Technical Projects

CTN / CTY Program - Fanshawe College

INFO5110: Technical Projects

Summer 2017

Table of Contents

Overview and Objectives 3
Company Overview 4
Organizational Structure 6
Topologies 7
Phase 1: Planning & Basic Configuration 12
Task 1 - Initial Planning 12
Network Requirements 12
System Requirements 14
Presentation 15
Submission Requirements 15
Task 2 – Basic Configuration 16
Network Requirements 16
System Requirements 17
Presentation 17
Submission Requirements 18
Phase 2: Advanced & Security Configuration 19
Task 3 – Advanced Configuration 19
Network Requirements 19
System Requirements 20
Presentation 21
Submission Requirements 21
Task 4 – Security Configuration 22
Network Requirements 22
System Requirements 23
Presentation 24
Submission Requirements 24
Phase 3: Technical Demonstration 25

Overview and Objectives

This case study will allow you to build and configure a complex network and systems infrastructure using knowledge gained from your previous course work. This case study is not a trivial task, it will require time, patience, good communication and teamwork, and is a significant accomplishment when completed as outlined. The end goal is to document and build out the IT solution for a medical practice.

The case study is presented in phases each with a unique set of tasks to serve as checkpoints. The following scenario describes the organization's structure and technical needs in general terms. Following the scenario, the project is broken into a number of tasks, each of which has a detailed list of requirements to act as milestones and ensure tasks are met in reasonable time. It is crucial that you read and understand each requirement, mistakes in one phase or task can create larger issues later on. Additionally, ensure you remain focused on the work assigned in the tasks you are working on, and do not deviate to work on other non-required, but perhaps related tasks.

This case study also includes a presentation component which is intended to improve upon your technical communication skills. As an IT professional you will work with people and audiences whose technical level varies and only require varying levels of information. For example, an IT manager is not concerned with the exact commands you used to configure a router, or which GUI was used to modify Active Directory (AD) information. However, an IT manager is concerned that the solution was implemented properly and on time (and within budget, but that is for another semester), in other words everything is working as intended. When you report back to the manager, whether formally or informally, you would keep the conversation at a high level perhaps describing a few key points, any issues that came up and how they were resolved, and especially report that you tested and how you tested the solution. Throughout this case study there are various types of communication, written and oral, requiring varying degrees of technical information. For example, router configurations will be very low-level technical while the presentations will be at the other end of the spectrum and highlight the key points of a phase or tasks, but still technical in nature.

This case study requires that you accomplish the following:

- Set up the physical layout of the network using the diagram and accompanying narrative
- Implement an IPv4 and IPv6 addressing solution
- Configure a LAN using dynamic and static routing where applicable
- Configure VLANs and Inter-VLAN Routing
- Configure NAT to support Internet connectivity
- Implement security on intermediary devices
- Configure Etherchannel and STP
- Set up an Active Directory environment
- Plan and configure Organizational Units, Group Policies and Groups
- Enable DHCP and DNS services
- Configure a Linux workstation
- Implement a patch management structure
- Plan and implement various services such as file, web and update services (etc.).
- Plan and implement a Microsoft SQL server solution

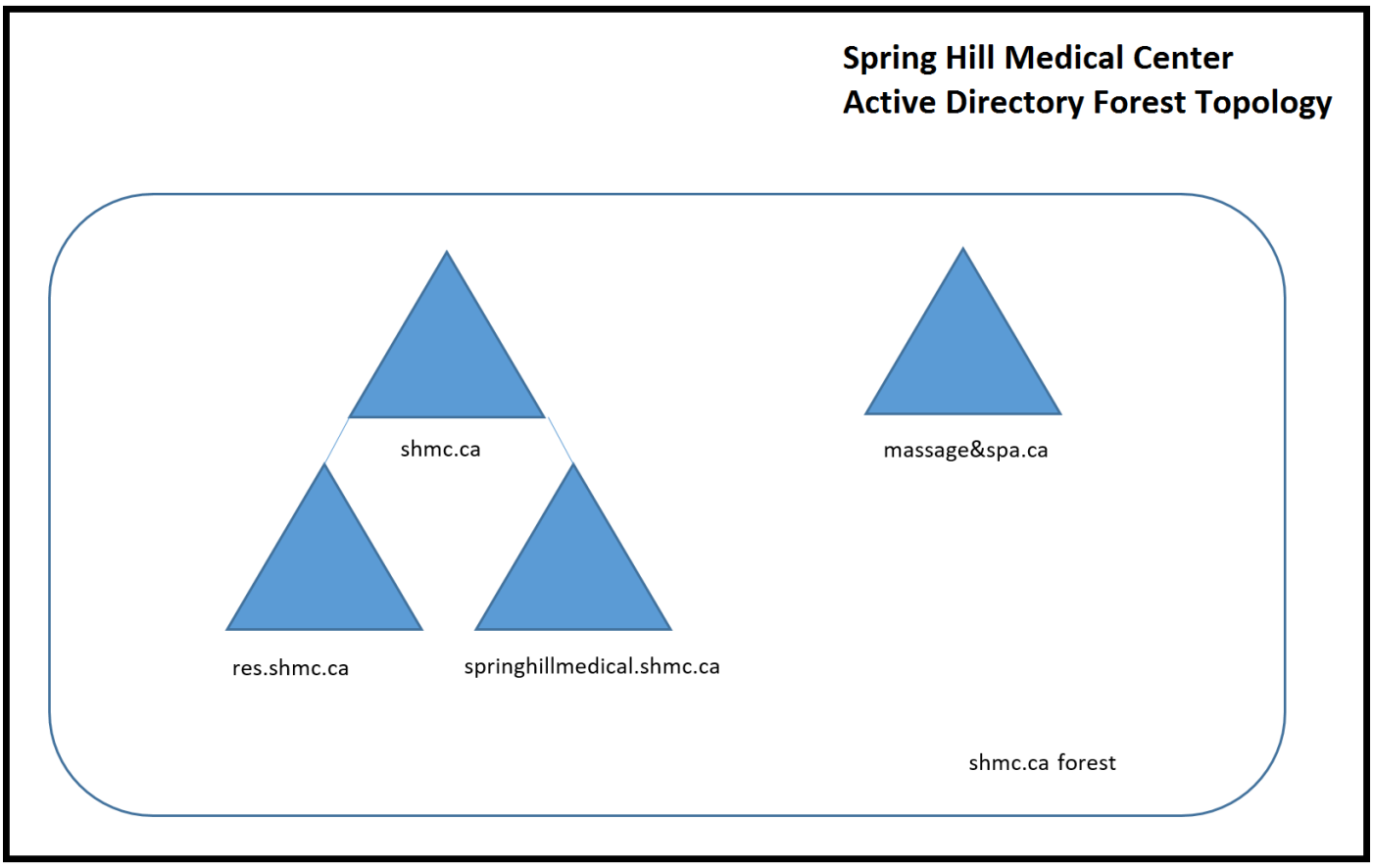
Company Overview

Company Description:
MedicOne is a startup company that builds and provides infrastructure and services to the medical industry. These are often one to three floor buildings providing various types of medical services including family doctors, medical labs, x-ray imaging, pharmacy services and other medical specialties.

