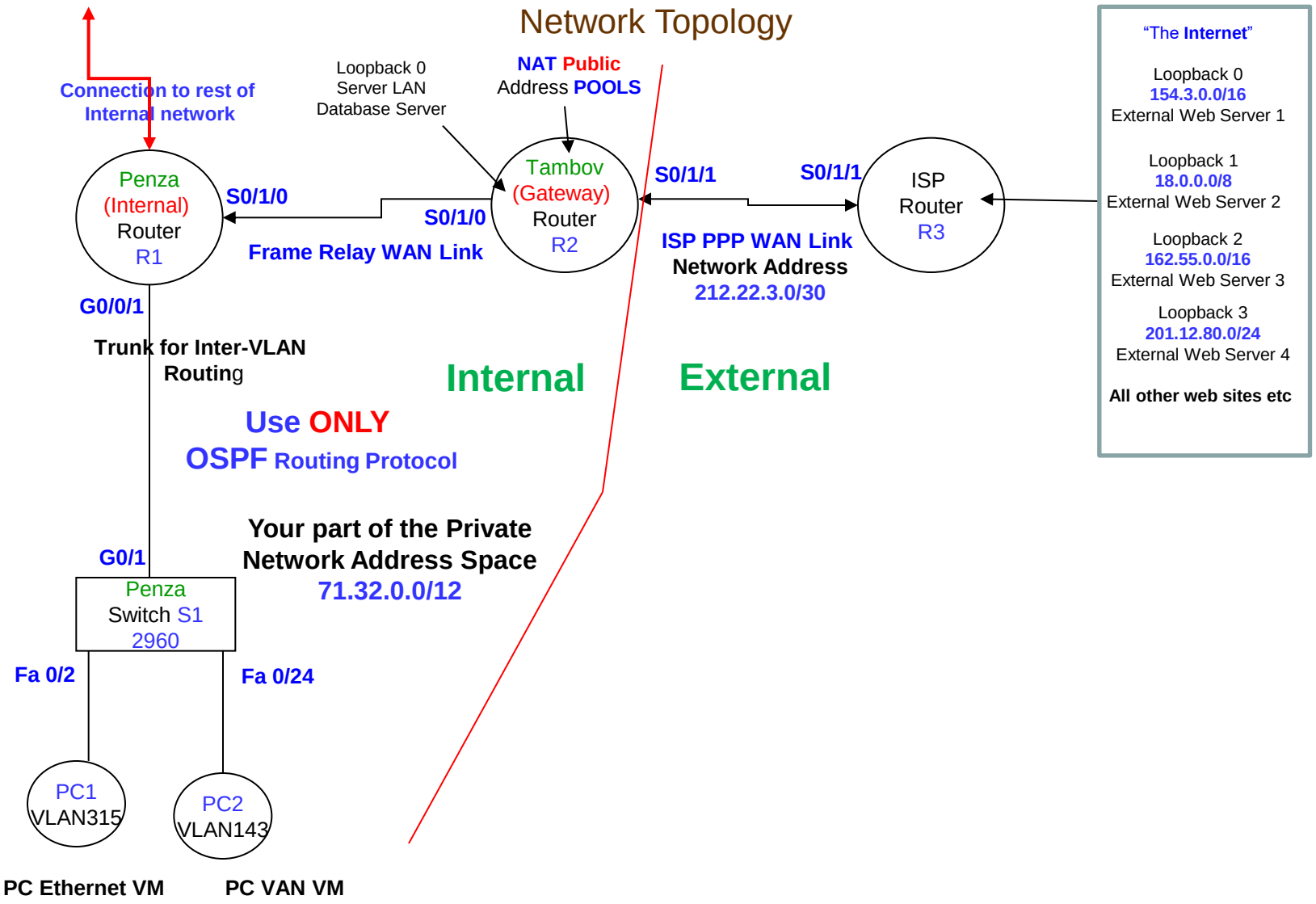
Scenario 6 (6 marks) - Frame Relay, PPP V2.7

A Network Configuration and Trouble Shooting Scenario

Network Topology



The Scenario – An Analytical and Systematic Approach

- The aim of this approach is to allow you to integrate the different topics (theory and practical) covered in the Unit, into the building of the network platform.

- Each scenario requires you to build a working network, then add new network services and functionality to the network platform.

- It is designed to be self re-enforcing, as what you have learnt in previous scenarios is required in future scenarios.

- It emphasizes an Analytical and Systematic approach to building the network platform:
  1. Produce a Network Topology
  2. Prepare the VLSM Design
  3. Follow a step-by-step process to ensure that, configuration, testing, and troubleshooting is done in an order and sequence that will achieve a working network.

- This approach is designed to prepare you (given the complexity of the network you will be required to build) for the Skills Exam.

