11/24/2023

Chris Nelson
President
Greenfield Properties
123 Sophia 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 have given careful thought to the network architecture, organization, and security required to make your network the most secure, available, and easy-to-administer it can be. The attached report includes my recommendations for the network, as a starting point.

The next step would be to meet with your IT staff and key decision-makers to create a more detailed network roll-out plan. Please let me know if you have any questions about this report, or are ready to move to the next step in the process.

Sincerely,

Luis Parra

Introduction

Greenfield Properties, a dynamic and growing enterprise, has presented a request for a comprehensive proposal to design and implement a robust network infrastructure. This proposal aims to address their current and future networking needs, ensuring scalability, security, and efficiency in their operations.

Greenfield Properties operates in the competitive real estate sector, specializing in both commercial and residential properties. As a mid-to-large size enterprise, they have a diverse and expanding workforce with a range of technological needs. Their operations span various departments, including sales, administration, finance, and field services, each with unique IT requirements.

The client's primary expectations are centered around building a network infrastructure that can support a growing number of devices, ensure secure and seamless connectivity, and adapt to the changing dynamics of the real estate industry. They require a network that is not only reliable and fast but also secure from external threats and capable of supporting various types of devices, including PCs, tablets, and smartphones.

Key aspects of the request include:

- Network Architecture: Designing an architecture that balances performance with security, and is scalable for future growth.
- Cabling and Connectivity: Selection of appropriate cabling for various parts of the network, considering factors like speed, cost, and installation.
- Server Infrastructure: Identification and setup of necessary servers, deciding between on-site, cloud-based, or a hybrid approach.
- Operating Systems: Choosing suitable operating systems for the servers based on compatibility, support, and performance criteria.
- Virtualization: Evaluating the benefits and drawbacks of server virtualization and making informed recommendations.
- Network Segmentation and Printing Solutions: Implementing network segmentation for improved performance and security, and deciding on the optimal printing network setup.
- Wi-Fi Networking: Ensuring full Wi-Fi coverage with a robust and trouble-free setup, including recommendations on the number of devices to support, infrastructure components, and security standards.
- Security Measures: Developing a comprehensive security strategy to protect both the network's digital and physical assets.

Network Infrastructure

For Greenfield Properties, a client/server architecture is recommended. This model is highly efficient for a mid-to-large size enterprise due to its centralized management, enhanced security, and scalability. It allows for centralized control of resources and data, which is critical for managing a diverse and geographically dispersed workforce.

The network should primarily use Category 6 twisted-pair cables for Ethernet connections. These cables support high-speed data transfer and are cost-effective for office environments. Fiber optic cables are recommended for backbone connections due to their higher bandwidth and longer-range capabilities, which are essential for connecting different floors or buildings.

The proposed server setup includes a Web Server, Mail Server, File Server, Database Server, Application Server, and Print Server. Each server has a specific role: the Web Server for hosting websites, the Mail Server for managing email communications, the File Server for centralized file storage, the Database Server for data management, the Application Server for running business applications, and the Print Server for managing print jobs.

A hybrid approach is recommended. Critical servers like the File and Database Servers should be on-site for security and control, while less critical servers like the Web and Mail Servers can be cloud-based for flexibility and scalability.

The servers should run a mix of Windows Server and Red Hat Enterprise Linux (RHEL). Windows Server is user-friendly and widely supported, making it ideal for file and application servers. RHEL offers stability and security, suitable for web and database servers.

Virtualization allows running multiple virtual servers on a single physical server, leading to cost savings, easier management, and better resource utilization. Given the scenario, virtualization is recommended for non-critical servers to maximize efficiency and reduce hardware costs.

Network Segmentation and Printing

Subnetting enhances network performance and security. It segments a large network into smaller, manageable parts, reducing congestion and improving traffic management. This is particularly beneficial in a diverse environment like Greenfield Properties, where different departments have varying IT needs.

The network will be segmented into 8 subnets, each catering to specific departmental needs and device types. Implementing VLANs is advised to further segment the network, increasing security and improving traffic management by isolating network traffic at the data link layer.

/Mask Bits, Subnet Mask
/29, 255.255.255.248
/29, 255.255.255.248
/29, 255.255.255.248
/29, 255.255.255.248
/28, 255.255.255.240
/28, 255.255.255.240
/28, 255.255.255.240
/27, 255.255.255.224

Printing

A combination of print servers and direct IP printing is recommended. Print servers offer centralized control and are ideal for high-volume, on-site printing. Direct IP printing is suitable for remote and mobile employees, offering simplicity and cost savings. Please see the chart and my brief explanation.

