NETWORK BULLS
WHERE CAREERS FLY

CCNP
ROUTING & SWITCHING
PRACTICAL LAB WORKBOOK

DARE TO CHALLENGE YOUR SKILLS

COMPLETE THE TESTS & TAKE YOUR CAREER TO NEXT LEVEL

“**CONQUER** THE CCNP WORK BOOK CHALLENGES & YOU WILL BE READY FOR **CCIE** ”

Yes, this Network Bulls’ CCNP Work Book is full of tough questions and you need to find the solutions.
Solve the workbook, master the challenges and Take Your Career to the Next Level.

No solutions, only hurdles!!
Develop a winning attitude by solving it.
We know it’s tough, in fact very tough but **you can do it.**

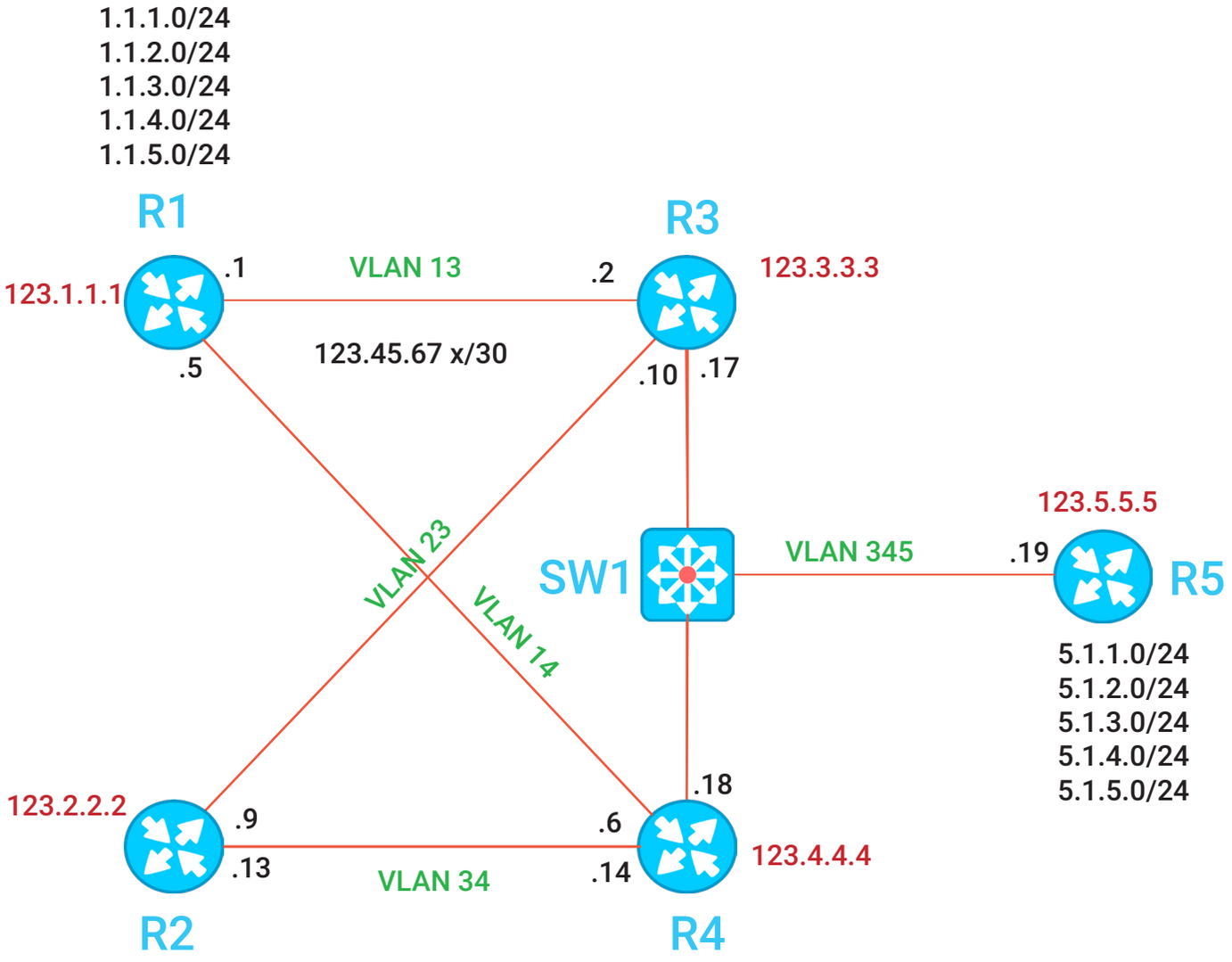
WHEN GOING IS TOUGH, ONLY TOUGHER GETS GOING

Use every bit of knowledge that you have till date; it’s time to implement what you have learned. This workbook will take you through the hardest questions of CCNP but once you do it; we assure you that your future is

SUPER BRIGHT

“ **START** WITH ZEAL, WORK WITH PASSION & YOU WILL **FINISH** IT WITH EASE ”

EIGRP Classic Mode



Guidelines for the task

If you are creating this topology on racks then make use of VLANs. However, if you are creating it on GNS then VLANs are not required.

- **Task 1** is the basic configuration task. Follow the question to accomplish the task and configure addressing as shown in diagram.
- **Task 2** is path selection using interface characteristics that means you have to tweak bandwidth or delay of the interfaces to do this task.
- **Task 3** is basic route-summarization task and also involves leakmap. Remove the configuration of Task 2 before starting this task.
- **Task 4** is about path selection using summarization. Consider longest match first rule for completing the task. Remove the configuration of task 3 before starting with task 4.
- **Task 5** is all about default route-origination in EIGRP. Use redistribution method for accomplishing the task.
- **Task 6** is about EIGRP route-filtering, use standard ACL, extended ACL, prefix-list and route-map for completing the task. Use each method one by one to perform filtering and remove previous filtering task before starting with the next task. For e.g.- if filtering is done using standard ACL then remove the filtering done (Standard ACL) before starting with extended ACL and so on.

Task 1: Basic Configuration

(A) Configure the IP addressing on the routers as shown in the diagram. 123.45.67.x is the major network, where x is the relevant subnet number. Use/30 on point-to- point segments and /29 on multi-access segments.

(B) Configure EIGRP on all the routers (classic mode). Autonomous system number will be 123 and every router should have 123.x.x.x/32 configured as the router-id explicitly.

(C) Enable EIGRP on routers for configured networks. Run EIGRP specifically on all the subnets specifically assigned to the physical interfaces and the loopback used as router id. Use any method for remaining networks.

(D) Configure the routers such that they should use hello interval of 3 sec's and hold for 9 sec's on all interfaces. Routers should not receive any EIGRP route from the router that is more than 3 hops away.

(E) All the EIGRP routers should use delay as the relevant component for the metric calculation and delay value should be 100 usecs on all the interfaces.

Task 2: EIGRP Path Selection (using interface characteristics)

(A) In the topology, R1 and R2 should receive all the loopback routes of R5 via R3 and R4 both as the best routes. R5 should receive all the loopback routes of R1 and R2 via R3 and R4 both as the best routes.

(B) Now, ensure that R1 and R2 should receive each other's routes and routes from R5 (loopbacks) via R3 as the best routes and via R4 as the backup routes.

(C) To accomplish all the above tasks you are allowed to alter only the interface characteristic (bw, delay, load, reliability, mtu).

Task 3: EIGRP Route - Summarization

(A) R1 and R2 should receive each other's routes specifically via R3 and they should receive a summary of /16 via R4.

(B) R1 and R2 should receive R5's routes specifically via R4, and they should receive a summary of /16 via R3.

(C) R5 should receive routes of R1 and R2 specifically via R3 and a summary of /16 via R4.

(D) R1 and R2 should receive the loopback 5.1.5.1 via R3 and R4 as /24 route.

Task 4: Path Selection using Route - Summarization

(Please remove the previous task to do this one)

(A) R1 and R2 should take path via R4 to reach the loopbacks of R5; this should be revealed by the trace output.

(B) R1 and R2 should take path via R3 to reach each other's loopback this should be revealed by trace output.

(C) R5 should take path via R4 to reach the loopbacks of R1 and R2 but specifically to reach the R1 loopback 1.1.1.1 and R2 loopback 2.1.1.1, R5 should go via R3. This should be revealed by the trace output.

(D) In order to accomplish this task you are not allowed to change any interface characteristic. Do not use offset-lists and do not use route-filtering.

Task 5: EIGRP Default-Route Advertisement

(A) Consider R1 and R2 to be the edge routers connected to ISP. Originate a default route from R1 and R2 both but all routers (R3, R4, R5) should use the default route of R1 as primary route. If R1 fails then all routers should use R2's default route. To verify your task configure a loopback 8.8.8.8 as the Google DNS server on R1 and R2. Don't advertise it in EIGRP. R3, R4 & R5 trace should follow R1 to reach 8.8.8.8 and if R1 fails, it should follow R2.

Task 6: EIGRP Route - Filtering using Distribute-List

Standard acl only

(A) R1 must receive the loopback routes of R2 only via R3 and routes of R5 loopbacks only via R4.

(B) R2 must receive the loopback routes of R1 only via R4 and routes of R5 loopback only via R3.

(C) R5 must receive R1 routes via R3 and R5 should receive R2 routes only via R4 (loopback routes). To achieve the above task classification should be done with standard ACL.

(D) Create 10 loopbacks on R5 from 55.1.1.1-55.1.10.1/24 and advertise them in EIGRP. R1 and R2 should receive all the odd loopbacks of the given range via R3 only and even loopbacks via R4 only (Standard ACL).

Extended ACL only

(A) Repeat all the above tasks using extended ACL for classification.

(B) R5 should receive all the odd routes only via R3 and even routes via R4. Use the extended ACL and apply the filter only on R5.

ROUTE-FILTERING (Prefix-list for the Classification)

(A) Create the loopbacks of variable length subnet mask from network 5.2.0.0/24 (for ex- 5.2.0.0/25,5.2.0.128/26 etc. till/30) and advertise them in the EIGRP. Now, R1 should receive all these loopbacks only via R3 and R2 should receive them only via R4. Create a prefix-list and name it as FILTER. Prefix-list must have only two statements.

(B) Similarly, create loopbacks on R1 and R2 of variable length subnet mask from networks 1.2.0.0/24 and 2.2.0.0/24 respectively (from/24-/30). Now, the task is that R5 should receive R1 loopback routes only via R3 and R2 loopback routes via R4 only (use prefix-list).

ROUTE-FILTERING using route-maps

(A) Do not remove the loopbacks that were created in all the tasks.

(B) Apply the route-tag (1.1.1.1) on all the routes injected by R1, route-tag (2.2.2.2) on all the routes injected by R2, and route-tag (5.5.5.5) on all the routes injected by R5.

(C) R1 must receive all the routes with route-tag (2.2.2.2) via R3 and routes with route-tag (5.5.5.5) via R4 only.

(D) R2 must receive all the routes with route-tag (1.1.1.1) via R4 and routes with route-tag (5.5.5.5) via R3 only.

(E) R5 must receive all the routes with route-tag (1.1.1.1) only via R3 and routes with route-tag (2.2.2.2) via R4 only.

REDISTRIBUTION AND FILTERING

(A) Disable EIGRP on all R5 loopbacks and redistribute them in EIGRP with metric (1000000 10 255 1 1500) and a route-tag 5.5.5.5. You only need to redistribute the loopbacks no other physical interface.

(B) Disable EIGRP on all R1 and R2 loopbacks and redistribute them on R1 and R2 with route-tag (1.1.1.1 and 2.2.2.2) respectively.
Now repeat the task given above again.

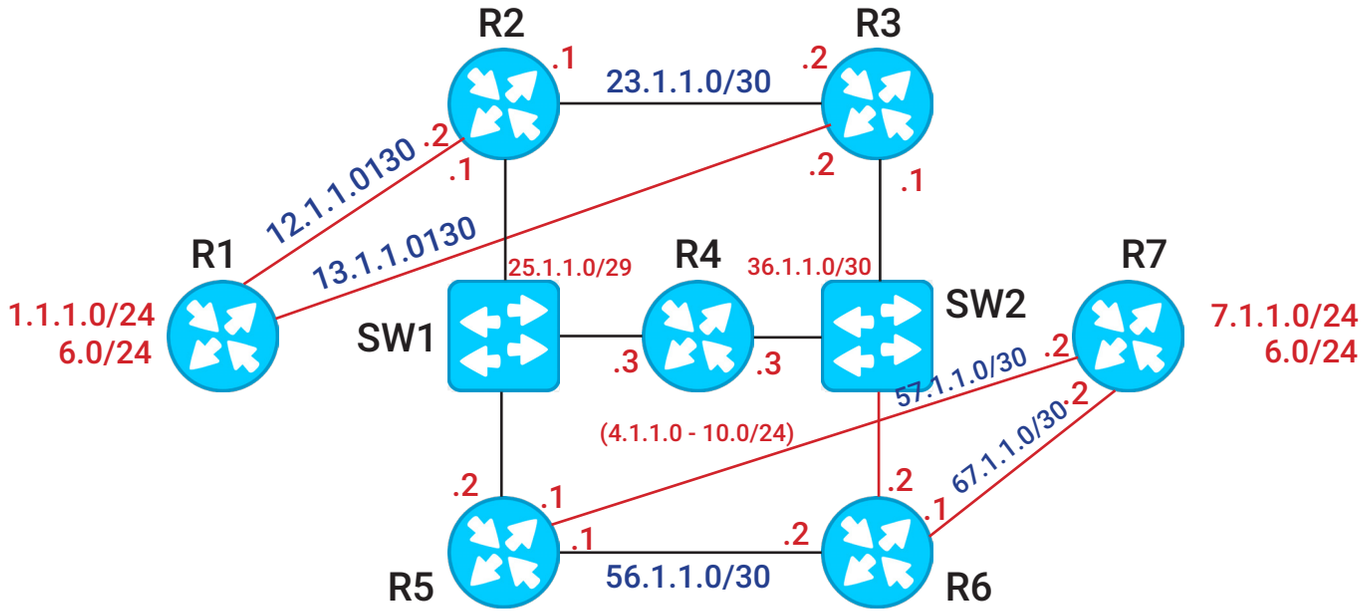
“

Congrats,
you have completed the first Milestone Successfully.

ROAD AHEAD IS TOUGHER BUT WE KNOW YOU CAN DO IT. KEEP MARCHING ON…
ALL THE BEST!

”

EIGRP Named Mode



Guidelines for the task

- **Task 1** is to configure the addressing according to diagram.
- **Task 2** is about path selection by tweaking interface characteristics like bandwidth or delay.
- **Task 3** is about route-summary in named mode. Remove the configuration of task 2 before starting with task 3.
- **Task 4** is about path selection task using the route summarization. Use the longest match first rule to accomplish this task and remove the configuration of task 3 before starting this task.
- **Task 5** is about default route-origination. Make use of redistribution method in EIGRP for accomplishing the task.

In order to do task 6,7 and 8 please follow the instructions:

- **Task 6** is about EIGRP route-filtering, use standard ACL, extended ACL, prefix-list and route-map for completing the task. Use each method one by one to perform filtering and remove previous filtering task before starting with the next task. For e.g.- if filtering is done using standard ACL then remove the filtering done (Standard ACL) before starting with extended ACL and so on.

Task 1: Basic Configuration (Topology 2)

(A) Configure the IP addressing on all the routers as shown in the diagram.

(B) Configure EIGRP on all the routers use autonomous system no. 147 on all the routers and make sure all the routers should calculate 64 bit metric (use any name for the process).

(C) Enable EIGRP AS 147 on all the interfaces. All routers must authenticate each other on all point-to-point links and on multi-access segments (DO NOT USE MD5). Use password “NETWORKBULLS?”.

(D) When routers receive routes they should scale their metric by the factor of 192 and delay of all the interfaces should be configured 10 uses explicitly on all the interfaces including loopbacks as well.

(E) After the above configuration is done make the following verifications

1. R1 must receive the routes of R4 loopbacks and R7 loopbacks via R2 and R3.
2. R7 must receive the routes of R1 loopbacks and R4 loopbacks via R5 and R6.
3. R4 must receive the routes of R1 loopbacks via R2 and R3 and R7 loop backs via R5 and R6.

Task 2: Path Selection (Using Interface Characteristics Only)

(A) R1 must receive all the routes of R4 and R7 loopbacks via R2 as the best routes and via R3 as backup routes. Do not make any changes on R1 and R4.

(B) R7 must receive all the routes of R1 and R4 via R5 as the best routes and via R6 as backup routes. Do not make any changes on R7 and R4.

(C) R4 must receive R1 loopbacks via R3 as the best route and R7 loopbacks via R6 as the best route.

Make sure all the 3 tasks must not affect each other

Task 3: Route-Summarization (To do this task undo the previous task)

(A) R1 must receive the summary of R4 loopbacks as /16 route via R3 as a best route and via R2 as a backup route (do not change any interface cost).

(B) R7 must receive the summary of R4 loopbacks as /16 route via R6 as the best route and via R5 as a backup route (do not change any interface cost).

(C) R4 must receive R1 loopbacks as summary of /16 route via R2 as the best route and via R3 as the backup route. In addition, R4 must receive R7 loopbacks as summary of /16 route via R5 as the best route and via R6 as the backup route (do not change any interface cost).

Task 4: Path Selection Using Summarization (To do this task undo the previous task)

(A) R1 must receive R4 loopback routes as summary of /16 from R2 and R3. To reach the even loopbacks of R4 traffic should go via R2 and to reach the odd loopbacks of R4 traffic should go via R3.

(B) Similarly, R7 also must receive a summary of R4 loopback routes as /16 from R5 and R6 both. To reach the even loopbacks of R4 traffic should go via R6 and to reach the odd loopbacks of R4 traffic should go via R5.

(C) Now, R4 must receive the summary of R1 loopback routes as /16 from R2 and R3. To reach the odd loopbacks of R1 traffic should go via R3 and to reach the even loopbacks of R1 traffic should go via R2. R4 must receive a summary of R7 loopback routes as /16 from R5 and R6. To reach the odd loopbacks of R7 traffic should go via R5 and to reach the even loopbacks of R7 traffic should go via R6.

Above tasks can be verified through the trace output

Task 5: EIGRP Default Route Origination

(A) Consider R2, R3, R5 and R6 as the four edge router which will originate the default route. Now, make sure R1 must prefer R2's default route, R7 must prefer R5's default route, and R4 must receive a default route via R2 and R5 as the best route.

(B) Now, create a loopback 1.2.3.4/32 on routers 2, 3, 5, 6 as internet route and do not advertise it inside of EIGRP. R1 trace must go via R2, R7 trace must go via R5 and R4 trace must be sent to R2 and R5 both.

Task 6: Route-Filtering (Classify Through Standard Access-List)

(A) R1 must receive all the even routes of R4 and R7 only via R2 and all the odd routes of R4 and R7 via R3 only.

(B) R7 must receive all the odd routes of R4 and R1 only via R5 and all the even routes of R4 and R1 only via R6.

(C) R4 must receive all the even routes of R1 only via R3 and all the odd routes via R2. R4 must receive all the odd routes of R7 via R6 and all the even routes via R5.

(D) Perform the above task using extended access-list. Do not specify any interface while applying access-list with distribute list (use the relevant source in ACL).

Task 7: Route-Filtering (Classification Through Extended Access -List)

(A) Create variable length loopbacks on R1, R4 and R7; for example - on R1 (1.2.0.0/25 to /30), R2 (4.2.0.0/25-/30), R7 (7.2.0.0/25-/30). Advertise them in EIGRP using a single network command under the EIGRP process.

(B) Now, R1 must receive all the routes of R4 only via R2 and all the routes of R7 only via R3. Use prefix-lists to classify any prefix. The list must not have more than two statements.

(C) R7 must receive all the routes of R1 only via R5 and all the routes of R4 only via R6. Use prefix-lists to classify any prefix. The list must not have more than two statements.

(D) R4 must receive all the routes of R1 only via R3 and all the routes of R7 only via R5. Use prefix-lists to classify any prefix. The list must not have more than two statements.

Task 8: Route-Filtering Using Route-Tags

(A) Apply the route-tags on all the loopbacks injected by R1, R4 and R7 into EIGRP. Now, the route-tags will be R1 (1.1.1.1), R4 (4.4.4.4) and R7 (7.7.7.7).

(B) R1 must receive all the routes with tag value 4.4.4.4 only via R2 and all the routes with tag value 7.7.7.7 only via R3. While filtering do the classification on the basis of route-tags.

(C) R7 must receive all the routes with route-tag 1.1.1.1 only via R5 and all the routes with route-tag 4.4.4.4 only via R4. While filtering do the classification on the basis of route-tags.

(D) R4 must receive all the routes with route-tag 1.1.1.1 only via R2 and all the routes with route-tag 7.7.7.7 only via R6. While filtering do the classification on the basis of route-tags.

Task 9: Query Control

(A) Now configure the network in such a way that R1, R4 and R7 must not receive any query when any network in the topology goes down.

Task 10: Redistribution

Now disable EIGRP between R1-R2 and R1-R3 link and run OSPF 1 in area 0 between them. Similarly, disable EIGRP on R7-R5 and R7-R6 link and run OSPF 2 in area 0 on them.

(a) Now do the mutual redistribution between EIGRP and OSPF on routers R2, R3, R5, R6.

R1 must receive the routes of R7 and R4 via R2 and R3 both.
Similarly, R7 must receive the routes of R1 and R4 via R5 and R6 both.

“

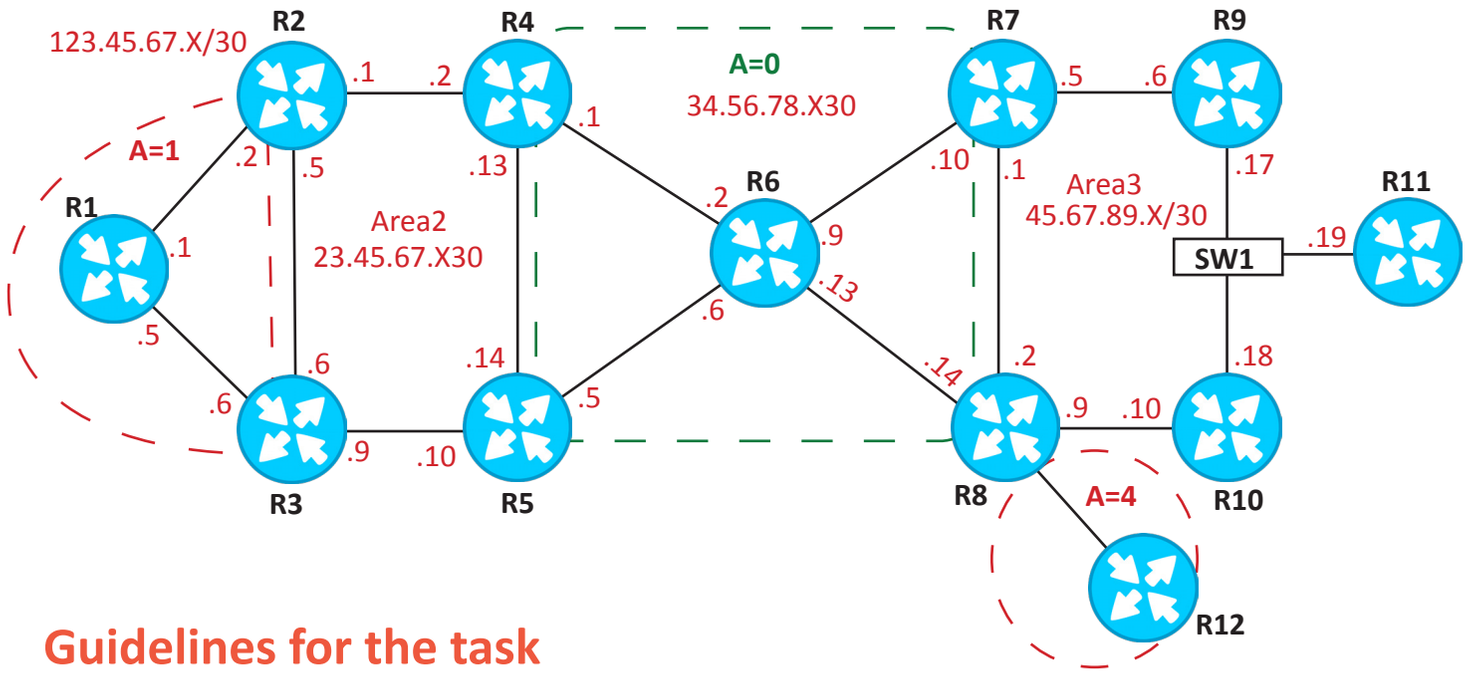
Wow,

You are here finally. 2nd Milestone is also completed successfully.

KEEP YOUR MIND ON THE GO AND GET READY FOR NEXT SET OF CHALLENGES.

”

OSPF Multi Area



Guidelines for the task

- **Task 1** Basic configuration.
- **Task 2** is about virtual link configuration. Four virtual links should be configured between R2-R4, R2-R5, R3-R4 and R3-R5. If we Configure password “?ccie?” then to use “?” as a character press CTRL+V, release and press symbol “?”.
- **Task 3** is a basic route-summary task at ABR, ASBR and path selection using summarization.
- **Task 4** is a default route origination task in which you have to prefer one over the other but without changing OSPF cost (hint use metric-type E1, E2)
- **Task 5** is a redistribution task and a path preference task.
- **Task 6** is an inter-area route-filtering task and external route-filtering task using area filter-list and distribute-list respectively. Remove task 3 before starting with this task.
- **Task 7** is a route-filtering task using stub areas in OSPF. Remove task 6 before starting with this task.
- **Task 8** is about some features of OSPF –
  - We have to suppress the prefix on the segments between routers.
  - In the second part, we have to use domain lookup or DNS lookup for OSPF router id.

Task 1: Basic Configuration

(1) Configure the IP addressing as shown in the diagram on all the routers. Ensure that all the routers have a loopback configured as x.x.x.x where x is the router number.

(2) Now, enable OSPF in the entire network according to the areas defined in the diagram. Configure all the areas except area 0 using the network command in OSPF.

(3) All the routers must have OSPF enabled on their physical interfaces as well as on their loopback interface. Every router's loopback must be configured as its router-id manually. OSPF process-id must be 1234.

(4) All the routers must have the dead interval configured as 1 second and hello interval configured as 250 ms for faster convergence.

(5) All the routers must not install more than 6 equal cost routes.

(6) Routers must not perform the dr and bdr election on the point-to-point ethernet segments.

(7) Cost of every ethernet interface must be 100. You are not allowed to use "IP OSPF cost" command under any of the interface.

Task 2: Virtual-Links and Authentication

(1) In the above diagram, configure the virtual links as many as possible.

(2) In the above configuration, authenticate all the virtual links using type-2 authentication in OSPF with password “NETWORKBULLS?”.
Note: Parenthesis (“) not included in password.

Task 3: OSPF Route-Summarization

(A) For Inter-area Routes

(1) Configure Loopbacks 2.1.1.1-6.1/32 on router 2 and loopbacks 10.1.1.1-6.1/32 on router 10. Advertise R2 loopbacks in area 2 and R10 loopbacks in area3.

(2) Configure network summarization in such a way that when we trace-route from R6 to the loopbacks of R2 the trace must go via R5.

(3) Configure network summarization in such a way that when we trace-route from R6 to the loopbacks of R10 it must always go via R7.

Note:- Do not change the interface cost to do 2nd and 3rd part of task A.

(B) For External Routes

(1) Create loopbacks 1.1.1.1/32 to 1.1.6.1/32 on router R1 and loopbacks 11.1.1.1/32 to 11.16.1/32 on R11 and redistribute them in OSPF without advertising these loopbacks in any other routing protocol with metric type2 and metric value 10 and also make sure only five out of 6 loopbacks get redistributed in OSPF.

(2) Now R6 must receive the summary of loopbacks of R1 as a best route via R4 & R5 and summary of R11 loopbacks as best route via R7 and R8.

Task 4: Default-Route Origination In OSPF

(1) Consider R4 and R7 as the edge routers and originate the default route from R4 and R7 both.

(2) All the routers must consider R4 default route as best route in their routing tables. To accomplish this task do not change any physical interface cost. The routers that will originate the default route must have the default route installed in their RIB.

Task 5: OSPF External Type-1 and Type-2 Routes

(1) Configure the loopback 1.2.3.4 on the routers R4, R5, R7, and R8 and redistribute this loopback only into OSPF with metric type-2 in such a way that all the routers (except R4, R5 and R8) must prefer that route only via R7.

(2) Configure a loopback 4.3.2.1 on the router R2, R3, R9 and R10 and redistribute this loopback into OSPF with metric type-1 on all the routers in such a way that all the routers (except R3, R2, R10) must prefer that route-via R9 only.

Task 6: Route-Filtering

(A) Using Area Filter-Lists

(1) Loopbacks of R2 in area 2 must be received in area 0 and area 4 but area 1 & area 3 must not receive them.

(2) Similarly, the loopbacks of R10 in area 3 must only be received by area 0 and area 4 but other areas must not receive them.

(A) Using Distribute-List

(1) R1 must only receive the odd loopbacks of R11 and R11 should only receive the even loopbacks of R1. However, R6 must receive all the odd as well as even loopbacks of both R1 and R11.

Task 7 : Route - Filtering using Stub Areas (Remove the previous filtering task to do this one)

1. Create loopbacks 12.1.1.1-6.1/32 on R12 and advertise them into OSPF. area 4 has only one exit point out of area. So make sure it must not receive any of the routes from other areas and routes injected by redistribution in OSPF instead it must receive a default-route only but other areas must receive the routes originated in area 4.
2. Configure area 3 in such a way that it must receive all the inter-area routes but it must not receive any of the external routes. However, other areas must receive the routes that are redistributed in area 3.

Verification - After configuration when we trace route to the loopbacks of R1 sourcing the loopbacks of R11 that are redistributed in OSPF, they must go via R7 as the primary path but if R7 fails it should go via R8. Verify backup by disabling the interfaces of R7 in area 3.

Task 8 : Some Features of OSPF (Remove all the filtering tasks before)

1. Configure the network in such a way that all the routers must have only loopback routes installed in their routing table. None of the routers should have the routes of transit segments installed in their routing tables.
2. Configure router R6 in such a way that the database of all the routers must be installed using their names instead of router-ids.

For eg.- 123.1.1.1 must be shown as ROUTER1 when we run ‘sh ip OSPF database command’.

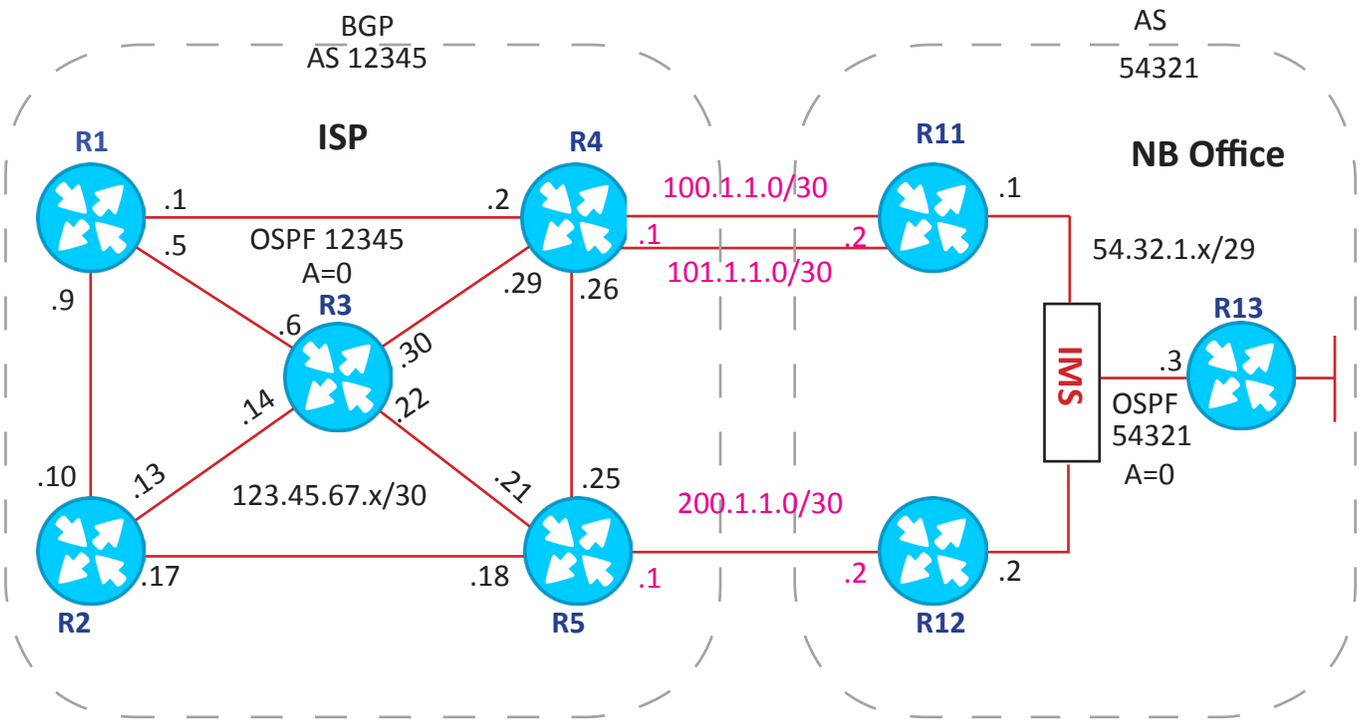
“

Force your heart,
mind and soul to serve your turn until you are done.

YOU ARE JUST FEW MORE CHALLENGES AWAY FROM THE FINISH LINE, GIVE YOUR BEST SHOT!!

”

BGP



Guideline for the task

- **Task 1** is IP addressing and IGP configuration task.
- **Task 2, 3 and 4** are the basic BGP configuration tasks.
- **Task 5** is a route aggregation task. In this task the summary must be originated with different origin code. To complete this task you can use the attribute-map after aggregate command, you can also do it in other ways as well.
- **Task 6** is a default route origination task in which the default route must be originated as per neighbor. (use per neighbor default-originate command)
- **Task 7** is a BGP routing policy task using BGP path attributes. Remove the peer-group in AS 12345 before starting this task and configure full mesh iBGP peering in AS 12345. Before starting this task remove the configuration of task 5.
- **Task 8** remove the configuration of task 7 before starting with this task.
- **Task 9** remove the configuration of Task 8 before starting this task.

Task 1: Basic IGP Configuration

(1) Configure IP addressing in AS 12345 as shown in the diagram. Configure loopback 123.x.x.x on all the routers in BGP AS 12345 where x is the router number.

(2) Configure IP Addressing as shown in the diagram in AS 54321. Configure loopback 54.x.x.x on all the routers where x is the router number.

(3) Configure OSPF in BGP AS 12345. OSPF process id should be 12345 and don't use network command to configure OSPF. Every router's loopback must be configured as its router-id manually and must be seen as an OSPF internal route by all the other routers in the AS.

(4) Configure OSPF in BGP AS 54321. OSPF process id should be 54321 and loopback on the router must be configured as its router-id. Use any method to configure OSPF in this AS.

(5) Verify the IGP configuration all the routers must receive all the routes in their respective BGP AS.

Task 2 : BGP Configuration in AS 12345 (ISP)

(1) Configure BGP in AS 12345/. All the routers must run BGP in AS 12345 and all the routers must form the BGP sessions sourced from their loopbacks and destined to the other router loopbacks.

(2) All the routers in AS 12345 must form the full mesh of iBGP and manage all the sessions using peer-group name IBGP

Task 3 : BGP Configuration in AS 54321 (NB Office)

(1) Configure an IBGP session between R11 and R12 using their loopback addresses. R13 must not run BGP at all.

Task 4 : EBGP Configuration Between AS 12345 and AS 54321

(1) Configure EBGP session between R4 and R11 using their loopback addresses; don't run any IGP between them

(2) Configure the EBGP session between R5 and R12 using their physical interface addresses.

Task 5 : Route-Aggregation in BGP

(1) Create loopbacks (1.1.1.1/32- 1.1.6.1/32) on R1, (2.1.1.1/32-2.1.6.1/32) on R2 and (13.1.1.1/32-13.1.6.1/32) on R13.

(2) Now, advertise the loopbacks of R1 and R2 in OSPF.

(3) Now, on R4 and R5 aggregate the loopbacks of R1 1.1.0.0/16 as a summary-only. R4 must originate it with the origin code incomplete and R5 must originate it with the origin code IGP.

(4) Also generate an aggregate of R2 loopbacks 2.1.0.0/16 as summary-only. R4 must originate it with the origin code IGP and R5 must originate it with the origin code incomplete.

Task 6 : Default Route Origination

(1) R4 and R5 must give a default route via BGP to their corresponding EBGP neighbors. Both of them must originate the default route but they must not have the default route in their routing table.

(2) Now, that R11 and R12 must send this default route to R13, and R13 must prefer R11's default route over the R12's.

Task 7 : BGP Routing Policy

(1) USING WEIGHT-

(A) Configure AS 12345 routers R1, R2 and R3 in such a way that to reach any network in AS 54321 they must prefer R4 as the primary exit point.

(B) Configure routers in AS 54321 in such a way that the traffic going to AS 12345 from R13 must primarily exit via R11.

(2) USING LOCAL-PREFERENCE

(A) Make sure the traffic originated sourcing the loopbacks of R1 destined to R13 loopbacks must go out via R5 and return via R4.

(B) Make sure the traffic originated sourcing the loopbacks of R2 destined to R13 loopbacks must go out via R4 and return via R5.

(C) Make sure the traffic originated sourcing the loopbacks of R13 destined to R1 loopbacks must go out via R11 and return via R12

(D) Make sure the traffic originated sourcing the loopbacks of R13 destined to R2 loopbacks must go out via R12 and return via R11.

Note- Policy for task A and B must be enforced on R4 and R5 only.
Policy for task C and D must be enforced on R11 and R12 only.

(3) USING MED

(A) Make sure the traffic originated sourcing the loopbacks of R13 destined to R1 loopbacks must go out via R11 and return via R12.

(B) Make sure the traffic originated sourcing the loopbacks of R13 destined to R2 loopbacks must go out via R12 and return via R11.

(3) USING ORIGIN CODES

(A) R4 and R5 must originate the loopbacks of R1 into BGP with the origin code incomplete and IGP respectively.

(B) R4 and R5 must originate the loopbacks of R2 into BGP with the origin code IGP and incomplete respectively.

Note- NO REDISTRIBUTION is allowed on any router (R4, R5, R11 and R12)

Task 8 : Route-Filtering

(1) USING ACL

(A) R1 must receive the loopbacks of R13 only via R5 and R2 must receive the loopbacks of R13 only via R4.

(B) R13 must receive the loopbacks of R1 only via R11 and loopbacks of R2 only via R12.

Task 9 : Using Prefix-Lists

Create variable length loopbacks on R1 from network 1.2.0.0/8, 2.2.0.0/8, and 13.2.0.0/8 on router R1, R2 and R13 respectively.

(A) Now make sure R1 must receive all the variable length loopbacks of R13 only via R4 and R2 must receive only via R5.

(B) Make sure R13 must receive all the variable length loopbacks of R1 only via R12 and the loopbacks of R2 only via R11.

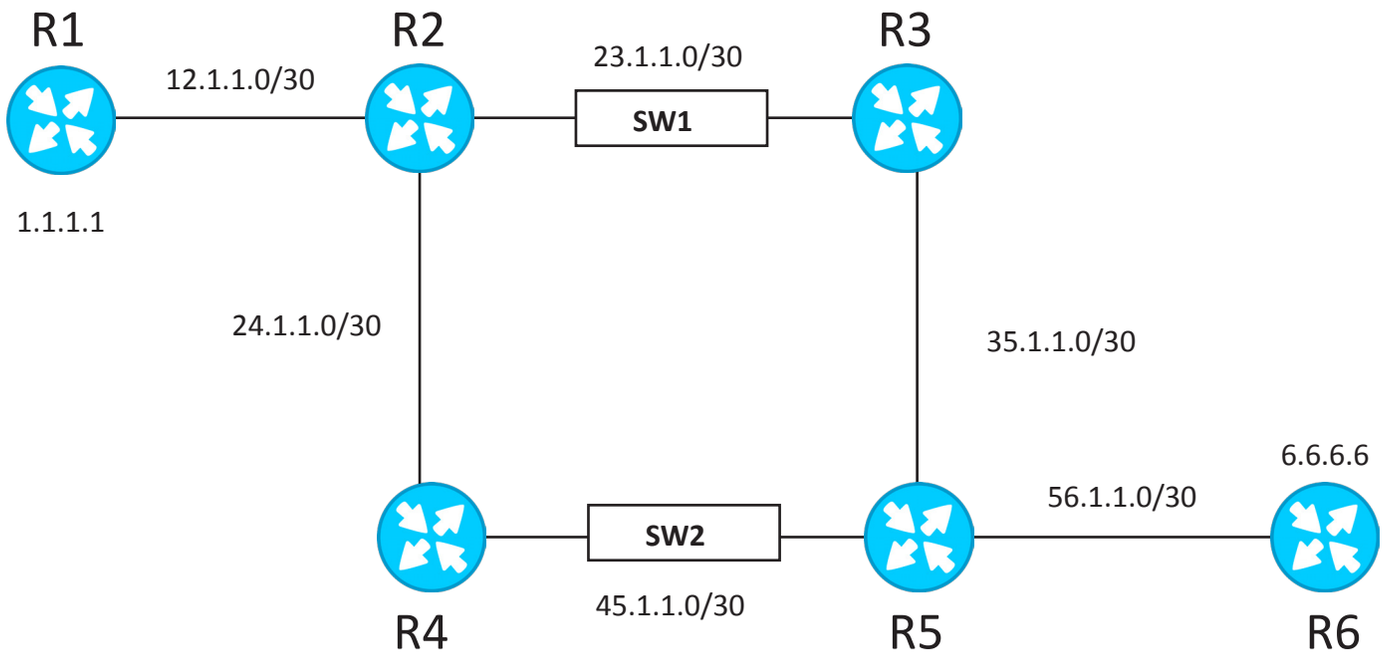
Task 10 : Using Route-Map for Filtering

Add the route-tag “1.1.1.1” on all the loopbacks of R1, route-tag “2.2.2.2” on R2 loopbacks and route-tag “13.13.13.13” on R13 loopbacks.

(A) R1 must receive all the loopbacks with route-tag 13 only via R5 and R2 must receive all the loopbacks with route-tag 13 via R4.

(B) R13 must receive all the networks with route-tag 1.1.1.1 via R11 only and 2.2.2.2 via R12 only.

POLICY-BASED ROUTING AND IP SLA



Policy-Based Routing and IP SLA

(1) Configure the IP addressing as shown in the diagram.

(2) Configure the static routing only for the loopbacks of R1 and R6 on all the routers. Do not add any route for the network assigned on the transit segments.

(3) While configuring static routes, add all the possible routes for the loopback of R1 and R6 towards all available paths with AD value 1 only.

(4) After configuring the static routes make sure that the trace from R1 should go to the loopback of R6 via R3 and R4 as well.

(5) Similarly, the trace from R5 should go to the loopback of R1 via R3 and R4 as well.

Task 1

Now, make sure traffic originated from the R1 loopback to the R6 loopback must go via R3 only. Trace to the loopback of R1 from the loopback of R6 must go via R4.

Verify the above task using the traceroute.

Task 2

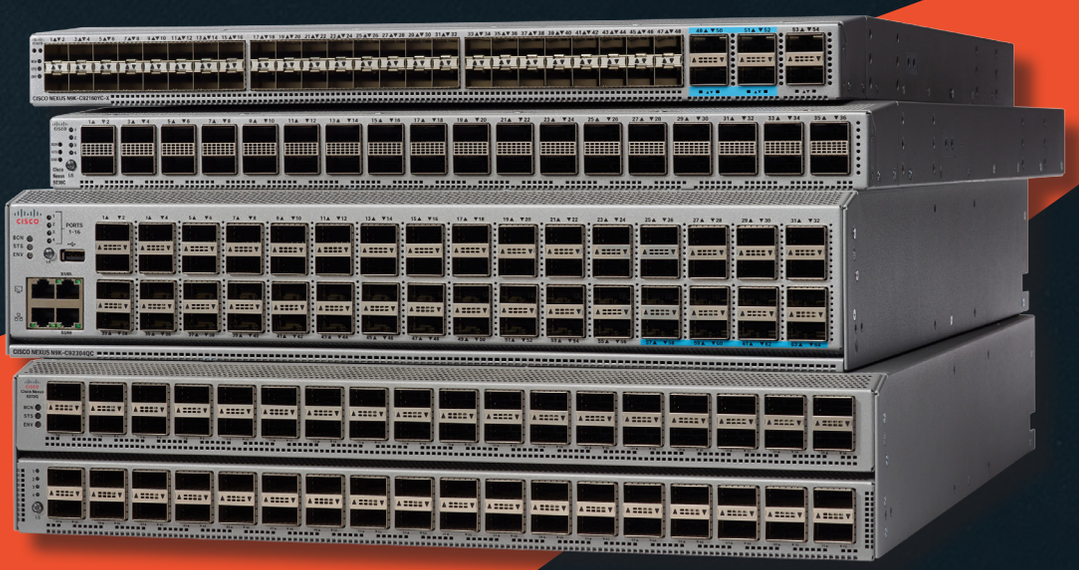
Now, shutdown the interface of R3 that is connected to the switch. Now, the trace from R1 loopback to R6 loopback must go via R4.

Task 3

Now, bring up (no shut) R3 interface and shutdown R4 interface which is connected to the switch. The traffic from R6 to the loopback of R1 must go via R3.

To verify the above task use traceroute.

CCNP



SWITCHING PRACTICAL

Things To Remember

Before Starting With The Practicals Run This Sequence Of Commands To Get The Desired Results

For Routers

1. In Privilege Mode, delete Startup Configuration.
2. In Global Configuration mode, run these commands,

```
line console 0
exec-timeout 0 0
logging synchronous
history size 100
exit
no ip domain-lookup
no logging console
no ip routing
default int fa0/0
default int fa0/1
no cdp run
```

For SW:- (Do it for all switches)

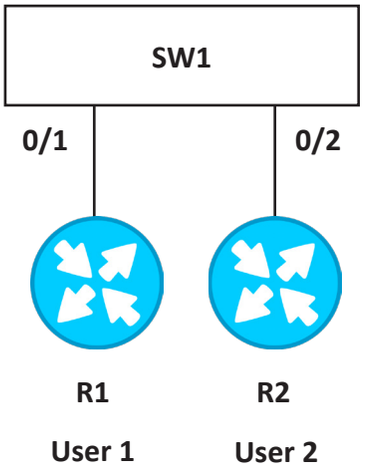
1-In Privilege mode
SWITCH# delete flash:VLAN.dat
Delete filename [VLAN.dat]?
!--- Press Enter
Delete flash:VLAN.dat? [confirm]
!--- Press Enter

SWITCH# write erase
Erasing the nvram file system will remove all files! Continue? [confirm]
Erase of nvram: complete
SWITCH# reload
System configuration has been modified. Save? [yes/no]: n
Proceed with reload? [confirm] y

After Reloading
In Global Configuration Mode run these commands:-

```
line console 0
exec-timeout 0 0
logging synchronous
history size 100
exit
no cdp run
no ip domain-lookup
no logging console
vtp mode transparent
```

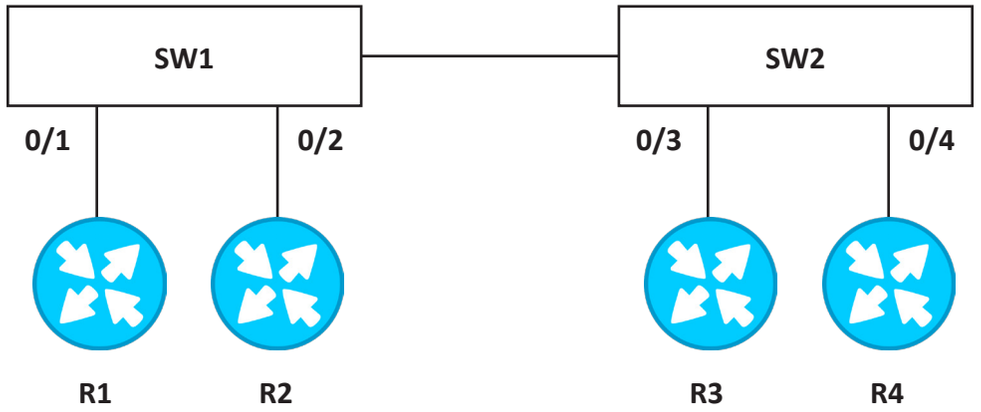
MAC ADDRESS TABLE 1



Configure this physical topology on the rack and check the following things:-

1. Configure hostname for Switch as NBSWITCH.
2. Configure VLAN 9 on the switch.
3. Configure ports 0/1 and 0/2 as access.
4. Both ports must be the member of VLAN 9 and also verify the same.
5. Configure Network for R1 and R2 as 192.168.9.0/30
6. Ping from user1 to user2 should be successful.
7. Check mac address table on NBSWITCH for port 0/1, you must get mac-address learned on that port as dynamic and VLAN should be 9.
8. Do same for port 0/2.
9. Check ARP table on both users and they must be learning each other's mac address.

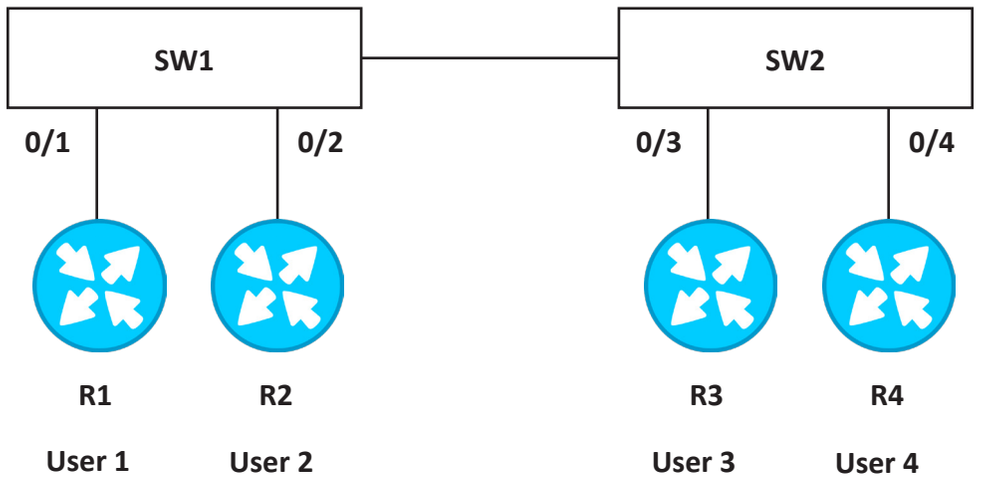
MAC ADDRESS TABLE 2



Configure this physical topology on the rack and check the following things:-

1. Configure hostname for Switch1 as NBSW_GF and Switch2 as NBSW_FF.
2. Configure VLAN 99 on both switches manually.
3. Configure ports connected to users as access and in VLAN 99.
4. Configure network for users as 192.168.99.0/29.
5. All users must be able to communicate with each other.
   (You are not allowed to configure trunk)
6. Check mac address table for port 0/1 and 0/2 on SW1, they should be learning mac-address of user1 and user2 respectively.
7. Check mac address table for port 0/3 and 0/4 on SW2, they should be learning mac-address of user3 and user4 respectively.
8. Check mac address table for port 0/21 on SW1 and SW2. Verify that SW1 is learning the mac address of users connected to SW2 and vice versa.
9. Make sure switches should not keep mac addresses for VLAN 99 for more than 100 sec, if not used.
10. Verify how many more mac address this switch can learn.

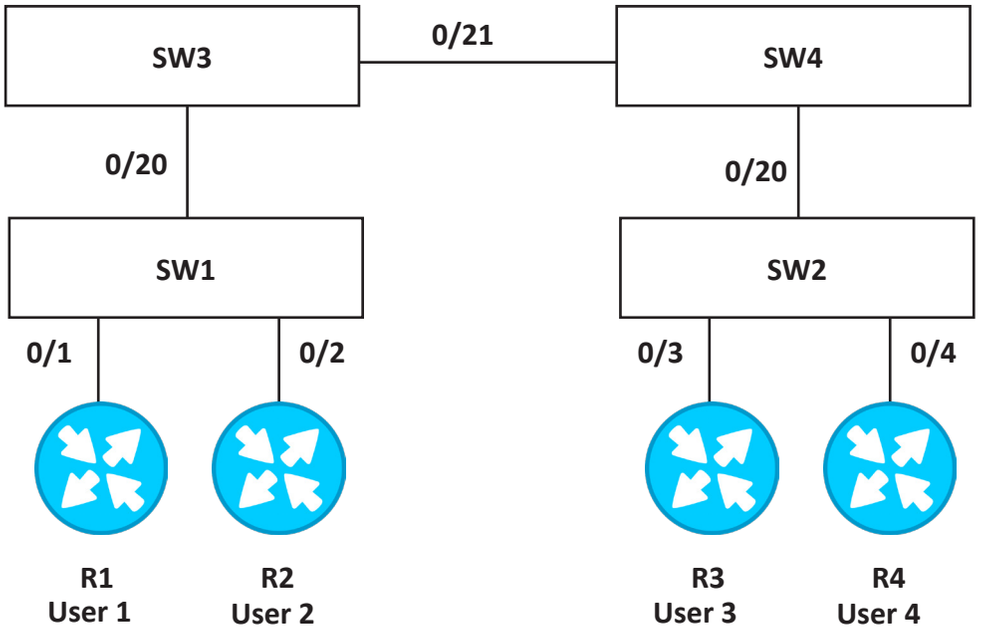
MAC ADDRESS TABLE 3



Configure this physical topology on the rack and check the following things:-

1. Configure hostname for Switch1 as NBSW_GF and Switch2 as NBSW_FF.
2. Configure VLAN 99 on both switches manually.
3. Configured ports connected to users must transition to forwarding state and act as access. (Use a single command to do this)
4. Configure network for users as 192.168.99.0/29.
5. All users must be able to communicate with each other.
   (You are not allowed to configure trunk)
6. Switches (SW1 and SW2) must learn MAC addresses of users statically not dynamically.
7. Make sure when you verify MAC address table on SW1 and SW2, all user MAC addresses should be present in table as static.
8. After how long static entries will age out?

VLAN + DTP 1



Configure this physical topology on the rack and check the following things:

1. Configure hostname on switches as follows:

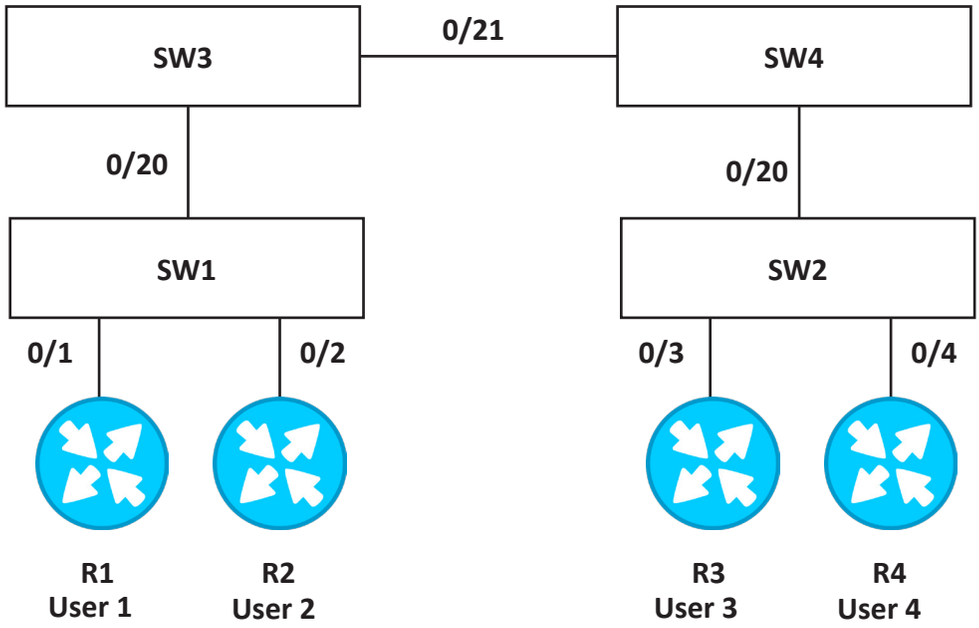
   SW-NB_FF_MGMT
   SW-NB_FF_RACK
   SW3-NB_GF_PRIMARY
   SW4-NBGF_SECONDARY

2. Create VLAN 99.199 on all switches manually
3. Verify that all VLAN info is saved in VLAN.dat file present in flash.
4. Configure port 0/1, 0/3 as access as well as in VLAN 99 and ports 0/2, 0/4 as access as well as in VLAN 199.
5. Configure link between SW1 and SW3 as static trunk and make sure that this link is using open standard encapsulation. Do the same for link between SW3 and SW4, SW4 and SW2.

   Also verify trunk links.

6. Use Network 192.168.99.0/30 for VLAN 99 and 192.168.199.0/30 for VLAN 199.
7. Ping from user1 to user3 and user2 to user4
8. Check MAC address table of SW3 for port 0/20. It should be learning MAC address for VLAN 99 and VLAN 199.

VLAN + DTP 2



Configure this physical topology on the rack and check the following things:

1. Configure hostname on switches as follows:

   SW-NB_FF_MGMT
   SW-NB_FF_RACK
   SW3-NB_GF_PRIMARY
   SW4-NBGF_SECONDARY

2. Create VLAN 99.199 on all switches manually
3. Verify that all VLAN info is saved in VLAN.dat file present in flash.
4. Configure port 0/1, 0/3 as access as well as in VLAN 99 and ports 0/2, 0/4 as access as well as in VLAN 199.
5. Configure trunk according to the requirement:

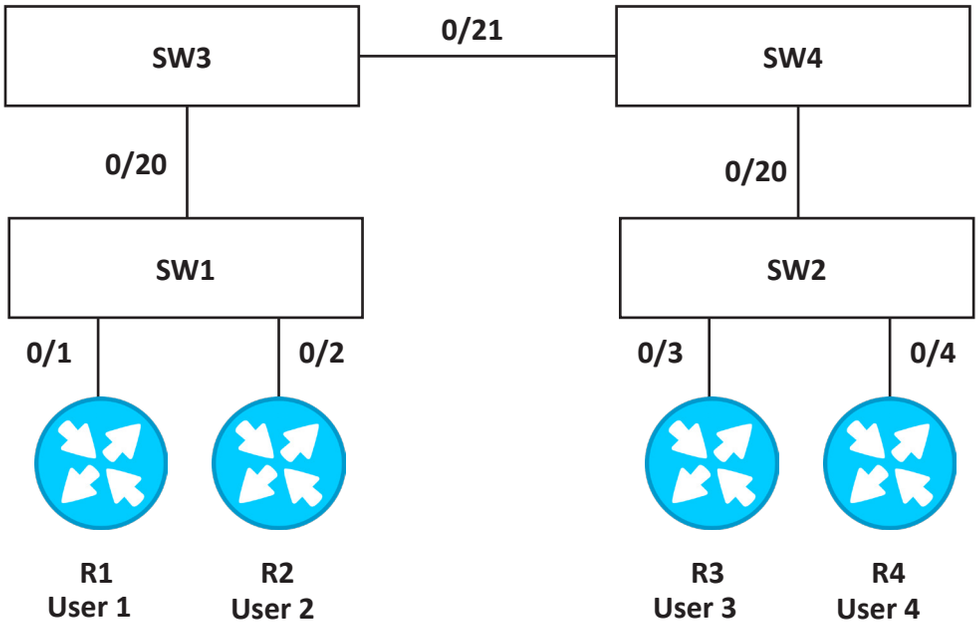
	Encapsulation	Static/Dynamic
SW1-SW3	ISL	STATIC
SW3-SW4	DOT1Q	DYNAMIC (SW3 should initiate)
SW4-SW2	ISL	DYNAMIC (SW4 should initiate)

6. Ping from user1 to user3 and from user2 to user4 should be successful.

   Use same networks as used for previous task

7. Verify MAC table for trunk link, they should learn MAC address for VLAN 99 and VLAN 199.

VLAN + DTP 3



Configure this physical topology on the rack and check the following things:

1. Configure hostname similar to the previous one.
2. Configure VLAN 99 and VLAN 199 on all switches manually.
3. Create VLAN 99.199 on all switches manually
4. Make sure all ports connected to the users must act as access and should move to forwarding state as they come up. (Use a single command to do it)
5. Configure ports 0/1, 0/3 in VLAN 99 and port 0/2, 0/4 in VLAN 199.
6. Configure trunk between switches according to the following requirements:-

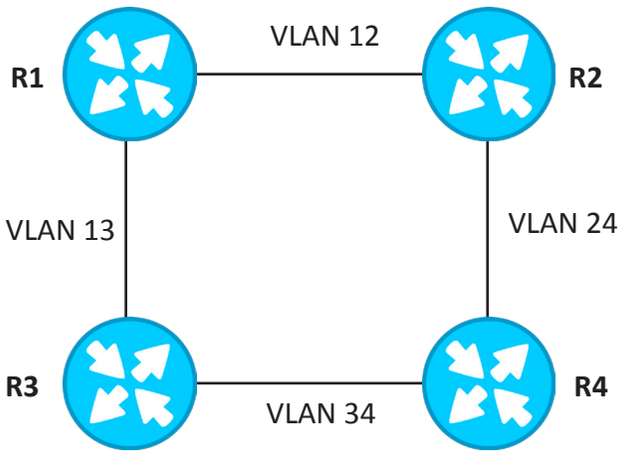
	Encapsulation	Static/Dynamic
SW1-SW3	DOT1Q	STATIC
SW3-SW4	DOT1Q	DYNAMIC (None of the switch negotiate)
SW2-SW4	DOT1Q	DYNAMIC (SW2 should initiate)

   Also verify trunk links.
7. Use same network as given in the previous tasks.
8. User1 should ping User3 and User2 should ping User4.
9. Make sure that none of the trunk links should add tag for VLAN 99.

   Ping from User1 to User3 should be unsuccessful.

VLAN + DTP 4

All of you know the physical topology of Rack, using that topology make this logical topology. Routers should ping directly connected interfaces.



Network used:

VLAN12 – 192.168.12.0/24

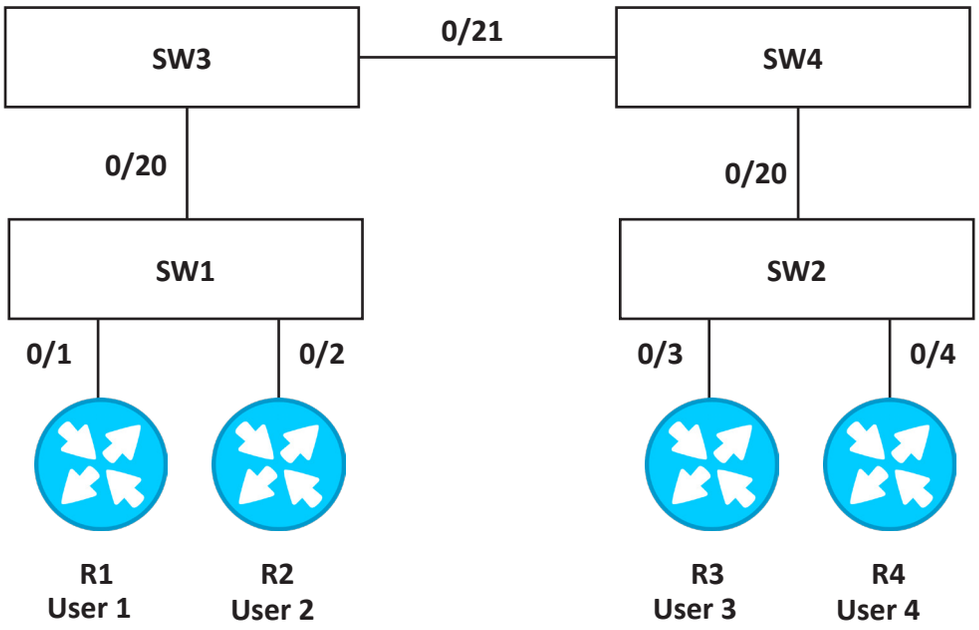
VLAN13 – 192.168.13.0/24

VLAN24 – 192.168.24.0/24

VLAN34 – 192.168.34.0/24

R1 should ping R2 and other routers should do the same.

VTP 1



Configure this physical topology on the rack and check the following things:

1. Configure hostname similar to the previous one.
2. Configure trunk links as follows:-

	Encapsulation	Static/Dynamic
SW1-SW3	Dot1q	STATIC
SW3-SW4	ISL	STATIC
SW4-SW2	Dot1q	STATIC

   None of the switches should negotiate trunk.

   Also verify trunk links.

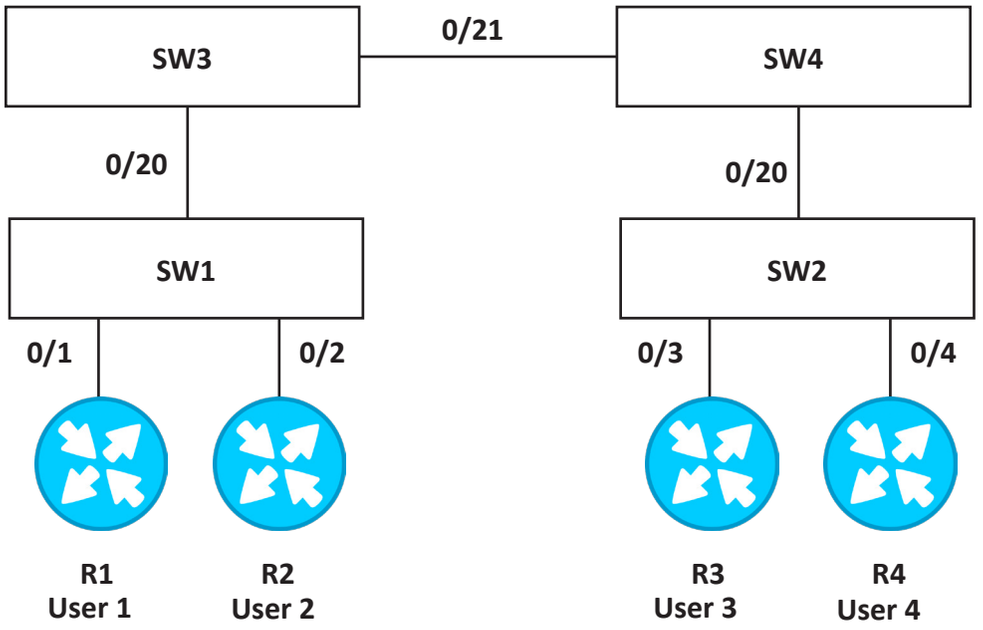
3. Configure SW3 in such a way that it is responsible for distributing all VLAN information throughout L2 SW network.
4. SW1, SW4, SW2 are not allowed to distribute VLAN information, but they must get updated from the SW3.
5. Use Domain NB_L2.com and password cisco123?123.
6. Use VTP version 2.
7. Create some VLANs on SW3 like 99, 199, they must be propagated throughout on all switches.

VLAN 99- name SALES
VLAN 199- name MARKETING

Verify above task.

8. Configure ports connected to users as access as well as in VLAN 99 and 199 respectively.
9. User of same VLAN should be able to communicate with each other.
10. VLAN 99 name is changed from SALES to NB_SALES. Verify this change in your network.

VTP 2



Configure this physical topology on the rack and check the following things:

1. Configure hostname similar to the previous tasks
2. Configure trunk links as follows:-

	Encapsulation	Static/Dynamic
SW1-SW3	Dot1q	STATIC
SW3-SW4	ISL	STATIC
SW4-SW2	Dot1q	STATIC

   None of the switches should negotiate trunk.

   Also verify trunk links.

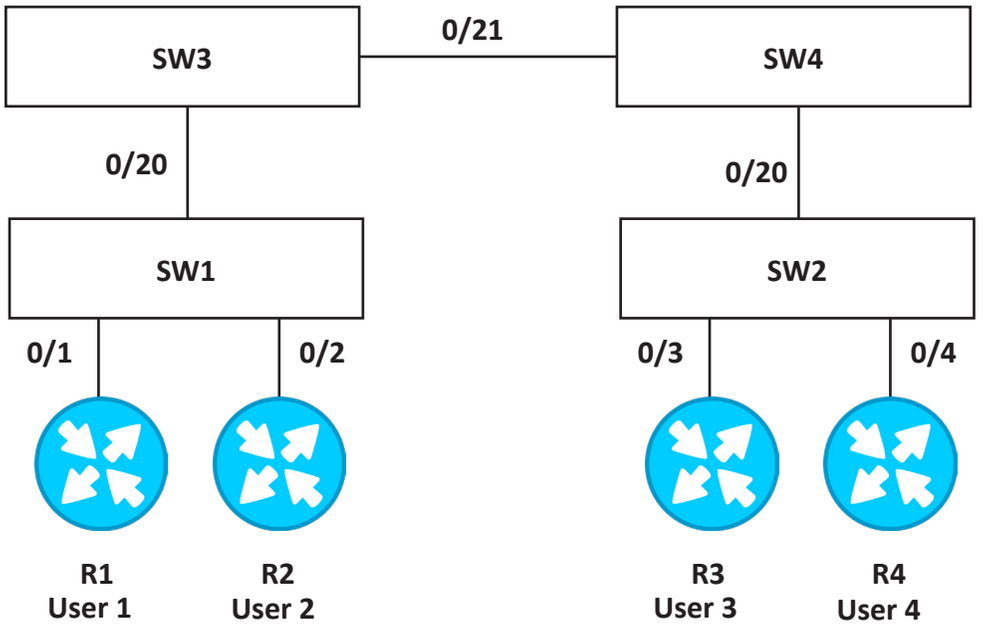
3. Configure Switches as per the requirements:-

   VTP Domain-Networkbulls.com
   SW1 should distribute VLAN information throughout L2 Network.
   SW4 must not increment CR No. in any case.
   SW3 and SW2 should act as a client.

4. SW1 must forward update with its identity as 143.1.1.1.5.
   In domain Networkbulls.com use password cisco123?123.

5. Create VLAN on server:-
   VLAN10- SALES
   VLAN 20-HR
6. All Switches must have VLAN 10 and 20 except SW4.
7. Configure User1 and User3 in VLAN 10 and User2 and User4 in VLAN 20.
8. User connected ports should not negotiate trunk.
9. Configure VTP version 2.
10. Now create VLAN100-Dummy VLAN on Server.
    All Switches except SW4 must get these VLANs.
    Transparent SW should forward VLAN info without checking version.
11. Make sure your VTP domain is secure with plain text password cisco123?123.
12. Use Network 192.168.10.0/28 for VLAN 10 and 192.168.20.0/28 for VLAN 20.
13. Ping must be successful from user1 to user3 and user2 to user4.

VTP 3



Configure this physical topology on the rack and check the following things:

1. Configure hostname similar to the previous one.
2. Configure trunk links as follows:-

	Encapsulation	Static/Dynamic
SW1-SW3	Dot1q	STATIC
SW3-SW4	ISL	STATIC
SW4-SW2	Dot1q	STATIC

   None of the switches should negotiate trunk.

   Verify trunk links.

3. Configure Switches as per the requirements:-
   VTP Domain - Networkbulls.com
   SW1 should distribute VLAN information throughout L2 Network.
   SW3, SW4 and SW2 should act as a client.
4. SW1 must forward update with its identity as 130.1.1.135.
5. Create VLAN on server:-
   VLAN10- SALES
   VLAN 20-HR

6. Verify CR NO. on all switches, it must be identical.
7. Configure User1 and User3 in VLAN 10 and User2 and User4 in VLAN 20. Use Network 192.168.10.0/28 for VLAN 10 and 192.168.20.0/28 for VLAN 20.
8. Users must be able to communicate with each other.
9. Now SW2 is facing some hardware issues so you have to replace SW2 with a new switch (you cannot perform such tasks in lab).

   You should follow these instructions to understand the issue.

   Shutdown port 0/20 on SW2.

   Create some new VLANs on SW2 like VLAN 501, 502, 503, 504, 505, 506 such that the configuration revision number of SW2 is higher than the configuration revision number of the network.

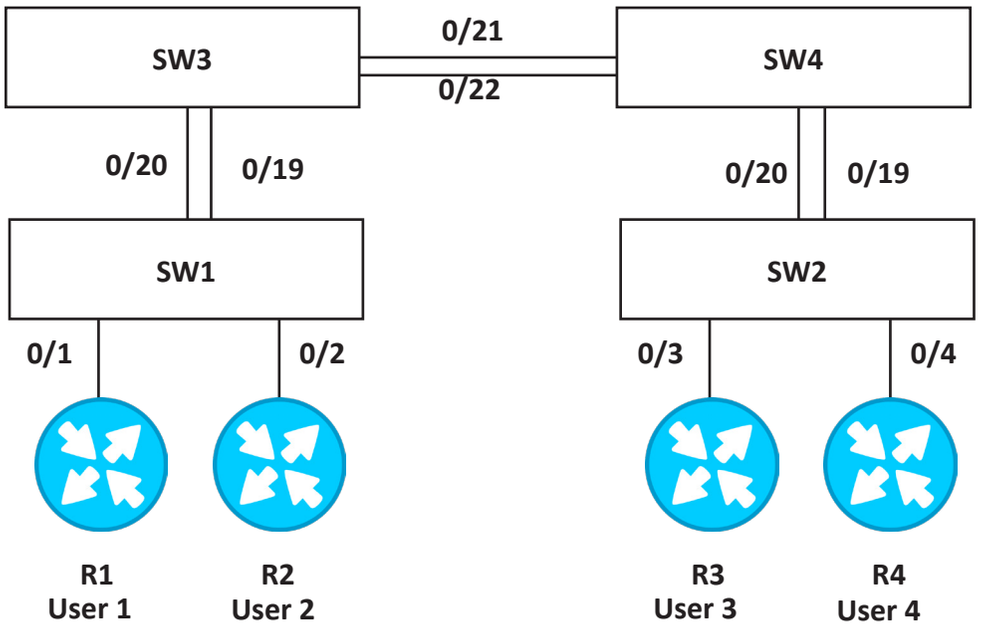
   Now, add SW2 back to the network and verify that it update all other switches because of its higher CR No.

   Now, ping between users and it should be unsuccessful.

   Find the reason?

   Do this task again but this time network should not be impacted, take measures.
10. Users must be able to communicate.
    Adding a new SW should not impact running network.

ETHERCHANNEL



Configure this physical topology on the rack and check the following things:

1. Configure hostname as same as of previous one.
2. Configure ether channel according to the following requirements –

Switches	Type	PO
SW1-SW3	Static	Static
SW3-SW4	DYNAMIC (SW3 should initiate)	34(PaGP)
SW4-SW2	DYNAMIC (SW4 should initiate)	24(LACP)

3. Configure trunk links as follows

	Encapsulation	Static/Dynamic
SW1-SW3	ISL	Static
SW3-SW4	DOT1Q	Static
SW4-SW2	ISL	Static

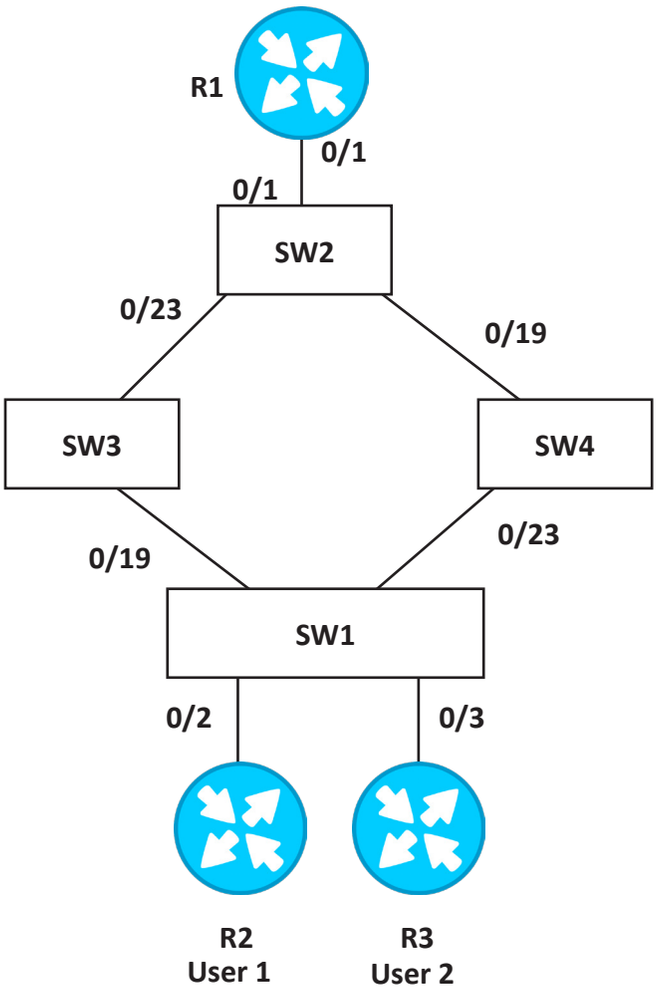
None of the switches should negotiate trunk.
Make sure you are not running any command for trunking on physical interfaces.

4. Now configure VTP in domain networkbulls.com in such a way that all Switches must not relay any VLAN information they receive.

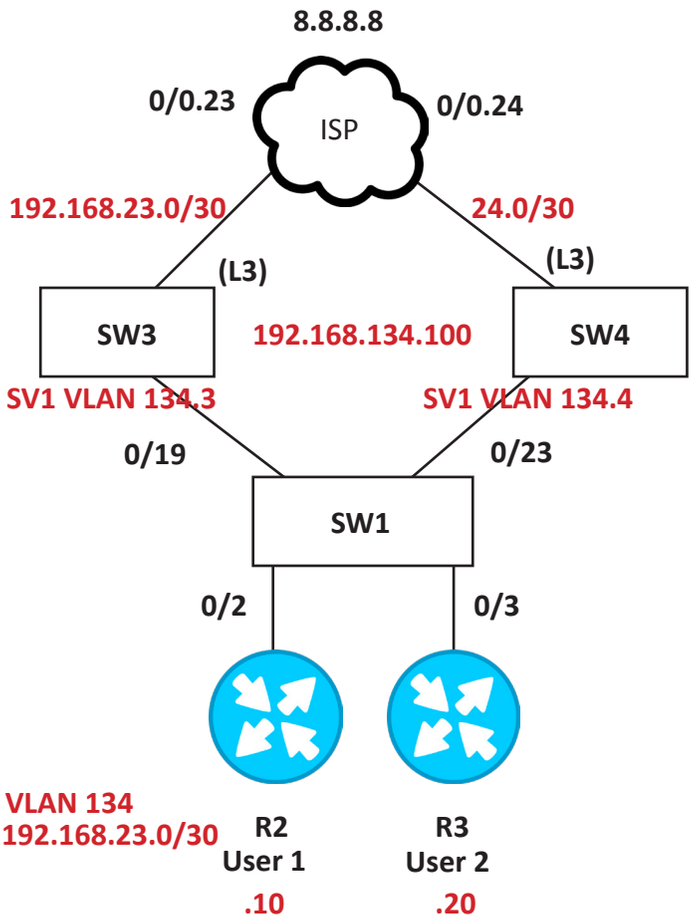
5. Create VLAN 10 and 20 in networkbulls.com domain.
6. Configure ports connected to users as access and user 1 and 3 should be member of VLAN 10 and user2 and 4 should be member of VLAN 20.
7. Use Network 192.168.10.0/28 for VLAN 10 and 192.168.20.0/28 for VLAN 20.
8. VLAN 10 users must communicate with each other but VLAN 20 users must not communicate at all.

HSRP

Physical



Logical



Configure this logical topology on the rack and check the following things:

Ports between SW1-SW3 and SW1-SW4 should be trunk.

1. Assign IP addresses according to the networks shown.

   User 2 -192.168.134.10
   User 3-192.168.134.20
   SW3 –SVI VLAN 134-192.168.134.3
   SW4-SVI VLAN 134-192.168.134.4

   User2 and user3 should be member of VLAN 134.

2. Run EIGRP in WAN to provide user access to 8.8.8.8.
3. Configure VLAN interface 134 as passive on both SW3 and SW4 for EIGRP.
4. Configure Cisco propriety first hop redundancy protocol to provide gateway redundancy for users in VLAN 134 using virtual IP shown in topology.
5. SW3 must act as active and SW4 as standby.
6. Switches must send coup and resign message whenever they hear hello with high priority value.
7. Switches must change their role whenever WAN interface goes down. The value of priority to be decremented should be 15.
8. The ICMP traffic generated by end hosts should go out via SW3 towards 8.8.8.8. If SW3 WAN link fails then it must go via SW4.

Load Balancing In Same Scenario

Note - Create one more VLAN 135 on SW3, SW4 and SW1.

Assign user2 in VLAN 134 and User 3 in VLAN 135.

User3 (new IP) 192.168.135.20

Configure SVI VLAN 135 on SW3 and SW4 with IP 192.168.135.3 and 192.168.135.4 respectively.

Use virtual IP 192.168.135.100 for VLAN 135.

1. Make sure SW3 must act as active for VLAN 134 and SW4 should act as active for VLAN 135.
2. Ping from user 3 and user 4 to check the desired results.

MLS

Configure Physical Topology As Shown:-

(1) Create Dot1q trunks across all links existing between switches.
(No SW is allowed to negotiate the trunk)

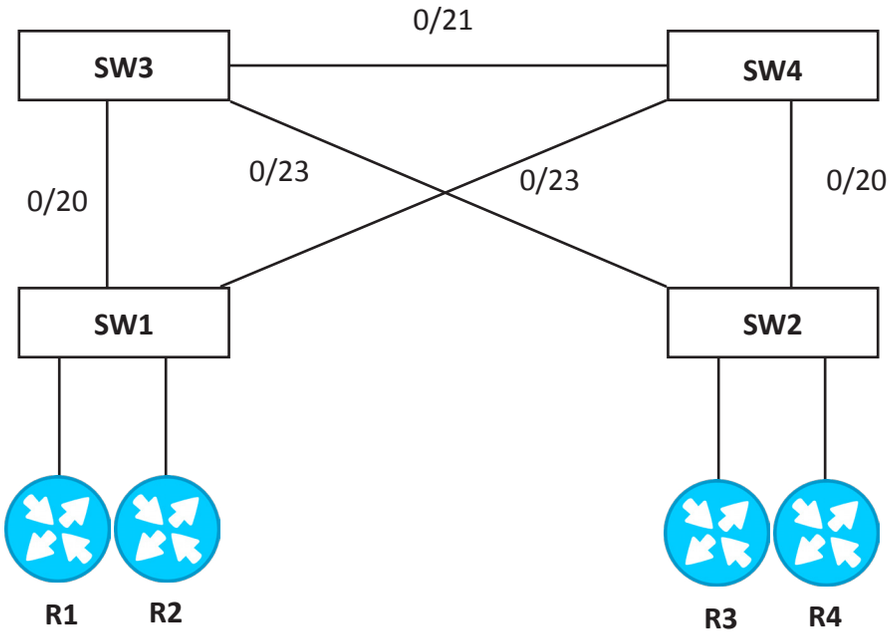
(2) Configure ports connected to users as access.

(3) Create VLAN 123 and 321 manually on both Switches. Configure R1 in VLAN 123 and R2 in VLAN 321.

(4) Use network 192.168.12.0/24 for VLAN 123 and 192.168.13.0/24 for VLAN 321.

(5) Make sure both the VLAN users should communicate using layer 3 logic of switches.

MLS+DHCP



Configure Physical Topology As Shown:-

DTP

1. Create Dot1q trunks across all links existing between switches. (No SW is allowed to negotiate the trunk)
2. Configure ports connected to the users as access.

VTP

Configure VTP according to following requirements:-

1. SW3 is responsible for updating all other Switches with its own VLAN information.
2. Other Switches must get updated from SW3.
3. Use VTP domain networkbulls.com and secure VTP domain using plain text string network bulls.
4. Configure VLAN 123, 321 and verify VTP is working correctly?

VLAN Assignment

1. Configure user1 and user3 in VLAN 123; user2 and user4 in VLAN 321.

Spanning Tree

1. Configure SW3 as RB for VLAN 123 and SW4 as backup.
2. Configure SW4 as RB for VLAN 321 and SW3 as backup.

MLS

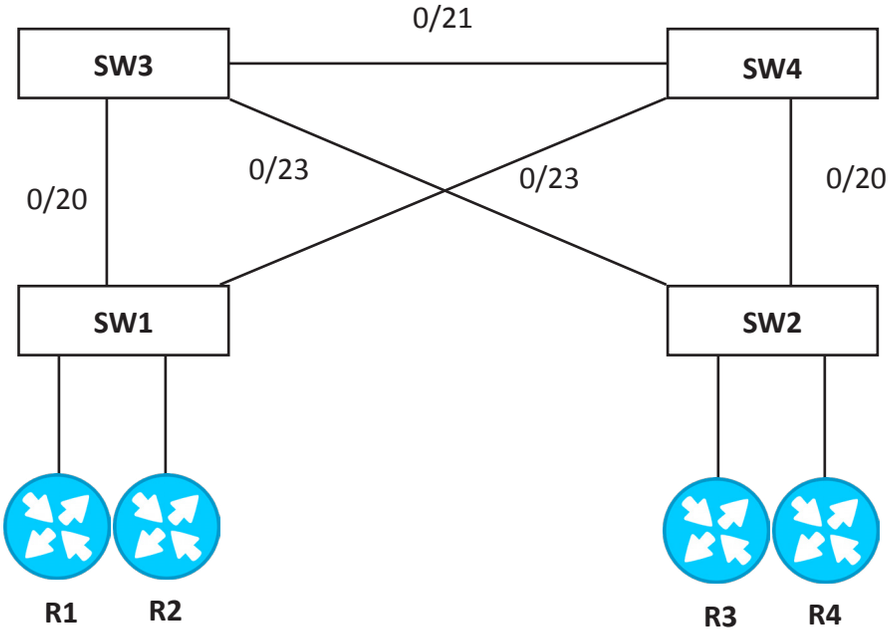
1. Distribution layer switches must perform gateway functionality. (Provide routing)

DHCP

1. Configure R1 as DHCP server for both the VLANs. User R2, R3 and R4 must get IP address from DHCP server.

Use network VLAN 123- 192.168.12.0/24
VLAN 321 -192.168.13.0/24

STP 1



Configure Physical Topology As Shown:-

Shut down all the unused ports and assign them in VLAN 1000.

DTP

1. Create Dot1q trunks across all links existing between switches. (No SW is allowed to negotiate the trunk)
2. Configure ports connected to users as access.

VTP

Configure VTP according to the following requirements:-

1. SW3 is responsible for updating all other Switches with its own VLAN information.
2. Other SW must get updated from SW3.
3. Use VTP domain networkbulls.com and secure VTP domain using plain text string networkbulls.
4. Create VLAN 123 on SW3 and ensure that VTP is working correctly.

VLAN Assignment

1. Configure Users connected to SW1 and SW2 in VLAN 123.
2. Use any network for these users.

Spanning Tree

1. Configure SW3 as root-bridge and SW4 as back up root, in case SW3 goes down. (You are not allowed to change priority manually)
2. Make sure Loop free path exist from SW1 to SW2 via SW3. (Check CAM table to verify the result)

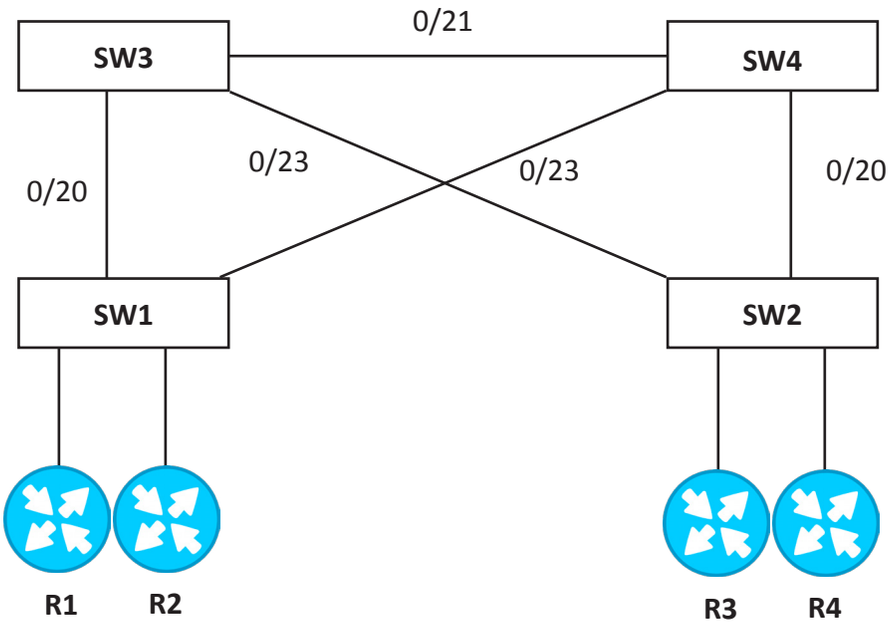
STP (Root Path Manipulation)

3. Make sure traffic from R1 to R3 must flow from SW1--> SW4--> SW3-->SW2

STP (Timers)

4. Configure the root bridge so that switches generate Spanning-Tree hello packets every 3 seconds.
5. When a new port becomes active, it should wait for 20 seconds before transitioning to the forwarding state.
6. If the switches do not receive a configuration message within 10 seconds then they should attempt reconfiguration.
7. Make sure all access ports must move to forwarding state as soon as we connect them to a switch port.

STP 2



Configure Physical Topology As Shown:-

Shut down all the unused ports and assign them in VLAN 1000.

DTP

1. Create Dot1q trunks across all links existing between switches. (No SW is allowed to negotiate the trunk)
2. Configure ports connected to users as access.

VTP

Configure VTP according to the following requirements:-

1. SW3 is responsible for updating all other Switches with its own VLAN information.
2. Other SW must get updated from SW3.
3. Use VTP domain networkbulls.com and secure VTP domain using plain text string network bulls.
4. Create VLAN 123, 321 on SW3 and ensure that VTP is working correctly.

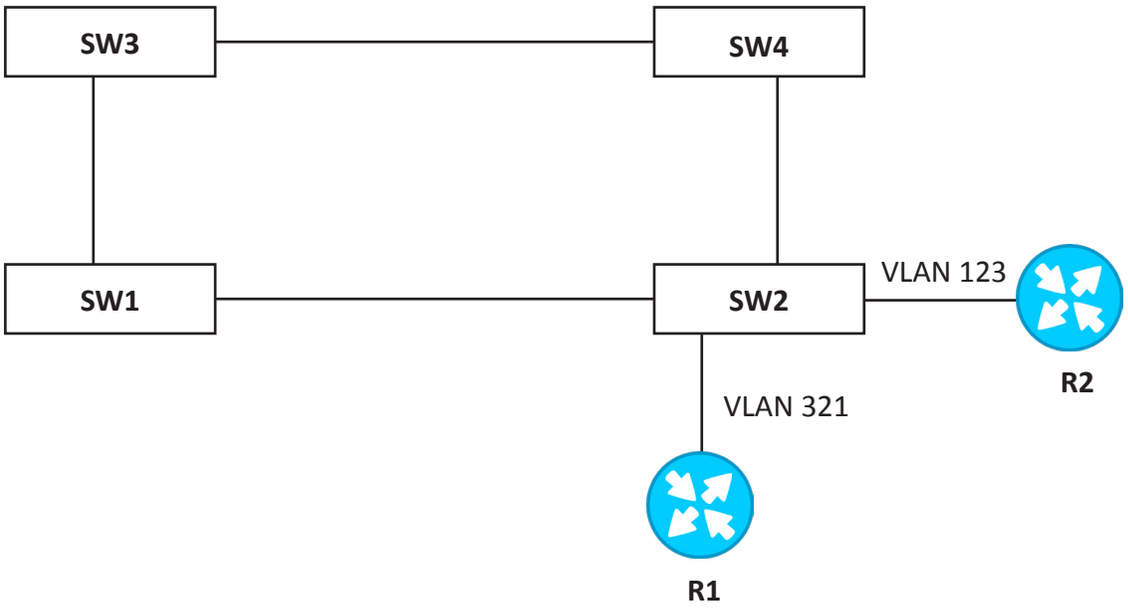
VLAN Assignment

1. Configure user1 and user3 in VLAN 123, user2 and user4 in VLAN 321. (Use any network for these users.)

Spanning Tree

1. Configure SW3 as RB for VLAN 123 and SW4 as backup.
2. Configure SW4 as RB for VLAN 321 and SW3 as backup. (You are not allowed to change priority manually)
3. Make sure loop free path for VLAN 123 should be SW1-SW3-SW2 and for VLAN 321 should be SW2-SW4-SW1. (Load balancing)
4. Now, configure loop free path in such a way that for VLAN 123 tracffic should go via SW1-SW4-SW3-SW2.
5. Link between SW1 and SW4 should not be used to forward traffic for VLAN 321.
6. Make sure all access layer switches must transit block port to new root port in case of root port failure at the same time.

STP 3



Configure Physical Topology As Shown:-

Shut down all the unused ports and assign them in VLAN 1000.

DTP

1. Create Dot1q trunk across all the links existing between switches. (No SW is allowed to negotiate the trunk)
2. Configure ports connected to users as access.

VTP

Configure VTP according to the following requirements:-

1. SW3 is responsible for updating all other Switches with its own VLAN information.
2. Other SW must get updated from SW3.
3. Use VTP domain networkbulls.com and secure VTP domain using plain text string network bulls.
4. Create VLAN 123, 321 on SW3 and ensure VTP is working correctly.

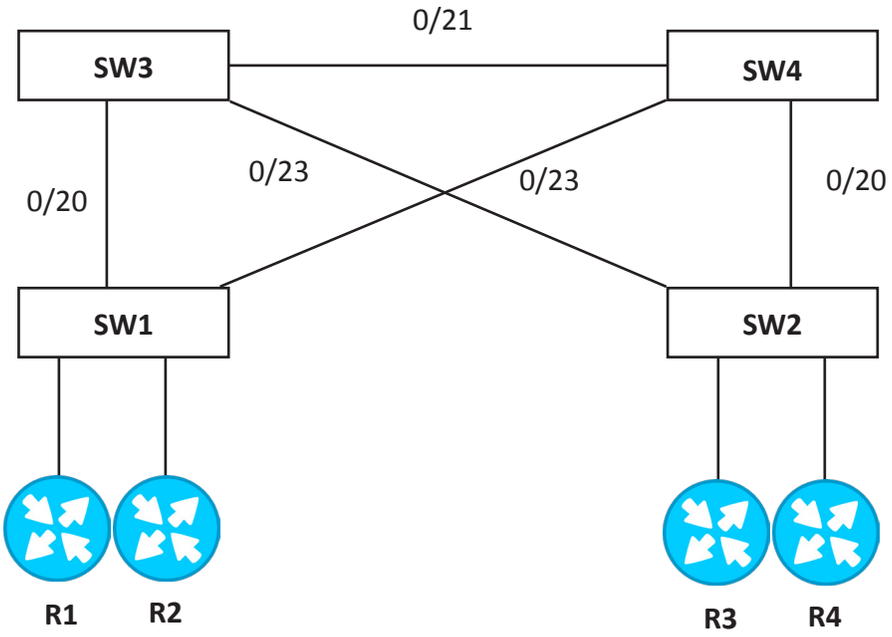
VLAN Assignment

1. Configure user1 in VLAN 123 and user2 in VLAN 321. (use any network).

Spanning Tree

1. Make sure Spanning-tree must immediately delete dynamically learned MAC address entries on a per-port basis upon receiving a topology change.
2. Configure SW3 as root-bridge. (Use any method to accomplish the task)
3. All access ports must transition to forwarding state as they come up. (Use a single command on all access layer switches)
4. All access ports must move to error disable state if they receive any BPDU. (Use a single command to do so)
5. Configure automatic recovery for these ports and recovery interval should be 120 sec.
6. Access layer SW2 (In our case) should not become Root Bridge. In case, if by mistake its priority is lowered it should not have impact on current root.
7. All Switches must not convert non-designated ports to designated ports in case of loss of BPDU's.

STP 4



Configure Physical Topology as shown:-

Shut down all the unused ports and assign them in VLAN 1000.

DTP

1. Create Dot1q trunk across all the links existing between switches. (No SW is allowed to negotiate the trunk)
2. Configure ports connected to users as access.

VTP

Configure VTP according to the following requirements:-

1. SW3 is responsible for updating all other Switches with its own VLAN information.
2. Other SW must get updated from SW3.
3. Use VTP domain networkbulls.com and secure VTP domain using plain text string network bulls.
4. Create VLAN 123 on SW3 and ensure VTP is working correctly.

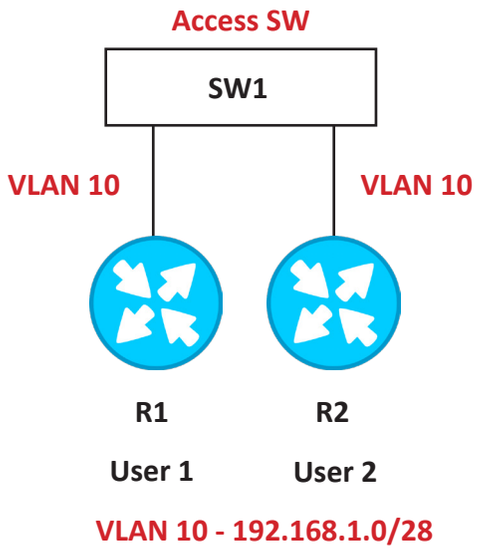
VLAN Assignment

1. Configure user1 and user3 in VLAN 123 and user2 and user4 in VLAN 321. (use any network)

Spanning Tree

1. Make sure you are using manual instance based spanning tree.
2. Configure two instances (1 and 2), VLAN 1 and VLAN 123 should be member of instance1 and VLAN 321 should be the member of instance2.
3. Configure SW3 as RB for instance1 and SW4 as RB for instance2.
4. Make sure two different loop free paths should exist in the topology.

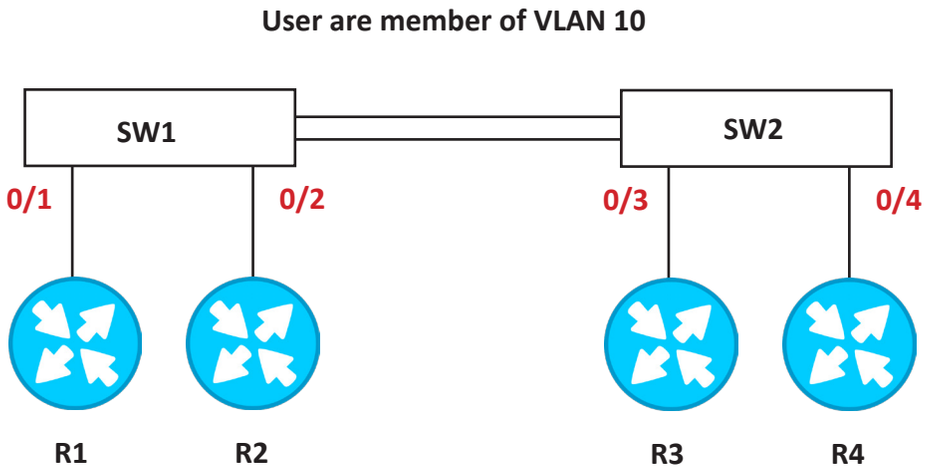
Port Security



Port Security

1. Configure topology as shown.
2. Create VLAN 10 and both users should be member of VLAN 10.
3. Port 0/1 on SW1 should not learn more than one MAC address.
4. It should only learn MAC address of R1 in all cases.
5. Port 0/2 on SW1 should not learn more than two MAC addresses.
6. Both ports should generate log in case of any violation.

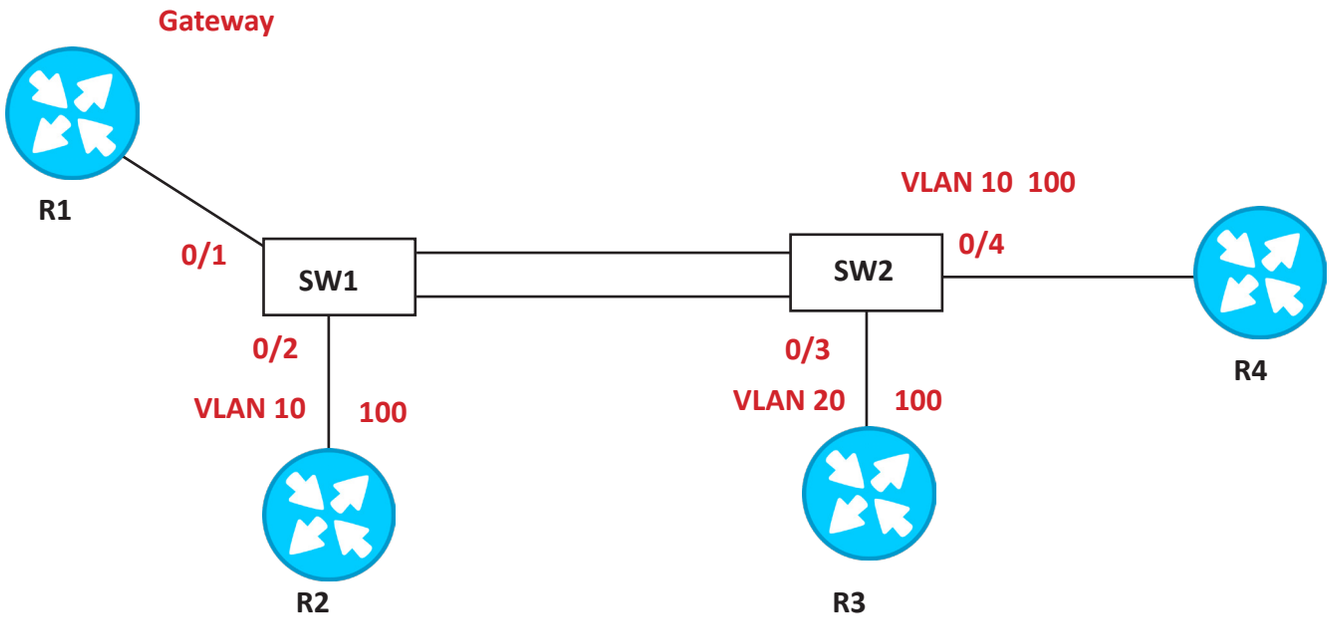
VLAN ACL



VLAN ACL

1. Configure VLAN 10 and all ports should be the member of VLAN 10.
2. Configure dot1q trunks between switches.
3. Configure R3 as HTTP Server.
4. Configure telnet and SSH on R4.
   Username - NB
   Password - networkbulls
5. Make sure user1 (R1) is able to telnet and SSH R4.
6. Make sure user2 (R2) is able to access HTTP Server.
   You are not allowed to create standard ACL or access class for these tasks.
   Use Networks as follows:
   VLAN 10 – 192.168.1.0/29

Private VLAN

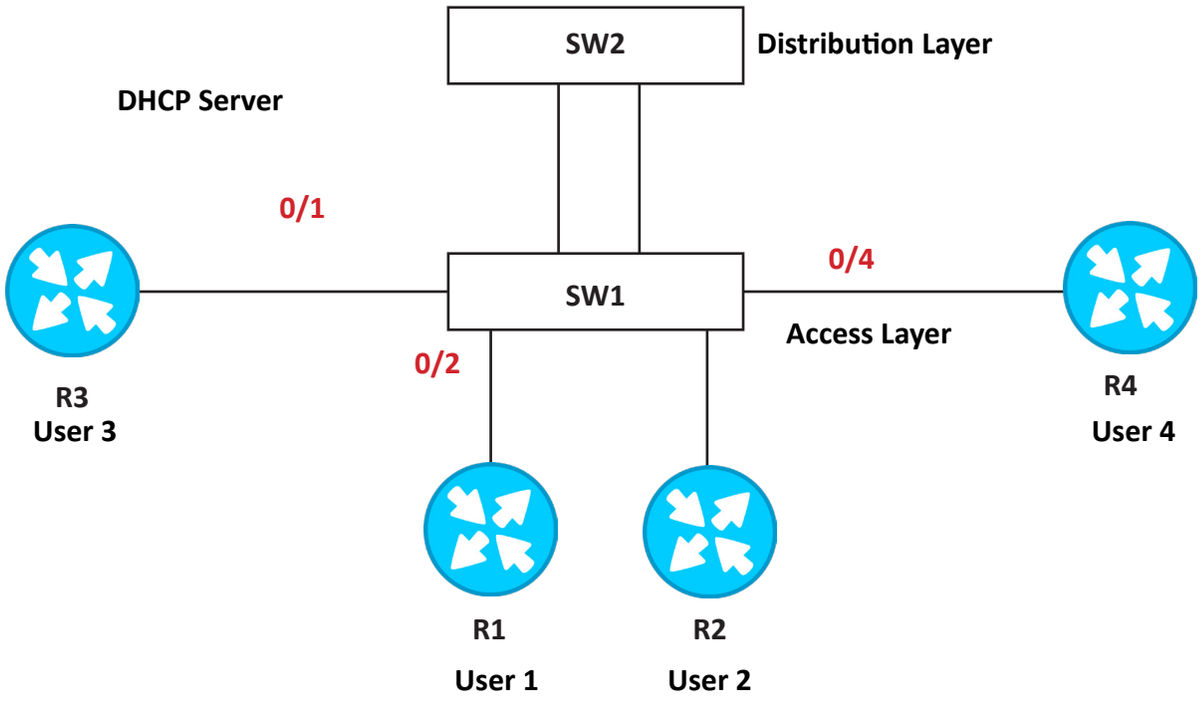


Network to use for VLAN 100 192.168.1.0/24

Configure Topology As Shown:

1. Configure VLAN 100 as primary, VLAN 10 as community and VLAN 20 as isolated.
2. Configure ports 0/1 in such a way that it forwards all secondary VLAN traffic in addition to the primary VLAN traffic.
3. Configure port 0/2, 0/3 and 0/4 as shown in the topology.
4. Make sure that the users in same community can communicate with each other.
5. only User3 is allowed to reach gateway.
6. Configure port 0/4 in normal VLAN 10 and check it is still communicating with community VLAN 10 user or not.

DHCP Snooping



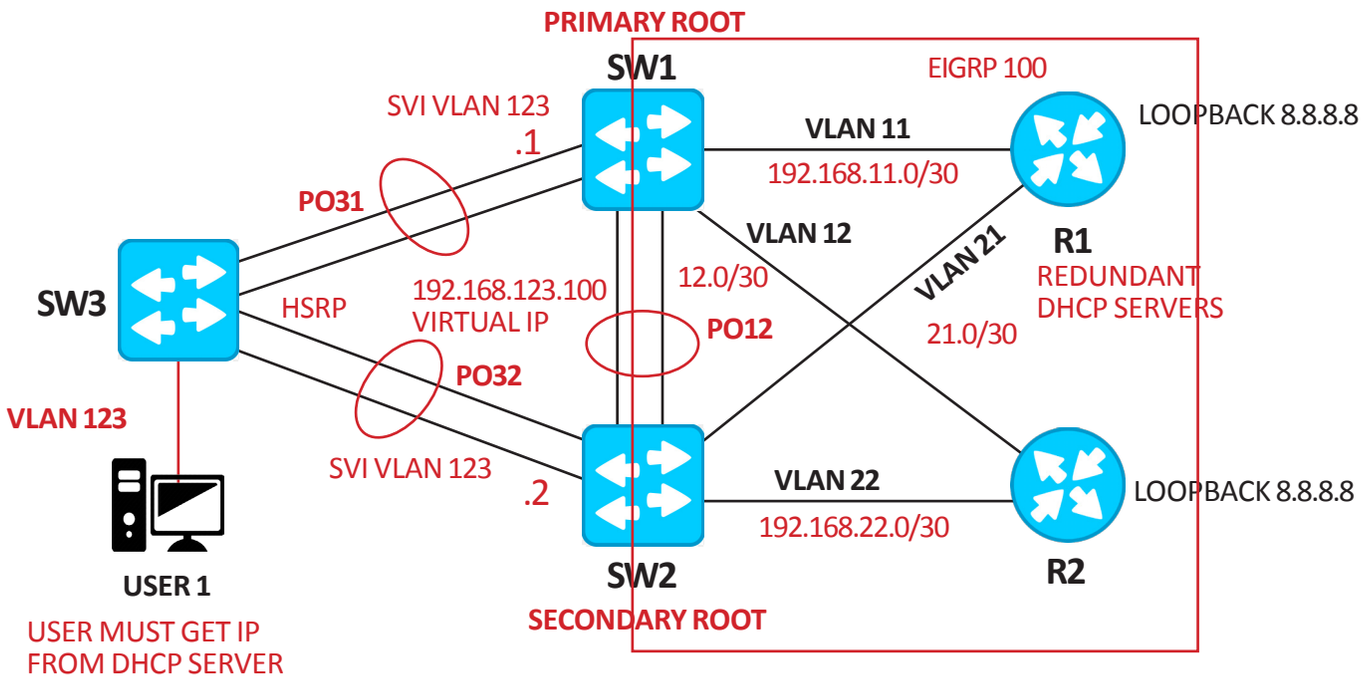
Configure Physical Topology As Shown:

1. Configure VLAN 10 on both the switches.
2. Configure all users in VLAN 10.
3. Configure SW2 as DHCP server for VLAN 10.
   Use network- 192.168.10.0/24, Default-Gateway- 192.168.10.100
4. All users should get IP address from DHCP server.
5. Make sure, if any one connects rogue DHCP server in our network, it should not be used for providing IP addresses. (Use DHCP feature)
6. SW1 should only allow users who got IP address from DHCP server to send traffic.
7. Make sure network must not suffer from IP or MAC confliction.
8. Configure manual IP address on R4. Make sure R4 is able to communicate with gateway and other users.

NB LAB CHALLENGES

Considering CCNP Level, NB Challenges are tough to conquer but with Hard Work, Smart Studies and by improving logical concepts **YOU CAN DO IT!**

CHALLENGE 1



Configure Physical Topology As Shown Above And Perform Following Tasks:-

EtherChannel

1. Bundle links between switches according to the following requirements:-

	Type	PO
SW1-SW3	Dynamic (SW3 should initiate)	13
SW2-SW3	Dynamic (SW3 should initiate)	23
SW1-SW2	Static (No initiation)	12

DTP

1. Configure static dot1q trunk links between SW1 - SW3, SW2 - SW3, SW1 - SW2 (You are not allowed to run any command on physical interface)

VTP

1. Configure SW3 as server and other switches as clients.
2. Use VTP domain name networkbulls.com.
3. Use password networkbulls to secure your VTP domain. Configure VLAN 11, 12, 21, 22 and 123 on server.

Port Assignment

1. Assign ports to the specific VLANs as mentioned in the topology.
2. Create SVI's on SW1 and SW2 for VLANs as shown in the topology, such as on SW1 for VLAN 123, 11, 12.

Services

1. Configure R1 and R2 as redundant DHCP server for VLAN 123. SW1 and SW2 must act as DHCP relay agent.

Routing

1. Configure EIGRP 100 on SW1, SW2, R1 and R2 so that user in VLAN 123 can reach 8.8.8.8.

Gateway Redundancy

1. Configure Cisco's first hop redundancy protocol for providing gateway redundancy to the users in VLAN 123.
2. Make sure SW1 should switch its role in case any upstream link goes down.

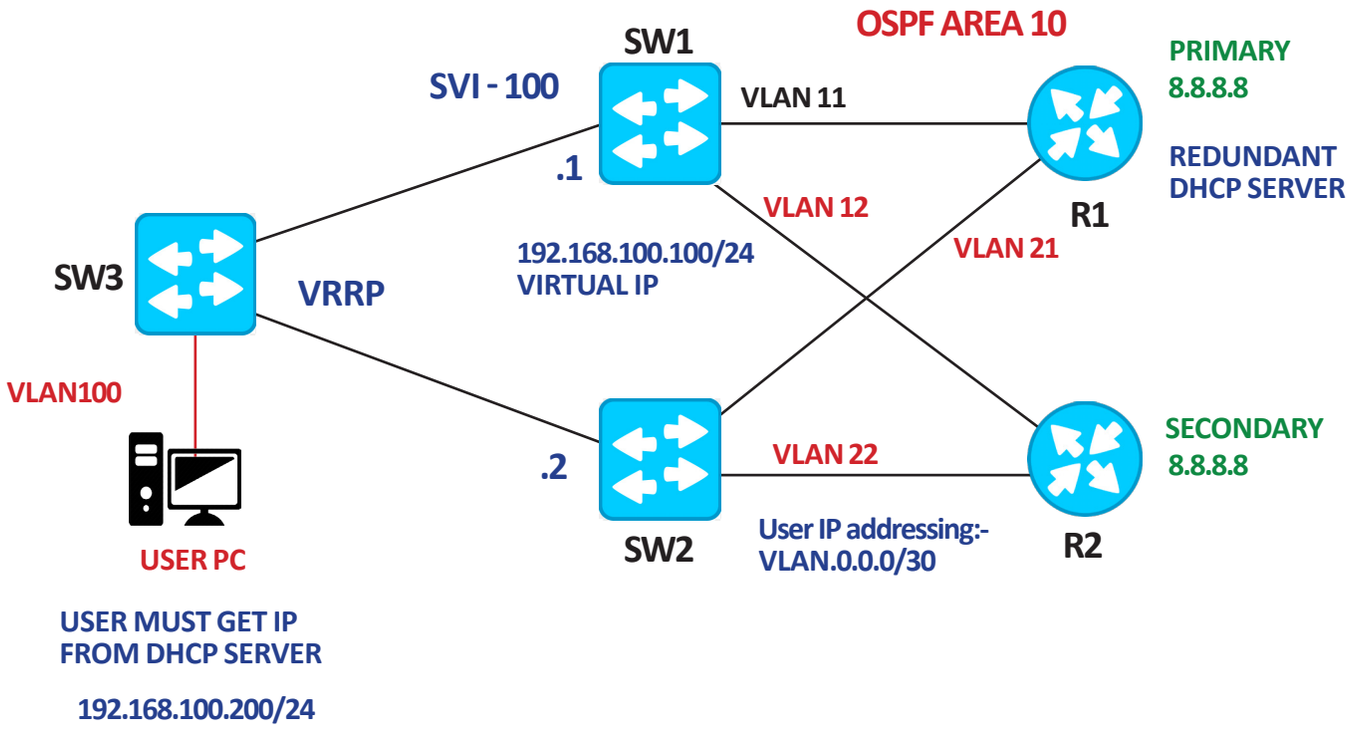
Conclusion

1. Make sure user can ping 8.8.8.8 through SW2 by default.
2. If link between SW2 and ISP goes down then SW1 should become active.

Security

1. Provide access layer security to the user. Port connected to user must allow only user's MAC address.

CHALLENGE 2



Configure Physical Topology As Shown On The Rack:-

VLAN

1. All switches must not share VLAN information.
2. Create VLAN as shown in the topology.
3. Create SVI's according to the topology.(Use IP addresses as shown)

DTP

1. Make sure all switches should form dot1q trunk through negotiation.
2. SW3 should negotiate in both cases.

STP

1. Configure instance based spanning tree.
2. Make sure SW1 should act as Root Bridge for odd VLAN's and SW2 should act as Root Bridge for even VLAN's.
   User name - Networkbulls
   Revision-10

STP Protection

1. Access layer SW must not share BPDU information with the user. (Use a single command to accomplish the task)

Routing Protocol

1. Configure OSPF AREA 10 as shown in the topology.
2. User must use R1 as primary and R2 as secondary router to reach 8.8.8.8. It should not be advertised in OSPF or in any other IGP.
   (Redistribution is not allowed)

Protocol Specific

1. OSPF should use cost 10 for 100Mbps links.
2. On SW1 and SW2, configure int. VLAN 100 and advertise it in area 0, so that we can start getting VLAN 100 as inter-area route in area 10.
3. Area 10 must not receive any external LSA.
4. All interfaces in OSPF should use md5 authentication.

IP Services

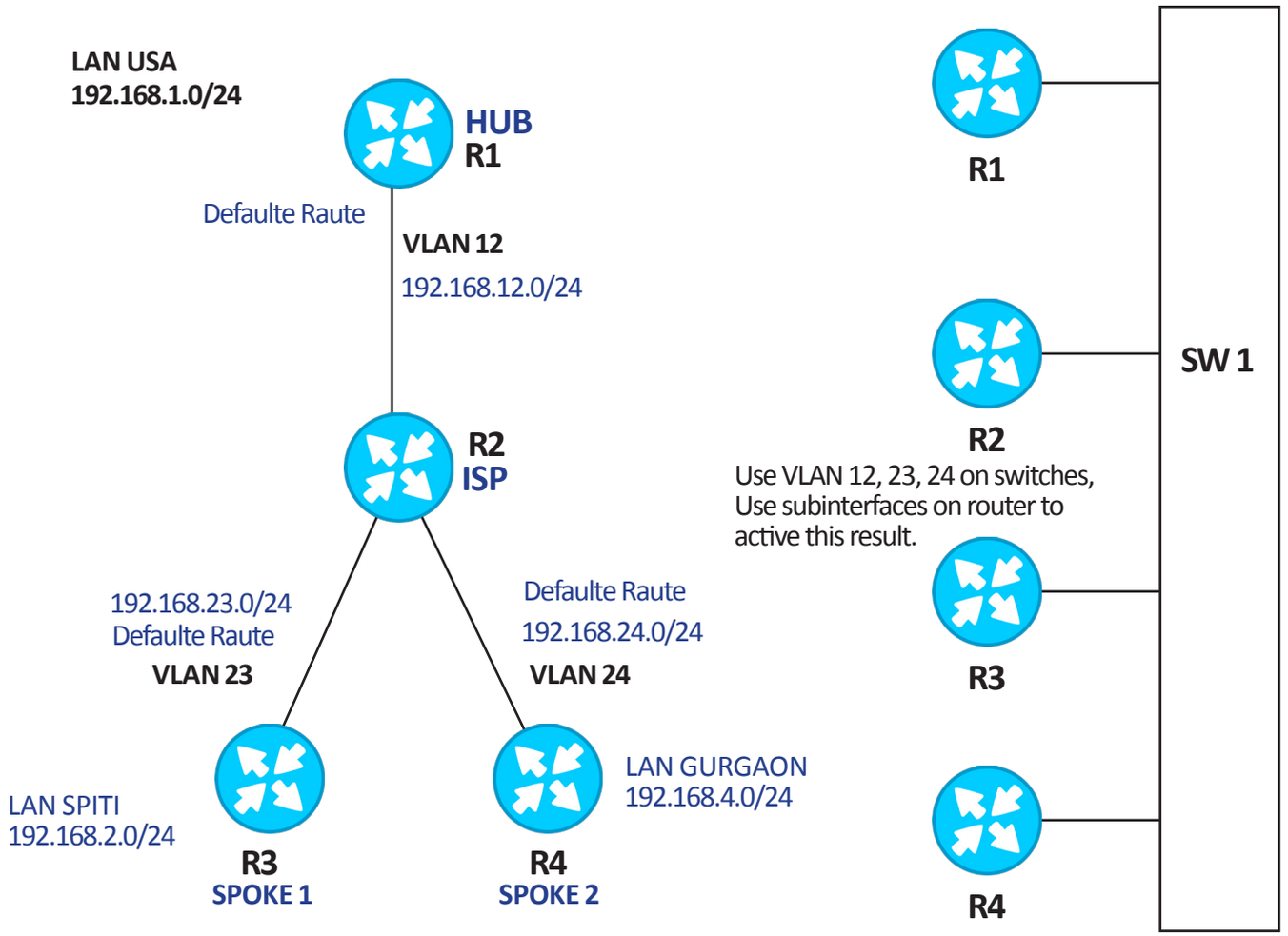
1. Configure open standard first hop redundancy protocol.
2. SW1 should be master.
3. Both SW's must fallback to backup in case of upstream link failure.

4. R1 and R2 should act as DHCP servers.
5. Make sure user should always get the IP as shown in the topology.

Additional

1. Both switches must not share any control plane information other than VRRP and some required protocols.

CHALLENGE 3



Configure Logical Topology as shown:

IP Addressing

1. Configure IP addresses as shown in the topology.
2. Configure loopbacks on routers as LAN Networks.

Default Routing

1. Make sure all sites must reach NBMA IPs.
2. Default route should be removed from the routing table in case of WAN link failure.

Verify

Hub - Ping 192.168.23.x (Spoke1)

Ping 192.168.24.x (Spoke2)

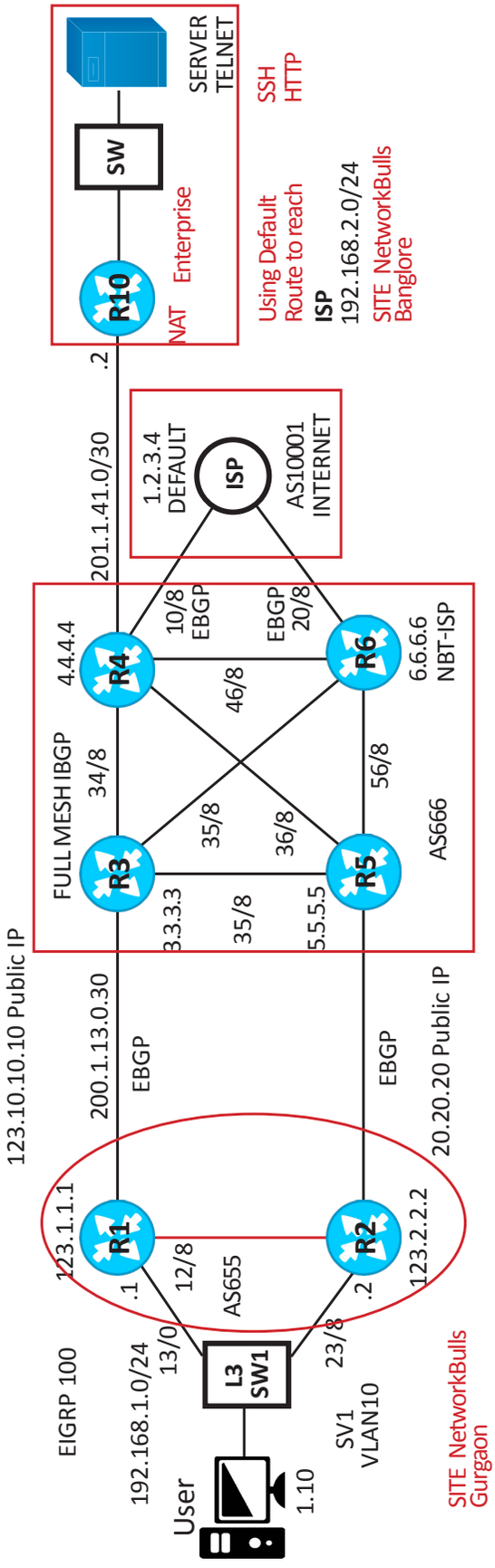
VPN

1. Both spokes should form P2P tunnels with the hub.
2. Hub must authenticate both spokes.
3. Spokes must send registration request in every 10min.

Routing Over VPN

1. Make sure both spokes should communicate via hub. (Use IGP to achieve this)

CHALLENGE 4


SERVER
TELNET
SW
R10
NAT
Enterprise
SSH
HTTP
Using Default
Route to reach
ISP
192.168.2.0/24
SITE NetworkBulls
Banglore
.2
201.1.41.0/30
1.2.3.4
DEFAULT
ISP
AS10001
INTERNET
4.4.4.4
R4
10/8
EBGP
EBGP
20/8
R6
6.6.6.6
NBT-ISP
46/8
FULL MESH IBGP
34/8
R3
35/8
36/8
R5
56/8
AS666
3.3.3.3
35/8
5.5.5.5
123.10.10.10 Public IP
200.1.13.0.30
EBGP
EBGP
20.20.20 Public IP
123.1.1.1
R1
.1
12/8
AS655
R2
.2
123.2.2.2
EIGRP 100
192.168.1.0/24
13/0
L3
SW1
23/8
SV1
VLAN10
User
1.10
SITE NetworkBulls
Gurgaon

Configure physical topology as shown :-

Introduction to the task:-

Here, we have two locations of same company connected together via NBT-ISP. Site NetworkBulls, Gurgaon is using BGP with ISP as it is having multiple connections to ISP whereas the other site is using default route to reach ISP as it is single homed. Here we go –

IP Addressing

1. Configure hostname as shown in the topology.
2. Configure IP addresses as shown in the topology.

AS655

1. Configure 64 bit version of EIGRP to provide connectivity inside AS655.
2. EIGRP should not be running on any interface external to the AS.
3. User must ping 123.1.1.1 and 123.2.2.2.
4. EIGRP should only use metric weight K3 for metric calculation.

AS666

1. Configure OSPF in AS666 to provide connectivity inside AS666.
2. All Routers must use 123.x.x.x/32 as Router id. (X is a router number)
3. OSPF should not be running on any interface external to the AS.

   Verify

   R3#ping 4.4.4.4

   Do the same for all the loopbacks from all the routers inside AS666.
4. R3, R4, R5 and R6 should not install any OSPF route in routing table other than loopbacks (connected subnets are also allowed).

AS Network Bulls, Bangalore

1. Configure router as server.
2. Telnet, SSH and HTTP services should be active on the Server.
3. Make sure R10 is having a default route in routing table to reach the internet.

BGP

1. Connect AS655 and NBT-ISP-AS666.
2. Configure EBGP peering between AS655 and AS666 as shown in the topology on interface basis.
3. Configure IBGP between R1 and R2.

NBT-ISP AS666

1. Configure Full mesh IBGP in AS666 on the basis of loopbacks.

Connecting AS666 AND AS10001 (NBT-ISP)

1. Configure EBGP peering between AS666 and AS10001 as shown in the topology on interface basis.
2. ISP should advertise default and 1.2.3.4 network to NBT-ISP. (Use any method to advertise the network)

Verify

AS655 must get 0.0.0.0 and 1.2.3.4 routes from NBT-ISP.

BGP Challenge

1. R1 and R2 in AS655 must be able to ping 201.1.41.2.

Redistribution

1. In AS655, routes 1.2.3.4, 0.0.0.0 and 201.1.41.0/30 must be seen as EIGRP external routes.

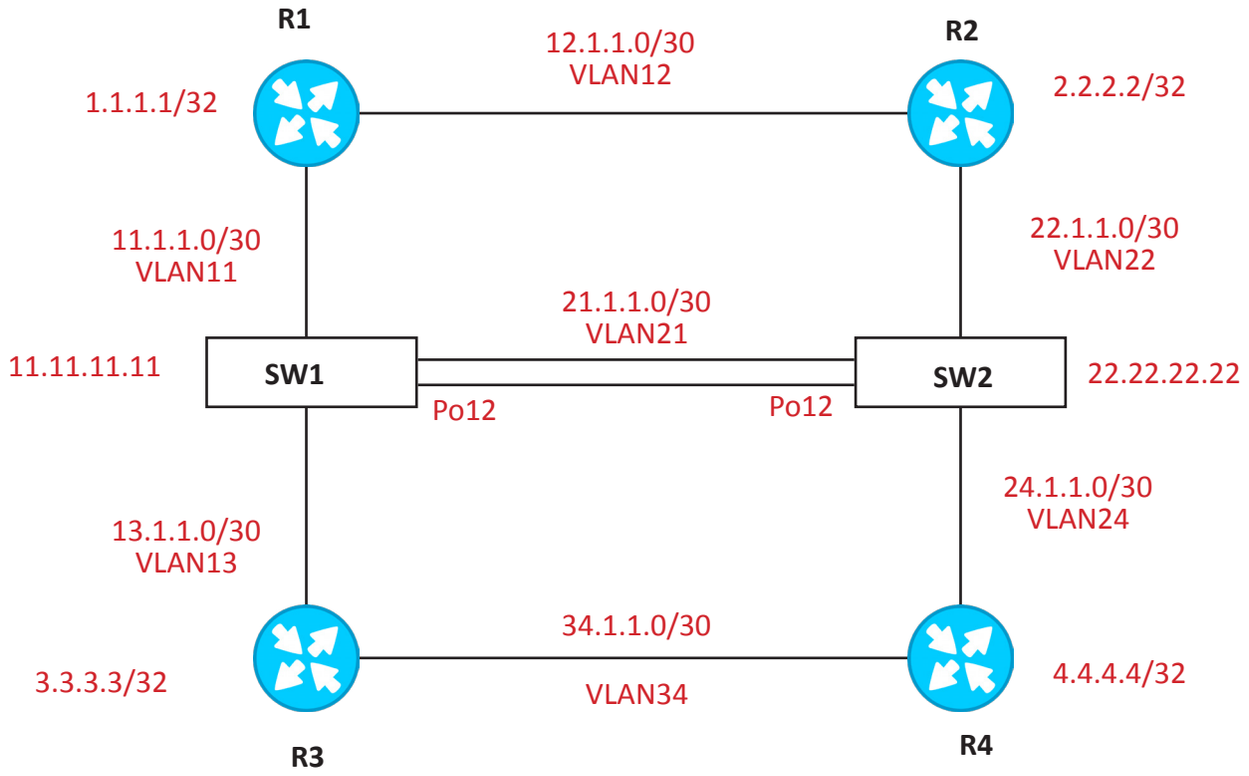
NAT

1. Users traffic for AS655 should get translated to 123.10.10.10 or 123.20.20.20.
2. Make sure users from AS655 can access server at Network Bulls, Bangalore.

Add-On

1. R1 must act as primary gateway for AS655. R2 should be used in case primary gateway goes down.
   In AS666, R6 should be used to forward traffic to 1.2.3.4.
   (If R6 is by default, make R4 as best)
   Verify using Trace.

CHALLENGE 5



CONFIGURING LAYER 2

VTP

(1) Configure SW1 as VTP server and SW2 as VTP client as shown in the diagram.

(2) VTP domain must be NETWORKBULLS.

(3) VTP password must be NETWORKBULLS rocks?

(4) Switch 2 must receive all the VLANs shown in the topology from SW1 as a VTP update.

TRUNKING and VLANS

(1) All the links between SW1 and SW2 must be configured as 802.1q static trunk.

(2) SW1 and SW2 must not negotiate trunking dynamically.

(3) SW1 and SW2 must maintain the dynamically learned mac address entries for at least 3 hrs.

(4) Do the VLAN configuration in such a way that all the routers must be able to reach other routers on the same segment after addressing is done.

SPANNING-TREE

(1) SW1 must be the primary root for all the VLANs and SW2 must be the backup root for all the VLANs.

(2) SW1 must undergo proposal and agreement mechanism during their spanning-tree election process.

(3) All the access-ports must be configured as static access and ports must have an edge status. Verify using show spanning-tree command.

(4) Access-ports must not send and receive BPDUs at all.

LINK AGGREGATION

(1) Configure link aggregation between SW1 and SW2 links using LACP.

(2) SW1 must be the controlling authority while negotiating the aggregate.

(3) SW1 and SW2 must perform the traffic distribution across the EtherChannel using source and the destination MAC of the incoming frame.

IP ADDRESSING

(1) Configure IP addressing as shown in the topology and make sure routers must be able to reach the other router on the same segment.

(2) SW1 and SW2 are the layer 3 switches; they must have virtual interfaces configured on them for their layer 3 connectivity with routers and each other.

CONFIGURING OSPF

(1) Configure OSPF with process-id 1 on all the routers and switches as well as in area 0.

(2) Every layer 3 device must have its router-id configured as loopback manually.

(3) All the loopbacks configured as the router-id must be reachable in OSPF.

(4) SW1 must be the DR on all its segments and SW2 must be BDR on all its segments.

(5) All the routers must have their hello-time to be configured as 250 ms and dead-time as 1 sec.

(6) All the OSPF routers must not be able to perform load balancing on more than 2 links.

OSPF PATH SELECTION USING COST

(1) Configure the network in such a way that the loopback of router 4 must be reachable as the best route to R1 via R2 and SW1 both.

(2) Configure the network in such a way that the loopback of router 3 must be reachable as the best route to R2 via R1 and SW2 both.

OSPF Route-Summarization

(1) Configure loopback 1.2.1.1-1.2.6.1/32 on R1, 2.1.1.1-2.1.6.1/32 on R2, 3.1.1.1-3.1.6.1/32 and 4.1.1.1-4.1.6.1/32 on R4.

(2) Now SW1 and SW2 must receive the summary of all the loopbacks of R1, R2, R3 and R4.

(3) Do not redistribute the loopbacks on R1, R2, R3 and R4 into OSPF.

OSPF DEFAULT ROUTE-ORIGINATION

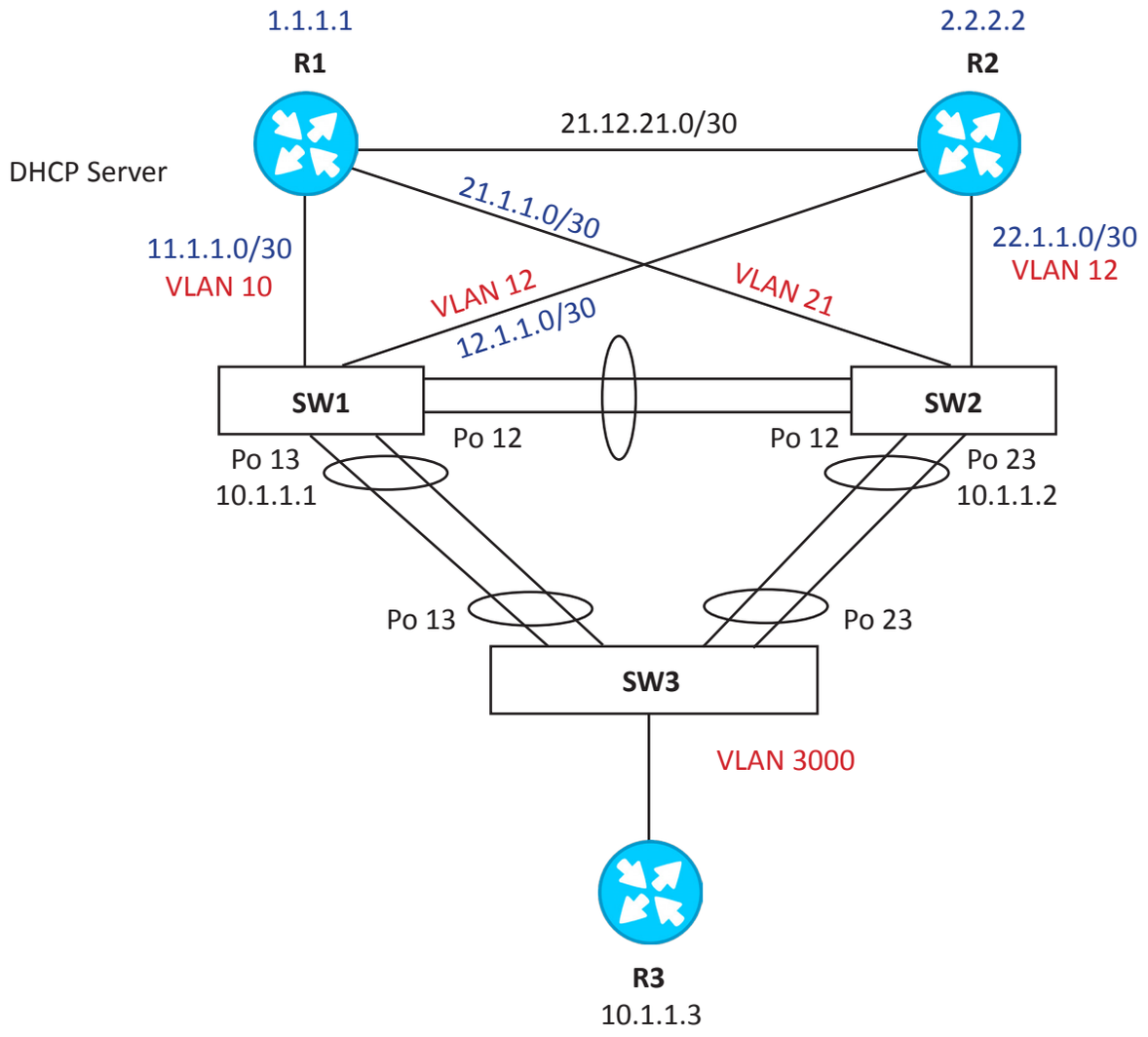
(1) Consider R1 and R2 to be the edge routers. Originate the default route from R1 and R2 into OSPF.

(2) Do not configure any static default route on R1 and R2.

(3) All the routers must prefer the default route from R1 as best route and R2 as backup route.

(4) To verify, configure a loopback 8.8.8.8 on R1 and R2. Do not advertise it into OSPF and traceroute to the loopback 8.8.8.8 from R3 and R4 must terminate at R1.

CHALLENGE 6



VTP

(1) Configure the VTP domain name NETWORKBULLS on SW1, SW2 and SW3.

