Brian Bergstrom

ITCO 251 – Network Infrastructure Basics

4/27/17

Discussion 5

**LabSim**

LabSim I usually do not have that much trouble with. This time I am having trouble with the last two labs involving VOIP. I have no idea what I am doing wrong, but I cannot seem to establish a network connection in the Executive Office. I did enjoy learning about the virtual machines and ways to utilize more hardware usage on machines. I also think the info on SCADA devices was interesting as more and more companies are starting to implement the cloud technology. Do they even sell computers with CD-ROM drives anymore?

**General**

Working with virtualizations can be useful when you want to test out certain things in a virtual environment. You can create what is called a virtual sandbox where you can mess up as much as you want because the environment only exists virtually and is not released to the public unless you deem it so (LabSim, 2017, Section 9.4.1). I used to work for a web hosting company where we implemented many different web services through VirtualBox on both Linux and Windows environments. We as administrators had all our server software running on a distro of Linux because it was more secure, but we had to make sure all was working on the Windows end of things, as most of our clients used Windows. Logging into the server from home was also useful because any problems that arose could possibly be fixed remotely instead of travelling all the way to the datacenter when all that needed to be done was flip a switch or monitor a situation.

One of the drawbacks to virtualizations is that they can pose the same security risks as real operating systems and hardware. The tricky part is that virtual data cannot be physically removed like it can normally. Virtual firewalls are key to help protecting virtualizations and software within them. A common technique to help is to route all network traffic into a physical network using a virtual router (LabSim, 2017, Section 9.4.5). There is also settings on the VMWare like Hyper-V to help protect against the virtualization from being taken over by unauthorized users and using it for malicious activity.

Cloud computing has totally revolutionized the way work can be done from outside of one location. Many companies and organizations have all their software and storage on the cloud to save lots of money and it is very convenient and easy to use. When you log onto the organization’s network, you can do your work from anywhere you can find an internet connection such as a library or the Starbucks down the street. Keep in mind however that public Wi-Fi hotspots are less secure than traditional connections you may have at the home or office. If anyone is snooping they can steal valuable company information because you wanted to get that silly unicorn stuff down the street. Using the cloud for things also makes you dependent on having a reliable internet connection (Lynch, 2016). Cloud services do not store anything on your computer or laptop. Without an internet connection, you will not be able to access your files you have been working on. On the flip side, if you use multiple devices such as a cell phone and laptop to type up notes, the cloud will save your work automatically and you can retrieve the information from multiple devices. Say your laptop busts. Saving backup to them cloud will allow you to pick up where you left off from another computer so your boss will be none the wiser.

**Remote Management**

When I worked from home we managed a lot of the troubleshooting remotely to do things such as allocate space for a new client or check to make sure traffic was flowing smoothly. If a server was down, we just switched the clients over to one of the backup servers within a few clicks, so they would barely notice any downtime. If it was a physical hardware problem or upgrade the client requested, then remote management would not do anything. We had to physically change the hardware out and fix what needed to be fixed. Having backups of stuff is always a good policy. That way if you make mistake in your troubleshooting, remotely or physically, you know your mistake can easily be overwritten and no harm is noticeable to the end user. Maintaining backups should be done regularly and should be logged so you know the date your data was active on the system. Also maintaining security within the network is important. In order to gain remote access, you needed a password, and we used a software called KeyPass that stored our passwords for us, so that we just had to copy/paste them when asked for login credentials. This helped prevent key loggers from tracking what we typed. It also helped because we had multiple logins to manage to access different things.

**Monitoring**

Like all networks, traffic needs to be monitored. If traffic gets too high, it is the duty of the administrator to redirect that traffic somewhere else so more can get through to clear up lanes. When traffic is high, end users will notice and bitch. If they notice nothing, all is well. If they can’t access their PowerPoint on the network, hopefully you can fix it fast. It is a good idea to get a good picture of what your typical traffic flow looks like (Dean, 2013, p.628). To do this you need to use what is called a network analyzer which captures traffic and many other things about the network. The dangerous part is they can capture some sensitive information such as passwords if they are not encrypted. Also, it may contain private user information that might be protected under HIPAA laws or other privacy laws that prevent you from sharing the information publically. To avoid getting information you do not really need, filters can be set to only get information from one specified MAC address for example (Dean, 2013, p.627). Using this and a packet sniffer can be a useful way to troubleshoot any networking problem. Regular maintenance is recommended so you don’t have to use the tools unless serious problems arise. They are good, however, for getting an idea of what goes on through various levels of the OSI model. This is why understanding the OSI model and what is at each level is important.

**Fault Tolerance**

Fault tolerance is an important aspect of network management. If something goes down on your network such as the power, you want that to be back up as fast as possible. Fault tolerance can be defined as “the capacity for a system to continue performing despite an unexpected hardware or software malfunction” (Dean, 2013, p.652). Having a backup generator for when the power goes out will keep any hardware running without disrupting network traffic. Again, the goal is for the end user not to notice. If they do, it could cost them or the company money to replace what was lost or missing. If you have a lot of redundancy in your system, you have your data backed up in multiple locations so you can troubleshoot the damaged component while you redirect everything onto a separate network for example. Of course, cost is a major drawback to redundancy, but if it keeps the clients and end users happy, it’s worth it (Dean, 2013, p.658). Testing any troubleshooting can be easier and cost less if practiced in a virtual environment to save the company money. The physical environment physical devices are in matters a lot too. Make sure areas are temperature controlled and are free of any moisture from humidity (Dean, 2013, p.653). I remember moisture was big deal when working in the datacenter. Everything was kept cool to prevent things from overheating and no moisture could get past a certain point around the server cabinets.

References

Dean. (2013). *Network+ Guide to Networks*, 6th Edition. [Bookshelf Online]. Retrieved from <https://online.vitalsource.com/#/books/9781133608196/>

Lynch, J. (2016). What are the benefits and drawbacks of cloud computing? *TechSoup*. Retrieved from <http://www.techsoup.org/support/articles-and-how-tos/what-are-the-benefits-and-drawbacks-of-cloud-computing>

TestOut (2017). Network Customization. *LabSim.*  Retrieved from http://www.testout.com