Network Infrastructure Administration

(IT326-1604B-01)

Veterans Health Administration Network Implementation Project

Richard South

December 3, 2016

Contents

[Target Organization 3](#_Toc467313047)

[Proposed Network Solution 4](#_Toc467313048)

[Network Design 5](#_Toc467313049)

[Installation and Configuration 6](#_Toc467313050)

[Maintenance and Troubleshooting 7](#_Toc467313051)

[Remote Access 8](#_Toc467313052)

[Network Pro Prep Toolkit 9](#_Toc467313053)

Section 1: Target Organization

The Veterans Health Administration (VHA) is one of three components that makes up the United States Department of Veterans Affairs or VA for short. The VHA is comprised of approximately 168 medical facilities and 1,053 Community Based Outpatient Clinics (CBOCs) throughout the nation including Guam, American Samoa, and the Philippines which are broken down into 21 geographically Veterans Integrated Service Networks, known as VISNs (VA, 2016). Each VISN is comprised of one or several medical facilities, and each facility will have several CBOCs assigned to it which are located throughout that particular region.

The VHA employs over 300,000 healthcare professional and support staff with an annual budget of approximately $59 billion (VA, 2016). The VHA serves over 8.9 million veterans from all military branches a year with their medical needs and concerns (VA, 2016). The VHA must be able to communicate, access and relay information to and from other medical facilities and clinics within the VHA system in a timely, efficient and secure manner.

Section 2: Proposed Network Solution

With the size of the VHA, a wide area network must be considered for this project. A client/server model would be the network solution. The network will be configured that primary servers will be located at the main medical facility for each VISN. The remote CBOCs locations and other VHA medical facility will be connected through VPN to safeguard the data sent to and from the parent medical facility. DNS will offer any VHA facility the ability to access the internal servers including external servers on the Internet. DHCP would be the ideal client/server protocol since it is flexible regarding assigning IP addresses based on the open ranges in the routers to which the devices are connected.

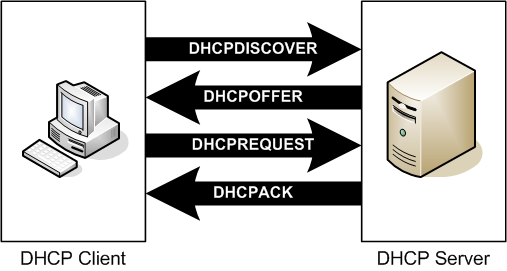
Network protocols are formal rules that contain methodology on how communication between at least two devices transmit over a network and is typically used in many organizations. A few protocols likewise bolster message affirmation and intelligence pressure intended for stable or potentially superior network communication. IP Routing, along with switches, will serve the devices in the VHA facilities to transmit and direct traffic to external IP addresses.

Certificate Services is an active directory running on a Windows server operating system, and it receives demands for new certificates over transports (Microsoft, 2016). It checks every order against custom or site-particular arrangements, sets discretionary properties for an endorsement to issue, and issues the declaration. It permits administrators to add components to a certificate revocation list (CRL) and to distribute marked CRLs all the time. It incorporates programmable interfaces for making support for other transports, arrangements, and authentication properties and configurations (Rouse, 2016). Certificates will be applied between VA medical facilities and clinics to guarantee that the devices that are communicating with each other belong to the properly permitted parties. Also, SSL certificates will be the encryption standard within the VHA. WINS will not be considered since on devices operating on the network will using DNS.

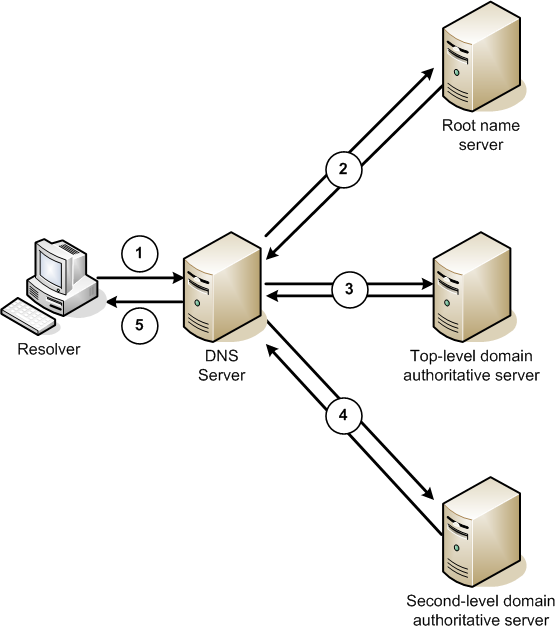
This is a very classic configuration that will sufficiently support the VHA presently and for many years. This network setup will allow it to be flexible should this organization decide to expand or upgrade. These standards will assist IT specialist to identify any problems that may occur with the network quickly.

Section 3: Network Design

The network design of the Veterans Health Administration (VHA) would analyze the requirements of the network regarding devices, how these devices would work together and how these devices would be configured to work properly, to support the movement of data to and from other medical facilities and clinics within the VHA system. The network design will cover the DNS, DHCP, Network Protocols, WINS, IP routing and certificate services as part of the requirements. The Dynamic Host Configuration Protocol (DHCP) is a service which will automatically configure the TCP/IP and IP address settings by assigning workstations at the facility dynamically and reclaiming them after a given period or when they are not in use.