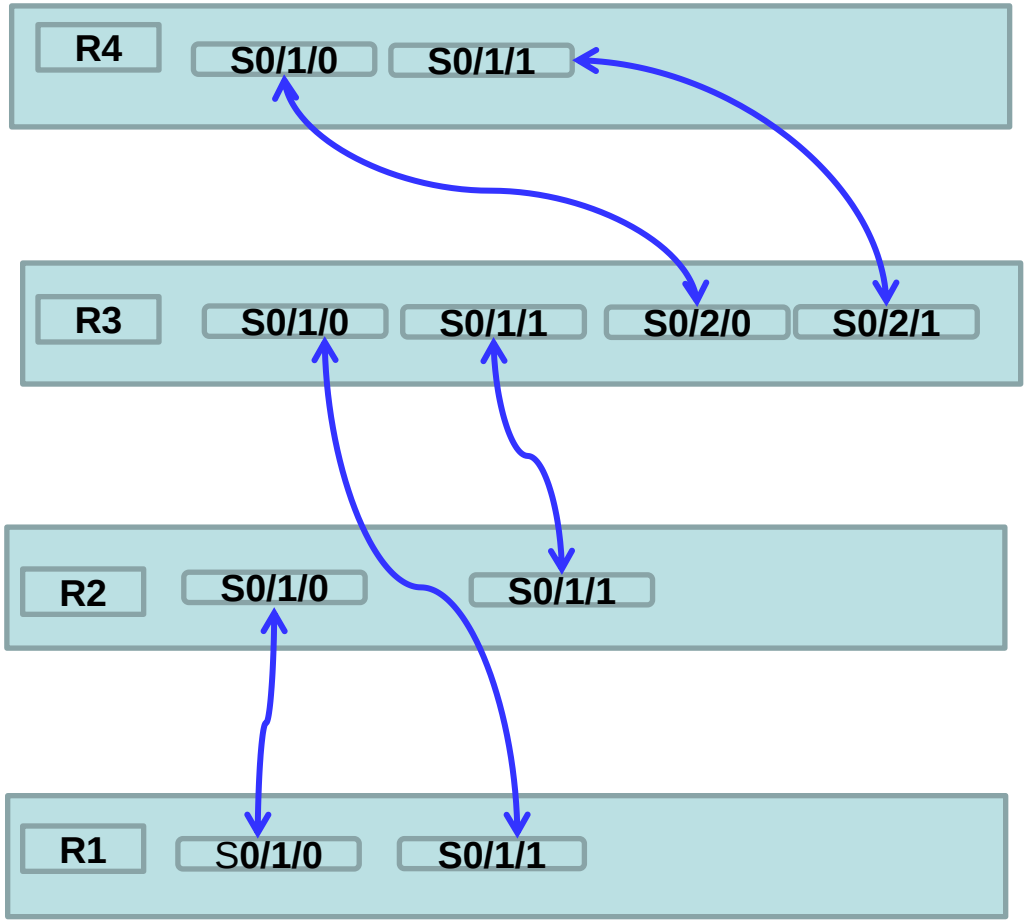
Scenario 6 - Introduction

- This scenario can be completed independent of the lecture material as configuration details are provided on pages 17 to 34
- Your instructor will give you an overview of the scenario at the beginning of the lab
- As a How to Configure Guide, it is recommended you obtain a copy of “CCNA Portable Commands Guide (CCNA Self-Study) 2/3/4 Ed”, Scott Empson, Cisco Press
- **What is new?**
  - You will configure a **Frame Relay** WAN Link between Penza and Tambov routers
  - You will configure a **PPP** WAN Link
  - You will configure **CHAP** Authentication on a PPP WAN Link
  - NAT **Overload**
  - ACLs to deny a VLAN access to Database Server LAN
  - DHCP and the use of a **helper ip address**

- **Network Topology**
  - Internal, your internal network
  - External, the link to the ISP and the Internet
  - The Internet is represented be a number Loopbacks
  - The Corporate Private Network Address, **71.0.0.0/8.**
  - The corporate address has been **divided up** and you have been given the address space **71.32.0.0/12** to build your part of the Corporate Network.
  - Do not configure the connection to the rest of the internal network
  - ISP Link Address, **212.22.3.0/30**
  - NAT Public Address Pool **141.50.128.0/24**

Kit - Router Serial Cable Mapping

Rooms ATC328 and ATC329



Students are NOT allowed to remove serial cables, as removal often causes damage to the serial interface. If you believe a serial interface is not working, please inform your instructor !

Scenario 6 – Assessment

1. **Assessment due**
   - Scenario 6 will ONLY be assessed up to the end of your allocated Lab in week 11
   - Scenario 6 will NOT be assessed (no marks given) after your allocated lab in week 11
2. Scenarios must be completed individually
3. **. Assessment Process**
   - Email your Packet Tracer File to your tutor for assessment
   - OR if you have remotely accessed a lab kit, ask your tutor to assess your scenario in the lab
     - Your tutor may:
       - ask you questions about your scenario
       - ask you to further configure your routers, switches, PCs
       - break your network and then ask you to troubleshoot, find and fix, the problem
   - The **aim** of this process is:
     - to ensure you get feedback on your understanding of the material
     - to allow your tutor to help in your understanding of the material
     - to develop your troubleshooting skills so that if a problem occurs during the skills exam you can find and fix it
4. **Assessment Marking**
   - Up to 6 Unit Marks will be given
   - **Note:** A MOTD banner, recording your **student id, family name**, and **lab time** must be configured on **all** routers and switches. If the banners have **NOT** been configured you will get **0 Marks**

Scenario 6 -Tasks

1. VLSM Design and Documentation

a) As a first task it is important to get your addressing scheme correct and documented.
Design IP VLSM Addressing Scheme, using this part **71.32.0.0/12** of Corporate Network Address space with:

- **VLAN 315** Cows 800 hosts
- **VLAN 143** Sheep 200 hosts
- **VLAN 615** Goats 120 hosts
- **Tambov Database Server LAN** loopback 0 20 hosts,
- **VLAN 33 Management** 6 hosts,
- **Internal Serial** 2 hosts

b) You can use a VLSM calculator

c) Record VLSM Subnet Addresses

Subnet	IP Address/Prefix	Host IP address Range
VLAN 315		
VLAN 143		
VLAN 615		
Database Server LAN		
VLAN 33		
Internal Serial		

Scenario 6 – **Task 2** Record IP Host Address Assignment

Tambov	IP Address/Prefix	Next Router
S0/1/0		
S0/1/1		
Loopback 0		

Penza	IP Address/Prefix	Next Router
S0/1/0		
G0/0/1.		
G0/0/1.		
G0/0/1.		

