Scott Laird
2660 Winchester Woods Apt H
Wooster, OH 44691
(330) 347-8736

2/4/2024

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

Dear Mr. Nelson:

My name is Scott Laird and I am reaching out in response to your request to have a consultation regarding building your network for Greenfield Properties. After going over the details of the current situation and considering the potential for future growth, I believe I have the perfect solution for your company's needs.

In summary, Greenfield is preparing to move from a peer-to-peer network to a client server network. Although money is not unlimited, you wish to have a good quality, reliable network that is easy to use. The following report will give you an easy-to-understand analysis of what I think is best for Greenfield Properties and their network. I will walk you through step-by-step and provide concise details on what technologies will be used to accomplish your goals.

If you have any questions or concerns, I will make myself indisposable and follow up with you through your preferred method of contact.

Sincerely,

Scott Laird

Introduction

I have prepared the following document to explain the necessary steps to carry out your desire to implement a new client/server network at Greenfield Properties. I am aware that your IT team has limited experience with network administration and, as a result, ease of administration is a high priority. Another requirement is that your network must be very secure. This is because your employees deal with highly sensitive data such as credit card information. The final major concern is that your network must be accessible. This is because you have several associates who work remotely or in the field and must be able to connect to the company's resources. The aforementioned topics will be expanded upon and will be included in the following sections: Network Infrastructure, Network Segmentation, Printing, Wi-Fi Networking, and Security Measures .

Network Infrastructure

As you have requested, I believe a client/server network architecture will be the best option to meet your company's needs. With the amount of devices that Greenfield will have to support, in addition to the hierarchy of executives, a client/server network will provide controlled access to the company's resources whereas, in a peer-to-peer network, all the computers communicate and share information equally. The client/server will provide security and privacy by using this controlled access.

Here is an overview of the way I would set up your network infrastructure:

- Build server room to accommodate all networking equipment.
- Use Category 6A cables to connect supported devices to switches.
- Implement a hybrid "on-premises and cloud" server solution.
- Use Windows Server Standard as the operating system for the servers.
- Manage costs by using virtualization and putting multiple servers on one machine.

Because your new location will be a single-story office building, your network will be considered a Local Area Network or LAN. This network will be built with a primary Server Room and Wireless Access Points or WAPs. Wireless Access Points allow users to connect to the company's network using any type of mobile device. I recommend using Category 6A cables to connect everything in your building, from WAPs, printers, and PCs, to the servers. Cat 6A is a twisted pair cable that uses copper wires to achieve speeds of up to 10 gbps. This will provide an excellent balance of price-to-performance and will suit your needs. For cables running above the ceiling, they should be plenum-rated – meaning that they will not give off toxic gases if there is a fire that occurs.

I believe Greenfield should use a hybrid approach when it comes to the implementation of their server systems and use the following:

- File server - stores files and responds to requests to access and manage those files - located on-premises
- Active Directory server - allows controlled access and management for user authentication and authorization - located on-premises
- Database server - responds to queries and other requests from users to access stored information sets - located on-premises
- Web server – connects to the internet and responds to client requests for web pages and web-based application access - cloud
- Application server – makes applications remotely available to network users; application servers often also integrate with databases connected to the applications - cloud
- Mail server – stores and forwards incoming and outgoing email messages for a certain domain, such as the domain that the company owns - cloud
- Print server - enables multiple clients to access the services of multiple printers - cloud

I would have the file, Active Directory, and database servers on-premises and the web, application, mail, and print servers should be stored in the cloud. The file, Active Directory, and database servers would probably be the most demanding, as far as bandwidth and should take advantage of the faster ethernet connection on premises. The other servers will most likely not be as demanding and we can get by with the relatively slower network connection through the ISP.

The next concern is what type of operating systems should be implemented on the servers. I think the company should use Windows Server Standard because it has an easy learning curve with a Graphical User Interface or GUI. Windows Server Standard bases its pricing on the amount of CPU cores the server uses. The difference between the Standard and Datacenter editions is that the Datacenter allows companies to have an unlimited number of virtual machines running on one server. The Standard version only allows for 2 virtual machines. We could go about this in a few ways. Either we use the Standard edition and run 2 of the 3 servers on one machine and put the third on another. Or we can use an app called VMware and put all three virtual machines on one machine.