(2) Configure the VTP mode on all the switches in such a way so that they allow the configuration of the above task.

(3) Configure the VTP ver 2 and VTP password CCIE.

TRUNKING

(1) All the links between SW1, SW2 and SW3 must be configured as the 802.1q static trunk.

(2) Dynamic trunking negotiation must be disabled on all the trunk links.

(3) All the trunk links must allow the trunking of only those VLANs that are shown in the topology including default native VLAN.

LINK AGGREGATION

(1) All the trunk links between the switches must be aggregated using the Cisco proprietary protocol.

(2) Use the channel groups according to the port number shown in the diagram.

(3) SW1 and SW2 must distribute the incoming frames on the basis of source and destination address of the packet.

(4) SW3 must distribute the incoming frames on the basis of source MAC.

IP ADDRESSING

(1) Configure IP addressing as shown in the diagram. Router 1, 2 and SW1, 2 must be able to reach each other on their directly connected segments.

IGP CONFIGURATION

(1) Configure EIGRP between R1, R2, SW1 and SW2 as IGP using AS no. 1212.

(2) Configure EIGRP in such a way that it must support multiple address-families under the single process.

(3) Make sure that all the routers must use only delay as the relevant metric component.

(4) Enable on all the loopback interfaces as well.

DEFAULT-ROUTE Origination

(1) Assume R1 and R2 to be the edge routers and both must originate a default route into EIGRP.

(2) Make sure that the traffic of LAN users must always go out via R1 primarily.

(3) For verification configure a loopback 1.2.3.4 on both R1 and R2 as the Internet route. Do not advertise it in EIGRP.

HIGH AVAILABILITY

(1) Configure HSRP on SW1 and SW2 to provide high availability of default gateway to user in VLAN 3000 connected to SW3.

(2) Use HSRP ver 2 and group 12 on both SW1 and SW2.

(3) Virtual IP must be configured to 10.1.1.10

(4) SW1 must be configured as the active router and SW2 as a standby router. However, SW2 must be able to takeover in case SW1 fails.

(5) Both the switches must track the reachability of default route. The switch on which the track fails must lose its active role.

DHCP

(1) Configure R1 as the DHCP server in such a way that it must provide IP address to R3, as shown in the diagram.

(2) R3 must act as a host but do not disable routing on R3.

DHCP-SNOOPING

(1) Configure DHCP snooping on SW3 and it should receive the DHCP offers only on those interfaces where DHCP server is located.

(2) Do not disable option 82 on SW3.

(3) Now reinitiate the DHCP request from the host R3 to verify.

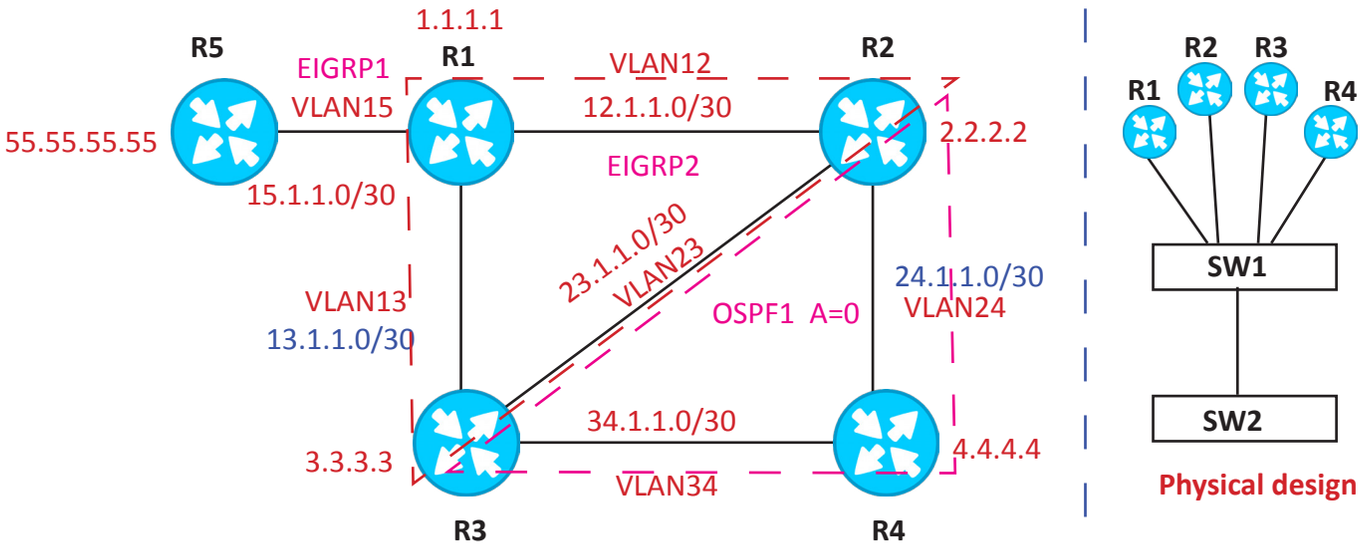
FINAL VERIFICATION

(1) Now, from R3 trace the route to 1.2.3.4. It must go via SW1 and terminate at R1.

(2) Now, filter the default route on SW1 then trace the route. It must go via SW2 and terminate at R1 again.

CHALLENGE 7

Task Redistribution on Rack



Task 1: Basic Configuration

(A) Use as shown in the physical diagram and create the logical topology shown out of it.

(B) All the switch ports must be configured according to the requirement as trunk or access. The trunk and access, if used then they must come up immediately

(C) Configure the IP addressing as shown in the diagram.

(D) Make sure all the routers must be able to ping all the connected routers on their common segments.

Task 2: IGP CONFIGURATION

(A) Configure EIGRP 1 between R5 and R1.

(B) Configure EIGRP 2 between R1, R2 and R3 on segments in VLAN 12, 13 and 23.

(C) Configure OSPF1 area 0 on R2, R3 and R4 for segments in VLAN 24 and 34.

Task 3: REDISTRIBUTION

(A) Now mutually redistribute EIGRP 1 and 2 on R1.

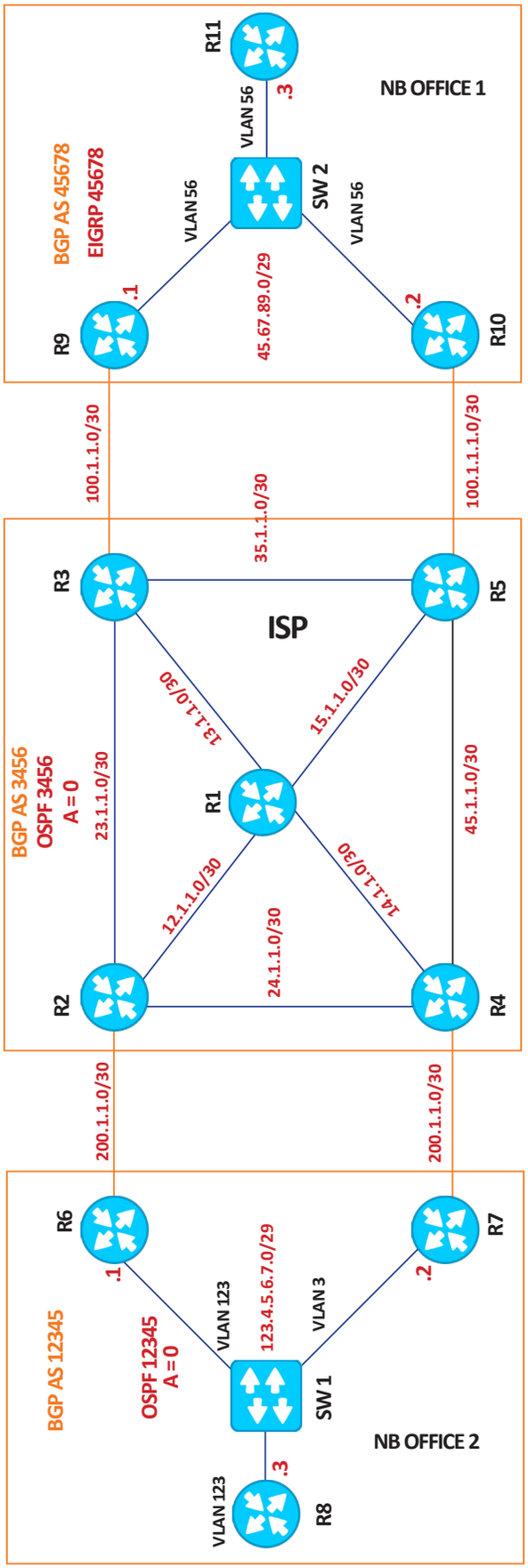
(B) Mutually redistribute EIGRP 2 and OSPF 1 on R2 and R3.

VERIFICATION

After redistribution the loopback of R5 and network on segment VLAN 15 must be reachable to R4 via R2 and R3 both. This should be revealed by the trace output.

Note:- You are not allowed to change AD value on any router. Do not use access-list and prefix-list to accomplish this task.

CHALLENGE 8


R11
.3
NB OFFICE 1
VLAN 56
BGP AS 45678
EIGRP 45678
VLAN 56
SW 2
VLAN 56
.1
.2
R9
45.67.89.0/29
R10
100.1.1.0/30
35.1.1.0/30
100.1.1.1.0/30
R3
R5
ISP
13.1.1.0/30
15.1.1.0/30
BGP AS 3456
OSPF 3456
A = 0
23.1.1.0/30
R1
45.1.1.0/30
14.1.1.0/30
12.1.1.0/30
24.1.1.0/30
R2
R4
200.1.1.0/30
200.1.1.0/30
R6
R7
.1
.2
123.4.5.6.7.0/29
VLAN 123
VLAN 3
BGP AS 12345
OSPF 12345
A = 0
SW 1
NB OFFICE 2
.3
VLAN 123
R8

Guidelines for the task

- Task1 is basic IP addressing and IGP configuration task in different BGP AS.
- Task2 is BGP configuration task to form EBGP and iBGP peering.
- Task3 is a route origination and route aggregation task without using aggregate address command. (Hint –originate a static route as a BGP route).
- Task 4 is a BGP default route origination task.
- Task 5 use any BGP path attribute to complete the task and try to use MED and LOCAL-PREFERENCE. Remove task 4 before starting this task.
- Task 6 remove task 5 to complete task 6

Task 1

IP Addressing

1. Configure IP addressing in BGP AS 12345, 34567 and 45678 as shown in the diagram.
2. Configure a loopback on all the routers as x.x.x.x where x is the router number.

Basic IGP Configuration (NB Office 1)

1. EIGRP configuration BGP AS 45678.
2. Configure EIGRP 45678 in BGP AS 45678 only for all the intra-AS links. Ensure EIGRP must not run on any inter-AS link.
3. All the routers must use 64-bit metric calculation and only delay must be used as the relevant metric component.
4. All the routers must use authentication with password CCIE. Do not use md5.

OSPF Configuration in BGP AS 12345 (NB Office 2)

1. Configure OSPF 12345 in BGP AS 12345 only for intra-AS links. Do not enable OSPF on any inter-AS link.
2. All the routers must use type 2 authentication .
3. All the OSPF routers must use the hello interval of 250 ms and dead interval of 1 sec.
4. R8 must be elected as the DR and R6 must be elected as the BDR.

OSPF Configuration In BGP AS 34567 (ISP)

1. Configure OSPF 34567 in BGP AS 34567 only for the intra-AS links. Do not enable OSPF on any inter-AS link.
2. Configure OSPF in such a way that none of the router in the AS performs the DR and BDR election.
3. Do not use network command in OSPF in BGP AS 34567.

Task 2

BGP Configuration-IBGP

1. **BGP configuration AS 12345.**
    a. Configure IBGP session between R6 and R7 using their loopback addresses.
    b. R8 must not run BGP at all.
2. **BGP configuration AS 34567**
    a. Configure IBGP full mesh in BGP as 34567 using the loopback addresses of the routers.
    b. Use peer-group IBGP for easy manageability.
3. **BGP Configuration AS 45678**
    a. Configure IBGP session between R9 and R10 using their loopback addresses.
    b. Do not configure BGP on R11.

EBGP Configuration

1. Configure EBGP session between R6-R2 and R7-R4 using their physical interface addresses.
2. Configure EBGP between R3-R9 and R5-R10 using their physical interface addresses.

Task 3

BGP NLRI Origination

1. Create loopbacks 11.1.1.1-11.1.6.1/32 on router R11.
2. Create loopbacks 8.1.1.1-8.1.6.1/32 on R8.
3. Now, originate the loopbacks of R11 into BGP on R9 and R10 using network command.
4. Originate the loopbacks of R8 on R6 and R7 into BGP using network command.
5. After the above tasks, make sure that R8 must receive all the loopbacks of R11 and R11 must receive all the loopbacks of R8.

Route-Aggregation

1. R9 and R10 must originate the aggregate 11.1.0.0/16 of the loopbacks of R11, do not use 'aggregate-address' command on R9 under BGP.
2. R6 and R7 must originate the aggregate 8.1.0.0/16 of the loopbacks of R8, do not use 'aggregate-address command under BGP on R7.

Task 4

Default-Route Origination

1. Originate the default route from R1 into BGP.
2. Make sure R8 must receive that default route as a OSPF route and R11 must receive that default-route as EIGRP route.
3. Now, create a loopback 1.2.3.4 on R1. Do not advertise that loopback into OSPF and BGP as well.
4. Now, make sure R8 can reach that loopback sourcing loopback 8.1.1.1.
5. Also R11 can reach that loopback sourcing loopback 11.1.1.1.

Task 5

BGP Path Selection

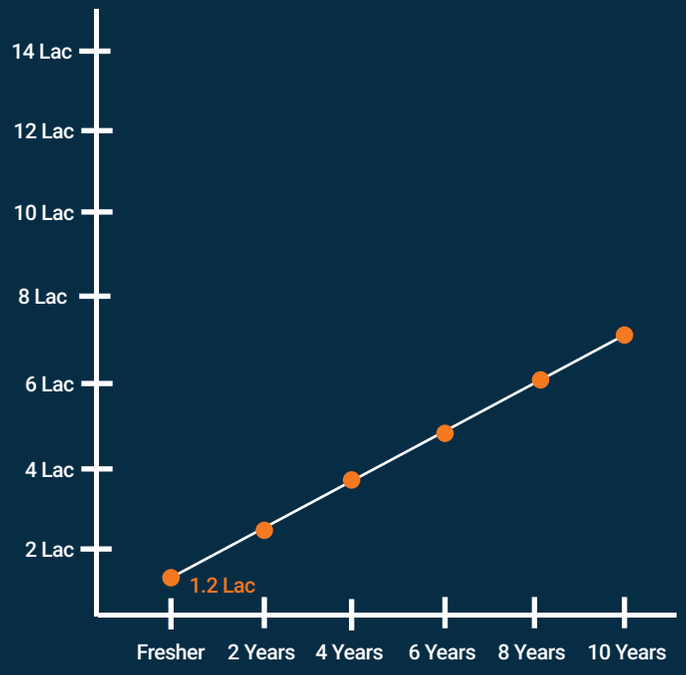
1. Perform the path selection in such a way that traffic originated from the loopbacks of R8 to the loopbacks of R11 must exit AS 12345 via R6 and return via R7.
2. Make sure the traffic originated from the loopbacks of R11 to the loopbacks of R8 must exit R10 and return via R9.
3. To perform the above task use any BGP path attribute wherever you want.

Task 6

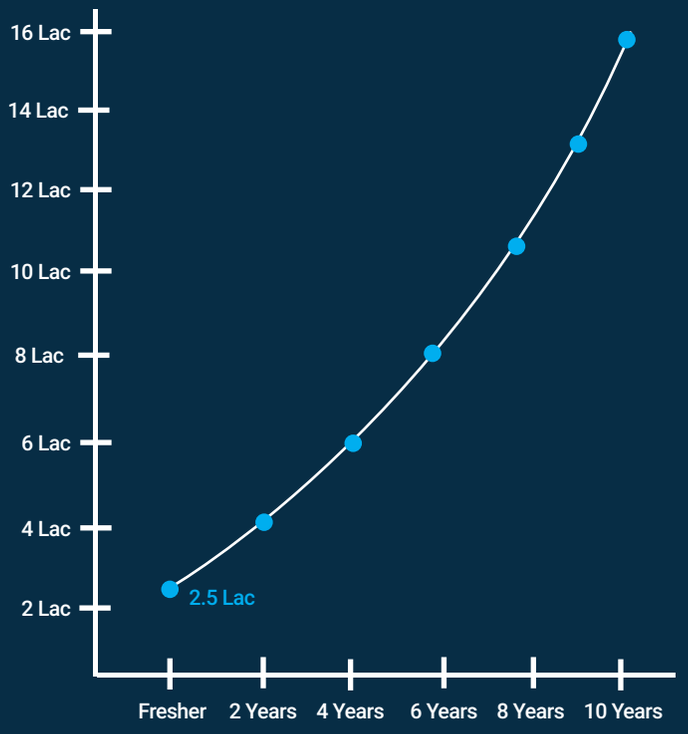
BGP Route-Filtering

1. Make sure R6 must receive only the even loopbacks of R11 and R7 must receive only the odd loopbacks of R11.
2. Similarly, R9 must only receive the odd loopbacks of R8 and R10 must only receive the even loopbacks of R8.

YOUR 10 YEAR GROWTH CHART AFTER CCNA, CCNP & CCIE?

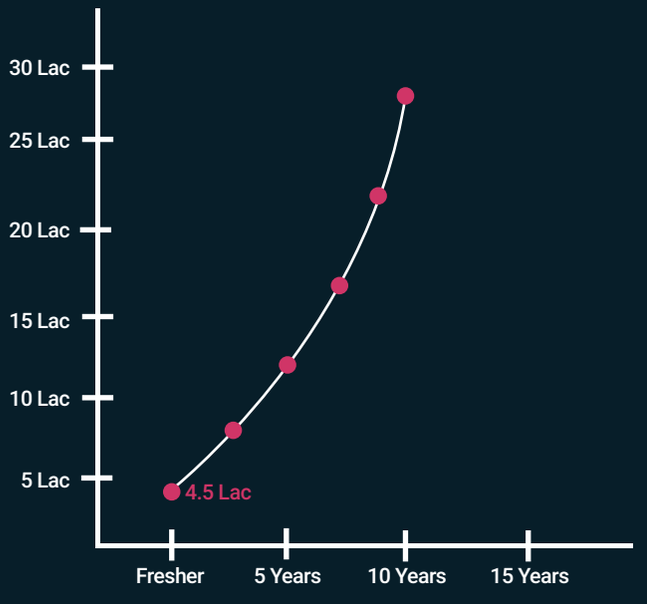


STUDENT WITH CCNA OR CCNP LEVEL KNOWLEDGE



STUDENT WITH CCIE WRITTEN CERTIFICATION

CAREER PATH OF CCIE LAB CERTIFIED STUDENT



“ CCIE Lab Certified Students get 2x career growth compared to students who have CCIE written Certification and 5x career growth compared to students with CCNA, CCNP level knowledge. So,

Go for CCIE Lab Certification & Make your Career FLY! ”

Our Special **Thanks to!**

TRAINERS

Mr. Ajaypal CCIE R&S #51341 & Data Center Written Certified
Mr. Piyush Kataria CCIE R&S V5 #50204
Mr. Mohit Bhalla CCIE #42145, CCSI #34989
Mr. Vikas Kumar Triple CCIE #30078 (R&S, Security and Voice)
Mr. Navneet CCNA R&S + CCNP R&S

DESIGNERS

Mr. Vishwa Ajit Singh
Mr. Nandan Kumar

CONTENT WRITER

Ms. Sparna Saxena

For their contribution in making of this world Class Practical Workbook

Getting to world class begins with single step. Start today

HAPPY LEARNING