

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



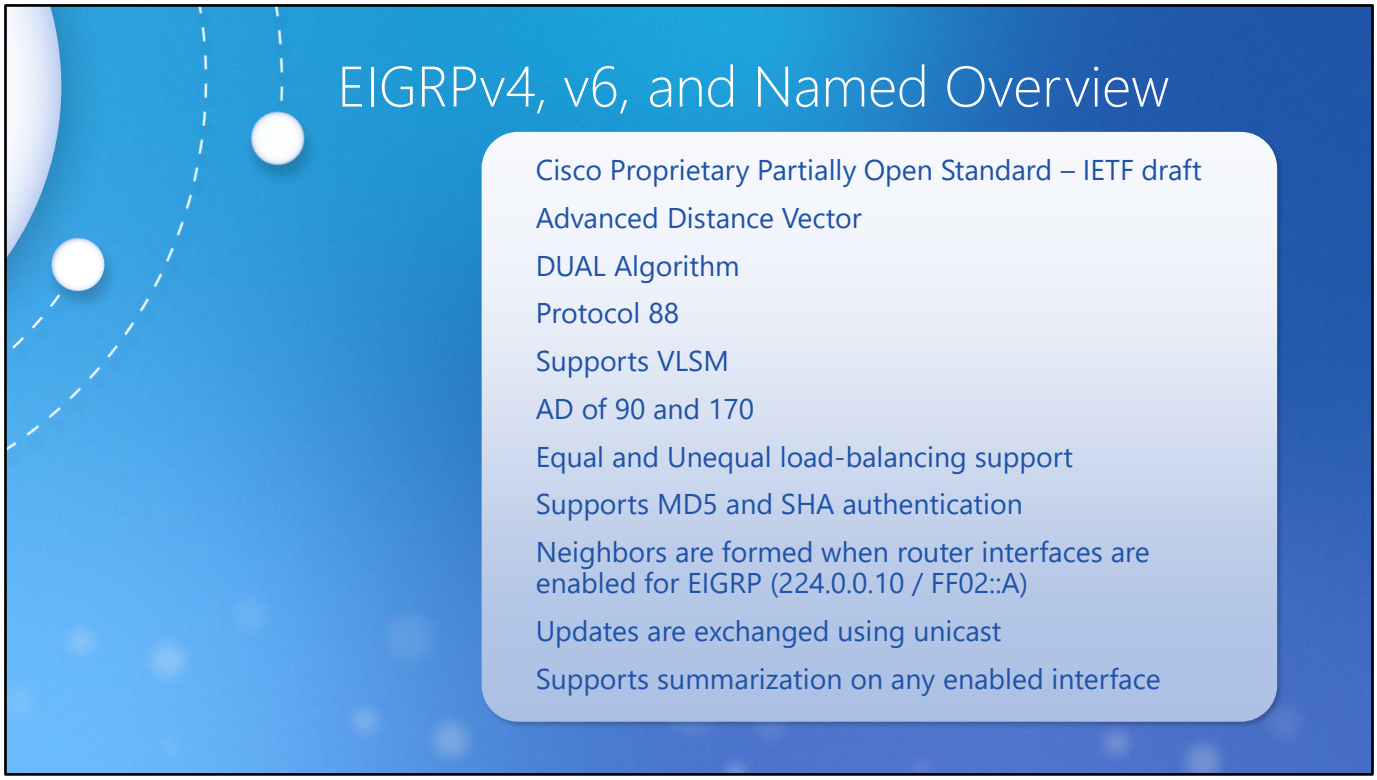
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_eigrp/configuration/xe-16-5/ire-xe-16-5-book.html

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Title slide

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



*Dual Algo
*Adv Dist Vector
*Protocol 88 (Own Layer 4 proto) (RTP – reliable transport protocol)

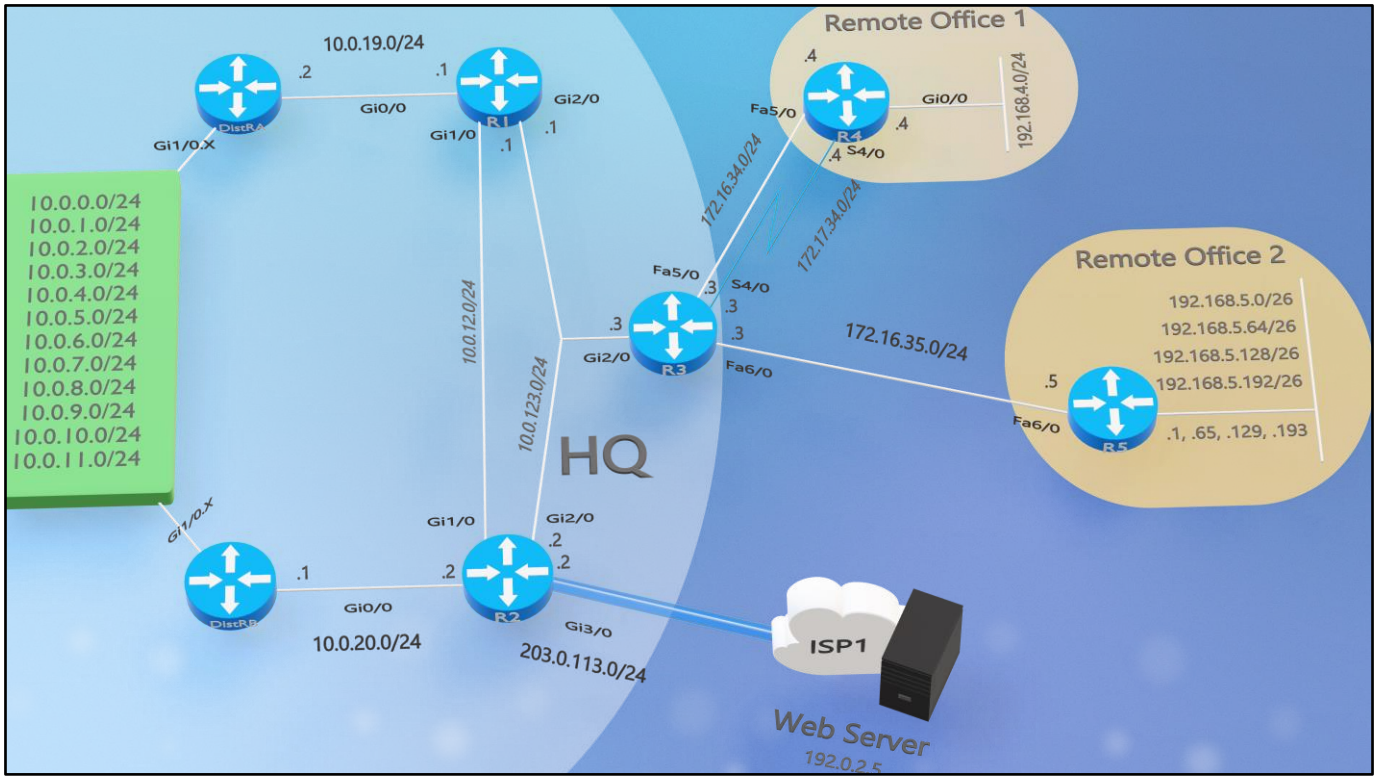
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



DEMO: Configure all interfaces except ISP interface for EIGRP.

Unicast between r3 and r5 as multicast is disabled on interfaces (ACL).

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



DEMO: Configure all interfaces except ISP interface for EIGRP.

Why do we enable the routing process on the interface??? (2 reasons)

1. **So the interface will join multicast group 224.0.0.10 and send/receive EIGRP hello packets (sent 5 sec, dead after 15sec (60/180 on slow speed wan links [1mbps ad less]) on the interface to form a neighbor adjacency.**
2. **To inject the network ID/subnet ID the interface is part of into the EIGRP routing process so it can be shared with the other routers.**

Unicast between r3 and r5 as multicast is disabled on interfaces (ACL).

inject a static default route on R2 “redistribute static”

Show ip protocols
Show ip eigrp interface
Show ip eigrp interface detail
Show ip eigrp neighbor
Show ip eigrp neighbor detail
Show ip eigrp topology

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Show ip route

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



DEMO: Configure all interfaces except ISP interface for EIGRP.

Unicast between r3 and r5 as multicast is disabled on interfaces (ACL).

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

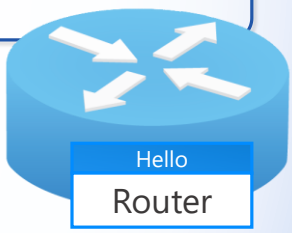
Router-ID

Uniquely identifies the router
Used as a loop prevention mechanism

If not manually configured:

- **Highest loopback**
- **Highest IP**

```
eigrp router-id x.x.x.x
```



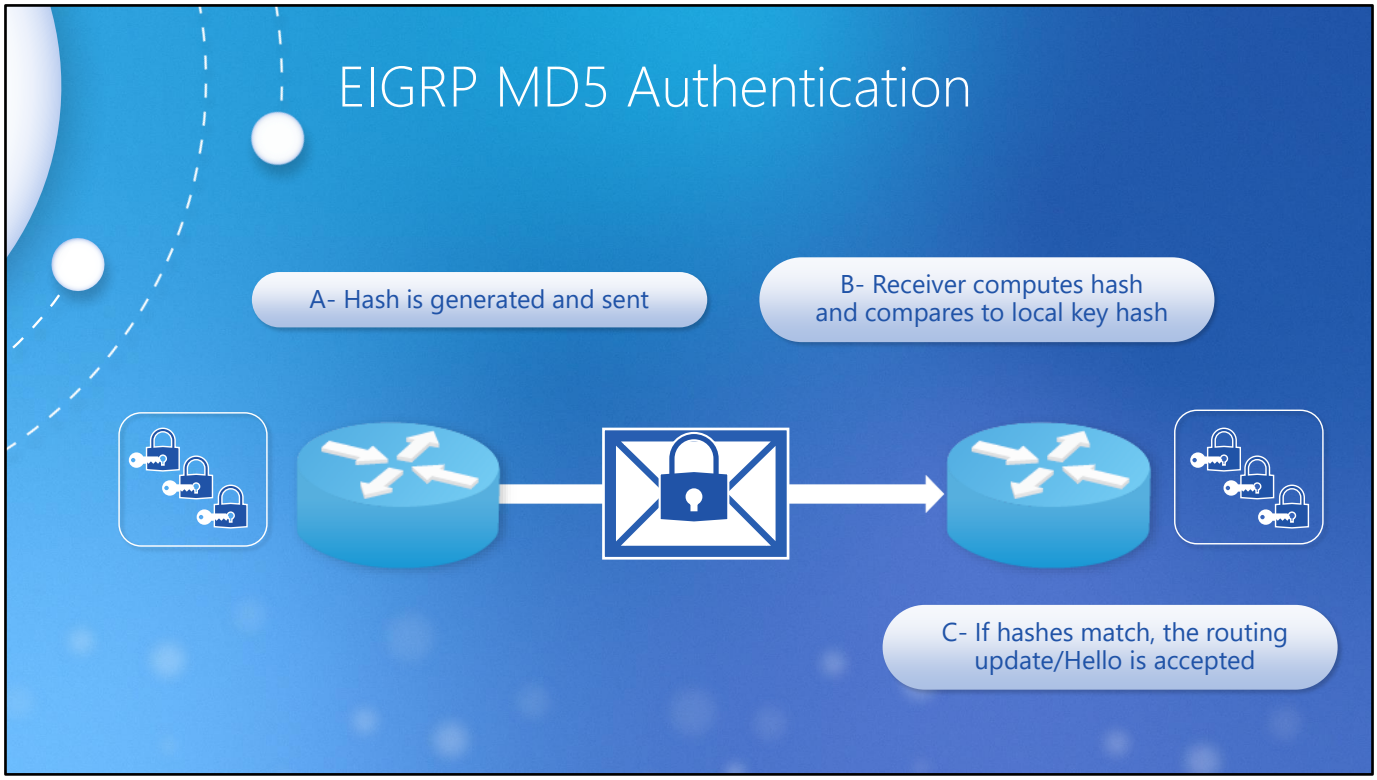
Subcommand will force adjacency to bounce (will not be displayed on the “show ip eigrp neigh”)

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



PASSIVE INTERFACE AND AUTHENTICATION

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



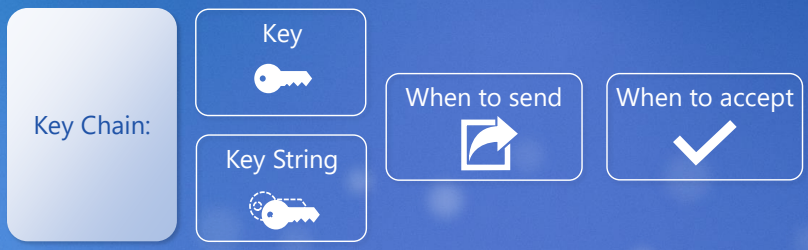
With classic EIGRP only MD5 is support. With Named MD5 and HMAC-SHA-256 is supported. (authentication mode hmac-sha-265 password XYZ in address family interface config mode.)

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Time-Based Key Chains

EIGRP supports key chains:

- Key Chains support multiple keys
- Recommended to change keys frequently
- Typically you'll associate a Send time and Accept time
- A key chain is applied to an interface and as ingress traffic enters interface, it checks keychain

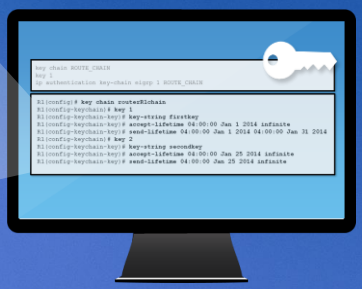


©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

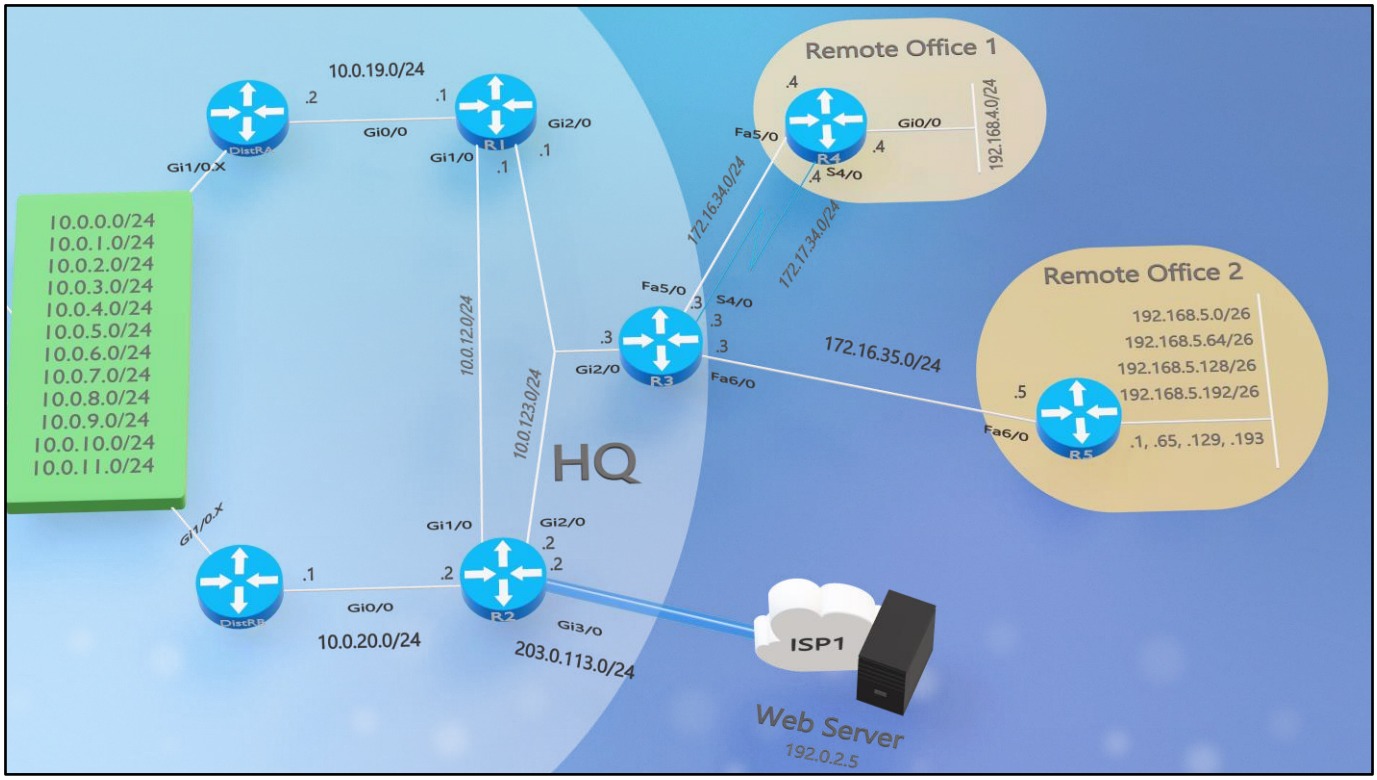
Configuring Key Chains



```
R1(config)# key chain routerR1chain
R1(config-keychain)# key 1
R1(config-keychain-key)# key-string firstkey
R1(config-keychain-key)# accept-lifetime 04:00:00 Jan 1 2014 infinite
R1(config-keychain-key)# send-lifetime 04:00:00 Jan 1 2014 04:00:00 Jan 31 2014
R1(config-keychain)# key 2
R1(config-keychain-key)# key-string secondkey
R1(config-keychain-key)# accept-lifetime 04:00:00 Jan 25 2014 infinite
R1(config-keychain-key)# send-lifetime 04:00:00 Jan 25 2014 infinite
```



©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



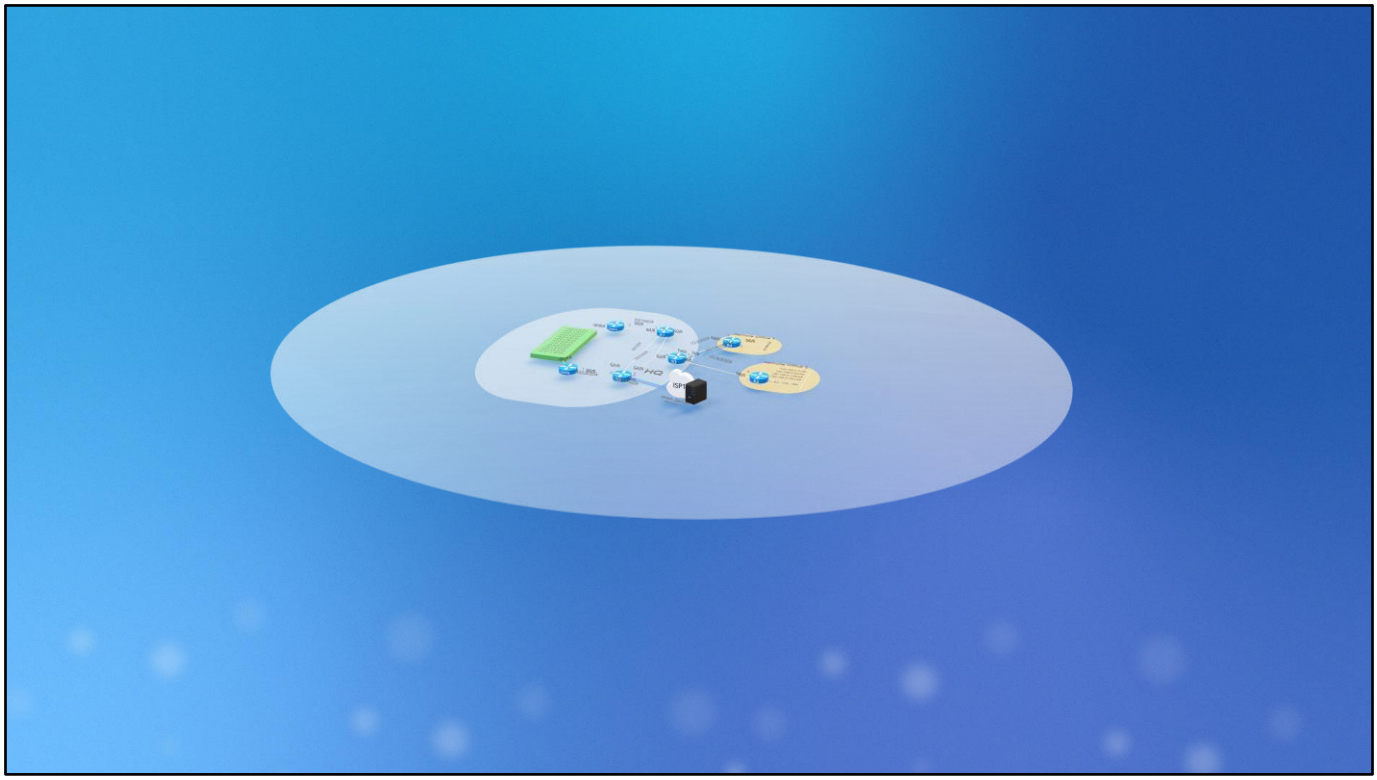
DEMO: Authentication between R1 and R2 as well as Passive interface.

Create key chain and keys
Interface level commands:

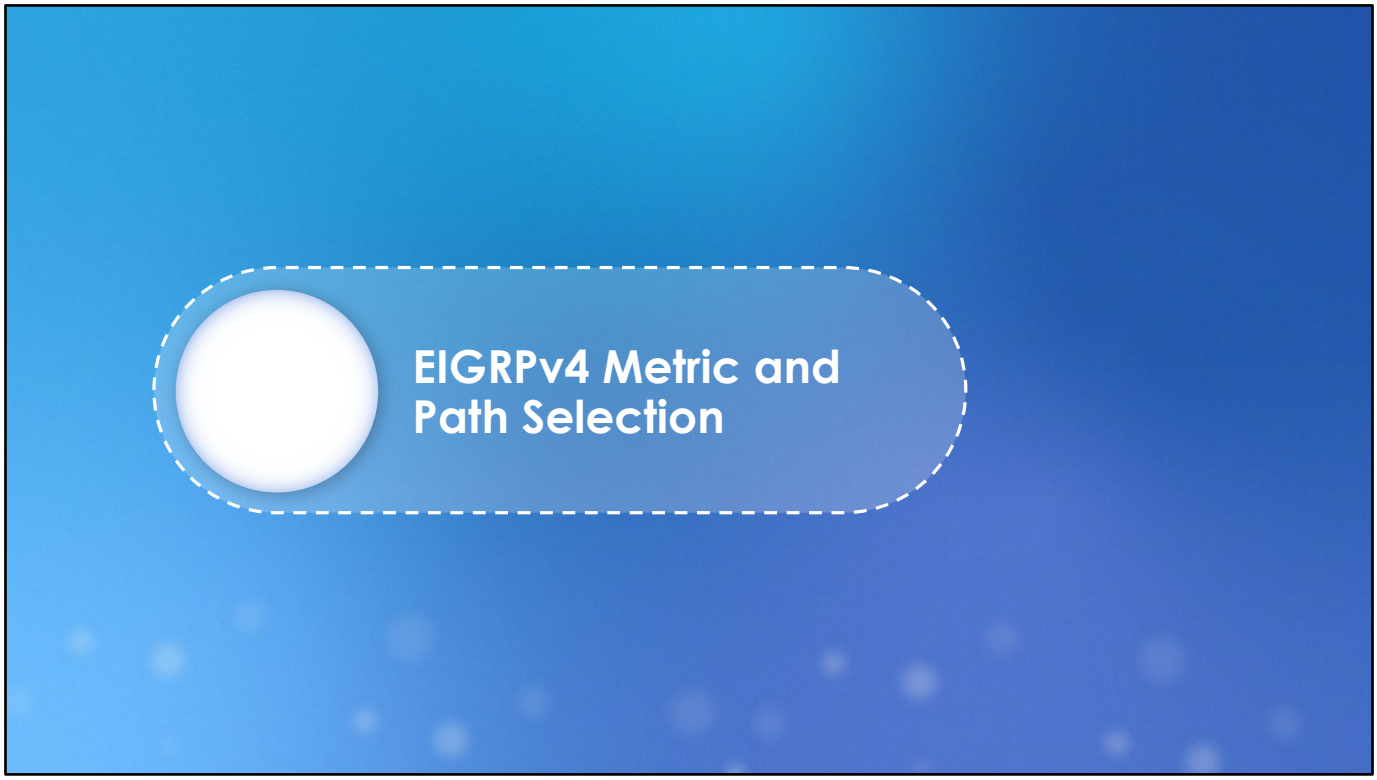
```
ip authentication mode eigrp 1 md5
ip authentication key-chain eigrp 1 routerR1chain
```

***

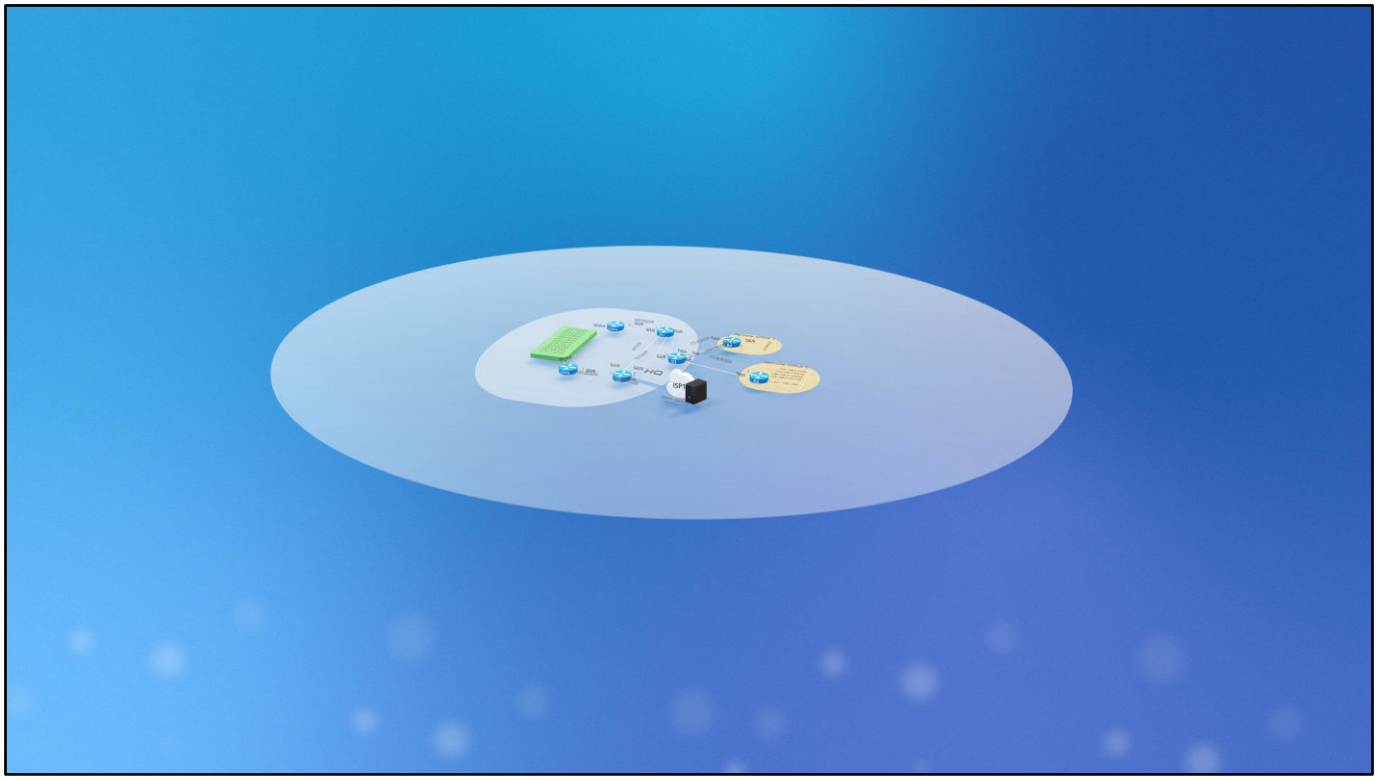
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



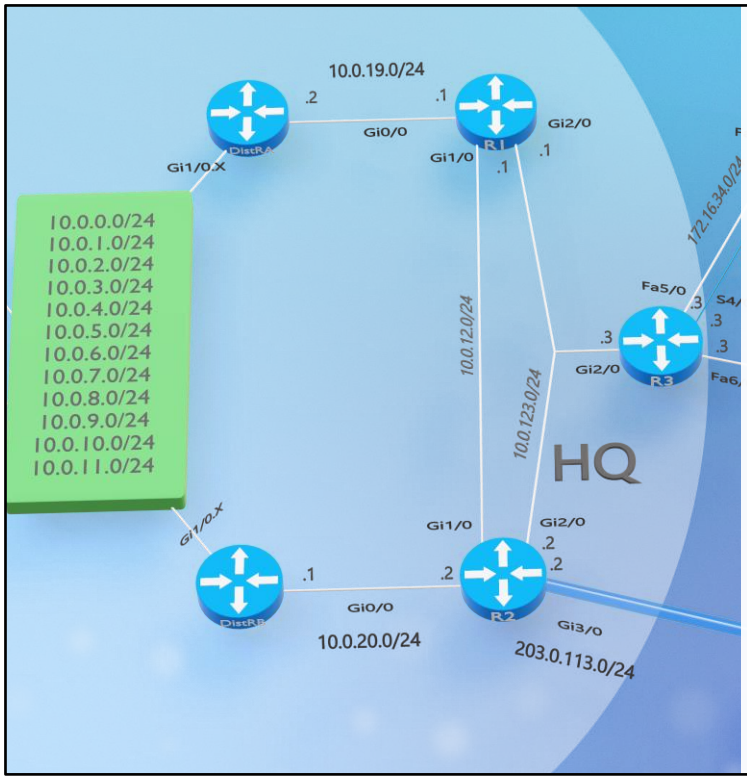
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Feasible Distance (FD)

Metric value of the lowest-metric path for a prefix

Reported Distance (RD)

Metric value to reach prefix reported by neighbor

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_eigrp/configuration/15-sy/ire-15-sy-book/ire-wid-met.html

Show ip protocols
Show interface name/number

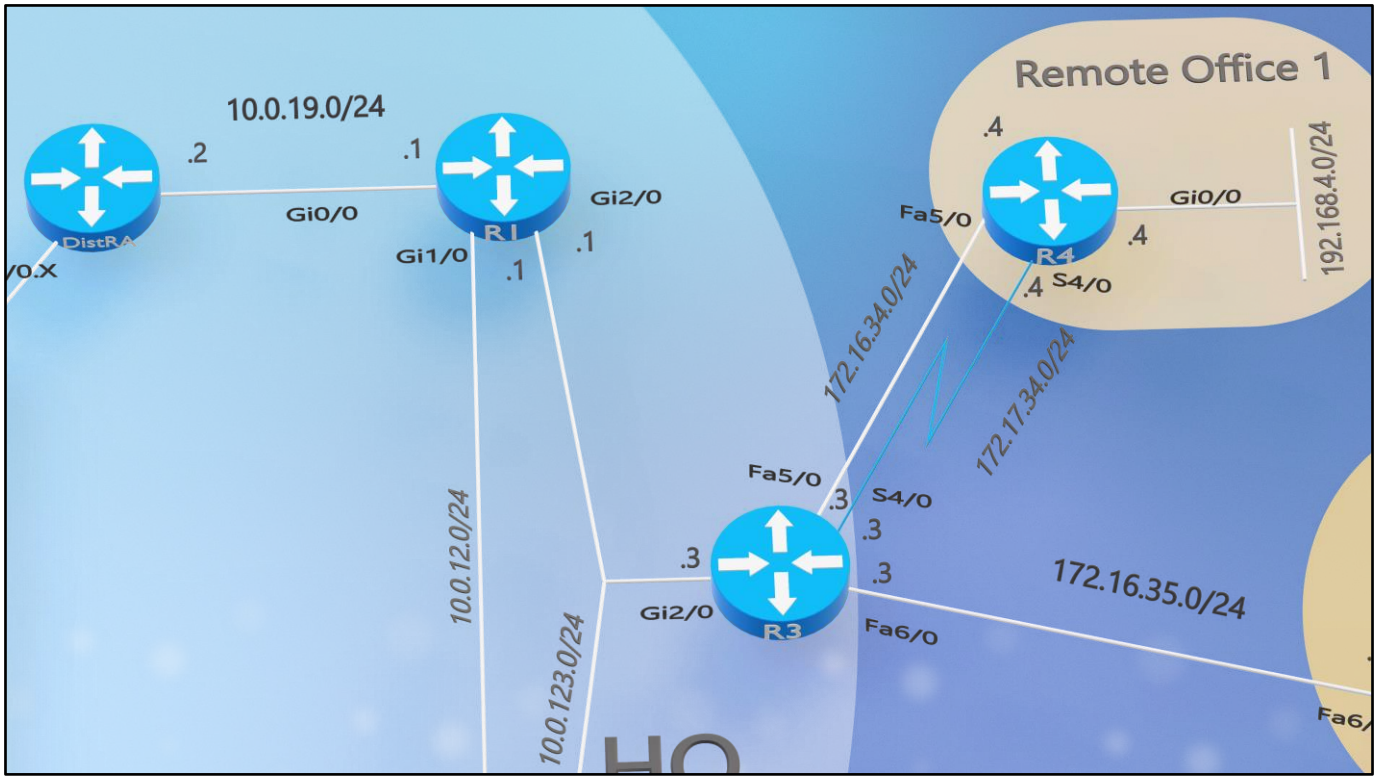
Scaled bandwidth is 10^7/minimum bandwidth
Scaled delay is cumulative delay in 10s of microseconds.

Demo changing K values and stress the must match

```
metric weights 0 1 0 1 1 0

Neighbor x.x.x.x  (int x/x) is down: metric changed
Neighbor x.x.x.x  (int x/x) is down: K-value mismatch
```

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

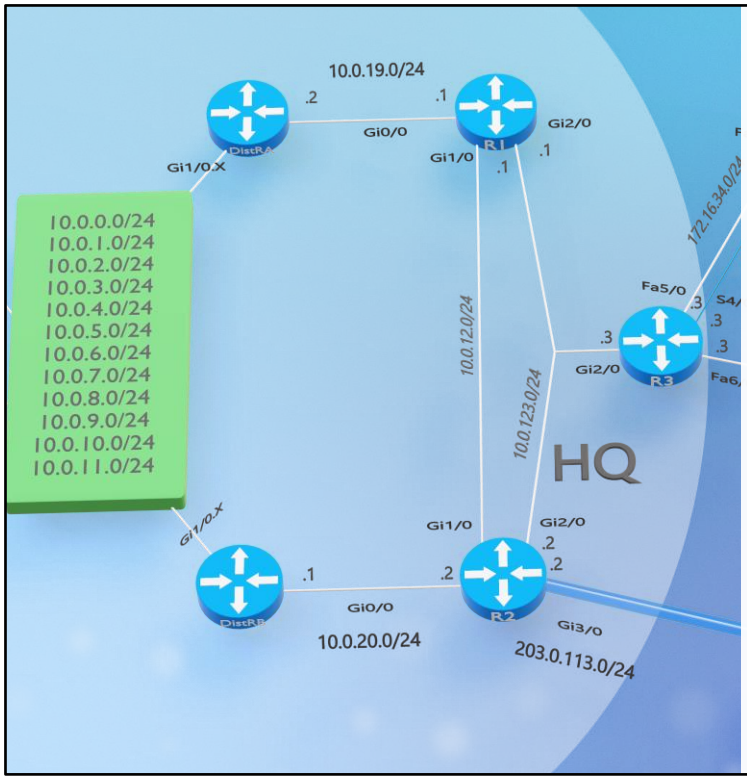


https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_eigrp/configuration/15-sy/ire-15-sy-book/ire-wid-met.html

Demo calculation from R4 192.168.4.0/24 to DSW1.

```
show interfaces name x/x
show ip eigrp topology {dest prefix}
```

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Successor – Best Path

Feasible Successor – Backup

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_eigrp/configuration/15-sy/ire-15-sy-book/ire-wid-met.html

Show ip protocols
Show interface name/number

Demo changing K values and stress the must match

```
metric weights 0 1 0 1 1 0

Neighbor x.x.x.x  (int x/x) is down: metric changed
Neighbor x.x.x.x  (int x/x) is down: K-value mismatch
```

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Feasibility condition exists to ensure a loop free network.

FS = LFA (loop free alternative path)

Search for "EIGRP Loop-Free Alternate Fast Reroute"
EXAM: https://www.cisco.com/en/US/docs/ios-xml/ios/iproute_eigrp/configuration/15-2s/ire-ipfrr.html
Shared link risk group

EIGRP Loop-Free Alternate (LFA) Fast Reroute (FRR)
EIGRP Loop-Free Alternate (LFA) Fast Reroute (FRR) is a feature that allows EIGRP to switch to a backup path in less than 50 ms. Fast reroute means we switch to another next hop, Loop-free alternate is an alternative path in the network that is loop free.
Now you might be thinking that this sounds familiar. After all, EIGRP has feasible successors. Those are loop-free alternate paths that EIGRP has calculated. If the successor fails, EIGRP can use a feasible successor right away.
This is true, but there's one big "gotcha". EIGRP feasible successors are not

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

installed in the routing table right away. Only the successor route is installed. When the successor fails, EIGRP installs the feasible successor, and this takes time. Fast reroute installs both the successor route and the feasible successor route in the routing table which makes convergence even faster.
IGPs can calculate LFAs using different methods:
•**Per-link**: all prefixes that are reachable through a certain link share the same information, they all use the same next hop address. When we calculate the LFA per link, we calculate a single backup next hop address for all prefixes that use the link. This means that if the primary link fails, all prefixes are switched to a secondary link. The advantage of per-link LFAs is that it's simple to calculate, it uses less CPU and memory resources. The disadvantage, however, is that once the primary link fails, all traffic to the prefixes that used the primary link are suddenly switched to a single backup link. It is possible that your backup link gets overburdened with this sudden spike of traffic.
•**Per-prefix**: we calculate an LFA for each prefix, in other words for each possible destination. This requires more resources, but it does offer better load balancing. It's possible that two prefixes currently use the same path, but once the primary link fails, they use different backup next hops. This spreads your traffic more throughout the network.
When you have multiple possible LFAs, fast reroute has to select one LFA. EIGRP will not just select the "best" (lowest metric) feasible successor but uses some "tie-breakers" to select the best LFA. When you use per-prefix LFA, we have these four attributes:
•**Interface disjoint**: don't select an LFA that uses the same outgoing interface as the primary path. Imagine we have R1, connected to R2 and R3 on a multi-access segment. R1 also has a connection to R4 using a different interface. R2, R3, and R4 all offer a path to a certain destination. R2 is the successor, R3 and R4 are feasible successors. R3 has a better metric. Which feasible successor would you prefer? R1 can reach R2 and R3 using the same interface, R4 through a different interface. There is a risk that once R2 is unreachable that R3 also becomes unreachable (maybe the switch fails). It might be a better idea to prefer R4 instead...I'm going to show you this in an example, later in this lesson.
•**Line card disjoint**: don't select an LFA that shares a line card with the primary card. The same logic as the interface-disjoint applies here. There is a risk that your line card fails which means that both the successor and feasible successor are unusable.
•**Lowest repair path metric**: don't select an LFA with a high metric. This ensures that only the lowest metric LFAs remain.
•**Shared Risk Link Group (SRLG)**: don't select LFAs that use the same

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

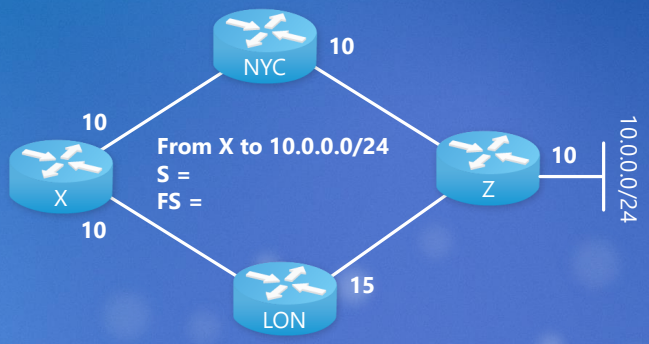
SRLG. This one requires some more explanation. Imagine we have R1, connected to R2, R3, and R4. R2 and R3 use the same uplink to reach a certain destination. R4 uses a different link to reach the same destination. R2 is the successor, R3 and R4 are feasible successors, but R3 has a better metric. Which feasible successor would you prefer? R3 has a lower metric, but it uses the same uplink...that's a risk. By adding R2 and R3 to the same SRLG, you can tell EIGRP to prefer R4 since it uses a different uplink. I will show you an example of SRLG on some routers later in this lesson.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Feasibility Condition

Loop prevention mechanism

In order to become FS… Reported Distance < Feasible Distance of Successor



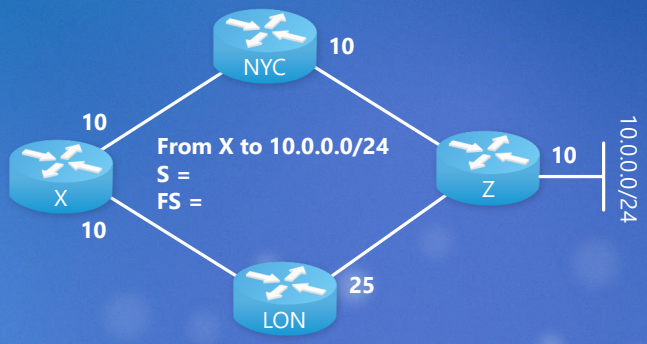
To be a FS your reported distance must be less than the feasible distance of the current successor.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Feasibility Condition

Loop prevention mechanism

In order to become FS… Reported Distance < Feasible Distance of Successor



To be a FS your reported distance must be less than the feasible distance of the current successor.

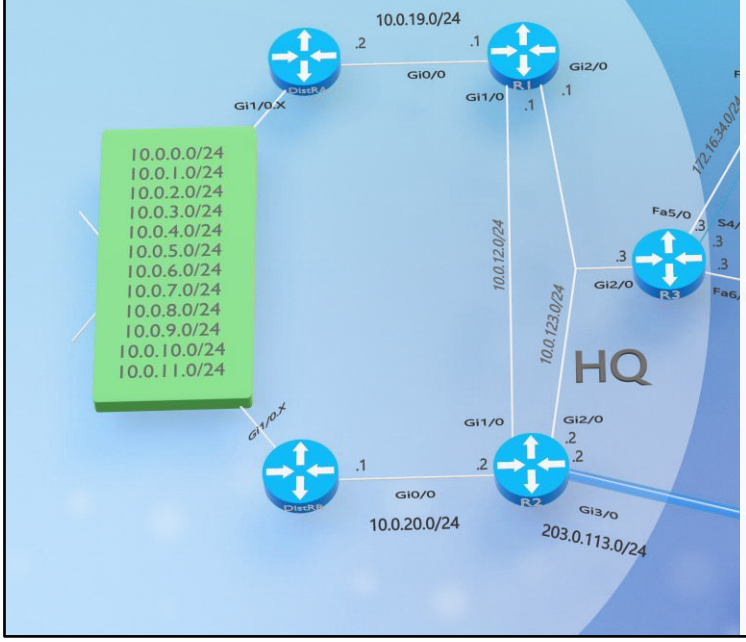
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Demo: Feasibility condition

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

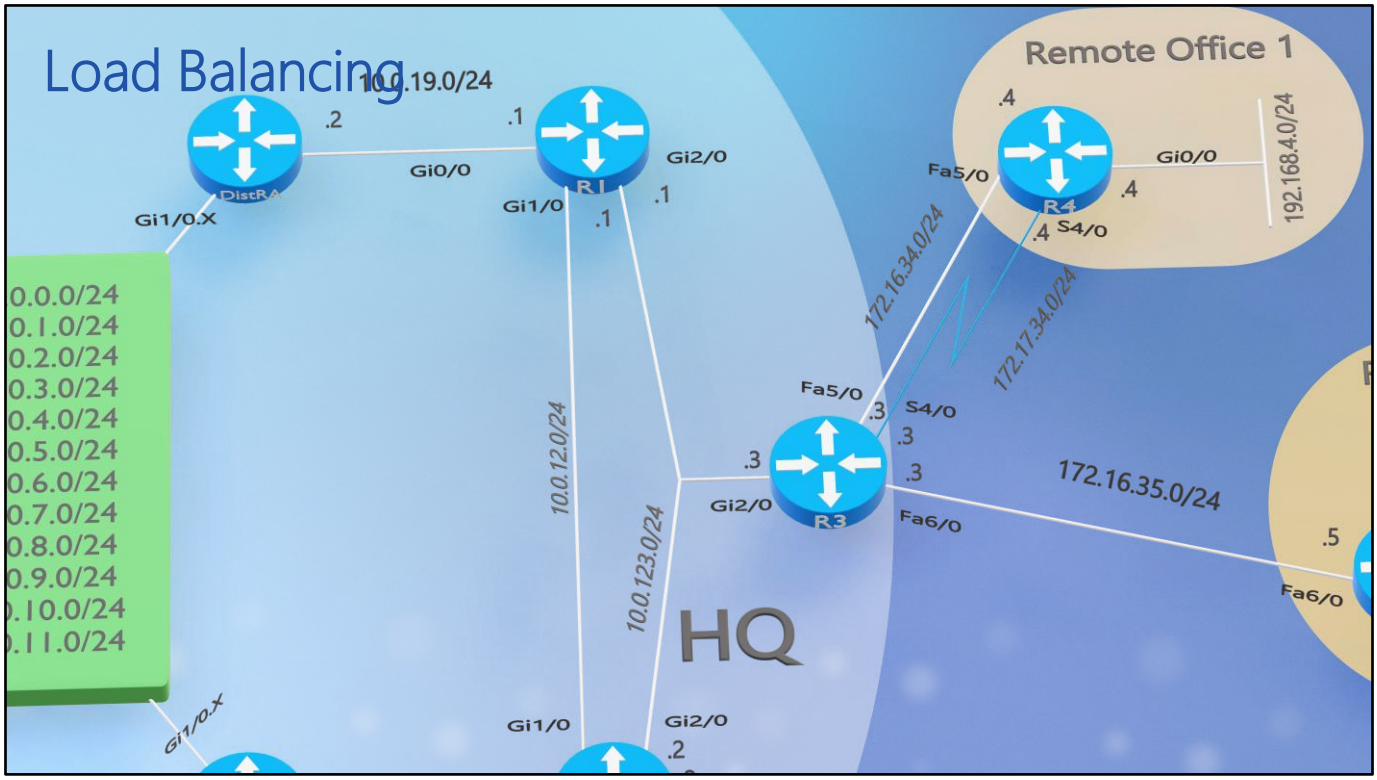
Load Balancing



Equal and Un-equal load balancing supported

- Equal cost load balancing up to 4 paths by default
- Unequal load balancing with "variance" command

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Demo: Load Balancing

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

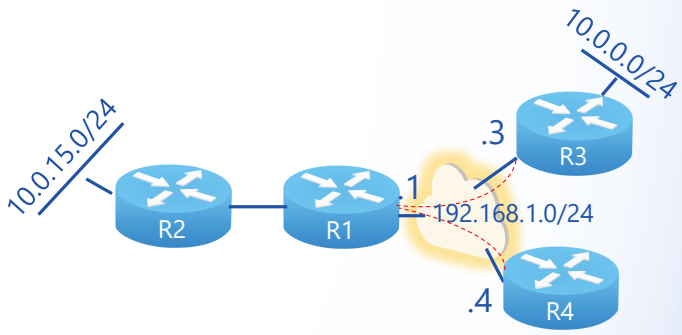


©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

EIGRP Split Horizon

Rule

Do not advertise routes in the same direction you learned them



Shut off split horizon or use sub interfaces to solve the problem.
Int

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Changing Timers

Configured on interface:

```
int gigabitethernet 0/1
    ip hello-interval eigrp AS# time_seconds
    ip hold-time eigrp AS# time_seconds
```

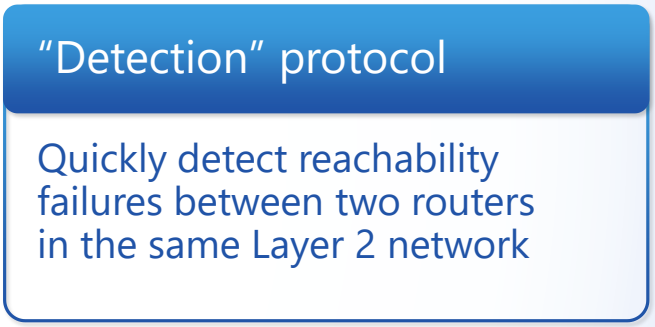
Verification:

```
show ip eigrp interface detail
```

5 and 15
60 and 180 (less than 1mbps links)

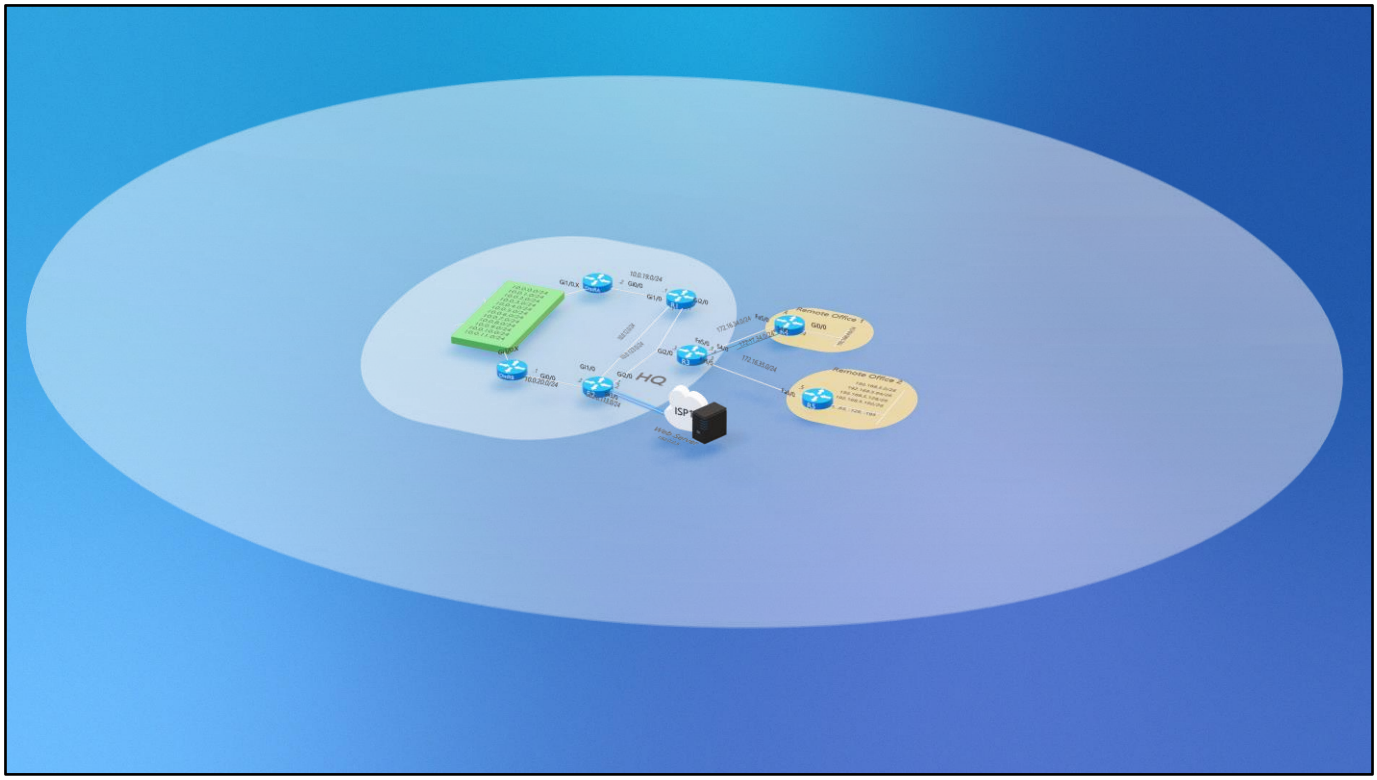
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Bi-directional Forwarding Detection



to quickly detect reachability failures between two routers in the same Layer 2 network so that network issues can be identified as soon as possible, and convergence can occur at a far faster rate.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



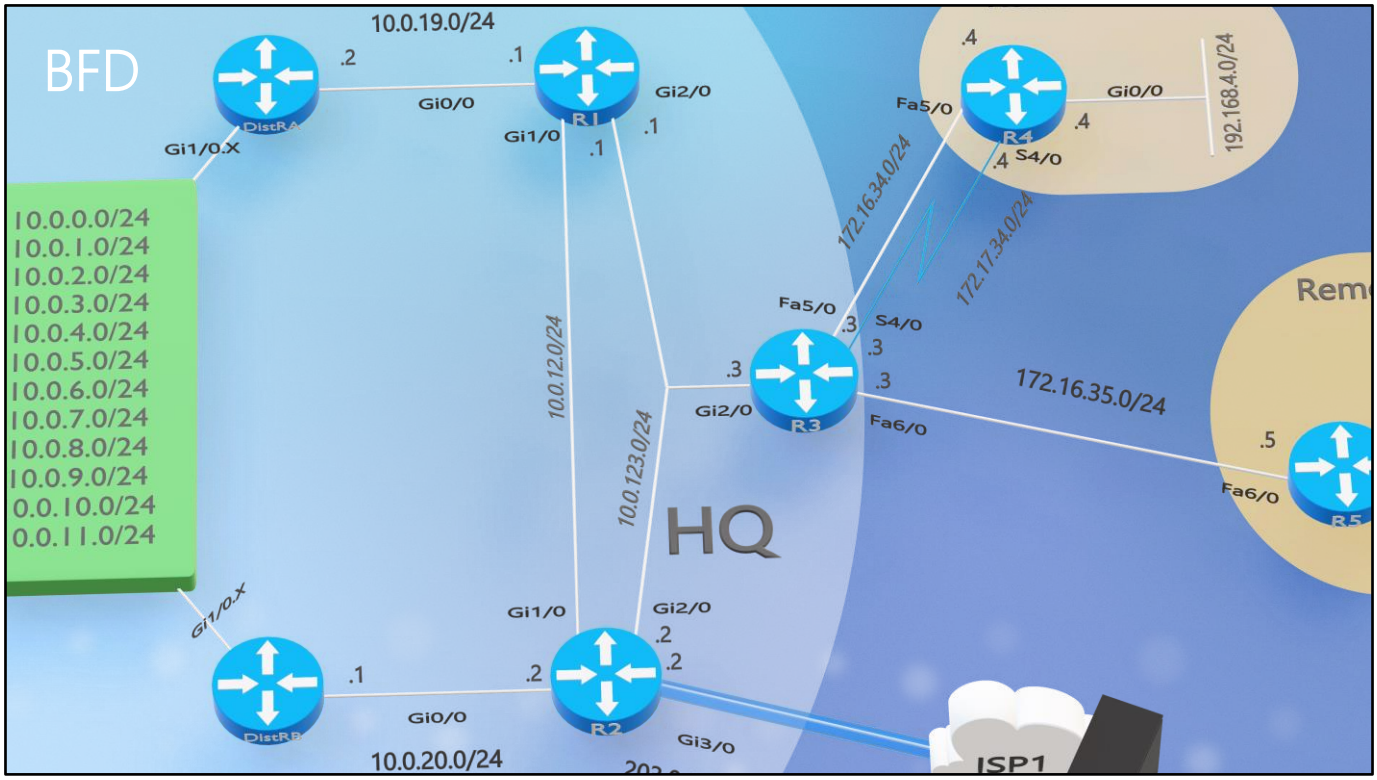
Configre BFD between R1 and R2

R1#show run int gig 1/0
Building configuration...

Current configuration : 204 bytes
!
interface GigabitEthernet1/0
bfd interval 500 min_rx 500 multiplier 3

R1#show run | s eigrp
router eigrp 100
bfd interface GigabitEthernet1/0

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Configre BFD between R1 and R2

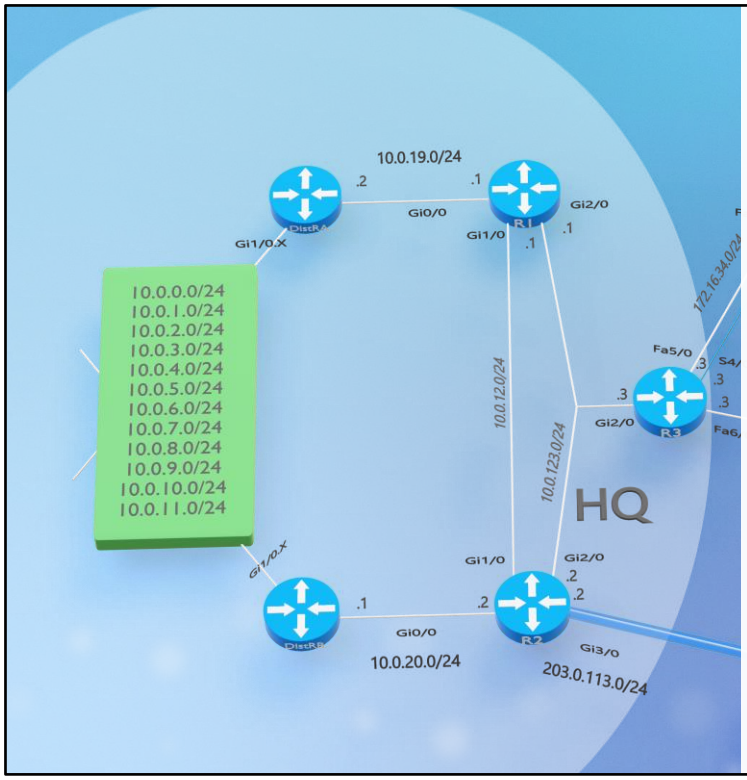
IPCEF MUST BE RUNNING

R1#show run int gig 1/0
Building configuration...

Current configuration : 204 bytes
!
interface GigabitEthernet1/0
bfd interval 500 min_rx 500 multiplier 3

R1#show run | s eigrp
router eigrp 100
bfd interface GigabitEthernet1/0

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



EIGRP Message Types

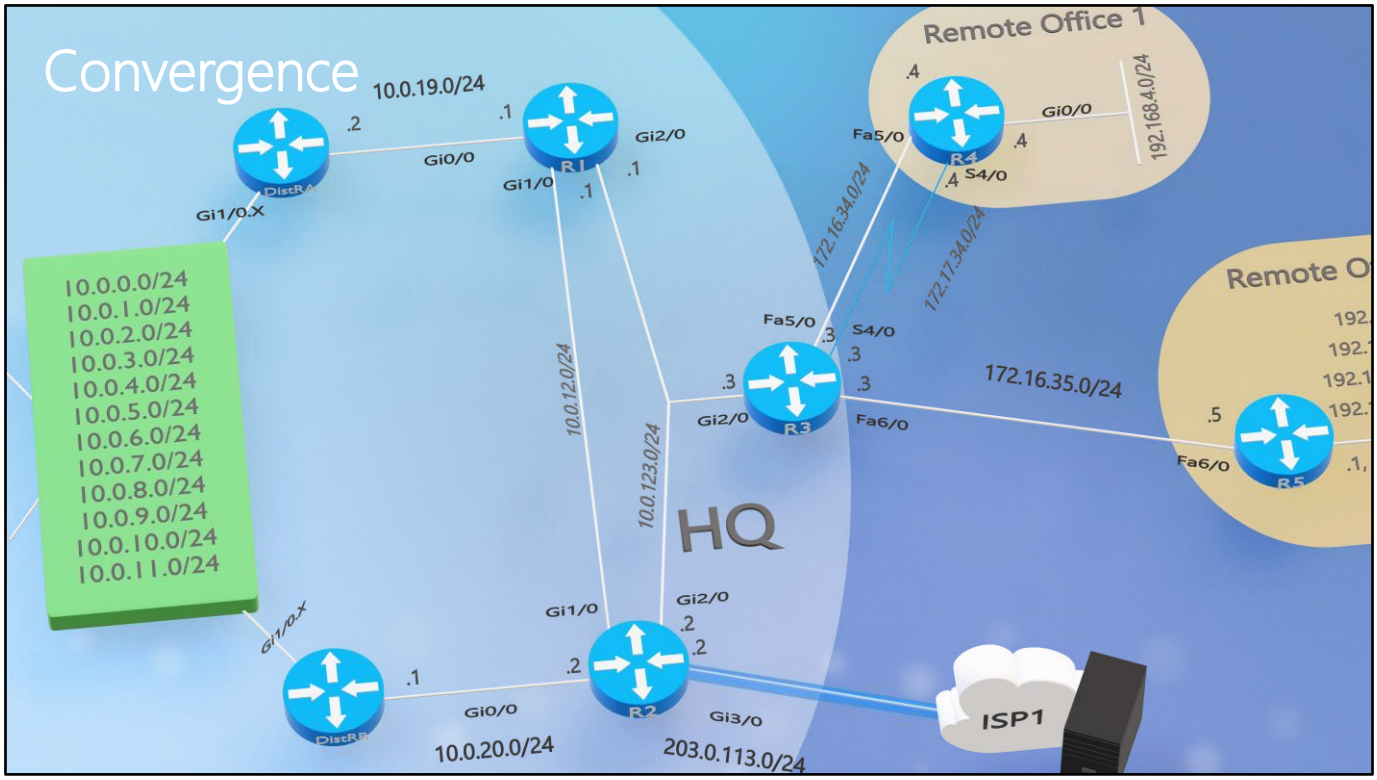
- Hello - Neighbor discovery & maintaining relationships (hello 5 / dead 15)
- Update - Link cost and/or metric changes
- Query - Sent when destinations enter active state
- Reply - Sent to origination of a Query
- ACK - Acknowledge the receipt of an EIGRP update

Commands to verify:

```
R1#debug eigrp packet
R1#show ip eigrp traffic
```

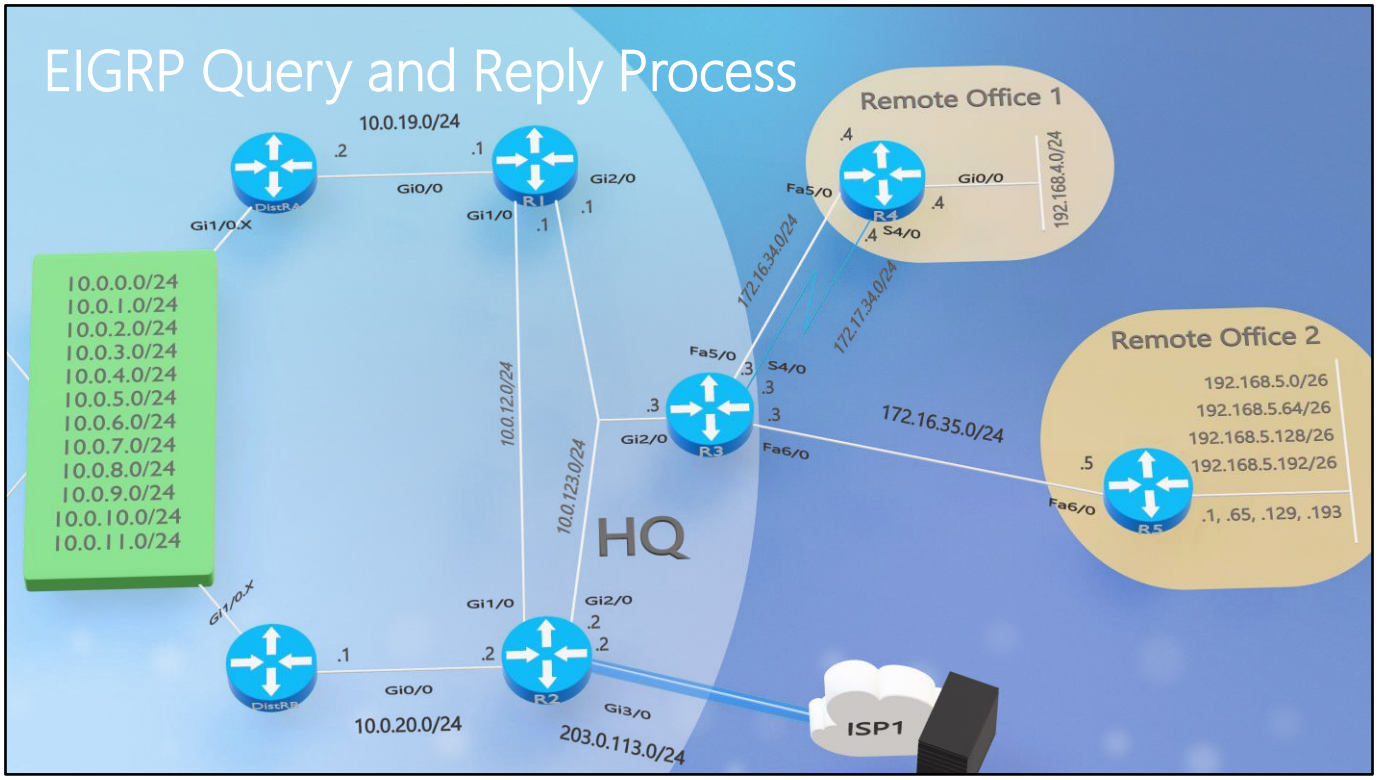
Hello is multicast
Update is unicast
Query is multicast
Reply and ack are unicast

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Let's say R1 losses it's connection to DSW1. R1 determines if there is a FS in the topology table… if there is (R2 in this case), it installs it and sends an update out the other interfaces to notify the neighbors that a change has occurred and present them with the new metrics for the calculations. The other routers will update accordingly.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



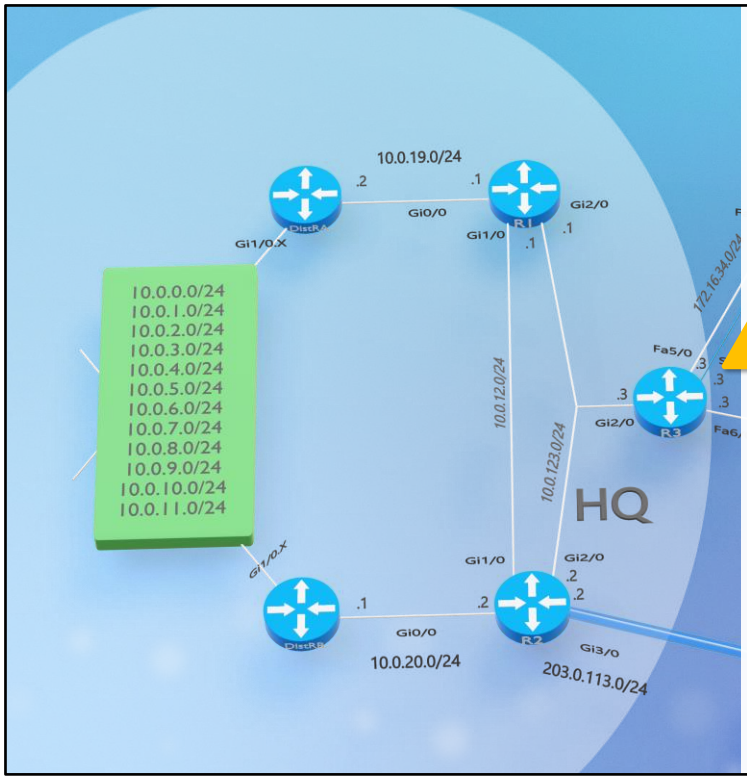
Route goes active if there is no successor or feasible successor.
A query is sent out all eigrp interfaces to neighbors to see if anyone has a path to get to the network.

if the neighbor has a single alternate path then it can reply back and the scope of the queries goes no further

if the neighbor has no alternate it will query out all its interfaces to neighbors to find out if they have a path to get to the missing network.
Once the original router gets a reply to all it's queries then the network can converge. Until then it is in the active state for that network.

If you do not get a reply for all your queries you are considered SIA.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Stuck in Active (SIA)

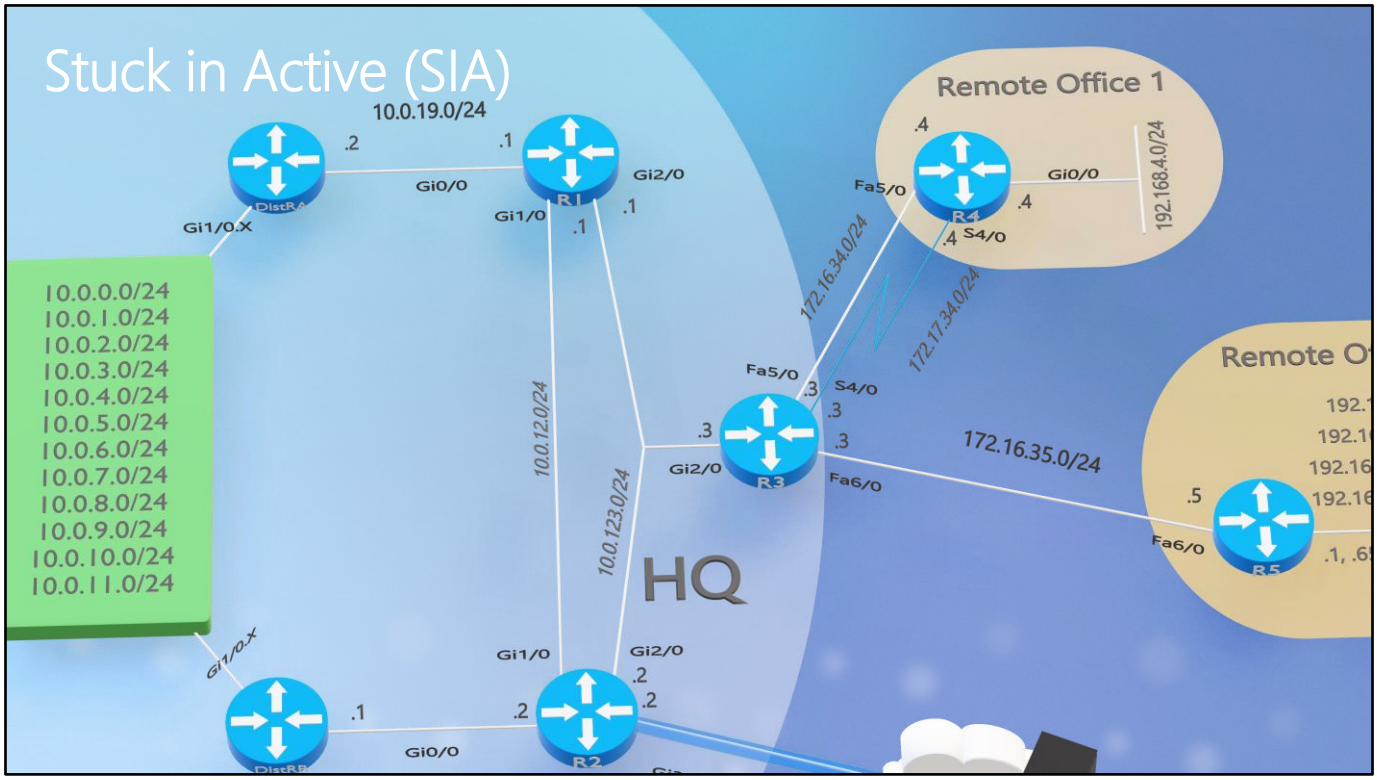
- Route will go Active if there's no Successor or Feasible Successor
- Once Active, queries sent
- Replies must be received in response to queries
- If a reply is lost, and timers expired a route is considered SIA

To view Query Process:

```
debug eigrp packets query reply
```

DUAL is very efficient at finding loop-free paths quickly, and it normally finds backup path in seconds. Occasionally, an EIGRP query is delayed because of packet loss, slow neighbors, or a large hop count. EIGRP maintains a timer, known as the active timer, which has a default value of 3 minutes (180 seconds). EIGRP waits half of the active timer value (90 seconds) for a reply. If the router does not receive a response within 90 seconds, the originating router sends a stuck in active (SIA) query to EIGRP neighbors that did not respond.

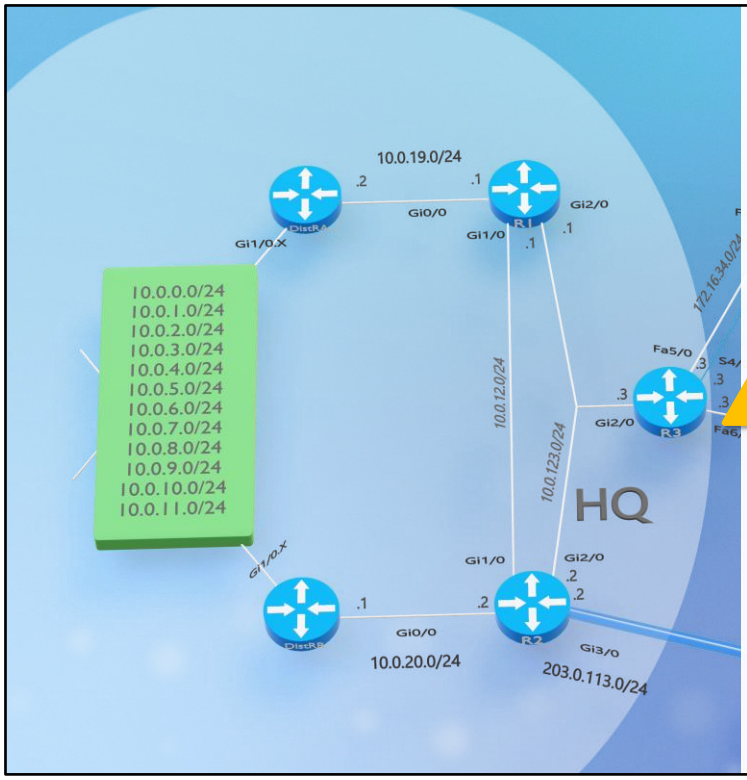
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



This can last for up to 3 minutes. Originally, once this timer expired any neighborship that existed for queries that were not responded to would get reset which means tables would be wiped of all info from that neighbor and all information would have to be relearned.

Now days we have a SIA query and reply messages. This is like the message you send to someone who has not responded to your email or text in the last 24hrs. (Hey… did you get my message?? If your friend responds you wait longer. If not you start to worry.) Well this SIA query is sent at the ½ way mark. If the neighbor router responds you know they are alive and working on their own query issues with their neighbor. If they don't respond, then you start to worry. Once the 3 mins expire any SIA reply that was returned is confirmation that the neighbor exists, and they do not have better information so the neighborship does not have to be torn down. However, any missing SIA replies indicate that the neighbor is not there and therefore the neighborship needs to be reset.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Limiting the Query Scope (EIGRP Stub)

Stub Router is not "Queried"

- Increases stability
- Reduces resource utilization

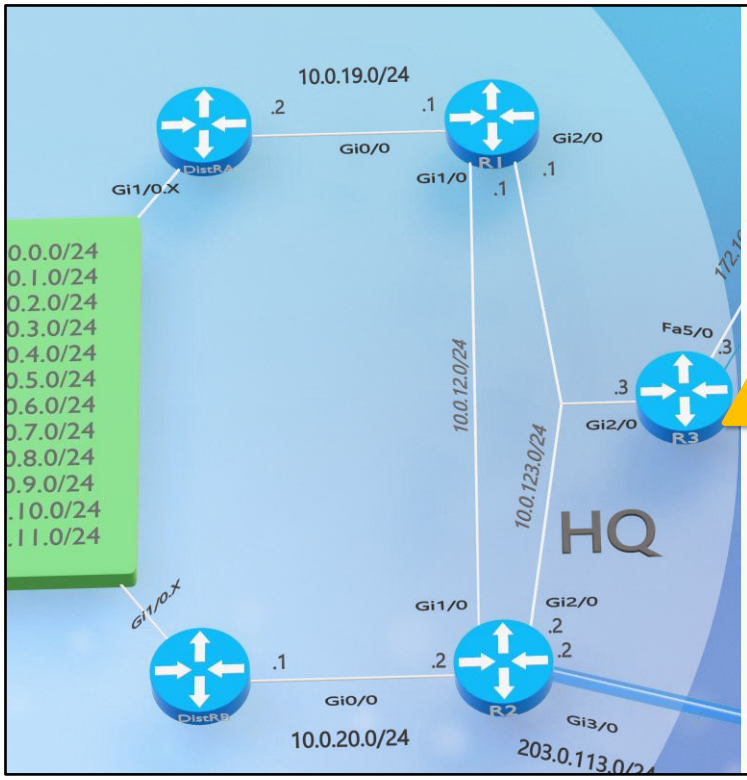
General Guidelines:

- Edge routers are configured as Stub
- Hub-n-spoke - only "spokes" should be Stubs

To Configure:

```
router eigrp 1
        eigrp stub
```

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Limiting the Query Scope (EIGRP Stub)

Stub Router is not "Queried"

- Increases stability
- Reduces resource utilization

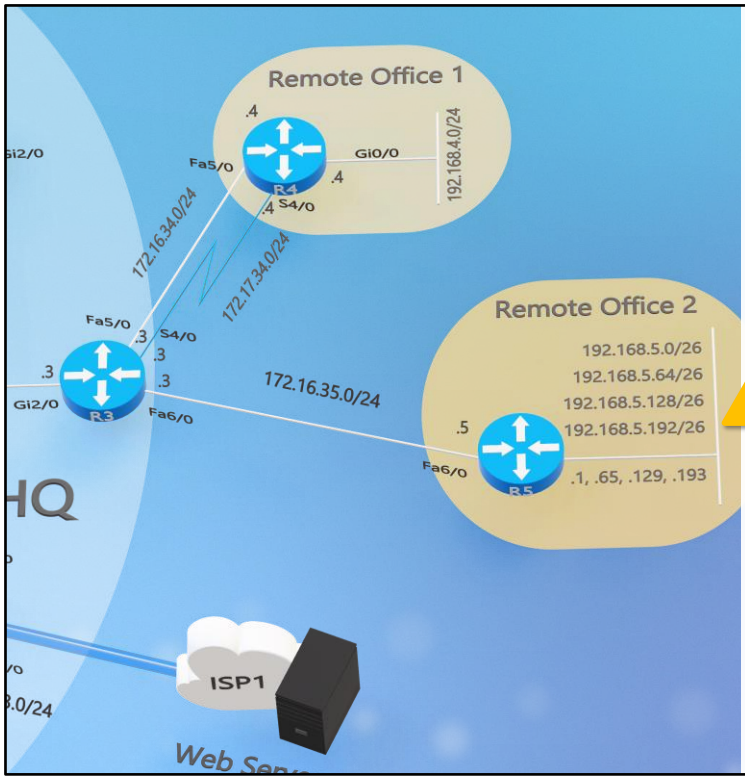
General Guidelines:

- **Edge routers are configured as Stub**
- Hub-n-spoke - only "spokes" should be Stubs

To Configure:

```
router eigrp 1
        eigrp stub
```

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

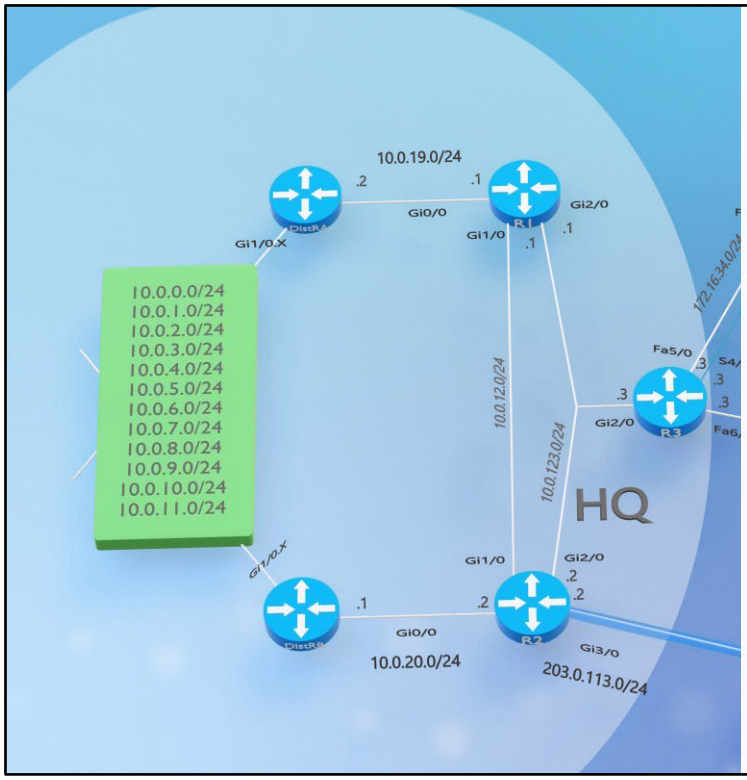


Limiting the Query Scope (EIGRP Stub)

- Stub Router is not "Queried"
  - Increases stability
  - Reduces resource utilization
- General Guidelines:
  - Edge routers are configured as Stub
  - **Hub-n-spoke - only "spokes" should be Stubs**
- **To Configure:**

```
router eigrp 1
        eigrp stub
```

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Limiting the Query Scope (EIGRP Stub)

Stub Options:

```
router eigrp 1
        eigrp stub
```

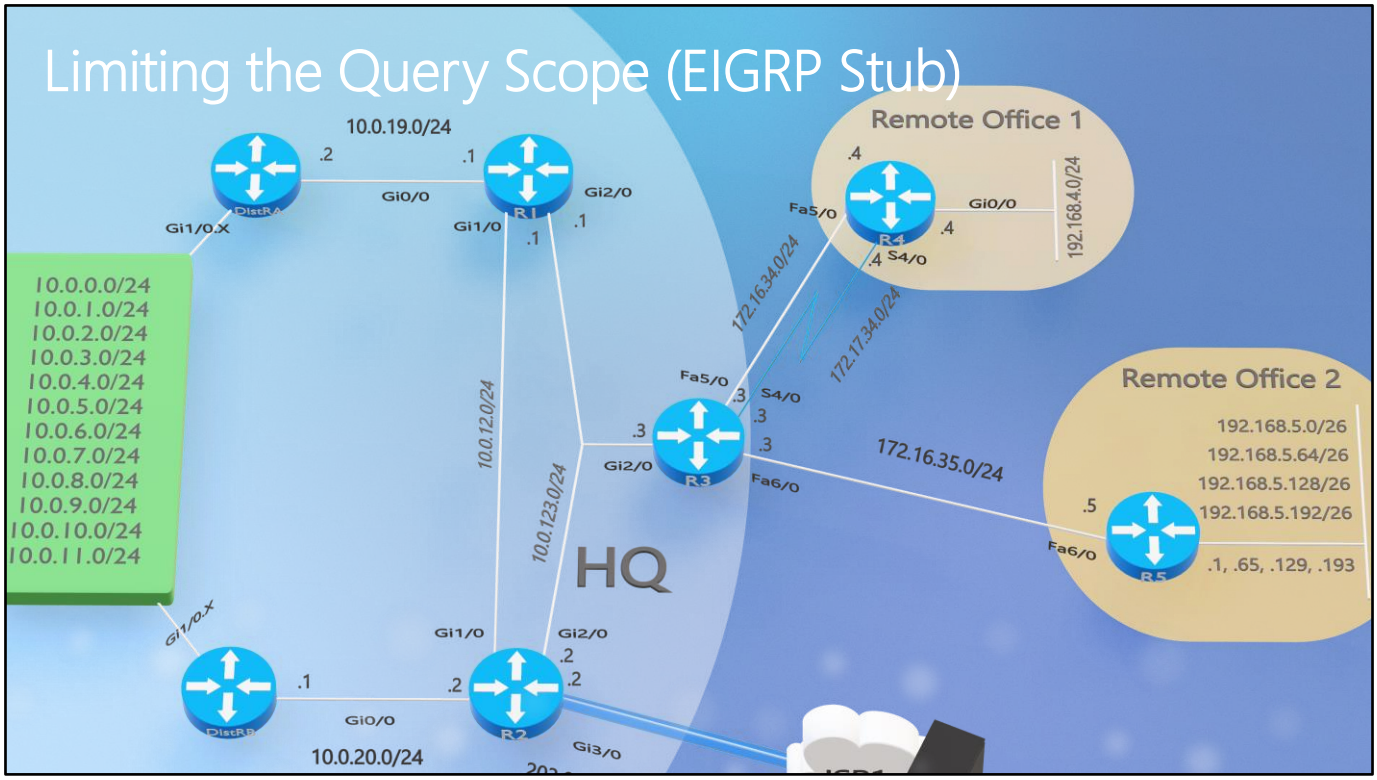
- ***Connected***: advertises connected routes (default)
- ***Summary***: advertises any configured summary routes (default)
- ***Redistribute***: advertises redistributed routes
- ***Receive-only***: prevents stub from sending any routes
- ***Static***: advertises static routes, only when redistribute static is configured

Verify:

```
show ip eigrp neighbors detail
Show ip protocols
```

With the command we just saw: **`eigrp stub`** `EIGRP will advertise any connected and summary routes`

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

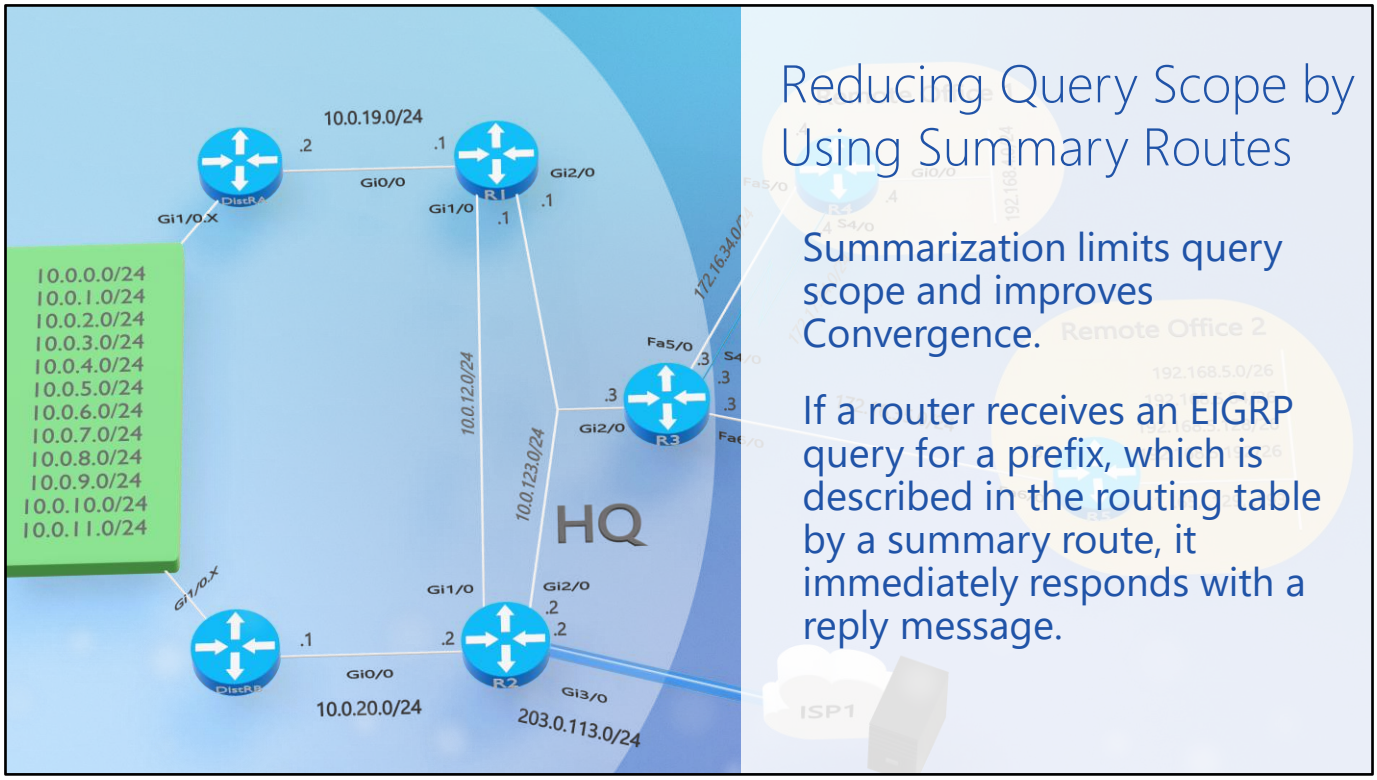


DEMO EIGRP STUB ON R3 and R5

What would happen if R3 configured as EIGRP stub?

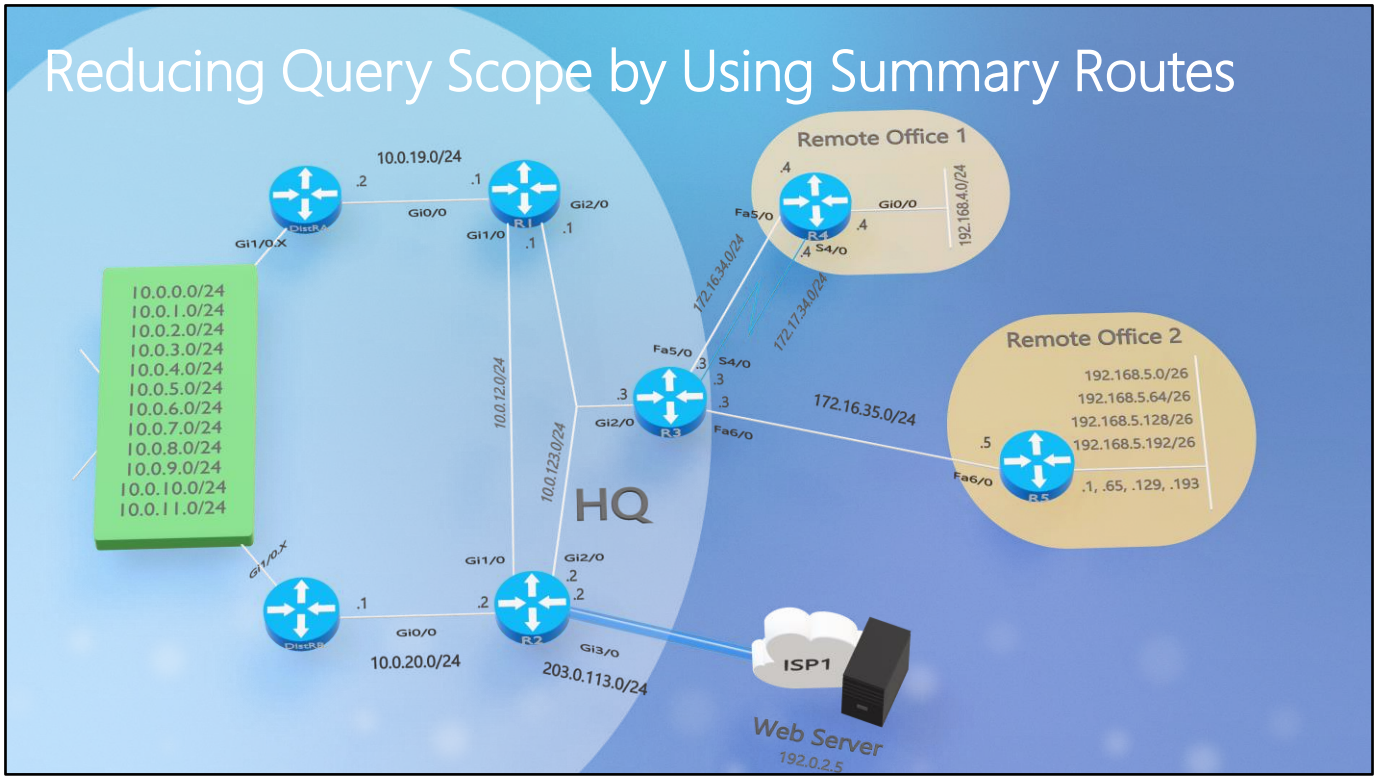
R5 and R3 would only get the connected and summary routes of R3 which means many routes would be missing on R4 and R5. The rule is to configure the end devices with EIGRP stub. So the branch routers. You could also do the distribution routers. Many access/dist MLSs have this feature enabled by default because they would not have a valid alternate path to the destination that is being queried.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



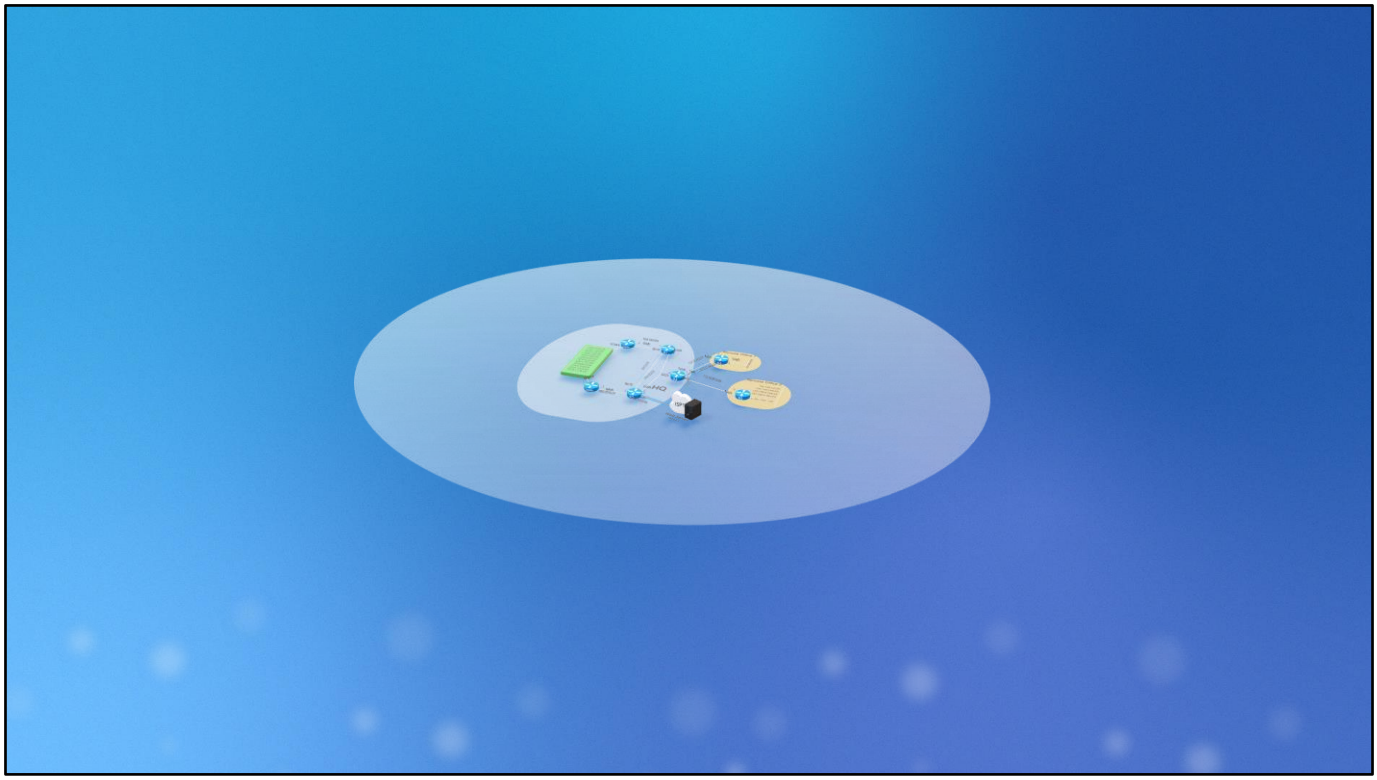
R5 sends summary to R3. R5 looses route to 192.168.5.0/26. R5 queries R3. R3 has a summary for 192.168.5.0/24 and therefore responds back to the query with a reply. So the query is prevented from propagating to the other routers in this case.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



R5 sends summary to R3. R5 looses route to 192.168.5.0/26. R5 queries R3. R3 has a summary for 192.168.5.0/24 and therefore responds back to the query with a reply. So the query is prevented from propagating to the other routers in this case.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

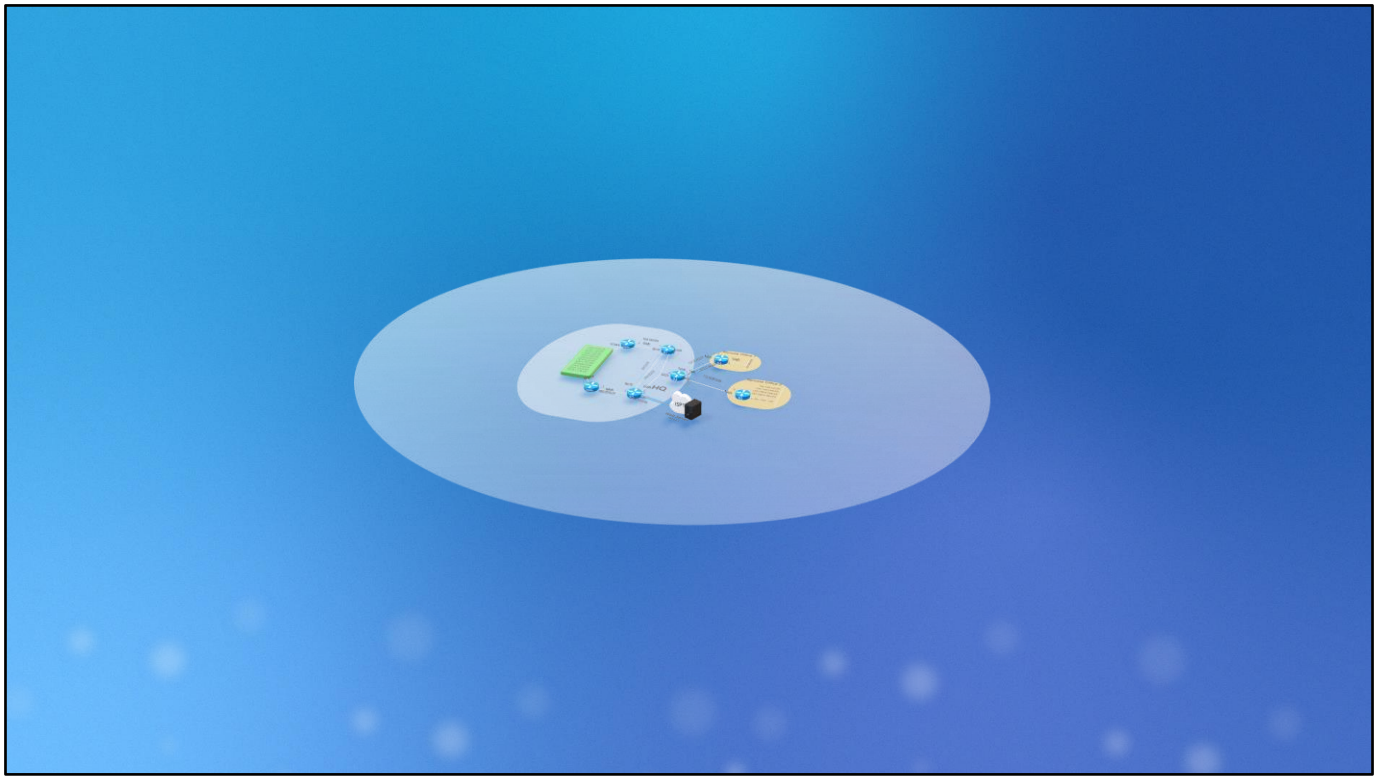


R5 sends summary to R3. R5 looses route to 192.168.5.0/26. R5 queries R3. R3 has a summary for 192.168.5.0/24 and therefore responds back to the query with a reply. So the query is prevented from propagating to the other routers in this case.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

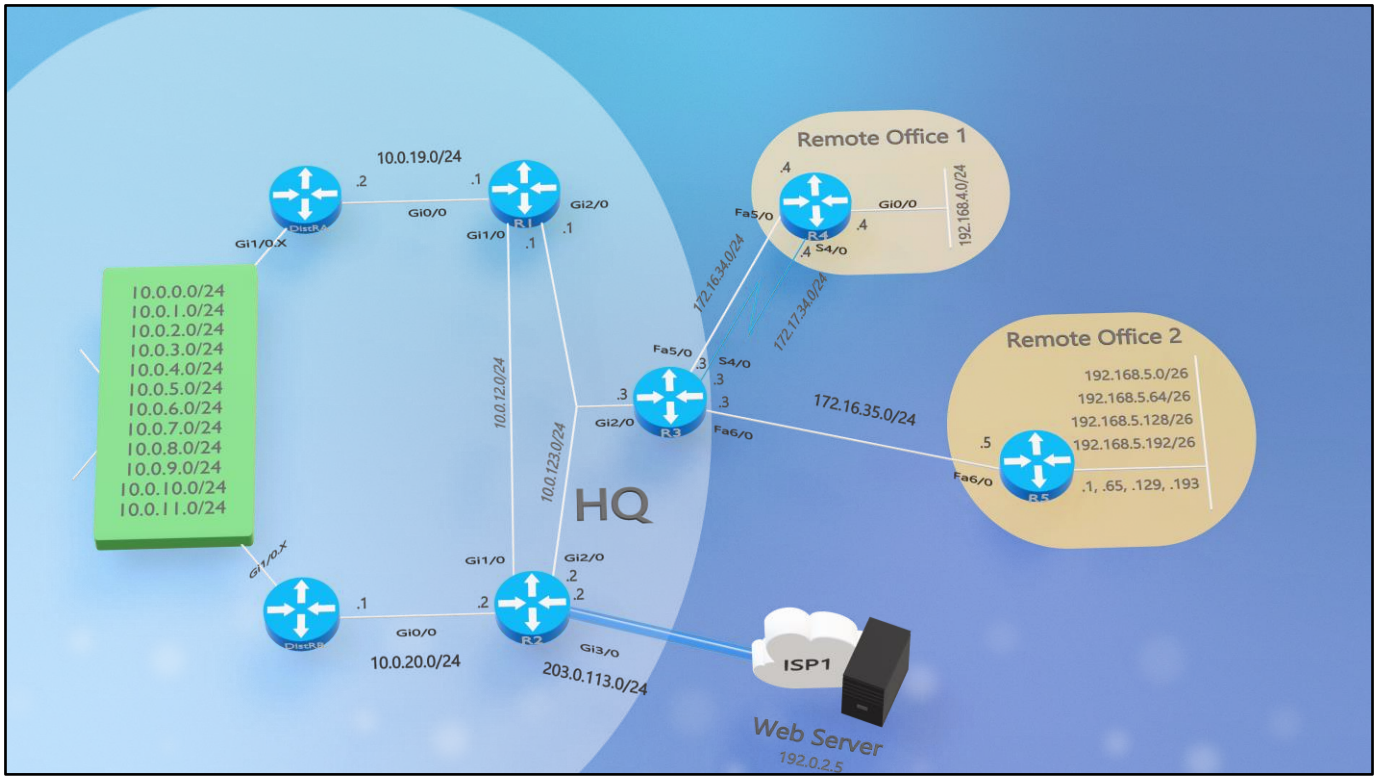


©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



R5 sends summary to R3. R5 looses route to 192.168.5.0/26. R5 queries R3. R3 has a summary for 192.168.5.0/24 and therefore responds back to the query with a reply. So the query is prevented from propagating to the other routers in this case.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

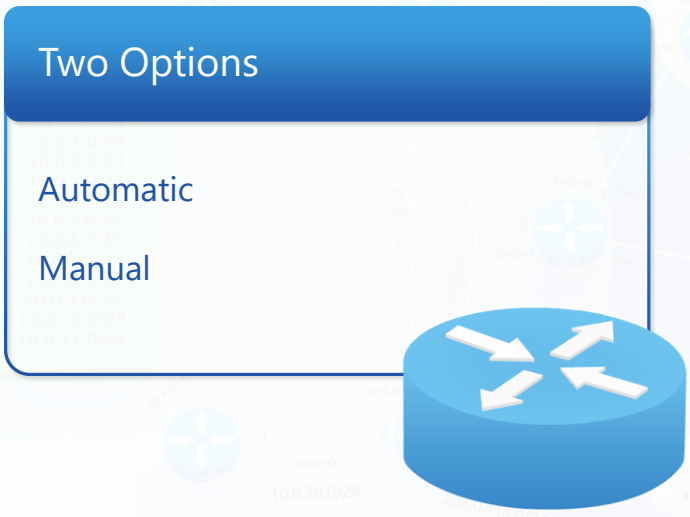


So… with Summarization we can reduce query scope and improve convergence time but we can also…

Improve resource utilization by reducing the size of the topology table and the routing table.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Summarization



So… with Summarization we can reduce query scope and improve convergence time but we can also…

Improve resource utilization by reducing the size of the topology table and the routing table.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

EIGRP Auto Summarization

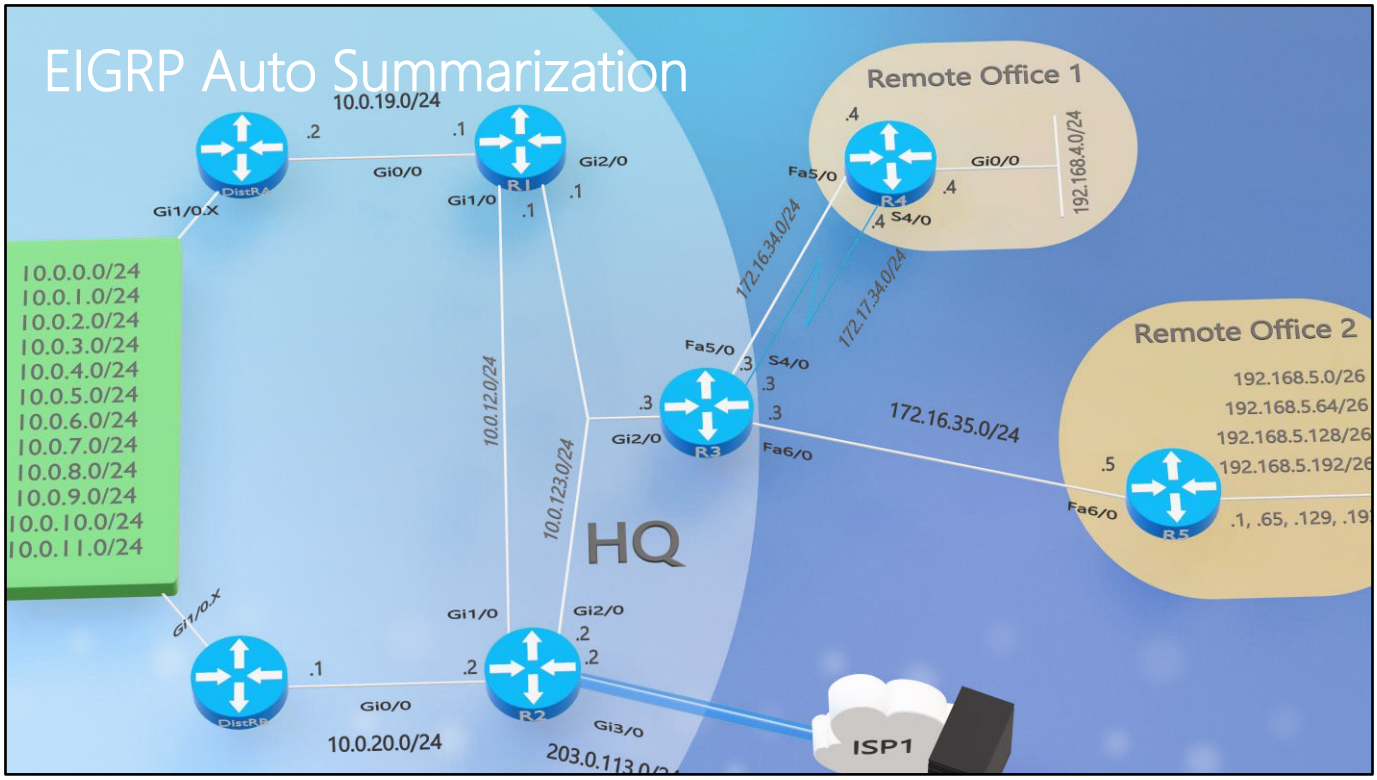
Auto Summarization

Disabled by default on IOS version 15.0 and later

Automatically sends the classful subnet mask with classful prefix when configured



©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

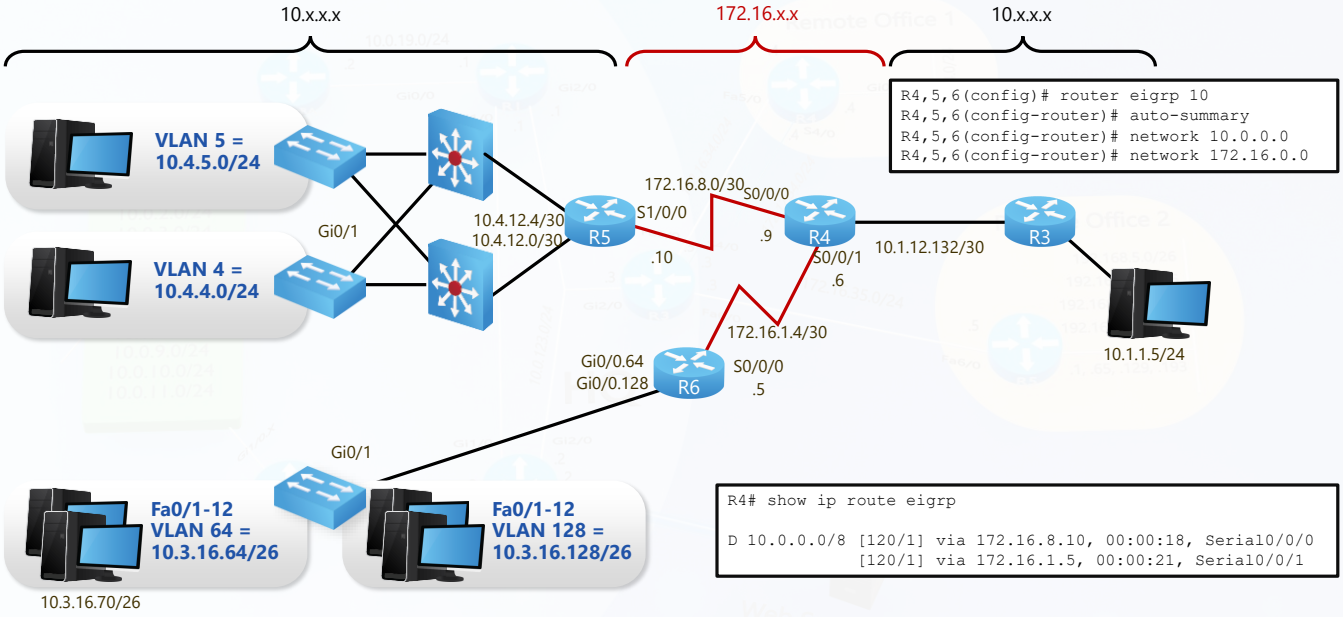


Demo Auto Summarization
Turn on auto summary on R3. Notice how R4 and R5 get 10.0.0.0/8 and R1 and R2 get 172.16.0.0/16.

