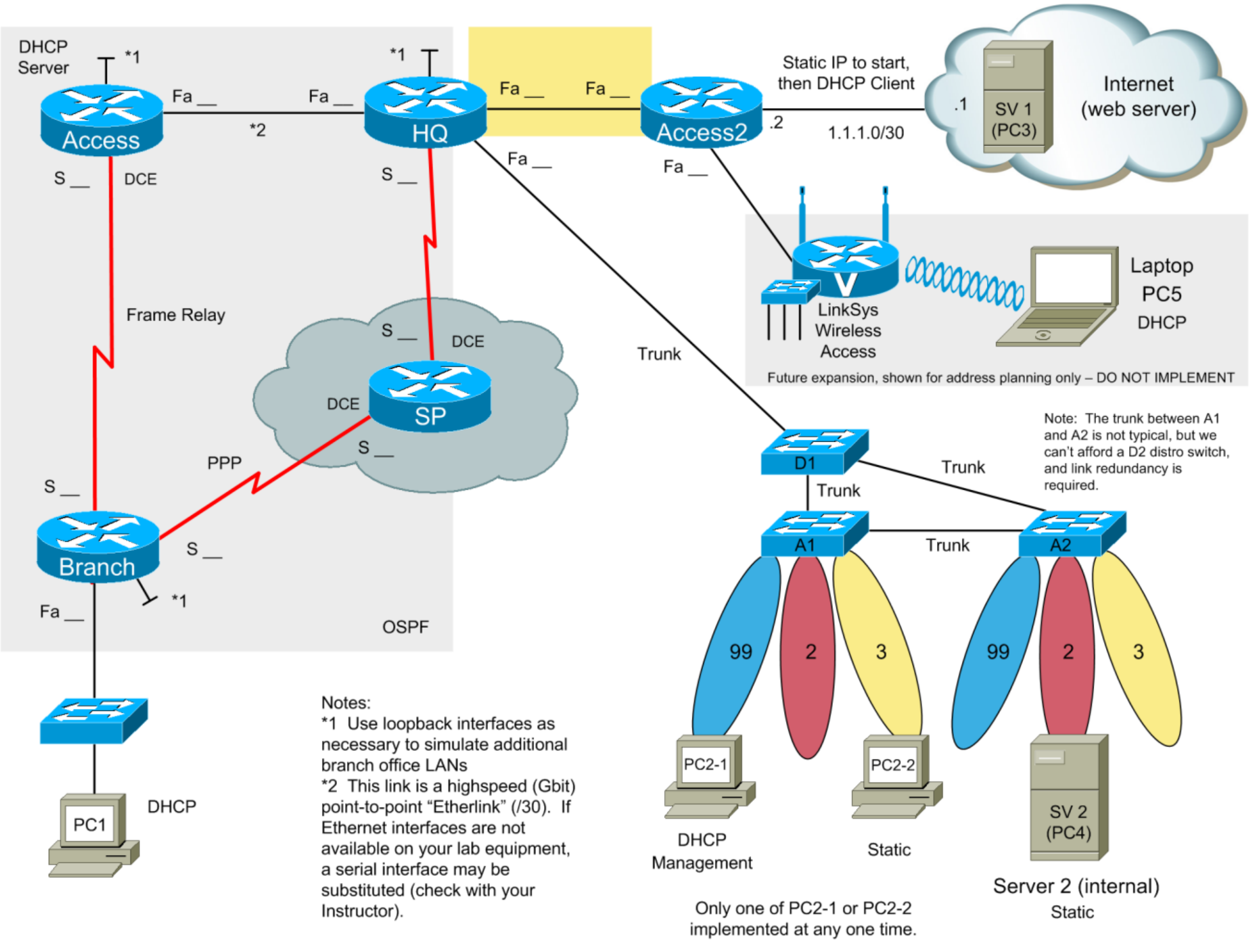
CIS 292 AB1 – Case Study – Dec 1, 2015

Names: ____ Group #______

Engineering journal only allowed.

Topology



Note: The trunk between A1 and A2 is not typical, but we can't afford a D2 distro switch, and link redundancy is required.

Notes:
*1 Use loopback interfaces as necessary to simulate additional branch office LANs
*2 This link is a highspeed (Gbit) point-to-point "Etherlink" (/30). If Ethernet interfaces are not available on your lab equipment, a serial interface may be substituted (check with your Instructor).

Only one of PC2-1 or PC2-2 implemented at any one time.

Scenario

The topology represents a medium sized company that is restructuring their Network. The HQ router is a high performance router intended to handle all corporate VLAN traffic. The Access router is used to connect to the Branch office with more Branch offices expected. Static routing will be used between the HQ router and the Internet access device (Access2). The LinkSys device will be used for future implementation of wireless (do not implement at this time). The Branch office is connected via a high speed PPP link through a WAN service provider and a slower Frame Relay link as a backup WAN connection.

