**PORTFOLIO PROJECT**

Networking Solution at ABC Accounting

Ismail Elmaliki

ITS 315 – Introduction to Networks

Colorado State University – Global Campus

Professor Georgette Jones

April 07, 2018

Networking Solution at ABC Accounting

Ensuring the most appropriate network infrastructure and setup is essential to ABC Accounting and its continuing expansion of onboarding more employees. Here we’ll go over the following on setting up a corporate network: topology and network devices, IP Infrastructure, and security. By covering these three essentials in depth, it’ll ensure a strong foundation for the corporate network setup and will account for scalability without compromising speed.

**Topology**

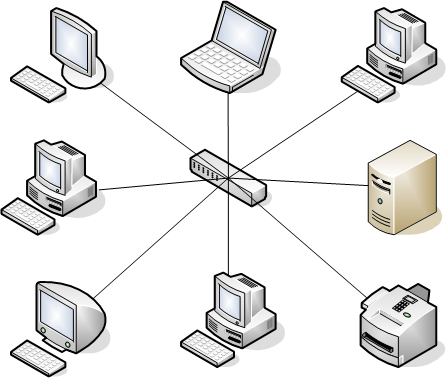
When it comes to computer networking, the best way of describing a topology according to Bradley Mitchell (2017) is the layout of connected devices within a network. With that in mind, the best network topology for this growing firm is the star topology. Here’s a list of reasons as to why the star network topology is the most appropriate choice:

• Centralization

• Easy to troubleshoot

• Scalability (ability to expand)

**Centralization –** this allows all network devices to connect to a central node (wired or wirelessly); this is an advantage of the star topology because all devices on the network can communicate with one another since they’re all connected to that central node without having excessive cabling connections like the mesh topology. Another advantage of centralization is scalability – the ability to easily connect network devices to the network. All that’s required for one new network device to communicate with all devices on that network is to connect to the central node; in other topologies, installation becomes more difficult as the number of staff members grow. As shown below in the photo, laptops, workstations, servers, and printers can all be centralized via the star topology.



**Easy to troubleshoot –** with having about 200 staff members networking issues will become inevitable. A cable will go bad, a computer can’t connect to the network, and many other scenarios can occur. The beauty of a star topology is that it’s easy for a technician to isolate causation of a network issue. For example, if one device is having trouble connecting to the network but all other devices can connect, then clearly the issue is with that device. Also, if all network devices suddenly can’t connect, clearly the issue is with the centralized node. On the other hand, topologies like mesh and ring would require extensive troubleshooting – especially because many of the devices are interconnected and there’s no central connection.

**Scalability** – this topic was briefly touched upon when discussing centralization but having the ability to expand a network easily makes the star topology a no-brainer. To add another network device, simply connect it to the centralized node and just like that, it can connect to other devices within the network. What about 50 more network devices? In a ring topology, those additional 50 devices have to be interconnected with another and would take quite some time. In a mesh topology, adding 50 additional devices can easily get messy and would require a lot of time (and making sure that all devices are interconnected with one another). With a star topology, those devices just need to connect to the centralized node and nothing more! In addition, if the centralized node has reached its max number of devices then another central node can easily be added to the current network infrastructure.

**Network Devices**

Now that we covered which logical network topology is best for the company and its expansion in the foreseeable future, which network devices should be purchased to make the star topology and its benefits a reality? The following are a must to account for wired and wireless internet connectivity – switches, routers, WLAN controller, and wireless access points. After reviewing their definitions and importance to the firm, we’ll then discuss IP Infrastructure and how to secure a network.

**Switches** – as Cisco’s Building a Small Office Network (2018) webpage describes in layman’s terms, “switches connect multiple devices (computers, printers, servers) on the same network within a building or campus. A switch enables connected devices to share information and talk to each other” (2018). Without switches to tie devices together, building a network in which devices can connect to company resources (like printers, scanners), having file sharing options and managing resources in a central location wouldn’t be possible. Business enterprise switches must be considered to account for future network demands and security.

