Report on Lan Topology for Fayetteville NC Project

William Pascoe

IT-212: Intro to Computer Networks

Brent Newcomb

August 16, 2025

Report on Lan Topology for Fayetteville NC Project

We're excited to announce our expansion into Fayetteville, North Carolina! Our new office will be staffed by fifty employees, including our new Executive Vice President of Sales and Marketing. To ensure a successful launch, we need to set up our new location for optimal performance from day one. This includes establishing reliable internet with sufficient bandwidth for all staff and teleconferencing needs as well as a robust network infrastructure, including switches, firewalls, computers, and cabling, to ensure seamless operations and maintain data security. We will also need to carefully consider our budget and the distance from our home office.

To ensure a successful launch and future scalability, getting our IT infrastructure right from the start is crucial, saving both time and money. Our staff will primarily use laptop computers, necessitating docking stations for reliable hard-wired network connectivity. For network traffic management, we will require switches. Understanding the OSI (Open Systems Interconnection) model is key here. The OSI model provides a standardized framework for network communication, making troubleshooting more efficient. Layer 2, the data link layer, switches are designed for relaying information within a local network, based on MAC addresses. Layer 3, the network layer, devices, like routers, handle data transmission across different networks using IP addresses. I recommend implementing Layer 3 switches. These devices combine the functionality of both Layer 2 switching for local traffic and Layer 3 routing for inter-network communication, offering a more integrated and efficient solution. To secure our data, we will employ a multi-layered approach. A network firewall will protect the overall office network, while each laptop will have antivirus and firewall protection installed on it.

Implementing domain logins will also enhance security by allowing centralized control and enabling remote lockdown or data wiping if a laptop is compromised or stolen.

To handle our daily internet traffic, teleconferencing needs, and VPN tunneling back to the Albany office, we'll need a fiber internet connection. Fiber offers substantial bandwidth and high reliability, ensuring we're always connected. A site-to-site VPN will also be crucial for seamless connection to our home office, enabling file sharing and printing between locations.

This project comes with two main constraints budget and distance. We need to be mindful of spending, making wise decisions like purchasing reasonably priced computers and potentially recycling unused equipment from other offices. We'll also get competitive bids from contractors to ensure cost-effectiveness as far as distance goes, Fayetteville is about 700 miles from Albany, which presents challenges for centralized IT support, meetings, and other office functions. While VPN tunneling will connect our networks, the significant distance could still impact performance and communication.

When it comes to network topology, several options exist. One type is the tree topology. This type is easily scalable and allows for growth and expansion. The con to this type is that it can get complex the larger it grows and if there is a failure near the top it can put several other computers out of service as well. Another type of topology is the star type. With this type each computer has a direct connection to the server. This means if one line goes down it won't affect other computers, which makes troubleshooting easier. However, running all the cable makes this type cost more than other topologies. For our office I would recommend the star topology. While it might require more cabling and potentially more switches, the increased reliability and easier problem isolation make it the best choice for us, minimizing catastrophic failures. With this topology we will have a centralized switch or maybe switches and then we will run ethernet cables to each workstation and needed location throughout the office suite. By having a standardized labeling system we will be able to identify any problems that occur and either make repairs or move that workstation to another branch and get them up and running quickly.

As for our IP addressing, we'll use a Class C range (192.168.0.0 to 192.168.255.255). This range provides ample IP addresses for our current needs and allows for future expansion without issue, especially by utilizing private IP addresses with public router addresses.

The Fayetteville area has several internet providers that offer reliable business internet connections. The two that I have looked at as being good for the company are Metronet and Spectrum. Metronet is a nationwide internet provider offering services in 19 states. The coverage in the Fayetteville area is limited, however, with only 69% of the area available in the city and surrounding areas (*Metronet Internet: Coverage & Availability Map*, n.d.). This will limit our usage depending on the final decision of what part of the area the office is located in. They do offer fiber internet and have reliable speeds up to 5 Gbps. Another provider that offers a lot more coverage is Spectrum. Their coverage is almost anywhere in the city and surrounding areas (*Spectrum Internet: Coverage & Availability Map*, n.d.). They also offer fiber internet with reliable speeds up to 100Gbps. Both providers offer security built in and would work for our business needs.