Hand-In Requirements

You will produce and hand in a series of screenshots that will demonstrate your understanding of the systems implemented and tasks completed. Choose your screenshots to best demonstrate your understanding (i.e. "show run" is not usually a very good way, a show status such as "show ip route" is better, and an interactive debug output is typically better yet) The screenshots should always include your pod name, Router Name and/or PC name so that they can be uniquely identified. Keep your screenshots focused on what you are demonstrating. (see note 1)

Where it indicates "verify" in this set of requirements, you are required to produce the appropriate output to show your verification.

You will hand in a final word document to cismoodle.ufv.ca (one for each group). The document must list the tasks in the same order as this case study document. Insert any necessary notes, brief descriptions, circles and/or arrows to make it easy to locate and verify the tasks completed to specification.

Address Design

The address plan for the company network should use 172.16.X.0/20 private network address space, where X is determined by your group number (X = 16 * group#).

In planning for future expansion at HQ, the addressing design should allow for up to 8 VLANs of up to 200 hosts each. The first 2 will be implemented for general use and the 8th HQ subnet address will be applied to the management VLAN (VLAN 99).

Design for 8 Branch Office LANs where each should be able accommodate up to 100 hosts. The branch office address block should begin at the half way point of the total assigned address block for the company. Only 1 branch office subnet, the lowest one, will be physically implemented. The 2nd and 8th should be implemented as loopback interfaces.

The wireless network addressing should be designed to accommodate up to 126 wireless hosts, will use DHCP, and will be addressed as the 2nd last /25 address block. In this case study, do not implement the wireless network.

The last 128 addresses of the companies address block are reserved for point-to-point connections and will use the /30 mask. Implement the first 4 /30 subnets (from the last 128 addresses) for the high speed HQ-Access Etherlink, the HQ-SP link, the SP-Branch PPP link, and the Access-Branch frame-relay link (in that order).

The network between HQ and Access2 should be implemented as a /30 and will use the 5th subnet of this block. Use the 6th /30 subnet address for the EtherLink to the LinkSys wireless access point device.

Your address design should allow for efficient summarization of the HQ LANs, and efficient summarization of the Branch Office LANs. These are the only two summarizations and should only be done once everything has been tested.

Use the first address in each subnet for the address of the default gateway. Use addresses starting at .10 (or .140 as required) for assignment to fixed address hosts. Begin any DHCP pools at address .20 (or .150 as required).

Routing Protocols

Use static routing between the HQ router and the Access2 router. You will require one, two or three static routes on Access2 (depending on your design). The routing protocol used among the remaining routers should be OSPF (single area) with a default route advertised from HQ. There should be no routing protocol traffic on the WAN interface or the LAN interface of Access2.

Note: The LinkSys wireless device does not support NAT and RIP to be operational at the same time, therefore since NAT is required, RIP will not be used on LinkSYS (not applicable).

VLANs, Trunking and VTP

Although there are many VLANs planned for in your design, only the management VLAN, VLAN 2 and VLAN 3 should be implemented.

a) VLAN99 Management
b) VLAN2 Student
c) VLAN3 Faculty

Configure 4 ports on each of the two access switches for each of the 3 implemented VLANs (fa0/1-4 for VLAN 2, fa0/5-8 for VLAN 3, fa0/21-24 for VLAN 99).

VLAN trunks using the 802.1Q protocol should be implemented between each pair of switches and to the HQ router.

Set up a VTP domain of CISX (X is your group number). The switch that is the VTP domain server should be the switch closest to the HQ router with all other switches configured as VTP clients. Verify correct operation of VLANs, VLAN trunks and VTP.

Spanning Tree

Implement RPVST+ spanning tree on all switches, ensuring that the switch closest to HQ is the root bridge. Configure all ports connected to PCs with port-fast (12 ports on each access switch). Verify correct operation.

PPP

Configure the PPP datalink protocol for the primary connection to the Branch Office. Use the serial DSU interfaces and set the clock rate to 56Kbps on the DCE interface as indicated in the topology diagram. Configure a user on ISP called “chap_user” and a user on BRANCH called “chap_user”. Both of these “users” should be configured for a password of “cisco” that will be used with CHAP. Adjust as necessary. Verify operation.

Frame Relay

Configure Frame Relay as a backup connection to the Branch Office. Begin by implementing a 56K CSU/DSU back-to-back link between Access and Branch using the default HDLC encapsulation and ensure it operates correctly. Then convert it to a back-to-back Frame Relay link with the following specifications:

- One PVC with a DLCI = 100 + group#

- Disable the LMI protocol(s) and enable the frame relay interface(s) to operate without it (no keepalive).
- Map the interface layer 3 address(es) to the layer 2 DLCI(s)
- To allow OSPF operation over this frame relay link, ensure the interface bandwidth is set to the correct value and that multicasts/broadcasts are enabled over the link.
- Verify operation.

