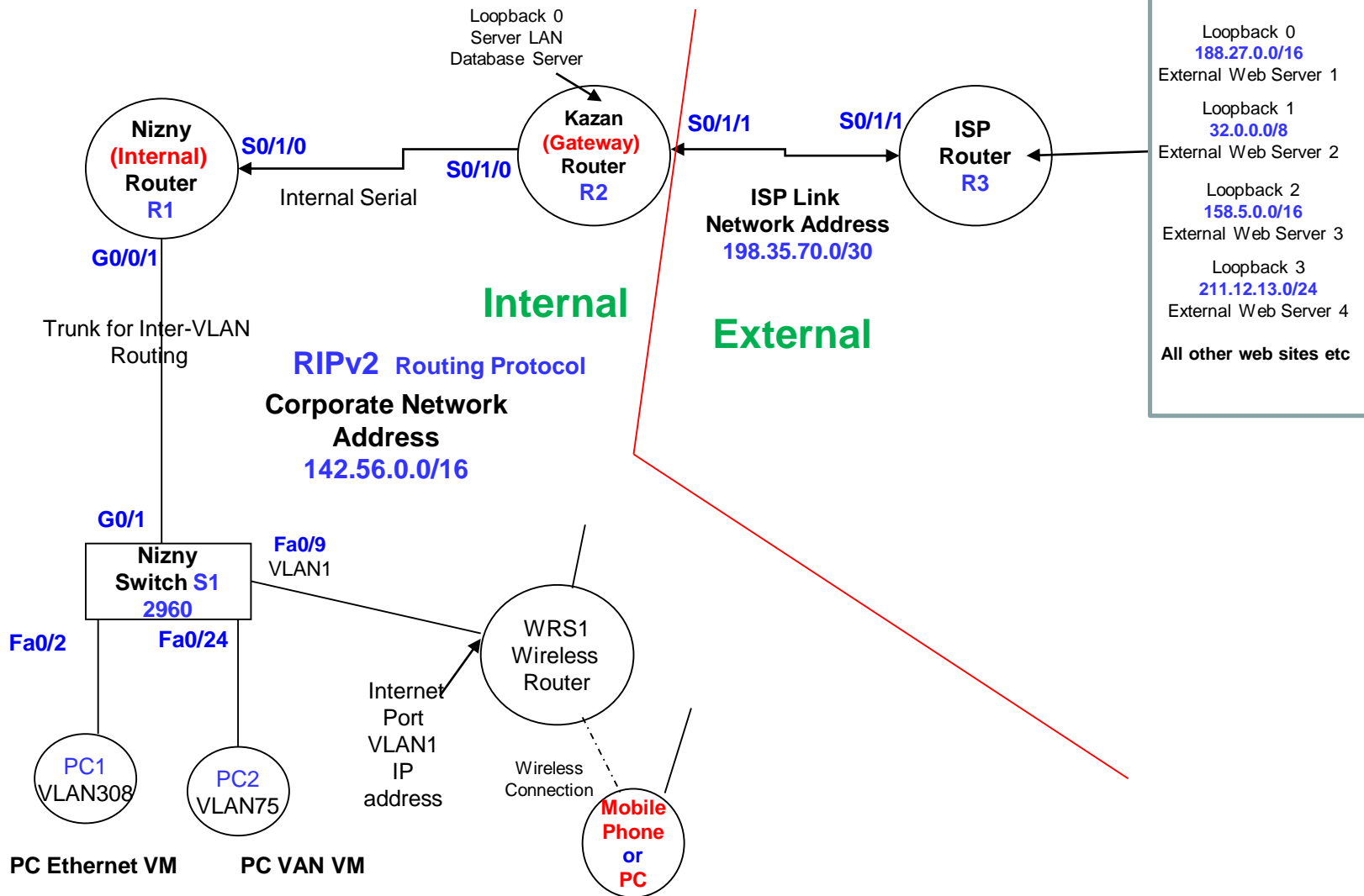# Scenario 1 RIP Routing Protocol – V2.2
A Network Configuration and Trouble Shooting Scenario
Network Topology

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 Diagram
  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.
  - enable you to build an internal network for a small company

Introduction

- This scenario can be completed independent of the lecture material as configuration details are provided on pages 11 to 18

- 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?**
  - Configuration of a dynamic routing protocol **RIP** (Routing Information Protocol) V2
  - RIP V2 supports VLSM addressing
  - Configuration of a static and a default route
  - The integration of a Wireless network into the fixed infrastructure

