Unit 4 Research Project

Eddie S. Jackson

Kaplan University

IT540: Management of Information Security

Kenneth L. Flick, Ph.D.

10/14/2014

Table of Contents

Abstract

The unit four research project presents a two-part assignment that challenges the graduate student to research alternate processing sites. The primary objective of the research project is to reinforce the fundamentals associated with business continuity. Part one of the assignment lists a series of questions to be researched and answered in essay form. The questions consist of topics related to a third party data center hosting an alternate processing site; firewalls, remote access, and physical security must be considered when evaluating the third party company. In part two of the assignment, Pixel, a video animation company, requires the design and implementation of an alternate processing site. The company has provided network specifications, security policies, and report requirements that must be reviewed and factored into the business continuity plan. Ultimately, the project is meant to build knowledge associated with critical business operations, business continuity, and network disaster recovery planning.

Unit 4 Research Project

Part I - Questions

Is a firewall needed? The first question leads to the assessment of firewalls and understanding the level of importance they hold within any network design. Firewalls are hardware devices and software applications that act as barriers between public and private networks. The use of firewalls allow companies to filter and control traffic by managing the communication stream. This is accomplished by blocking and allowing connectivity to network resources based upon TCP/IP ports, IP addresses, and computer services (Google Patents, 2002). Considering the question, *"Is a firewall needed?"* the answer would be yes. The answer is *yes* because a firewall will be required to protect Pixel's assets from unwanted, outside connections; meaning, firewalls will be utilized to protect company data located at an alternate processing site, even if that site is hosted by a third party servicer. Additionally, many firewalls, such as the Cisco PIX 500 Series Firewall, have the ability to track and monitor network connectivity; thus offering more robust perimeter security (Cisco, n.d.).

Is remote access required? One last essential feature of firewalls is virtual private network (VPN) capability, which segues into the next topic of remote access. In the scenario where an alternate processing site is being brought online, having the ability to remotely connect to and use Pixel network resources will be crucial in maintaining business continuity; this will allow displaced personnel to work from home, while keeping support costs as low as possible (Mitchell, n.d.). VPNs, and thus remote connectivity, are important in the design and implementation of a network disaster site. Offering remote connectively via VPNs will help get Pixel employees back to work faster, while at the same reducing the space requirements at an alternate processing site (Mitchell, n.d.). Due to the benefits of remote connectivity, remote access is required.

What is the physical security? Considering a third party outsourced data center, the physical security of servers that contain Pixel data should be of paramount concern. Although the third party servicer is liable for the loss or theft of Pixel data, it is ultimately the responsibility of Pixel to verify the third party servicer is meeting the security standards of the organization. A few security requirements include: secured server rooms (meaning, locked rooms); surveillance of server equipment and network racks; and finally, completed background checks for everyone who has access to the servers (Shinder, 2007). By maintaining the physical security of network resources, company assets can be protected from intruders and thieves (and even track accidents and negligence in server areas).

Part II – Alternate Processing Site

In part two of the assignment, Pixel has provided network specifications and security policies that must be used in the design and implementation of an alternate processing site. Once the current information has been reviewed, a sixteen point report is created to document and detail everything required to bring an alternate processing site online; the report discusses the mission critical components, illustrates network connectivity, and provides operating procedures that are essential to maintaining business continuity. The last two points of the report discuss strategies for cutting over to the alternate processing site, as well as cutting back to the main site.

After reviewing the current information that Pixel has provided, it has been determined that a *cold site* would be best suited for the needs of the company. A cold site is a building that has heating, air, electrical, plumbing, and basic network wiring to maintain business continuity, if and when a disaster strikes (Core Xchange, n.d.). Now that the type of disaster recovery site has been selected, a full report must be drawn up to address the specific needs of the Pixel organization.

Report

(1/11). The first item in the report identifies all the mission critical and non-critical applications. Important applications include operating systems, email, databases, anti-virus, and video publishing software. A few applications that can be dropped at the alternate processing site are: the client-side intrusion detection software–this will be managed by a Cisco firewall; the web server and SFTP software, which will be outsourced; the printer server software–will not be needed, as a centralized commercial copier will be accessible by everyone (as well as a few local printers); and finally, the server backup software will not be necessary–backups will be performed manually.

