Naa Aku Allotey-McGruder

CMIT 350 6389

Professor Sanusi

UMGC

March 1st 2020

The report details the network infrastructure design, security recommendations and technical details for all three Bacon Institute campuses in Toronto, Orlando and Phoenix.

Table of Contents

Site Challenges and Implementation (Orlando – Phoenix – Toronto)

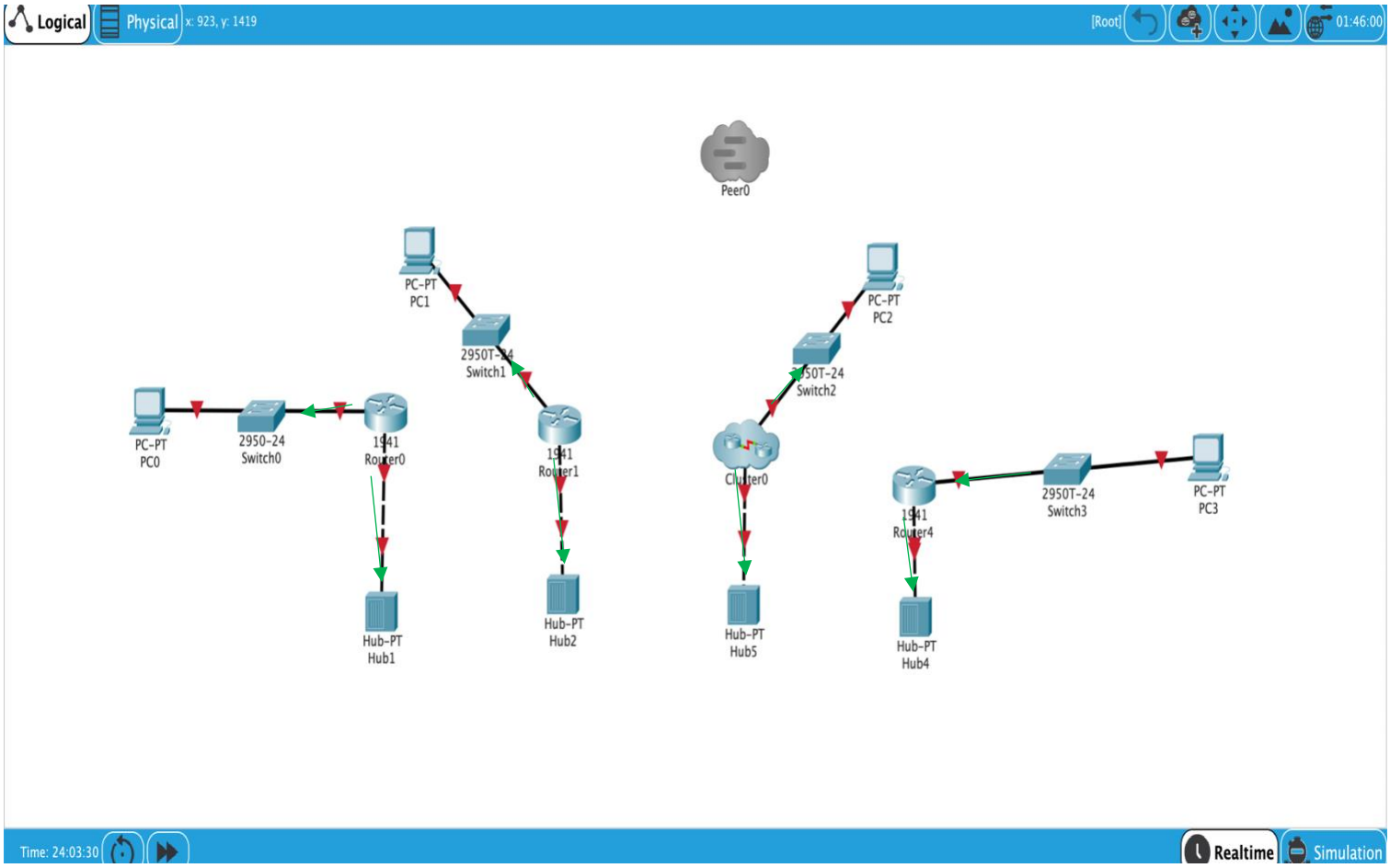
Bacon Institute offers cutting edge education solutions to students across North America. The institution offers bacon branded which focuses primarily on the student and is available to the regular public. Co-branded is the same as bacon branded, with the exception of being sold by a third party and branded as "…powered by Bacon". Lastly, the institution offers white label, which again are the same services but branded with third parties only. All security threats which can lead to corporate espionage or theft must be taken into account and planned for. There will need to be prevention methods, active threat detection methods and a recovery plan for any lost data or compromise in security. (Resource, 2020)

