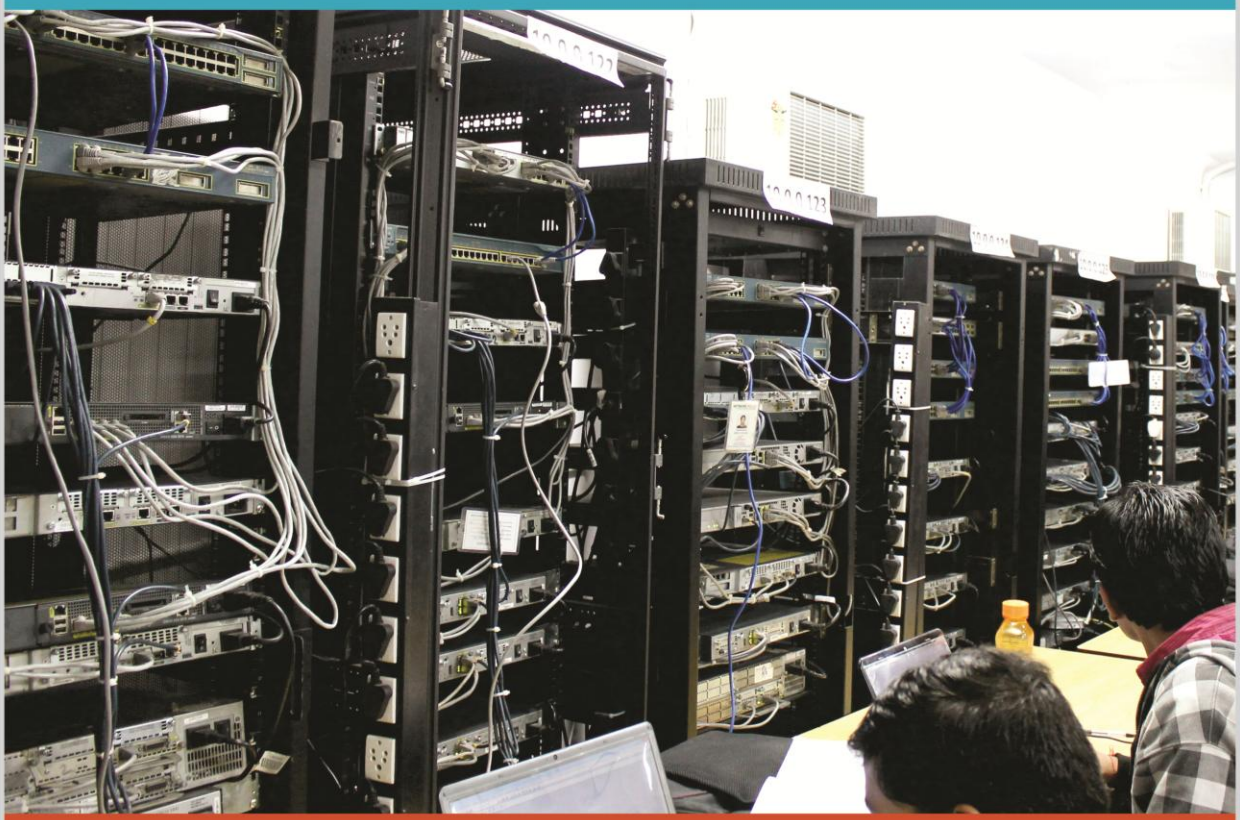
NETWORK BULLS

Training | Consulting | Implementation

CCNP R&S

PRACTICAL WORKBOOK



www.networkbulls.com I www.networkbulls.in

Our Special Thanks To!

Mr. Mohit Bhalla-CCIE R&S#42145, CCSI#34989, CCIE SP & Security Written

Mr. Piyush Kataria- CCIE R&S Written.

Mr. Vikas Kumar CCIEx3#30078

Ms. Amrita, Ms. Shruti Kaushik, Ms. Bandna Bhalla,
Mr. Nandan Kumar, Mr. Gaurav Chauhan.

for their contribution in making of this world class Practical Workbook

Getting to world class begins with a single step. start today.

Happy Learning!!

www.networkbulls.com | www.networkbulls.in

CCNP Route Basics

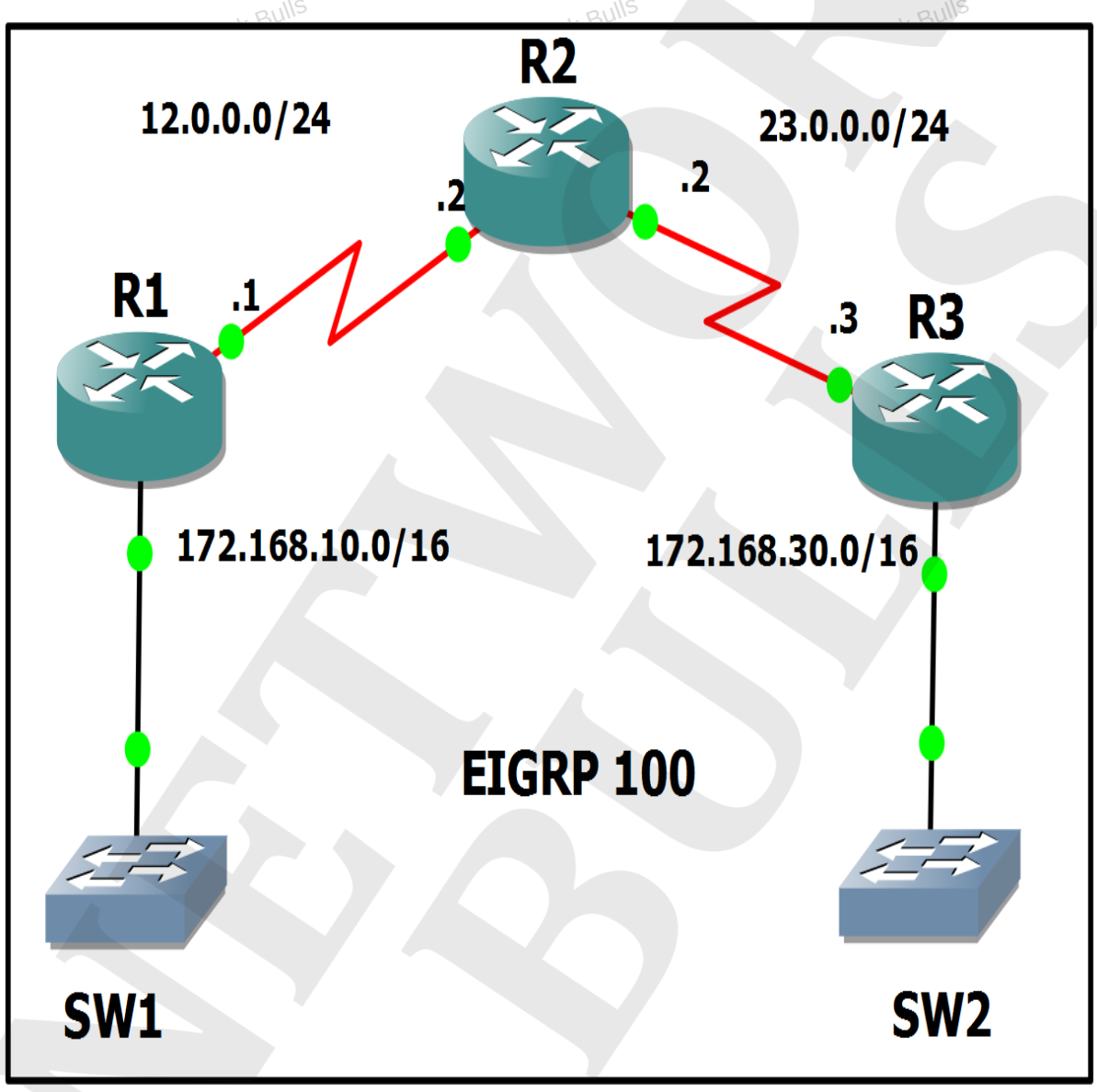
Table of Contents

BGP Neighborship i. IBGP. ii. EBGP.
Route Aggregation
Route Authentication
BGP Timers
Default Routing
BGP Terminology i. Update Source. ii. EBGP Multi-hop. iii. Redistribute Internal. iv. Next Hop Self. v. Route Reflector Client.
Route Filtering i. Using Distribute-List with an ACL. ii. Using Distribute-List with a Route Map. iii. Using Prefix-List.
BGP Best Path Selection i. Weight. ii. Local Preference. iii. AS Path. iv. MED.
BGP Load Balancing
Redistribution
Basic IGP Redistribution i. Mutual Redistribution. ii. Redistribution into EIGRP and Setting Metric for Redistributed Routes. iii. Redistributed into OSPF as E1 Routes. iv. Redistributed into OSPF and Setting OSPF Metrics on Redistributed Routes.
Advanced IGP Redistribution i. Redistribution Filtering with the Distribute- list Command. ii. Preventing Routing Domain Loops with AD. iii. Preventing Routing Domain Loops with higher metrics.
IPv6- Internet Protocol Version 6
RIPng for IPv6
EIGRP for IPv6
OSPFv3 for IPv6
Static Route for IPv6
IPv6 Tunnel
GRE Tunnel

EIGRP (Enhanced Interior Gateway Routing Protocol)

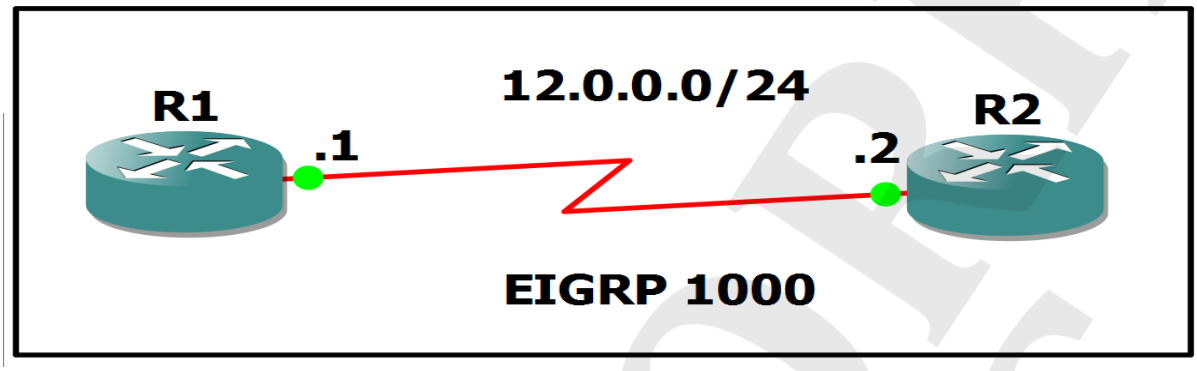
Practical 1: Manipulating Hello and hold interval of EIGRP.

Task: The "hello" and "hold" interval of EIGRP is 5 seconds and 15 seconds by default which makes the convergence process of EIGRP slow. To make theconvergencefaster, change "hello" and "hold" intervals of all the EIGRP routers.



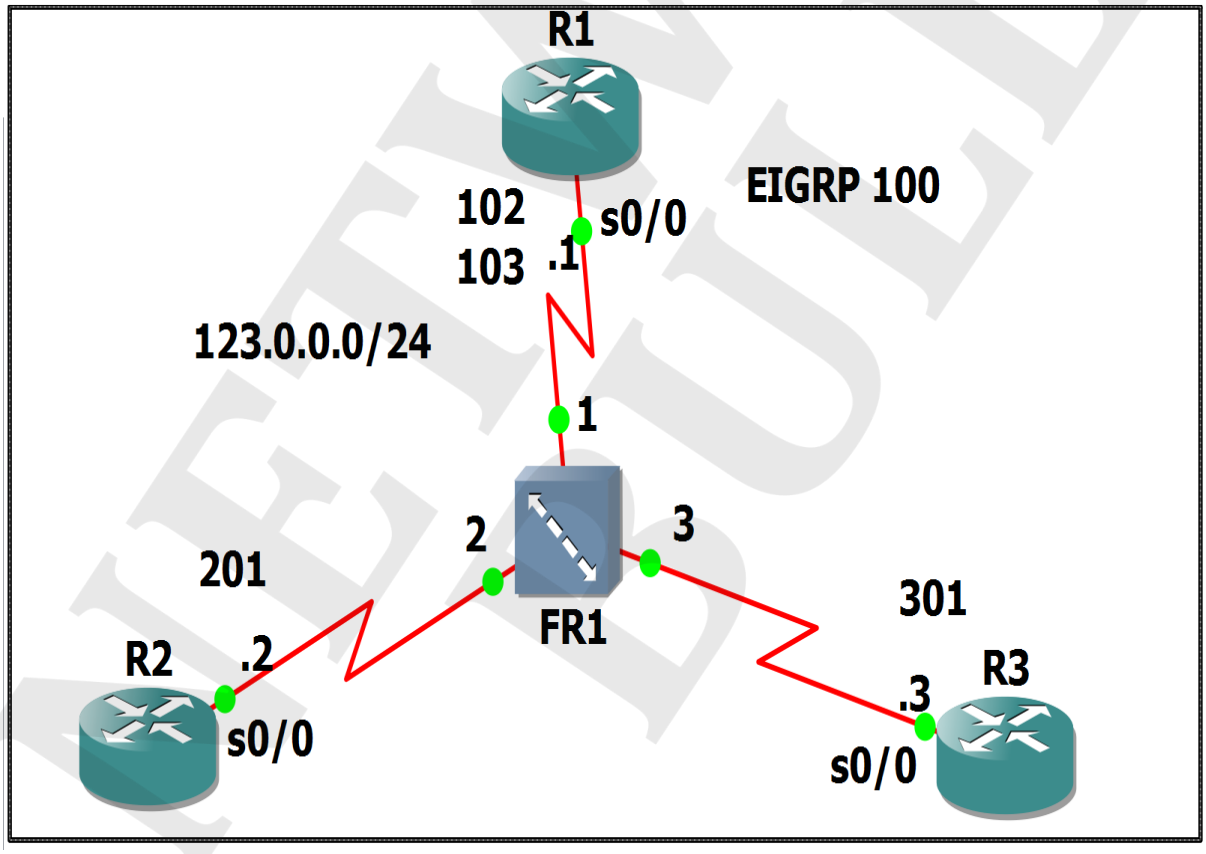
Practical 2: EIGRP Authentication

Task: Build authentication between R1 and R2 in order to authenticate every EIGRP message.



Practical 3: Static Neighborship in EIGRP

Task: To define static neighborship between R1 – R2 and R1 – R3. The condition is to configure frame-relay over EIGRP without using broadcast keyword.

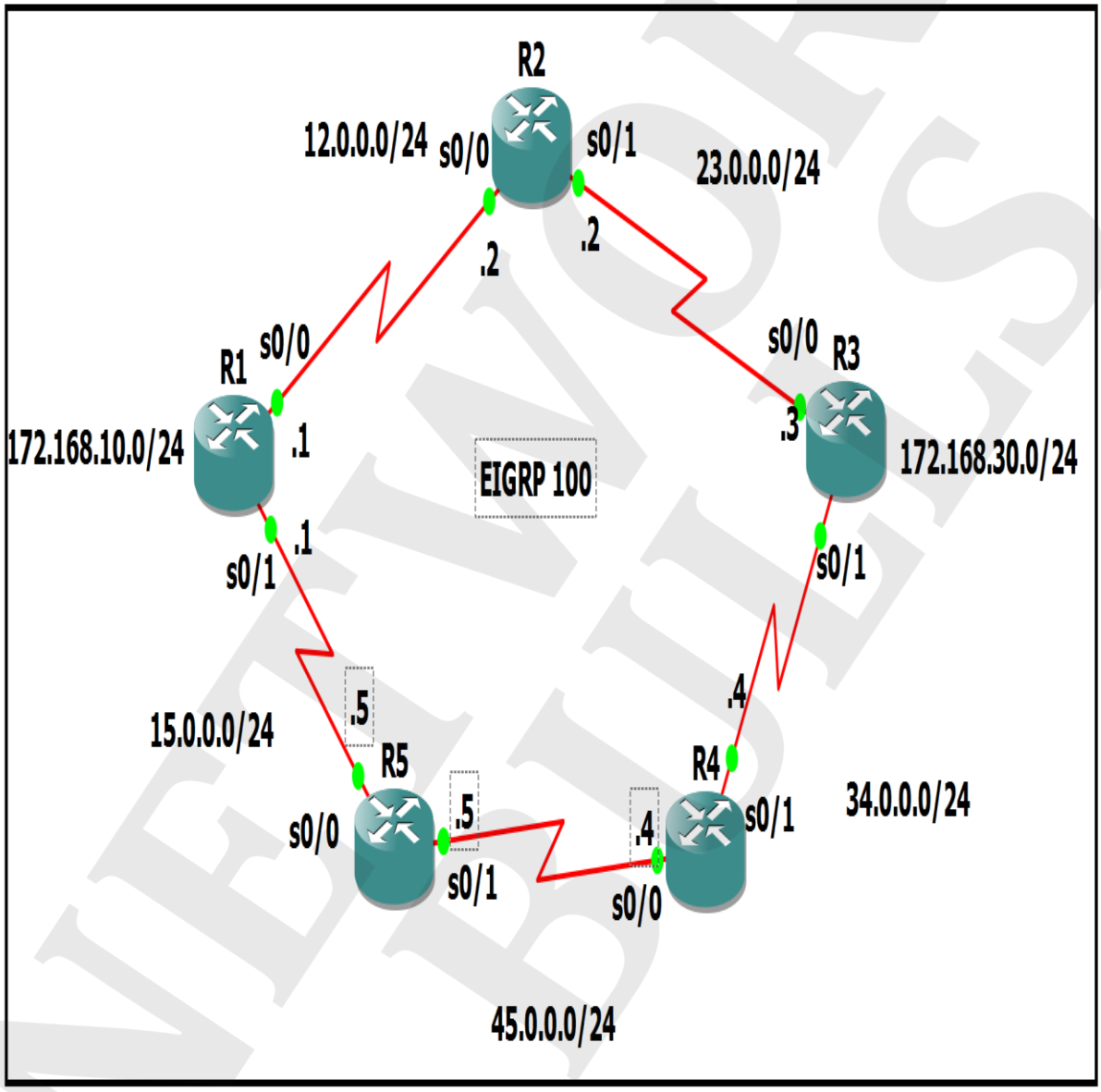


Practical 4: EIGRP Metric Tuning

The best route for the network 172.168.30.0/24 of R3 from R1 is via R2.The task is to make the route via R4 and R5 best for the network 172.168.30.0/24of R3.

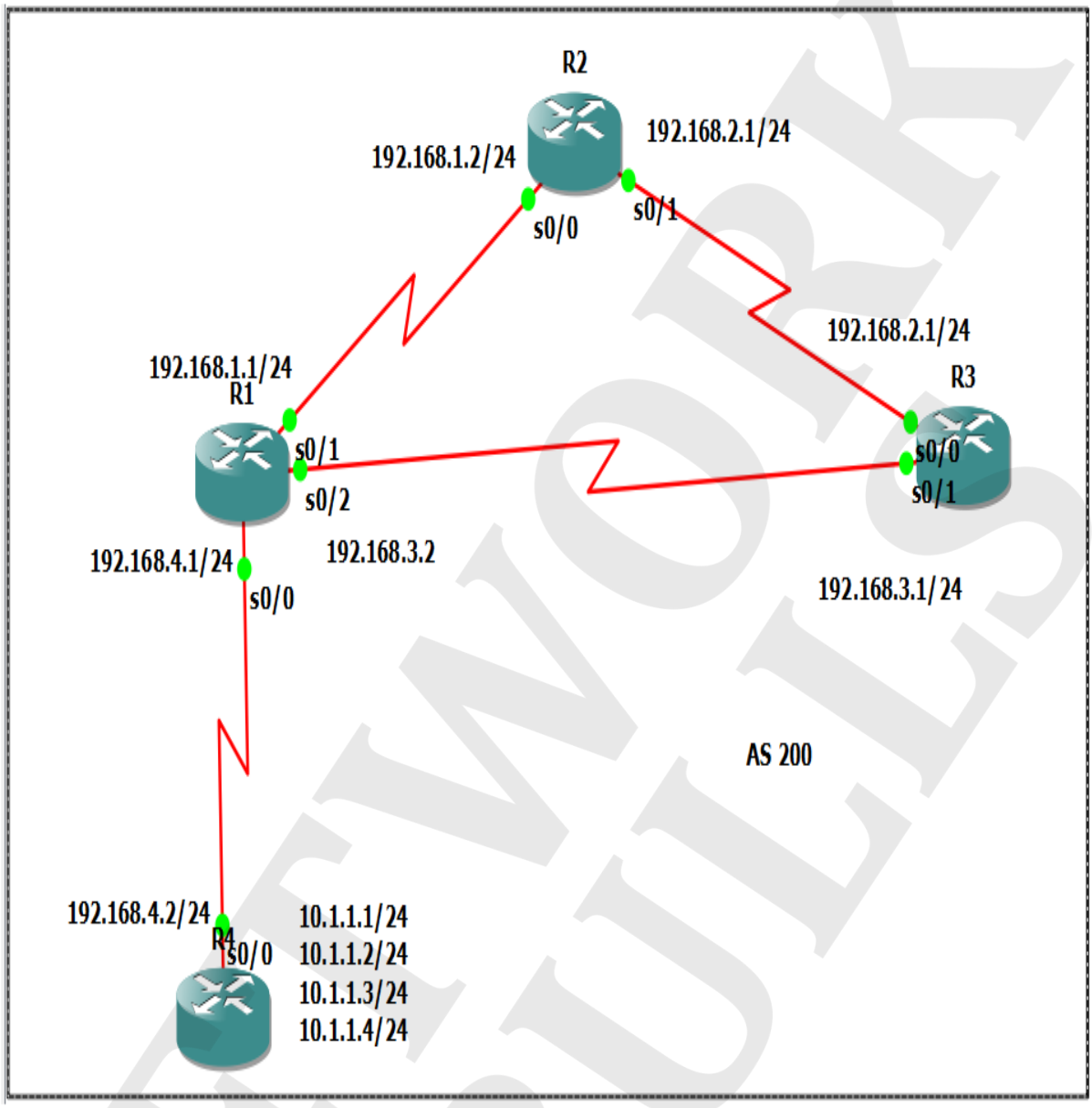
Task:

1. Configure metric values and to make the path viaR4 and R5 as the best path for the network of R3 from R1.
2. Use offset list and to make the path via R4 and R5 as the best path for the network of R3 from R1.



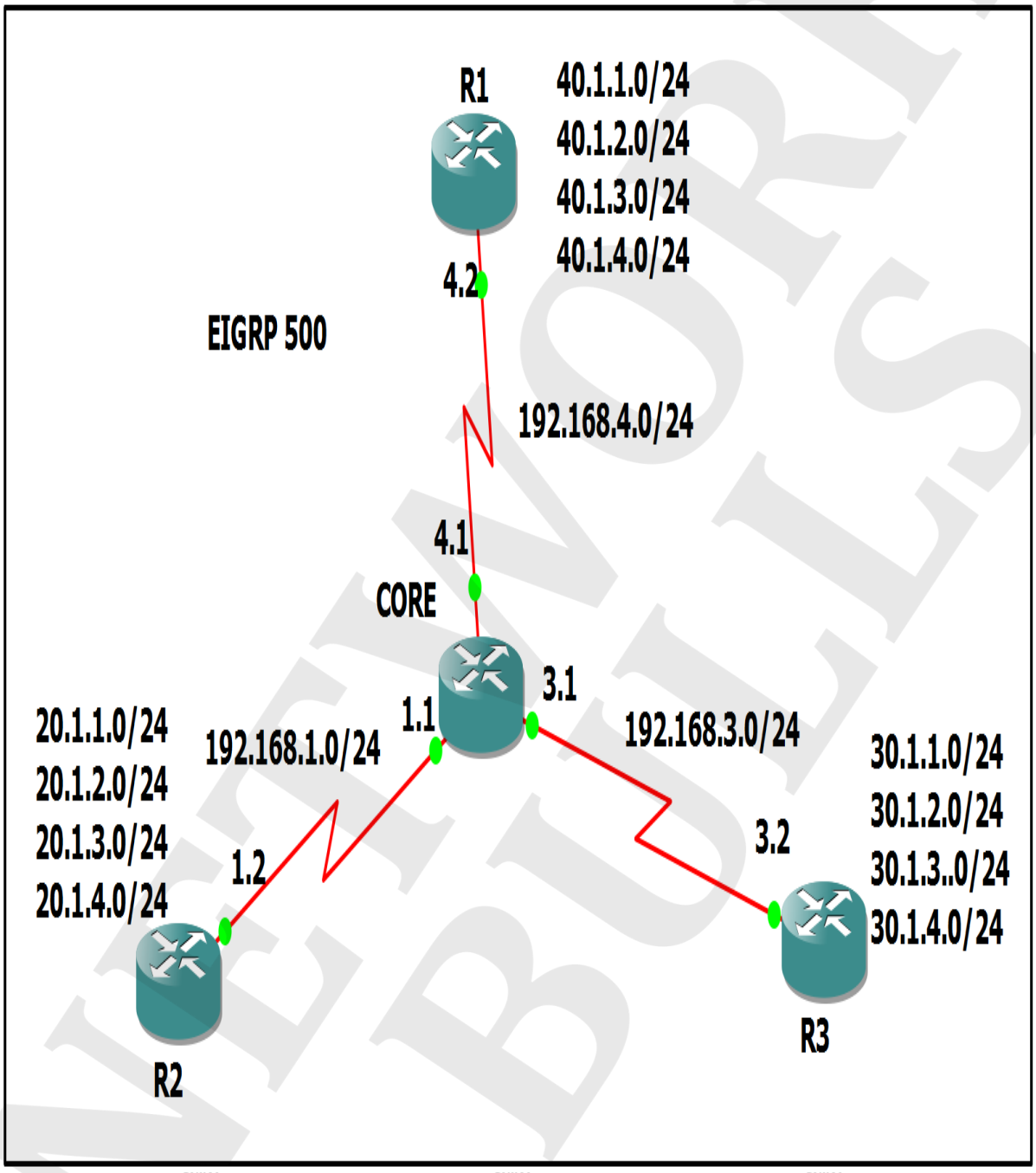
Practical 5: Route-filtering using distribute-list with a standard ACL.

Task: To filter the loopback networks of R4 from the routing table of R2 and R3.



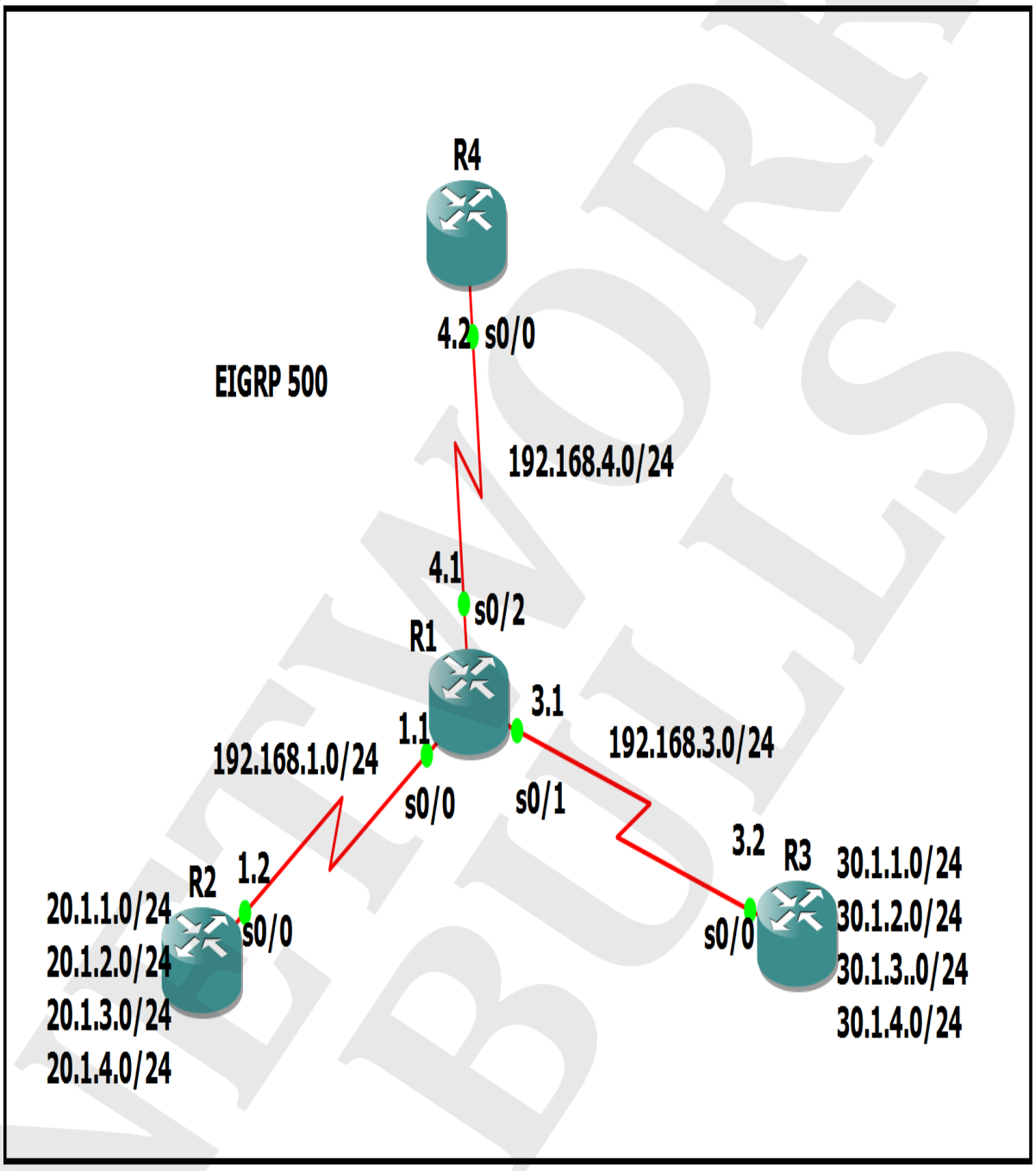
Practical 6: Route-filtering using distribute-list with an extended ACL.

Task: To filter the loopback networks of R2 from the routing table of R3 by using distribute-list with an extended ACL.



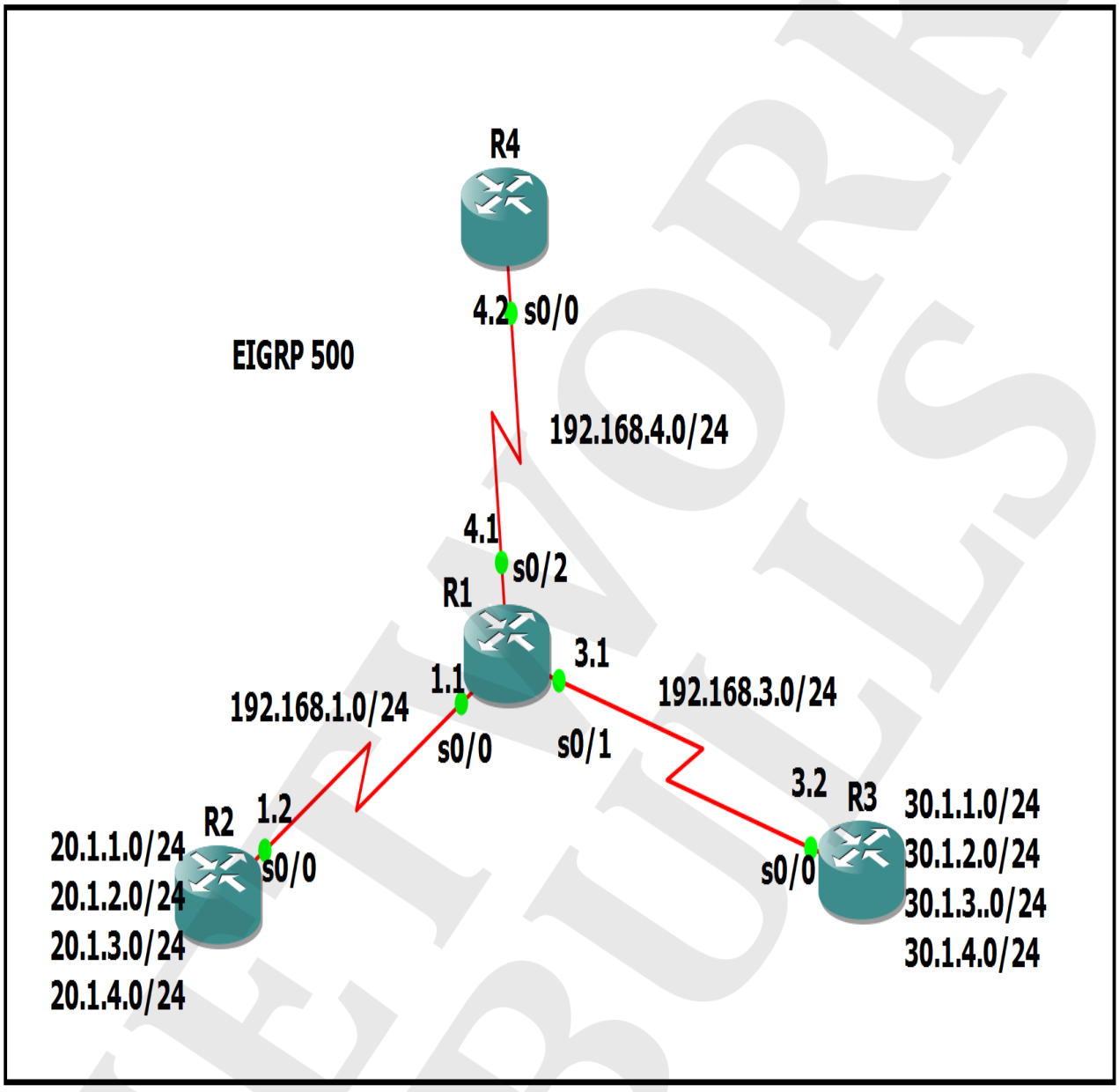
Practical 7: Route-filtering using distribute-list with a Route-map.