**Routers** – referring back to Cisco’s Building a Small Office Network (2018) webpage, “routers tie multiple networks together” (2018). Continuing, a “router connects your networked computers to the Internet. This enables all connected computers to share one single Internet connection” (2018). Also, “a router acts as a dispatcher, choosing the best route for your information to travel” (2018). Ideally within ABC Accounting Inc. it’s best to have more than one business-grade router.

**WLAN Controller and Wireless Access Points** -with home and small business networks, a single access point would need to be configured and is the source of both internet connectivity and emitting wireless connectivity; whereas with an enterprise networks, a wireless network controller is required and is the single access point for configuring all wireless access points on a corporate network. In a typical enterprise environment, there can easily be a minimum of 15 access points that require configuration from the wireless network controller. Taking a look at Cisco’s WLAN Solutions document (2017), it explains how business grade network devices and solutions are included with the following tools:

- Rugged network equipment to withstand harsh outdoor environments

- Platforms both on the web and using mobile apps to keep track of analytics and network performance

- Prioritizing wireless app traffic with included features like load-balancing

- High internet performance

**Cost Breakdown** – before diving into cost breakdown, the name brand that’s highly recommended for this organization is Cisco Meraki; because of its cloud management system, seamless setup, network security features and world-class business support, Cisco Meraki is a no brainer. Below are the suggested network devices, quantity, and price per device:

*Wireless Access Points* – MR42, General-purpose coverage with 1-year license; Suggested Quantity: 15; Price: $1,249/AP

*Router* – MX 250 with 1-year Advanced Security License; Suggested Quantity: 1; Price: $19,995

*Switches*

* + MS410-16 Distribution switch with 1-year license; Suggested Quantity: 1; Price: $9000
  + MS250-48 Access Switch with 1-year license; Suggested Quantity: 6; Price: $8865/Switch

**Total:** $100,920

**IP Infrastructure**

Dynamic Host Configuration Protocol (DHCP) is a protocol that’s used to provide automatic and central management for the distribution of IP addresses. Without us realizing it, DHCP plays a part in assigning our devices (such as mobile devices and computers) IP addresses so they can connect to the web. In every home that has an internet service provider, usually a wireless router is included so our devices can connect wirelessly – that router acts a DHCP server to assign IP addresses automatically! What would happen if that router didn’t have DHCP enabled? If DHCP isn’t enabled, then IP address would have to be manually configured on every device! Just the thought of that is frustrating since we have so many network devices at home today. The same applies with large scale corporate environments, which have even more devices connected. Here we’ll explore DHCP and its benefits in a large-scale network environment.

Earlier a simplified home example was used to explain the DHCP protocol and how it’s relevant in our daily lives. Typically, a home will have a router that acts as its DHCP server, whereas in large network environments there’s a dedicated DHCP server that’s usually handled by IT administrators. The beauty of DHCP is that IP addresses are dynamically assigned to workstations on the network, which means there’s no manual configuration on the part of IT Administrators! Because of dynamic assignments, new workstations that get setup can easily join the network and the IT administrator won’t have to worry about assigning a specific IP address. Although the DHCP server in a large-scale environment handles these automatic IP assignments, it does require configuration on the part of an IT administrator. As Tim Fisher (2017) in his article on DHCP describes it, “a DHCP server defines a scope, or range, of IP addresses that it uses to serve devices with an address.” Another part that requires configuration in a DHCP server is the lease period – a specific period of time in which DHCP assigns an IP address. This means that within a short period of time (depending on configuration), the assigned IP address will eventually change when the lease period expires then renews itself to receive assignment of another IP. According to an article from Udemy titled Static vs. Dynamic IP: What Do You Really Need (2014), having a lease period in place is beneficial from a security standpoint. Of course, another advantage is avoiding the time-consuming process of manually configuring each workstation in the network and decreasing human-made errors like typos.