MISSION CRITICAL APPLICATIONS	NON-CRITICAL APPLICATIONS
Email client software; Microsoft Outlook	Client-side intrusion detection software
Email server software; Microsoft Exchange	Public facing web server
Red Hat Linux operating system	Secure FTP (SFTP) software
Apple Mac OS X Leopard	Printer server software
Microsoft Vista operating system	Server backup software
Windows Server 2008 operating system	
- File sharing service	
- DNS	
- Email service	
Video rendering software; Adobe After Effects	
Office productivity software; MS Office	
Database software; Microsoft SQL	

Anti-virus software; for MAC & PC	

(2/11). The second item in the report identifies all the hardware equipment that will need to be installed at the alternate processing site. It is important to note, that in a disaster recovery scenario, fifty percent of the staff will remotely connect to the office and perform their duties over a VPN connection; thus, the chart reflects the necessary resources to support fifty onsite users and fifty remote users. A few significant differences between the active site and the alternate processing site, are at the secondary site: a Cisco ASA 5510 firewall has been selected to provide VPN and DHCP services (to remote users); a single Windows server will be installed to combine DNS, file sharing, and email services; lastly, rather than managing enterprise backups via software, two external hard drives will be connected to the Windows server (for redundancy) (Geier, 2011). Manual backups will be performed by each end-user to appropriate, access controlled folders located on the storage device.

MISSION CRITICAL EQUIPMENT	**NON-CRITICAL EQUIPMENT**
30 Vista-based workstations	30 Vista-based workstations
20 MAC-based workstations	20 MAC-based workstations
10 dual processor Xeon servers; 3D rendering	10 Dual processor Xeon servers
1 Windows Server 2008 (DNS, File sharing, Mail)	2 Windows Server 2008
1 Cisco Firewall; Cisco ASA 5510 (VPN/DHCP)	SOHO firewall
1 Cisco Router; 1700 series	1 Cisco Router; 3640 series
1 Brighthouse broadband modem (10MB)	
2 4 TB external hard drive for manual backups	RAID backup array

1 Xerox commercial scanner/copier	
10 desktop printers	20 Desktop printers
1 48 port Cisco Switch (1GB)	2 48 port Cisco Switch (1GB)
1 24 port Cisco Switch (1GB)	3 24 port Cisco Switch (1GB)
2 racks with monitors and keyboards	4 racks with monitors and keyboards

(3/11). The next step in bringing the alternate processing site online is to install the equipment. Coordinating the installation of workstations and network equipment can be quite time consuming; thus, the process requires formulating a technical strategy to facilitate a smooth transition from the active site to the alternate site (Ready, 2012). This strategy includes knowing which equipment needs to be installed and who is responsible for installing it. Additionally, a general timeline will keep the synchronized effort on track. Note, the expected installation time to bring the alternate site online is seven hours; this includes the installation and testing of all equipment, as well as coordinating installation efforts to adhere to a strict timeline–the timeline will be managed by the security officer, which reports directly to the CEO. The technical strategy for equipment installation can be seen in the chart below.

