Introduction to Networking Final Touchstone

Sarah Gillard

November 4th, 2023

Sarah Gillard
90 Some Lane
Somewhere, MA 12345
781-555-5505

11/04/2023

Chris Nelson
President
Greenfield Properties
123 Sophia Way
Minneapolis, MN 55000

Dear Mr. Nelson:

Thank you for allowing me to make networking recommendations for your new company, Greenfield Properties, during its merger of Bluegrass Rentals and Redstone Property Management. I am excited to share my suggestions with you and hope they serve as informational guidance along the way.

I have reviewed all the requirements and recommendations you have provided for the network at Greenfield Properties. I will be sure to include these in my proposal. I will be sure to focus on the network's availability, security, ease of use and administration, plus room for potential growth.

After you have reviewed my recommendations, we should plan to meet with your IT staff and create a finalized plan for implementation. Please let me know if you have any questions about my report and when you are ready to plan our meeting. I look forward to hearing from you.

Sincerely,

Sarah Gillard

Introduction

This document guides Greenfield Properties as they go about creating a new network to support their new company formed from the result of merging Bluegrass Rentals and Redstone Property Management.

Network Infrastructure

The new company, Greenfield Properties, will have 46 employees. There will be 26 PCs, 30 tablets, and 39 smartphones, totaling 95 devices used amongst the employees.

Bluegrass Rentals and Redstone Property Management both use peer-to-peer networks, which means each has a network of connected peer computers with no central controller. Peer-to-peer networks are most beneficial to small companies where employees can access shared resources without extra permissions. Greenfield Properties is justified in the decision to move to a client-server network since most larger companies use this network architecture. A client-server network is a network in which a client computer requests resources from a server computer. In this architecture, network administrators can manage access to company resources, like files and databases. All Greenfield Properties employees must be able to access shared resources like files and printers, as well as access to the company's custom-built property management app.

However, certain employees need access to specific secure databases, and a client-server model allows administrators to grant access to only those employees who need it. The company wants to require the network to authenticate users and authorize them for the privileges they need to do their work, which the client-server architecture will allow.

A local area network (LAN) is an interconnection of computers that are in relative proximity to each other. Greenfield can maintain a LAN as the new office building is in one location and comprises one floor. When working remotely, employees will be able to gain access to the company's resources stored on the LAN, which we will discuss later. A LAN has high bandwidth and low latency, adding to its benefits. A WAN is not the best choice as it tends to have low bandwidth and high latency. Therefore, we will provide ways for remote employees to gain access to resources found on the office LAN. In the office, PCs will be able to connect to the LAN via Ethernet, which provides higher security. Wireless devices such as tablets and smartphones will access the LAN wirelessly through access points.

When it comes to wiring, copper cables are less expensive but lack bandwidth when compared to fiber-optic cables. Since the company wants to prioritize good-quality hardware and software over keeping costs as low as possible, fiber-optic cable is preferred. Fiber-optic cable does a better job of maintaining high availability since copper can encounter interference emitted by other electronics. Fiber is immune to both electromagnetic and radio frequency interference due to using light impulses rather than electricity to transmit signals. Fiber also offers higher security with encryption. Unfortunately, fiber-optic is more challenging to install and troubleshoot but is still advantageous compared to copper.

I recommend using single-mode fiber because it is best at spanning long distances and fasted at transmitting data. Multimode fiber won't be the best choice as it can be unreliable after 3,000 feet, so it's typically used only within a small area of an office. Greenfield Properties is about 60,000 square feet, as its dimensions are 300 ft x 200 ft.

A Client Operating System functions on an individual user's personal computer, and a Server Operating System runs on a network server. Therefore Greenfield Properties will want to use a Server OS. The company will want to select various Server OS connections. I recommend the following:

- A web server to connect to web pages and web-based applications.
- A mail server to store and forward incoming and outgoing email messages on the network.
- A file server that will allow all employees to store and access shared files, and for certain employees with special permission to access other files upon authentication.
- A database server, so authenticated employees can access specific server databases to run queries and other requests.
- An application server, which makes applications remotely available to network users. All employees will need access to the company's custom-built property management application from anywhere.
- A print server so all employees can access the company's shared printers from anywhere.

I recommended that these servers be a hybrid of on-premises and cloud-based. Cloud-based will be beneficial as not all employees will be working on-premises each day, but they will still need access to the network resources such as files and printers. However, cloud-based servers will go down in the event of an outage, so an on-premise server will be beneficial during these times when employees must maintain access to network resources.

I suggest using Windows Server, which is Microsoft's server product. IT will have less of a learning curve than with some other server operating systems due to its Graphic User Interface (GUI. This server is not command line-based and will not require the administrator(s) to learn many new commands. A drawback is that Windows-based products are frequently targeted by malware, but we will address this later when reviewing the network's security.