Network Segmentation and Printing

With 46 current employees and a total of 95 devices that need to be supported, Greenfield may run into a network traffic congestion issue. This is because your Local Area Network (LAN) is considered a broadcast domain and, whenever there is traffic within the network, it will broadcast signals to all devices within that domain. To alleviate this, we would divide your network into several subnets. Subnetting allows you to break up a larger network and gives you the benefits of increased network performance and simplified management and troubleshooting.

I propose segmenting your network into four sections with the number of nodes (or devices) they will support:

- PC’s – supporting 39 devices
- Printers – supporting 18 devices
- Wireless Devices – supporting 99 devices
- Guests – supporting 30 devices

I would have a separate subnet for guests so that they cannot access the company’s resources and only use basic internet functionality.

When it comes to assigning security controls to these subnets, I think we should accomplish this by using a Virtual Local Area Network or VLAN. A VLAN is great at segmenting a network into different parts that need certain security and privacy requirements. A VLAN essentially does the same thing that a subnet does, in that, it divides a larger network into more efficient subnetworks. It just does this at a physical level whereas a subnet does this at a logical level.

A VLAN works by taking all the ethernet ports on a switch and separates them into logical subnetworks. So, you could have all of your devices plugged into the same switch, but you could separate all of them into different subnetworks with different security permissions.

I would divide Greenfield’s network into the following parts:

- Executives/Management
- IT department
- All other employees

I think this strategy will help give a good foundation to prevent sensitive information from reaching the wrong hands.

Printing

When it comes to how Greenfield’s printers will be configured and managed, there are two ways in which this can be done: Direct IP Printing and a print server. Direct IP Printing means that every computer and user has direct access to the printer and can set their own personalized settings. This boosts efficiency because if there is a driver issue or print issue, it will only affect one user. The downside of this is that it quickly becomes a management nightmare as the IT team will have to go around to each station and download the latest firmware updates and troubleshoot each individual station.

This is where print servers swoop in to save the day. A print server will allow the company to manage settings, add new users and update print permissions from a centralized point. Print servers are also able to scale to larger environments – adding new users as a company grows. Some cons of using a print server are that it requires additional hardware which costs money and will impact the network bandwidth. And it is a single point of failure which means that, if a print server goes down, the company will not be able to print.

In my professional opinion, I believe print servers are the only choice to meet Greenfield Properties’ needs. I believe the benefits far outweigh any drawbacks and it will help your business run more efficiently and will scale with any future growth.

Wi-Fi Networking

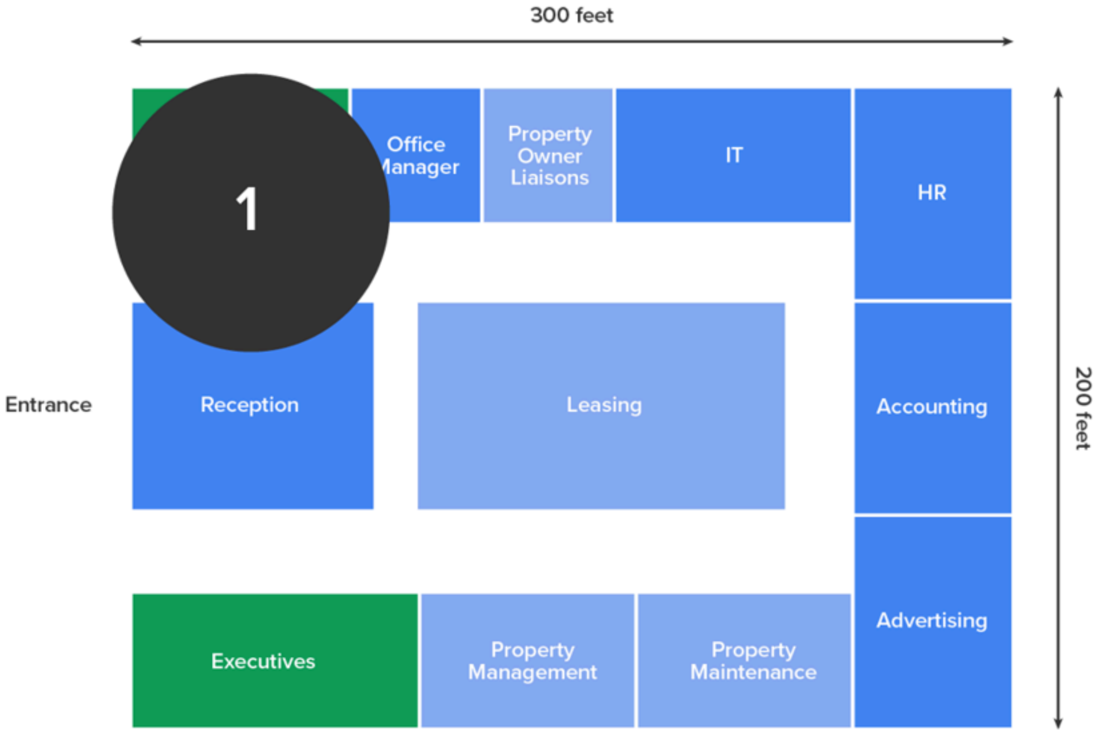
With the type of work that is done at Greenfield, having a robust and comprehensive Wi-Fi network is fundamental. From the document you have provided me, there are currently 69 wireless devices that need to be supported. However, considering a potential for 50% future growth and the fact that you may have visitors using your network, I am going to anticipate Greenfield needing to support 134 wireless devices (104 for company future growth and 30 potential visitors).

