Network Proposal

Byron J. Laferriere

Southern New Hampshire University

IT201 Platform Technologies

When it comes to your network needs, I have created a list to help MilleniAds succeed. Focusing on lightning fast internet speeds and full scalability for future business expansion. Since your company only has 10 employees right now, I suggest starting smaller, but having all the pieces in place for when you are ready to grow.

Starting from the ground up we will examine connection types first. An infrastructure connection method is recommended over Adhoc connections. Infrastructure connection will allow for easy scalability as your business grows, adding more hosts as needed. Adhoc connection is used more for peer-to-peer connection in two or three computers at most, while the infrastructure connection method can support multitudes of server hosts simultaneously. The infrastructure connection is recommended for networks that support ten or more hosts, which will be perfect for MilleniAds. Next, we will look at which 802.11 type will work best for your business. There are many good options available nowadays, but we need to focus on what will work best for your business now and in the future. 802.11ac will be the best choice for your connection. Although it has half the range of 802.11n, its speed makes up for loss in distance. Distance has been proven to dramatically affect speeds so having twice the coverage capability doesn’t necessarily make it the better choice. 150ft of wireless transmission range will be plenty for your small office. 802.11ac also uses MU-MIMO and channel bonding to strengthen and reinforce signal transmission, making it the best option for your office.

The next consideration to make is what type of network you in the office. There are many options, but after elimination of the slower operating network options, it leaves only two to be considered. There is a LAN or wired connection and a powerful WLAN for the office. The WLAN would be connected to your desktops used for graphic design and we would encourage employees to bring their own devices from home. Going wireless in the office will help alleviate the clutter of wires and give users mobile accessibility. With your wireless network you will need a managed switch to help control how your business consumes the network. Managed switches now have graphical interfaces so you as the CEO can manage the switch easily without using command line interfacing to do so. For the two employees who will be mainly operating outside of the office we will set up a VPN for them, to provide access to necessary files at any time. The employees can provide their own mobile equipment to be formatted for VPN access, or you can supply them with notebooks specifically for work. When picking your router you want to be sure that you pick one that supports VPN access as well.

Using Remote Desktop will require upgrading from Windows 10 to Windows 10 Pro, but it will provide the file sharing that you desire for your employees. For your shared folders, users will have read/write capabilities and be required to log in every time to ensure there is no intrusion using domain authentication and a domain controller. We will also implement a screensaver password after three minutes to add an additional layer of security.

By using VoIP, you will be able to eliminate the need for landlines in your office. Additional telephone lines for your business will only cost more each month, tallying up on your yearly reports. VoIP technology has gotten fantastic in recent years and now offers the same capability as the ancient landlines did. With most communication happening via the internet currently, landlines are no longer a necessity for a successful business.

Your wireless network should have SSID Broadcast disabled as well, and users will be required to ask for the password and SSID from CEO. By leaving broadcast enabled you leave your network open to intrusion, it is never worth having an easily discoverable network with valuable information on it. I would recommend adding additional layers of security to ensure that no information can be easily stolen. Universal Threat Management devices (UTM) provide many necessary additional security measures to your network with things like gateway antivirus, URL blocking, and intrusion prevention. There is another option when it comes to additional layers of security for your network. There is also the next-generation firewall (NGFW) which does everything that a UTM offers, but it also has specific application-level inspection software that a UTM doesn’t offer. This can protect your network from an employee making a silly mistake that could have been costly. Although the NGFW seems more appealing, it is much more expensive, and they aren’t designed for small businesses. The UTM will give you plenty of additional protection for your network.

Specific Recommendations:

* Dell SonicWALL UTM
* TrendNet AC2600 Streamboost MU-MIMO Router (VPN friendly)

References:

2019 How-to Guide: Small Office Network Setup

Adam Lovinus - <https://www.neweggbusiness.com/smartbuyer/over-easy/small-office-network-setup/>

A Utm Provides Enterprise Network Security Features For Smbs

Adam Lovinus – https://www.neweggbusiness.com/smartbuyer/networking/a-utm-provides-enterprise-network-security-features-for-smbs/

Testout: <https://cdn.testout.com/client-v5-1-10-555/startlabsim.html>