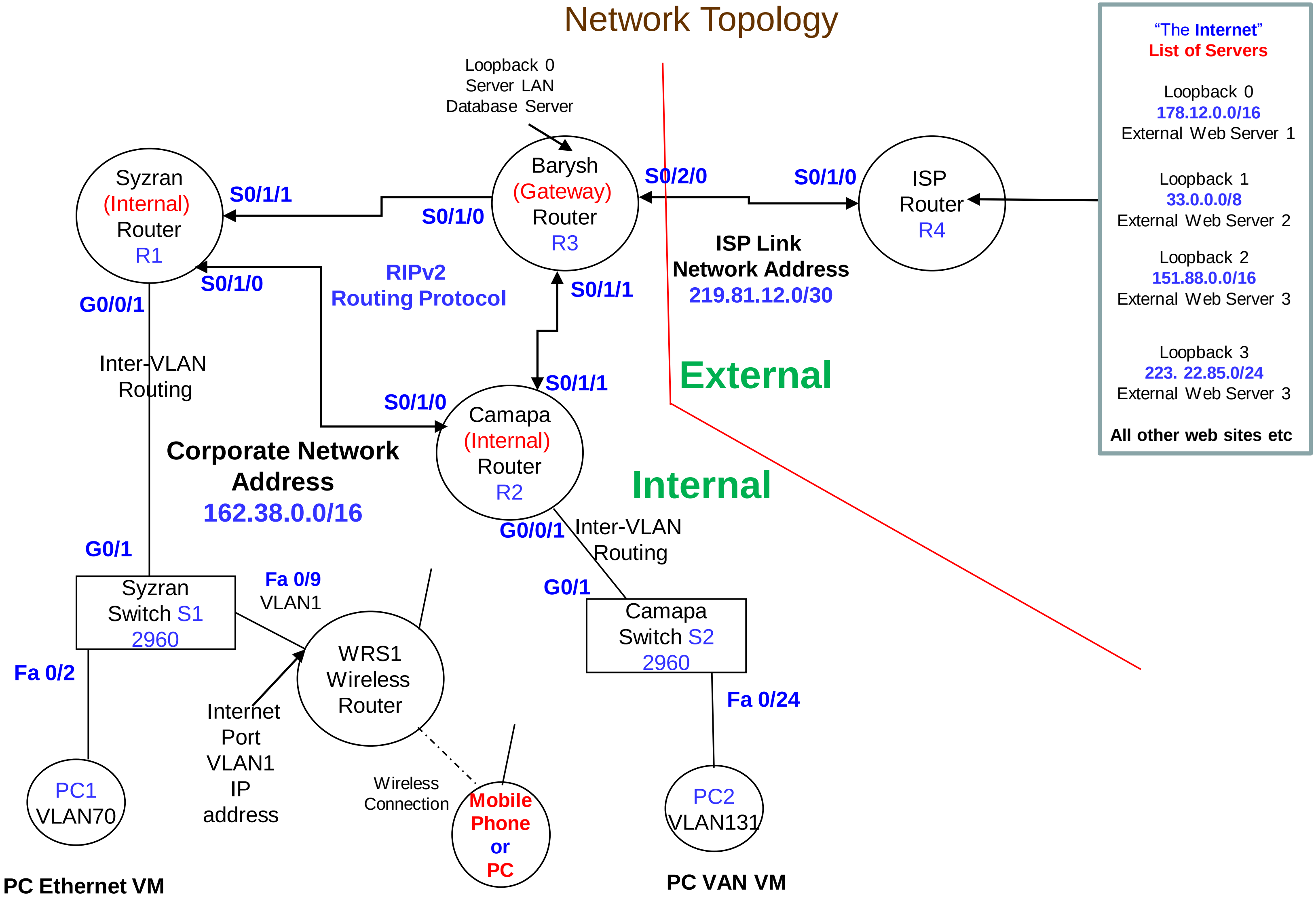
Scenario 2 – RIP, ACLs, Wireless V2.4

A Network Configuration and Trouble Shooting Scenario

Network Topology



Loopback 0
Server LAN
Database Server

Syzran (Internal) Router R1

S0/1/1

S0/1/0

Barysh (Gateway) Router R3

S0/2/0

S0/1/0

ISP Router R4

ISP Link Network Address 219.81.12.0/30

S0/1/0

G0/0/1

RIPv2 Routing Protocol

S0/1/1

S0/1/1

S0/1/0

Inter-VLAN Routing

Camapa (Internal) Router R2

External

Internal

Corporate Network Address 162.38.0.0/16

G0/0/1

Inter-VLAN Routing

G0/1

Syzran Switch S1 2960

Fa 0/9 VLAN1

WRS1 Wireless Router

G0/1

Camapa Switch S2 2960

Fa 0/2

Internet Port VLAN1 IP address

Wireless Connection

Fa 0/24

PC1 VLAN70

Mobile Phone or PC

PC2 VLAN131

PC Ethernet VM

PC VAN VM

"The Internet"
List of Servers

Loopback 0
178.12.0.0/16
External Web Server 1

Loopback 1
33.0.0.0/8
External Web Server 2

Loopback 2
151.88.0.0/16
External Web Server 3

Loopback 3
223. 22.85.0/24
External Web Server 3

All other web sites etc

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 2 - Introduction

- This scenario can be completed independent of the lecture material as configuration details are provided on pages 13 to 21

- Your tutor 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?**
  - Creating and testing a backup path to the gateway router
  - You will configure ACLs (Access Control Lists) to control the flow of traffic from each of the VLANs.
  - ACLs are introduced early in the semester to give you time to appreciate their usefulness in managing the flow of IP traffic and the testing that is required to ensure they perform correctly
  - You will be creating and using NAMED **extended** ACLs, eg:

    ```
    ip access-list extended ACLVLAN70
    ```

    This means the ACL is self-documenting, the above is the ACL for VLAN 70

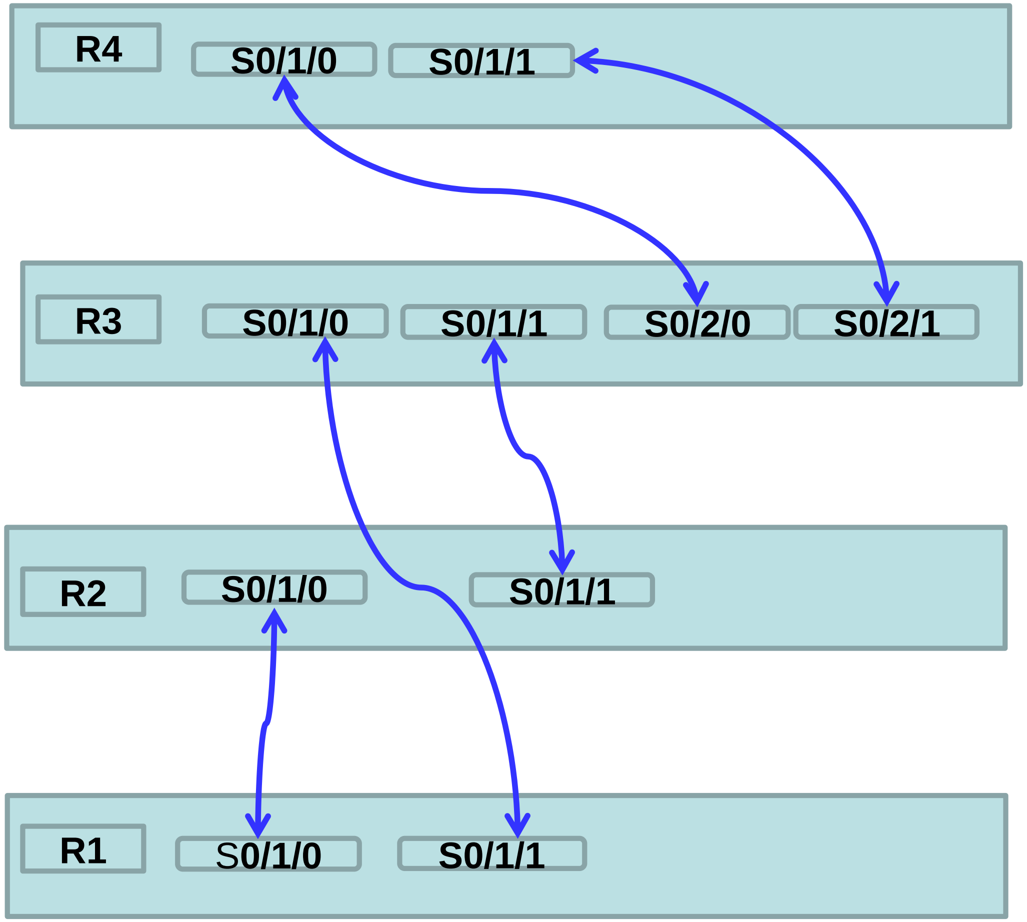
- Network Topology
  - Internal, your internal network
  - External, the link to the ISP and the Internet
  - The Internet is represented be a single Loopback
  - Corporate Network Address, **162.38.0.0/16**
  - ISP Link Address, **219.81.12.0/30**

Scenario 2 – Assessment

1. **Assessment due**
   - Scenario 2 will ONLY be assessed up to the end of your allocated Lab in week 4
   - Scenario 2 will NOT be assessed (no marks given) after your allocated lab in week 4
2. Scenarios must be completed individually
3. **Assessment Process**
   - Assessment is **ONLY** by in person interview, with **your** tutor, **ONLY** during **your allocated** Lab time.
   - You must demonstrate your running network
   - 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**
   - Demonstrate on Lab Kit - Up to 1 Unit Mark will be given
   - Demonstrate using Packet Tracer - Up to 0.5 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**

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 tutor !

Scenario 2 -Tasks

1. On each router, ensure router config-register is set to 0x2142: router(config)# config-register 0x2142 (refer page 25)

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

3. Internal Network VLSM Design

a) Design IP VLSM Addressing Scheme with following requirements::

i. Switch S1 **VLAN 70** Shirts 250 hosts and **VLAN 1** 18 hosts

ii. Switch S2 **VLAN 131** Hats 100 hosts, **VLAN 150** Sandals 50 hosts, **VLAN 1** 18 hosts

iii. 3 **Internal Serials** 2 hosts each

iv. Barysh **Database Server LAN** loopback 0 40 hosts

b) Document assignment of ip addresses to router interfaces and PC Hosts

c) You can use a VLSM calculator

4. 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 images !!**

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

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

5. Cable Connection

a) Connect Syzran router to switch S1 port G0/1

b) Connect Camapa router to switch S2 port G0/1

c) Check routers are connected via serial links (refer page 4)

d) Connect PC1 to switch S1 Fa 0/2 using the patch panel, connect PC2 to switch S2 Fa 0/24 using the VAN

6. 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)
```

7. 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 2 -Tasks

8. Switch Configuration

- **a)** Refer to pages 18 to 21 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)** On switch S1
  - i. create VLAN 70 Shirts
  - ii. configure ports 2,3 as VLAN 70 access ports
  - iii. configure Port Security, mac address sticky on ports 2,3 max 4, with **violation shutdown**
- d) On switch S2
  - i. create VLAN 131 Hats, VLAN 150 Sandals
  - ii. configure port 24 as VLAN 131 as access port
  - iii. configure a static mac address, VLAN 131, on Fa 0/24 to the MAC address of PC2
- **e)** On both switches configure G0/1 as a **trunk** port
- **f) Switch Management –** on both switches 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 accessed via Telnet

9. Trouble Shooting VLANs

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

10. 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

11. Network IP Address Configuration

- **a)** Configure **ALL** router **serial** and **loopback** interfaces with ip addresses
- **b) Syzran and Camapa Routers**
  - i) Refer page 17 and to **your journal** and lab exercises from prior unit on **Basic Inter-VLAN Routing**
  - ii) Configure **Inter-VLAN routing** on G0/0/1
    - Syzran configure separate sub-interfaces for VLAN 1 (the management VLAN) and VLAN 70
    - Camapa configure separate sub-interfaces for VLAN 1 (the management VLAN) and VLAN 131
    - Configure each **sub-interface** with an ip address
- **c)** Configure PC1 and PC2 Hosts with specified VLAN:
  - i) IP address and subnet mask.
  - ; ii) Default Gateway IP address.
- **d) Check** default gateway configured on both switches

Scenario 2 -Tasks

12. Trouble Shooting Trunking – between each Switch and its Router

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

b) Check correct interface has been configured for trunking !

13. 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.
- 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.

14. Trouble Shooting Inter-VLAN Routing Test

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

b) PC1 ping VLAN 1 ip address of Switch S1, PC1 telnet to Switch S1

c) PC2 ping VLAN 1 ip address of Switch S2, PC2 telnet to Switch S2

15. Routing Protocol Configuration (refer pages 15,16)

a) Syzran and Camapa

- RIP V2
- Configure passive-interface as appropriate to avoid sending unnecessary routing information

b) Barysh

- RIP V2, 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 internal routers

c) ISP Router

- **Do not configure RIP**
- **Only** configure a static route (default class B mask) to your internal network
- Configure loopbacks for Web Servers (If you are using Packet Tracer may need to use Server Devices)

Scenario 2 -Tasks

16. 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) External Router

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

- Check there is static route back to your internal network

c) Common problems:

- Routing protocol is not advertising a subnet
- An interface is down
- Internal serial links, IP addresses/masks incorrect
- Static or Default route not configured

17. Trouble Shooting End-to-End Path Testing

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

b) Ping from PC1 Host in VLAN 70 to External Web Servers (the Internet)

c) Ping from PC2 Host in VLAN 131 to External Web Servers (the Internet)

d) Ping from PC1 Host in VLAN 70 to PC2 Host in VLAN 131

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

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

g) Check if a subnet is missing from a routing table, use - **show ip route**

h) End-to-End Path Test Failed ? - Common problems:

- Default gateway IP address not configured on a PC.
- PC connected to incorrect interface.
- Incorrect static route on ISP
- Subnet not advertised
- Default route not propagated/Gateway of last resort not set

18. Trouble Shooting Switch Management

a) To check that you have remote access to the switch(es)

b) From PC1 telnet to the switch(es)

Scenario 2 -Tasks

19. **Trouble Shooting** **Testing Backup Link**

a) On router Camapa determine current exit interface to destination Database Server Lan – **show ip route**

b) Shut down the interface

c) Did backup route install in the routing table ? – **show ip route**

20. **Wireless Router Configuration**

a) You will configure a Wireless Router and connect it to the fixed network infrastructure.

b) Refer to page **24** and **Wireless Supporting Material**

c) If you use your mobile phone as the wireless device to ping the Internet, you need to download ping utilities from your App store to your mobile phone

d) On WRS1 Wireless Router configure:

i) Internet Port with VLAN 1 IP address ii) SSID as W<*student id*> iii) DHCP to provide addresses for Wireless LAN PCs and your Mobile Phone iv) allow inbound ping requests v) **Do not** configure wireless security

e) Connect a straight through UTP cable between Syzran Switch S1 Fa 0/9 (port in VLAN1) and Internet Port (in VLAN1) on Wireless Router

f) VLAN 1 will carrier wireless traffic

g) On ISP Router use – **debug ip icmp**

h) From your Mobile Phone or Wireless PC, Ping the Internet, What source ip address is shown by the debugging?

21. **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 Web Servers and connect it to the ISP Router

c) **This allows you to test your ACLs using a Browser**.

Scenario 2 - Tasks

22. **Access List Requirements Syzran Router**

a) Refer **Lab Exercises on Access Control Lists**

b) You must create a **NAMED** Extended ACL for VLAN 70 based on following requirements:

- PCs in VLAN 70 denied **HTTP** access to an External Web Server (select one of the External Web Servers from the List) and permitted **ALL** other access to this External Web Server and the Internet
- PCs in VLAN 70 permitted only **HTTP** access to another External Web Server (select one of the External Web Servers from the List) and deny ALL other access to this External Web Server
- PCs in VLAN 70 denied all access to another External Web Server (select one of the External Web Servers from the List)
- PCs in VLAN70 permitted **ALL** access to the rest of The Internet.
- **ALL** means **IP**

c) 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 70 using the template on page 13, refer Task 23

ii) **Test** the ACL for VLAN 70 refer Task 24

23. **Creating and Configuring NAMED Access Lists on Syzran Router**

a) Refer **Lab Exercises on Access Control Lists**

b) Use **Notepad** to create your ACLs, note ACL names are **case sensitive** eg aclvan70 and Aclvlan70 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, refer template on page 13>

! 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, refer page 14.

f) Paste ACL from Notepad into router (router must be in global configuration mode)

g) Configure ACL on correct interface

Scenario 2 - Tasks

24. Trouble Shooting Access Lists on Syzran Router

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

Scenario 2 – ACL Templates

ACL for VLAN 70 on Syzran Router

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

no ip access-list extended ACLVLAN70 (Delete previous version of the ACL for VLAN 70)
Ip access-list extended ACLVLAN70 (Self-documenting, the ACL for VLAN 70, ! means comment)

! Rule 1 - Deny ONLY HTTP access to a selected External Web Server in the List
deny tcp source subnet wildcard (inverse of subnet mask) destination host ip address eq www

! Rule 2.1 - Permit ONLY HTTP access to a selected (different from Rule 1) External Web Server in the List
permit tcp source subnet wildcard (the inverse of subnet mask) destination host ip address eq www
! Rule 2.2 - Deny all other access to the External Web Server selected in Rule 2.1
deny ip source subnet wildcard (inverse of subnet mask) destination host ip address

! Rule 3 - Deny IP access to a selected (different from Rules 1,2) External Web Server in the List
deny ip source subnet wildcard (inverse of subnet mask) destination host ip address

! Rule 4 - Permit ALL other access
permit ip any any

ACL Placement - On Sub Interface G0/0/1.70 on Syzran Router

interface G0/0/1.70
ip access-group ACLVLAN70 in (This access list is filtering inbound ip traffic from VLAN 70 to the router)

Scenario 2 – ACL Overview

ACL Case Sensitivity

- ACL names are case sensitive eg aclvlan70 and AclVlan70 are **different** ACLs
- Should decide to use either all uppercase - ACLVLAN70 or all lowercase – aclvlan70 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 to other destinations
- Extended ACL – place as close as possible to source network or device, to block traffic early to reduce network congestion

ACL Trouble Shooting Commands

- show access-lists (shows all access lists)
- clear access-list counters (clears ip packet hits against a rule)
- Refer Task 24

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 should have a static route pointing to the corporate’s Network with the relevant class A, B, C default mask
- Do not configure the ISP router with a routing protocol advertising the corporate’s network

RIP Configuration

- Configure on Syzran Router