The provider that I think would be best for our situation would be Spectrum. They offer faster speeds to allow teleconferencing, and office needs as well as allow expansion in the future. They also have the biggest coverage area so any physical office considerations would be met.

The next consideration for the office setup is hardware and software. For hardware on top of the switches, routers and cables, we will need to use laptops for all office staff. This will allow hybrid work environment of both at home and office work. To make internet connections easier we will use docking stations for the staff for when they come into the office to work. This way they can plug in and get to work and do not have to worry about connecting cables or finding outlets for charging. Each laptop will have BitLocker disk encryption, anti-virus software and data loss prevention (DLP) to ensure that our network and data are kept safe and secure. We will use firewall protection at the office to deter data breaches. For teleconferencing we will use conference room web cameras and teleconferencing table phones. This will allow everyone involved in the meeting to be heard and make any presentation seem professional.

The printer we will use will be a networked copier, printer and fax machine. We will use badge login to track and control access to documents being printed. By using a networked printer, we can save on buying multiple printers and ink and make tracking what is printed and by whom easier. This adds another layer of data security. The site-to-site VPN will also allow for jobs to be printed back in the NY home office if special documents and signage are needed over there.

Bandwidth will also be an important consideration. For teleconferencing we will need a range of 3-5Mbps for group calls with high quality video to 500Mbps for the entire office network. With our prospective internet provider able to offer up to 100 Gbps internet speed we should be able to easily meet these needs while being able to maintain other office functions on a stable connection.

As you can expect, with a network that is this big and could potentially get bigger, there can be potential errors that occur. Some of those errors include slow network, connectivity issues and security breaches. Using constant monitoring tools and troubleshooting techniques we will be able to resolve most issues quickly.

Slow network speeds refer to reduced data transfer rates across a network, impacting tasks like file downloading, web browsing, and video streaming. The causes of this range from bandwidth limitations, network congestion, outdated hardware, or misconfigured network settings (Buenning, n.d.). To troubleshoot this, we will use network monitoring tools to aid us in determining any misconfigurations as well as network congestion. If we need more bandwidth we will go with our internet provider to offer us more. We will also use software tools to ensure that our hardware and software are up to date.

Connectivity issues can be either physical or things like not connecting to the printer. This can be caused by damaged cables, or in case of not connecting to printer, network congestion. We can troubleshoot these problems with network tools, like cable testers.

Security breaches can sometimes be the hardest problems to detect. With monitoring tools like SIEM, security information and event management, and log reviews we can hopefully quickly identify if there is a security breach and what the cause was. We can deter attacks by using firewalls, keeping software up to date, and doing things like account login for computers. Alos having access controls for the office and printer usage will also add another layer of security and help deter someone who is not authorized to be in the building coming in and stealing data.

There are many network monitoring tools on the market to help us with our operations. Network monitoring provides visibility across a business network. With fast, in-depth insights into the full range of network devices and services, admins can better manage network connectivity and troubleshoot issues (SolarWinds, n.d.). SolarWinds and Manage Engine seem to be good options for us. The SolarWinds Network Performance Monitor will aid in discovering network devices for monitoring. The Manage Engine suite of tools will aid us with network monitoring, asset inventory as well as other needed tasks. I think this suite is a better option for us. Using Patch manager plus to keep us up to date, Ops Manager for network monitoring and Asset explorer to help control inventory we can cover all the bases and use minimal programs. Another software tool that we can use to troubleshoot network issues is Wireshark. Wireshark is tool that monitors packets of data moving across the network. This can be useful when we are experiencing things like packet loss.

References:

Metronet Internet: Coverage & Availability Map. (n.d.). BroadbandNow. https://broadbandnow.com/Metronet

Spectrum Internet: Coverage & Availability Map. (n.d.). BroadbandNow. https://broadbandnow.com/Spectrum-Internet

Buenning, M, (n.d.) 8 Common Network Issues & How To Fix Them. NinjaOne. *https://www.ninjaone.com/blog/common-network-issues/*

Solarwinds. (n.d.). *Network Monitoring Software*. Www.solarwinds.com. https://www.solarwinds.com/network-performance-monitor/use-cases/network-monitoring-software

ManageEngine. (n.d.). *ManageEngine - IT Operations and Service Management Software*. Www.manageengine.com. https://www.manageengine.com

Wireshark Foundation. (2024). *Wireshark*. Wireshark.org. https://www.wireshark.org/