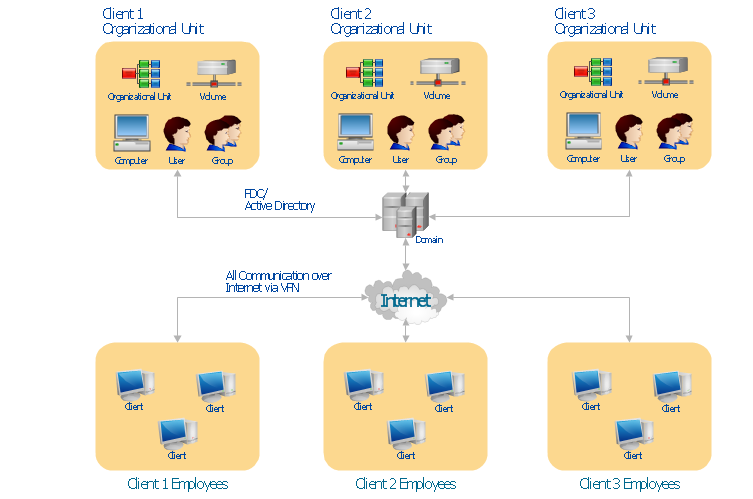
The DNS server would perform name resolutions for devices connected to the organization network enabling them to partake in the internet and active directory communications. The Domain name system would be responsible for converting host names into IP addresses. The DNS would consist of root name servers and top-level domain servers which would enable VHA and its connected medical facilities to access various web pages on the internet. Given that the facility was going to run an Active Directory, at least on DNS server would be required to support the DNS Server service on Windows Server 2008.



Given that the remote CBOCs locations and other VHA medical facility would be connected through VPN to safeguard the data sent to and from the parent medical facility VPN routers would be applicable for setting up VPN connections. Other technologies that would be used to create the VPN included an IPsec tunneling protocol and a generic routing encapsulation. Configurations such as Network Address Translation (NAT) and other basic security configurations (Cisco, 2016). Other than VPNs, use of firewalls, encryption, routing filters and definition of security zones would be used to protect VHA’s data and system resources from damage or theft.

The mechanism for addressing would involve subnetting the IP addresses for the different connected facilities, super netting and private IP addressing. IP routing would involve the use of class inter-domain routing where facilities connected to VHA would be assigned a range of IP addresses, use of routing policies and various routing protocols such as BGP or RIP. The Server running Windows Server 2008 or 2012 would offer certificate services and would receive digital certificates over transport protocols such as HTTP. Certificate services would enable administrators in the various facilities to add components to a certificate revocation list (CRL) and publish CRLs on a constant basis. Routers used by the facility.

Performance architecture of the network design would define how network resources would be allocated to users in the facilities as well as devices. Furthermore, it would involve capacity planning, quality of service, SLAs, access control and resource management. Given that VHA wanted to implement a WAN defining a topology model and a client-server flow model would be essential. These models would support key the networks key functions such as Internet Service Providers, intranets/extranets, single or multitier performance and also end to end models.



Above is the overall network design drawn using concept draw.