ISP	IP Address/Prefix	Next Router
S0/1/1		

PC Host	IP Address/Prefix	Gateway IP Address	DHCP Y/N
PC1			
PC2			

Penza Switch	IP Address/Prefix	Gateway IP Address
VLAN 33		

Scenario 6 -Tasks

3. On each router, ensure router config-register is set to 0x2142: router(config)# config-register 0x2142, refer to page **35**

4. Do not configure **enable passwords** OR **line console passwords** on router and switches, unless specified by the task

5. PC Setup

a) Hard Reboot: Turn Desk Top PC Off then On (Clears Memory, as PCs are on 24/7)

b) Virtual PCs will be used to connect to the network. They are launched using the **Virtual Machine (VM) Launcher**.

c) Down load new PC Virtual images !!

d) Launch PC1 Ethernet (PC1 connected via physical Ethernet cable)

e) Launch PC2 VAN (PC2 connected via Yellow VAN cable)

6. Cable Connection

a) Connect Penza router to switch port G0/1

b) Check routers are connected via serial links, refer to page **4**

c) Connect PC1 to Fa 0/2 using the patch panel, connect PC2 to Fa 0/24 using the VAN

7. Helpful Configurations

a) Configure the line console on each router and switch, as shown below:

line console 0
logging synchronous *(stops system messages overwriting your typing)*
exec-timeout 0 0 *(ensures you do not return to user executive mode)*

b) Turn off DNS (Domain Name Service)

no ip domain-lookup *(ensures if you miss-type a command, the router will not try to resolve the command as a URL web address)*

8. Message of the Day (MOTD) Banner Configuration (If banners are not configured, then 0 marks for the scenario)

You must configure a MOTD Banner, recording your student id, family name and lab time, on all routers and switches, as shown below:

banner motd &
Welcome to Hostname
Your Student Id, *Your Family Name*, Your *Lab Time*
&

Scenario 6 -Tasks

9. Switch Configuration

a) Refer to pages **26 to 29** and to **your journal** and lab exercises from prior unit on **Basic Switch and VLAN Configuration**

b) Check the switch is clean, if NOT then:

i) Delete the vlan.dat file to remove old VLANs from the Switch, use - **delete vlan.dat**

ii) Use - **erase startup-config** then **reload**

c) Create VLAN 315 Cows, VLAN 143 Sheep, VLAN 615 Goats and VLAN 33 Management

d) Configure G0/1 as a **trunk** port

e) Configure as **access ports**, only VLAN 315 ports 2,3 and VLAN 143 port 24

f) Switch Management – configure an ip address on interface VLAN 33 and configure a default gateway, refer to page **7**

g) Configure **enable password cisco** and **Line vty** with password **cisco** and **login**, so each switch can be configured via Telnet

h) Configure Port Security, VLAN 315 , mac address sticky on ports 2,3 max 2, with **violation shutdown**

i) Configure a static mac address, VLAN 143, on Fa 0/24 to the MAC address of PC2

10. Trouble Shooting VLANs

a) To check VLANs created, use – **show vlan brief**

11. Trouble Shooting Port Security

a) To check port security is enabled, use - **show port-security**

b) A table will be displayed showing the security status of the switch ports

Scenario 6 -Tasks

12. Network IP Address Configuration

a) Configure **ALL** the router serial and loopback interfaces with ip addresses, refer Task 1 and Task 2

b) Penza Router

i) **Inter-VLAN Routing Configuration**

- Refer page **24** and to **your journal** and lab exercises from prior unit on **Basic Inter-VLAN Routing**
- Configure **Inter-VLAN Routing** on G0/0/1
- Only create separate sub-interfaces for VLANs 33, 315 and 143
- Assign each sub-interface with an ip address

c) PC Configuration

i) Configure PC1 and PC2 IP addresses

d) Penza Switch

- Check default gateway configured on switch, use VLAN1 G0/0/1 .1 sub-interface ip address

13. Trouble Shooting Trunking – between Switch and Router

a) To check Trunking is activated, on switch(es), use – **show interface trunk**

b) Check correct interface has been configured for trunking !

Scenario 6 -Tasks

14. Trouble Shooting Point-to-Point Single Link Testing

a) This test is to check that each individual link in the network is working.

b) Ping (command) – ensure you can ping from one end of each link to the other:

- PC to Router in same subnet/VLAN/network.
- PC to PC in same subnet/VLAN/network
- Switch to Router
- Router to each direct neighbour Router over a serial link.

c) Link NOT working ? - Common problems:

- Physical connection not made.
- The clock rate is not configured on DCE interface of a serial link.
- An incorrect IP address or subnet mask is configured on one interface of a link
- The interface is shutdown.