Company Structure:
MedicOne is two entrepreneurs who have invested in this newer medical delivery model which contrasts the stand-alone doctor's office of the past. The company owners rely on industry experts in various fields, from construction technology to information technology, to build out the final solution.

IT Environment:
The IT environment must be capable of meeting all business requirements. This includes web and storage/access solutions for patient records. Since this network will carry sensitive medical information, securing data at rest and while in transit is critical, as well as securing end and intermediary devices as they represent an entry point to accessing data. Some of these security measures will be addressed in this case study, while others are beyond the scope of this project. The ideal solution should implement redundancy where appropriate, and effectively utilize network and systems resources to maximize performance and provide fault tolerance.

Information Technology Overview:
The property owners, MedicOne, will provide all IT services through contractors. You are a member of an IT contracting company that will build and configure IT solutions in support of the business enterprises located in the Springhill Medical Center. It has been decided that the overall Active Directory forest below will meet the requirements of the businesses in the medical center. The shmc.ca domain name has been secured and will be used for the AD forest and root domain. A second root domain is needed for the Massage & Spa Co, since its owner wishes to maintain a clear division from the other organizations for legal reasons. Furthermore, Springhill Medical (physicians) requires a stronger password policy and therefore, must have its own domain. Other businesses will exist as organizational units in the res.shmc.ca resource domain. The IT infrastructure is centralized and shared by all businesses in the building. Servers are located on-site and maintained under the control of MedicOne.

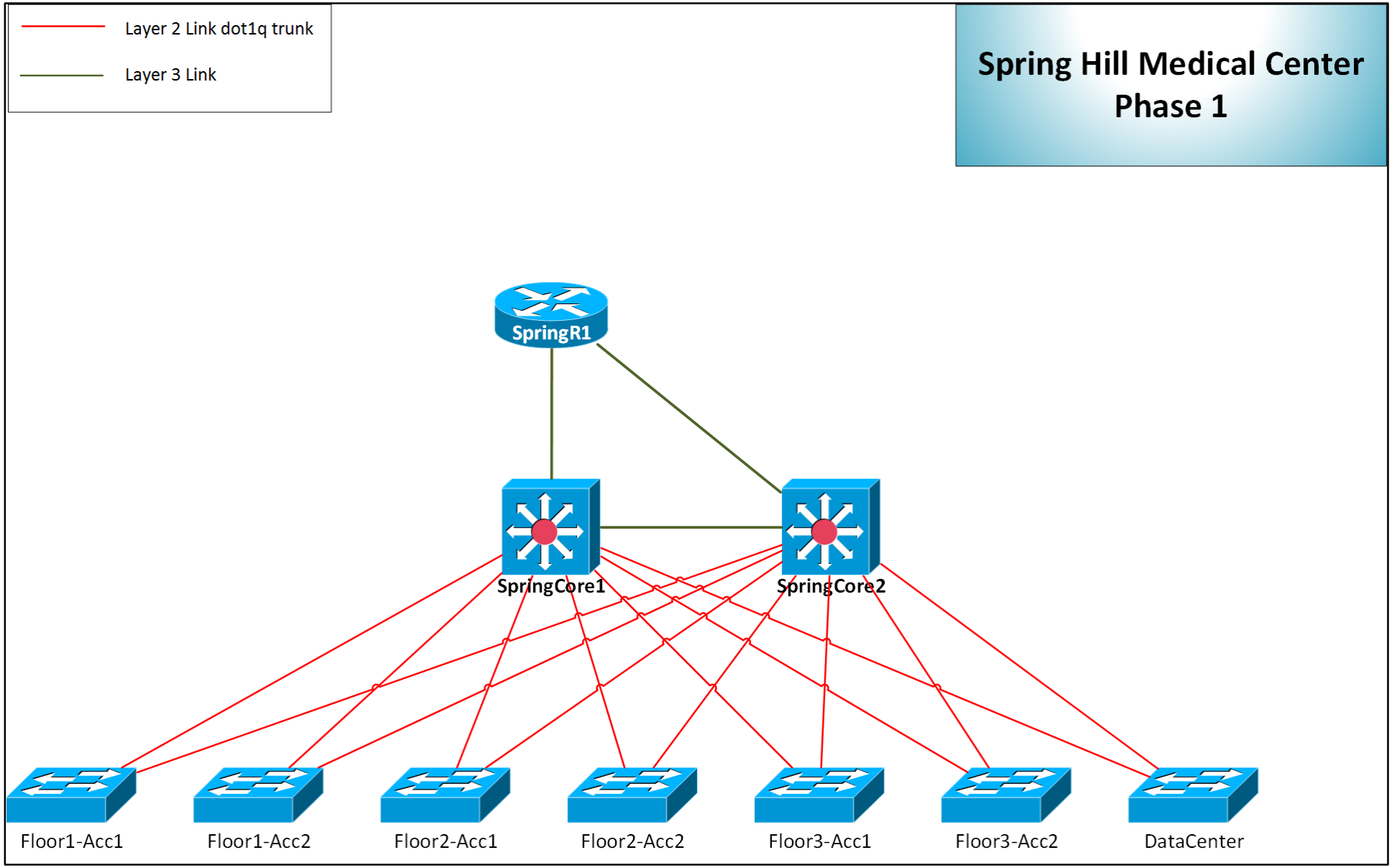

Spring Hill Medical Center
Active Directory Forest Topology
shmc.ca
massage&spa.ca
res.shmc.ca
springhillmedical.shmc.ca
shmc.ca forest