Section 4: Installation and Configuration

TBD

Section 5: Maintenance and Troubleshooting

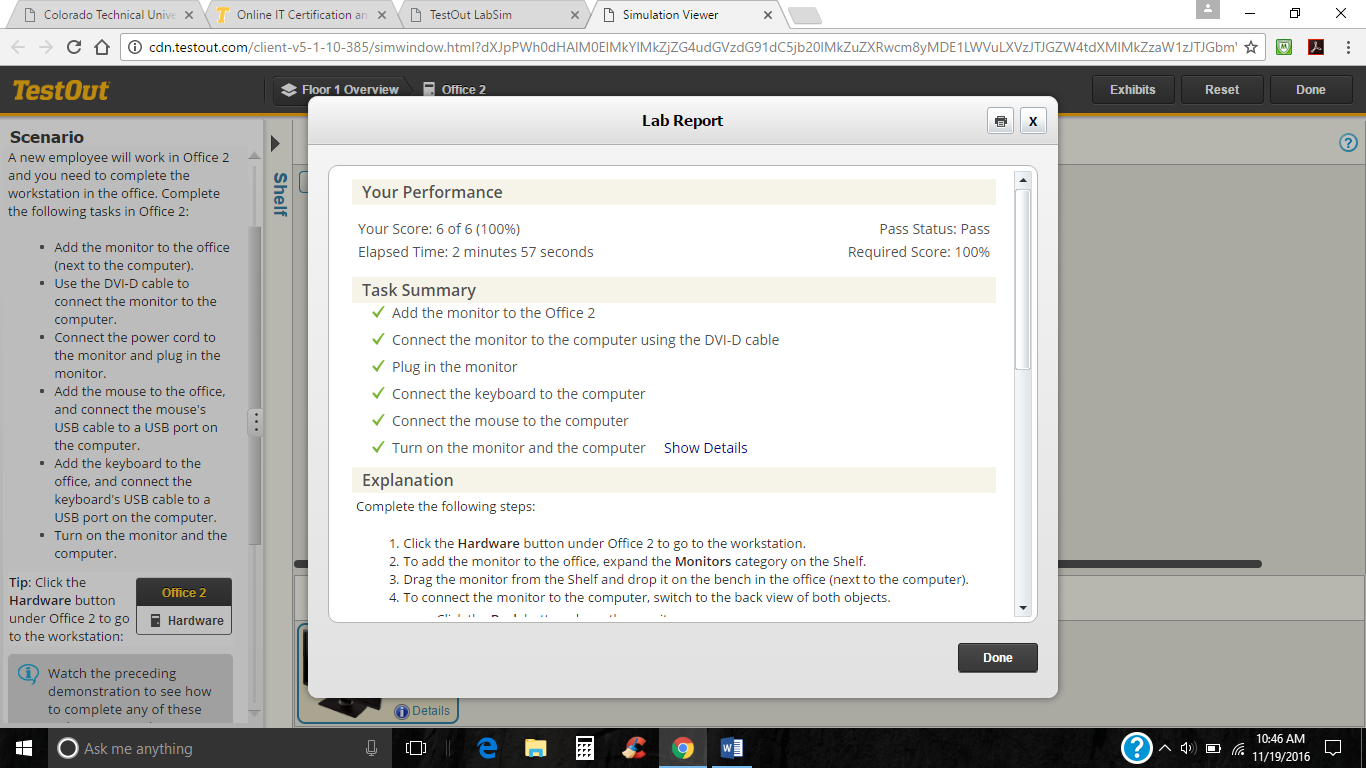
TBD

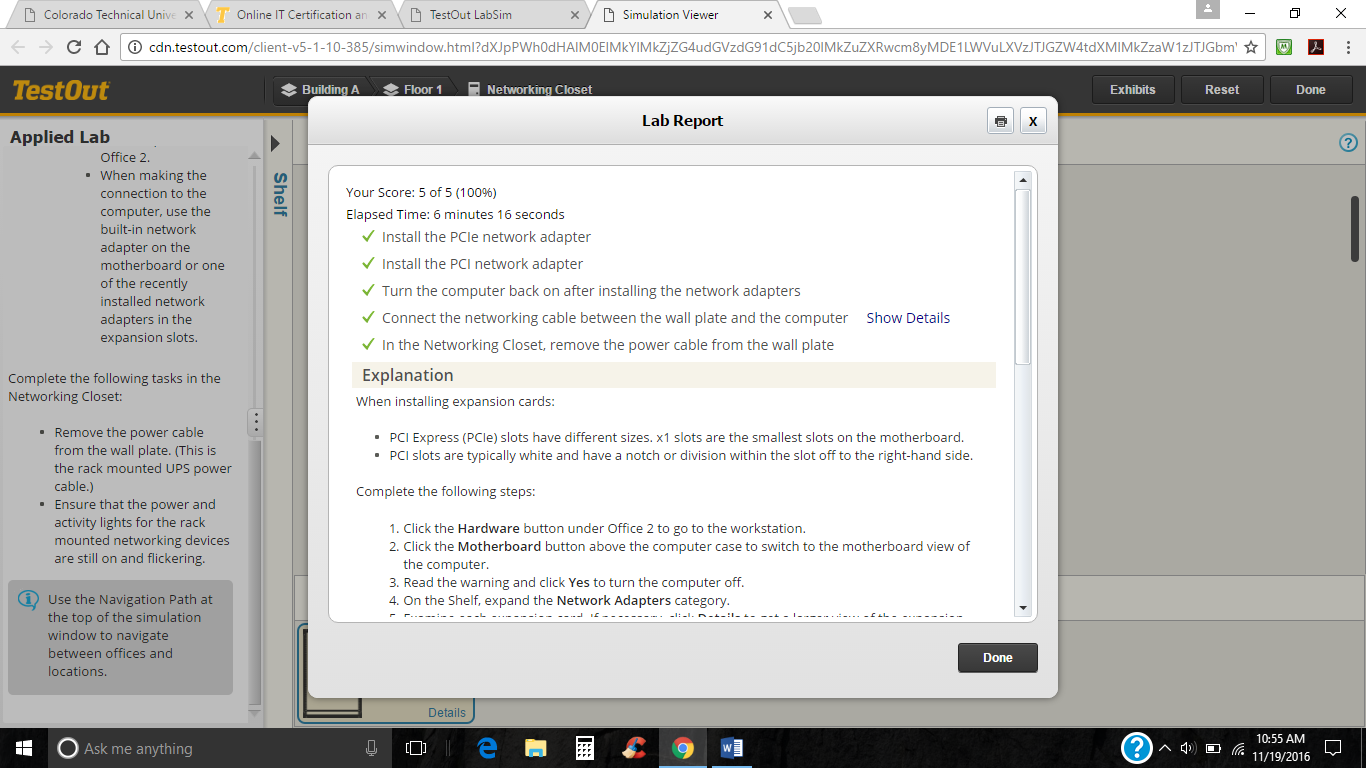
Section 6: Remote Access

TBD

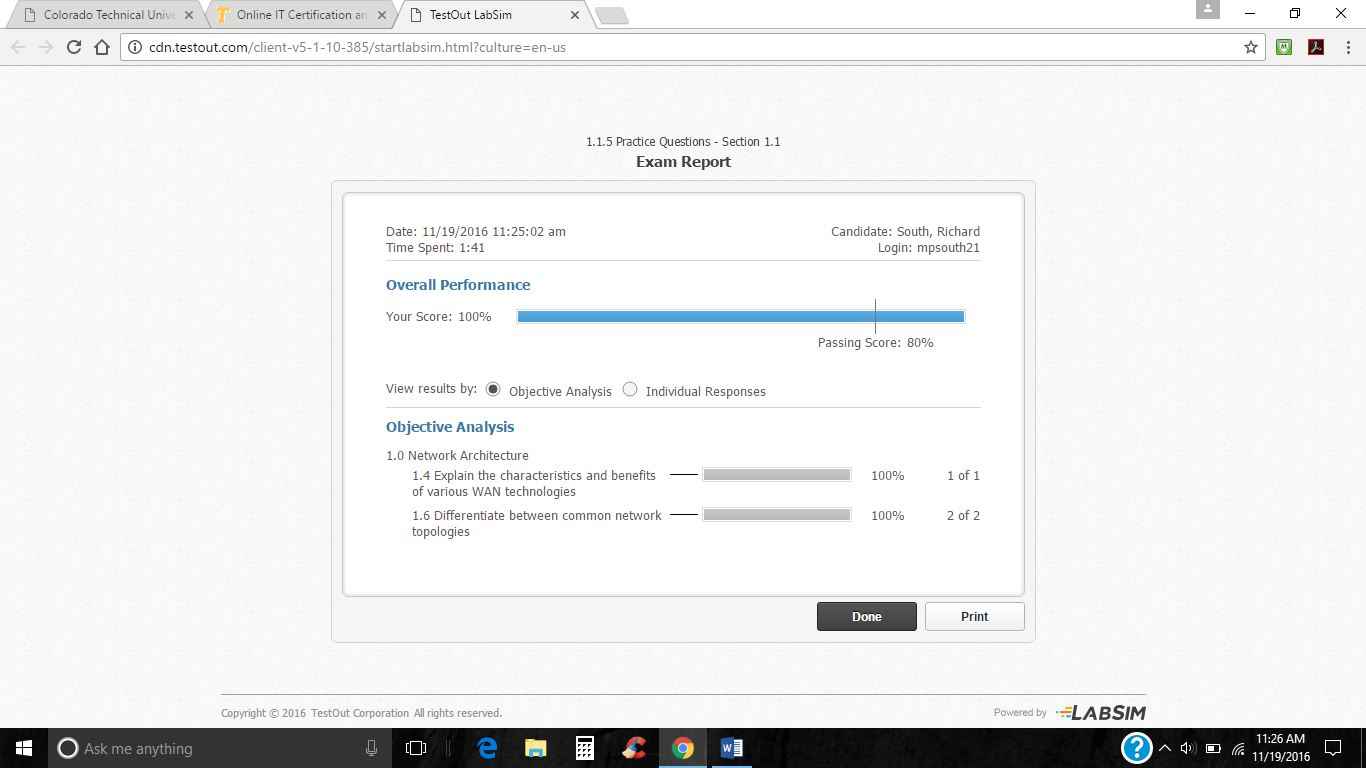
Section 7: Network Pro Prep Toolkit

