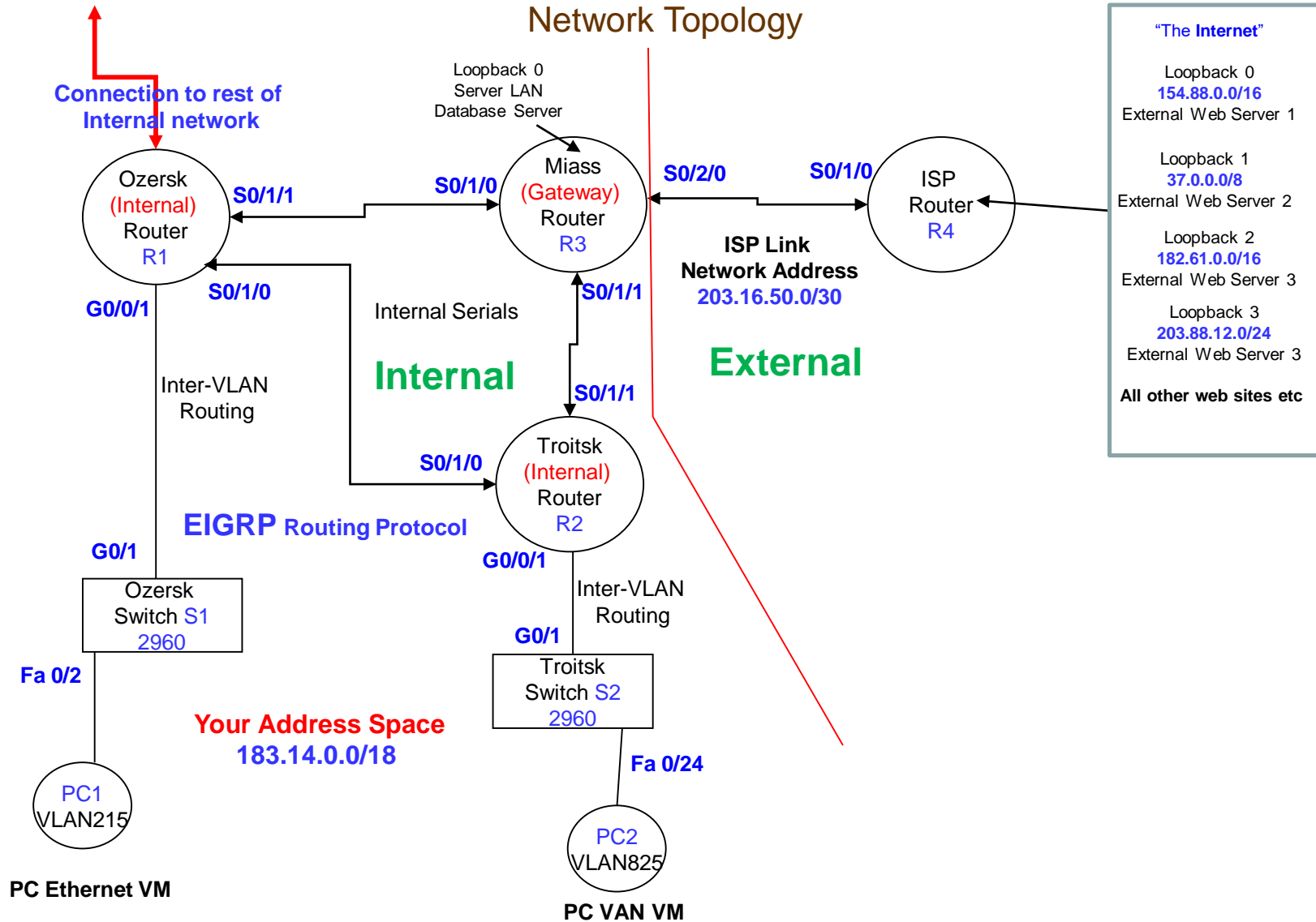


## Scenario 3 (2 marks) - EIGRP, ACLs, 4R V2.7

### A Network Configuration and Troubleshooting 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 3 - Introduction

- This scenario can be completed independent of the lecture material as configuration details are provided on pages 13 to 23
- 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?**
  - You will configure **EIGRP** (Enhanced Interior Gateway Routing Protocol) on the routers
  - The use of **standard** ACLs to **control Telnet access to the routers**
- Network Topology
  - **Internal**, your internal network
  - **External**, the link to the ISP and the Internet
  - The Internet is represented by a single Loopback
  - The Corporate Network Address, **183.14.0.0/16**.  
The corporate network address has been **divided up** and you have been given the address space **183.14.0.0/18** to build your section of the Corporate Network.
  - Do not configure the connection to the rest of the internal network
  - ISP Link Address, **203.16.50.0/30**

# Scenario 3 – Assessment

## 1. Assessment due

- Scenario 3 will ONLY be assessed up to the end of your allocated Lab in week 6
