as constant maintenance as new vulnerabilities are constantly being discovered.

Limited Support for Mobile Networks:

TCP/IP was not originally designed for mobile networks and devices. While various adaptations and extensions are available to fill the gap, the architecture is not as good as the original infrastructure. Many of the customers accessing the FloorsRUs website may be doing so through mobile devices. The experience may not be as ideal as accessing sale info through a traditional desktop environment.

Network Traffic Analysis and Recommendations (Week 3)

FloorsRUs plans on expanding the online storefront in the coming years. In anticipation of increased network traffic, the network infrastructure must grow alongside. Failure to move on these upgrades could result in network congestion, making it difficult for customers to access the online storefront where they would get product information and/or make purchases. If the website goes down, the virtual side of the business goes down with it which FloorsRUs plans to lean heavily on in the coming years.

Major Uses of Distributed Network:

File Sharing and Collaboration among employees internally in FloorsRUs will account for a high volume of data transfers. These are transactions ranging in size of small documents (invoices for example) to large multimedia files. The traffic related to this side of employee production would peak during heavy collaborative work and would be increased during regular business hours. Several large files in a quick row may strain the network bandwidth. According to According to Tanenbaum pg. 406, “The network layer is concerned with getting packets from the source all the way to the destination.” The basic functions required to maintain the business run through the company’s network infrastructure.

Distributed computing could be utilized by FloorsRUs to better understand the market conditions. Business Intelligence as this is somewhat known as. With quality data input, FLoorsRUs could use distributed computing to price product more accurately, profile an ideal customer, make more effective ad campaigns, and the list goes on. The depth of distributed computing isn’t a large priority over upgrades to higher priority network infrastructure. The traffic estimates would be high intensity tasks in quick succession between nodes and would peak during such tasks are present. The heavy number crunching would typically occur outside of normal business hours, so the resources involved had all the network bandwidth otherwise utilized by office staff.

Cloud Services would be helpful for employees to have access to. All documents and data that might go on an internal hard drive could be stored on a company internal cloud server instead. If an employee has an accident and their laptop hard drive is destroyed, the data is safely stored on the company servers in the office. PC upgrades would be much easier as all the data would be in the same location as it had always been. Traffic estimates are varied. The uses of cloud services include data storage, various application usages attached to distributed computing and communication media. The peak hours would

include normal business hours, with extra peaks based on global patterns. Cloud Services has a large amount of user activity that when sending back and forth large-scale data transfers could lead to heavy network congestion.

Content Delivery Networks (CDNs) have high volume data distribution. According to Tanenbaum pg. 11, “A CDN is a large collection of servers that are geographically distributed in such a way that content is placed as close as possible to the users that are requesting it.” CDNs include the webpage for FloorsRUs and additional promotional videos and images. Additional resources would be set up for promotional and marketing events in the main sales room in the front office space. In the event of FloorsRUs becoming an overnight sensation, having these additional resources would mitigate the sudden spike in usage that might overwhelm the main network resources.

Recommendations:

The recommendation right out of the gate is to implement an infrastructure. Acquiring better adapted routers, network switches and access points would bring immediate improvements to network performance. Hardware should be purchased based on the needs of the company regarding projected volume and the acceptance tolerance for network congestion. According to Tanenbaum pg. 406, “...researchers discovered that many network devices tend to have more memory than they need, a concept that became known as bufferbloat.” The recommendation would be to not wildly over purchase in some areas of the network infrastructure hardware.

There are Quality of Service requirements set out to characterize the needs of successful data transfer. According to Tanenbaum pg. 406, “A stream of packets from a source to a destination is called a flow (Clark, 1988). A flow might be all the packets of a connection in a connection-oriented network, or all the packets sent from one process to another process in a connectionless network. The needs of each flow can be characterized by four primary parameters: bandwidth, delay, jitter, and loss. Together, these determine the QoS (Quality of Service) the flow requires.” If any/all these metrics are not above/below specific levels as described by the QoS, the network is said to be experiencing varying levels of outage which is network congestion. QoS goes through the act of characterizing all the packets flowing through to place them somewhere onto a priority queue. Voice and video data would be placed higher on the queue over other small data quantities such as simple word documents. These decisions are made on the network layer (layer 3) and the transport layer (layer 4) of the OSI networking model. According to Tanenbaum pg. 408, “File transfer applications, including email and video, are not delay sensitive. If all packets are delayed uniformly by a few seconds, no harm is done. Interactive applications, such as Web surfing and remote login, are more delay sensitive. Real-time applications, such as telephony and videoconferencing, have strict delay requirements.” Once the classifications of packets is complete by the QoS protocols, other mechanisms in these two layers manage an even flow of data based on this information. The goal would be to prevent any singular server from becoming overloaded. This is done through passing off tasks to other open servers through load balancing.