Aspect	Print Server Connection	Direct IP Printing
Centralized Management and Scalability	**Pro:** Offers centralized control and management for multiple printers, making it easier to manage settings, update drivers, and troubleshoot. More scalable in larger environments.	**Con:** Lacks centralized management, making it less efficient for multiple printers. Each printer must be managed individually, which can be cumbersome in larger networks.
Cost and Complexity	**Con:** Higher initial setup cost and complexity due to the need for a dedicated server and its maintenance.	**Pro:** More cost-effective and simpler setup as it eliminates the need for a dedicated server. Each printer is configured independently, which is straightforward in smaller environments.

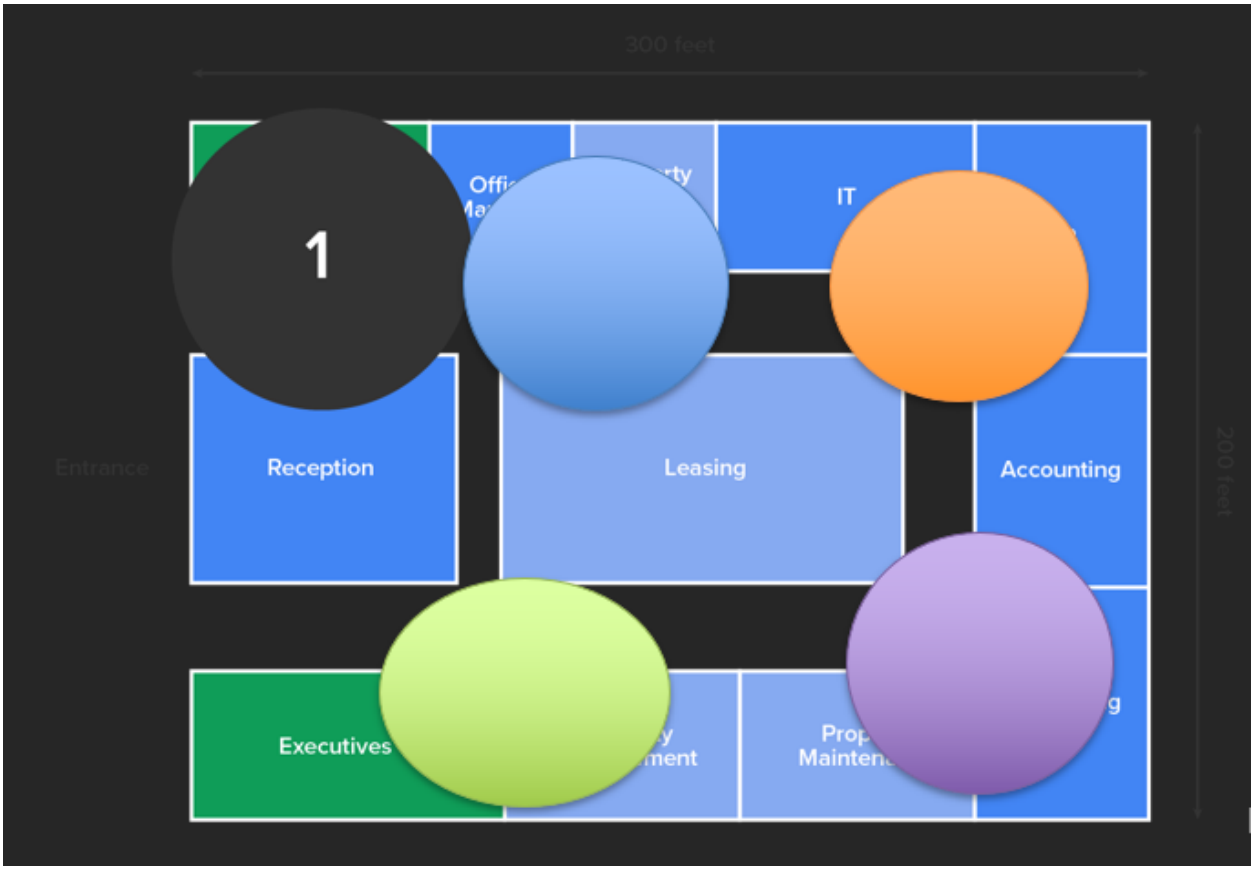
For Print Server Connection, it's best suited for larger networks where centralized management and scalability are critical. The initial investment in a server and its maintenance is offset by the ease of managing multiple printers.