When can this be a problem?????
With a discontiguous network.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

EIGRP Auto Summarization

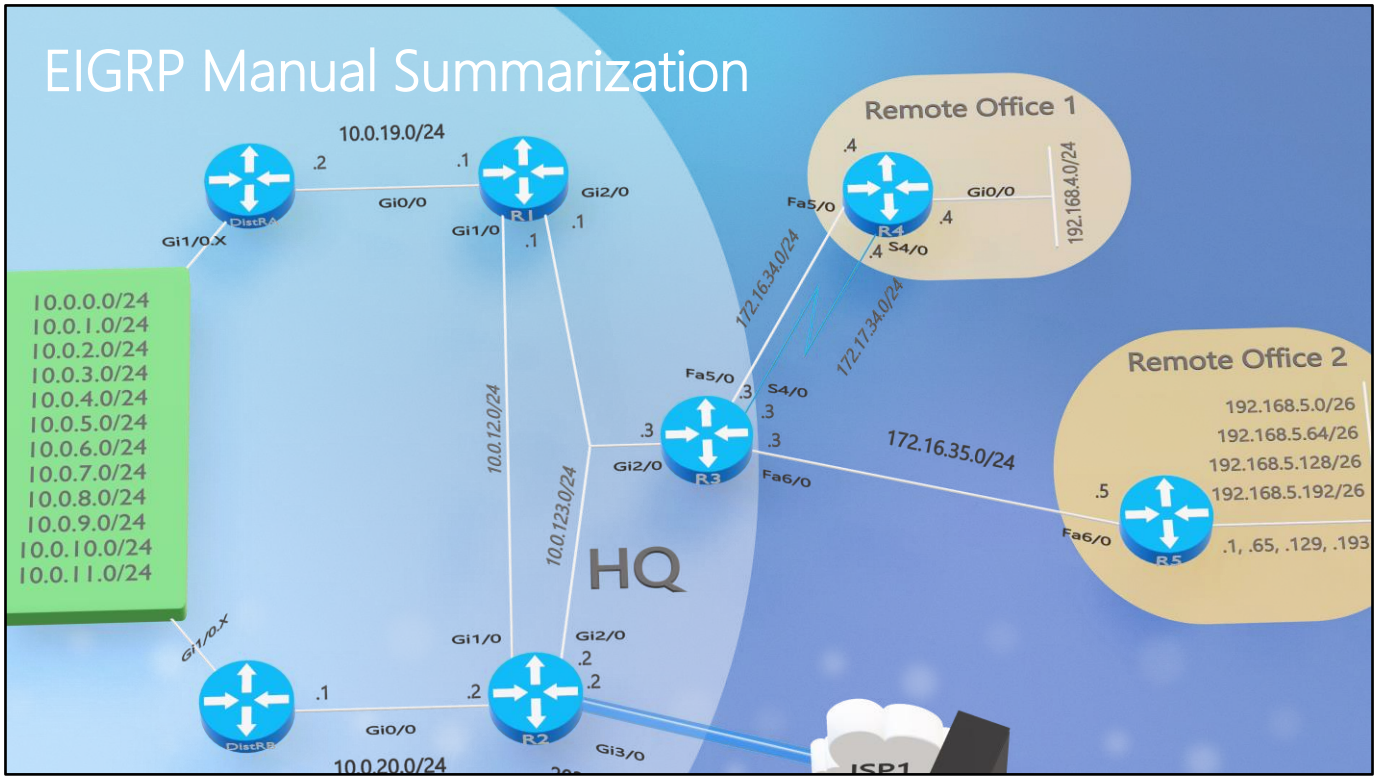



```
R4,5,6(config)# router eigrp 10
R4,5,6(config-router)# auto-summary
R4,5,6(config-router)# network 10.0.0.0
R4,5,6(config-router)# network 172.16.0.0
```

```
R4# show ip route eigrp

D 10.0.0.0/8 [120/1] via 172.16.8.10, 00:00:18, Serial0/0/0
             [120/1] via 172.16.1.5, 00:00:21, Serial0/0/1
```

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



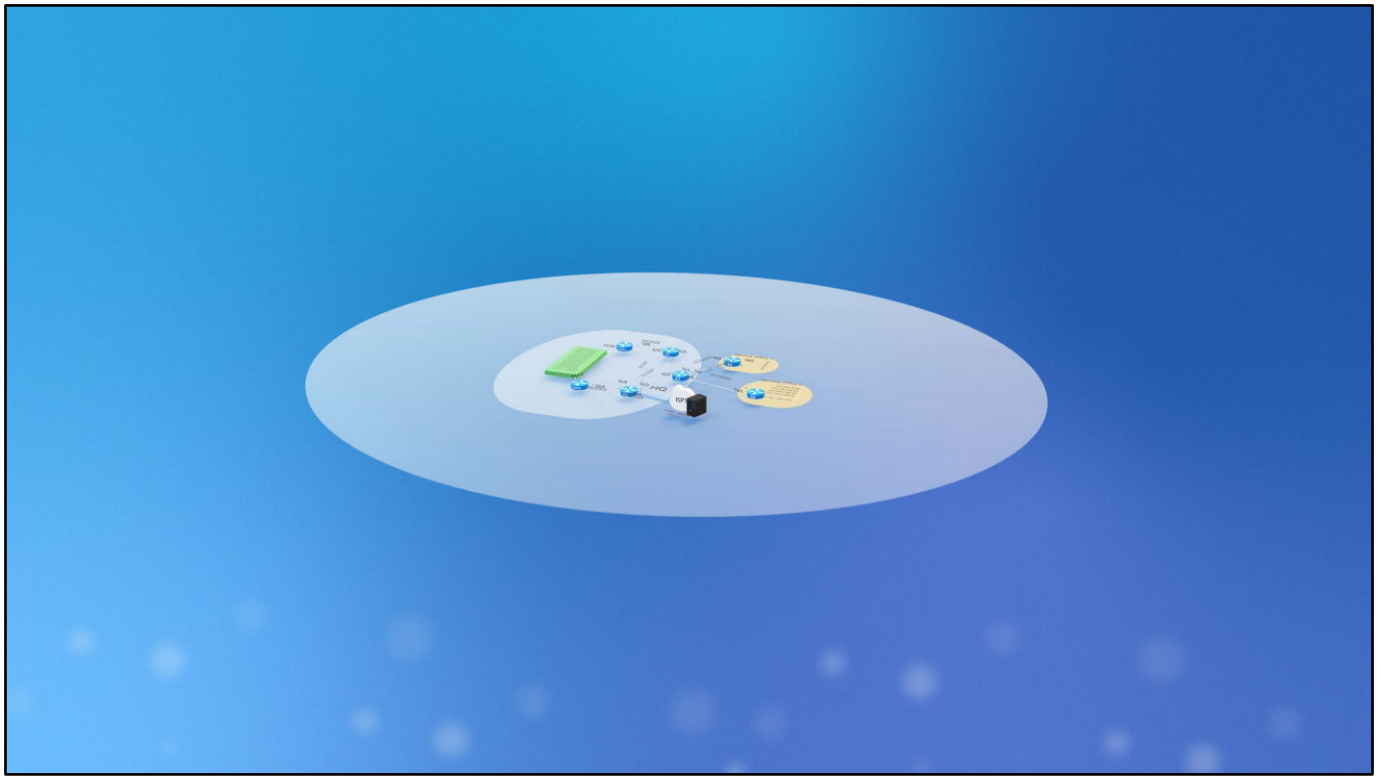
1) We could summarize from R5 to R3.
2) We could summarize from DSW1 and 2 out or R3 out to R4 and R5.

How do we figure out the summary address… binary…
192.168.5.00000000
192.168.5.11000000
Where do the common bits end?
That is the new mask.
Append it to the first address.

How do we figure out the summary address… binary…
10.0.0.0 = 10.0.00000000.0
10.0.11.0 = 10.0.00001011.0
Where do the common bits end?
That is the new mask.
Append it to the first address.

DON'T FORGET ABOUT A SUMMARY OF 0.0.0.0/0 from r3 to r5

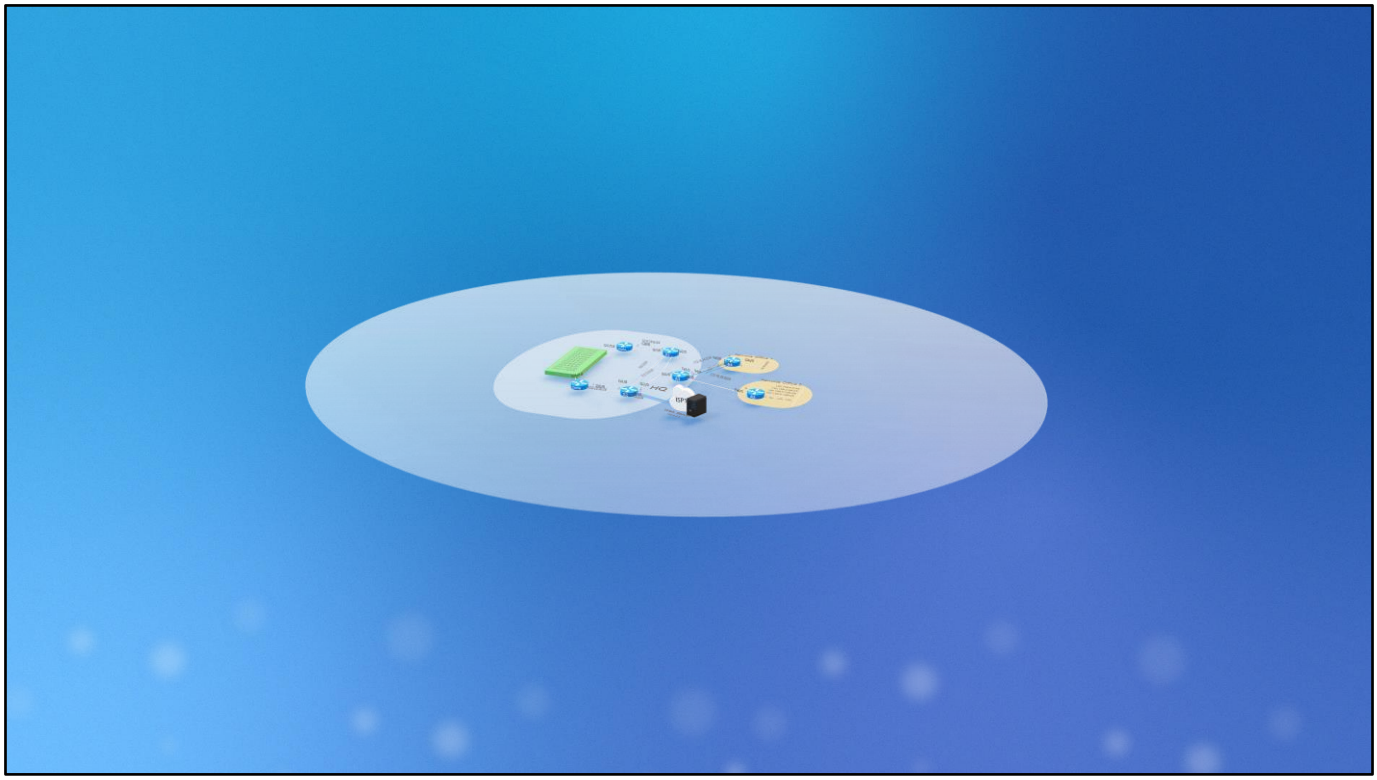
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



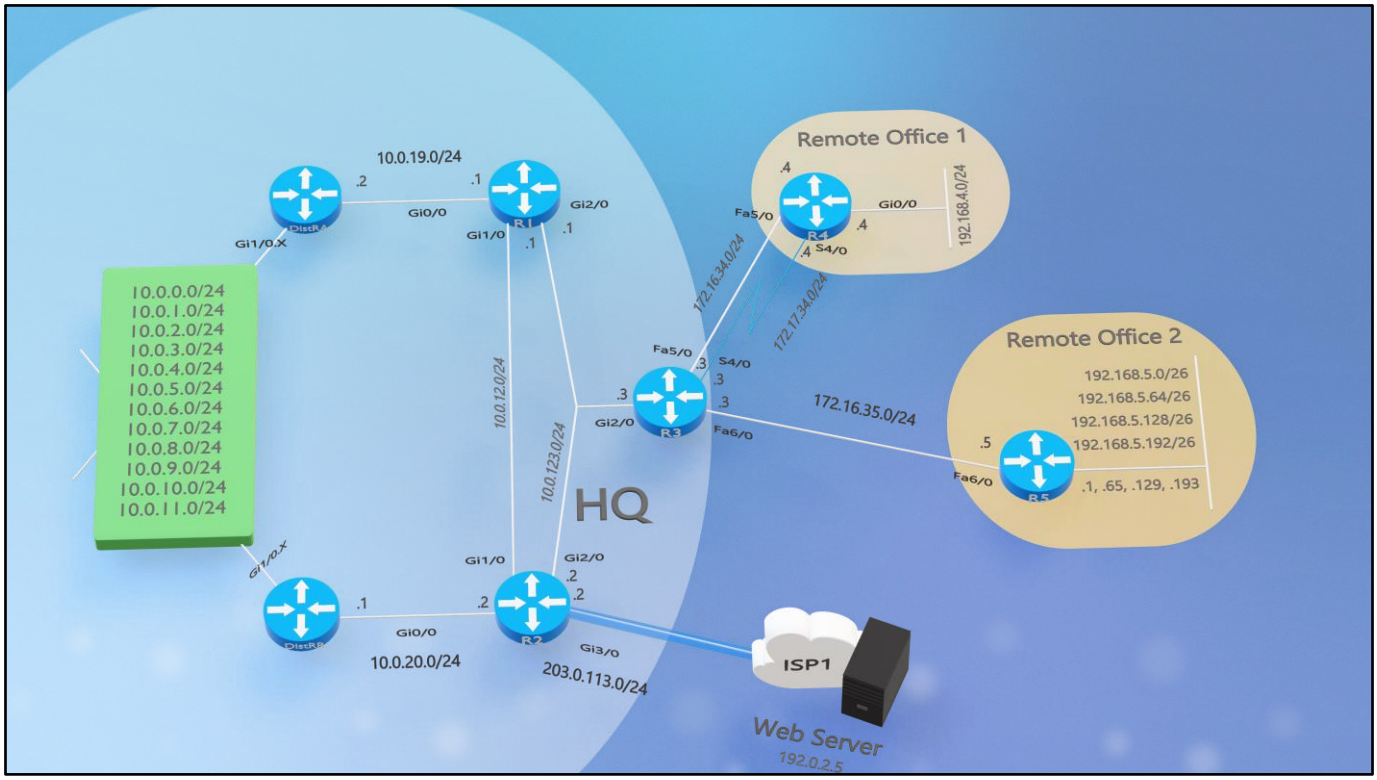
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

ROUTE Manipulation

Route Filter (Distribute List)

Control the updates that are sent or received from neighboring routers

- Inbound or Outbound on any EIGRP enabled interface

Traffic Steering (Offset List)

Control the path that is taken by modifying the metric

- Inbound or Outbound on any EIGRP enabled interface

Traffic Steering (AD)

Control the path that is taken by modifying the AD

- Inbound on any EIGRP enabled interface

ALSO Using Summarization

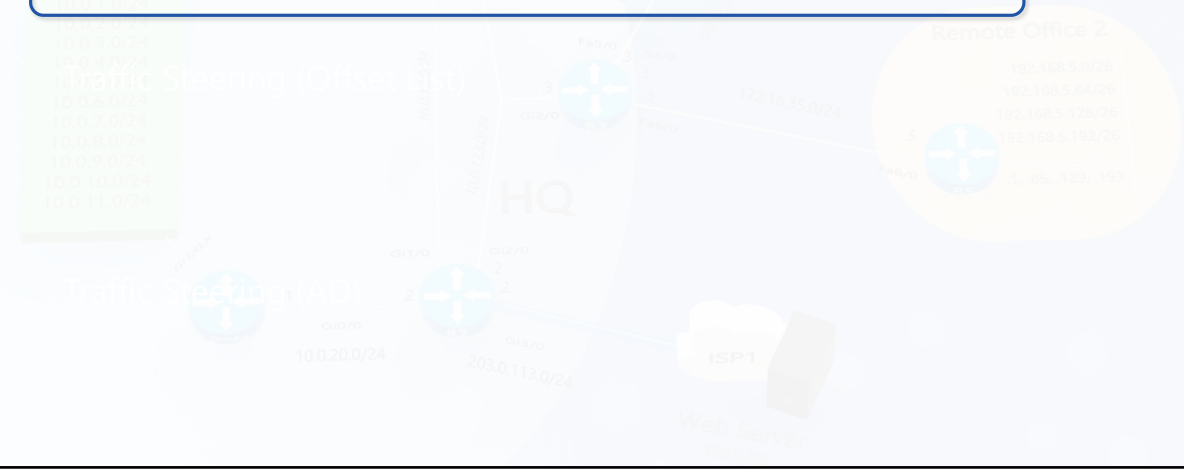
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

ROUTE Manipulation (cont…)

Traffic Steering (Summarization)

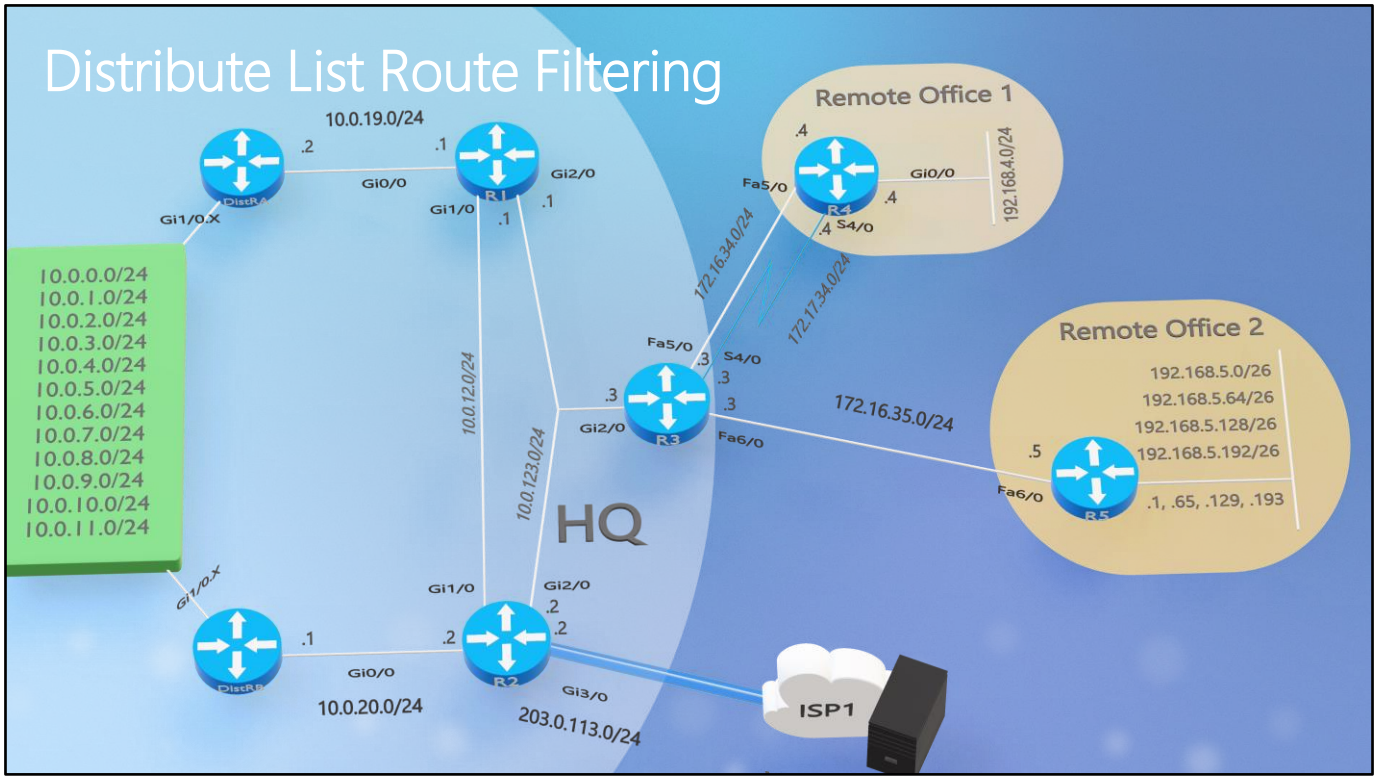
Control the path that is taken by using the longest match rule

- Outbound on any EIGRP enabled interface



ALSO Using Summarization

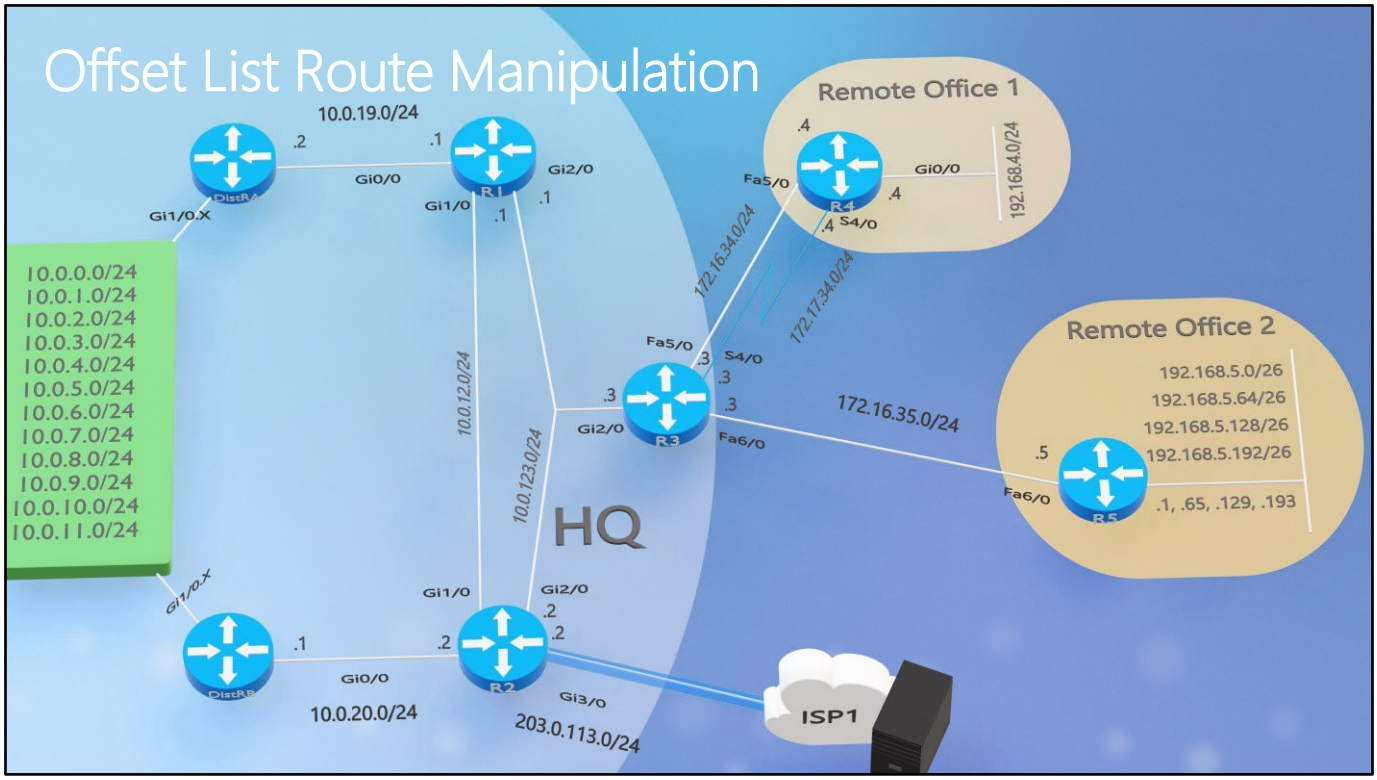
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



On R1
Ip prefixlist FILTER deny 192.168.4.0/24
Ip prefix list FILTER permit 0.0.0.0/0 le 32

Ditribute-list prefix FILTER in gig 2/0

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



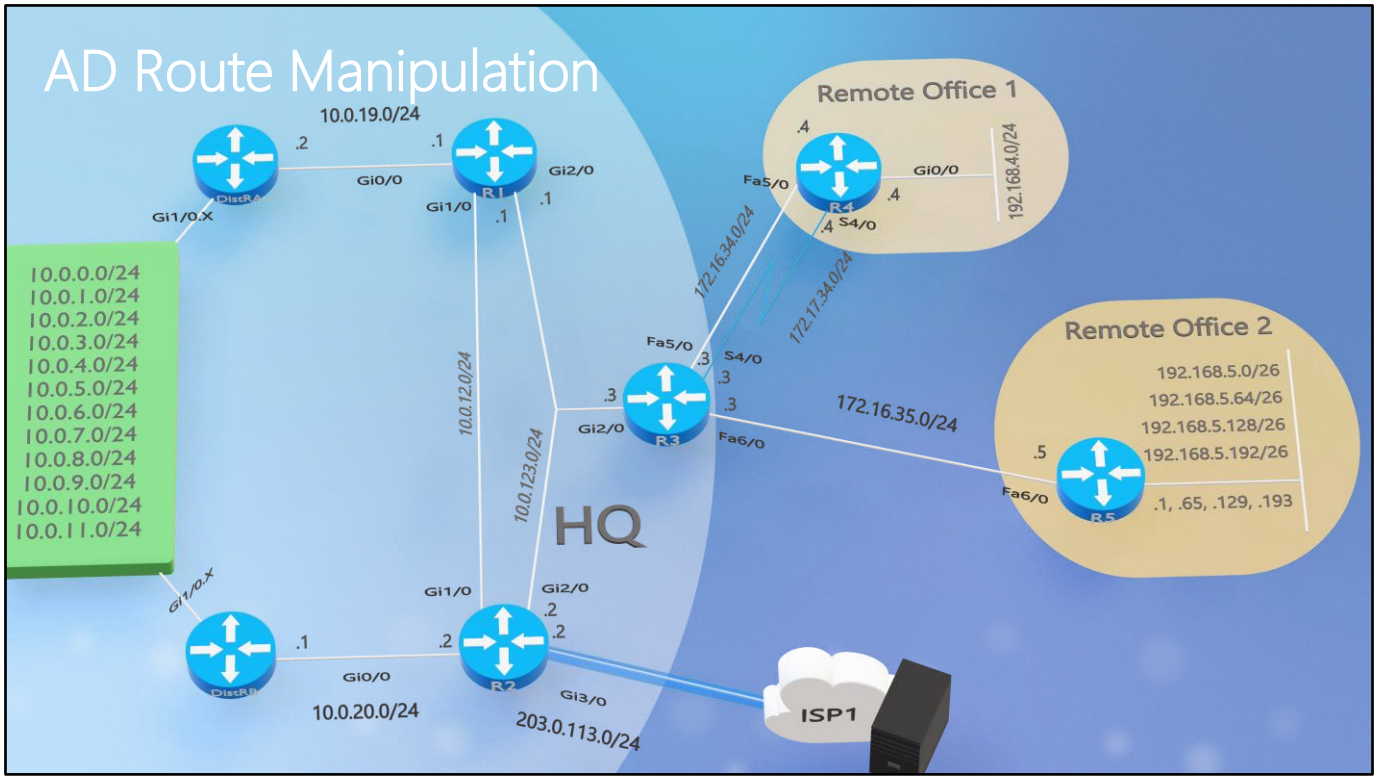
Show ip route
Show ip eigrp topology

R1 uses r3 to get to R4
Offset incoming from R3 so that R1 uses R2.

R1#show access-lists
Standard IP access list EIGRPOFFSET
10 permit 192.168.4.0 (3 matches)

R1(config-router)#offset-list EIGRPOFFSET in 1000000000 gigabitEthernet 2/0

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

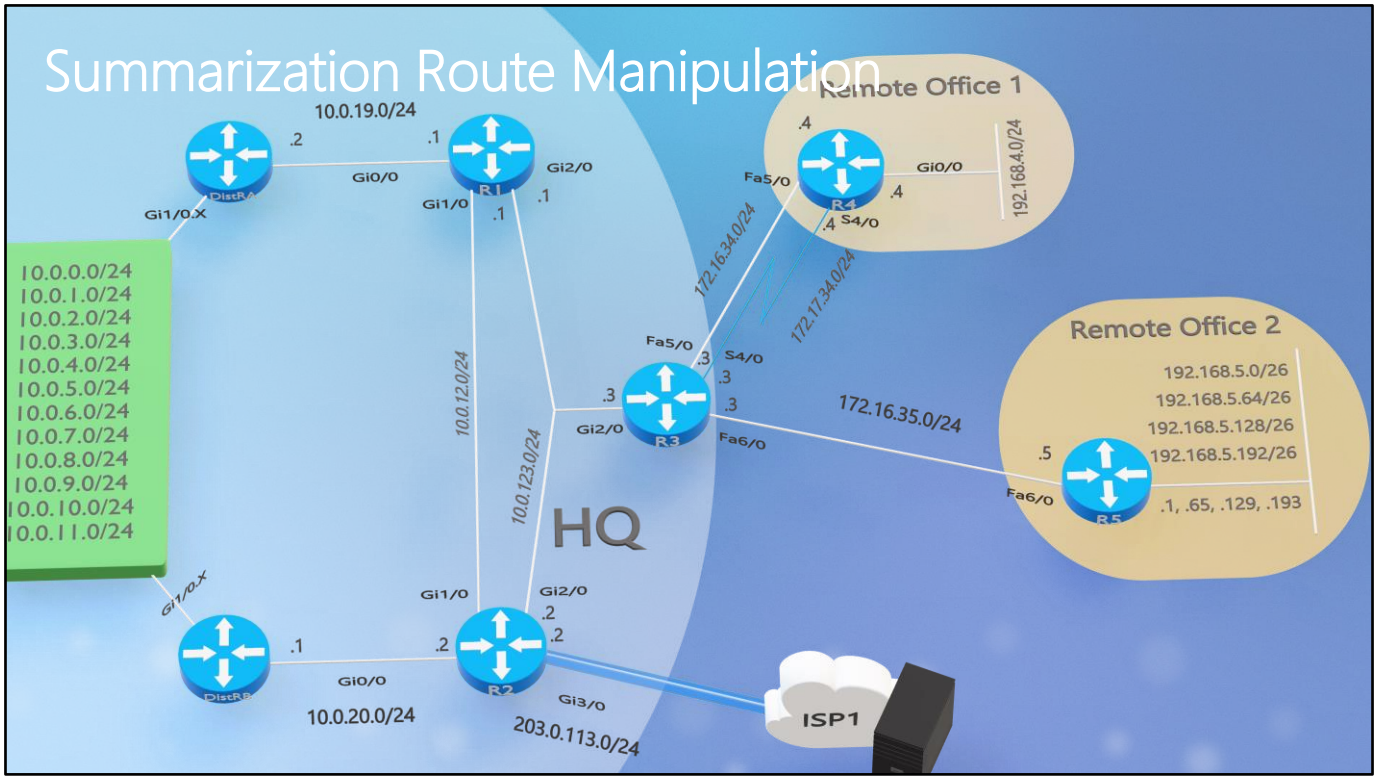


DEMO: AD route manipulation

distance eigrp 90 170 would affect all routes learned from all neighbors

distance 95 10.0.123.3 0.0.0.0 would affect routes only learned from that neighbor. (only works with internal routes)

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

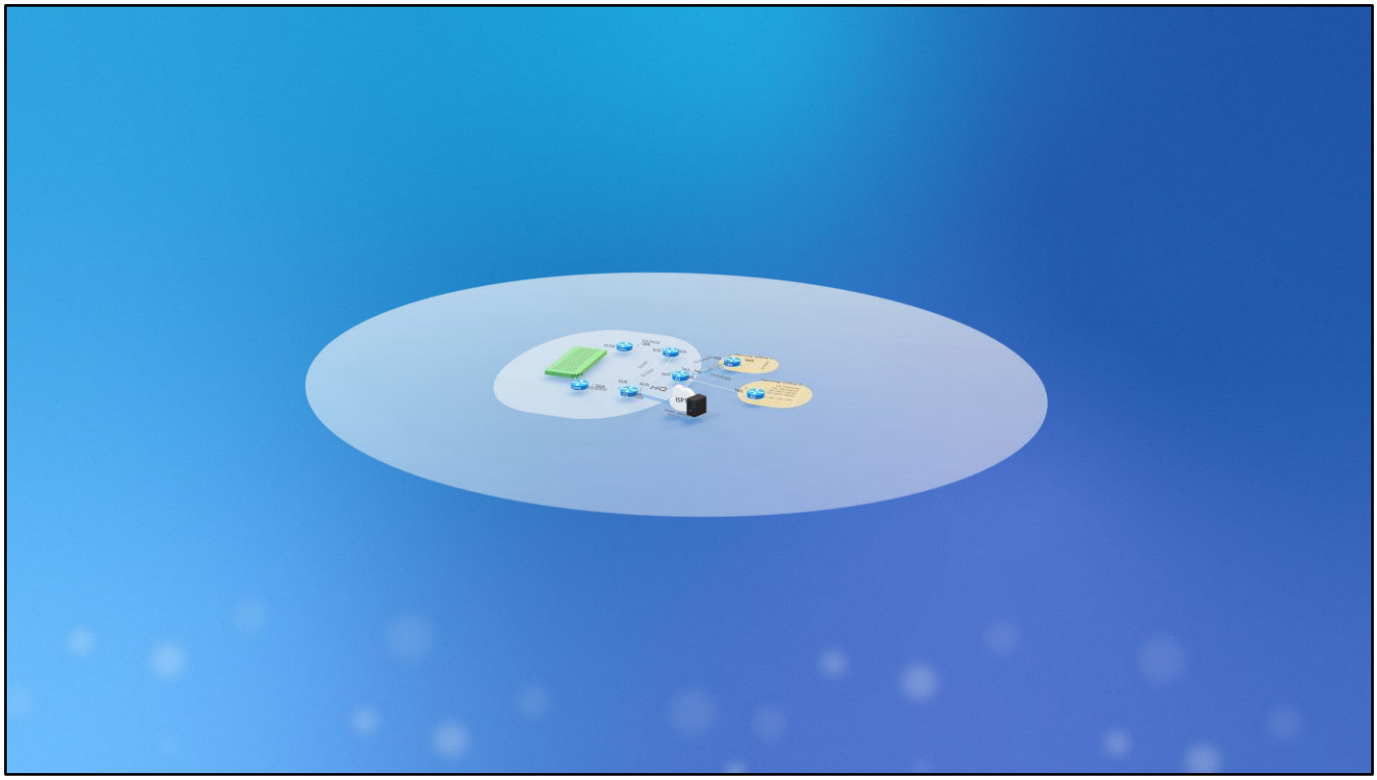


Configure DISTRA with summary but not DISTRB.

Therefore DISTRB advertises specific routes and DISTRA advertises summary

Longest match rule wins.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Troubleshooting Neighbor Adjacencies

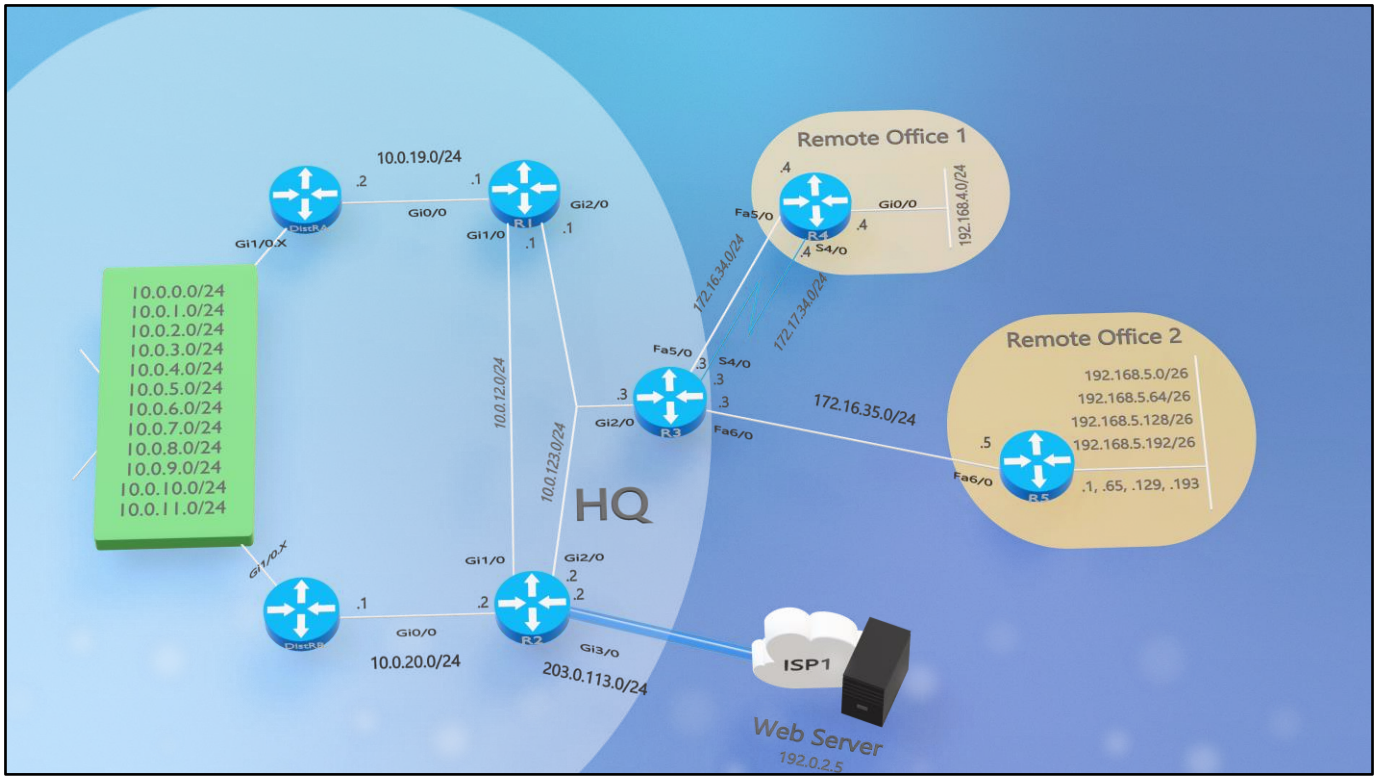


- Interface must be up/up
- Autonomous System numbers must match
- The interface must be participating in the routing process
- K values must match
- Interface can't be passive
- Interfaces must be in the same subnet
- Authentication parameters must match
- Inbound interface ACLs must be permitting EIGRP packets
- Timers must be configured correctly.*

What must be true in order to form an EIGRP neighborship????

*** They don't have to match… but if they are skewed enough the neighborship will flap.**

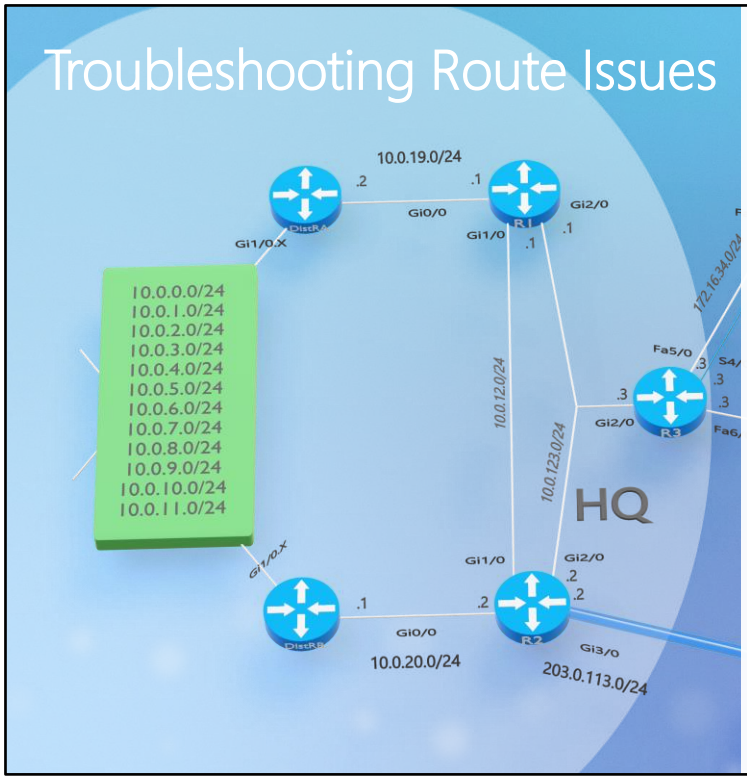
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



What must be true in order to form an EIGRP neighborship????

*** They don't have to match… but if they are skewed enough the neighborship will flap.**

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

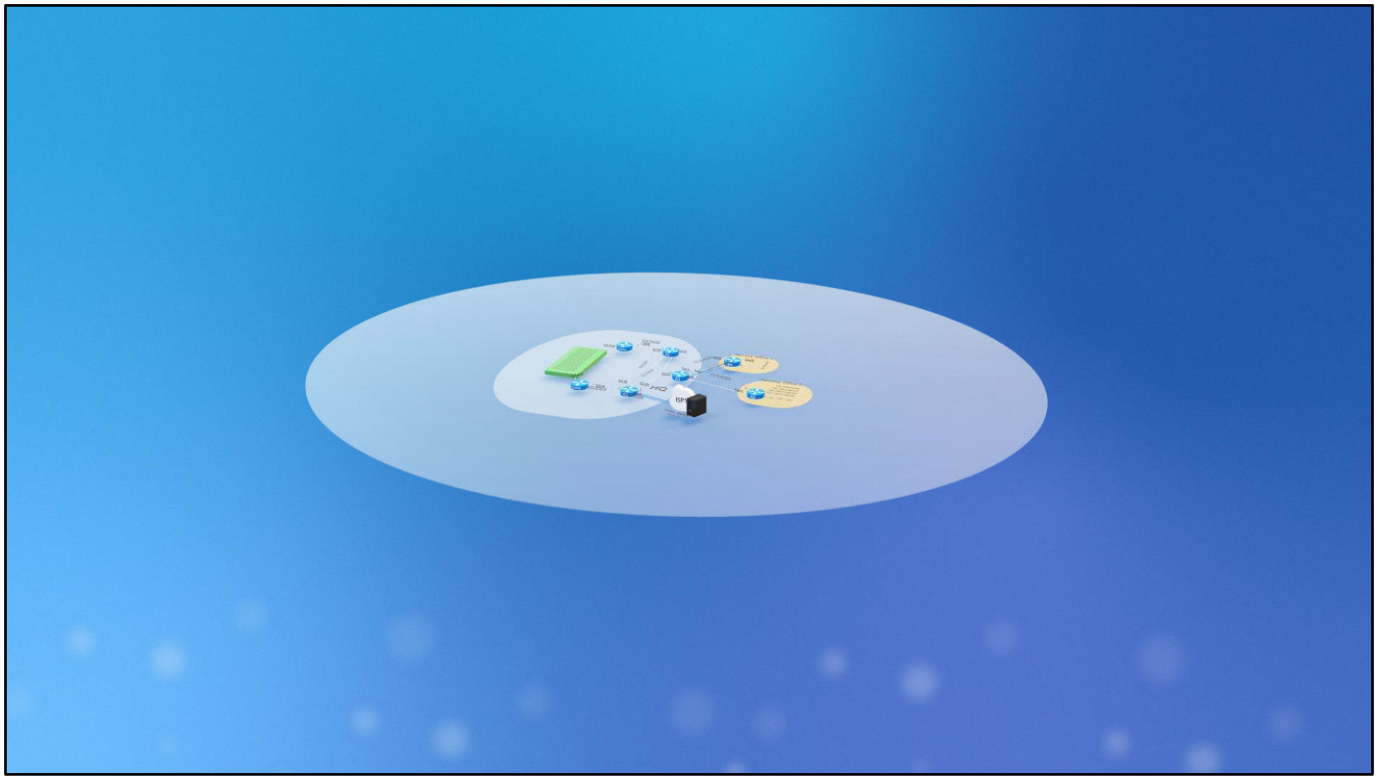


- Bad or missing network command
- Better source of information
- Route filtering
- Offset Lists
- Stub configuration
- Interface is shut down
- Split horizon

What must be true in order to form an EIGRP neighborship????

*** They don't have to match… but if they are skewed enough the neighborship will flap.**

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

EIGRPv4 vs EIGRPv6

Feature	EIGRPv4	EIGRPv6
Layer 3 protocol for EIGRP messages	IPv4	IPv6
Reserved multicast address	224.0.0.10	FF02::A
Concept of the link-local address to establish EIGRP neighbor relationship	No	Yes
Layer 3 header protocol type	88	88
Uses composite metric, by default uses bandwidth and delay	Yes	Yes
Uses successor, feasible successor	Yes	Yes
Router ID format	IPv4	IPv4

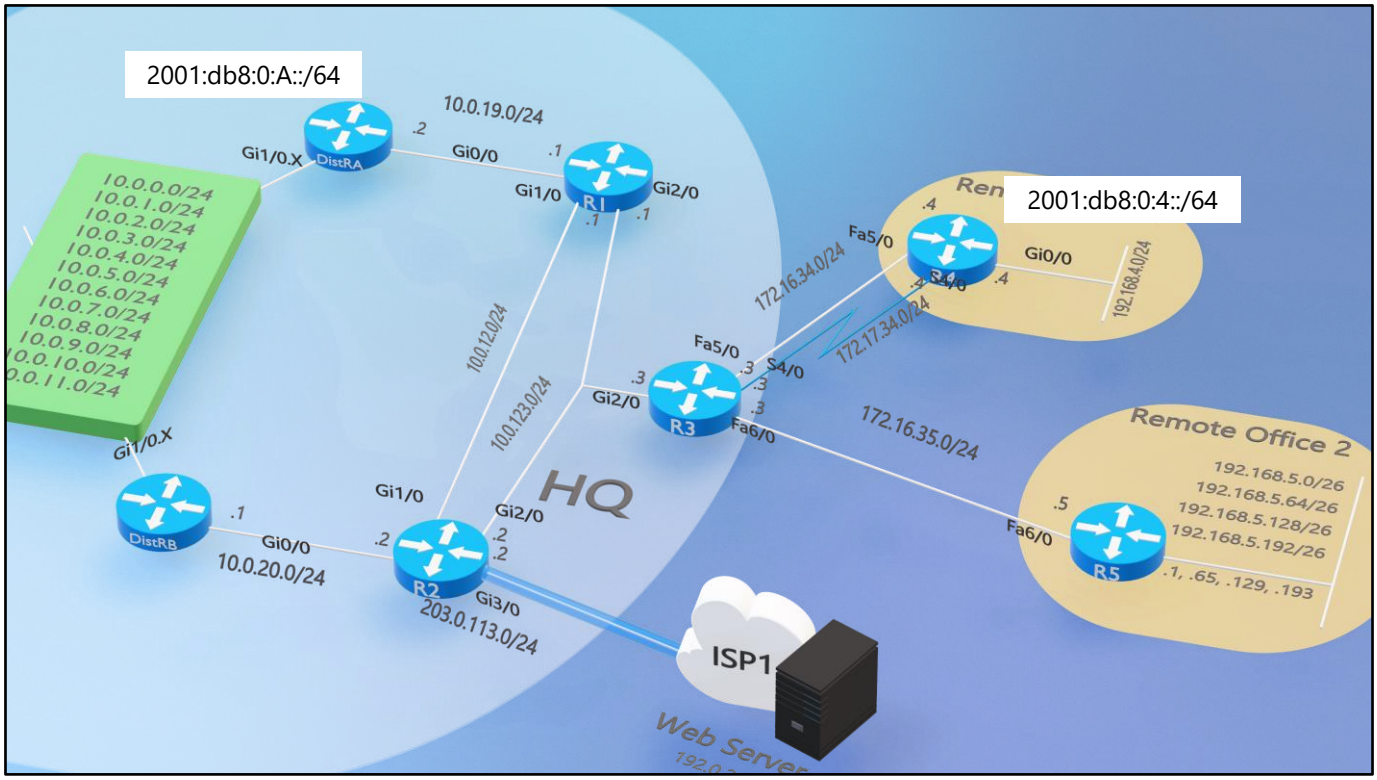
Des redo/reword

`RID (32 bit dot decimal)

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Instructor Notes:
Demo everything

Note – with EIGRPv6 you do not have to be in the same subnet… you just have to be able to reach each others link local address. Since link local addresses are not routable this implies that you have to be in the same Layer 2 lan. (so 0 router hops away from each other.)
K values the same
Metric calculation the same

Configure all interfaces from DSW1 to R4 for EIGRPv6 but only use the link local addresses on the routers and the global addresses on the ends.
Configure gig 0/0 on R4 as passive
Configure DSW1 int vlan 100 as passive

Show ipv6 protocols
Show ipv6 eigrp interfaces
Show ipv6 eigrp interfaces detail
Show ipv6 eigrp neighbors

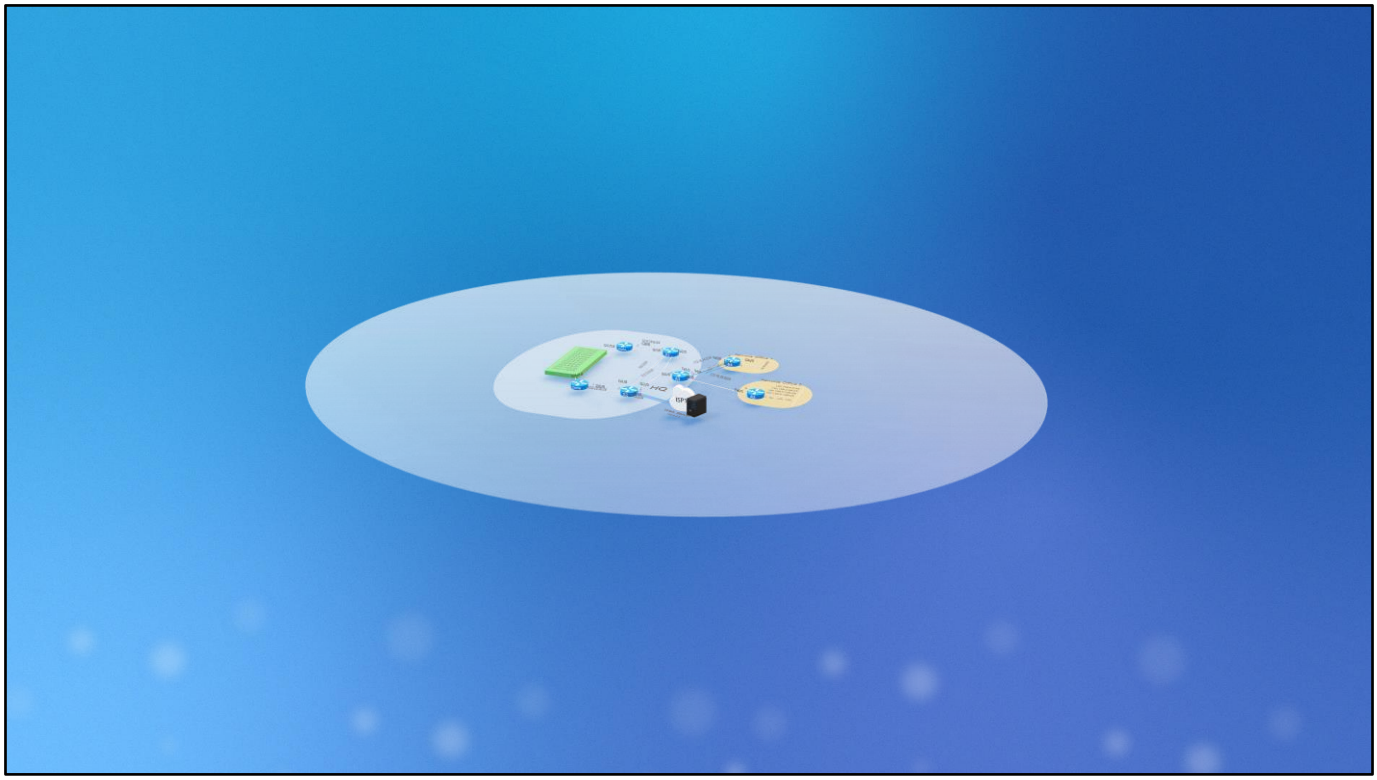
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Show ipv6 eigrp neighbors detail
Show ipv6 eigrp topology
Show ipv6 eigrp route

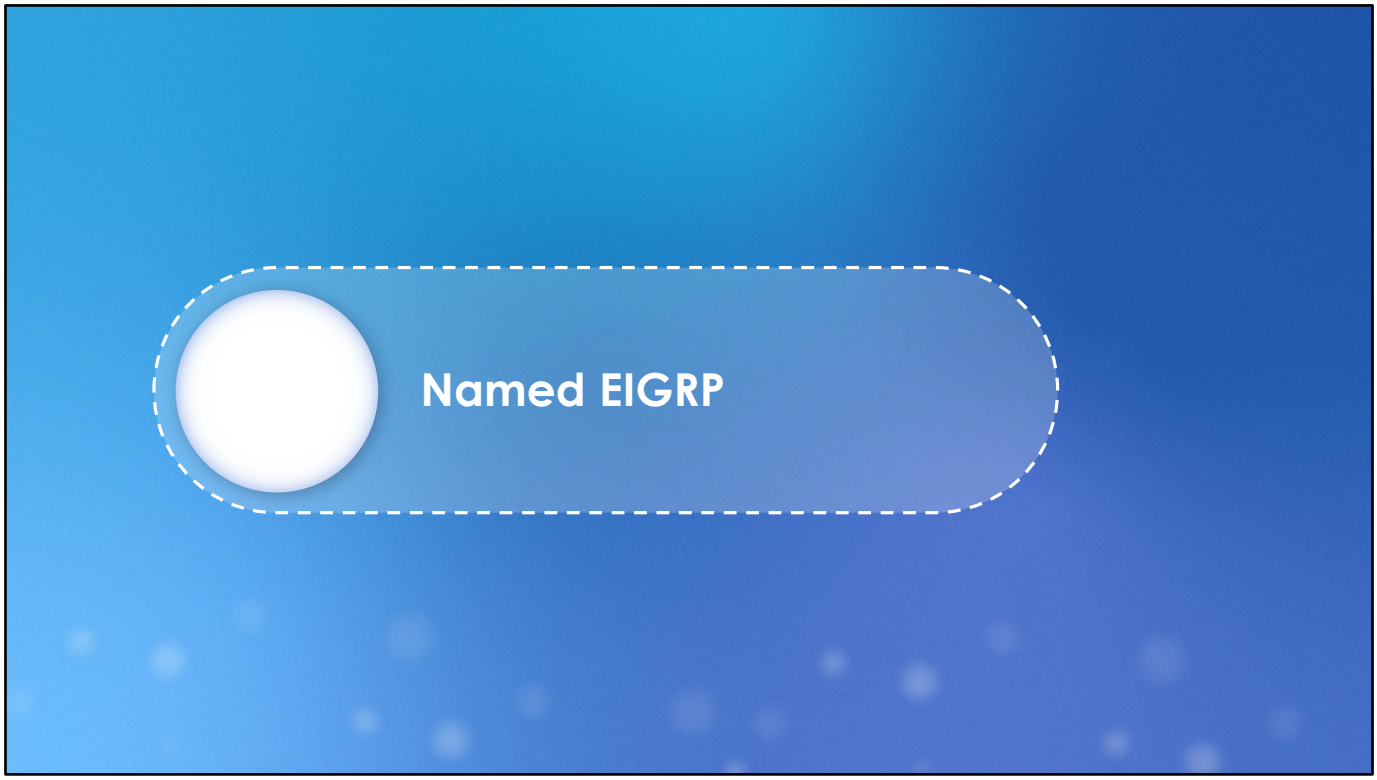
Configure summary from R3 to R4 on fa and ser interface – 2001:db8:0::/48 or even ::/0

Configure R4 as a stub router

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

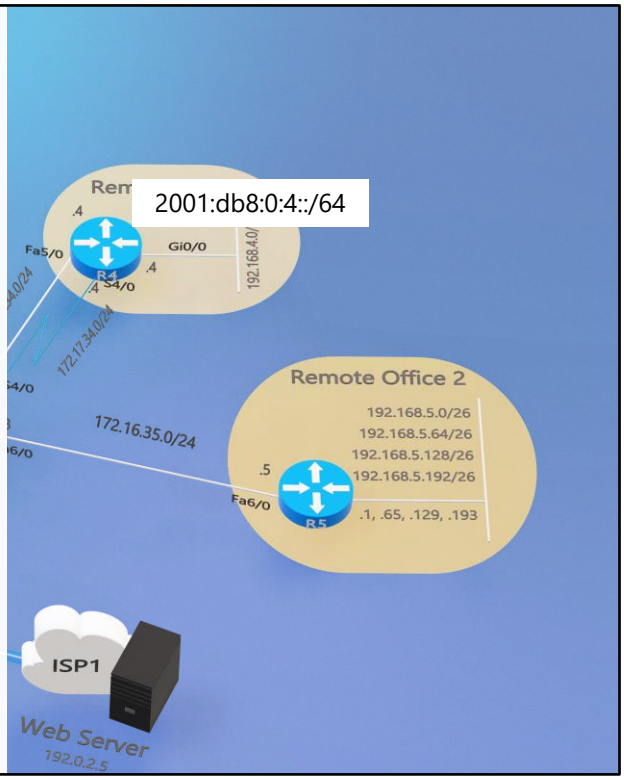
Named EIGRP

Cons to Traditional "Classic" EIGRP Configuration:

- Different commands for IPv4 and IPv6
- Placement of commands varies

Pros to EIGRP Named Configuration:

- EIGRP configuration is done in one place
- Compatible with routers using classic EIGRP



`Complexity for dual stack (summarization / authentication / multiple instances)
`Makes it easier

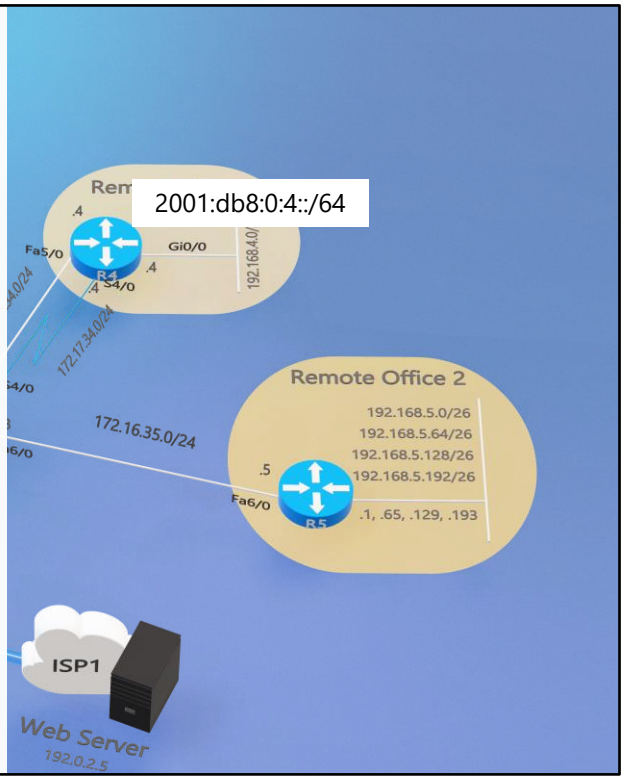
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

EIGRP Named

Real-World Reason

Support for VRF

Support for higher speed interfaces



https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_eigrp/configuration/xe-16-5/ire-xe-16-5-book/ire-wid-met.html

Anything above a 10Gbps interface gets a metric of 256 using the classic calculation. NO GOOD!

GigabitEthernet:
Scaled Bandwidth = 10,000,000 / 1,000,000
Scaled Delay = 10 / 10
Composite Metric = 10 + 1 * 256 = 2816

10 GigabitEthernet:
Scaled Bandwidth = 10,000,000 / 10,000,000
Scaled Delay = 10 / 10
Composite Metric = 1 + 1 * 256 = 512

11 GigabitEthernet:
Scaled Bandwidth = 10,000,000 / 11,000,000
Scaled Delay = 10 / 10

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Composite Metric = 0 + 1 * 256 = 256

20 GigabitEthernet:
Scaled Bandwidth = 10,000,000 / 20,000,000
Scaled Delay = 10 / 10
Composite Metric = 0 + 1 * 256 = 256

NAMED Mode uses "wide-metrics" 64-bit vs 32-bit to support higher speed interfaces.

Supports up to 4.2 terabit interfaces.

Metric Backward Compatibility
EIGRP wide metrics were designed with backward compatibility in mind. EIGRP wide metrics set K_1 and K_3 to a value of 1 and set K_2, K_4, K_5, and K_6 to 0, which allows backward compatibility because the K value metrics match with classic metrics. As long as K_1 through K_5 are the same and K_6 is not set, the two metric styles allow adjacency between routers.

EIGRP is able to detect when peering with a router is using classic metrics, and it *unscales* the metric

This conversion results in loss of clarity if routes pass through a mixture of classic metric and wide metric devices. An end result of this intended behavior is that paths learned using wide metric peers always look better than paths learned using classic paths. Using a mixture of classic metric and wide metric devices could lead to suboptimal routing, so it is best to keep all devices operating with the same metric style.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

EIGRP Metric:

metric = 256*((K1*Scaled Bw) + (K2*Scaled Bw)/(256 – Load) + (K3*Scaled Delay)*(K5/(Reliability + K4)))

Named EIGRP Metric:

metric = [(K1*Minimum Throughput + {K2*Minimum Throughput} / 256-Load) + (K3*Total Latency) + (K6*Extended Attributes)]* [K5/(K4 + Reliability)]

K-Values:

K1 = 1

K2 = 0

K3 = 1

K4 = 0

K5 = 0

K6 = 0

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_eigrp/configuration/15-sy/ire-15-sy-book/ire-wid-met.html

Composite Cost Metric = (K1*Minimum Throughput) + (K3*Total Latency)
Minimum Throughput = (10^7*** 65536**)/Bw), where 65536 is the wide-scale constant.
Total Latency for bandwidths below 1 gigabit = (Delay***65536)/10**, where 65536 is the wide-scale constant.
Total Latency for bandwidths above 1 gigabit = (10^7* 65536/10)/ Bw, 65536 is the wide-scale constant.

Anything above a 10Gbps interface gets a metric of 256 using the classic calculation.
NO GOOD!

GigabitEthernet:
Scaled Bandwidth = 10,000,000 / 1,000,000
Scaled Delay = 10 / 10
Composite Metric = 10 + 1 * 256 = 2816

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

10 GigabitEthernet:
Scaled Bandwidth = 10,000,000 / 10,000,000
Scaled Delay = 10 / 10
Composite Metric = 1 + 1 * 256 = 512

11 GigabitEthernet:
Scaled Bandwidth = 10,000,000 / 11,000,000
Scaled Delay = 10 / 10
Composite Metric = 0 + 1 * 256 = 256

20 GigabitEthernet:
Scaled Bandwidth = 10,000,000 / 20,000,000
Scaled Delay = 10 / 10
Composite Metric = 0 + 1 * 256 = 256

NAMED Mode uses "wide-metrics" 64-bit vs 32-bit to support higher speed interfaces.

Supports up to 4.2 terabit interfaces.

Metric Backward Compatibility
EIGRP wide metrics were designed with backward compatibility in mind. EIGRP wide metrics set K_1 and K_3 to a value of 1 and set K_2, K_4, K_5, and K_6 to 0, which allows backward compatibility because the K value metrics match with classic metrics. As long as K_1 through K_5 are the same and K_6 is not set, the two metric styles allow adjacency between routers.

EIGRP is able to detect when peering with a router is using classic metrics, and it *unscales* the metric

This conversion results in loss of clarity if routes pass through a mixture of classic metric and wide metric devices. An end result of this intended behavior is that paths learned using wide metric peers always look better than paths learned using classic paths. Using a mixture of classic metric and wide metric devices could lead to suboptimal routing, so it is best to keep all devices operating with the same metric style.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Named EIGRP Modes

AF Configuration Mode:

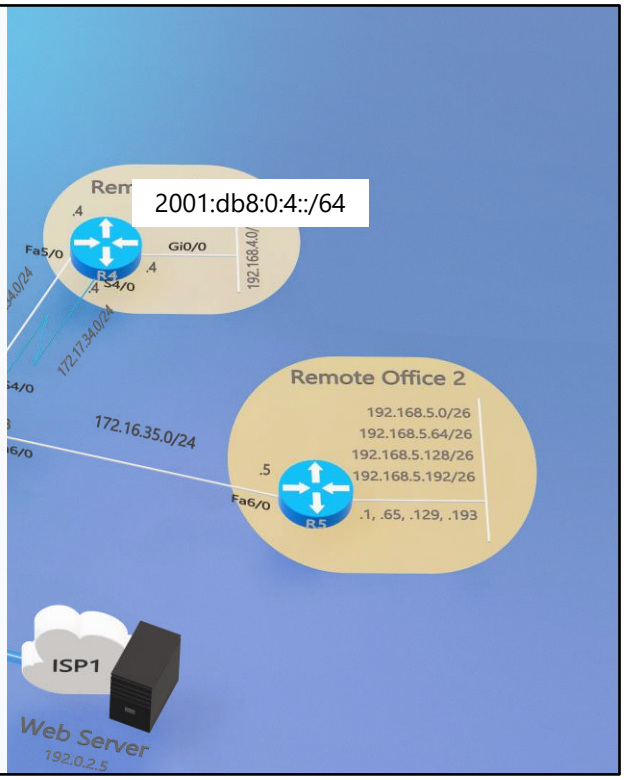
General commands: **router-id, network, eigrp stub**

AF Interface Configuration Mode:

Interface-specific commands: **summary-address, passive-interface, hello-interval, hold-time**

AF Topology Configuration Mode:

Commands directly affecting topology table: **variance, maximum-paths, redistribute**



*********Supports wide metrics

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

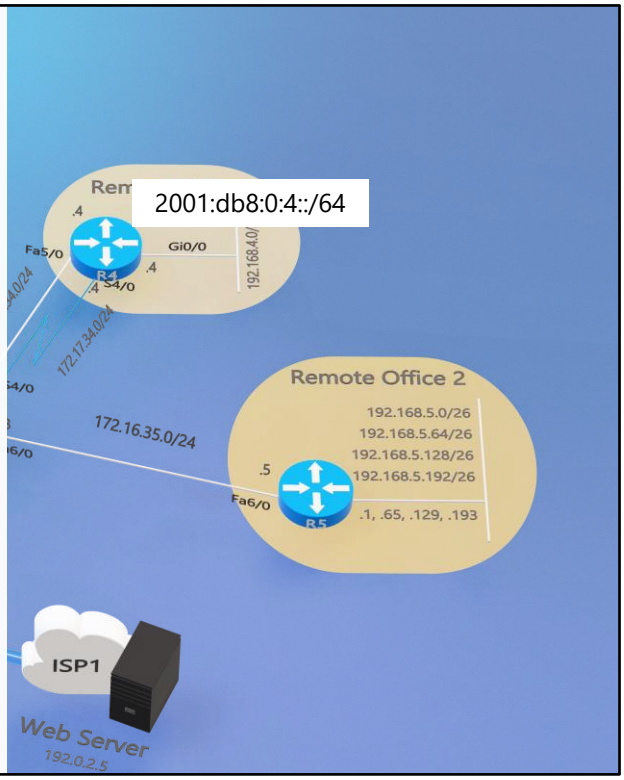
Classic vs. Named EIGRP Configuration

Named

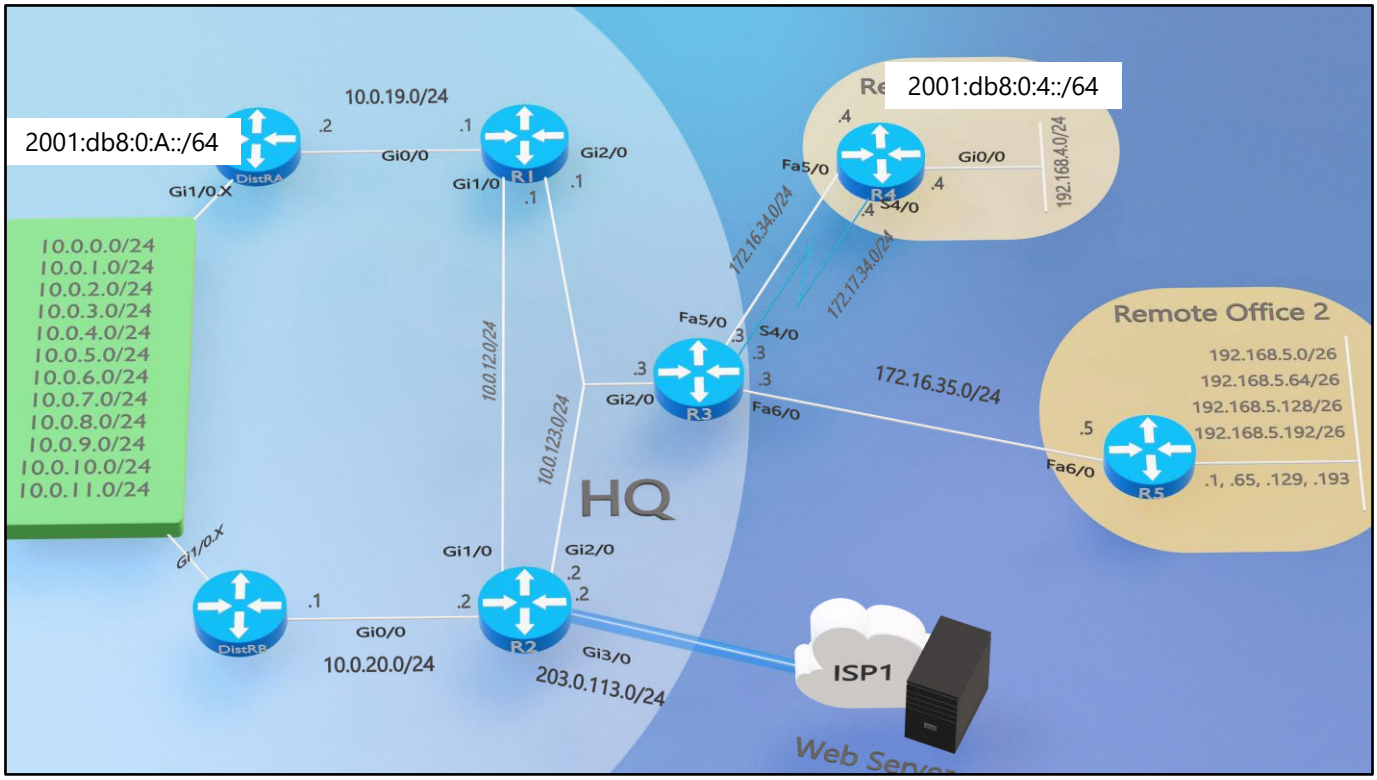
```
router eigrp LAB
 !
 address-family ipv4 unicast
autonomous-system 1
  !
  af-interface default
   passive-interface
  exit-af-interface
  !
  af-interface Ethernet0/0
  summary-address 192.168.2.0/23
  no passive-interface
  exit-af-interface
  !
  topology base
  exit-af-topology
  network 0.0.0.0
 exit-address-family
 !
 address-family ipv6 unicast
autonomous-system 1
  !
  topology base
 exit-af-topology
 exit-address-family
```

Classic

```
interface Loopback1
 ip address 192.168.3.1 255.255.255.0
 ipv6 address 2001:DB8:0:3::1/64
 ipv6 eigrp 1
!
interface Ethernet0/0
 ip address 172.16.1.6
255.255.255.252
 ip summary-address eigrp 1
192.168.2.0 255.255.254.0
 ipv6 address 2001:DB8:0:101::2/64
 ipv6 eigrp 1
!
router eigrp 1
 network 0.0.0.0
 passive-interface default
 no passive-interface Ethernet0/0
!
ipv6 router eigrp 1
```



©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



DEMO NAMED EIGRP

Note: Be mindful that EIGRPv6 will be automatically enabled on every interface with an IPv6 address as soon as you create the address family. If you don't want an interface enabled you have to disable it in af-interface config mode with the "shutdown" command.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

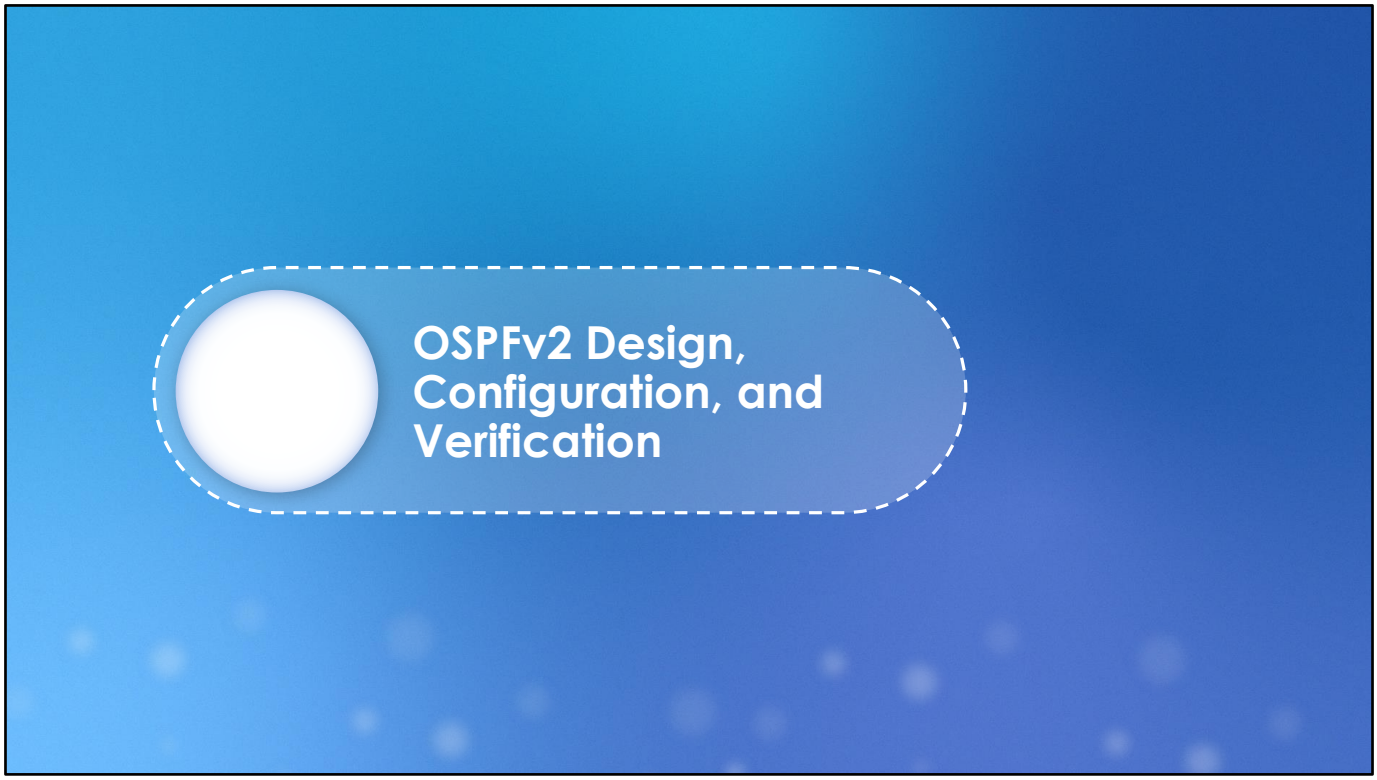


*********Supports wide metrics

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Title slide

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



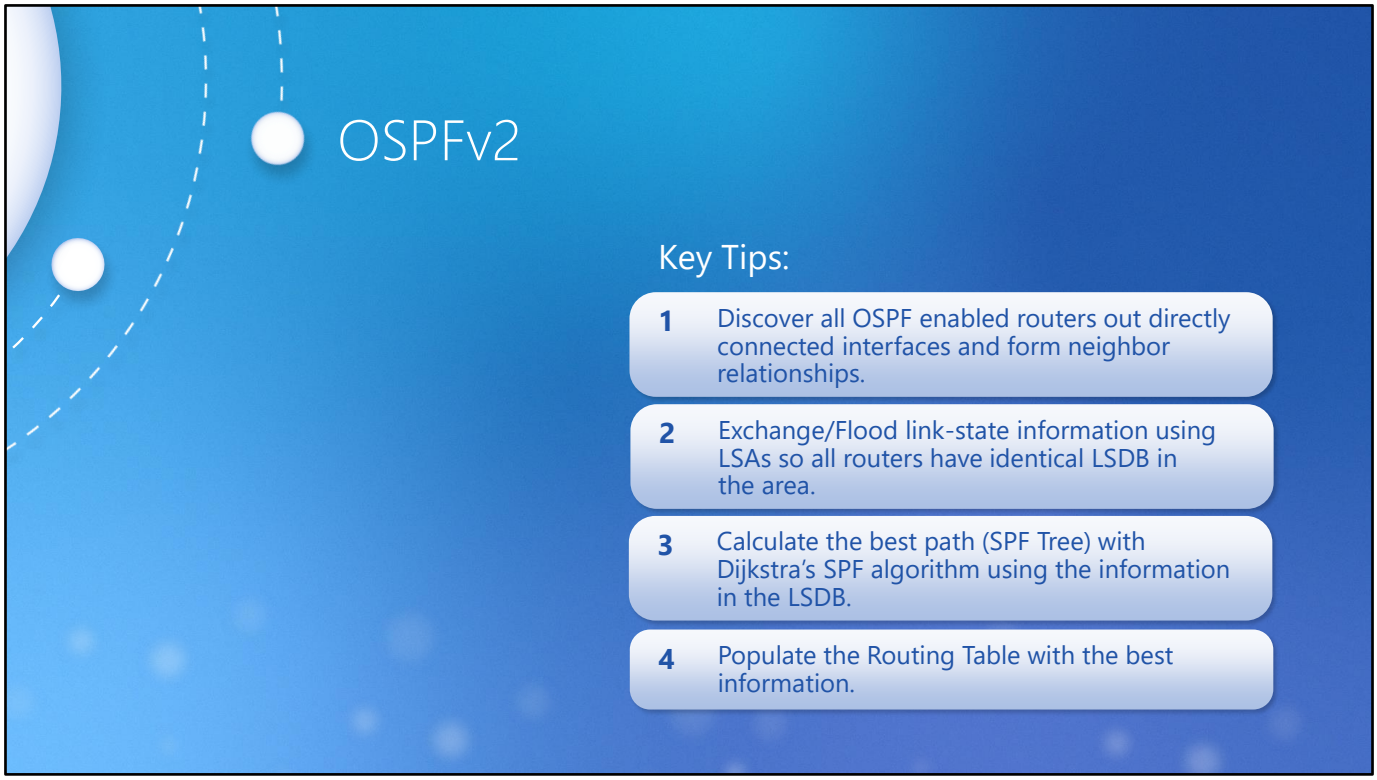
IPv6 uses OSPFv3 specified in RFC 5340

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



IPv6 uses OSPFv3 specified in RFC 5340

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



IPv6 uses OSPFv3 specified in RFC 5340

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Scalability

- Single Area – limited
- Multi-Area – virtually unlimited

The larger the network grows the more information there is. Therefore, the longer it takes to perform SPF calculations and

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

the longer it takes to converge the network when a change occurs.

Building a multiarea ospf network reduces the size of the LSDB in each area and therefore, reduces the amount of information in an area that SPF will have to perform a calculation on.

Information within an area is detailed.
Information between areas is not-detailed or it is a subset of information.

Area 0 is known as the backbone area, or transit area… typically there are no users here. You could classify it as the core. All traffic between areas must pass through this area. It has to be contiguous, can't be split up.

All other areas are normal or nonbackbone areas. These areas will contain users and resources. Could be based on functional or geographical groupings.

A full SPT calculation runs when a link flaps within the area.

With a single area, the LSDB increases in size and becomes unmanageable.

The LSDB for the single area grows, consumes more memory, and takes

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

longer during the SPF computation process.

With a single area, no summarization of route information occurs.

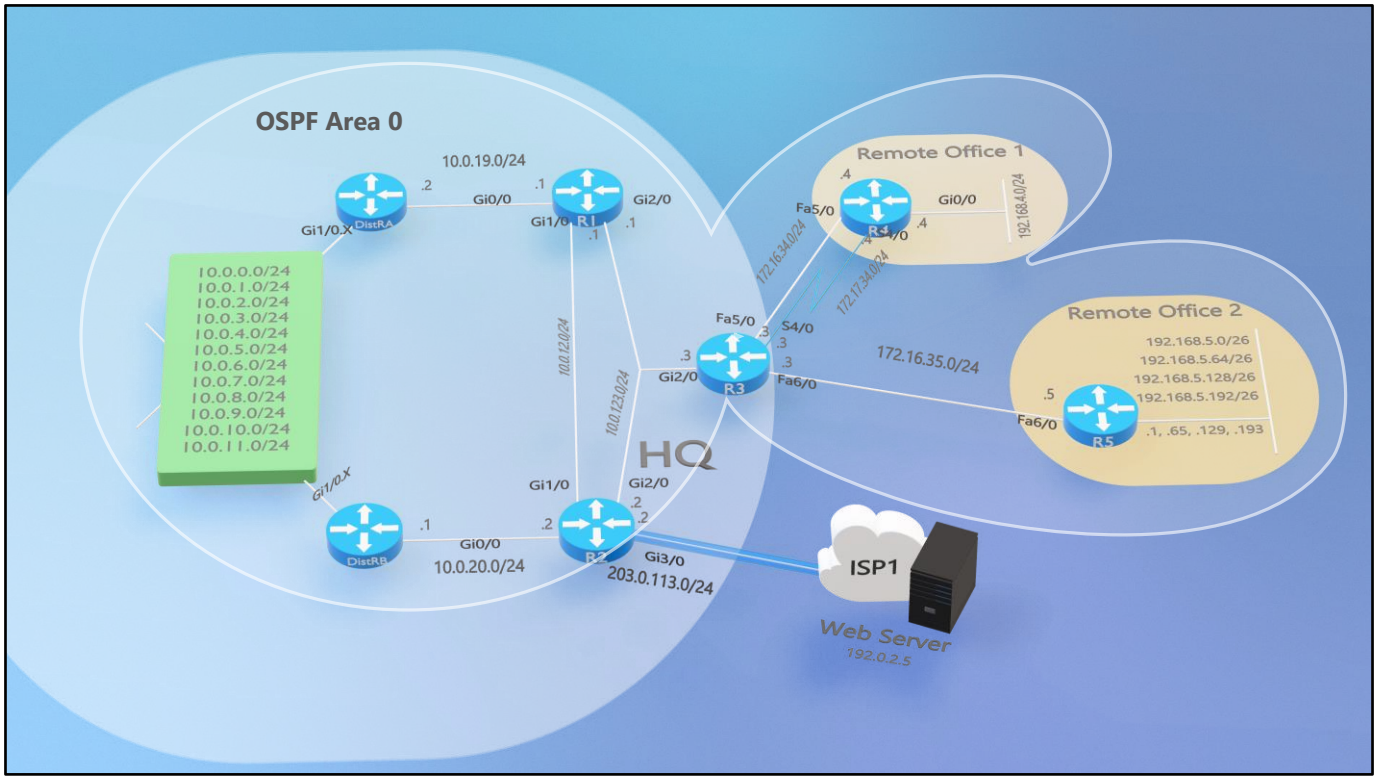
Router Types:

Backbone router - a router with at least 1 interface in area 0
Internal router - all interfaces are in a single area
ABR – has at least one interface in area 0 and another interface in any other area
ASBR – has at least one interface in any area and another interface connected to a different routing

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

domain

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Scalability

Single Area – limited

Multi-Area – virtually unlimited

The larger the network grows the more information there is. Therefore, the longer it takes to perform SPF calculations and

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

the longer it takes to converge the network when a change occurs.

Building a multiarea ospf network reduces the size of the LSDB in each area and therefore, reduces the amount of information in an area that SPF will have to perform a calculation on.

Information within an area is detailed.
Information between areas is not-detailed or it is a subset of information.

Area 0 is known as the backbone area, or transit area… typically there are no users here. You could classify it as the core. All traffic between areas must pass through this area. It has to be contiguous, can't be split up.

All other areas are normal or nonbackbone areas. These areas will contain users and resources. Could be based on functional or geographical groupings.

A full SPT calculation runs when a link flaps within the area.

With a single area, the LSDB increases in size and becomes unmanageable.

The LSDB for the single area grows, consumes more memory, and takes

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

longer during the SPF computation process.

With a single area, no summarization of route information occurs.

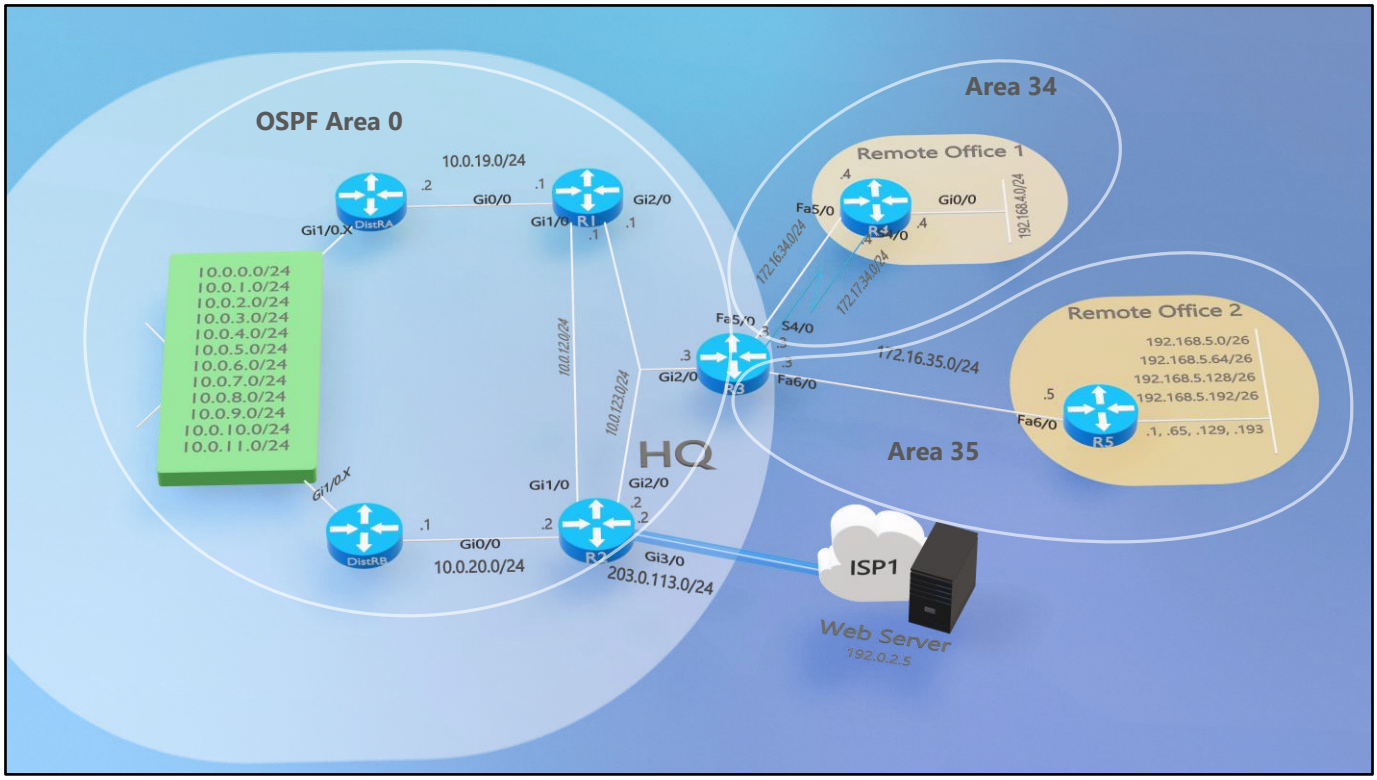
Router Types:

Backbone router - a router with at least 1 interface in area 0
Internal router - all interfaces are in a single area
ABR – has at least one interface in area 0 and another interface in any other area
ASBR – has at least one interface in any area and another interface connected to a different routing

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

domain

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Scalability

Single Area – limited

Multi-Area – virtually unlimited

The larger the network grows the more information there is. Therefore, the longer it takes to perform SPF calculations and

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

the longer it takes to converge the network when a change occurs.

Building a multiarea ospf network reduces the size of the LSDB in each area and therefore, reduces the amount of information in an area that SPF will have to perform a calculation on.

Information within an area is detailed.
Information between areas is not-detailed or it is a subset of information.

Area 0 is known as the backbone area, or transit area… typically there are no users here. You could classify it as the core. All traffic between areas must pass through this area. It has to be contiguous, can't be split up.

All other areas are normal or nonbackbone areas. These areas will contain users and resources. Could be based on functional or geographical groupings.

A full SPT calculation runs when a link flaps within the area.

With a single area, the LSDB increases in size and becomes unmanageable.

The LSDB for the single area grows, consumes more memory, and takes

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

longer during the SPF computation process.

With a single area, no summarization of route information occurs.