Multiple servers will be virtualized on a single physical server because this will enable a single physical computer to have multiple OS instances installed and running concurrently. I suggest implementing OS-level virtualization as it requires less overhead since you don't have to run

multiple copies or server OSs at once. One drawback is that Windows Server must be used on all computers as each must have the same OS.

I suggest using the Datacenter Azure Edition version of Windows Server as it is the same as the Datacenter version but with additional Azure support. The Datacenter version will work for large networks and has an unlimited number of users per license. It will also allow for the designation of a Network Controller, which will work well for Greenfield since there are 46 employees, and may be more in the future. Plus, they want a controller who can grant authorization to employees based on what they need access to for their particular position. With the added Azure support, remote employees will be able to access the cloud platform Azure.

Network Segmentation and Printing

Subnetting allows one large network to be segmented into a set of smaller networks, which brings ease of use to network administrators as it is easier to identify and troubleshoot issues on these smaller networks than if they were one large network. With subnets, devices will not have access to the entire network, so the company can provide appropriate hardware to users depending on what their role needs access to. This is an added layer of protection for sensitive data that not all employees will need access to. In a subnetted network, traffic is decreased on each broadcast domain as more broadcast domains (these are created by routers) means less network traffic on each network subnet. This will help improve network performance and prevent bottlenecks that can cause lags.

I suggest that the company have a LAN in-office and provide access to remote employees via VPN and VLAN, which I will soon discuss in more detail. I propose four subnets as follows:

- **In-Office devices using LAN or VLAN**: For full-time in-office workers, which includes these devices: 15 PCs, 2 tablets, and 10 phones. For hybrid employees, this includes 10 PCs, 28 tablets, and 28 phones. In total 93, so have room for 100.

- **VoIP (Voice-Over Protocol):** This will need to support at least 38 in-office devices using VoIP, which employees will need for phone calls and videoconferencing. In total 39, so have room for 45.
- **Remote devices (using VPN and/or VLAN):** This will need to support 1 PC and 1 phone fully remote, plus 10 hybrid PCs, 28 hybrid tablets, and 28 hybrid phones. Need room for 68 current remote/hybrid workers, so make room for 75.
- **Printers:** This will need to support the 12 printers, but add the potential for 5 more for a total of 17.

This subnet is not large, with 108 devices currently (PCs, tablets, phones, and printers), so it's not large enough that segmenting by department makes sense, and there is only one office so segmenting by office is not necessary here. It will be beneficial to segment by different functions, such as VoIP, remote connection to the VLAN, and printing. With four subnets and up to 126 hosts per subnet at 25 mask bits, the subnet mask would be 255.255.255.128 and the host address range should be 192.168.0.1 - 192.168.0.126.

Subnets and VLANs (Virtual Local Area Networks) are both used to break down a network into smaller networks. A subnet separates networks physically and a VLAN separates networks virtually. I do recommend implementing VLANs as well as the subnets because VLANs can help connect in-office workers with remote workers. VLANs also provide ease of use to administrators when making changes to the network infrastructure. A downside to VLANs is that they come with a high threat of infection as one infected system can spread throughout the entire network.

I propose also utilizing a Virtual Private Network (VPN) which will connect authorized users to the corporate network resources and encrypt data to increase security. A VPN is an excellent

way to connect remote workers to the main office with an added layer of security. The VLANs will help to segment and manage network traffic virtually, the subnets will help manage and segment the network physically, and a VPN will help create secure connections for remote workers who need to access the network remotely while still managing the privacy of data.

Printing

Printers can be connected to a network using a print server or using direct IP printing. There are many pros and cons to each of these printing deployment types. Below I will provide a brief overview of some of these pros and cons.

Pros of Using a Print Server: ● Scale well as companies grow (can add new users and update permissions as needed) ● Distributes and prioritizes jobs to prevent backlogs ● Easy setup and management with steps laid out in your OS ● Can enable print reporting and auditing to see where money goes and adjust print policies accordingly ● Automated driver updates pushed ● Increased security- allows control over who can print what and where ● End users aren't in charge of adding or updating printings themselves, leading to simplified use for employees	**Pros of Using Direct IP Printing**: ● Easiest set-up for administrators ● No single point of failure ● Lower network traffic, maintenance, and cost ● End users have control over their printing which can be an advantage with troubleshooting that takes some work off the IT department ● There is no additional hardware to buy or maintain
Cons of Using a Print Server: ● Hardware, software licensing, and maintenance can be costly ● There is a single point of failure ● Centralized management is advantageous, but also increases the workload of IT staff	**Cons of Using Direct IP Printing**: ● Users have control over their own drivers and print settings, creating more work for them and less control for the administrators ● Becomes unmanageable as company size increases and workers are within multiple locations or remote ● Time-consuming for IT to configure ● Software updates are inefficient as IT will need to configure each workstation individually

I suggest using a print server to deploy the printers because of the increased security, ease of use, and management for the IT staff as the company grows, and the ability for the company to audit and adjust printing policies to be sure money on printing is well-spent. Direct IP printing will be more time-consuming for IT to set up and maintain as they cannot push out updates in bulk or have employees printing from multiple locations. Greenfield Properties employees will need to be able to access the company's printers from any location.