15. Trouble Shooting Inter-VLAN Routing Test

a) This test is to check Inter-VLAN routing is working

b) Ping PC1 – VLAN 315 to PC2 – VLAN 143

c) Check IP address/Mac address mapping on the router, **show arp**

16. Trouble Shooting Telnet to Switch

a) To check you can telnet to the switch

b) From PC1 DOS command window – telnet to the switch

c) Common problems:

- Switch Vlan1 interface shutdown
- Switch has no default gateway IP address
- Switch Line vty not configured with login and password
- Inter-VLAN routing failure

Scenario 6 -Tasks

17. Routing Protocol Configuration (refer page **22**)

a) Penza

- **OSPF** using wildcards for each subnet
- Configure passive-interface as appropriate to avoid sending unnecessary routing information

b) Tambov

- **OSPF** using wildcards for each subnet
- Do not advertise the external network address
- Configure passive-interface as appropriate to avoid sending unnecessary routing information
- Configure default route to ISP Router
- Advertise default route to Penza Router

c) ISP Router

- **Do not configure OSPF**
- Configure loopbacks for Web Servers (If you are using Packet Tracer may need to use Server Devices)

18. Trouble Shooting OSPF Neighbor Adjacency

a) Verify that the routers have formed an adjacency with each other, use - **show ip ospf neighbor**

b) Adjacency NOT Formed ? - If an adjacency has not formed it could be due to:

i) subnet masks on each end of link do not match

ii) the directly connected subnet is not included in the **network** statements

c) Other trouble shooting commands: **show ip protocols, debug ip ospf events**

19. Trouble Shooting Routing - Presence of Subnets

a) Internal Routers

- Use **show ip route** to display the **routing table** on each router:

- Check all the subnets are present
- Check there is a default route

b) Common problems:

- Routing protocol is not advertising a subnet
- An interface is down
- Static or Default route not configured

Scenario 6 -Tasks

20. Trouble Shooting Internal Private End-to-End Path Testing

a) This test is to check that the **internal routing - static and dynamic**, is working.

b) Use **debug ip icmp** on Tambov router to check ping request arrives

c) Ping from PC Hosts in VLAN 315 and VLAN 143 to Database Server on Tambov

d) Use **traceroute** to pin point problems.

e) Internal Private End-to-End Path Test Failed ? - Common problems:

- Default gateway IP address not configured on a PC.
- PC connected to incorrect interface.
- Subnet not advertised
- Subnet missing from routing table
- Default route not advertise

21. NAT Configuration

a) Configure NAT Pools on the **Tambov Router**

- Refer to page **21** and **Lab on NAT Configuration**
- Create separate NAT Pools and ACLs for VLANs 33, 315, 143
- Overload each NAT pool

b) ISP router

- Configure a static route to the **public NAT Pool address** on **Tambov**

22. Trouble Shooting NAT - Internal Private to External Public End-to-End Path Testing

a) This test is to check that NAT is working - that the private IP address is being translated to a public IP address

b) Use **debug ip nat** on Tambov to view the NAT translations

c) Use **debug ip icmp** on ISP router to check ping request arrives

d) Ping from PC Hosts in VLAN 315 and VLAN 143 to the Internet – pick an External Web Server

e) NAT Failed ? – Common Problems:

- ACL and Pool names are case sensitive, check names are correct
- ACL incorrectly configured
- NAT pool incorrectly configured
- Binding of ACL to NAT Pool incorrectly configured
- Inside and outside interfaces incorrectly or not configured
- On ISP static route is not pointing to NAT pool

f) Useful commands, use - **show ip nat translation**s, **debug ip nat**

Scenario 6 -Tasks

23. **DHCP Configuration – Dynamic IP address allocation**

- Configure DHCP on **Tambov Router**
- Configure helper ip address for DHCP on **Penza Router**
- Refer to page **20** and **Lab on DHCP Configuration**
- Create separate DHCP Pools for VLANs 315 and 143
- Exclude the first four IP addresses
- Configure PC1 and PC2 to obtain IP address automatically

24. Trouble Shooting DHCP

a) Use **debug ip dhcp server events** on Tambov Router, to view the DHCP process
b) Open DOS CMD window on PC1 and PC2 – **ipconfig /release** then **ipconfig /renew**
c) Addresses obtained ? NO – check router configuration,
use – **show ip dhcp pool**, **show ip dhcp binding, show run**

25. HTTP Servers on Routers

a) Configure a HTTP server on ISP Router, use – **ip http server**
b) If you are using Packet Tracer you must configure a Web Server and connect it to the ISP Router
b) This allows you to test your ACLs using a Browser.

26. Telnet Access to Routers

a) Configure **line vty** with password **cisco** and login, so you can connect to each router can via Telnet
b) NO enable password is required as you are **NOT** configuring the router
c) This allows you to test your ACLs using Telnet.

Scenario 6 - Tasks

27. Frame Relay Link Configuration (Point-to-Point)

a) Configure the link between Penza and Tambov routers as Frame Relay link, refer to page **30**

b) Changing the encapsulation to frame relay on the serial interfaces will break the neighbor adjacency between Penza and Tambov. You must shutdown both interfaces, then no shutdown, so the neighbor adjacency can be re-established.