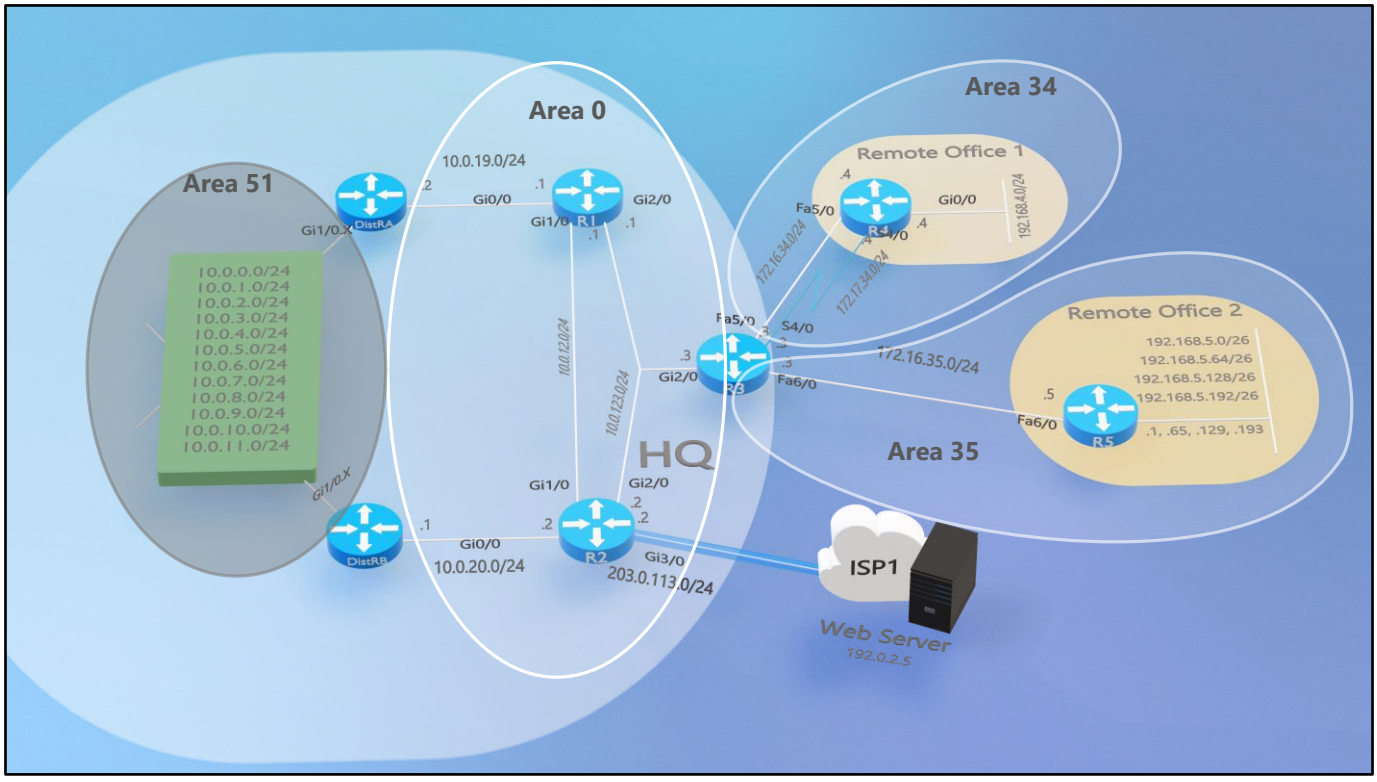
Router Types:

Backbone router - a router with at least 1 interface in area 0
Internal router - all interfaces are in a single area
ABR – has at least one interface in area 0 and another interface in any other area
ASBR – has at least one interface in any area and another interface connected to a different routing

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

domain

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Scalability

Single Area – limited

Multi-Area – virtually unlimited

The larger the network grows the more information there is. Therefore, the longer it takes to perform SPF calculations and

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

the longer it takes to converge the network when a change occurs.

Building a multiarea ospf network reduces the size of the LSDB in each area and therefore, reduces the amount of information in an area that SPF will have to perform a calculation on.

Information within an area is detailed.
Information between areas is not-detailed or it is a subset of information.

Area 0 is known as the backbone area, or transit area… typically there are no users here. You could classify it as the core. All traffic between areas must pass through this area. It has to be contiguous, can't be split up.

All other areas are normal or nonbackbone areas. These areas will contain users and resources. Could be based on functional or geographical groupings.

A full SPT calculation runs when a link flaps within the area.

With a single area, the LSDB increases in size and becomes unmanageable.

The LSDB for the single area grows, consumes more memory, and takes

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

longer during the SPF computation process.

With a single area, no summarization of route information occurs.

Router Types:

Backbone router - a router with at least 1 interface in area 0
Internal router - all interfaces are in a single area
ABR – has at least one interface in area 0 and another interface in any other area
ASBR – has at least one interface in any area and another interface connected to a different routing

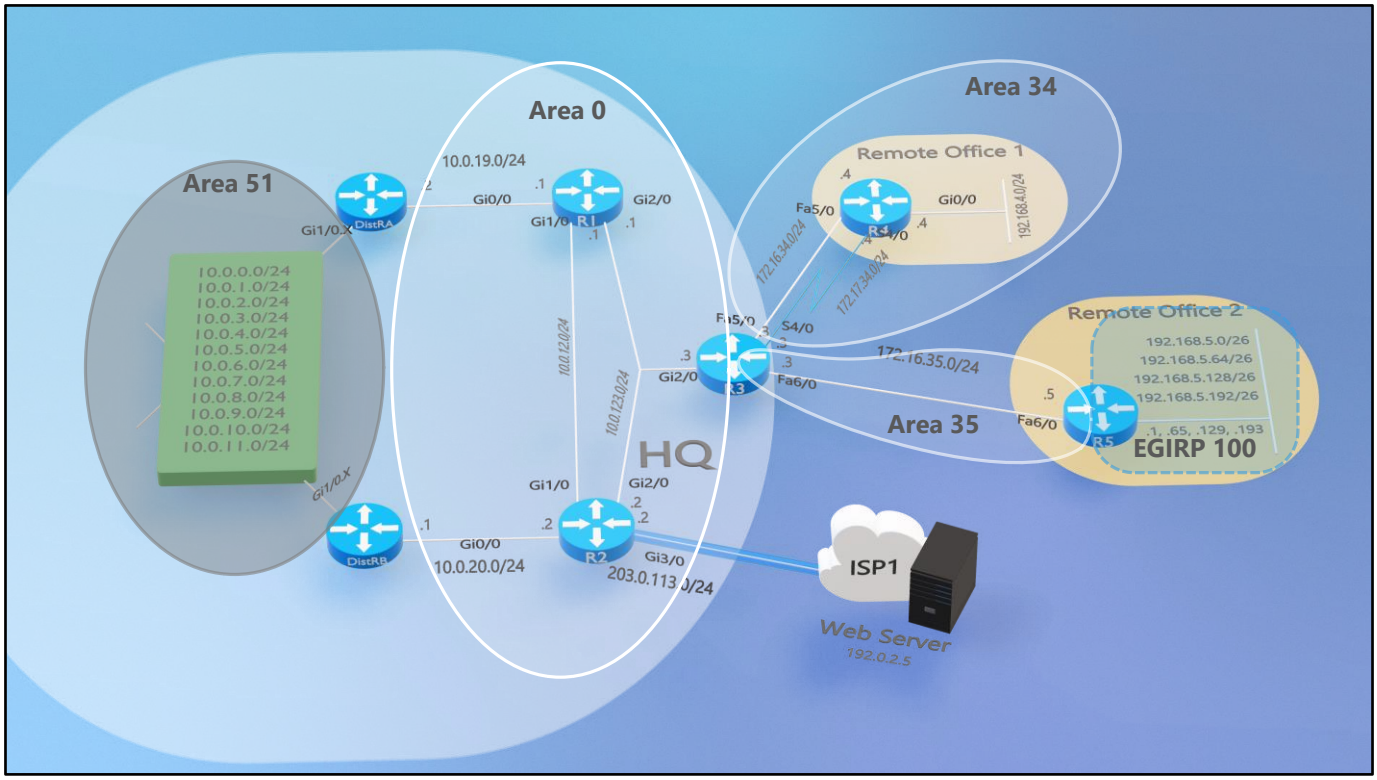
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

domain

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Demo Complete Configuration:
Don't forget default information originate
Don't forget about authentication

Adjacency based on matching hellos:

- Area ID
- Timers
- Stub
- Authentication
- MTU

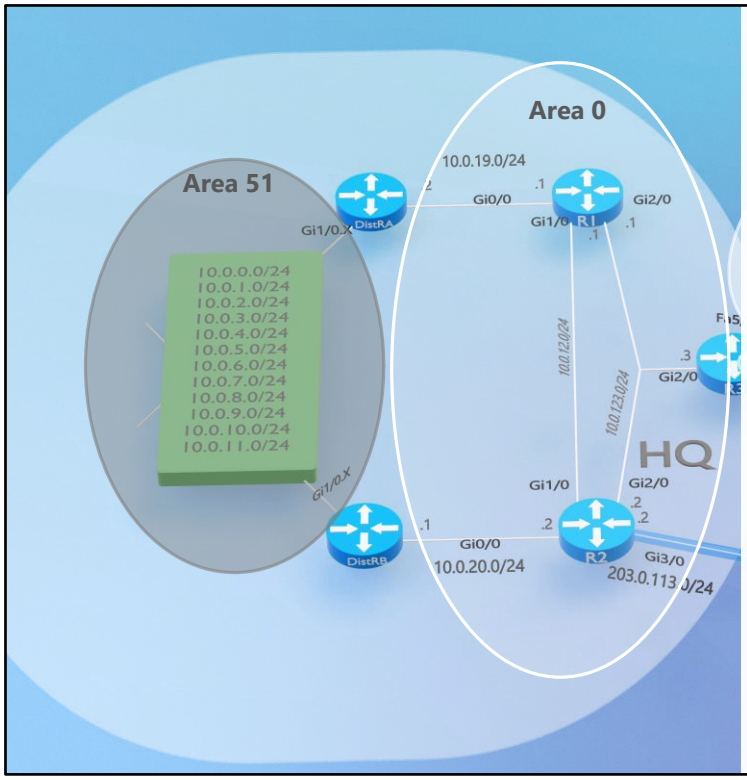
Configure OSPF on all interface except R2 ISP interface.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Static config between R3 and R5
Inject default route on r2 (**`default-info originate`**)
Redistribute eigrp into ospf
Configure Passive Interface on all dist interfaces, and r4 interfaces

Show ip protocols
Show ip ospf
Show ip ospf interface brief
Show ip ospf interface
Show ip ospf neighbor
Show ip ospf database
Show ip route ospf

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



OSPF Router-ID

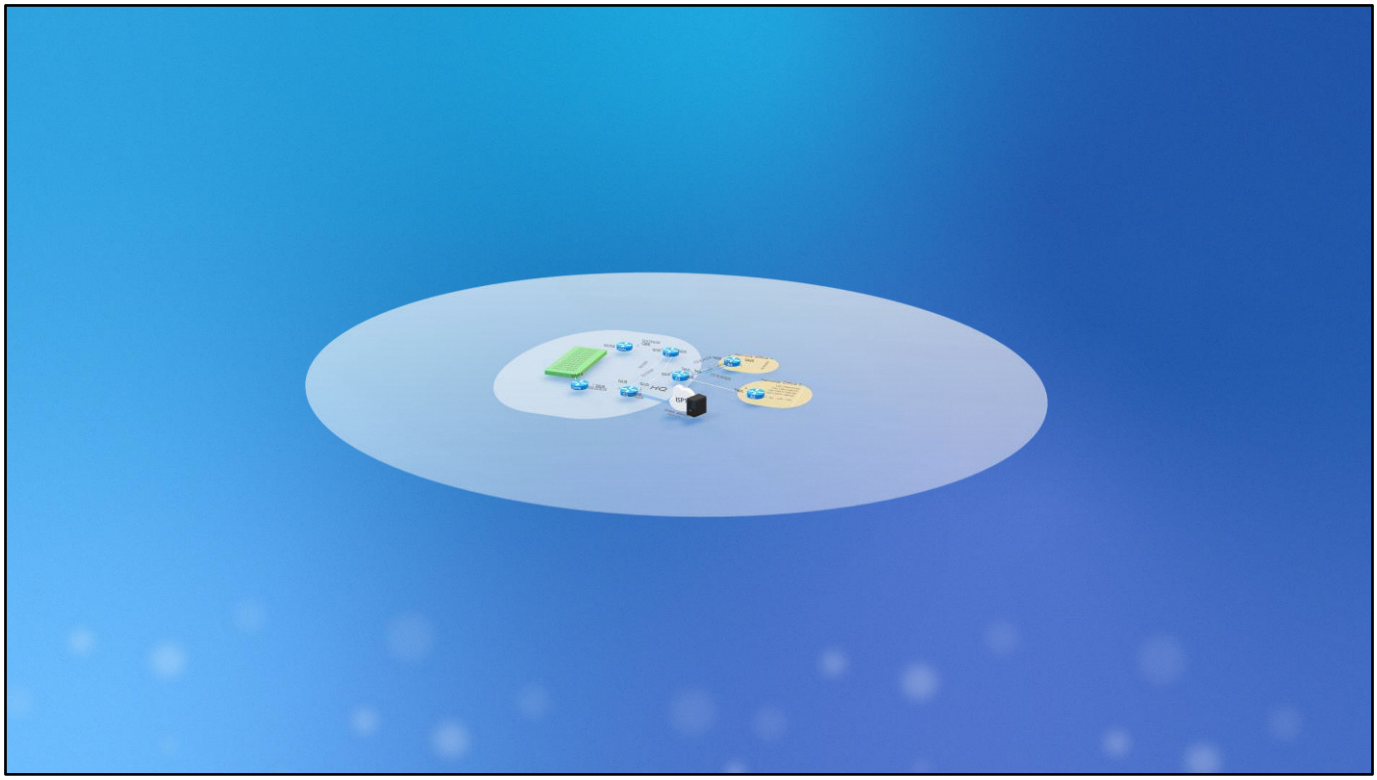
How a router uniquely identifies itself in OSPF

It can be manually configured with the `router-id`.

If `router-id` is not configured, the highest IP address on a loopback interface when OSPF starts is the router ID

If there is no loopback interface, then the router selects the highest IP address on any interface when OSPF process begins

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Passive interface and authentication

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

OSPF Authentication

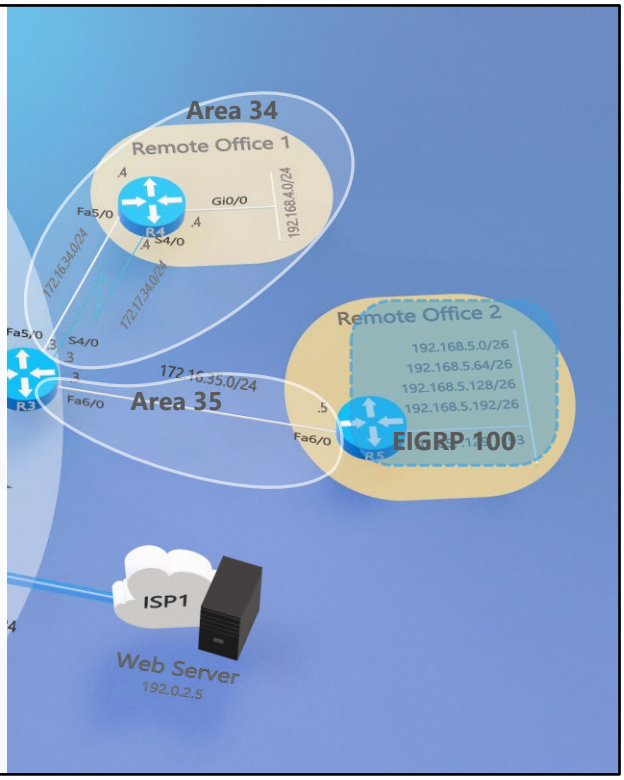
OSPFv2 authentication is a 64-bit field in the message supported two ways:

- Enabled per Interface
- Enabled per Area

Authentication type field in the message:

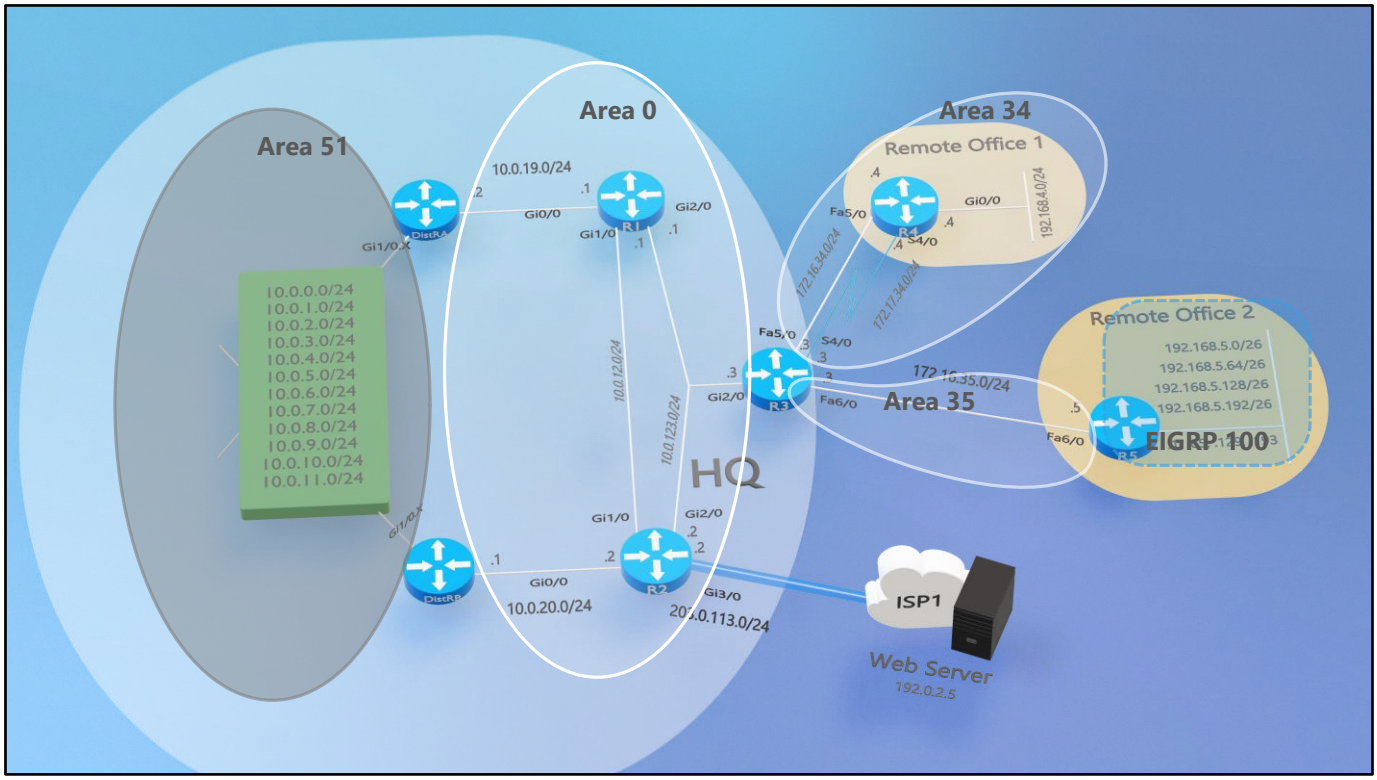
- 0—Authentication Disabled *default
- 1—Cleartext password
- 2—MD5 authentication

Cryptographic Authentication also exists



https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/configuration/xe-16-5/iro-xe-16-5-book/iro-ospfv2-crypto-authen-xe.html

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



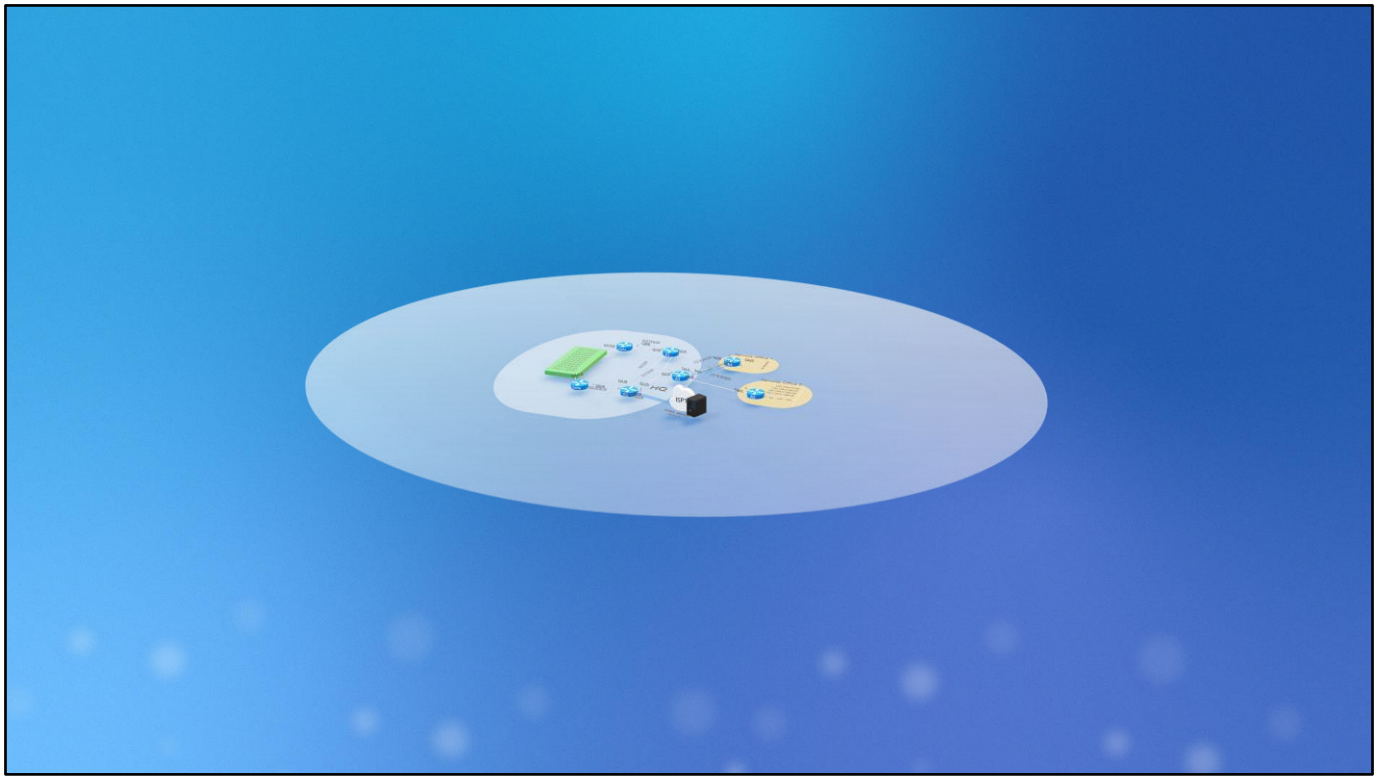
MD5 Authentication *recommended

interface s 0/0
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 CCNP

Or for entire area:
interface s 0/0
ip ospf message-digest-key 1 md5 CCNP
router ospf 1
area 1 authentication message-digest

Also Do Passive Interface

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

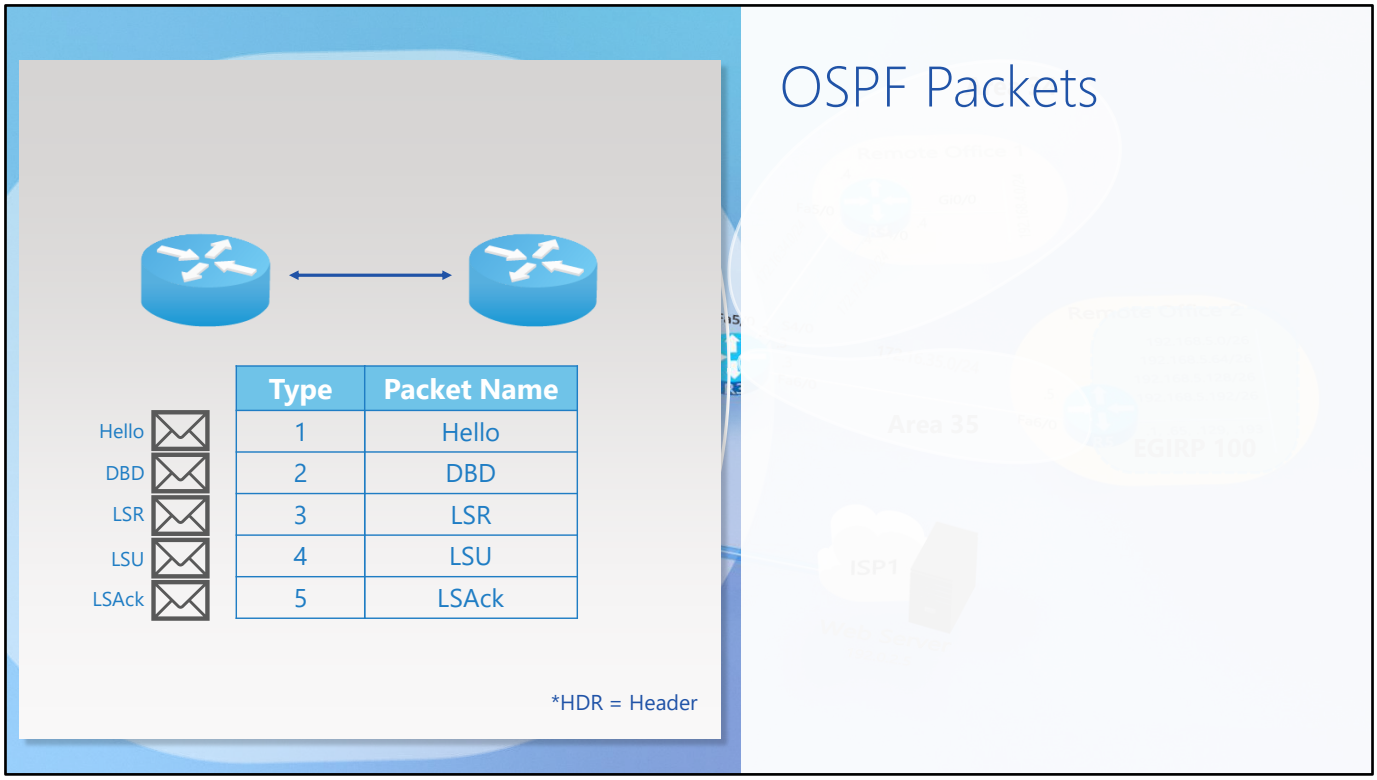


©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Title slide

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Instructor Notes:

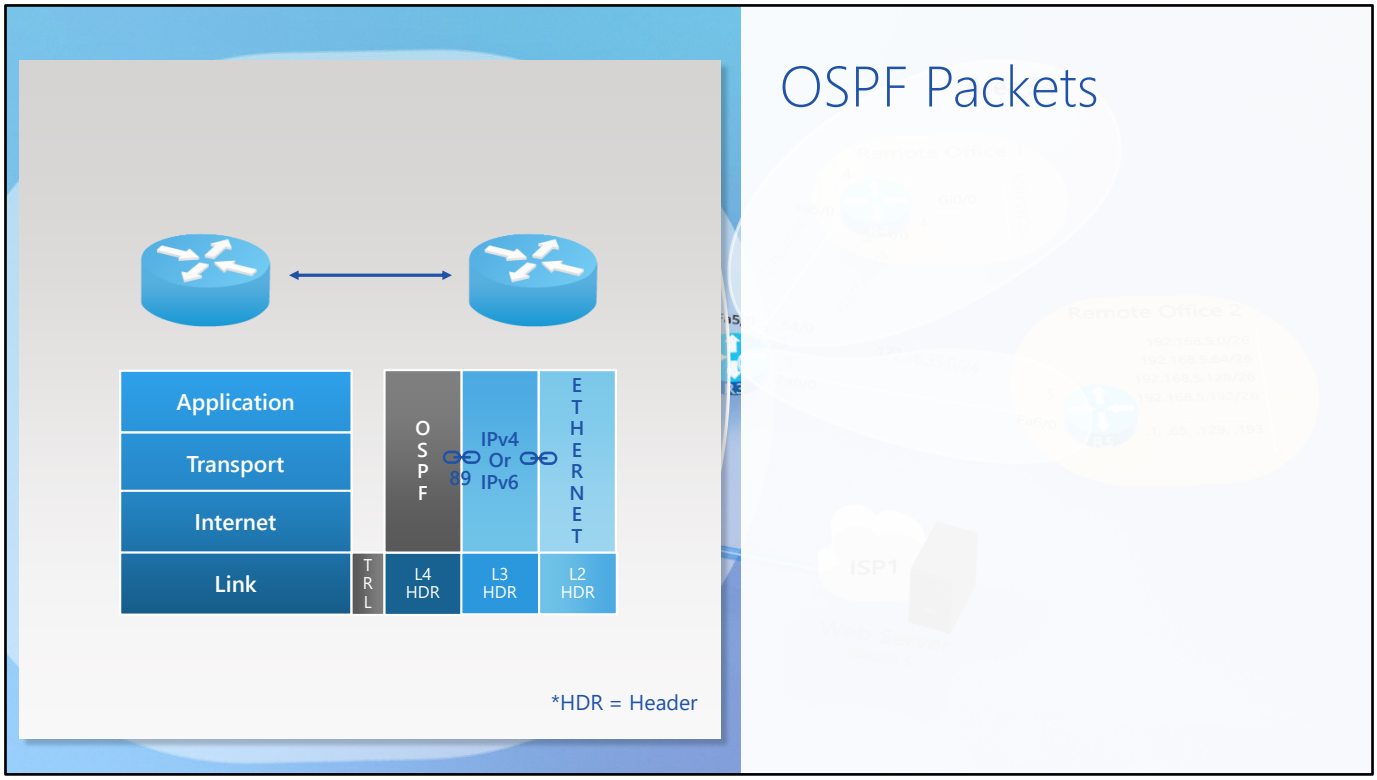
1
Hello
Packets are sent out periodically on all OSPF interfaces to discover new neighbors while ensuring that other neighbors are still online.
2
Database description (DBD) or (DDP)
Packets are exchanged when an OSPF adjacency is first being formed. These packets are used to describe the contents of the LSDB.
3
Link-state request (LSR)
When a router thinks that part of its LSDB is stale, it may request a portion of a neighbor's database using this packet type.
4
Link-state update (LSU)
This is an explicit LSA for a specific network link, and normally it is sent in direct response to an LSR.
5

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Link-state acknowledgement

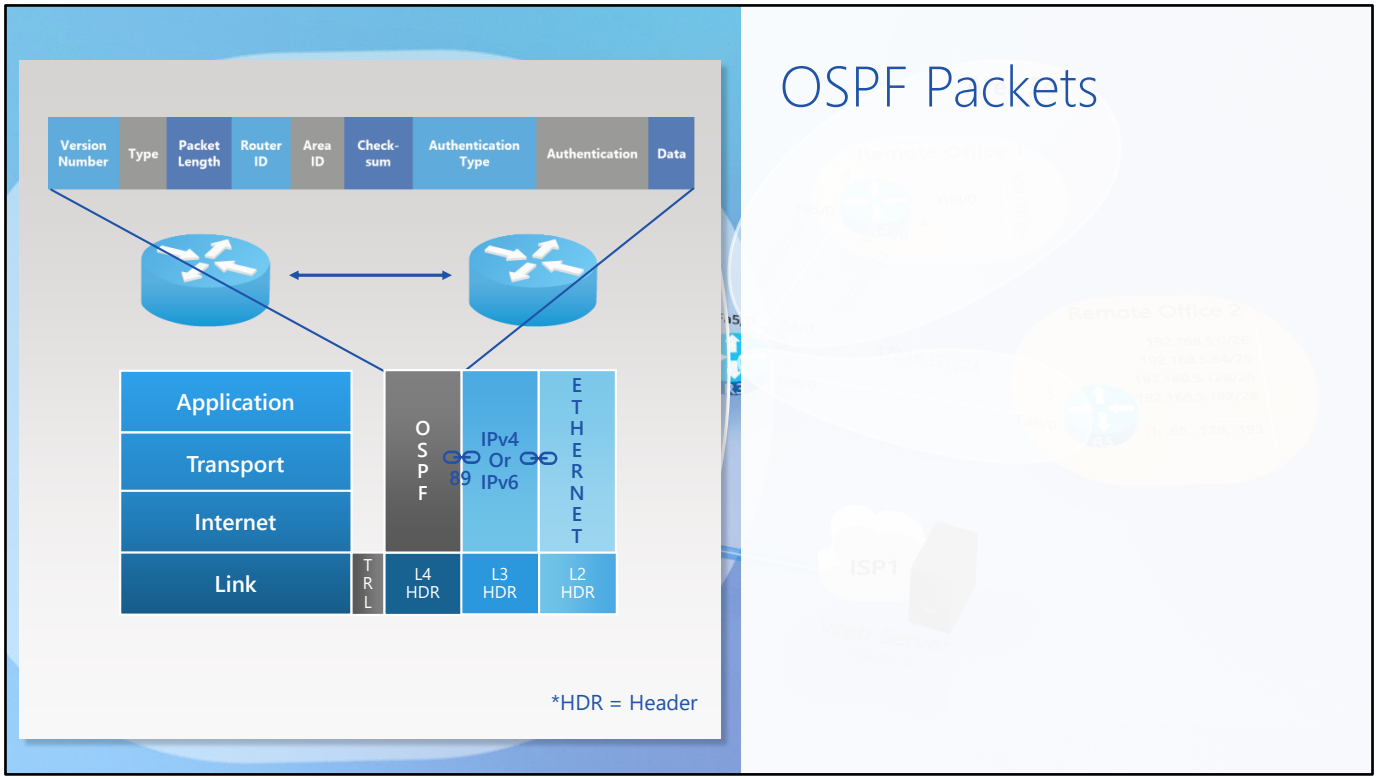
These packets are sent in response to the flooding of LSAs, thus making the flooding a reliable transport feature.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



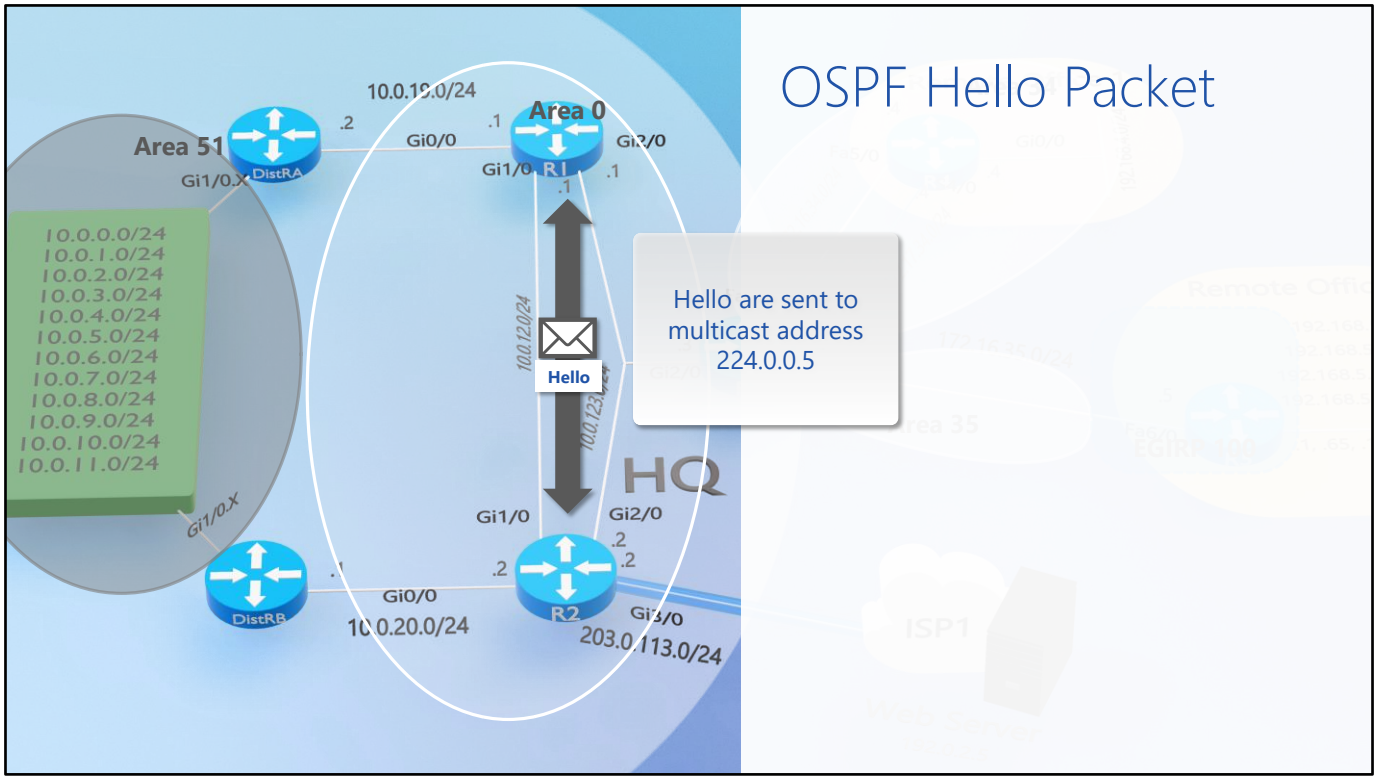
Instructor Notes:

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Instructor Notes:
Data contains the HELLO/DBD/LSR/LSU

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Demo:

Adjacency based on matching hellos:

- Area ID
- Timers
- Stub
- Authentication
- MTU

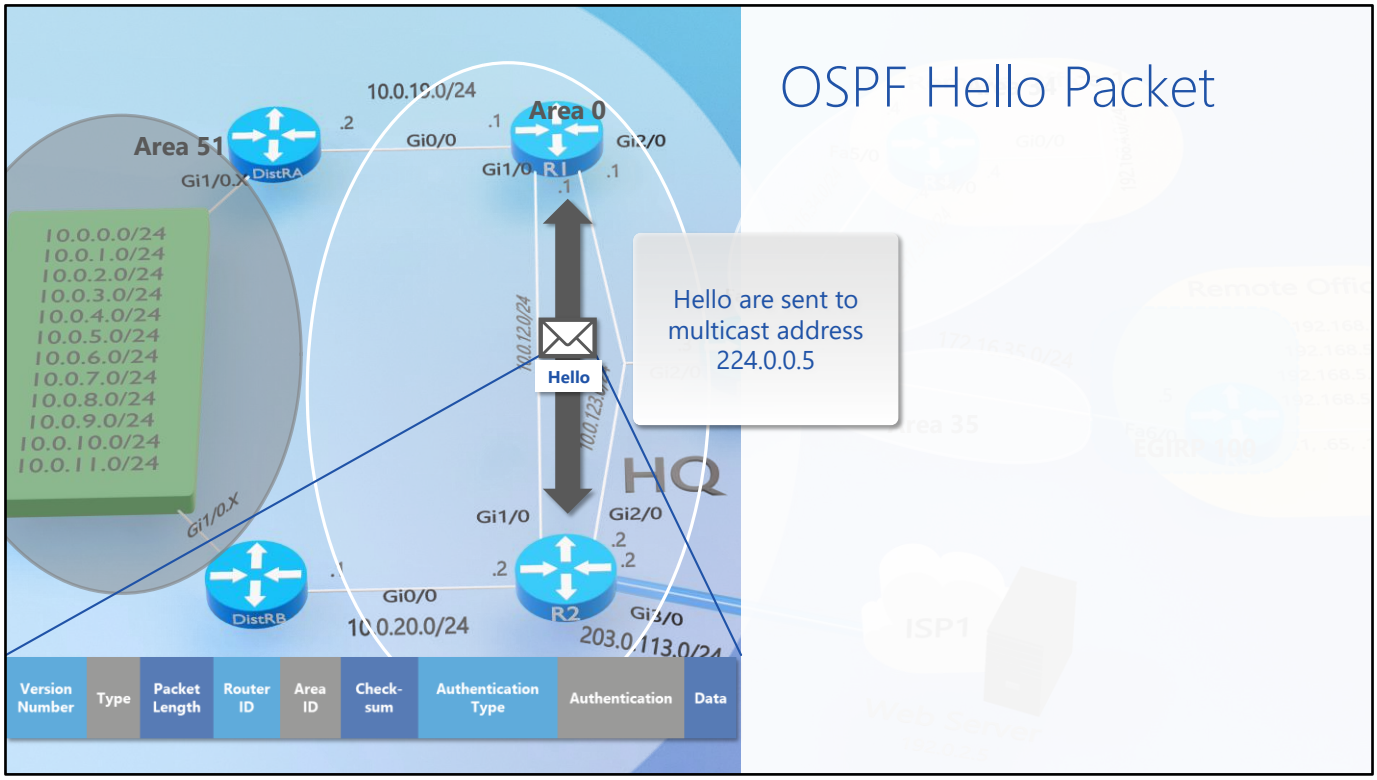
Configure OSPF on all interface except R2 ISP interface.
Static config between R3 and R5
Inject default route on r2 (**`default-info originate`**)
Redistribute eigrp into ospf

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Configure Passive Interface on all dist interfaces, and r4 interfaces

Show ip protocols
Show ip ospf
Show ip ospf interface brief
Show ip ospf interface
Show ip ospf neighbor
Show ip ospf database
Show ip route ospf

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Demo:

Adjacency based on matching hellos:

- Area ID
- Timers
- Stub
- Authentication
- MTU

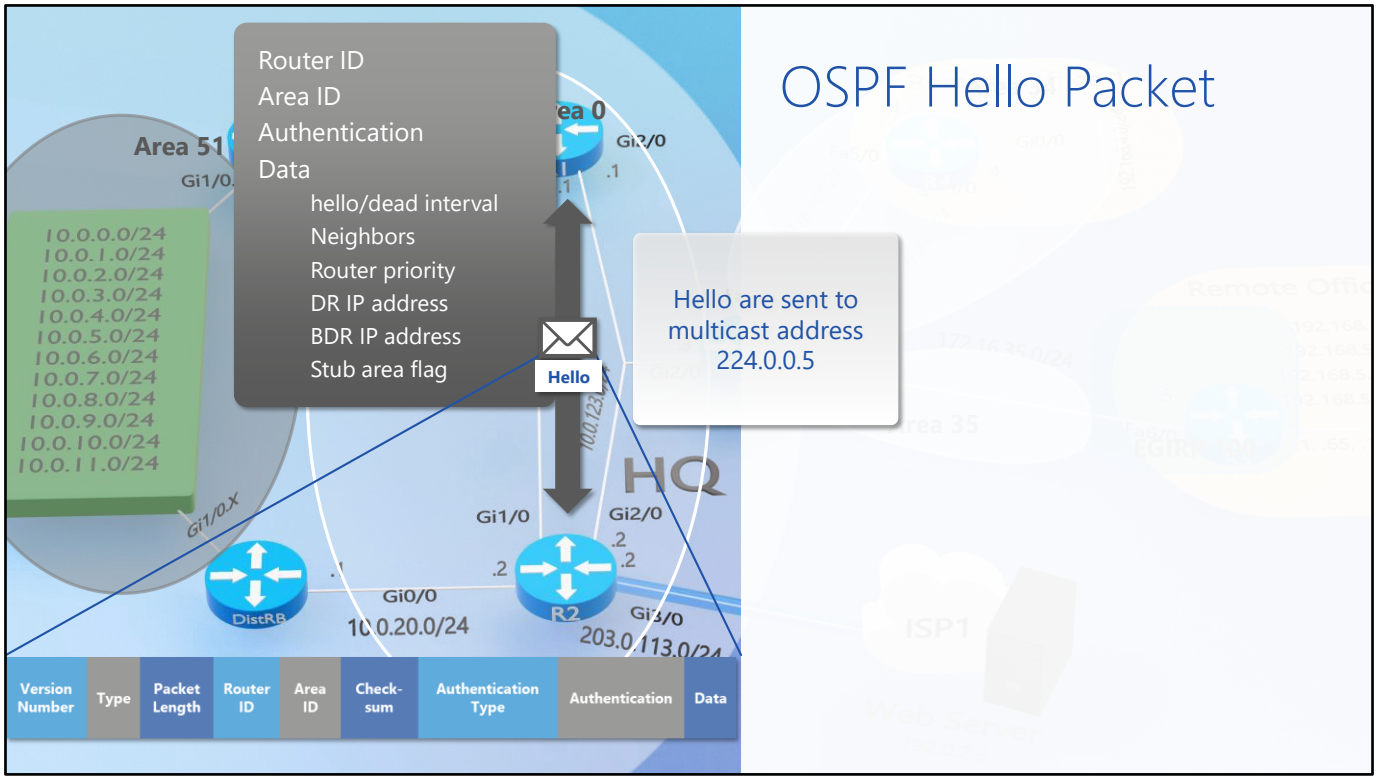
Configure OSPF on all interface except R2 ISP interface.
Static config between R3 and R5
Inject default route on r2 (**`default-info originate`**)
Redistribute eigrp into ospf

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Configure Passive Interface on all dist interfaces, and r4 interfaces

Show ip protocols
Show ip ospf
Show ip ospf interface brief
Show ip ospf interface
Show ip ospf neighbor
Show ip ospf database
Show ip route ospf

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Router ID –
Area ID –
Authentication –
Data –

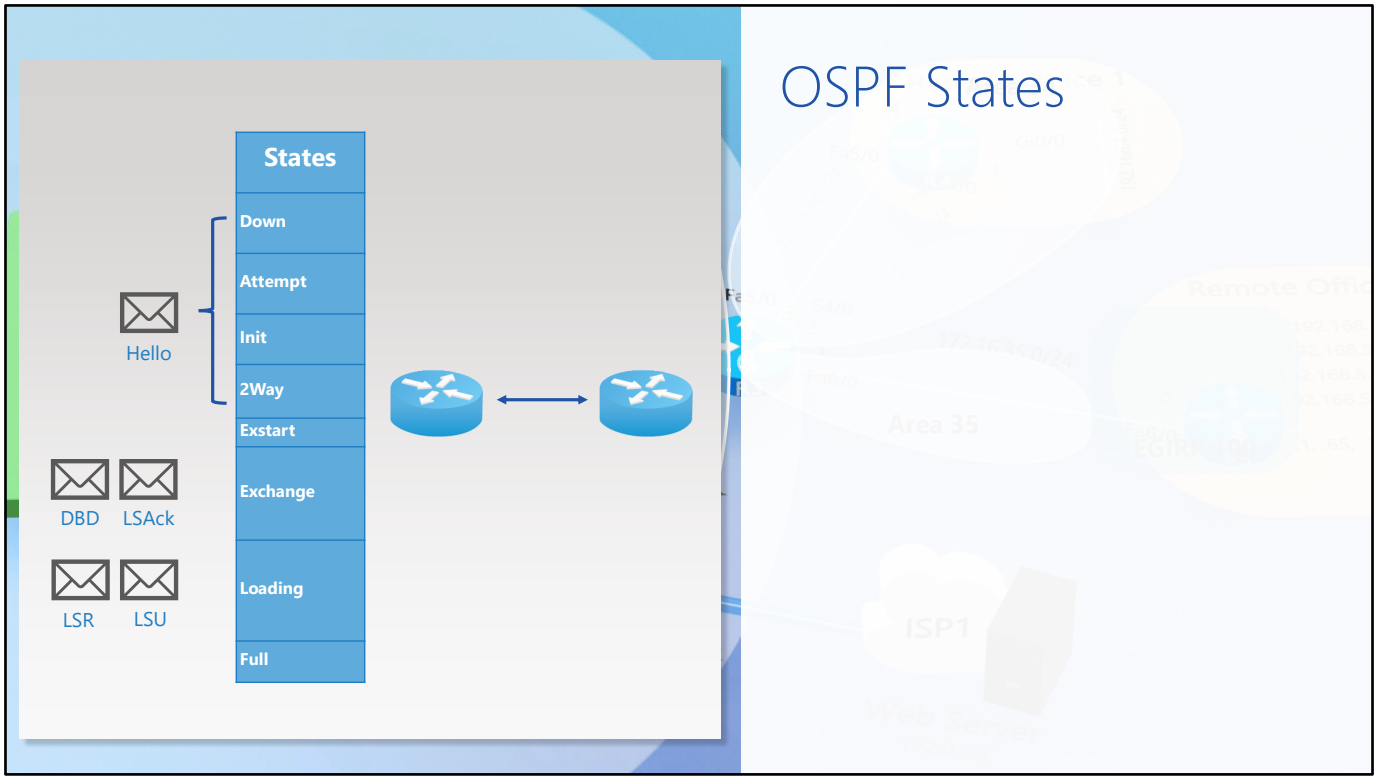
1) hello/dead interval
2) Neighbors
3) Router priority
4) DR IP address
5) BDR IP address
6) Stub area flag

Router ID (RID) - A unique 32-bit ID within an OSPF domain
Authentication Options - Allows A field that allows secure communication between OSPF routers to prevent malicious activity. Options are none, clear textplaintext, or mMessage dDigest 5 (MD5) authentication.
Area ID - The OSPF area that the OSPF interface belongs to. It is a 32-bit number that can be written in dot-decimal format (0.0.1.0) or decimal (256).
Interface Address Mask - The network mask for the primary IP address for the

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

interface that out which the hello is sent out.
Interface Priority - The router interface priority for DR elections.
Hello Interval - The time interval, in seconds, that at which a router sends out Hello hello packets on the interface.
Dead Interval - The time interval, in seconds, that a router will waits to hear a Hello hello from a neighbor router before it declares that router down.
Designated Router & and Backup Designated Router - The IP address of the DR and backup DR (BDR) for that network link.
Active Neighbor - A list of OSPF neighbors seen on that network segment. Must have received a Hello hello from the neighbor within the dead interval.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/13685-13.html

Down
This state indicates that no hellos have been received from a neighbor.

Attempt
This state occurs after a router sends a unicast hello (as opposed to a multicast hello) to a configured neighbor and has not yet received a hello from that neighbor.

Init
This state occurs on a router that has received a hello message from its neighbor; however, the OSPF RID of the receiving router was not contained in the hello message. If a router remains in this state for a long period, something is probably preventing that router from correctly receiving hello packets from the neighboring router.

2Way
This state occurs when two OSPF routers have received hello messages from each

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

other, and each router saw its own OSPF RID in the hello message it received. The 2Way state is an acceptable state to stay in between DROthers on an Ethernet LAN.

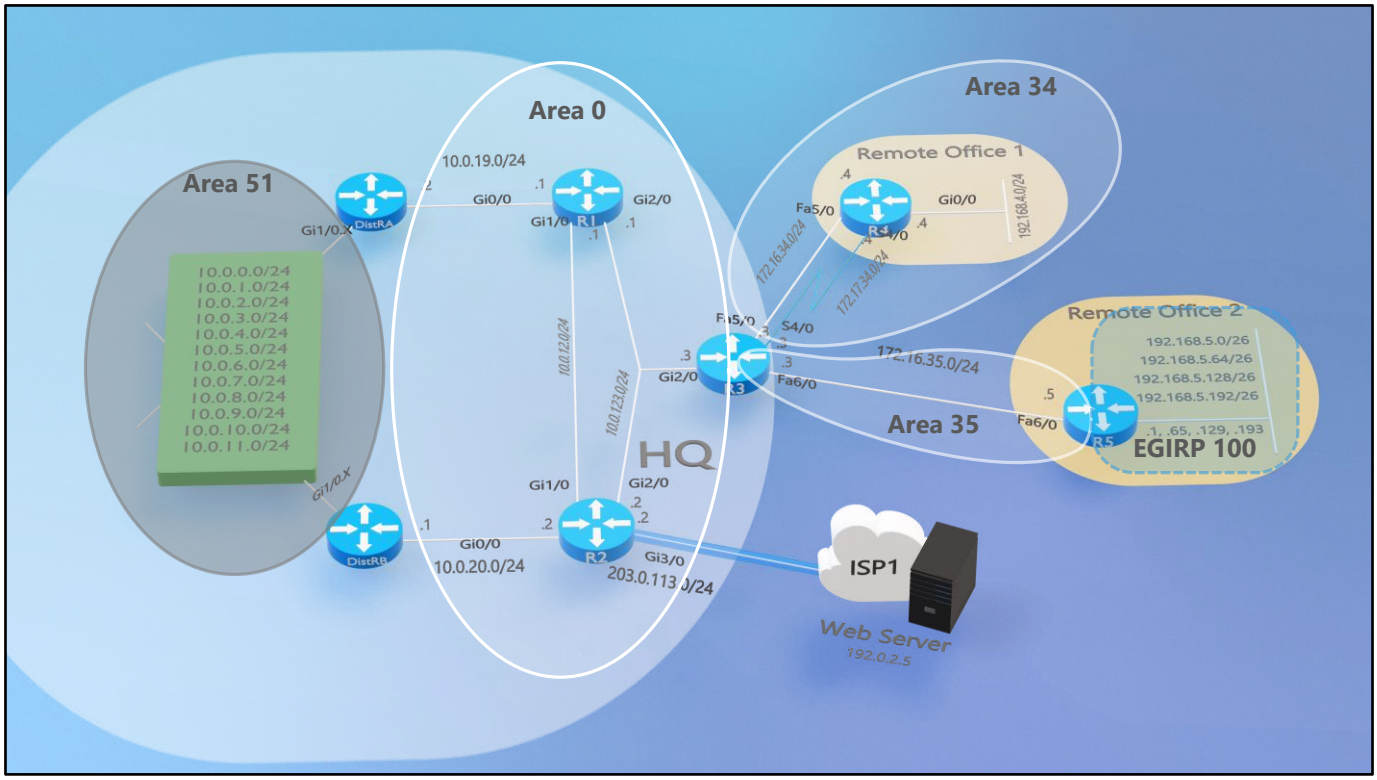
Exstart
This state occurs when the routers forming a full neighbor adjacency decide who will send their routing information first. This is accomplished using the RID. The router with the higher RID becomes the master and the other will become the slave. The master will send the routing information first. In a multiaccess network, the DR and BDR have to be determined first before this state starts. However, the DR does not have to be the master because each master/slave election is on a per-neighbor basis. If a router remains in this state for a long period, a maximum transmission unit (MTU) mismatch could exist between the neighboring routers, or a duplicate OSPF RID might exist.

Exchange
This state occurs when the two routers forming an adjacency send one another database descriptor (DBD) packets containing information about a router's link-state database. Each router compares the DBD packets received from the other router to identify missing entries in its own database. If a router remains in this state for a long period, an MTU mismatch could exist between the neighboring routers.

Loading
Based on the missing link-state database entries identified in the Exchange state, the Loading state occurs when each neighboring router requests the other router to send those missing entries. If a router remains in this state for a long period, a packet might have been corrupted, or a router might have a memory issue. Alternatively, it is possible that such a condition could result from the neighboring routers having an MTU mismatch.

Full
This state indicates that the neighboring OSPF routers have successfully exchanged their link-state information with one another, and an adjacency has been formed.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



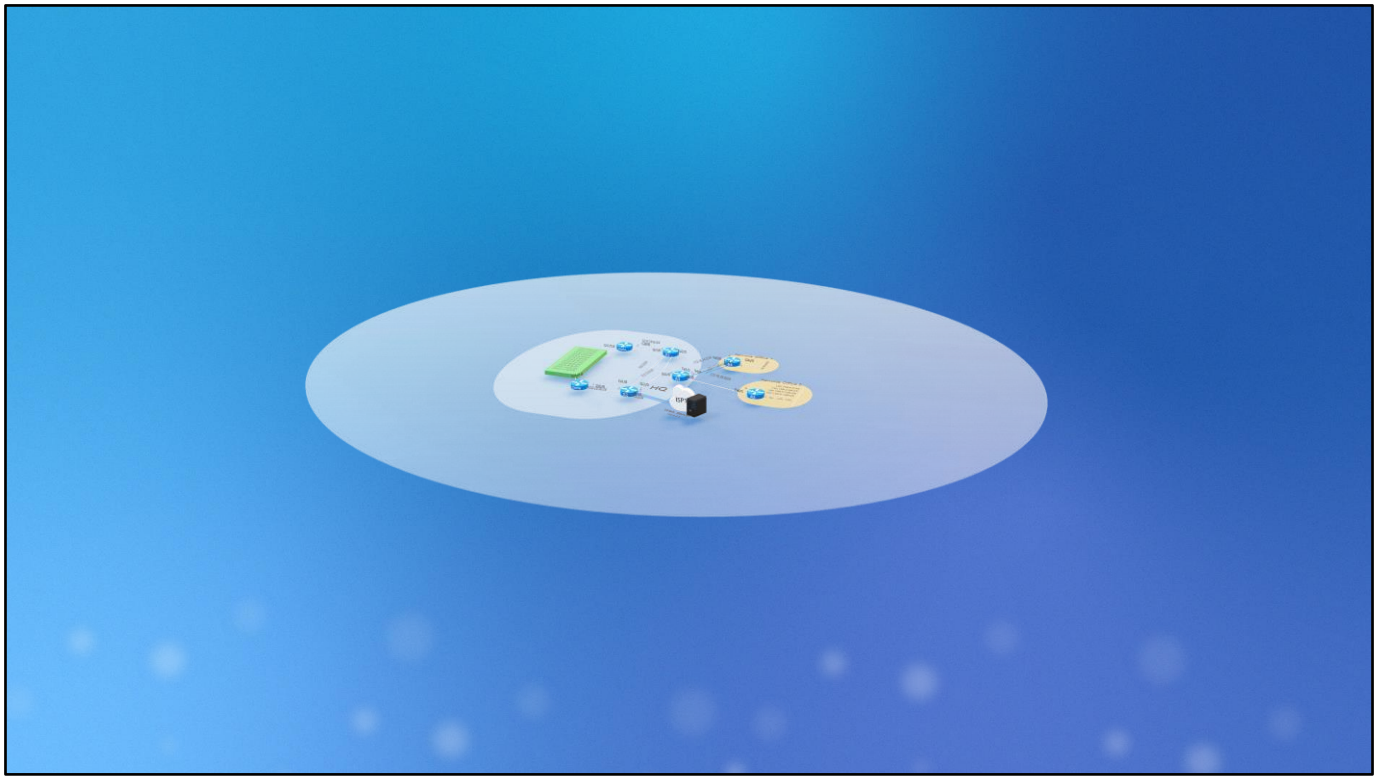
How do all of the routers share information with each other….LSAs

What information is shared…. Depends on scenario.

With EIGRP… easy… what ever your neighbor is using as the FD they will share with you.

With OSPF…. Depends on router type and area and more.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Title slide

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

OSPF Route Types

- O – OSPF destination in the same area
- OI – OSPF destination in a different area
- OE1/2 – Destination outside OSPF domain

```
DSW1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 10.0.120.2 to network 0.0.0.0

     172.17.0.0/24 is subnetted, 1 subnets
O IA    172.17.34.0 [110/658] via 10.0.10.1, 00:05:35, GigabitEthernet1/44
     172.16.0.0/24 is subnetted, 1 subnets
O IA    172.16.34.0 [110/21] via 10.0.10.1, 00:05:35, GigabitEthernet1/44
O IA 192.168.4.0/24 [110/22] via 10.0.10.1, 00:05:35, GigabitEthernet1/44
     10.0.0.0/24 is subnetted, 9 subnets
C       10.0.10.0 is directly connected, GigabitEthernet1/44
O       10.0.12.0 [110/11] via 10.0.10.1, 00:05:35, GigabitEthernet1/44
...output omitted...
O       10.0.20.0 [110/11] via 10.0.120.2, 00:05:35, Port-channel12
O       10.0.123.0 [110/11] via 10.0.10.1, 00:05:35, GigabitEthernet1/44
C       10.0.120.0 is directly connected, Port-channel12
O*E2 0.0.0.0/0 [110/1] via 10.0.120.2, 00:05:35, Port-channel12
               [110/1] via 10.0.10.1, 00:05:35, GigabitEthernet1/44
```

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

OSPF LSAs

Used to exchange link-state information between routers

- As soon as a neighborship is formed
- When a change occurs
- Every 30 mins

LSA Type	Description
1	Router LSA = O routes
2	Network LSA
3	Summary LSA = O IA routes
4	ASBR summary LSA
5	Autonomous system LSA = E routes



LSA Sequences

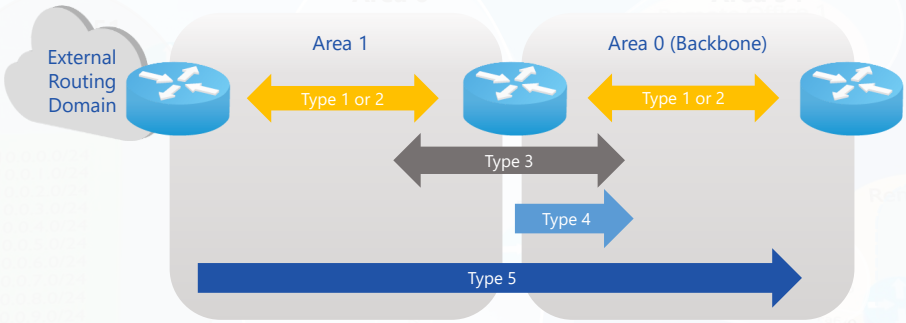
OSPF uses the sequence number to overcome problems caused by delays in LSA propagation in a network. The LSA sequence number is a 32-bit number used to control versioning. When the originating router sends out LSAs ~~out~~, the LSA sequence number is incremented. If a router receives an LSA sequence that is greater than the one in the LSDB, it processes the LSA. If the LSA sequence number is lower than the one in the LSDB, the router deems the LSA ~~as~~ old and discards ~~the LSA~~it.

LSA Age and Flooding

~~All~~ Every OSPF LSA~~s~~ includes an age that is entered in~~-~~to the local LSDB that increments by ~~one~~ 1 every second. When a router's OSPF LSA age exceeds 1800 seconds (that is, 30 minutes) for its networks, the originating router advertises a new LSA with the LSA age set to ~~zero~~0. As each router forwards the LSA, the LSA age is incremented with a calculated delay that reflects the link (~~it~~ which is minimal). If the LSA ~~Age~~ age reaches 3600, ~~then~~ the LSA is deemed invalid and is purged from the LSDB. The repetitive flooding of LSAs is a secondary safety mechanism to ensure that all routers maintain a consistent LSDB within an area.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

LSA Types



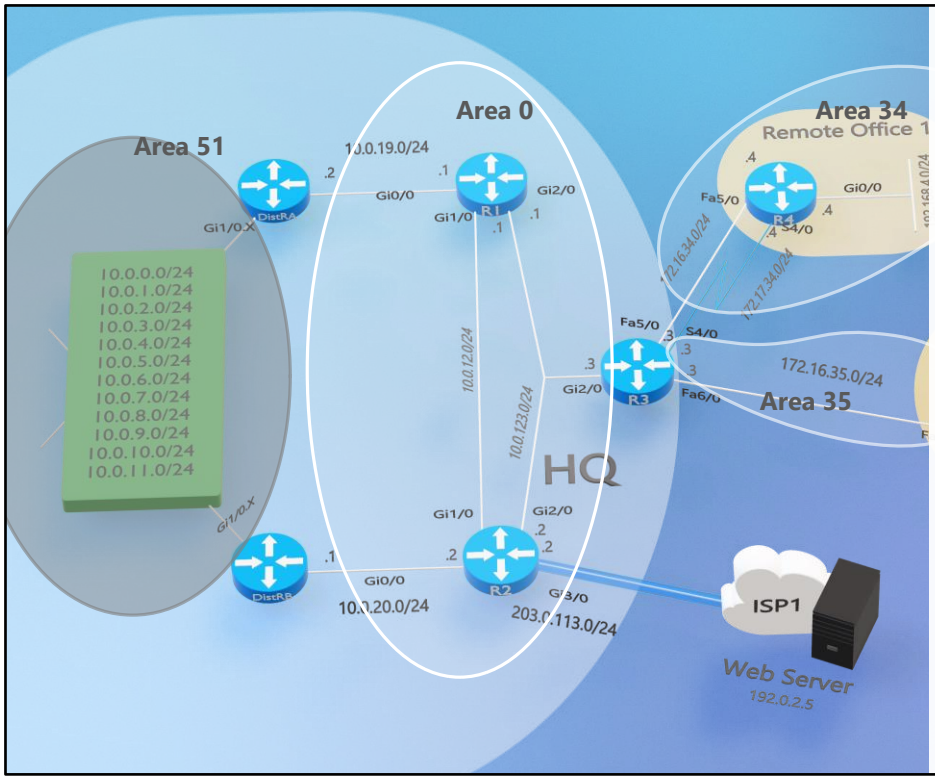
LSA Type	Description
1	Router LSA = O routes
2	Network LSA
3	Summary LSA = O IA routes
4	ASBR summary LSA
5	Autonomous system LSA = E routes

1: (router) every router in area generates (state of router links & the cost to each)
2: (Net) Generated by DR & flooded (in bcast – more than 2 routers) to tell all routers about a new network {when new type 2 & 3's are rec'd – run SPF algo}

- **DR**: When there is a change in the network status, instead of flooding each and every path with the LSAs, the update is only sent to the DR. The DR then floods the routers in its network segment with the update.

3: Generated by ABR & advertised between/among areas
4: Only used if the prescence of ASBR
5: Generated by an ASBR for advertising external routes (eigrp route)

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



LSA Types

LSA Type	Description
1	Router LSA = O routes
2	Network LSA
3	Summary LSA = O IA routes
4	ASBR summary LSA
5	Autonomous system LSA = E routes

LSA's used to create LSDB LSA Types:

Type 1 – Router

Generated by all OSPF routers and floods to all routers in an area. Describes routers and connected OSPF enabled interfaces.

Type 2 – Network

Generated by DR and floods to all routers in an area. Describes multi-access network DR is connected to.

Type 3 – Summary

Generated by ABR and flooded into a different area. Describes networks outside of area but still within OSPF domain.

Type 4 – ASBR Summary

Generated by ABR, flooded into an area, describes how to reach ASBR

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

outside of area.

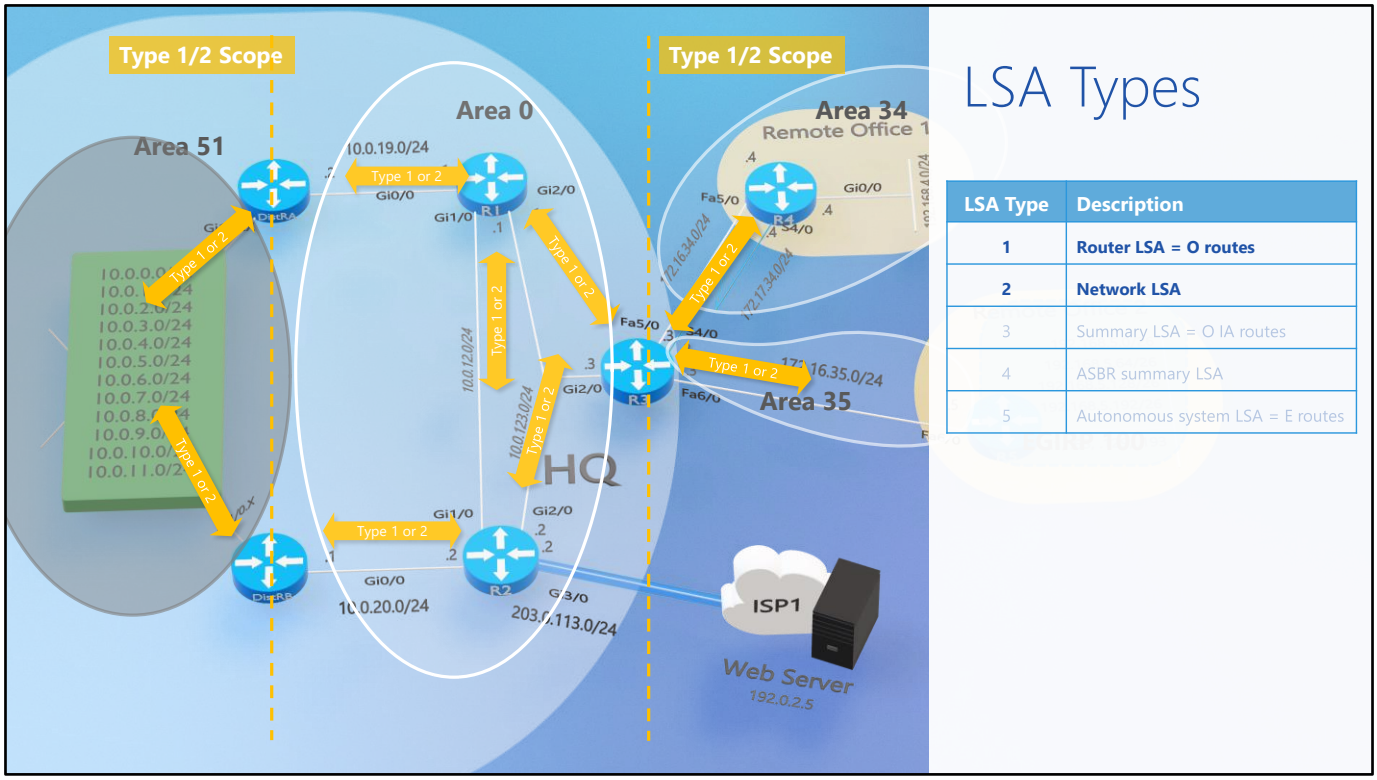
Type 5 – External Link

Generated by ASBR, flooded throughout entire OSPF domain. Describes external networks.

Type 7 – NSSA External Link

Generated by ASBR and flooded into area. Describes external routes to the NSSA area.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



LSA Types

LSA Type	Description
1	Router LSA = O routes
2	Network LSA
3	Summary LSA = O IA routes
4	ASBR summary LSA
5	Autonomous system LSA = E routes

LSA's used to create LSDB LSA Types:

Type 1 – Router

Generated by all OSPF routers and floods to all routers in an area. Describes routers and connected OSPF enabled interfaces.

Type 2 – Network

Generated by DR and floods to all routers in an area. Describes multi-access network DR is connected to.

Type 3 – Summary

Generated by ABR and flooded into a different area. Describes networks outside of area but still within OSPF domain.

Type 4 – ASBR Summary

Generated by ABR, flooded into an area, describes how to reach ASBR

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

outside of area.

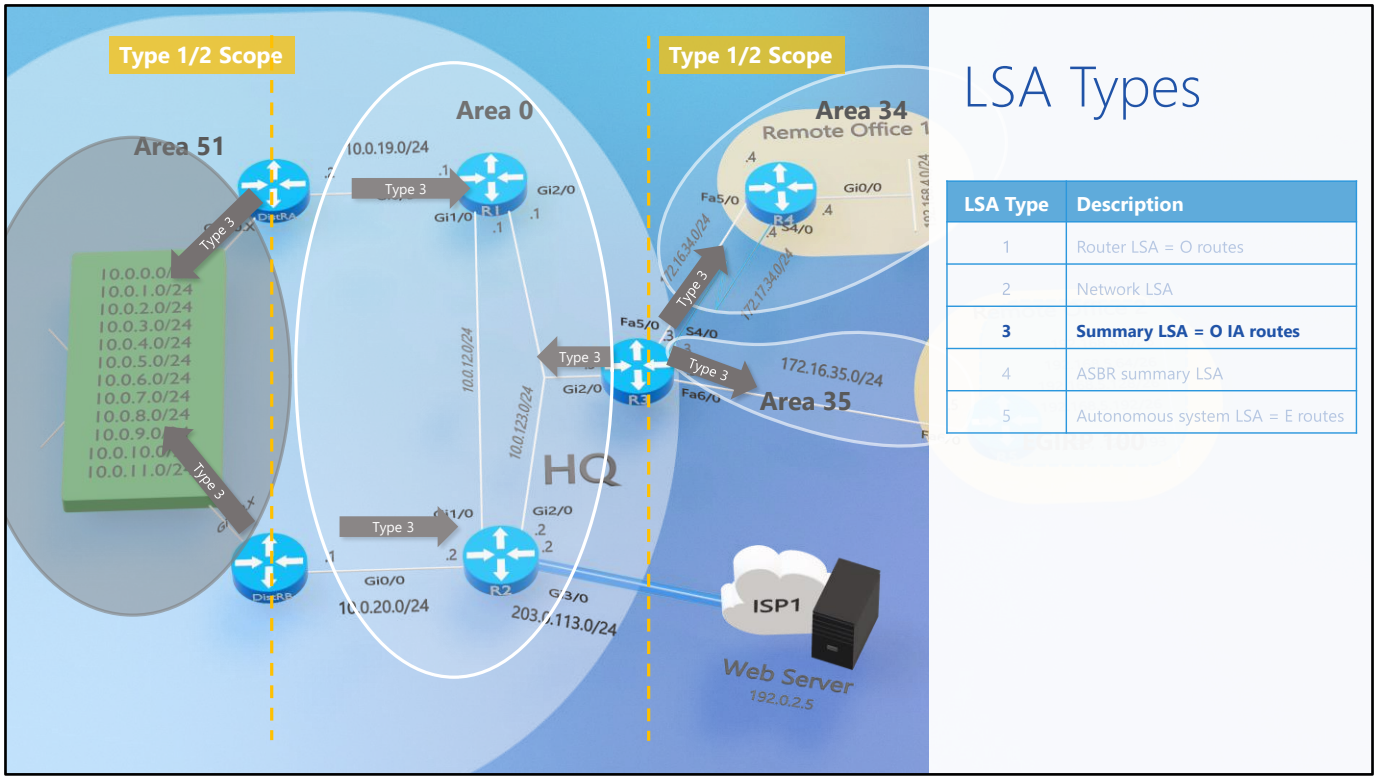
Type 5 – External Link

Generated by ASBR, flooded throughout entire OSPF domain. Describes external networks.

Type 7 – NSSA External Link

Generated by ASBR and flooded into area. Describes external routes to the NSSA area.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



LSA Types

LSA Type	Description
1	Router LSA = O routes
2	Network LSA
3	**Summary LSA = O IA routes**
4	ASBR summary LSA
5	Autonomous system LSA = E routes

LSA's used to create LSDB LSA Types:

Type 1 – Router

Generated by all OSPF routers and floods to all routers in an area. Describes routers and connected OSPF enabled interfaces.

Type 2 – Network

Generated by DR and floods to all routers in an area. Describes multi-access network DR is connected to.

Type 3 – Summary

Generated by ABR and flooded into a different area. Describes networks outside of area but still within OSPF domain.

Type 4 – ASBR Summary

Generated by ABR, flooded into an area, describes how to reach ASBR

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

outside of area.

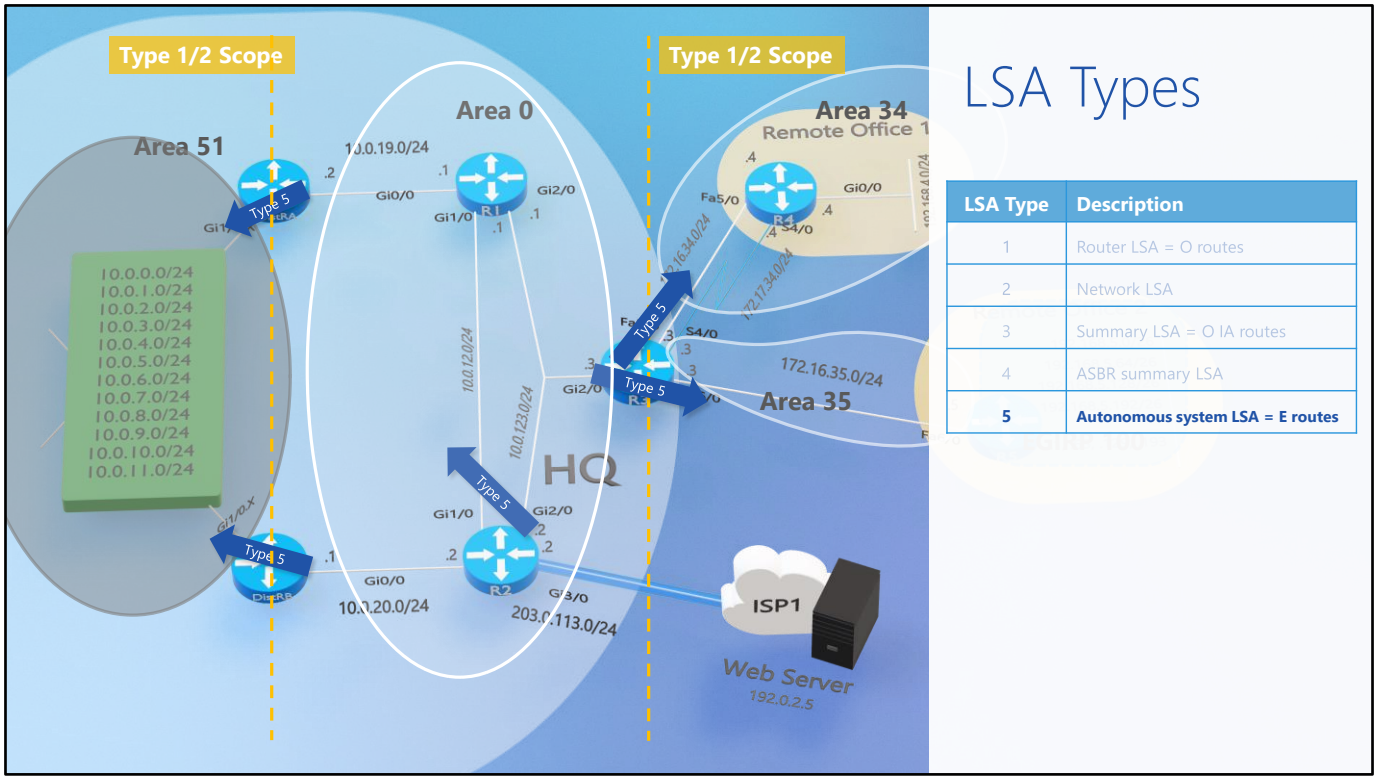
Type 5 – External Link

Generated by ASBR, flooded throughout entire OSPF domain. Describes external networks.

Type 7 – NSSA External Link

Generated by ASBR and flooded into area. Describes external routes to the NSSA area.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



LSA Types

LSA Type	Description
1	Router LSA = O routes
2	Network LSA
3	Summary LSA = O IA routes
4	ASBR summary LSA
5	**Autonomous system LSA = E routes**

LSA's used to create LSDB LSA Types:

Type 1 – Router

Generated by all OSPF routers and floods to all routers in an area. Describes routers and connected OSPF enabled interfaces.

Type 2 – Network

Generated by DR and floods to all routers in an area. Describes multi-access network DR is connected to.

Type 3 – Summary

Generated by ABR and flooded into a different area. Describes networks outside of area but still within OSPF domain.

Type 4 – ASBR Summary

Generated by ABR, flooded into an area, describes how to reach ASBR

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

outside of area.

Type 5 – External Link

Generated by ASBR, flooded throughout entire OSPF domain. Describes external networks.

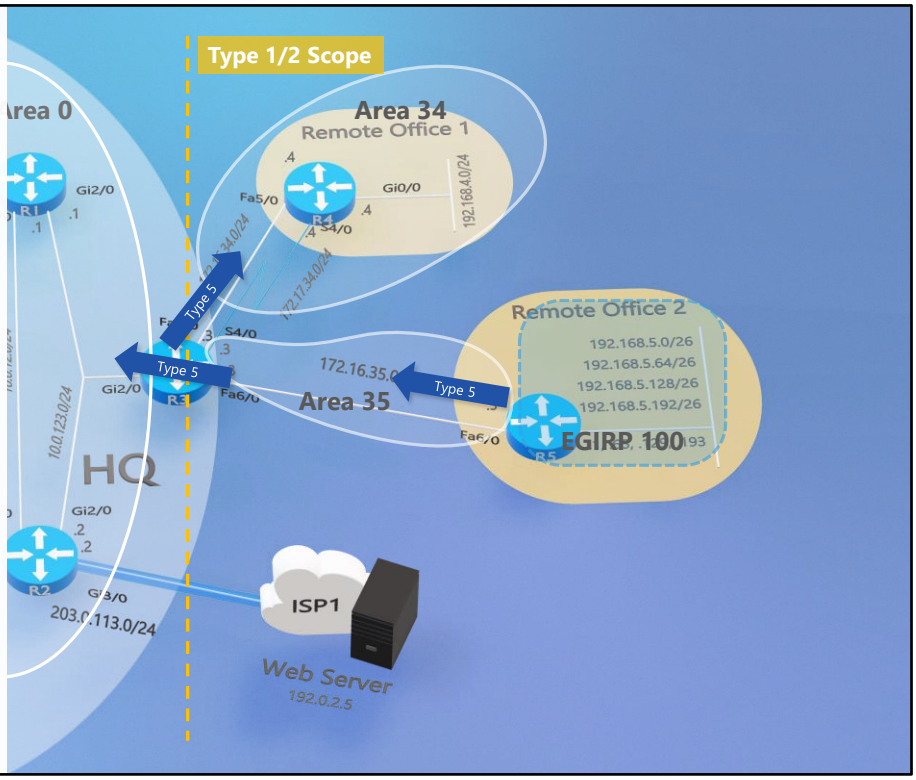
Type 7 – NSSA External Link

Generated by ASBR and flooded into area. Describes external routes to the NSSA area.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

LSA Types

LSA Type	Description
1	Router LSA = O routes
2	Network LSA
3	Summary LSA = O IA routes
4	ASBR summary LSA
5	**Autonomous system LSA = E routes**



LSA's used to create LSDB LSA Types:

Type 1 – Router

Generated by all OSPF routers and floods to all routers in an area. Describes routers and connected OSPF enabled interfaces.

Type 2 – Network

Generated by DR and floods to all routers in an area. Describes multi-access network DR is connected to.

Type 3 – Summary

Generated by ABR and flooded into a different area. Describes networks outside of area but still within OSPF domain.

Type 4 – ASBR Summary

Generated by ABR, flooded into an area, describes how to reach ASBR

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

outside of area.

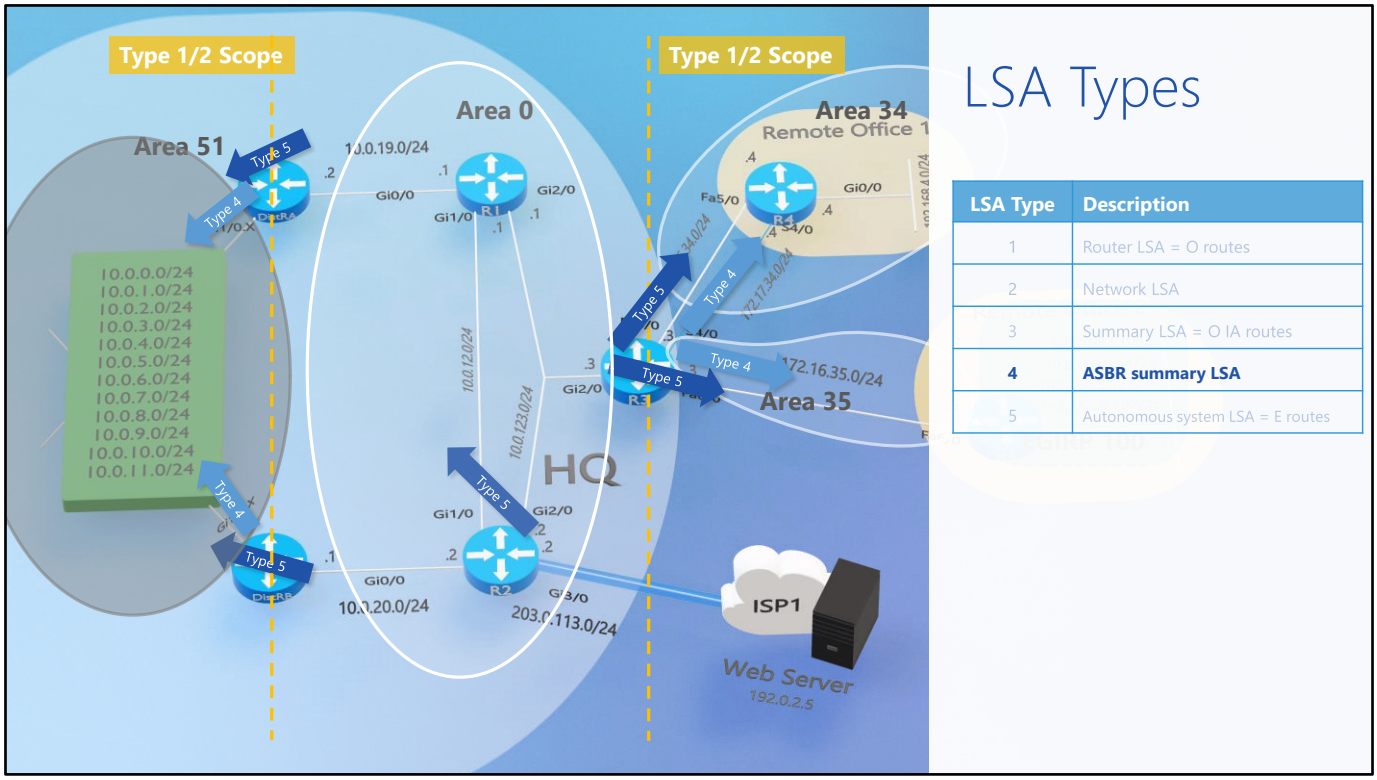
Type 5 – External Link

Generated by ASBR, flooded throughout entire OSPF domain. Describes external networks.

Type 7 – NSSA External Link

Generated by ASBR and flooded into area. Describes external routes to the NSSA area.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



LSA Types

LSA Type	Description
1	Router LSA = O routes
2	Network LSA
3	Summary LSA = O IA routes
4	**ASBR summary LSA**
5	Autonomous system LSA = E routes

LSA's used to create LSDB LSA Types:

Type 1 – Router

Generated by all OSPF routers and floods to all routers in an area. Describes routers and connected OSPF enabled interfaces.

Type 2 – Network

Generated by DR and floods to all routers in an area. Describes multi-access network DR is connected to.

Type 3 – Summary

Generated by ABR and flooded into a different area. Describes networks outside of area but still within OSPF domain.

Type 4 – ASBR Summary

Generated by ABR, flooded into an area, describes how to reach ASBR

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

outside of area.

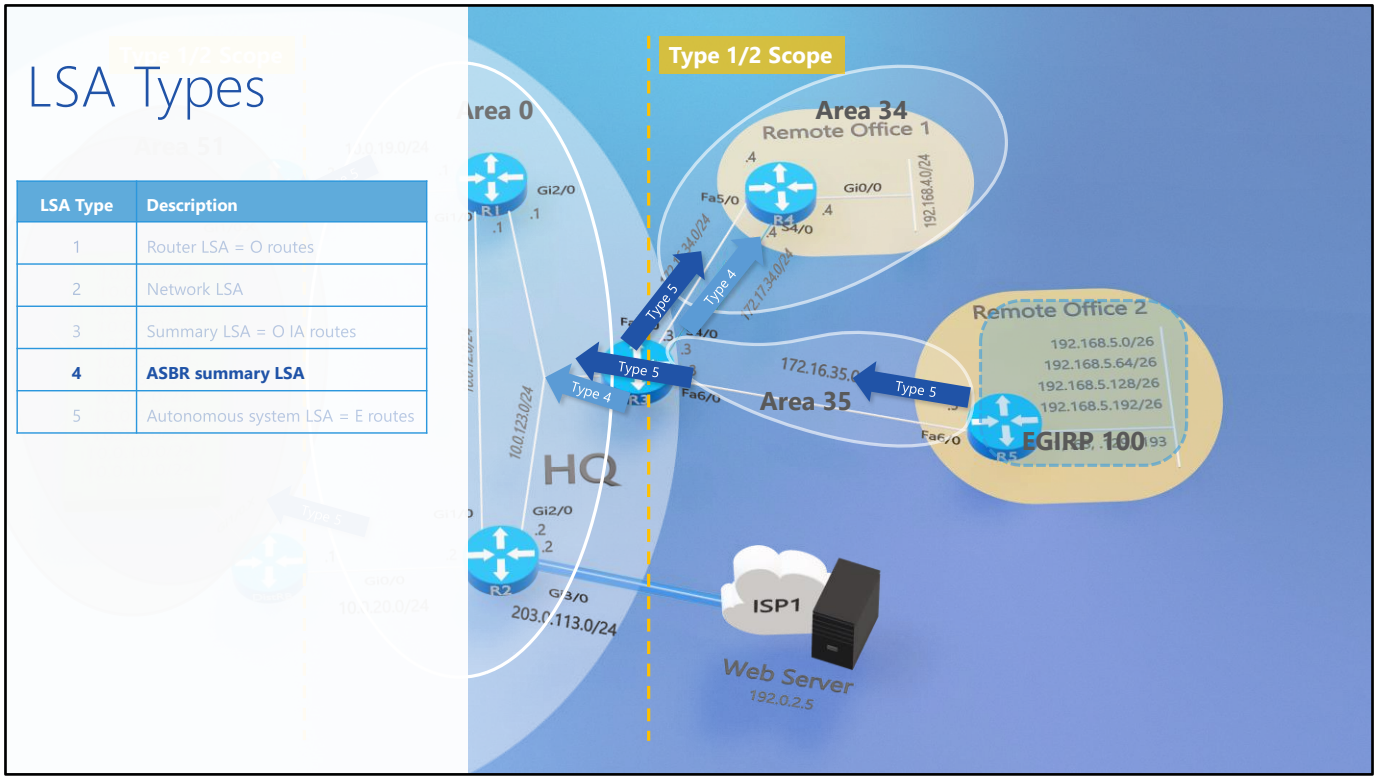
Type 5 – External Link

Generated by ASBR, flooded throughout entire OSPF domain. Describes external networks.

Type 7 – NSSA External Link

Generated by ASBR and flooded into area. Describes external routes to the NSSA area.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



LSA's used to create LSDB LSA Types:

Type 1 – Router

Generated by all OSPF routers and floods to all routers in an area. Describes routers and connected OSPF enabled interfaces.

Type 2 – Network

Generated by DR and floods to all routers in an area. Describes multi-access network DR is connected to.

Type 3 – Summary

Generated by ABR and flooded into a different area. Describes networks outside of area but still within OSPF domain.

Type 4 – ASBR Summary

Generated by ABR, flooded into an area, describes how to reach ASBR

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

outside of area.

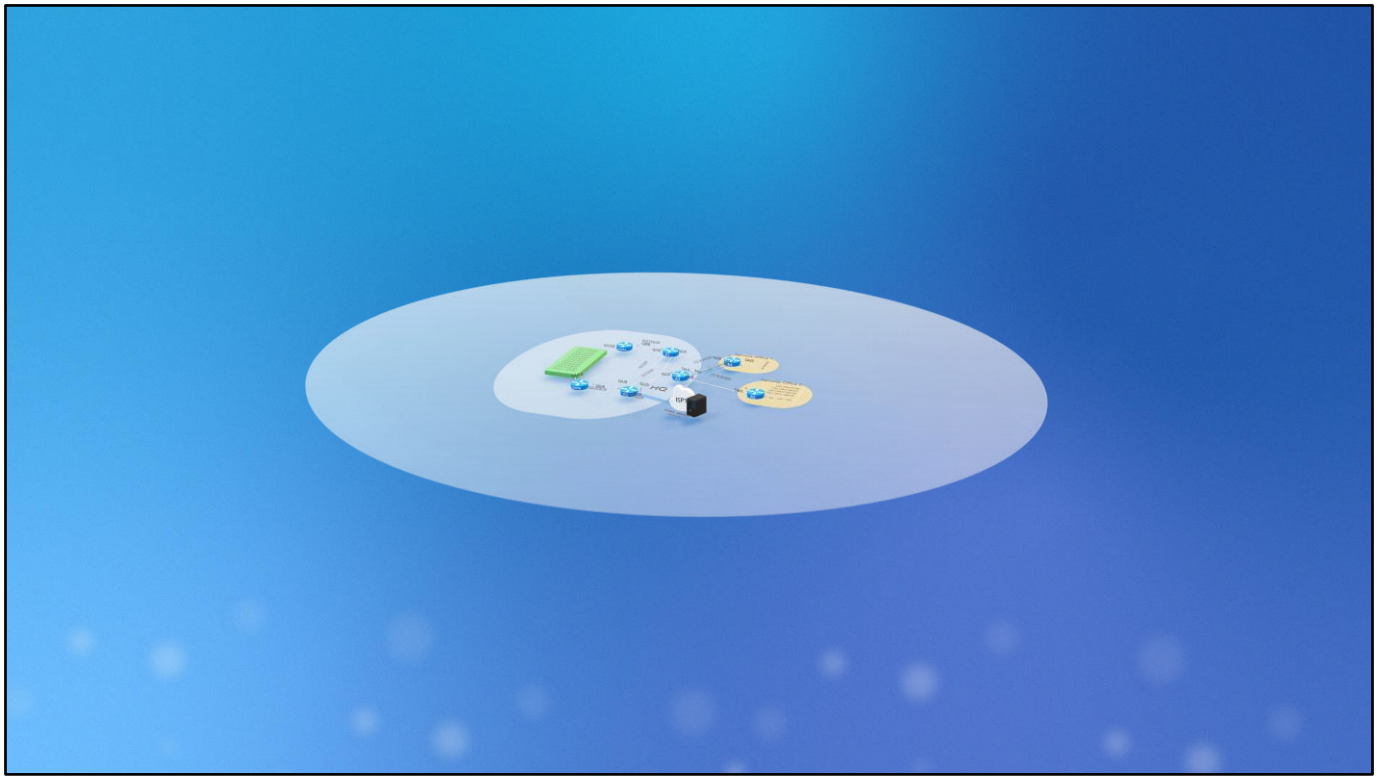
Type 5 – External Link

Generated by ASBR, flooded throughout entire OSPF domain. Describes external networks.

Type 7 – NSSA External Link

Generated by ASBR and flooded into area. Describes external routes to the NSSA area.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

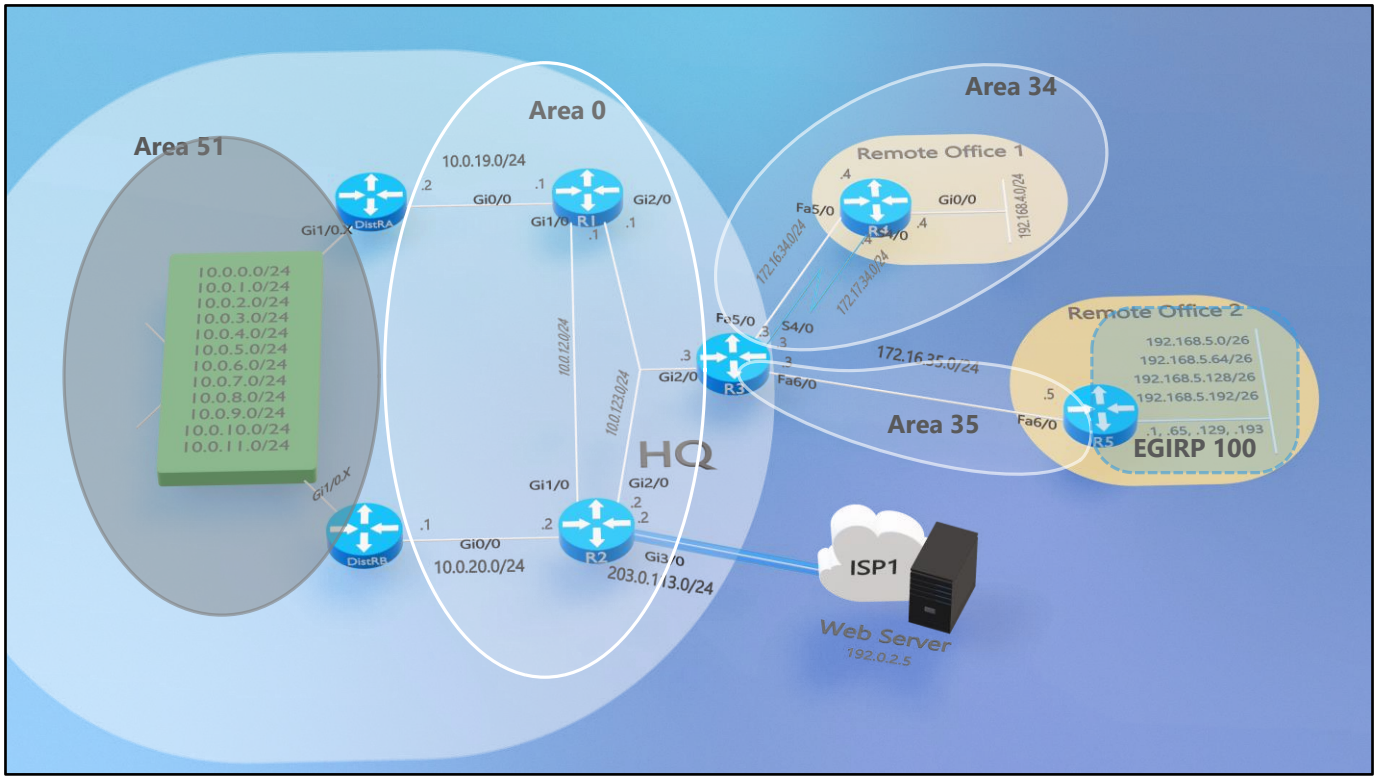


©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Title slide

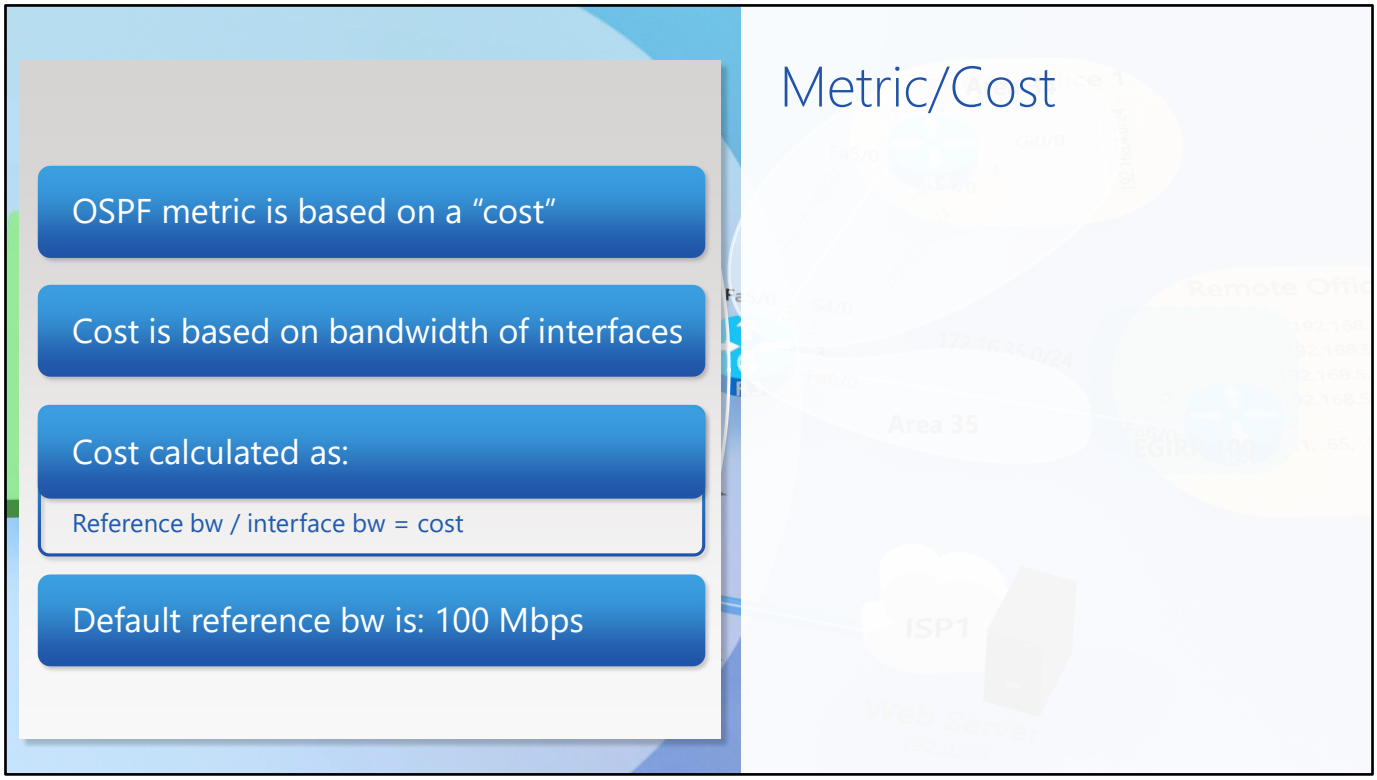
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



COST DISCUSSION

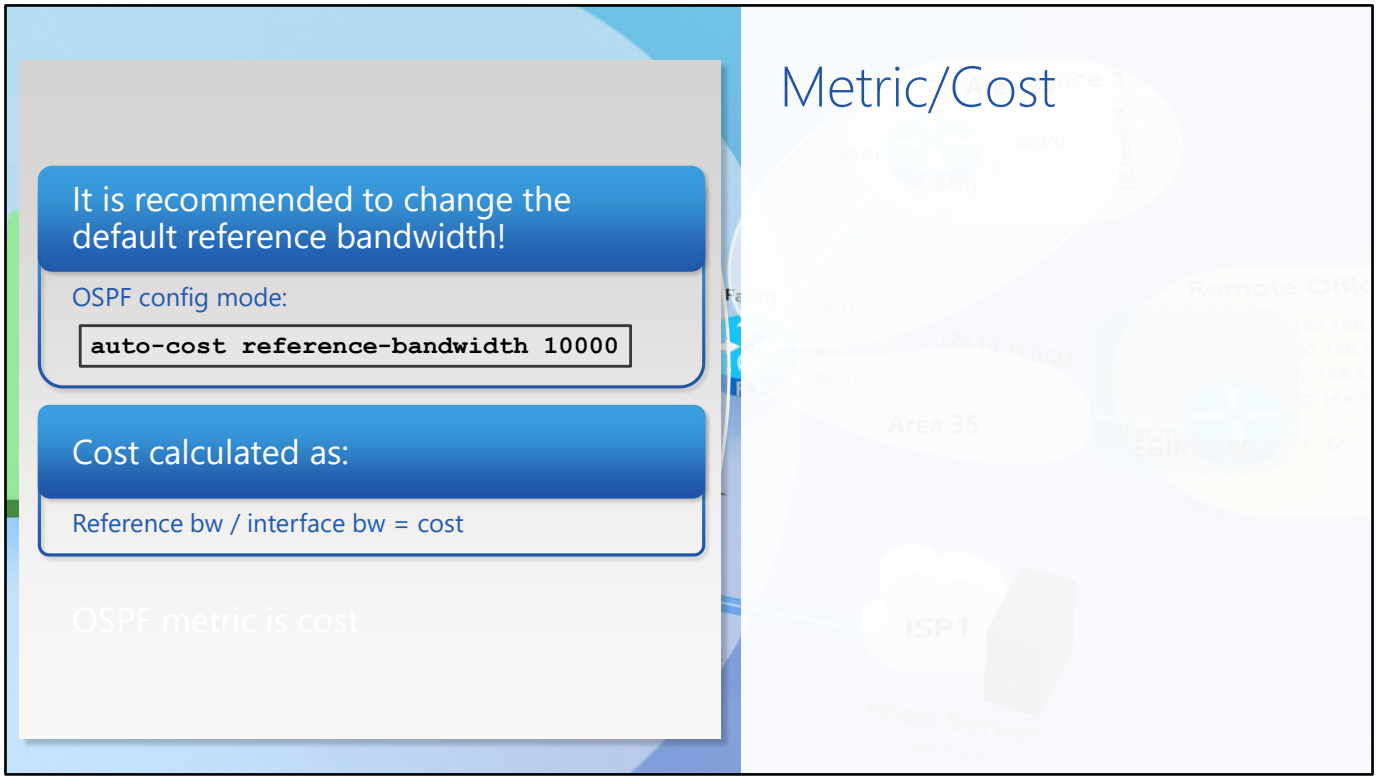
How is cost calculated????

