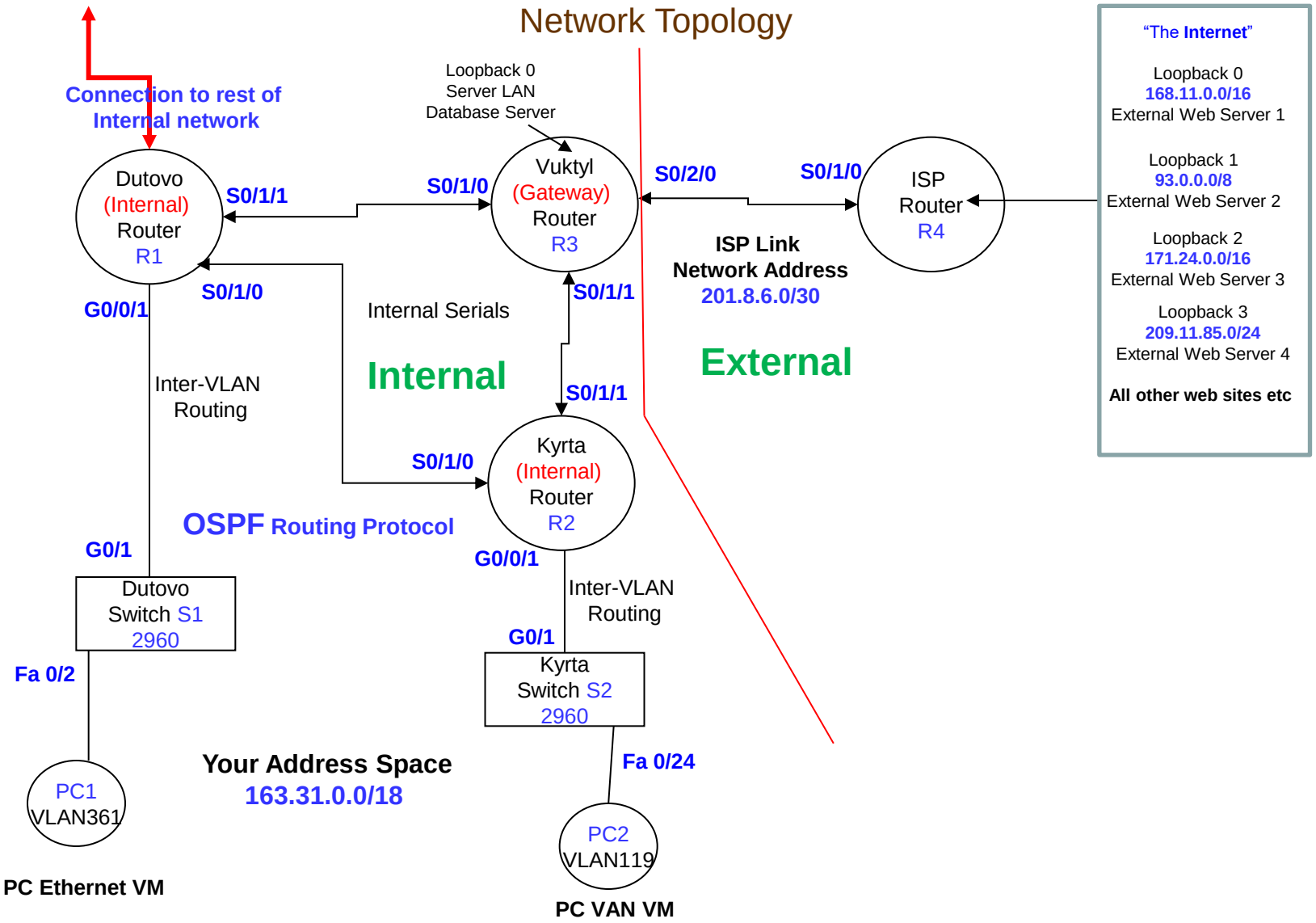
Scenario 4 (5 marks) - OSPF, ACLs, 4R V2.4

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 4 - Introduction

- This scenario can be completed independent of the lecture material as configuration details are provided on pages 13 to 23

- Your instructor will give you an overview of the scenario at the beginning of the lab