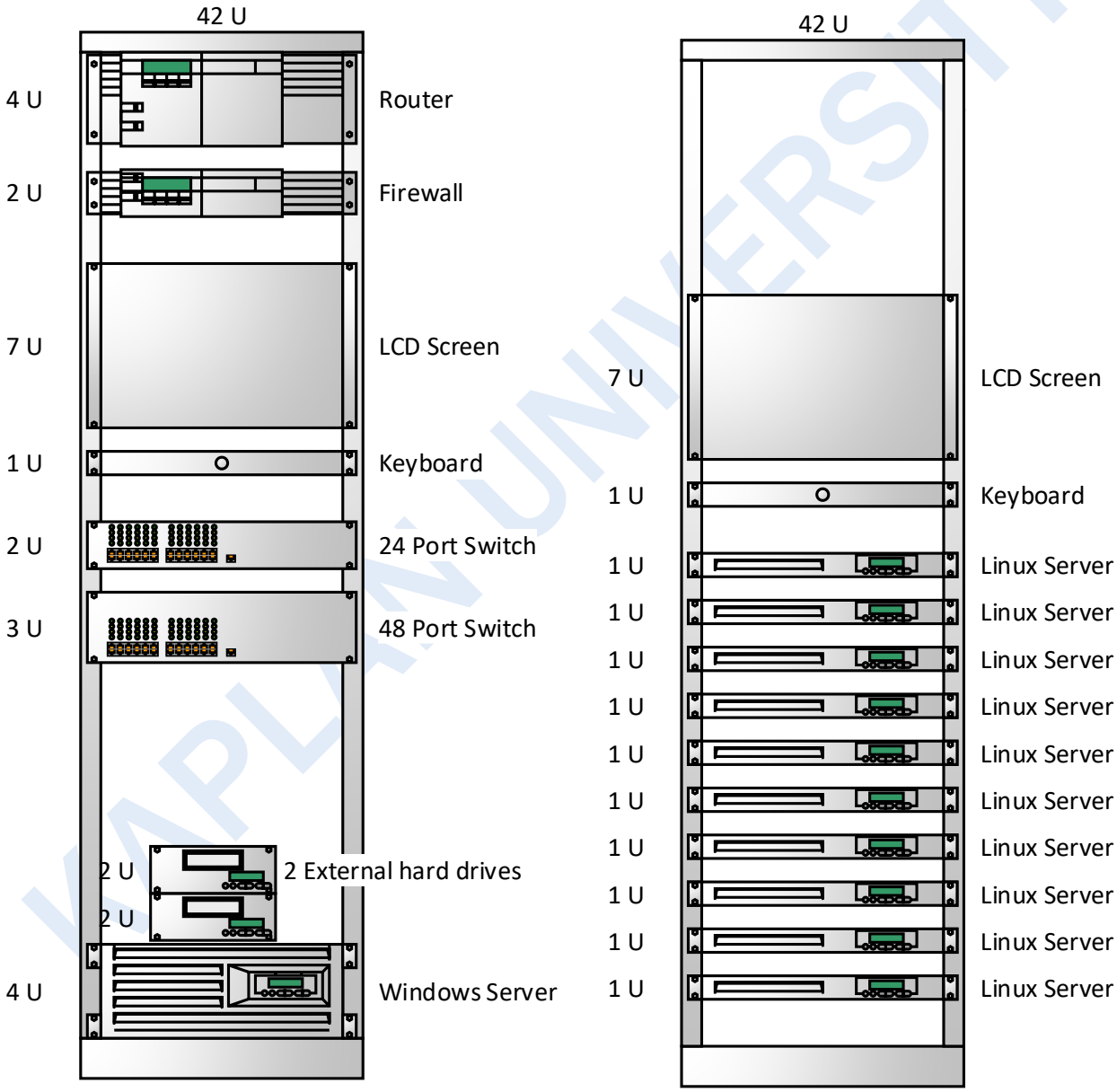
EQUIPMENT TO BE INSTALLED	**INSTALLER**	**TIMELINE**
1 Windows Server 2008	Pixel system administrator	7:00 AM - 8:00 AM
2 Racks with monitors and keyboards	Pixel network administrator	7:00 AM - 8:00 AM
1 Cisco 1700 series	Pixel network administrator	8:00 AM - 9:00 AM

30 Vista-based workstations	4 Pixel employees (Vista users)	8:00 AM - 3:00 PM
20 MAC-based workstations	3 Pixel employees (MAC users)	8:00 AM - 3:00 PM
2 4 TB external hard drive for manual backups	Pixel system administrator	8:00 AM - 9:00 AM
1 Brighthouse modem	Brighthouse	9:00 AM - 11:00 AM
1 Xerox Copier	3rd party servicer	9:00 AM - 11:00 AM
Cisco ASA 5510 firewall	Pixel network administrator	10:00 AM - 11:00 AM
10 dual processor Xeon servers	Pixel system administrator	10:00 AM - 03:00 PM
1 24 port Cisco Switch (1GB)	Pixel network administrator	11:00 AM-12:00 PM
1 48 port Cisco Switch (1GB)	Pixel network administrator	11:00 AM - 12:00 PM
10 desktop printers	1 Pixel employee	11:00 AM - 3:00 PM