- Scenario 3 will NOT be assessed (no marks given) after your allocated lab in week 6

## 2. Scenarios must be completed individually

## 3. Assessment Process

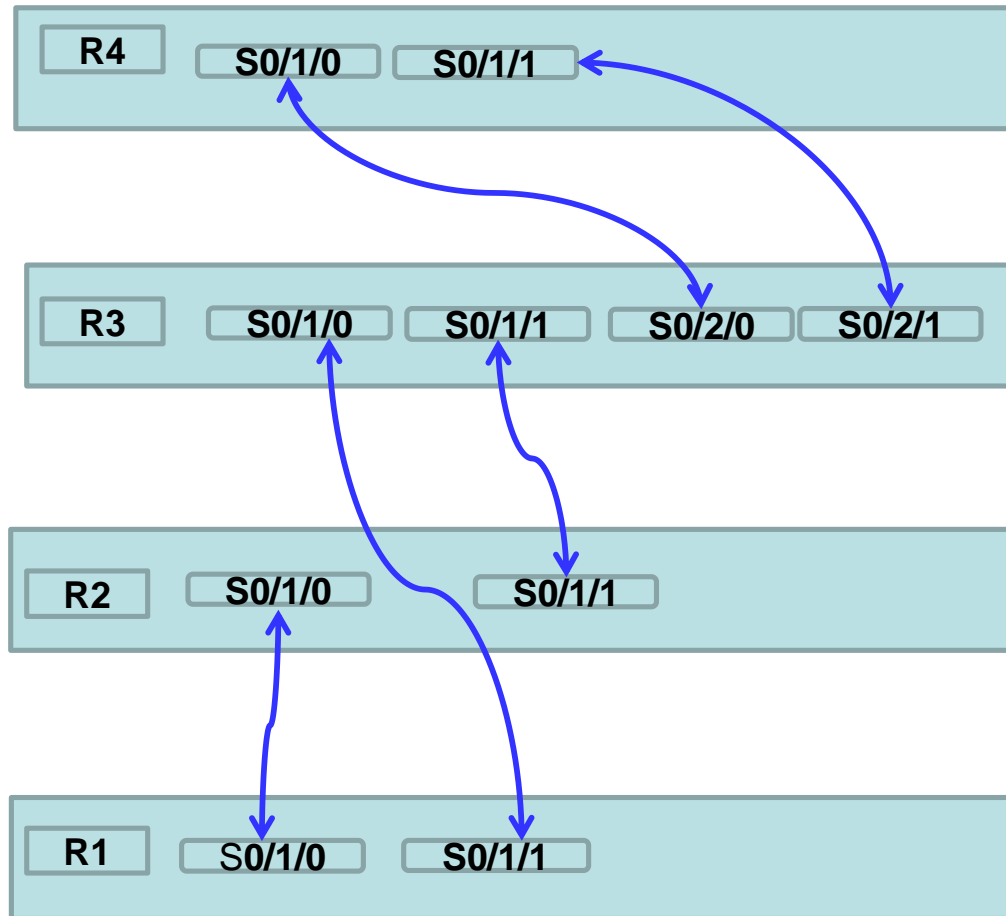
- Email your Packet Tracer File to your tutor for assessment, or if you have remotely accessed a lab kit, ask your tutor to assess your scenario in the lab
- Your tutor may:
  - ask you questions about your scenario
  - ask you to further configure your routers, switches, PCs
  - break your network and 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 2 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 3 -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 215** Flower 450 hosts and management **VLAN 55** 20 hosts
  - ii. Switch S2 **VLAN 825** Shrub 200 hosts, **VLAN 328** Tree 50 hosts, and management **VLAN 55** 6 hosts
  - iii. Miass **Database Server LAN** loopback 0 24 hosts
  - iv. **3 Internal Serials** 2 hosts each
- b) **Document** assignment of ip addresses to router interfaces, switches 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 Ozersk router to Ozersk switch 1 port G0/1
- b) Connect Troitsk router to Troitsk switch 2 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