```
router rip
 version 2   (Version 2 supports VLSM)
 network 162.38.0.0 (Advertise the internal network)
 passive-interface G0/0/1.1  (Do not send routing updates to LAN subnets)
 passive-interface G0/0/1.70  (Do not send routing updates to LAN subnets)
```

- Configure on Barysh Router

```
ip route 0.0.0.0   0.0.0.0   S0/2/0   (The default route to the Internet)
router rip
 version 2
 network 162.38.0.0
 default-information originate   (Advertise default route to other internal routers)
 passive-interface loopback  0  (Do not send routing updates to Server LAN)
```

- Configure on Camapa Router

  What do you think ?

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

```
ip route 162.38.0.0   255.255.0.0   S0/1/0  (ISP configure a static route to internal network)
```

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 <dotted decimal> <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 <dotted decimal> <subnet mask>

    etc ……
```

Switch Configuration

- Switch S1 - Configure VLANs

```
vlan 70
   name Shirts
```

- Switch S2 - Configure VLANs

```
vlan 150
   name Sandals
vlan 131
   name Hats
```

- Switch S1 and S2

  - Configure IP address for management vlan

```
interface vlan 1
  ip address <ip address>  <mask>
```

  - 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 131 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
- 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

Setting up the Wireless Router – Linksys WRT300N

Also refer Wireless Supporting Material A and B

1. **Configuring Wireless Router**
   - a) Power UP wireless router (get a wireless router from your tutor)
   - b) Reset it to factory default – push reset button and hold until **blue** symbol flashes
   - c) Start up PC Ethernet VM, configure to obtain ip address automatically
   - d) Ethernet Connection – plug blue UTP cable from your PC into any Ethernet port (1 to 4) on the wireless router
   - e) Open DOS Command Window – type ipconfig /all to confirm PC Ethernet has been obtained an ip address from wireless router
   - f) Use a Browser to connect to factory default ip address 192.168.1.1 on the wireless router
   - g) Authentication – username: admin, password: admin
   - h) Wireless Router Setup
     - **i.** **Ensure** you always **click save** at the bottom of each screen
     - ii. Internet Setup
       - a. Internet Connection type: static IP
       - b. Assign an ip address from VLAN 1 address range
     - iii. Network Setup - DHCP
       - a. For Wireless PCs
       - b. Use 192.168.1.0 address space for wireless LAN
     - iv. Disable/Enable PC Ethernet LAN connection to pick up a new ip address from Wireless LAN address space
     - v. Use a Browser to re-connect to new (default gateway) ip address on the wireless router
     - vi. Security
       - a. Disable Firewall
     - vii. Wireless Wi-Fi Protected Setup
       - a. Wireless Configuration: manual
       - b. SSID: student Id