Although DHCP has many advantages and features to offer, it may be impractical at times to assign dynamic IP addresses to stationary network devices that constantly need access. For example, with a printer and file server it would be best to assign a static IP address instead – that way clients can always access those devices. On the other hand, if the IP address of a printer changes, then those clients need to setup the printer again. For an IT administrator, having to setup the printer on all those clients again in a large-scale environment definitely wouldn’t be practical. Not to mention it can easily lead to downtime within the company.

Lastly on this topic, it’s important to briefly touch IP Address classes. As defined by Microsoft’s TechNet article titled Address Classes (2018), IP address classes accommodate networks of different sizes and support a different number of hosts. Here’s a breakdown of each address class:

* Class A: allows for 126 networks and 16,777,214 hosts per network; ideal for networks that have a very large number of hosts.
* Class B: allows for 16,384 networks and 65,534 hosts per network; ideal for medium-sized to large-sized networks.
* Class C: allows for 2,097,152 networks and 254 hosts per network; ideal for small networks.

Based on this information and the needs of the organization, the Class B address class would be the best choice in order to create more networks and support many hosts on that network.

**Security**

Every person we know today has a lock on their door entrance to prevent unknown and malicious intruders from entering their home. Within a network, that very same concept applies – with that in mind, it’s important to lock-down and prevent cyber-intruders from disrupting the company’s network. The first step to increase security, before diving into the security features that should be enabled on network devices, is to create a security conscious environment within the company. The way to do this is by having annual security training sessions and having every new employee attend a mandatory security session as a part of their new-hire training. Some things that can easily be highlighted during these security sessions include:

* How security can affect the company’s reputation.
* Examples of real day-to-day security issues like phishing, social engineering, and suspicious security violations: how to identify them, prevent them, and report them appropriately.
* Reviewing current company security protocols and the consequences of violating those protocols.

By creating a security conscious environment, there’ll be more user awareness of potential security threats and a more security conscious environment will be created as a result.

At this point, we can now review security measures that should be implemented within the network. According to an article from TestOut titled Switch Security Facts (2018), here are security measures that should be enabled for network switches: VLAN, MAC filtering, and Port authentication (802.1x). A virtual LAN is simply a logical grouping of computers based on a switch port. For example, within the accounting firm if there are three teams – tech, marketing, and accounting – each team can have their own VLAN which helps organize and better control the flow of traffic. With MAC filtering enabled on a network switch, this’ll prevent unauthorized devices from connecting directly to the company switch and to any open Ethernet port in the office. On top of that, port authentication can be enabled for an even more added security layer – meaning that if an authorized device is able to connect, it must authenticate with credentials like a username and password, smart card, or another authentication device. Once the authorized device is authenticated, only then will it be able to access the company network. With switch security taken care of, let’s discuss router and wireless security measures.

On the topic of security for routers and Wireless LAN controllers, enabling the network firewall within the router portal and wireless LAN controller portal then selecting appropriate inbound/outbound rules that should be allowed based on the company’s network usage would greatly enhance security. As described in Wideband’s blog on Host-Based vs Network-Based Firewalls (2016), firewalls use different types of filtering mechanisms: they analyze packets, act as a proxy recipient for data, mark key features of outgoing requests and establish whether incoming data matches those outgoing requests. In other words, it’s constantly monitoring all incoming and outgoing traffic on the network and prevents suspicious traffic from entering the network. In addition to firewalls, utilizing Network Access Control Lists are also important in order to keep track of which devices and their corresponding users are connecting to the company network. Diving deeper into wireless security, here are some best practices as referenced from Wireless Security Facts (2018) via TestOut:

* SSID obfuscation: changing the default SSID to something that doesn’t obviously identify the company and turning broadcasting off.
* Encryption: making sure access to the internal wireless network is encrypted using the highest standard – AES with WPA2.
* Authentication: when used in conjunction with MAC filtering, this will make sure the authorized device connecting to the wireless network authenticates – those authentication credentials of course have to match to a directory service like Active Directory.
* Separating internal and external network: create a guest network and make it policy that employees bringing their own device can only connect to the guest network. For work devices and servers, they can connect to the hidden and separate internal network.
* Utilizing VPN: if the network has both internal and external usage, using a VPN would be ideal for an even securer connection. In addition, users that utilize corporate laptops and need to be able to connect to outside networks to continue their work **should** be utilizing a VPN to connect securely. Also, having a VPN server in place would also be ideal for more control over users.