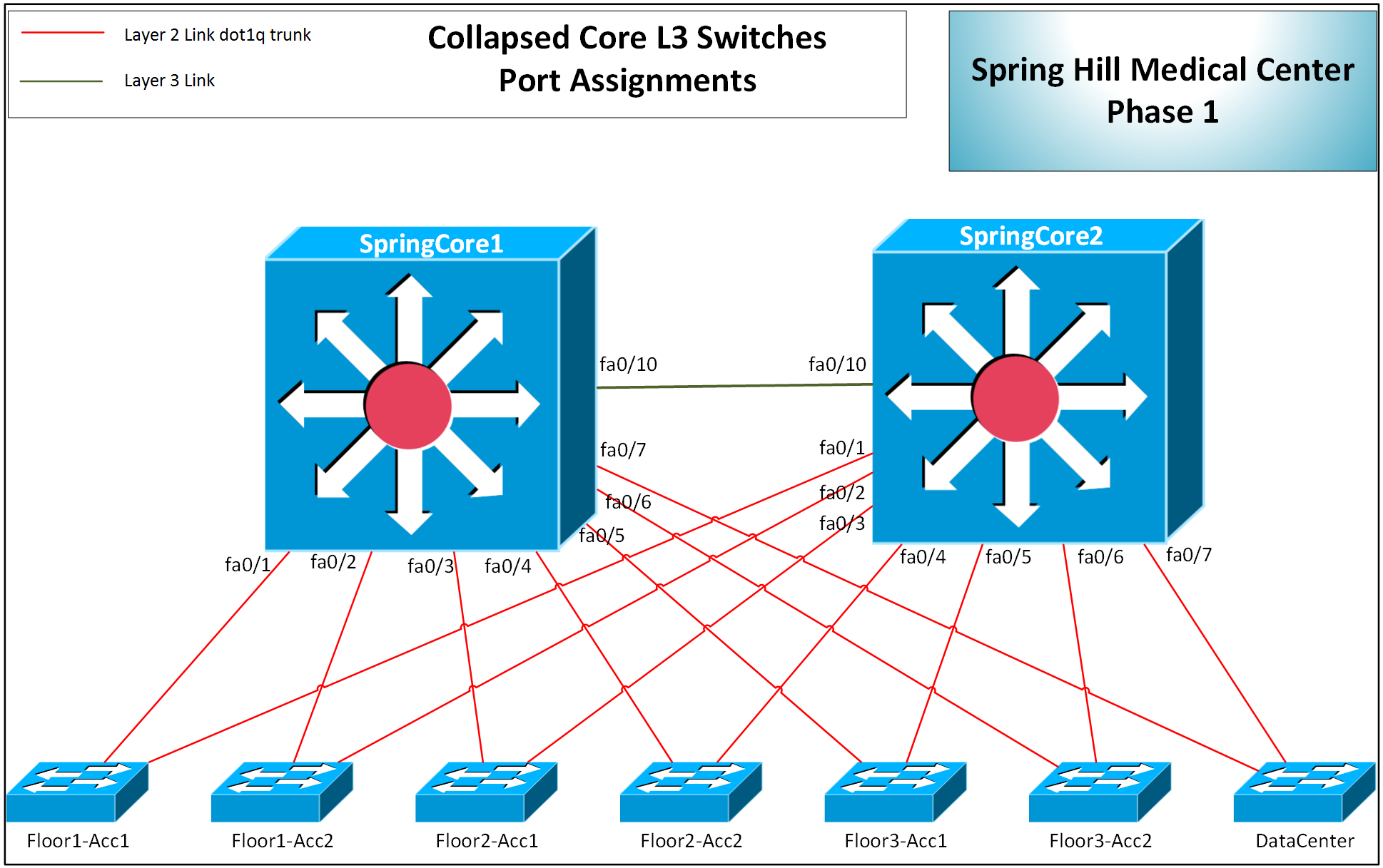
Organizational Structure

The organizational structure is unique in that it serves several different organizations. MedicOne is the building owner and provides building wide services including reception, security, facility maintenance and IT services. Below is a list of the ten businesses located in the medical center.

Springhill Medical Center	**Company Name**	**Staff**	Managers	Doctors	Dentists	Pharmacists	Lab Technicians	Company Receptionist	Assistants	Sales staff	Massage Therapists	Physio Therapists	**Clients /Customers**
X-Ray Laboratories	Coolidge Labs	**22**	1	0	0	0	12	3	4	2	0	0	**78**
Pediatric Office	Childrens Health Center	**10**	0	4	0	0	0	2	4	0	0	0	**300**
Pharmacy	PharmaPlus	**21**	2	0	0	2	4	0	2	11	0	0	**public**
Physicians	Springhill Medical	**18**	0	7	0	0	0	4	7	0	0	0	**650**
Dental Office	The Dental Office	**15**	0	0	4	0	1	2	8	0	0	0	**500**
Massage and Spa	Massage & Spa Co	**26**	3	0	0	0	0	4	5	2	12	0	**public**
Physio-therapy	Springhill Physio Inc	**22**	0	0	0	0	0	2	10	0	2	8	**250**
Blood work	DynaLabs	**15**	2	0	0	0	12	1	0	0	0	0	**300**
ENT	Springhill ENT	**4**	0	3	0	0	0	1	0	0	0	0	**150**
Allergist	Achoo Inc.	**4**	0	2	0	0	0	1	1	0	0	0	**100**

Topologies


Layer 2 Link dot1q trunk
Layer 3 Link
Spring Hill Medical Center
Phase 1
SpringR1
SpringCore1
SpringCore2
Floor1-Acc1
Floor1-Acc2
Floor2-Acc1
Floor2-Acc2
Floor3-Acc1
Floor3-Acc2
DataCenter