2. **Associating with Wireless Router, Use**
   - **a) Mobile Phone**
   - **b) OR Laptop, refer below:**
     - i. Associate with the wireless LAN broadcasting your student ID as its SSID
     - ii. Configure to obtain ip address automatically
     - iii. Open DOS Command Window – type ipconfig /all to confirm an ip address has been obtained from wireless router
     - iv. Ping default gateway on the wireless router to confirm connection is working

3. **Connecting Wireless Router to Network Infrastructure:**
   - a) Remove blue UTP cable from your PC, get a new blue UTP cable, plug into Internet Port
   - b) Connect new blue UTP cable to Desk Top coloured Enclosure port, then patch from patch panel to Syzran switchport Fa0/9

4. **Testing Connection**
   - a) From Mobile/Laptop Ping to default gateway for VLAN 1 to confirm the connection is working

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?

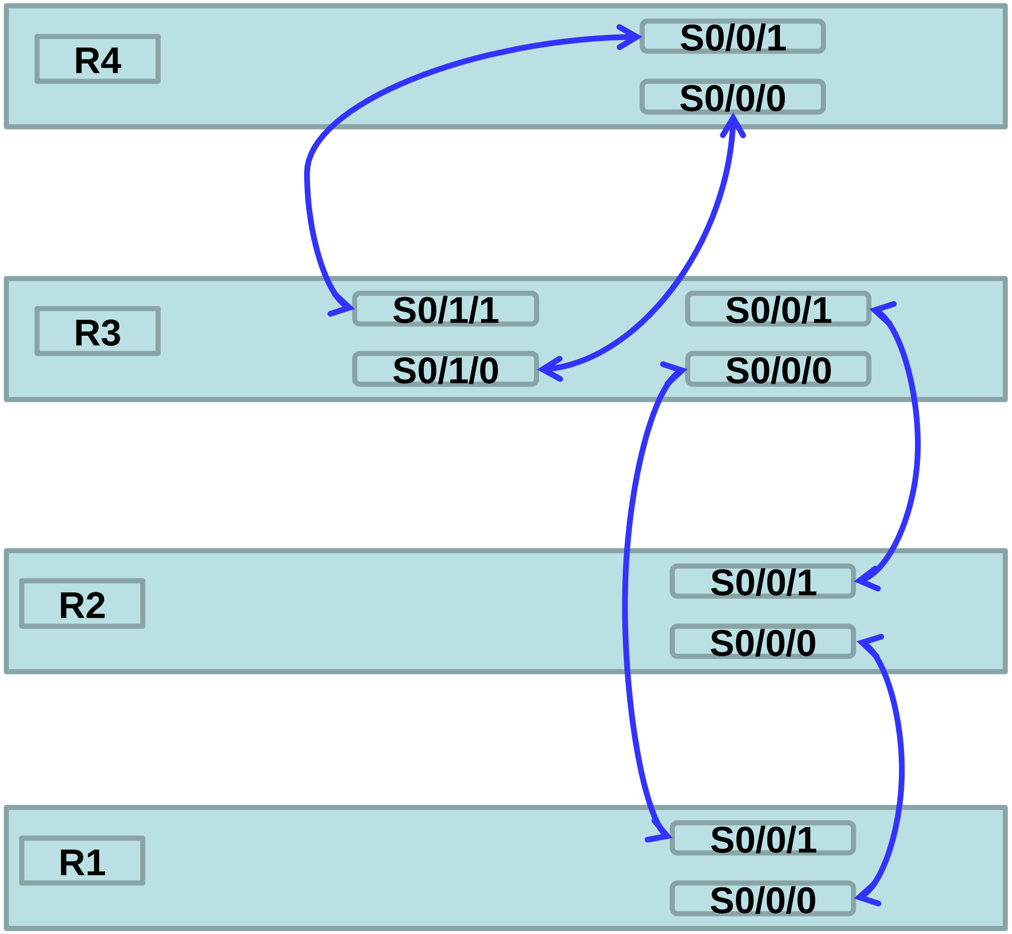
Changing the config register will ensure that from then on the router will bypass the startup configuration on boot up.
This means you will not have to first erase someone else's configuration or do a password recovery, saving time and hassle.
However you can still load the startup configuration if you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