**0.1.2**

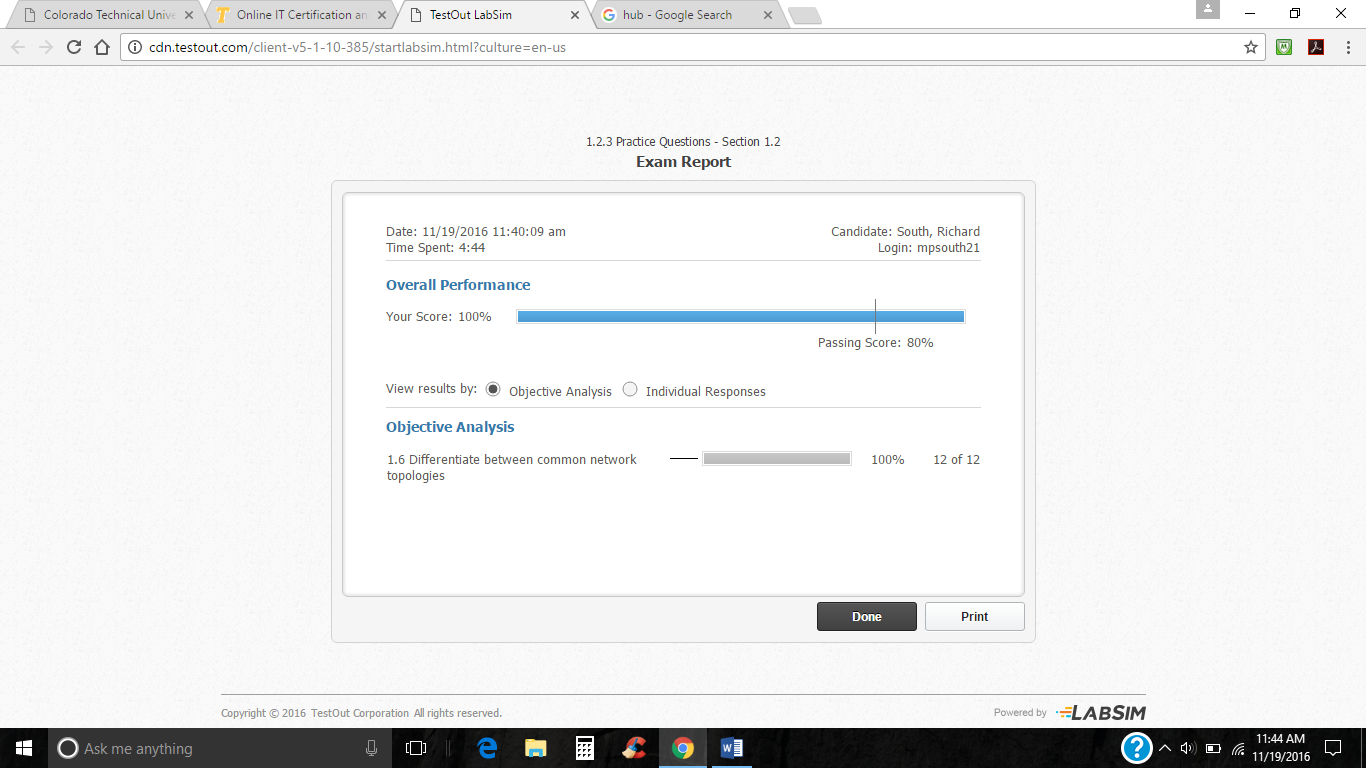


**0.1.3**

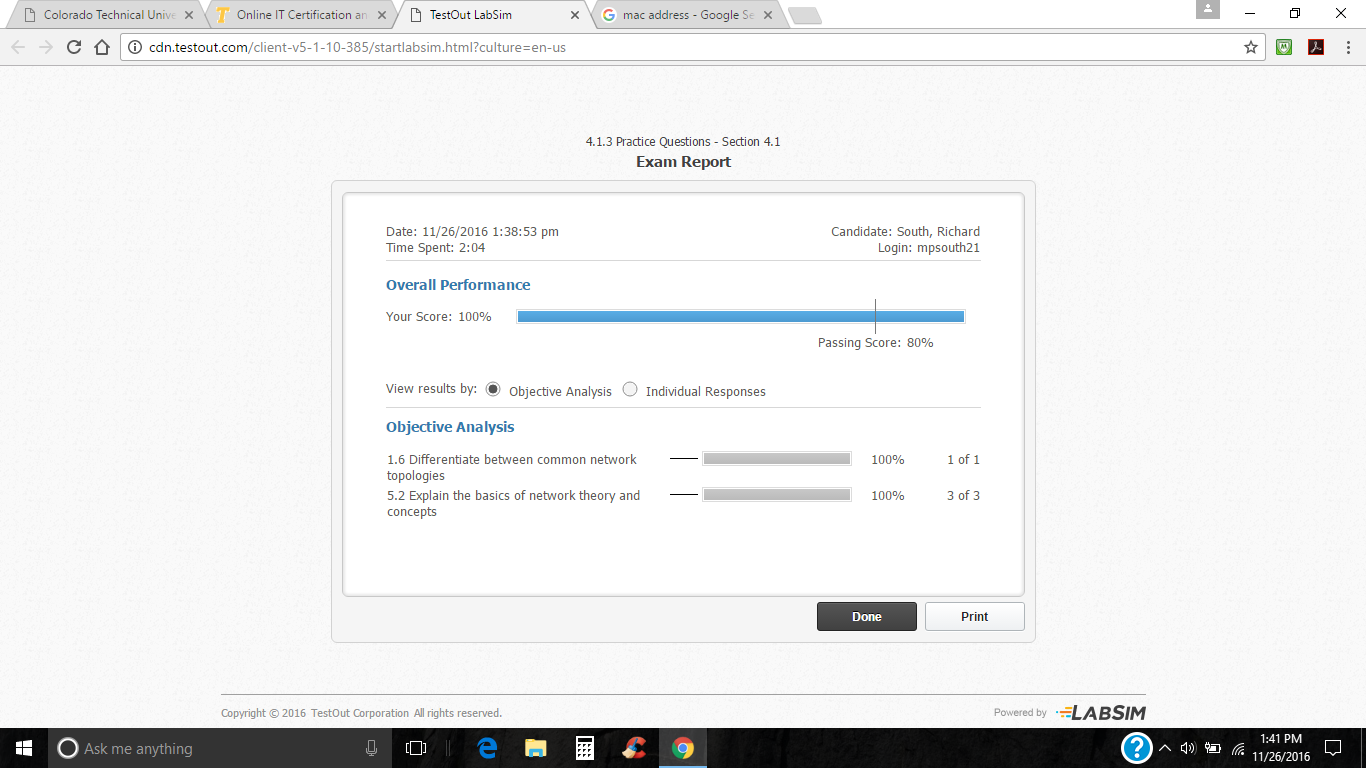
**1.1.5**



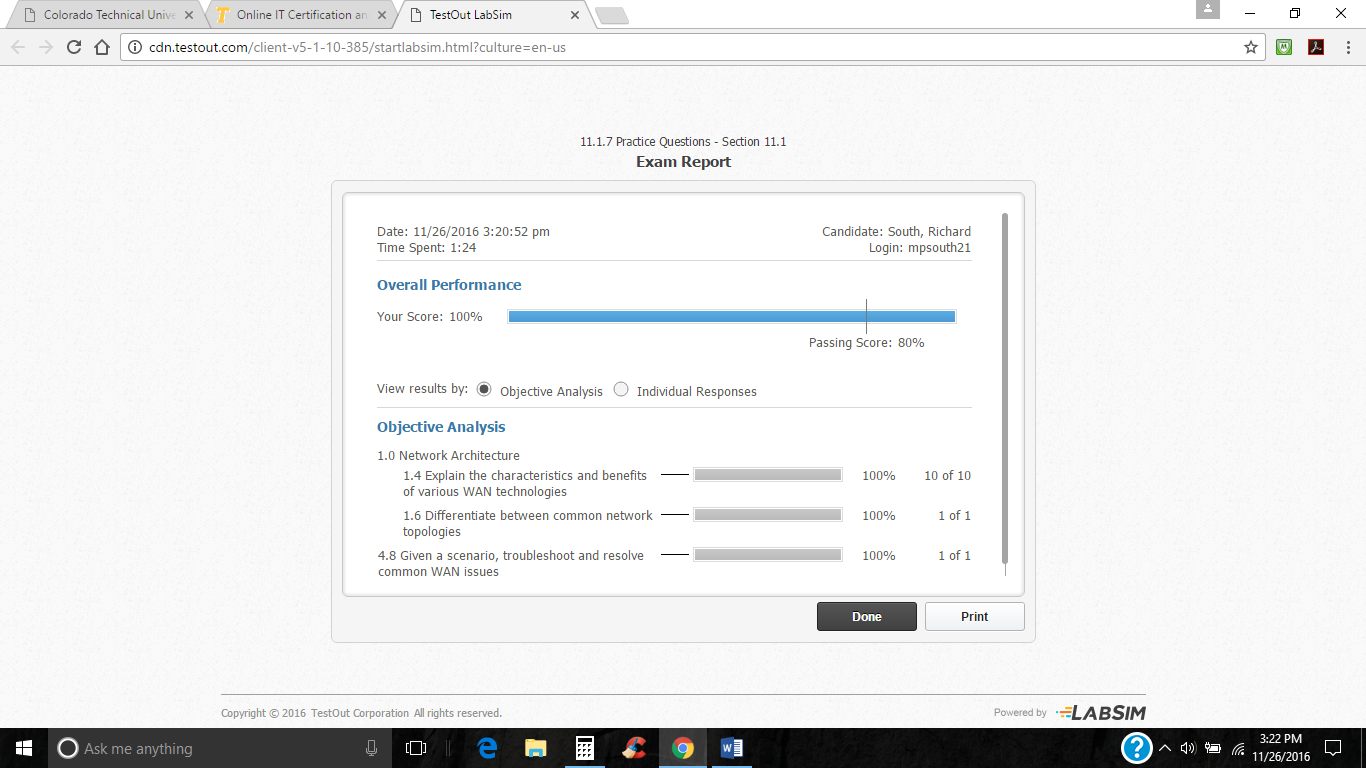
**1.2.3**



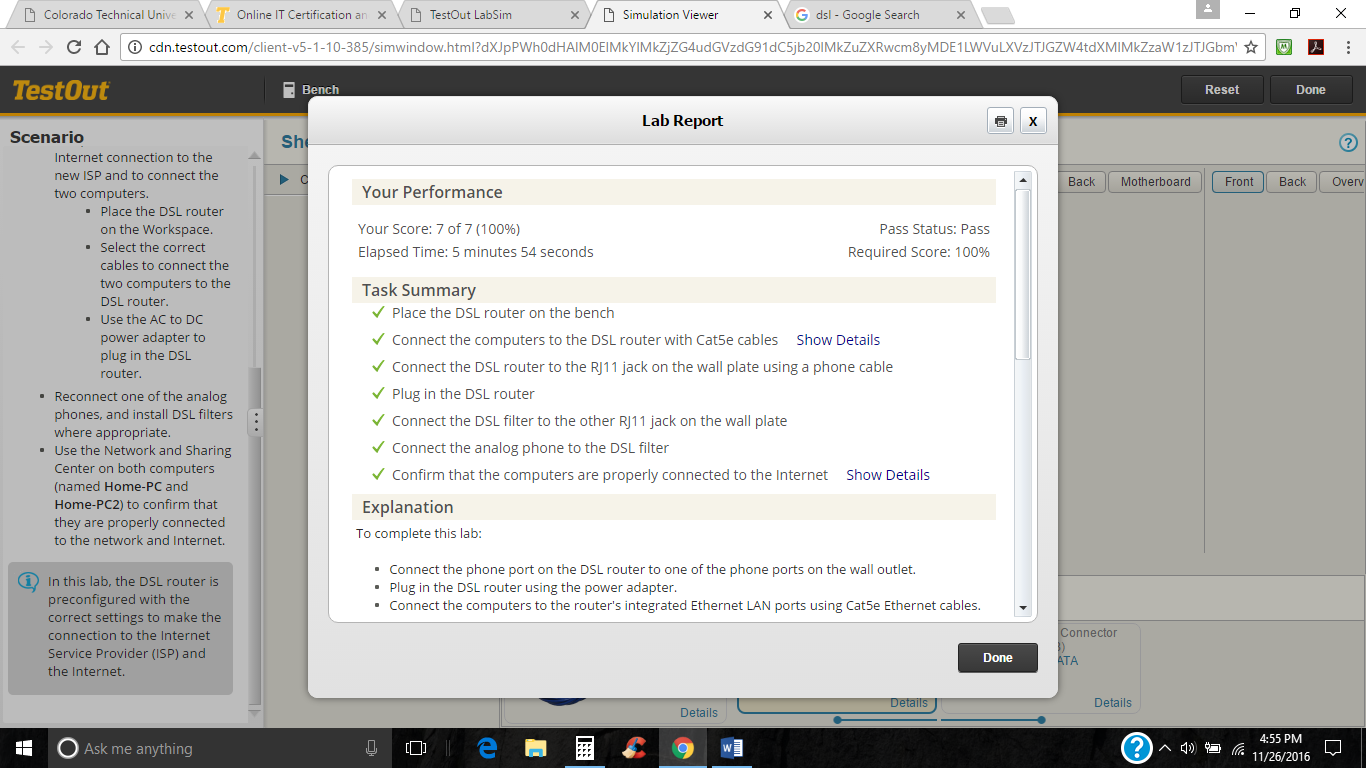
**4.1 Ethernet**



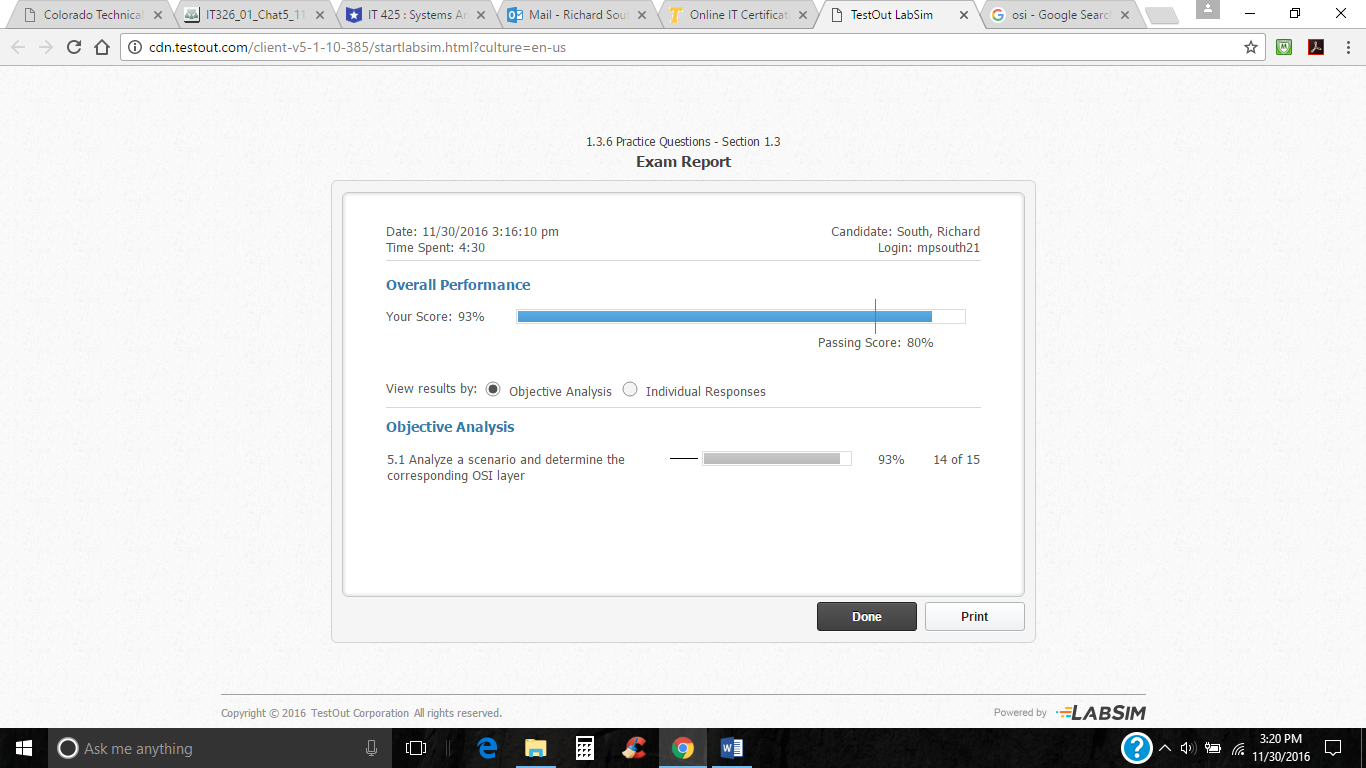
**11.1 WAN Concepts**



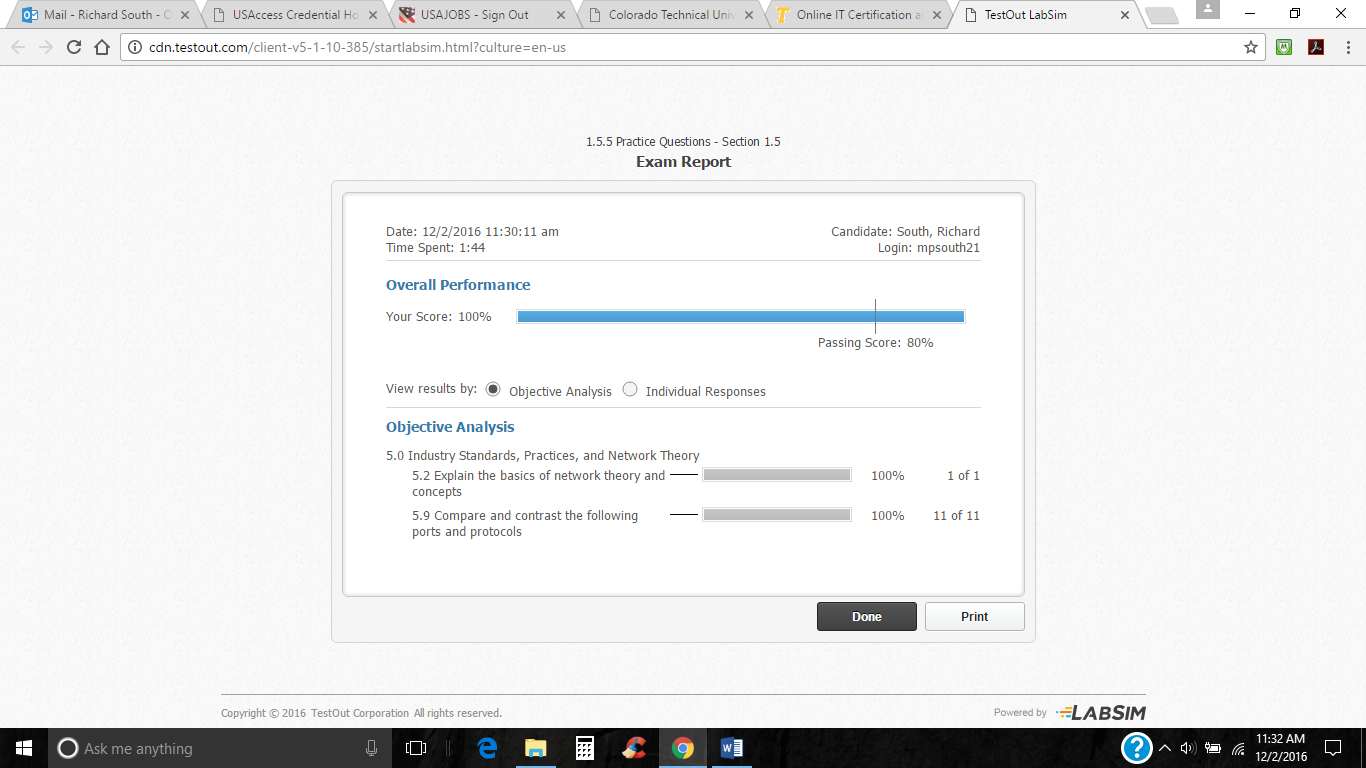