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



100 mbps, 1G, or 10G = cost of 1

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



100 mbps, 1G, or 10G = cost of 1

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

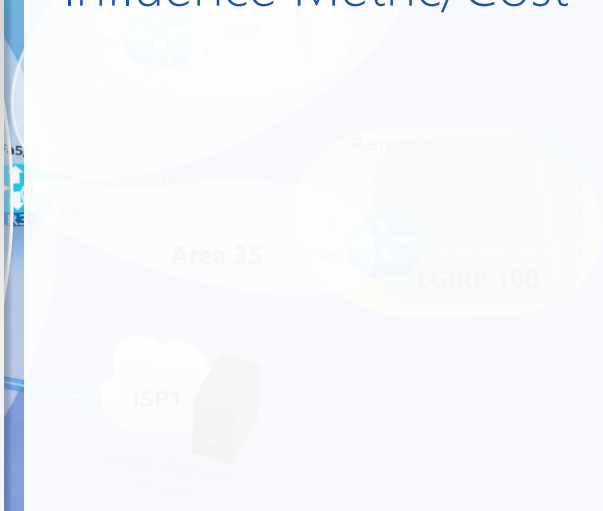
Additional Ways to Influence Metric/Cost

Manually set the cost per Interface

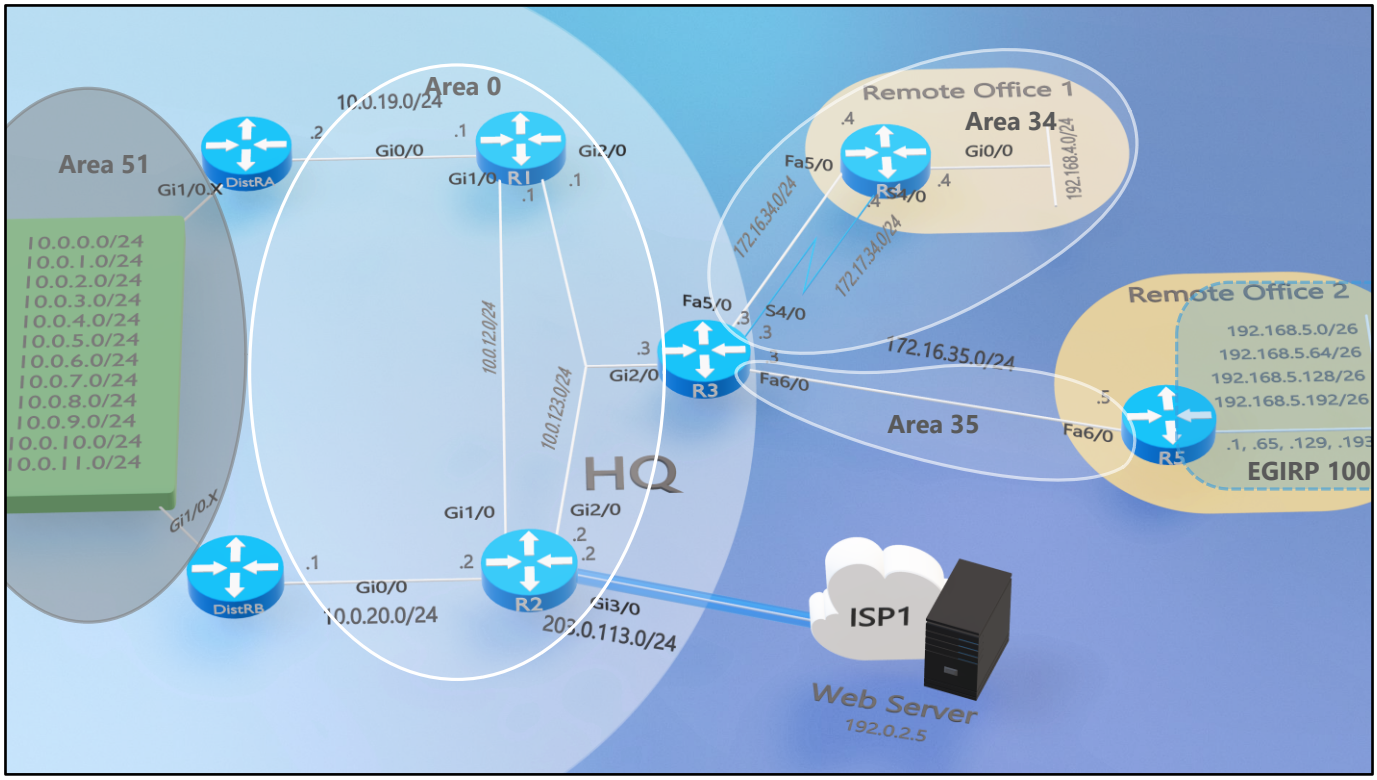
```
interface serial 1/0
   ip ospf cost 100
```

Manually increase interface bandwidth

```
interface fa 0/0
   bandwidth 10000
```



©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



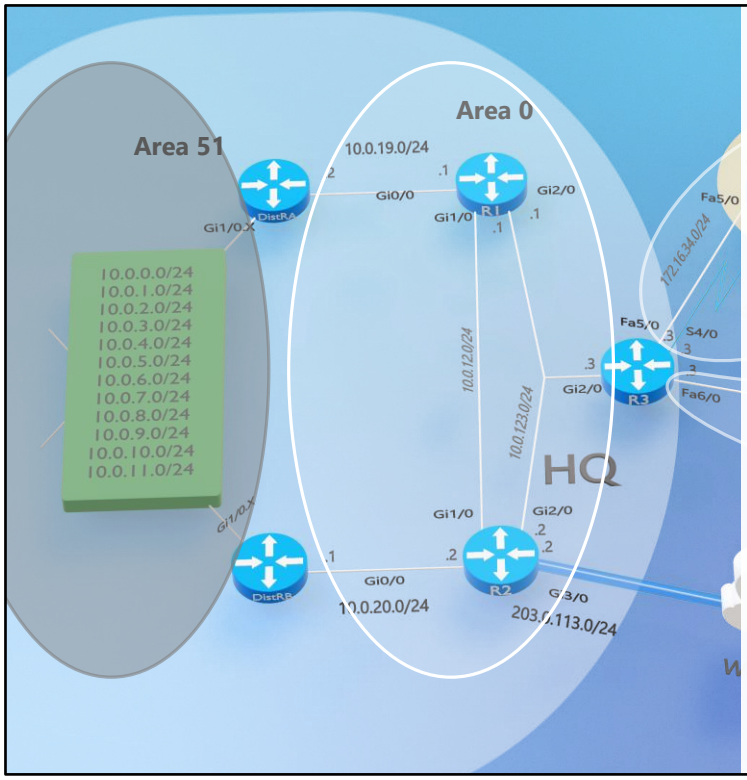
How total cost is calculated depends on where the network is…..

If it is an O route…. Calculated based on the Dyjkstra SPT calculation to get there.

If it is an OIA route…. Calculated based on the Dyjkstra SPT calculation to get to the ABR + what the ABR has included in its TYPE3 LSA.

If it is an E route…. Depends on Metric-Type E1 vs E2. With E2 the metric injected by the ASBR is preserved throughout the entire OSPF domain. If it is E1 it is based on the metric injected by the ASBR + the metric used to get to the ASBR. More on this later in our redistribution discussion.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Router Decision Making Process

Determine best source of information using AD

If the best source is OSPF, prefer route type:

- O – OSPF destination in the same area
- OI – OSPF destination in a different area
- OE1 – Destination outside OSPF domain
- ON1 – Destination outside OSPF domain
- OE2 – Destination outside OSPF domain
- ON2 – Destination outside OSPF domain

If there is a tie within route type:

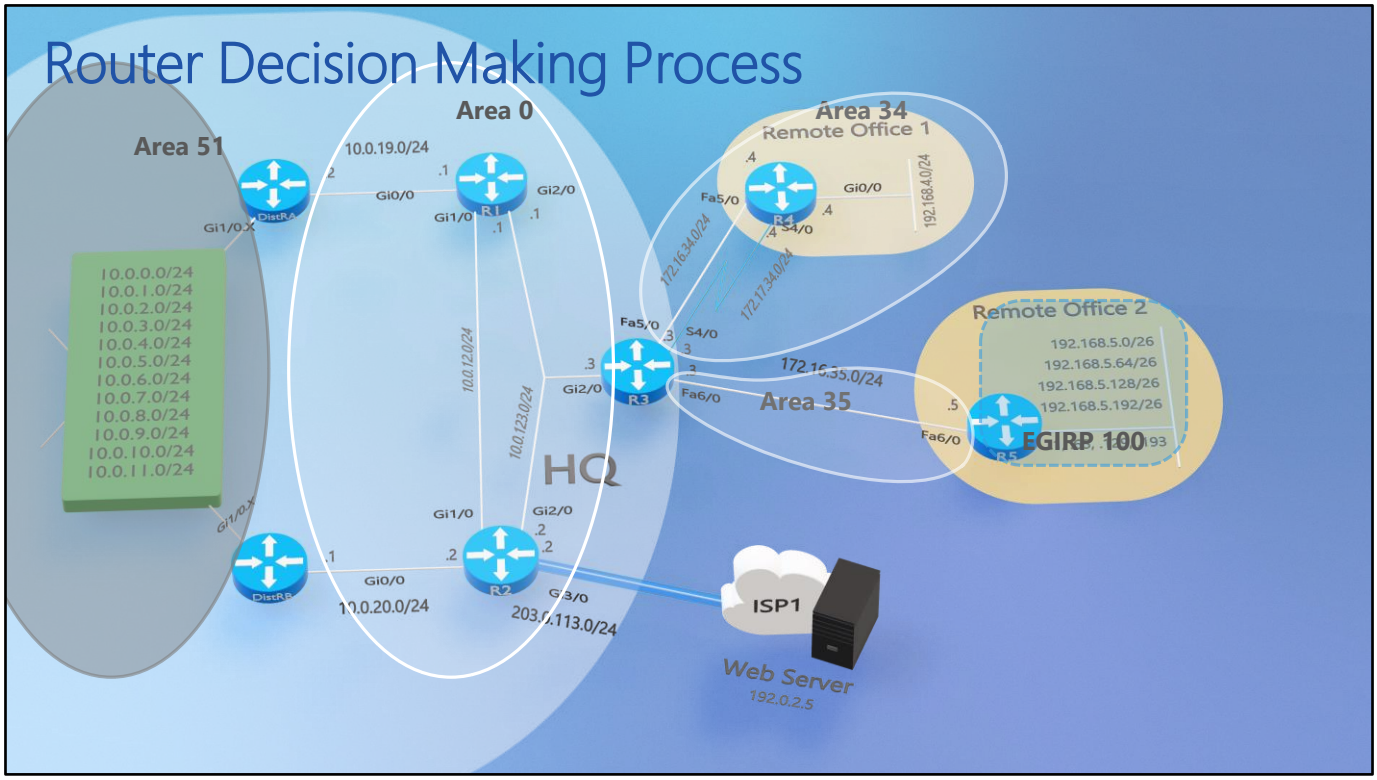
- Use metric to break the tie / load balance

Instructor Notes:
Draw:
Let's say for the sake of this scenario that Gi1/0.x on DISTRA and DISTRB are not passive.

Consider R2 learns 10.0.19.0/24 from R1 as an O router and it will learn it from DISTRB as a OIA route.

It makes sense now that R2 should prefer the O router over the OIA route because it is in the same area. If for some reason Gi1/ and 2/0 went down on R1 then R2 would use the OIA route from DISTRB because it is the only option available.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

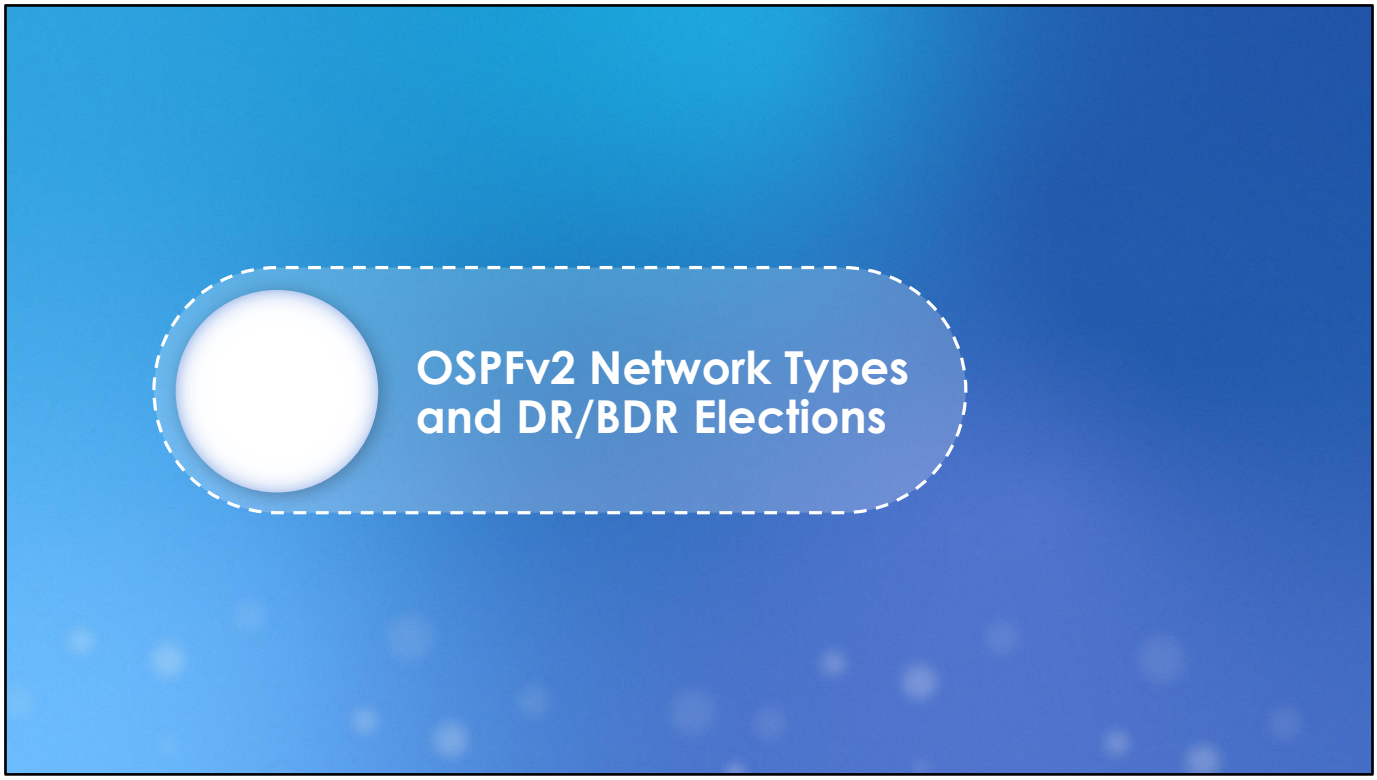


©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



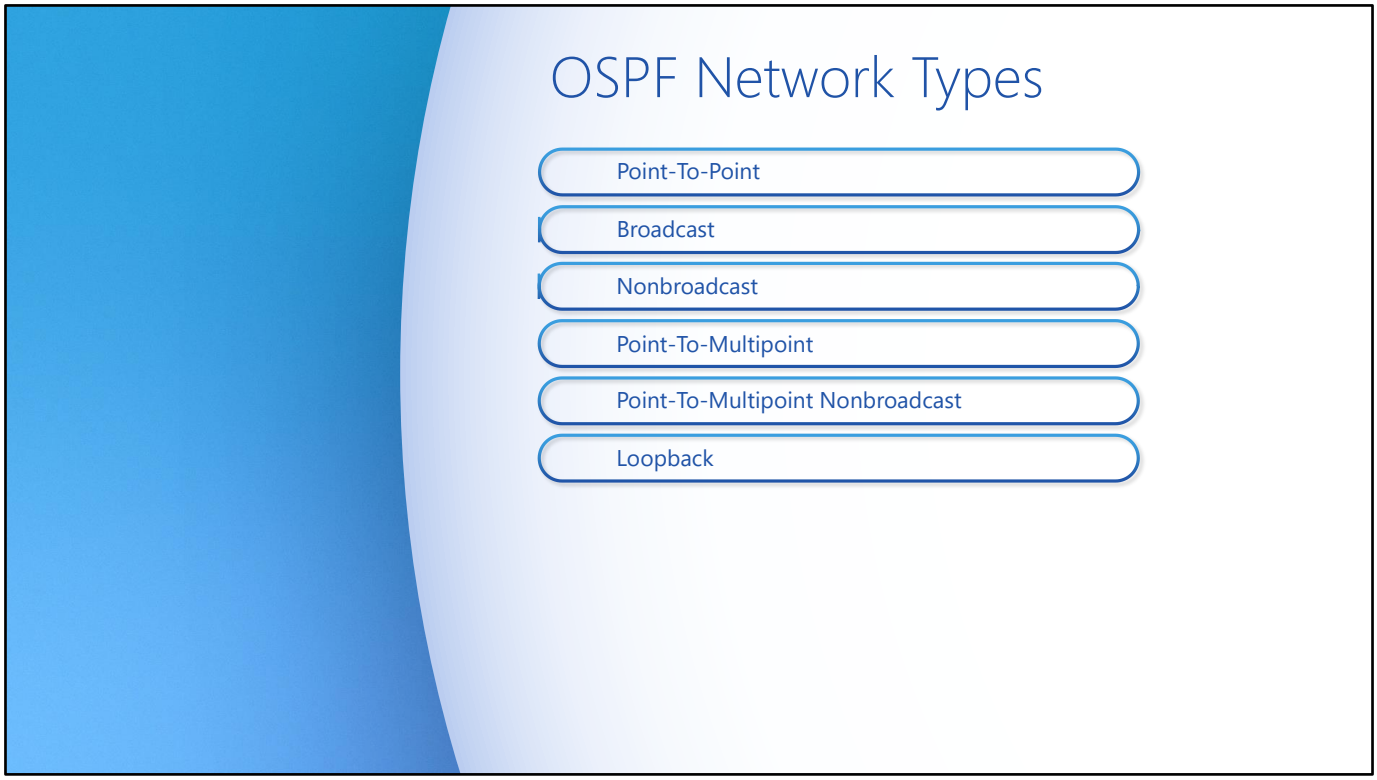
Demo: How did DistRA come up with metric for 192.168.4.0/24
COST is cumulative

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



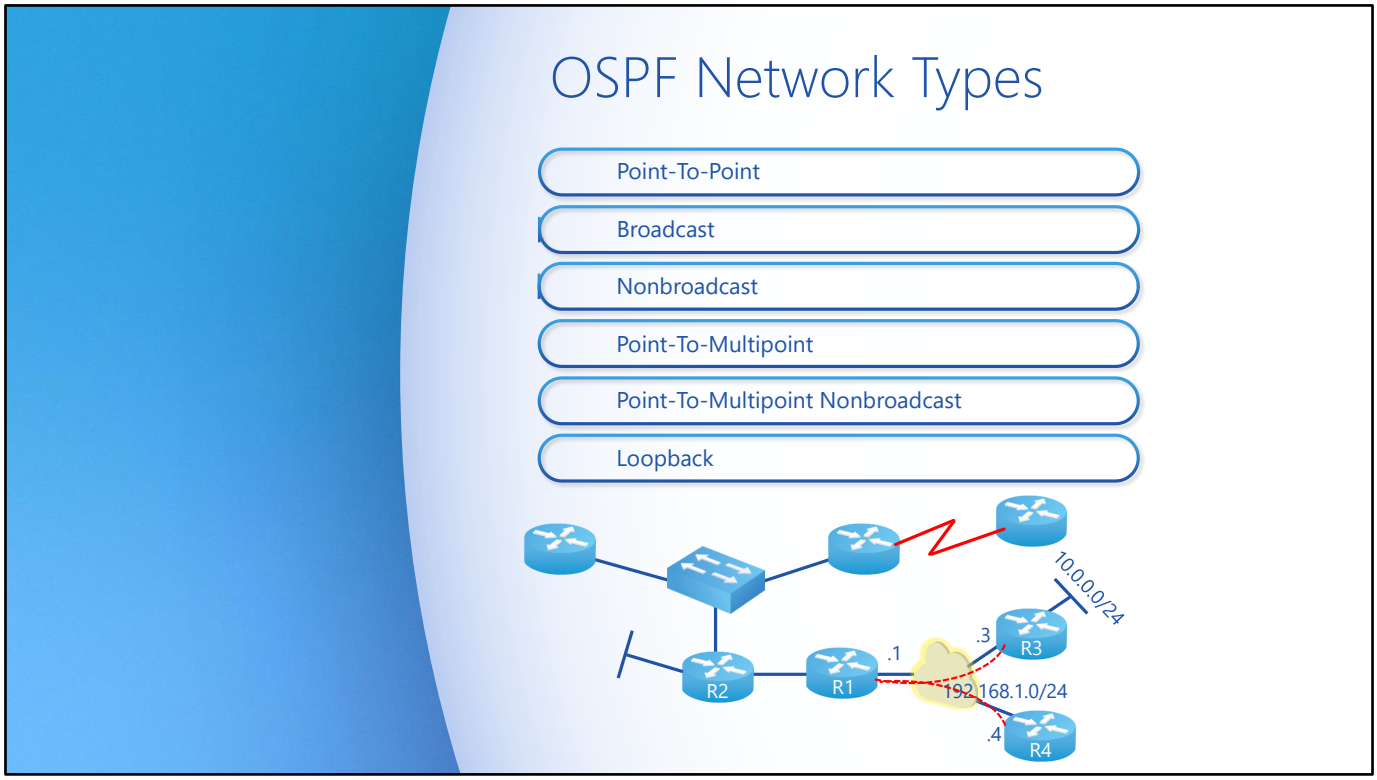
Title slide

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



The default OSPF network type is set based on the media used for the connection and can be changed independently of the actual media type used. Cisco's implementation of OSPF considers the various ~~mediums~~ media and provides five OSPF network types.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



The default OSPF network type is set based on the media used for the connection and can be changed independently of the actual media type used. Cisco's implementation of OSPF considers the various ~~mediums~~ media and provides five OSPF network types.

Broadcast - Ethernet

Default setting on OSPF--enabled Ethernet links.
DR/BDR Elected Yes
Hello: 10
Wait: 40
Dead: 40

Nonbroadcast - Frame Relay, ATM, and X.25

Default setting on enabled OSPF Frame Relay main interface or Frame Relay multipoint subinterfaces.
DR/BDR Elected Yes
Hello: 30
Wait: 120
Dead: 120

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Point-to-point – HDLC, PPP, GRE, FrameRelay subinterfaces

Default setting on enabled OSPF Frame Relay point-to-point subinterfaces or serial interfaces using PPP or HDLC
DR/BDR Elected No
Hello: 10
Wait: 40
Dead: 40

Point-to-multipoint

Not enabled by default on any interface type.
Primarily used for hub-and-spoke topologies so that it behaves like a bunch of point to point links
DR/BDR Elected No
Hello: 30
Wait: 120
Dead: 120

Point-to-multipoint Nonbroadcast

Not enabled by default on any interface type.
Primarily used for hub-and-spoke topologies so that it behaves like a bunch of point to point links, but it supports static neighbor adjacencies for networks that do not support multicast… in addition it allows you to control the cost to each neighbor on an individual by individual basis where the other options all neighbors have the same cost.
DR/BDR Elected No
Hello: 30
Wait: 120
Dead: 120

Loopback – default for loopback

Default setting on OSPF enabled loopback interfaces.
Interface is advertised as a host route (/32).
N/A
N/A

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

OSPF Network Types

	Timers	Neighbors	DR Election
Point-To-Point	10/40	Dynamic	No
Broadcast	10/40	Dynamic	Yes
Nonbroadcast	30/120	Static	Yes
Point-To-Multipoint	30/120	Dynamic	No
Point-To-Multipoint Nonbroadcast	30/120	Static	No
Loopback	N/A	N/A	N/A

The default OSPF network type is set based on the media used for the connection and can be changed independently of the actual media type used. Cisco's implementation of OSPF considers the various ~~mediums~~ media and provides five OSPF network types.

Broadcast - Ethernet

Default setting on OSPF--enabled Ethernet links.
DR/BDR Elected Yes
Hello: 10
Wait: 40
Dead: 40

Nonbroadcast - Frame Relay, ATM, and X.25

Default setting on enabled OSPF Frame Relay main interface or Frame Relay multipoint subinterfaces.
DR/BDR Elected Yes
Hello: 30
Wait: 120
Dead: 120

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Point-to-point – HDLC, PPP, GRE, FrameRelay subinterfaces

Default setting on enabled OSPF Frame Relay point-to-point subinterfaces or serial interfaces using PPP or HDLC
DR/BDR Elected No
Hello: 10
Wait: 40
Dead: 40

Point-to-multipoint

Not enabled by default on any interface type.
Primarily used for hub-and-spoke topologies so that it behaves like a bunch of point to point links
DR/BDR Elected No
Hello: 30
Wait: 120
Dead: 120

Point-to-multipoint Nonbroadcast

Not enabled by default on any interface type.
Primarily used for hub-and-spoke topologies so that it behaves like a bunch of point to point links, but it supports static neighbor adjacencies for networks that do not support multicast… in addition it allows you to control the cost to each neighbor on an individual by individual basis where the other options all neighbors have the same cost.
DR/BDR Elected No
Hello: 30
Wait: 120
Dead: 120

Loopback – default for loopback

Default setting on OSPF enabled loopback interfaces.
Interface is advertised as a host route (/32).
N/A
N/A

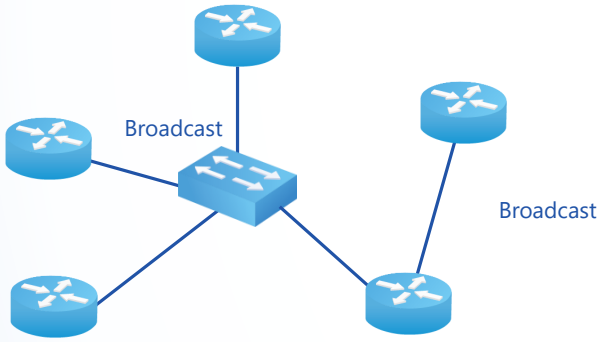
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

OSPF DR/BDR

Optimizes OSPF Adjacency Behavior

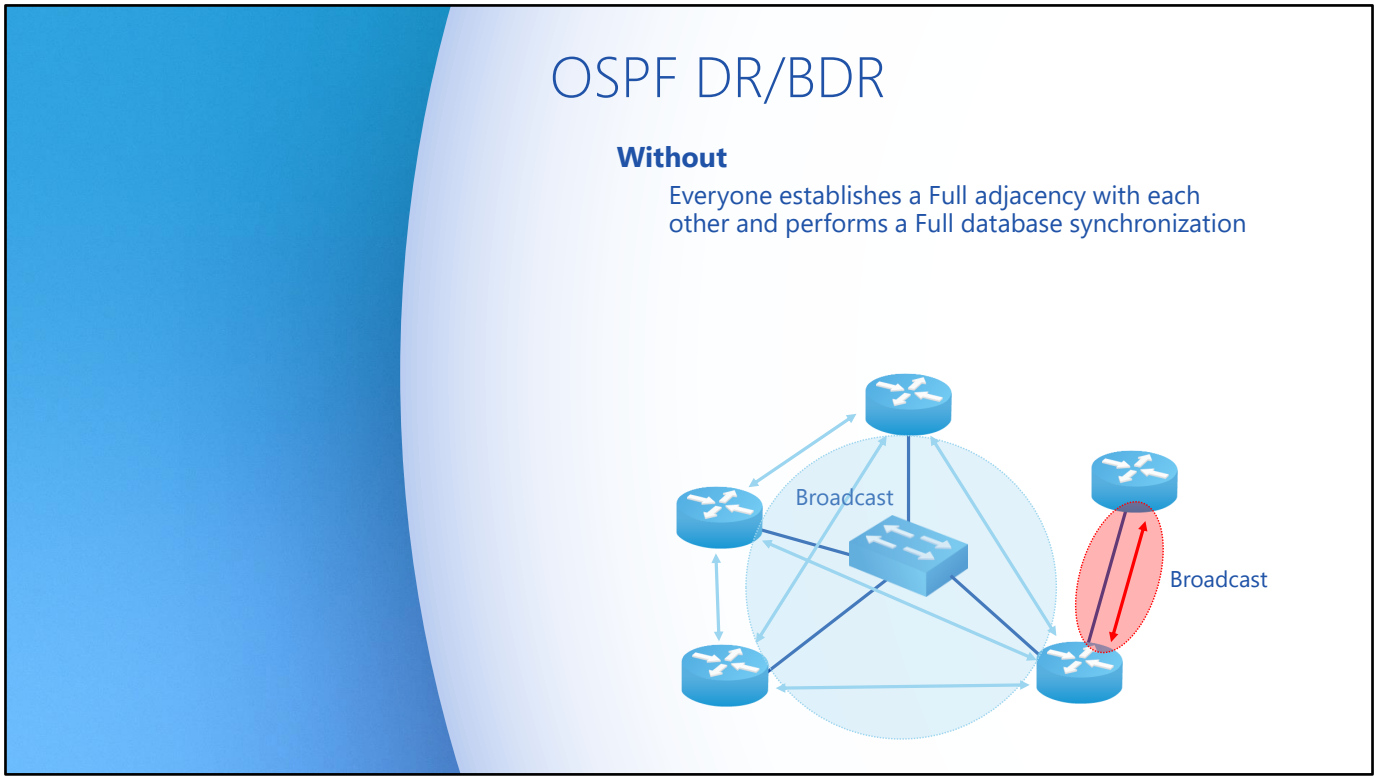
Reduces routing update traffic

Manages link state synchronization



Elected in Broadcast and NonBroadcast Multiaccess network types

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



This is wasteful

Using the number of edges formula, $n(n-1)/2$, where n represents the number of routers, if 5 routers were present on a segment that is, $5(5-1)/2 = 10$, then 10 OSPF adjacencies would exist for that segment. Continuing the logic, adding 1 additional router would makes 15 OSPF adjacencies on a network segment. Having so many adjacencies per segment consumes more bandwidth, more CPU processing, and more memory to maintain each of the neighbor states.

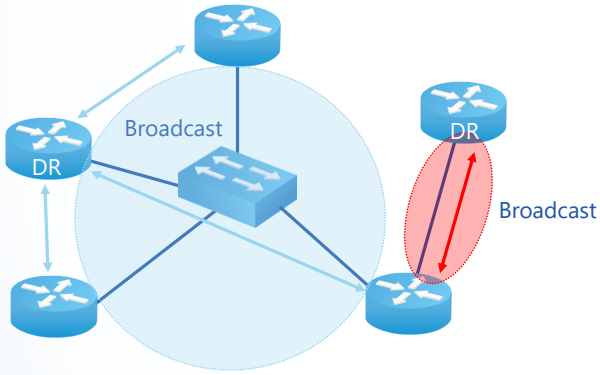
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

OSPF DR/BDR

With

Everyone establishes a Full adjacency with the DR and only Fully synchronize LSDB with the DR using 224.0.0.6.

DR uses 224.0.0.5 to propagate LSAs to routers



Therefore reducing routing update traffic and improving the management of link-state information and synchronization (reducing the possibility of errors and unsynchronized LSDBs).

SPF overcomes this inefficiency by creating a pseudonode (that is, a virtual router) to manage the adjacency state with all the other routers on that broadcast network segment. A router on the broadcast segment, known as the *designated router* (*DR*), assumes the role of the pseudonode. The DR reduces the number of OSPF adjacencies on a multi-access network segment because routers ~~only~~ form a full OSPF adjacencies only~~y~~ with the DR and not each other. The DR is then responsible for flooding the update to all OSPF routers on that segment as updates occur.

The DR notifies all other routers of new LSAs

All routers will have full adjacency with DR & BDR (all other states are 2-way)

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Non-DR’s only exchange LSDB with DR & BDR

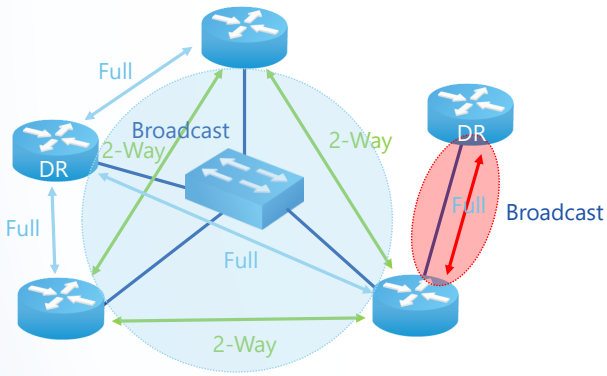
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

OSPF DR/BDR

With

Everyone establishes a Full adjacency with the DR and only Fully synchronize LSDB with the DR using 224.0.0.6.

DR uses 224.0.0.5 to propagate LSAs to routers



Therefore reducing routing update traffic and improving the management of link-state information and synchronization (reducing the possibility of errors and unsynchronized LSDBs).

The DR notifies all other routers of new LSAs

All routers will have full adjacency with DR & BDR (all other states are 2-way)

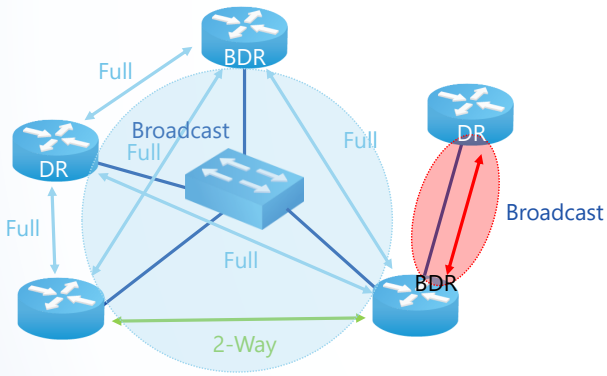
Non-DR's only exchange LSDB with DR & BDR

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

OSPF DR/BDR

BDR

Will also fully synchronize with every other router so that if the DR fails the BDR can immediately take over.



Therefore reducing routing update traffic and improving the management of link-state information and synchronization (reducing the possibility of errors and unsynchronized LSDBs).

The DR notifies all other routers of new LSAs

All routers will have full adjacency with DR & BDR (all other states are 2-way)

Non-DR's only exchange LSDB with DR & BDR

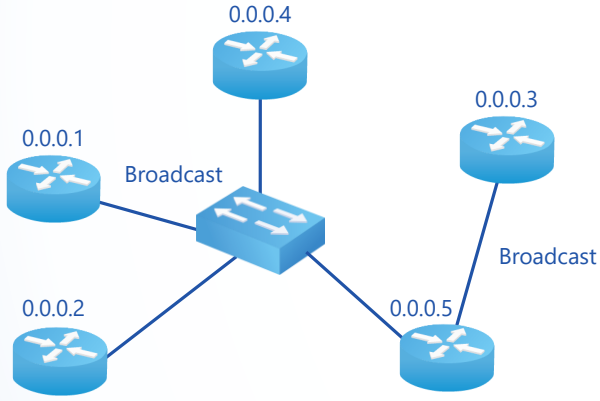
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

OSPF DR/BDR

A **Designated Router** (DR) is elected in Multi-access Networks

Highest Priority (Default Priority = 1)

if tied Highest Router ID



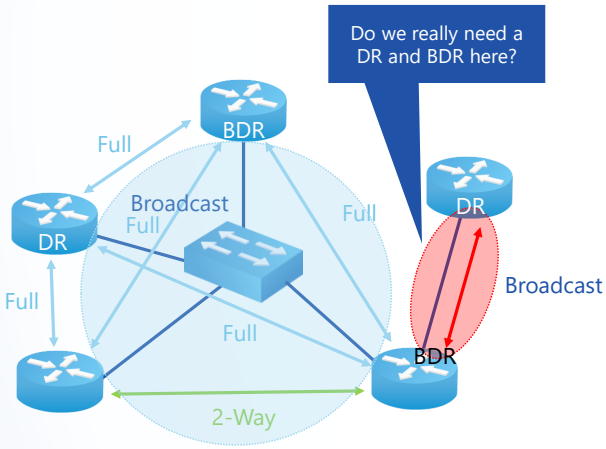
This is only true for 40 seconds which equals the wait timer on an interface.

Other than that…whoever is the DR stays the DR until the interface fails/neighborship is broken and then some other device becomes the DR.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

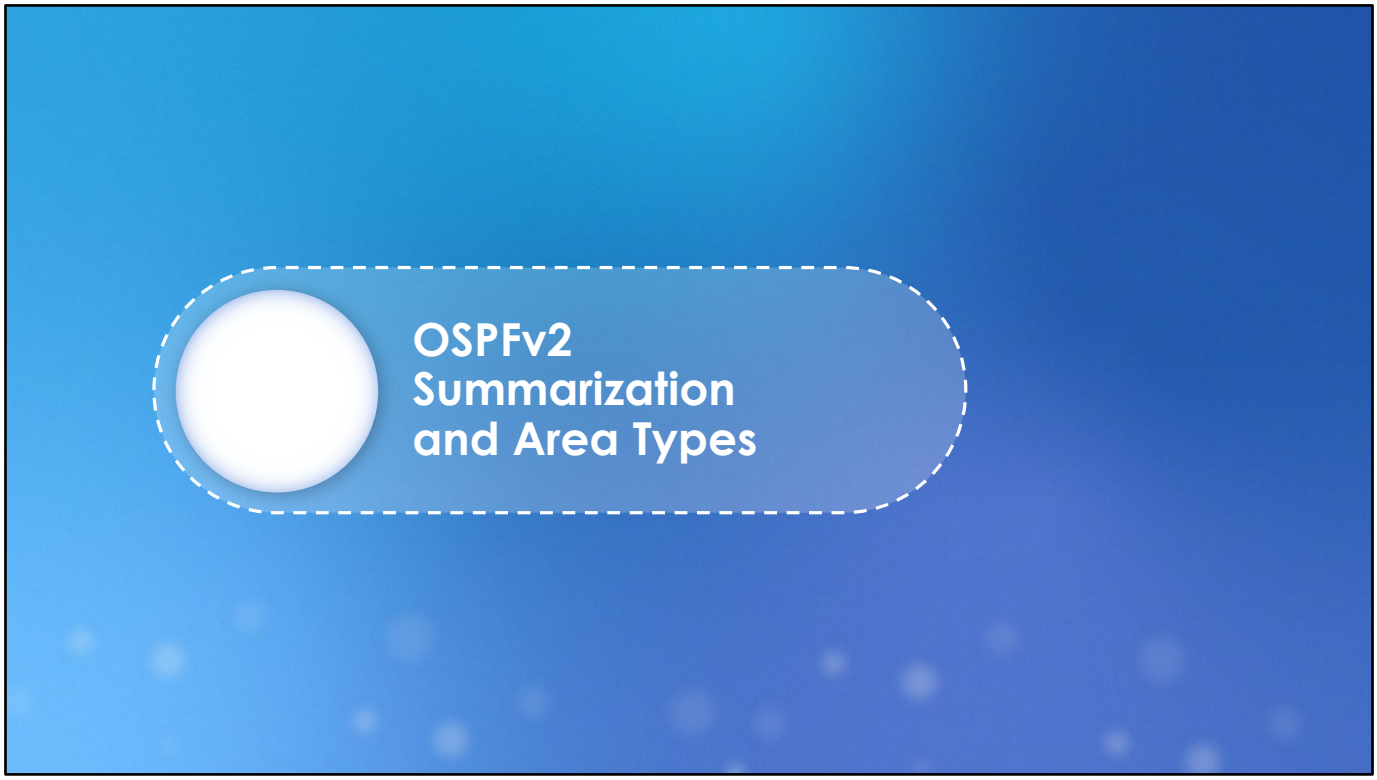
OSPF DR/BDR

A **Designated Router** (DR) is elected in Multi-access Networks



NO… it makes no difference. Change the type to point to point on each interface. Ip ospf network point-to-point

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Title slide

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



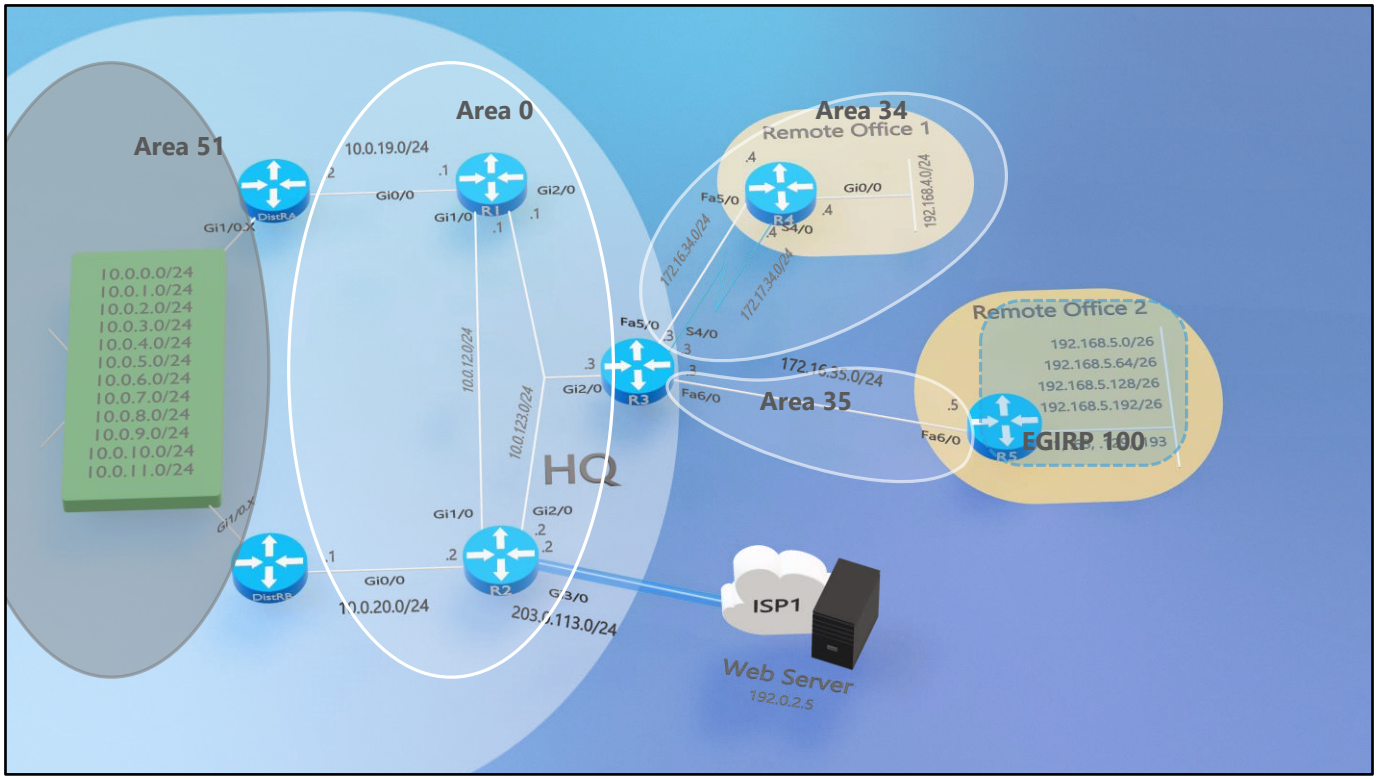
Demo: Route types

O – OSPF destination in the same area

OI – OSPF destination in a different area

OE1/2 – Destination outside OSPF domain

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Demo: Route types

O – OSPF destination in the same area

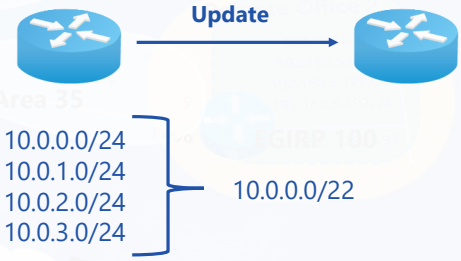
OI – OSPF destination in a different area

OE1/2 – Destination outside OSPF domain

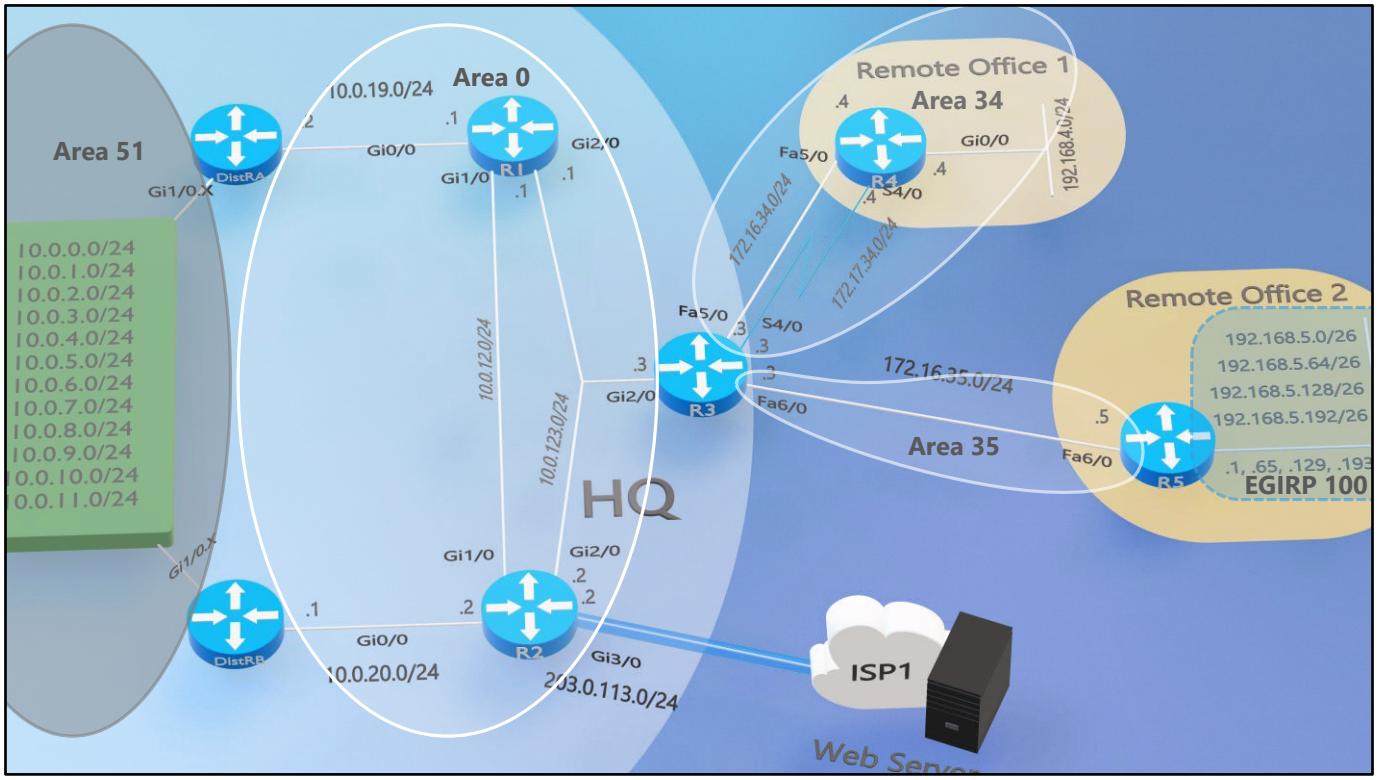
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

OSPF Summarization

- Summarization can only be configured on ABR's and ASBRs!
  - Type 3 and Type 5 LSAs
- Summarizing helps localize topology changes
- Summarizing reduces the amount of LSAs to reduce CPU cycles
- Summarization assists with smaller routing tables
  - *OSPF doesn't support auto summarization



©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Demo: Summarization

How do we figure out the summary address… binary…
10.0.0.0 = 10.0.00000000.0
10.0.11.0 = 10.0.00001011.0
Where do the common bits end?
That is the new mask.
Append it to the first address.

Type 3 summary:
Demo DISTRA summarizing 10s into Area 0
Demo DISTRB summarizing 10s into Area 0
mention how you could use this for path manipulation…. If DISTRA is summary and DISTRB is not then based on the longest match rule traffic would go through DISTRB all the time unless it fails. So you could use the for primary/backup scenarios.

Demo how you can't summarize if you don't have the type 1 LSAs that go along with the summary. So try to summarize 10s on R3 going into Area 34 and 35.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Type 5 summary:
Demo R5 summary
How do we figure out the summary address… binary…
192.168.5.00000000
192.168.5.11000000
Where do the common bits end?
That is the new mask.
Append it to the first address.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Special OSPF Area Types

Stub Area

```
Suppress type 5
```

Totally Stubby Area

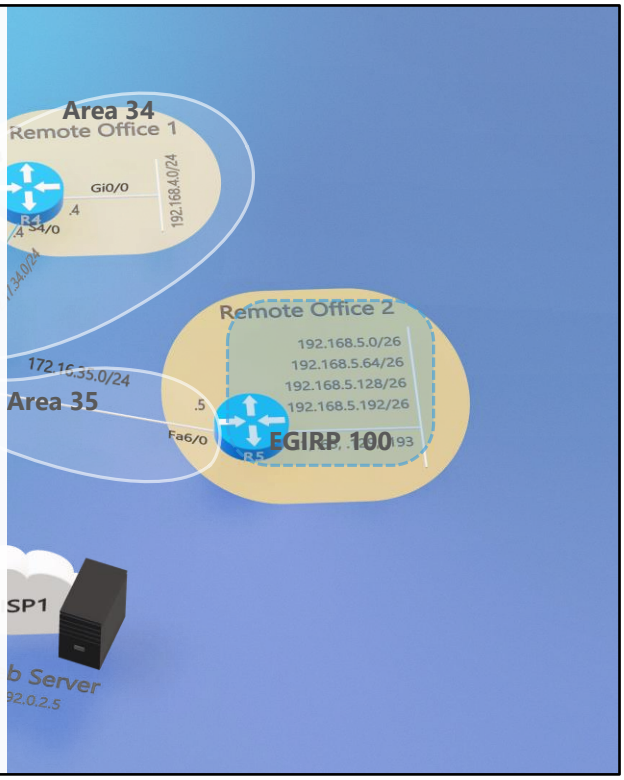
```
Suppress type 5 and 3
```

Not so Stubby Area

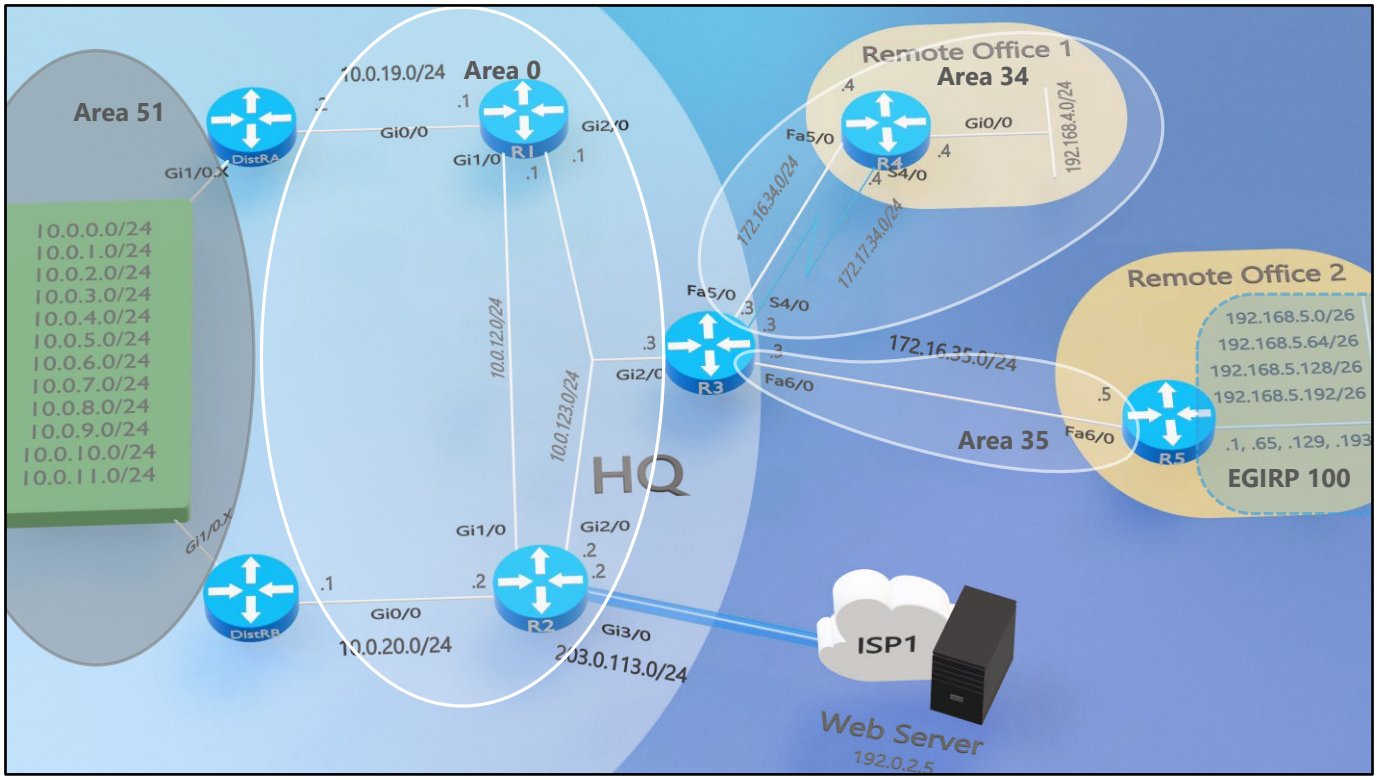
```
Suppress type 5
```

Totally Not so Stubby Area

```
Suppress type 5 and 3
```



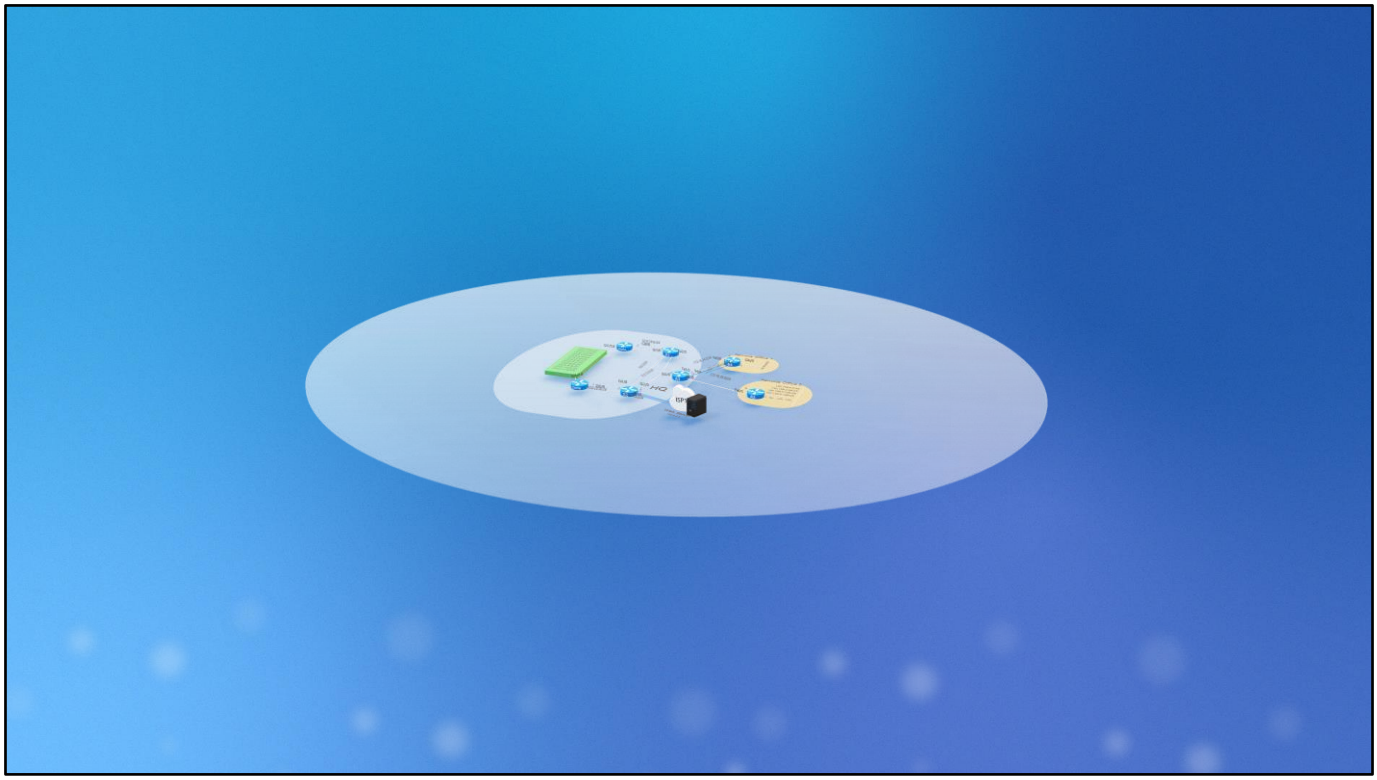
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Demo: Stub, Totally Stubby, NSSA, Totally NSSA

area x stub (suppress type 5 inject type 3 default route)
area x stub no-summary (suppress type 345 and inject type 3 default route)
area x nssa (suppress type 5 and manually inject type 7 default route)
area x nssa no-summary (suppress type 345 and inject type 3 default route)

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

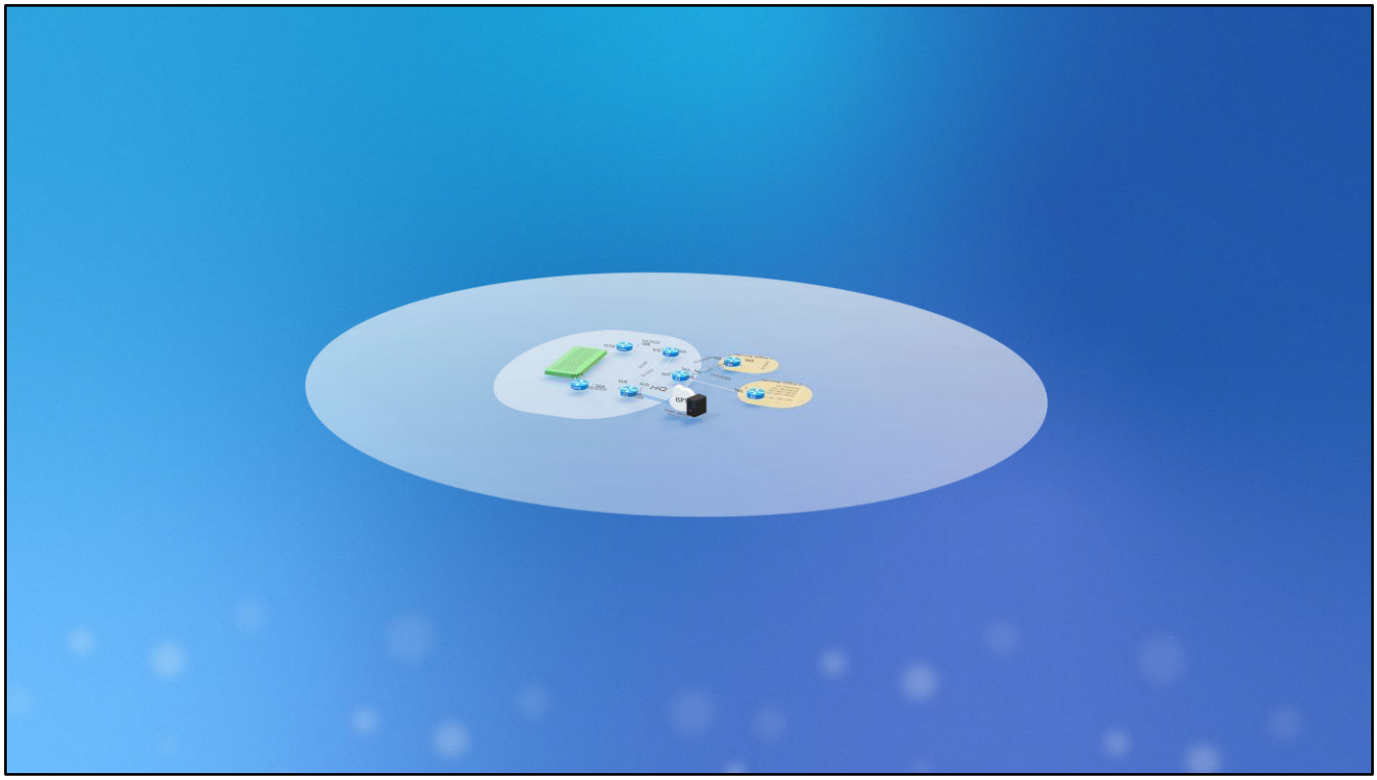


©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Title slide

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

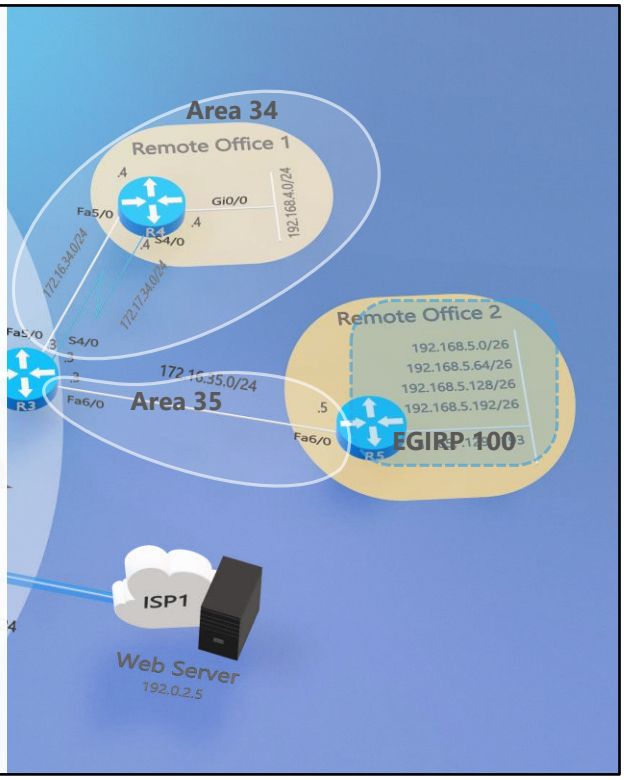


©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

OSPF Filtering

Used to control:

- What can be placed in the routing table
- What will be shared with other routers



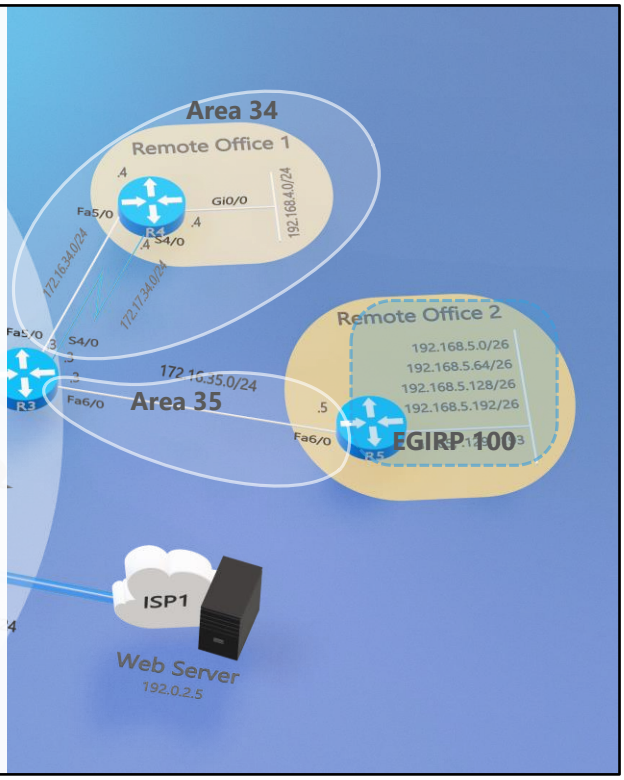
https://blog.ine.com/2009/08/17/ospf-route-filtering-demystified

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

OSPF Filtering

Used to control:

- What can be placed in the routing table
  - Distribute-List



Create a prefix-list or ACL to identify route you want to deny
Create a distribute-list and attach the acl or prefix list to it “in”

Change to R4:

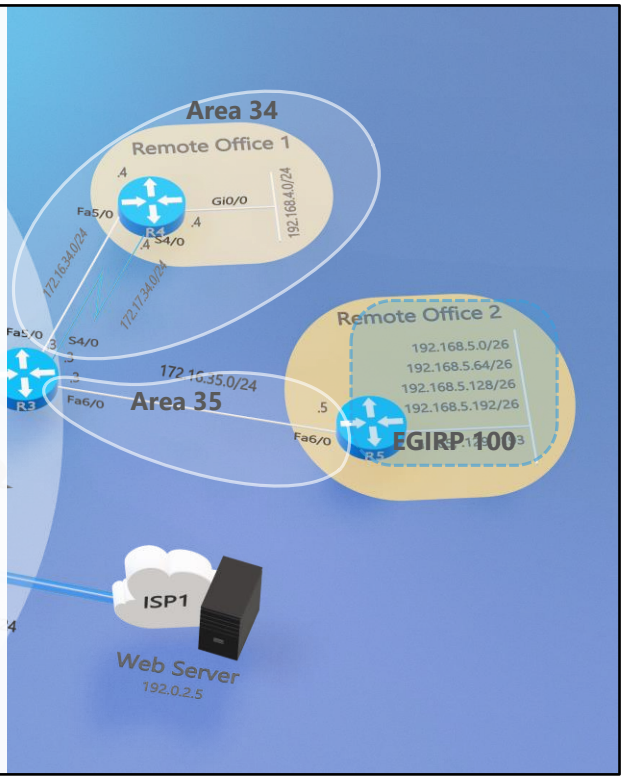
```
R3#configure terminal
Enter configuration commands, one per line.  End with
CNTL/Z.
R3(config)#ip prefix-list FILTER deny 10.0.0.0/24
R3(config)#ip prefix-list FILTER permit 0.0.0.0/0 le 32
R3(config)#router ospf 1
R3(config-router)#distribute-list prefix FILTER in
R3(config-router)#end
R3#
```

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

OSPF Filtering

Used to control:

- What will be shared with other routers
  - Type 3
  - Type 5

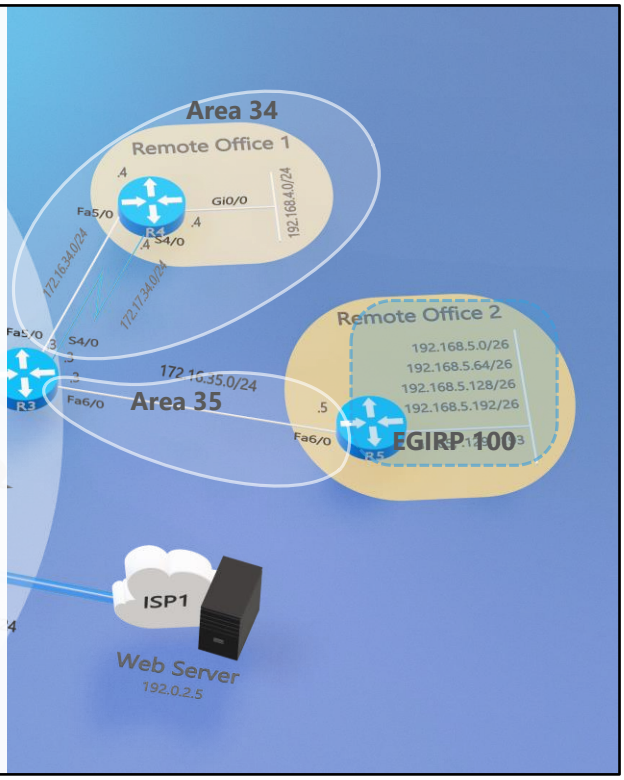


©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

OSPF Filtering

Used to control:

- What will be shared with other routers
  - Type 3 – filter list or area range
  - Type 5



this command applies after all summarization has been done and filters the routing information from being used for type-3 LSA generation. It applies to all three type of prefixes: intra-area routes, inter-area routes, and summaries generated. It filters when building and sending the type 3 into the area.

OPTION 1:

```
R3#configure terminal
Enter configuration commands, one per line.  End with
CNTL/Z.
R3(config)#ip prefix-list FILTER deny 10.0.0.0/24
R3(config)#ip prefix-list FILTER permit 0.0.0.0/0 le 32
R3(config)#router ospf 1
R3(config-router)#area 34 filter-list prefix FILTER ?
  in   Filter networks sent to this area
  out  Filter networks sent from this area

R3(config-router)#area 34 filter-list prefix FILTER in
R3(config-router)#end
R3#
```

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

OPTION 2: area range command

```
R3#configure terminal
Enter configuration commands, one per line.  End with
CNTL/Z.
R3(config)#router ospf 1
R3(config-router)#area 0 range 10.0.0.0 255.255.255.0
not-advertise
R3(config-router)#end
R3#
```

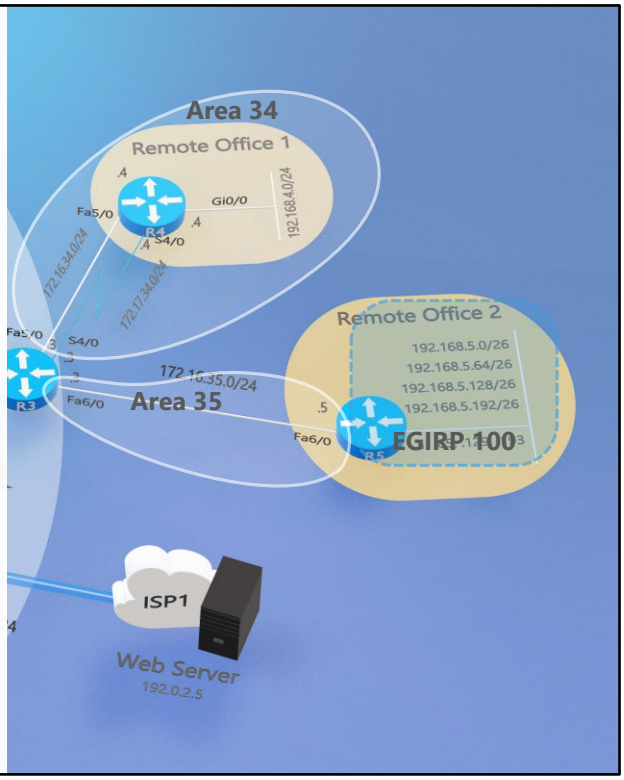
NOTE: if the ABR is connected to multiple areas + 0 then this may not be the best option because it would filter from area 0 into all areas other than 0.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

OSPF Filtering

Used to control:

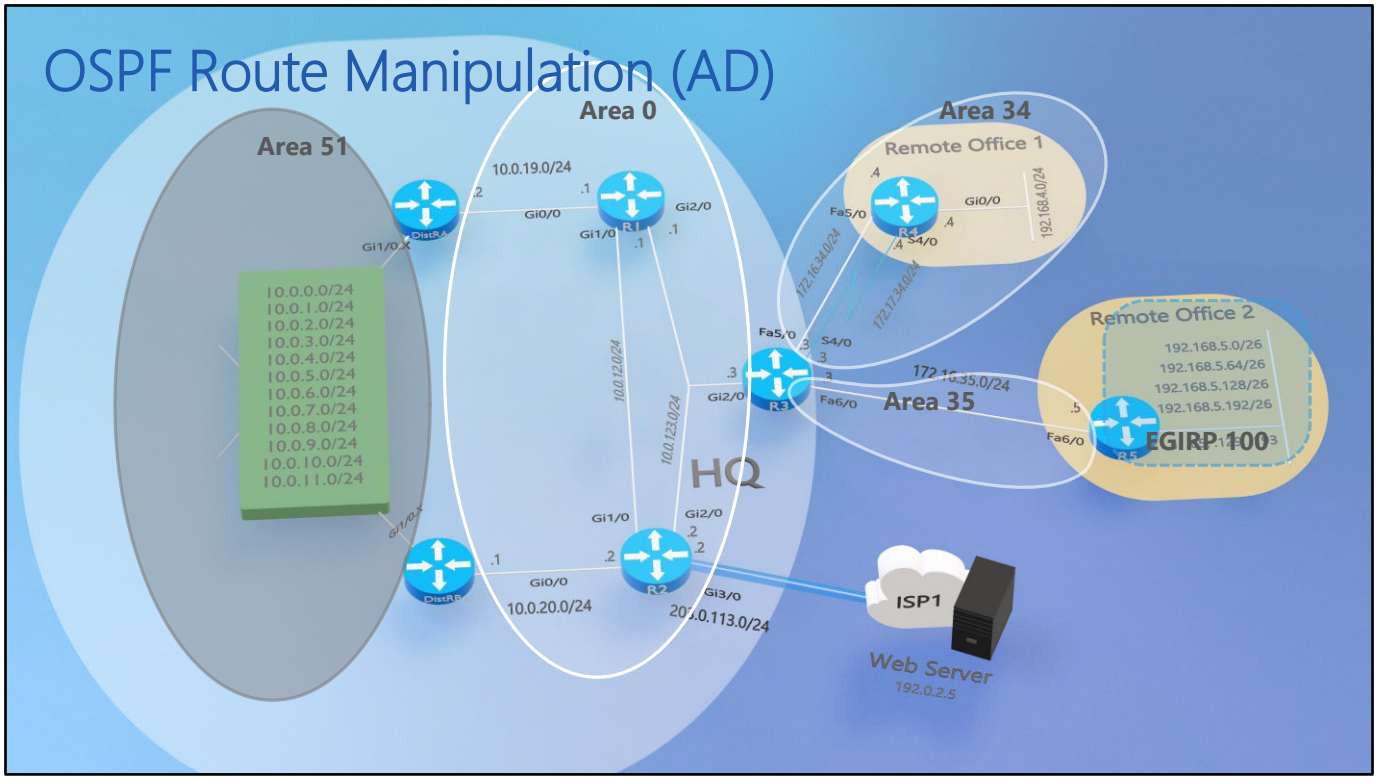
- What will be shared with other routers
  - Type 3
  - Type 5 – summary-address or route-maps during redistribution




```
R2(config-router)#summary-address 192.0.2.0 255.255.255.0
not-advertise
```

Another option is to add the filtering within the redistribute command with a route map

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Demo:

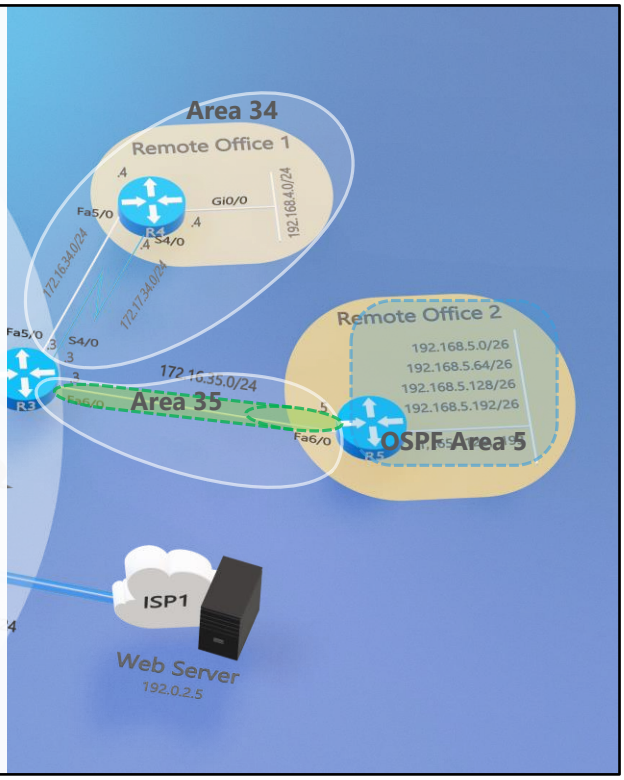
On R1 change the AD of intra / inter / and external 30 / 50 / 70
On R1 change the AD of 10.0.0.0 route learned from DISTRA so that the AD is 25.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Virtual Links

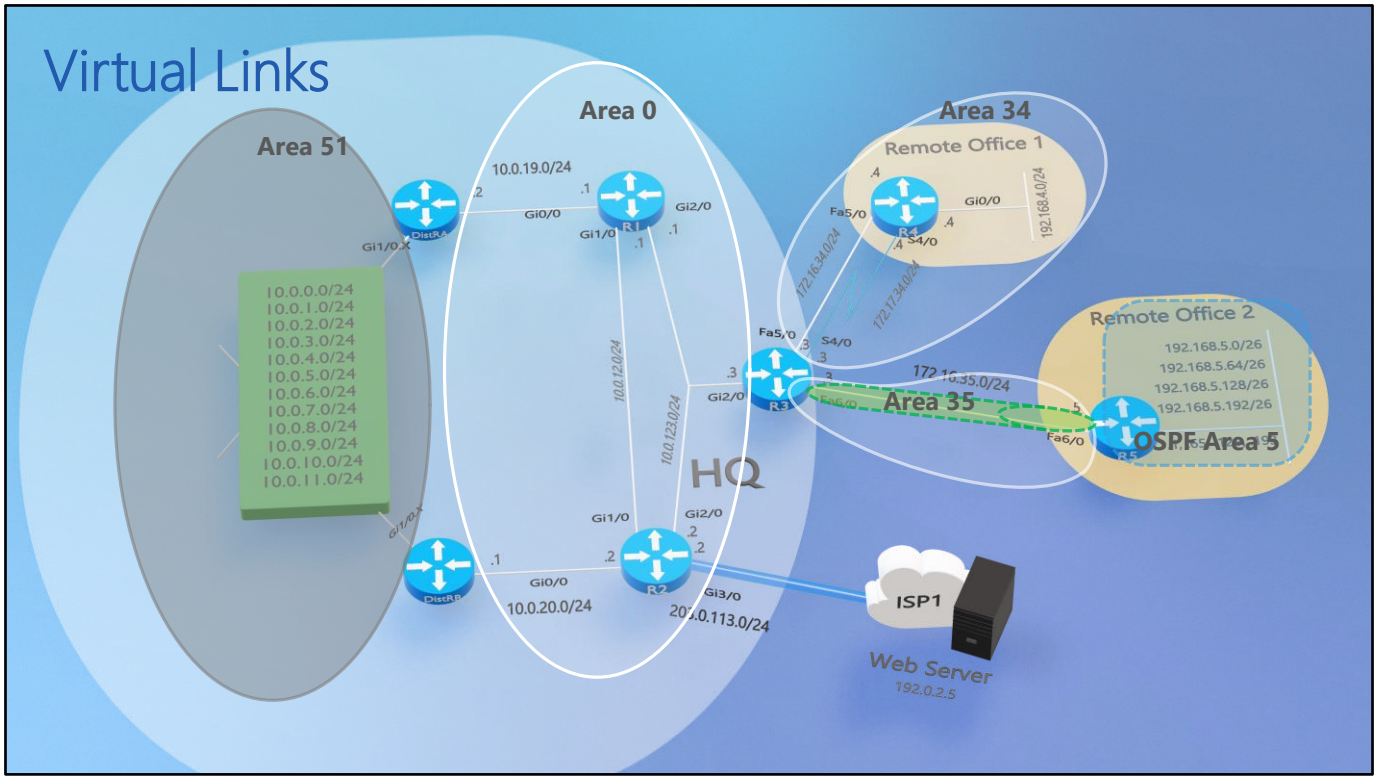
A feature that allows you to virtually directly connect:

- An area to Area 0 when it is not physically connected to it
- A discontiguos Area 0 (One Area 0 to another Area 0 when they are not directly connected)



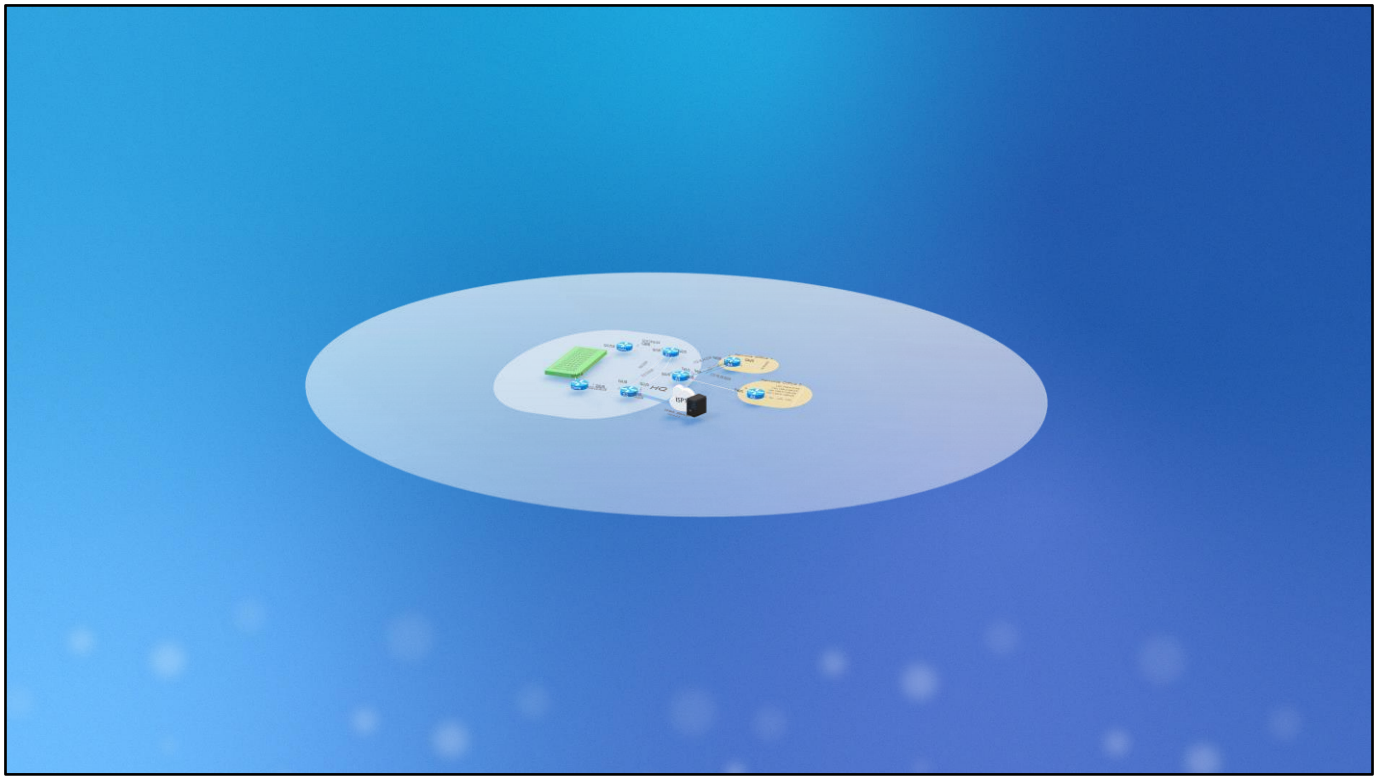
Remove stub config on r3 and r5. put interfaces in area 5. create virtual link.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Remove stub config on r3 and r5. put interfaces in area 0. create virtual link.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

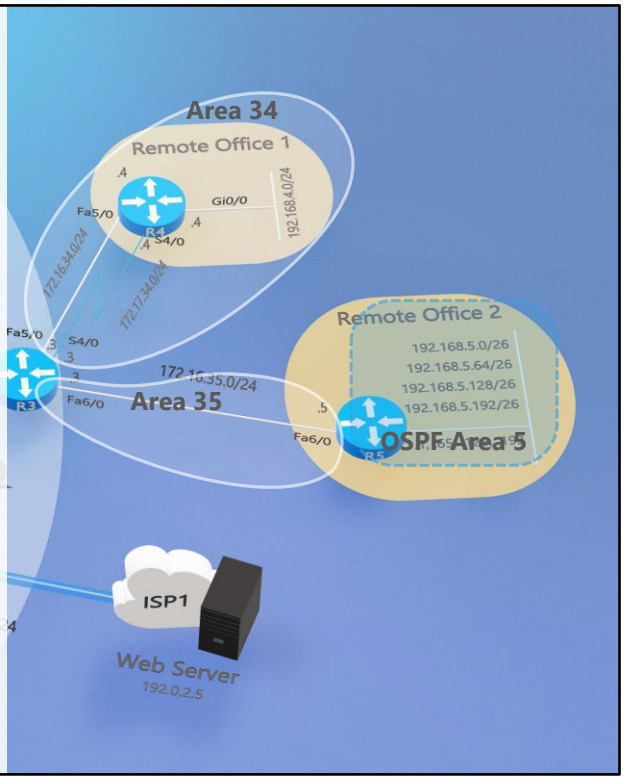
Changing OSPF Timers

Configured on interface with commands:

```
interface gig1/0
  ip ospf hello-interval 1
  ip ospf dead-interval 4
```

Verify OSPF Timers:

```
show ip ospf interface
```



10 and 40 (4 times the hello)

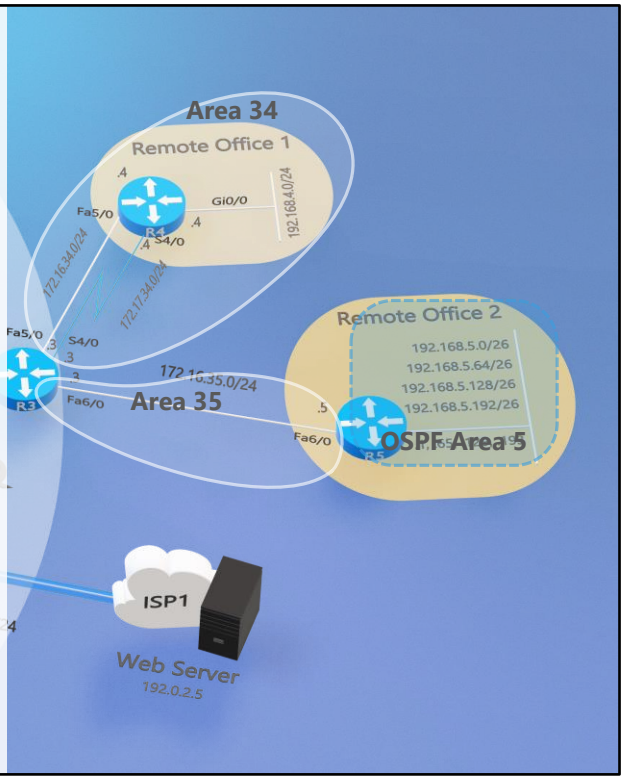
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Bi-directional Forwarding Detection

"Detection" protocol

quickly detect reachability failures between two routers in the same Layer 3 network

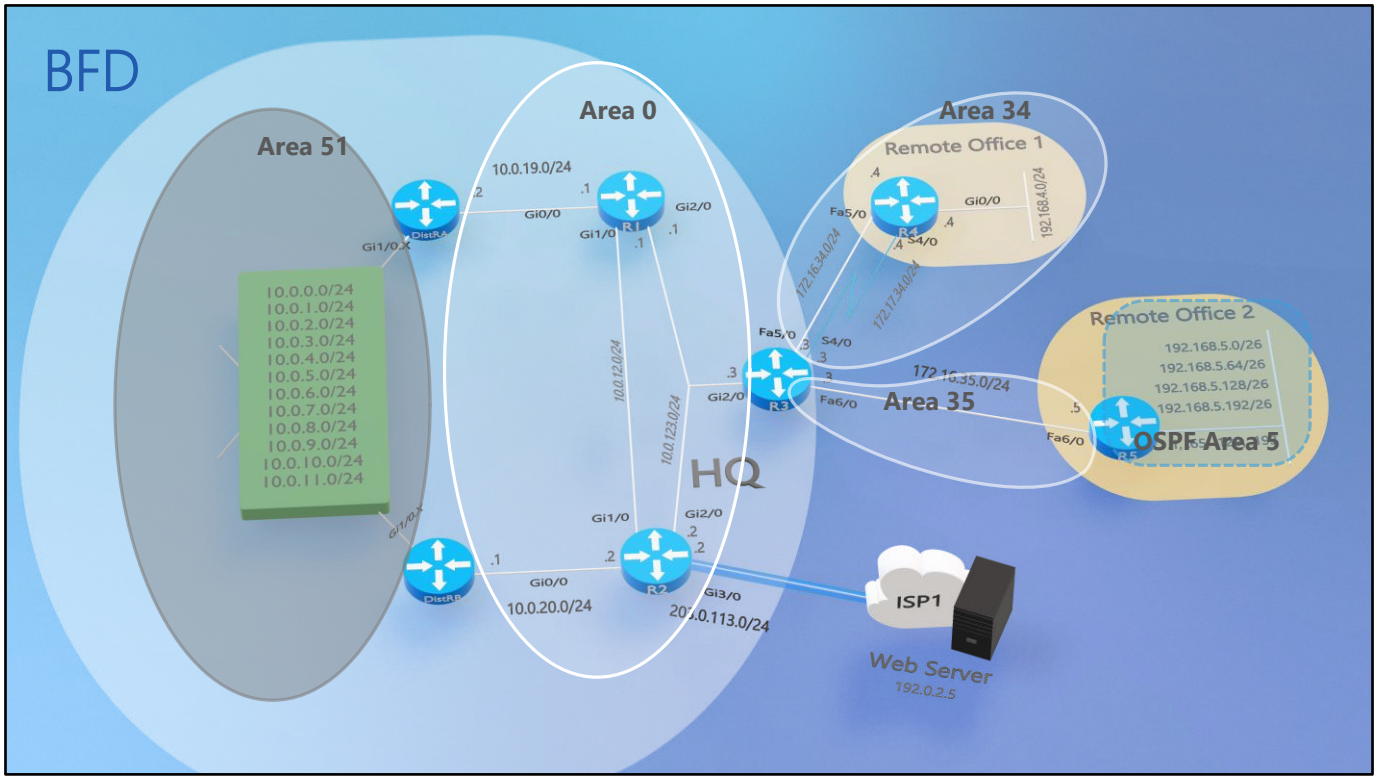




to quickly detect reachability failures between two routers in the same Layer 3 network so that network issues can be identified as soon as possible, and convergence can occur at a far faster rate.

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bfd/configuration/xe-16-5/irb-xe-16-5-book/irb-bi-fwd-det.html#GUID-D0709898-8C5E-4F5E-8BAF-E411E9251D7E

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Configre BFD between R1 and R2

There are two methods for enabling BFD support for OSPF:
You can enable BFD for all of the interfaces for which OSPF is routing by using the **bfd all-interfaces** command in router configuration mode. You can disable BFD support on individual interfaces using the **ip ospf bfd** [**disable**] command in interface configuration mode.
You can enable BFD for a subset of the interfaces for which OSPF is routing by using the **ip ospf bfd** command in interface configuration mode.

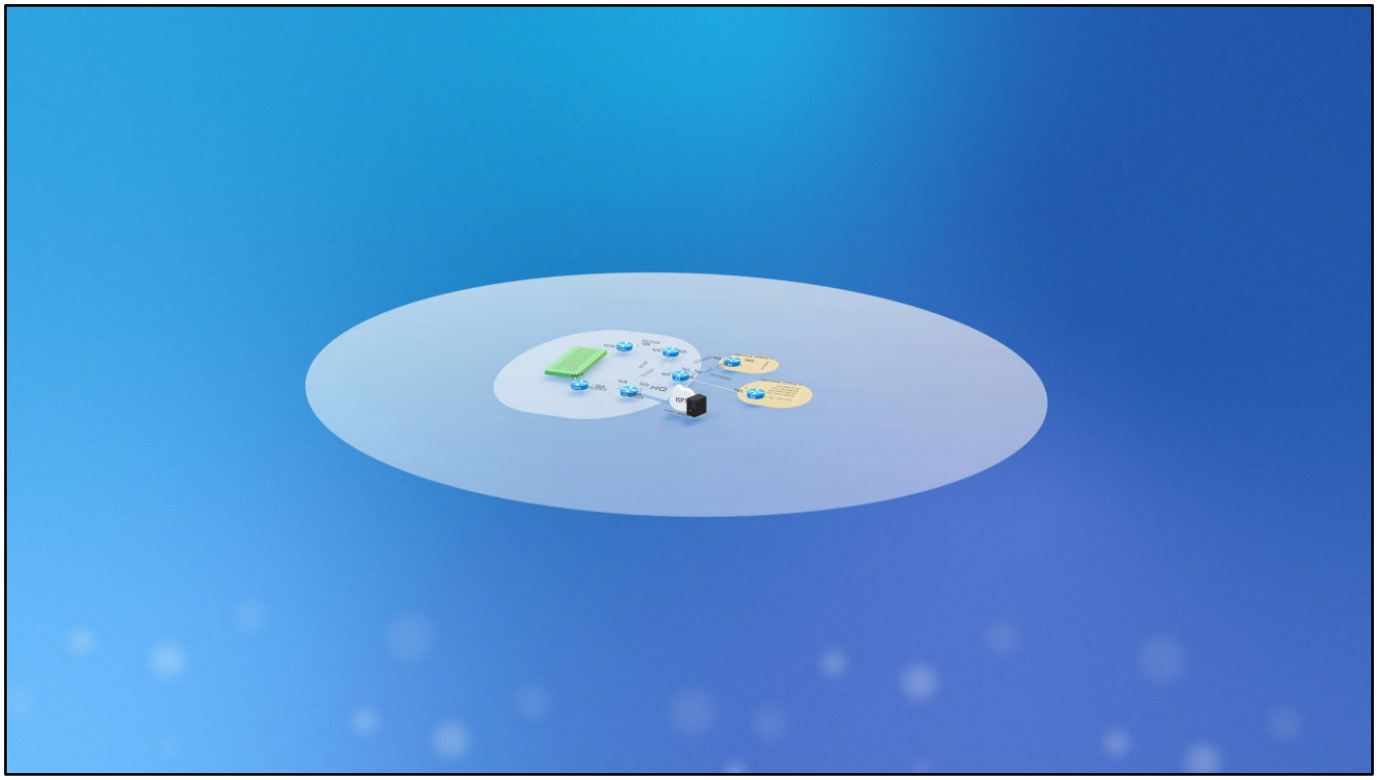
R1#show run int gig 1/0
Building configuration...