- Network Topology
  - Internal, your internal network
  - External, the link to the ISP and the Internet
  - Corporate Network Address, **142.56.0.0/16**
  - ISP Link Address, **198.35.70.0/30**

Scenario 1 – Assessment

1. **Assessment due**
   - Scenario 1 will ONLY be assessed in your allocated Lab in week 2
   - Scenario 1 will NOT be assessed (no marks given) after your allocated lab in week 2
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
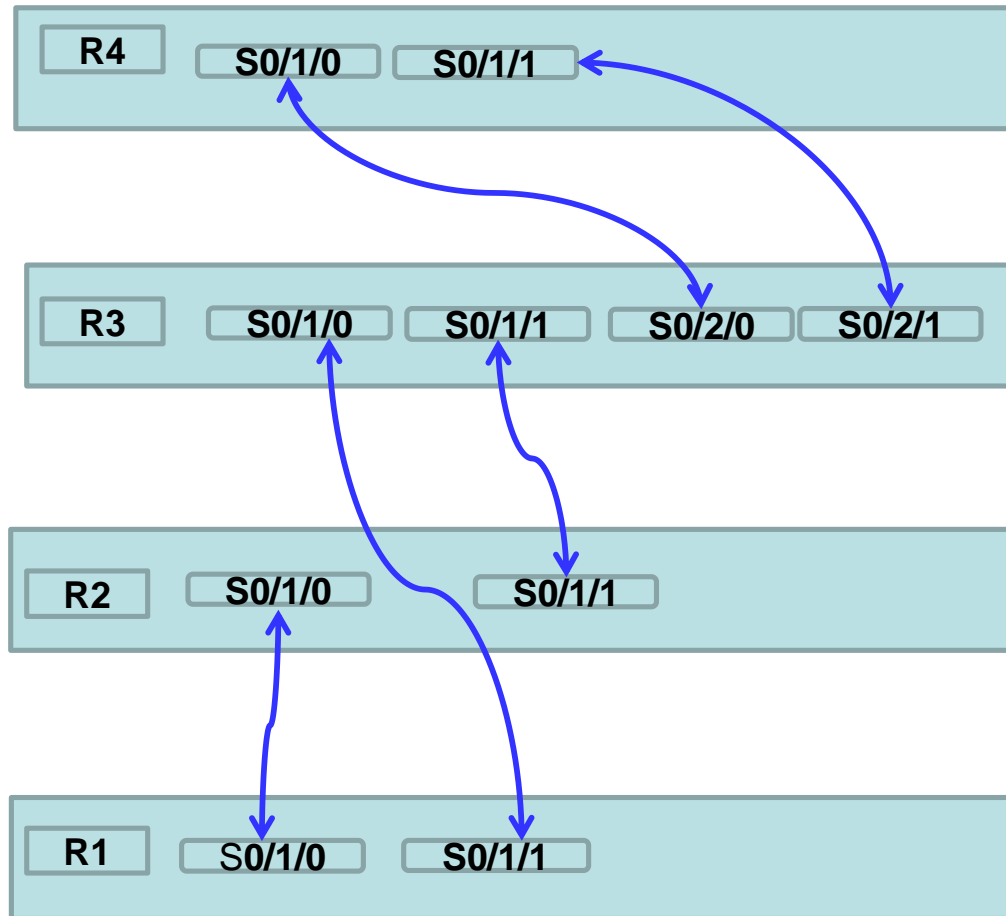
R4 S0/1/0 S0/1/1

R3 S0/1/0 S0/1/1 S0/2/0 S0/2/1

R2 S0/1/0 S0/1/1

R1 S0/1/0 S0/1/1

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 1 -Tasks

1. On each router, ensure router config-register is set to 0x2142: router(config)# config-register 0x2142 (refer page 22)

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: **VLAN 308** Hindi 1200 hosts, **VLAN 75** German 100 hosts

    VLAN 625 Spanish 50 hosts, **VLAN 1** 18 hosts, **Internal Serial** 2 hosts, Kazan **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 Nizny router interface G0/0/1 to Nizny switch port G/0/1

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

  c) Connect PC1 to Fa0/2 using the patch panel, connect PC2 to Fa0/24 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 1 -Tasks