28. Trouble Shooting Frame Relay

a) To confirm the Link is active, use - **show frame-relay map**

b) Link NOT Active ? - To watch Link Establishment to determine what the problem is, use - **debug frame-relay events**

c) Link Active ? – Ping next hop IP address, to confirm layer 3 addressing is correct

29. Point-to-Point Protocol (PPP) Configuration

a) Configure the link between Tambov and ISP routers as PPP link, refer to page **31**

b) Ping across the link between Tambov and ISP to check it is working

30. CHAP Configuration

a) Configure, refer to page **32,** CHAP authentication on the link between Tambov and ISP

31. Trouble Shooting CHAP

a) Ping across the link between Tambov and ISP

b) Ping failed ? – Common problems:

- Host name incorrectly configured
- Password incorrectly configured with space at front
- Encapsulation incorrectly configured

c) To check authentication, use - **debug ppp authentication**

Scenario 6 - Tasks

32. Access List Requirements

a) Refer to pages **17 to 19** and **Lab Exercises on Access Control Lists**

b) You must create a **NAMED Extended** ACL for VLAN 315 based on following requirements:

- PCs in VLAN 315 permitted **HTTP** access to an External Web Server (you choose one) and denied **ALL** other access to that External Web Server.
- PCs in VLAN 315 denied **PING** request to PCs in VLAN 143
- PCs in VLAN 315 permitted **PING** reply to PCs in VLAN 143
- PCs in VLAN 315 permitted **ALL** access to the Internet – all the other External Web Servers

c) You must create a **NAMED Extended** ACL for VLAN 143 based on following requirements:

- PCs in VLAN 143 denied ALL access to Database Server LAN
- PCs in VLAN 143 permitted **ALL** access to the Internet – all the other External Web Servers
- **ALL** means **IP**

d) You must create **NAMED Standard** ACLs to control Telnet access to the routers based on following requirements:

- ONLY PCs in VLAN 315 permitted **TELNET** access to Penza Router
- ONLY PCs in VLAN 315 denied **TELNET** access to Tambov Router

e) You need to be **analytical and systematic** in our approach to translating the above requirements into a set of rules – the ACL statements, which then must be tested to ensure the above requirements have been satisfied:

i) **Create** a **NAMED Extended** ACL for VLAN 315 using the template on page **16**, refer Task 31
ii) **Test** the ACL for VLAN 315 refer Task 32
iii) **Create** a **NAMED Standard** ACLs for Telnet access using the template on page **16**, refer Task 31
iv) **Test** the ACLs for Telnet access refer Task 32

Scenario 6 - Tasks

33. Creating and Configuring NAMED Access Lists

a) Refer **Lab Exercises on Access Control Lists**
b) Use **Notepad** to create your ACLs, note ACL names are **case sensitive** eg aclvan315 and Aclvlan315 are different acls
c) Identify each requirement then configure an ACL rule for each requirement.
d) Create a **NAMED** access list in **Notepad**, consider the ordering of the rules, use the following **template**:

! ACL for VLAN <*No*> on Router <*router name*>
! Deletes previous version of access list
no ip access-list extended ACLVLAN<*No*>
! Insert Latest version of access list
ip access-list extended ACLVLAN<*No*>

<Your ACL rules follow>

! For most situations this should be the last rule ie permit all other access to "The Internet"
permit ip any any

e) Combine ACL rules as required to form your access list, carefully consider the order in which the rules should be arranged.
f) Paste ACL from Notepad into router (router must be in global configuration mode)
g) Configure ACL on correct interface

34. Trouble Shooting Access Lists

It is important to verify that the **ACL rules** actually work as intended, refer to the **steps** below:

1. **Use show access-lists**
   - If all rules tested **go to 5**
   - Else Identify which rule you want to test
2. **Use clear access-list counters**
   - Clear any counts against the rules
3. Go to PC in VLAN<Id> perform test eg **Ping**, **Telnet**, **Browser** etc to trigger a match with the identified rule
4. **Use show access-lists**
   Was the identified rule matched ?
   - **Yes** – rule action correct, Repeat process, **go to 1**
   - **No** – Debug
     - Was another rule matched ?
     - Where no rules matched ?
     - Check syntax and order of rules – make changes – Repeat process **go to 1**
5. **Trouble Shooting completed**

ACL Templates

ACL for VLAN 315 on Penza Router

The Access List – Extended Named (**create in Notepad**, then paste into router config mode)

no ip access-list extended ACLVLAN315 (Delete previous version of the ACL for VLAN 315)
ip access-list extended ACLVLAN315 (Self-documenting, the ACL for VLAN 315, ! means comment)

! Only permit HTTP access to External Web Server
permit tcp source subnet wildcard host ip address eq www

! Deny ALL other access to the External Web Server
deny ip *source subnet* *wildcard* host *ip address*

! Permit ping reply (echo-reply) to a destination – PCs in VLAN 143 subnet
permit icmp source subnet wildcard destination subnet wildcard echo-reply

! Deny PING request to a destination - PCs in VLAN 143 subnet
deny icmp source subnet wildcard destination subnet wildcard

! Permit access to The Internet
permit ip any any

ACL Placement - On Sub Interface G0/0/1.315 on Penza Router
interface G0/0/1.315
ip access-group ACLVLAN315 in

ACL Templates

ACL to control Telnet Access to Penza and Tambov Routers

The Access List – Standard Named (**create in Notepad**, then paste into router config mode)

```
! On Penza
no ip access-list standard ACLTELNET
ip access-list standard ACLTELNET
! Permit VLAN315 Telnet Access to Penza
   permit source subnet wildcard
   deny any

! On Tambov
no ip access-list standard ACLTELNET
ip access-list standard ACLTELNET
! Deny VLAN315 Telnet Access to Tambov
   deny source subnet wildcard
   permit any
```