## 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 3 -Tasks

## 8. Switch Configuration

- a) Refer to pages 19 to 22 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 215 Flower and VLAN 55 Management
  - ii. configure ports 2,3 as VLAN 215 access ports
  - iii. configure Port Security, mac address sticky on ports 2,3 max 2, with **violation shutdown**
- d) On switch S2
  - i. create VLAN 825 Shrub, VLAN 328 Tree and VLAN 55 Management
  - ii. configure port 24 as VLAN 825 access port
  - iii. configure a static mac address 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 55 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 **serial** and **loopback** interfaces with ip addresses
- b) Ozersk and Troitsk Routers
  - i) Refer page 18 and to **your journal** and lab exercises from prior unit on **Basic Inter-VLAN Routing**
  - ii) Configure **Inter-VLAN routing** on G0/0/1
    - Ozersk configure separate sub-interfaces for VLAN 55 (the management VLAN) and VLAN 215
    - Troitsk configure separate sub-interfaces for VLAN 55 (the management VLAN) and VLAN 825
    - 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 3 -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
  - 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.

### 14. Trouble Shooting Inter-VLAN Routing Test

- a) This test is to check Inter-VLAN routing is working
- b) **Ping** PC1 – VLAN 215 to VLAN 55 ip address of Ozersk Switch S1, **Telnet** PC1 to Switch S1
- c) **Ping** PC2 – VLAN 825 to VLAN 55 ip address of Troitsk Switch S2, **Telnet** PC2 to Switch S2
- d) Check IP address/Mac address mapping on the router, **show arp**

### 15. Routing Protocol Configuration (refer pages 16, 17,18)

- a) Ozersk and Troitsk
  - **EIGRP** using wildcards for each subnet. Autonomous system number 65
  - Configure passive-interface as appropriate to avoid sending unnecessary routing information
- b) Miass
  - **EIGRP** using wildcards for each subnet. Autonomous system number 65
  - 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 EIGRP**
  - **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 3 -Tasks

## 16. Trouble Shooting EIGRP Neighbor Adjacency

- a) Verify that the routers have formed an adjacency with each other, use - **show ip eigrp neighbors**
- 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) routers configured with different EIGRP AS values
  - iii) the directly connected network is not included in the **network** statements
- c) Other trouble shooting commands: **show ip protocols, show ip eigrp topology, debug eigrp neighbor**

## 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) 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
- 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 215 to PC2 in VLAN 825
- b) **Ping** from PC Hosts in VLAN 215 and VLAN 825 to External Web Server and the Internet
- c) Use **tracert** 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 3 - Tasks

### 19. EIGRP Link Bandwidth Settings

- a) Link Miass to Troitsk            configure bandwidth 512    (on each end of the link)
- b) Link Ozersk to Miass            configure bandwidth 64    (on each end of the link)
- c) Link Ozersk to Troitsk           configure bandwidth 128   (on each end of the link)
- d) Check routing table in each router, use - **show ip route**, are the best routes shown ?

### 20. Trouble Shooting Check for EIGRP Feasible Successors

- a) On each internal router, use – **show ip eigrp topology**, does a feasible successor exist in the topology table ?

