Case Study 2

Configure ISDN Backup and VPN Connection

Cisco Networking Academy Program

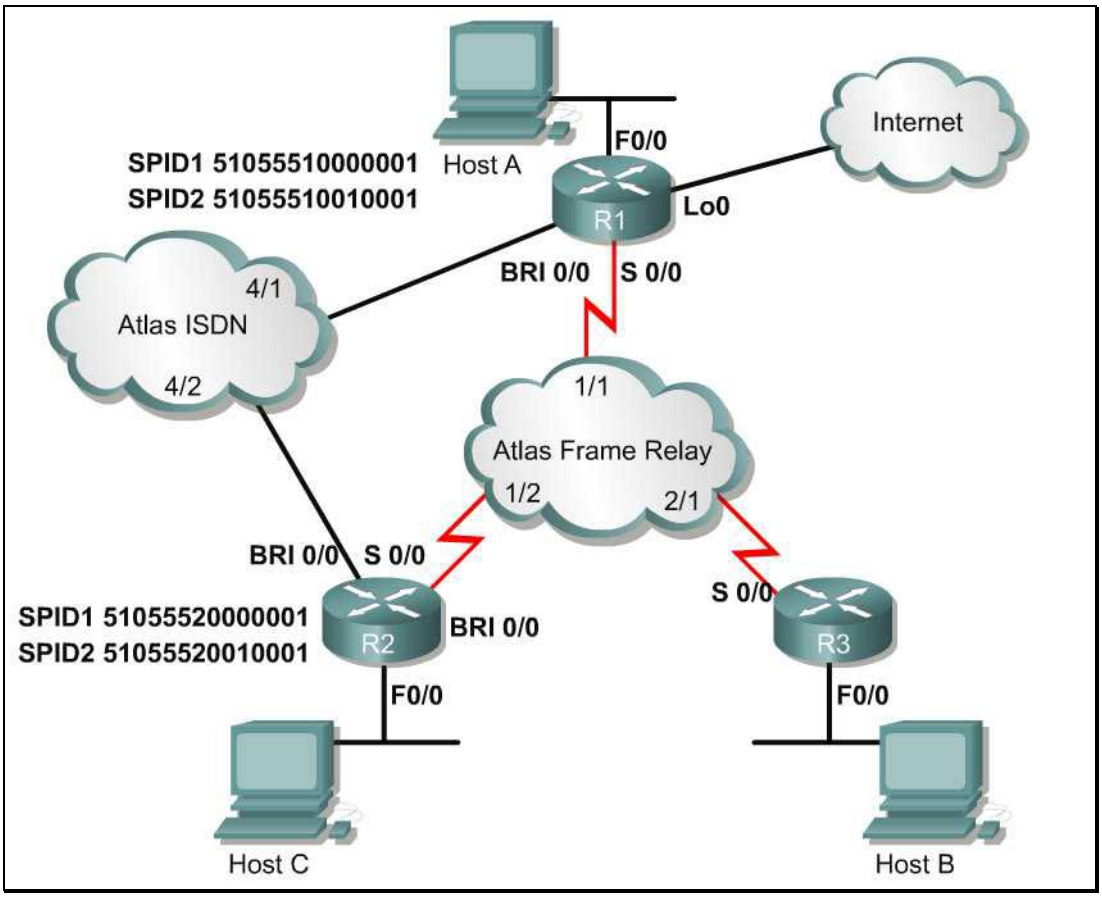
CCNP 2: Remote Access v3.1

Objectives

In this case study, the following concepts are covered:

- AAA authentication
- Multipoint Frame Relay with Sub-interfaces
- ISDN dial backup
- Floating Static Routes
- Dynamic NAT
- Multipoint VPN with NAT
- QoS- Class Based Weighted Fair Queuing

Scenario



The Air Guitar Company wants ISDN backup for the primary Frame Relay Links. In addition they have asked for a multipoint VPN connection to R3.

Initial Configurations

- Physically connect the network devices according the above diagram. Be sure that the cables are connected to the appropriate Adtran ports as labeled in the diagram.
- Configure the F0/0 interface on R1 and R2, as well as their respective hosts so that they belong to the 10.x.x.x/24 network. The x represents the router number. OR – Substitute the x for the router number. Example: R1 F0/0 = 10.1.1.1 /24. Be sure to configure the respective hosts on R1 and R2 to use the appropriate gateway IP.
- Configure Host B and the F0/0 interface on R3 so that they belongs to the 192.168.3.0 /24 network.
- Configure R1 with a Loopback interface using the IP address 1.1.1.1/24. The loopback address will be used to simulate a connection to an external network.
- Configure all three routers using the privilege EXEC mode password **cisco**.