Interface Placement - line vty 0 4, on Penza and Tambov Routers

```
line vty 0 4
  password cisco
  login
  access-class ACLTELNET in
```

ACL Overview

ACL Case Sensitivity

- ACL names are case sensitive eg aclvlan315 and AclVlan315 are **different** ACLs
- Should decide to use either all uppercase - ACLVLAN315 or all lowercase – aclvlan315 names to reduce errors

ACL Rule Order

- ACL rules in the access list should be in order of most specific to least specific
- The last rule should be permit All other access

ACL Placement Rules

- Standard ACL – place as close as possible to destination network or device, to avoid unnecessarily blocking traffic
- Extended ACL – place as close as possible to source network or device, to block traffic earlier to reduce congestion

ACL Trouble Shooting

- show access-lists
- clear access-list counters
- Use the following for testing the rules: ping, telnet, a browser

DHCP Configuration

- **Configure DHCP pools on Router Tambov**

  service dhcp (turns on DHCP service)

  ip dhcp pool poolVLAN315
  network *subnetwork subnetwork mask*
  default-router *ip address of G0/0/1.315*

  ip dhcp pool poolVLAN143
  network *subnetwork subnetwork mask*
  default-router *ip address of G0/0/1.143*

- **Configure on Router Penza**

  – Configure an ip helper address, refer **Lab on DHCP Configuration**

- **Trouble Shooting Commands**

  – show ip dhcp pool
  – show ip dhcp binding
  – clear ip dhcp binding *
  – debug ip dhcp server events
  – open DOS CMD window on PC1 and PC2 – **ipconfig /release** then **ipconfig /renew**

NAT Configuration

- **Configure on Router Tambov**
  - The NAT Public Address Pool, provided by the ISP is **141.50.128.0/24, this is a range of ip addresses,** divide 3 ways, do not VLSM
  - **Address Pool Nat Pools**

    ip nat pool POOLVLAN315 starting IP address ending of IP address> netmask ?.?.?.?

    ip nat pool POOLVLAN143 starting IP address ending of IP address> netmask ?.?.?.?

    ip nat pool POOLVLAN33 starting IP address ending of IP address> netmask ?.?.?.?
  - **NAT Access Control Lists**

    ip access-list extended ACLVLAN315

    permit ip source subnet wildcard any

    ip access-list extended ACLVLAN143

    permit ip source subnet wildcard any

    ip access-list extended ACLVLAN33

    permit ip source subnet wildcard any
  - **Establish dynamic source translation by binding the pools with the access control lists**

    ip nat inside source **list** ACLVLAN315 **pool** POOLVLAN315

    ip nat inside source **list** ACLVLAN143 **pool** POOLVLAN143

    ip nat inside source **list** ACLVLAN33 **pool** POOLVLAN33
  - **Specify inside and outside NAT interfaces**

    interface s0/1/0

    ip nat inside

    interface s0/1/1

    ip nat outside
  - **Overload each NAT pool – refer Lab on NAT Configuration**

- **Trouble Shooting Commands**
  - show ip nat translations
  - clear ip nat translation *
  - show ip nat statistics
  - debug ip nat
  - debug ip nat detailed

Routing Configuration Rules

- Each router should only advertise its internal directly connected networks
- Routing updates must not be sent to LANs/VLANs
- A default route to the Internet should only be configured on the gateway router
- Only the gateway router must advertise the default route to the internal routers
- The ISP router
  - If the company is using:
    - a public network address, the ISP should have a static route pointing to the corporate's public Network with the relevant class A, B, C mask
    - a private network address, the ISP should have a static route pointing to the corporate's public NAT Pool with relevant mask
- Do not configure the ISP router with a routing protocol advertising the corporate's network

OSPF Configuration ONLY if Specified

- Configure on Internal Penza Router

router OSPF 9 (9 is just a process id, routers may use different process ids)
network **?.?.?.?** ?.?.?.? area 0 (VLAN 315, ospf routers exchange updates with routers in the same area)
network **?.?.?.?** ?.?.?.? area 0 (VLAN 143, **?** wildcard is inverse of subnet mask)
network **?.?.?.?** ?.?.?.? area 0 (VLAN 33 wildcard is inverse of subnet mask)
network **?.?.?.?** ?.?.?.? area 0 (Serial Link – Penza to Tambov)
passive-interface *interface* (As appropriate to avoid unnecessarily sending routing information)

- Configure on Internal Gateway Tambov Router

router OSPF 10
network **?.?.?.?** ?.?.?.? area 0 (Loopback Database LAN)
network **?.?.?.?** ?.?.?.? area 0 (Serial Link – Penza to Tambov)
ip route **?.?.?.?** ?.?.?.? S0/1/1 (The default route to the Internet)
default-information originate (Advertise default route to other internal routers)
passive-interface *interface* (As appropriate to avoid unnecessarily sending routing information)

- Configure on External ISP Router (OSPF is not configured in ISP)

ip route **?.?.?.?** ?.?.?.? S0/1/1 (ISP configure a static route to Public NAT Pool)

EIGRP Configuration ONLY if Specified

- Configure on Internal Router

router EIGRP 15 (15 is the autonomous system number, both routers need to use the same number in order to exchange updates)

network **?.?.?.?>** ?.?.?.? (wildcard is inverse of subnet mask, **? means** insert)

“

passive-interface *interface* (As appropriate to avoid unnecessarily sending routing information)