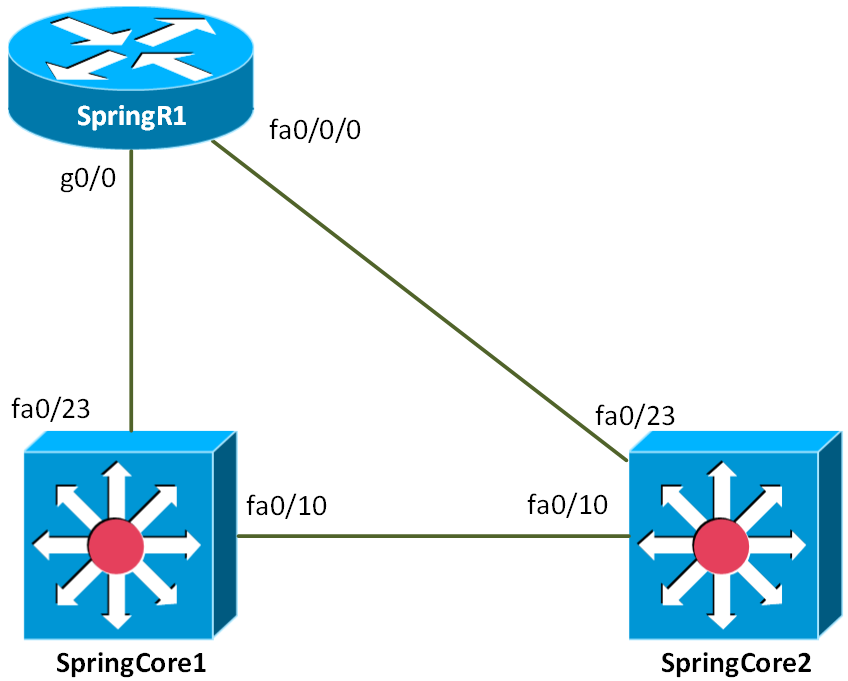

Layer 2 Link dot1q trunk
Layer 3 Link
Collapsed Core L3 Switches
Port Assignments
Spring Hill Medical Center
Phase 1
SpringCore1
SpringCore2
fa0/10
fa0/10
fa0/7
fa0/1
fa0/6
fa0/2
fa0/5
fa0/3
fa0/1
fa0/2
fa0/3
fa0/4
fa0/4
fa0/5
fa0/6
fa0/7
Floor1-Acc1
Floor1-Acc2
Floor2-Acc1
Floor2-Acc2
Floor3-Acc1
Floor3-Acc2
DataCenter