DHCP

Configure a central DHCP service on the Access router (normally this would be a service running on a Windows or Linux based computer). This DHCP service should provide IP configuration for all DHCP based LANs indicated in the topology diagram including the 3 HQ LANs and the Branch Office LAN.

- Configure all default gateways to be the first IP address in the subnet.
- Set the domain name to ufv.kom
- Configure a DNS server at 192.168.17.2
- Set the IP address pools to .20 - .29 (or .150 to .159)
- Configure Helper addresses to allow central DHCP operation.
- Verify operation.

NAT

Configure NAT overload on the Access2 device so that NAT occurs on the WAN connection of the Access2 device for outbound connections.

Configure static NAT for inbound access to your internal (web) server (Server 2).

Previously, the design included the LinkSys device in the place of the Access2 device. During testing your planning team determined that the LinkSys device was not going to scale well as the bandwidth needs of the organization have grown. It was also determined that the LinkSys device does not support NAT and RIP at the same time, and where some difficulty was caused. Therefore, to ensure the overall design meets current needs and is scaleable for future needs, you were asked to implement the revised plan (already done) that incorporates the Access2 device and moves the LinkSys device for use as “wireless only”. The revised plan specifies that an ISR router is to be used as Access2. The LinkSys device will be used for wireless only, but will not be implemented at this time.

Basic Security

No inbound security implemented at this time (other than NAT on Access2).

Implement basic outbound security using ACLs. Implement a numbered extended ACL on the outbound interface of the HQ router that satisfies the following requirements:

- All traffic to 1.1.1.0 /24 allowed
- HTTP traffic out to cisnet.ufv.ca (198.162.104.88) allowed
- HTTP traffic out to apache2.ufv.ca (198.162.104.116) blocked
- HTTP reply traffic from Server 2 allowed out (tcp source port = 80).
- All other outgoing TCP traffic blocked

- All other outgoing UDP traffic blocked
- All other outgoing ICMP traffic blocked

Hint: To assist you with your ACL design, implement the above with one ACL rule each and in the order indicated (i.e. your ACL should have 7 rules). Use notepad. Verify operational.

Tuning

Implement route summarization on HQ to summarize the HQ LANs. Implement summarization on Branch to summarize the Branch LANs and verify. Do so ONLY after everything else is tested and working.

Wireless

Plan for wireless LAN operation using PC5. Implementation not applicable.

Upgrade (challenge)

Suggest a solution including commands, however implementation not required.

An additional requirement has arisen. Management has decided that 2 additional IP subnets each with a maximum of 120 hosts, are required in the headquarters “C building”. You have decided that it best to connect these subnets to additional interfaces on the Access router (use loopback interfaces to model this). Use the next available /25 IP network addresses from your assigned address range, but do not use the IP addresses from the blocks previously reserved for HQ and for Branch offices.

Clean up

Erase the device configurations and reload the routers. Disconnect and store the cables.

Documentation requirements

Due date: Within approximately 5 days - see moodle (one report for each group)

Hand in a brief report that includes the following:

1. For each router, capture command output to text files including the running configs and routing tables. Neatly edit these and include them as appendices in your report.
2. A diagram of your complete topology that neatly includes all relevant information including device names, interface names, IP addresses (or “dhcp”) of devices and networks, DCE/DTE indications, bandwidth indications if helpful, DLCIs, authentication type, trunks, VLANs, etc. A skeleton drawing with device symbols will be provided for you to use as a base.
3. Your layer 3 addressing plan and a brief summary of your rationale for its design.
4. A description of each part of the case study that you implemented and tested (i.e. OSPF, IP address plan, frame relay, etc). In your descriptions provide the relevant configurations with an explanation of the operation, a diagram as may be helpful, any issues encountered and your solution(s).

Note 1 – Screenshot capture:

You will use a suitable screen capture utility such as “Snipping Tool” that is included as a Windows 7 accessory. Your capture utility should be run from your local desktop (not from PC-A / PC-C). It is typically best that you capture the required images / screenshots and then annotate them after your Case Study is completed. Your captured screenshots MUST have a clear indication of your pod number, router name and / or your PC name as appropriate. It is important that your screenshots are captured during the same working session, as attempting to continue at a later time will cause difficulty in the interpretation of the information. Ensure your screenshots are “focused” on the information being captured.

Note 2 – Order of implementation:

The requirements in this Case Study are listed in a similar order that they appear in the lab exercises that you completed previously. This may not necessarily be your preferred order of implementation. As a general approach it is best to first implement and verify functionality, then tighten, close and harden after the required functionality has been verified. The implementation of “auto secure” is an example of a “lock down” that you may deem better to apply later on. If you determine it best to modify the order of implementation, make sure that this is reflected in your documentation.

Notes: