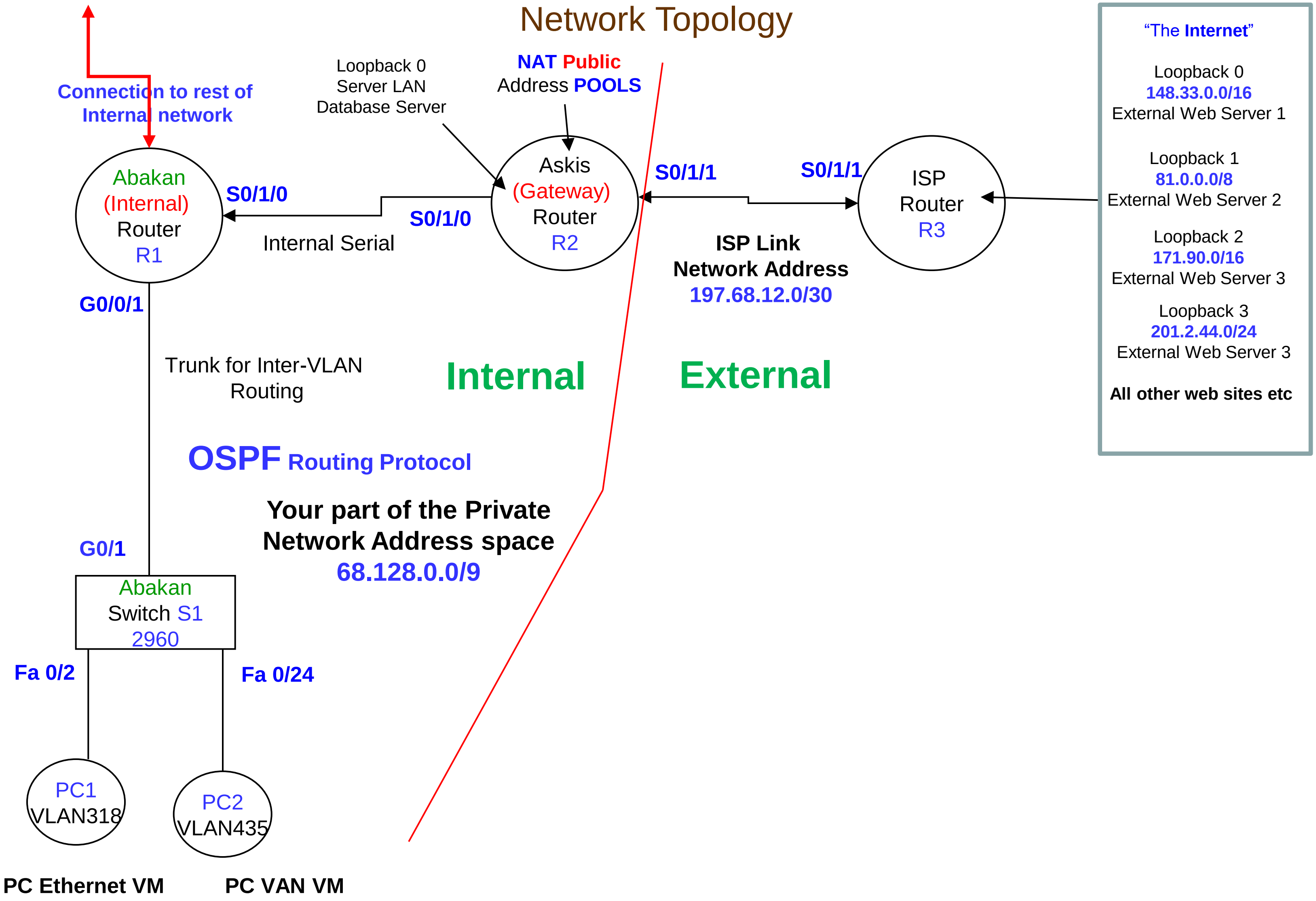
Scenario 5 (6 marks) - DHCP, NAT V2.3

A Network Configuration and Trouble Shooting Scenario

Network Topology


Connection to rest of Internal network
Abakan (Internal) Router R1
S0/1/0
Internal Serial
S0/1/0
Loopback 0 Server LAN Database Server
NAT Public Address POOLS
Askis (Gateway) Router R2
S0/1/1
S0/1/1
ISP Router R3
ISP Link Network Address 197.68.12.0/30
"The Internet"
Loopback 0 148.33.0.0/16 External Web Server 1
Loopback 1 81.0.0.0/8 External Web Server 2
Loopback 2 171.90.0/16 External Web Server 3
Loopback 3 201.2.44.0/24 External Web Server 3
All other web sites etc
G0/0/1
Trunk for Inter-VLAN Routing
Internal
External
OSPF Routing Protocol
Your part of the Private Network Address space 68.128.0.0/9
G0/1
Abakan Switch S1 2960
Fa 0/2
Fa 0/24
PC1 VLAN318
PC2 VLAN435
PC Ethernet VM
PC VAN VM

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.

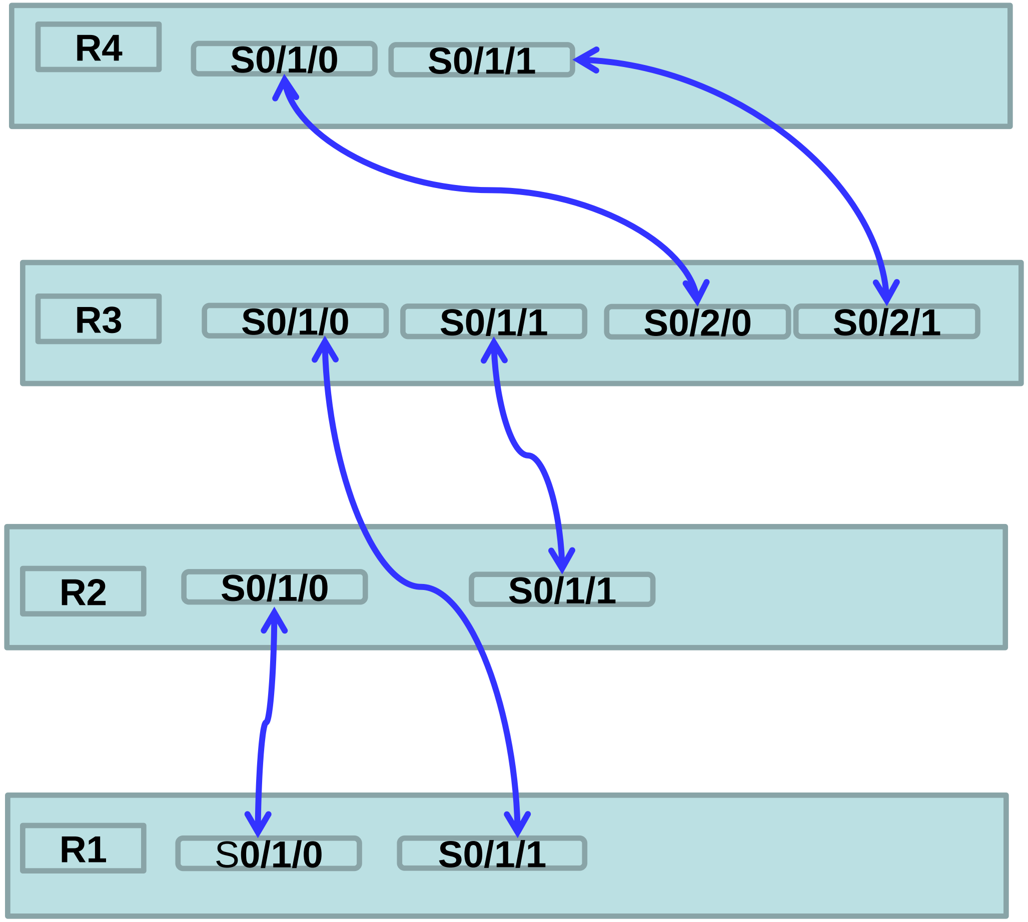
- This approach is designed to prepare you (given the complexity of the network you will be required to build) for the Skills Exam.

Scenario 5 - Introduction

- This scenario can be completed independent of the lecture material as configuration details are provided on pages 14 to 25
- 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 **DHCP** (**D**ynamic **H**ost **C**onfiguration **P**rotocol) on an internal router to provide ip address details to the internal LAN subnets
  - You will configure **NAT** (**N**etwork **A**ddress **T**ranslation) on the gateway router to map internal private ip addresses to public ip addresses allowing access to the Internet
  - ACLs to permit a subnet to **send ping replies** to a specified subnet
- Network Topology
  - Internal, your internal network
    - The Corporate Private Network Address, **68.0.0.0/8.**
    - The corporate address has been **divided up** and you have been given the address space **68.128.0.0/9** to build your part of the Corporate Network.
    - Do not configure the connection to the rest of the internal network
  - External, the link to the ISP and the Internet
    - The Internet is represented by a number of Loopbacks on the ISP
    - ISP Link Address, **197.68.12.0/30**
    - The NAT Public Address Pool, provided by the ISP is **132.14.0.0/24**

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 5 – Assessment

1. **Assessment due**
   - Scenario 5 will ONLY be assessed up to the end of your allocated Lab in week 10
   - Scenario 5 will NOT be assessed (no marks given) after your allocated lab in week 10
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 5 -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 **68.128.0.0/9** of Corporate Network Address space with:

- **VLAN 318** Blue 1000 hosts
- **VLAN 435** Green 20 hosts
- **VLAN 615** Yellow 180 hosts
- **Askis Database Server LAN** loopback 0 30 hosts,
- **VLAN 1** 14 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 318	68.128.0.0 /22	68.128.0.1 - 68.128.3.254
VLAN 435		
VLAN 615		
Database Server LAN		
VLAN 1		
Internal Serial		

Scenario 5 – **Task 2** Record IP Host Address Assignment

Askis	**IP Address/Prefix**	**Next Router**
S0/1/0		
S0/1/1		
Loopback 0		

Abakan	**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			

Abakan Switch	**IP Address/Prefix**	**Gateway IP Address**
VLAN 1		

Scenario 5 -Tasks

3. On each router, ensure router config-register is set to 0x2142: router(config)# config-register 0x2142 (refer page 28)

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 Abakan router to switch port G0/1

b) Check routers are connected via serial links (refer 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 5 -Tasks

9. **Switch Configuration**

- **a)** Refer to pages **24 to 27** 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 318 Blue, VLAN 435 Green, VLAN 615 Yellow
- **d)** Configure G0/1 as a **trunk port**
- **e)** Configure as **access ports**, only VLAN 318 ports 2,3 and VLAN 435 port 24
- **f) Switch Management –** configure an ip address on interface VLAN 1 and configure a default gateway
- **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 318 , mac address sticky on ports 2,3 max 4, with **violation protect**
- **i)** Configure a static mac address, VLAN 435, 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 5 -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) **Abakan Router**

i) **Inter-VLAN Routing Configuration**

- Refer page **23** and to **your journal** and lab exercises from prior unit on **Basic Inter-VLAN Routing**
- Configure **Inter-VLAN Routing** on G0/0/1
- Create separate sub-interfaces for VLANs 1, 318 and 435
- Assign each sub-interface with an ip address

c) **PC Configuration with static IP address**

i) Configure PC1 and PC2 with IP addresses

d) **Abakan 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 5 -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 Testing

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

b) Ping PC1 – VLAN 318 to PC2 – VLAN 435

c) Ping PC1 – Switch 1

d) On Abakan Router – show arp, to check the IP address to MAC address mapping

16. Routing Protocol Configuration (refer pages **21,22**)

a) Abakan

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

b) Askis

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

Scenario 5 -Tasks

16. 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**

17. 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:

- Internal routers, routing protocol is not advertising a subnet
- An interface is down
- Default route not configured on Askis
- Default route not advertised by Askis

18. 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 Askis router to check ping request arrives

c) Ping from PC Hosts in VLAN 318 and VLAN 435 to **Database Server** on Askis

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 advertised

Scenario 5 - Tasks

19. NAT Configuration

a) Configure NAT Pools on the **Askis router**

- Refer to page **20** and **Lab on NAT Configuration**
- Create separate NAT Pools and ACLs for VLANs 1, 318, 435

b) ISP Router

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

20. 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 Askis to watch NAT translations

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

d) Ping from PC Hosts in VLAN 318 and VLAN 435 **to the Internet – pick an External Web Server**

e) Ping from Switch **to the Internet – pick an External Web Server**

f) 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

g) Useful commands, use - **show ip nat translations, debug ip nat, debug ip icmp**

21. DHCP Configuration – Dynamic IP address allocation

- Configure DHCP on **Abakan**
- Refer to page **19** and **Lab on DHCP Configuration**
- Create separate DHCP Pools for VLANs 318 and 435
- Exclude the first three IP addresses
- Configure PC1 and PC2 to obtain IP address automatically

22. Trouble Shooting DHCP

a) Use **debug ip dhcp server events** on Abakan 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**

Scenario 5 - Tasks

23. **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**.

24. **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 5 - Tasks

25. Access List Requirements

a) Refer to pages **14 to 18** and **Lab Exercises on Access Control Lists**

b) You must create a **NAMED** Extended ACL for VLAN 318 based on following requirements:

- PCs in VLAN 318 permitted **HTTP** access to an External Web Server (you choose one) and denied **ALL** other access to that External Web Server.
- PCs in VLAN 318 denied **PING** request to PCs in VLAN 435
- PCs in VLAN 318 permitted **PING** reply to PCs in VLAN 435
- PCs in VLAN 318 permitted **ALL** access to the Internet – all the other External Web Servers
- **ALL** means **IP**

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

- ONLY PCs in VLAN 318 permitted **TELNET** access to Abakan Router
- ONLY PCs in VLAN 318 denied **TELNET** access to Askis Router

d) 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 318 using the template on page **16**, refer Task 25
ii) **Test** the ACL for VLAN 318 refer Task 26

iii) **Create** a **NAMED** Standard ACLs for Telnet access using the template on page **17**, refer Task 25
iv) **Test** the ACLs for Telnet access refer Task 26

Scenario 5 - Tasks

26. 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 aclvan318 and Aclvlan318 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 structure:

```
! Deletes previous version of access list
  no  ip access-list extended ACLVLAN<Id>
 ! Insert Latest version of access list
  ip access-list extended ACLVLAN<Id>

              <Your  ACL rules>

 ! 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

27. 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 318 on Abakan Router

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

no ip access-list extended ACLVLAN318 (Delete previous version of the ACL for VLAN 318)
ip access-list extended ACLVLAN318 (Self-documenting, the ACL for VLAN 318, ! 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 435 subnet
permit  icmp  source subnet   wildcard   destination subnet   wildcard echo-reply

! Deny PING request to a destination - PCs in VLAN 435  subnet
 deny icmp source subnet   wildcard   destination subnet   wildcard

! Permit access to The Internet
permit  ip      any   any
```

ACL Placement - On Sub Interface G0/0/1.318 on Abakan Router

```
interface G0/0/1.318
ip access-group ACLVLAN318 in
```

ACL Templates

ACL to control Telnet Access to Abakan and Askis Routers

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

```
! On Abakan
no ip  access-list  standard  ACLTELNET
ip  access-list  standard  ACLTELNET
! Permit VLAN318 Telnet Access to Abakan
    permit    source subnet    wildcard
    deny any

! On Askis
no ip  access-list  standard  ACLTELNET
ip  access-list  standard  ACLTELNET
! Deny VLAN318 Telnet Access to Askis
    deny    source subnet    wildcard
    permit any
```

Interface Placement - line vty 0 4, on Abakan and Askis Routers

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

ACL Overview

ACL Case Sensitivity

- ACL names are case sensitive eg aclvlan318 and AclVlan318 are **different** ACLs
- Should decide to use either all uppercase - ACLVLAN318 or all lowercase – aclvlan318 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 Commands

- show access-lists
- clear access-list counters

DHCP Configuration

- **Configure on Router Abakan**

```
service dhcp  (turns on DHCP service)

ip dhcp pool poolVLAN318
    network  subnetwork  subnetwork mask
    default-router  ip address of G0/0/1.318

ip dhcp pool poolVLAN435
   network subnetwork  subnetwork mask
   default-router  ip address of G0/0/1.435
```

- **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** (release IP Address)
    - **ipconfig /renew** (renew IP address)

NAT Configuration

- **Configure ONLY on Router Askis**
  - The NAT Public Address Pool, provided by the ISP is **132.14.0.0/24, this is a range of Ip addresses,** divide 3 ways, do not VLSM
  - **Nat Pools for each VLAN**

```
ip nat pool POOLVLAN318   starting IP address   ending IP address   netmask ?.?.?.?
ip nat pool POOLVLAN435   starting IP address   ending IP address   netmask ?.?.?.?
ip nat pool POOLVLAN1     starting IP address   ending IP address   netmask ?.?.?.?
```

  - **NAT Access Control Lists**

```
ip access-list extended ACLVLAN318
   permit  ip    source subnet   wildcard   any
ip access-list extended ACLVLAN435
   permit  ip    source subnet   wildcard   any
ip access-list extended ACLVLAN1
   permit  ip    source subnet   wildcard   any
```

  - **Establish dynamic source translation by binding the pools to the access control lists**

```
ip  nat   inside  source  list   ACLVLAN318      pool  POOLVLAN318
ip  nat   inside  source  list   ACLVLAN435      pool  POOLVLAN435
ip  nat   inside  source  list   ACLVLAN1        pool  POOLVLAN1
```

  - **Specify inside and outside NAT interfaces**

```
interface  serial 0/1/0
  ip nat inside
interface serial 0/1/1
   ip nat outside
```

- **Trouble Shooting Commands**
  - show   ip nat   translations
  - clear   ip nat   translation * (use this to allow you to delete pools)
  - 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

- Configure on Internal Abakan Router

```
router OSPF 18 (18 is just a process id, routers may use different process ids)
  network ?.?.?.? ?.?.?.?  area 0 (VLAN 318, ospf routers exchange updates with routers in the same area)
  network ?.?.?.? ?.?.?.?  area 0  (VLAN 435, ? wildcard is inverse of subnet mask)
  network ?.?.?.? ?.?.?.? area 0 (VLAN 1 wildcard is inverse of subnet mask)
  network  ?.?.?.? ?.?.?.? area 0 (Serial Link – Abakan to Askis)
  passive-interface  interface (As  appropriate to avoid unnecessarily sending routing information)
```

- Configure on Internal Gateway Askis Router

```
router OSPF 19
  network ?.?.?.? ?.?.?.?  area 0 (Loopback Database LAN)
  network ?.?.?.? ?.?.?.?  area 0 (Serial Link – Abakan to Askis)
  ip route 0.0.0.0  0.0.0.0   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)
```

Inter-VLAN Routing Configuration

- Configure on the required Router

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

    interface G0/0/1.1
     description A logical Sub Interface
     description VLAN 1 VLAN Management
     encapsulation dot1q 1
     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 318
   name Blue
 vlan 435
    name Green
 vlan 615
    name Yellow
```

- Configure IP address for management vlan

```
interface vlan 1
  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 1 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 435 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 ATC238 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
```

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?

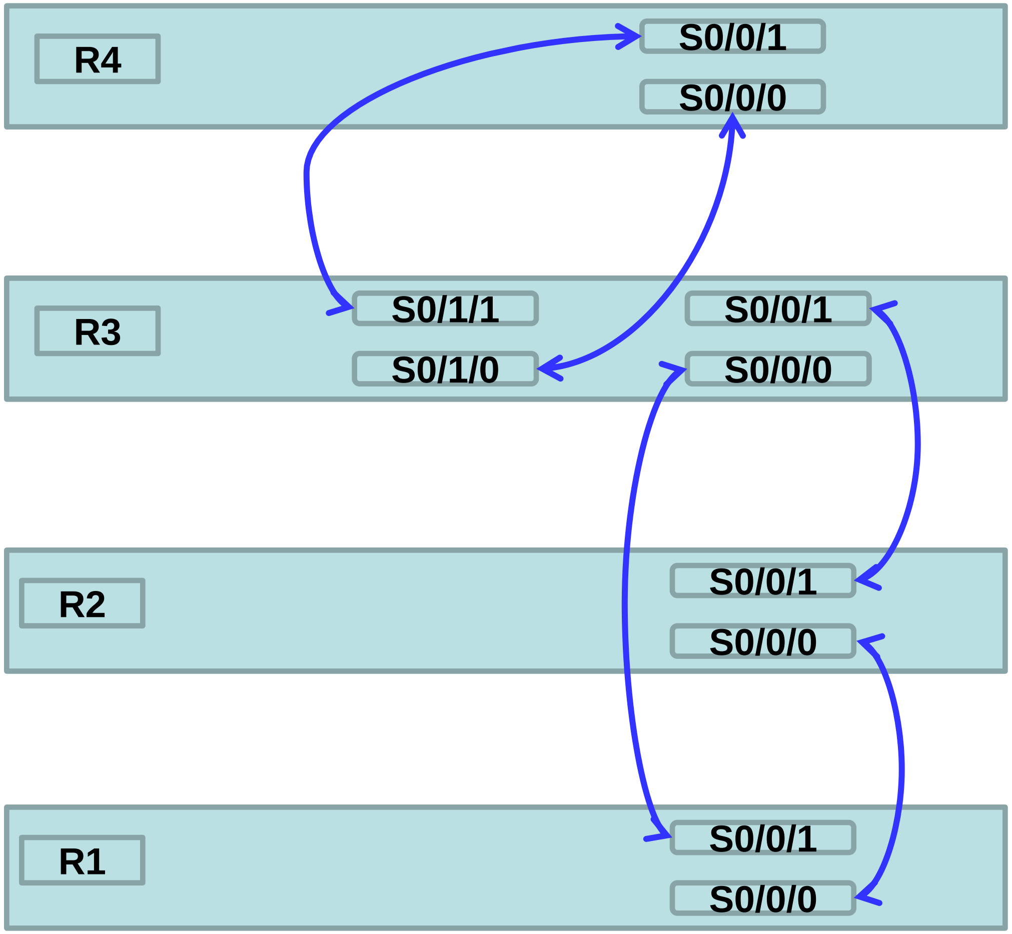
Changing the config register will ensure that from then on the router will bypass the startup configuration on boot up. This means you will not have to first erase someone else's configuration or do a password recovery, saving time and hassle. However you can still load the startup configuration if you 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 !