**11.3 Internet Connectivity**



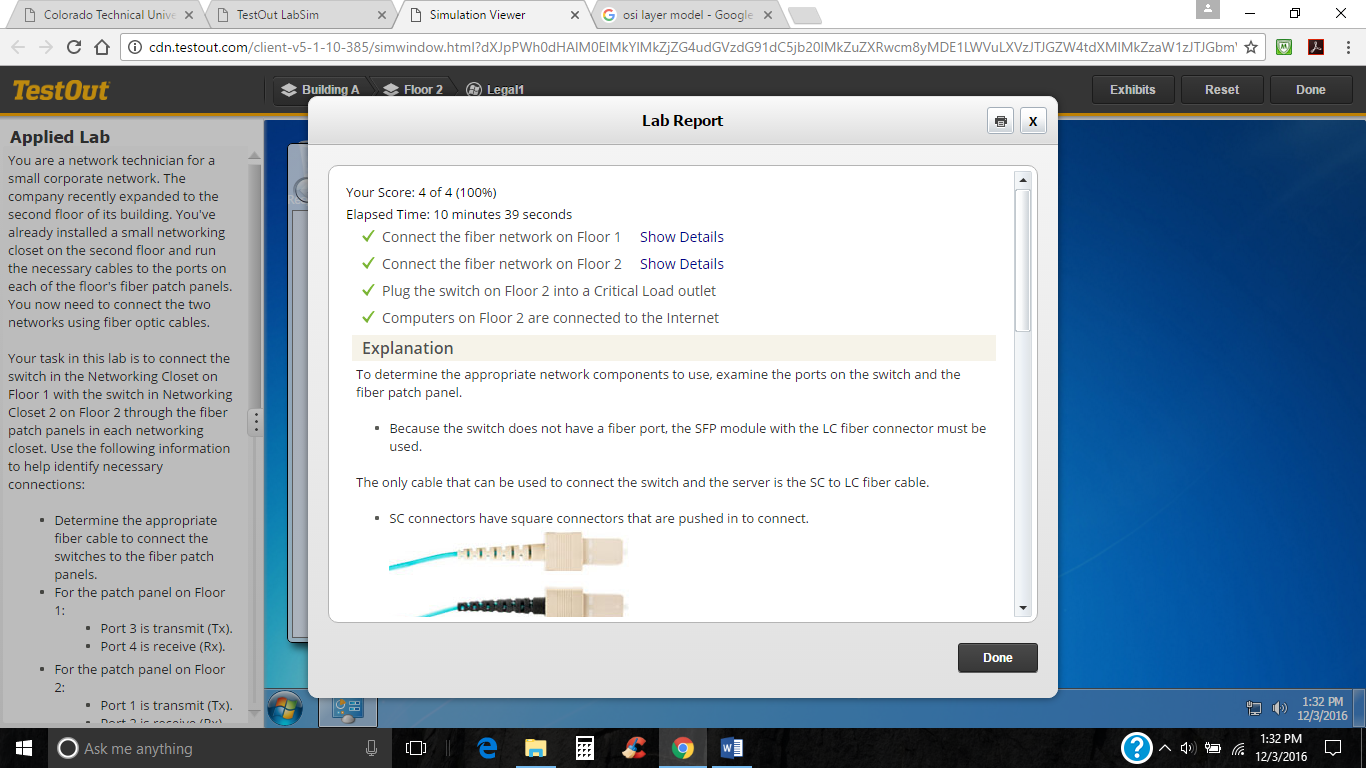
1.3 OSI Model



**1.5 Protocols**



**4.3 Network Connections**



References

Cisco. (c. 2016). *Cisco IOS VPN Configuration Guide*. Retrieved from http://www.cisco.com/c/en/us/td/docs/security/vpn\_modules/6342/vpn\_cg/6342site3.html

Rouse, M. (2016, May). Information Security information, news and tips - SearchSecurity. What is Certificate Revocation List (CRL)? - Definition from WhatIs.com. Retrieved from <http://searchsecurity.techtarget.com/definition/Certificate-Revocation-List>

Microsoft. (c.2016). *Certificate Services*. Retrieved from https://msdn.microsoft.com/en-us/library/windows/desktop/aa376539(v=vs.85).aspx

Microsoft. (c. 2016). *Chapter 2 – Threats and Countermeasures*. Retrieved from https://msdn.microsoft.com/en-us/library/ff648641.aspx

Microsoft (c. 2016). Learn to Develop with Microsoft Developer Network | MSDN. Certificate Services (Windows). Retrieved from http://msdn.microsoft.com/en us/library/windows/desktop/aa376539(v=vs.85).aspx

VA (c. 2016). U.S. Department of Veterans Affairs. About VHA - Veterans Health Administration. Retrieved November 20, 2016, from <http://www.va.gov/health/aboutvha.asp>