Chris Nelson

President

Greenfield Properties

123 ABC Way

Minneapolis, MN 55000

Dear Mr. Nelson:

Thank you for the opportunity to provide network planning guidance to Greenfield Properties as you embark on this exciting new venture of combining Bluegrass Rentals and Redstone Property Management.

I have reviewed the information provided about Greenfield Properties' current staffing and devices, and reflected on the necessary network architecture, organization, and security to make your network the most secure, most available, and easiest to administer that it can be. The attached report contains my recommendations for the network based on this.

After that, this would be the right time to meet with your IT staff and key decision-makers for the purpose of starting to define a more detailed network roll-out plan. Finally, do not hesitate to call me if you have any questions about this report or if you are ready to move into the next step.

Sincerely,

Sushanta Poudel

Introduction

This document presents my proposed network recommendations for Greenfield Properties, which will facilitate the company's expansion following the merger of Bluegrass Rentals and Redstone Property Management.

Network Infrastructure

Greenfield Properties has outgrown the peer-to-peer network and the 46 staff and the 95 devices that are in use by our former businesses, Bluegrass Rentals (BR) and Redstone Property Management (RPM). A small network of 12 devices or fewer is better suited for it.

I would consider a client-server network topology architecture. There are two switches connected to the wired hosts according to Figure 2 by a Category 6 cable. The remaining ones are to run across the ceiling surface. One should use the plenum cable that comprises fire-resistant shielding. It does not release any poisonous fumes when it is on fire; employees will be less at risk of breathing poisonous gas in case of a fire.

These would be connected to a router so all the nodes can access the Internet over a connection received from an Internet Service Provider. The main distribution frame would rest in a room allocated to network equipment with the servers.

As defined, a client/server network should consist of a minimum of one server with centralized control of network traffic. I would suggest the addition of the following server functions to the network:

- Active Directory, to centralize user authentication, caching, and accounting.
- A file server, to share specifically required data files among the employees of the company.
- A mail server to which the company's email system is to be administered. Otherwise, you must host your mail system entirely on some outside company's web hosting services.

- Web server: This is where the company's website—and the management apps that allow tenants and owners to have access to online management and payment tools—are hosted. My preference is for a cloud-based web server, primarily for the reason of not requiring as much initial capital. I do not think that a full web server is necessary; using a web hosting service may be much more convenient and cheaper.

Network Segmentation and Printing

One way to design a network is by connecting all nodes to the same Local Area Network (LAN), or in other words, to the same broadcast domain. In this way, each node can communicate directly with each other in just a single hop. Thus, by splitting a network, one will be left with the possibility of a stronger or more competent network. This is because every node has a much lower traffic load to process.

The subnets will also be required to support different sets of permissions that have specific needs. For example, printers and other infrastructure devices are not given the same treatment as a user PC. Similarly, security needs differ for Wi-Fi-connected devices versus wired ones. I'm suggesting the four subnets as follows:

- Wired PCs: Presently, 26 are needed, and expansion is planned for 39 in the future.
- Wi-Fi User Devices: Though some of they will not be active/connected at one time, the configuration should support that would be the case for the safety factor. Currently, 69 is installed, and a planned expansion to 104 in the future.
- Infrastructure Network Devices: The Number is not yet concrete, but is roughly around 30 in estimation. This is expected expansion to 45 for future growth.
- Printers: 12 are installed a future expansion to18 is planned.

Because the number of devices in the network is small, that is, 100, there would be no necessity to segment the users' devices based on which department they belong to in the company, and only because the company has only one location. In fact, it may be helpful to group the hosts according to what types and levels of permissions they need.

I would also recommend employing Virtual LANs (VLANs). VLANs allow one not to be tied to the physical connectivity to a switch that a host is using to propagate its information when defining it to a VLAN. For example, we don't care what switch or what port on a switch a host is connected to with VLANs. That may require that, as this company grows, I add users to some subnets that require multiple physical connections to some switches.

Given the remote work and access requirements, cloud-based servers are recommended for Greenfield Properties to simplify management and reduce costs. Windows Server, with its user-friendly interface, is suggested due to the IT staff's limited experience with client/server networks.

Servers, each performing a single function, can be virtualized to run multiple instances on the same hardware, offering cost savings. The choice between the standard and Enterprise versions of Windows Server depends on the number of virtual servers needed, with the latter supporting unlimited virtual servers.