A network infrastructure design which can meet the stated requirements for the Orlando, Phoenix, and Toronto sites is essential for the success of the three locations. Each facility must by 83.3 yards by 133.3 yards, and need to have three floors, which are all connected to the location in each city. The first floor of every building requires 150 network connections, with the data center on the third floor and an additional 75 connections. Orlando being the central location will house the primary data center and fall over will go to phoenix. Invasion protected will be outlined. All servers will have redundancy and multi-layered security methodology will be implemented.

All servers must have redundancy which means the servers will have 2 NIC cards presenting an extra challenge. Because the phoenix site is the failover data center, that cite will need another connection. All hosts must also be connected to a switch before connecting to a router so that all routers are connected site to site, this presents an additional layer of challenges that must be overcome for full implementation.

Site Solutions and Technologies (Orlando – Phoenix - Toronto)

In order to adhere to the network requirements for all three cities, we must configure various VLAN connections to access switches, and configure the ports to the VLANS accordingly. There will be a trunk port between the access switches and the Distros, that will allow the configure VLANS. The IP scheme below will show the WAN interface connections. All PC's will be connected to a switch than a router. (Student, 2020)



Sample Configuration (Orlando – Phoenix - Toronto)

Table 1: Current Router Networking and Information (Sims, 2020)

	Site number	
Orlando Site Router	1	**Management VLAN** IP - 192.168.1.0 **Production VLAN** IP - 192.168.11.0 **Internet VLAN** IP- 192.168.1.0/32 **IP Assignments** Loopback - 10.1.1.1/32 **VPN Tunnels** TBD - based on requirements
Phoenix Site Router 1	2	**Management VLAN** IP - 192.168.2.0

	Site number	
		Production VLAN IP - 192.168.22.0 **Internet VLAN** IP- 192.168.2.0/32 **IP Assignments** Loopback - 10.2.2.2/32 **VPN Tunnels** TBD - based on requirements
Phoenix Site Router 2	3	**Management VLAN** IP - 192.168.3.0 **Production VLAN** IP - 192.168.33.0 **Internet VLAN** IP- 192.168.3.0/32 **IP Assignments** Loopback - 10.3.3.3/32 **VPN Tunnels**

	Site number	
		TBD - based on requirements
Toronto Site Router	4	**Management VLAN** IP - 192.168.4.0 **Production VLAN** IP - 192.168.44.0 **Internet VLAN** IP- 192.168.4.0/32 **IP Assignments** Loopback - 10.4.4.4/32 **VPN Tunnels** TBD - based on requirements

Table 2: Orlando Site

Net ID	**Usable Range**	**Subnet Mask**	**CIDR Value**	**Broadcast**
192.168.1.0	192.168.1.1 – 192.168.1.254	255.255.255.0	/24	192.168.1.255

Table 3: Phoenix Site

Net ID	Usable Range	Subnet Mask	CIDR Value	Broadcast
192.168.2.0	192.168.2.1-192.168.2.254	255.255.255.0	/24	192.168.1.255
10.1.1.1	10.1.1.1	255.255.255.2555	/32	10.1.1.1