- Configure on Gateway Router

router EIGRP 15

network **?.?.?.?** ?.?.?.? (wildcard is inverse of subnet mask, **? means** insert)

“

ip route 0.0.0.0 0.0.0.0 S0/1/1 (The default route to the Internet)

redistribute static (Advertise default route to other internal routers)

passive-interface *interface* (As appropriate to avoid unnecessarily sending routing information)

- Configure on ISP Router (EIGRP is not configured in ISP)

ip route **?.?.?.?** ?.?.?.? S0/1/1 (ISP configure a static route to Public NAT Pool)

Inter-VLAN Routing Configuration

- Configure on the required Router

```
interface G0/0/1
 description The Physical Interface
 no shutdown

    interface G0/0/1.33
     description A logical Sub Interface
     description VLAN 33 VLAN Management
     encapsulation dot1q 33
     ip address  address   subnet mask


   interface G0/0/1.vlan id
    description A logical Sub Interface
    description VLAN vlan Id  vlan name
   encapsulation dot1q vlan id
   ip address  address   subnet mask

  etc ……
```

Switch Configuration

- Configure VLANs

```
vlan 315
  name Cows
vlan 143
  name Sheep
vlan 615
  name Goats
```

- Configure IP address for management vlan

interface VLAN 33
ip address *address mask* (This allows the switch to be configured remotely via Telnet)

- Configure Default Gateway

ip default-gateway *ip address of router interface* (Use VLAN 33 subinterface IP address)

Switch Configuration

- Configure a switch ACCESS port (note you can specify a range of switch ports):

  interface fa 0/3 (or interface range fa 0/3 – 5)
  switchport access vlan <*number*> (assigns port to a vlan)
  switchport mode access (sets port to access, for PCs)
  switchport port-security (enables port security, do not forget this command)

  switchport port-security maximum 1 (maximum of 1 mac address(es) can stick)
  switchport port-security mac-address sticky
  switchport port-security violation shutdown (shuts down port, default when security turned on)
  OR
  switchport port-security violation protect (protects, but does not shut down the port)

- Configure a static MAC address entry in Mac Address Table

  mac address-table static AAAA.BBBB.CCC vlan 143 interface fa 0/24
  (replace AAAA.BBBB.CCCC with the mac address of the PC)

Switch Configuration

- Configure a switch TRUNK port (three types of switch available)
- **Rooms ATC315 and ATC329**

2960 Series Switch

```
interface G0/1
 switchport mode trunk (sets port to trunk)
```

3650 Series Switch

```
interface G0/1
 switchport mode trunk (sets port to trunk)
```

- **Room ATC330**

2960 Series Switch

```
interface Fa0/1
 switchport mode trunk (sets port to trunk)
```

3560 Series Switch

```
interface Fa0/1
 switchport trunk encapsulation dot1q (must specify 802.1q encapsulation)
 switchport mode trunk (sets port to trunk)
```

Switch Commands

Managing the MAC Address Table

- show mac address-table (displays entries in table)
- show mac address-table dynamic (displays only dynamic entries in table)
- clear mac address-table (deletes all entries from table)
- clear mac address-table dynamic (deletes only dynamic entries from table)

Re-activating a switch port that has been violated

- When a violation causes a switch port to block traffic, it must be re-activated
- This is achieved by doing a **shutdown** then a **no shutdown** on the switch port, refer below:

```
interface fa0/10
 shutdown
 (wait until shutdown confirmed)
no shutdown
```

Frame Relay Configuration

- Configure on Penza Router

```
interface serial 0/1/0
  ip address ?.?.?.?  ?.?.?.?
  encapsulation frame-relay ietf  (turns on frame relay encapsulation)
  ip ospf network point-to-point (include ONLY if your are using OSPF)
  no keepalive  (as this is a point-to-point link and not via a WAN switch, no keepalive messages are sent)
  no frame-relay inverse-arp
  frame-relay map ip    next hop ip address   111 ietf broadcast  (static mapping)
```

- Configure on Tambov Router

```
interface serial 0/1/0
  ip address ?.?.?.?  ?.?.?.?
  encapsulation frame-relay ietf
  ip ospf network point-to-point (include ONLY if your are using OSPF)
  no keepalive
  no frame-relay inverse-arp
  frame-relay map ip    next hop ip address 111 ietf broadcast
```

- Notes
  - **111** the data-link connection identifier (DLCI) identifies the logical virtual circuit (VC)
  - **broadcast** if you use dynamic routing protocols across the link

- Trouble Shooting Commands
  - debug frame-relay events
  - show frame-relay map
  - show frame-relay pvc

PPP Configuration

- **Configure on Router Tambov**

```
interface S0/1/1
  description Link to ISP
  ip address address subnet mask
  encapsulation ppp
  no shutdown
```

- **Configure on Router ISP**

```
interface  S0/1/1
  description Link to Tambov
  ip address address subnet mask
  encapsulation ppp
  no shutdown
```

- **PPP Trouble Shooting Commands**

  – debug ppp negotiation
  – debug ppp packet

CHAP Configuration – Create User Accounts

- **Configure on Router Tambov**

```
username ISP password cisco    (username and password are case sensitive)

interface S0/1/1
 ppp authentication chap
```

- **Configure on Router ISP**

```
username Tambov password cisco

interface S0/1/1
 ppp authentication chap
```

- **The Password Problem**

  – You need to ensure the password does not have spaces at the front or the end else the authentication will fail