Printing

Printer Servers:

- Pros:
    - Managing multiple printers gets easier with Centralized administration and configuration.
    - Suitable for business or enterprise environments with many printers and computers.
    - Functionality hasn’t changed for years; therefore, the maintenance is simple for an experienced technician.
- Cons:
    - If the server fails or goes offline, it affects everyone.
    - It may not be too simple or too excessive for small offices.
    - Requires ongoing maintenance and might lead to potential costs.

Direct IP Printing:

- Pros:
    - Low maintenance and cost-effective adoption.
    - Resource usage is lower.
    - Reduces overall network traffic.
    - No single point of failure on the network.
    - Users have control over drivers and print settings.
- Cons:
    - Can’t track printing costs or job activity.

- Not ideal for remote work environments.
- Configuration can be time-consuming.
- Not scalable for large setups.

This would be a direct IP print as this is not that large and complex network environment, with only 12 printers and about 100 hosts. Some of the benefits of IP printing that apply to this are:

Direct printing will reduce the workload of IT staff because they need not set up and then maintain a print server.
Eliminate the print server—and the associated cost of IT hardware and software.

Eliminate any single point of failure for printing—any problems affect only one user at a time.

Users are in control of their print jobs; they may send them to any printer. It does not generate as much network traffic.

Wi-Fi Networking

Currently, there exist 69 wirelessly connecting devices, in that they account for well over two-thirds of the count. This goes on to really show wireless connectivity. In the future, the network should be capable of concurrently supporting up to 104 wirelessly connecting devices.

This will necessitate about 12 WAPs, in addition to the supportive hardware and cabling for the whole Wi-Fi coverage. These WAPs must be placed inside the building in a way that Wi-Fi access signals are strong from every corner. If power outlets are not readily available in the ceiling, PoE can be used to power the WAPs.

Set your WAPs to be stationed in any of these three channels—for instance, 1, 6, or 11. This will prevent overlapping between all the channels, as depicted in the diagram below.

Each WAP is given an SSID, which a user would field when their computer scans for a WAP to connect with. Usually, all WAPs have the same SSID set so that the user can freely roam from one access point to neighbor without having to configure the WAP. Other WAPs configured with differing SSIDs can then be deployed within departments such as Human Resources and IT, where data and information are more sensitive.

A WAP must be added to the network, with the use of a wireless LAN controller; this would make it easier for the IT staff to manage all the WAPs.

Since the WAPs are not cable-constrained, extreme security must be in place. I would recommend the latest encryption on WPA3 because it has better encryption abilities.

Security Measures

An organization's assets are exposed to different kinds of risks. Here is a short explanation of some security measures that an organization can adopt.

Physical Security

The physical security of Greenfield Properties is going to be improved by implementing several numbers of measures. Some of them include employing security guards, installing door locks, and setting up a perimeter intrusion detection system.

Infrastructure Access

One way to facilitate access to the infrastructure of Greenfield Properties is to use Secure Sockets Layer (SSL). If you do not want anyone to access information as it passes between your browser and the web server (s), installing an SST is crucial. SSL stands for Secure Sockets Layer; SSL ensures that all data passed between a user and a web server is encrypted, therefore anybody who intercepts the data will just see characters in no specific arrangement.

Authentication

Greenfield Properties should adopt the Remote Authentication Dial-In User Service (RADIUS) for authentication. This authentication is relevant because it allows users on different types of links to be monitored, such as dial-up demands. It retains client login IDs and passwords, enabling numerous validation attempts.

Lockout Policy

It is also a measure that ensures security during operations at Greenfield Properties. This policy is designed to log a user out if s/he forgets to sign out from their account, and next time he/she try to log in, he/she must input all needed information again.

Password Complexity Requirements

The passwords must be formulated according to requirements designed to increase the difficulty for third parties to guess them. Among the stated parameters are a minimum number of eight characters, both uppercase and lowercase letters, at least one special symbol, as well as a digit.

Firewall

As a security measure, a Firewall serves as a security check, making sure only the entitled people are allowed to pass through a network while blocking others, and works just like a security guard but with more precision than a human.

Anti-Malware

I would suggest that Greenfield Properties utilize host-based anti-malware as the most effective anti-malware software. Host-based anti-malware provides the organization with full command over the entire protection process for its network, and it must be updated frequently. Also, an organization might consider using server-based anti-malware if it demands less processing power, does not need regular updates, and provides them with the capability to access up-to-date malware data.