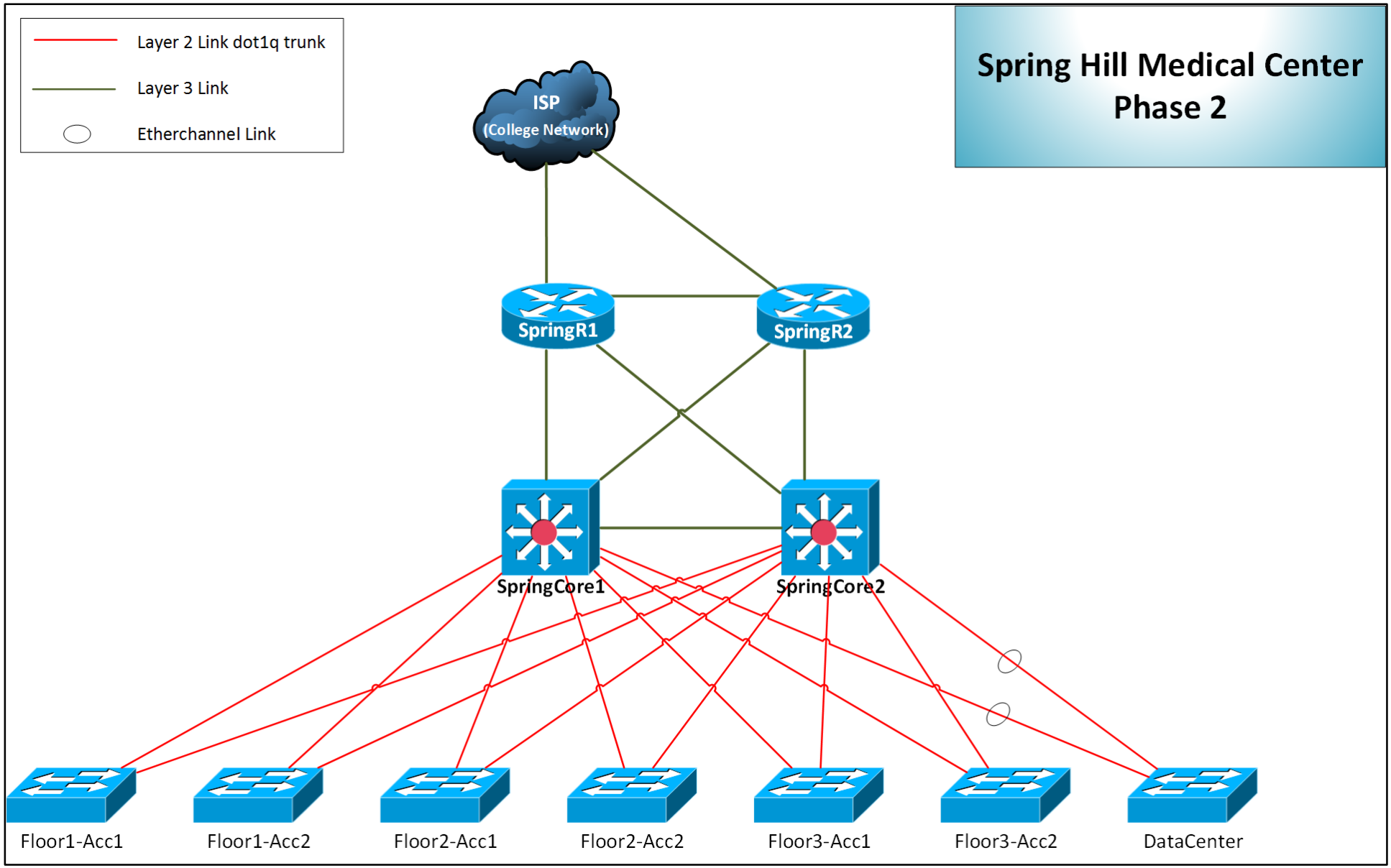
Layer 2 Link dot1q trunk

Layer 3 Link

Edge Routed Network Port Assignments

Spring Hill Medical Center Phase 1



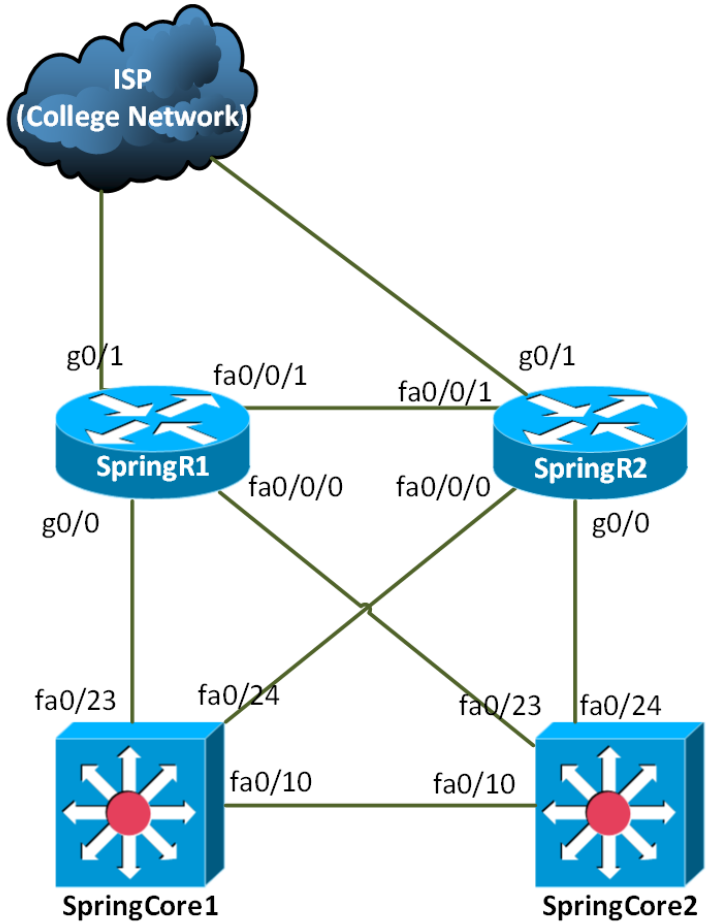

Layer 2 Link dot1q trunk
Layer 3 Link
Etherchannel Link
Spring Hill Medical Center
Phase 2
ISP
(College Network)
SpringR1
SpringR2
SpringCore1
SpringCore2
Floor1-Acc1
Floor1-Acc2
Floor2-Acc1
Floor2-Acc2
Floor3-Acc1
Floor3-Acc2
DataCenter

Layer 2 Link dot1q trunk

Layer 3 Link

Edge Routed Network Port Assignments

Spring Hill Medical Center Phase 2



Phase 1: Planning & Basic Configuration

Task 1 - Initial Planning

Network Requirements

- Based on the company structure and needs create an IP addressing solution. Since it may be the case other MedicOne offices will interconnect with this new building the previous network administrator has assigned 172.30.0.0 /16 to be used throughout Spring Hill Medical Center. This is sufficient addressing space for the current needs and future growth, thus each VLAN can be assigned a /24 subnet. Use the provided template IPv4 Addresing Schema.xlsx to populate your IPv4 addressing solution.
- Create a solution that allows for route summarization where applicable, for example summarize all the networks per floor.
- Use the last /24 network address in your overall summary for appropriately sized point-to-point subnets.
- Reserve static addressing where appropriate.
- All default gateways should be the first addresses in their assigned networks, *not* the last address in the assigned network. This is to remain consistent with other MedicOne infrastructures.
- The DataCenter switch will be on floor 1, so keep this in mind when creating a subnet for it and thinking about route summarization.
- Do not implement the IP solution yet, this is simply your proposed solution.
- For all switches, set the VTP mode to Transparent, and create VLANs based on tables below (**Note**: VTP cmds will need to be added manually to your captures as they will not show in the output of a show running-config).
- **Floor1-Acc1 & Floor1-Acc2**

VLAN ID	VLAN Name	Port Assignment
100	Reception	0/1 – 0/3
110	Security	0/4 – 0/6
120	PharmaPlus	0/7 – 0/9
130	DynaLabs	0/10 – 0/12
140	Facilities	0/13 – 0/15
199	Visitor1	0/16 – 0/18
500	IT	0/19 – 0/20
Trunk	n/a	0/23 – 0/24

- **Floor2-Acc1 & Floo2-Acc2**

VLAN ID	VLAN Name	Hosts per VLAN
200	CoolidgeLab	0/1 – 0/3
210	ChildrensHealth	0/4 – 0/6
220	Physicians	0/7 – 0/9
230	MassageSpa	0/10 – 0/12
299	Visitor2	0/13 – 0/16
500	IT	0/17 – 0/19
Trunk	n/a	0/23 – 0/24

- **Floor3-Acc1 & Floor3-Acc2**

VLAN ID	VLAN Name	Hosts per VLAN
300	DentalOffice	0/1 – 0/3
310	ENT	0/4 – 0/6
320	Allergist	0/7 – 0/9
330	Physiotherapy	0/10 – 0/12
399	Visitor3	0/13 – 0/15
500	IT	0/16 – 0/18
Trunk	n/a	0/23 – 0/24

- **DataCenter**

VLAN ID	VLAN Name	Hosts per VLAN
1000	DataCenter	0/1 – 0/18
Trunk	n/a	0/19 – 0/24

- Document a proposal to address the following design and planning issues. This will likely be one page, but no more than two pages indicating techniques, technologies, or combinations of the two used to address the following:
    - Securing remote sessions with intermediary devices.
    - Ensuring end devices using DHCP consistently receive an address and in a timely manner.
    - Preventing unauthorized switches from automatically forming trunk links.
    - Preventing access ports from forming trunk links.
    - Prevent clients from receiving addressing from unauthorized DHCP servers.

- Securing trunk links and ports.

- Use the Test Plan template provided to run a few tests to ensure functionality. This helps to isolate problems at this stage so they do not grow or become problems with the functionality you are trying to implement in the next stage.
  - Unit testing examples
    - Use the output from the appropriate show commands (could be more than one obviously) as evidence that the VLANs are configured properly on the appropriate devices. It is unnecessary to create a test plan for each, but write a test plan for 2-3 switches to demonstrate you understand how to test this.
  - Integration testing examples
    - Since we are manually creating VLANs and have yet to implement any layer 3 addressing we have not interconnected units (routers, switches, laptops, servers, etc.) yet, meaning we have not integrated devices so we cannot test anything of significance yet at this scope. Sure the routers and switches may be exchanging CDP, but we are not overly concerned with how or if CDP is operating right now.
  - System wide examples
    - If we have not but units together then to be sure we have not created a system yet, so at this point there is no testing to be done at this level either.

System Requirements

- Using Microsoft Best Practices build the Active Directory Structure for shmc.ca and document the following:
  - Server naming convention used
  - IPv4 address assignments
  - Placement of DNS
- Build all required domain controllers (GUI)
- Configure your domain controllers
- Configure FSMO Role and GC placement
- Ensure all DNS zones in use are configured and fault tolerant
- Create an OU Structure to support the businesses, scope of management and delegation of permissions
- Minimum post-installation verification testing:
  - Verify DNS by running lookups on domain names from the other domains
  - Create a computer object and make sure it replicates to other DC
  - Create a user object and make sure it replicates to the other DC
  - If tests fail, correct as needed
- Verify and document your Active Directory structure, include GC and FSMO Role placements
- Collect post configuration screen captures demonstrating your solution has been configured successfully. Include results from your verification testing. For each screen capture, provide a brief

explanation of what you have captured and how it supports the design. (Limit of 5 Screen Captures per Service)

Presentation

- Your target audience is an IT manager overseeing this project. The end goal of the mini-presentation is that you demonstrated a solid understanding of this phase and have demonstrated completion of the tasks, note these are two distinct things: you understand the requirements *and* you met the requirements. Prepare a presentation which will present a *high level* overview of what you completed in this phase. Omit specific details such as command output, rather include technical content and supporting rational. For example, state why preventing access ports from automatically forming trunk links is important, the technique or technology used to accomplish this, and why you chose this approach (rational). Do not put the exact commands to do this on a slide and present it. From this example you should also note that anything you submit, not just configuration files, may be part of your presentation. This means any documents and/or proposals.
- Your audience is technical, so you do not need to explain technical terms. However, you need to win over your audience by demonstrating you have a firm functional solution, an understanding of that solution, and are ready to proceed to the next phase.
- Come prepared and well-rehearsed. Ensure all group members present an equal portion of the presentation. Ensure you can fit all key points into your allotted time. Non key points should be removed from your presentation. As part of this evaluation, you need to demonstrate that you can pick out what is relevant for you to present and what can be left out.