### 21. Trouble Shooting Testing Backup Link

- a) On **Ozersk** 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 3 - Tasks

### 24. Access List Requirements Ozersk and Miass Routers

a) Refer to pages 11 to 15 and Lab Exercises on Access Control Lists

b) You must create a **NAMED Extended** ACL for VLAN 215 based on following requirements:

- PCs in VLAN 215 permitted **HTTP** access to an External Web Server (you choose one) and denied **ALL** other access to that External Web Server.
- PCs in VLAN 215 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 215 permitted **TELNET** access to Ozersk Router
- **ONLY** PCs in VLAN 215 denied **TELNET** access to Miass 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 215 using the template on page 13, refer Task 25

ii) **Test** the **NAMED** ACL for VLAN 215 refer Task 26

iii) **Create** **NAMED Standard** 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 3 - 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 aclvan215 and Aclvlan215 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 3 – ACL Templates

### ACL for VLAN 215 on Ozersk Router

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

no ip access-list extended **ACLVLAN215** (Delete previous version of the ACL for VLAN 215 )

ip access-list extended **ACLVLAN215** (Self-documenting, the ACL for VLAN 215, ! means comment)

**! Permit ONLY HTTP access to a selected External Web Server**

permit tcp source subnet wildcard host ip address eq www

**! Deny ALL other access to this 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 G0/0/1.215 on Ozersk Router**

interface G0/0/1.215

ip access-group ACLVLAN215 in

## Scenario 3 – ACL Templates

### ACL to control Telnet Access to Ozersk and Miass Routers

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

**! On Ozersk**

```
no ip access-list standard ACLTELNET
```

```
ip access-list standard ACLTELNET
```

**! Permit ONLY VLAN215 Telnet Access to Ozersk**

```
    permit source subnet wildcard (inverse of subnet mask)
```

```
    deny any
```

**! On Miass**

```
no ip access-list standard ACLTELNET
```

```
ip access-list standard ACLTELNET
```

**! Deny ONLY VLAN215 Telnet Access to Miass**

```
    deny source subnet wildcard (inverse of subnet mask)
```

```
    permit any
```

### Interface Placement - line vty 0 4, on Ozersk and Miass Routers

```
line vty 0 4
```

```
    password cisco
```

```
    login
```

```
    access-class ACLTELNET in
```

## Scenario 3 – ACL Overview

### ACL Case Sensitivity

- ACL names are case sensitive eg `aclvlan215` and `AcVlan215` are **different** ACLs
- Should decide to use either all uppercase - `ACLVLAN215` or all lowercase – `aclvlan215` names to reduce errors

### 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 early to reduce congestion

### 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 Trouble Shooting Commands

- show access-lists (**shows all access lists**)
- clear access-list counters (**clears ip packet hits against a rule**)
- Use the following to test the rules: ping, telnet, a browser

# 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



# EIGRP Configuration

- **Configure** on Ozersk Router

router EIGRP 65 (65 the autonomous system number, all internal routers need to use the same number in order to exchange updates)

network 152.10.?.? <?.?.?.?> (VLAN 215 wildcard is inverse of subnet mask, ? means insert)

network 152.10.?.? <?.?.?.?> (VLAN 55 wildcard is inverse of subnet mask, ? means insert)

network 152.10.?.? <?.?.?.?> (Serial Link – Ozersk to Miass)

network 152.10.?.? <?.?.?.?> (Serial Link – Ozersk to Troitsk)

**Passive Interface Options:**

passive-interface G0/0/1.55 (Do not send routing information to LAN subnets)

passive-interface G0/0/1.215 (Do not send routing information to LAN subnets)

OR

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

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

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

- **Configure** on Troitsk Router

router EIGRP 65 (65 the autonomous system number, all internal routers need to use the same number in order to exchange updates)

network 152.10.?.? <?.?.?.?> (VLAN 825 wildcard is inverse of subnet mask, ? means insert )

network 152.10.?.? <?.?.?.?> (VLAN 55 wildcard is inverse of subnet mask, ? means insert)

network 152.10.?.? <?.?.?.?> (Serial Link – Troitsk to Miass)

network 152.10.?.? <?.?.?.?> (Serial Link – Troitsk to Ozersk )

passive-interface G0/0/1.55 (Do not send routing information to LAN subnets)

passive-interface G0/0/1.825 (Do not send routing information to LAN subnets)