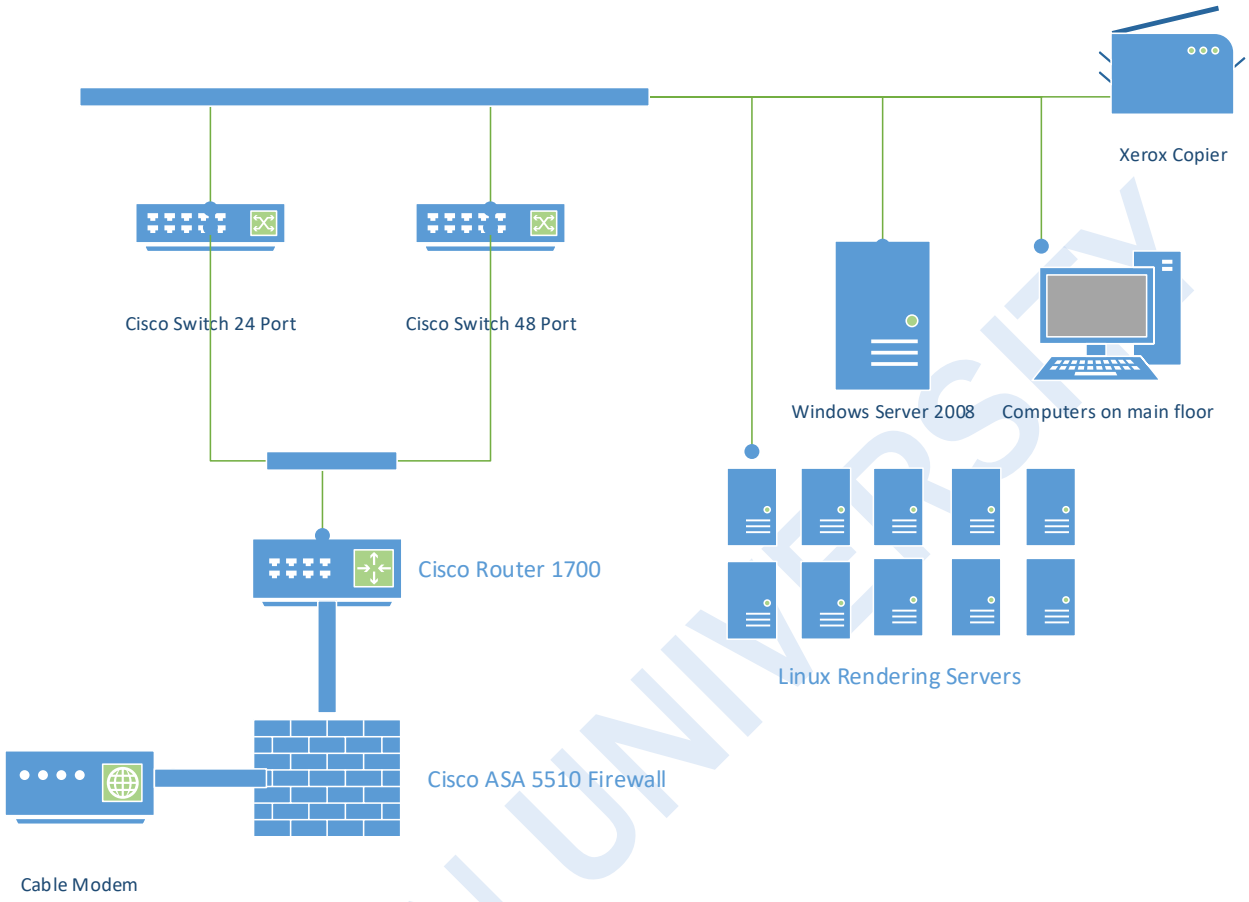
(4/11). The fourth item on the report outlines a plan for updating the software located at the alternate process site. The primary applications, such as office productivity software, video publishing software, and email client software, are part of managed company images, thus will not require updating. However, there are several alternate site applications that need data transferred and imported from the active site; this includes client data, video project files, and email stored on the Microsoft Exchange server. The strategy for moving the data from one site to the next is to wait until all workstations, servers, and network devices have been setup and fully tested. At that time, the active site will be taken offline, the client data, video project files, and email backed up to storage media, and then that storage media transferred to the alternate site (IBM, n.d.). Once at the site, the system administrator will import the email data into the

Exchange server, copy the video project files to the Linux rending farm, and import client data into the SQL database.