- **PPP Trouble Shooting Commands**

  –debug ppp authentication

PC Command Window
Useful Trouble Shooting Commands

- ipconfig
  - Allows you check your PC's addresses
  - ipconfig /all
  - ipconfig /? for help
  - To request the DHCP server to release or renew the PC's IP address use:
    - ipconfig /release, ipconfig /renew

- netstat
  - Displays the TCP/IP network protocol statistics and information
  - netstat –a
  - netstat –e
  - netstat –s
  - netstat /? for help

- nbtstat
  - Displays protocol statistics and current TCP/IP connections
  - nbtstat –n
  - nbtstat /? for help

PC Command Window
Useful Trouble Shooting Commands

- arp
  - Displays the Address Resolution table
  - arp -a
  - arp /? for help
- route print
  - Displays the routing table of your PC
  - route /? for help
- ping
  - ping 127.0.0.1 Checks your PC's IPv4 Protocol stack
  - ping 192.168.1.10 ping a destination
  - ping /? for help
- tracert
  - Traces individual hops to the destination
  - tracert 192.168.1.10
  - tracert /? for help

By passing the startup configuration on boot up

I would ask all students to change the **configuration register** on each router via:

router(config)# config-register 0x2142

Why?

Changing the config register will ensure that from then on the router will bypass the startup configuration on boot up.

This means you will not have to first erase someone else's configuration or do a password recovery, saving time and hassle.

However you can still load the startup configuration if you want to use it.

Try this Example:

! Configure router with name Melb

router#config t

router(config)#hostname Melb

router(config)#end

Melb#

! To change the router's register so that it bypasses the startup-configure

config t

Melb(config)# config-register 0x2142

Melb(config)#end

! To check that the register will be changed

Melb# show version

! Save configuration

Melb# copy running-configure startup-configure

! Turn router off

! Turn router on, it will bypass startup-configure and will boot up un-configured eg

router>

! RELOAD Startup Configuration from NVRAM, if you **DO** want to use it

router>enable

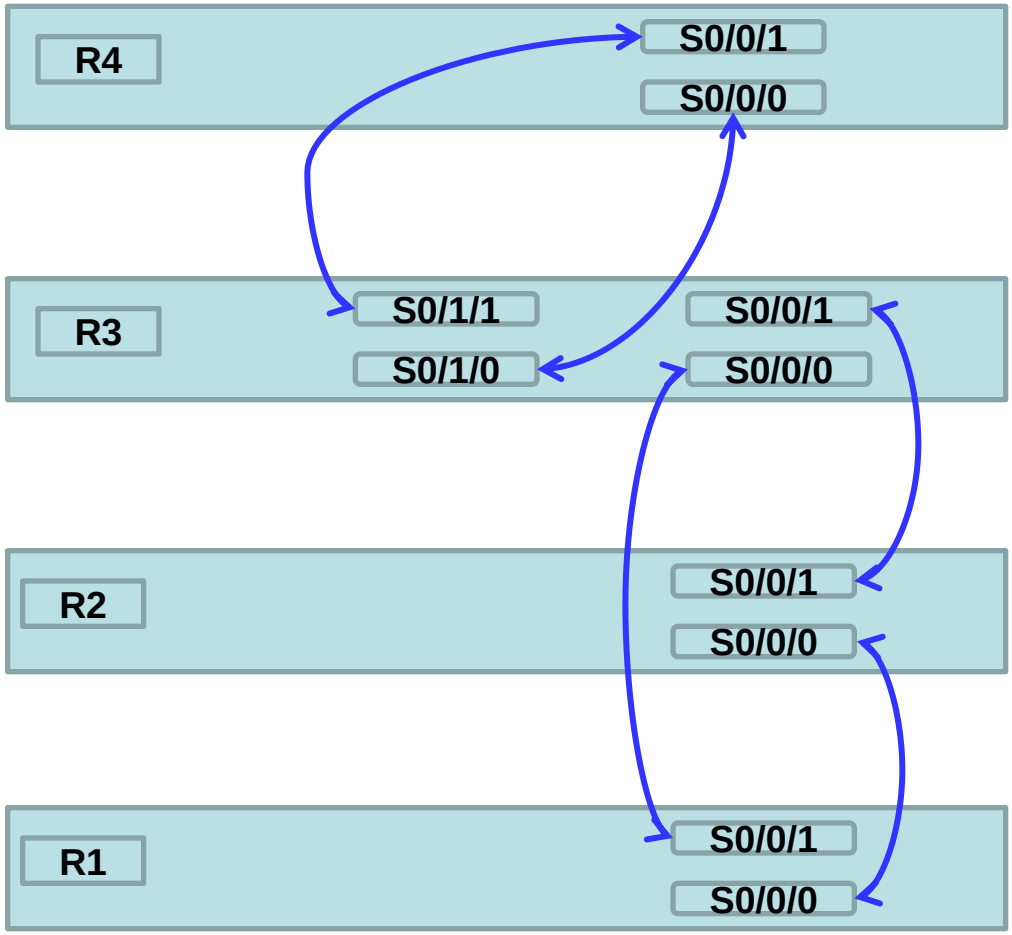
router#

router#copy startup-configure running-configure

Melb#

Kit - Router Serial Cable Mapping

Room ATC330



Students are NOT allowed to remove serial cables, as removal often causes damage to the serial interface. If you believe a serial interface is not working, please inform your instructor !