Task: To filter the loopback networks ofR2 from the routing table ofR3usingdistribute-list with a route-map.



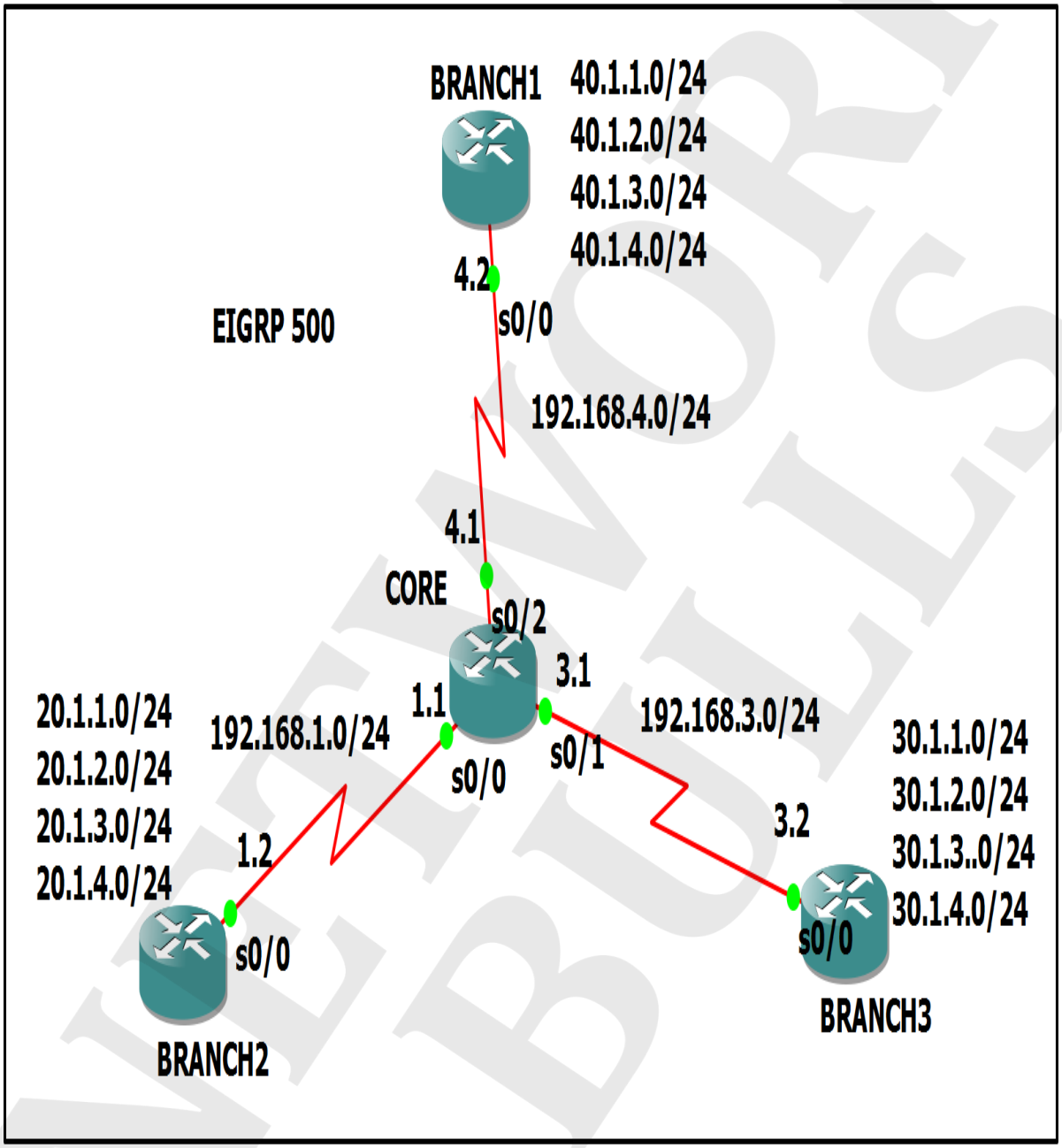
Practical 8: Route-filtering using distribute-list with an IP prefix-list.

Task: To filter routes of R3 from the routing table of R2 using IP prefix-list.



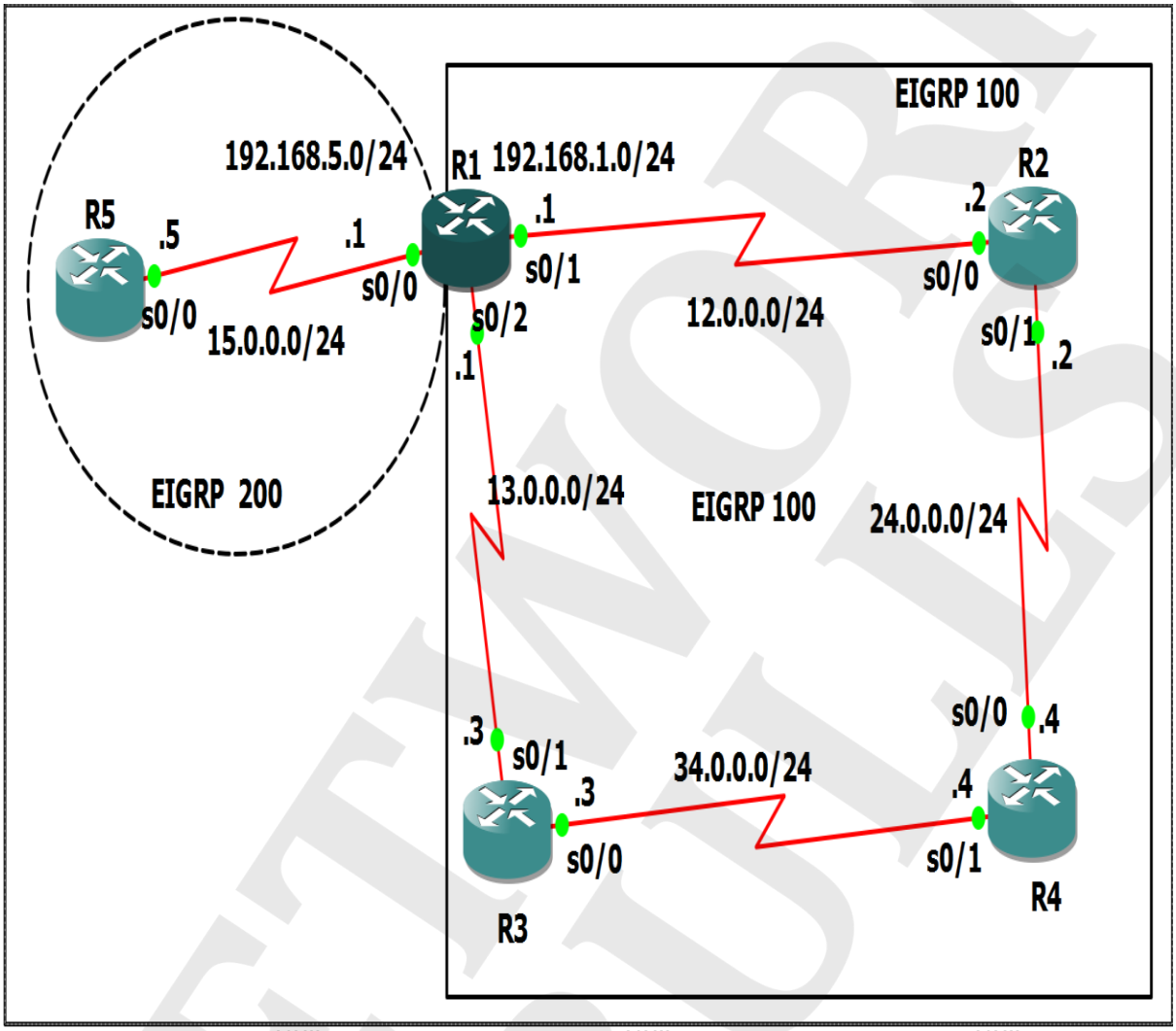
Practical 9: Route Summarization

Task: To summarize routes of all the branches so that the core will get only summary route of all the branches instead of individual routes.



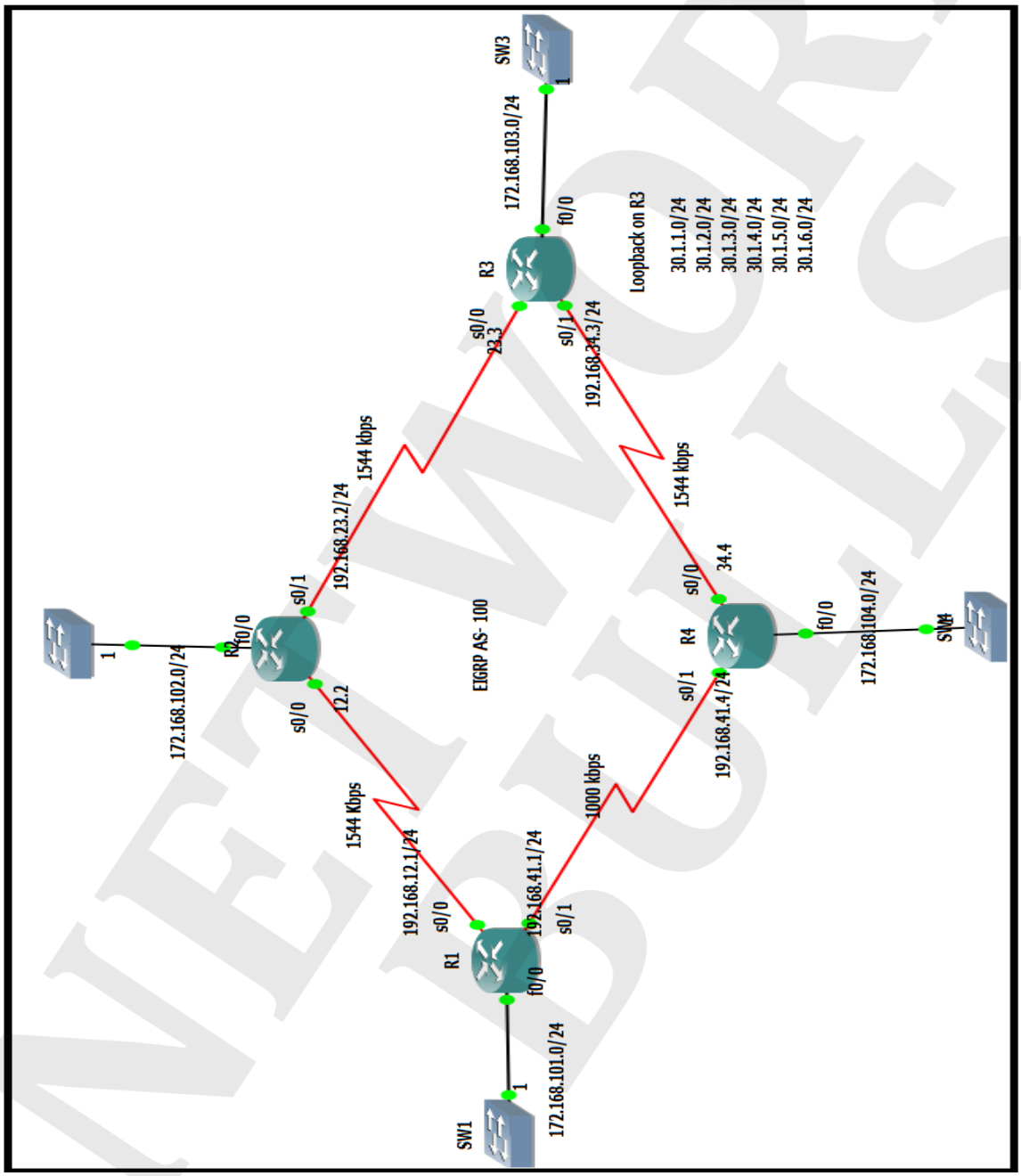
Practical 10: EIGRP Default Routing

Task: Configure default routing on R1to perform routing between two different AS (AS 100 and AS 200) of the EIGRP.



Practical 11: Unequal Cost Load Balancing

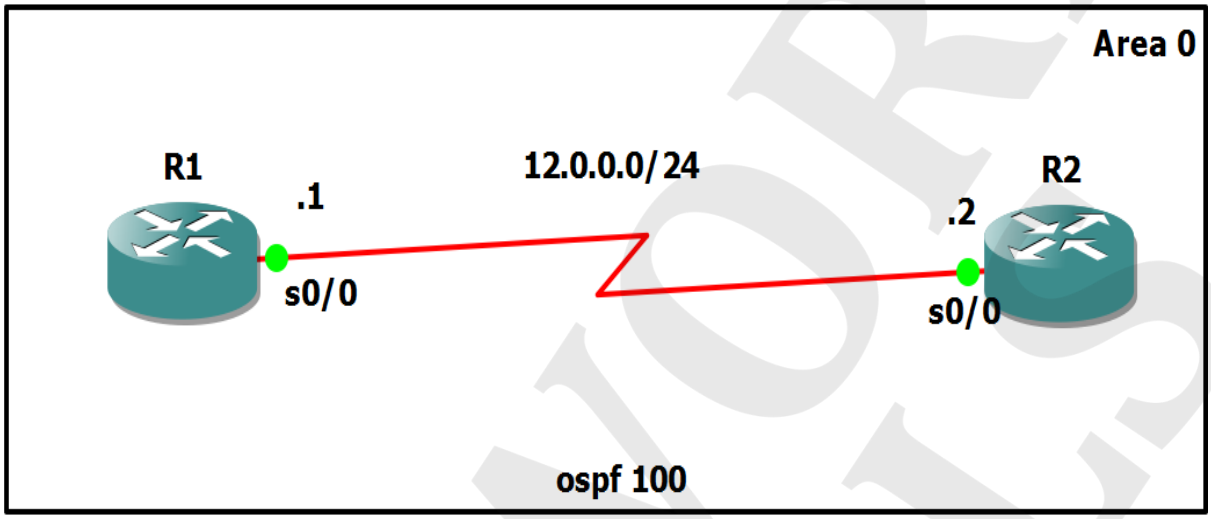
Task: By default R1 is receiving all loopback network of R3 from its neighbor R2. So whenever R1 will send any traffic towards loopback interfaces of R3 it will follow the path via R2. However, R1 is having two links towards the R3's networks. Now user wants to perform load balancing on both of the existing links for networks of R3.



OSPF Authentication:

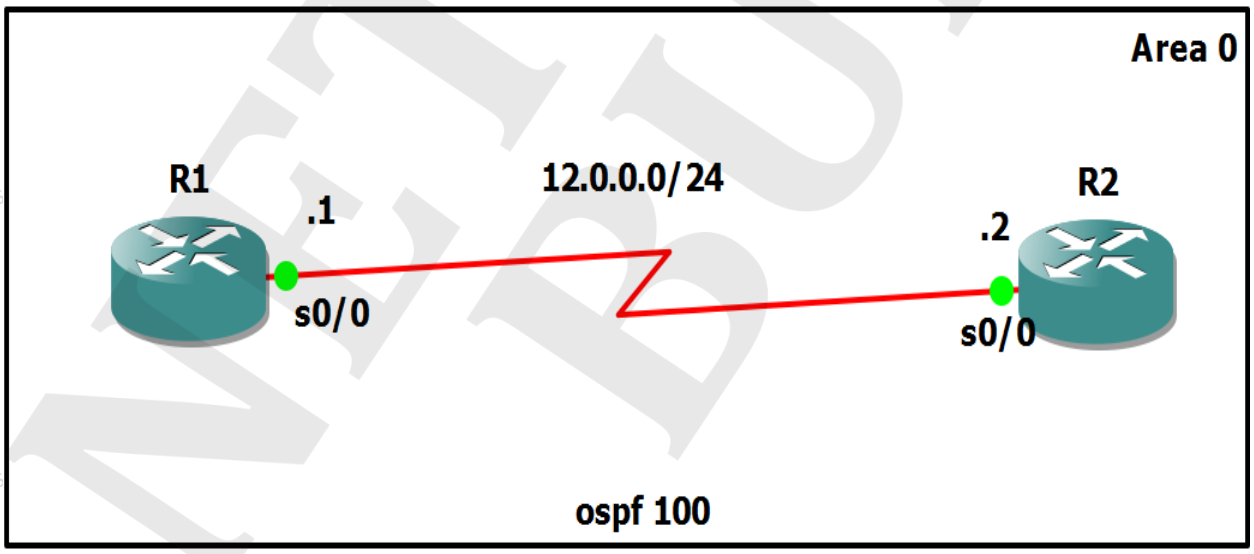
Practical 12: Clear Text Authentication.

Task: To configure type-1 authentication between R1 and R2 which authenticates OSPF neighbors.



Practical 13: MD5 authentication

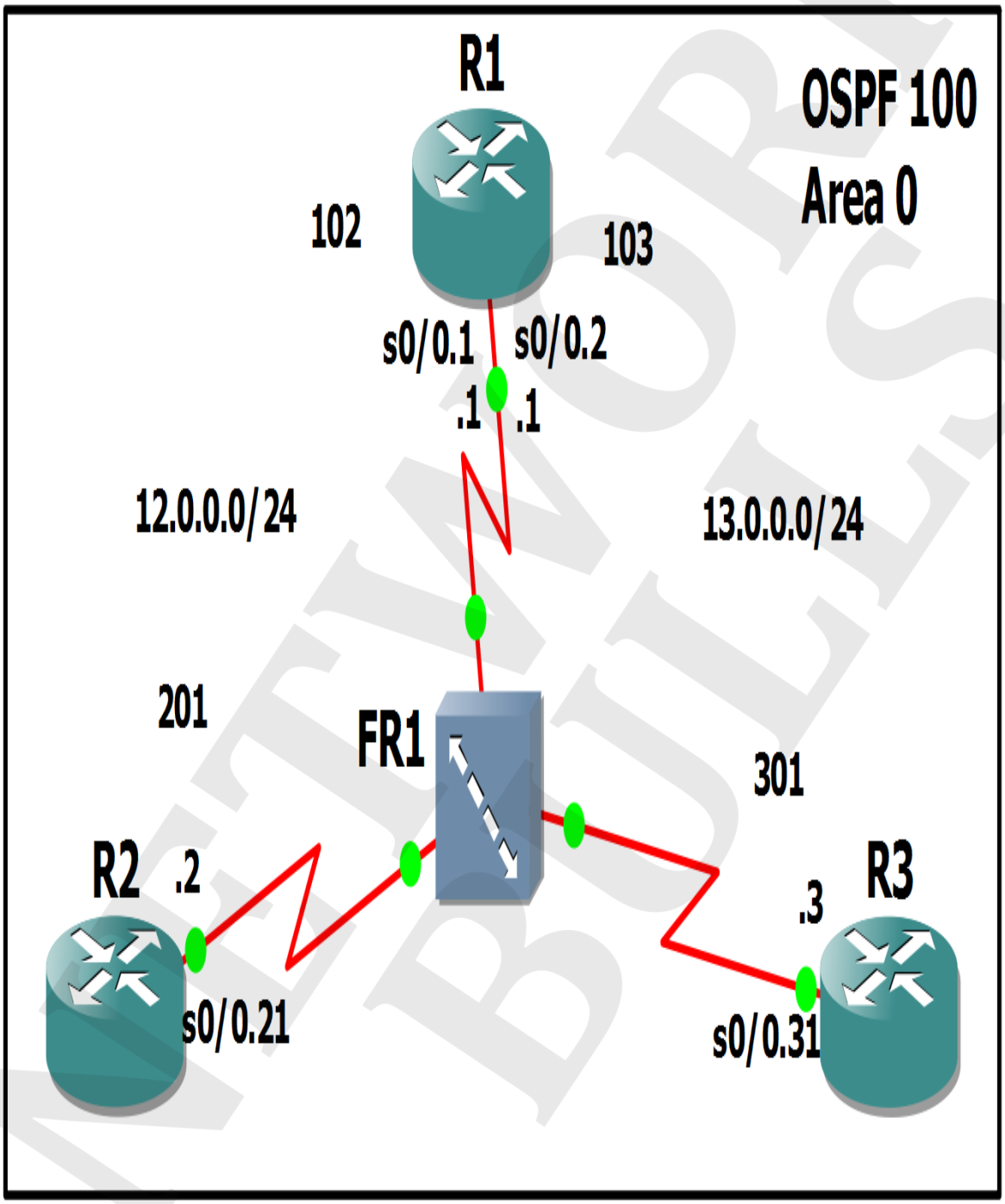
Task: To configure type-2authentications between R1 and R2.Also verify the configuration.



OSPF Network Types

Practical 14: OSPF point-to-point network

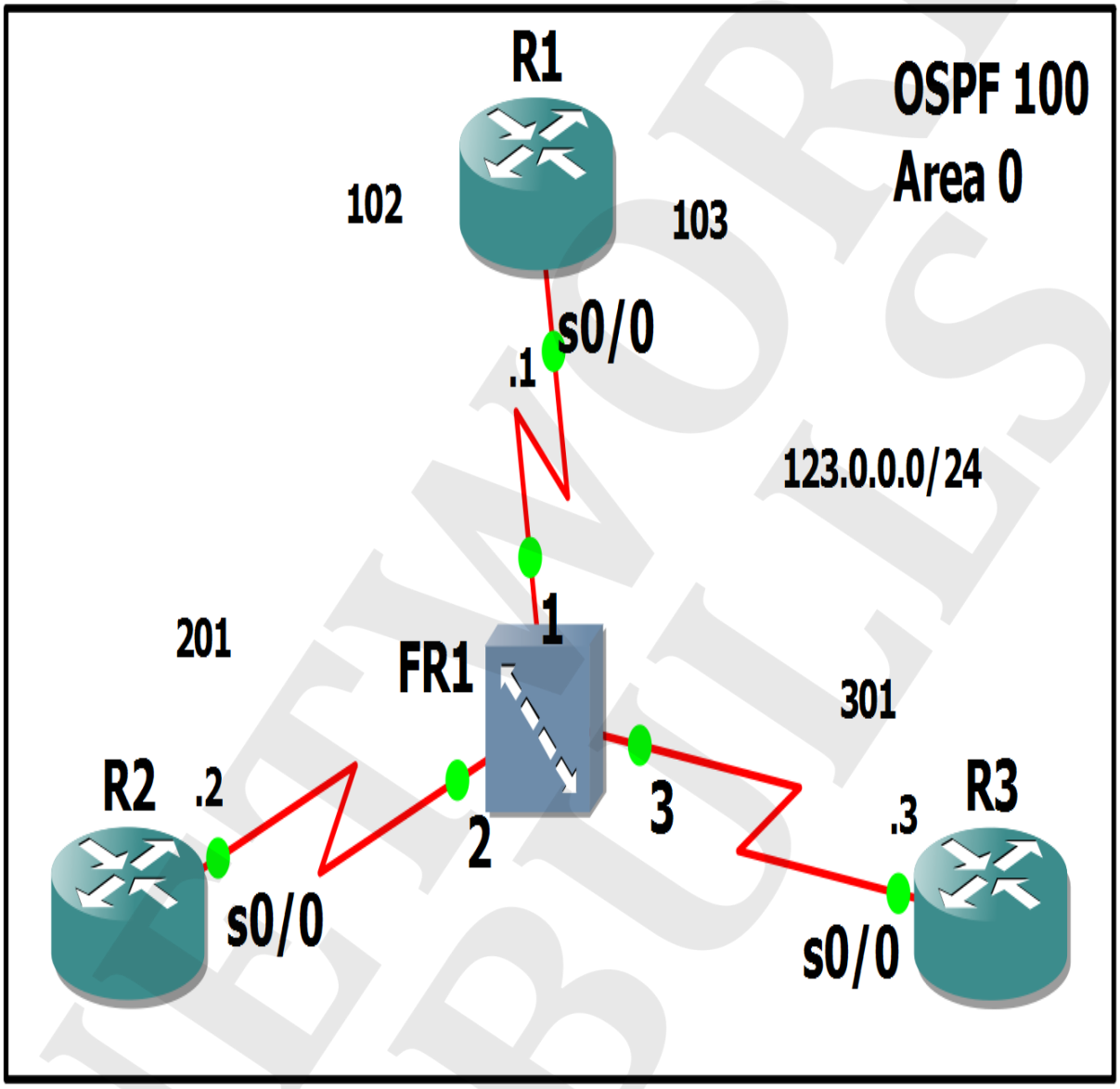
Task: To configure neighborship over frame-relay point-to-point sub-interfaces and to verify the configuration.



Practical 15: OSPF Broadcast network

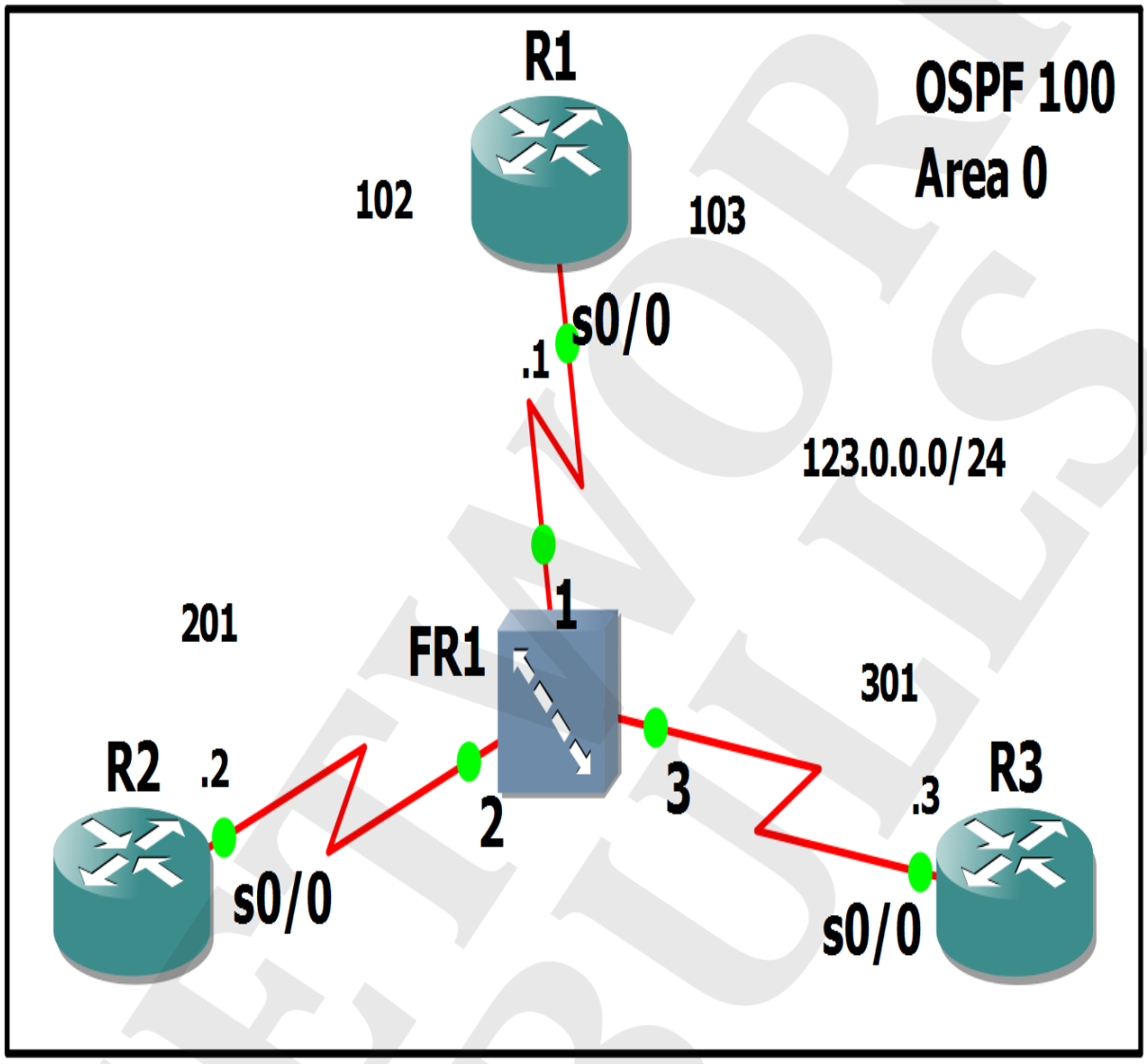
Task:

1. To configure OSPF broadcast network type over Frame-Relay hub and spoke network and to verify DR and BDR.
2. To configure spoke routers so that they never participate in DR and BDR election.



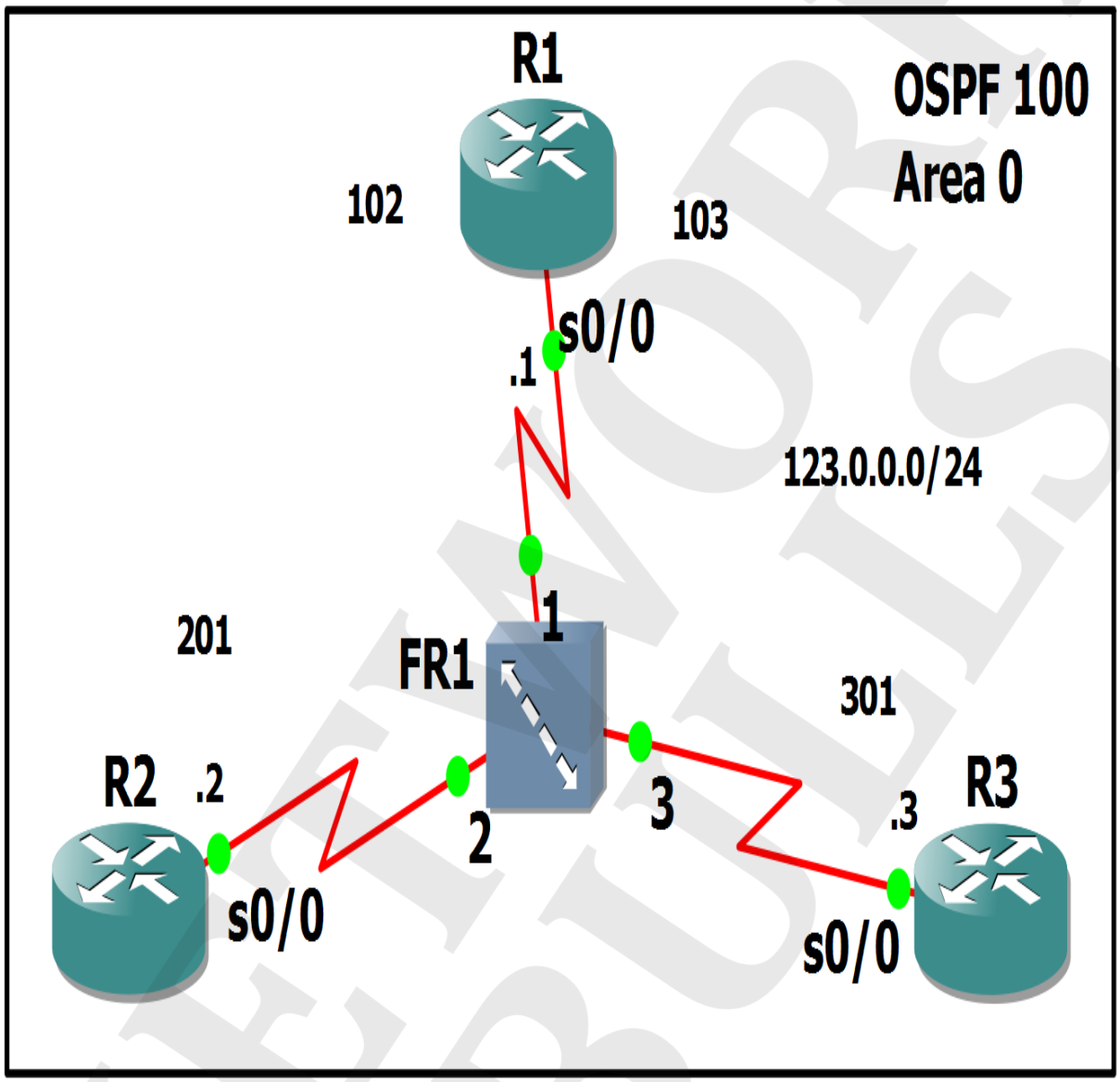
Practical 16: OSPF Non-Broadcast Multi Access (NBMA) network

Task: To configure OSPF Non-Broadcast Multi Access network on Frame Relay and to verify the configuration.



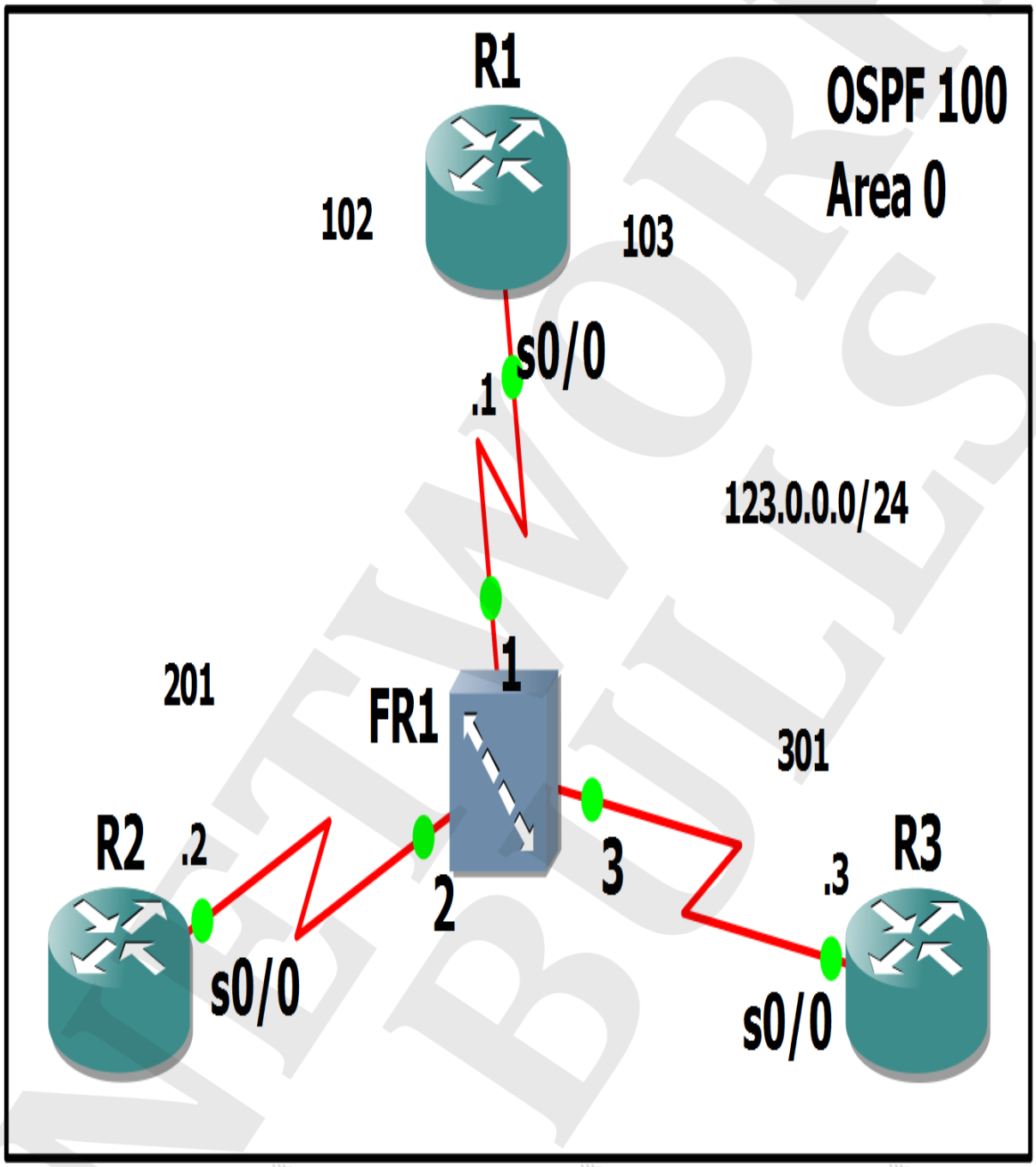
Practical 17: OSPF point-to-multipoint network

Task: To configure point to multipoint network on Frame Relay and verify the configuration.



Practical 18: OSPF Point-to-Multipoint Non-Broadcast network

Task: To configure point-to-multipoint network in Frame Relay and verify the configuration.

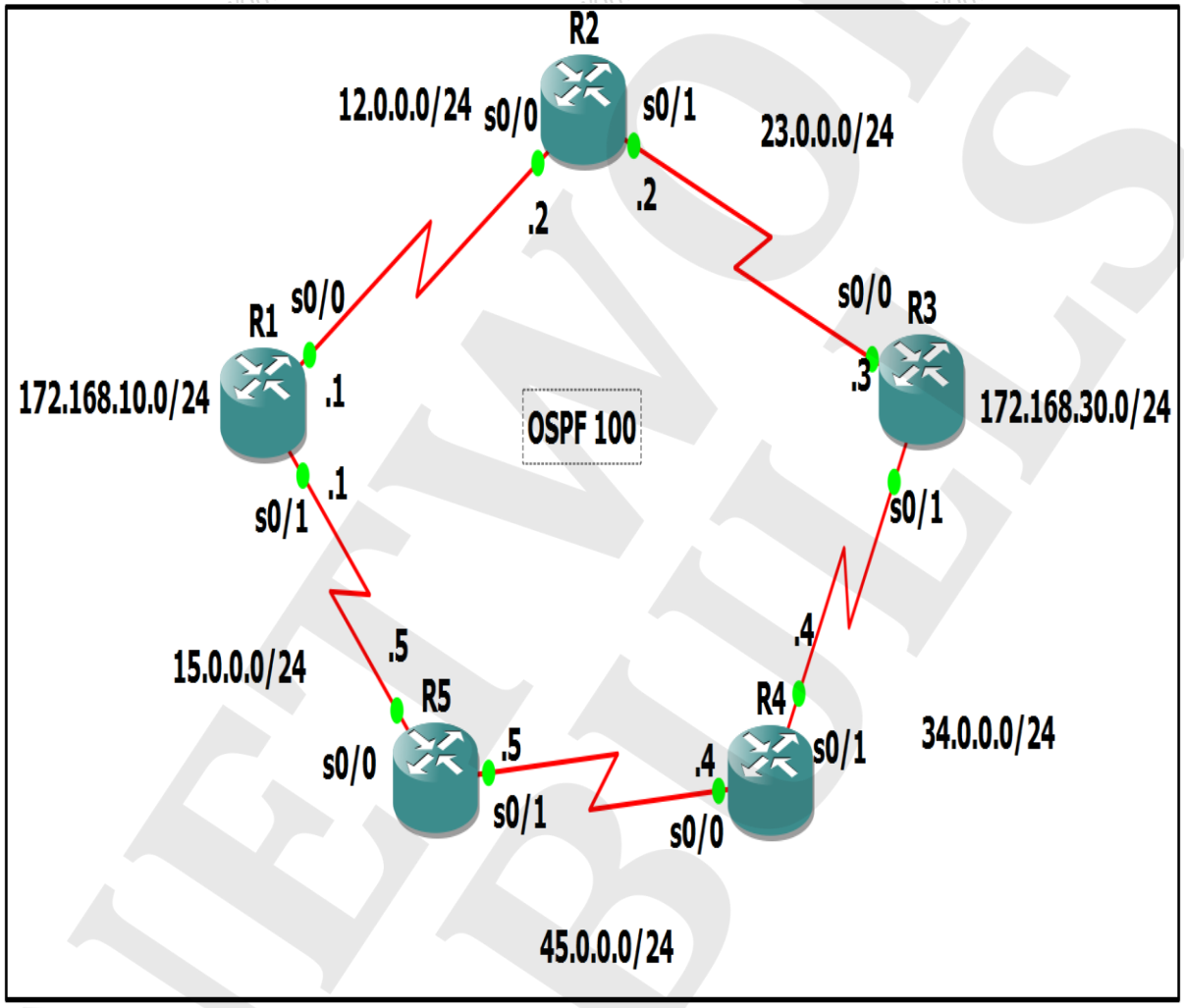


Practical 19: OSPF metric tuning

The best route for the network 172.168.30.0/24 of R3 from R1 is via R2.The task is to make the route via R4 and R5 which is best for the network 172.168.30.0/24of R3.

Task: To configure the metric values and to make the path via R4 and R5 as the best path fornetwork of R3 from R1:

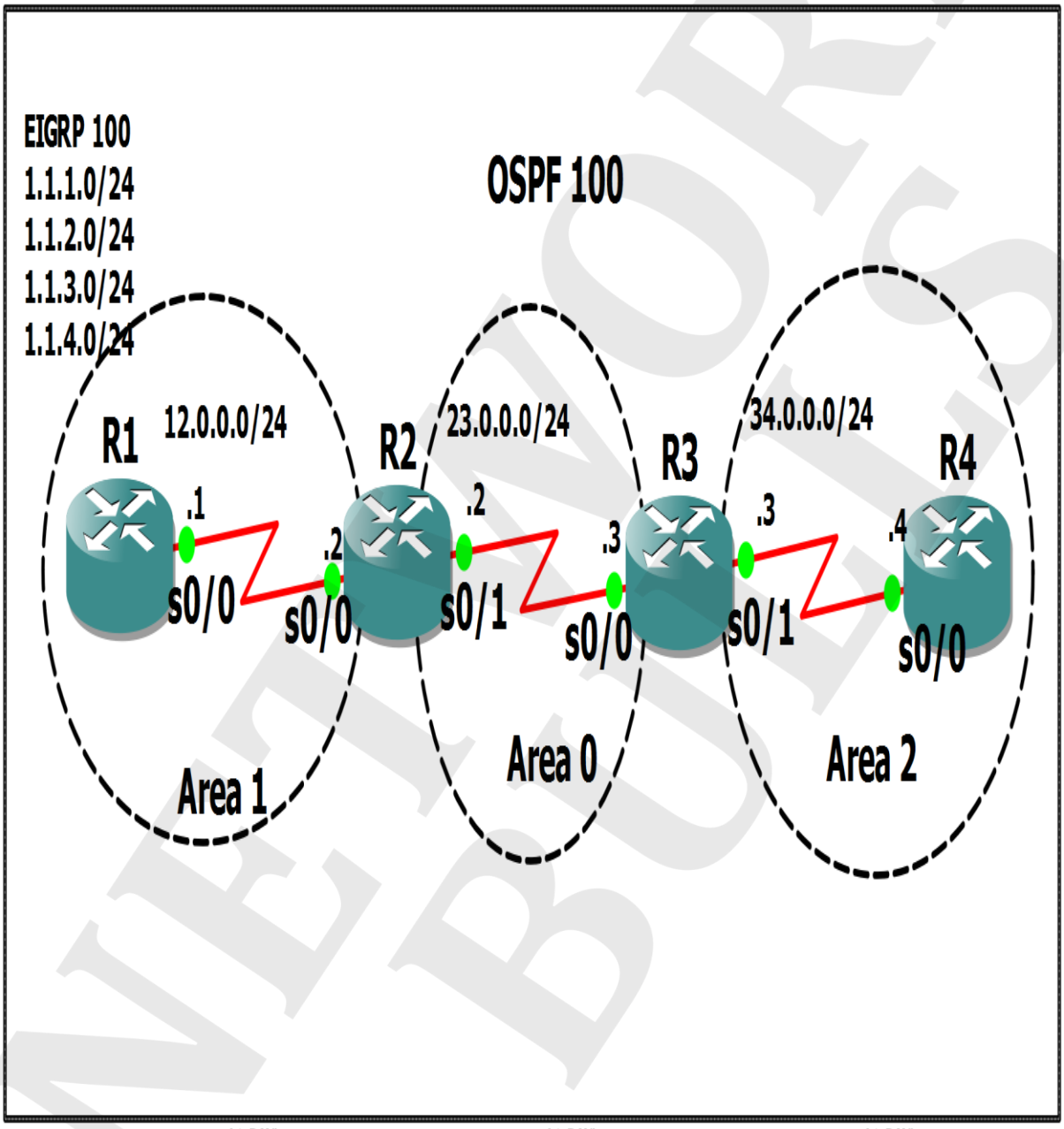
1. **Change Reference bandwidth**
2. **Changing cost**



Practical 20: OSPF stub and totally stub area

Task:

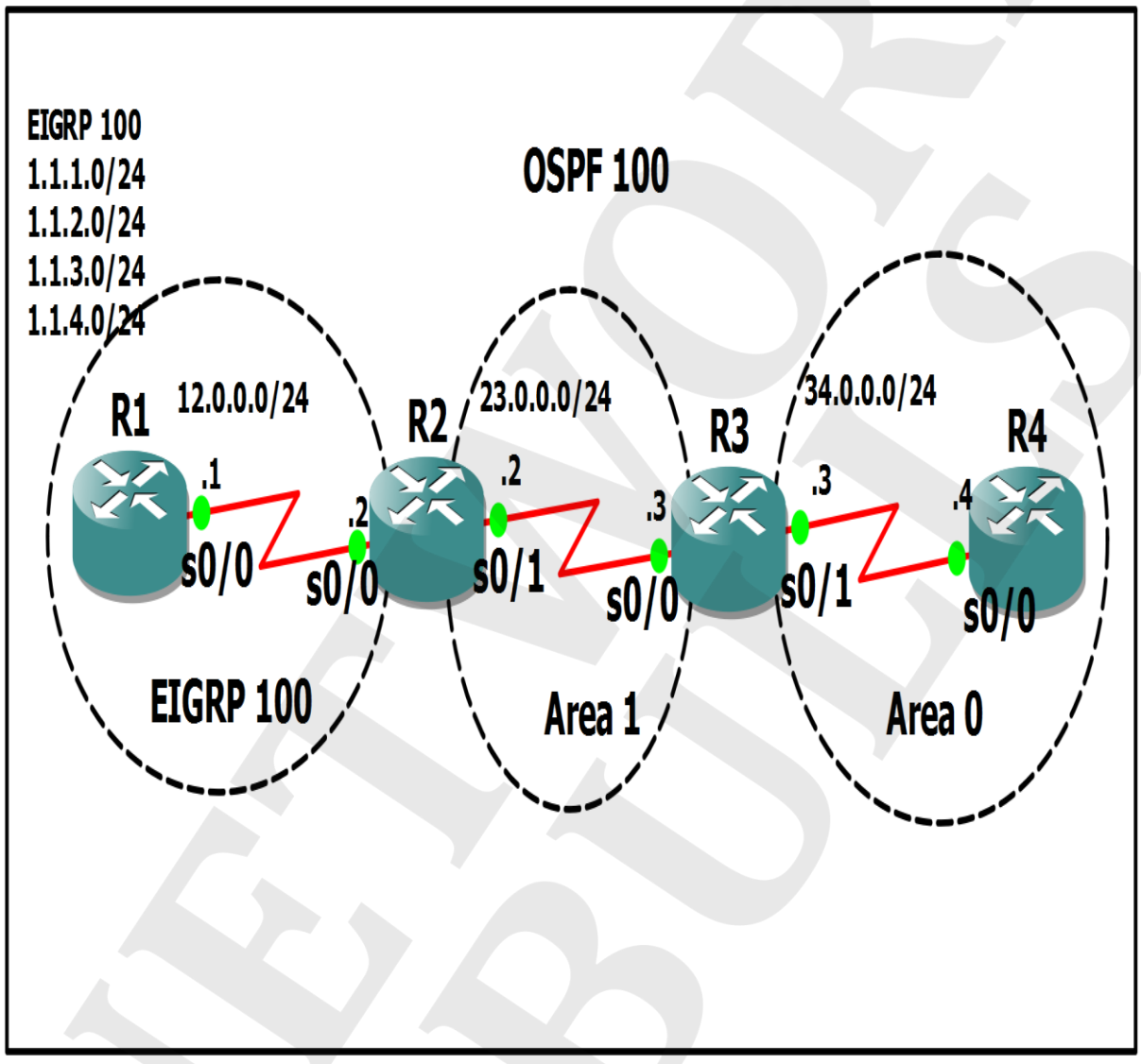
1. To configure area 2 as a stub area and to verify its effect on the network.
2. To configure the area 2 as a totally stub area and to verify its effect on the network.



Practical 21: NSSA and total NSSA

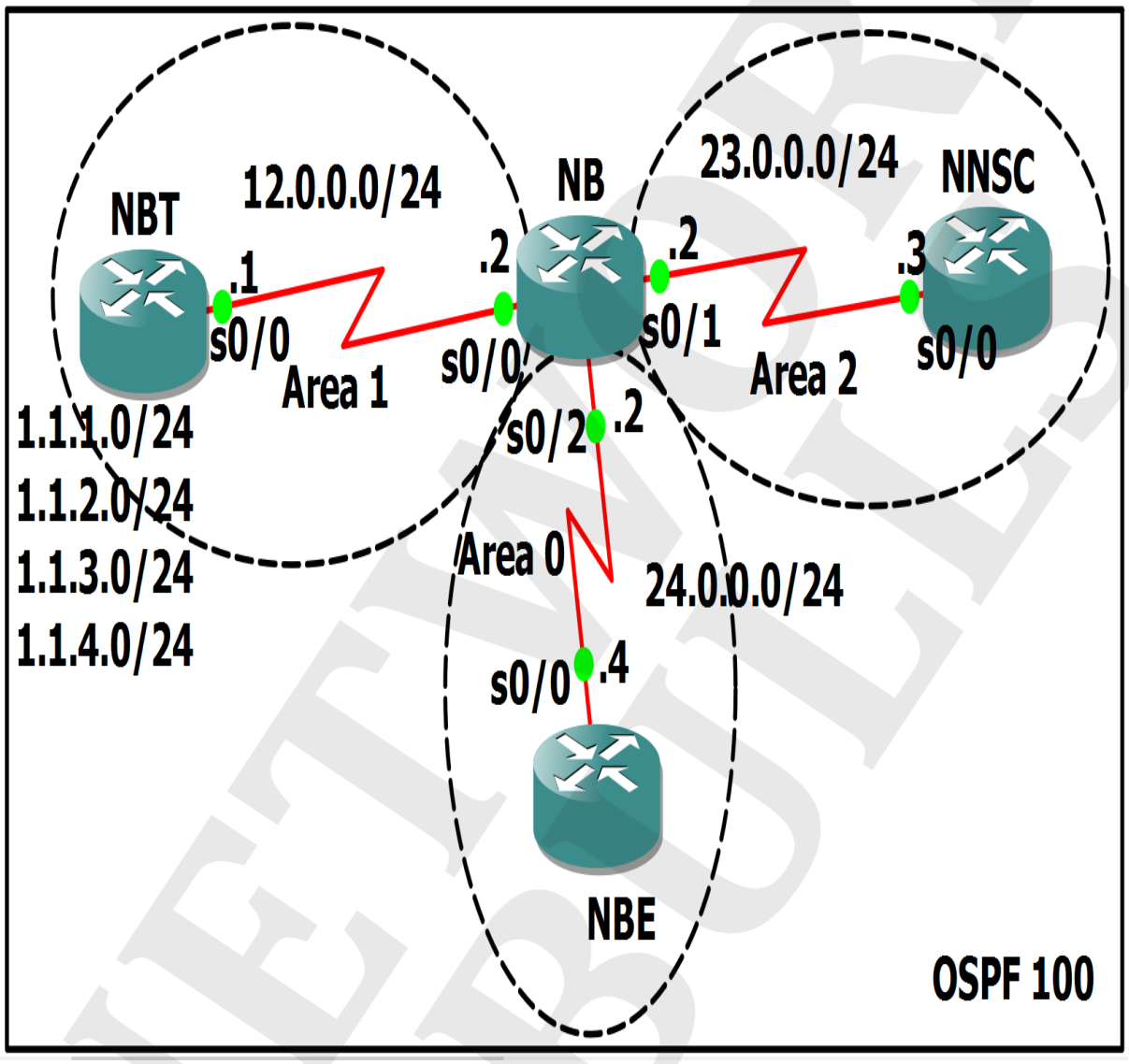
Task:

1. To configure area 1 as a NSSA and to verify its effect on the network.
2. To configure area 1 as a totally NSSA and to verify its effect on the network.



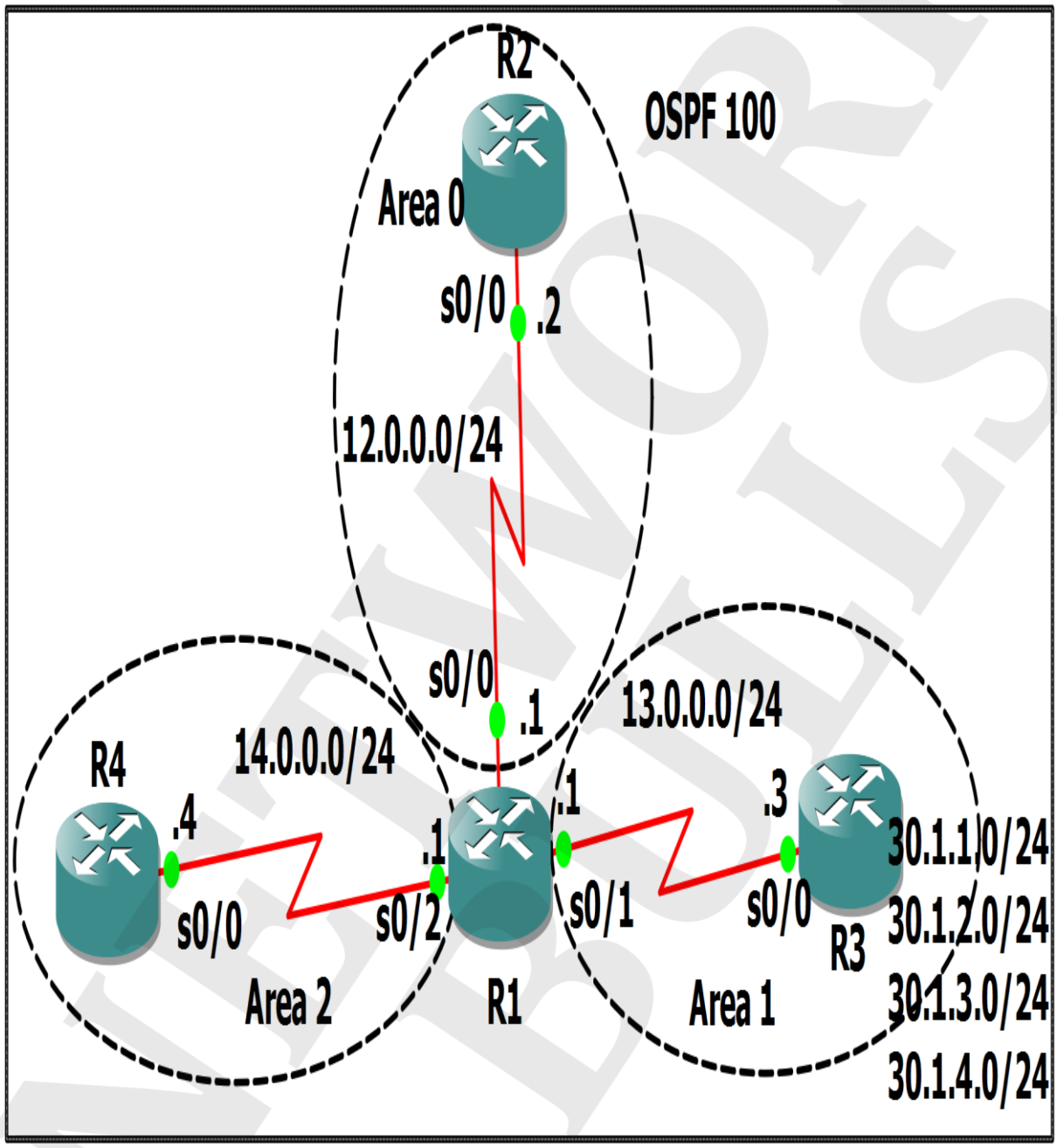
Practical 22: Type-3 LSA filtering using Area-filter list

Task: Toconfigure type-3 LSA filtering so that NB router which is an ABR, filters type-3 LSA are sent to the area 2. Also verify that NNSC can never receive routes of NBT where NBE still continues to receive routes of NBT.



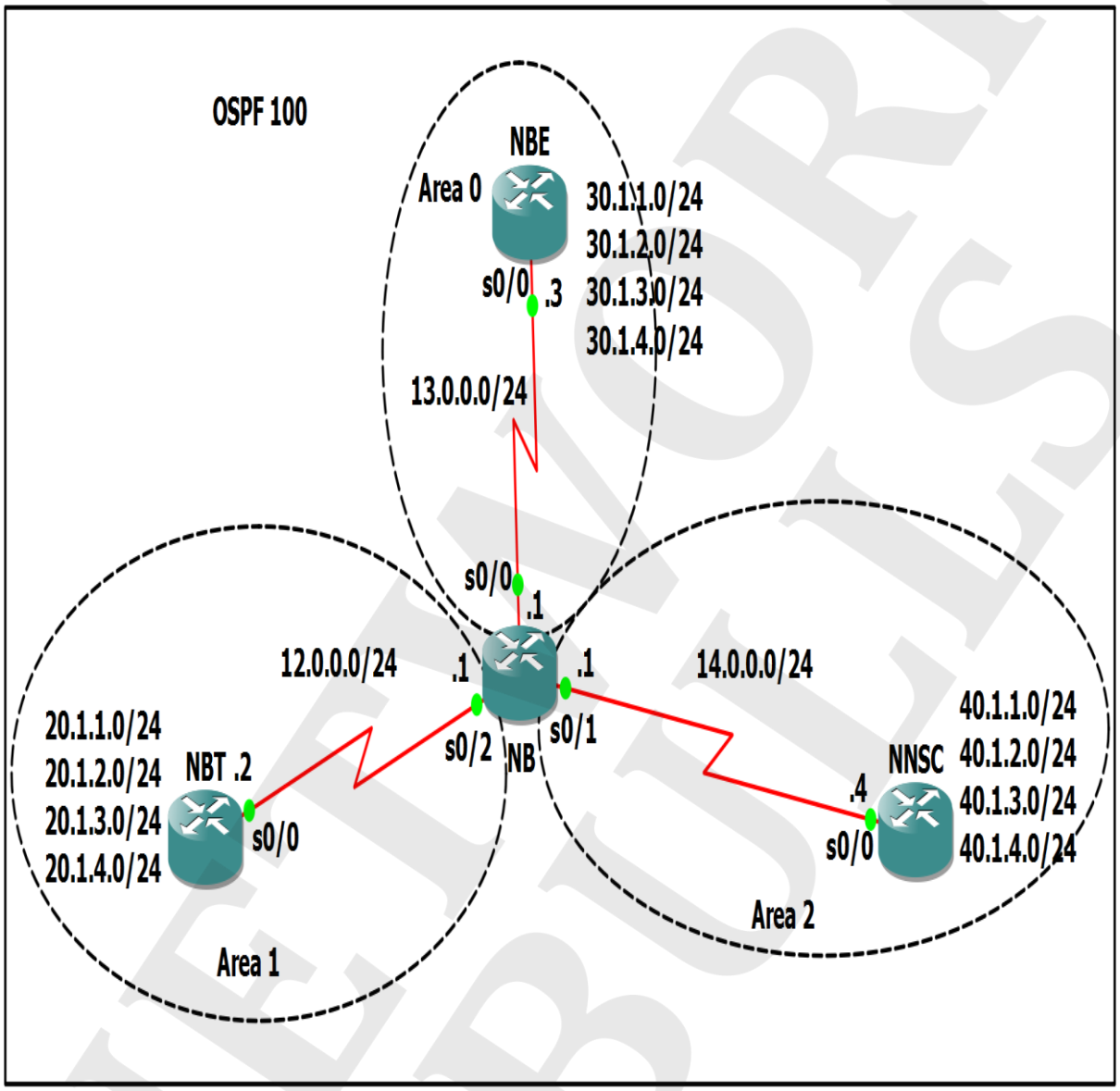
Practical 23: Route-filtering in OSPF with a distribute-list

Task: Toconfigure route-filtering using distribute-list with ACL so that R2 never receives routes of R3.



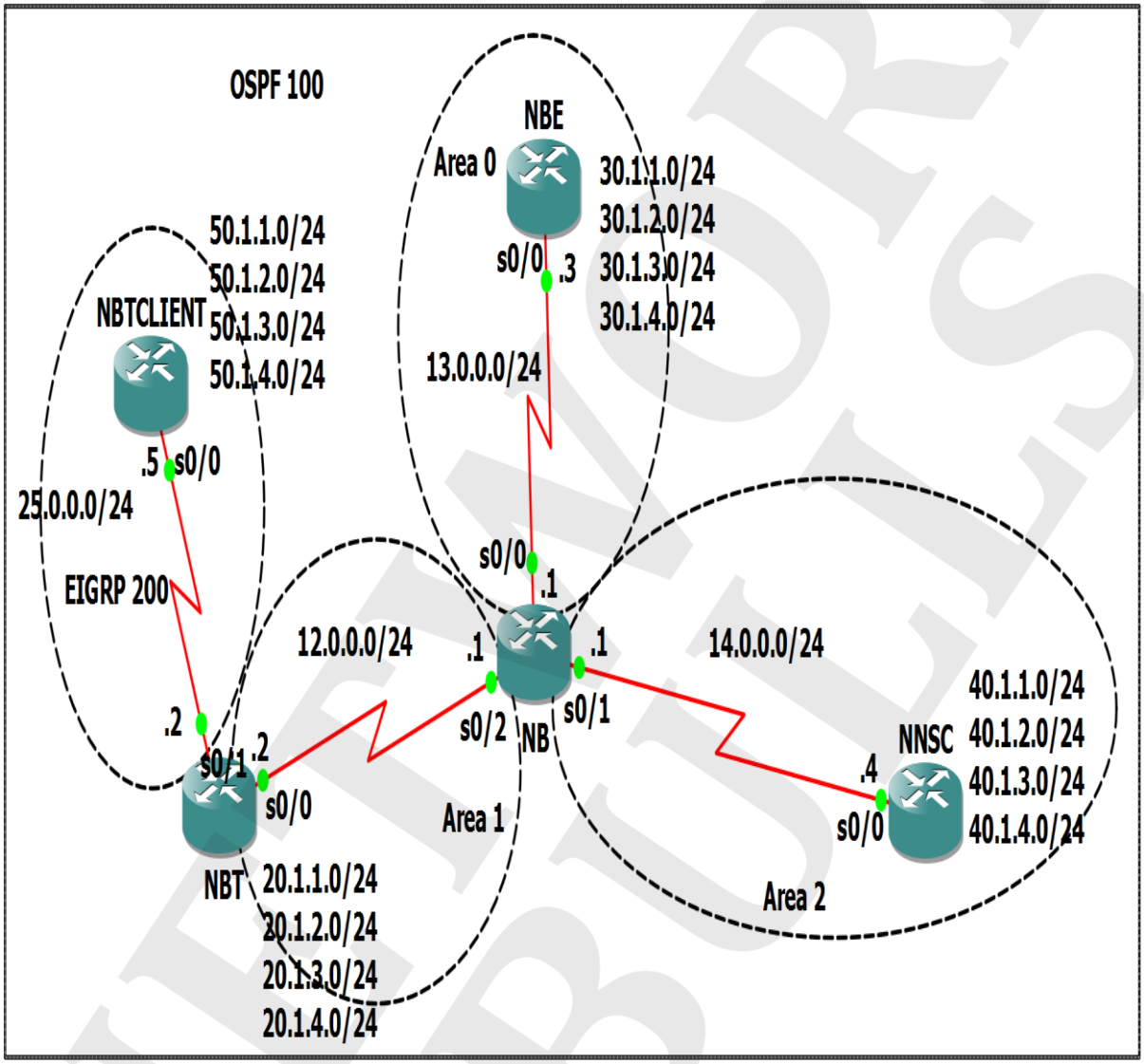
Practical 24: Summarization at ABR

Task: To configure summarization at NB which is ABR. This will make all the branches of NB (NBE, NNSC and NBT) to receive the routes of the other branches in a summarized manner.



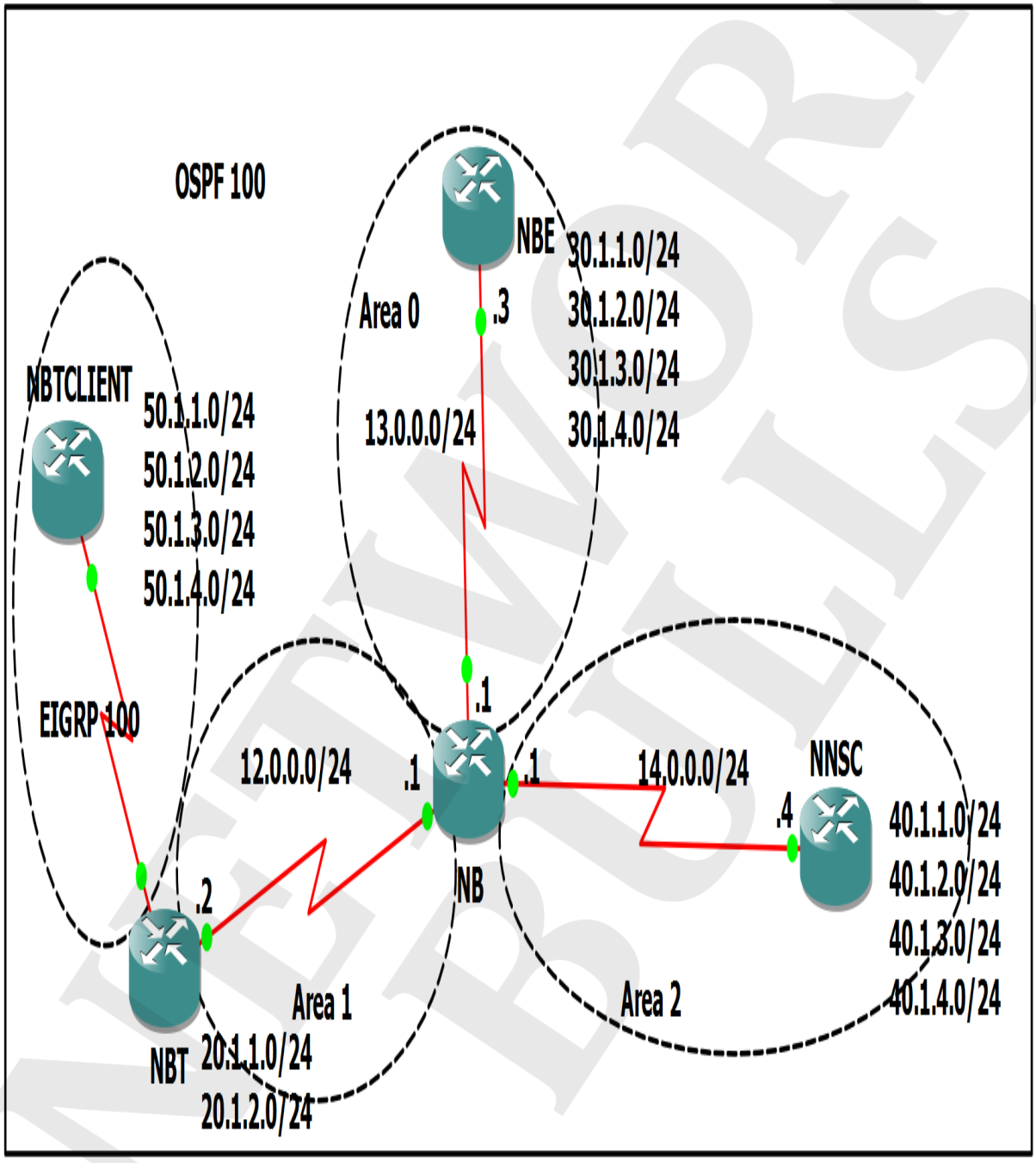
Practical 25: Summarization at ASBR

Task: To configure summarization at NBT. Summarization is configured on an ASBR router i.e. NBT which will make all the other branches of NB. This will make these branches receive routes of NBTCLIENT in a summarized manner.



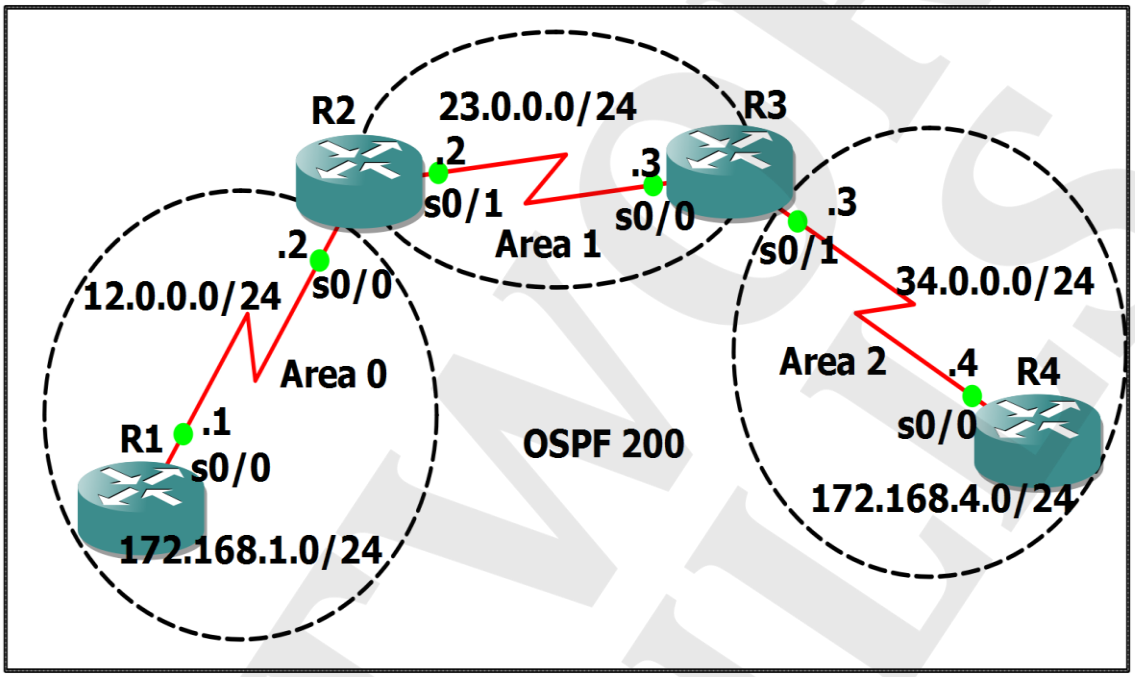
Practical 26: Default Routing in OSPF

Task: To configure default routing at NBT in order to perform routing between OSPF and EIGRP domain. Condition is that OSPF routes must be redistributed under EIGRP domain.



Practical 27: OSPF Virtual link with no authentication

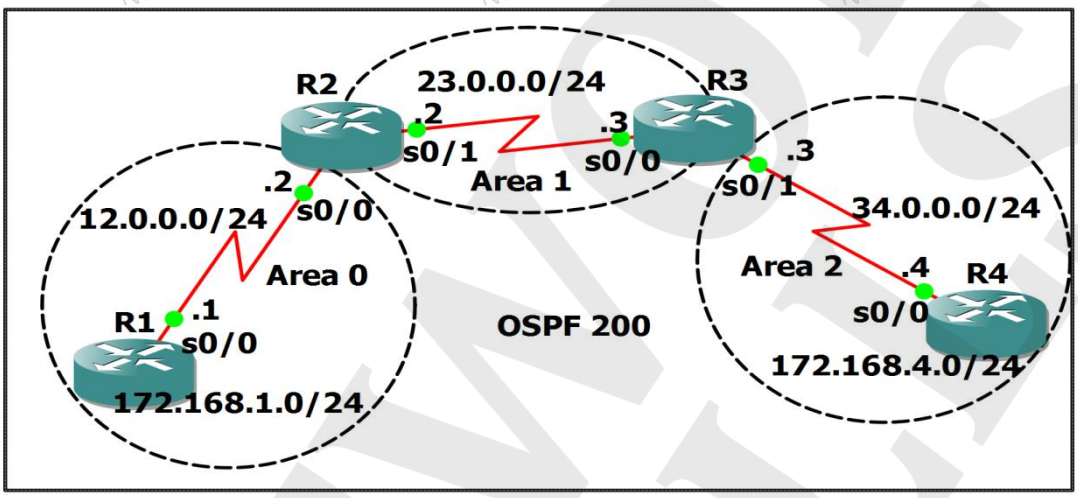
Task: To configure virtual-link between R2 and R3 without using authentication. This virtual-link connects area 2 to area 0 which is the backbone area.



Practical 28: OSPF Virtual link with authentication

Task: To configure virtual-link between R2 and R3 using authentication. This virtual-link connects area 2 to area 0 which is the backbone area.

1. Using Simple authentication
2. Using MD5 authentication



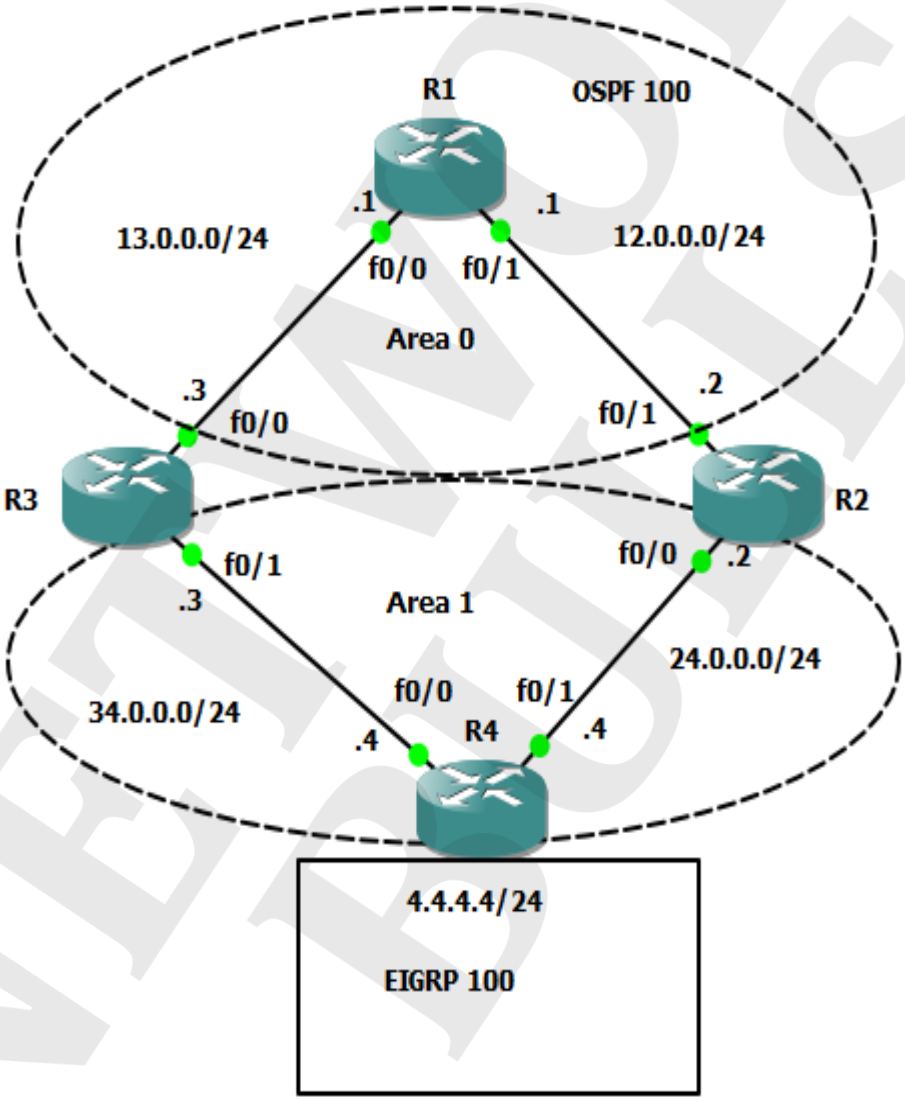
Routing Advanced Practicals

Practical Topologies

Practical 29: OSPF

Task:

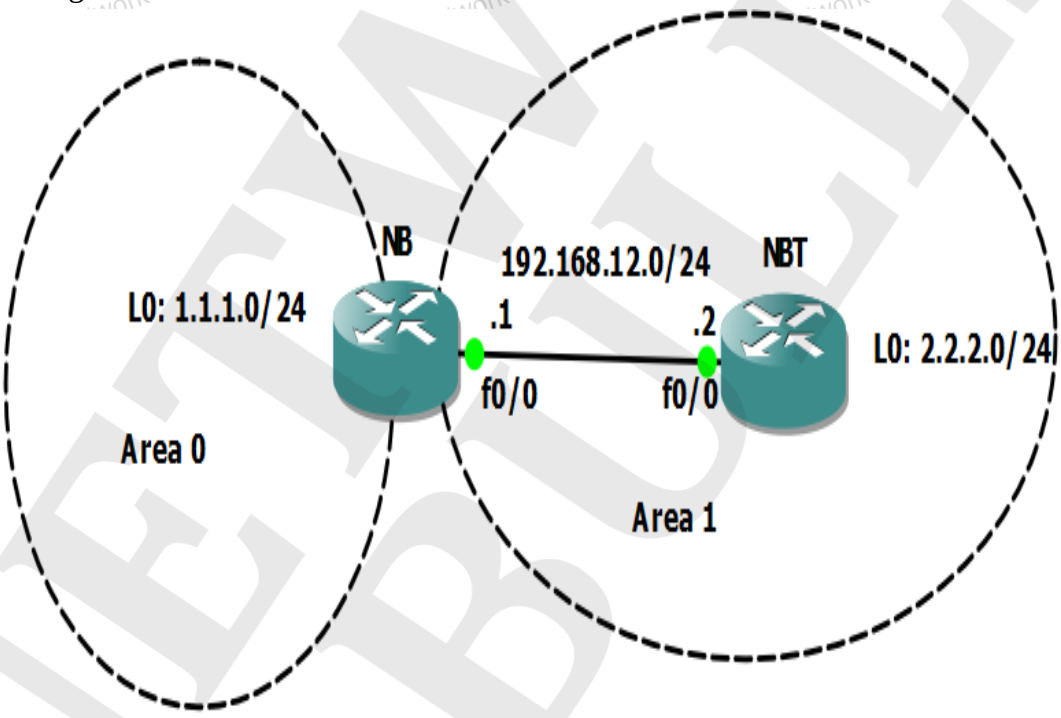
1. To configure OSPF area 1 as NSSA.
2. To redistribute loopback 0 interface of R4 into OSPF area 1.
3. To ensure router R3 is the router performing the translation from LSA 7 to type 5 into area 0.



Practical 30: OSPF

Task:

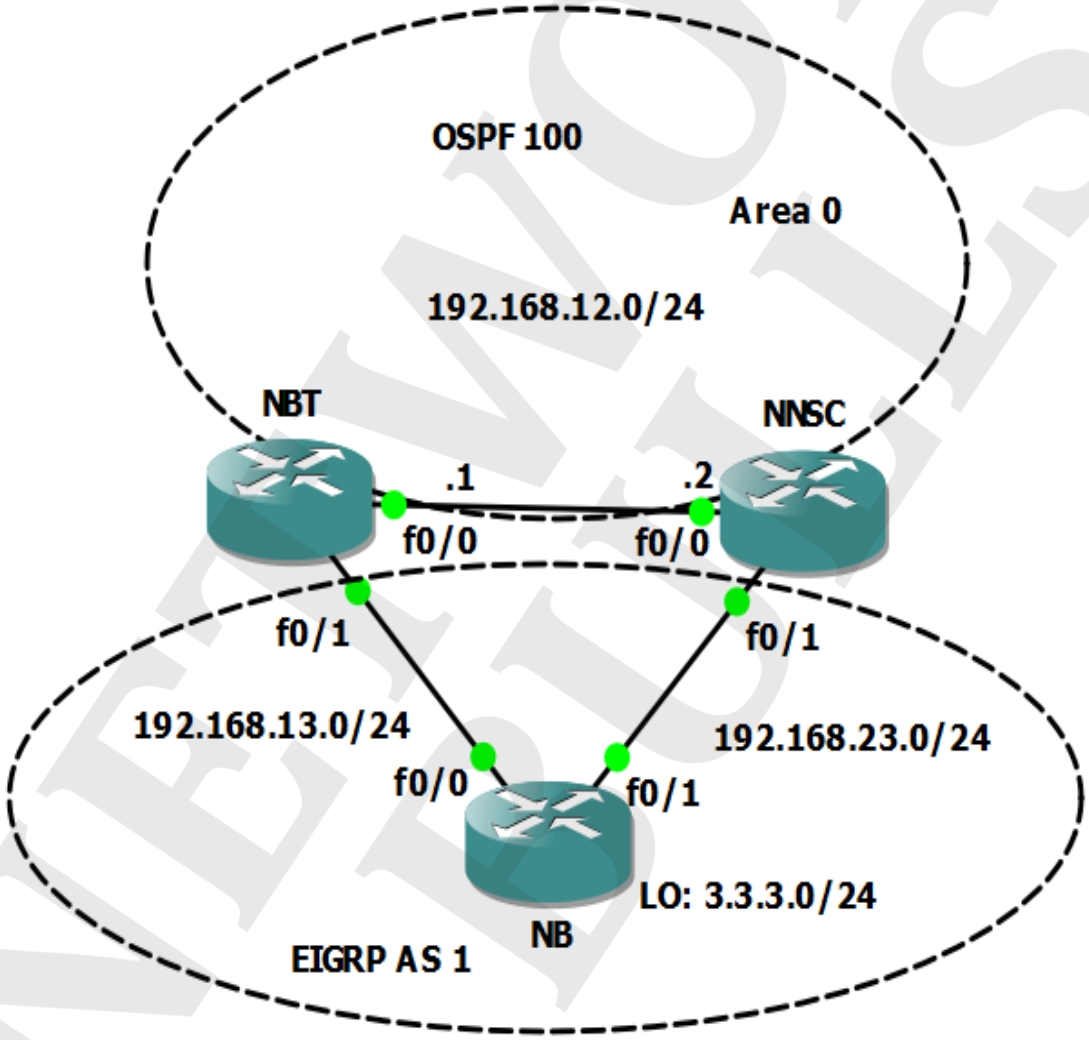
1. To configure OSPF on both the routers, using following policy:
   On router NB: loopback 0 should be in area 0.
2. On router NB: Create 4 loopbacks:
   L1: 10.0.0.1/24
   L2: 10.0.0.2/24
   L3: 10.0.0.3/24
   L4: 10.0.0.4/24
   To advertise these networks into OSPF, without using "network" command to achieve this.
3. Take a look at the routing table of router NBT, all the 4 networks should be present in the routing table and must be reachable.
4. To change the area type of area 1 so that these 4 networks are no more present in the routing table of NBT.



Practical 31: Redistribution of EIGRP into OSPF

Task:

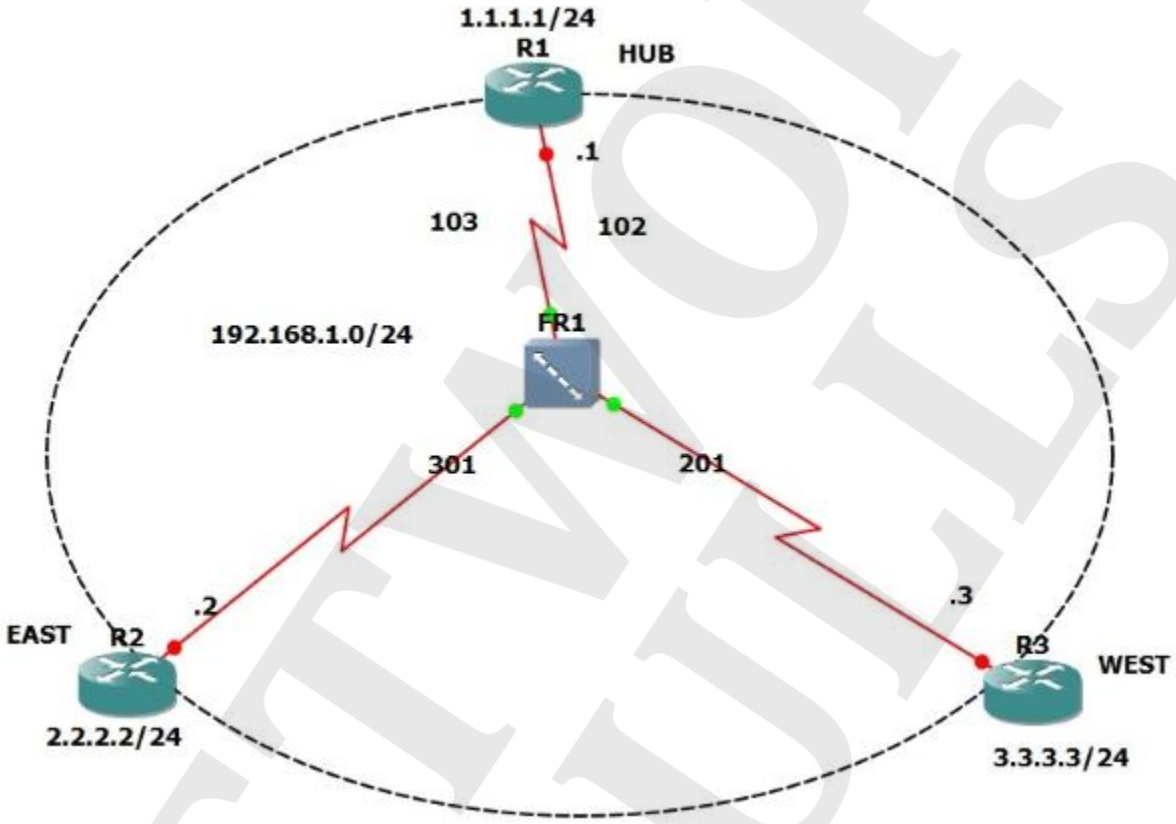
1. To configure OSPF on router NBT and NNSC and only advertise networks 192.168.13.0/24 and 192.168.23.0/24.
2. To redistribute EIGRP information into OSPF on router NBT.
3. Do a traceroute from router NBT or NNSC to network 3.3.3.0/24.
   In the traceroute output, it can be noticed that it is not using most of the optimal path. Fix the problem so that the router NNSC uses most of the optimal path.



Practical 32: EIGRP over Frame-Relay

Task:

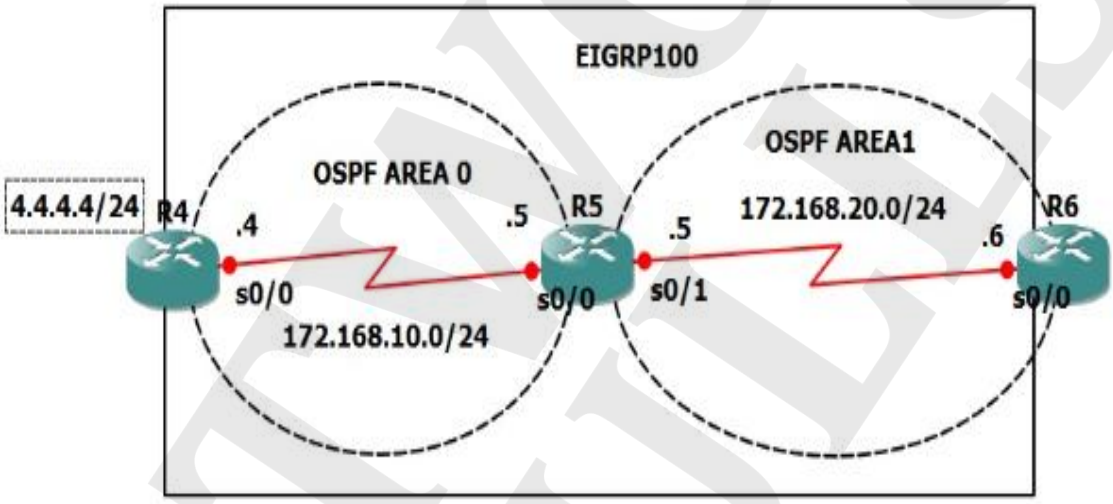
1. To configure EIGRP 100 over Frame-Relay.
2. To disable FR inverse ARP.
3. To advertise loopbacks in EIGRP.
4. To ensure loopbacks of East and West must ping.



Practical 33: EIGRP and OSPF

Task:

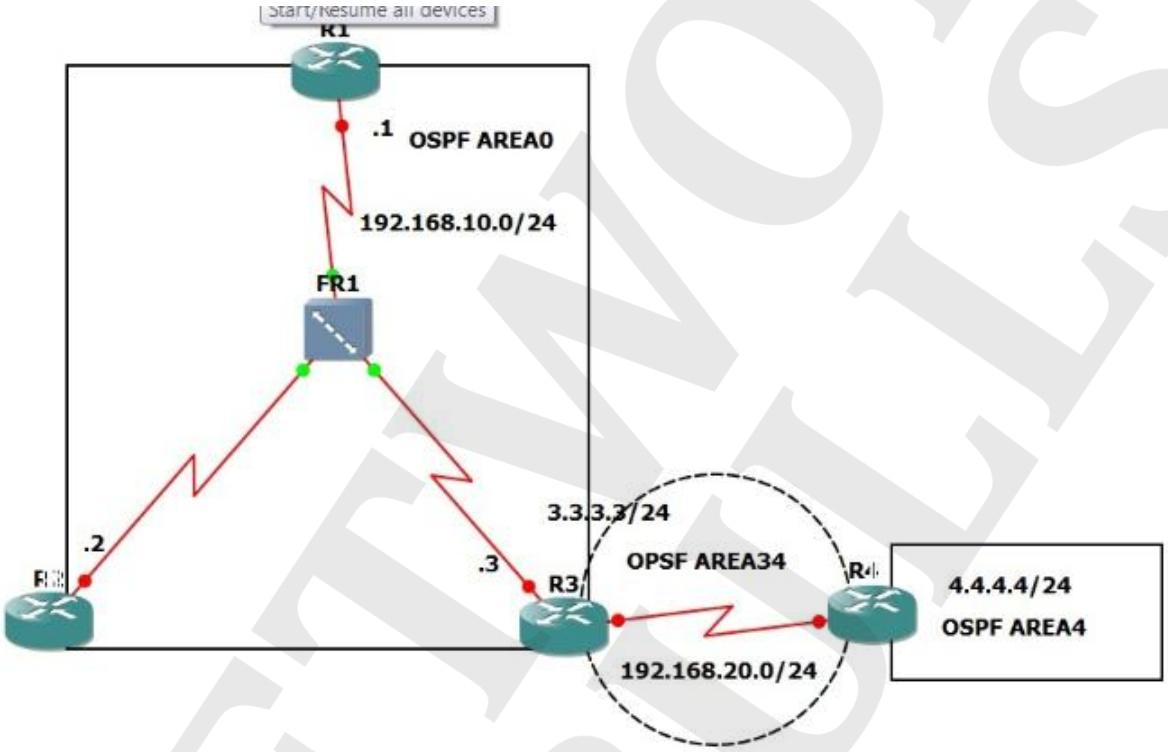
1. To configure EIGRP 100 and OSPF as shown in the topology.
2. R6 must ping the loopback networks of R4 via OSPF only.
   In the routing table of R6, the route for the network 4.4.4.4/24 should be present there.



Practical 34: OSPF over Frame-Relay

Task:

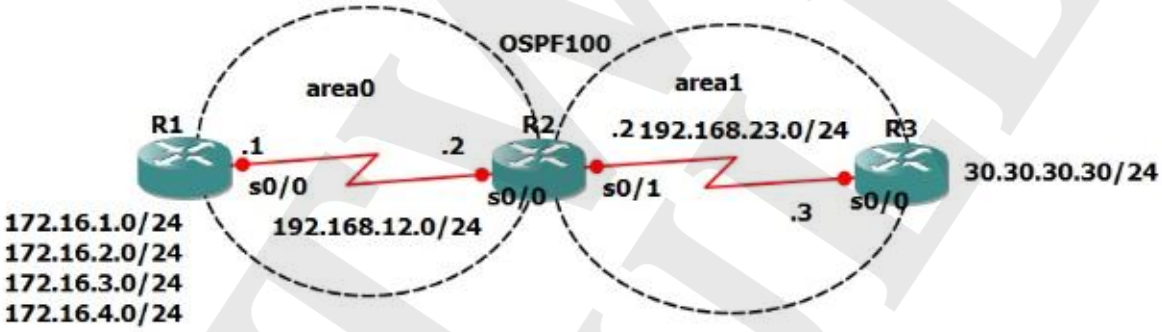
1. To configure OSPF over Frame-Relay.
2. To create a virtual-link over area 34.
3. Loopbacks must be advertised with the exact mask.
4. To configure neighborship between R2 and R3.
5. Ping from loopback of R4 to 1.1.1.1/24.



Practical 35: OSPF

Task:

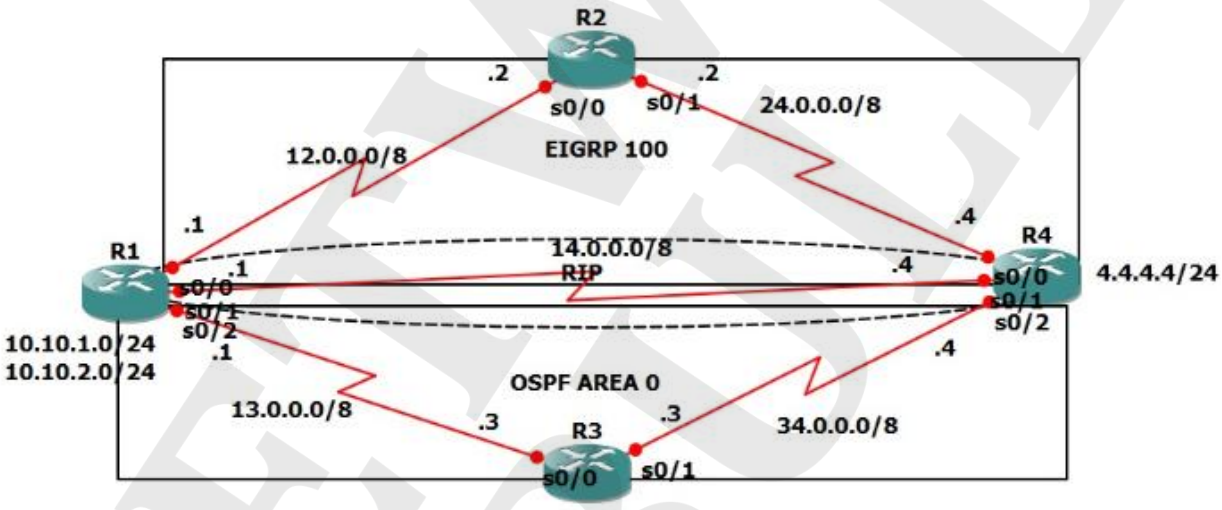
1. To configure IP addresses and OSPF as shown in the topology.
2. To redistribute networks (loopbacks on R1) into OSPF without using network command.
3. To change the area type for area 1 so that you cannot see 4 networks anymore in the routing table but only the default route.
4. To create a loopback on R3 as shown in the topology. Redistribute this loopback network in OSPF and ensure this loopback network should ping R1 loopback.



Practical 36: Source Based Routing

Task:

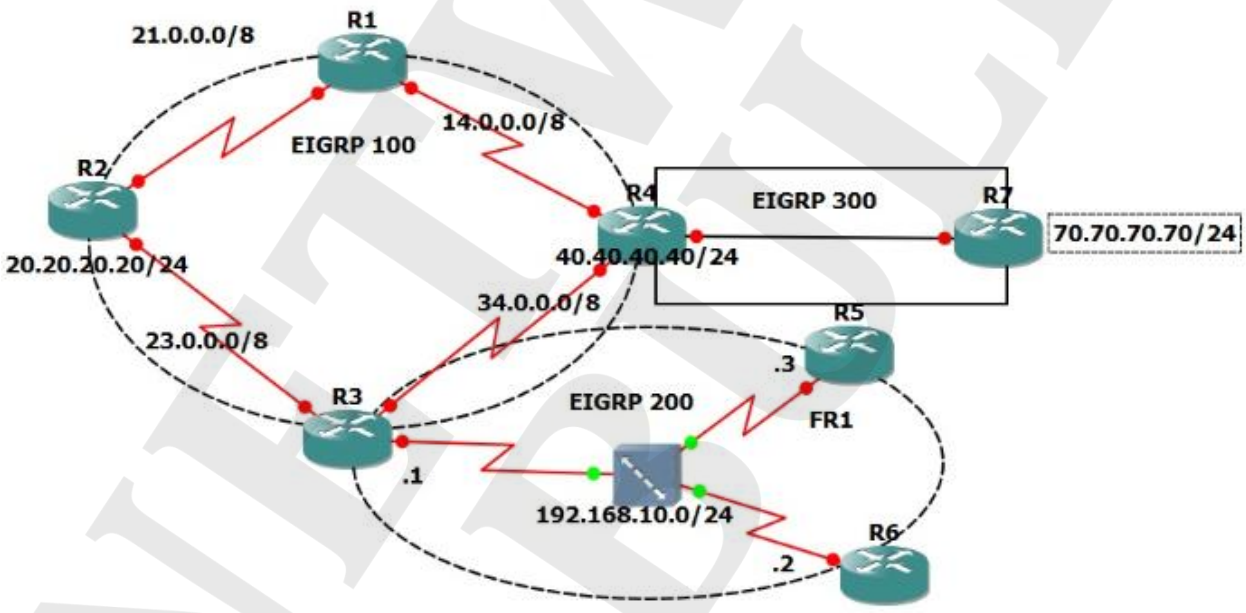
1. To configure the topology as shown in the figure.
2. To take a look on the routing table of R1and verify the routing table preferred by the network 4.4.4.4/24.
3. To create loopbacks on R1.
4. To configure source based routing such that if you ping from LB1to R4's loopback, RIP path must be preferred otherwise any.



Practical 37: EIGRP

Task:

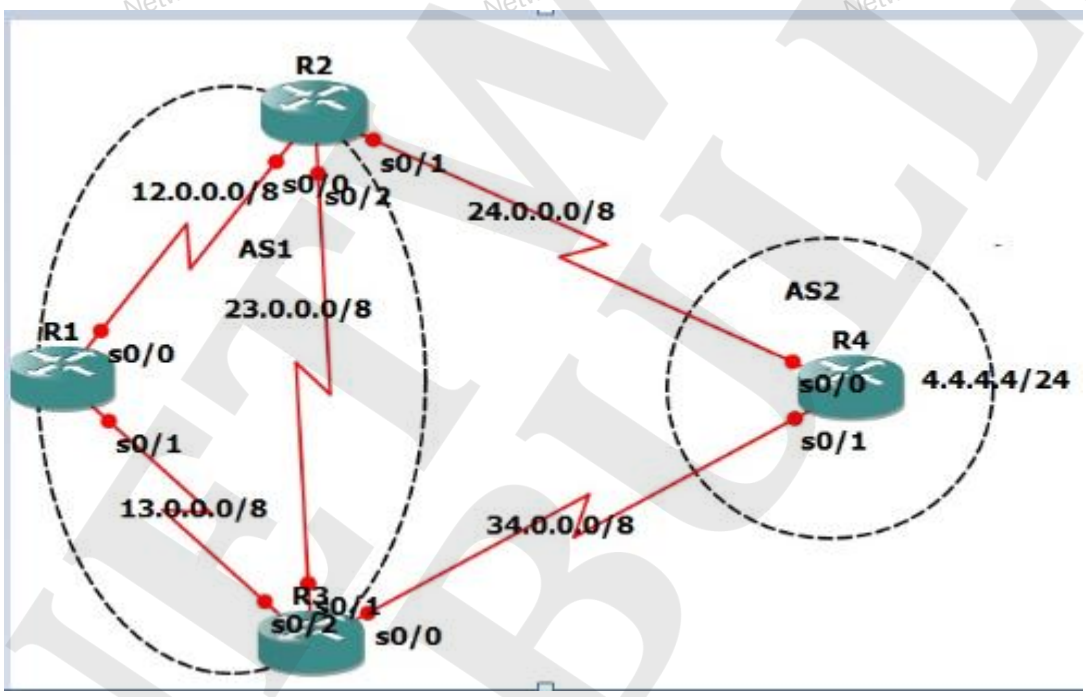
1. To configure EIGRP 100 and 300 as shown in the topology.
2. To create loopbacks on R2, R4 and R7.
3. To configure path from R7 to R2 via R3 as successor and other as a feasible successor. For this, use reliability as a metric.
4. To configure EIGRP MD5 authentication between R4 and R7.
5. To configure EIGRP 300 over Frame-Relay using point to multipoint sub interfaces.



Practical 38: BGP

Task:

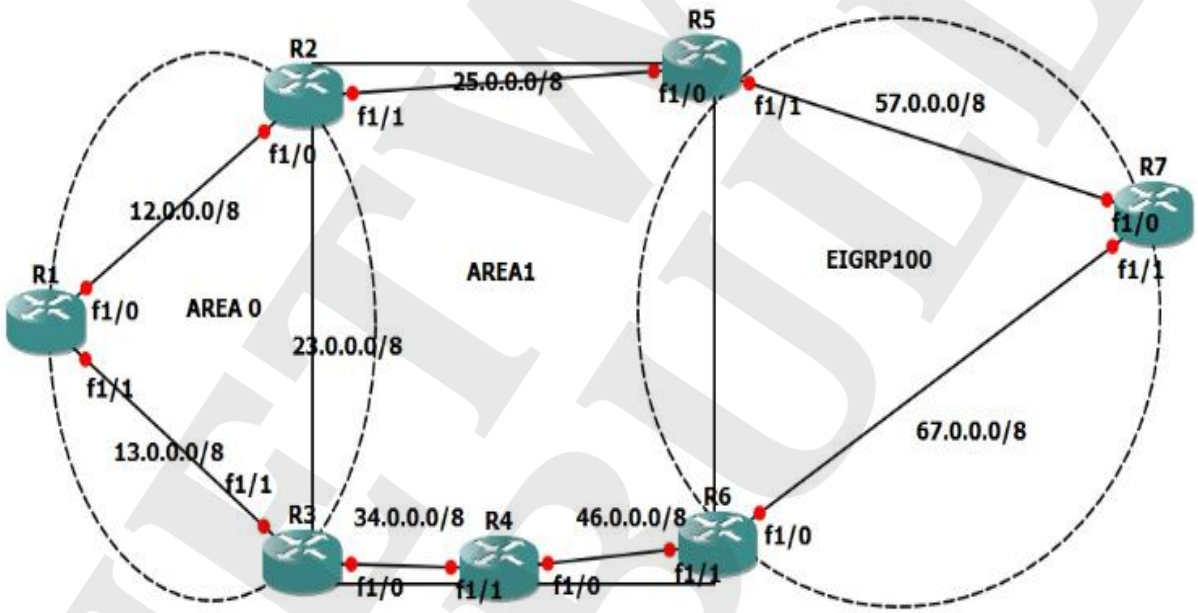
1. To configure iBGP in AS1 and eBGP between AS1 and AS2.
2. To ensure AS1 will use the link between R3 and R4 to send the traffic.
   Note: Use MED attribute for doing this task.
   Also, find if there is any other attribute which can be used to accomplish this task or not.



Practical 39: Redistribution

Task:

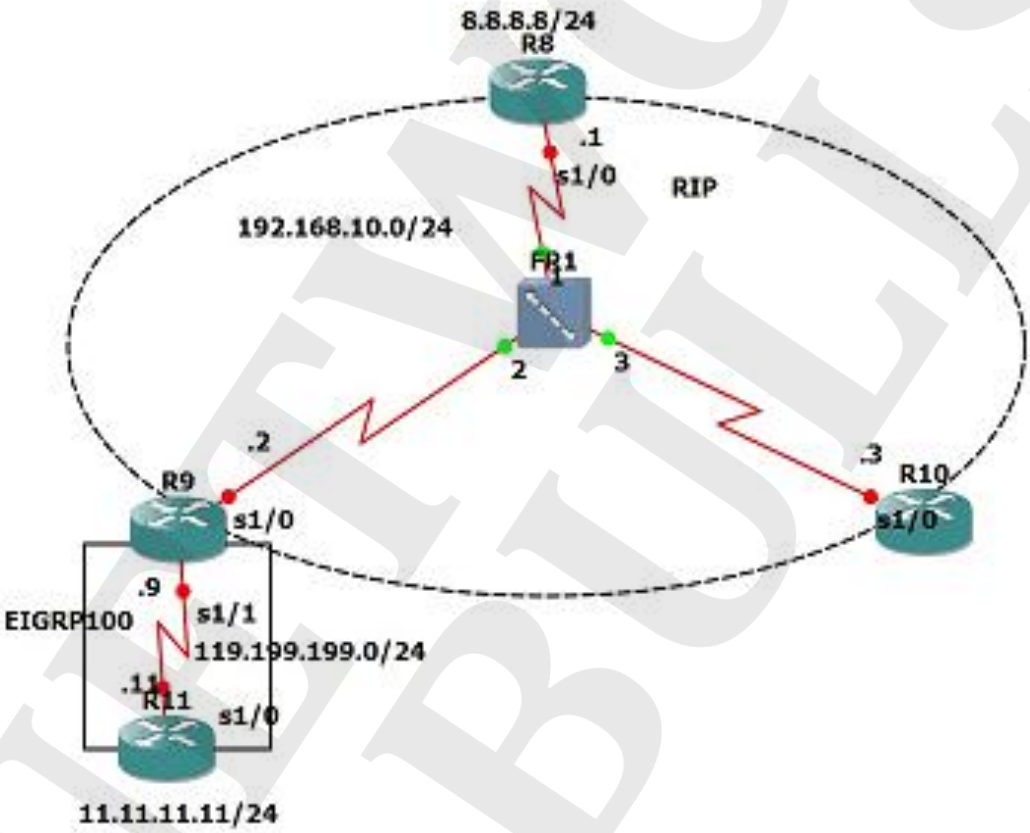
1. To configure EIGRP 100 and OSPF as shown in the topology.
2. To create loopback 7.7.7.7/24 on R7.
3. To redistribute the route received from R7 into OSPF domain on R5 and R6.
4. To configure redistribution in such a way that R1 will get the routes from both the sides in its routing table.
   Note: Use default metric type E2.



Practical 40: FRAME RELAY

Task:

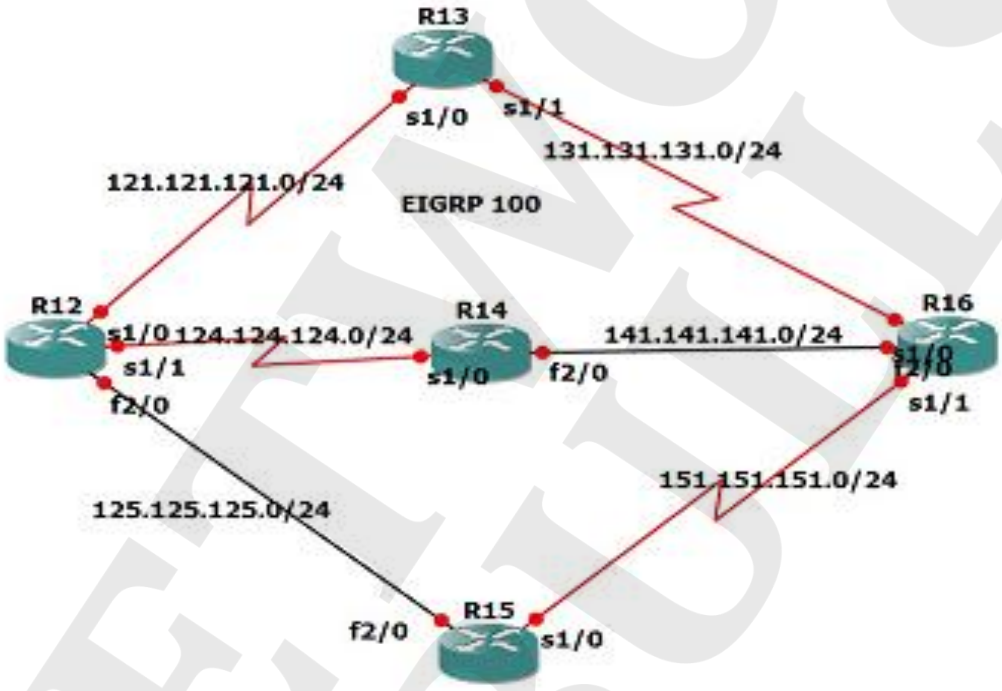
1. To configure RIP over Frame-Relay.
2. To configure PPP and CHAP authentication with password “CISCO” between R9 and R11.
3. Ping from R11 loopback to R8 loopback.



Practical 41: EIGRP

Task:

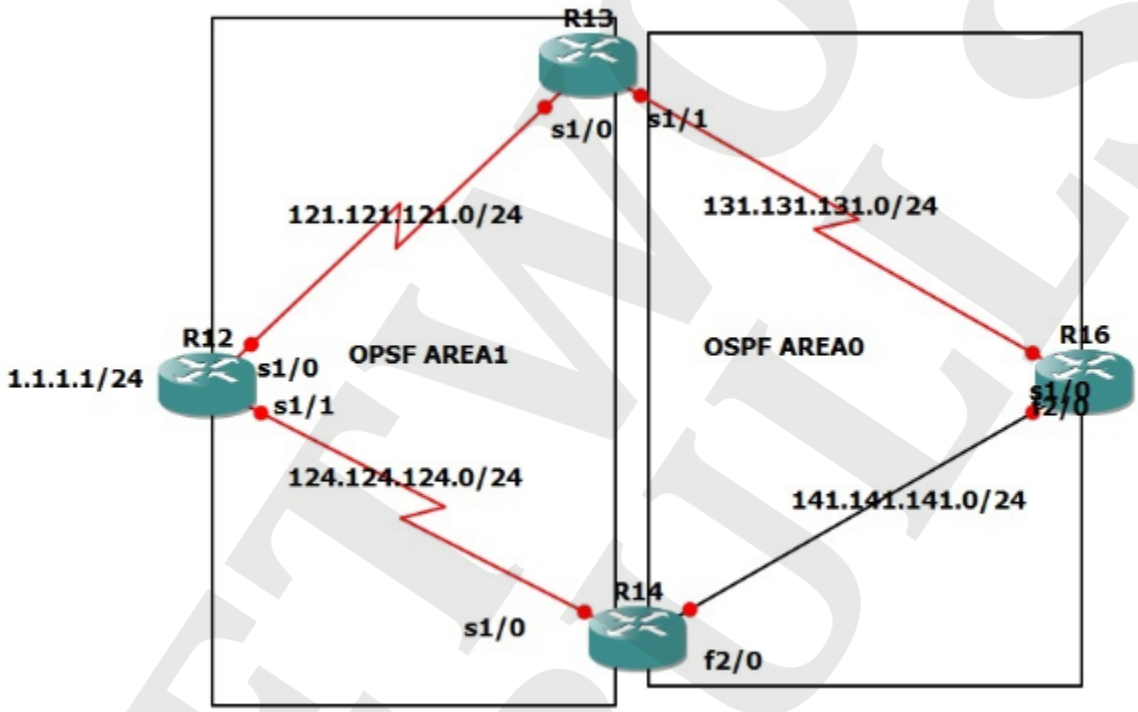
1. To configure EIGRP 100.
2. To check for successor and feasible successor for the loopback of R16 in the routing table of R12.
3. To configure path via R15 as a successor using variance.



Practical 42: OSPF

Task:

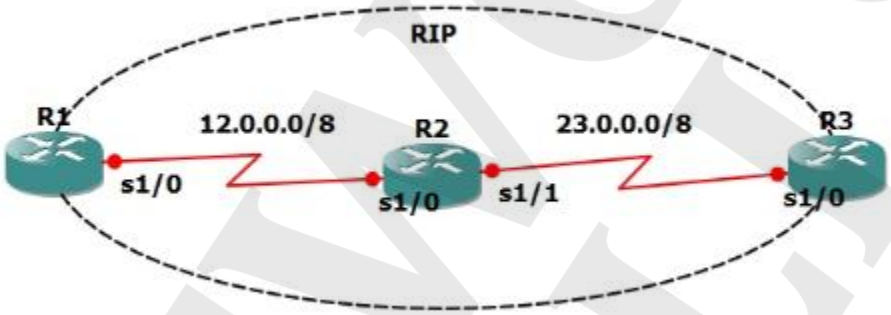
1. To configure OSPF as shown in the figure.
2. To verify full connectivity.
3. To configure OSPF area 1 as NSSA.
4. To redistribute loopback 1.1.1.1/24 on R12 in OSPF.
5. To look up in the routing table of R16.



Practical 43: RIP

Task:

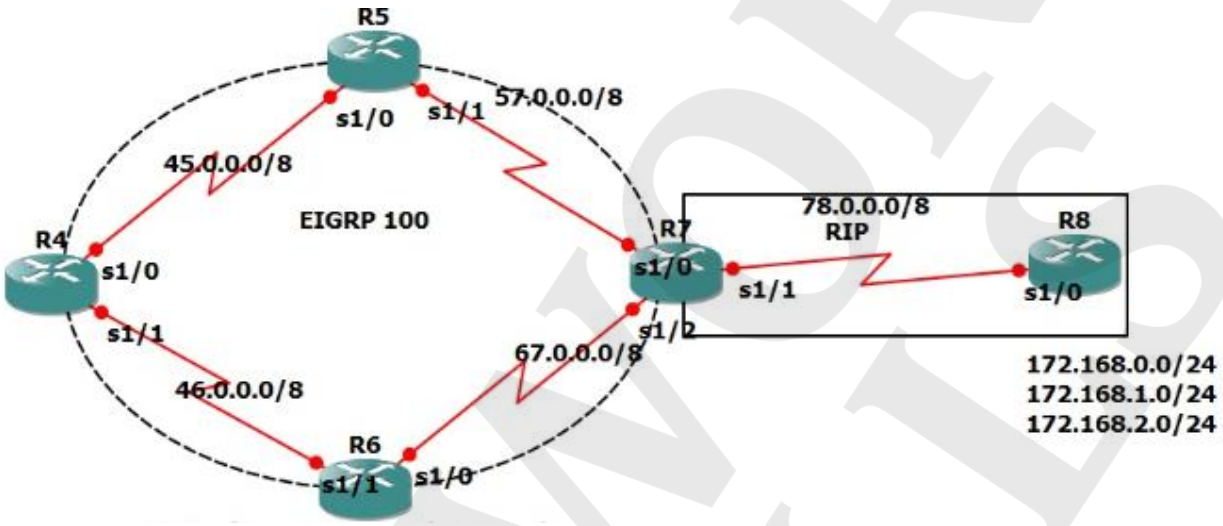
1. To configure RIP as shown in the figure.
2. To use RIP version 2.
3. To configure authentication between R1 and R2 and between R2 and R3.
4. To configure timers in such a way that convergence become 6 times faster.
5. To use debug command to see the effects.



Practical 44: Redistribution

Task:

1. To configure EIGRP and RIP as shown in the figure.
2. To perform redistribution.
3. To create summary route on R8 for the loopbacks and these routes must be reachable to R4 via R6.

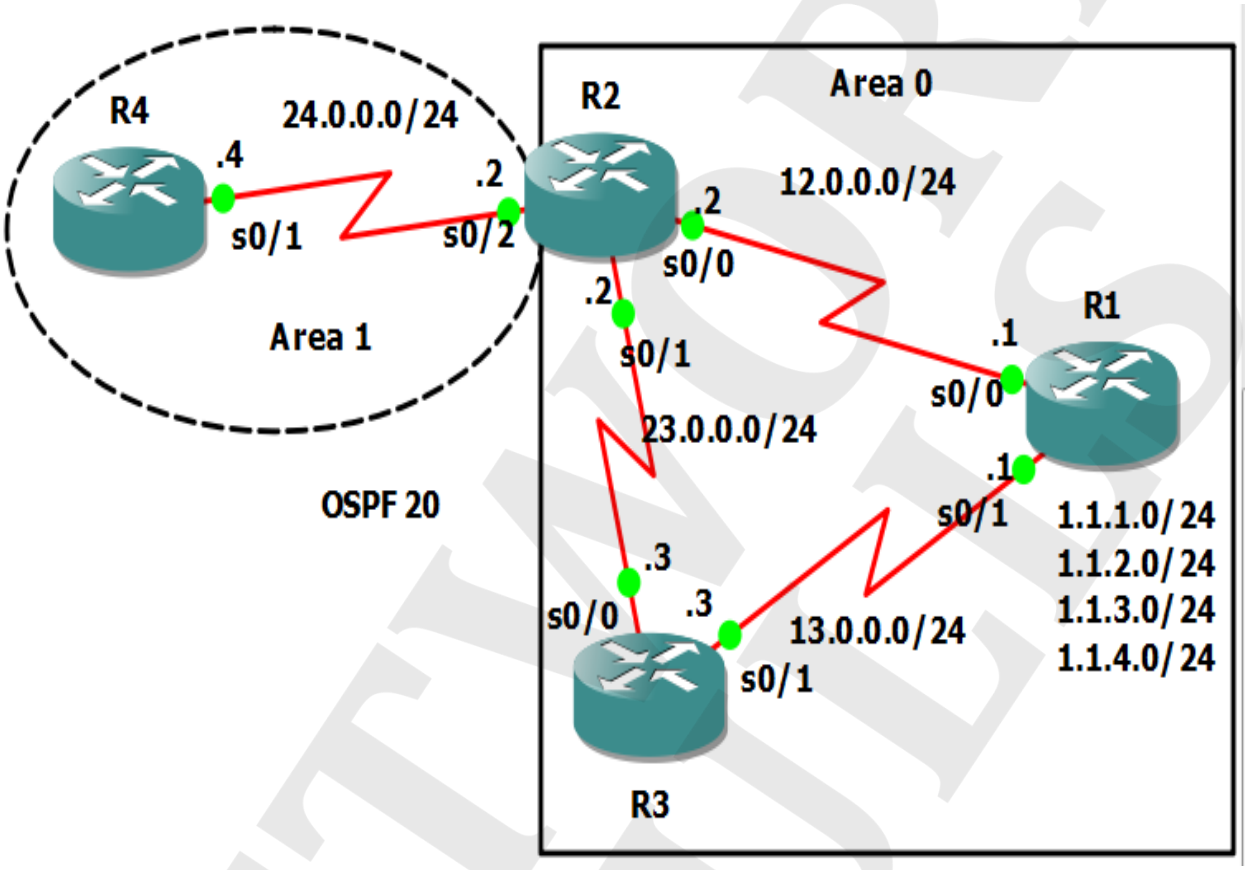


Practical 45: OSPF

Task:

1. To configure OSPF on all the routers and configure the areas as specified in the topology.
2. To configure R2, so that R4 do not receive the routes of R1 in its routing table.

   Note: Route-filtering is not allowed.



CCNP Switch: Basics& Advanced

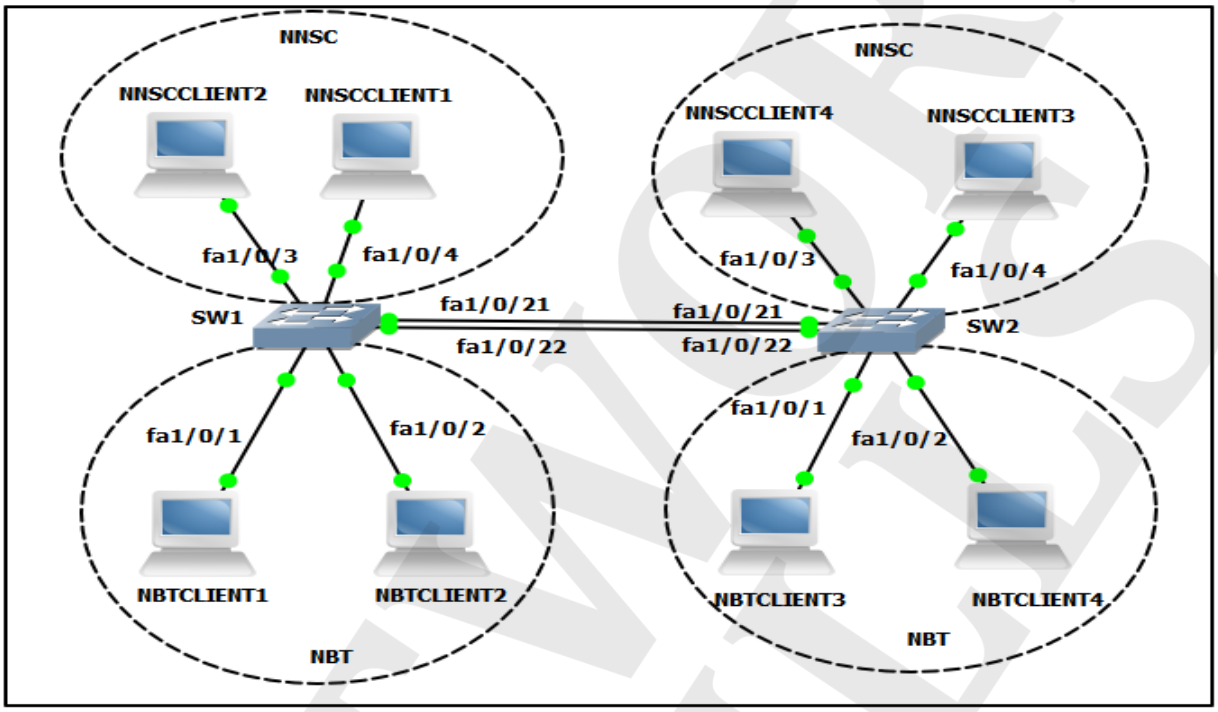
CCNP Switching: Table of Contents

I) Configuration of Port-security II) Manual errdisable recovery in port-security III) Auto errdisable recovery in port security
DHCP
I) DHCP Relay agent II) DHCP Snooping
DHCP Snooping
IP source guard

VLAN (Virtual LAN)

Practical 46: Creating VLAN and Port assignment

Task: To configure two VLANs and name them as NBT and NNSC on both the switches. Also assign SwitchportFa1/0/1 and Fa1/0/2 to VLAN NBT and SwitchportFa1/0/3 and Fa1/0/4 to NNSC.



Trunking and allowed VLAN

- VLANs are local to each switch's database, and VLAN information cannot be passed in between the switches.
- Trunk links provide VLAN identification for frames traveling in between the switches.
- Cisco switches have two Ethernet trunking mechanisms: ISL and IEEE 802.1Q.
- Trunks carry traffic from all VLANs to and from the switch by default but can be configured to carry only specified VLAN traffic.
- Trunk links must be configured to allow trunking on each end of the link.

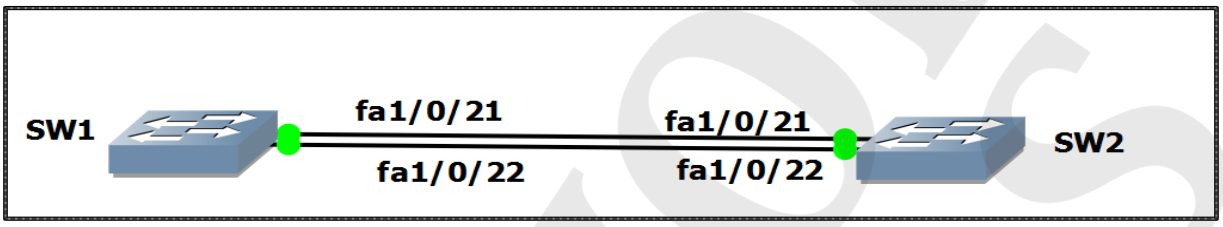
A trunk port is by default a member of *all* the VLANs that exist on the switch and carry traffic for all those VLANs between the switches. To distinguish between the traffic flows, a trunk port must mark the frames with special tags as they pass in between the switches.

Practical 47: Trunking with ISL encapsulation

Task: To configure an ISL trunk in between Switch 1 and Switch 2 using port Fa 1/0/21 and Fa 1/0/22 while using the following policy:

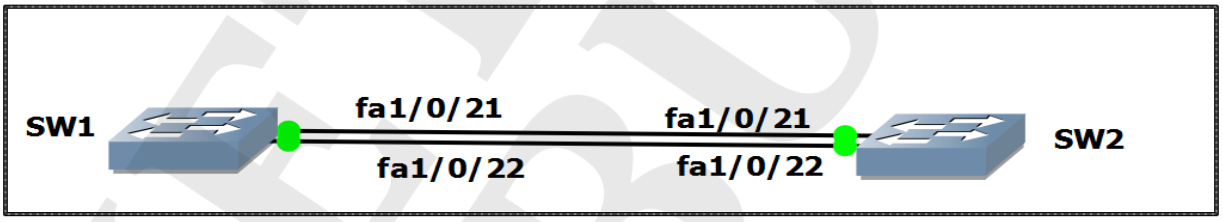
On Sw1: The ports on switch 1 should be configured into permanent trunking mode and they should negotiate to convert the neighboring interfaces into trunk.

On Sw2: The ports on switch 2 should be configured to actively participate to convert the link into a trunk.



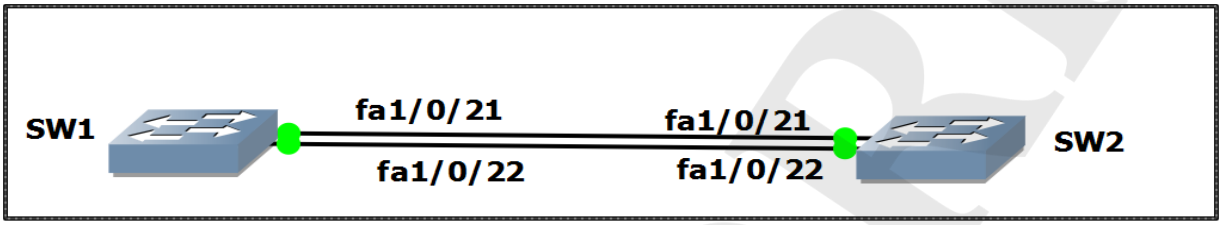
Practical 48: Trunking with ISL encapsulation using Dynamic desirable modes on both switches

Task: To configure ISL trunk in between both the switches. The ports should be configured such that these ports negotiate to convert neighboring interfaces into ISL trunk.



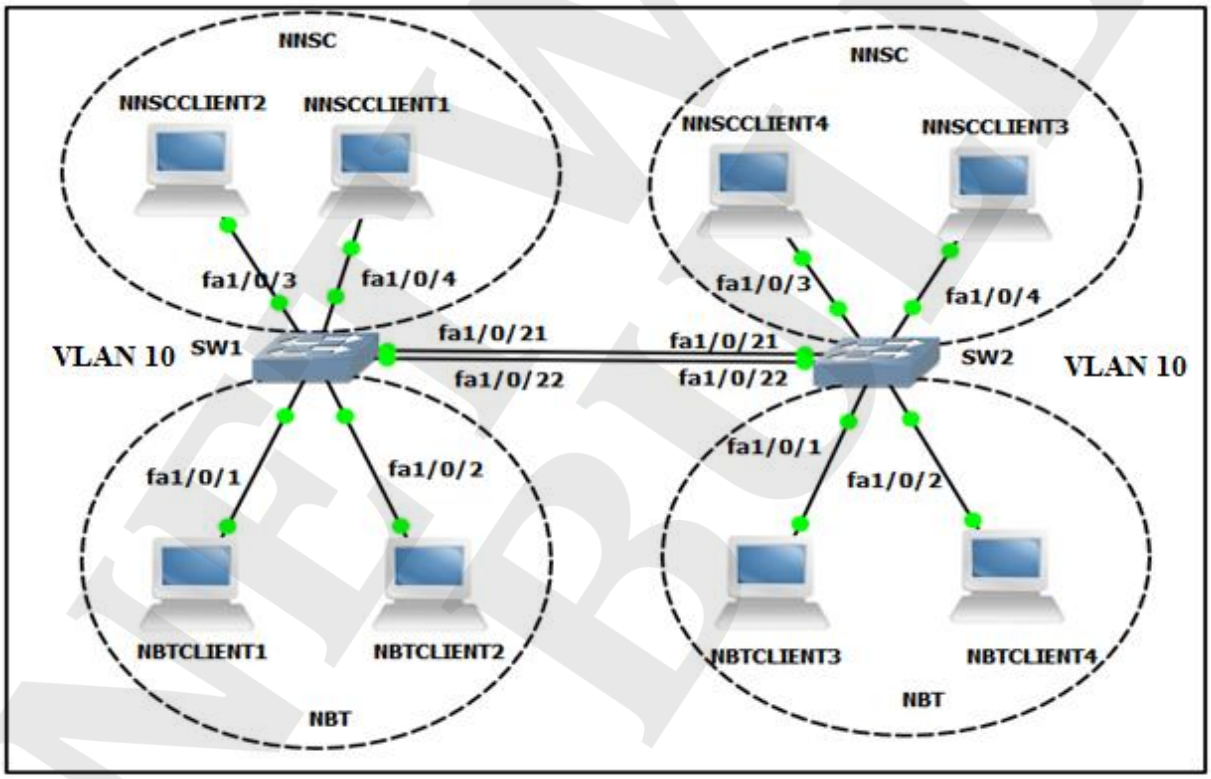
Practical 49: Trunking with dot1q encapsulation

Task: To configure dot1q trunk in between both the switches. The ports should be configured such that these ports negotiate to convert the neighboring interfaces into ISL trunk.



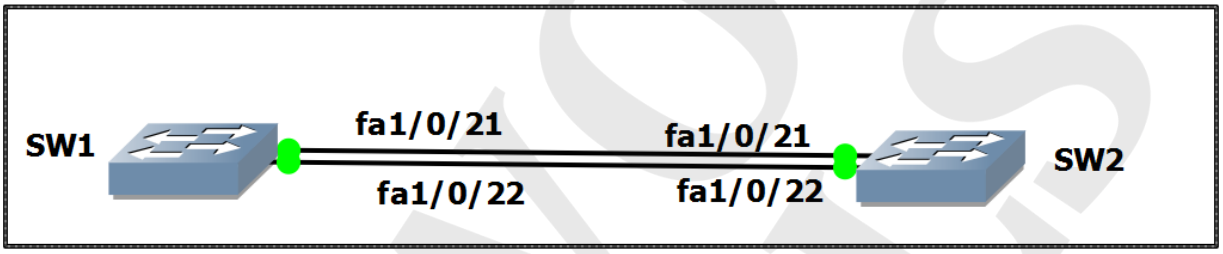
Practical 50: Trunking with dot1q encapsulation and allowed VLAN

Task: To configure dot1q trunk in between both the switches and also configure the allowed VLAN so that only VLAN 10 would be allowed on the links.



Practical 51: Disable DTP (Dynamic Trunking Protocol)

Task: To configure an ISL trunk in between Sw1 and Sw2 and disable DTP so that these ports shouldn't use DTP to negotiate a trunk.



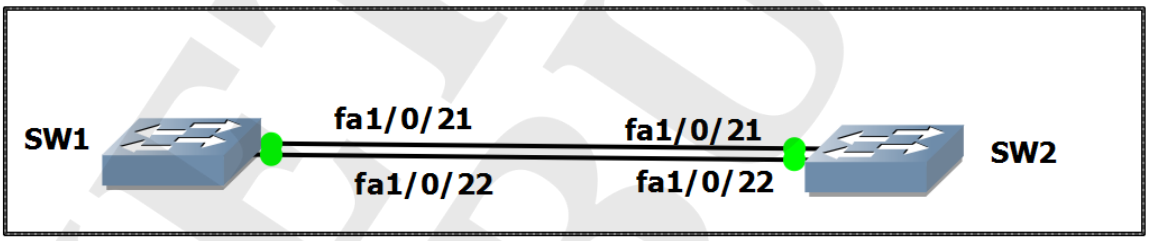
VTP (VLAN Trunking Protocol)

VTP reduces administration in a switched network. When a new VLAN is configured on one VTP server, the VLAN is distributed through all switches in the domain. This reduces the need to configure the same VLAN everywhere.

Practical 52: VTP Basics

Task:

1. To verify the following parameters of VTP on both the switches:
    - Verify the number of VLANs existing on both the switches.
    - VTP mode of operation
    - VTP domain name
    - Running VTP version
    - VTP password
2. To change the following parameters of VTP on both the switches:
    - VTP mode of operation:
      On Switch 1: VTP mode-Server
      On Switch 2: VTP mode -client
    - VTP domain name to "NETWORKBULLS"
    - VTP version to version 2
    - VTP password to "EDUCATINGNETWORKS"



VTP modes

VTP has three different modes.

• Server Mode

• Client Mode

• Transparent Mode

The configuration revision number is a 32-bit number that indicates the level of revision for a VTP packet. Each VTP device tracks the VTP configuration revision number that is assigned to it. Most of the VTP packets contain the VTP configuration revision number of the sender.

This information is used to determine whether the received information is more recent than the current version. Each time that you make a VLAN change in a VTP device, the configuration revision is incremented by one. In order to reset the configuration revision of a switch, change the VTP domain name, and then change the name back to the original name.

VLAN Trunking Protocol (VTP) Server Mode

VLAN Trunking Protocol (VTP) Server mode is the default VTP mode for all Catalyst switches. At least one server is required in a VTP domain to propagate VLAN information within the VTP domain. One can create, add, or delete VLANs of a VTP domain in a Switch which is in VTP Server mode and change VLAN information in a VTP Server. The changes made in a switch in server mode are advertised to the entire VTP domain.

VLAN Trunking Protocol (VTP) Client Mode

VLAN Trunking Protocol (VTP) client mode switches listen to the VTP advertisements from the other switches and modify their VLAN configurations accordingly. A network switch in VTP client mode requires a server switch to inform it about the VLAN changes. One CANNOT create, add, or delete VLANs in a VTP client.

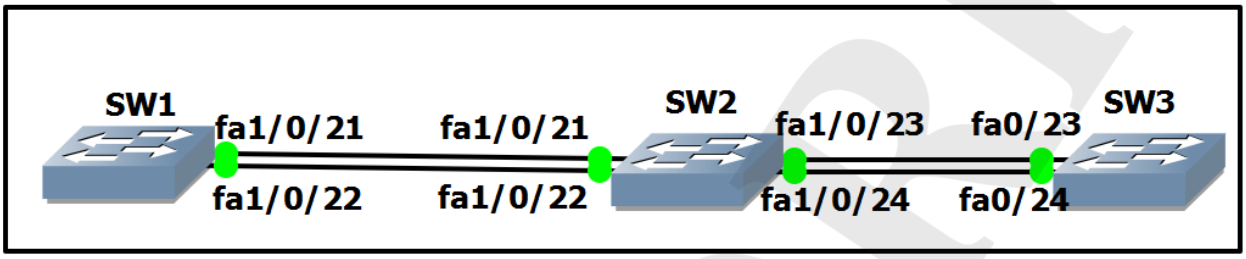
VLAN Trunking Protocol (VTP) Transparent Mode

VLAN Trunking Protocol (VTP) transparent mode switches do not participate in the VTP domain, but VTP transparent mode switches can receive and forward VTP advertisements through the configured trunk links.

Practical 53: VTP modes

Task:

1. To configure Switch 1 as Server, Switch 2 as Transparent and Switch 3 as Client.
2. To create VLAN 2, 3, 4 and 5 on Server and verify the impact on whole VTP domain.



VTP Pruning

VTP pruning is disabled by default in Cisco switches. VTP pruning helps to send broadcasts only to those trunk links that actually needs the information.

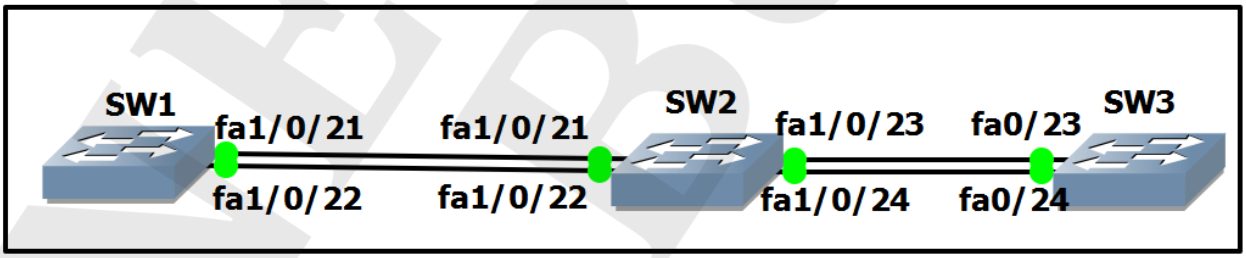
Practical 54: VTP Pruning

Task: To configure VTP Pruning on the VTP server and verify that the configuration was propagated to the VTP Client.

Sw1-Server

Sw2-Client

Sw3-Client



Etherchannel

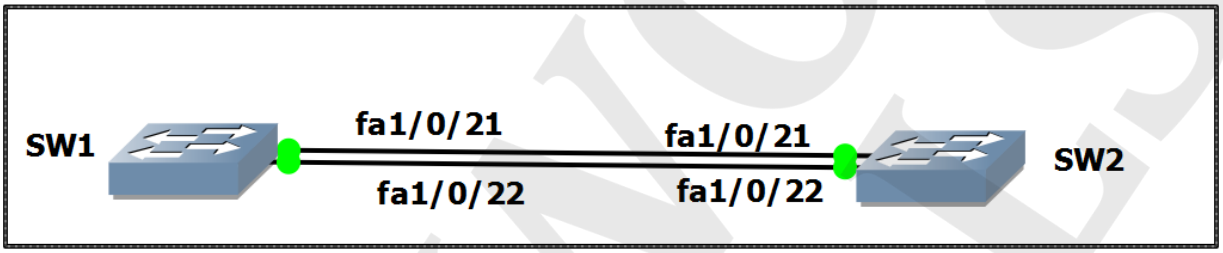
EtherChannel is the technology which is used to combine several physical links in between switches or routers into one logical connection and treat them as a single link.

A maximum of 8 Fast Ethernet or 8 Gigabit Ethernet ports can be grouped together when forming an EtherChannel.

Practical 55: Manual Etherchannel

In manual Etherchannel, no negotiation is required. The interfaces become members of the EtherChannel immediately. When using this mode make sure the other end must use this mode too because they will not check if port parameters match. Otherwise the EtherChannel would not come up and may cause some troubles.

Task: To configure Etherchannel between sw1 and sw2 manually.

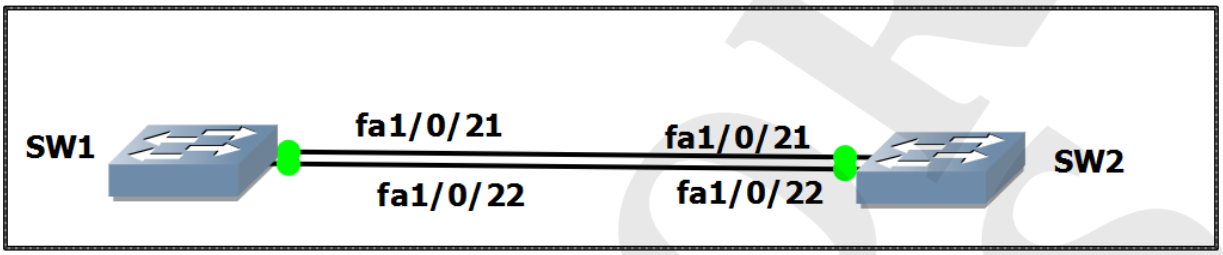


Practical 56: Etherchannel using PAgP

Port Aggregation Protocol (PAgP) is a Cisco Proprietary protocol.

PAgP uses two types of port modes; auto and desirable. PAgP mode desirable attempts to initiate a PAgP dynamic ether-channel whereas auto does not but accepts the PAgP initiation attempted from a device set to desirable.

Task: To configure Etherchannel in between Sw1 and Sw2 by using PAgP.

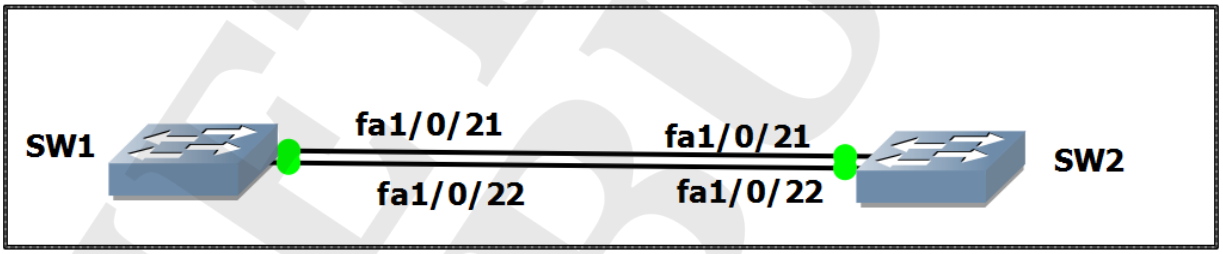


Practical 57: Etherchannel using LACP

Link Aggregation Control Protocol (LACP) is the IEEE standard.

LACP uses two types of port modes; active and passive. LACP active mode unconditionally forms a LACP dynamic ether-channel whereas passive will only accept LACP negotiation attempted from a device set to active.

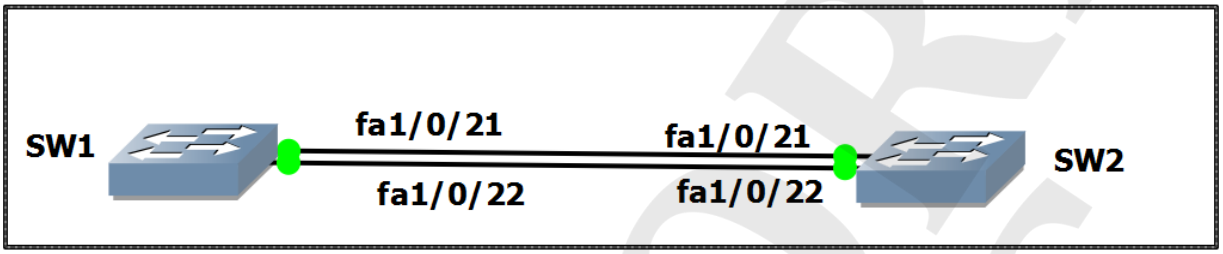
Task: To configure Etherchannel between Sw1 and Sw2 by using LACP.



Practical 58: Layer-3 Etherchannel

Layer 3 EtherChannel bundles allow you to create a virtual portchannel link that can be configured with an IP address.

Task: To configure ports Fa1/0/21 and Fa1/0/22 on SW1 and SW2 as a single layer two links. SW1 should be configured with an IP address of 192.168.1.1 and SW2 should be configured with an IP address of 192.168.1.2.



STP (Spanning Tree Protocol)

IEEE standardized a solution (IEEE 802.1D) to prevent bridging loops in data networks and provide loop-free topologies. This standardized solution is called Spanning Tree Protocol (STP).

The operation of STP is as follows:

STP enabled switches exchange BPDU messages in between them to agree upon the "root bridge" the process is called Root Bridge Election.

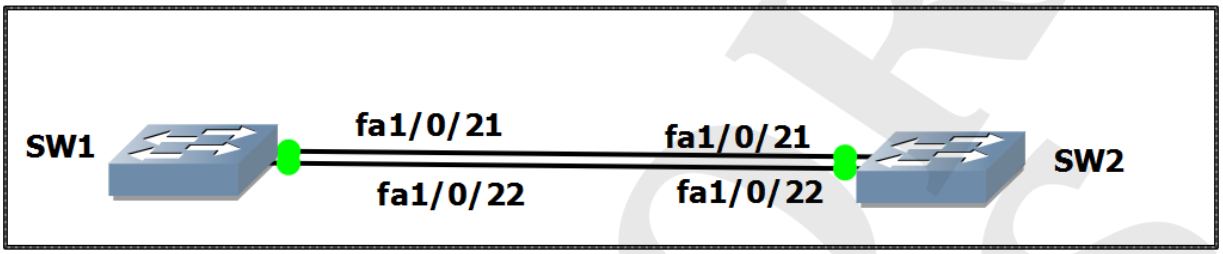
Once the root bridge is elected, every switch has to determine which of its ports will communicate with the root bridge. Therefore Root Port Election takes place on every network switch.

Finally, Designated Port Election takes place in order to have only one active path towards every network segment.

Practical 59: Root Bridge Election in STP

Task:

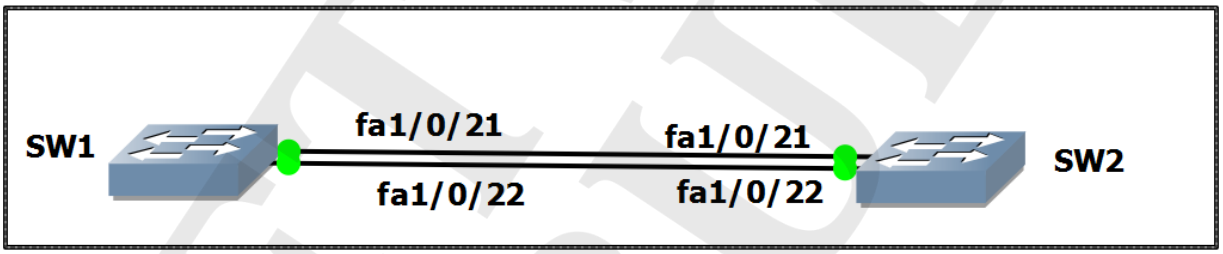
1. To verify the following:
   - Current root bridge
2. To configure the following:
   - SW2 as root bridge



Practical 60: Root Port Election in STP

Task:

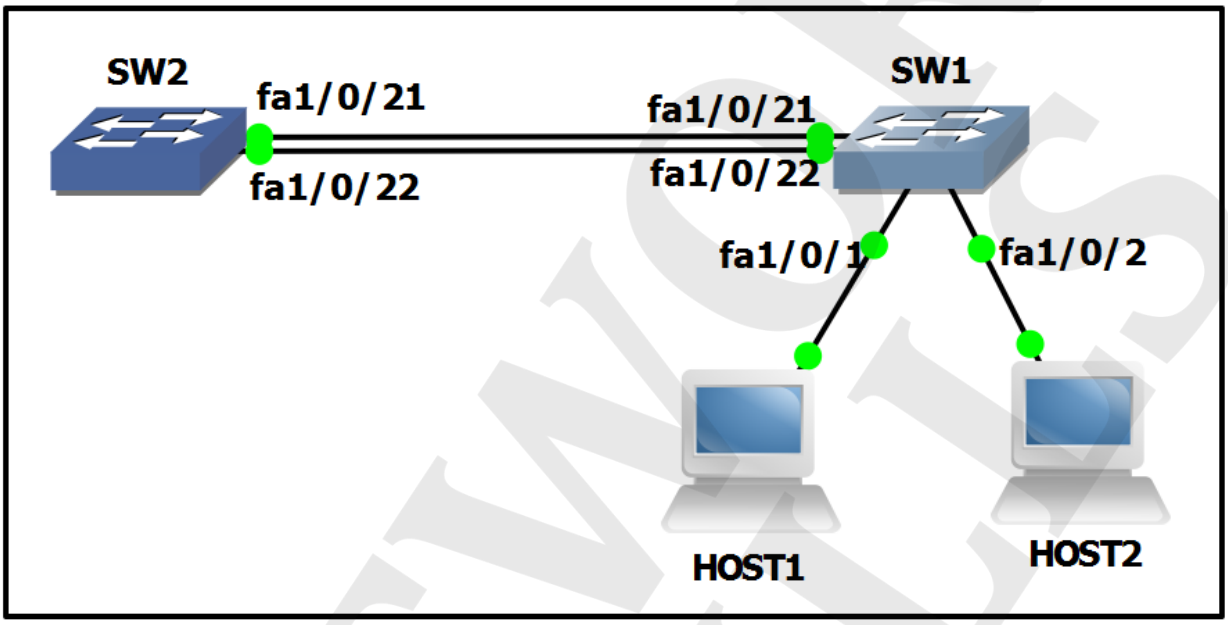
1. To verify the Root Port (RP) and Designated Port (DP) on SW1 and SW2.
2. To configure the following Fa1/0/22 as root port.



Practical 61: Port Fast in individual interfaces

PortFast will immediately transition a port to the forwarding state and will not attempt to detect a switching loop unless a BPDU is received on the port with PortFast enabled.

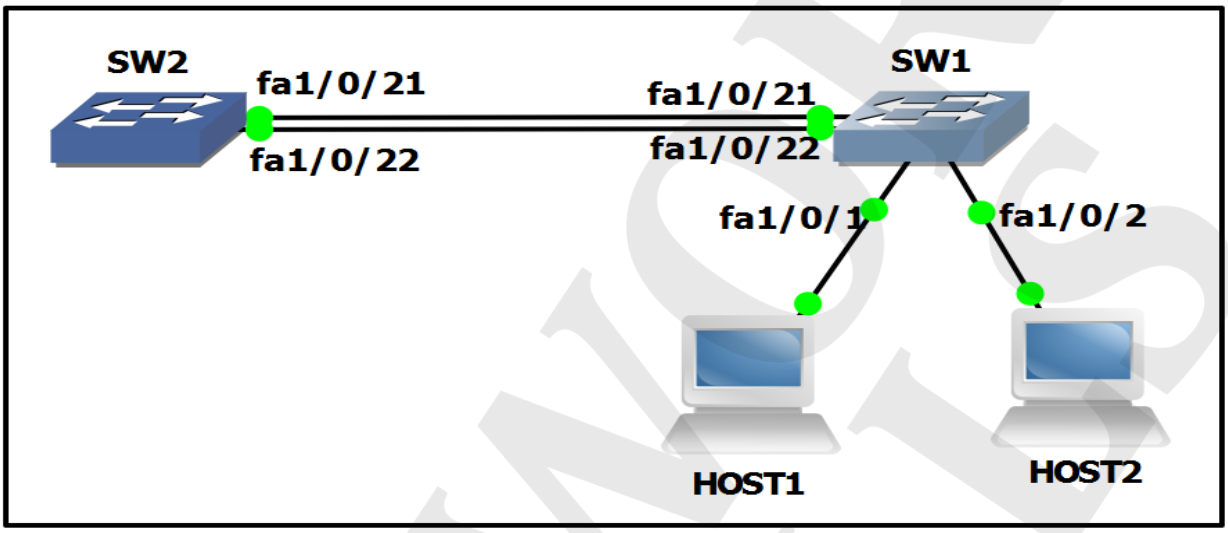
Task: To configure PortFast on fa1/0/1 and fa1/0/2 on SW1 by enabling Portfast in interface configuration mode.



Practical 62: Port Fast in STP in default mode

PortFast causes a switch or trunk port to enter the spanning tree forwarding state immediately, bypassing the listening and learning states.

Task: To globally enable Portfast across the entire switch.



STP Protection

Protecting against unexpected BPDU

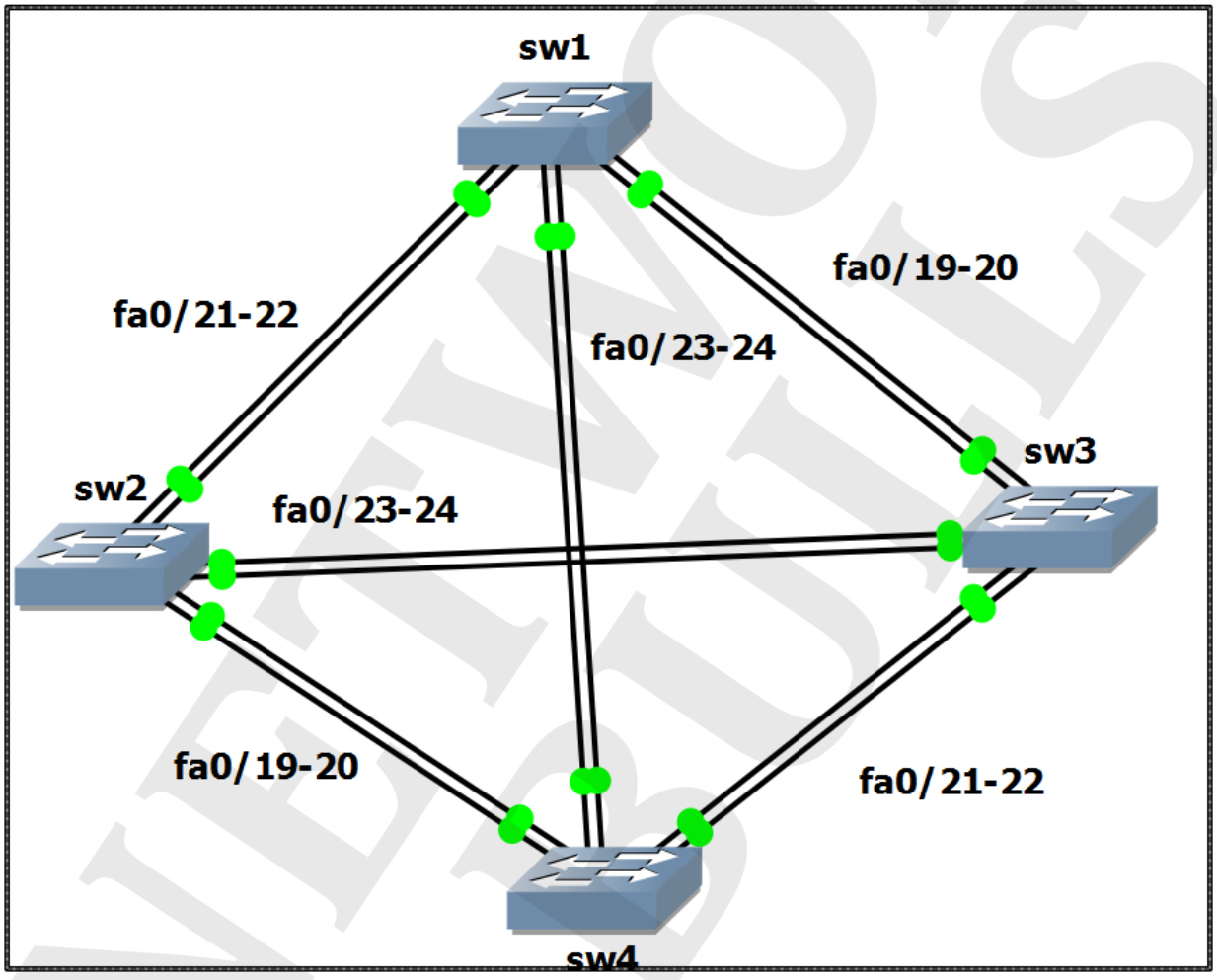
A network running STP uses BPDUs to communicate in between switches (bridges). Switches become aware of each other and of the topology that interconnects them. After a Root Bridge is elected, BPDUs are generated by the root and are relayed down through the spanning-tree topology. Eventually, all switches in the STP domain receive the root's BPDUs so that the network converges and a stable loop-free topology forms.

To maintain an efficient topology, the placement of the Root Bridge must be predictable. Hopefully, you configured one switch to become the Root Bridge and a second one to be the secondary root. What happens when a "foreign" or rogue switch is connected to the network, and that switch suddenly is capable of becoming the Root Bridge? Cisco added two STP features that help prevent the unexpected: Root guard and BPDU guard.

Practical 63: Root Guard

The root guard ensures that the port on which root guard is enabled is the designated port. Normally, root bridge ports are all designated ports, unless two or more ports of the root bridge are connected together. If the bridge receives superior STP Bridge Protocol Data Units (BPDUs) on a root guard-enabled port, root guard moves this port to a root-inconsistent STP state. This root-inconsistent state is effectively equal to a listening state. No traffic is forwarded across this port. In this way, the root guard enforces the position of the root bridge.

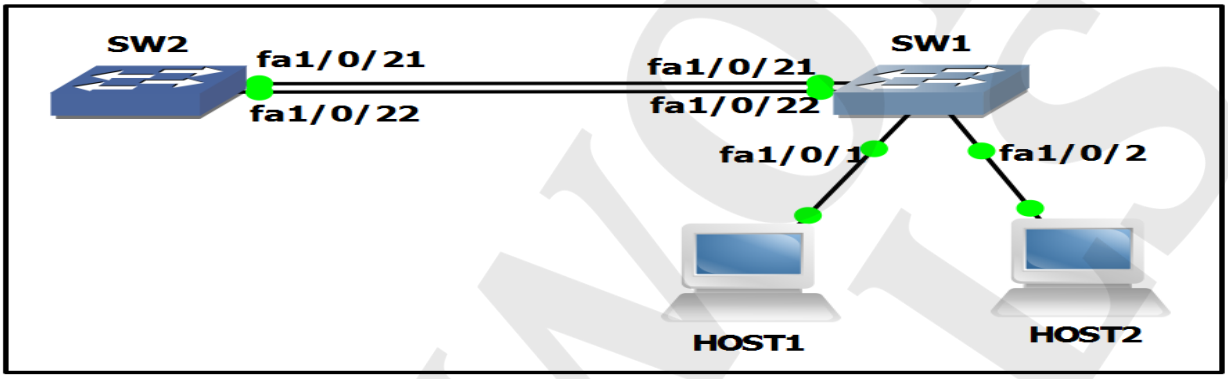
Task: To configure root guard and to make sure SW1 always remain the root bridge for the whole domain.



Practical 64: BPDU Guard

A PortFast port should never receive configuration BPDUs. If configuration BPDUs is received by a PortFast port, this reception indicates another bridge is somehow connected to the port, and it means that there is a possibility of a bridging loop formation during the Listening and Learning phases. In a valid PortFast configuration, configuration BPDUs should never be received, so Cisco switches supports a feature called asPortFast BPDU Guard, which shuts down a PortFast-enabled port in the event a BPDU is received. This feature ensures that a bridging loop cannot be formed because the switch's shutting down the port removes the possibility of a loop formation.

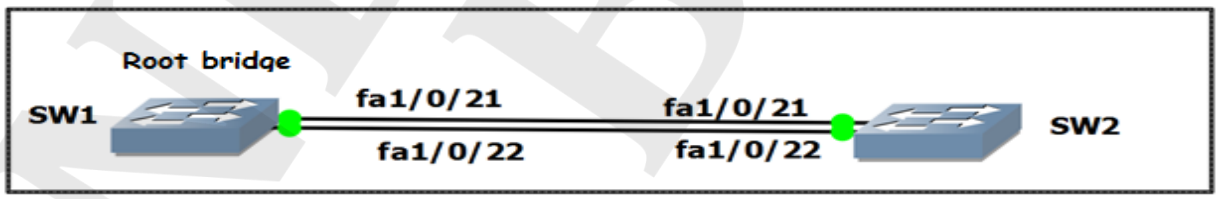
Task: To configure BPDU guard globally on SW1 so that it will not receive any BPDU.



Practical 65: Loop Guard

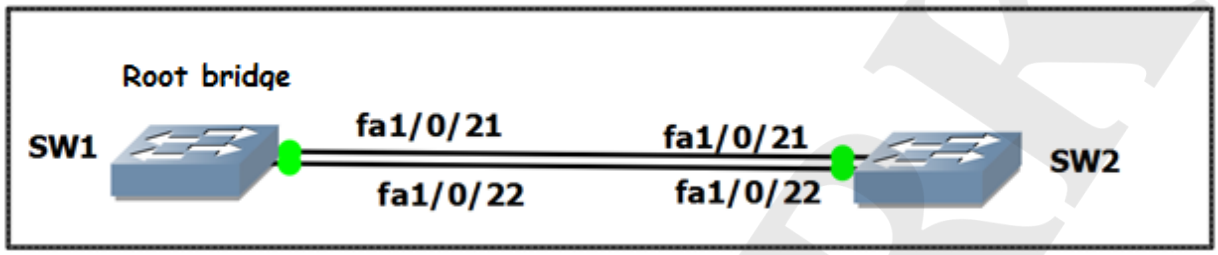
The loop guard feature is enabled on a per-port basis. However, as long as it blocks the port on the STP level, loop guard blocks inconsistent ports on a per-VLAN basis (because of per-VLAN STP). That is, if BPDUs are not received on the trunk port for only one particular VLAN, only that VLAN is blocked (moved to loop-inconsistent STP state).

Task: To enable loop guard on SW2 and show its effect on SW2 switchports.



Practical 66: BPDU filter

Task: To configure BPDU filter on SW1 and show its effect.

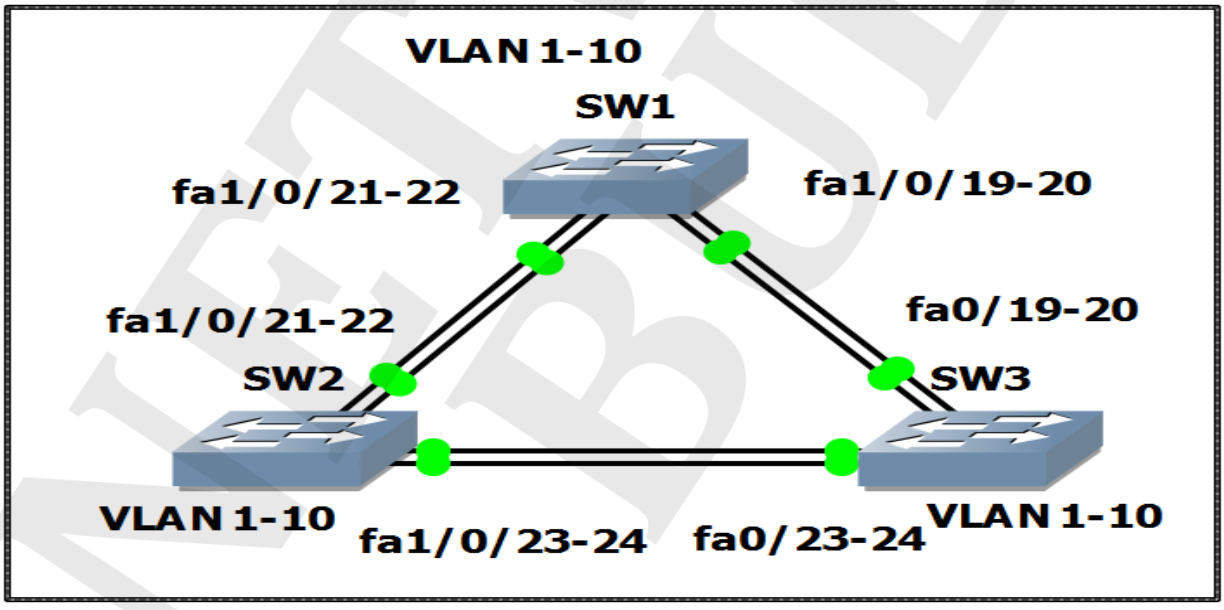


RSTP

STP has a drawback that its convergence is low which is very important in switched network. To overcome this problem, Rapid Spanning Tree Protocol (RSTP) with IEEE standard 802.1w is evolved which significantly reduces the convergence time after a topology change occurs in the network. While STP can take 30 to 50 seconds to transit from a blocking state to a forwarding state, RSTP is typically able to respond in less than 10 seconds of a physical link failure.

Practical 67: RSTP

Task: To configure RSTP in the given topology.

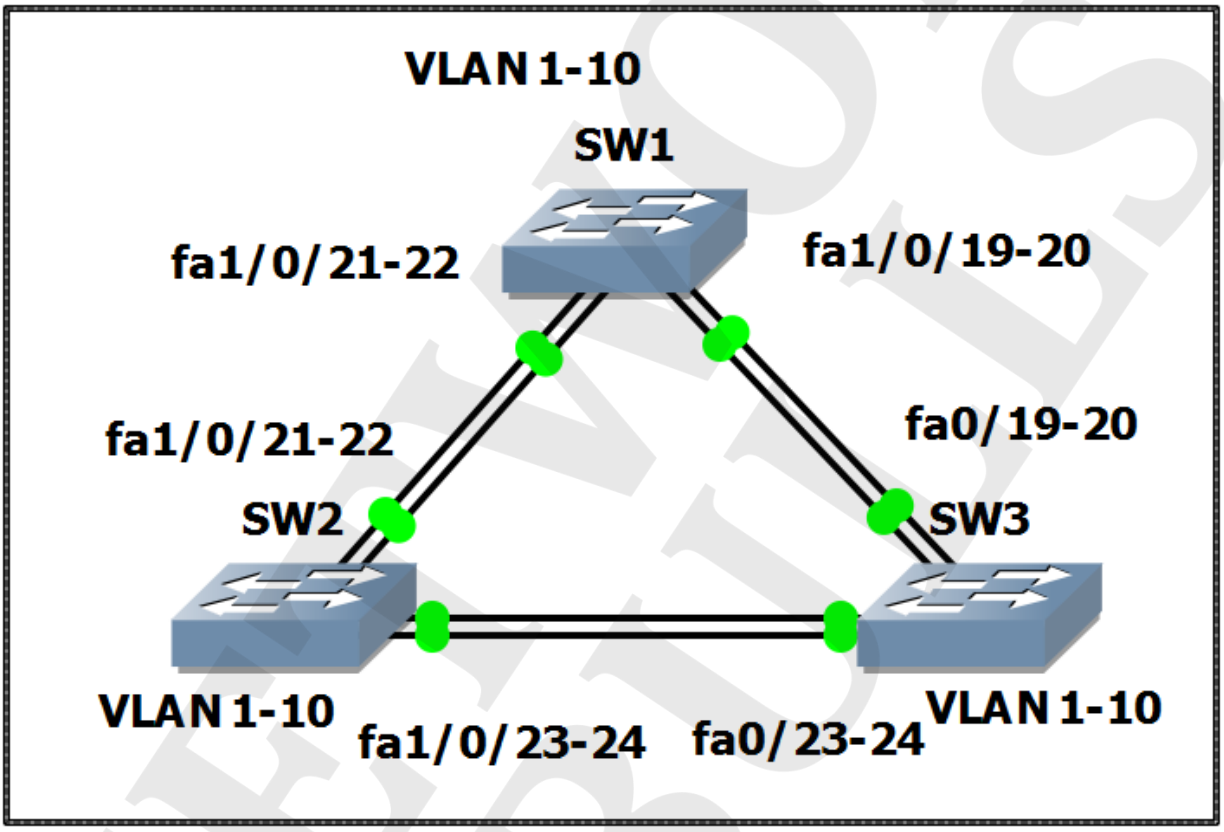


MSTP

Practical 68: MSTP

Task:

1. To configure SW1, SW2 and SW3 to run MST using the revision number 1 and region name NETWORKBULLSand then configure VLANs 1-5 to run on SW1 MST instance 1.
2. To configure SW1, SW2 and SW3 to run MST using the revision number 2 and region name Cisco then configure VLANs 1-5 to run on SW1 MST instance 2.



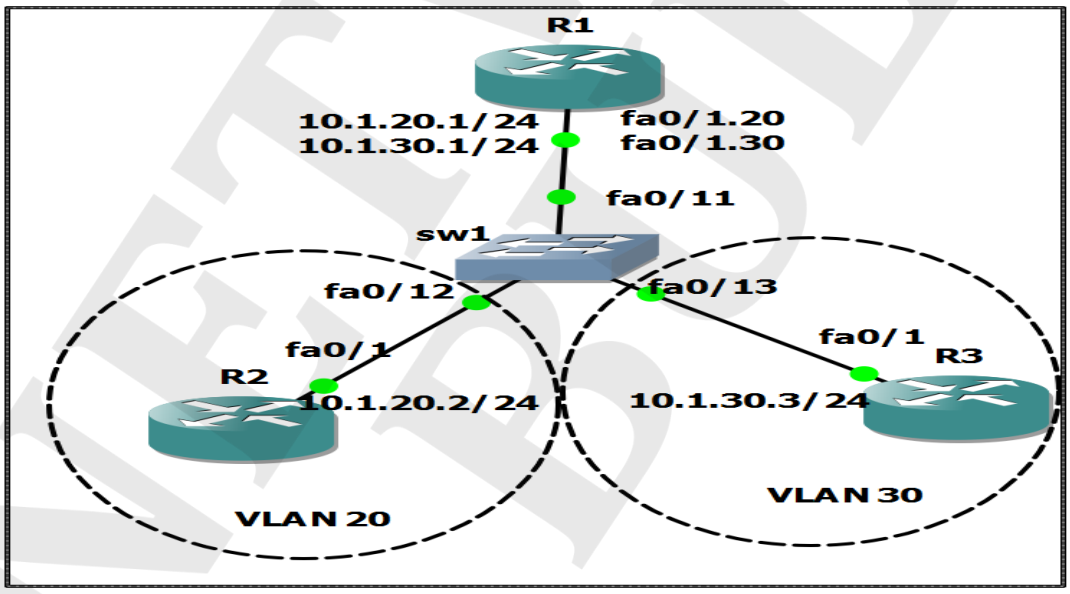
Practical 69: IVR (Inter VLAN Routing) using router as a stick

The following information should be preconfigured:

- Create VLAN's 20 and 30 on SW1 and configure interface Fa0/11 on SW1 as an 802.1q trunk link.
- On SW1 configure interface Fa0/12 to access VLAN20 and Fa0/13 to access VLAN 30.
- Configure the IP address 10.1.20.2/24 on R2's FastEthernet0/1 interface.
- Configure the IP address 10.1.30.3/24 on R3's Fastethernet0/1 interface.

Task:

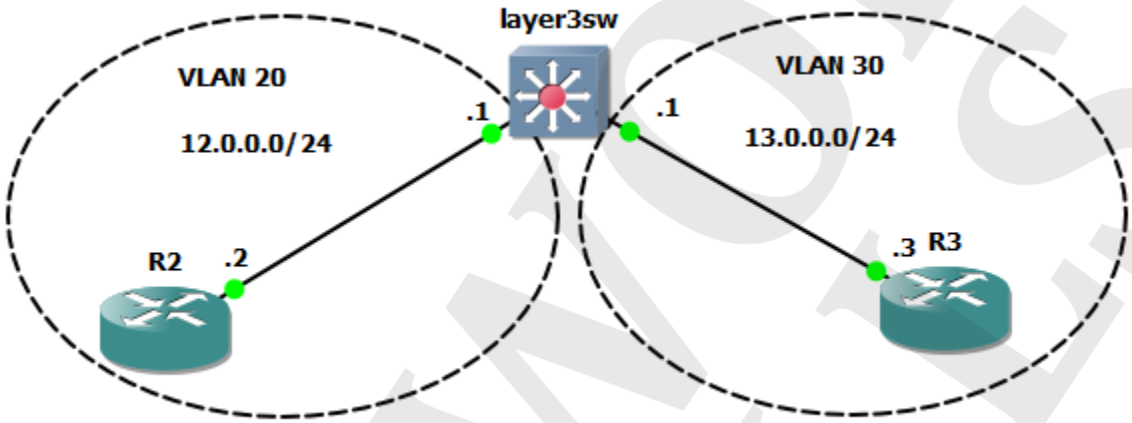
1. To configure a new Sub-Interface on R1 to match the VLAN 20 (Fa0/0.20) and configure the sub-interface to use 802.1q encapsulation and the Dot1q tag of 20. Configure the sub-interface to use the IP address 10.1.20.1/24.
2. To configure a new Sub-Interface on R1 to match the VLAN 30 (Fa0/0.30) and configure the sub-interface to use 802.1q encapsulation and the Dot1q tag of 30. Configure the sub-interface to use the IP address 10.1.30.1/24.
3. To disable IP Routing on R2 and R3 and configure the default gateway on R2 and R3 to use R1's respected Sub-interface as the default gateway.
4. Verify that R2 can ping R3's FastEthernet0/0 interface using R1 as the default-gateway.



Practical 70: IVR (Inter VLAN Routing) using layer-3 switch

In IVR using multi-layer switch, IP addresses are configured for each VLAN and these IP addresses will serve as the default gateways for the clients on each VLAN. By adding an IP address to a VLAN, those networks will be added to the routing table as directly connected routes, allowing routing to occur.

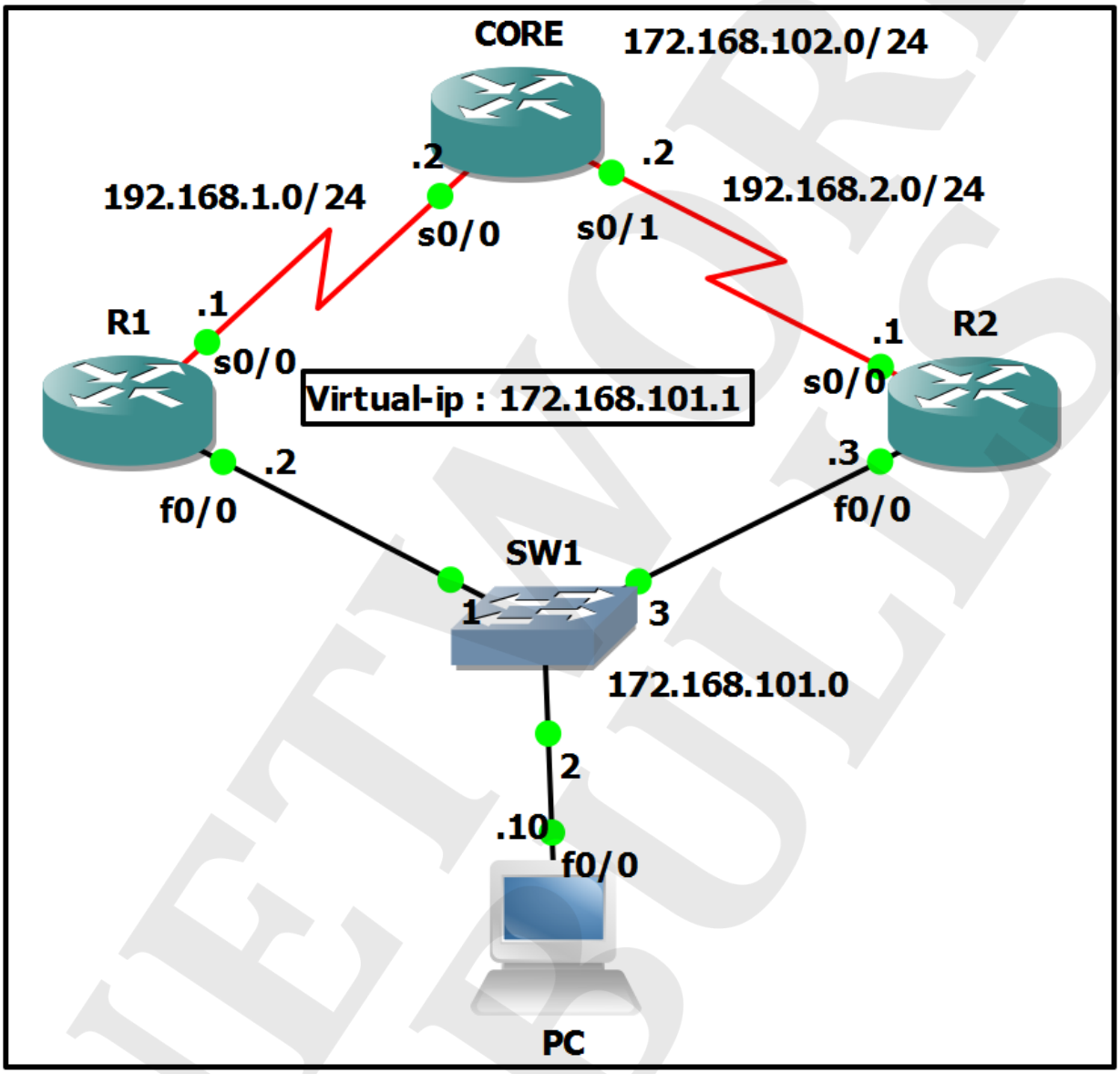
Task: To configuration of inter-VLAN routing on a multilayer switch or layer-3 switch.



Layer-3 High availability

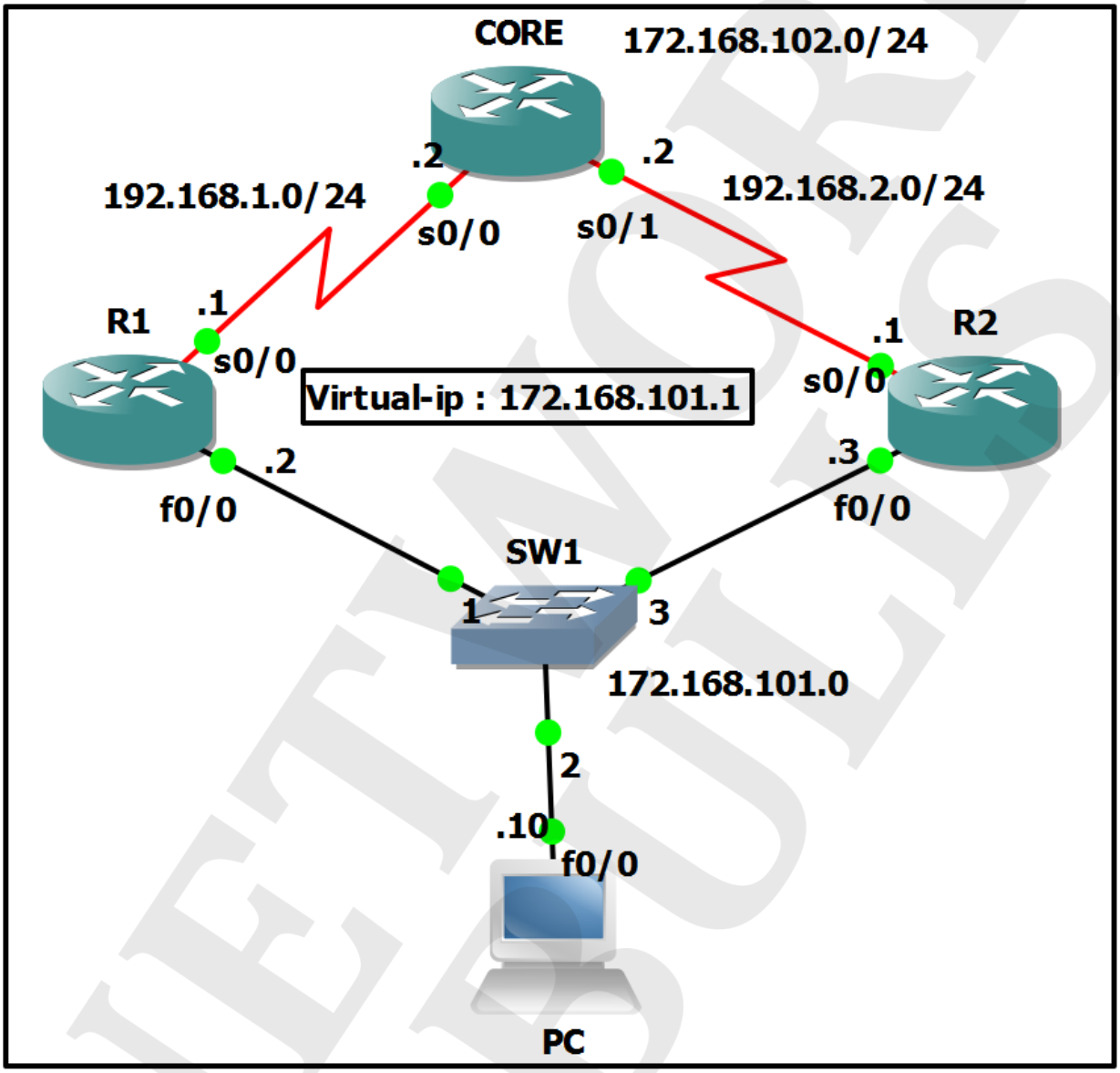
Practical 71: HSRP

Task: To configure HSRP in the given topology and also verify the configurations.



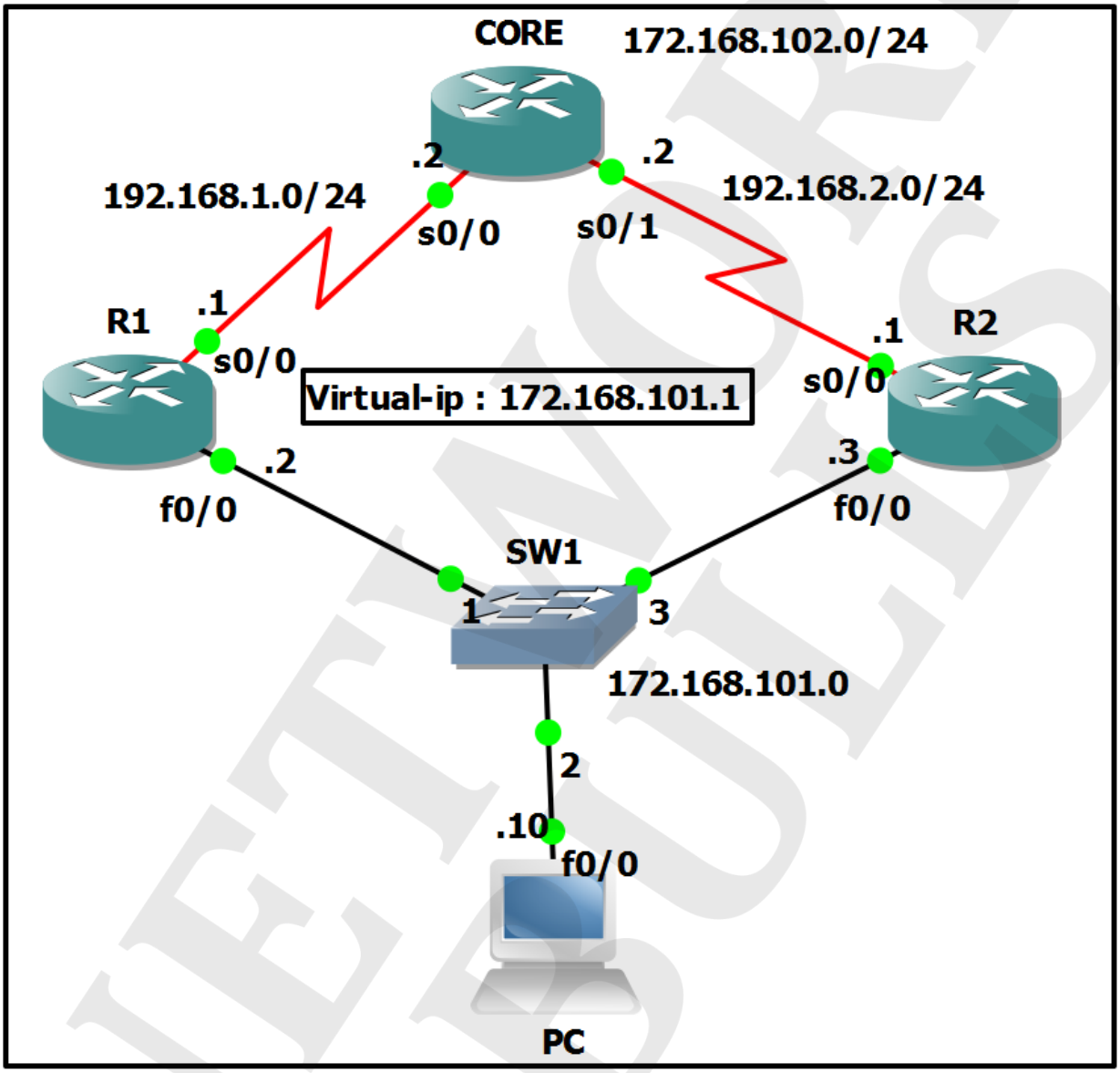
Practical 72: VRRP

Task: To configure VRRP in the given topology and also verify the configurations.



Practical 73: GLBP

Task: To configure GLBP in the given topology and also verify the configurations.



Port-Security

Port security with dynamically learned and static MAC addresses is used to restrict a port's ingress traffic by limiting the MAC addresses that are allowed to send traffic into the port. When you assign secure MAC addresses to a secure port, the port does not forward ingress traffic that has source addresses outside the group of defined addresses. If you limit the number of secure MAC addresses to one and assign a single secure MAC address, the device attached to that port has the full bandwidth of the port.

A security violation occurs in either of these situations:

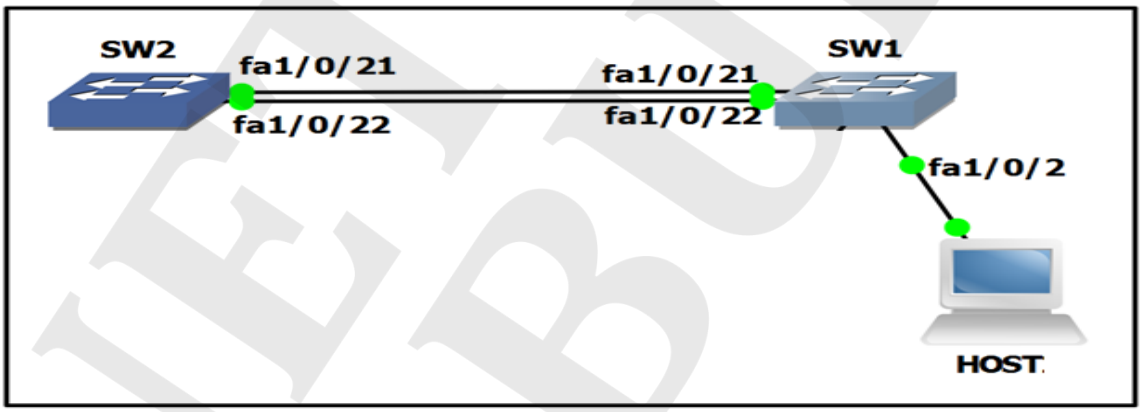
- When the maximum number of secure MAC addresses is reached on a secure port and the source MAC address of the ingress traffic is different from any of the identified secure MAC addresses, port security applies the configured violation mode.

- If traffic with a secure MAC address that is configured or learned on one secure port attempts to access another secure port in the same VLAN, applies the configured violation mode.

Practical 74: Configuration of Port-Security

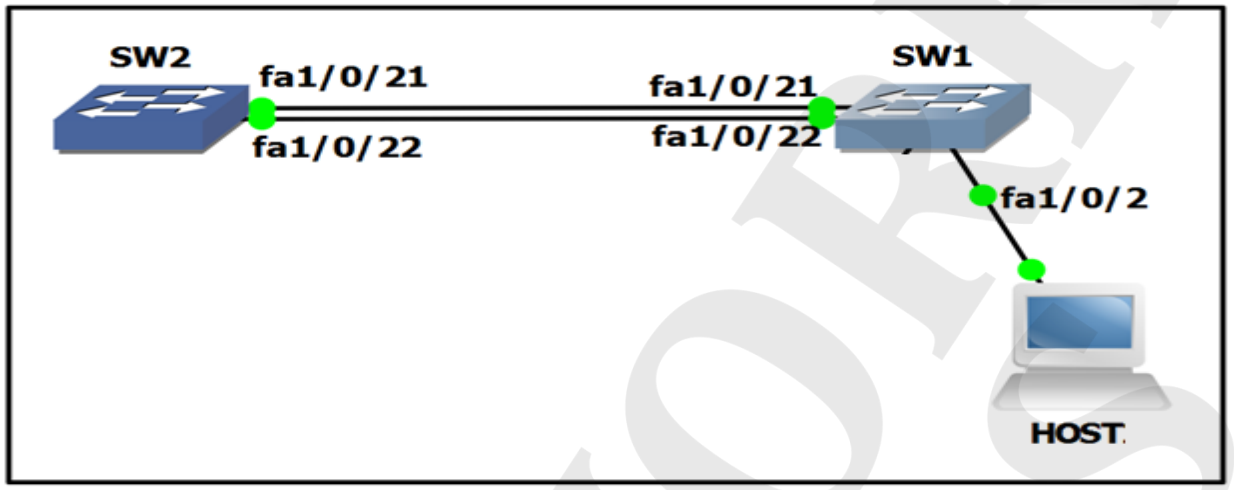
Task:

1. To configure port-security on Fa 1/0/2 port of SW1.
2. To configure different source MAC address of the ingress traffic from the identified secure MAC addresses.



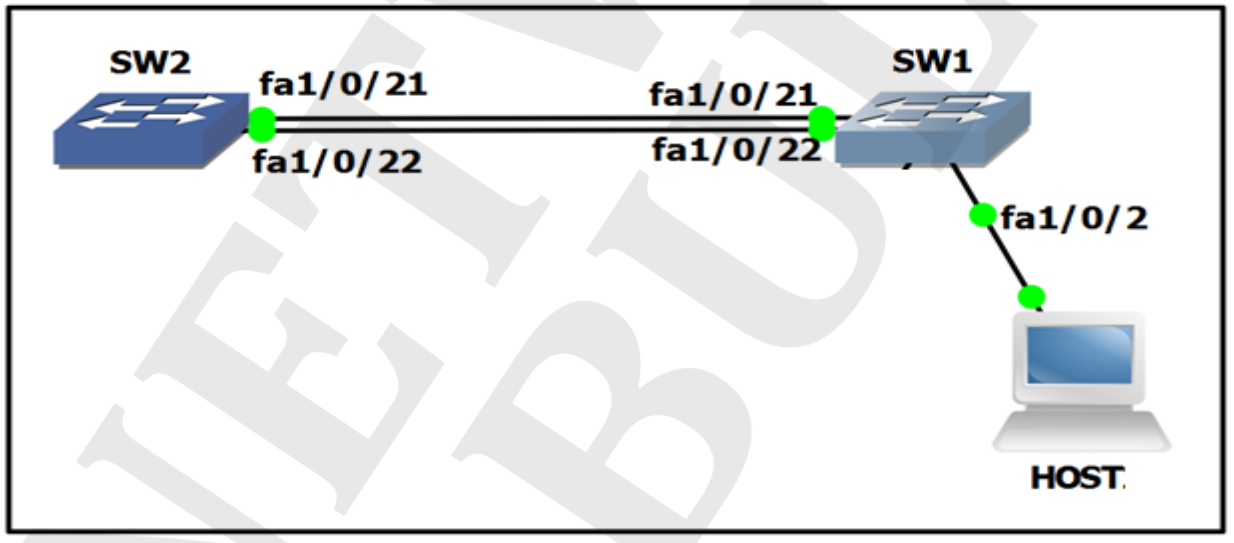
Practical 75: Manual err disable recovery in Port-Security

Task: To recover fa1/0/2 port of SW1 from errdisable state manually.



Practical 76: Auto errdisable recovery in Port-Security

Task: To configure auto-errdisable recovery for Fa1/0/2 port of SW1.



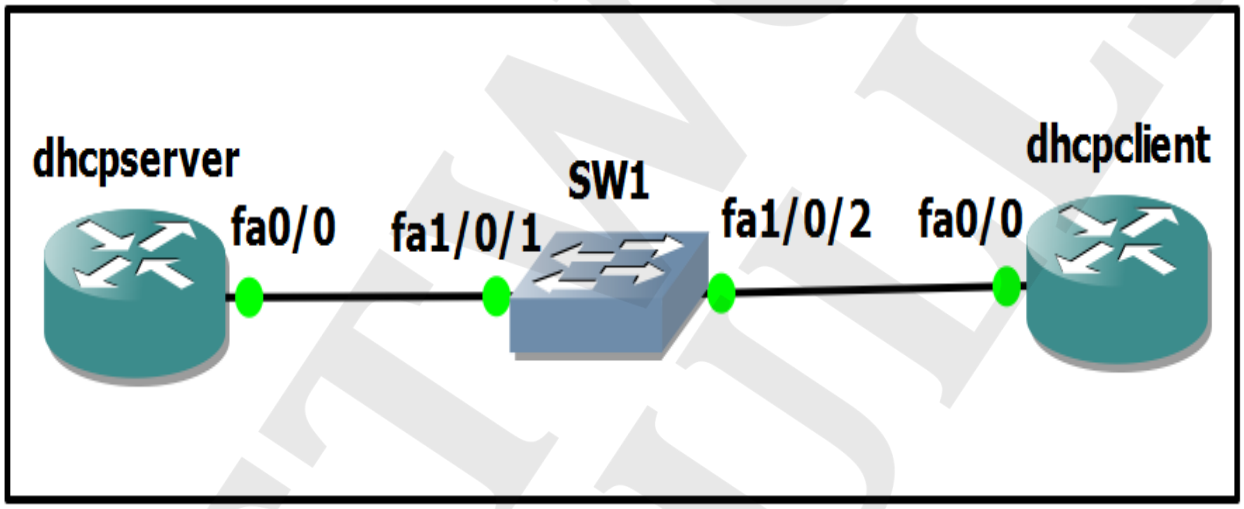
DHCP

Dynamic Host Configuration Protocol (DHCP) is a network protocol that enables a server to automatically assign an IP address to a computer from a defined range of numbers (i.e., a scope) configured for a given network.

Practical 77: Configuration of DHCP

Task:

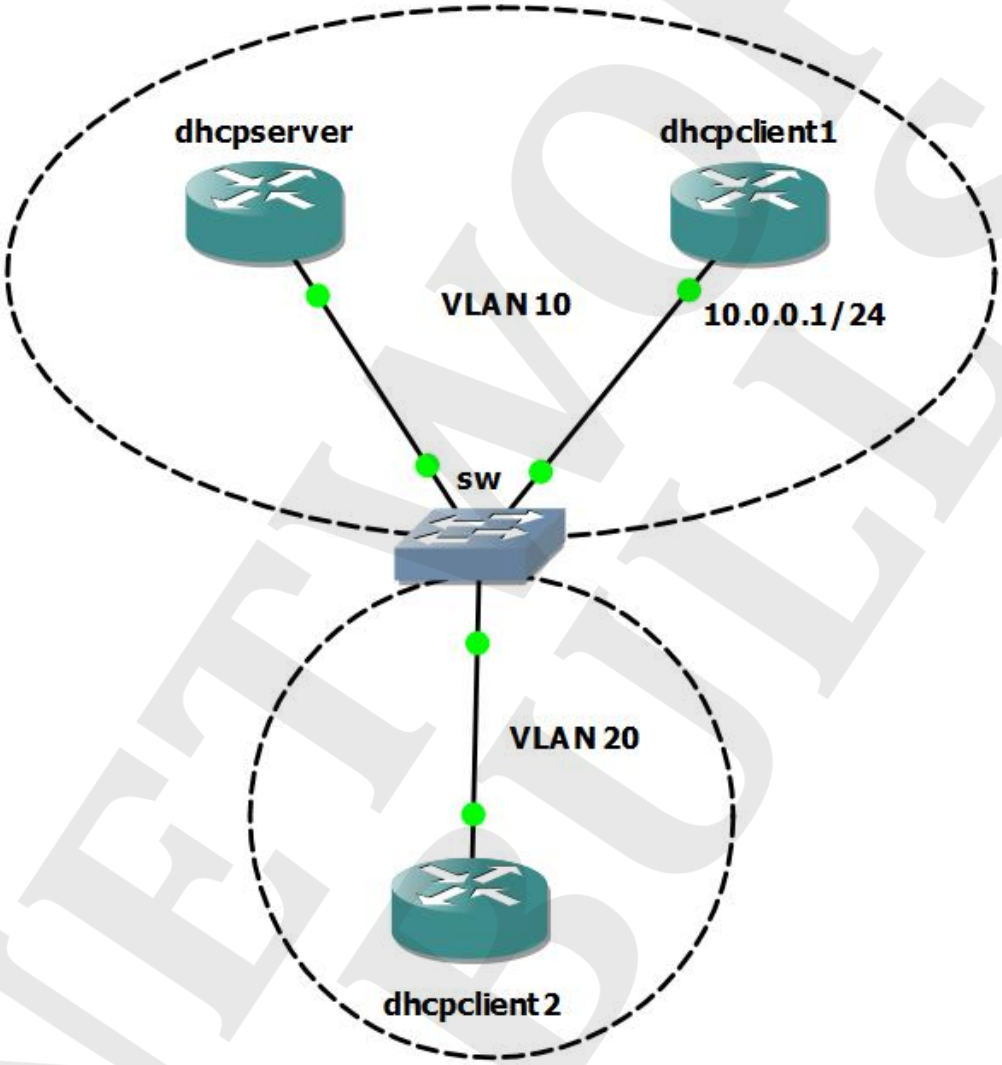
1. To configure DHCP server using following parameters:
    a. DHCP pool name should be “Networkbulls”.
    b. Network range should be “192.168.101.0/24”.
    c. Default gateway address should be set to "192.168.101.1/24”.



Practical 78: DHCP Relay Agent

DHCP IP Helper addresses are IP addresses configured on a routed interface such as a VLAN Interface or a routers Ethernet interface that allows that specific device to act as a "middle man" which forwards BOOTP (Broadcast) DHCP request it receives on an interface to the DHCP server specified by the IP Helper address via unicast.

Task: To configure switch as DHCP relay agent.

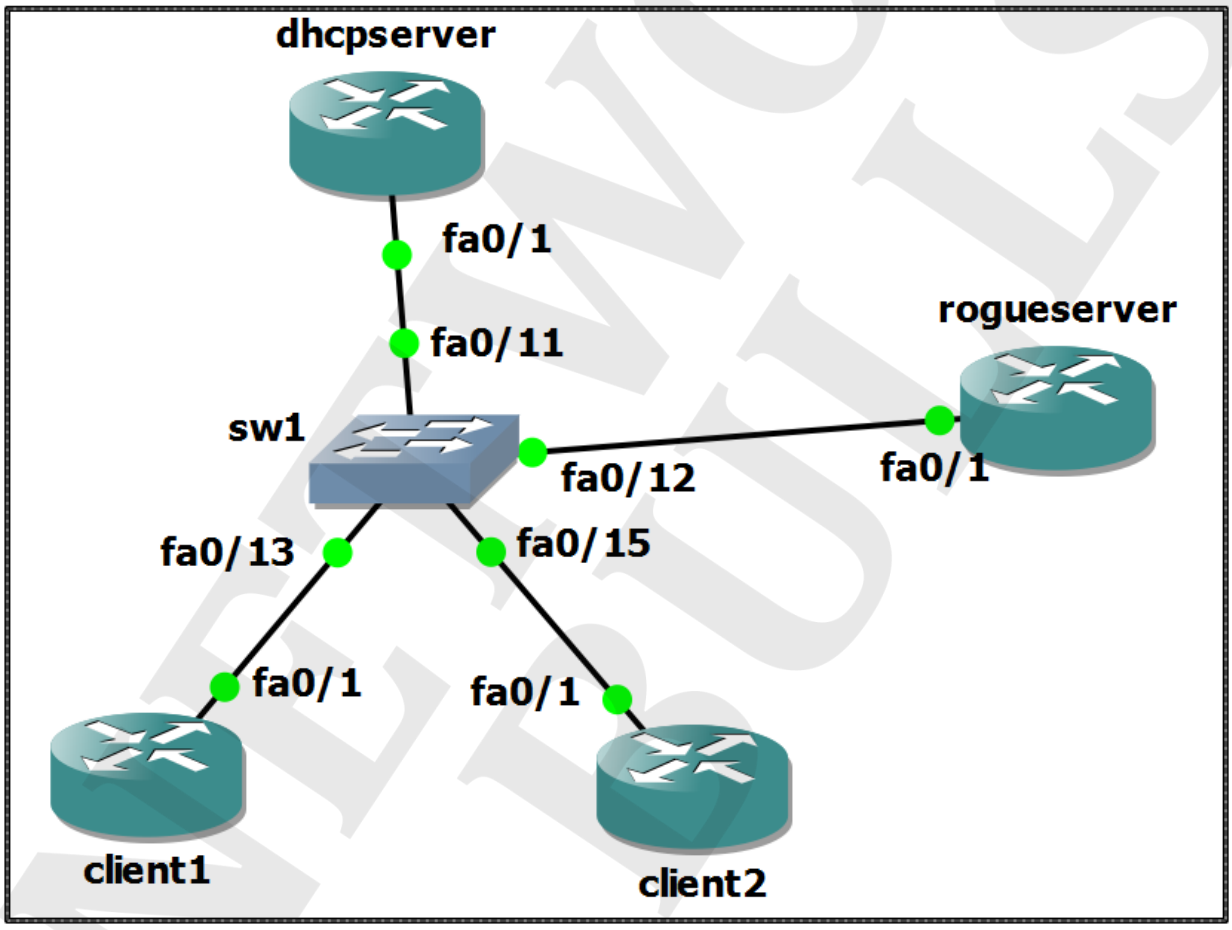


DHCP Snooping

The DHCP snooping feature determines whether traffic sources are trusted or untrusted. An untrusted source may initiate traffic attacks or other hostile actions. To prevent such attacks, the DHCP snooping feature filters messages and rate-limits traffic from untrusted sources.