Submission Requirements

- Use the Project Management.xlsx template (FOL) to complete weekly updates of tasks completed and/or started. Each Sunday submit one completed form to the dropbox. Although one group member will submit the form it is your responsibility to ensure this document is up to date and correct.
- Capture the running-config and vlan brief output for each device configured to an individual text file. Edit the files so they can be reused for subsequent phases, do not submit the raw output from a show run command. Don't forget to add no shutdown to appropriate interfaces. Include a commented header at the top of each config file detailing the following:
    - Your names and Group Number.
    - The Date
    - INFO5110 Technical Projects – Phase 1 Task 1
    - The router/switch name that corresponds to each file.
- Using the IPv4 Addressing Schema.xlsx template provided on FOL, submit your IPv4 addressing solution to the FOL Drop Box. You may alter (improve upon) this template to suit your needs.
- Save your Network Document as a PDF named "NetworkProposal.pdf" and submit to the FOL Drop Box.
- Save your Systems Document as a PDF named "SystemsPlan.pdf" and submit to the FOL Drop Box.
- Using the template provided on FOL, submit your Peer Evaluation to the FOL Drop Box.

Task 2 – Basic Configuration

Network Requirements

- Implement the following base configuration on routers and switches, only configure what is required in this phase. Use hostnames from the provided topologies, if not already completed in task 1.

- Configure RSTP with load balancing as follows:
    - VLANs on Floor 1 will use SpringCore1 as its primary root bridge and SpringCore2 as its secondary root bridge.

    - VLANs on Floor 2 and Floor 3 will use SpringCore2 as its primary root bridge and SpringCore1 as its secondary root bridge.

    - Use the above load balancing configuration as a guide to determine which SpringCore# switch will be configured as a default gateway for a VLAN.

- Configure RSTP to ensure DHCP clients do not encounter a timeout during DHCP exchanges, thus receiving an IP address in a timely manner.

- Configure IP addressing where appropriate
    - Physical interfaces on routers and appropriate layer 3 switch ports based on the topology.
    - SVIs on appropriate core layer switches to act as default gateways for clients.
        - For example, the VLANs on floor 1 are using SpringCore1 as their root bridge, so implement the default gateways for those VLANs on the appropriate layer 3 device.

- Implement EIGRP using AS 100 and create summarizations where appropriate based on the IP addressing solution provided. The summarization may occur by floor.

- Use the Test Plan template provided to run a few tests to ensure functionality. This helps to isolate problems at this stage so they do not grow or become problems with the functionality you are trying to implement in the next stage.
    - Unit testing examples
        - IP addressing is properly assigned/configured by using appropriate show commands on routers/switches. Not required to show every interface in a test plan, but complete 2-3 test plans, so you get the idea and can demonstrate you understand how to actually test something.
    - Integration testing examples
        - On SpringCore2 view the route table and determine if all the routes advertised by SpringCore1 are appearing.
        - On SpringCore2 view the route table and determine if the appropriate route summarization is appearing in the route table as advertised by SpringCore1.
        - PING between networks, use output from tracert commands as evidence.

- System wide examples
  - We are not quite there yet, we are assuming this would be a test between two different sites. However, one could make the case this is a test within the LAN from end to the other, so the "system" in this case is considered the LAN. PING from a device in any VLAN to an edge router, say SpringR1.

System Requirements

- Implement DHCP services on the domain controllers, so that client machines in all the companies are able to obtain an IPv4 address properly
- Configure DHCP in a fail-over or fault-tolerant manner
- Build one Windows client VM to be used for testing DHCP functionality
- Build one member server in the res.shmc.ca domain to provide file, print and web services
- Configure AD groups and set up shared folders for each business in the medical center
- Make sure that only users belonging to a specific business are able to access the folder that belongs to that company
- Create printers for each of the businesses on the member server (print devices are not needed)
- Configure permissions on each printer as appropriate
- Utilize standardized naming conventions for all servers, shares, printers, policies and groups
- Configure group policy objects (GPO) so that springhillmedical.shmc.ca domain requires 12 character complex passwords. All other domains will require eight-character complex passwords.
- Additional password policy settings should be considered and implemented for each domain.
- Minimum post-installation verification testing:
  - Verify DHCP in each domain using the Windows client VM
  - Using test user(s) ensure that permissions on each of the shared folders are correct set
  - Verify that your password policies behave as expected
  - If tests fail, correct as needed
- Collect post configuration screen captures demonstrating your solution has been configured successfully. Include results from your verification testing. For each screen capture, provide a brief explanation of what you have captured and how it supports the design. (Limit of 5 Screen Captures per Service)

Presentation

- Prepare a presentation which will present a high level overview of what you completed in this phase. Include technical content, test plan and supporting rational.
- Your audience is technical, so you do not need to explain technical terms. However, you need to win over your audience by demonstrating you have a firm functional solution, solid understanding of your solution, and are ready to proceed to the final phase.
- Come prepared and well-rehearsed. Ensure all group members present an equal portion of the presentation. Ensure you can fit all key points into your allotted time. Non key points should be

removed from your presentation. As part of this evaluation, you need to demonstrate that you can pick out what is relevant for you to present and what can be left out.