8. Switch Configuration

  a) Refer to pages 14 to 17 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 308 Hindi, VLAN 75 German, VLAN 625 Spanish

  d) Configure G0/1 as a trunk port

  e) Configure as access ports, **only** VLAN 308 ports 2,3 and VLAN 75 port 24

  f) Switch Management – configure an ip address on interface VLAN1 and configure a default gateway IP address

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

  h) Configure Port Security only for VLAN 308, mac address sticky on ports 2,3 max 4, with **violation protect**

  i) Configure a static mac address, VLAN 75, on Fa0/24 to the MAC address of PC2

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) Nizny Router

   i) Refer page 13 and to **your journal** and lab exercises from prior unit on **Basic Inter-VLAN Routing**

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

   – Configure separate sub-interfaces for VLAN 1 (the management VLAN) and VLANs 308 and 75

   – 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 switch to Nizny router, use VLAN1 G0/0/1.1 sub-interface ip address

12. 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 1 -Tasks

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) Ping PC1 – VLAN308   to   PC2 – VLAN75

    c) Telnet PC1 to the switch S1

15. Routing Protocol Configuration (refer pages 11,12)

    a) Nizny

      – RIP V2

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

    b) Kazan

      – 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 Nizny Router

    c) ISP Router

      – **Do not configure RIP**

      – **Only** configure a static route (default class B mask) to your internal network

      – Configure loopbacks to simulate '**The Internet'**

Scenario 1 -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
- 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 PC Hosts in VLAN308 and VLAN75 to External Web Servers - 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 1 -Tasks

18. **Wireless Router Configuration**

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

    b) Refer to page **21** 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 (desk top to the patch panel) between Nizny Switch Fa0/9 (port in VLAN1) and Internet Port (in VLAN1) on Wireless Router

    f) VLAN 1 will carry 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?

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 Address with the relevant class A, B or C default mask

- Do not configure the ISP router with a routing protocol

RIP V2 Configuration

- Configure on Nizny Router

  router rip (The routing protocol))
    version 2   (Version 2 supports VLSM)
    network 142.56.0.0 (Advertise the internal network)
    passive-interface G0/0/1.1 (Do not send routing updates to VLAN subnets)
    passive-interface G0/0/1.308
    passive-interface G0/0/1.75

- Configure on Kazan Router (the gateway router)

  ip route 0.0.0.0   0.0.0.0   S0/1/1   (Configure the default route to the Internet)
  router rip
    version 2
    network 142.56.0.0
    default-information originate   (Advertise default route to other internal routers)

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

  ip route 142.56.0.0   255.255.0.0   S0/1/1   (ISP configure a static route to company's 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

- **Configure** VLANs

  vlan 308
     name Hindi
  vlan 75
     name German
  vlan 625
     name Spanish

- **Configure** IP address for management vlan 1

  interface vlan 1
     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 1 subinterface IP address)

Switch Configuration

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

  interface Fa0/3 (or interface range Fa0/3 – 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 75 interface Fa0/24
            (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)

16

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 example below:

  interface Fa0/10
   shutdown
   (wait until shutdown confirmed)
  no shutdown

SSH – Secure Shell

1. Configure switch or router with a hostname:
    hostname S1

2. Configure a local user account:
    username labuser privilege 15 secret cisco

3. Configure domain name:
    ip domain-name scenario.lab

4. Configure SSH Certificate:
    crypto key generate rsa general-keys modulus 1024

5. Configure Line vty
     line vty 0 15 (4 for a router)
      transport input SSH
      login local
     end

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

Configuring the Wireless Router – Linksys WRT300N
Also refer Wireless Supporting Material A and B