The recommendation continues with implementing software for real-time network traffic monitoring. If the IT team isn’t aware of network congestion, how would they know they need to fix it? The goal of this implementation is to take a more productive approach to the problem with awareness. The IT team would be tasked with monitoring the metric of packet loss which is done with a mechanism known as Random Early Detection (RED). This algorithm watches the queue length on packet transactions and in the event it gets too long, it starts to drop packets at random points in the queue instead of dropping the

next in line packets or back of the line packets. This prevents a single source having dropped packets in higher amounts than other sources. According to Tanenbaum pg. 403, “To determine when to start discarding, routers maintain a running average of their queue lengths. When the average queue length on some link exceeds a threshold, the link is said to be congested and a small fraction of the packets are dropped at random.” A few lost packets spread out across the network is way better than having a whole failed task, isolating a specific nodes request.

In addition, this software should allow functionality to load balance tasks to less strained servers and provide levers to throttle max network bandwidth utilization. CDNs could be implemented when the main servers are too backed up and extra resources are required to keep systems going. The software recommendation suggests having these overflow servers on standby for a quick boot up in the scenario such traffic volume arrives. According to Tanenbaum pg. 409, “An easy solution to provide good quality of service is to build a network with enough capacity for whatever traffic will be thrown at it. The name for this solution is overprovisioning.” Finding the line between having plenty of resources and bufferbloat as discussed earlier is the ability to scale up quickly and then scale back down just as quickly. Both sides of the line can be covered with the ability to turn on/off these additional CDN servers as described.

By implementing these recommendations, FloorsRUs can bring its network to a level critical to long-term health and success for the future. This organization’s network needs to be able to handle various diverse usage scenarios that will test the network infrastructure into folding. The recommendations laid out above will help mitigate network mitigation from both regular and peak usage periods, which is the goal.

Network Design and Architecture (Week 4)

Now we will explain a high-level breakdown of the network design and architecture. Estimates of scale assume FloorsRUs employs 200 people. Estimate of $10,000 for each one of the recommended servers with installation costs.

Starting with a breakdown of the hardware components with amounts recommended. The order of items on the list below are in order on the stack starting from incoming data coming from the internet to the bottom endpoint users who benefit. Consider this a rough form of a flow chart that reads from top to bottom.

Internet Connection

Good internet access from a quality Internet Service Provider on their business class package.

Networking Hardware

4 routers to be located at strategic positions to avoid dead zones within the facility. Firewalls and other hardware security measures would be included.

Rough Estimate: $4000

Security

Software will be in place for network intrusion detection, notification, and prevention. Hard drives for all PCs will be fully encrypted. It would be preferred to have functionalities for remote hard drive wiping. Confidential customer and internal data stores need to be protected. Access control systems will be in place to prevent physical breach of the facility.

Monitor and Management Software

One of the servers will be dedicated to hosting monitoring and management roles, with an additional redundant server at the offsite data center. Wireshark is a known packet sniffing software.

Load Balancers (2)

Balances out server loads through managing network traffic volumes. Physical device sits between switches/routers and the servers.

Rough Estimate: $20,000

Backup and Storage Solutions (Servers)

Offsite backup server as described below serve as main source of data for disaster recovery scenarios.

Web Servers (5)

The recommendation would include 2 of the webservers to be located offsite as backup servers.

Rough Estimate: $50,000

Database Servers (2)

The recommendation is for one of the database servers to also be offsite.