(5/11). The fifth item in the report illustrates rack and network diagrams. The diagrams provide visual guides for setting up the network. The rack diagram can be seen below.



This is the network connectivity diagram:



(6/11). The sixth item in the report details the exact network configuration. This information is meant to be used in configuring each of the devices connected to the network. It is important to note, a class C private IP addressing scheme has been selected due to the small amount of hosted devices at the alternate processing site. A class C IP addressing scheme ranges from 192-223 in the first octet (VLSM-Calc, n.d.). One important caveat is how IP addresses will be assigned to devices; VPN connections will be assigned IP addresses by the DHCP on the Cisco ASA 5510 firewall; however, IP addresses will be manually inputted on the workstations located onsite. The network configuration data can be seen in the chart below.

Network Device	IP Address
Cable modem	66.43.21.6 9 (public address)
Cisco ASA 5510 firewall	192.168.0.1, 192.168.0.2
Cisco 1700 series	192.168.0.3
30 Vista-based workstations	192.168.0.50-192.168.0.80
20 MAC-based workstations	192.168.0.81-192.168.0.101
1 Xerox Copier	192.168.0.200
10 dual processor Xeon servers	192.168.0.5-192.168.0.15
Windows Server 2008	192.168.0.16 (DNS, email, file services)

(7/11). In the seventh report item, power consumption is considered, researched, and the information added to a power consumption chart; the total power consumption is 28,847 watts. This data can be seen below.

EQUIPMENT	POWER CONSUMPTION
Cable modem	15 watts
Cisco ASA 5510 firewall	30 watts
Cisco 1700 series	20 watts
30 Vista-based workstations	45 watts x 30 = 1,350 watts
20 MAC-based workstations	60 watts x 20 = 1,200 watts
52 LCD Screens	300 watts x 52 = 15,600 watts
2 4 TB external hard drive for manual backups	14 watts x 2 = 28 watts
1 Xerox Copier	1,331 watts

10 dual processor Xeon servers	800 watts x 10 = 8,000 watts.
1 24 port Cisco Switch (1GB)	30 watts
1 48 port Cisco Switch (1GB)	45 watts
10 desktop printers	120 watts x 10 = 1,200 watts

(Prelec, n.d.)

(8/11). The eighth report item assesses the bandwidth at the alternate processing site. To meet the current bandwidth standards, 10 megabit/second has been selected as the minimum speed of the cable modem. Pixel requires the 10 megabit/second due to Internet use, email, and online collaboration with clients on projects. Also, the internal speeds of the network will operate at one gigabit. This will insure that working on and moving the larger-sized video files will not be affected by slower network speeds (Rogers, n.d.).

(9/11). In the ninth report item, security components such as firewalls and VPNs are discussed, as they are critical to business continuity and the protection of company assets. When setting up an alternate processing site, a firewall is required to create a technology barrier between public networks and Pixel's private network. Specifically, the Cisco ASA 5510 Security Appliance has been selected to protect the internal network. The Cisco firewall has VPN and DHCP features; both of these features will be required at the alternate processing site to allow personnel to remotely connect to network resources in a secure fashion (using SSL VPN). Additionally, the Cisco security appliance offers intrusion prevention, URL filtering, and anti-spam features (Cisco, n.d.). These features will enhance the perimeter security, while at the time protecting the internal network from spam and phishing attempts. Thus, incorporating the Cisco ASA 5510 Security Appliance into the security architecture at the alternate processing is a necessity.

(10/11). The tenth report item outlines the strategy for performing the cutover from the active site to the alternate processing site. One of the most important elements in the cut over plan is knowing who is in charge; that is, who will give the command to switch business operations from one site to the next. For Pixel, that person is the security information officer, which reports directly to the CEO. Once the secondary site has been signed off on by the network administrator, the system administrator, and the personnel involved in setting up workstations and printers on the main floor, the security information officer will perform a walk-through at the alternate site; the network administrator and system administrator will accompany the information security officer. All systems will be verified operational at this time.