Current configuration : 204 bytes
!
interface GigabitEthernet1/0
bfd interval 500 min_rx 500 multiplier 3
ip ospf bfd (disable)

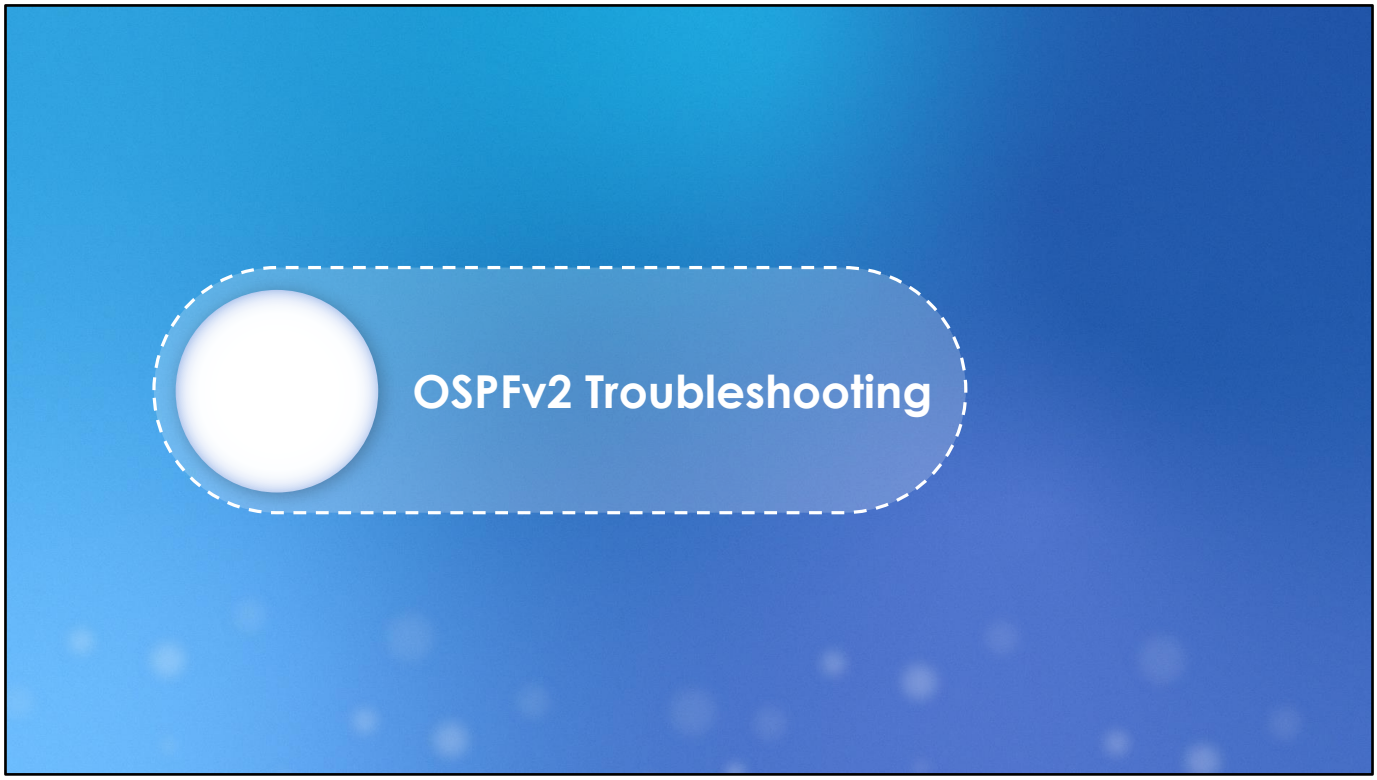
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

```
R1#show run | s eigrp
router ospf 1
 bfd all interfaces
```

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

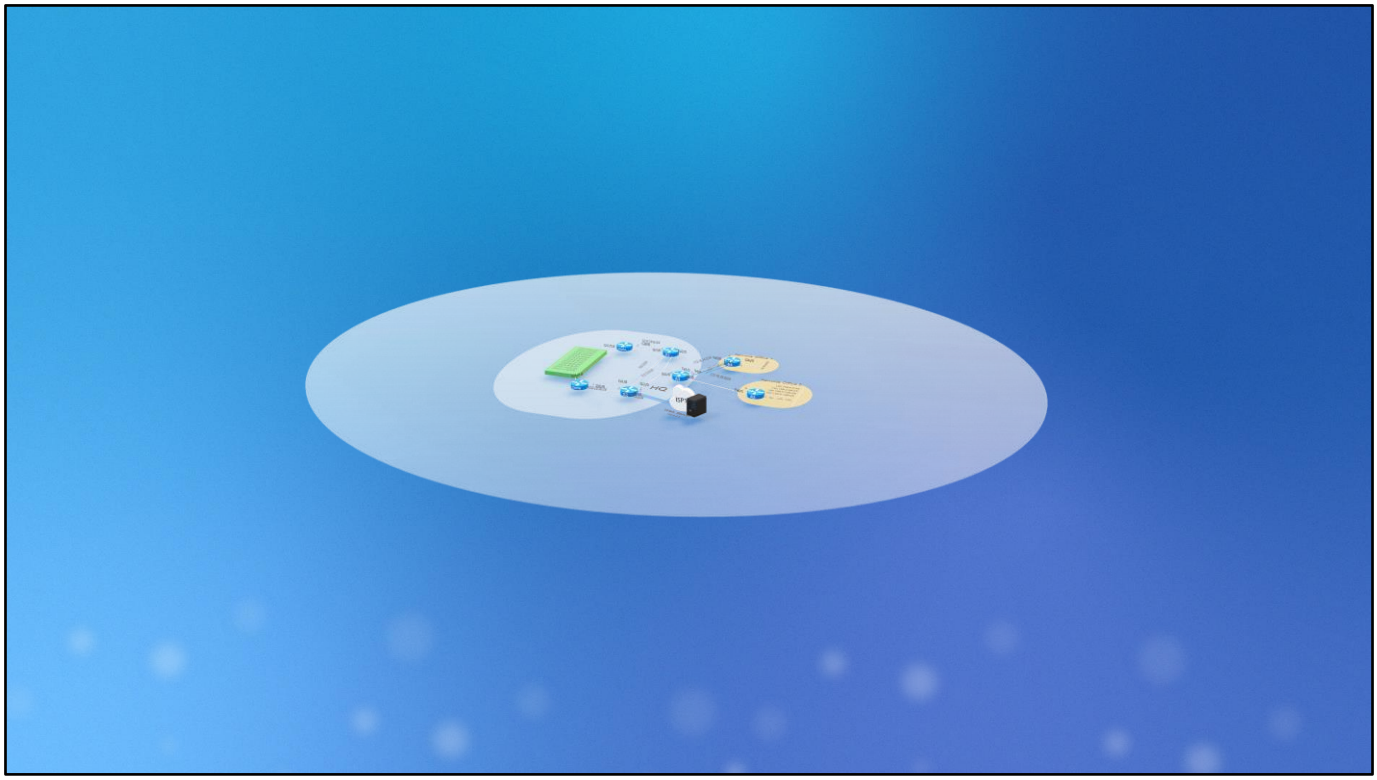


©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

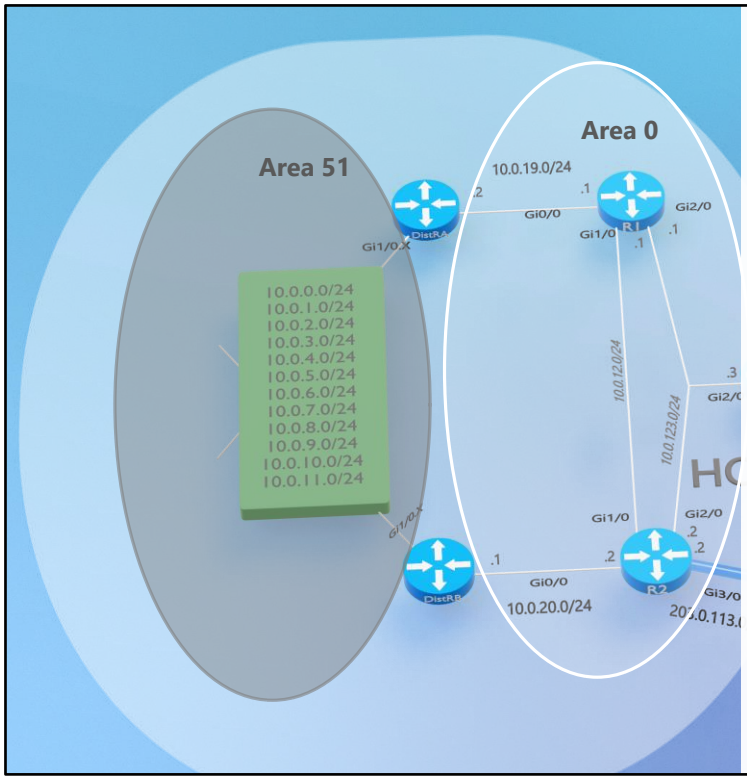


Title slide

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



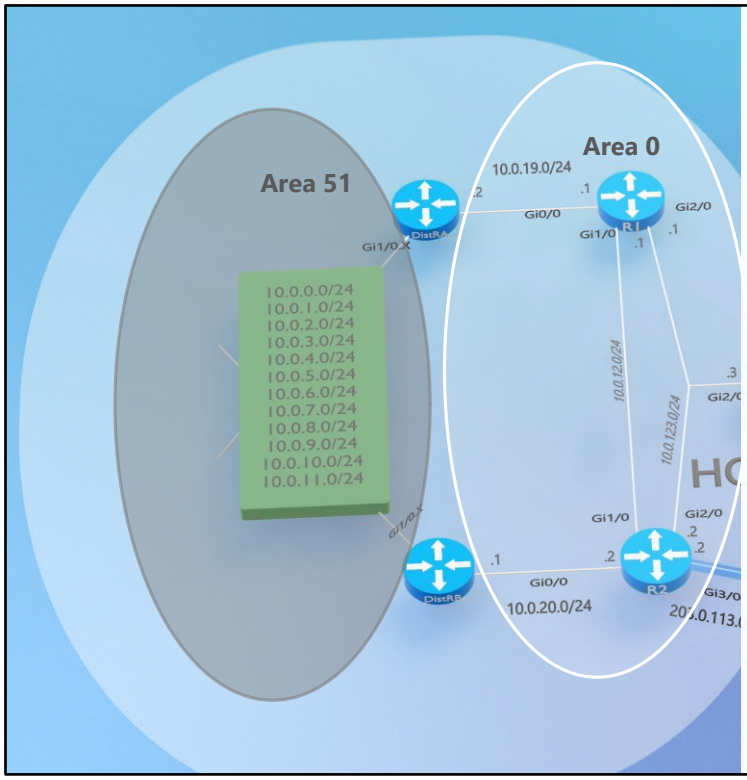
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Troubleshooting OSPF Neighborships

- Interface must be up/up
- Interface needs to be participating in the OSPF process
- Timers needs to match
- Area numbers need to match
- Area types need to match
- Interfaces must be in the same subnet
- Interfaces can't be passive
- Authentication Information must match
- Inbound ACLs must be permitting OSPF
- Interface MTU must match
- Router IDs must be unique
- Network types must be compatible

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Troubleshooting OSPF Neighborships

- Interface not participating in the OSPF process
- Better source of routing information
- Route filters are preventing routes from being shared
- Stub area configuration
- Interface is disabled
- Wrong DR has been elected
- Duplicate RIDs

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Title slide

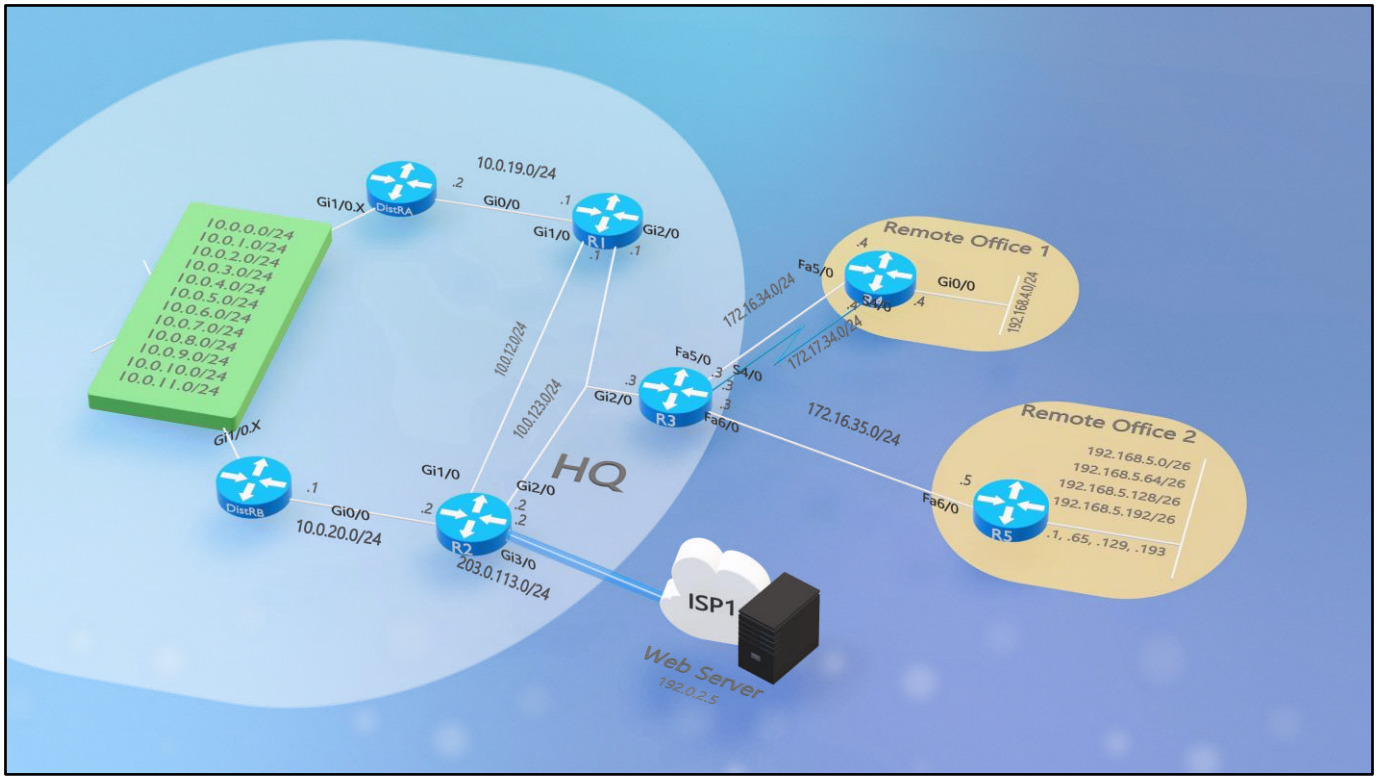
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



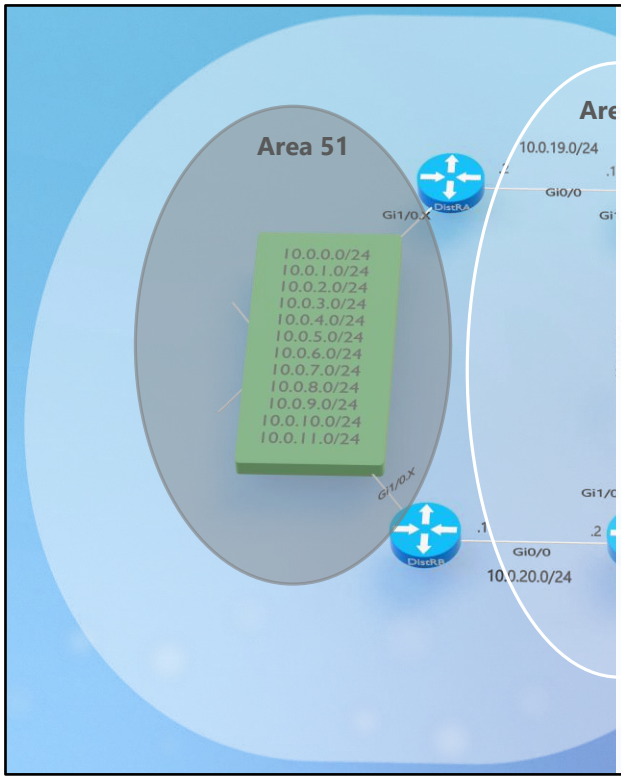
DEMO: Configure all interfaces except ISP interface for EIGRP.

Unicast between r3 and r5 as multicast is disabled on interfaces (ACL).

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



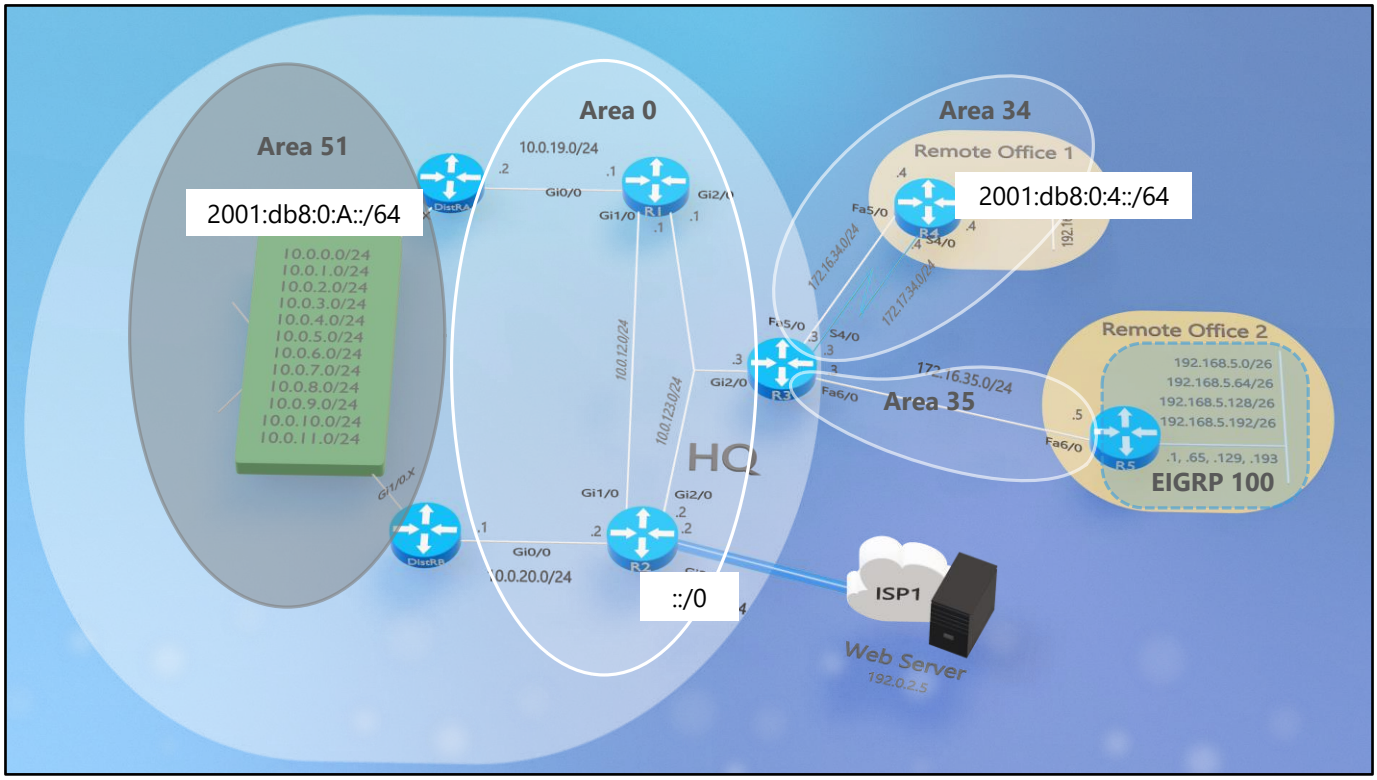
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



OSPFv3 for IPv6 Characteristics

- OSPFv2 (IPv4) and OSPFv3 (IPv6) run independently
- Router ID is a 32-bit number assigned if an IPv4 address is present or use router-id command
- Multicast FF02::5 and FF02::6
- Adjacencies and next-hop attributes use link-local addresses
- OSPFv3 is enabled per interface

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Instructor Notes:
Demo everything

Note – with OSPFv3 you do not have to be in the same subnet… you just have to be able to reach each others link local address. Since link local addresses are not routable this implies that you have to be in the same Layer 2 lan. (so 0 router hops away from each other.)

Configure all interfaces from DistRA to R4 for OSPFv3 but only use the link local addresses on the routers and the global addresses on the ends.
Configure gig 0/0 on R4 as passive
Configure DSW1 int vlan 100 as passive

Show ipv6 protocols
Show ipv6 ospf interfaces
Show ipv6 ospf interfaces detail
Show ipv6 ospf neighbors
Show ipv6 ospf neighbors detail
Show ipv6 ospf topology

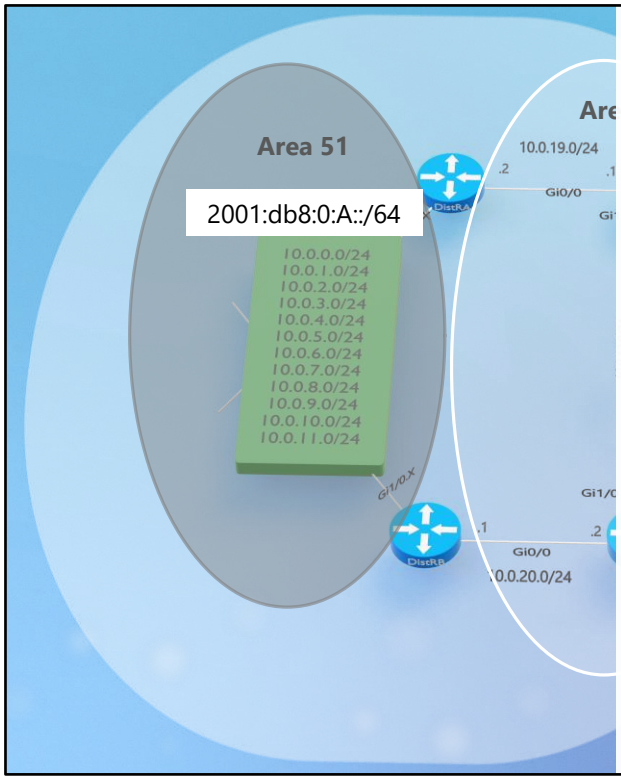
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Show ipv6 ospf route

Configure summary from R3 to R4 on fa and ser interface – 2001:db8:0::/48 or even ::/0

Configure R4 as a stub router

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



IPv6 OSPFv3 Link State Database

LSA's used to create LSDB LSA Types:

Type 1 – Router/Device

Generated by all OSPF routers and floods to all routers in an area. Describes routers.

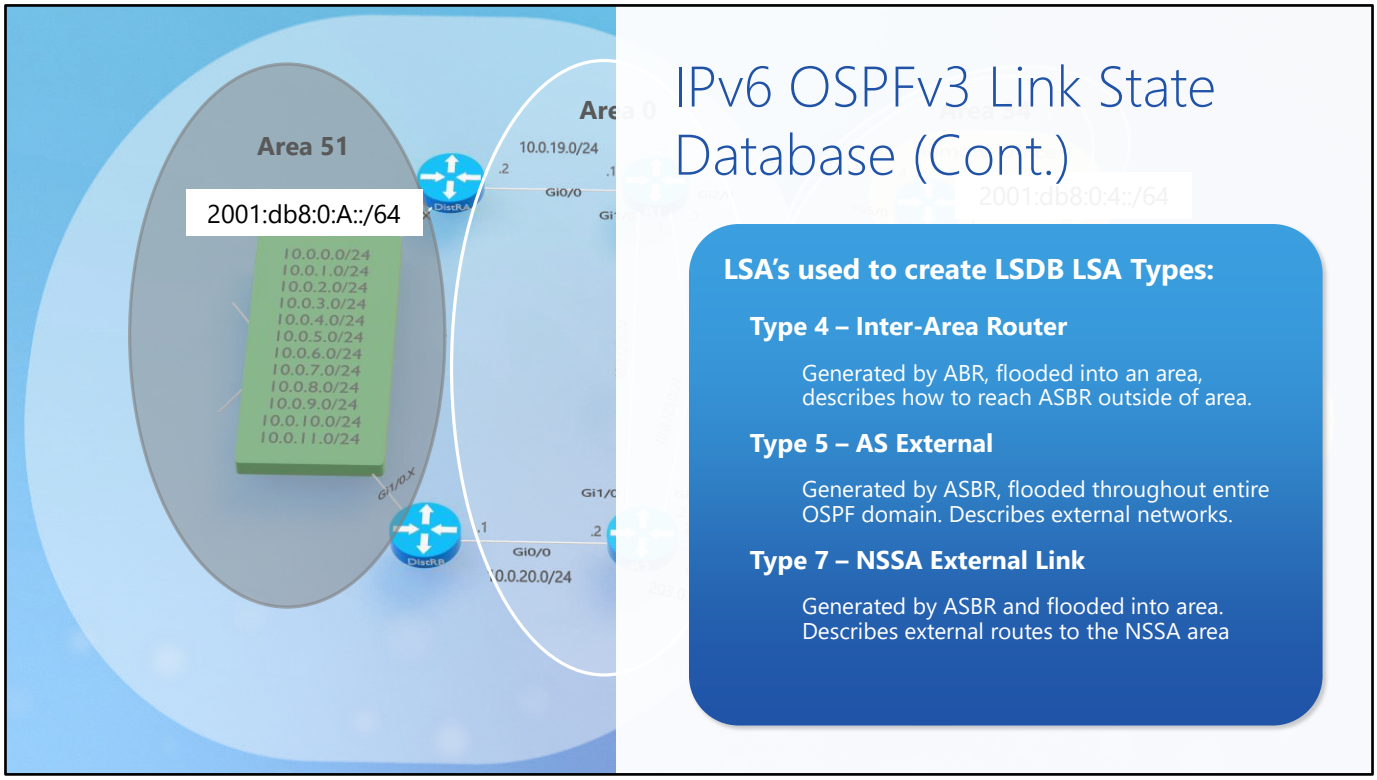
Type 2 – Network

Generated by DR and floods to all routers in an area. Describes multi-access network DR is connected to.

Type 3 – Inter-Area Prefix

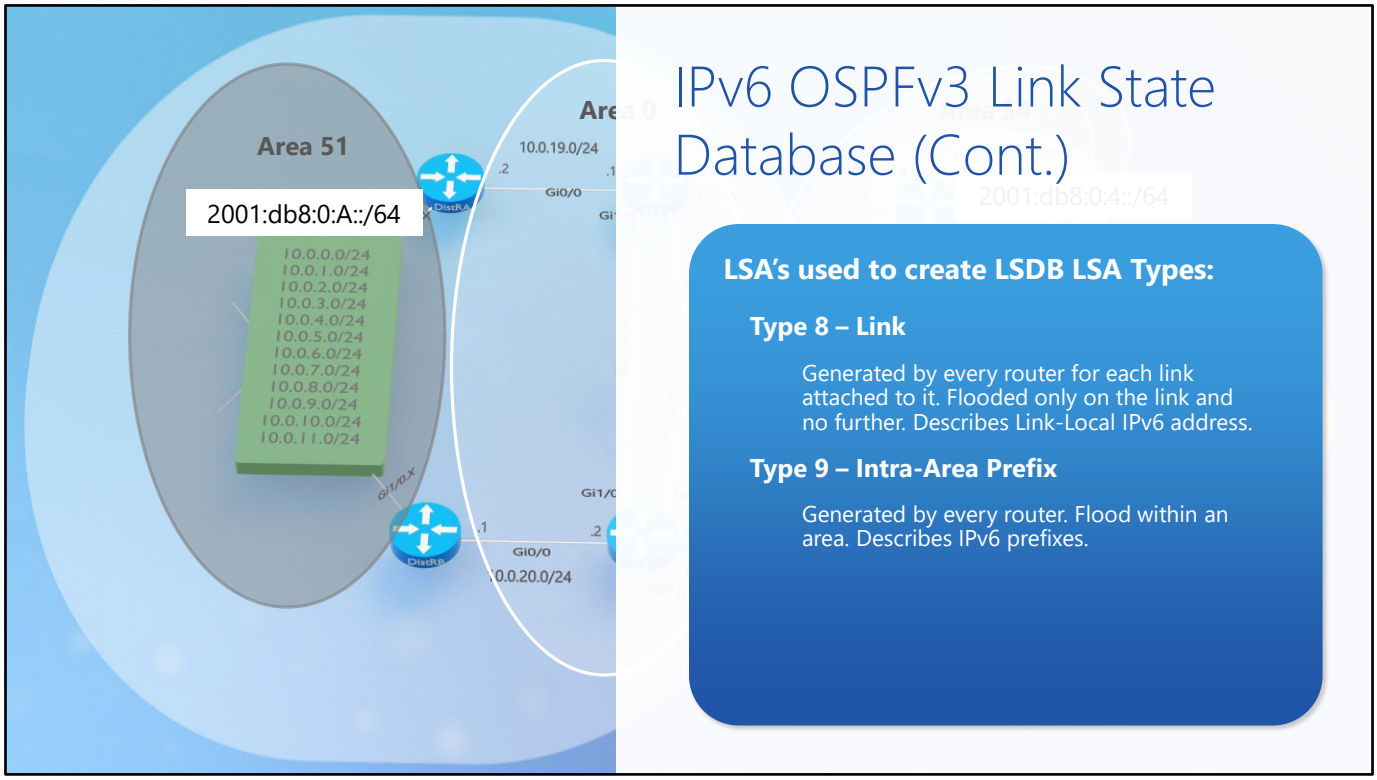
Generated by ABR and flooded into a different area. Describes networks outside of area but still within OSPF domain.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Type 4 – ASBR summary
Type 5 – External Link
Type 7 – NSSA External Link

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

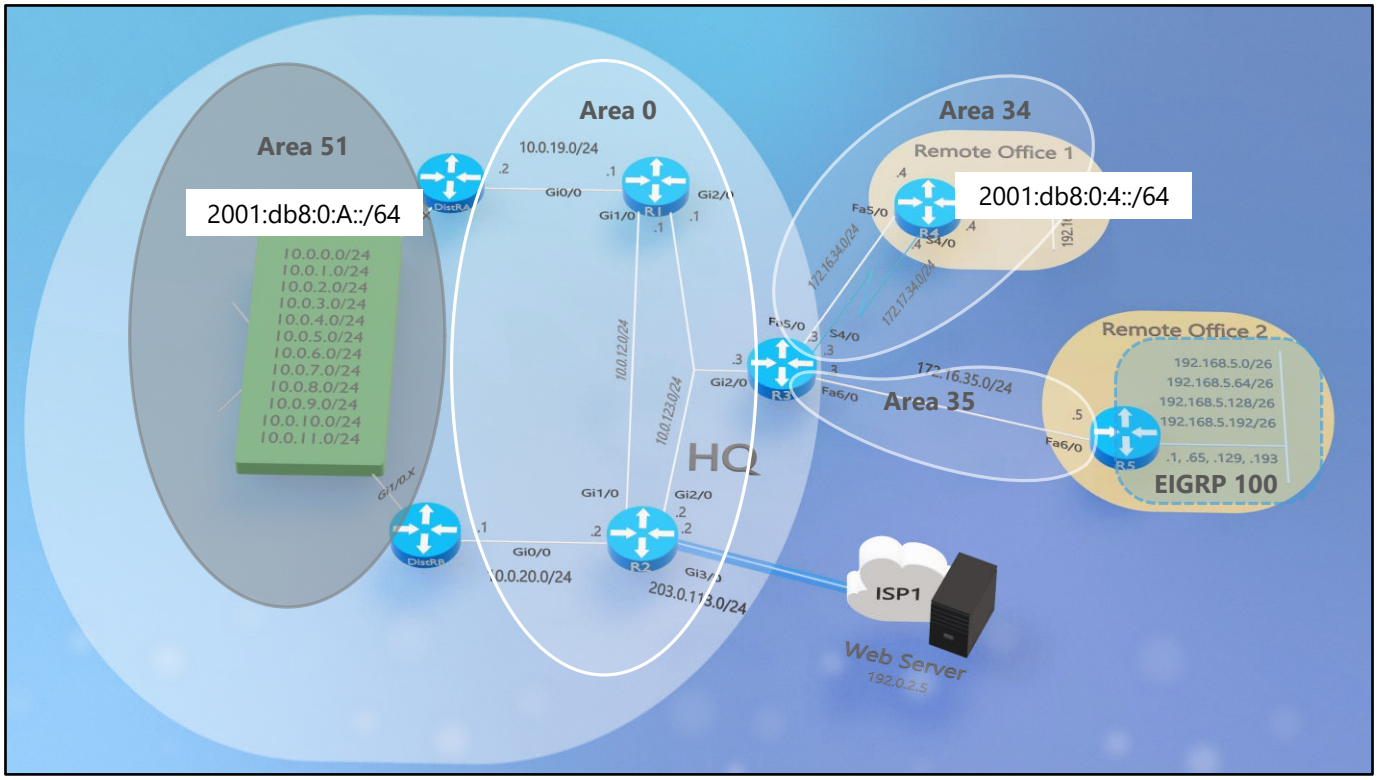


https://sites.google.com/site/amitsciscozone/home/important-tips/ipv6/ospf

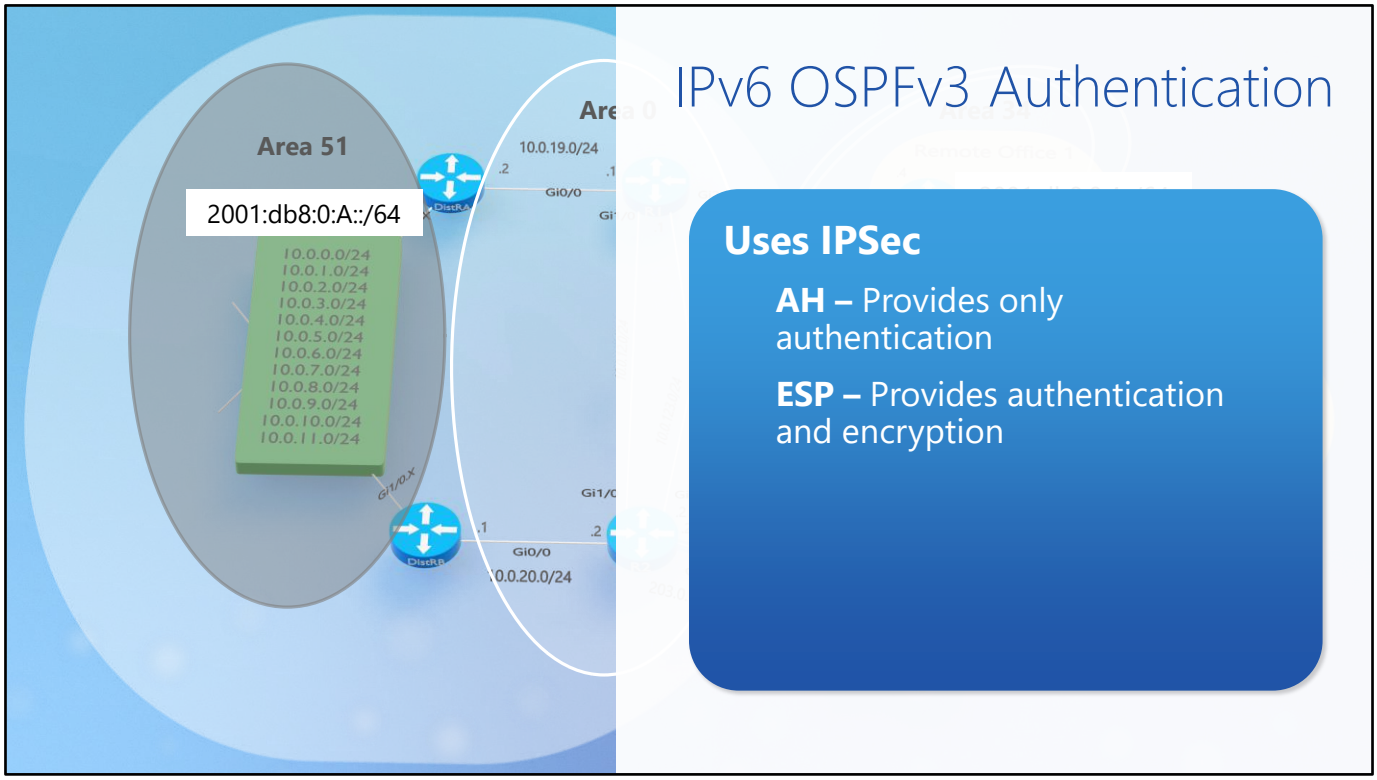
The link LSA maps all the global unicast address prefixes associated with an interface to the link-local interface IP address of the router. The link LSA is shared only between neighbors on the same link.

The intra-area-prefix LSA is used to advertise one or more IPv6 prefixes that are associated with a router, stub, or transit network segment.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



OSPFv3 Authentication

***INSERT KEY TOPIC

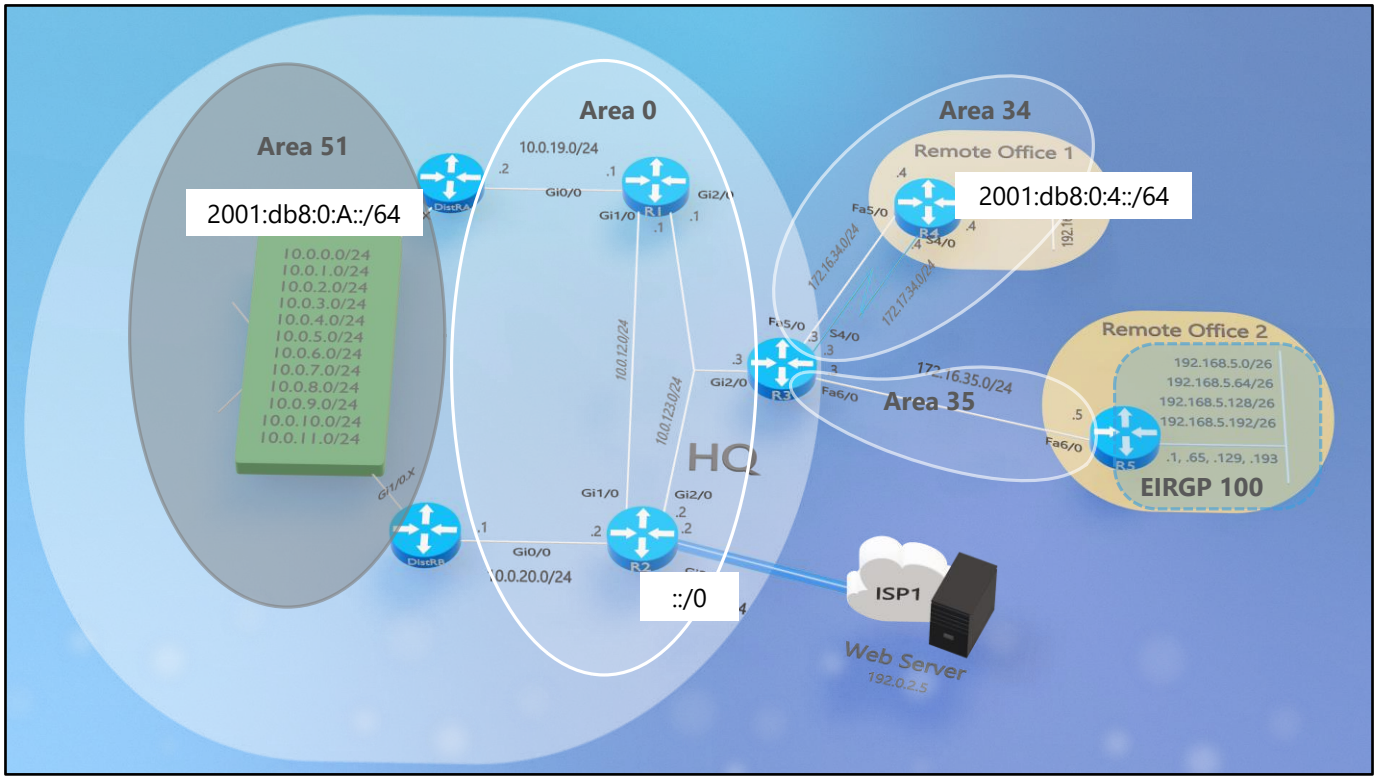
OSPFv3 does not support neighbor authentication within the protocol itself. Instead, the routing protocol utilizes IP Security (IPsec) to provide authentication. IPv6 Authentication Header (AH) or Encapsulating Security Payload (ESP) extension headers may be added to the OSPF packets to provide authentication, integrity, and confidentiality:

[lb] **Authentication Header (AH):** Provides authentication

[lb] **Encapsulating Security Payload (ESP):** Provides authentication and encryption

Ipv6 ospf authentication ipsec spi 500 md5 12345678901234567890123456789012

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

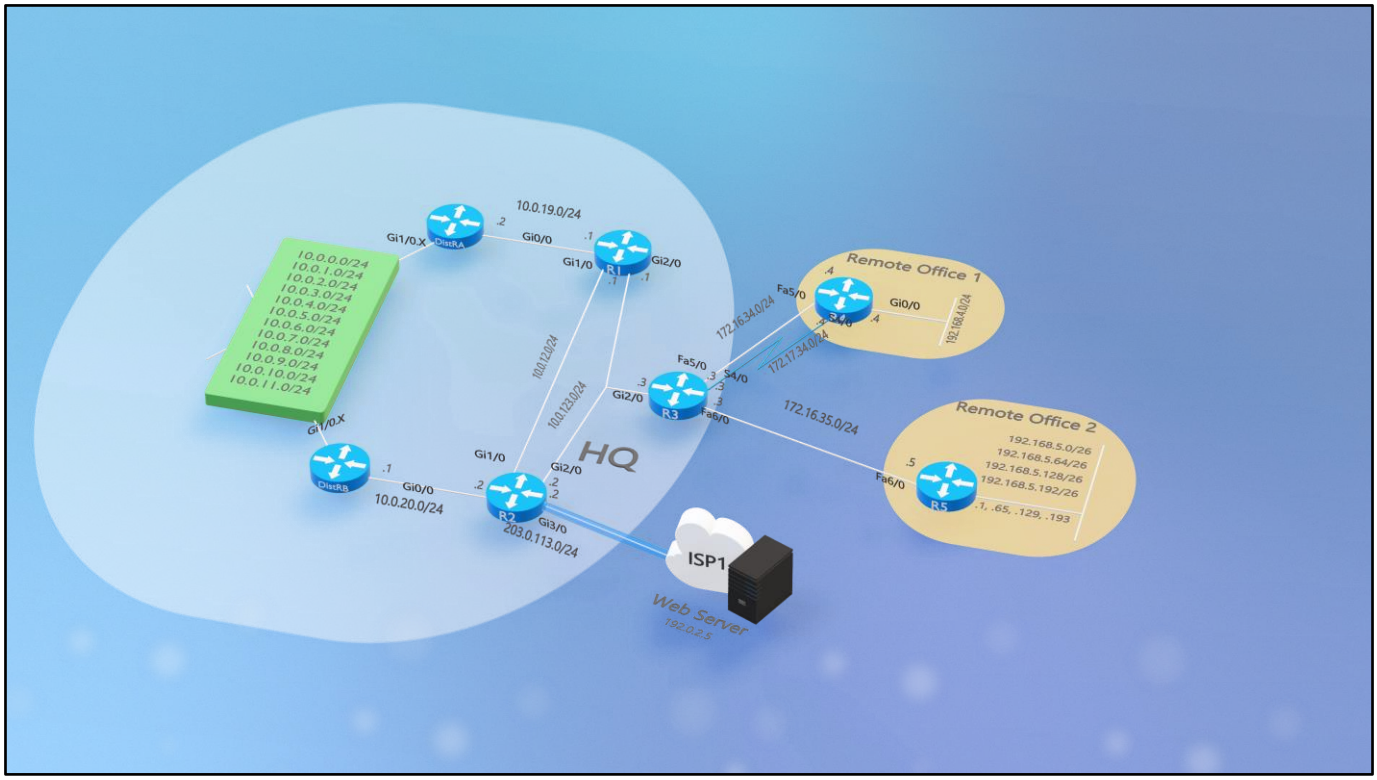


Title slide

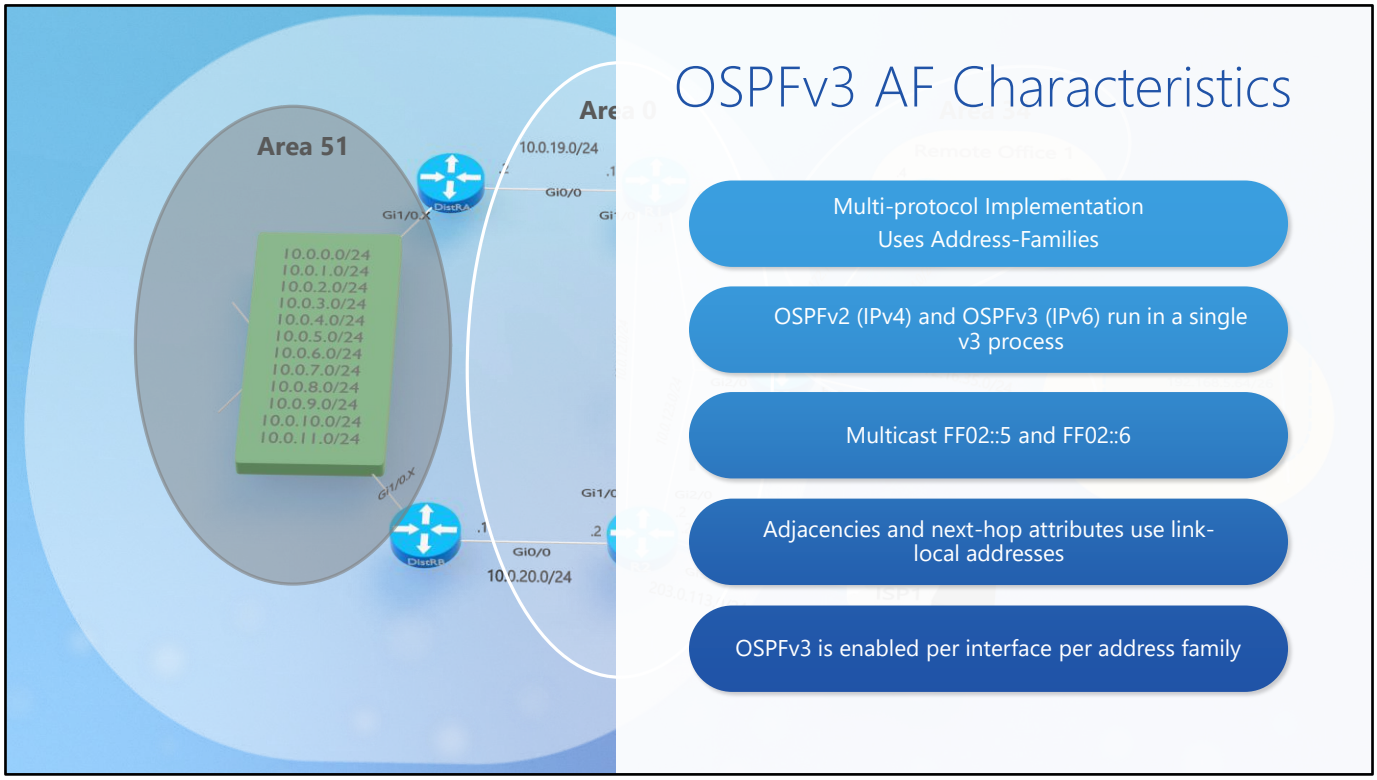
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



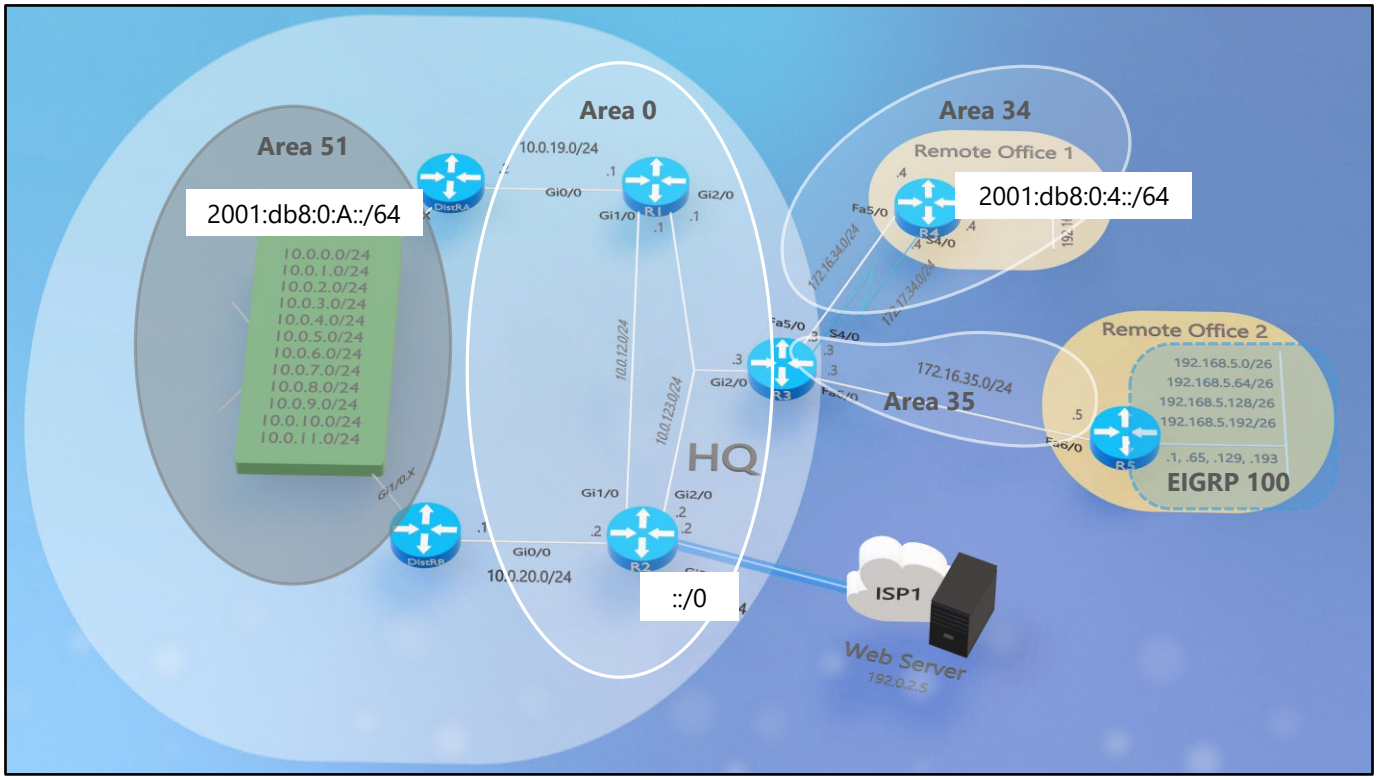
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/configuration/xe-16-5/iro-xe-16-5-book/ip6-route-ospfv3-add-fam-xe.html

Requires IPv6 to be enabled on an interface.

Benefit: takes advantage of OSPFv3 LSA types 8 and 9. So it is more efficient and less resource intensive

Not compatible with OSPFv2 classic because LSA are transported over IPv6 using link-local addresses

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Instructor Notes:
Demo everything

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Instructor Notes:
Demo everything

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Multi-Protocol Border Gateway Protocol v4 (MP-BGPv4)

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



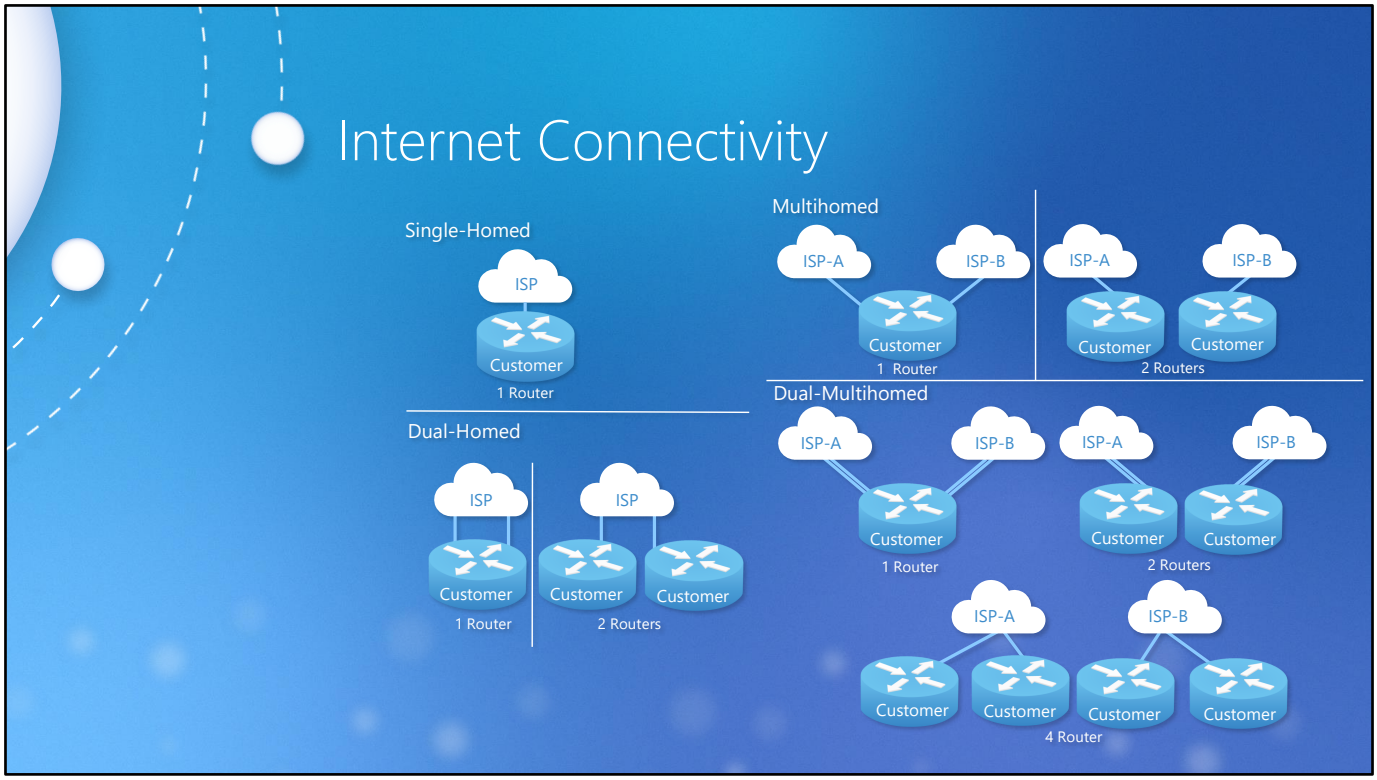
Title slide

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Border Gateway Protocol

- **Routing Protocol For the Internet**
- **Very Scalable**
- **Used heavily by ISPs**
- **Used lightly by non-ISPs**

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Is BGP really needed in single and dual homed. Not really as static default routes (floating) will work.

The same is true for multihomed. If routing is simple then floating routes will work.

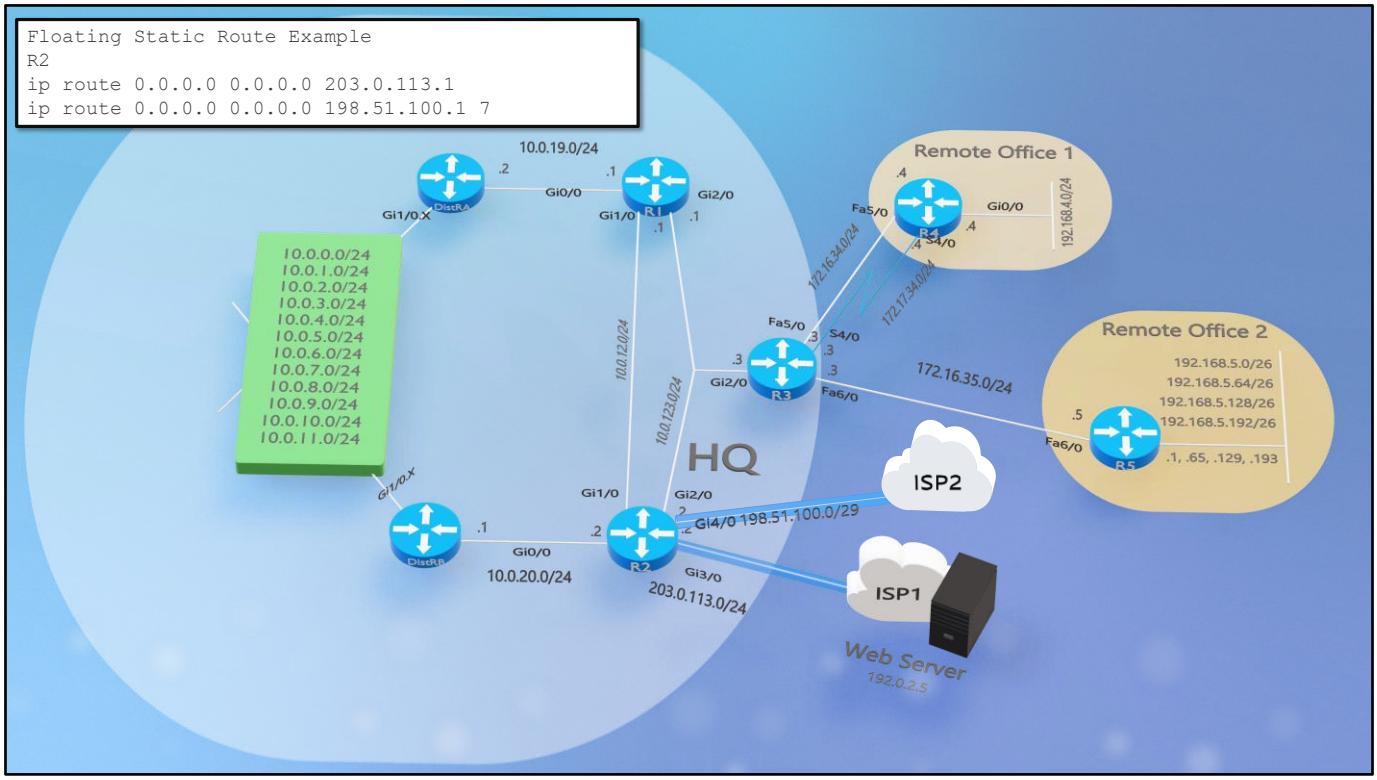
However, in the multihomed scenario, if you want to manipulate routes in and out of your network you will need to use BGP.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



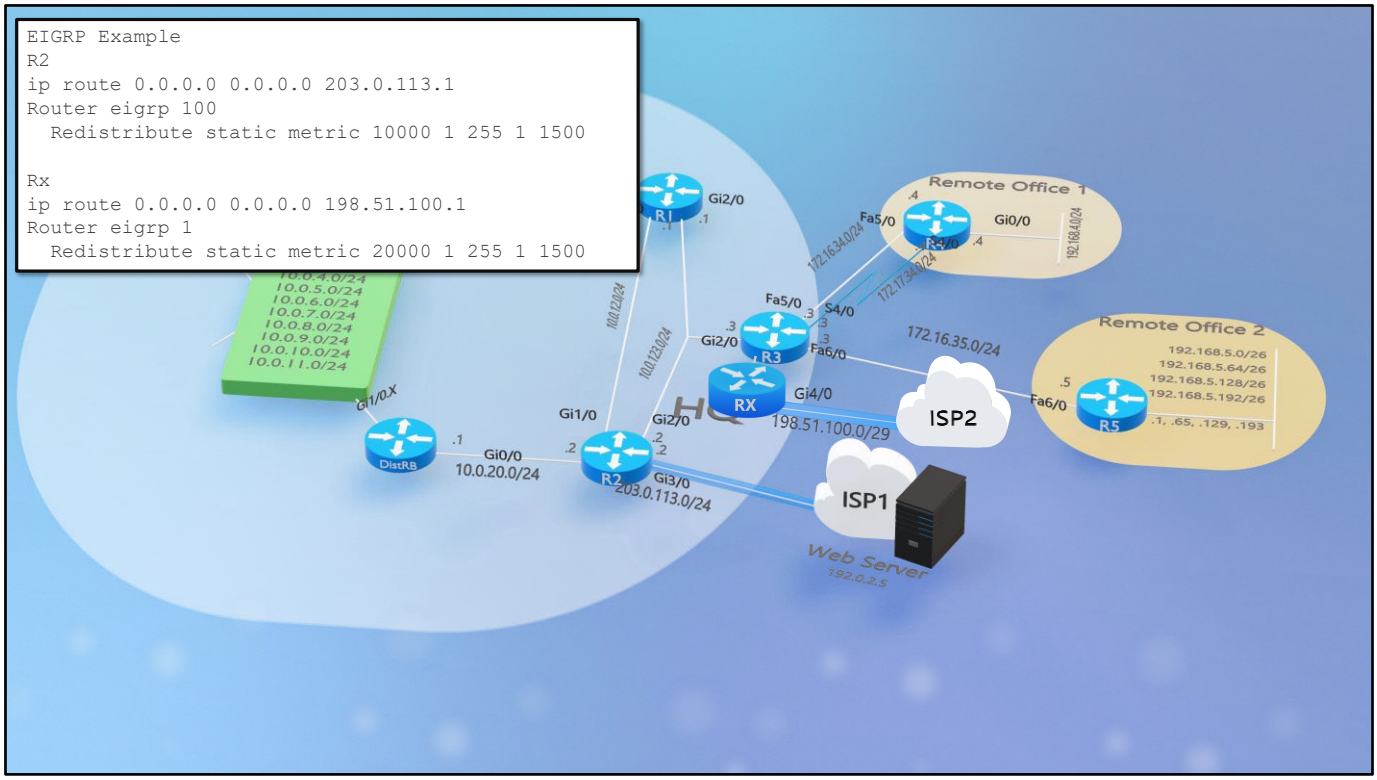
Review R2s single router dual home connectivity with floating routes and IPSLA.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



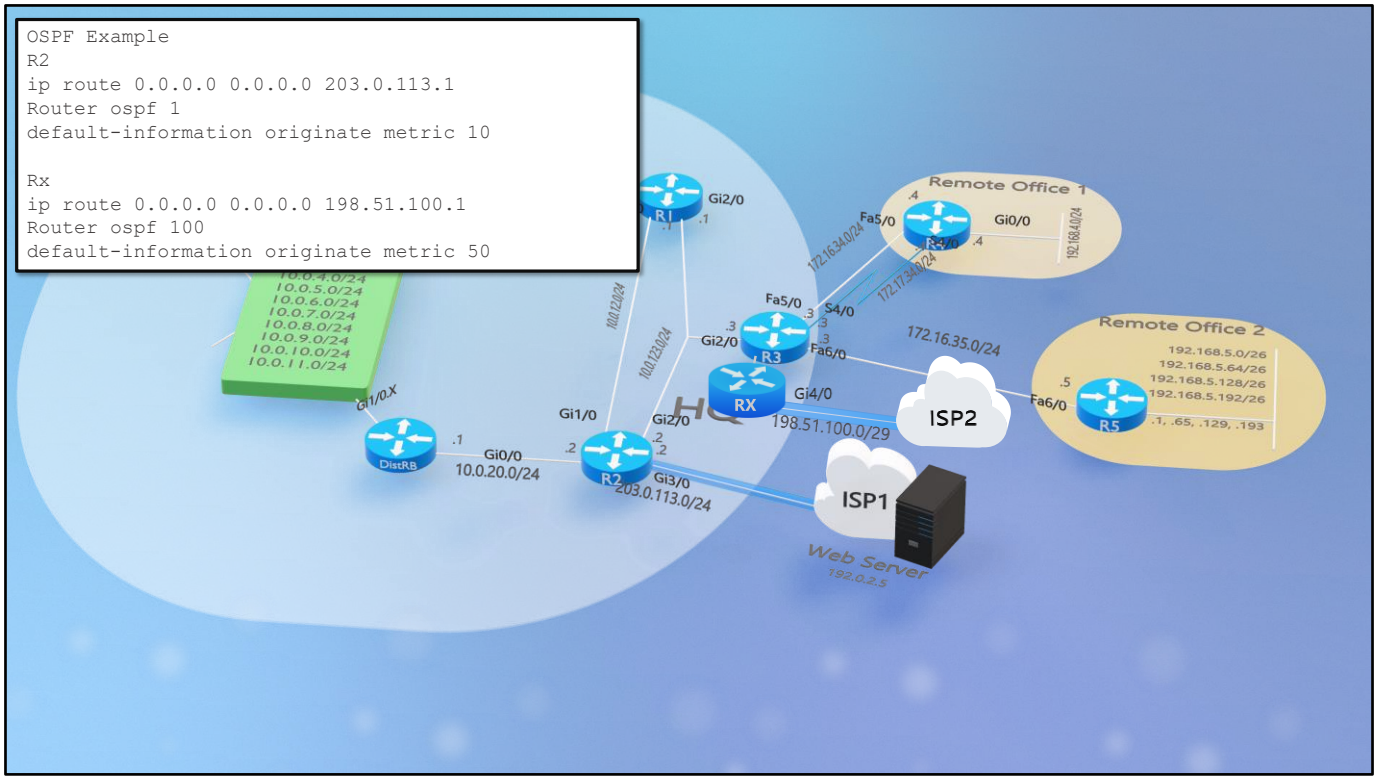
Review R2s single router dual home connectivity with floating routes and IPSLA.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



With this config all routers will use ISP1 because of the lower metric. However, if and when there is an issue getting to ISP1… R2 withdrawals the DF route and the route from RX is the only one remaining so ISP2 is used.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

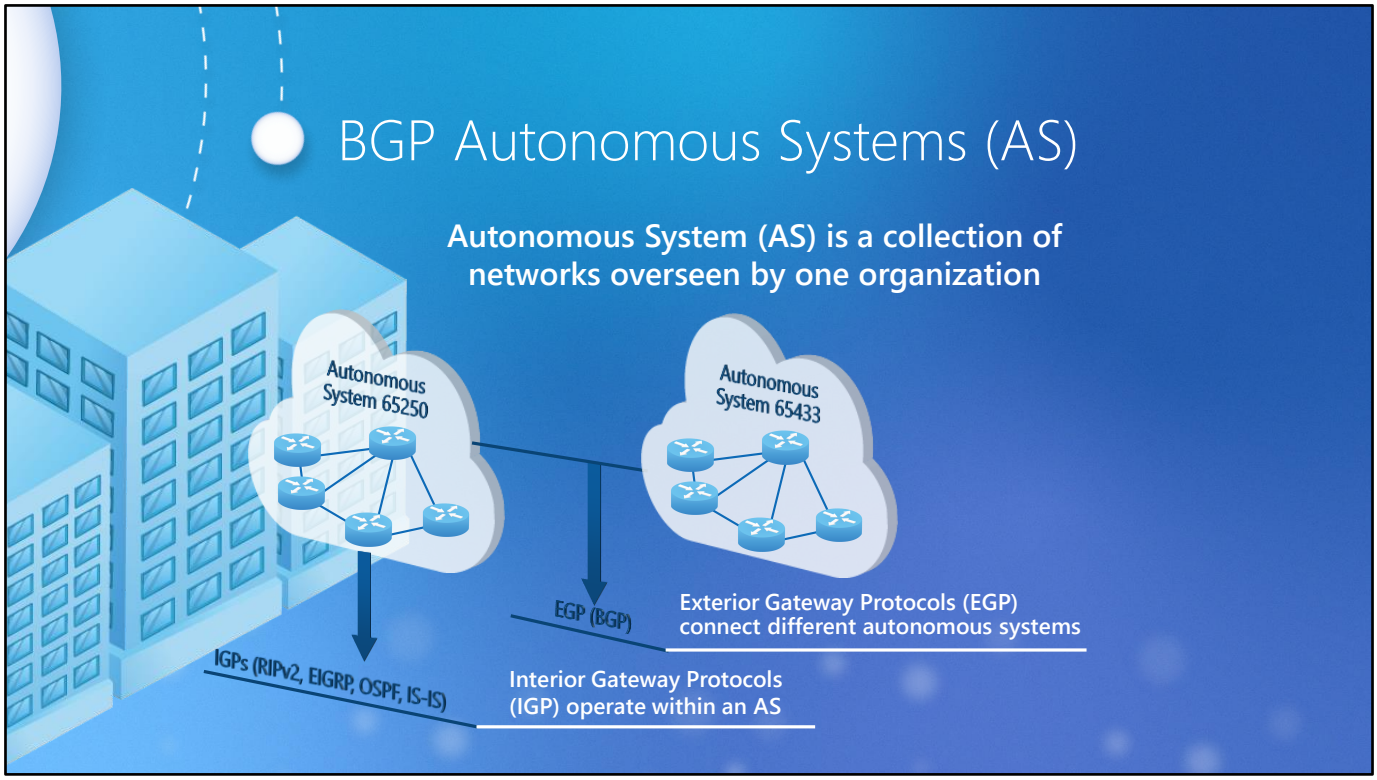


With this config all routers will use ISP1 because of the lower metric. However, if and when there is an issue getting to ISP1… R2 withdrawals the DF route and the route from RX is the only one remaining so ISP2 is used.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



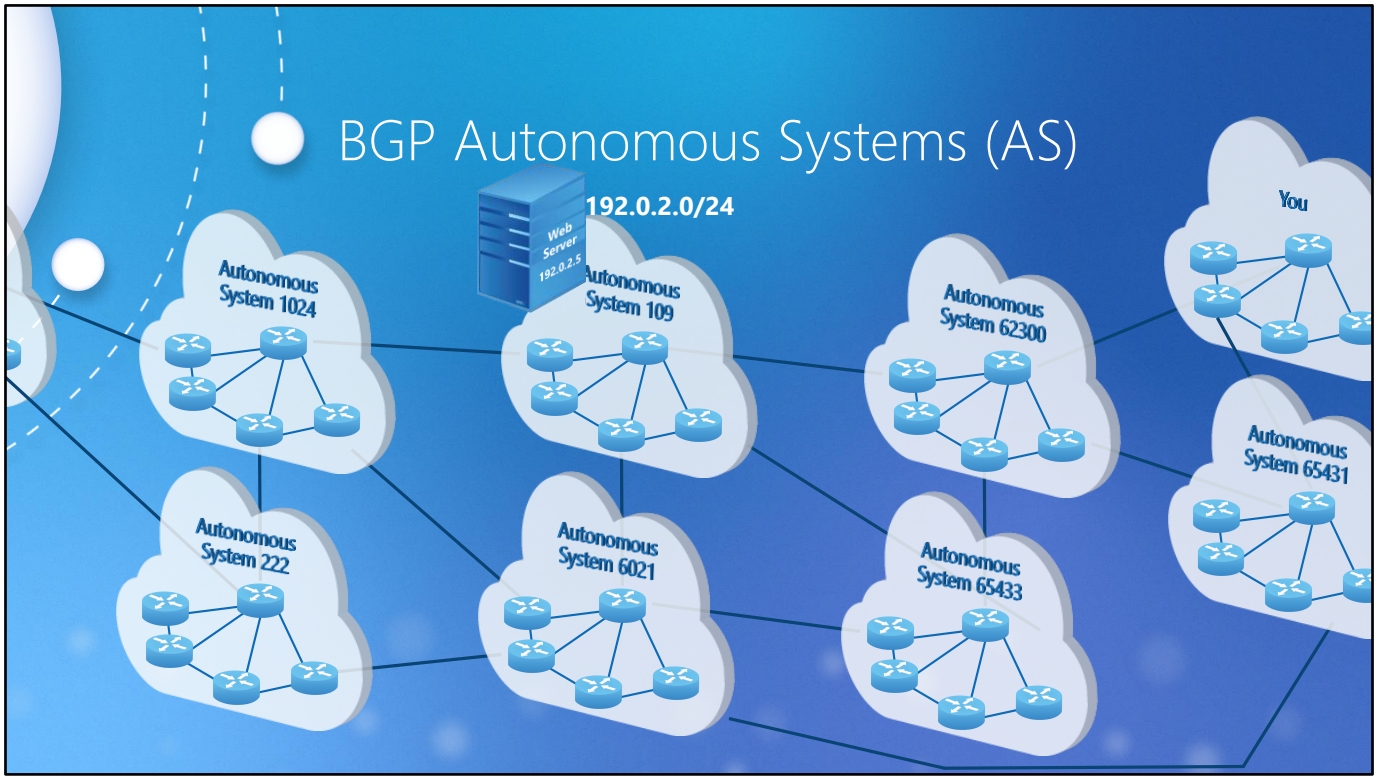
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



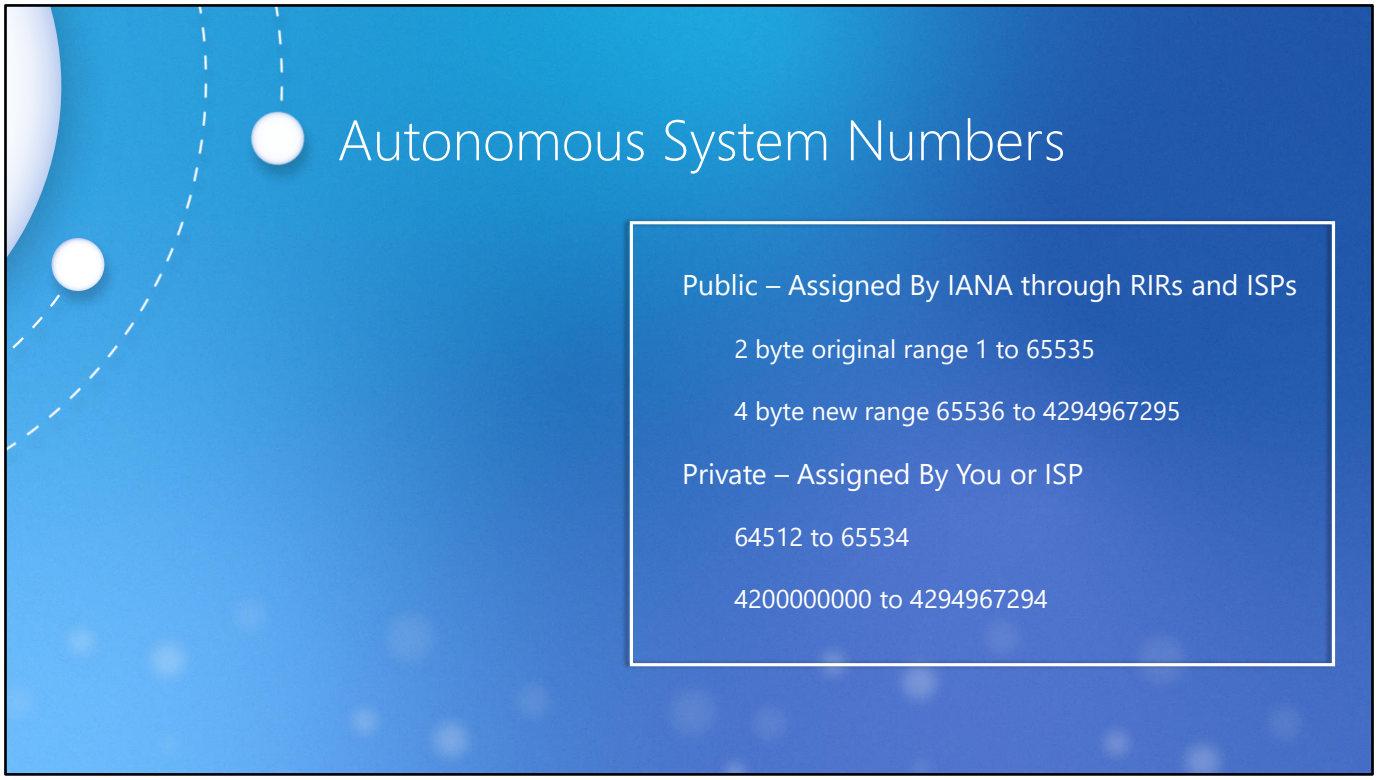
SO an AS defines who owns the IPv4 and IPv6 prefixes.
THEY MUST BE UNIQUE

From the perspective of BGP, an autonomous system (AS) is a collection of routers and their prefixes under a single organization's control, and it uses one or more Interior Gateway Protocols (IGPs) and common metrics to route packets within the AS. If multiple IGPs or metrics are used within an AS, the AS must appear consistent to external ASs in routing policy. An IGP is not required within an AS; an AS could use BGP as the only routing protocol.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



AS numbers are critical to BGP success

Represenation:
Asplain—Decimal value notation where both 2-byte and 4-byte AS numbers are represented by their decimal value. For example, 65526 is a 2-byte AS number and 234567 is a 4-byte AS number.
Asdot—Autonomous system dot notation where 2-byte AS numbers are represented by their decimal value and 4-byte AS numbers are represented by a dot notation. For example, 0.65526 is a 2-byte AS number and 1.169031 is a 4-byte AS number (this is dot notation for the 234567 decimal number).

Autonomous System Numbers (ASNs)
An organization requiring connectivity to the Internet must obtain an ASN. ASNs were originally 2 bytes (in the 16-bit range), which made 65,535 ASNs possible. Due to exhaustion, RFC 4893 expanded the ASN field to accommodate 4 bytes (in the 32-bit range). This allows for 4,294,967,295 unique ASNs, providing quite an increase from the original 65,535 ASNs.
Two blocks of private ASNs are available for any organization to use, as long as these ASNs are never exchanged publicly on the Internet. ASNs 64,512 through 65,535 are private ASNs in the 16-bit ASN range, and 4,200,000,000 through 4,294,967,294 are private ASNs in the extended 32-bit range.
***BEGIN NOTE

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Note[em]It is imperative to use only the ASN assigned by the IANA, the ASN assigned by your service provider, or a private ASN. Using another organization's ASN without permission could result in traffic loss and cause havoc on the Internet.

https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/13756-32.html

Generally customer networks and their routing policies are an extension of the respective Internet Service Providers (ISPs). When a customer network is large, the service provider may assign an AS number using a couple of different methods in order to manage the network and routing policies.

One way is by permanently assigning an AS number in the range of 1 to 64511. This is done when a customer network connects to two different ISPs, such as multihoming. This situation mandates that customer network should have a unique AS number so that it can uniquely propagate its BGP routes to a global BGP mesh via two ISPs.

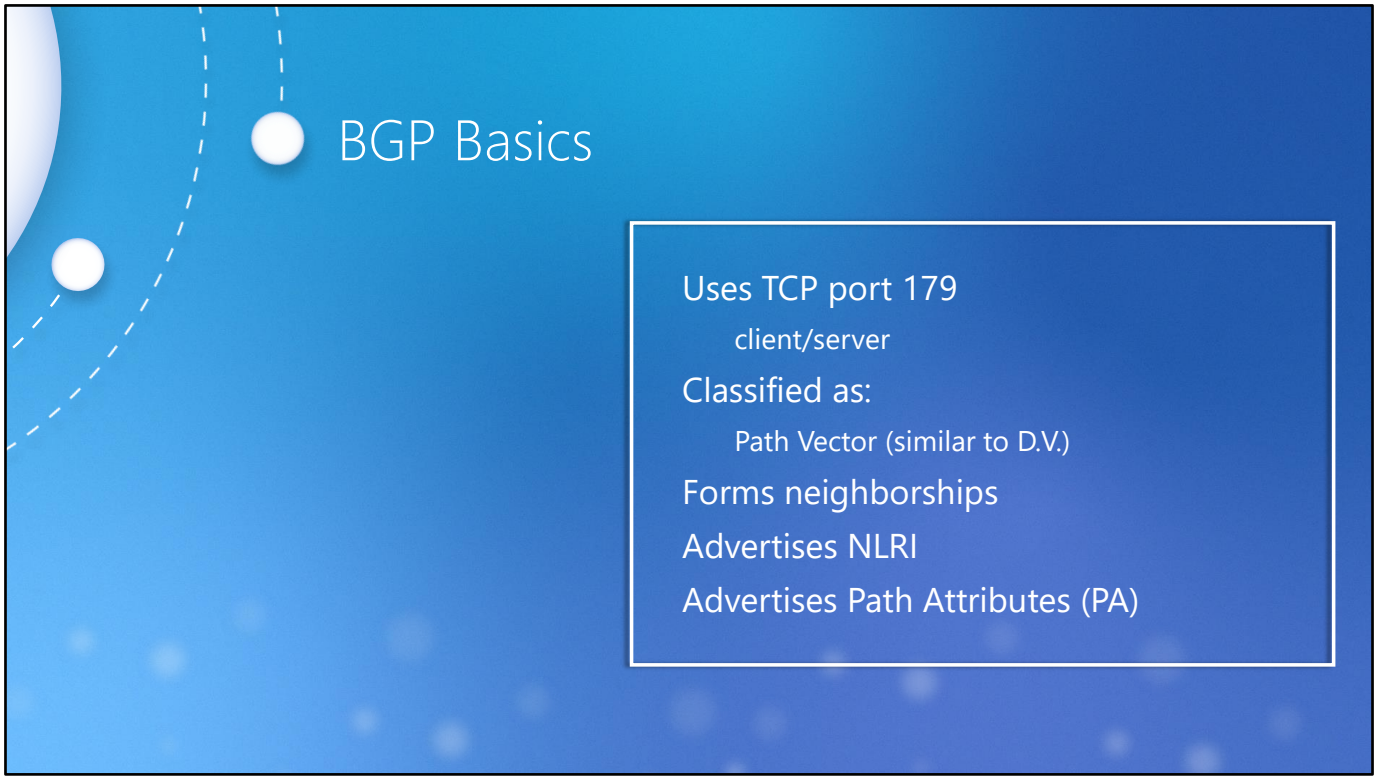
A second way is by assigning a Private AS number in the range of 64512 to 65535. This is done when a customer network connects to a single ISP (either single-homed or dual-homed to the same ISP) and the intention is to conserve the AS numbers. It is not recommended that you use a private AS number if you are planning to connect to multiple ISPs in the future.

When a private AS number is allocated to the customer network, the BGP updates from the customer network to ISP will have the private AS number in its AS_PATH list. When the ISP propagates its network information to the global BGP table (Internet), it should not propagate the AS_PATH with the private AS number of the customer to the Internet. To help the ISP remove the private AS number from its AS_PATH list, use the Cisco IOS **remove-private-as** command.

To remove the private AS number, use the **neighbor x.x.x.x remove-private-as** router configuration command.

The **neighbor x.x.x.x remove-private-as** per-neighbor configuration command forces BGP to drop the private AS numbers. You can configure this command for external BGP neighbors. When the outbound update contains a sequence of private AS numbers, this sequence is dropped.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



NLRI – network layer reachability information (fancy way to say subnet or prefix/mask)

Loop Prevention
BGP is a path vector routing protocol and does not contain a complete topology of the network, as do link-state routing protocols. BGP behaves like distance vector protocols, ensuring that a path is loop free.
The BGP attribute AS_Path is a well-known mandatory attribute and includes a complete list of all the ASNs that the prefix advertisement has traversed from its source AS. AS_Path is used as a loop-prevention mechanism in BGP. If a BGP router receives a prefix advertisement with its AS listed in AS_Path, it discards the prefix because the router thinks the advertisement forms a loop.

Path Attributes
BGP uses *path attributes* (*PAs*) associated with each network path. The PAs provide BGP with granularity and control of routing policies in BGP. The BGP prefix PAs are classified as any of the following:
[lb] Well-known mandatory
[lb] Well-known discretionary
[lb] Optional transitive
[lb] Optional non-transitive
Well-known attributes must be recognized by all BGP implementations. Well-known mandatory attributes must be included with every prefix advertisement; well-known discretionary attributes may or may not be included with the prefix advertisement.
Optional attributes do not have to be recognized by all BGP implementations. Optional attributes can be set so that they are transitive and stay with the route advertisement from AS to AS. Other PAs are *non-transitive* and cannot be shared from AS to AS. In BGP, the *Network Layer Reachability Information* (*NLRI*) is the routing update

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

that consists of the network prefix, prefix length, and any BGP PAs for that specific route.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

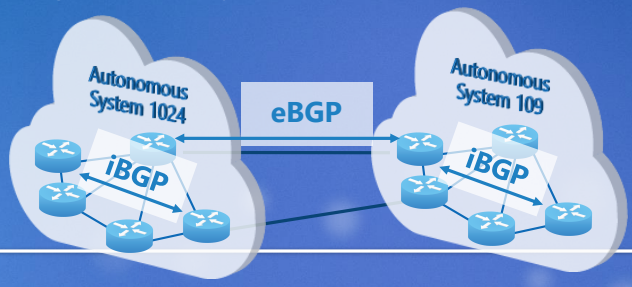
eBGP vs iBGP

eBGP

Peering between directly connected routers in different AS, AD of 20

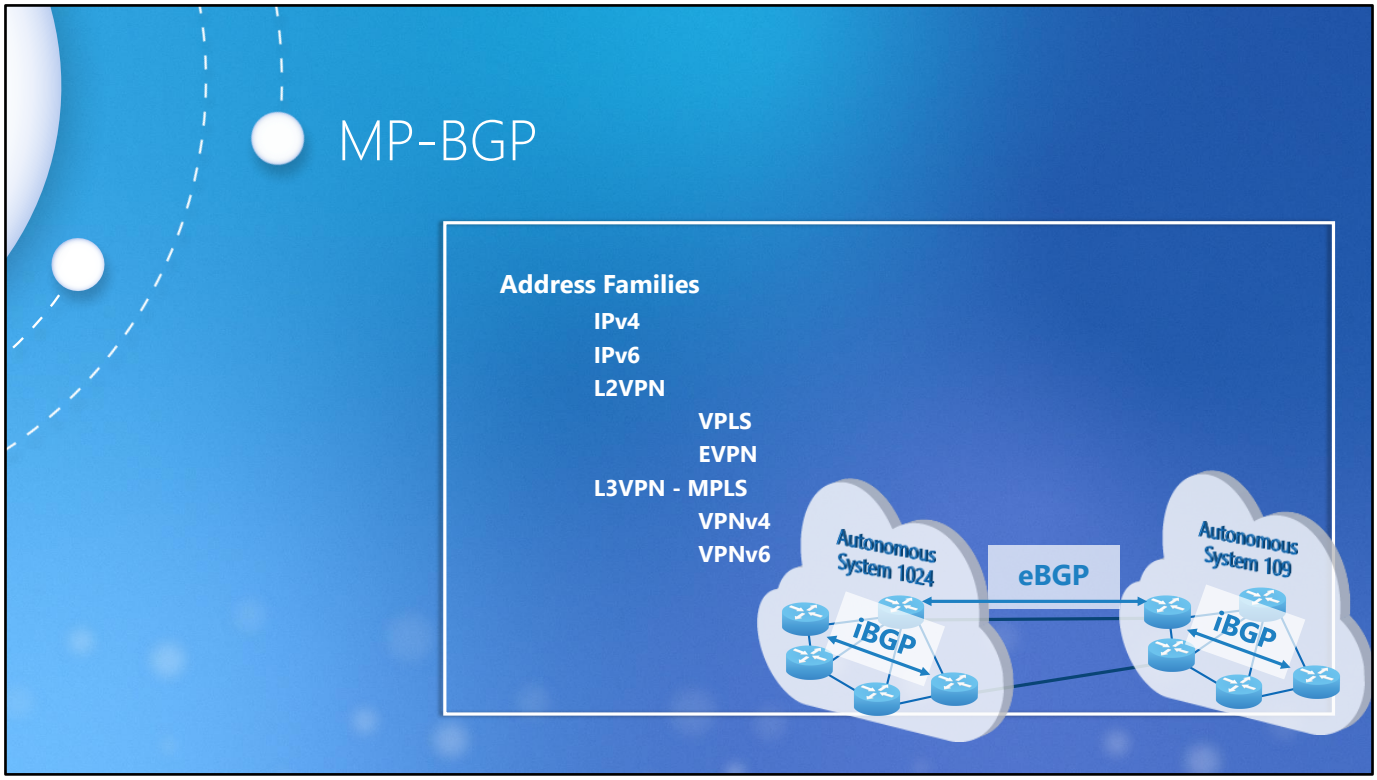
iBGP

Peering between any routers in same AS, AD of 200



Higher AD for iBGP means?

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



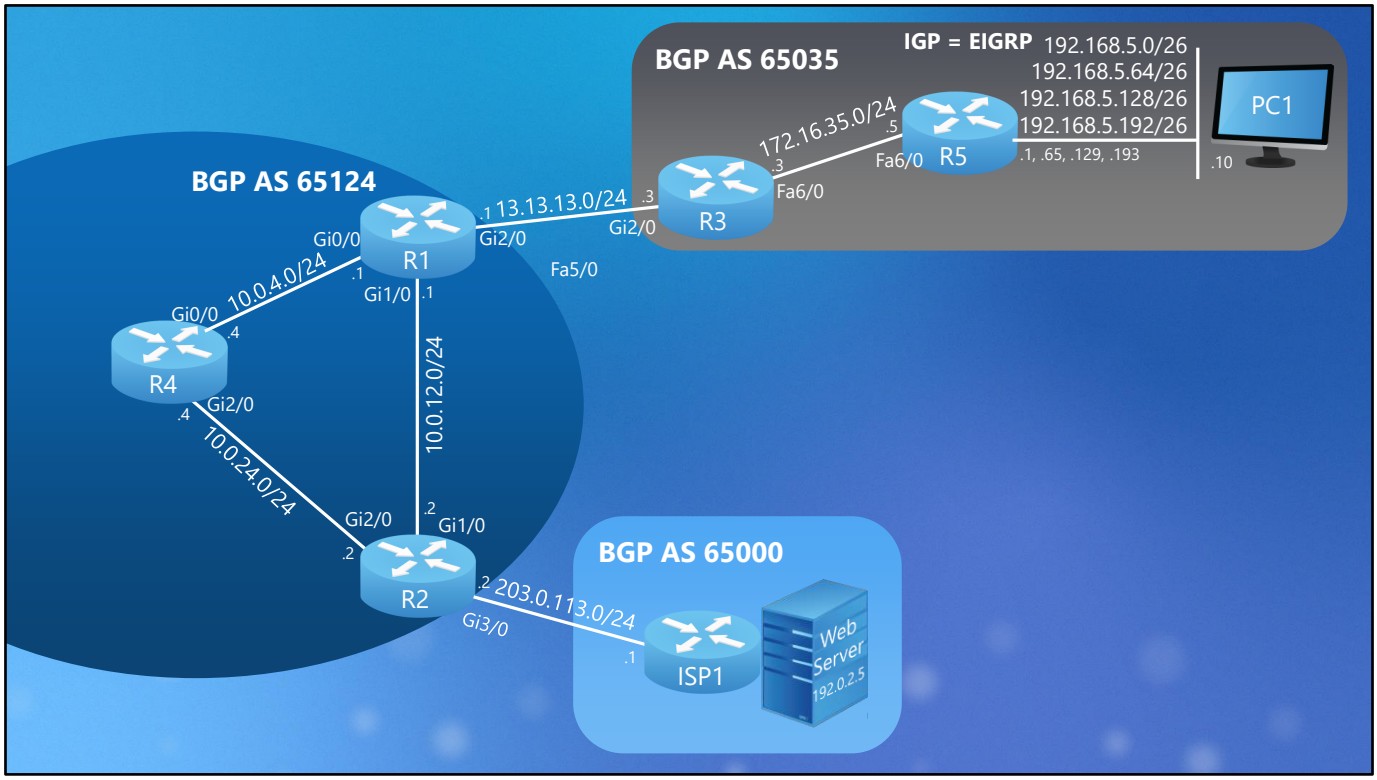
The available address families will depend on the platform and the installed license. Smaller platforms may only have IPv4 and IPv6. Large service-provider platforms will have many address-family options.
The strength of MP-BGP is that it can carry several address families at once. It is used with MPLS VPN's, as it can carry MPLS information as well as IPv4 and IPv6 information. This makes it a great choice for service providers. They can create a backbone network, and use BGP and VRF's to carry routes for several customers.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Title slide

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



DEMO:

Use address families (global mode relates to transport config info / address family related to information pertaining to NLRI)

ebgp between r1 and r3. (also set r1 as client and r3 as server [neighbor 13.13.13.3 transport connection-mode ???])
Advertise from r3 to r1. network 192.168.5.0/26 redistribute other 3 (remember to use prefix list and route map which are already configured)
Configure authentication between R1 and R3 (clear ip bgp *)
Redistribute static route on r3 into eigrp.
Ebgp between r2 and web AS (isp already configured)
Ibgp between r1 and r2 using loopback interfaces (update-source)
Fix next-hop-self between r1 and r2
Ping from pc1 to verify connectivity to web server

Extra: ebgp multi hop from R2 to ISP1. (just show the command that would be used [neighbor 203.0.1113.1 ebgp-multihop ???].

Notes:
no bgp default ipv4-unicast shut off automatic IPv4 activation

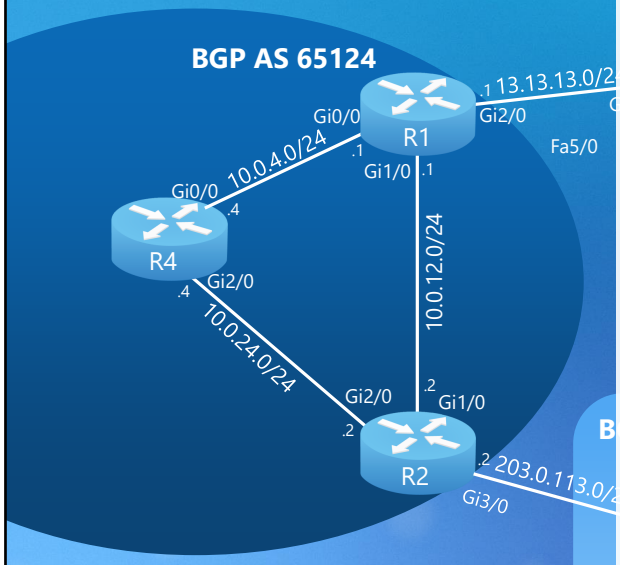
Show bgp ipv4 unicast
Show bgp ipv4 unicast summary

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Show bgp ipv4 unicat neighbor

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Advertisement of NLRI



NLRI are aka:

- BGP prefixes

BGP table is where these learned prefix and their Path Attributes PA are stored.

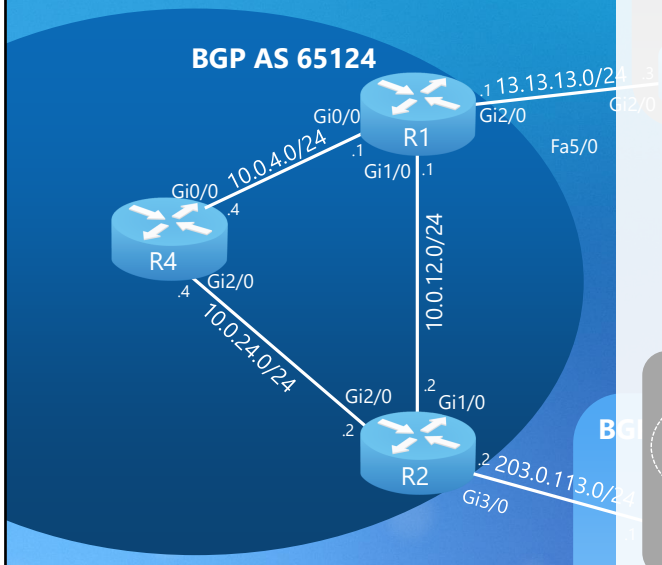
Learned via:

- Network command
- BGP updates
- Redistribution

Des p. 548

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

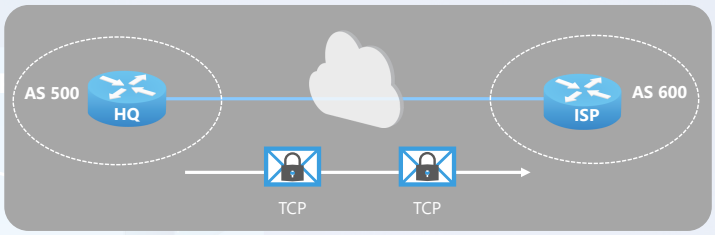
BGP Authentication



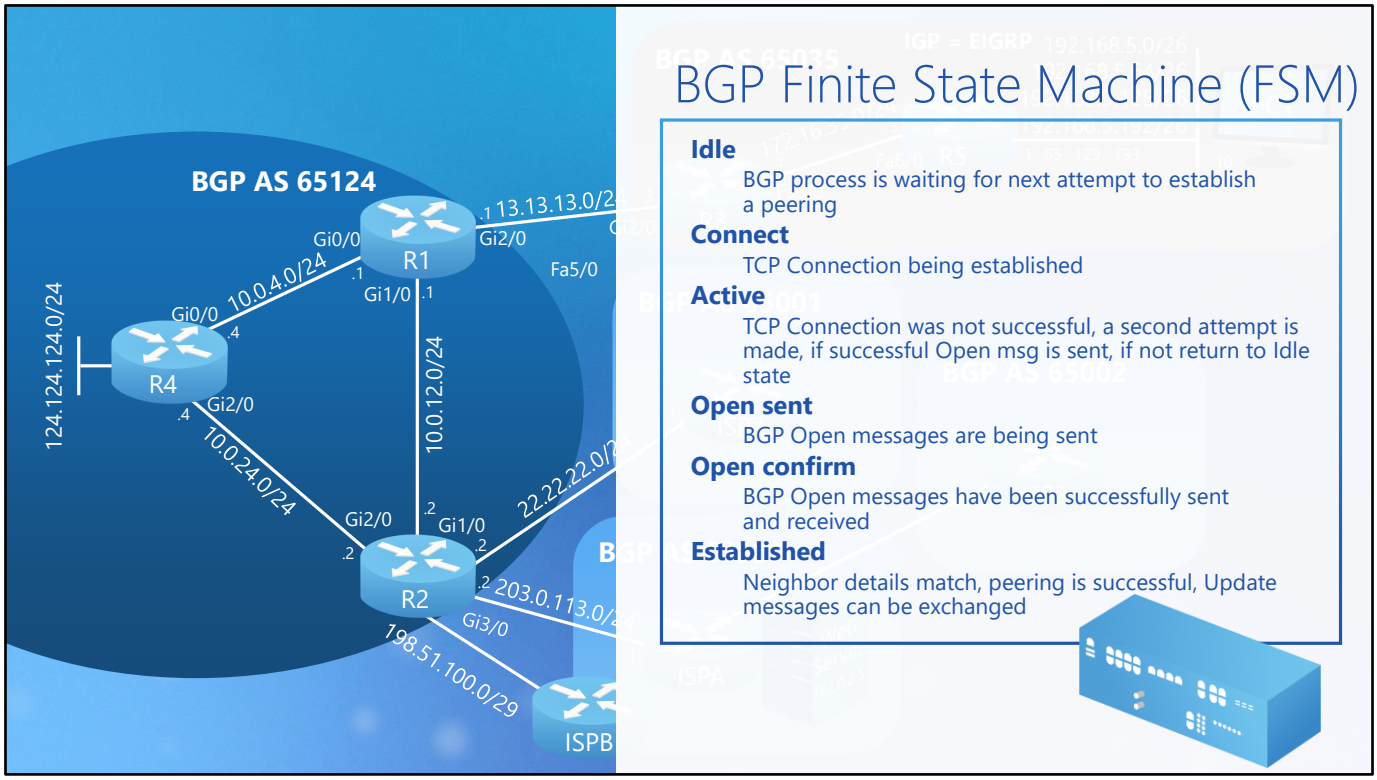
BGP uses MD5 for authentication

Router uses the source IP for authentication

Before TCP connection is established, the router will verify MD5 digest



©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



https://en.wikipedia.org/wiki/Border_Gateway_Protocol

Idle State:

Refuse all incoming BGP connections.
Start the initialization of event triggers.
Initiates a TCP connection with its configured BGP peer.
Listens for a TCP connection from its peer.
Changes its state to Connect.
If an error occurs at any state of the FSM process, the BGP session is terminated immediately and returned to the Idle state. Some of the reasons why a router does not progress from the Idle state are:

- TCP port 179 is not open.
- A random TCP port over 1023 is not open.
- Peer address configured incorrectly on either router.
- AS number configured incorrectly on either router.

Connect State:

Waits for successful TCP negotiation with peer.
BGP does not spend much time in this state if the TCP session has been successfully established.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Sends Open message to peer and changes state to OpenSent.
If an error occurs, BGP moves to the Active state. Some reasons for the error are:

- TCP port 179 is not open.
- A random TCP port over 1023 is not open.
- Peer address configured incorrectly on either router.
- AS number configured incorrectly on either router.

Active State:

If the router was unable to establish a successful TCP session, then it ends up in the Active state.
BGP FSM tries to restart another TCP session with the peer and, if successful, then it sends an Open message to the peer.
If it is unsuccessful again, the FSM is reset to the Idle state.
Repeated failures may result in a router cycling between the Idle and Active states. Some of the reasons for this include:

- TCP port 179 is not open.
- A random TCP port over 1023 is not open.
- BGP configuration error.
- Network congestion.
- Flapping network interface.

OpenSent State:

BGP FSM listens for an Open message from its peer.
Once the message has been received, the router checks the validity of the Open message.
If there is an error it is because one of the fields in the Open message does not match between the peers, e.g., BGP version mismatch, the peering router expects a different My AS, etc. The router then sends a Notification message to the peer indicating why the error occurred.
If there is no error, a Keepalive message is sent, various timers are set and the state is changed to OpenConfirm.

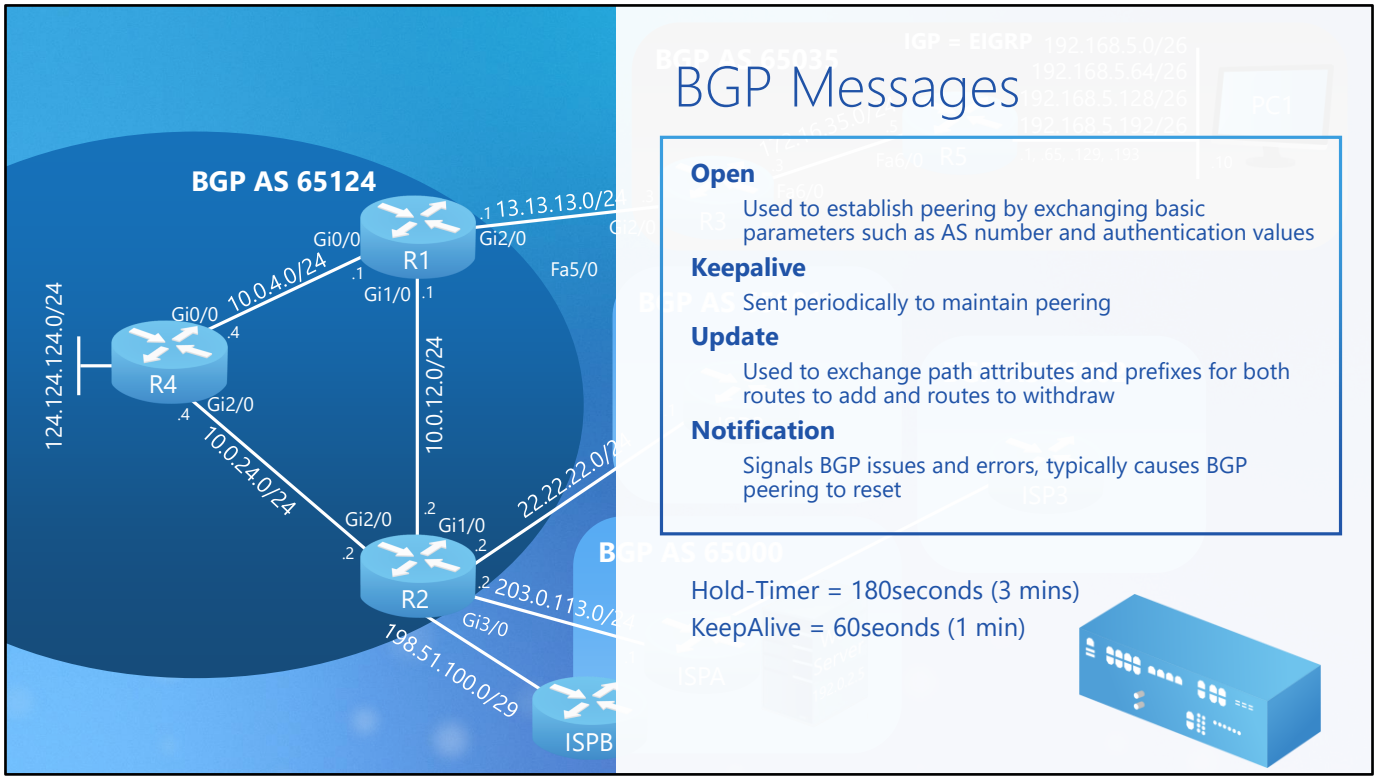
OpenConfirm State:

The peer is listening for a Keepalive message from its peer.
If a Keepalive message is received and no timer has expired before reception of the Keepalive, BGP transitions to the Established state.
If a timer expires before a Keepalive message is received, or if an error condition occurs, the router transitions back to the Idle state.

Established State:

In this state, the peers send Update messages to exchange information about each route being advertised to the BGP peer.
If there is any error in the Update message then a Notification message is sent to the peer, and BGP transitions back to the Idle state.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



OPEN
An OPEN message is used to establish a BGP adjacency. Both sides negotiate session capabilities before BGP peering is established. The OPEN message contains the BGP version number, the ASN of the originating router, the hold time, the BGP identifier, and other optional parameters that establish the session capabilities:

KEEPALIVE
BGP does not rely on the TCP connection state to ensure that the neighbors are still alive. KEEPALIVE messages are exchanged every one-third of the hold timer agreed upon between the two BGP routers. Cisco devices have a default hold time of 180 seconds, so the default keepalive interval is 60 seconds. If the hold time is set to 0, no KEEPALIVE messages are sent between the BGP neighbors.

UPDATE
An UPDATE message advertises any feasible routes, withdraws previously advertised routes, or can do both. The Update message holds the NLRI, which includes the prefix and associated BGP PAs when advertising prefixes. Withdrawn NLRI routes include only the prefix. An UPDATE message can act as a keepalive to reduce unnecessary traffic.

NOTIFICATION
A NOTIFICATION message is sent when an error is detected with the BGP session, such as a hold timer expiring, neighbor capabilities changing, or a BGP session reset being requested. This causes the BGP connection to close.

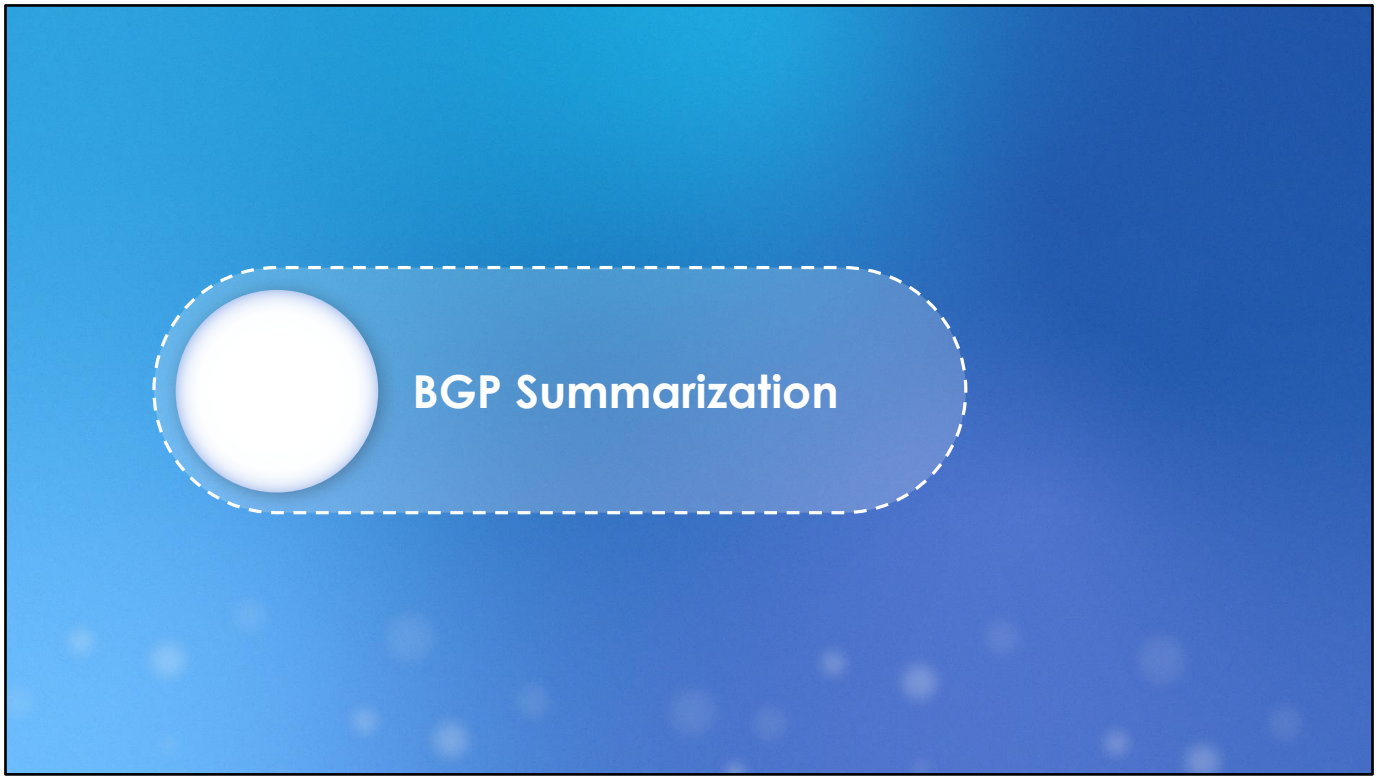
timers do not have to match – they are negotiated and the lower value is used.
Modify the BGP timers (optional). BGP relies on a stable network topology due to the size of a routing table. BGP KEEPALIVE and UPDATE messages ensure that the BGP neighbor is established. The default hold timer requires that a packet be received every 3 minutes (180 seconds) to maintain the BGP session. The hold timer is negotiated

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

when the BGP session is first established.

By default, BGP sends a KEEPALIVE message to a BGP neighbor every 60 seconds. The BGP keepalive timer and hold timer can be set at the process level or per neighbor session. Some designs may require BGP timers to be set more aggressively or adaptably, depending upon the design. The BGP timers can be modified for a session with the command **neighbor** *ip-address* **timers** *keepalive holdtime* [*minimum-holdtime*].

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Title slide

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

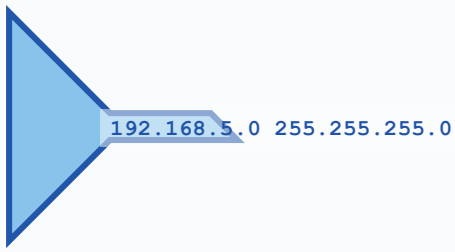
Route Summarization

BGP Summarization

Conserves router resources and accelerates best-path calculation by reducing the size of the tables

Provides the benefit of stability by hiding route flaps from downstream routers, thereby reducing routing churn

192.168.5.0/26
192.168.5.64/26
192.168.5.128/26
192.168.5.192/26

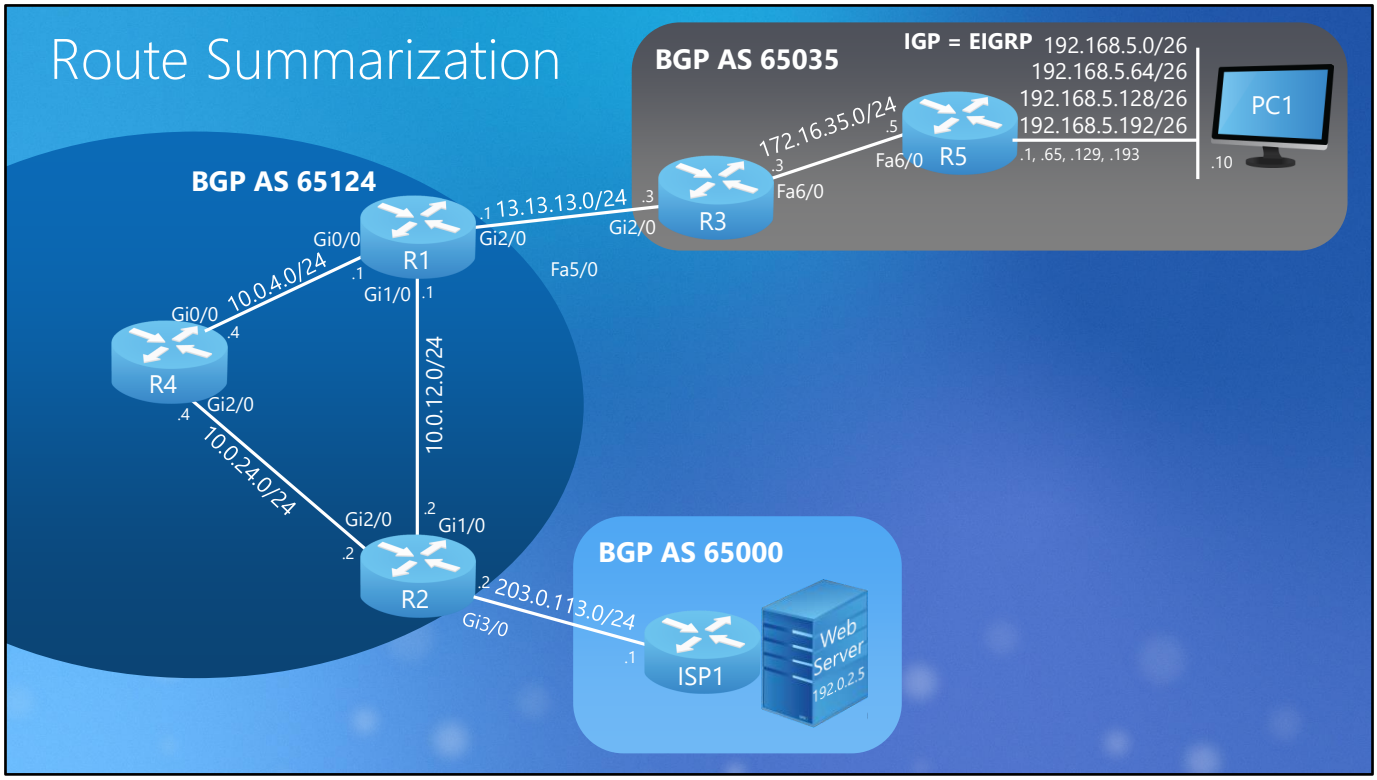



```
Router bgp 65035
 address-family ipv4
  aggregate-address 192.168.5.0 255.255.255.0 summary-only
```

Requires routes to be in the bgp table for it to work.
R3(config-router-af)#aggregate-address 192.168.5.0 255.255.255.0 (this one advertises the summary and the specific routes)

R3(config-router-af)#aggregate-address 192.168.5.0 255.255.255.0 summary-only (this one advertises just the summary)

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.




```
Requires routes to be in the bgp table for it to work.
R3(config-router-af)#aggregate-address 192.168.5.0
255.255.255.0 (this one advertises the summary and the
specific routes)

R3(config-router-af)#aggregate-address 192.168.5.0
255.255.255.0 summary-only (this one advertises just the
summary)

***don't forget to show the router to NULL0 on R3****

Delete what you did and do the same thing on R2 and look
at the AS PATH on ISP1… ouch.
R2(config-router-af)#aggregate-address 192.168.5.0
255.255.255.0 (this one advertises the summary and the
specific routes)
R2(config-router-af)#aggregate-address 192.168.5.0
255.255.255.0 summary-only (this one advertises just the
summary)
```

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

ON ISP 1 - Show bgp ipv4 unicast (no ASPATH INFO
ON ISP 1 - Show bgp ipv4 unicast 192.168.5.0 (look for atomic aggegate attribute)
***Aggregated routes act like new BGP routes with a shorter prefix length. When a BGP router summarizes a route, it does not advertise the AS_Path information from before the aggregation. BGP path attributes like AS_Path, multi-exit discriminator (MED), and BGP communities are not included in the new BGP aggregate prefix.
The *atomic aggregate attribute* indicates that a loss of path information has occurred.

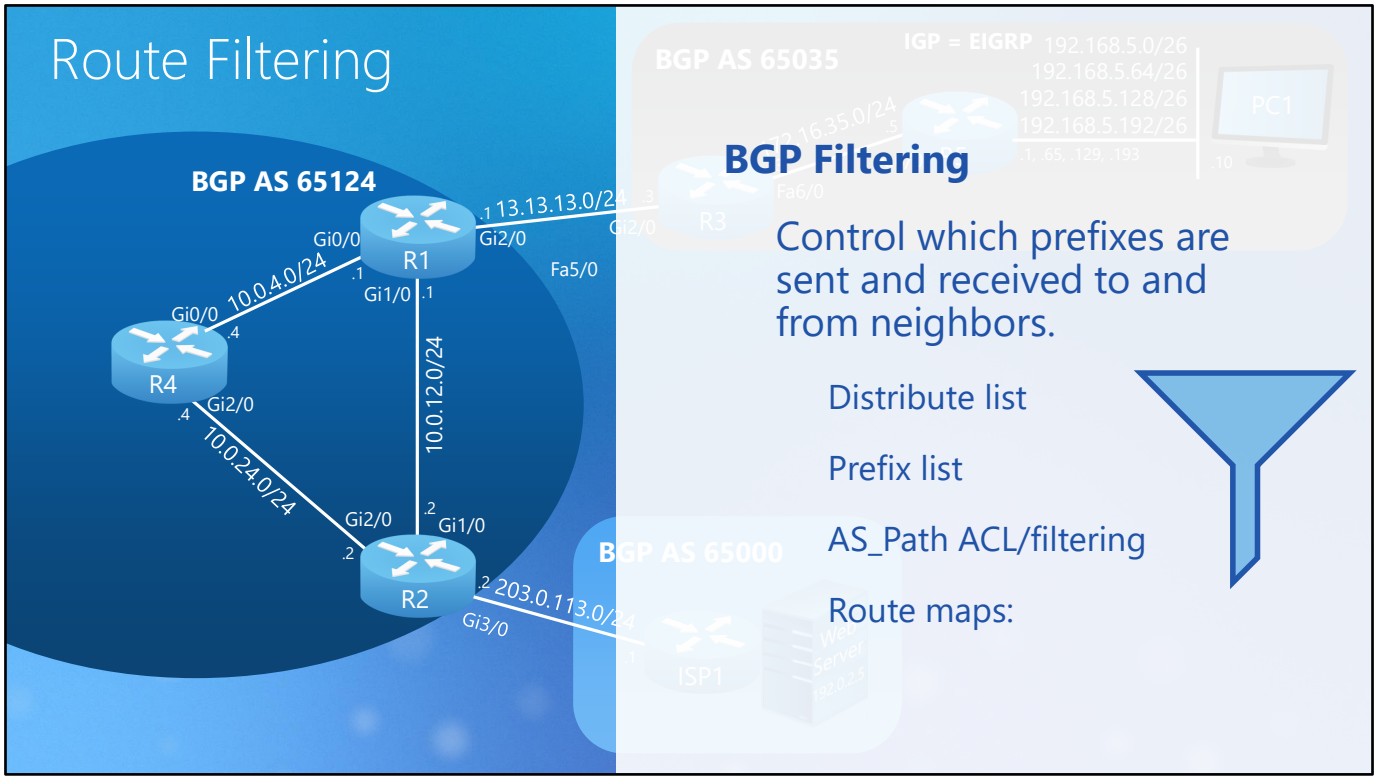
Add the AS-SET option to the command on R2 to preserve the information.
Check the output on ISP1 now.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Title slide

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



a method for selectively identifying prefixes that are advertised or received from peers. Selected routes can be modified or removed to manipulate traffic flows, reduce memory utilization, or improve security.

BGP Filtering

Control which prefixes are sent and received to and from neighbors.

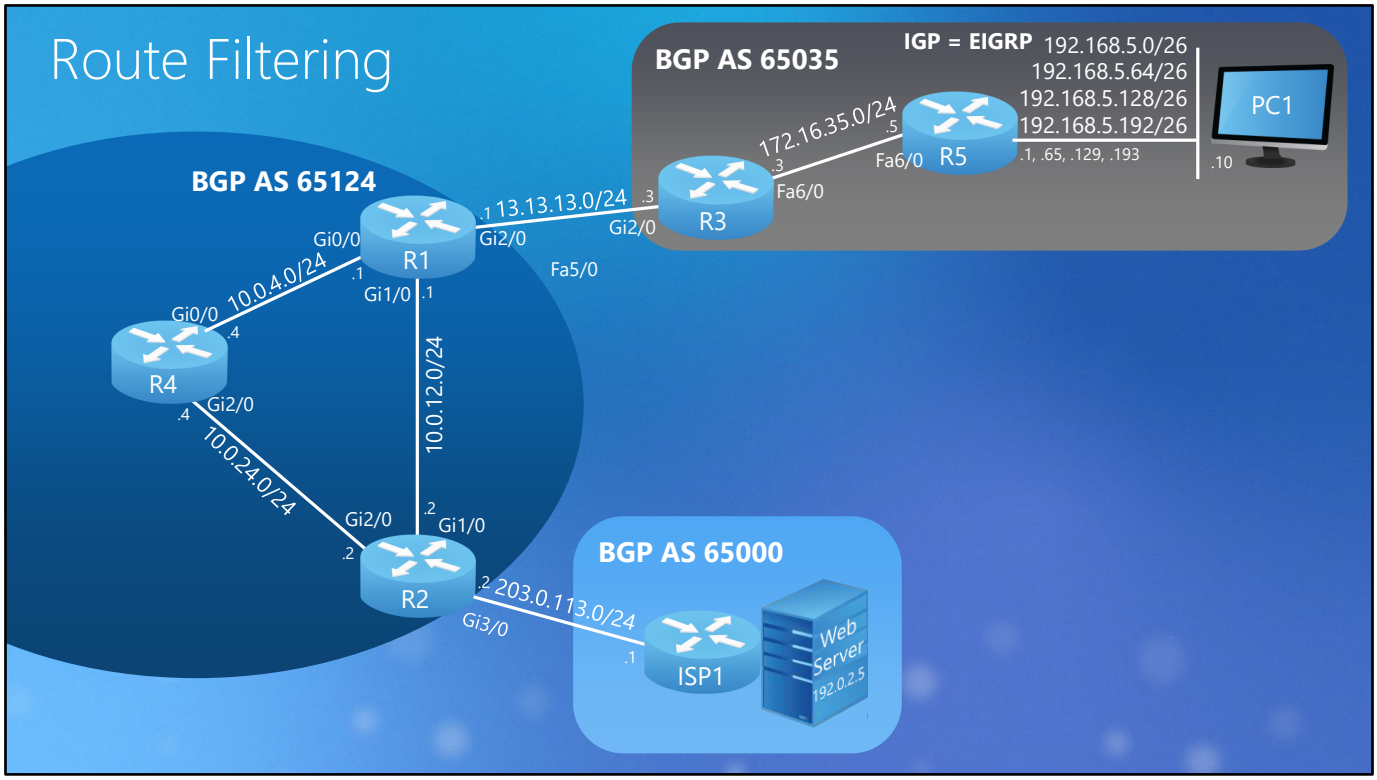
lb] **Distribute list:** A distribute list filters network prefixes based on a standard or extended access control list (ACL). An implicit deny is associated with any prefix that is not permitted.

[lb] **Prefix list:** A list of prefix-matching specifications that permit or deny network prefixes in a top-down fashion, much like an ACL. An implicit deny is associated with any prefix that is not permitted.

[lb] **AS_Path ACL/filtering:** A list of regex commands that allows for the permit or deny of a network prefix, based on the current AS_Path values. An implicit deny is associated with any prefix that is not permitted.

[lb] **Route maps:** Route maps provide a method of conditional matching on a variety of prefix attributes and allow you to take a variety of actions. An action could be a simple permit or deny or could include the modification of BGP path attributes. An implicit deny is associated with any prefix that is not permitted.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.




```
Verification with:
     sho ip pro
     Show bgp ipv4 unicast neighbor #.#.#.#

Distribute List
R3
ip access-list extended DISTBGP
deny ip 192.168.5.0 0.0.0.0 host 255.255.255.192 (this is
the subnet mask)
Permit ip 192.168.5.0 0.0.0.255 host 255.255.255.192
(this is the subnet mask)

router bgp 65035
 address-family ipv4 unicast
 neighbor 13.13.13.1 distribute-list DISTBGP out

Prefix List
R1
ip prefix-list FILTER deny 192.168.5.64/26
```

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

```
ip prefix-list FILTER permit 0.0.0.0/0 le 32
router bgp 65124
 address-family ipv4 unicast
 neighbor 13.13.13.3 prefix-list FILTER in
```

AS_Path ACL/filtering

R2 to ISP

ip as-path access-list 1 deny ^$

Ip as-path access-list 1 permit .*

router bgp 65124

address-family ipv4 unicast

neighbor 203.0.113.1 filter-list 1 out

ROUTE-MAPS

Route maps provide more functionality than pure filtering; they and provide a method to manipulate BGP path attributes as well. Route maps are applied on a BGP neighbor basis for routes that are advertised or received. We will stick to filtering at this point and examine attributes later.

R2

```
ip prefix-list FILTER permit 192.168.5.128/26
```

Route-map BGPFILTER deny 10

Match ip address prefix-list FILTER

Route-map BGPFILTER permit 20

Router bgp 65000

Neighbor 203.0.113.2 route-map BGPFILTER in

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Regular Expression (Regex) Query Modifiers

Modifier	Description
_ (underscore)	Matches a space
^ (caret)	Indicates the start of the string
$ (dollar sign)	Indicates the end of the string
[] (brackets)	Matches a single character or nesting within a range
- (hyphen)	Indicates a range of numbers in brackets
[^] (caret in brackets)	Excludes the characters listed in brackets
() (parentheses)	Used for nesting of search patterns
| (pipe)	Provides or functionality to the query
. (period)	Matches a single character, including a space
*** (asterisk)**	Matches zero or more characters or patterns
+ (plus sign)	Matches one or more instances of the character or pattern
? (question mark)	Matches one or no instances of the character or pattern

There may be times when conditionally matching network prefixes may be too complicated, and identifying all routes from a specific organization is preferred. In such a case, path selection can be used with the BGP AS_Path. AS_Path filtering is accomplished using an AS_Path ACL, which uses regular expressions for matching. The following sections explain the components for this task.

Regular Expressions (Regex)

To parse through the large number of available ASNs (4,294,967,295), you can use *regular expressions* (*regex*). Regular expressions are based on query modifiers to select the appropriate content.

The characters .^$*+()[]? are special control characters that cannot be used without using the backslash \ escape character. For example, to match on the * in the output, you would use the * syntax.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Regular Expression (Regex) Examples

Expression	Meaning
.*	Anything
^$	Locally originated routes (empty AS path)
^500_	Learned from AS 500
_500$	Originated in AS 500
_500_	Any ASPATH with 500 in it anywhere

There may be times when conditionally matching network prefixes may be too complicated, and identifying all routes from a specific organization is preferred. In such a case, path selection can be used with the BGP AS_Path. AS_Path filtering is accomplished using an AS_Path ACL, which uses regular expressions for matching. The following sections explain the components for this task.

Regular Expressions (Regex)

To parse through the large number of available ASNs (4,294,967,295), you can use *regular expressions* (*regex*). Regular expressions are based on query modifiers to select the appropriate content.

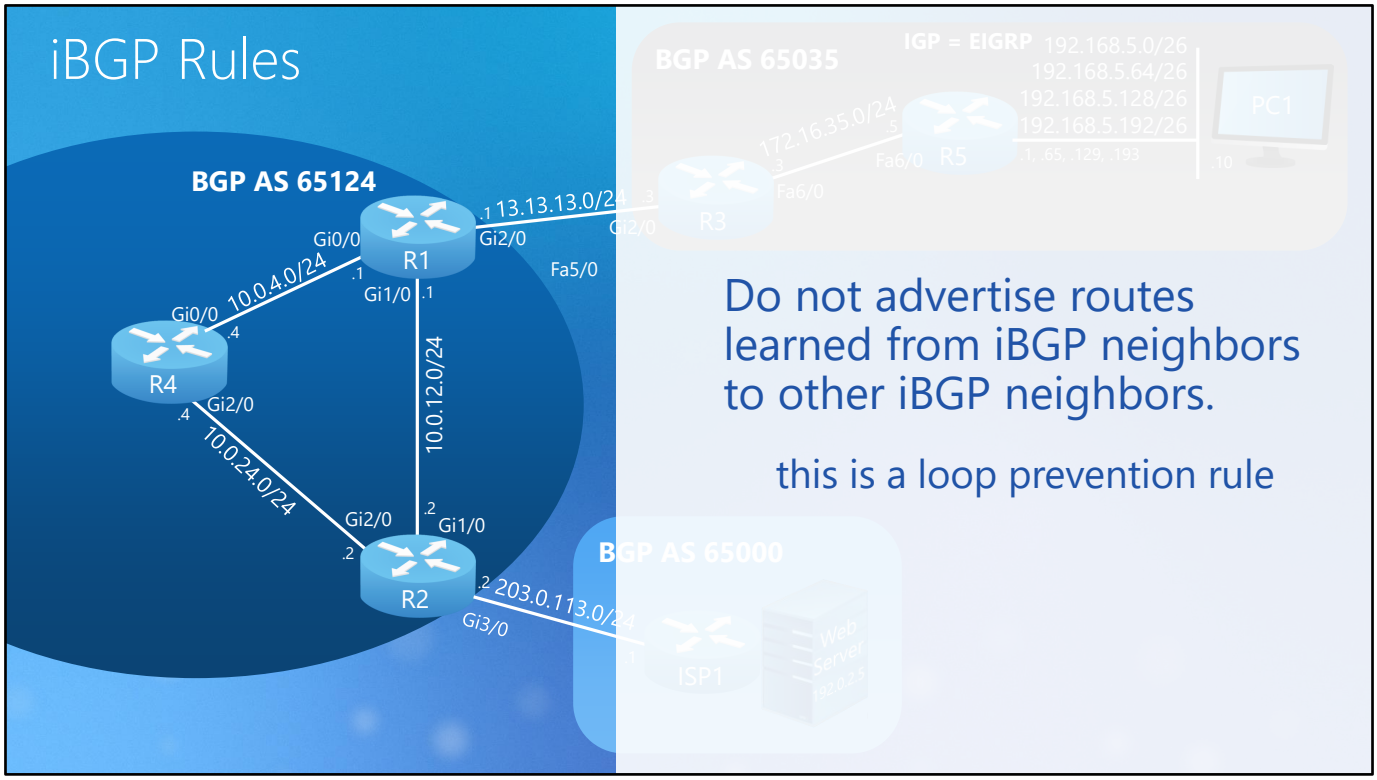
The characters .^$*+()[]? are special control characters that cannot be used without using the backslash \ escape character. For example, to match on the * in the output, you would use the * syntax.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Title slide

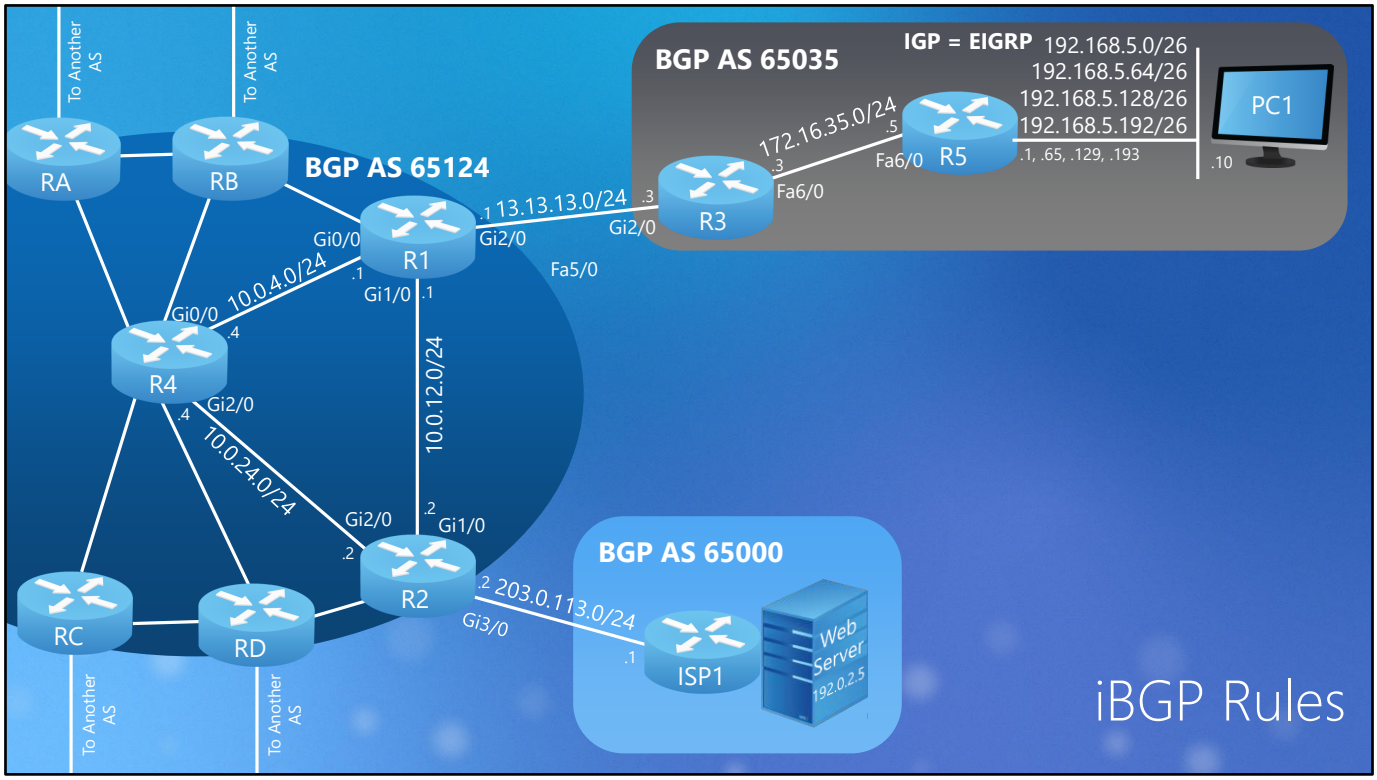
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



IBGP rules:
Do not advertise routes learned from iBGP neighbors to other iBGP neighbors. (this is a loop prevention rule)
Why? Well with eBGP the rule is do not listen/accept routes with your own AS number in it. Well, we can't use that rule with iBGP because we are learning from others in our own AS. So, to ensure a loop free topology iBGP will not advertise iBGP learned routes to other iBGP neighbors.

Next slide

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

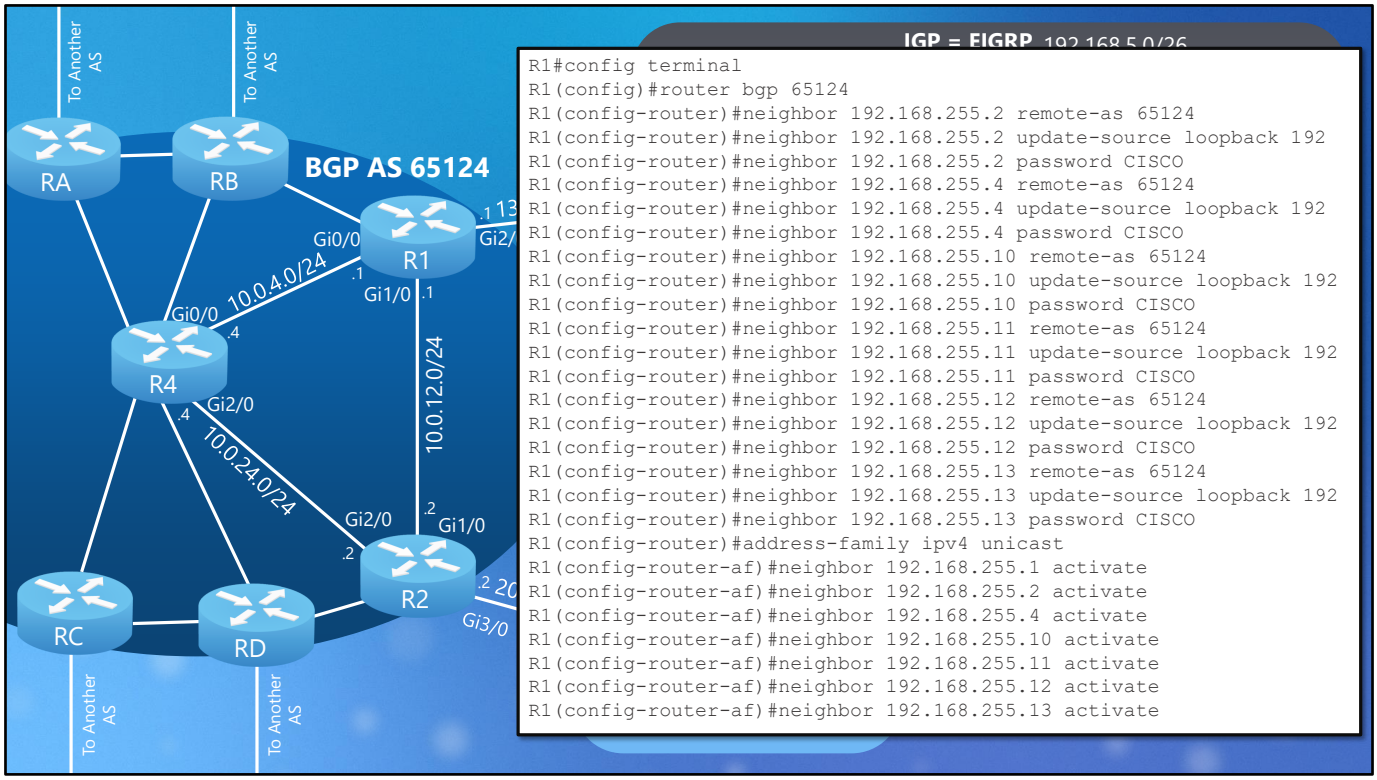


So if R1 and R4 are neighbors…. And R4 and RD are neighbors…. R1 will teach R4 about 192.168.5.0/26 as an example but R4 will not teach RD about it.

What does this mean???? You need to form neighborships with everyone you want to exchange routes with.

So because there are multiple paths in AS 65124 you would configure everyone with a loopback address and form BGP neighbor adjacencies with these loopbacks and make sure to up date source and noext hop self.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

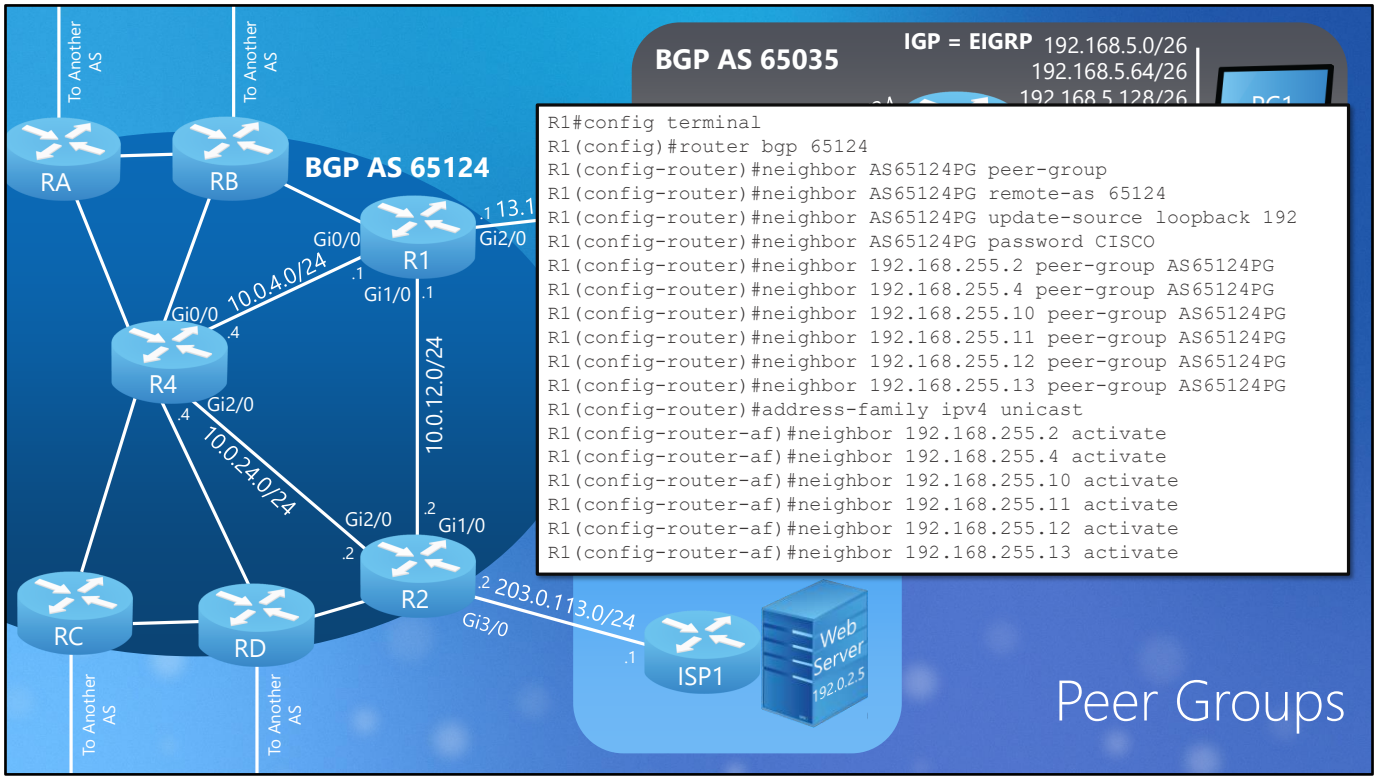


Here it is for the sake of time!!!!! ☺

This will be very hard to manage, and the config would be huge. So how can I manage the config better.

PEER GROUPS TO THE RESCUE

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



PEER GROUPS TO THE RESCUE

ADLIB!!!!
Think of it as a template

Although PGs make config a little easier….

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Although PGs make config a little easier….

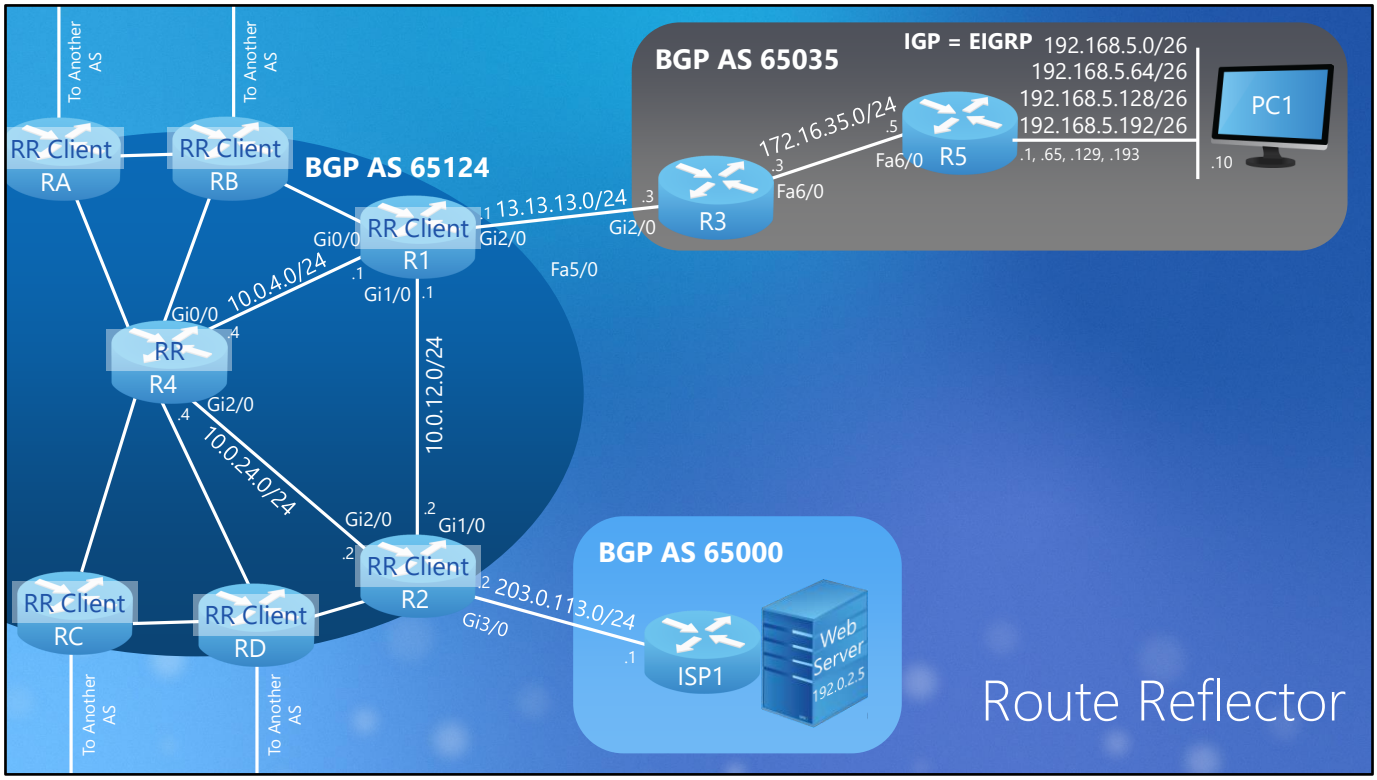
The inability of BGP to advertise a prefix learned from one iBGP peer to another iBGP peer can lead to scalability issues within an AS. The formula *n*(*n* [ms] 1)/2 provides the number of sessions required, where *n* represents the number of routers. A full mesh topology of 5 routers requires 10 sessions, and a topology of 10 routers requires 45 sessions. iBGP scalability becomes an issue for large networks.

In our case with 7 routers that is 21 sessions. YIKES!!!!

Although this helps… for greater scalability we need…

ROUTE REFLECTORS TO THE RESCUE

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



RFC 1966 introduces the idea that an iBGP peering can be configured so that it reflects routes to another iBGP peer. The router that is reflecting routes is known as a *route reflector* (*RR*), and the router that is receiving reflected routes is a *route reflector client*. Route reflectors and route reflection involve three basic rules:

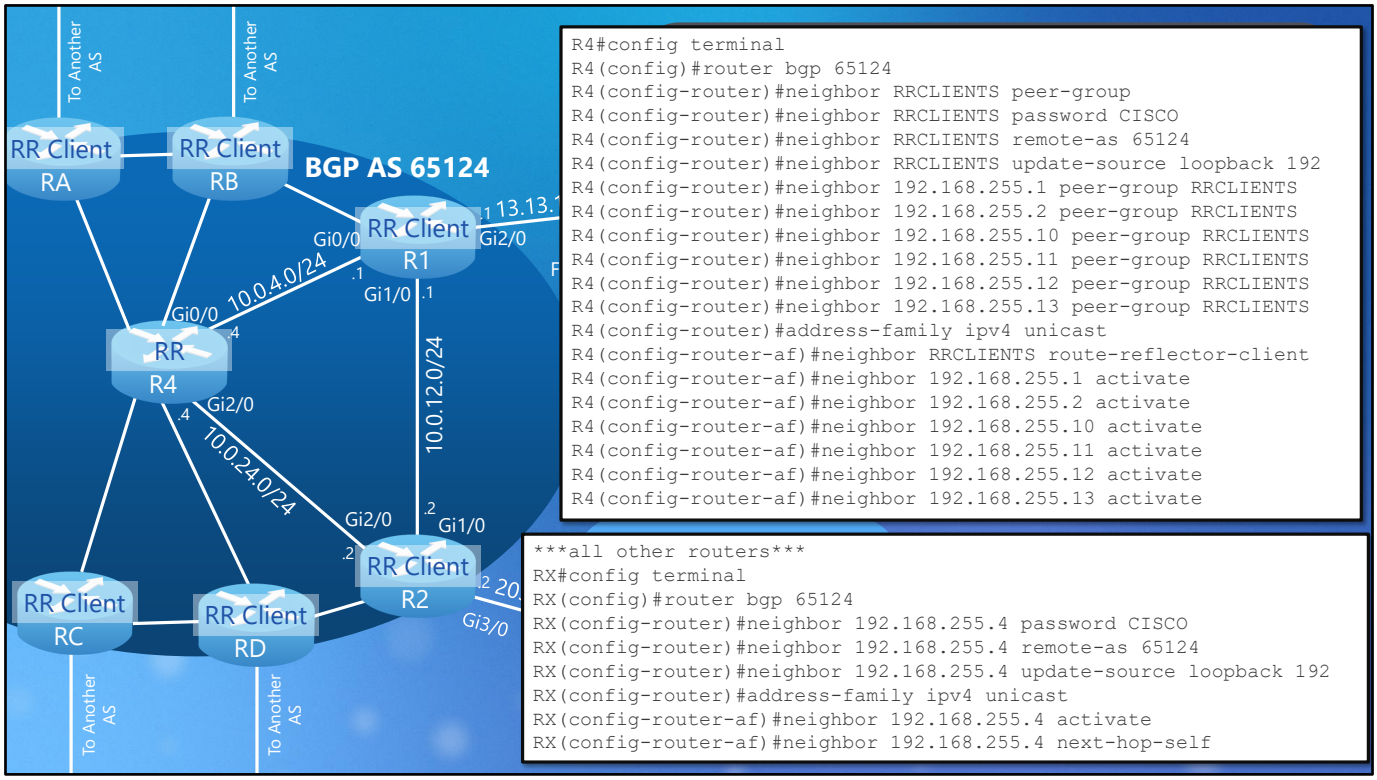
[lb] **Rule 1:** If an RR receives an NLRI from a non-RR client, the RR advertises the NLRI to an RR client. It does not advertise the NLRI to a non-RR client.

[lb] **Rule 2:** If an RR receives an NLRI from an RR client, it advertises the NLRI to RR clients and non-RR clients. Even the RR client that sent the advertisement receives a copy of the route, but it discards the NLRI because it sees itself as the route originator.

[lb] **Rule 3:** If an RR receives a route from an eBGP peer, it advertises the route to RR clients and non-RR clients.

So if we all form neighborships using loopbacks with the RR we can reach it using any path and then we can share routes with it and let the other routers learn from it.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



RFC 1966 introduces the idea that an iBGP peering can be configured so that it reflects routes to another iBGP peer. The router that is reflecting routes is known as a *route reflector* (*RR*), and the router that is receiving reflected routes is a *route reflector client*. Route reflectors and route reflection involve three basic rules:

[lb] **Rule 1:** If an RR receives an NLRI from a non-RR client, the RR advertises the NLRI to an RR client. It does not advertise the NLRI to a non-RR client.

[lb] **Rule 2:** If an RR receives an NLRI from an RR client, it advertises the NLRI to RR clients and non-RR clients. Even the RR client that sent the advertisement receives a copy of the route, but it discards the NLRI because it sees itself as the route originator.

[lb] **Rule 3:** If an RR receives a route from an eBGP peer, it advertises the route to RR clients and non-RR clients.

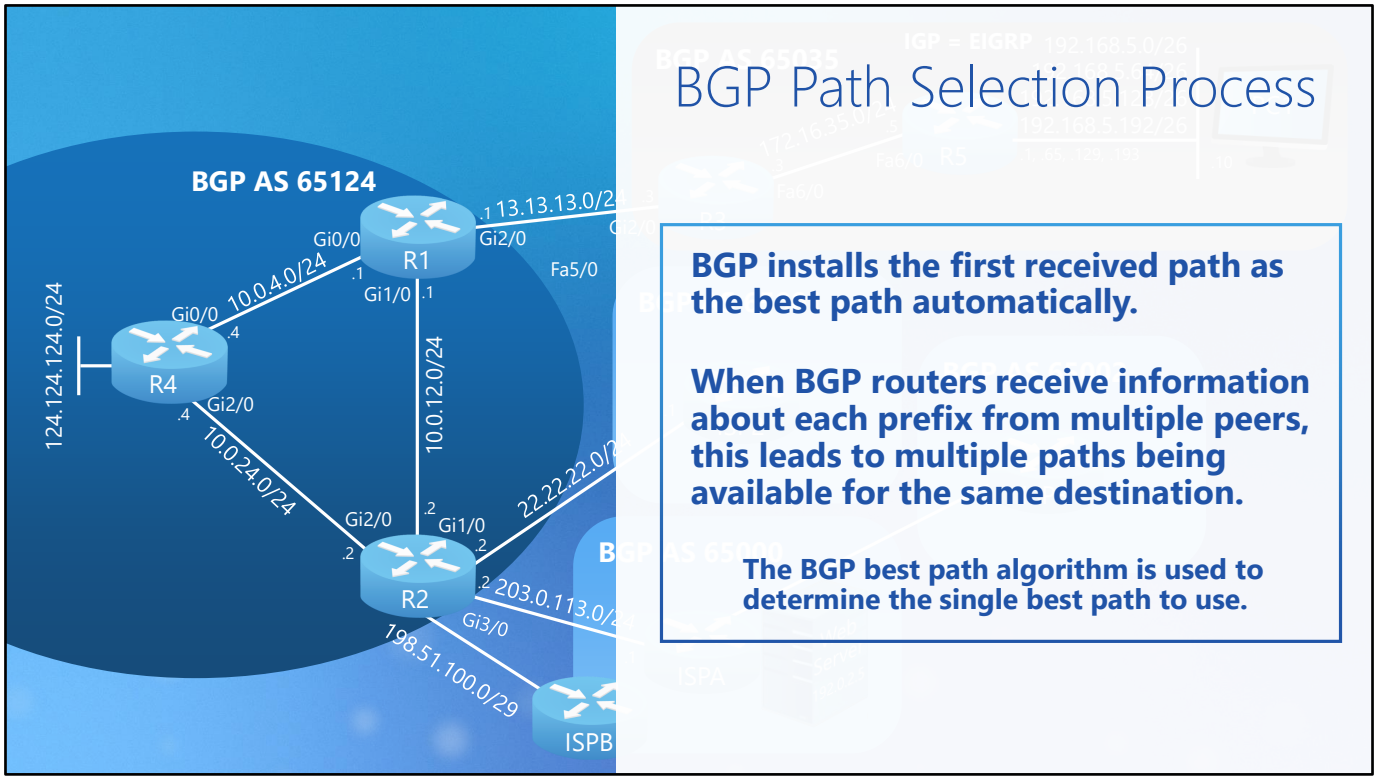
So if we all form neighborships using loopbacks with the RR we can reach it using any path and then we can share routes with it and let the other routers learn from it.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



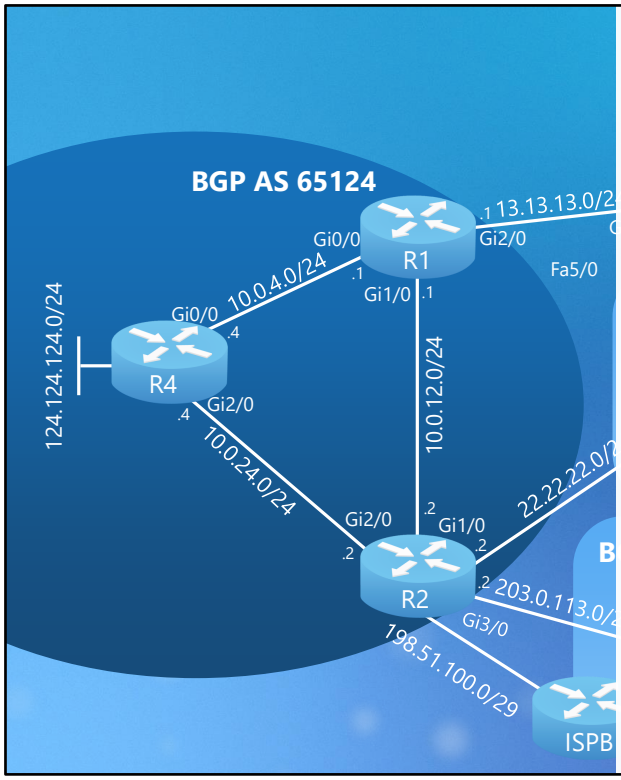
Title slide

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/13753-25.html

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



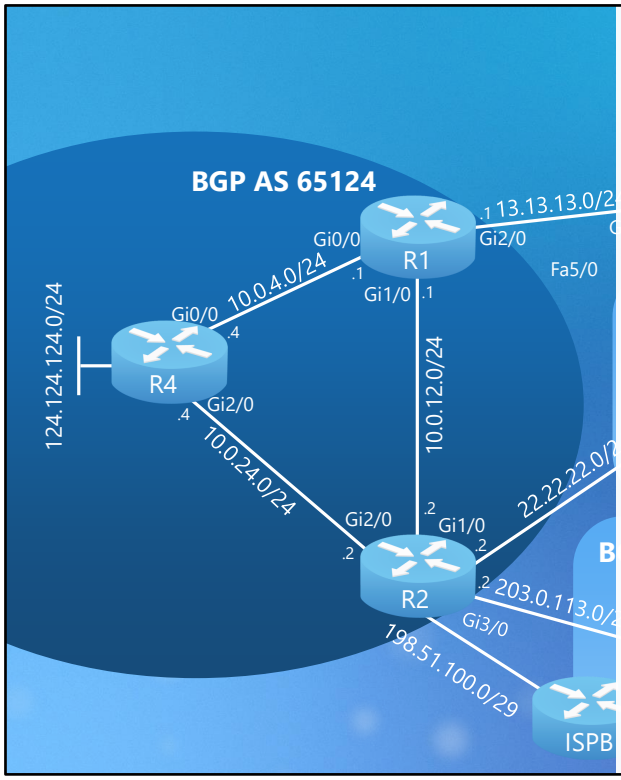
Cisco BGP Path Selection Process

1. Ignore paths that
   1. Have a next hop IP address not reachable
   2. Have a path that contains own local AS number
2. Prefer the path with the highest **WEIGHT**.
3. Prefer the path with the highest **LOCAL_PREF**.
4. Prefer the path what was locally **ORIGINATED**.
5. Prefer the path with the shortest **AS_PATH**.
6. Prefer the path with the lowest **Multi-exit discriminator** (MED)
7. Prefer eBGP over iBGP paths.
8. Prefer the path with the lowest IGP metric to the BGP next hop.

https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/13753-25.html

show ip bgp 1.0.0.0/24 | i from|weight
show ip bgp 1.0.0.0/24 | i from|localpref
show ip bgp 1.0.0.0/24 | i from|0.0.0.0
show ip bgp 1.0.0.0/24 | i from|13335
show ip bgp 1.0.0.0/24 | i from|Origin
show ip bgp 1.0.0.0/24 | i from|metric
show ip bgp 1.0.0.0/24 | i from|external|internal
8 really only applicable if #7 is iBGP and tied.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



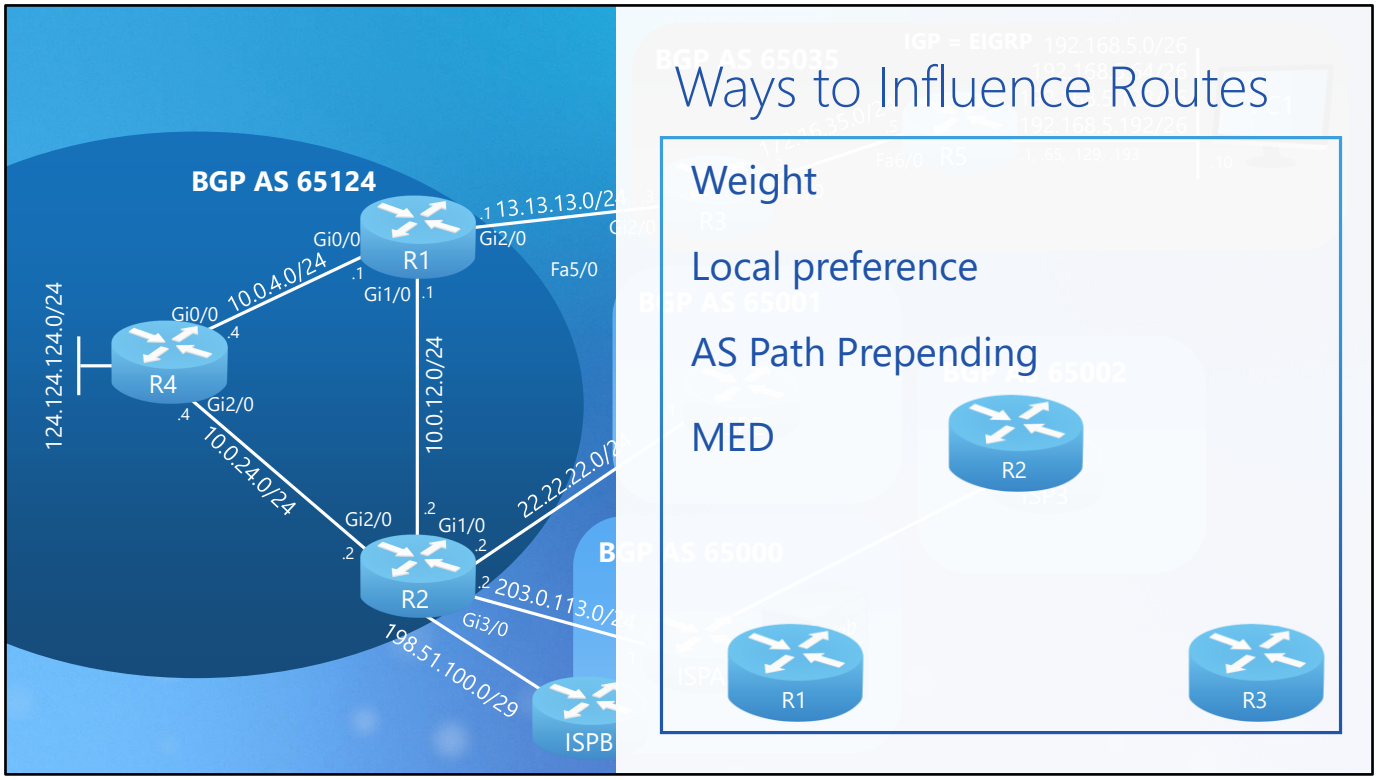
Cisco BGP Path Selection Process

9. Prefer the older path.
10. Prefer the path with the peering router that has the lower router ID.
11. Prefer the path with the peer who has the lower neighbor address.

https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/13753-25.html

show ip bgp 1.0.0.0/24 | i from|weight
show ip bgp 1.0.0.0/24 | i from|localpref
show ip bgp 1.0.0.0/24 | i from|0.0.0.0
show ip bgp 1.0.0.0/24 | i from|13335
show ip bgp 1.0.0.0/24 | i from|Origin
show ip bgp 1.0.0.0/24 | i from|metric
show ip bgp 1.0.0.0/24 | i from|external|internal
8 really only applicable if #7 is iBGP and tied.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Weight

Weight – Cisco Proprietary / Locally significant to the router

- Use it to influence path leaving AS when a router has dual connections
- Higher is better (default for learned is 0, for locally generated 32768)
- Can't be passed to a neighboring BGP router

Configured with a Route Map:

```
ip prefix-list PL_WEIGHT seq 5 permit 192.0.2.0/24
route-map WEIGHT permit 10
 match ip address prefix-list PL_WEIGHT
 set weight 70
route-map WEIGHT permit 20
router bgp 65124
 neighbor 22.22.22.1 route-map WEIGHT in
```

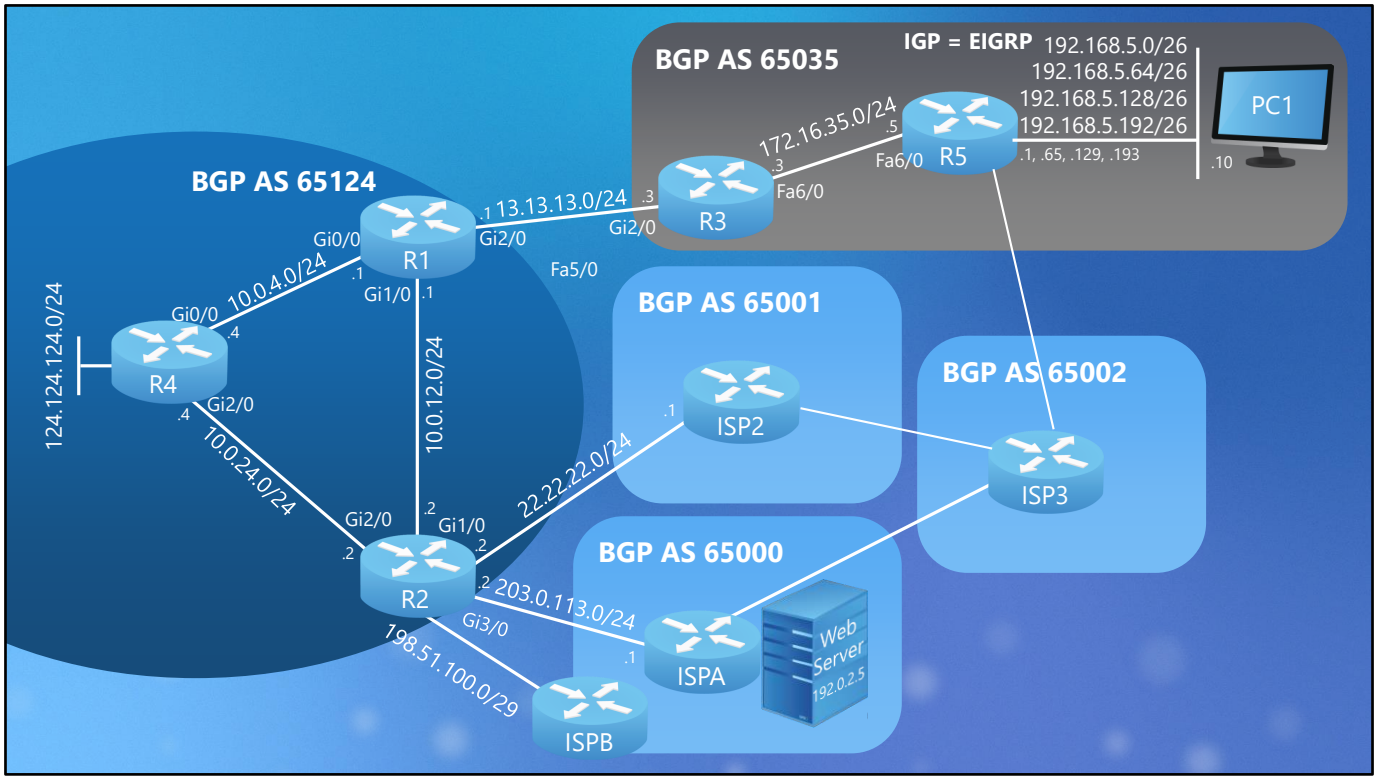
Clearing a route to refresh new attributes:

```
clear ip bgp * in
```

Configured without Route Map:

```
router bgp 65124
 neighbor 203.0.113.1 weight 40 in
```

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



1) Neighbor 203.0.113.1 weight 40 (r2 to isp1a)
2) Neighbor 22.22.22.1 route-map WEIGHT in (r2 to isp2)

```
ip prefix-list PL_WEIGHT seq 5 permit 192.0.2.0/24

route-map WEIGHT permit 10
 match ip address prefix-list 192.0.2.0
 set weight 70
route-map WEIGHT permit 20
```

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Local Preference

Local Preference – Passed to other routers in an AS

- Use it to influence path leaving AS when multiple AS peering's exist.
- Force routers inside an AS to prefer one ISP over another.
- Default value is 100 and higher is better.
- Can be set as eBGP routes are learned.

Configured with a Route Map:

```
ip prefix-list PL_LP seq 5 permit 192.0.2.0/24
route-map LOCAL_PREF permit 10
 match ip address prefix-list PL_LP
 set local-preference 171
route-map LOCAL_PREF permit 20
router bgp 65124
 neighbor 22.22.22.1 route-map LOCAL_PREF in
```

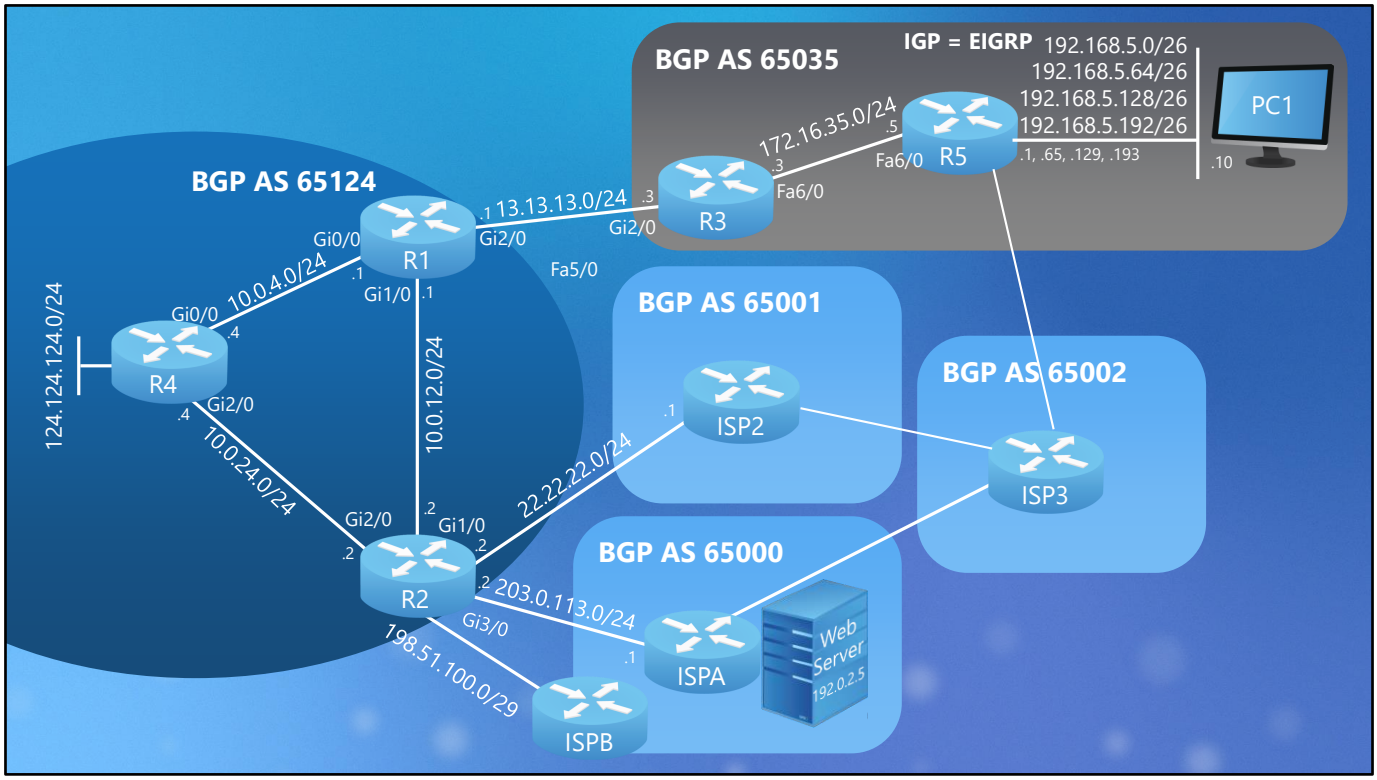
Clearing a route to refresh new attributes:

```
clear ip bgp * in
```

Set local pref of all routes advertised to iBGP peers:

```
router bgp 65124
 bgp default local-preference 150
```

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.




```
router bgp 65124
 bgp default local-preference 150
```

```
ip prefix-list PL_LP seq 5 permit 192.0.2.0/24
route-map LOCAL_PREF permit 10
 match ip address prefix-list PL_LP
 set local-preference 171
route-map LOCAL_PREF permit 20
router bgp 65124
 neighbor 22.22.22.1 route-map LOCAL_PREF in
```

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

AS Path Prepend

AS Path Prepend – Passed to other routers in other AS

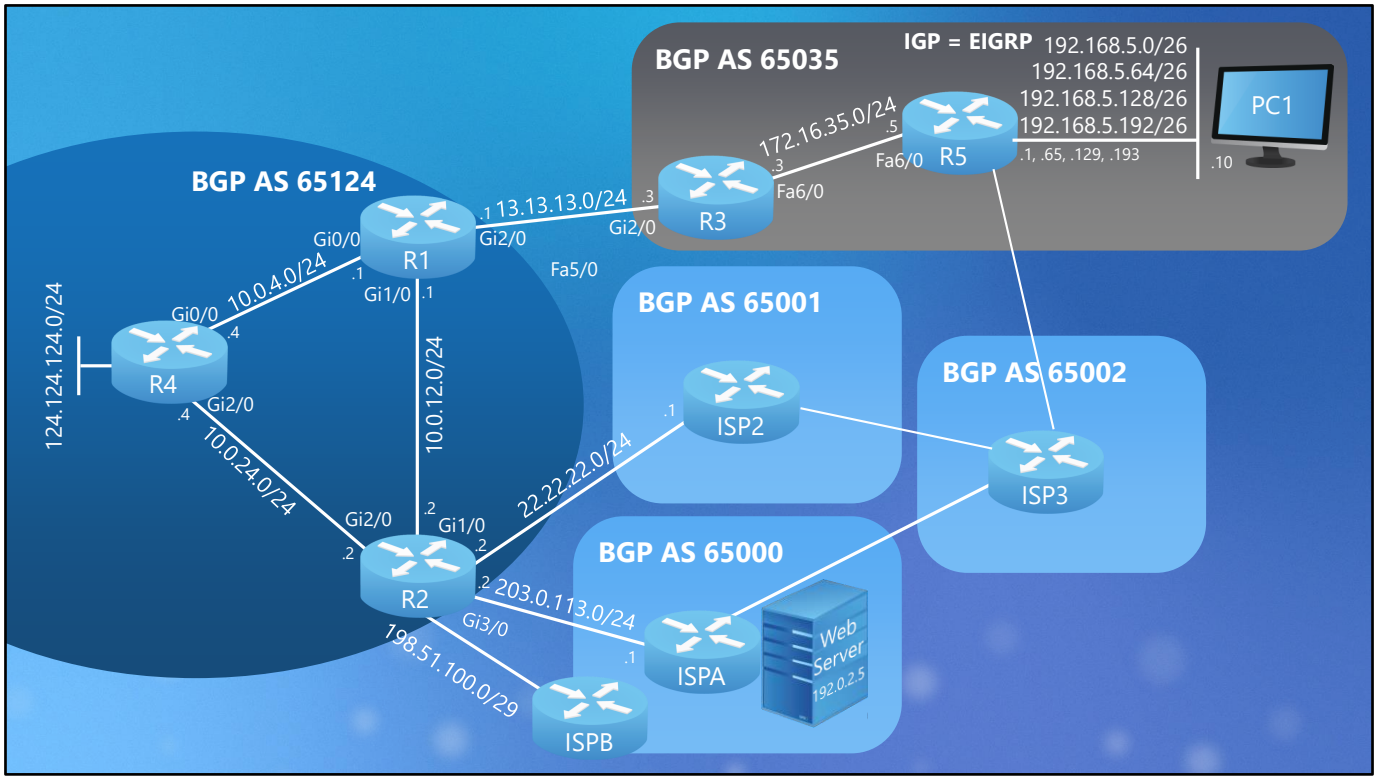
Use it to influence path to your AS when multiple AS peering's exist.

Manually configured to make return path less preferred by adding "additional hops"

Configured with a Route Map:

```
ip prefix-list PL_ASPATH seq 5 permit 124.124.124.0/24
route-map ASPATH permit 10
 match ip address prefix-list PL_ASPATH
 set as-path prepend 65124 65124 65124 65124 65124
route-map ASPATH permit 20
router bgp
 neighbor 198.51.100.1 route-map AS_PATH out
 neighbor 203.0.113.1 route-map AS_PATH out
```

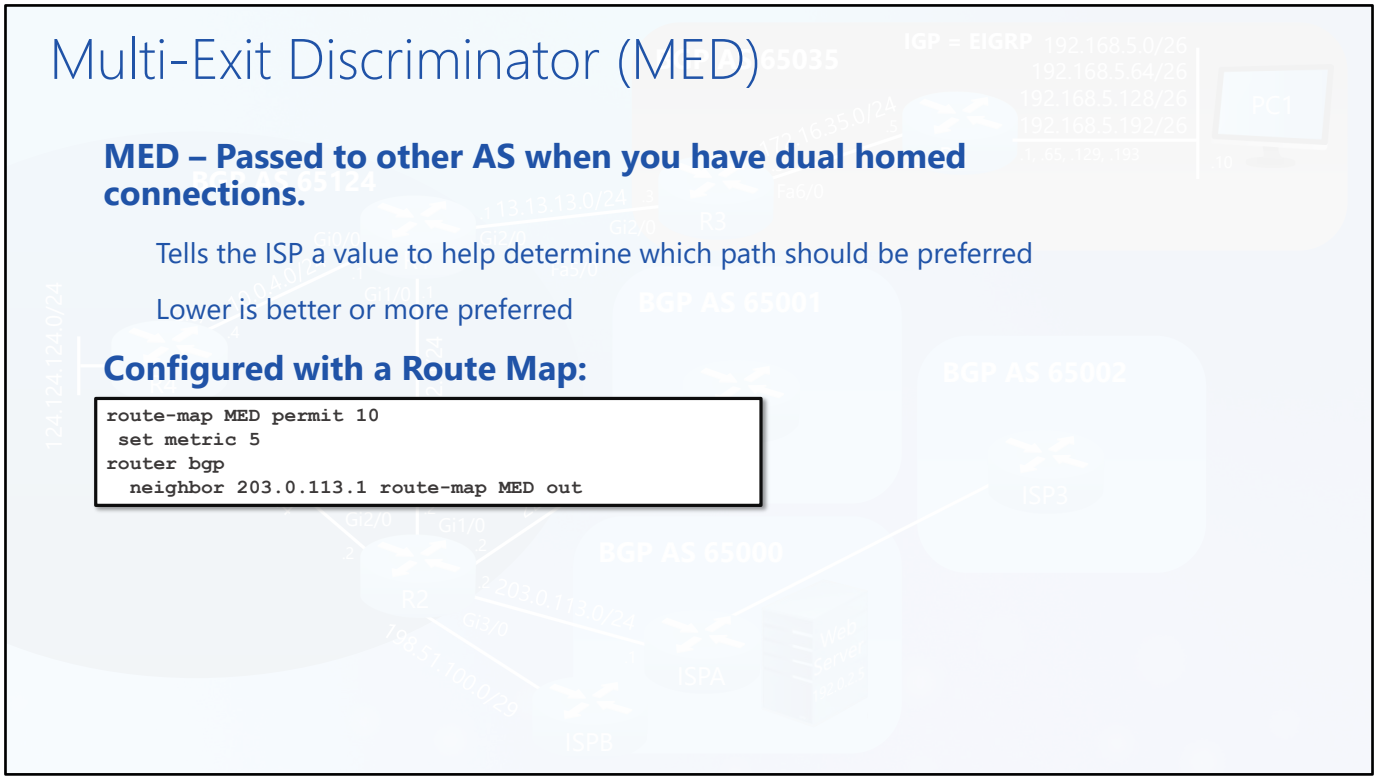
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.




```
ip prefix-list PL_ASPATH seq 5 permit 124.124.124.0/24
route-map ASPATH permit 10
 match ip address prefix-list PL_ASPATH
 set as-path prepend 65124 65124 65124 65124 65124
route-map ASPATH permit 20
router bgp
 neighbor 198.51.100.1 route-map AS_PATH out
 neighbor 203.0.113.1 route-map AS_PATH out
neighbor 22.22.22.1 route-map AS_PATH out
```

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Multi-Exit Discriminator (MED)



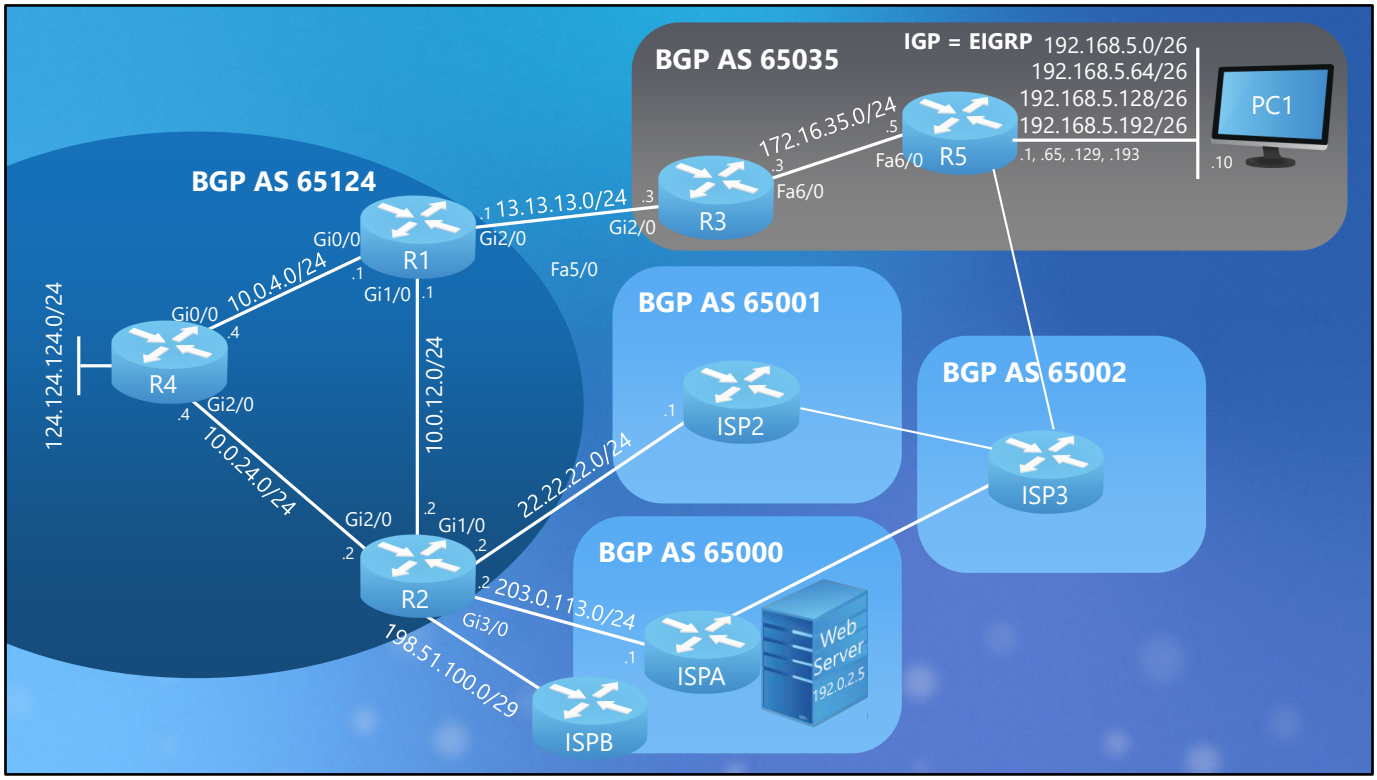
MED – Passed to other AS when you have dual homed connections.

- Tells the ISP a value to help determine which path should be preferred
- Lower is better or more preferred

Configured with a Route Map:

```
route-map MED permit 10
 set metric 5
router bgp
  neighbor 203.0.113.1 route-map MED out
```

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



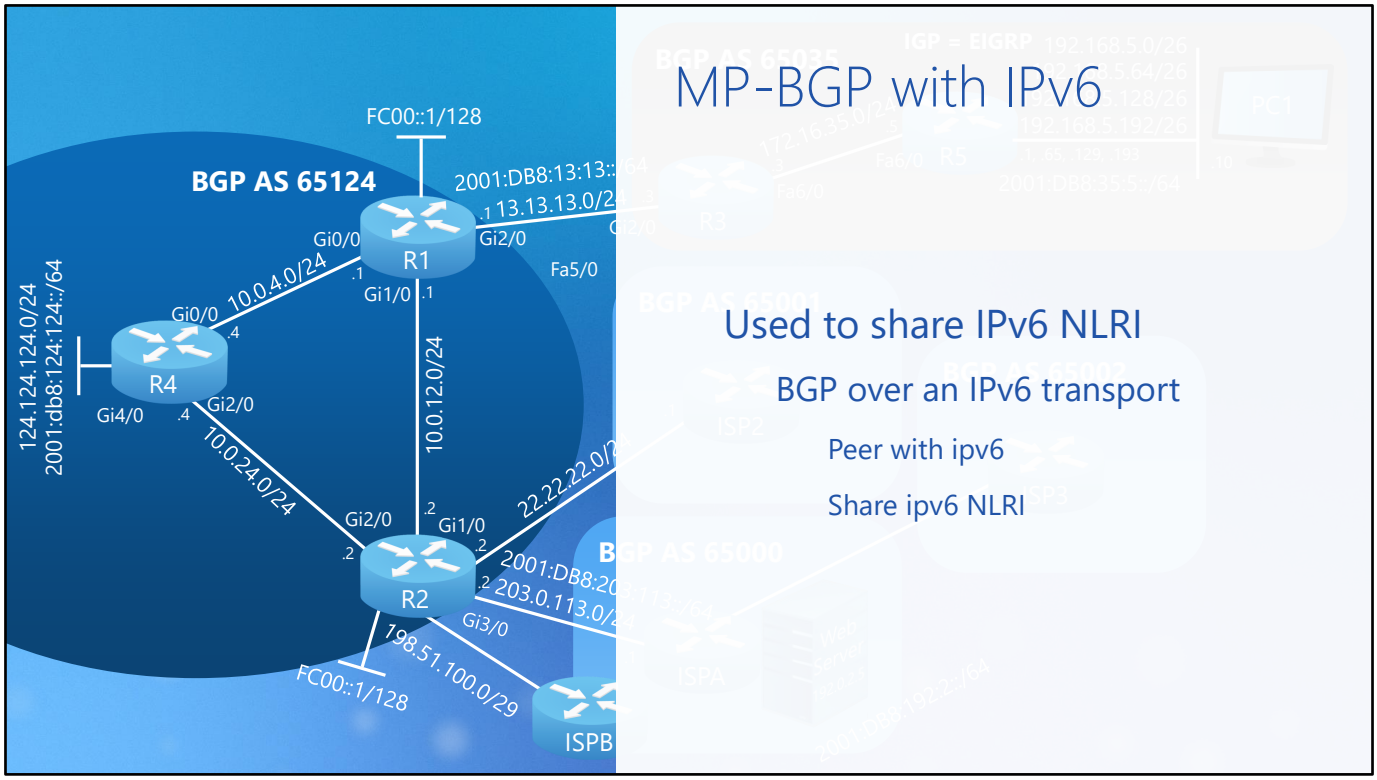

```
route-map MED permit 10
 set metric 5
router bgp
  neighbor 203.0.113.1 route-map MED out
```

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Title slide

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



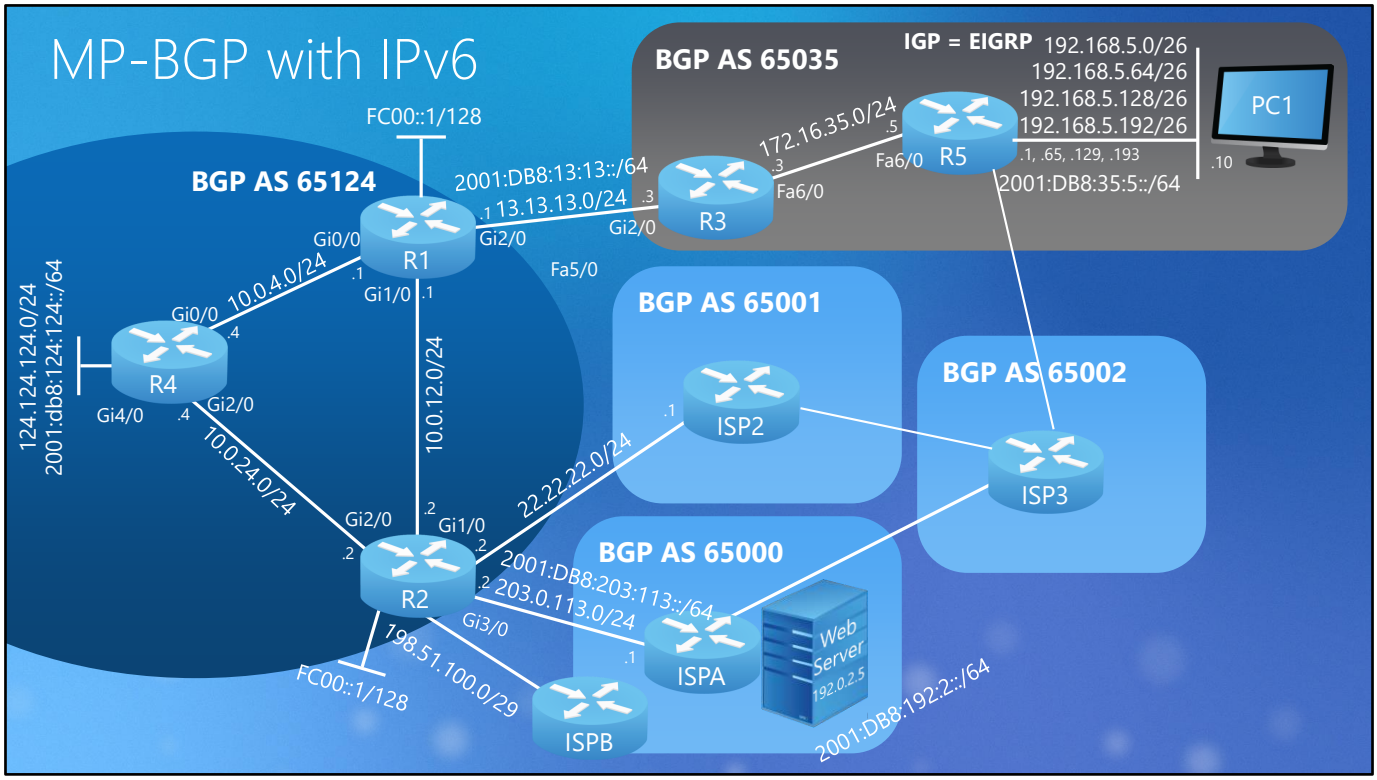
What we just did was:

BGP over an IPv4 transport

Peer with ipv4

Share IPv4 NLRI

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



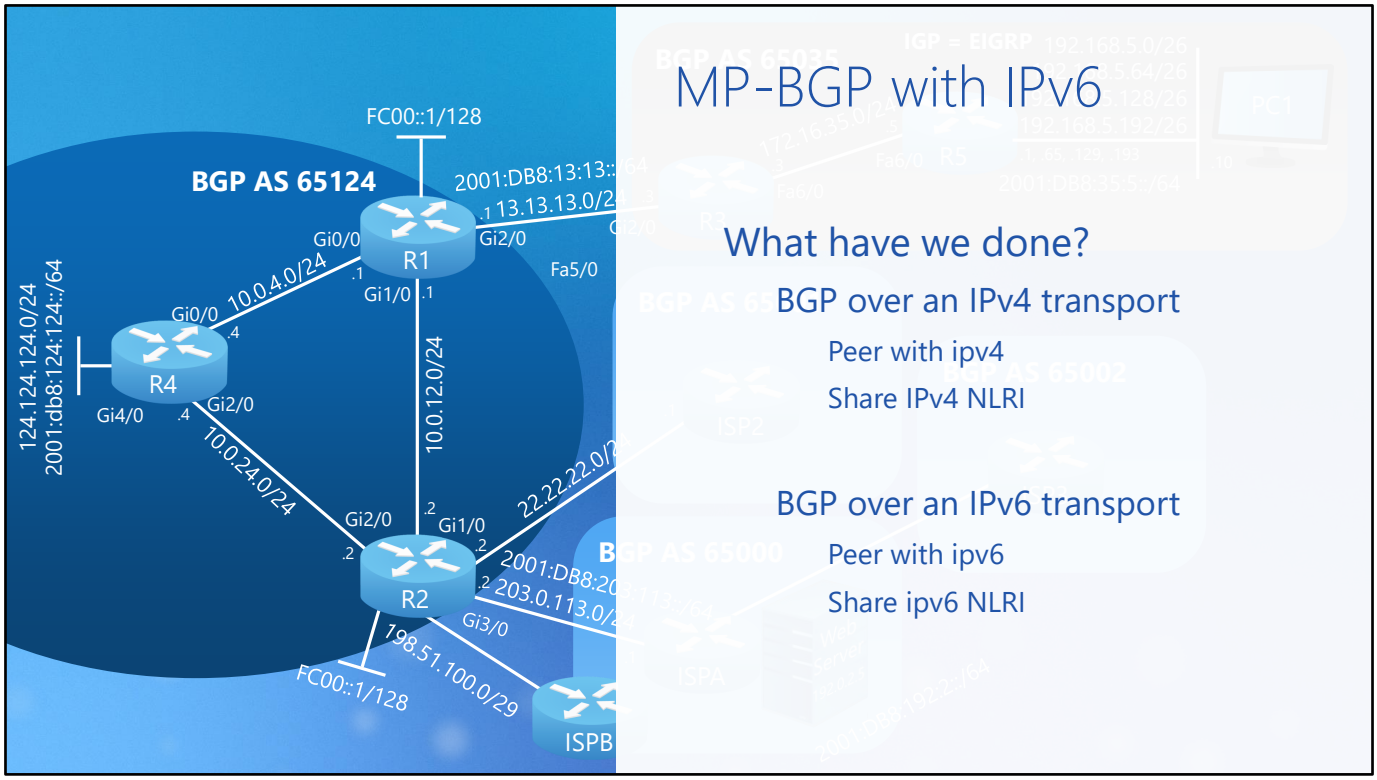
Demo config for BGP IPv6

This create multiple BGP sessions. One for IPv4 one for IPv6. We are using two “control planes”

If this is what needs to be done fine….

But you can use one session for both.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

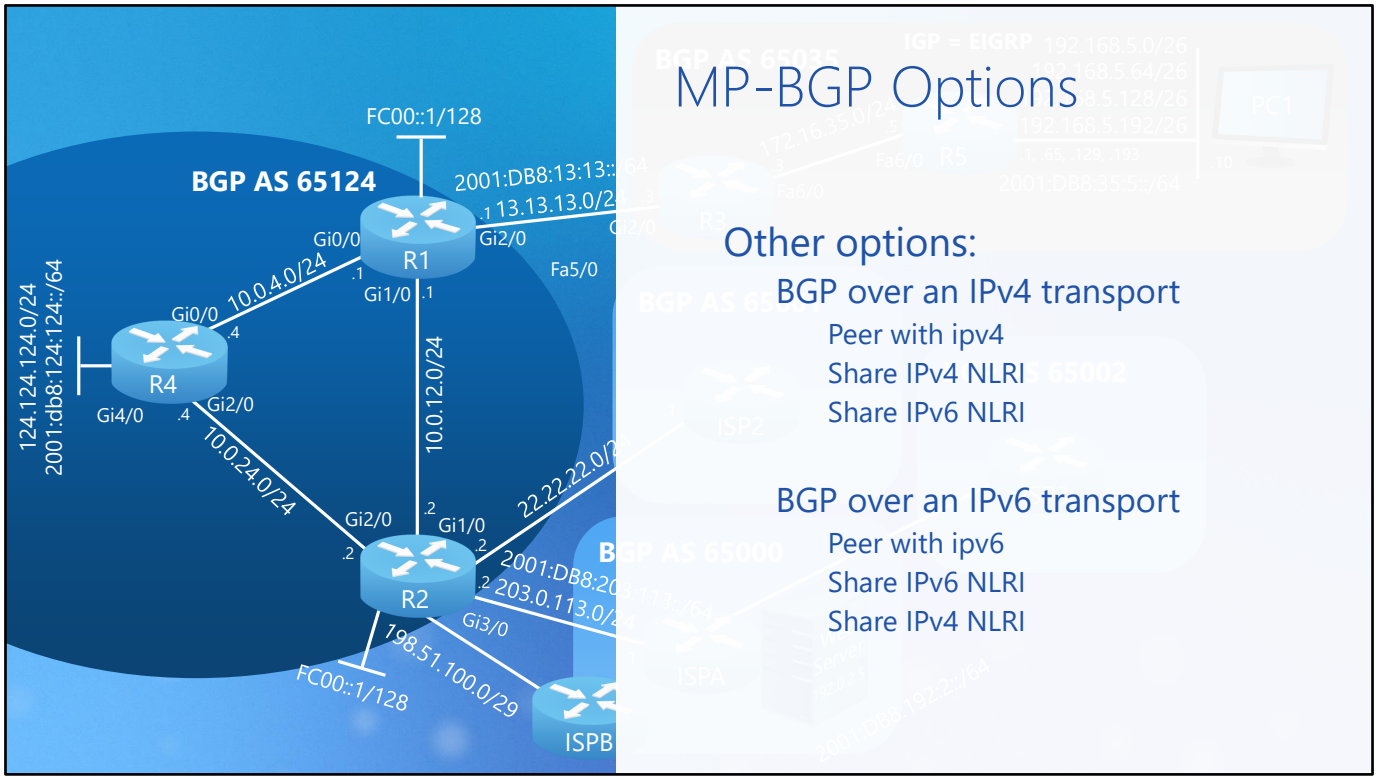


This create multiple BGP sessions. One for IPv4 one for IPv6. We are using two "control planes"

If this is what needs to be done fine….

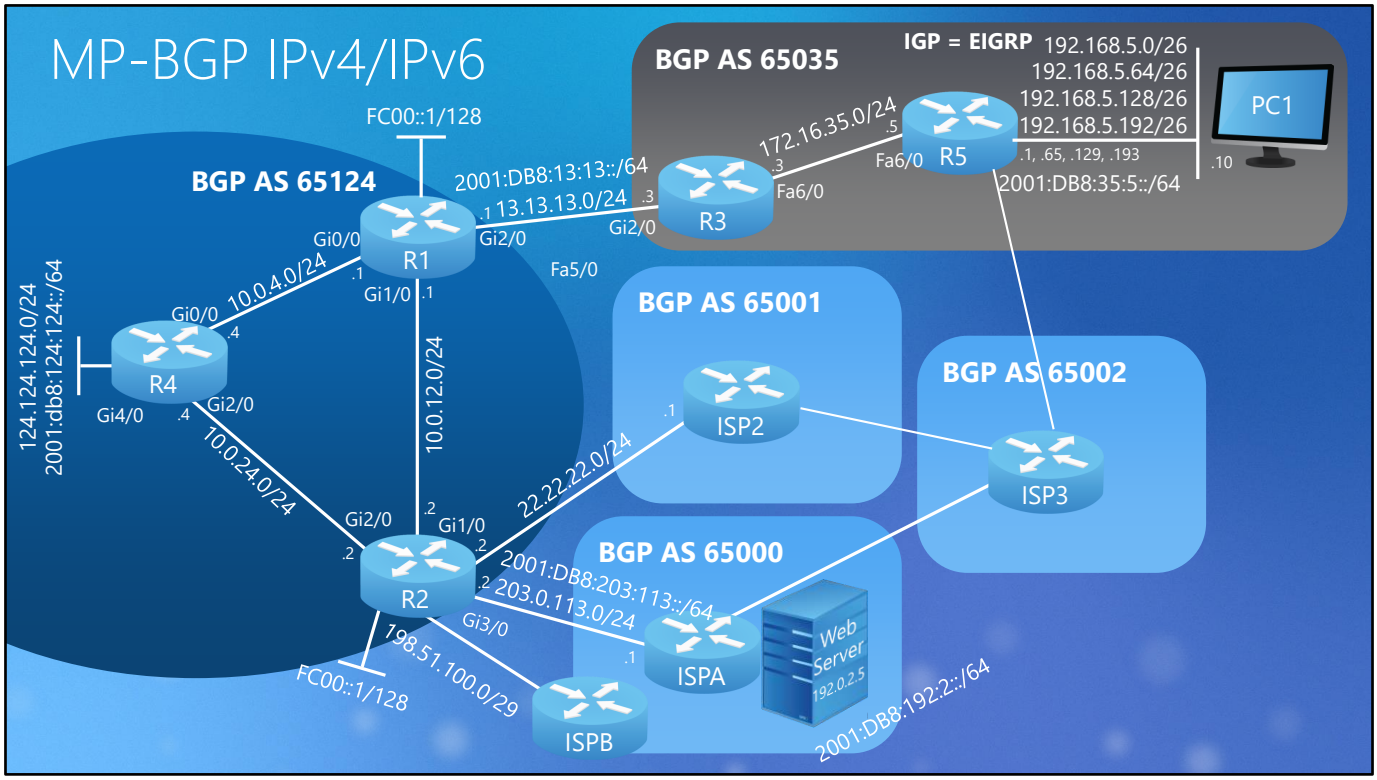
But you can use one session for both.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



One control plane to rule them all.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Demo:

BGP over an IPv4 transport

- **Peer with ipv4**
- **Share IPv4 NLRI**
- **Share IPv6 NLRI**

Remove bgp config on R1 and R3.

Peer R1 and R3

- Router bgp #
- Neighbor 13.13.13.x remote-as X
- Address family ipv4 neighbor activate

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Network x.x.x.x mask x.x.x.x
Address family ipv6 neighbor activate
Network X:X:X:X::/64

Show bgp ipv4 unicast is fine
Show bgp ipv6 unicast is not fine
Learned addresses are not being installed in the routing table because of next hop (it is an IPv4 encoded address). (must fix this)
no bgp default ipv6-nexthop to affect outbound updates (do this on R1 to fix R3 do this on R3 to fix R1) (NOTE: this affects all peers)
Use a route map (do this on R1 to fix R3) (note: this affects only the peer you want it to.)
Route-map FIXNH
Set ipv6 next-hop 2001:db8:13:13::1
Router bgp 65124
Address family ipv6 unicast
Neighbor 13.13.13.3 route-map FIX_IPV6_NH out

Peer R1 and R2
Router bgp 65124

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Neighbor 192.168.255.x remote-as 65124
Neighbor 192.168.255.x update-source loop 192
Address family ipv4 neighbor activate
neighbor 192.168.255.x next-hop-self
Address family ipv6 neighbor activate
Neighbor 192.168.255.x nex-hop-self

GRRRR look at the next hop in **show bgp ipv6 unicast** (have to fix with **route map** or **no bgp default ipv6-nexthop)**

Demo:
BGP over an IPv6 transport
Peer with ipv6
Share IPv6 NLRI
Share IPv4 NLRI

Peer R1 and R3
R1:
router bgp 65124
neighbor 2001:DB8:13:13::3 remote-as

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

65035
 address-family ipv4
  network 124.124.124.0 mask
255.255.255.0
  neighbor 2001:DB8:13:13::3 activate
 address-family ipv6
  network 2001:DB8:124:124::/64
  neighbor 2001:DB8:13:13::3 activate

R3:

router bgp 65035
 neighbor 2001:DB8:13:13::1 remote-as
65124
 address-family ipv4
  network 192.168.5.0 mask
255.255.255.192
  neighbor 2001:DB8:13:13::1 activate
 address-family ipv6
  network 2001:DB8:35:5::/64
  neighbor 2001:DB8:13:13::1 activate

Show bgp ipv6 unicat (everything great)
Show bgp ipv4 unicast (GRRRRR next hop)
(have to fix with route map)

route-map FIXIPV4NH permit 10

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

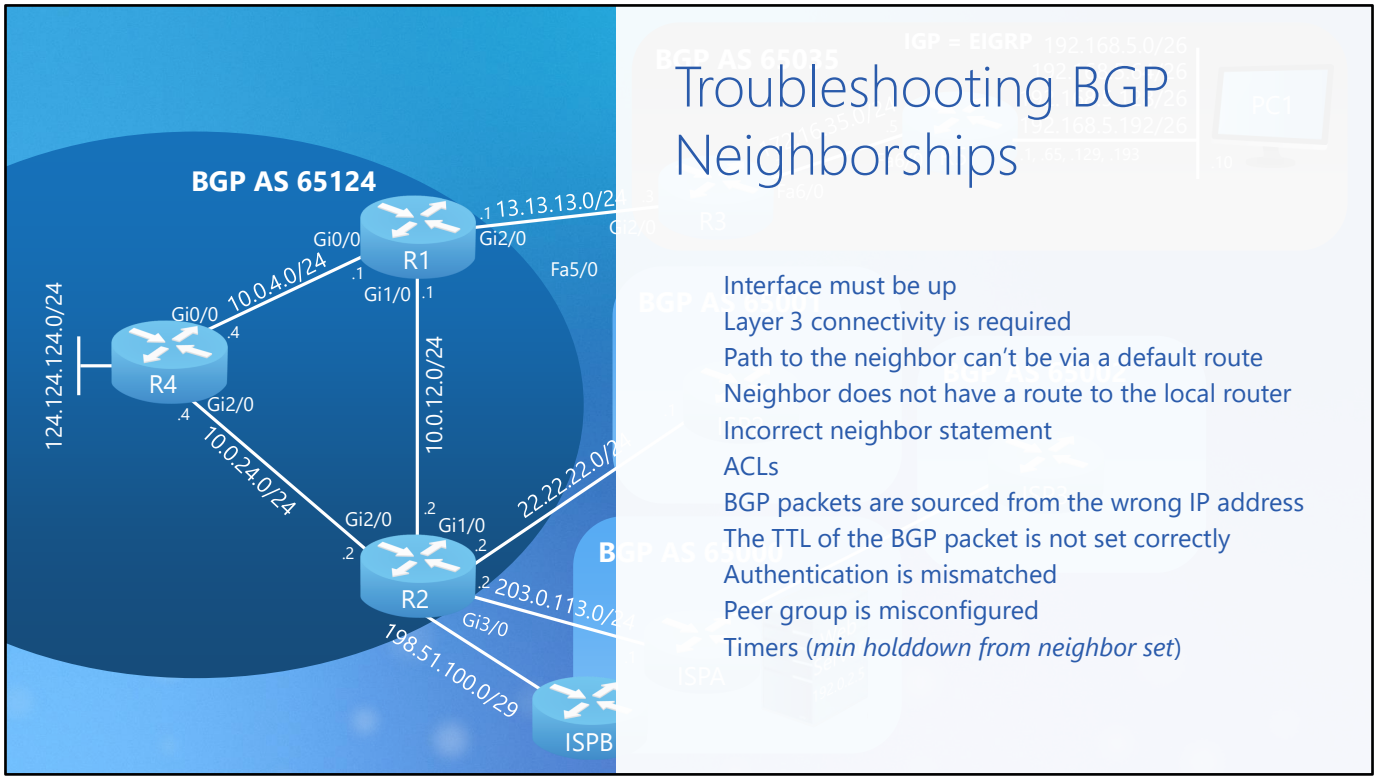
```
set ip next-hop 13.13.13.1
*Dec  9 11:58:29.779: % Warning: Next hop
address is our address
router bgp 65124
address-family ipv4 unicast
neighbor 2001:DB8:13:13::3 route-map
FIXIPV4NH out
do clear bgp ipv4 uni * out
```

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



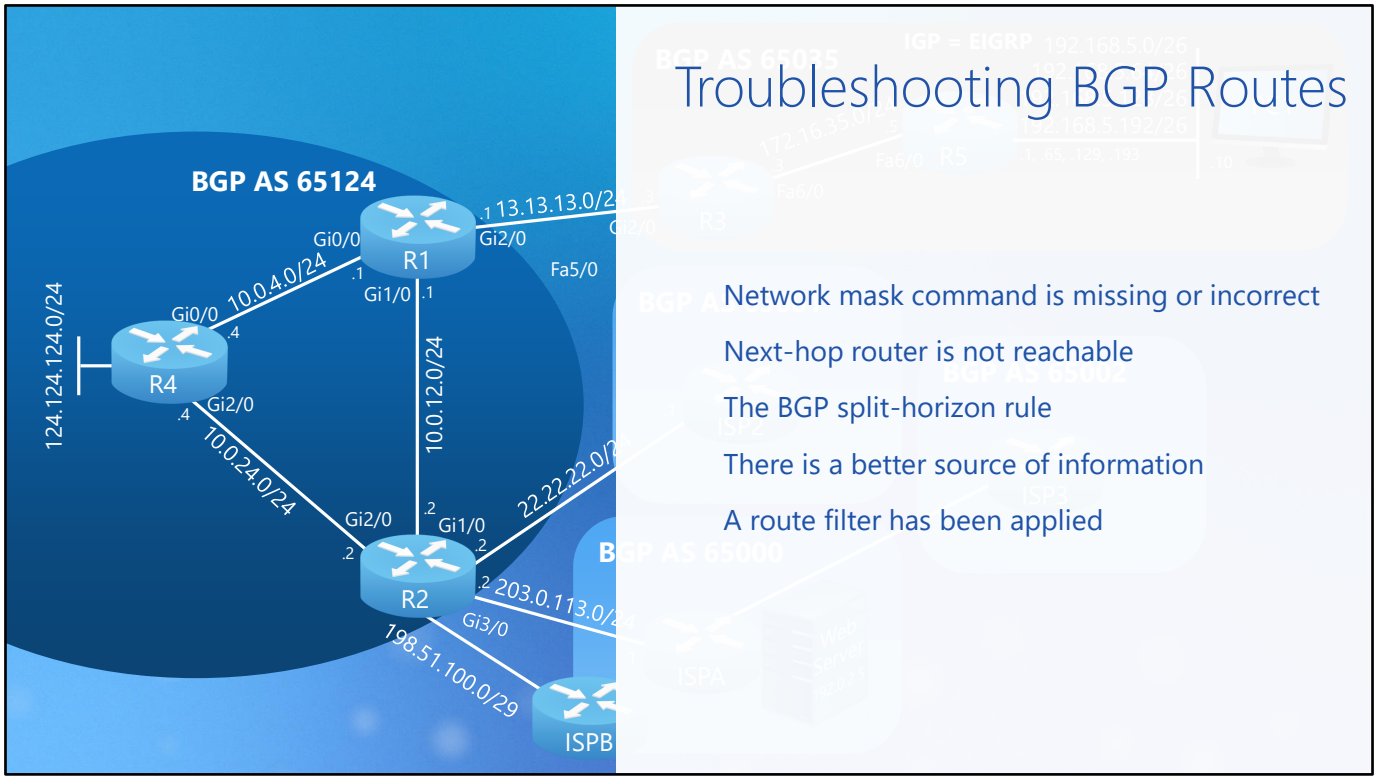
Title slide

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



- [lb] Interface is down: The interface must be up/up.
- [lb] Layer 3 connectivity is broken: You need to be able to reach the IP address you are trying to form the adjacency with.
- [lb] Path to the neighbor is through the default route: You must be able to reach the neighbor using a route other than the default route.
- [lb] Neighbor does not have a route to the local router: The two routers forming a BGP peering must have routes to each other.
- [lb] Incorrect neighbor statement: The IP address and ASN in the neighbor ip_address remote-as as_number statement must be accurate.
- [lb] ACLs: An access control list (ACL) or a firewall may be blocking TCP (Transmission Control Protocol) port 179.
- [lb] BGP packets sourced from the wrong IP address: The source IP (Internet Protocol) address of an inbound BGP packet must match the local neighbor statement.
- [lb] The TTL (time-to-live) of the BGP packet expires: The peer may be further away than is permitted
- [lb] Mismatched authentication: The two routers must agree on the authentication parameters.
- [lb] Misconfigured peer group: Peer groups simplify repetitive BGP configurations; however, if not carefully implemented, they can prevent neighbor relationships from forming or routes from being learned.
- [lb] Timers: Timers do not have to match; however, if the minimum holddown from neighbor option is set, it could prevent a neighbor adjacency.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



[lb] **Missing or bad network mask command:** An accurate network command is needed to advertise routes.

[lb] **Next-hop router not reachable:** To use a BGP route, the next hop must be reachable.

[lb] **BGP split-horizon rule:** A router that learns BGP routes through an iBGP peering does not share those routes with another iBGP peer.

[lb] **Better source of information:** If exactly the same network is learned from a more reliable source, it is used instead of the BGP-learned information.

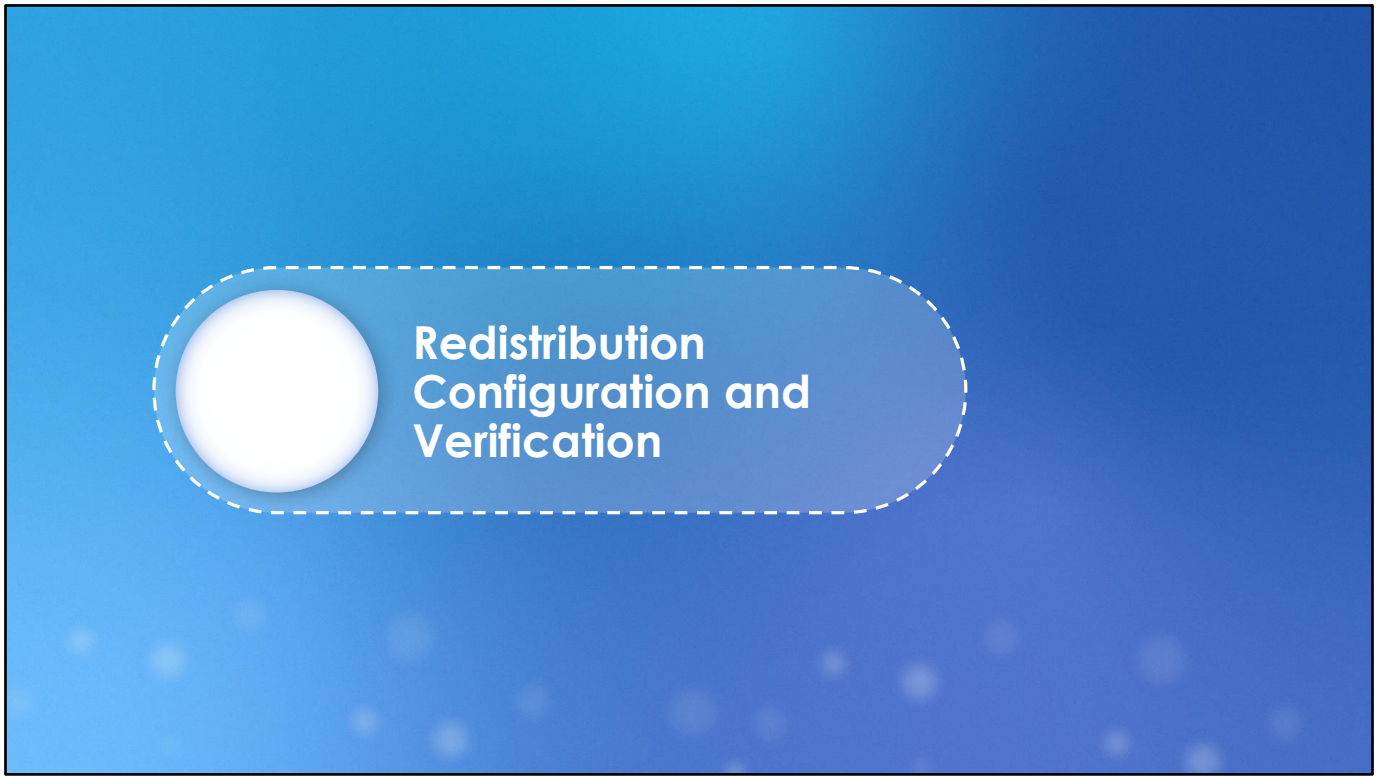
[lb] **Route filtering:** A filter might be preventing a route from being shared with neighbors or learned from neighbors.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



CLASSIC OSPFv3

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Title slide

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

What is Redistribution

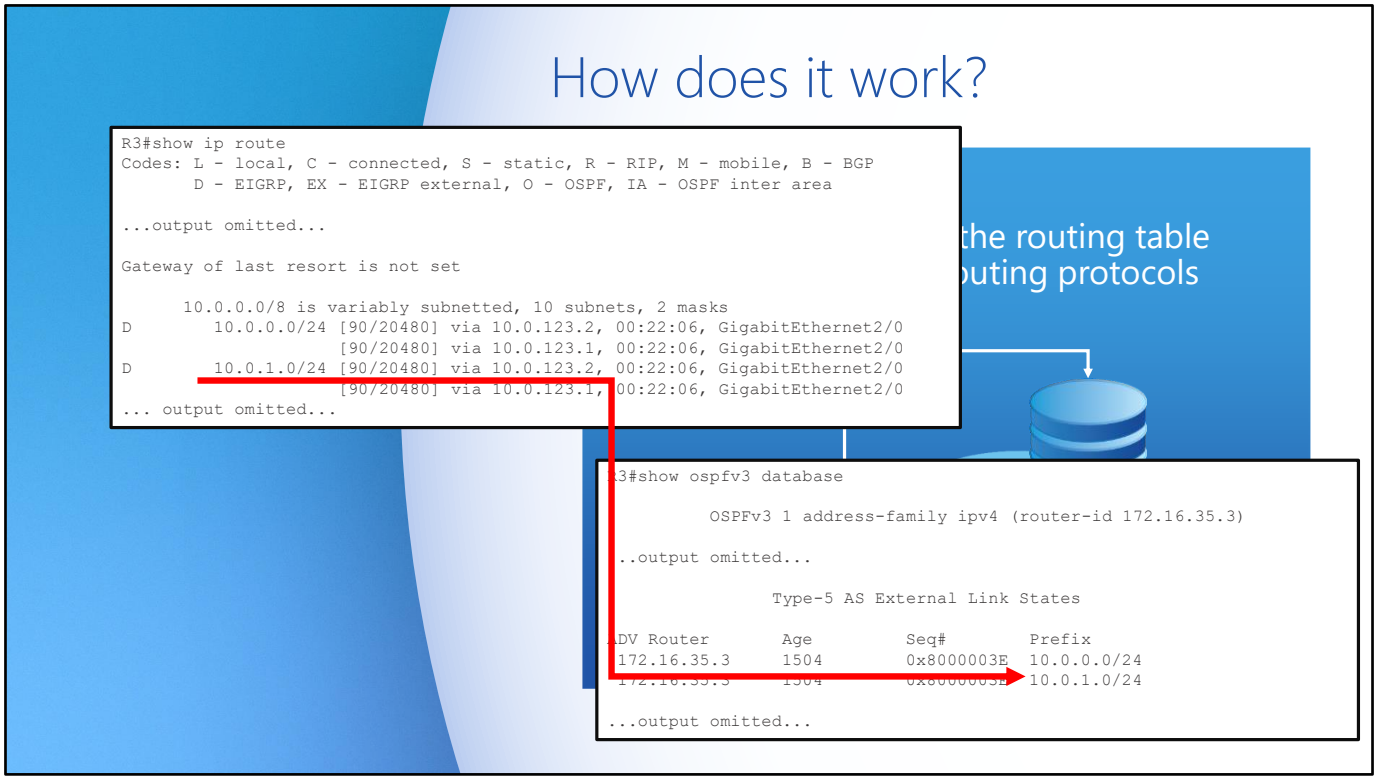
The exchange of routing information between two different sources.

Examples

- **OSPF into BGP**
- **BGP into OSPF**
- **EIGRP into OSPF**
- **OSPF into EIGRP**
- **Connected into OSPF**
- **Static into EIGRP**
- **…And more!**

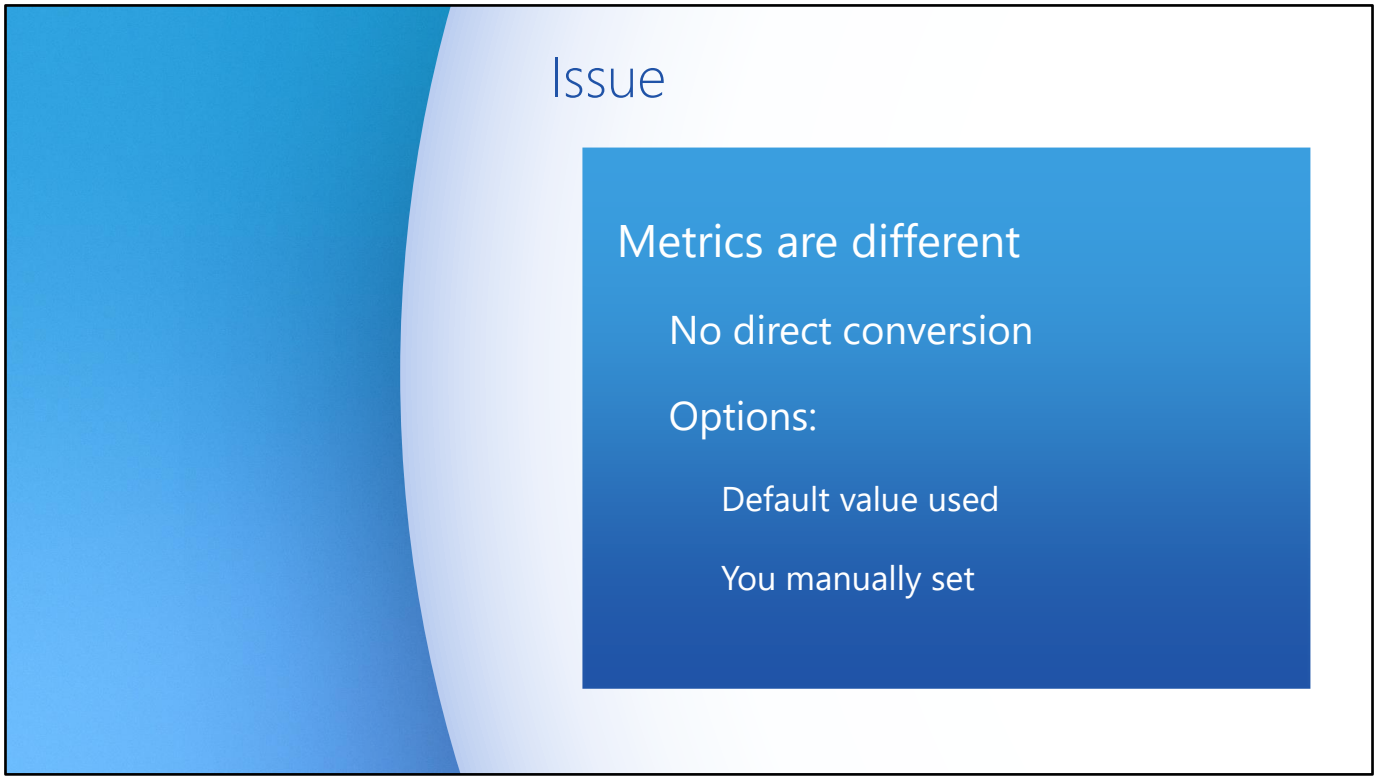
Can anyone think of why we might want to do redistribution?
Mergers with different IGP's, different divisions under different control, IGPs to BGP, MPLS

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



This means… .if the route is not in the routing table it can't be redistributed.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



OSPF COST
EIGRP FD
BGP ATTRIBUTES
RIP HOP COUNT

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Default Metrics

Anything redistributed into RIP/ EIGRP = Infinity

Anything* redistributed into OSPF = 20 (*BGP = 1)

Anything redistributed into BGP = IGP metric (MED)

NOTE:

OSPF to OSPF retains metric
EIGRP/connected/static to EIGRP retains metric

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Defining Metrics During Redistribution

1. Default Seed Metric
2. With the **default-metric** command

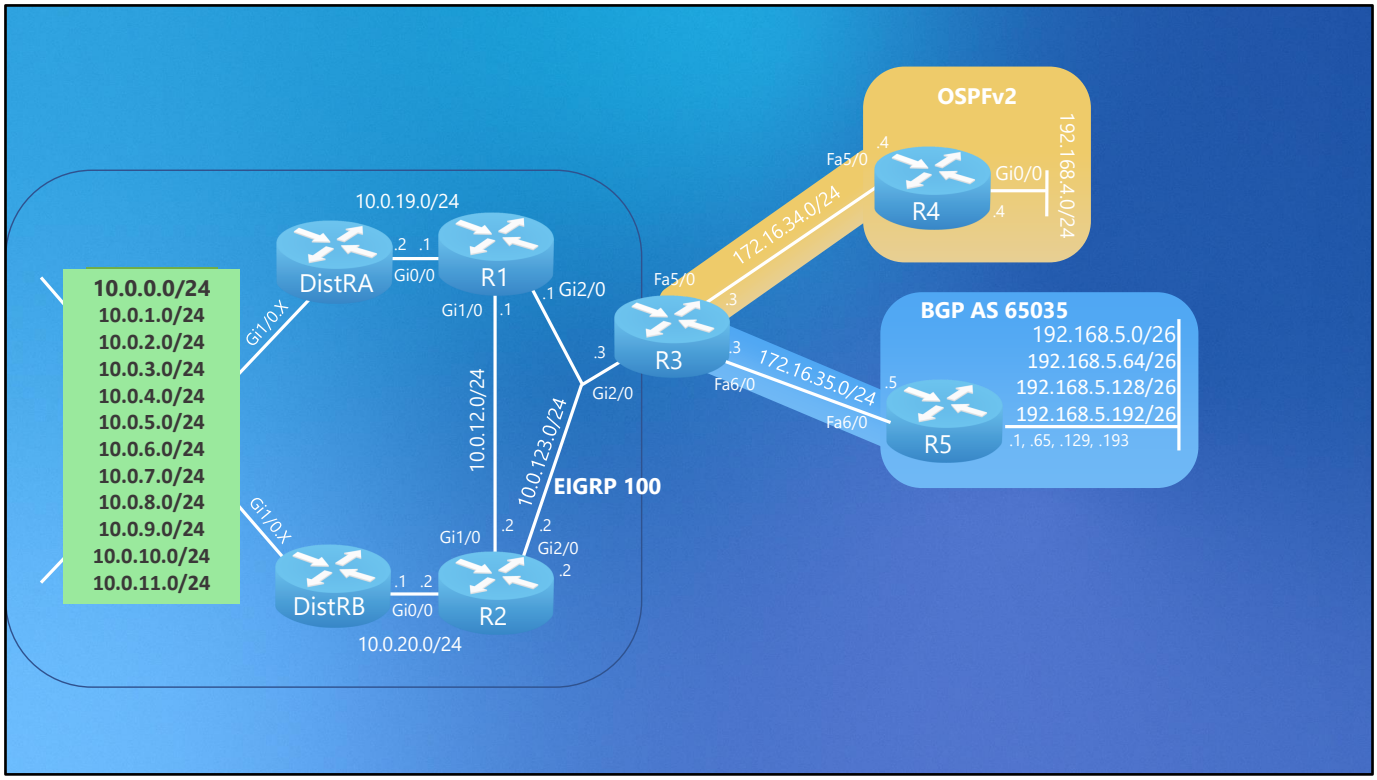
   R3(config-router-af)#default-metric 10
3. With the **redistribute** command

   R3(config-router-af)#redistribute eigrp 100 metric 12
4. With a route-map

   R3(config-router-af)#redistribute eigrp 100 route-map SET_METRIC

Preference = 4 3 2 1

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



By default only eBGP routes are redistributed into IGPs. To redistribute ibgp routes you have to enable it with the **bgp redistribute-internal** command in BGP AF configuration mode. (Do this first in BGP configuration mode.)

*****EXAM*** Also note that only internal ospf routes are redistributed into BGP by default when using classic OSPFv2. This rule does not apply to OSPFv3. So if you want to redistribute external ospf routes into BGP you have to indicate so with the redistribute command.**

Redistribute OSPF and BGP into EIGRP

```
router eigrp ENARSI
 address-family ipv4 unicast autonomous-system 100
  topology base
   redistribute bgp 65035 metric 100000 10 255 1 1500
   redistribute ospfv3 1 metric 100000 10 255 1 1500
```

Verify with show ip eigrp topology

Redistribute EIGRP and BGP in OSPFv3

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

router ospfv3 1
 address-family ipv4 unicast
  redistribute eigrp 100 (if we are using classic ipv4 ospf we have to issue the subnets keyword)
  redistribute bgp 65035 (if we are using classic ipv4 ospf we have to issue the subnets keyword)

Verify with show ospfv3 database

Redistribute OSPF and EIGRP into BGP
router bgp 65035
 address-family ipv4
  redistribute ospfv3 1
  redistribute eigrp 100

Verify with show bgp ipv4 unicast

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Title slide

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

FILTERING with Redistribution

- Distribute-List
  - Use prefix list
  - Use ACL
  - Use route-map
- Redistribute command
  - Use prefix list
  - Use ACL
  - Use route-map

Problem: Everything is redistributed by default. (So, let's filter)

Distribute list allows you to control which routes are redistributed.

A prefix list and acl only allow you to control what is or is not redistributed
A route-map allows you to control what is or is not redistributed as well as changing parameters like metric or metric type.

Redistribute command with Routemap

allows you to control which routes are redistributed and modify parameters during redistribution like metric or metric type..

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Prefix Lists

Problem: ACLs do not specify a subnet mask. They only specify the IP address.

Solution: Prefix Lists specify the address and mask.

```
ip prefix-list <name> permit x.x.x.x/xx
```

To verify:

```
show ip prefix list
show ip prefix-list detail
```

*detail cmd displays hit count

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Prefix List Example

Prefix-List named PFL2 permits:

10.10.11.0/24

10.10.12.0/24

```
ip prefix-list PFL2 seq 5 permit 10.10.11.0/24
ip prefix-list PFL2 seq 10 permit 10.10.12.0/24
```

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Prefix List Operators

Flexibility can be provided by utilizing operators

Operators can match on specific prefix or a range of prefixes

`le` – matches prefixes greater than or equal to value

`ge` - matches prefixes less than or equal to value

`ge & le` - matches prefixes between a range of values

```
ip prefix-list EXAMPLE permit 10.0.0.0/24 le 28
```

Des redo CLI
Des give examples of Operators

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Prefix List Operators

Flexibility can be provided by utilizing operators

Operators can match on specific prefix or a range of prefixes

`le` – matches prefixes greater than or equal to value

`ge` - matches prefixes less than or equal to value

`ge & le` - matches prefixes between a range of values

```
ip prefix-list EXAMPLE permit 192.168.5.0/24 ge 28 le 28
```

Des redo CLI
Des give examples of Operators

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Prefix List Operators

Flexibility can be provided by utilizing operators

Operators can match on specific prefix or a range of prefixes

`le` – matches prefixes greater than or equal to value

`ge` - matches prefixes less than or equal to value

`ge & le` - matches prefixes between a range of values

```
ip prefix-list EXAMPLE_A permit 0.0.0.0/0
ip prefix-list EXAMPLE_B permit  0.0.0.0/0 le 32
```

Des redo CLI
Des give examples of Operators

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Prefix List Operators

Flexibility can be provided by utilizing operators

Operators can match on specific prefix or a range of prefixes

`le` – matches prefixes greater than or equal to value

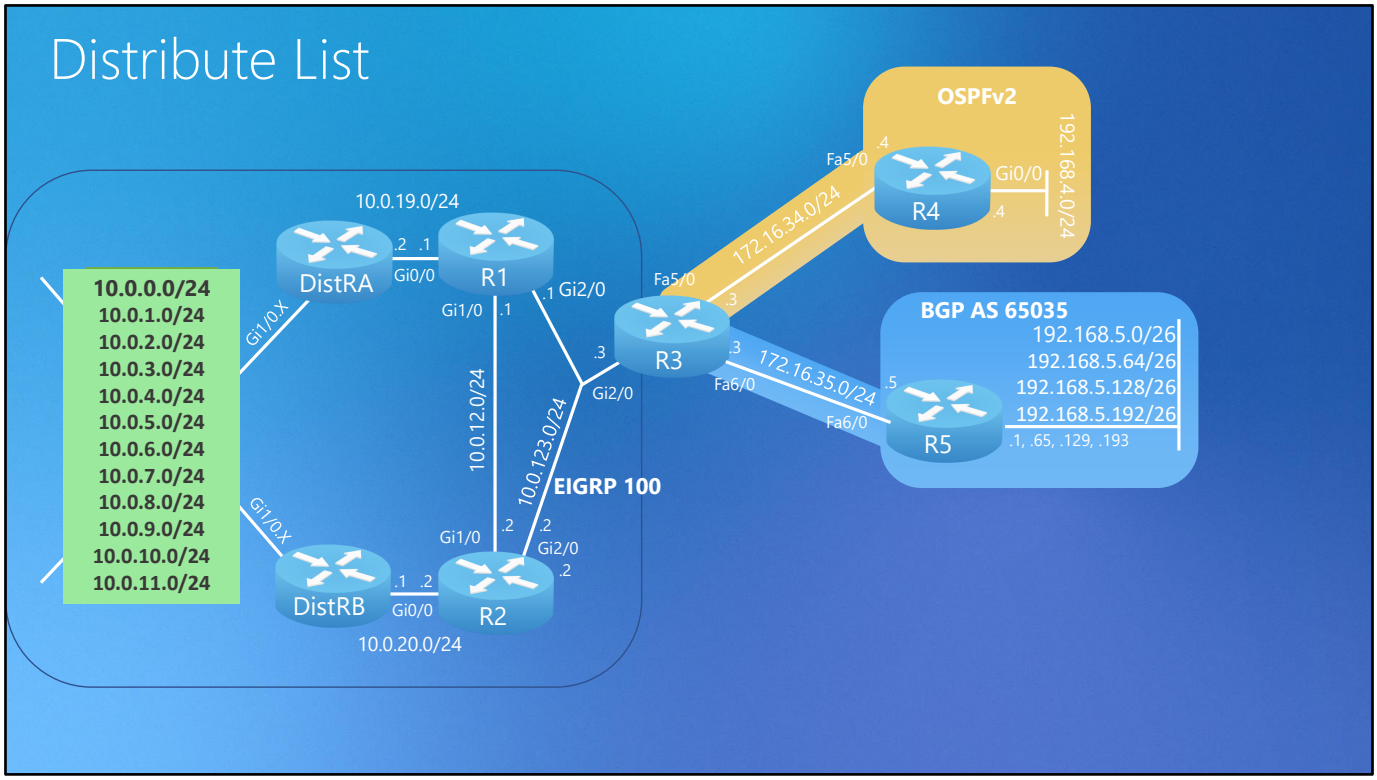
`ge` - matches prefixes less than or equal to value

`ge & le` - matches prefixes between a range of values

```
ip prefix-list EXAMPLE_A permit 10.0.0.0/24 le 28
ip prefix-list EXAMPLE_B permit 192.168.5.0/24 ge 28 le 28
ip prefix-list EXAMPLE_C permit 0.0.0.0/0
ip prefix-list EXAMPLE_D permit  0.0.0.0/0 le 32
```

Des redo CLI
Des give examples of Operators

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



R3:

```
ip prefix-list PL_INTO_OSPF deny 10.0.0.0/24
ip prefix-list PL_INTO_OSPF permit 0.0.0.0/0 le 32
router ospfv3 1
 address-family ipv4 unicast
  distribute-list prefix PL_INTO_OSPF out eigrp 100

ip prefix-list PL_INTO_BGP permit 10.0.0.0/24
ip prefix-list PL_INTO_BGP permit 192.168.4.0/24
router bgp 65035
 address-family ipv4
  distribute-list prefix PL_INTO_BGP out ospfv3 1
  distribute-list prefix PL_INTO_BGP out eigrp 100
  do clear bgp ipv4 unicast * (speed up refresh)
```

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Route Maps

Provide sophisticated route manipulation

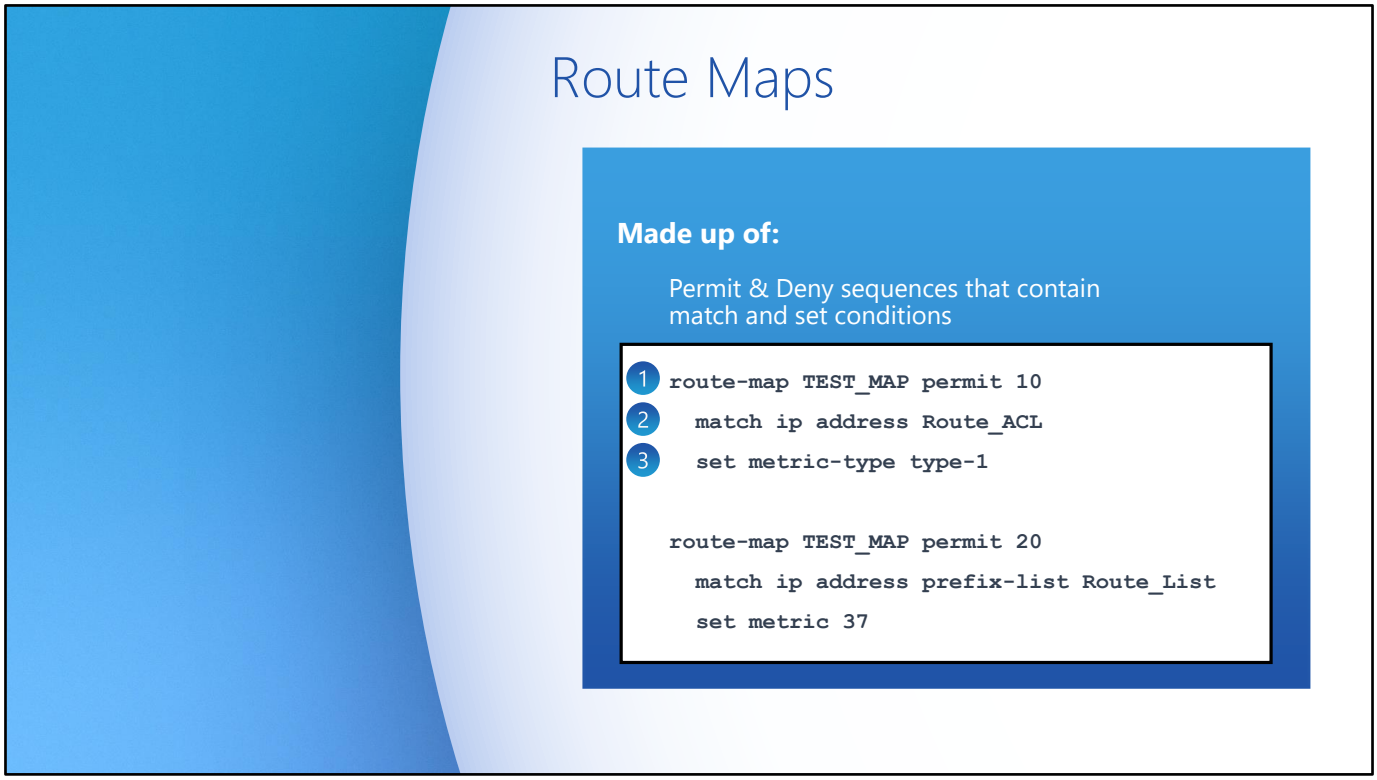
Made of "if & then" structured format

- Lines are number sequentially

Can be used for:

- Route Redistribution filtering instead of distribute lists
- Policy Based Routing (PBR)
- BGP policy manipulation

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



When we use a route map for redistribution a permit sequence means to redistribute anything that matches the sequence and set the values listed. A deny sequence means do not redistribute anything that matches the sequence.

If we are doing PBR it permit means PBR what matches and deny means route normally what matches.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Additional Route Map Notes

Multiple items referenced in one match statement = "or"

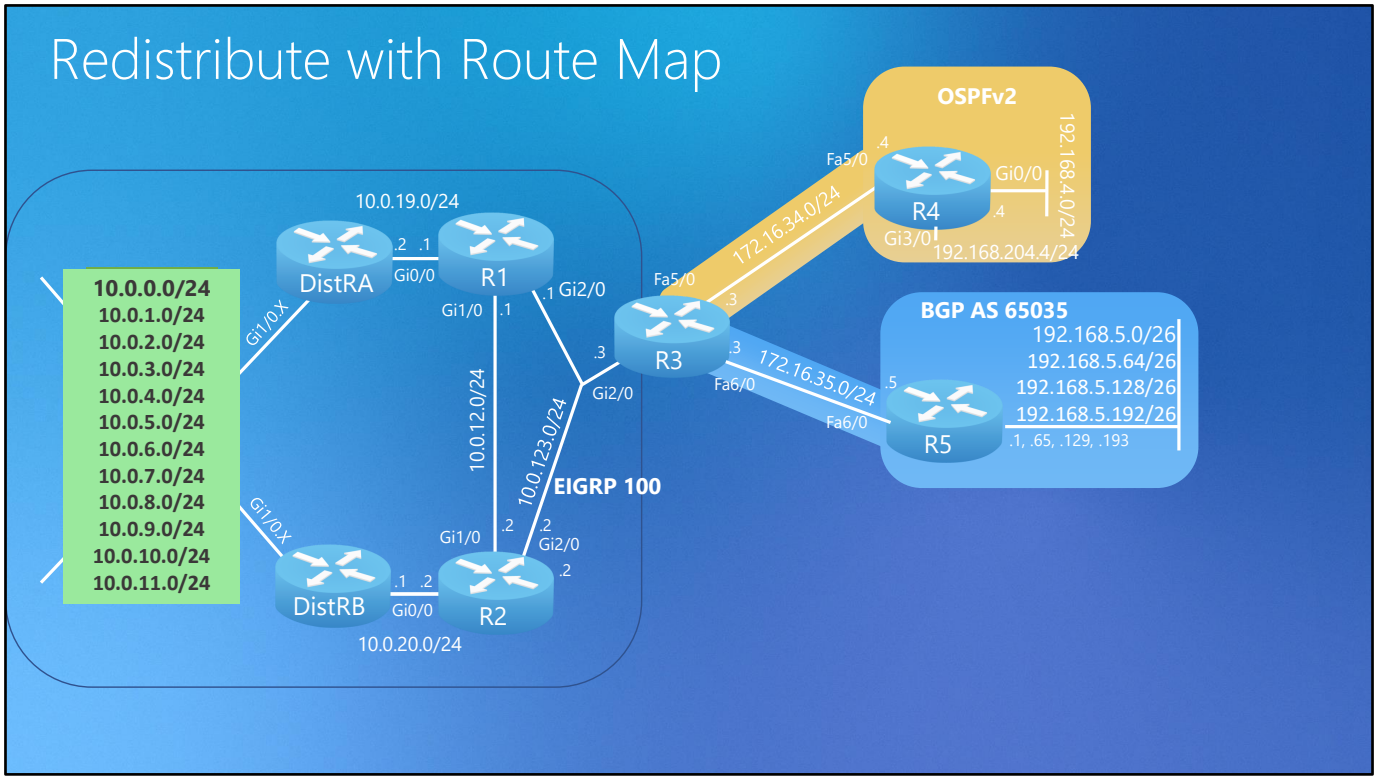
```
route-map TEST_MAP permit 10
  match ip address Route_ACL Test_ACL
  set metric-type type-1
```

Multiple items referenced in multiple match statement = "and"

```
route-map TEST_MAP permit 10
  match ip address prefix-list Test_List
  match metric-type E1
  set metric 27
```

*Multiple ACL's referenced – one or the other ("or")
*Multiple ACL's referenced on unique "match" statements must match all ("and")

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



INTO EIGRP:
ip prefix-list PL_INTO_EIGRP seq 5 permit 192.168.4.0/24
ip prefix-list PL_INTO_EIGRP2 seq 5 permit 192.168.204.0/24

route-map RM_INTO_EIGRP permit 10
 match ip address prefix-list PL_INTO_EIGRP
 set metric 1000 10 255 1 1500
route-map RM_INTO_EIGRP permit 20
 match ip address prefix-list PL_INTO_EIGRP2
 set metric 2000 1 100 100 1500

router eigrp ENARSI
 address-family ipv4 unicast autonomous-system 100
  topology base
   redistribute ospfv3 1 route-map RM_INTO_EIGRP (pop quiz: what happens when metrics are specified in the route-map and the command???? RM wins)

INTO OSPF:
ip prefix-list PL_OSPF1 permit 10.0.0.0/24

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

```
ip prefix-list PL_OSPF2 permit 10.0.1.0/24
ip prefix-list PL_OSPF3 permit 10.0.2.0/24

route-map INTO_OSPF permit 10
 match ip address prefix-list PL_OSPF1
 set metric 37
route-map INTO_OSPF permit 20
 match ip address prefix-list PL_OSPF2
 set metric-type type-1
route-map INTO_OSPF deny 30
 match ip address prefix-list PL_OSPF3
route-map INTO_OSPF permit 100

router ospfv3 1
 address-family ipv4 unicast
  redistribute eigrp 100 route-map INTO_OSPF
```

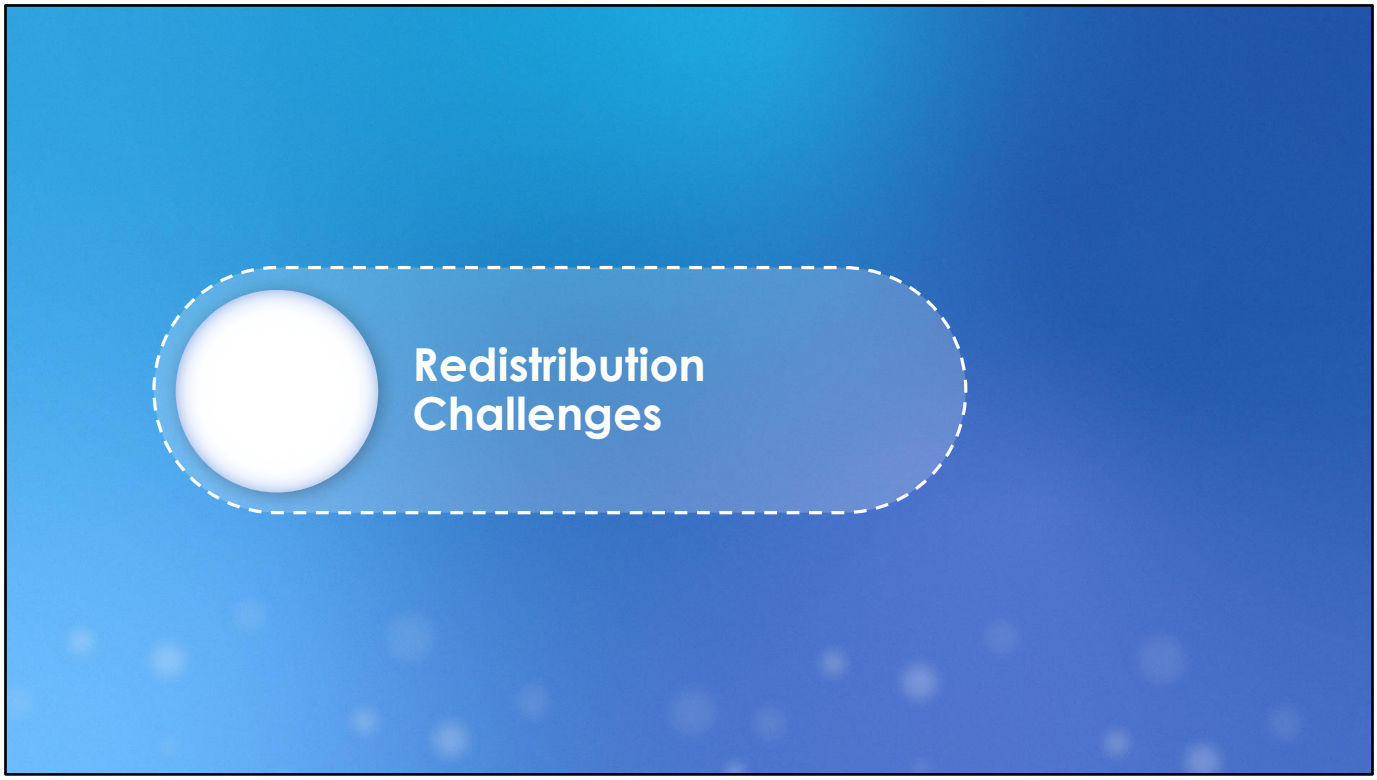
INTO BGP:

```
ip prefix-list PL_INTO_BGP1 seq 5 permit 10.0.0.0/24
ip prefix-list PL_INTO_BGP2 seq 5 permit 10.0.1.0/24
ip prefix-list PL_INTO_BGP3 seq 5 permit 10.0.2.0/24
ip prefix-list PL_INTO_BGP4 seq 5 permit 10.0.3.0/24
ip prefix-list PL_INTO_BGP5 seq 10 permit 10.0.12.0/24

route-map INTO_BGP permit 10
 match ip address prefix-list PL_INTO_BGP1
 set local-preference 200
route-map INTO_BGP permit 20
 match ip address prefix-list PL_INTO_BGP2
 set metric 12345
route-map INTO_BGP deny 30
 match ip address prefix-list PL_INTO_BGP3
route-map INTO_BGP permit 100

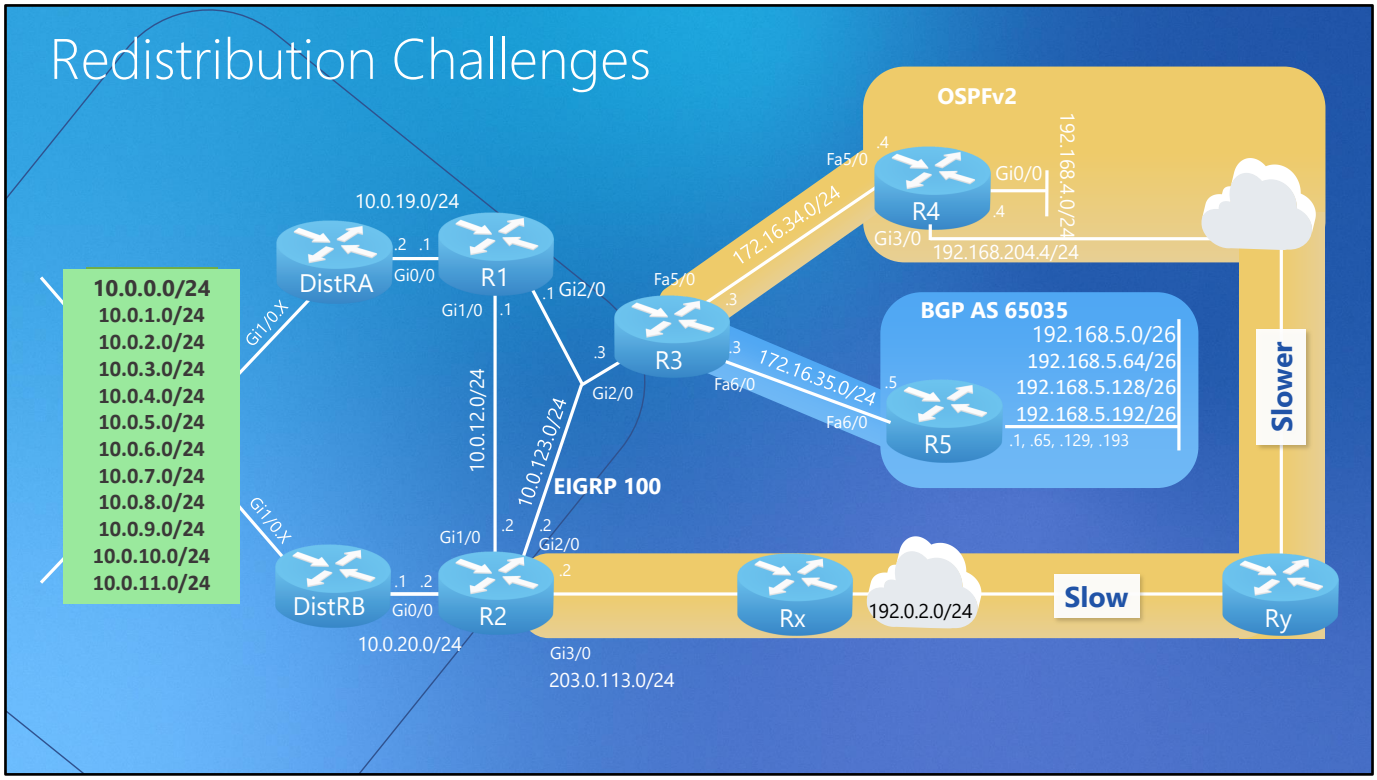
router bgp 65035
 address-family ipv4
  redistribute eigrp 100 route-map INTO_BGP
```

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Title slide

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



****** REMOVE ROUTE-MAPS ******

Issues with Redistribution:

Issue 1: Suboptimal Routing

Note: we are only redistributing on R3 at the moment. BGP injected into EIGRP and OSPF. Consider R2 now. Which way is R2 going to go to get to BGP networks. (DRAW IT)

Verify R2 **show ospfv3 database / show ip eigrp topology**

Ospf is preferred not eigrp **(why? Is it because of metric or AD) AD 110 vs 170 so you need to change the AD of the OSPF routes higher or the EIGRP routes lower.**

EIGRP

```
router eigrp ENARSI
 address-family ipv4 unicast autonomous-system 100
  topology base
   distance eigrp 90 109
```

OSPF

```
router ospfv3 1
```

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

address-family ipv4 unicast
distance 171 (would change for all ospf routes)
or distance ospf external 171 (only for external routes)

REMOVE LAST CONFIG

Let's redistribute on R2

R2:

router eigrp ENARSI
address-family ipv4 unicast autonomous-system 100
topology base
redistribute ospfv3 1 metric 100000 10 255 1 1500
router ospfv3 1
address-family ipv4 unicast
redistribute eigrp 100

verify on R2 show ospfv3 database (look for 10.0.0.0/24 as an example)
Verify on R2 show ip eigrp topology (look for 192.168.5.0/26 and 192.168.4.0/24 as an example)

Issue 2:

Go to R1 and verify path that is being taken to 192.168.4.0??? (show ip route) Via R2andR3 OMG…. Load balancing!!!! Is this OK?
What happens when R3 gets the packets... they go to R4… that is good.
What happens when R2 gets the packets… they go to Rx… that is not good.
Why is this happening… is it because of AD???… nope because R1 learns via EX EIGRP from both R2 and R3… so this is metric related. (the metric that is being injected is causing the load balancing)
To fix… we would modify the metric being injected on R3 so it is lower or R2 so it is higher. This will ensure that R1 chooses R3 over R2.

*** Note: We could use an offset list on R1 as well but not the best option in this case.***
Note2: We could modify the AD on R2 so EIGRP is lower… therefore, the OSPF route is not installed in the routing table and therefore not redistributed because the EIGRP route is preferred.

R3:

router eigrp ENARSI
address-family ipv4 unicast autonomous-system 100
topology base
redistribute ospfv3 1 metric 1000000 10 255 1 1500 (add an extra 0 to bandwidth)

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Go back to R1 type in show ip route and notice that 192.168.4.0 is only going to use R3 now. However, if R3 fails or the connection to 3 fails R1 still has the route through R2 as seen in show ip eigrp topology.

Issue 3:
Now we introduced another problem…. The 203.0.113.0/24 network on R2 will be reached through R3 instead of R2. Why??? Because when we modify the metric using the redistribute command it affects every route begin redistributed. How can we solve this???? With a route-map as we discussed earlier. We can single out the routes and then modify the metric for just those routes.

R3:

```
ip prefix-list PL_R4_NETWORKS permit 192.168.4.0/24
ip prefix-list PL_R4_NETWORKS permit 192.168.204.0/24
Route-map RM_R4_NETWORKS permit 10
        Match ip address prefix PL_R4_NETWORKS
        Set metric 1000000 10 255 1 1500
Route-map RM_R4_NETWORKS permit 20
        Set metric 100000 10 255 1 1500  (DON'T FORGET THIS)
router eigrp ENARSI
 address-family ipv4 unicast autonomous-system 100
  topology base
   redistribute ospfv3 1 route-map RM_R4_NETWORKS
```

R2:

```
ip prefix-list PL_R2_NETWORKS permit 192.0.2.0/24
ip prefix-list PL_R2_NETWORKS permit 203.0.113.0/24
Route-map RM_R2_NETWORKS permit 10
        Match ip address prefix PL_R2_NETWORKS
        Set metric 1000000 10 255 1 1500
Route-map RM_R2_NETWORKS permit 20
        Set metric 100000 10 255 1 1500 (DON'T FORGET THIS)
router eigrp ENARSI
 address-family ipv4 unicast autonomous-system 100
  topology base
   redistribute ospfv3 1 route-map RM_R2_NETWORKS
```

Use **SHOW IP ROUTE** R1. FLAP R3 interface Fa5/0 do see how failover will occur.

WOW!!!! OK.

WE ARE NOT DONE!

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Issue4: EXAM BUT BGP = RIP instead

Go to R1 and examine 192.168.5.0… notice we have to use R2 and R2 only. HMMMMM What is going on here. R3 knows about it from BGP (AD 200) redistributes into OSPF and EIGRP. R2 learns about it from EIGRP (AD 170) and OSPF (AD 110 and prefers OSPF and installs in the routing table). Therefore, it redistributes it into EIGRP. So R1 learns from R2 and R3… or does it?????? Consider what happens when R2 redistributes the route…. R3 learns about it from R2 EIGRP (AD 170) which is better than the BGP (AD 200) route. Oh OOOOOOO! Therefore, R3 replaces the BGP route in the routing table with the route from EIGRP. So, now we can't even get to the BGP networks. (WE HAVE A ROUTING LOOP! OMG)

Trace route from R1 to 192.168.5.1

Why is this happening???? Is it metric related or AD related???? AD related.
Where??? R1 (NO), R2 (NO), R3 (YES)
So on R3 we have to change the AD of EIGRP or BGP so BGP is preferred.
Let's change BGP because we have already shown you how to do EIGRP AD changes.

R3:

```
router bgp 65035
 address-family ipv4
  distance bgp 20 169 169
do clear ip bgp *
```

Trace route from R1 to 192.168.5.1

Note: because R3 and R2 are redistributing into EIGRP using the same metric R1 will load balance which means we have to fix our metric issue like we did before.

R3:

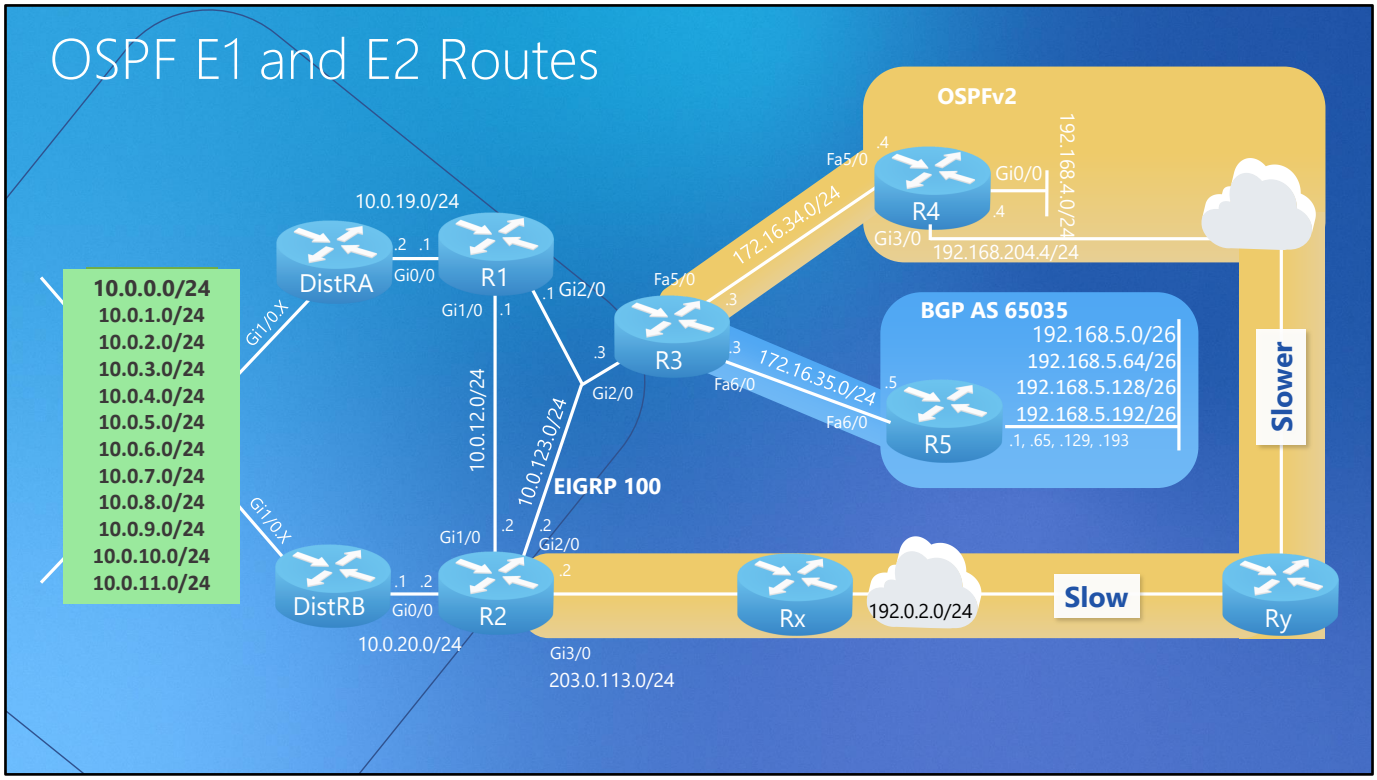
```
router eigrp ENARSI
 address-family ipv4 unicast autonomous-system 100
   topology base
    redistribute bgp 65035 metric 1000000 10 255 1 1500 (add a zero to BW)
```

Show ip route

Trace route from R1 to 192.168.5.1

***** These are just some examples… you would have to verify every network to make sure that you are getting the results you want from a forwarding basis. This requires you to have a diagram you can draw on to determine what you want and then verify it in the CLI, with ping, traceroute, ip route, etc.**

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



When we redistribute on R2 and R3 into OSPF, by default the metric is set to 20 and the metric type will be E2.

Let's look at Ry and R4 and Rx in this case.
Ry = show ip route (E2 / cost 20 / load balancing)
R4 = show ip route (E2 / cost 20 / go through R3)
Rx = show ip route (E2 / cost 20 / go through R2)

WHY?????

With E2 the metric set by the ASBR is preserved and used as the metric. (So why is R4 and Rx not load balancing?)

Load balancing will only occur if the path to the ASBRs is equal as well.

show ospfv3 database external 10.0.0.0 on Ry / R4 / Rx to determine advertising routers (the routers will then determine the cost to reach the ASBR "advertising router" and if the cost is the same LB will occur. If not, the ASBR with the shortest path will be used.

Now if the metric is modified at redistribution… let's say r3 is set to 10 and r2 remains at 20… the lower is preferred by all. The path to the ASBR does not come into play.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

```
R3:
router ospfv3 1
 address-family ipv4 unicast
  redistribute eigrp 100 metric 10
```

Problem: Rx now prefers R3 to get to the 10 networks. This is happening because of E2. E2 is really great when you want to prefer one ASBR over another. So if you have 2 or more ASBRs and you want to force all traffic to go through a specific one (set the metric type to E2 and give it a lower metric) and that will be the ASBR that will be used. If it fails, the other ASBR will be used.

So it is only a problem if you don't want all traffic to use R3. In this case… Do I? NO because of the slow links.

I am better off to have the routers also make a decision based on the internal cost of OSPF to reach the destination. That is what E1 is for. So on R3 and R2 if we used E1 instead of E2 then the cost will be cumulative from the router to the ASBR and include the seed metric.

We can also use a route map to set metrics and metric types on a route by route basis. So for example, if you wanted 10.0.0.0/24 through to 10.0.5.0/24 to be E2 and metric 10 and everything else to be E2 metric 20 on r3 when they are redistributed and have the reverse happen on R2 when they are redistributed… then you can force traffic from 10.0.0.0/24 through to 10.0.5.0/24 to use R3 and traffic to the rest of the networks to use R2.

Remember though… mixing E1 and E2 can causes issues as well. For example, if you E1 the 10.0.0.0/24 network on R2 and you E2 the same network on R3…. E1 prevails on all the routers in the OSPF domain. So this could be used as a way to prefer R2 over R3 as well but it could also cause suboptimal routing for some of the routers.

SO IN CONCLUSION… when performing multipoint redistribution…. You have to take your time and plan / config / verify every route and path to make sure you are getting the result you want.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

OSPF E1 and E2 Routes

The cost will vary depending on the way the external routes are configured with metric type

Type	Description	Cost Calculation
O E1	Type 1 external	Add the external cost to the internal cost of each link
O E2	Type 2 external	External cost is always the injected cost at the ASBR

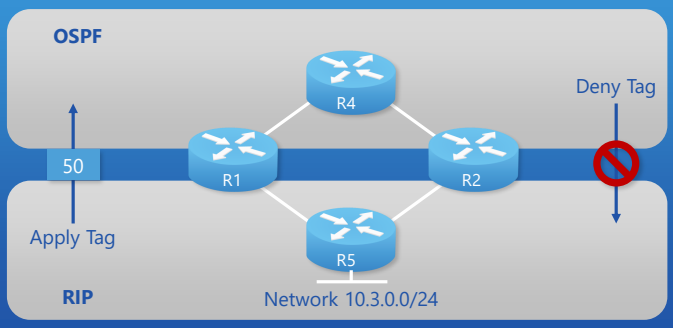
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Tagging with Redistribution

Route tags are simple labels that are attached to selected routes.

Route tagging enables filtering based on the tag.

Route maps are used to set and match route tags.

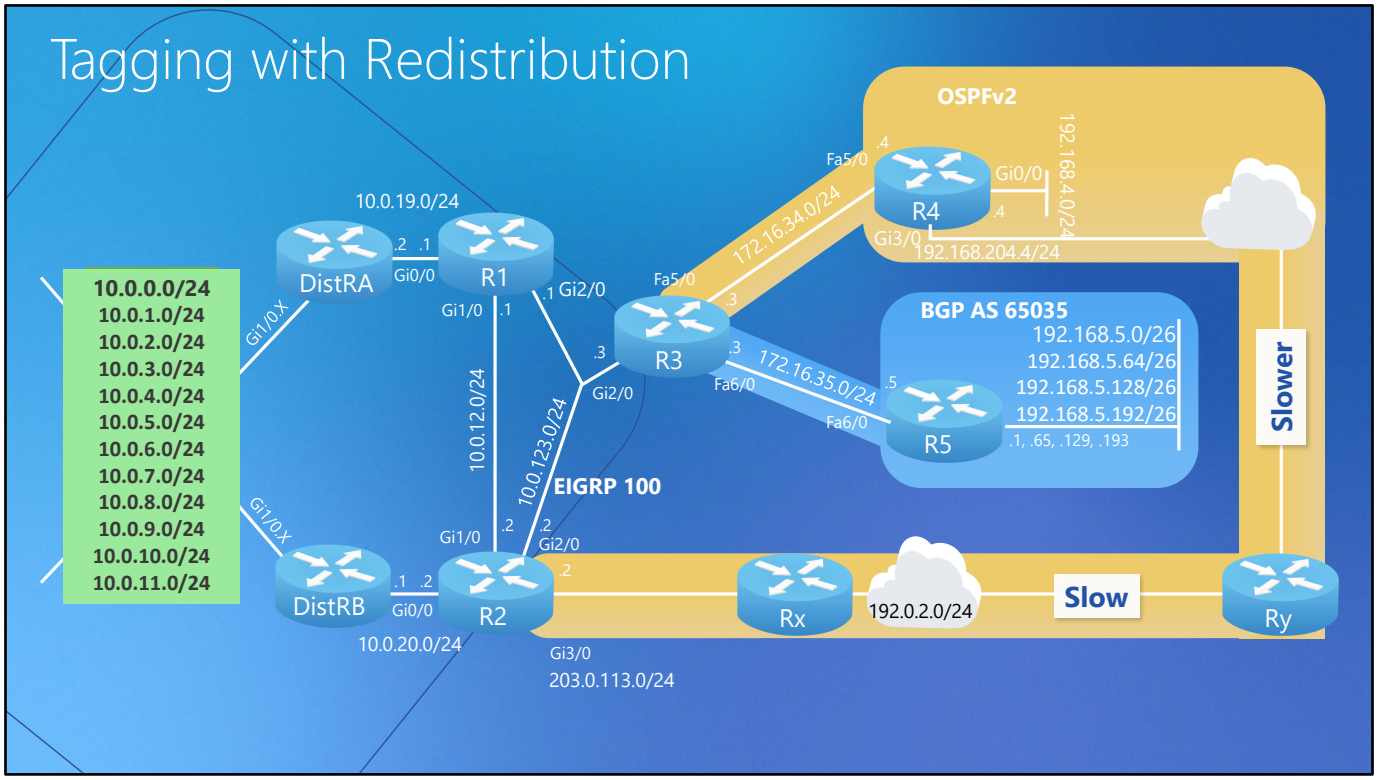


How can we prevent routes from being redistributed back into the routing protocol it was originally learned from?

Prefix lists with Distribute lists…. Prefix lists with Route maps… but that is tough to maintain.

TAGGING is a much better option.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Set tag into EIGRP on R3 and deny tag into OSPF on R2.

R3: set tag on routes from ospf into eigrp

```
route-map INTO_EIGRP permit 10
 set tag 54

router eigrp ENARSI
 address-family ipv4 unicast autonomous-system 100
  topology base
   redistribute ospfv3 1 metric 100000 10 255 1 1500 route-map SETTAG
```

R2: deny anything with a tag of 54

```
route-map INTO_OSPF deny 10
 match tag 54
route-map INTO_OSPF permit 100

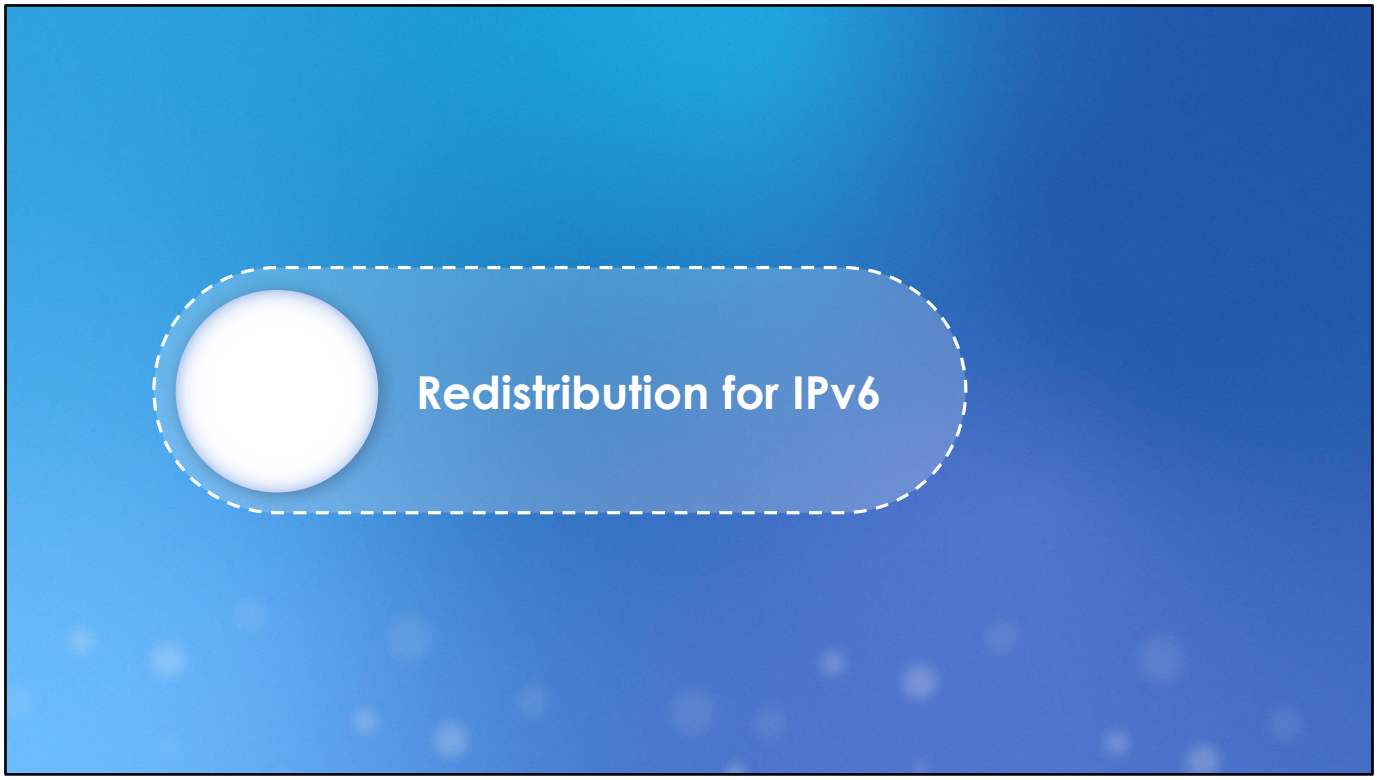
router ospfv3 1
 !
 address-family ipv4 unicast
  redistribute eigrp 100 route-map INTO_OSPF
```

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Set tag into EIGRP on R2 and deny tag into OSPF on R3.
Set tag into OSPF on R3 and deny tag into EIGRP on R2.
Set tag into OSPF on R2 and deny tag into EIGRP on R3.

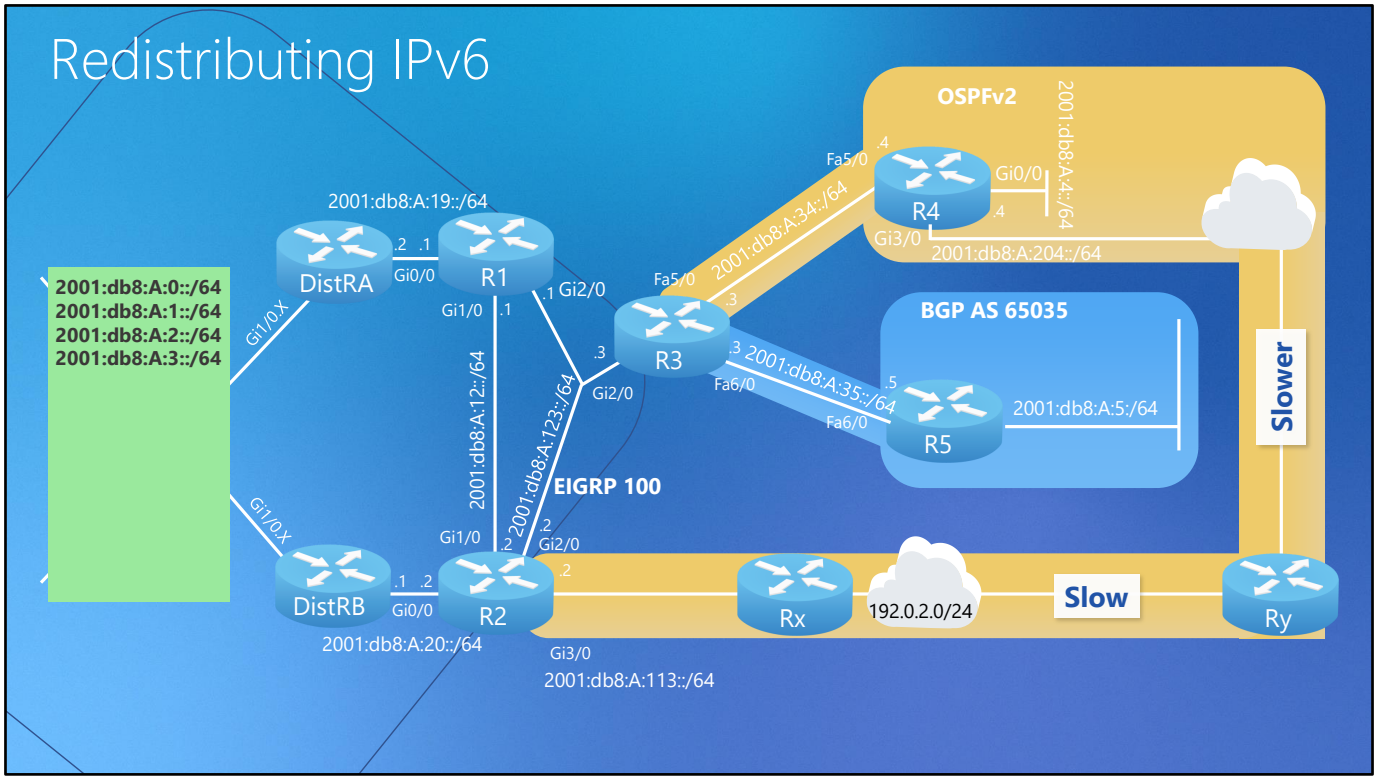
PROBLEM: example… if Rx loses connection to R4 thorough OSPF it will not know about it through R2 because the tag is stopping it from being redistributed. So, like before…. a thorough analysis of all possible scenarios needs to be considered when redistributing.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Title slide

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Everything is the same as IPv4 so we will not go over that again except know this….

With OSPFv2 (subnets keyword), with OSPFv3 IPv6 and OSPFv3 (no such thing as subnets keyword)

With IPv6 redistribution the connected networks participating in the routing process on the border router are not redistributed like IPv4. If you need to include them you would have to use the “include-connected” keyword.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Title slide

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Policy Based Routing (PBR)

A feature used to override the default forwarding decision:

- Default – forward based on destination IP address
- PBR – forward based on anything you want
  - source IP
  - port numbers
  - protocols
  - … and more
  - – mark packets for QoS purposes

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Policy Based Routing (PBR)

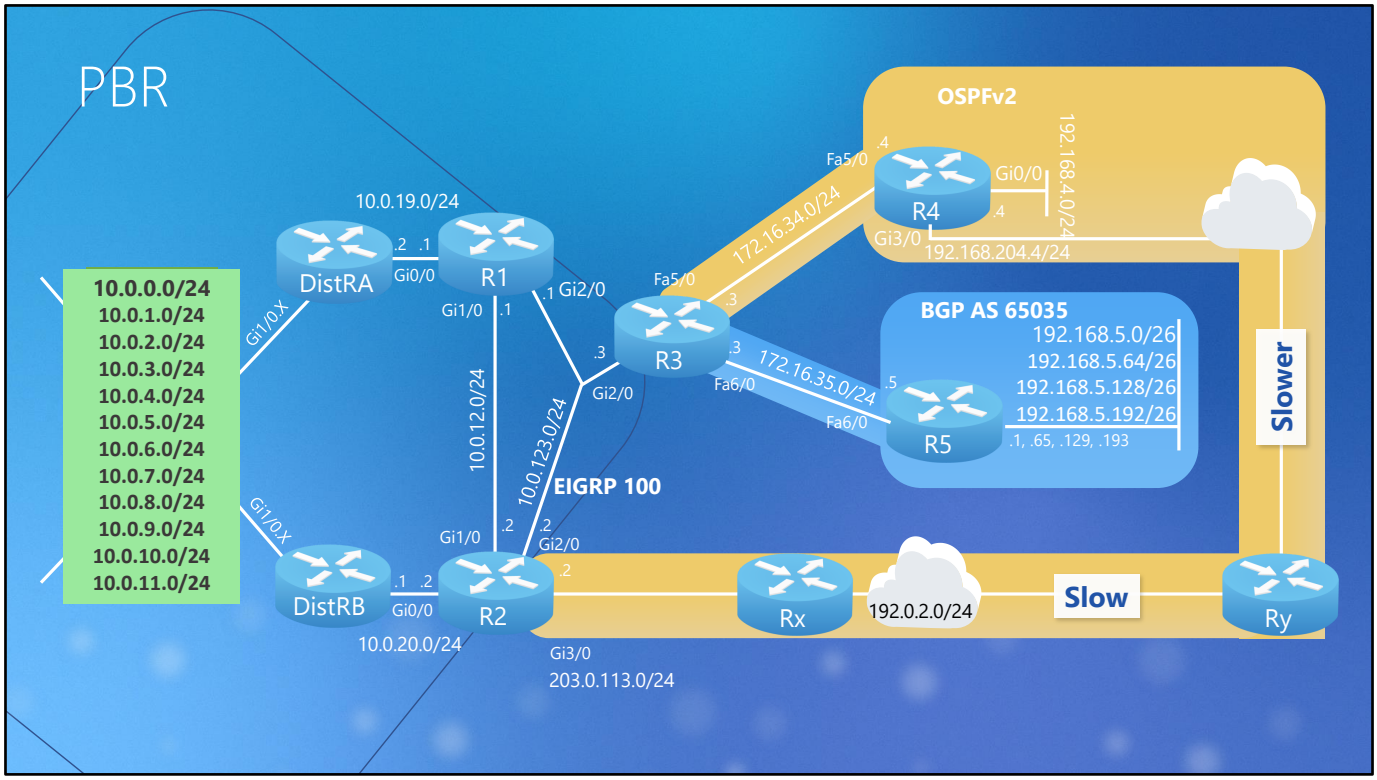
PBR creation:

- ACLs – for identification purposes
- Route Maps – to define what happens
  - match
  - set

PBR applied:

- inbound interface – for arriving packets
  - R1(config-if)#ip policy route-map *route-map_name*
- control plane – for packets generated by router
  - R1(config-if)#ip local policy route-map *route-map_name*

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Virtual PC
trace 192.168.204.4 -P 1
trace 192.168.4.4 -P 1

R1
ip access-list extended ACL_PBR
 permit icmp host 10.0.0.10 host 192.168.4.4

route-map RM_PBR permit 10
 match ip address ACL_PBR
 set ip next-hop 10.0.123.3????? (this will be based on the results of the traceroute)

interface GigabitEthernet0/0
 ip policy route-map RM_PBR

Debug Ip policy
Show ip policy
Show route-map (hit count)

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Virtual PC
trace 192.168.204.4 -P 1
trace 192.168.4.4 -P 1

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Policy Based Routing (PBR)

Default Keyword:

set ip next-hop *next_hop_ip*

vs

set ip default next-hop *next_hop_ip*

set interface *exit_interface*

vs

set default interface *exit_interface*

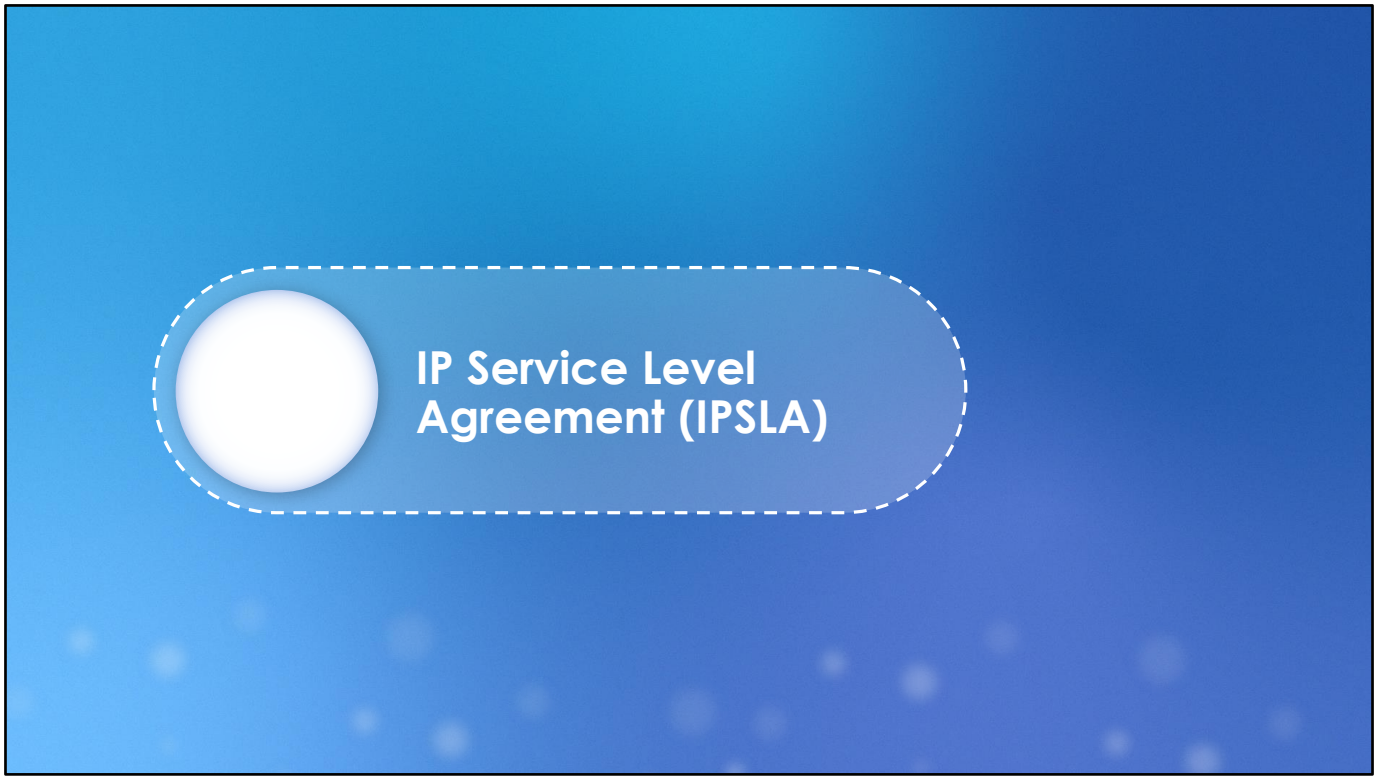
The first option states:

Do PBR and if there is no match in the route map… route normally

The second option states:

Route normally… however, if there is no match or the match is the default route do PBR.

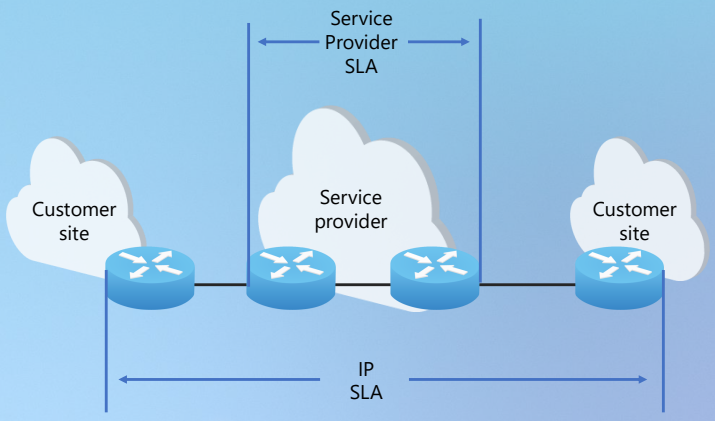
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Title slide

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

IP SLA Overview



- Tool built into Cisco IOS
  - Continuous monitoring of various aspects of the network
    - Delay (both round-trip and one-way)
    - Jitter (directional)
    - Packet loss (directional)
    - Packet sequencing (packet ordering)
    - Path (per hop)
    - Connectivity (directional)
    - Server or website download time
    - Voice quality scores

Graphics: build a cool 3D graphic that we can try to add a fly by to while I am talking.

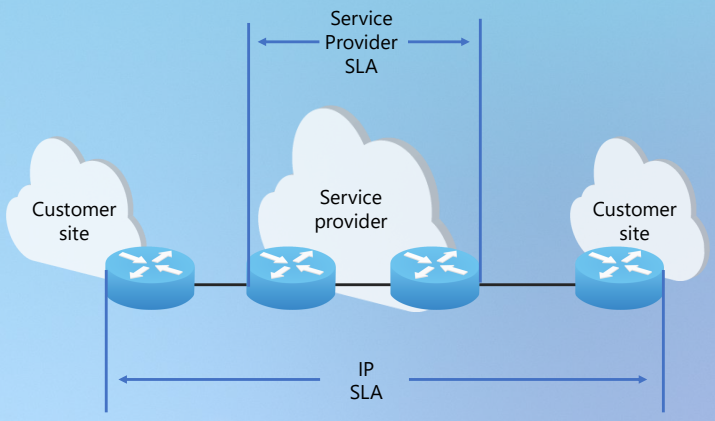
Instructor Notes: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipsla/configuration/xe-3e/sla-xe-3e-book/sla_overview.html
IP SLAs provides the following improvements over a traditional service level agreement:
End-to-end measurements--The ability to measure performance from one end of the network to the other allows a broader reach and more accurate representation of the end-user experience.
Sophistication--Statistics such as delay, jitter, packet sequence, Layer 3 connectivity, and path and download time that are broken down into bidirectional and round-trip numbers provide more data than just the bandwidth of a Layer 2 link.
Ease of deployment--Leveraging the existing Cisco devices in a large network makes IP SLAs easier and cheaper to implement than the physical probes often required with traditional service level agreements.
Application-aware monitoring--IP SLAs can simulate and measure performance statistics generated by applications running over Layer 3 through Layer 7.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Traditional service level agreements can only measure Layer 2 performance.
Pervasiveness--IP SLAs support exists in Cisco networking devices ranging from low-end to high-end devices and switches. This wide range of deployment gives IP SLAs more flexibility over traditional service level agreements.
When you know the performance expectations for different levels of traffic from the core of your network to the edge of your network, you can confidently build an end-to-end application-aware service level agreement

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

IP SLA Overview



Purpose

- increase productivity
- lower operational costs
- reduce the frequency of network outages
- Troubleshooting
- Problem analysis
- Designing networks

Graphics: build a cool 3D graphic that we can try to add a fly by to while I am talking.

Instructor Notes: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipsla/configuration/xe-3e/sla-xe-3e-book/sla_overview.html

Benefits of IP SLAs

IP SLAs monitoring

Provides service level agreement monitoring, measurement, and verification.

Network performance monitoring

Measures the jitter, latency, or packet loss in the network.

Provides continuous, reliable, and predictable measurements.

IP service network health assessment

Verifies that the existing QoS is sufficient for new IP services.

Edge-to-edge network availability monitoring

Provides proactive verification and connectivity testing of network resources (for example, indicates the network availability of a Network File System (NFS) server used to store business critical data from a remote site).

Troubleshooting of network operation

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

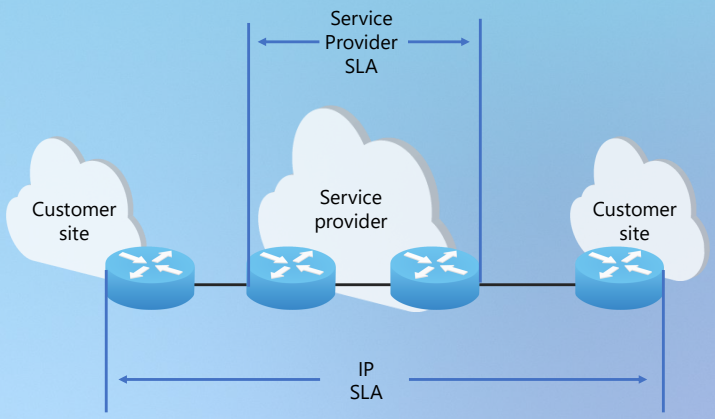
Provides consistent, reliable measurement that immediately identifies problems and saves troubleshooting time.

Voice over IP (VoIP) performance monitoring

Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) performance monitoring and network verification

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

IP SLA Overview

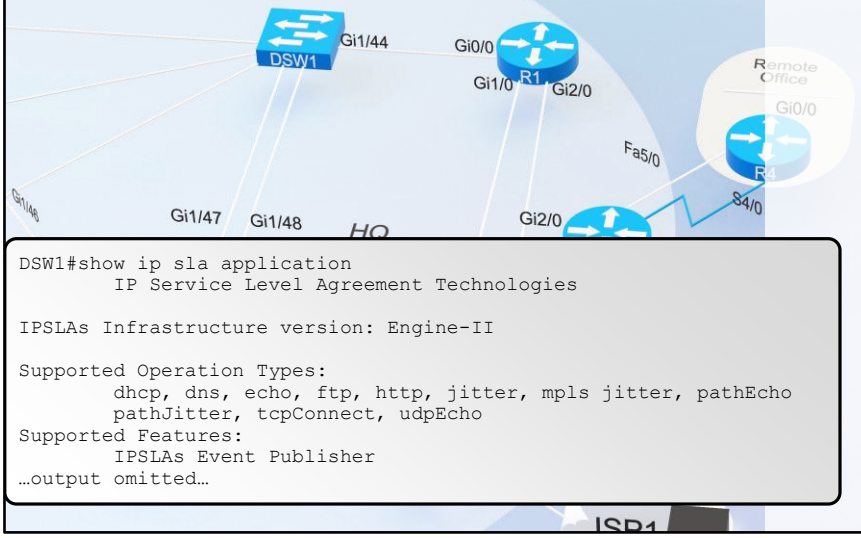


- Uses Active traffic monitoring
  - Send a probe in a continuous, reliable, and predictable manner
  - Collect results of the probe
    - Store in memory (CLI)
    - Store in SNMP MIB

Graphics: build a cool 3D graphic that we can try to add a fly by to while I am talking.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Verify Supported IP SLA Operations




```
DSW1#show ip sla application
        IP Service Level Agreement Technologies

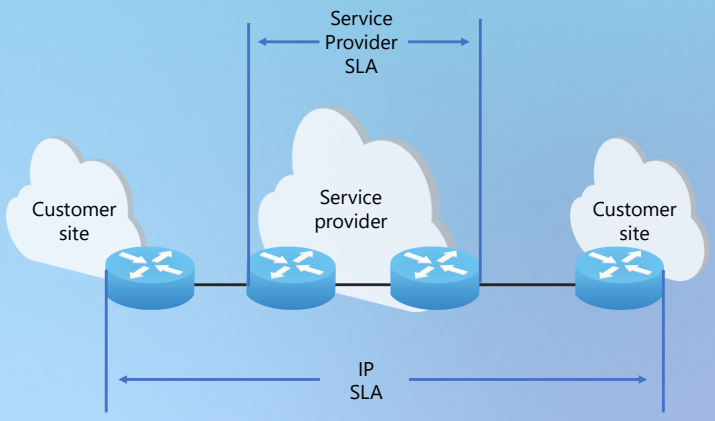
IPSLAs Infrastructure version: Engine-II

Supported Operation Types:
        dhcp, dns, echo, ftp, http, jitter, mpls jitter, pathEcho
        pathJitter, tcpConnect, udpEcho
Supported Features:
        IPSLAs Event Publisher
…output omitted…
```

Verify operations supported on local product

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

IP SLA



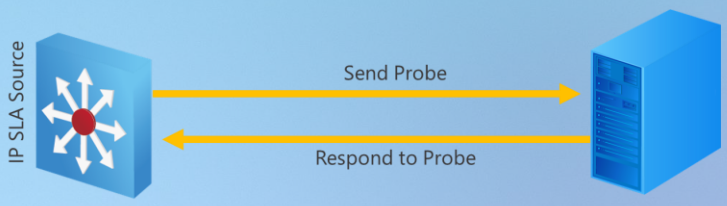
What do we do with gathered statistics?

- Verify we are getting what we are paying for
- Failover for floating static routes
- FHRP failover with "tracking"
- Send SNMP traps when threshold is exceeded
- … and more

Graphics: build a cool 3D graphic that we can try to add a fly by to while I am talking.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

IP SLA without Responder

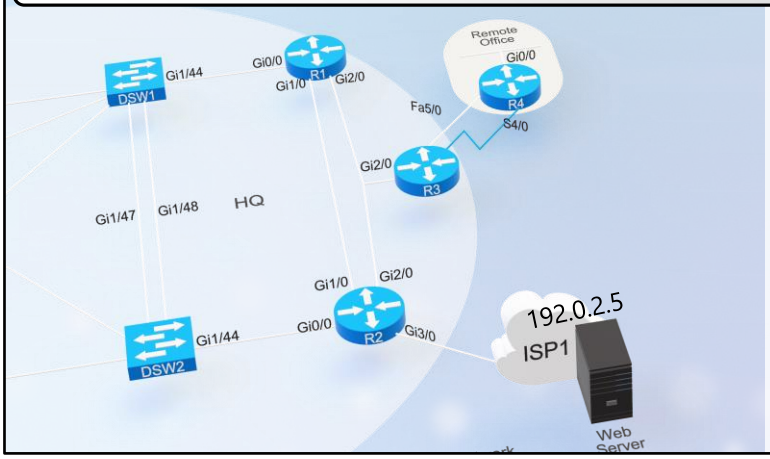


Any device that understands the probe being used!!

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

IP SLA without Responder

```
DSW1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DSW1(config)#ip sla 1
DSW1(config-ip-sla)#icmp-echo 192.0.2.5 source-ip 10.0.10.2
DSW1(config-ip-sla-echo)#frequency 5
DSW1(config-ip-sla-echo)#exit
DSW1(config)#ip sla schedule 1 start-time now life forever
DSW1(config)#end
DSW1#
```

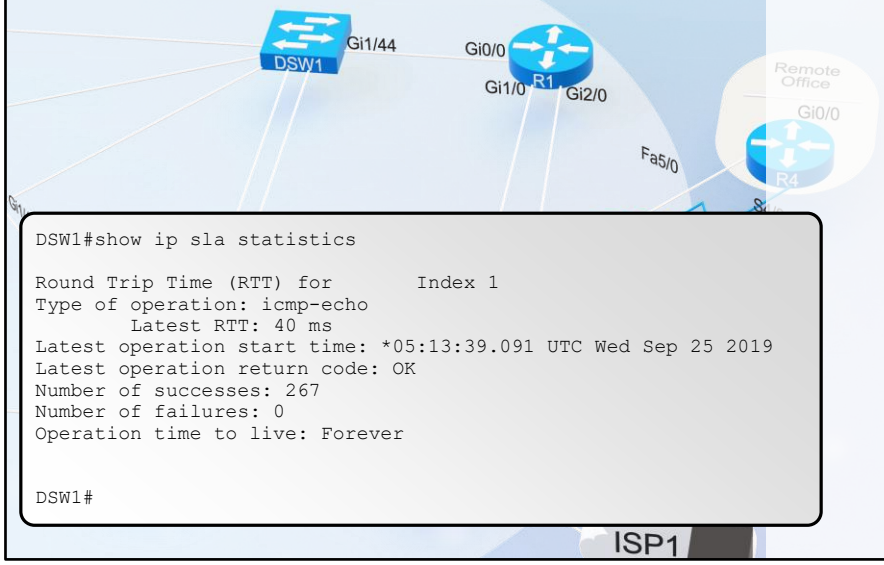


Talk about standard and extended

R1#traceroute 192.168.4.4 ?
  numeric display numeric address
  port   specify port number
  probe   specify number of probes per hop
  source   specify source address or name
  timeout specify time out
  ttl   specify minimum and maximum ttl
  <cr>

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

IP SLA without Responder



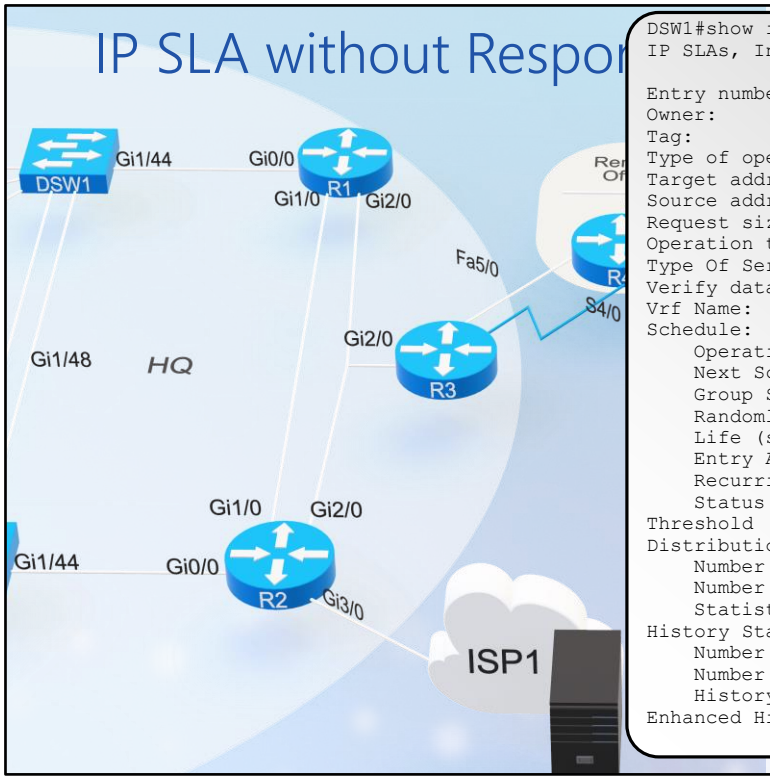

```
DSW1#show ip sla statistics

Round Trip Time (RTT) for       Index 1
Type of operation: icmp-echo
        Latest RTT: 40 ms
Latest operation start time: *05:13:39.091 UTC Wed Sep 25 2019
Latest operation return code: OK
Number of successes: 267
Number of failures: 0
Operation time to live: Forever


DSW1#
```

ISP1

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

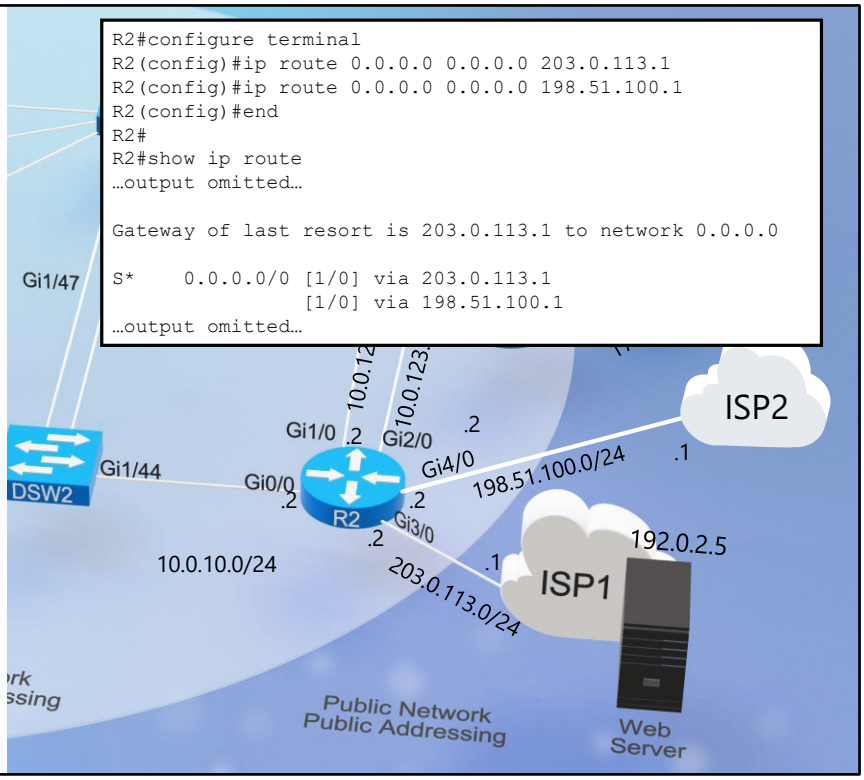



```
DSW1#show ip sla configuration
IP SLAs, Infrastructure Engine-II

Entry number: 1
Owner:
Tag:
Type of operation to perform: echo
Target address: 192.0.2.5
Source address: 10.0.10.2
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Vrf Name:
Schedule:
    Operation frequency (seconds): 5
    Next Scheduled Start Time: Start Time already passed
    Group Scheduled : FALSE
    Randomly Scheduled : FALSE
    Life (seconds): Forever
    Entry Ageout (seconds): never
    Recurring (Starting Everyday): FALSE
    Status of entry (SNMP RowStatus): Active
Threshold (milliseconds): 5000
Distribution Statistics:
    Number of statistic hours kept: 2
    Number of statistic distribution buckets kept: 1
    Statistic distribution interval (milliseconds): 20
History Statistics:
    Number of history Lives kept: 0
    Number of history Buckets kept: 15
    History Filter Type: None
Enhanced History:
```

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Floating Static Routing



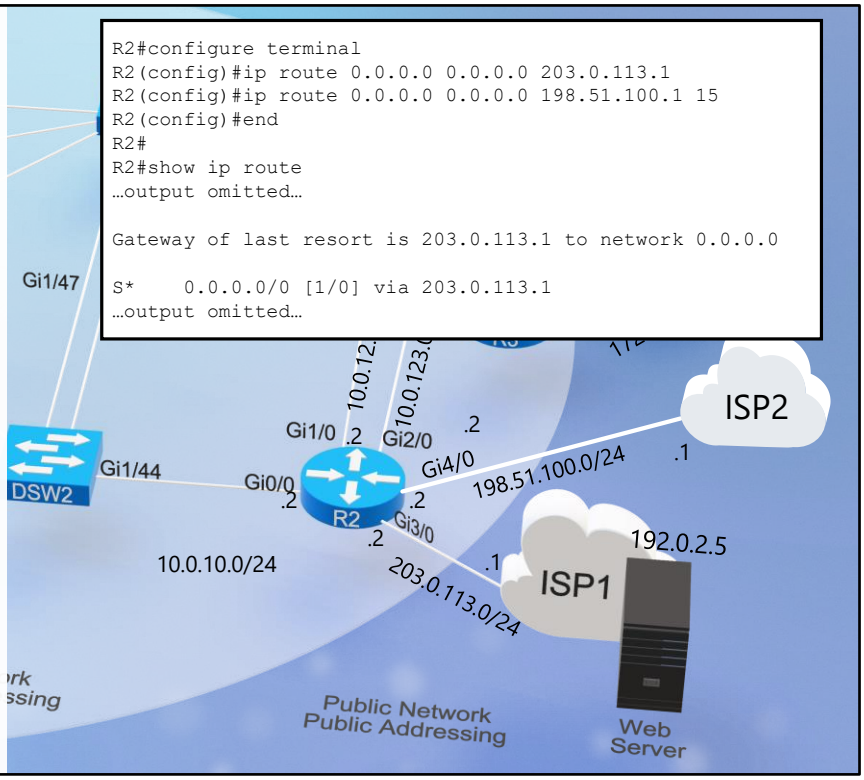
When might this be useful????