Wi-Fi Networking

Currently, there are 69 wireless devices (tablets and smartphones) and with room for 50% future growth, there should be room for 104 devices to connect to the network wirelessly. Network interface cards (NIC) are built into the devices, but you will need to install wireless access points (WAPs) to make the wireless network operate. Since the office building is one floor, flooring will not interfere with a WAP antenna, but walls can affect the reception.

It is best practice to enable security from the moment you turn on an Access Point (AP) so IT should plan to configure the APs right away. Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) allow data to be encrypted before being sent over a wireless connection. To configure the WAPs, you will need to pick a key to be used for the connections. WPA3 should be used as it is the newest version of this protocol and therefore the safest to potential threats. You will enter shared keys which will be a chosen password that must be protected and private. Then the device will hash the password into a key.

Setting up too many WAPs can cause interference if they are nearby and this results in slower speed and poorer connection quality. Too many WAPs can also create security risks if an attacker moves throughout them, making it harder for them to be tracked. Greenfield Properties office space is 300 ft x 200 ft for a total of 60,000 square feet. The WAPs should be placed

about 150 feet apart because the signal can typically extend that far as long as there are no thick walls. It is recommended that you have a WAP for every 800 square feet, so we would want 75 of them (60,000 square feet / 800 = 75) placed about 150 feet apart. Most of the WAPs can be installed in the ceiling which keeps them out of the way and adds extra security due to the hidden access. If possible, there should be at least 50 WAPs located near power outlets for the 17 full-in office employees and 28 hybrid employees, plus potential new employees, who will connect their PCs to a WAP for Ethernet connection which provides a more secure connection than a wireless connection. A wireless connection will be needed for the tablets and smartphones. All WAPs should be set to the same service set identifier (SSID) so that the name of the WiFi network will be known and seen when employees search for the wireless connection.

A wireless LAN controller is a device that manages and monitors all the WAPs in a single wireless network. A wireless LAN controller provides security as the network administrator can control wireless users' access privileges and prevent unauthorized wireless connections. It is also cost-effective due to the ability of the controller to deploy and monitor all WAPs from one central location. It also allows nearby APs to increase their power when a nearby AP goes down due to interference detection, which will help the company maintain excellent availability in the network.

Security Measures

I feel my current recommendations will best suit the needs of Green Properties. However, I already mentioned that despite the many advantages of this setup, there are downfalls when it comes to security. Therefore, I will now discuss ways we can make the network secure and protected from potential threats.

Physical Security

The company can use a multiple-barrier system to protect physical access to the servers. A security system should be designed with multiple points of access control. I suggest a key fob for the door to the room where the servers will be located, as well as biometric authentication to get through another door that leads to the servers. This biometric authentication can be a fingerprint or facial recognition, similar to the iPhone.

Infrastructure Access

A VPN will be used to allow remote workers to connect to the network resources. Intranet VPN will allow the company to connect remote workers securely over the internet to the main office.

Authentication

Two-factor authentication should also be utilized when sensitive data is being accessed, and this means a user who is granted access will need to present two factors of authentication, such as a password and code received through email.

Lockout Policy

Kerberos should be used to authenticate users and computers to the domain, and Radius should be used to authenticate devices to the network. Kerberos establishes the user's identity when they first log into a system and it provides strong encryption. Radius authenticates devices on both wired and wireless networks. Using both will help the company establish and maintain the high level of security they wish to have.

Password Complexity Requirements

Passwords should be at least 8 characters and not contain a word found in the dictionary. They should be a combination of letters, numbers, and symbols. Employees should keep these private and not store them in a place where someone else may find them.

Firewall

I suggest using a network-based stateful firewall because we are dealing with an entire network that wants high security, and this will allow us to monitor the status of connections passing through the network. A network-based firewall is designed to protect the entire network, while a host-based firewall protects only one machine. A stateful firewall monitors the status of all connections passing through while a stateless firewall does not monitor this.

Anti-Malware

I suggest using host-based anti-malware as this is a tool you put on each computer in the network to keep them safe from online threats like malware and viruses. It's advantageous because you will have full control but you will need to update it regularly. A downside is that you might need extra hardware to store the security software. This is still better than cloud-based antivirus products as those are highly dependent on an internet connection and might only scan essential files for threats rather than the whole computer.