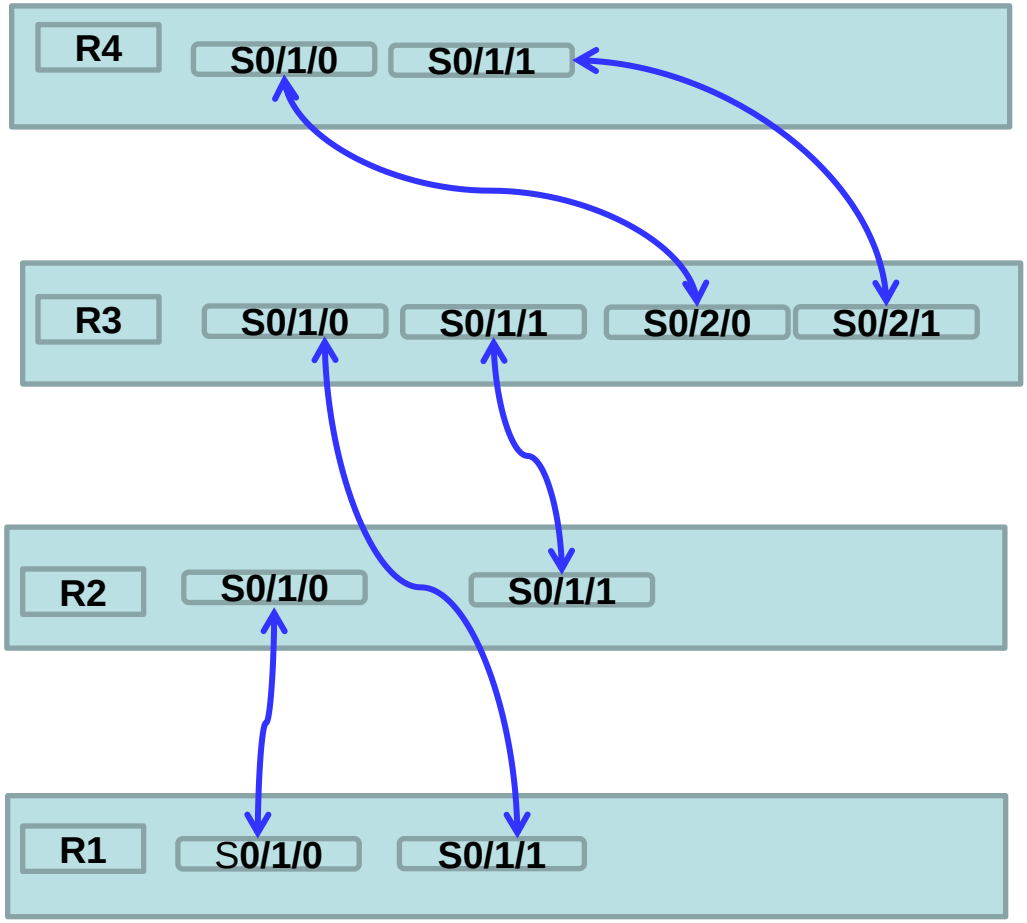
- As a How to Configure Guide, it is recommended you obtain a copy of “CCNA Portable Commands Guide (CCNA Self-Study) 2/3/4 Ed”, Scott Empson, Cisco Press

- **What is new?**
  - You will configure **OSPF** (Open Shortest Path First) Routing Protocol on the routers
  - ACLs to control pings between subnets

- Network Topology
  - Internal, your internal network
    - The Corporate Network Address, **163.13.0.0/16.**
      The corporate address has been **divided up** and you have been given the address space **163.31.0.0/18** to build your section 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, **201.8.6.0/30**

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 4 – Assessment

1. **Assessment due**
   - Scenario 4 will ONLY be assessed up to the end of your allocated Lab in week 9
   - Scenario 4 will NOT be assessed (no marks given) after your allocated lab in week 9
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 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**

Scenario 4 -Tasks

1. On each router, ensure router config-register is set to 0x2142: router(config)# config-register 0x2142 (refer page 26)

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

3. VLSM Design

a) Design IP VLSM Addressing Scheme with:

i. Switch S1 **VLAN 361** Sink 600 hosts, **VLAN 83** Management 18 hosts

ii. Switch S2 **VLAN 119** Tub 140 hosts, **VLAN 154** Shower 68 hosts, **VLAN 83** Management 12 hosts

iii. Vuktyl **Database Server LAN** loopback 0 20 hosts

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

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 Virtual 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 Dutovo router to Dutovo switch 1 port G0/1

b) Connect Kyrta router to Kyrta switch 2 port G0/1

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

d) Connect PC1 to Fa 0/2 using the patch panel, connect PC2 to 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 4 -Tasks

8. Switch Configuration

a) Refer to pages 20 to 23 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 361 Sink and VLAN 83 Management

ii. Configure ports 2,3 as VLAN 361 access ports

iii. Configure Port Security, mac address sticky on ports 2,3 max 2, with **violation protect**

d) On Switch S2

i. Create VLAN 119 Tub, VLAN 154 Shower and VLAN 83 Management

ii. Configure port 24 as VLAN 119 access port

iii. Configure a static mac address on port 24 to the MAC address of PC2

e) Configure G0/1 as a **trunk por**t on both switches

f) Switch Management – on both switches configure an ip address on interface VLAN 83 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

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 interfaces and any loopbacks with ip addresses

b) Dutovo and Kyrta Router

i) Refer page 19 and to **your journal** and lab exercises from prior unit on **Basic Inter-VLAN Routing**

ii) Configure **Inter-VLAN routing** on G0/0/1

- Dutovo configure separate sub-interfaces for VLAN 83 (the management VLAN) and VLAN 361
- Kyrta configure separate sub-interfaces for VLAN 83 (the management VLAN) and VLAN 119
- 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 gateways configured on switches

Scenario 4 -Tasks

12. Trouble Shooting Trunking – between Switch and Router

a) To check Trunking is activated, on switches, 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 Testing

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

b) Ping PC1 – VLAN 361 to ip address of Dutovo Switch 1

c) Telnet PC1 – VLAN 361 to ip address of Dutovo Switch 1

d) Ping PC2 – VLAN 119 to ip address of Kyrta Switch 2

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

15. Routing Protocol Configuration (refer page 17,18)

a) Dutovo and Kyrta

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

b) Vuktyl

- **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 other internal Routers

c) ISP Router

- **Do not configure OSPF**
- **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 4 -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 network is not included in the **network** statements

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

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) ISP 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
- Static or Default route not configured

18. 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 in VLAN 361 to PC2 in VLAN 119

b) Ping from PC Hosts in VLAN 361 and VLAN 119 to External Web Server and the Internet

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

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

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

f) 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

Scenario 4 - Tasks

19. OSPF Link Bandwidth Settings

a) Link Vuktyl to Kyrta configure bandwidth 512
b) Link Dutovo to Vuktyl configure bandwidth 128
c) Link Dutovo to Kyrta configure bandwidth 512
d) Check routing table in each router, use - **show ip route**, are the best routes shown ?

20. Link State Database Have a Look

a) On an internal router, use – **show ip ospf database**

21. Trouble Shooting Back Up Link Testing

a) On **Dutovo** router**,** check that if exit interface to ISP is shutdown a back up will appear in the routing table.

22. 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**.

23. 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 4 - Tasks

24. Access List Requirements

a) Refer to pages 13 to 15 and **Lab Exercises on Access Control Lists**

b) You must create a **NAMED Extended** ACL for VLAN 361 based on following requirements:

- PCs in VLAN 361 permitted **HTTP** access to an External Web Server (you choose one) and denied **ALL** other access to that External Web Server.
- PCs in VLAN 361 permitted **ALL** access to the Internet – all the other External Web Servers.
- **ALL** means **IP**

c) You must create a **NAMED Extended** ACL for VLAN 119 based on following requirements:

- PCs in VLAN 119 denied **PING** access to PCs in VLAN 361
- PCs in VLAN 119 permitted **ALL** access to the Internet. The Internet is represented be a single Loopback for testing, your ACL must allow access to all addresses in the Internet
- **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 361 permitted **TELNET** access to Dutovo Router
- ONLY PCs in VLAN 361 denied **TELNET** access to Vuktyl 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** **NAMED** ACLs for VLAN 361 and VLAN 119 using the template on page 13, refer Task 25
ii) **Test** the **NAMED** ACLs for VLAN 25 and VLAN 119 refer Task 26

iii) **Create** **NAMED** ACLs for Telnet access using the template on page 14, refer Task 25
iv) **Test** the **NAMED** ACLs for Telnet access refer Task 26

Scenario 4 - Tasks

25. 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 aclvan361 and Aclvlan361 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

26. 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**

Scenario 4 – ACL Templates

ACL for VLAN 361 on Dutovo Router

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

no ip access-list extended ACLVLAN361 (Delete previous version of the ACL for VLAN 361)
Ip access-list extended ACLVLAN361 (Self-documenting, the ACL for VLAN 361)
! Only permit HTTP access to External Web Server (! means comment)
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 access to The Internet
permit ip any any
ACL Placement - On Sub Interface G0/0/1.361 on Dutovo Router
interface G0/0/1.361
ip access-group ACLVLAN361 in

ACL for VLAN 119 on Kyrta Router

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

no ip access-list extended ACLVLAN119 (Delete previous version of the ACL for VLAN 119)
Ip access-list extended ACLVLAN119 (Self-documenting, the ACL for VLAN 119)
! Deny PING access to a destination - PCs in VLAN 361 subnet
deny icmp source subnet wildcard destination subnet wildcard
! Permit access to The Internet
permit ip any any
ACL Placement - On Sub Interface G0/0/1.119 on Kyrta Router
interface G0/0/1.119
ip access-group ACLVLAN119 in

Scenario 4 – ACL Templates

ACL to control Telnet Access to Dutovo and Vuktyl Routers

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

```
! On Dutovo
no ip access-list standard ACLTELNET
ip access-list standard ACLTELNET
! Permit VLAN361 Telnet Access to Dutovo
   permit source subnet  wildcard (inverse of subnet mask)
   deny any

! On Vuktyl
no ip access-list standard ACLTELNET
ip access-list standard ACLTELNET
! Deny VLAN361 Telnet Access to Vuktyl
   deny source subnet  wildcard (inverse of subnet mast)
   permit any
```

Interface Placement - line vty 0 4, on Dutovo and Vuktyl Routers

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

Scenario 4 – ACL Overview

Case Sensitivity

- ACL names are case sensitive eg aclvlan361 and AclVlan361 are **different** ACLs
- Should decide to use either all uppercase - ACLVLAN361 or all lowercase – aclvlan361 names to reduce errors

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 early to reduce congestion

Trouble Shooting Commands

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

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 mask
- Do not configure the ISP router with a routing protocol advertising the corporate's network

OSPF Configuration

- Configure on Dutovo Router

  router OSPF 1 (1 is just a process id, for OSPF routers may use different process ids)

  network **?.?.?.?** ?.?.?.? area 0 (VLAN 361, ospf routers exchange updates with routers in the same area)

  network **?.?.?.?** ?.?.?.? area 0 (VLAN 83 wildcard is inverse of subnet mask, **? means** replace)

  network **?.?.?.?** ?.?.?.? area 0 (Serial Link – Dutovo to Vuktyl)

  network **?.?.?.?** ?.?.?.? area 0 (Serial Link – Dutovo to Kyrta)

  Passive Interface Options:

  passive-interface G0/0/1.83 (Do not send routing information to LAN subnets)

  passive-interface G0/0/1.361 (Do not send routing information to LAN subnets)

  OR

  passive-interface default (Configure passive interface as default for all interfaces)

  no passive-interface S0/1/0 (Configure S0/1/0 to allow the flow of routing information)

  no passive-interface S0/1/1 (Configure S0/1/1 to allow the flow of routing information)

- Configure on Kyrta Router

  router OSPF 2

  network **?.?.?.?** ?.?.?.? area 0 (VLAN 119, ospf routers exchange updates with routers in the same area)

  network **?.?.?.?** ?.?.?.? area 0 (VLAN 1 wildcard is inverse of subnet mask, **? means** replace)

  network **?.?.?.?** ?.?.?.? area 0 (Serial Link – Kyrta to Vuktyl)

  network **?.?.?.?** ?.?.?.? area 0 (Serial Link – Kyrta to Dutovo)

  passive-interface G0/0/1.83 (Do not send routing information to LAN subnets)

  passive-interface G0/0/1.119 (Do not send routing information to LAN subnets)