Next, once the information security officer is satisfied that the alternate site is ready for switching over operations, systems at the main site will be taken offline, and backups will be performed. If backups are not available at the main site (due to an unforeseen disaster), backups will be acquired from offsite storage. When the backups arrive at the alternate processing site, data will be imported and systems restored to full operational capacity. The system administrator will perform necessary restoration tasks; and once complete, the information security officer will verify all systems are operational–remote connectivity, the Linux rendering servers, and the Windows server be checked for current operational statuses. If each system is working as intended, the information security officer will notify the CEO that the cut over was successful. The CEO will then send out a communication to all personnel, alerting them of the site changes, and that the company is operating in disaster recovery mode; attached to the CEO's communication will be the policy for the company operating in a disaster recovery status. (Arcserve, 2008)

(11/11). The final report item, number eleven, discusses the process for cutting back to the main site. The cut back process is very similar to the cut over strategy. The information security officer will be in charge of verifying that all systems at the main site are operating at normal capacity; and once again, will be accompanied by the network and system administrators. Once the primary systems, such as the web server, file and printer sharing, the Linux rendering servers, SFTP, and DHCP, have been confirmed as operational, the alternate site will be taken offline and backups acquired. The system administrator will perform the restoration tasks, and the information security officer will confirm each system as it becomes fully operational.

When the information security officer is satisfied that all systems are a go, the CEO is notified that the cut back has been successful. The CEO will send out a communication to all personnel notifying them that the company is back in normal operational status, and instruct employees to return to the main site the next work day. The alternate site will remain intact for forty-eight hours, or two business days. After that time, the equipment must be broken down, and returned to its original location. The personnel that was involved in installing the equipment at the alternate processing site must also be involved in the tear down. When all equipment has been removed from the secondary site, the information security officer will perform one final walk-through. If the site is clean and no equipment has been left behind, the CEO will be notified that the alternate processing site has been successfully cleared.

References

Arcserve. (2008). Business Continuity Planning. IT Survival Guide. Retrieved from http://www.arcserve.com/cn/~/media/files/whitepapers/business-continuity-planning-it-survival-guide.aspx

Cisco. (n.d.). Cisco PIX 515E Security Appliance. Retrieved from http://www.cisco.com/c/en/us/products/security/pix-515e-security-appliance/index.html

Cisco. (n.d.). EOL/EOS for the Cisco PIX 515E security appliance. Retrieved from http://www.cisco.com/c/en/us/products/collateral/security/pix-500-series-security-appliances/end_of_life_notice_for_the_Cisco_PIX_515E_Security_Appliance.html

CoreXchange. (n.d.). Disaster recovery hot, warm, cold sites: key differences. Retrieved from https://www.corexchange.com/blog/disaster-recovery-hot-warm-cold-sites-key-differences

Geier, Eric. (2011/1/18). Five VPN clients for Linux http://www.linuxplanet.com/linuxplanet/tutorials/7271/1

Google Patents. (2002/3/5). Firewall system and method. US 6353856 B1. Retrieved from http://www.google.com/patents/US6353856

IBM. (n.d.). Disaster recovery manager checklist. Retrieved from https://publib.boulder.ibm.com/infocenter/tsminfo/v6/index.jsp?topic=%2Fcom.ibm.itsm.srv.doc%2Fr_drm_chklist.html

Mitchell, Bradley. (n.d.). What are the advantages and benefits of a VPN? Retrieved from http://compnetworking.about.com/od/vpn/f/vpn_benefits.htm

Prelec. (n.d.). Home appliance wattage consumption guidelines. Retrieved from http://www.erakiprelec.co.za/wattage-consumption.html

Ready. (2012/10/25). IT disaster recovery plan. Retrieved from http://www.ready.gov/business/implementation/IT

Rogers, Joe. (n.d.). Using fast/gigabit Ethernet to satisfy expanding bandwidth needs. Retrieved from https://net.educause.edu/ir/library/html/cnc9805/cnc9805.html

Shinder, Deborah. (2007/7/16). Ten physical security measures every organization should take. Retrieved from http://www.techrepublic.com/blog/10-things/10-physical-security-measures-every-organization-should-take/

VLSM-Calc. (n.d.). IP address classes. Retrieved from http://vlsm-calc.net/ipclasses.php