Submission Requirements

- Use the Project Management.xlsx template (FOL) to complete weekly updates of tasks completed and/or started. Each Sunday submit one completed form to the dropbox. Although one group member will submit the form it is your responsibility to ensure this document is up to date and correct.
- Capture the running-config for each device to an individual text file for each device. Edit the files so they can be reused for subsequent phases, do not submit the raw output from a show run command. Don't forget to add no shutdown to appropriate interfaces. Include a commented header at the top of each config file detailing the following:
    - Your names and Group Number.
    - The Date
    - INFO5110 Technical Projects – Phase 1 Task 2
    - The router/switch name that corresponds to each file.
- Compress all .txt files into a single .zip file (not another compression technology) using the name "Network Task2.zip" and submit to the FOL Drop Box.
- Save your Network Test Plan as a PDF named "NetworkTestPlan-Task2.PDF" and submit to the FOL Drop Box.
- Save your Systems PowerPoint using the name "SystemsBuild-Task2.pptx" and submit to the FOL Drop Box.
- Save your Systems Test Plan as a PDF named "SystemsTestPlan-Phase2.PDF" and submit to the FOL Drop Box.
- Using the template provided on FOL, submit your Peer Evaluation to the FOL Drop Box.

The overall end goal of Phase 1 is to have the IPv4 network converge and core Windows services operational.

Phase 2: Advanced & Security Configuration

Task 3 – Advanced Configuration

Network Requirements

NOTE: you will be connecting to the college network in this phase. It is critical that you suppress EIGRP updates from leaving your case study network and entering the college production network.

- Install and configure SpringR2 to participate in the existing IPv4 network. This includes IPv4 addressing and routing. A strong suggestion is to complete this task (which includes ensuring functionality) first before moving forward with other network configuration.
- Create an IPv6 addressing schema. The ISP has provided the 2001:CAFE:BEAD:: /48 network address. All IPv6 subnets will use a /64 prefix length.
- Implement your IPv6 address solution using dual stack.
- Implement EIGRP IPv6 using AS 600.
- Configure Etherchannel to support access and redundancy to the data center. Use two physical cables per channel and the trunk interfaces identified in task 1 on the DataCenter switch.
- Set the ISP facing interfaces (college facing interfaces) on SpringR1 and SpringR2 using static addressing found in "Public IP Addresses (Networking Lab).pdf", clearly we are simulating a public ISP infrastructure. Implement NAT so that any device inside the building will use the IPv4 assigned to the outside interface when accessing the Internet (college network).
- Configure default routes on SpringR1 and SpringR2 using 172.17.190.1 or 172.17.193.1 depending on which college network you are using. Redistribute the default static route on SpringR1 into the EIGRP updates.

- Use the Test Plan template provided to run a few tests to ensure functionality. This helps to isolate problems at this stage so they do not grow or become problems with the functionality you are trying to implement in the next stage.
    - Unit testing examples
        - Use output from appropriate show commands (does the route table look right?).
        - Evidence that IPv6 is properly configured on intermediate and end devices. Again, not every device requires a test plan submission. However, create a few to demonstrate you understand how to gather evidence for this test on both types of devices.
    - Integration testing examples
        - PING between newly implemented and original devices, e.g. SpringR1 to SpringR2.
        - Want to impress: use Wireshark to capture EIGRP updates as evidence SpringR2 is properly implemented in the EIGRP AS, or use output from appropriate debug command. Convince your audience it is working.

        - Appropriate show command to show interface statistics that provide evidence that etherchannel has be implemented properly. Another way to test etherchannel is send a PING, shutdown one of the interfaces participating in etherchannel and send the PING again, this should work … right?
    - System wide examples
        - Again, we could consider this a test from one end of the LAN to the other, so in this case SpringR2 to an end device in any VLAN.
        - However, we now have connectivity to the college network. Send a tracert to a device on the college network, e.g. the college DNS server, from an end device as evidence of system wide functionality. Remember the college network is acting as an ISP for testing purposes.

System Requirements

- OPTIONAL: To reduce the number of VMs used in this course, you may elect to remove secondary domain controllers from the child domains only. You must use proper demotion techniques to achieve this.
- While maintaining your IPv4 configurations, implement IPv6 on all servers and clients by adding the necessary static and dynamic IP settings
- Using the existing member server, finalize your web server to include a sample web page
- Configure DNS so that the web page appears when **http://shmc.ca** is typed into a browser anywhere in the local AD forest
- Build a new member server and install Microsoft SQL Server on it
- Configure data storage solutions for the DynaLabs, The Dental Office and Achoo Inc. companies on the SQL server. Note: while the server is shared, users should only be able to access data that belongs to their respective companies.
- Create sample customer information (e.g name, address, phone number) in simple tables to be used for testing
- From the Windows client station run SQL select statements using the sqlcmd query utility
- Build a Linux workstation to be used as a client in the res.shmc.ca domain. This will be utilized by IT staff to manage network devices using Telnet.
- Minimum post-installation verification testing:
    - Verify IPv6 in each domain using the Windows client VM
    - Ensure that the SHMC web page is accessible from all domains
    - Using Transact-SQL verify the functionality of the storage solution for each business
    - Using the Linux workstation verify that you are able to access network device configurations
    - If tests fail, correct as needed
- Collect post configuration screen captures demonstrating your solution has been configured successfully. Include results from your verification testing. For each screen capture, provide a brief

explanation of what you have captured and how it supports the design. (Limit of 5 Screen Captures per Service)

Presentation

- Prepare a presentation which will present a high level overview of what you completed in this phase. Include technical content, test plan and supporting rational.
- Your audience is technical, so you do not need to explain technical terms. However, you need to win over your audience by demonstrating you have a firm functional solution and are ready to proceed to the next phase.
- Come prepared and well-rehearsed. Ensure all group members present an equal portion of the presentation. Ensure you can fit all key points into your allotted time. Non key points should be removed from your presentation. As part of this evaluation, you need to demonstrate that you can pick out what is relevant for you to present and what can be left out.

Submission Requirements

- Use the Project Management.xlsx template (FOL) to complete weekly updates of tasks completed and/or started. Each Sunday submit one completed form to the dropbox. Although one group member will submit the form it is your responsibility to ensure this document is up to date and correct.
- Capture the running-config for each device to an individual text file for each device. Follow the formatting style outlined in phase 1.
- Compress all .txt files into a single .zip file using the name “Network Task3.zip” and submit to the FOL Drop Box.
- Save your Network Test Plan as a PDF named “NetworkTestPlan-Task3.PDF” and submit to the FOL Drop Box.
- Save your Systems PowerPoint using the name “SystemsBuild-Task3.pptx” and submit to the FOL Drop Box.
- Save your Systems Test Plan as a PDF named “SystemsTestPlan-Task3.PDF” and submit to the FOL Drop Box.
- Using the template provided on FOL, submit your Peer Evaluation to the FOL Drop Box.

Task 4 – Security Configuration

Network Requirements

Security is typically, not always, left until the end for a few reasons. First, when we implement some security mechanism we must be certain it was the security measure that has created the actual restriction. For example, if you create an ACL to prevent users on the Visitor VLAN from accessing the data center we want to ensure it is actually the ACL preventing this access, and not a misconfigured route from a previous task preventing the access.