Rough Estimate: $20,000

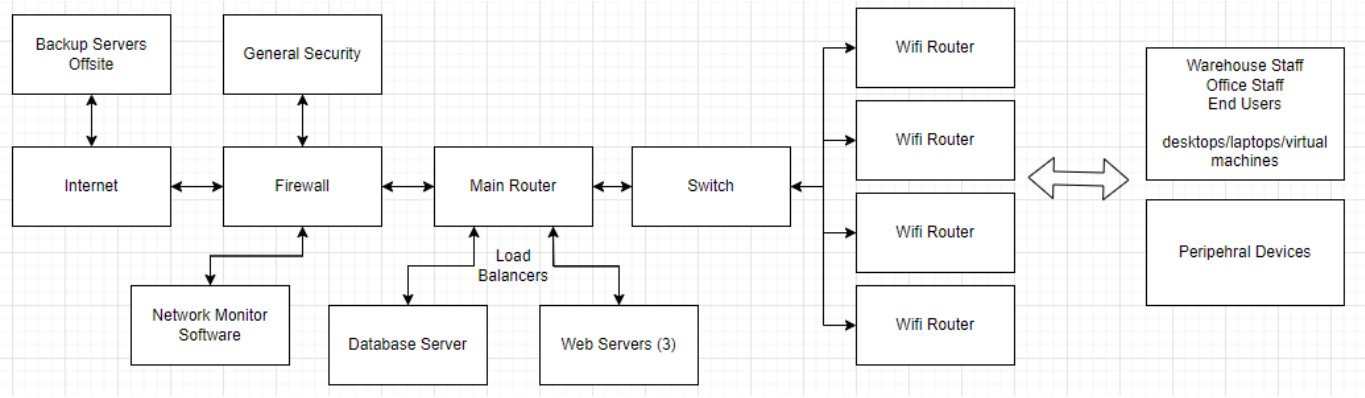
Endpoint Users

The individual bottom nodes of the network along with the servers that hold the data/complete tasks. If we estimate FloorsRUs employs 200 people, this will potentially mean 200 machines. These would be laptops, desktops and virtual machines running off thin client receivers. Office peripherals such as printers, faxing machines, projectors etc. would also be included. Prices on machines would vary. Virtual machine implementations would be cheapest while full laptops would be the expensive side of the options. These machines would be running Windows 10 or better. Windows 11 recently came out, but Windows 10 would still be ok.

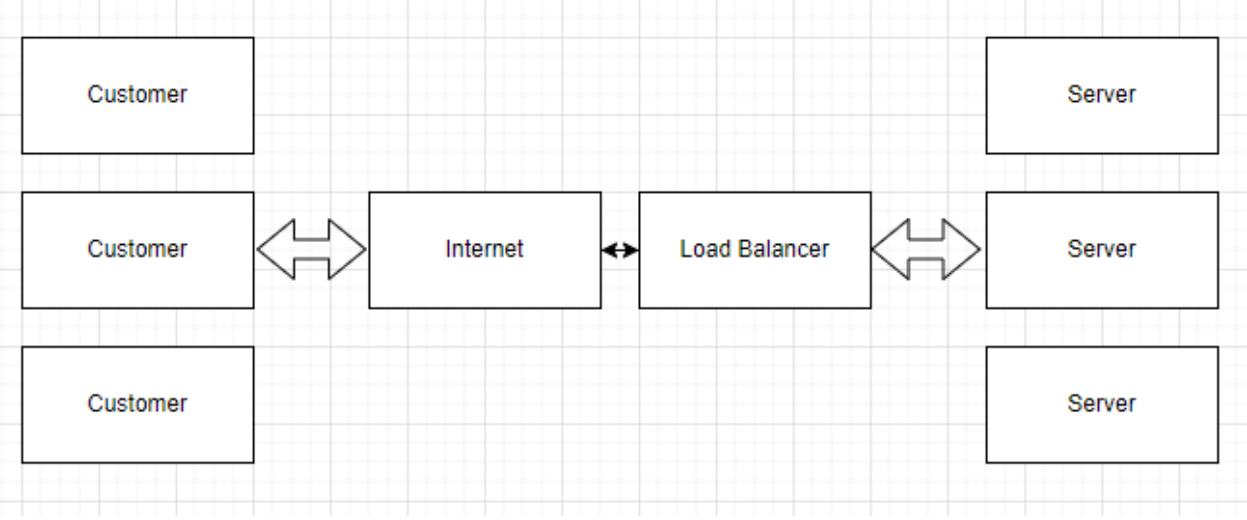
The implementation of a network would follow the steps of the OSI model. The layers of the model would serve as a checklist for completion. As each layer is passed, built in confirmation messages of transmission would provide confirmation. TCP/IP protocols will be followed for implementation.

Rough estimate on implementation of a network upgrade would price out at $100,000.

Here is a quick visual representation of what the upgraded network architecture could look like based on the recommendations. Wi-Fi routers would be placed at strategically placed locations throughout the facility to mitigate connection dead zones. The chart is meant to read left to right starting with the events that occur upon internet traffic arriving at the gates of the network (firewall). These clients could be either requesting packets or sending them, so the process flows need to be prepared for both.



We have another visual diagram explaining how the network would serve customers through the channels of the internet when accessing the FloorsRUs website. Customer data could pass through the internet into company databases for marketing campaigns or issues with customer orders. Orders will also be placed through the website. Customer would include all necessary shipping information.



Future Needs Analysis and Recommendations (Week 5)

TBD

References:

Tanenbaum, A. S., Feamster, N., & Wetherall, D. J. (2020). *Computer Networks* (6th ed.). Pearson Education (US). https://coloradotech.vitalsource.com/books/9780135407981