Practical79: Configuration of DHCP Snooping

Task: To configure DHCP snooping on SW1 in order to prevent clients from obtaining IPs from rougeserver.

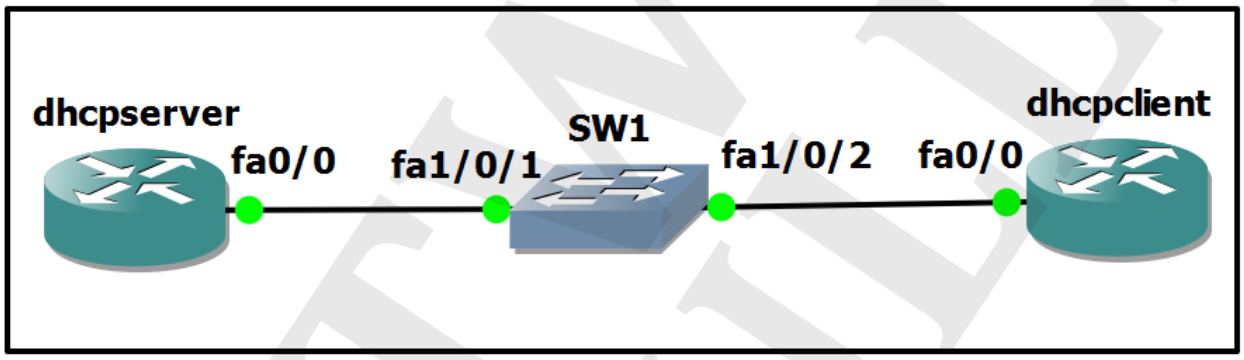


IP Source Guard

IP Source Guard uses the DHCP snooping binding's database. When IP Source Guard is enabled, the switch drops the incoming packets that do not match a binding in the binding's database. IP Source Guard can be configured to enforce just the source IP address or both the source IP address and source MAC address.

Practical 80: Configuration of IP Source guard

Task: To configure IP source guard on SW1.



T-SHOOT PRACTICALS

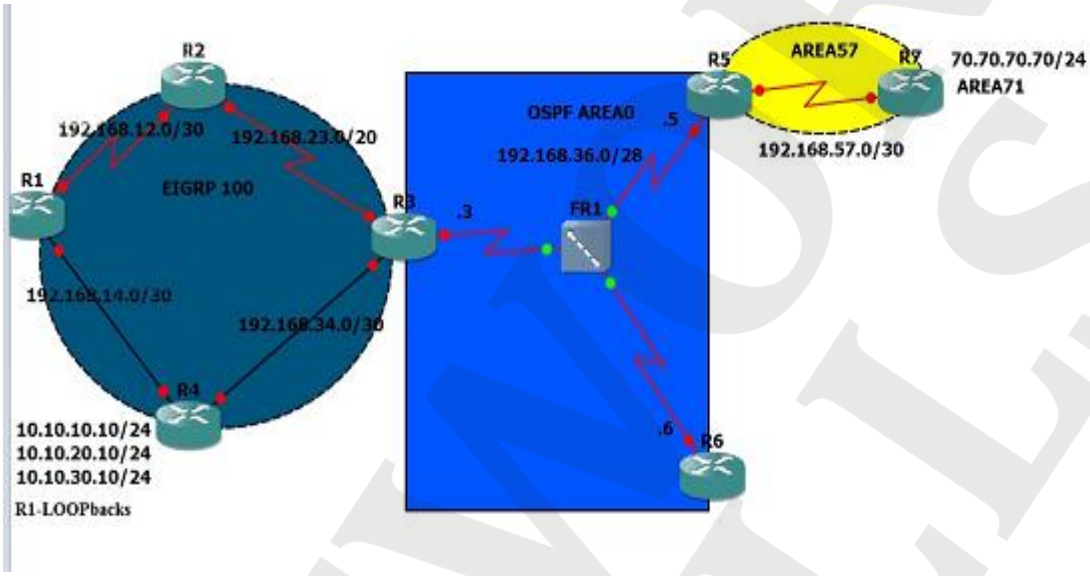
Note: To start with T-Shootpracticals, pre-configuration files of every single practical are required which can be taken from the Lab instructor or from the Lab's FTP Server.

Practical 81:

Task:

1. All IP addresses and routing protocols are preconfigured.
2. Ping from R1's loopback to R7's loopback.
3. Use traceroute to see which path is preferred.

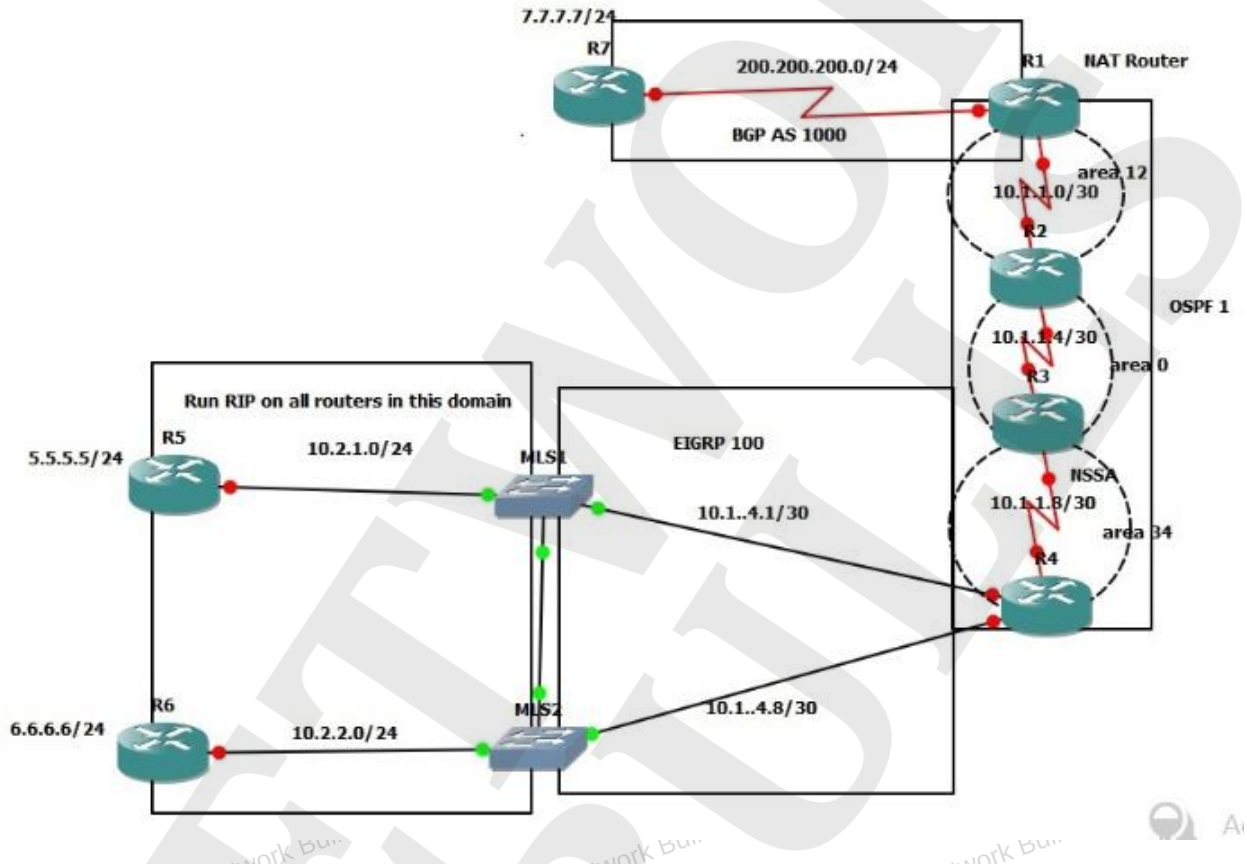
Note: You are not allowed to change the configuration. You can only modify it.



Practical 82:

Task:

1. All IP addresses and routing protocols are preconfigured.
2. Ping from R1's loopback to R5's loopback.
3. In routing table of R1, all routes are visible; change it so that you can see one default route.
4. Check for BGP neighborship between R7 and R1.

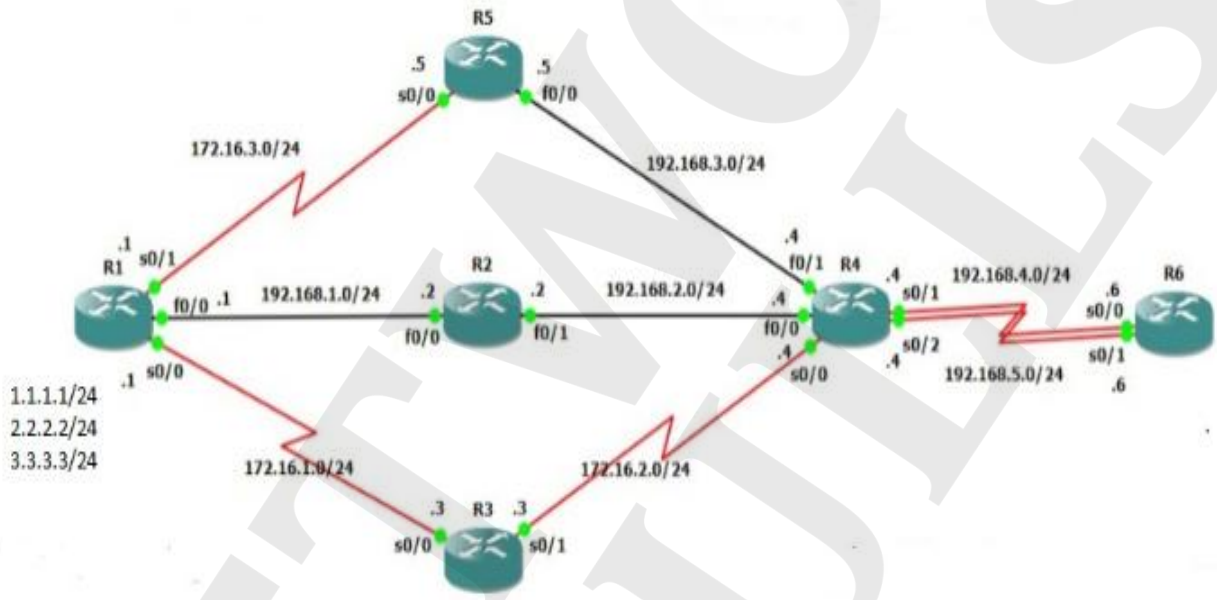


Practical 83:

Task:

1. All IP addresses and routing protocols are preconfigured.
2. Traceroute from R1's loopback to R6's loopback.
    a. For 1.1.1.1/24 via R5 should be preferred.
    b. For 2.2.2.2/24 via R3 should be preferred.
    c. For 3.3.3.3/24 via R2 should be preferred.

Note: You are not allowed to change the configuration. You can only modify it.

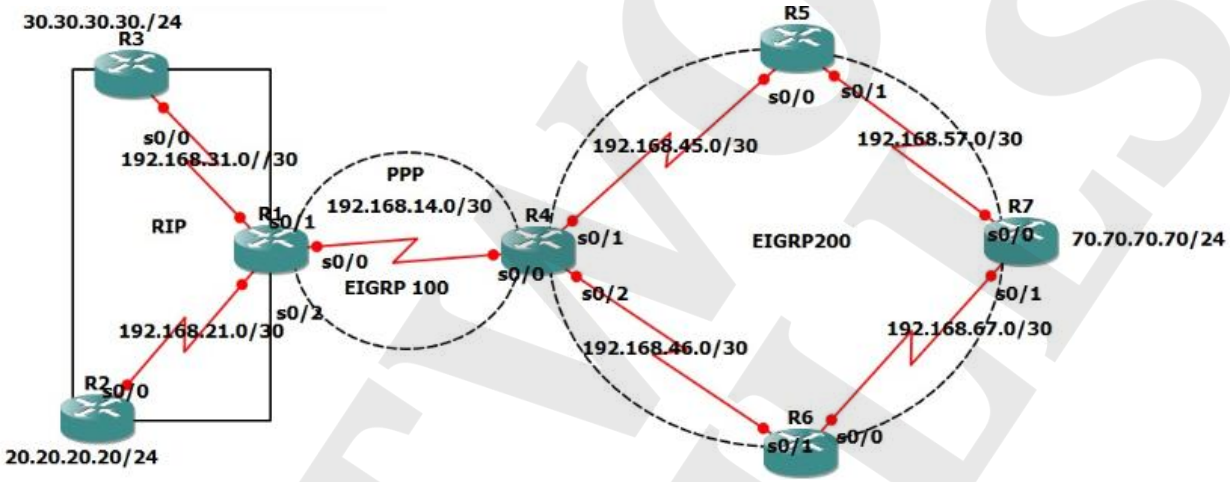


Practical 84:

Task:

1. All IP addresses and routing protocols are preconfigured.
2. Ping from 30.30.30.30/37 to R7's loopback.

Note: You are not allowed to change any configuration, you can only modify it.

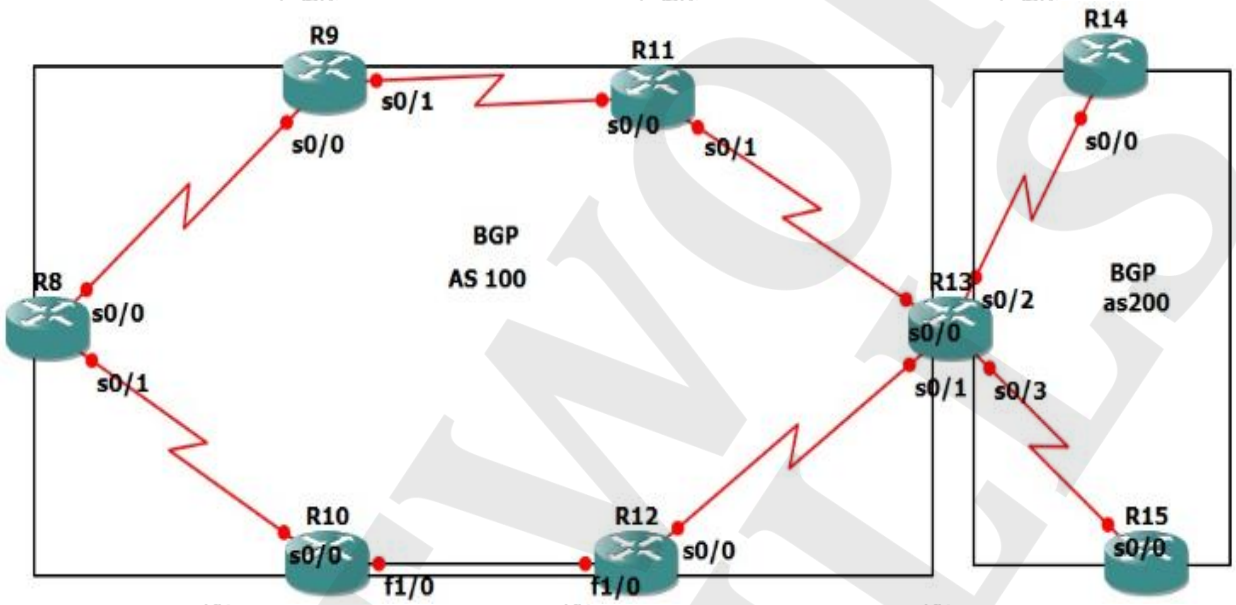


Practical 85:

Task:

1. All IP addresses and routing protocols are preconfigured.
2. Ping from R8's loopback to R15's loopback.

Note: You are not allowed to change any configuration, you can only modify it.

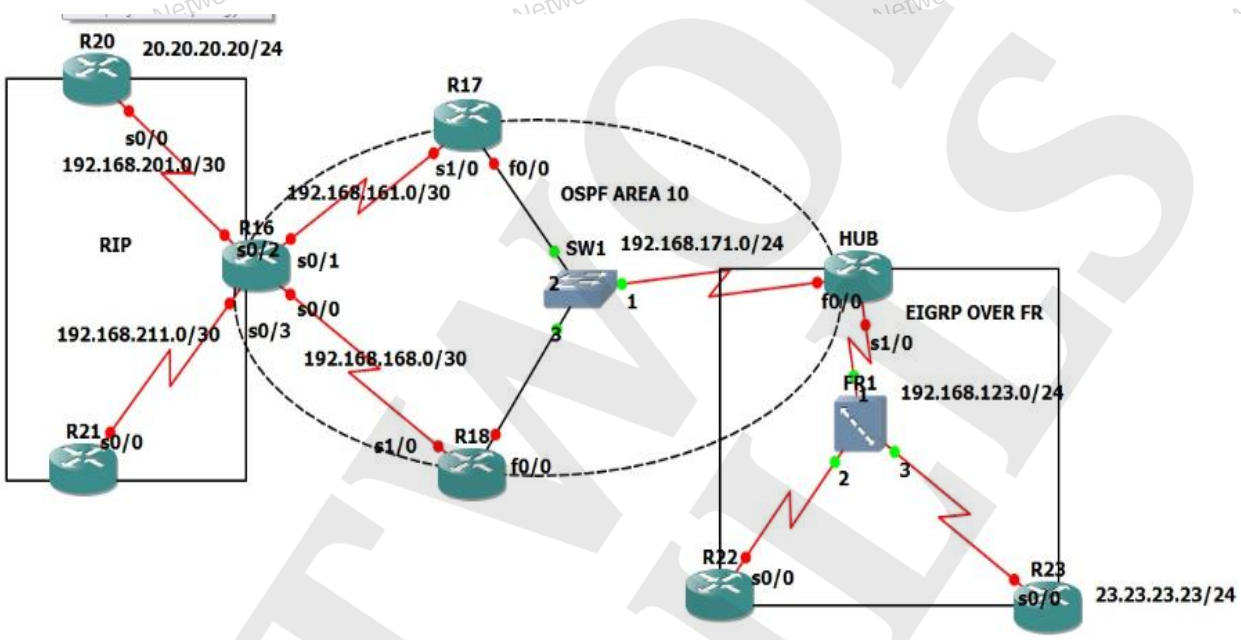


Practical 86:

Task:

1. All IP addresses and routing protocols are preconfigured.
2. Ping from R23 loopback to R20 loopback.
3. Path via R18 must be preferred, use traceroute for this.

Note: You are not allowed to change any configuration, you can only modify it.

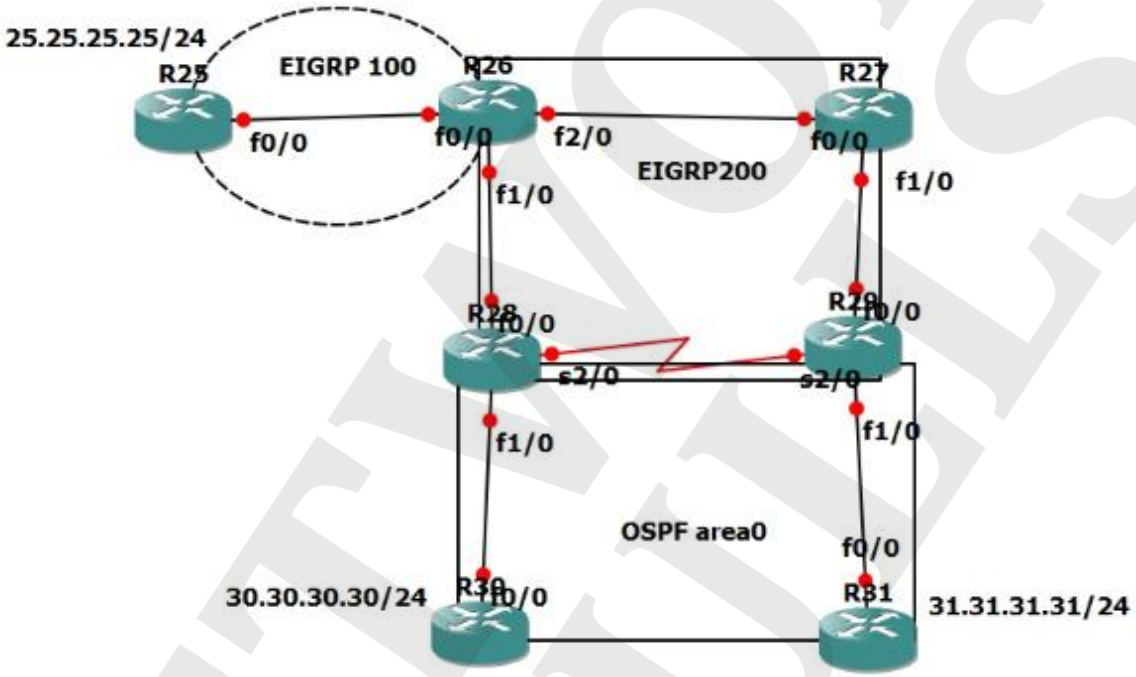


Practical 87:

Task:

1. All IP addresses and routing protocols are preconfigured.
2. Ping from R30 loopback to R25 loopback and path via R28 must be preferred.
3. When you ping from R31 loopback to R25 loopback, path via R29, R27 must be preferred.

Note: You are not allowed to change any configuration, you can only modify it.

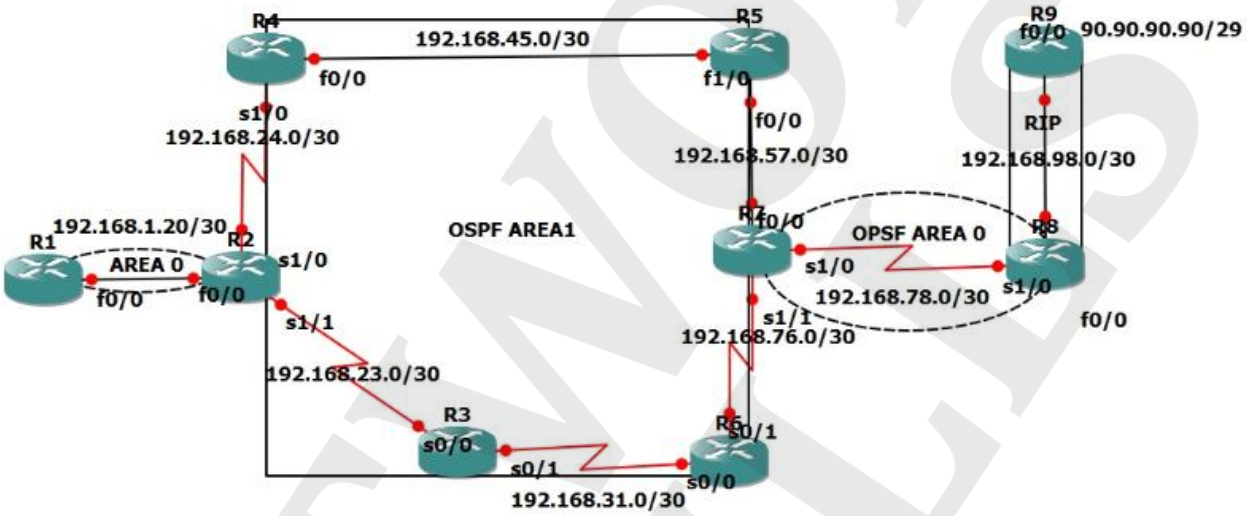


Practical 88:

Task:

1. All IP addresses and routing protocols are preconfigured.
2. Ping from R9 loopback to R1 loopback, use traceroute to check which path is preferred.
3. Prefer the path via R6-R3-R2.

Note: You are not allowed to change any configuration, you can only modify it.

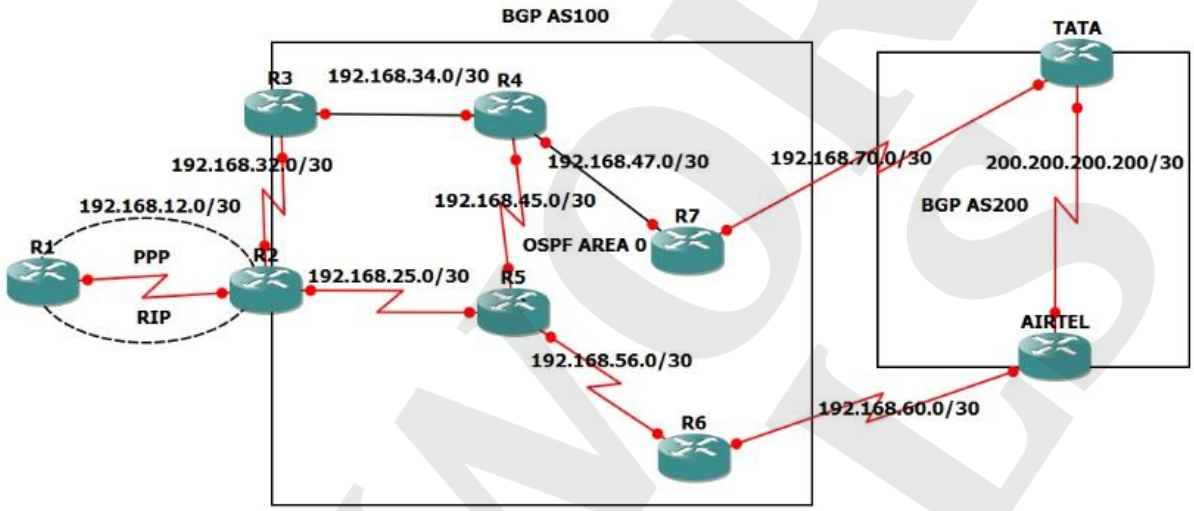


Practical 89:

Task:

1. All IP addresses and routing protocols are preconfigured.
2. Ping from R1 loopback to 10.10.10.10/30 to Tata and Airtel.

Note: You are not allowed to change any configuration, you can only modify it.

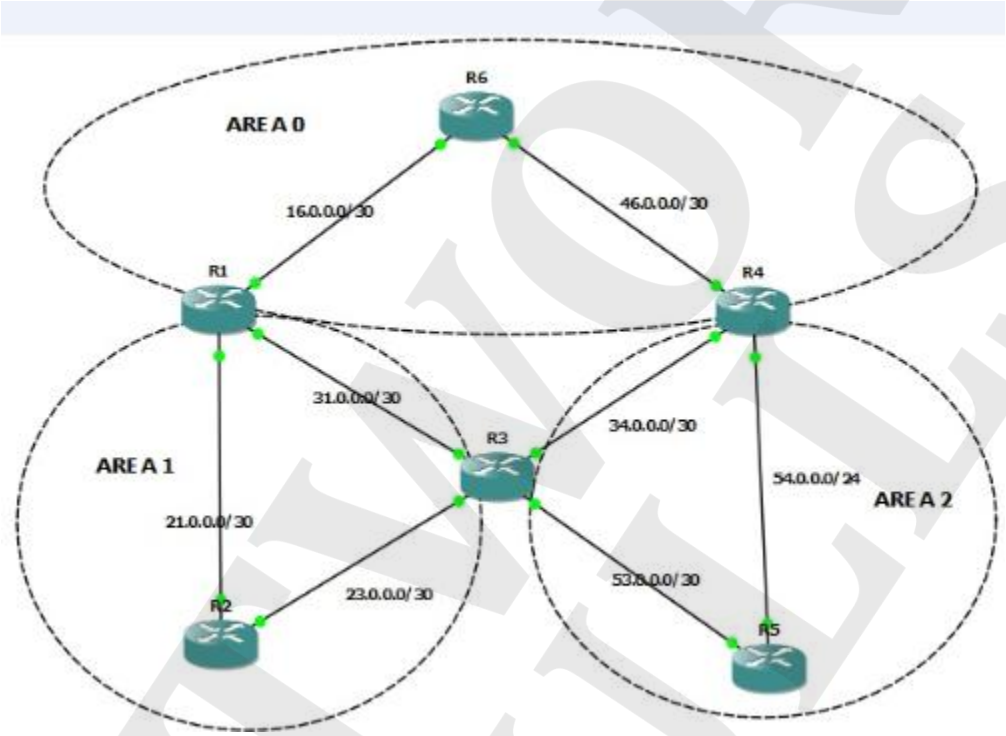


Practical 90:

Task:

1. All IP addresses and routing protocols are preconfigured.
2. Ping from R2 loopback 20.20.20.20/24 to R5 loopback 50.50.50.50/24.
3. Use traceroute to check which path is preferred; path via R3 should be preferred.

Note: You are not allowed to change any configuration, you can only modify it.

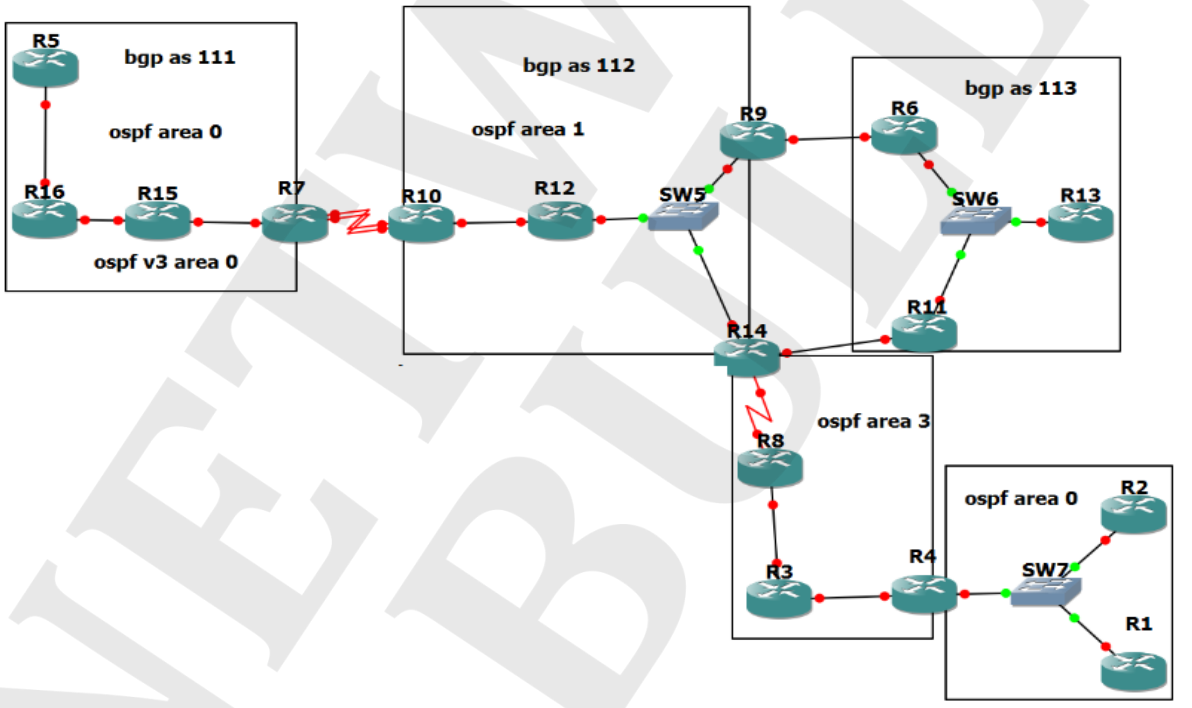


Practical 91:

Task: Configure the diagram according to the diagram.

Precautions:

1. IPv6 OSPF should be running in BGP AS 111 and R7 should be able to telnet R5 IPv6 OSPF network.
2. OSPD area 0 should not be reachable by OSPF area 3 and other OSPF areas.Do not use any type of filtering for it.
3. R13 always prefer R6 for any network of BGP AS 111.
4. No IGP should be used in BGP AS 113.
5. R1 should be able to ping R13 loopback.
6. OSPF should not be redistributed in BGP on R14.
7. You are not allowed to change BGP next-hop-self.
8. All OSPF areas should have md5 authentication with password CISCO.
9. All devices should be telnet enabled with password CISCO.
10. BGP AS 112 devices should be able to SSH any device in the whole topology.



Practical 92:

TSHOOT FINAL PRACTICAL

Task: You are not allowed to delete any configuration, just modify it.

- All IP addresses and routing protocols are pre-configured.
- Ping from R15 loopback to R14 loopback.
- Using traceroute check which path is preferred.
- Path via R2 must be preferred.
- Ping from R12 loopback to R15 loopback.

You cannot delete any ACL.