Another reason for leaving security until later is to ensure all of the basic network/system components are operational which mitigates troubleshooting activities. In this scenario we know everything should be working before we implement security, this way if something goes wrong after we implement security then it must be (or is very likely) the case that security has been misconfigured. For example, if we configure EIGRP and implement secure routing updates immediately afterwards, and then route tables are not populating, then it is unclear whether we misconfigured the routing protocol or the security measure. It is more systematic to configure routing and ensure it is working, and then secure the routing protocol.

This is a general approach that can be applied to other areas, e.g. ensure clients can get DHCP and then prevent the use of unauthorized DHCP servers. A final point, after you implement the security measure ensure the service/feature you are protecting is still available if applicable. In the last scenario a client should still be able to get an IP address via an authorized DHCP server even though you implemented some security measure against rogue (unauthorized) DHCP servers.

- Configure SSH (if not already done)
- Configure port security so only two laptops can use the IT VLAN ports
- Secure unused ports and disable unused services.
- Preventing unauthorized switches from automatically forming trunk links.
- Preventing access ports from forming trunk links.
- Prevent clients from receiving addressing from unauthorized DHCP servers.
- Secure trunk links to only allow necessary VLAN traffic.
- Create an ACL to prevent the visitor networks from accessing the data center. Since we are using L3 switches in the core the ACL will need to be applied to the appropriate SVI.
- Create an ACL to only allow DNS/HTTP/HTTPS from the visitor networks to the ISP (college network).
- Prevent the use of unauthorized DHCP servers

- Use the Test Plan template provided to run a few tests to ensure functionality. This helps to isolate problems at this stage so they do not grow or become problems with the functionality you are trying to implement in the next stage.
    - Unit testing examples
        - Ensure devices can remotely access routers/switches using SSH. Use a screen capture of an SSH login sequence as one example of a way to provide evidence.

        - Use show commands as evidence that a port moves to an err-disabled state in the IT VLAN if a security violation occurs. Use show interface *interface-name* to see the err-disabled state and show run will display the learned MAC addresses if you used stick

    - Integration testing examples
        - Provide evidence that visitor network cannot access the data center. Do not use the configuration as proof because it is not, this only demonstrates you wrote in those commands and nothing more. One way to prove this functionality is start a Wireshark capture and send a PING to the DataCenter from the Visitor network with ACL not implemented, this demonstrates you have connectivity. Next implement the ACL by binding it to an SVI, then run the PING again ensuring the capture is still running.
    - System wide examples
        - Provide evidence that the Visitor network can use HTTPS on the Internet. Use Wireshark to capture an HTTPS request from an inside VLAN, e.g. retrieve the FOL login page before implementing the ACL. Next, bind the ACL to the appropriate interface and try to get the FOL homepage again (don't forget to clear the cache or close/re-open your browser since a request for the FOL homepage may actually not leave your laptop).

System Requirements

- Plan and install WSUS server(s) and configure patch management for all four domains in the forest
- Finalize your configuration of your WSUS and avoid automatic restarts during business hours
- Create a helpdesk group in the massage&spa.ca domain and configure AD delegation of rights, so that the group is able to add, remove and modify user accounts in this domain
- Describe why this group cannot manage objects in the other domains and what would be needed to enable this
- Using the least amount of administration, configure a Windows firewall policy to block incoming and outgoing µTorrent sessions throughout the AD forest
- Harden all servers so no generic user accounts will be used, proper service accounts are being used and feature/roles not being used have been fully removed from the server.
- Document Group Policies you will create, consider both security, management and user setting configurations. For each policy, include how you will manage scope of management. Provide a brief explanation of each policy.
- Secure the Linux access to network devices by enforcing SSH
- Minimum post-installation verification testing:
    - Using the Windows client test to make sure you are able to obtain Windows updates as expected
    - Ensure the Helpdesk group is able to add a user account in massage&spa.ca
    - Verify that µTorrent cannot be run from any of the domains
    - Verify that you are able to access network device configurations using SSH

- If tests fail, correct as needed
- Collect post configuration screen captures demonstrating your solution has been configured successfully. Include results from your verification testing. For each screen capture, provide a brief explanation of what you have captured and how it supports the design. (Limit of 5 Screen Captures per Service)

Presentation

- Prepare a presentation which will present a high level overview of what you completed in this phase. Include technical content, test plan and supporting rational.
- Your audience is technical, so you do not need to explain technical terms. However, you need to win over your audience by demonstrating you have a firm functional solution and are ready to proceed to the next phase.
- Come prepared and well-rehearsed. Ensure all group members present an equal portion of the presentation. Ensure you can fit all key points into your allotted time. Non key points should be removed from your presentation. As part of this evaluation, you need to demonstrate that you can pick out what is relevant for you to present and what can be left out.

Submission Requirements

- Use the Project Management.xlsx template (FOL) to complete weekly updates of tasks completed and/or started. Each Sunday submit one completed form to the dropbox. Although one group member will submit the form it is your responsibility to ensure this document is up to date and correct.
- Capture the running-config for each device to an individual text file for each device. Follow the formatting style outlined in Phase 1.
- Compress all .txt files into a single .zip file using the name “Network Task4.zip” and submit to the FOL Drop Box.
- Save your Network Test Plan as a PDF named “NetworkTestPlan-Task4.PDF” and submit to the FOL Drop Box.
- Save your Systems PowerPoint using the name “SystemsBuild-Task4.pptx” and submit to the FOL Drop Box.
- Save your Systems Test Plan as a PDF named “SystemsTestPlan-Task4.PDF” and submit to the FOL Drop Box.
- Using the template provided on FOL, submit your Peer Evaluation to the FOL Drop Box.

The overall end goal of this phase is to have everything ready for deployment which is the single goal for phase 3, this means the network is converged, services are operational, and your systems can participate in network communications. Ensure you are testing with virtual machines on their appropriate subnets, *not* with virtual machines all on one laptop.

Phase 3: Technical Demonstration

- This phase requires you to demonstrate the network and systems operation. This phase does not include any new requirements so all configuration should be done before this phase is delivered. It is not ideal to be applying new configurations to the equipment in the lab during this demonstration.

- You will be required to cable the topology, get the network to a converged state, and bring systems online.

- Testing will consists of items identified in your test plan and/or feedback from your test plan.

- Virtual machines must be connected using the physical network infrastructure built for this case study. A penalty of up to 50% may apply to demonstrations where virtual machines communicate directly using VMware network segments and bypass the physical network.