Achieving this coverage will hinge three wireless network technologies:

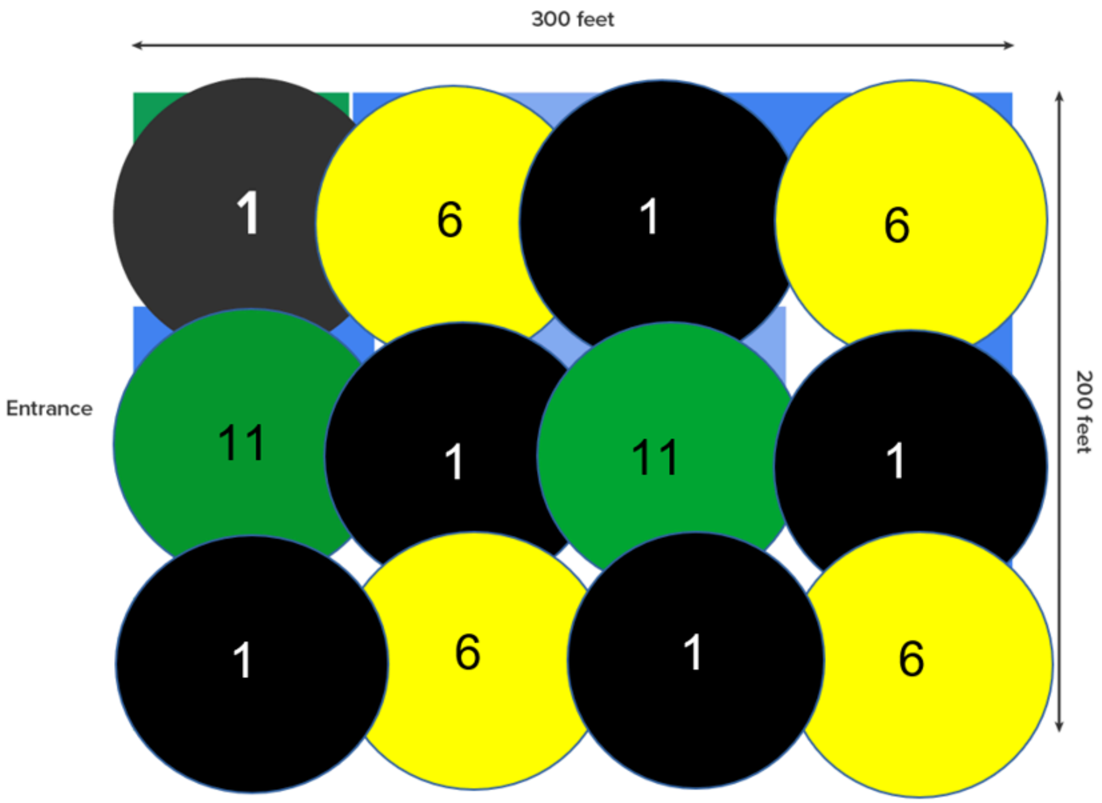
- Wireless Access Points or WAPs
- A Wireless LAN Controller or WLC
- Wireless Encryption

Wireless access points are devices that connect other wireless devices such as laptops, tablets, and phones to a network. They do this by sending and receiving radio signals in various frequencies. The placement of these should be up in the ceiling and away from any large objects that could prevent radio signals from reaching their intended destination. An on-site visit will be necessary to determine the proper placement of these devices using specialized software that will give us a Signal-to-Noise Ratio and Received Signal Strength Indicator reading.