- Configure all three routers with a local username and password database where the username will be the remote router name and password **cisco**. Example: **`username r1 password cisco`**.
- Configure AAA authentication on all routers to query the local username and password database.

Frame Relay

- The Atlas is preconfigured with multiple PVCs. For the purposes of this lab, the PVC between R1 and R3 will be ignored. After setting the Frame Relay encapsulation on R2, issue the following command**: no frame-relay inverse-arp ip 203**. After setting the Frame Relay encapsulation on R3, issue the following command: **no frame-relay inverse-arp ip 302**. The commands will prevent automatic mapping for this unused PVC.
- Configure Frame Relay on all three routers so that R2 and R3 will become spokes and R1 will be the Frame Relay Hub.
  - Configure sub-interfaces on R1 to directly connect to R2 and R3.
  - Configure the Frame Relay connection between each Hub and Spoke so that R1 and R2 belong to the 10.1.0.4/30 subnet and that R1 and R3 belong to the 10.1.0.8 /30 subnet.
- Configure default routes on R2 and R3 so that R1 will be the next hop router. Be sure to configure static routes on R1 to reach R2 connected LAN. Do not configure a static route on R1 to reach the R3 LAN.
- Use **ping** to verify connectivity between each router over the Frame Relay link.

NAT

- Configure Dynamic NAT on R3 so that traffic sourced from its inside local address 192.168.3.0/24 will be translated with a global address of 10.1.3.0/24.
- Configure an access-list on R3 so that packets sourced from its inside local address will not be translated with NAT when destined for the R1 and R2 remote LANs. Traffic destined for any other destination will be translated with NAT.
- Be sure to configure a default route on R3 to use R1 as the next hop router to reach any destination networks.
- Configure a static route on R1 and R2 to reach the R3 inside local address 192.168.3.0/24.
- Ping the Lo0/0 interface on R1 from Host B. Use the appropriate **show** commands to verify that R3 has translated packets from its LAN with an inside global address.
- **Ping** Host A and Host C from Host B. Use the appropriate **show** commands to verify that R3 has not translated packets from its LAN with an inside global address.

ISDN Dial Backup

- Use the SPID information from the network diagram to configure ISDN BRI on R1 and R2. The ISDN switch type used for the ISDN BRI connection is basic-ni.
- Configure R1 and R2 to secure the ISDN dial up connection to use PPP CHAP. Be sure that the **aaa authentication default** is defined for PPP.
- Configure the BRI interface on R1 and R2 so that it belongs to the VLSM 10.1.2.0/30 network.
- Test the ISDN connection by initiating a DDR connection. Ping the BRI0/0 interface on R2 from R1. If the pings fail troubleshoot as necessary.
- Configure ISDN dialer backup on R1 to use the BRI interface to backup the primary Frame Relay interface. The backup line should come up 5 seconds after the primary link fails and go down 20 seconds after the primary link comes back up.

IPSec

- Configure Hub and Spoke IPsec so that R2 will build an IPsec tunnel through R1 in order to reach R3.
- Configure a named access-list on all routers to define traffic from their respective LANs to be encrypted when traffic is destined for their neighboring remote LANs.
- Configure R1 and R2 so that traffic sourced from their FastEthernet LAN and destined for their respective neighboring remote LANs, is encrypted.
- Configure IPSec on R3 so that the inside local address will be encrypted and not be translated by NAT when traffic is destined for the R1 and R2 Ethernet networks. Packets destined for anywhere else will be translated with NAT.
- Configure the ISAKMP policy suite on R1 and R2 with the following parameters. Be sure to manually configure the same pre-shared key on both routers and to use pre-shared keys authentication.
- Configure the transform-set to use esp-des to build the IPSec security association. Be sure to configure and apply a crypto map to the defined parameters for IPSec protection on each routers s0/0 interface.
- To test your IPSec tunnel configuration enable the appropriate **debug** commands to monitor IPSec activity and **ping** Host C from Host B.

QoS

- Configure class based weighted fair queuing (CBWFQ) on all three routers to guarantee 32 kbps of Frame Relay bandwidth usage for Telnet traffic from any source to any destination.
- Use the appropriate configurations to verify your QoS configurations.

Check List

- R1 should query its local username and password database to authenticate remote login attempts.
- R1 should be able to initiate an ISDN DDR connection with R2 and vice versa.
- The ISDN connection on R1 and R2 should be able to back up the primary Frame Relay link in the event of link failure.
- LAN traffic from all three routers should be encrypted with an IPSec tunnel using pre-shared keys over a multipoint topology.
- RFC 1918 internal IP address on R3 should be encrypted with an IPSec tunnel when traffic is destined for the FastEthernet networks of R1 and R2.
- Telnet traffic should be guaranteed 32 kbps of Frame Relay bandwidth using CBWFQ.

