For the communications media I would choose fiber optic cabling as it is best for media streaming. Fiber optic cables are immune to electromagnetic interference, highly resistant to eavesdropping, and support extremely high data transmission rates (TestOut, 2022). Also, you can run optic cables long distances without needing a repeater (TestOut, 2022). Multi-mode should be used for the modal dispersion due to the multiple paths. This helps spread the signal in time because the optical signal is not the same for all modes. The connector type will be ST connector because it can support single-mode and multi-mode cabling. Also, you can switch multi-mode fiber to copper Ethernet wiring (TestOut, 2022). The mode of transport will be full duplex so it can send and receive at the same time. This mode requires Network Interface Cards NICs to be capable of full duplex (TestOut, 2022). Also, a switch will have to be used for the dedicated switch port using one per port. A full duplex will support bandwidth of 100 Mbps for a 100BaseT (TestOut, 2022). This communications media is part of layer one of the OSI model. This layer is responsible for transmitting raw bits. The physical signal is transmitted over a hardware transmission medium (TestOut, 2022) like a switch or router. The physical layer is anything referring to hardware that can send or receive data. I would also be using User Datagram Protocol for this as it is best with streaming services because of how fast the connection is, where Transmission Control Protocol is slower and not used for streaming services because of the three-way handshake.

The common network hardware components for this new location would be network interface cards for fiber optic cabling in full duplex mode. Also, a switch for full duplex mode for optic fiber cabling. Finally, a router for connecting the switches and connecting employees to other offices in Albany, NY, and Springfield, MA. Also, we need a firewall to block certain unwanted traffic from unknown external sources.

The IP range for a company of 50 employees including vice president of sales and marketing would be limited because the office only has 50 employees. The IP address of 192.168.1.13 on a subnet mask of 255.255.255.0 on a class C subnet mask is leaving 254 IP addresses. The 192.168.1.0 is reserved for network ID and the broadcast is 192.168.1.255. To remove unwanted IP addresses that could put the company in jeopardy of someone else connecting to their IP address. There should be an IP range of 192.168.1.20 to 192.168.1.70, with 192.168.1.1 to 192.168.1.20 being reserved for more control over the network that can help you deny certain services on the network. By limiting the number of IP addresses on the network, we can ensure that only the office employees are connected. Also, by implementing a firewall we can set rules and group policy for the 50% of employees who use VPN (Virtual Private Network) connection to access company resources.

The possible LAN topologies that could be used are bus, ring, star, mesh, and hybrid for the new building.

Having a bus topology is bad for this network because a bus at best can support five to ten people, this network has fifty people to support. Also, packet loss is high for a hub and the hub is slow compared to other types of topologies (GeeksforGeeks, 2020). The bus topology benefits are it is easy to connect or remove devices without affecting other devices on the network (GeeksforGeeks, 2020). Having a ring topology is bad for this network because if one computer goes down it can affect the flow of data. Ring topology must travel to all nodes on the network and replacing or removing any node can affect network activity. The benefits of ring topology are equal access to resources and speed to transfer the data is extremely high because of the topology (GeeksforGeeks, 2020). The ring topology is not scalable, and all computers must be turned on to communicate with each other (GeeksforGeeks, 2020). Having a mesh topology is bad for this network because the maintenance is difficult and inflated cost. The installation of a mesh topology is extremely difficult and complex to set up. The mesh topology has a substantial risk of redundant connections and is higher cost to install than other topologies (GeeksforGeeks, 2020). The advantages of a mesh topology are failure to a single device will not break the network and fault identification is straight forward (GeeksforGeeks, 2020). The star topology is best for this network as everything is connected at a central location and is easy to install. Cons of a star topology are that they are more expensive than a linear bus topology. If the network switch fails, the connected devices cannot connect to the internet (GeeksforGeeks, 2020). Also, star topology is very scalable and has no disruptions to the network when connecting or removing devices (GeeksforGeeks, 2020). The hybrid topology is another topology that is difficult to install and requires lots of cables. This topology is expensive (GeeksforGeeks, 2020). If there is a change in hardware the nodes can be exceedingly difficult to manage and control for the network. Hybrid’s advantages are flexibility, reliability, and handle a larger amount of traffic (GeeksforGeeks, 2020).

The LAN topology used would be a physical star topology. This would require the switch to be used for fiber optic cabling connection. A benefit of this is it is easy to administer and add new nodes or disconnect nodes without affecting the whole network infrastructure (GeeksforGeeks, 2020). This topology could also have a logical star or bus to be paired with the physical star topology if needed.

Internet service providers to compare are cable and fiber. Cable uses existing cable tv lines to provide bandwidth for internet access. Speeds of cable internet service providers are much faster than those provided by Digital Subscriber Line or DSL. The bandwidth of all users is shared in the same area as a neighborhood and actual speeds may be much less than the maximum (TestOut, 2022). Fiber internet service providers provide internet access through light signal transmitted to the end user by way of fiberoptic cables. The speed of fiber ISP are much faster than those provided by any other form of connection. The downfall is how expensive the fiber is and how time consuming the job can be because of the fragile fiber optic cables (TestOut, 2022). Cable security according to (NCTA, 2021) is good for IoT (Internet of Things) technology such as a light bulb being attacked to criminals attacking compromising healthcare equipment. The security of fiber ISPs is better because of the way it transmits its data by way of pulses of light across very thin strands of glass or plastic fiber (Charter Communications, 2019).

The reliability of cable ISPs is good if there is a storm but due to cable internet being connected by areas or neighborhoods you can get slow internet connections. Fiber ISPs are good for reliability because of the way they transmit data. The only way connection is lost is if a severe storm manages to wreak the ground because in this environment fiber optic cables should be placed underground for protection. Also, if the power goes out the fiber is still working which can let you still access the internet if the router has a backup generator to power it on (Goldman, 2021).

The fiber ISP meets the business goals and objectives of the location. Fiber is the fastest connection speeds, which will help when streaming live video teleconferencing calls and if the power goes out you can still send print jobs to billboard printers located in the company headquarters in Albany.

A hardware solution would be to have device metrics to help the IT department to troubleshoot problems. By checking CPU utilization, hard disk utilization, memory utilization, and temperature inside the computer. A hardware solution would be NIC teaming configured in a switch independent for fault tolerance. This will help make certain that if one NIC fails the other will take over to remain accessible on the network (TestOut, 2022). A hardware solution would be a load balancer to separate the workload between two or more computers which allows you to have higher resource utilization, throughput, and response time (TestOut, 2022). A surge protector is great for protecting equipment damage by preventing overvoltage situations (TestOut, 2022). A generator can help by providing backup power for an extended period, normally between 24 and 48 hours (TestOut, 2022). Multipathing is a fault-tolerance technique to help CPU and mass-storage appliances by giving two paths between them (TestOut, 2022).

For software solution network performance could help by measuring the bandwidth utilization, error rate, and latency. For software log file management log messages should be used. These help with timestamp of incident which indicates when the message was created. For which facility created the message such as “lpr” for printer subsystem (TestOut, 2022). Severity level for how serious the incident is. Mnemonic to help admins know the nature of the message. Message text to describe the event. Interface reset which indicates the number of times an interface has been completely reset. This happens if packets queued for transmission were not sent within several seconds. A packet sniffer is software that will capture records frames transmitted on the network (TestOut, 2022). A throughput tester can help test UDP by knowing if the bandwidth is below what it needs to send data. This device sends a specific amount of data through the network and measures the time it takes to transfer that data which gives the IT team the bandwidth measurement. Network interface monitor helps users know why their internet is slow by identifying the root cause of performance issues and network bottlenecks (TestOut, 2022). Finally, remote desktop protocol for VPNs (Virtual Private Network) to gain access to the network infrastructure to do their jobs effectively. Also, a packet analyzer to copy frames and view frame contents (TestOut, 2022). This also allows you to check for specific protocols on the network and check devices using restricted protocols (TestOut, 2022).

For printer configurations a wireless printer so that VPN (Virtual Private Network) employees can print from their remote locations. For printing from remote locations employees can use Google’s cloud print as remote employees only need to make a google account to use this. Another option is the new location can make a google account and share their printer with other employee accounts so that they can use the organizations printer. For tracking devices, you can use ThinPrint which is software that collects data on enterprise-wide printing activities and enters them into a SQL database (ThinPrint, 2022). IT admins can see this tracking and reporting website from anywhere and can adjust group management to make a group of users who use too much of the printing services or can import them into the active directory for a more detailed analysis (ThinPrint, 2022). The IT department can view trends of how the print volume has developed over time, distribution of which groups or users have printed the most and give an overview of the number of print jobs (ThinPrint, 2022). Thin print can track, automate drive distribution, and control access for users or groups by importing them into the active directory. Printer could also use driver updates provided by windows if the device is registered with Windows, it can do it automatically or can be turned off manually (TestOut, 2022).

Bandwidth for video conferencing should be 1.5 to 2.0 Mbps (Bell, 2021). The company should use 802.11ax for the best performance for their video conferencing and video streaming in high density environments. 802.11ax allows you to broadcast in more populated areas and can operate at 1 to 7.125 GHz range. Operating at 6 GHz allows more channels than operating at 5 GHz. Orthogonal frequency-division multiples access or OFDMA helps by making wireless channels into sub channels. It can divide a channel into 30 segments, assigning each segment a single device, and can send or receive signals at the same time (TestOut, 2022). 802.11ax has a technology called Basic Service Set Color or BSSC that the client transmits to identify them (TestOut, 2022). 802.11ax can help access points or APs by allowing them to function in the same radio frequency channel. Also, it can help with the latency between APs and wireless devices (TestOut, 2022). Finally, 802.11ax has a Target Wake Time or TWT. This technology can schedule a time for APs to communicate with devices at a certain time (TestOut, 2022). This solution provides devices with more channels to connect to while receiving or sending signals at the same time. Along with identifying clients by the color they transmit, allowing APs to function on the same radio frequency, and helps with latency between the devices and APs. TWT can help with large organizations that need constant connection for updates and activation (TestOut, 2022). Also, TWT helps by setting certain times for APs to communicate with devices.

Common networking issues that could occur on the new site are hardware failure to servers, routers, and computer failure to disks and tapes (TestOut, 2022). Another issue that could arise is gradual loss to optic fiber cabling which can cause signal loss (TestOut, 2022). Lastly, DNS issues in which a URL does not connect to the correct site (TestOut, 2022).

To troubleshoot these issues for the new site you could use a ping for the DNS issue to test the connection of the DHCP server (TestOut, 2022). If there are still issues the next step is to test the DNS configuration (TestOut, 2022). You can use the command line tool NSLOOKUP and dig to know if the domain server address matches the output from the command. If it does not match the domain server then it might not be updated since the non-authoritative server changed the address (TestOut, 2022). To troubleshoot hardware failure to routers or servers you can use the command line tool traceroute to see which router or server is failing (TestOut, 2022). The exact command could be traceroute [server name] or [IP address] after the command to identify the failing router. Finally, for troubleshooting low optical link budget you can use an optical power meter to measure the signal strength of the optic fiber cables (TestOut, 2022). Another tool according to (Orbitco, 2015) is using the “Optical Time Domain Reflectometer (OTDR) is an instrument used to create a virtual picture of a fiber optic cable route. The analyzed data can provide information on the condition and performance of the fibers, as well as any passive optical components along the cable path like connectors, splices, splitters, and multiplexers.” Also, for remote employees for this new site the ping command line tool should be used to see if the organization's connection to remote workers works at all (TestOut, 2022).

The resolution to the first network issue is meant by testing if the DHCP server is faulty first. If it is, the address is removed from the pool until the administrator resolves the problem by renewing their IP address, if it is IP address conflicts. If it is the DNS server then using NSLOOKUP can resolve the issues by troubleshooting the DNS server and host name. To troubleshoot hardware failure to router or servers use traceroute to find which router or server is failing and troubleshoot or replace the router to fix the problem. Finally, for troubleshooting low optical link budget use an optical power meter to measure if the fiber optic cable is sending enough signal strength for connection. If it is not sending enough strength it needs to be replaced to regain connection for remote workers to connect to the organization. Another tool that can be used for this is the Optical Time Domain Reflectometer as this will resolve the low fiber optical link budget issue by analyzing the performance of the fiber optic cables along the components such as connectors, splices, splitters, and multiplexers. This resolves issues by finding if any of these are affecting the cable enough for low signal strength.

For network monitoring a great one would be packet analyzing because you could view protocols of the network and identify frames on the network that could be causing errors for video transmitting and video conferencing. This network monitoring tool helps also by troubleshooting communication problems and investigating the source of heavy network traffic (TestOut, 2022). A packet sniffer would also be great for this type of new site because you can view packet contents sent from remote workers and analyze packets sent to and from a specific device (TestOut, 2022) helping security for the new site as sixty percent of the employees work from home, this will help monitor their traffic. Logs should be used for software applications to see how much of the system resources are being used such as processor, memory, and disk (TestOut, 2022). Also, IP scanners will be used to scan all IP and MAC addresses to stop attackers from exploiting vulnerabilities (TestOut, 2022). Port scanners will be for finding which ports are open on the network and what services are accessing them (TestOut, 2022).

Patch management options should be to have a group policy to select when feature updates, quality updates, and preview builds are received (TestOut, 2022). Also, use configuration manager tool to update business policies (TestOut, 2022). Windows update troubleshooter should be used in case something goes wrong during the update so you can restart (TestOut, 2022). This troubleshooter tool will help employees troubleshoot on their own as sixty percent of them are remote helping the organization not get an overflow of the same troubleshooting errors by employees. Update deployments will be semi-annually. Organization will defer automatic installed updates to wait for bug fixes or hot patches for applications. The new site will use lab testing or pilot deployments to test the latest updates security.

To control inventory the new site will use Internet Small Computer Systems Interface (iSCSI) because according to (TestOut, 2022) “the storage devices on the remote iSCSI target appear to the operating system on the iSCSI initiator as locally attached hard disks. The iSCSI initiator sends SCSI commands within IP packets to the iSCSI target over the network.” The SAN technology used would be distance because sixty percent of employees at the new site are remote and could be anywhere around the world. This technology helps accommodate for longer distances.

**References**

Bell, P. (2021, January 29). What Internet Speed do you Need for Video Conferencing? MegaMeeting. https://www.megameeting.com/news/what-internet-speed-for-video-conferencing/#:~:text=Video%20conferencing%20typically%20requires%20around%201.5%20to%202

TestOut. (2022). TestOut LabSim. Labsimapp.testout.com. https://labsimapp.testout.com/v6\_0\_525/index.html/productviewer/1190/9.1.6/1159b9ea-e076-4320-9aed-f022b1465c53

NCTA. (2021, October 29). How the Cable Industry Mitigates Cybersecurity Risks | NCTA — The Internet & Television Association. Www.ncta.com. https://www.ncta.com/whats-new/how-the-cable-industry-mitigates-cybersecurity-risks#:~:text=Cable%20ISPs%20are%20leaders%20in%20helping%20to%20put

Frontier. (2022). Is fiber-optic internet worth it for you? Frontier.com. https://frontier.com/resources/is-fiber-optic-internet-worth-it

Charter Communications. (2019). Why is fiber-optic communication technology more secure? | Spectrum Enterprise. Spectrum.com. https://enterprise.spectrum.com/support/faq/internet/why-is-fiber-optic-communication-technology-more-secure.html#:~:text=Fiber-optic%20communication%20offers%20higher%20security%20because%20of%20the

Goldman, K. (2021, January 26). How Will My Fiber Internet Perform in a Storm? Https://Blog.frontier.com/. https://blog.frontier.com/2021/01/how-will-my-fiber-internet-perform-in-a-storm/#:~:text=W%20hat%20makes%20fiber%20reliable%201%20Fiber-optics%20is

ThinPrint. (2022). Automated Print Management with ThinPrint Management Services. ThinPrint. https://www.thinprint.com/en/features/management-services/

Orbitco. (2015, November 9). *What is DHCP? How to troubleshoot DHCP Examples*. Orbit-Computer-Solutions.com. <https://www.orbit-computer-solutions.com/network-troubleshooting-dhcp/#:~:text=DHCP%20server%20uses%20the%20ping%20command%20to%20detect>

GeeksforGeeks. (2020, November 20). Advantages and Disadvantages of Star Topology. GeeksforGeeks. https://www.geeksforgeeks.org/advantages-and-disadvantages-of-star-topology/#:~:text=Disadvantages%20of%20Star%20Topology%201%20Requires%20more%20cable

GeeksforGeeks. (2020, November 1). Advantages and Disadvantages of Bus Topology. GeeksforGeeks. https://www.geeksforgeeks.org/advantages-and-disadvantages-of-bus-topology/#:~:text=Disadvantages%20of%20Bus%20Topology%20%3A%201%20Bus%20topology

GeeksforGeeks. (2020, October 20). Advantages and Disadvantages of ring topology. GeeksforGeeks. https://www.geeksforgeeks.org/advantages-and-disadvantages-of-ring-topology/#:~:text=Disadvantages%20of%20Ring%20topology%20%3A%201%20Due%20to

GeeksforGeeks. (2020, October 30). Advantages and Disadvantages of Hybrid Topology. GeeksforGeeks. https://www.geeksforgeeks.org/advantages-and-disadvantages-of-hybrid-topology/#:~:text=Disadvantages%20of%20Hybrid%20Topology%20%3A%201%20It%20is

GeeksforGeeks. (2020e, November 25). Advantage and Disadvantage of Mesh Topology. GeeksforGeeks. https://www.geeksforgeeks.org/advantage-and-disadvantage-of-mesh-topology/#:~:text=Disadvantages%20of%20Mesh%20Topology%20%3A%201%20It%E2%80%99s%20costly

TestOut. (2022). TestOut LabSim. Labsimapp.testout.com. https://labsimapp.testout.com/v6\_0\_520/index.html/productviewer/1190/5.1.2/1159b9ea-e076-4320-9aed-f022b1465c53

.