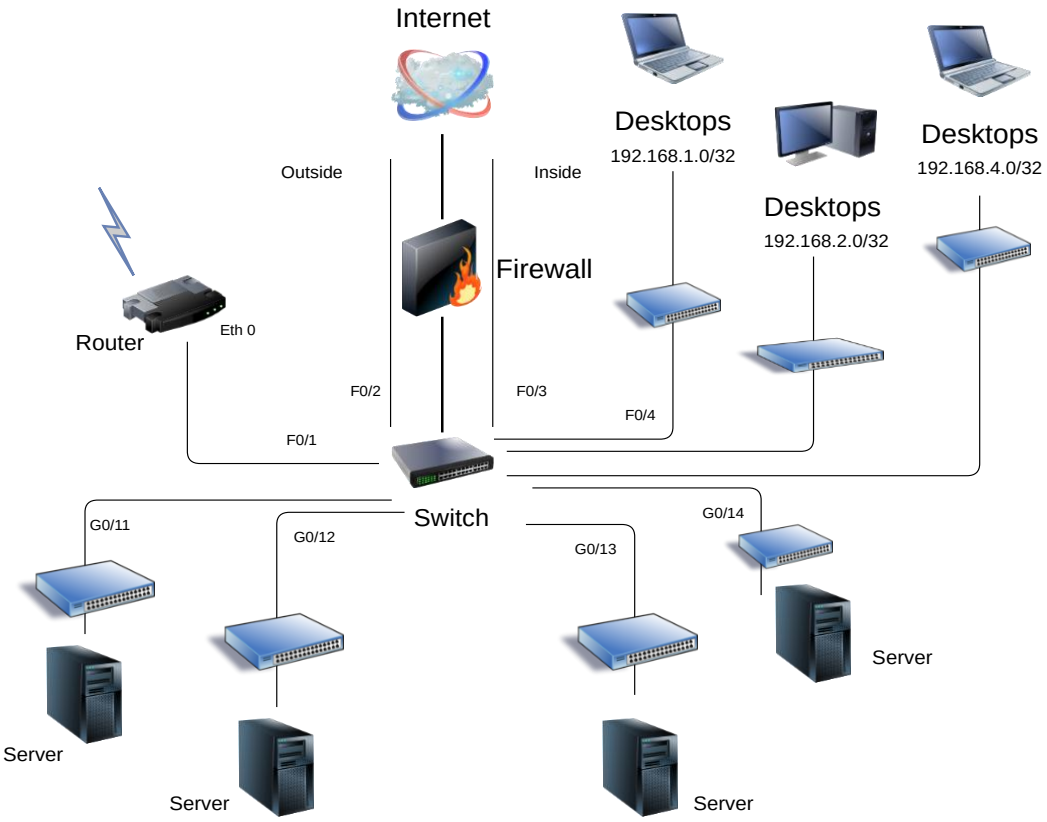
Phoenix Site 2

Net ID	Usable Range	Subnet Mask	CIDR Value	Broadcast
192.168.3.0	192.168.3.1 – 192.168.3.254	255.255.255.0	/24	192.168.1.255
176.26.5.0	176.26.5.1 – 176.26.5.2	255.255.255.252	/30	176.26.5.3
176.26.5.4	176.26.5.5 – 176.26.5.6	255.255.255.252	/30	176.26.5.7

Table 4: Toronto Site

Net ID	Usable Range	Subnet Mask	CIDR Value	Broadcast
192.168.4.0	192.168.4.1 – 192.168.4.254	255.255.255.0	/24	192.168.1.255

Network Infrastructure Design



Bibliography

Resource, U. L. (2020). Retrieved from Week 3 Routing : https://learn.umuc.edu/d2l/le/content/451079/Home

Sims, T. O. (2020). *8: IP Services* . Retrieved from https://cdn.testout.com/client-v5-1-10-612/startlabsim.html

Student, N. A.-M. (2020). *Packet Tracer Project 2* .