# EIGRP Configuration

- **Configure** on Miass Router

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

router EIGRP 65

network **152.10.??** *<??.??.?>* (Loopback Database LAN)

network **152.10.??** *<??.??.?>* (Serial Link – Miass to Ozersk )

network **152.10.??** *<??.??.?>* (Serial Link – Miass to Troitsk)

redistribute static (Advertise default route to other internal routers)

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

- **Configure** on ISP Router (EIGRP 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 G0/0/1.55
```

```
description A logical Sub Interface
```

```
description VLAN 55 VLAN Management
```

```
encapsulation dot1q 55
```

```
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 215

- name Flower

- vlan 55

- name Management

- Switch S2 Configure VLANs

- vlan 825

- name Shrub

- vlan 328

- name Tree

- vlan 55

- name Management

- On each Switch:

- Configure IP address for management vlan

- interface vlan 55

- ip address *<ip 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 55 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 825 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
```

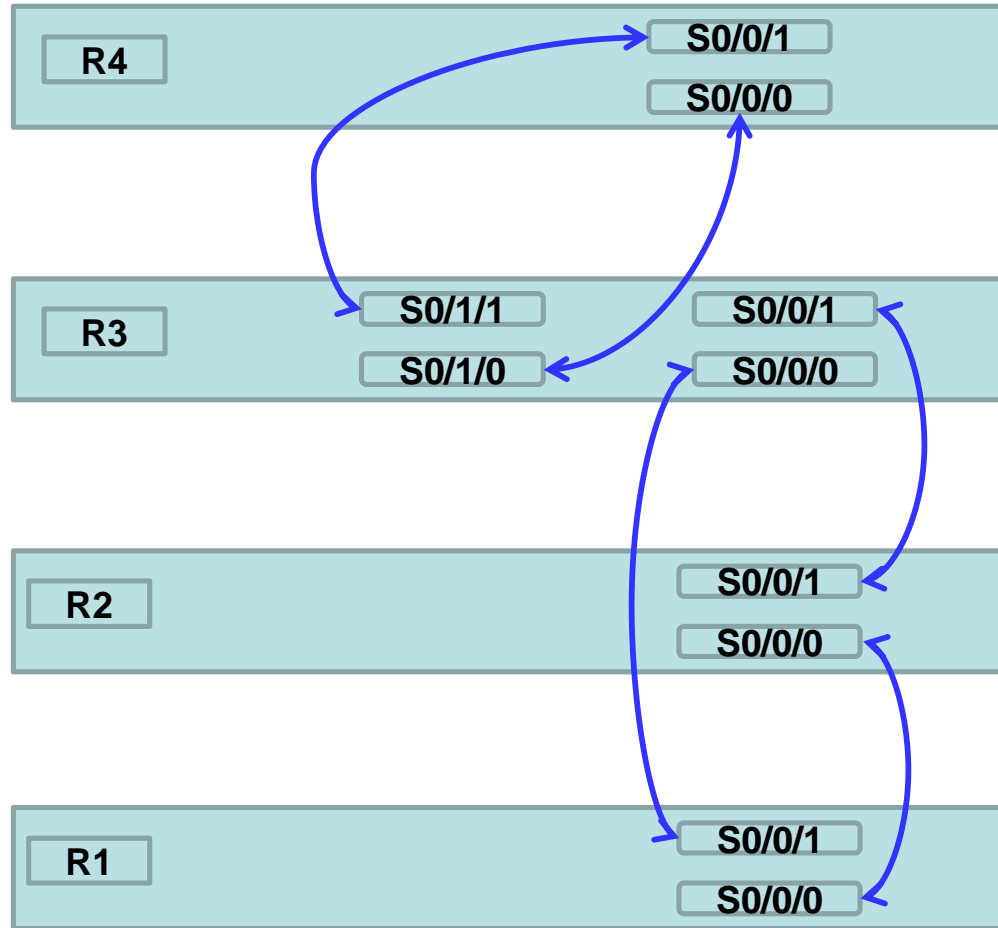
```
router#
```

```
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 tutor !**