1. Power UP wireless router (get a wireless router from your tutor)
2. **Reset** it to factory default – push reset button and hold until **blue** symbols flash
3. Start up PC Ethernet VM, configure to obtain ip address automatically
4. Ethernet Connection – plug blue UTP cable from your PC into any Ethernet port (1 to 4) on the wireless router
5. Open DOS Command Window – type ipconfig /all to confirm PC Ethernet has been obtained an ip address from wireless router
6. Use a Browser to connect to factory default ip address 192.168.1.1 on the wireless router
7. Authentication – username: admin, password: admin
8. Wireless Router Setup
    a) **Ensure** you always **click save** at the bottom of each screen
    b) Internet Setup
        I. Internet Connection type: static IP
        II. Assign an ip address from VLAN 1 address range
    c) Network Setup - DHCP
        I. For Wireless PCs
        II. Use address space for wireless LAN
    d) Disable/Enable PC Ethernet LAN connection to pick up a new ip address from Wireless LAN address space
    e) Use a Browser to re-connect to new (default gateway) ip address on the wireless router
    f) Security
        I. Disable Firewall
    g) Wireless Wi-Fi Protected Setup
        I. Wireless Configuration: manual
        II. SSID: student Id
9. **Use your Mobile Phone to connect to the Wireless Router OR Connect via your Laptop PC to the Wireless Router, refer below:**
    a) Look for the wireless tray icon – bottom right, click
    b) Associate with the wireless LAN broadcasting your student ID as its SSID
    c) Open DOS Command Window – type ipconfig /all to confirm an ip address has been obtained from wireless router
    d) From your Laptop PC Ping default gateway on the wireless router to confirm connection is working
    e) Wireless Router - Remove blue UTP cable from your PC, get a new blue UTP cable, plug into Internet Port
    f) Connect new blue UTP cable to Desk Top coloured enclosure port, then patch from patch panel to Nizny switch port Fa 0/9
    g) From your Laptop PC 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
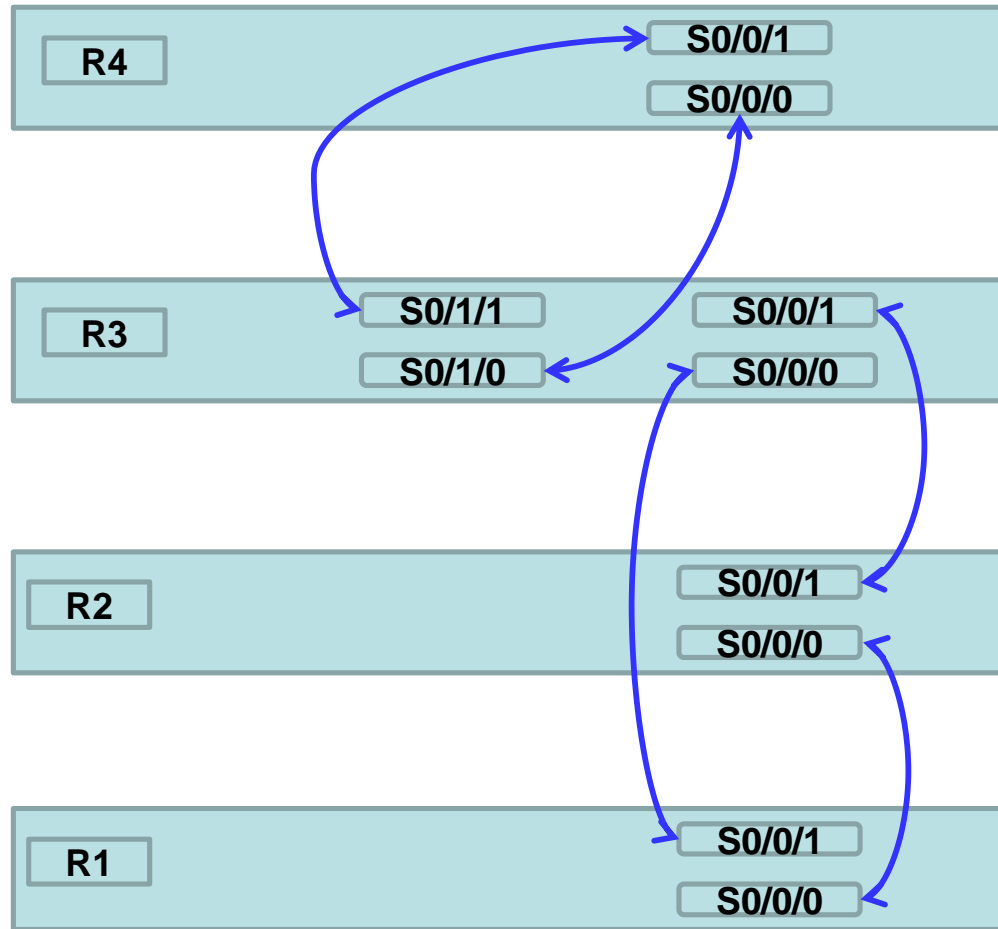   router>enable
      router#
      router#copy startup-configure running-configure
      Melb#

Kit - Router Serial Cable Mapping
Room ATC330

R4
S0/0/1
S0/0/0

R3
S0/1/1
S0/1/0
S0/0/1
S0/0/0

R2
S0/0/1
S0/0/0

R1
S0/0/1
S0/0/0

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 !