Below is a picture of the current layout of Greenfield Properties:



And here is a picture of preliminary placement of the Wireless Access Points:



The different colors and numbers within each circle represent a single WAP and the radio frequency channel that it will operate at. WAPs that operate at 2.4ghz can have a maximum range of 150 feet. However, the signal will be very weak at that distance, and it will require the company to operate each WAP at full power, which is problematic if there is a dip in power.

This is why I think each WAP should be placed much closer from 30 to 70 feet. The reason we can have these placed much closer and not have any interference is because we will configure each WAP to operate at a different channel within the 2.4ghz frequency range. There are three viable channels: 1, 6, and 11, and by strategically placing them as I have done in the picture above, users will not have to worry about any collisions on the network.

When it comes to the long-term configuration and management of the WAPs, I suggest Greenfield install a device called a Wireless LAN Controller or WLC. I would use a wireless LAN controller because it will allow the IT administrator to push out configuration updates from a centralized location. This will be useful when considering future growth and adding more space to their building and more access points. If they did not have a wireless LAN controller, each access point would have to be configured individually.

And finally, as far as securing communications over the Wi-Fi network, I would use the latest WPA3 encryption standard on the access points. WPA3 is the most recent standard for providing security to wireless networks. It provides 192-bit cryptographic strength and is backwards compatible.

Security Measures

Confidentiality, integrity, and availability, also known as the CIA triad, is crucial to the operation of any business. Essentially you need your data to be secure, trustworthy, and there for you when you need it. To accomplish this, I will go over the following topics: Physical Security, Infrastructure Access, Authentication, Lockout Policy, Password Complexity Requirements, Firewall, and Anti-Malware.

Physical Security

The company should have a dedicated server room that is essentially a network closet. This will have air-conditioning and is secured by a locked door with a physical lock on the outside. This should also have a cipher lock that has a keypad that employees can access with a password/number. The room/closet should also have a video camera inside to provide evidence of who comes and goes. Having the network room will restrict access and make it so that nobody accidentally interacts with the equipment. The locked door with a cipher lock will provide a double authentication so that only employees with security clearance can access it.

Infrastructure Access

One of the most effective ways to secure network access is to configure Access Control Lists. This provides the ability to restrict access based on the source or destination IP address. The company should do the following to prevent any unwanted access:

- Deny any addresses from internal networks.
- Deny any local host addresses.
- Deny any reserve private addresses.
- Deny any addresses in the IP multicast address range.

Authentication

As you might have guessed, all users will be required to enter their credentials and be authenticated before they can access the company's resources. I would recommend using TACACS+ for the authentication method. TACACS+ uses the connection-based TCP protocol and it separates the authentication and authorization which results in it being more stable and secure than the other popular method of authentication RADIUS. Essentially, TACACS+ will not only provide a secure key to grant access but it will also gather information about the session that can be used to determine any security breaches.

Lockout Policy

In order to prevent a breach in your system through brute-force password hacks, your IT team should set a limit for how many times someone can put in a password. I recommend the limit be five attempts. This should give enough flexibility for the average user to remember their password and also guard against hackers attempts to compromise your network.

Password Complexity Requirements

I would set the maximum password length to 15 characters that include a capital letter, a number, and a special character. I would set the password expiration time to 90 days. The password length and complexity will make it more difficult for hackers to guess/brute force. The password expiration time should be adequate for a company of this size and will alleviate any concerns with passwords being changed too often. I would also have everything be Single-Sign-On, meaning that they only need to remember one password to log in to the domain and it will provide a token for them to access multiple accounts and services.

Firewall

The purpose of a firewall is to restrict communication to and from a network by guarding various ports that are used. Greenfield should use a network-based, stateful firewall. A network-based firewall will protect an entire network instead of just one system that a host-based firewall covers. A stateful firewall will monitor the status of connections passing through it and will do a better job of preventing DoS attacks and IP spoofing.

Anti-Malware

Greenfield should deploy a next generation, network-based Intrusion Prevention System (IPS) device. This will provide the best results in keeping your data secure. The IPS does this because you can see what is happening outside of your network and learn to recognize exactly what’s getting through your defenses. The IPS will not only log and notify administrators of any suspicious activity, but it will also actively prevent attacks by changing network configurations, close sessions, and reroute the attacker so that it can learn the identity of said attacker. I would also recommend a VPN Concentrator so that remote employees can send and receive encrypted data. This will protect any sensitive information that employees will deal with when handling customer transactions.