OSPF Configuration

- Configure on Vuktyl Router

  router OSPF 3

  network **?.?.?.?** ?.?.?.? area 0 (Loopback Database LAN)

  network **?.?.?.?** ?.?.?.? area 0 (Serial Link – Vuktyl to Dutovo)

  network **?.?.?.?** ?.?.?.? area 0 (Serial Link – Vuktyl to Kyrta)

  ip route 0.0.0.0 0.0.0.0 *exit interface or next hop ip address* (The default route to the Internet)

  default-information originate (Advertise default route to other internal routers)

  passive-interface loopback0 (Do not send routing information to Server LAN)

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

  ip route **?.?.?.?** ?.?.?.? *exit interface or next hop ip address* (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 G0/0/1.83
     description A logical Sub Interface
     description VLAN 83 VLAN Management
     encapsulation dot1q 83
     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 361
    name Sink
  vlan 83
      name Management
- Switch S2 Configure VLANs
  vlan 119
    name Tub
  vlan 154
    name Shower
  vlan 83
      name Management

- Configure IP address for management vlan
  interface vlan 83
    ip address *ip address* *mask* (This allows the switch to be configured remotely via Telne

- Configure Default Gateway
  ip default-gateway *ip address of router interface* (Use VLAN 83 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 119 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

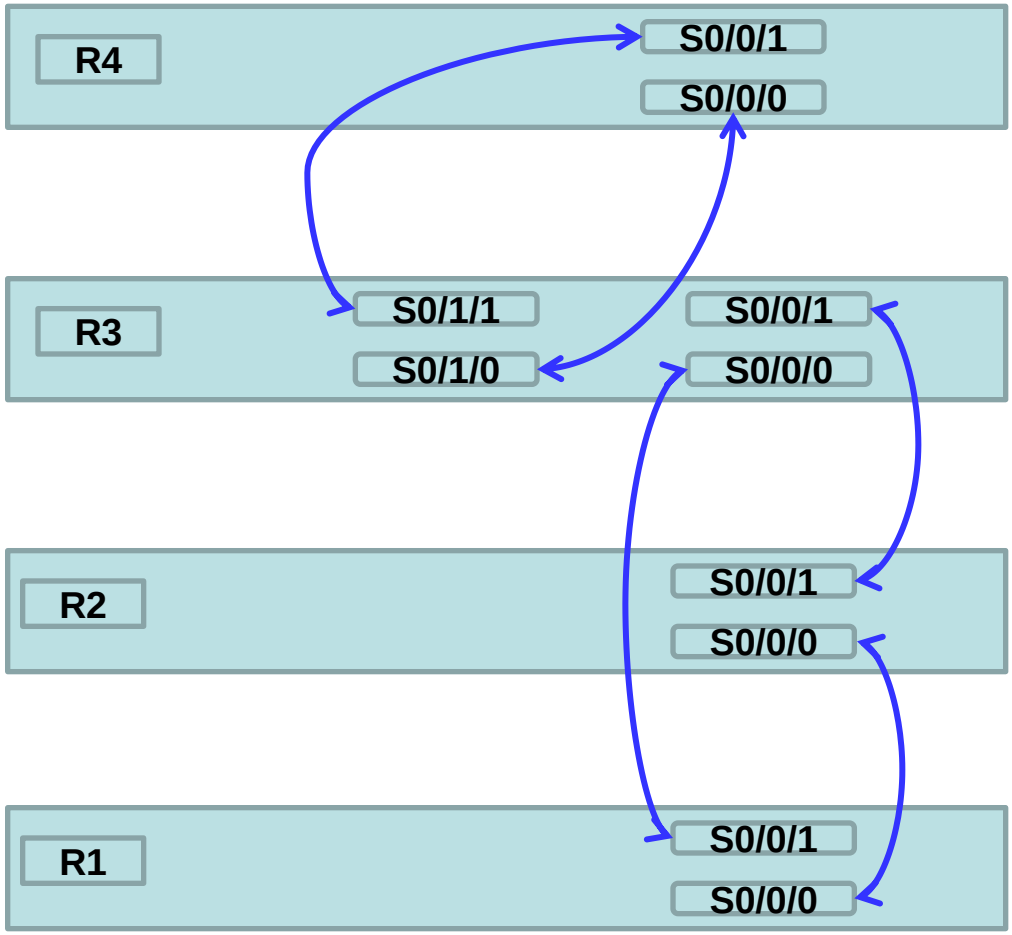
router#

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 !