For Direct Ip Printing, it's Ideal for smaller networks or situations where cost savings and simplicity in setup are prioritized over centralized control. Each printer operates independently, which reduces complexity but might not scale well in larger environments.

Wi-Fi Networking

Complete Wi-Fi coverage is crucial to ensure seamless connectivity for all wireless devices. Approximately 99 devices (60 smartphones and 39 tablets) are expected to connect wirelessly. Adequate coverage is vital for maintaining productivity and efficient communication.

A strategic placement of WAPs is planned to ensure robust and trouble-free Wi-Fi coverage. The diagram illustrates the placement of WAPs, with different colors indicating various channels to minimize interference. Overlapping coverage ensures no dead zones.



The infrastructure will include a robust wireless LAN with multiple access points, a wireless controller for managing these access points, and network switches to connect WAPs to the main network.

Using a wireless LAN controller is recommended for centralized management of WAPs. This ensures efficient performance management and facilitates seamless user connectivity across the network.

WPA3 is recommended for its advanced security features. It provides robust protection against external threats and ensures the safety of wireless communication.

Security Measures

For network security, a combination of stateful inspection and next-generation firewalls will be implemented. Additionally, Access Control Lists (ACLs) will be configured on switches and routers for securing network access. User authentication will be strengthened using multi-factor authentication (MFA), and a robust password policy requiring complex passwords that are regularly updated will be enforced.

Physical Security

Physical security measures like biometric access controls and surveillance cameras are recommended to protect servers, infrastructure equipment, and workstations. These measures ensure that only authorized personnel have access to sensitive areas, reducing the risk of physical breaches.

Infrastructure Access

Access to network infrastructure will be tightly controlled using role-based access controls (RBAC), ensuring that only authorized personnel have access to specific network segments and resources. This approach will help in minimizing the risk of internal threats and managing permissions more effectively.

Authentication

Multi-factor authentication (MFA) is recommended for user sign-in. MFA adds layers of security by requiring multiple forms of verification, making unauthorized access significantly more difficult.

Lockout Policy

A stringent account lockout policy will be implemented. After a set number of failed login attempts, the account will be temporarily locked, thereby mitigating the risk of brute force attacks.

Password Complexity Requirements

Enforcing a strong password policy is critical. Passwords should be complex, changed regularly, and old passwords should not be reused. This reduces the likelihood of password breaches and unauthorized access.

Firewall

A combination of stateful inspection and next-generation firewalls (NGFWs) is recommended. This dual approach layers security, providing comprehensive protection against a wide range of cyber threats.

Anti-Malware

Comprehensive anti-malware solutions like ESET are recommended. These solutions should include real-time scanning, automatic updates, and heuristic analysis to protect against both known and emerging threats.

In Conclusion

To wrap up, our plan for Greenfield Properties' network is like building a strong and flexible backbone that can grow and adapt with the company's needs. Think of it as constructing a high-tech highway system for all their digital traffic - data, emails, files, and more.

We're setting up a network that's like a well-organized office space - everything has its place, and there's a central point (the server) that helps manage everything efficiently. This setup is not only smart but also secure, kind of like having a top-notch security system for your digital world.

We're using the best cables for super-fast internet and a Wi-Fi setup that covers every corner, ensuring no one's left with a slow connection. It's like having high-speed roads and no dead zones where you can't get a signal.

For printing, we're using a mix of centralized control for big office printers and a more direct approach for smaller or remote ones. It's like having a main post office for big mailings and direct delivery for quick, smaller packages.

Security is a big deal here. We're putting in place a system where employees need more than just a password to get into the network. It's like having a special passcode, a keycard, and a secret handshake all in one. This makes it really tough for unwanted guests to sneak in.

Our Wi-Fi network is designed to be strong and seamless. We're setting it up so that everyone can move around freely without losing their connection, ensuring that everyone stays online no matter where they are in the building.

We're building digital walls and moats - firewalls and anti-malware - to keep out internet bad guys and viruses. And just like a fortress, we're also keeping a close eye on who gets to enter the server rooms in real life.

This whole plan is not just for today. It's built to grow with the company, ready to take on more employees, more devices, and whatever new technology comes down the road.