Now that switch, router, and wireless security practices have been covered, it’s important to close this section with overall security best practices. Without these practices in place, then all other security features enabled for network devices would be for nothing. To start off, the default username and password for switches, routers, and wireless LAN controllers to access the network portal for configuration and setup must be changed: because default manufacturer passwords are well-known, it’s a huge security risk to continue using the default username and password since anyone would be able to guess those credentials and sign in to manage network settings. Another important security practice is making sure all network devices and server/client operating systems are installed with the latest security patches such as software updates and firmware versions. This will ensure all devices are continually protected over the course of time.

**Conclusion**

Bringing everything together, we discussed the following aspects of setting up a network while accounting for the continual growth of ABC Accounting Inc. – topology and network devices, IP infrastructure, and security. With all of these bases covered this will ensure that employees are able to access the internet securely and be at their productive best to continually contribute to the expansion of this amazing company.

References

Address Classes. (2018). Retrieved from Microsoft website: https://technet.microsoft.com/en-us/

library/cc940018(d=printer).aspx

Building a Small Office Network. (2018). Retrieved from Cisco website:

https://www.cisco.com/c/en/us/solutions/small-business/resource-center/connect-employees-offices/primer-building-small-office-network.html

Cisco Wireless LAN Services. (2018). Retrieved March 12, 2018, from Cisco website:

https://www.cisco.com/c/dam/en\_us/services/downloads/wireless-lan-services.pdf

Cisco Wireless LAN Solutions. (2017). Retrieved March 12, 2018, from Cisco website:

https://www.cisco.com/c/dam/en/us/products/collateral/wireless/aironet-1140-series/C45-614928-00\_Channel\_AAG\_Cisco\_Unified\_Wireless\_Network\_Portfolio.pdf

Fisher, T. (2017, June 1). What is DHCP? (Dynamic Host Configuration Protocol). Retrieved

March 4, 2018, from Lifewire website: <https://www.lifewire.com/what-is-dhcp-2625848>

Meraki Cost Calculator. (n.d.). Retrieved April 8, 2018, from Cisco Meraki website:

https://meraki.cisco.com/buy/cost-calculator

Mitchell, B. (2017, February 24). Introduction to Business Computer Networks. Retrieved

February 26, 2018, from Lifewire website: <https://www.lifewire.com/business-computer>

networks-817883

Mitchell, B. (2017, July 4). Introduction to Computer Network Topology. Retrieved

February 25, 2018, from Lifewire website: <https://www.lifewire.com/computer-network-topology-817884>

O'Keefe, A. (2016, October 29). Host-Based vs Network-Based Firewalls. Retrieved March 25,

2018, from Wideband website: https://www.wideband.net.au/blog/host-based-vs-network-based-firewalls/

RICHA. (2014, April 28). Static vs Dynamic IP: What Do You Really Need? Retrieved

March 2, 2018, from Udemy website: <https://blog.udemy.com/static-vs-dynamic-ip/>

Star Topology [Photograph]. (2008, December 24). Retrieved from

<https://commons.wikimedia.org/wiki/File:Star_Topology.png>

Switch Security Facts. (2018). Retrieved from TestOut website: https://cdn.testout.com/

client-v5-1-10-501/startlabsim.html

Wireless Security. (2016). Retrieved March 12, 2018, from Cisco website:

<https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/digital-network-architecture/at-a-glance-c45-738315.pdf>

Wireless Security Facts. (2018). Retrieved from TestOut website: https://cdn.testout.com/

client-v5-1-10-501/startlabsim.html