In this scenario we are load balancing which might not be what we want…

It could cause asymmetric routing
It could cause higher costs if ISP2 is only a backup.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Floating Static Routing



This will load balance

How do I create a floating static route.

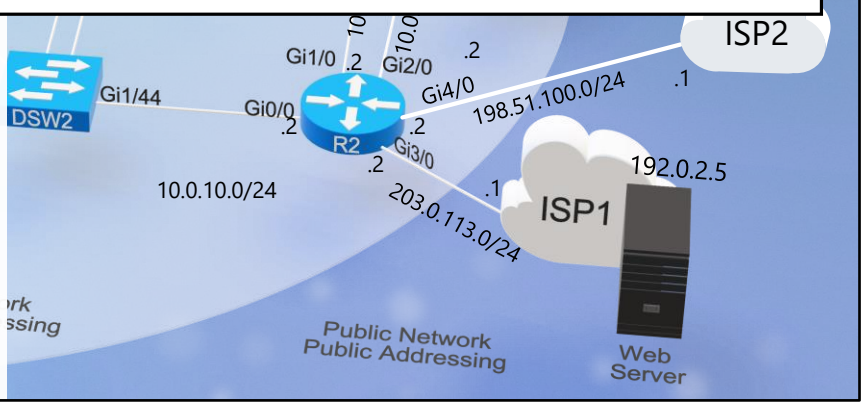
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Floati
Routi

```
R2#configure terminal
R2(config)#int gig 3/0
R2(config-if)#shut
R2(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet3/0, changed state to administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet3/0, changed state to down
R2(config-if)#end
R2#show ip route
…output omitted…

Gateway of last resort is 198.51.100.1 to network 0.0.0.0

S*    0.0.0.0/0 [15/0] via 198.51.100.1
…output omitted…
```



This will load balance

How do I create a floating static route.

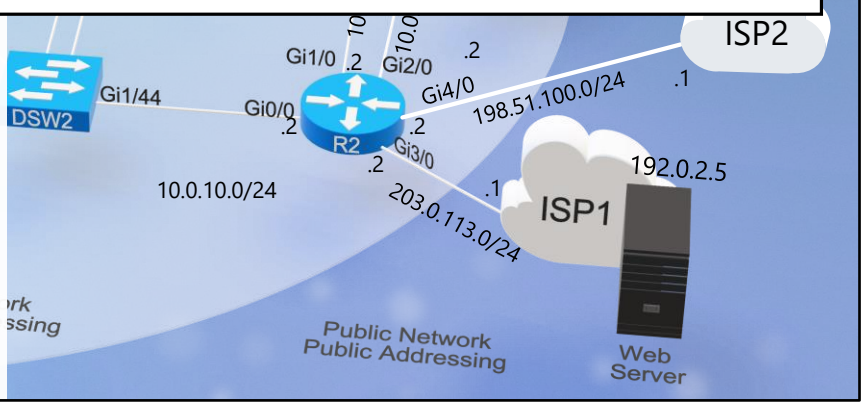
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Float
Routi

```
R2#configure terminal
R2(config)#interface gigabitEthernet 3/0
R2(config-if)#no shut
R2(config-if)#
%LINK-3-UPDOWN: Interface GigabitEthernet3/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet3/0, changed state to up
R2(config-if)#end
R2#
R2#show ip route
…output omitted…

Gateway of last resort is 203.0.113.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 203.0.113.1
…output omitted…
```

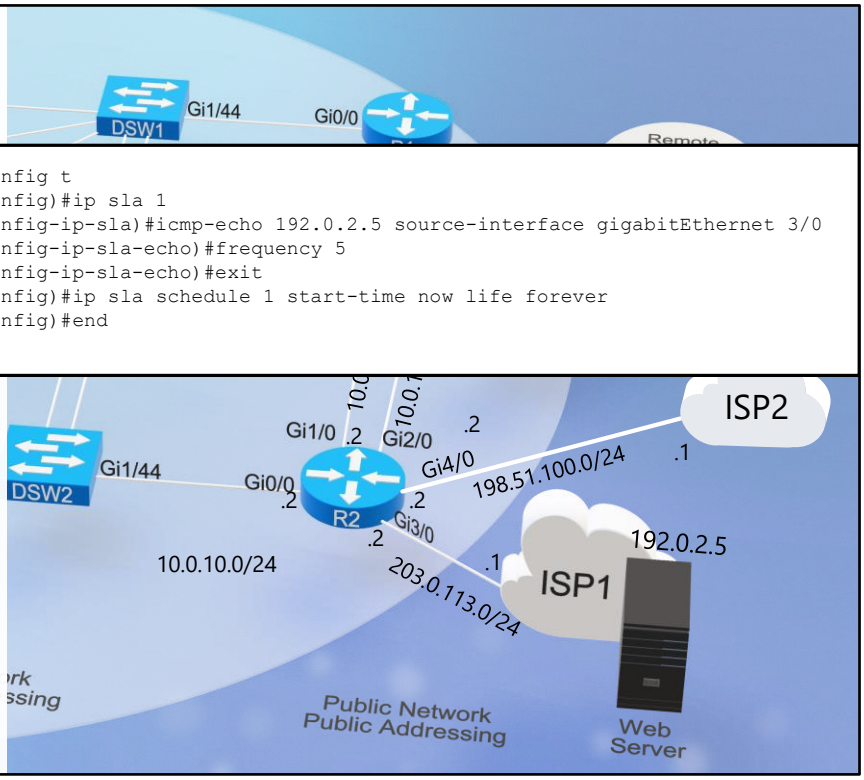


What is the problem with this scenario…. It only triggers if the local interface goes down. If the local interface does not go down then the failover does not happen.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

IPSLA and Floating Static Route

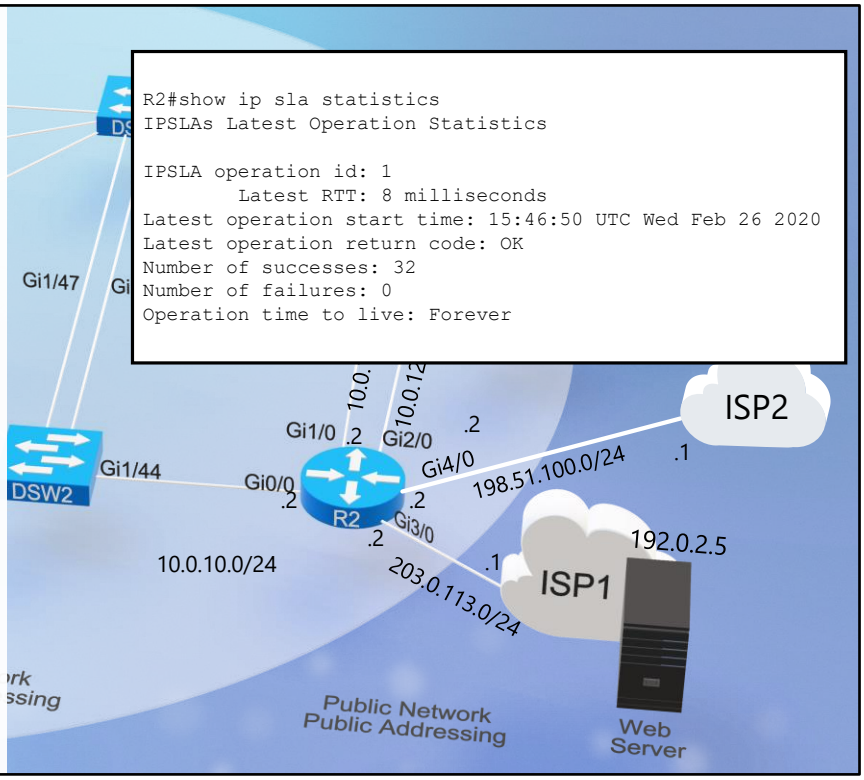
```
R2#config t
R2(config)#ip sla 1
R2(config-ip-sla)#icmp-echo 192.0.2.5 source-interface gigabitEthernet 3/0
R2(config-ip-sla-echo)#frequency 5
R2(config-ip-sla-echo)#exit
R2(config)#ip sla schedule 1 start-time now life forever
R2(config)#end
R2#
```



Create our probe….

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

IPSLA and Floating Static Route

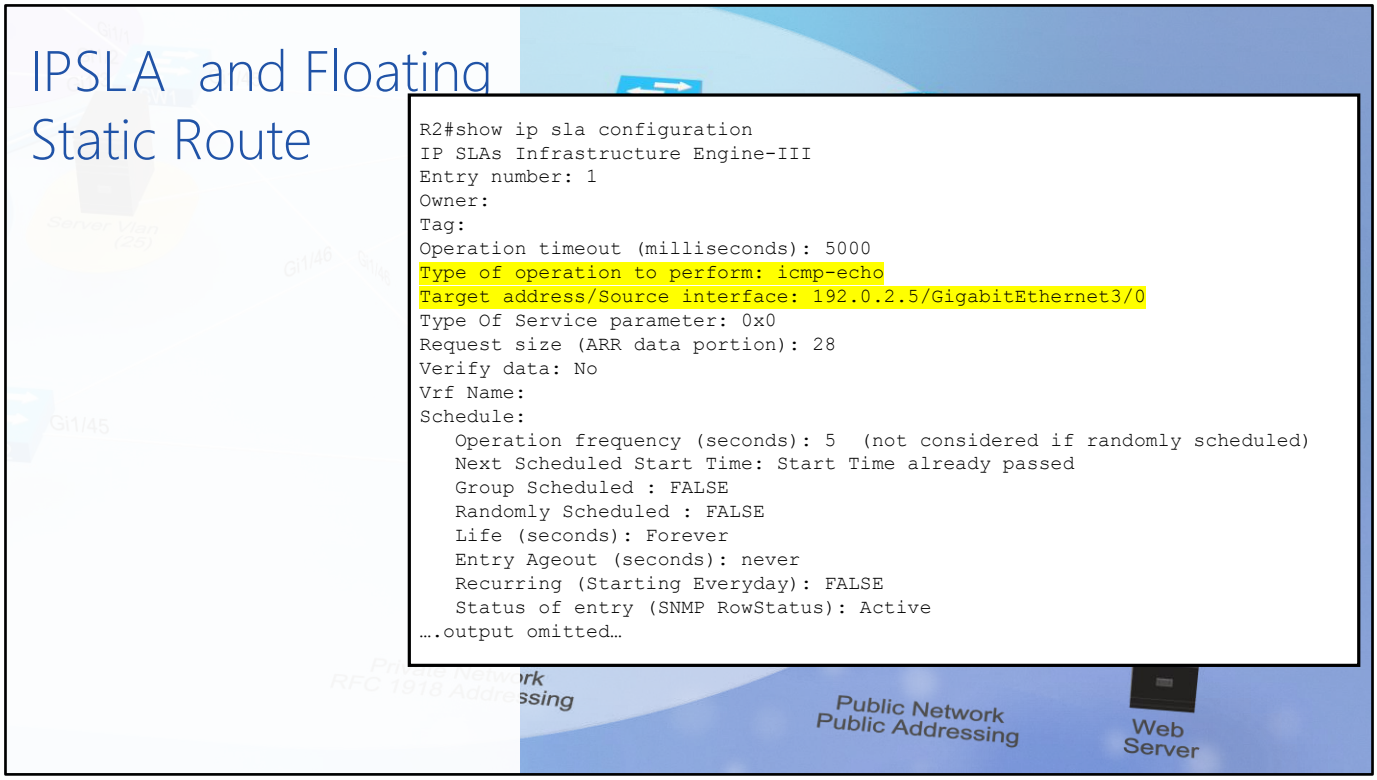


Create our probe….

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

IPSLA and Floating Static Route

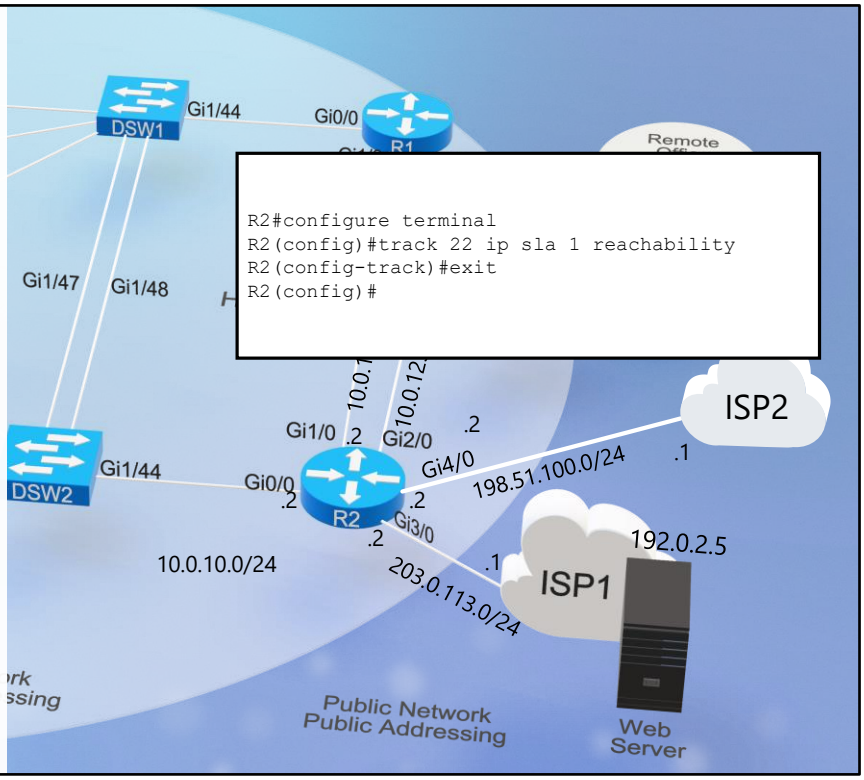
```
R2#show ip sla configuration
IP SLAs Infrastructure Engine-III
Entry number: 1
Owner:
Tag:
Operation timeout (milliseconds): 5000
Type of operation to perform: icmp-echo
Target address/Source interface: 192.0.2.5/GigabitEthernet3/0
Type Of Service parameter: 0x0
Request size (ARR data portion): 28
Verify data: No
Vrf Name:
Schedule:
   Operation frequency (seconds): 5  (not considered if randomly scheduled)
   Next Scheduled Start Time: Start Time already passed
   Group Scheduled : FALSE
   Randomly Scheduled : FALSE
   Life (seconds): Forever
   Entry Ageout (seconds): never
   Recurring (Starting Everyday): FALSE
   Status of entry (SNMP RowStatus): Active
….output omitted…
```



Create our probe….

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

IPSLA and Floating Static Route

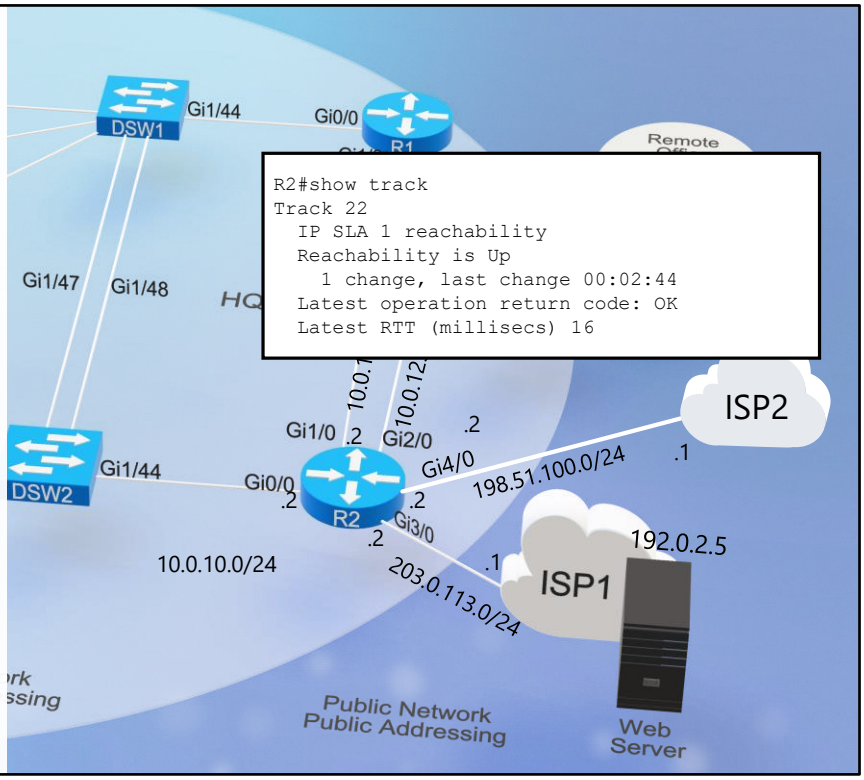


Create the tracking object that monitors the probe.

If probe is up… tracking object is up
If probe is down tracking object is down.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

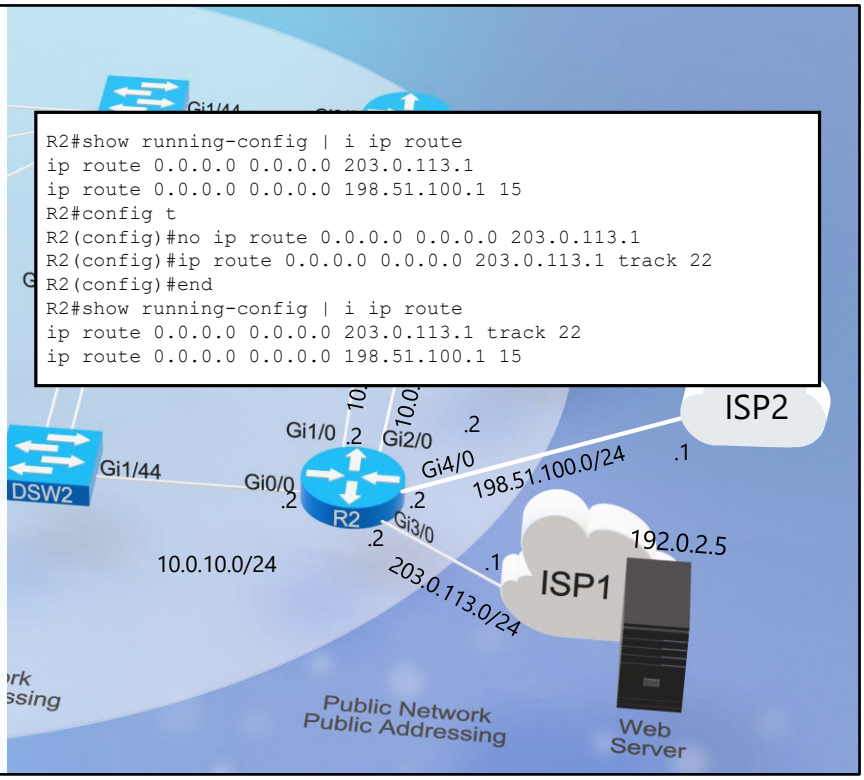
IPSLA and Floating Static Route



Create our probe….

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

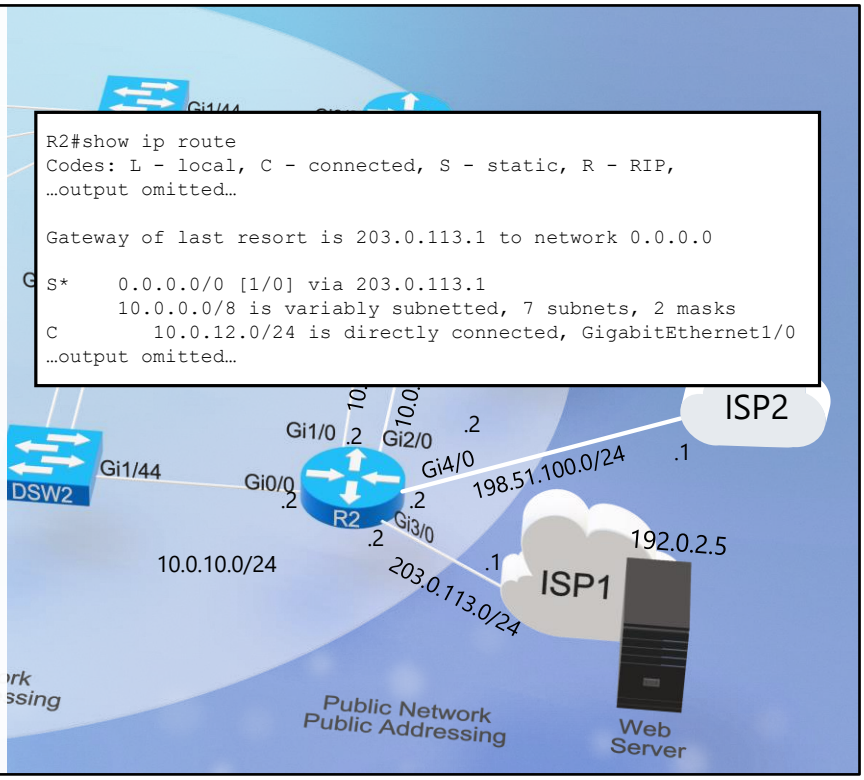
IPSLA and Floating Static Route



Create our probe….

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

IPSLA and Floating Static Route

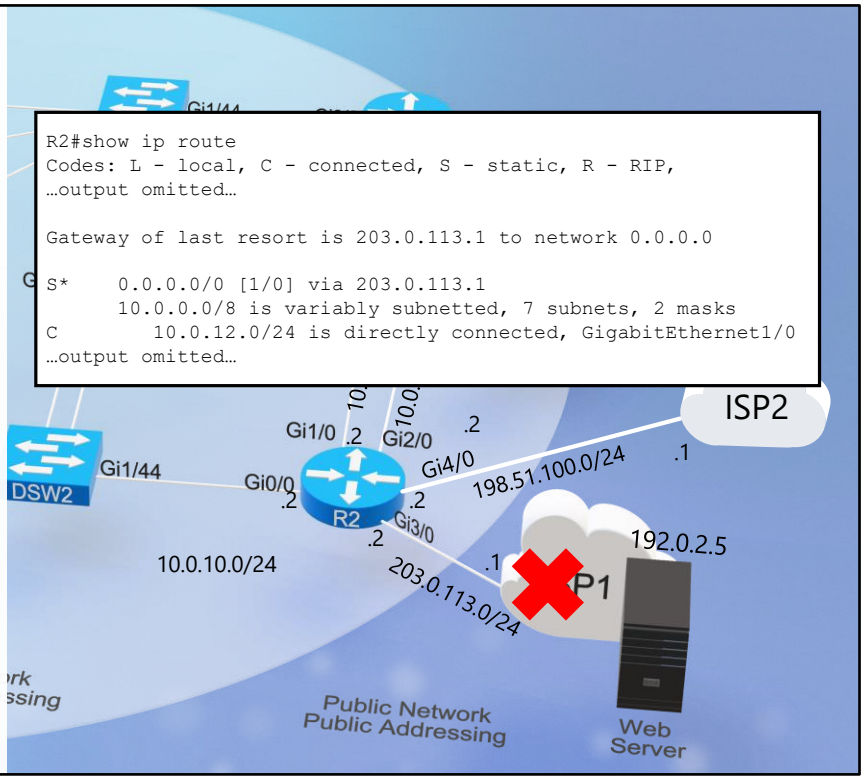


****exam****

Verify in real time with debug ip routing

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

IPSLA and Floating Static Route



****exam****

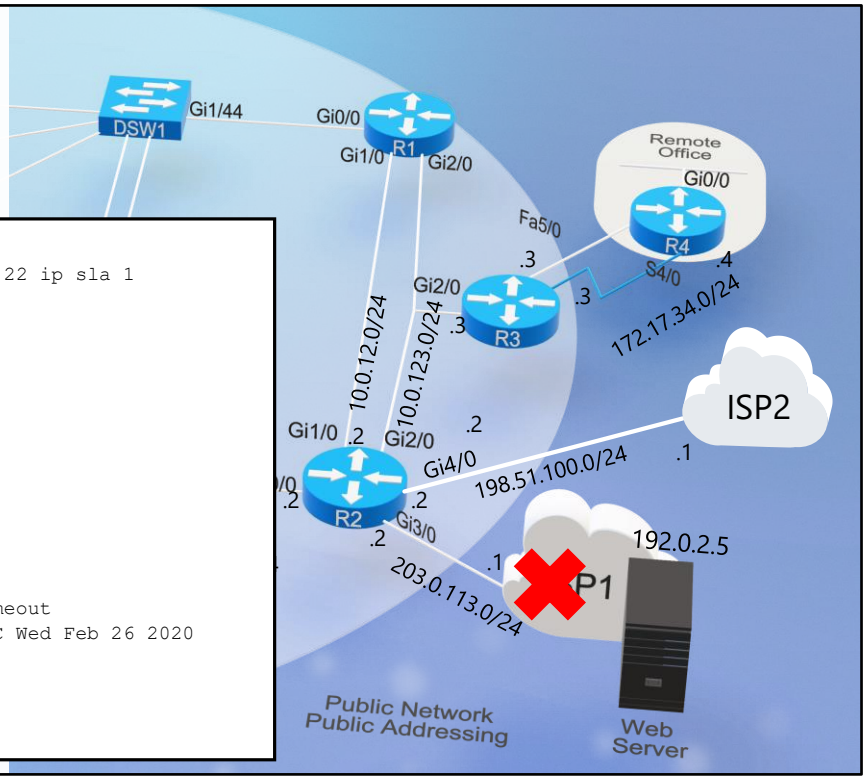
Verify in real time with debug ip routing

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

IPSLA and Floating Static Route

```
R2#
*Feb 26 15:59:09.211: %TRACKING-5-STATE: 22 ip sla 1
reachability Up->Down
R2#show track
Track 22
  IP SLA 1 reachability
  Reachability is Down
    2 changes, last change 00:00:16
  Latest operation return code: Timeout
  Tracked by:
    STATIC-IP-ROUTING 0
R2#show ip sla statistics
IPSLAs Latest Operation Statistics

IPSLA operation id: 1
        Latest RTT: NoConnection/Busy/Timeout
Latest operation start time: 15:59:20 UTC Wed Feb 26 2020
Latest operation return code: Timeout
Number of successes: 177
Number of failures: 3
Operation time to live: Forever
```

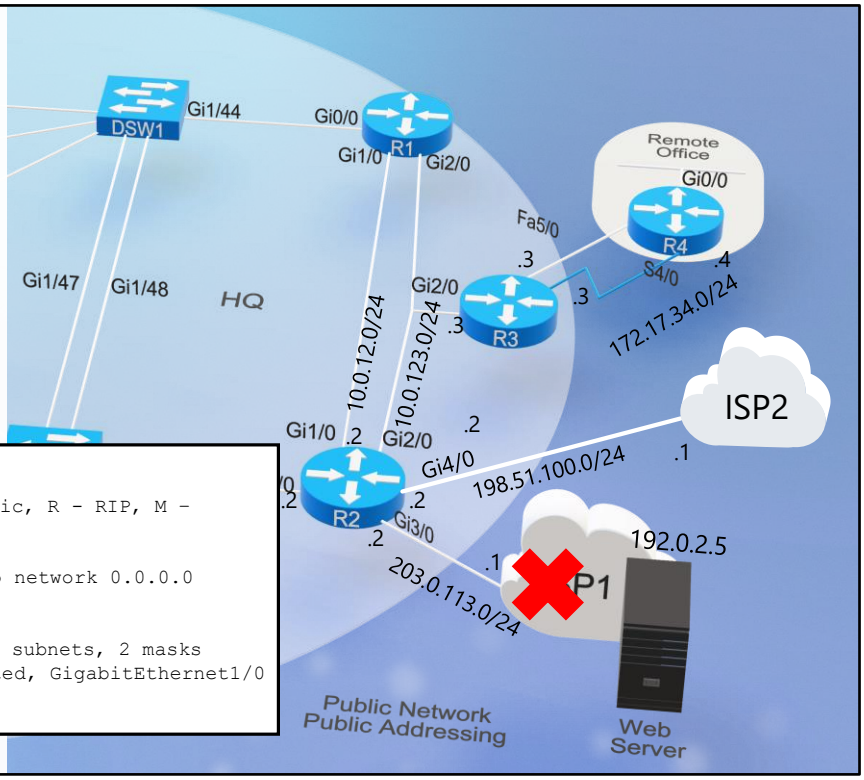


****exam****

Verify in real time with debug ip routing

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

IPSLA and Floating Static Route




```
R2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M -
…output omitted…

Gateway of last resort is 198.51.100.1 to network 0.0.0.0

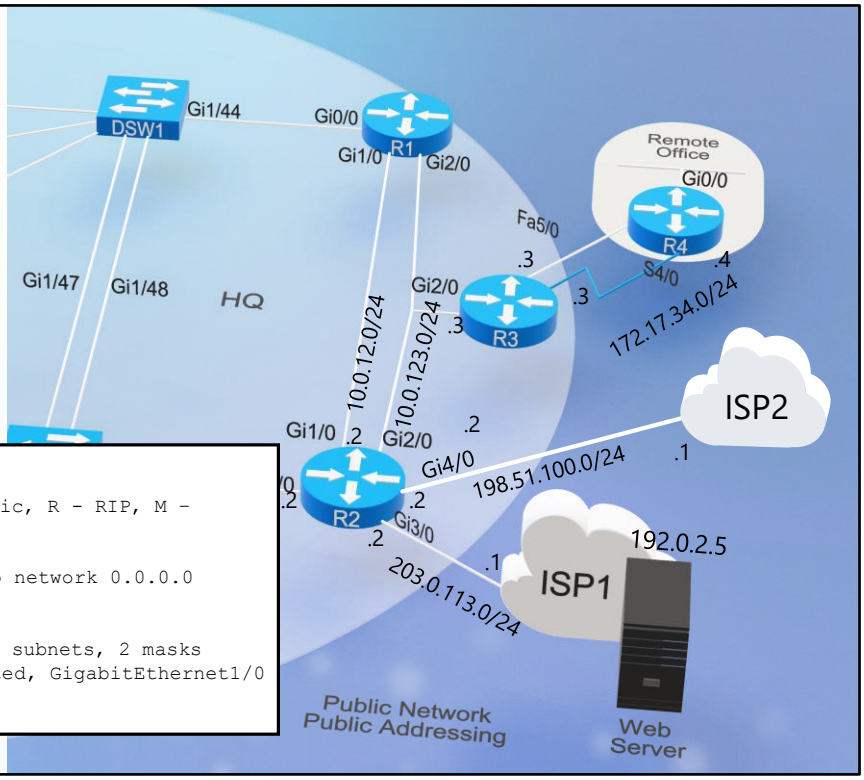
S*    0.0.0.0/0 [15/0] via 198.51.100.1
      10.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
C        10.0.12.0/24 is directly connected, GigabitEthernet1/0
…output omitted…
```

****exam****

Verify in real time with debug ip routing

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

IPSLA and Floating Static Route




```
R2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M -
…output omitted…

Gateway of last resort is 198.51.100.1 to network 0.0.0.0

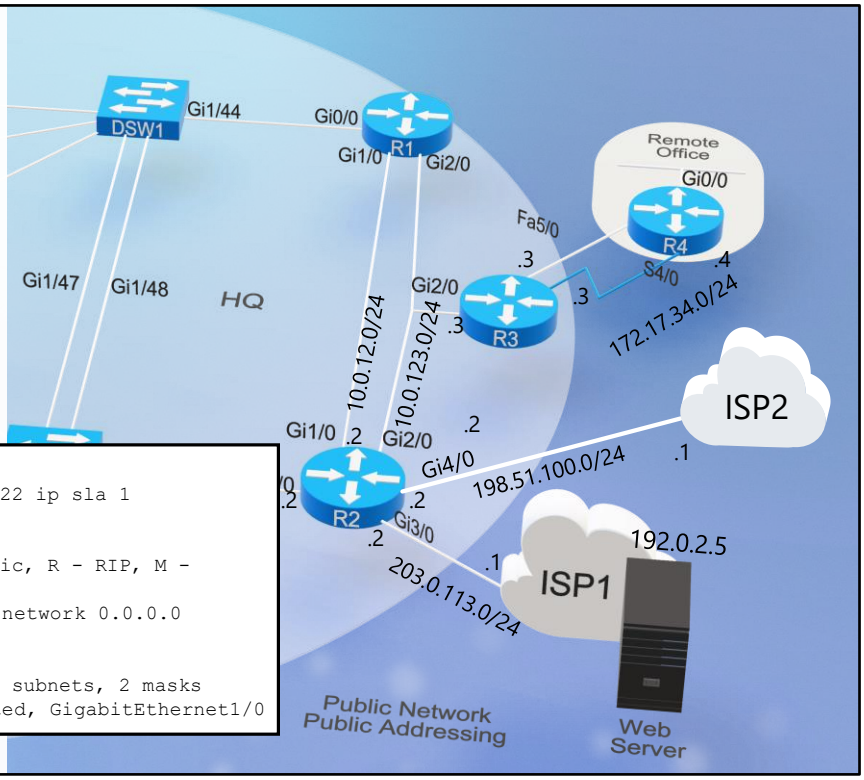
S*    0.0.0.0/0 [15/0] via 198.51.100.1
      10.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
C        10.0.12.0/24 is directly connected, GigabitEthernet1/0
…output omitted…
```

****exam****

Verify in real time with debug ip routing

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

IPSLA and Floating Static Route




```
R2#
*Feb 26 16:02:54.215: %TRACKING-5-STATE: 22 ip sla 1
reachability Down->Up
R2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M -
…output omitted…
Gateway of last resort is 203.0.113.1 to network 0.0.0.0

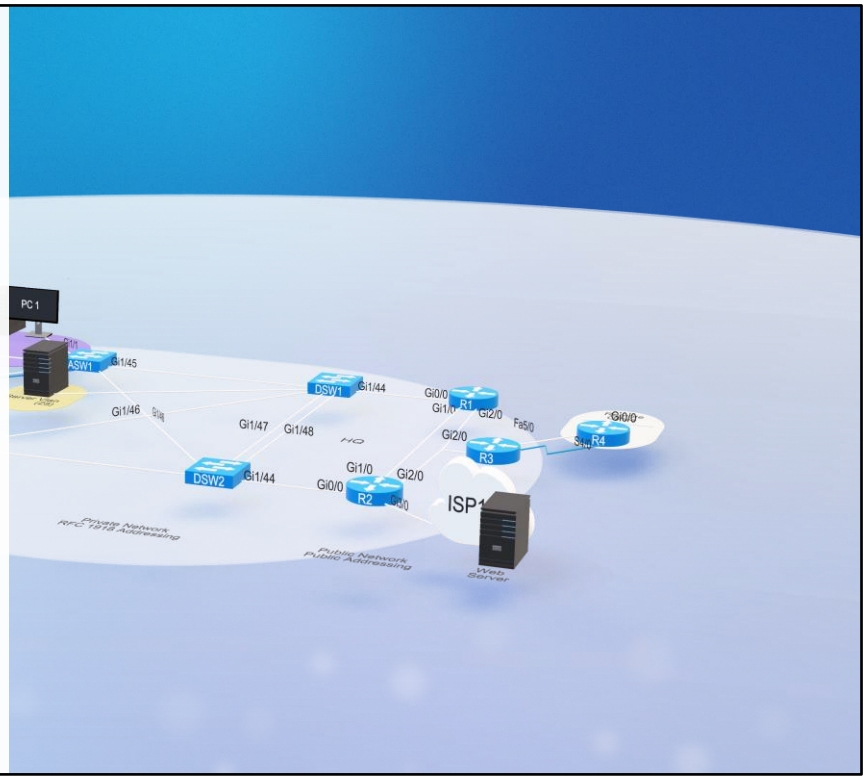
S*    0.0.0.0/0 [1/0] via 203.0.113.1
      10.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
C        10.0.12.0/24 is directly connected, GigabitEthernet1/0
```

****exam****

Verify in real time with debug ip routing

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

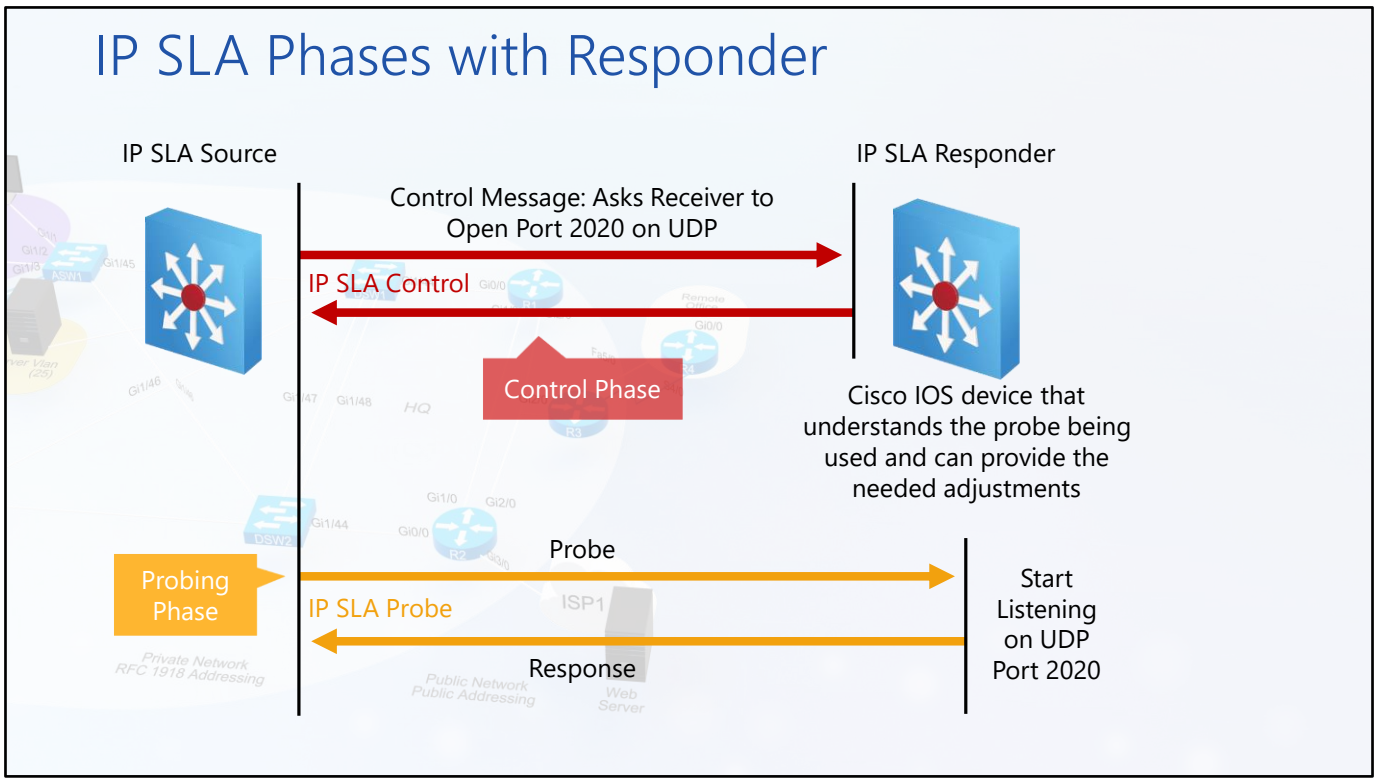
IPSLA and Floating Static Route



****exam****

Verify in real time with debug ip routing

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Responder is needed anytime you want hyper accurate measurements or when you need a device that understands the probe and make the needed adjustments.

For example: The IP Service Level Agreements (SLAs) UDP jitter operation diagnoses network suitability for real-time traffic applications such as VoIP, video over IP, or real-time conferencing. Jitter means inter-packet delay variance. When multiple packets are sent consecutively from a source to a destination, for example, 10 ms apart, and if the network is behaving ideally, the destination should receive the packets 10 ms apart. But if there are delays in the network (like queuing, arriving through alternate routes, and so on) the arrival delay between packets might be greater than or less than 10 ms. Using this example, a positive jitter value indicates that packets arrived greater than 10 ms apart. If packets arrive 12 ms apart, then positive jitter is 2 ms; if packets arrive 8 ms apart, negative jitter is 2 ms. For delay-sensitive networks like VoIP, positive jitter values are undesirable, and a jitter value of 0 is ideal.

UDP jitter operations are capable of measuring the following:
Per-direction jitter (source to destination and destination to source)
Per-direction packet loss
Per-direction delay (one-way delay)

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Round-trip delay (average round-trip time)

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipsla/configuration/xe-3e/sla-xe-3e-book/sla_udp_jitter.html

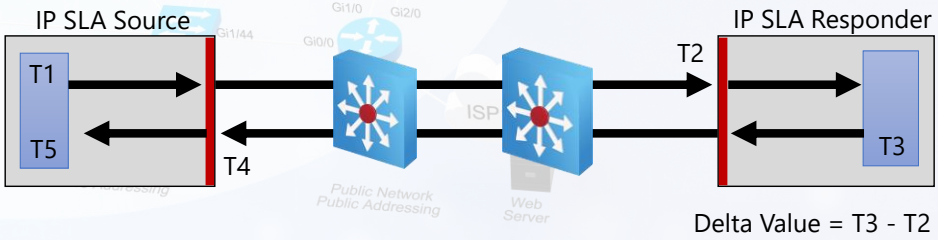
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Responder Time Stamps

The SLA responder utilizes two time stamps (T2 and T3).

The SLA responder factors out processing time, making results very accurate.

The SLA responder allows one-way measurements for latency, jitter, and packet loss.

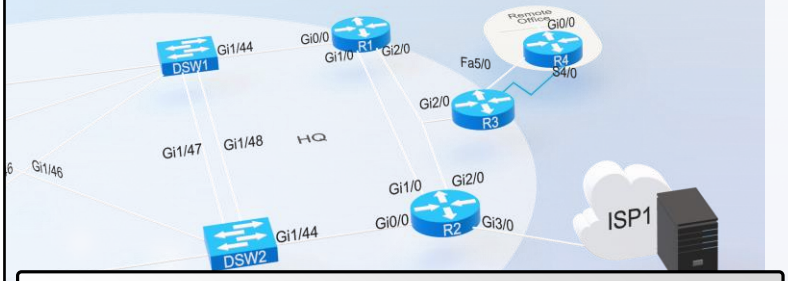


For this to work properly you need synchronized time. (NTP)

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

IP SLA with Responder

```
DSW1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DSW1(config)#ip sla 5
DSW1(config-ip-sla)#udp-jitter 192.168.4.4 7777
DSW1(config-ip-sla-jitter)#frequency 30
DSW1(config-ip-sla-jitter)#exit
DSW1(config)#ip sla schedule 5 start-time now life forever
DSW1(config)#end
DSW1#
```

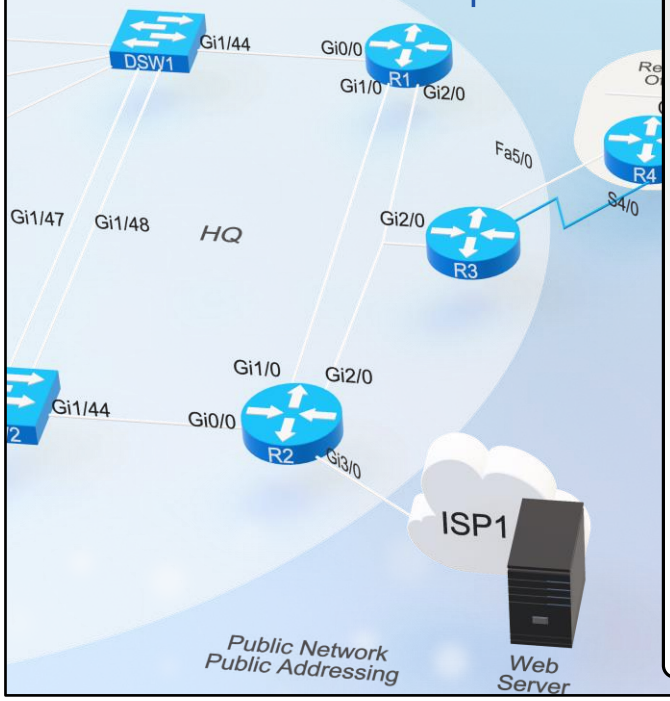



```
R4#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R4(config)#ip sla responder
```

Responder only needed to get more accurate info. In this case it would work without a responder configured but the statistics would not be as accurate.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

IP SLA with Responder

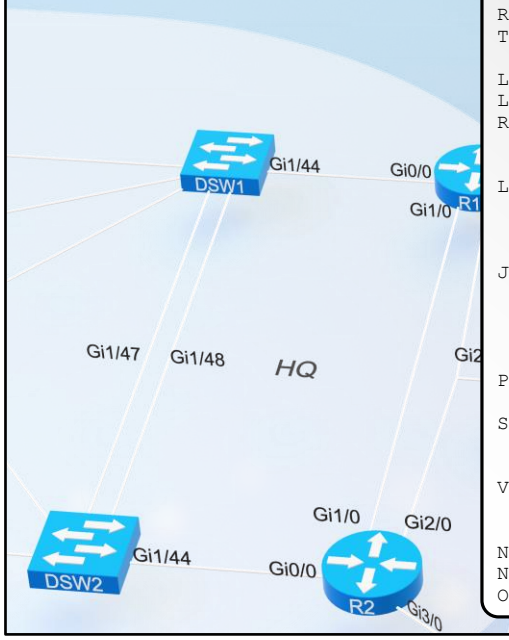



```
DSW1#show ip sla configuration 5
IP SLAs, Infrastructure Engine-II.

Entry number: 5
Owner:
Tag:
Type of operation to perform: udp-jitter
Target address/Source address: 192.168.4.4/0.0.0.0
Target port/Source port: 7777/0
Type Of Service parameter: 0x0
Request size (ARR data portion): 32
Operation timeout (milliseconds): 5000
Packet Interval (milliseconds)/Number of packets: 20/10
Verify data: No
Vrf Name:
Control Packets: enabled
Schedule:
    Operation frequency (seconds): 30
    Next Scheduled Start Time: Start Time already passed
    Group Scheduled : FALSE
    Randomly Scheduled : FALSE
    Life (seconds): Forever
    Entry Ageout (seconds): never
    Recurring (Starting Everyday): FALSE
    Status of entry (SNMP RowStatus): Active
Threshold (milliseconds): 5000
Distribution Statistics:
    Number of statistic hours kept: 2
    Number of statistic distribution buckets kept: 1
    Statistic distribution interval (milliseconds): 20
Enhanced History:
```

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

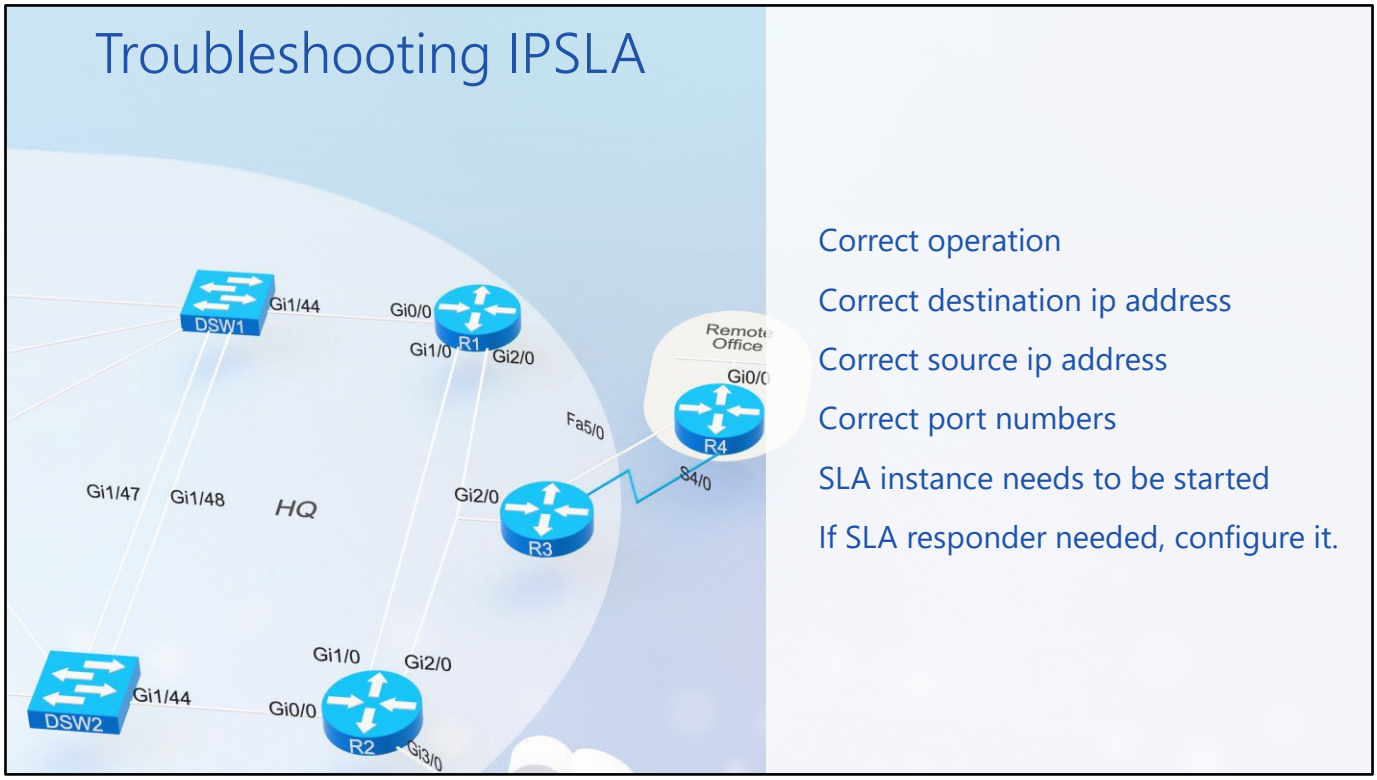
IP SLA with Responder




```
DSW1#show ip sla statistics 5

Round Trip Time (RTT) for       Index 5
Type of operation: jitter
        Latest RTT: 41 ms
Latest operation start time: 07:34:23.392 UTC Tue Sep 24 2019
Latest operation return code: OK
RTT Values
        Number Of RTT: 10
        RTT Min/Avg/Max: 30/41/58 ms
Latency one-way time milliseconds
        Number of Latency one-way Samples: 7
        Source to Destination Latency one way Min/Avg/Max: 28/36/43 ms
        Destination to Source Latency one way Min/Avg/Max: 1/6/23 ms
Jitter time milliseconds
        Number of SD Jitter Samples: 9
        Number of DS Jitter Samples: 9
        Source to Destination Jitter Min/Avg/Max: 0/6/15 ms
        Destination to Source Jitter Min/Avg/Max: 1/9/25 ms
Packet Loss Values
        Loss Source to Destination: 0           Loss Destination to
Source: 0
        Out Of Sequence: 0      Tail Drop: 0
        Packet Late Arrival: 0  Packet Skipped: 0
Voice Score Values
        Calculated Planning Impairment Factor (ICPIF): 0
        Mean Opinion Score (MOS): 0
Number of successes: 7
Number of failures: 0
Operation time to live: Forever
```

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



When troubleshooting Cisco IOS IP SLA, consider the following:

■ The correct operation needs to be chosen for the metrics you intend to measure.

■ The destination IP address needs to be reachable and correctly defined.

■ The source IP address needs to be reachable from the destination and correctly defined.

■ Any necessary port numbers need to be correctly identified.

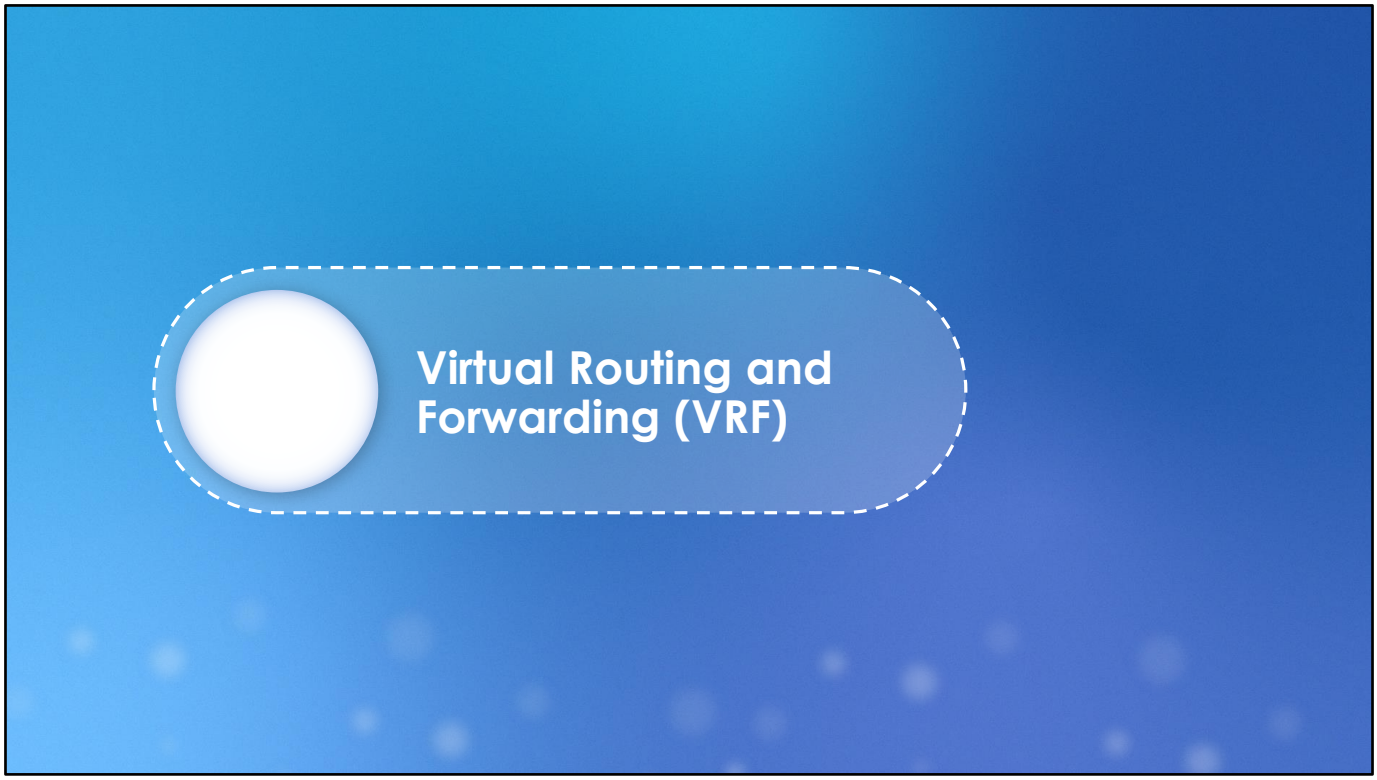
■ The SLA instance needs to be started.

■ If the operation needs an IP SLA responder, one must be configured and reachable

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

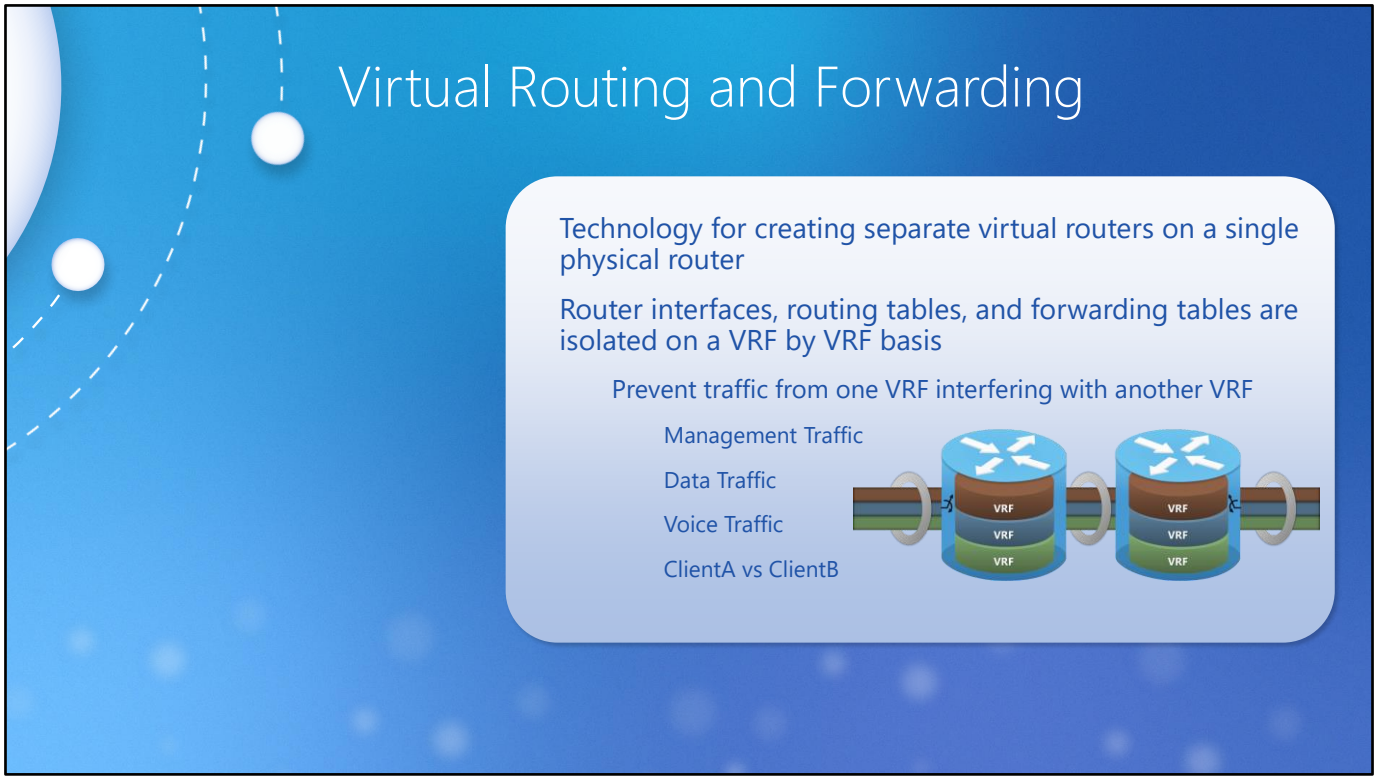


©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



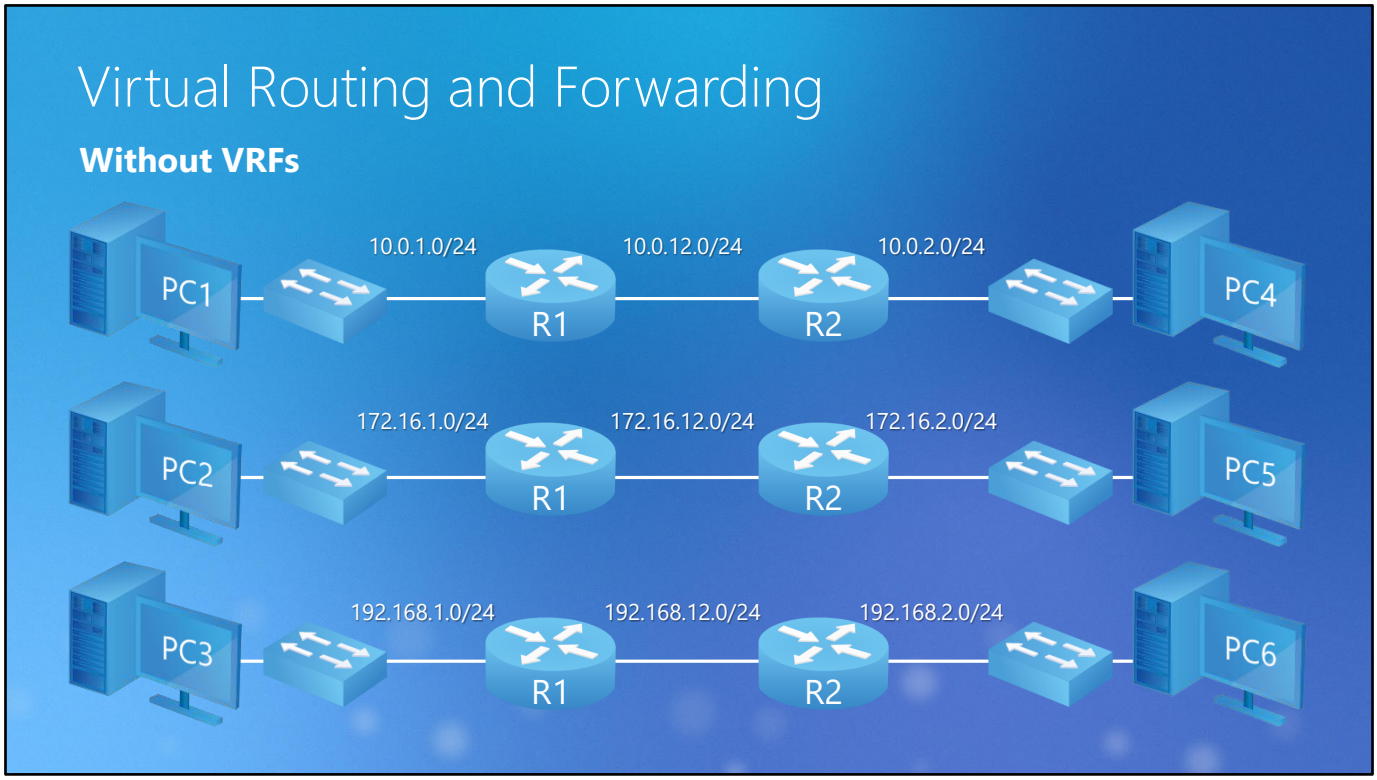
Title slide

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



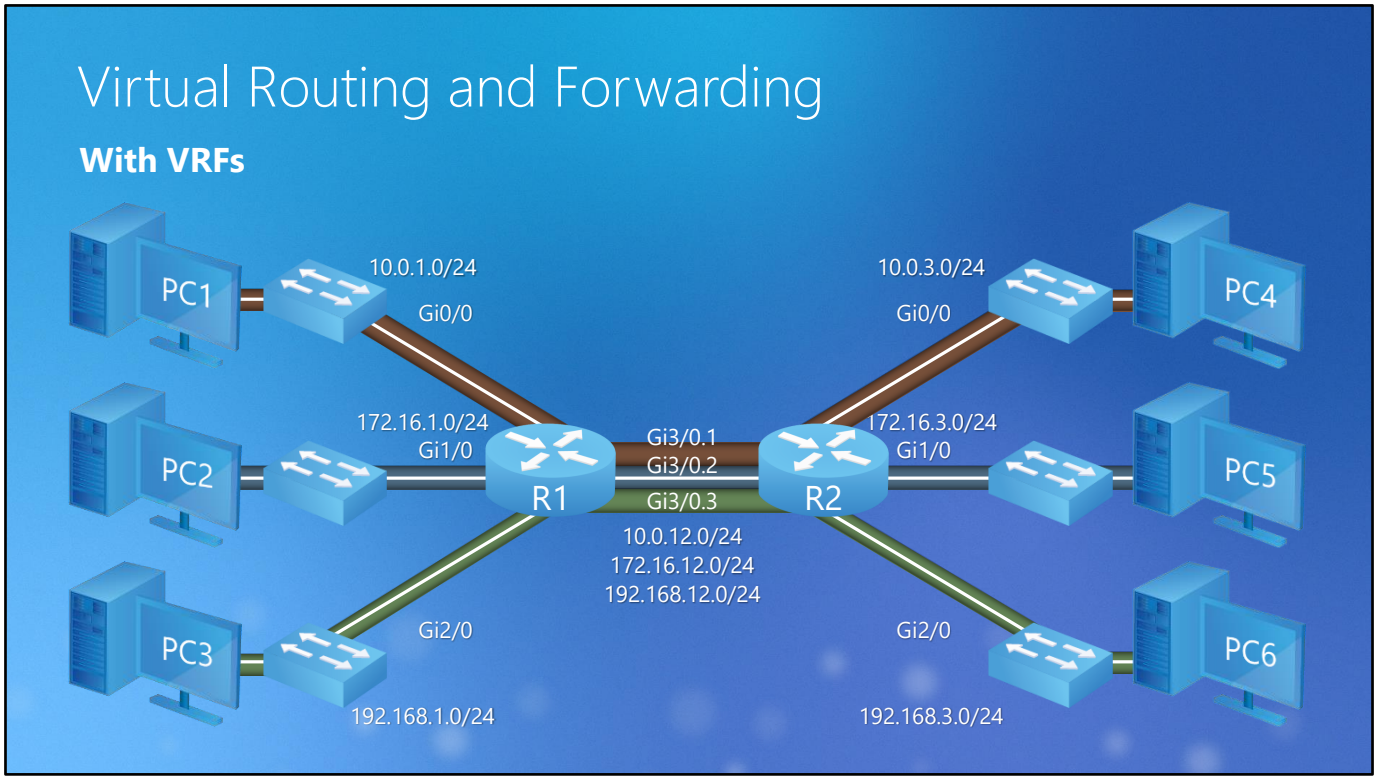
Why might you want to divide up your physical router into multiple virtual routers? Consider this scenario as a possible reason. Let's say for security reasons you need to build three different networks so that traffic in each network is isolated from the other. However, you only want to build a single physical network to accomplish this. With VRFs you would be able to do this. Here we have a single physical topology that is divided into three different logically isolated networks. For simplicity sakes we have called them the RED, GREEN, and BLUE networks.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



This is what we would need to do if VRFs did not exist

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

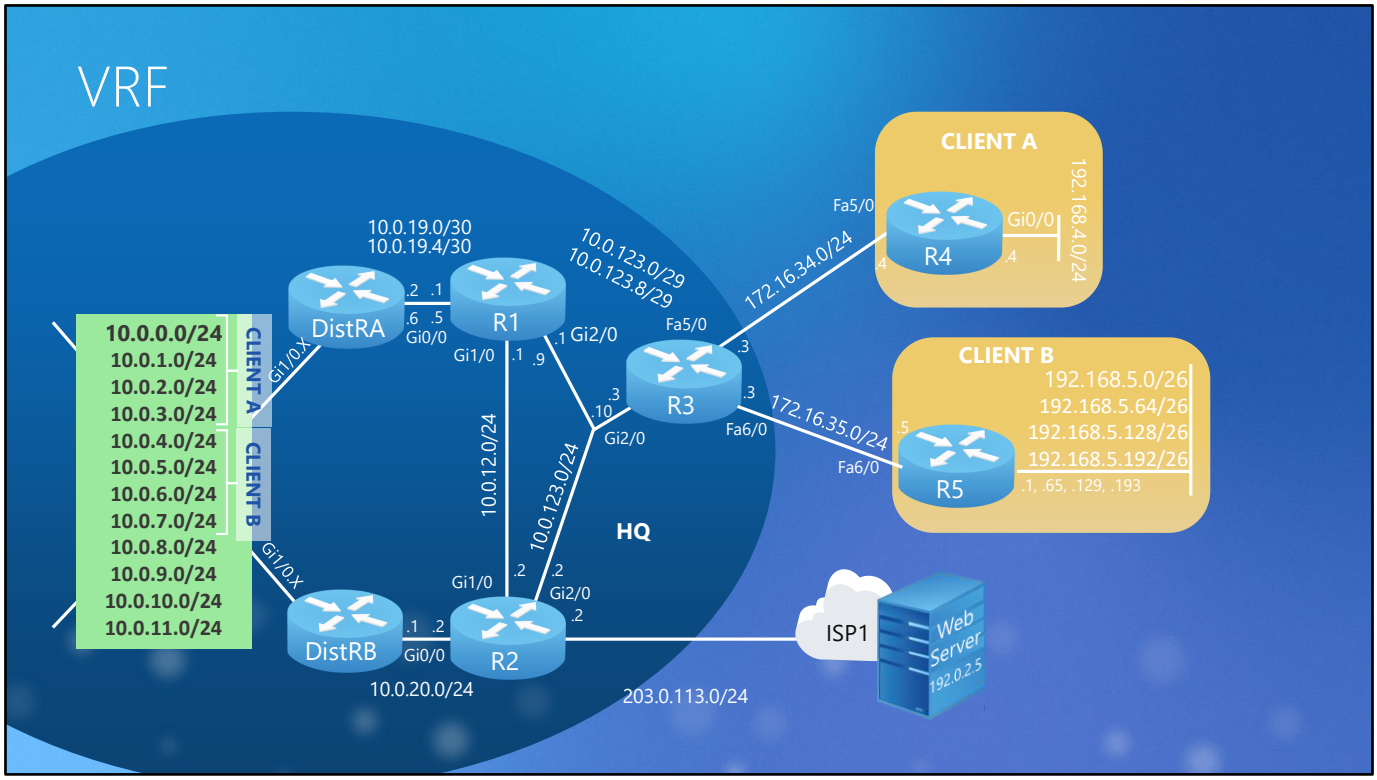


Instructor Notes:

This is what we can do with VRFs

The RED network is using the 10.0.0.0/8 addressing space, the GREEN network is using the 172.16.0.0/16 addressing space, and the BLUE network is using the 192.168.0.0/16 addressing space. With VRF-Lite we can isolate the traffic within the respective virtual networks and have multiple virtual routing tables on each router dedicated to the respective VRF.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Let's create 2 VRFs one for CLIENTA and one for CLIENTB.

VRF CLIENTA
10.0.0.0/24
10.0.1.0/24
10.0.2.0/24
10.0.3.0/24
10.0.19.0/30
10.0.123.0/29
172.16.34.0/30
192.168.4.0/24

VRF CLIENTB
10.0.4.0/24
10.0.5.0/24
10.0.6.0/24
10.0.7.0/24
10.0.19.4/30
10.0.123.8/29

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

172.16.34.4/30
10.0.44.0/24

****

DISTRA

```
vrf definition CLIENTA
                address-family ipv4
vrf definition CLIENTB
                address-family ipv4

interface gig 1/0.10
vrf forwarding CLIENTA
ip address 10.0.0.1 255.255.255.0
no shut

interface gig 1/0.11
vrf forwarding CLIENTA
ip address 10.0.1.1 255.255.255.0
no shut

interface gig 1/0.12
vrf forwarding CLIENTA
ip address 10.0.2.1 255.255.255.0
no shut

interface gig 1/0.13
vrf forwarding CLIENTA
ip address 10.0.3.1 255.255.255.0
no shut

interface gig 1/0.14
vrf forwarding CLIENTB
ip address 10.0.4.1 255.255.255.0
no shut

interface gig 1/0.15
vrf forwarding CLIENTB
ip address 10.0.5.1 255.255.255.0
no shut
```

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

```
interface gig 1/0.16
vrf forwarding CLIENTB
ip address 10.0.6.1 255.255.255.0
no shut

interface gig 1/0.17
vrf forwarding CLIENTB
ip address 10.0.7.1 255.255.255.0
no shut

interface gig 0/0
no ip address

interface gig 0/0.100
encap dot1q 100
vrf forwarding CLIENTA
ip address 10.0.19.2 255.255.255.252
no shut

interface gig 0/0.200
encap dot1q 200
vrf forwarding CLIENTB
ip address 10.0.19.6 255.255.255.252
no shut

**************************
R1

vrf definition CLIENTA
                address-family ipv4
vrf definition CLIENTB
                address-family ipv4

interface GigabitEthernet0/0
 no ip address

interface GigabitEthernet0/0.100
 encapsulation dot1Q 100
 vrf forwarding CLIENTA
 ip address 10.0.19.1 255.255.255.252
 no shut
```

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

```
interface GigabitEthernet0/0.200
 encapsulation dot1Q 200
 vrf forwarding CLIENTB
 ip address 10.0.19.5 255.255.255.252
 no shut

interface GigabitEthernet2/0
 no ip address

interface GigabitEthernet2/0.100
 encapsulation dot1Q 100
 vrf forwarding CLIENTA
 ip address 10.0.123.1 255.255.255.248
 no shut

interface GigabitEthernet2/0.200
 encapsulation dot1Q 200
 vrf forwarding CLIENTB
 ip address 10.0.123.9 255.255.255.248
 no shut

**********
R3

vrf definition CLIENTA
                address-family ipv4
vrf definition CLIENTB
                address-family ipv4

interface fa5/0
 vrf forwarding CLIENTA
 ip address 172.16.34.3 255.255.255.0
 no shut

interface fa6/0
 vrf forwarding CLIENTB
 ip address 172.16.35.3 255.255.255.0
 no shut

interface GigabitEthernet2/0
 no ip address
```

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

```
interface GigabitEthernet2/0.100
 encapsulation dot1Q 100
 vrf forwarding CLIENTA
 ip address 10.0.123.3 255.255.255.248
 no shut

interface GigabitEthernet2/0.200
 encapsulation dot1Q 200
 vrf forwarding CLIENTB
 ip address 10.0.123.10 255.255.255.248
 no shut
```

****

R4

Nothing to do in my case because they are using their global routing table.

****

R5

Nothing to do in my case because they are using their global routing table.

****

Routing
EIGRP NAMED EXAMPLE

R4:

```
router eigrp CLIENTA
 address-family ipv4 unicast autonomous-system 100
  network 172.16.34.4 0.0.0.0
  network 192.168.4.4 0.0.0.0
```

R5:

```
router eigrp CLIENTB
 address-family ipv4 unicast autonomous-system 200
  network 172.16.35.5 0.0.0.0
  network 192.168.5.0 0.0.0.255
```

R3:

```
router eigrp ENARSI_VRF
```

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

```
 address-family ipv4 unicast vrf CLIENTA autonomous-system 100
  network 10.0.123.3 0.0.0.0
  network 172.16.34.3 0.0.0.0
 address-family ipv4 unicast vrf CLIENTB autonomous-system 200
  network 10.0.123.10 0.0.0.0
  network 172.16.35.3 0.0.0.0
```

R1:

```
router eigrp ENARSI_VRF
 address-family ipv4 unicast vrf CLIENTA autonomous-system 100
  network 10.0.19.1 0.0.0.0
  network 10.0.123.1 0.0.0.0
 address-family ipv4 unicast vrf CLIENTB autonomous-system 200
  network 10.0.19.5 0.0.0.0
  network 10.0.123.9 0.0.0.0
```

DISTRA:

```
router eigrp ENARSI_VRF
 address-family ipv4 unicast vrf CLIENTA autonomous-system 100
  network 10.0.0.1 0.0.0.0
  network 10.0.1.1 0.0.0.0
  network 10.0.2.1 0.0.0.0
  network 10.0.3.1 0.0.0.0
  network 10.0.19.2 0.0.0.0
 address-family ipv4 unicast vrf CLIENTB autonomous-system 200
  network 10.0.4.1 0.0.0.0
  network 10.0.5.1 0.0.0.0
  network 10.0.6.1 0.0.0.0
  network 10.0.7.1 0.0.0.0
  network 10.0.19.6 0.0.0.0
```

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



2.1 Describe MPLS operations (LSR, LDP, label switching, LSP)

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Traditional IP Routing Review

Routers share IP prefixes with each other using routing protocols such as OSPF, EIGRP, IS-IS

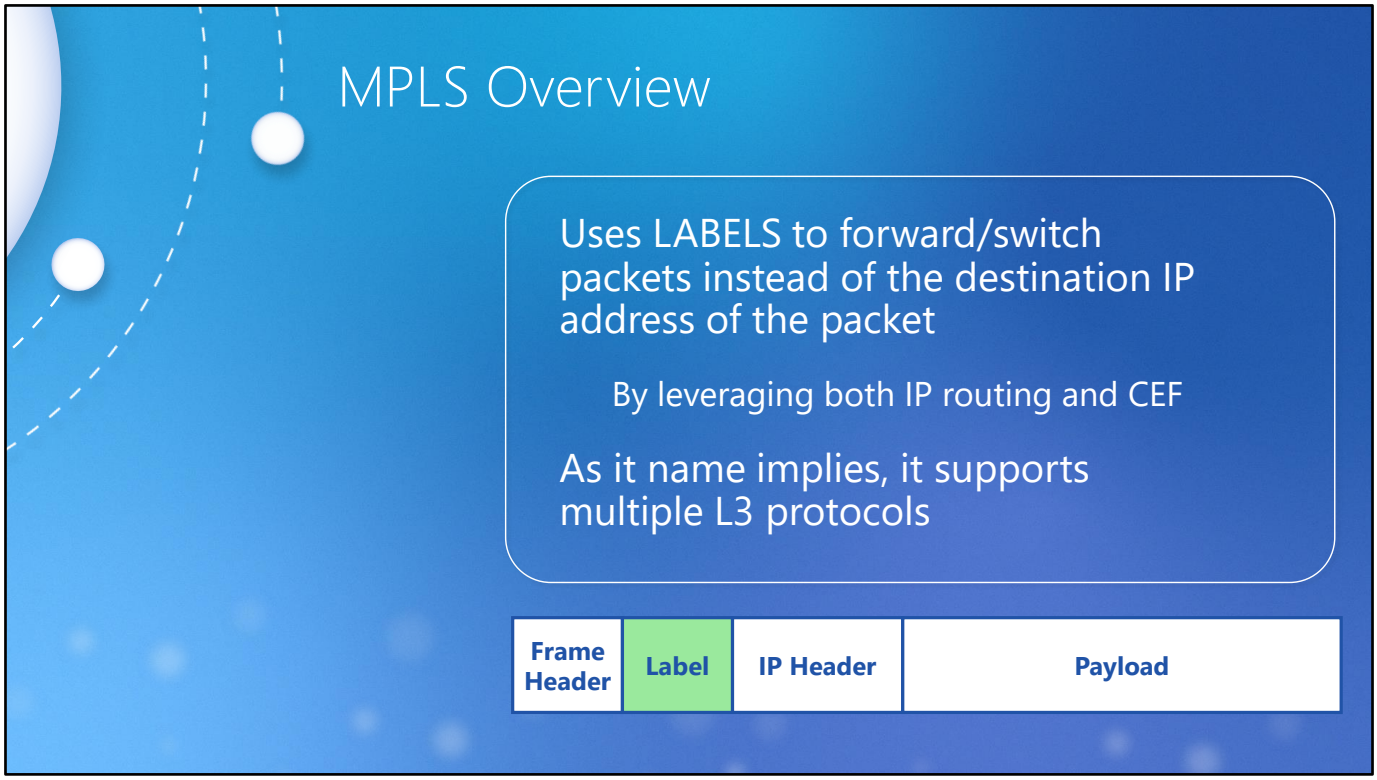
The best route to reach the prefix is installed in the RIB and the FIB

Packet forwarding is based on the destination IP address listed in the packet

- Every router analyzes the L3 header of each packet
- They compare the results to the FIB and find the best match
- They forward the packet out the interface listed in the FIB



©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

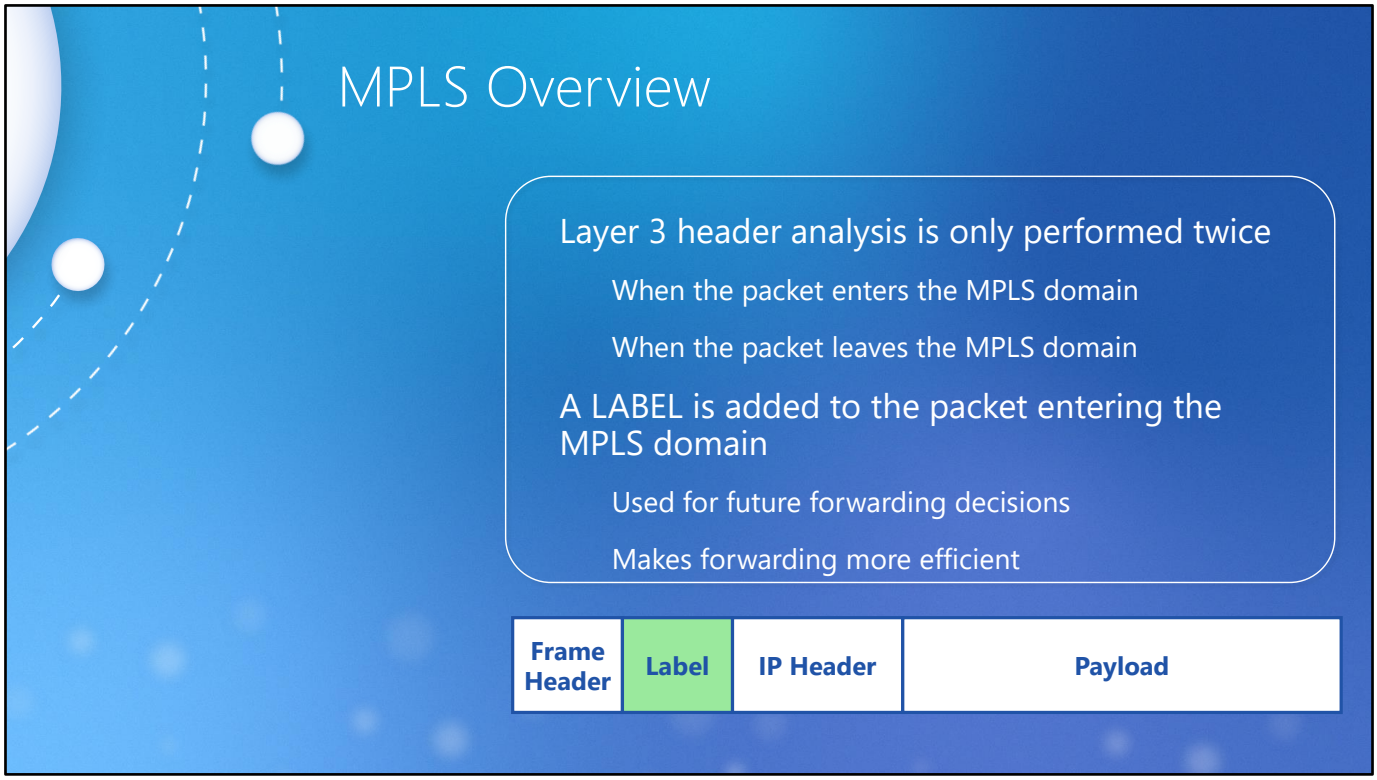


MPLS stands for Multiprotocol Label Switching. It is a routing technique in telecommunications networks that directs data from one node to the next based on short path labels rather than long network addresses, avoiding complex lookups in a routing table and speeding up traffic flows. The labels identify virtual links (paths) between distant nodes rather than endpoints.

MPLS operates at a layer that is considered to lie between traditional definitions of Layer 2 (data link layer) and Layer 3 (network layer), and thus is often referred to as a "layer 2.5 protocol." It was designed to provide a unified data-carrying service for both circuit-based clients and packet-switching clients which provide a datagram service model.

It can be used to carry many different kinds of traffic, including IP packets, as well as native ATM, SONET, and Ethernet frames.

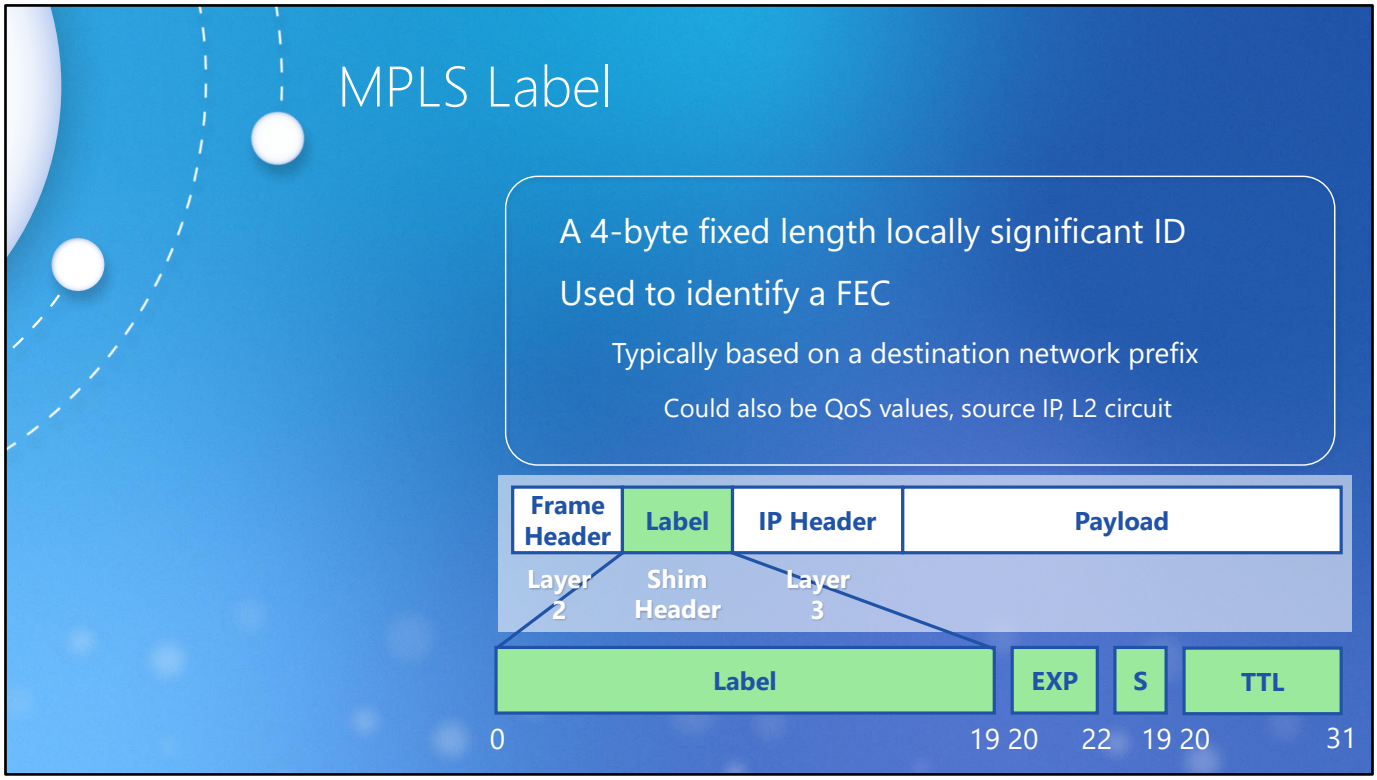
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Read the slide…. Than…

Here are the key features and benefits of MPLS:
1.Efficiency: MPLS increases routing efficiency and speeds up the traffic flow by making forwarding decisions based on labels rather than routing table lookups.
2.Flexibility: It supports different types of data transport and services, such as IP, ATM, and Frame Relay.
3.Scalability: MPLS is scalable to handle high-speed connections and a large number of nodes.
4.Quality of Service (QoS): It allows for the definition of QoS policies, enabling traffic prioritization and bandwidth allocation to different types of traffic, which is critical for voice over IP (VoIP) and multimedia applications.
5.Traffic Engineering: MPLS gives network operators the ability to direct and control traffic flows through the network, optimizing network performance and resource utilization.
MPLS is widely used in carrier networks and large enterprise networks for these reasons, enabling efficient and flexible data transport over a wide variety of technologies.

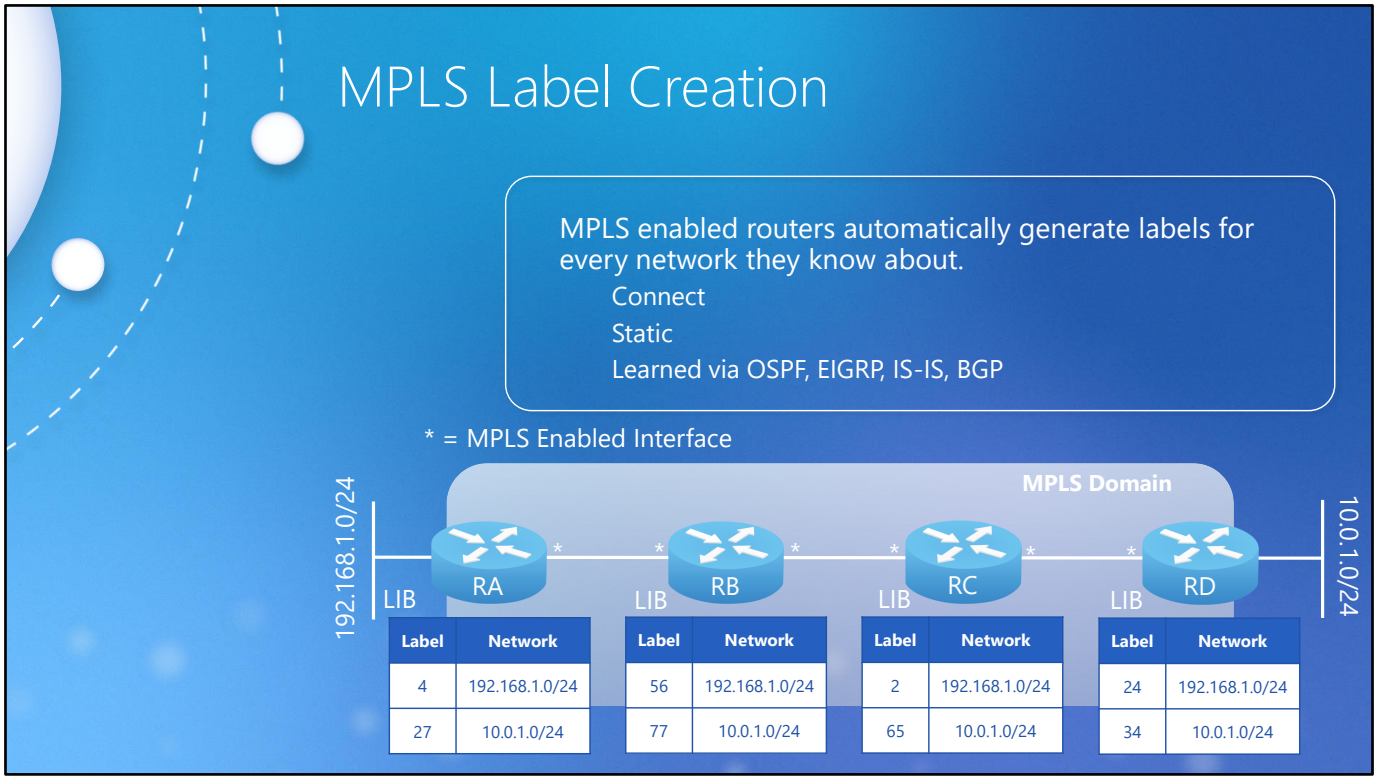
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



FEC = Forwarding Equivalence Class which is a group of packets that are forwarded in the same manner, over the same path, and with the same forwarding treatment.

EXAM
20-bit label: the label number
3-bit experimental field: used for QoS (CoS and IP precedence values)
Bottom-of-stack bit: identifies if this is the last label or not (MPLS VPNs use multiple labels which is known as a label stack. So if you have two labels, the first label would have the S bit set to 0 which means it is not the last label and the second label would have the S bit set to 1 which means it is the last label.)
8-bit TTL field: time to live just like the IP header and is used to prevent indefinite routing loops.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



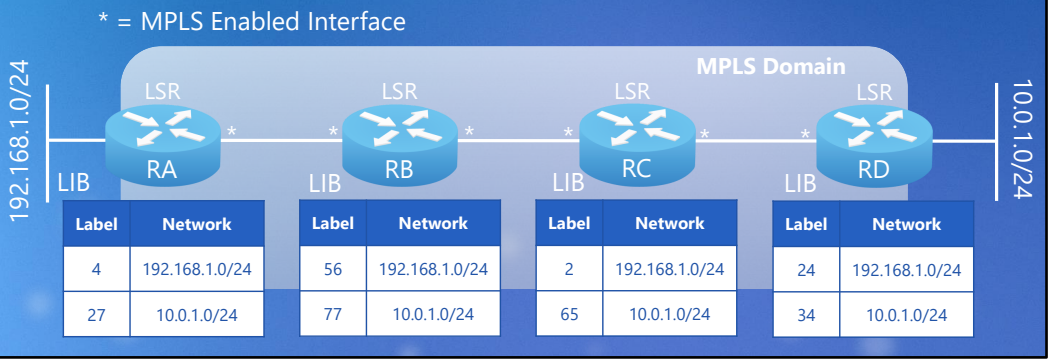
This is done as soon as you enable MPLS on interfaces.

RA gave a label of 4 to 192.168.1.0/24 and a label of 27 to 10.0.1.0/24.
RB gave …
RC gave …
RD gave …

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

MPLS Label Switch Routers

A router that supports MPLS
Receives and transmits MPLS labeled packets



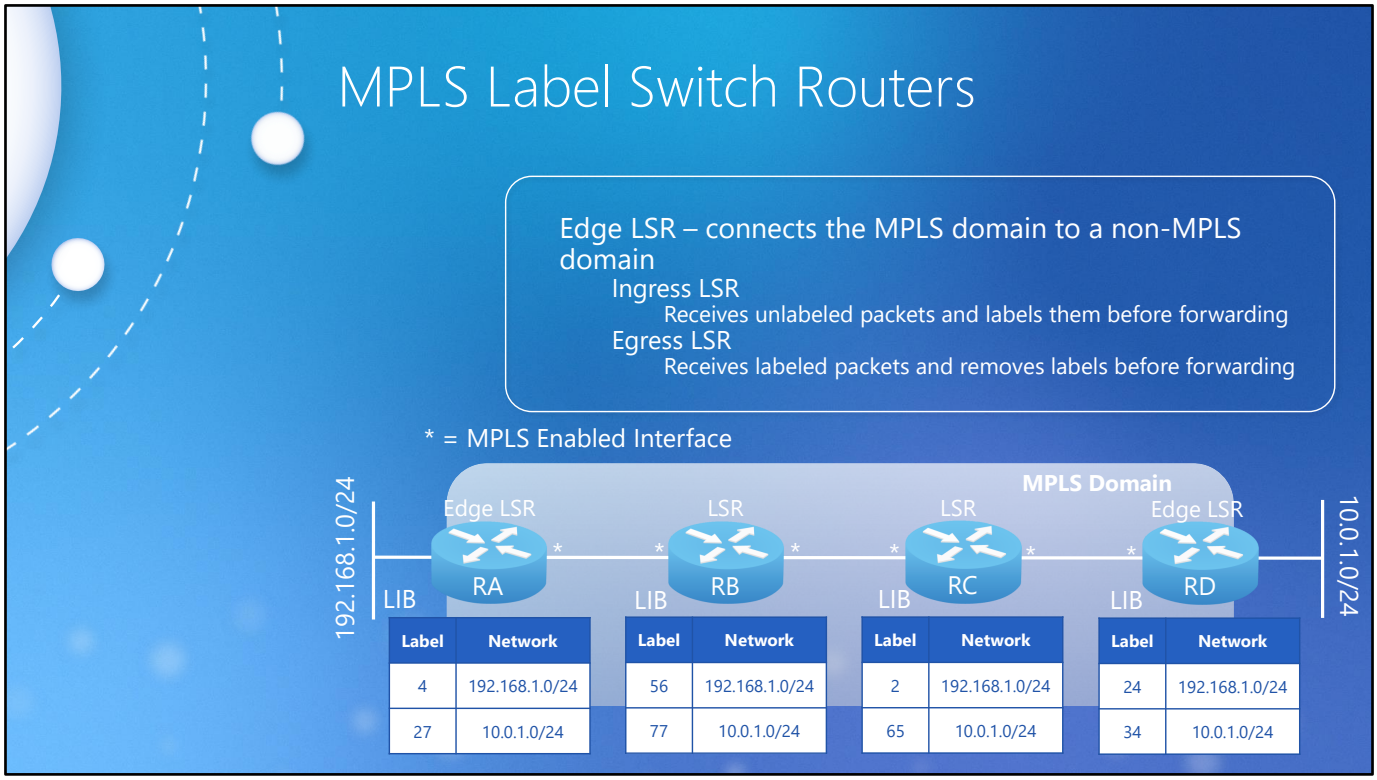
Label	Network
4	192.168.1.0/24
27	10.0.1.0/24

Label	Network
56	192.168.1.0/24
77	10.0.1.0/24

Label	Network
2	192.168.1.0/24
65	10.0.1.0/24

Label	Network
24	192.168.1.0/24
34	10.0.1.0/24

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



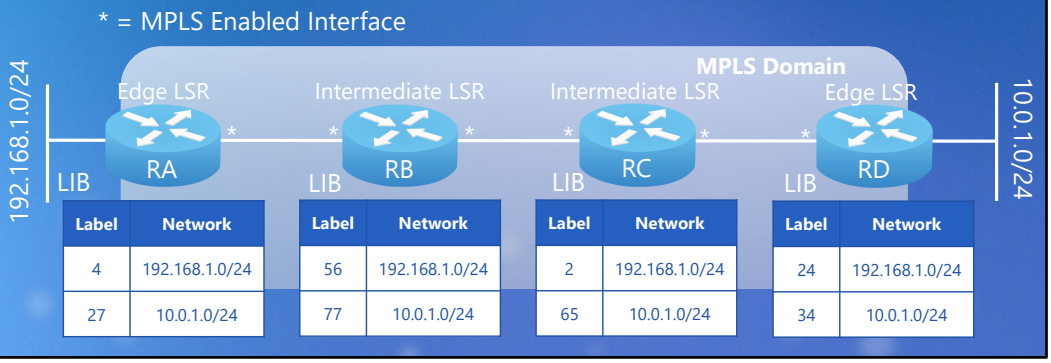
Add a label is called imposing a label
Removing a label is called popping a label

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

MPLS Label Switch Routers

Intermediate LSR

Reside in the MPLS domain, receive labeled packets, swap labels, forward labeled packets



Label	Network
4	192.168.1.0/24
27	10.0.1.0/24

Label	Network
56	192.168.1.0/24
77	10.0.1.0/24

Label	Network
2	192.168.1.0/24
65	10.0.1.0/24

Label	Network
24	192.168.1.0/24
34	10.0.1.0/24

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

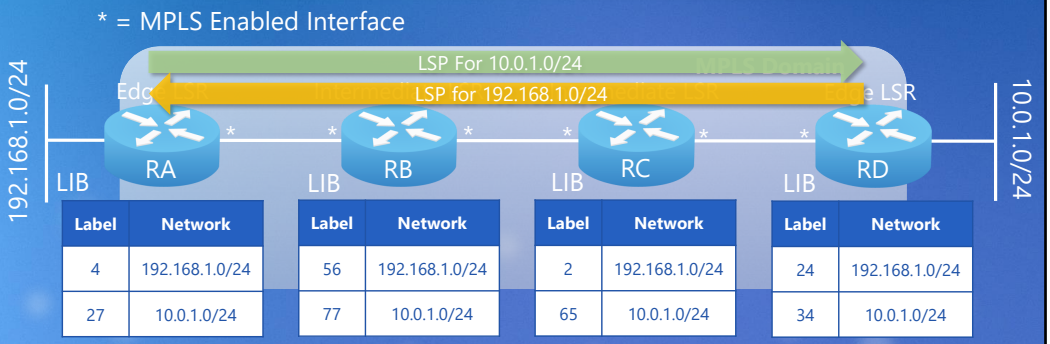
MPLS Label-Switched Path

The complete unidirectional labeled path through the MPLS domain

From source to destination

For a data packet

Discovered through the exchange of labels



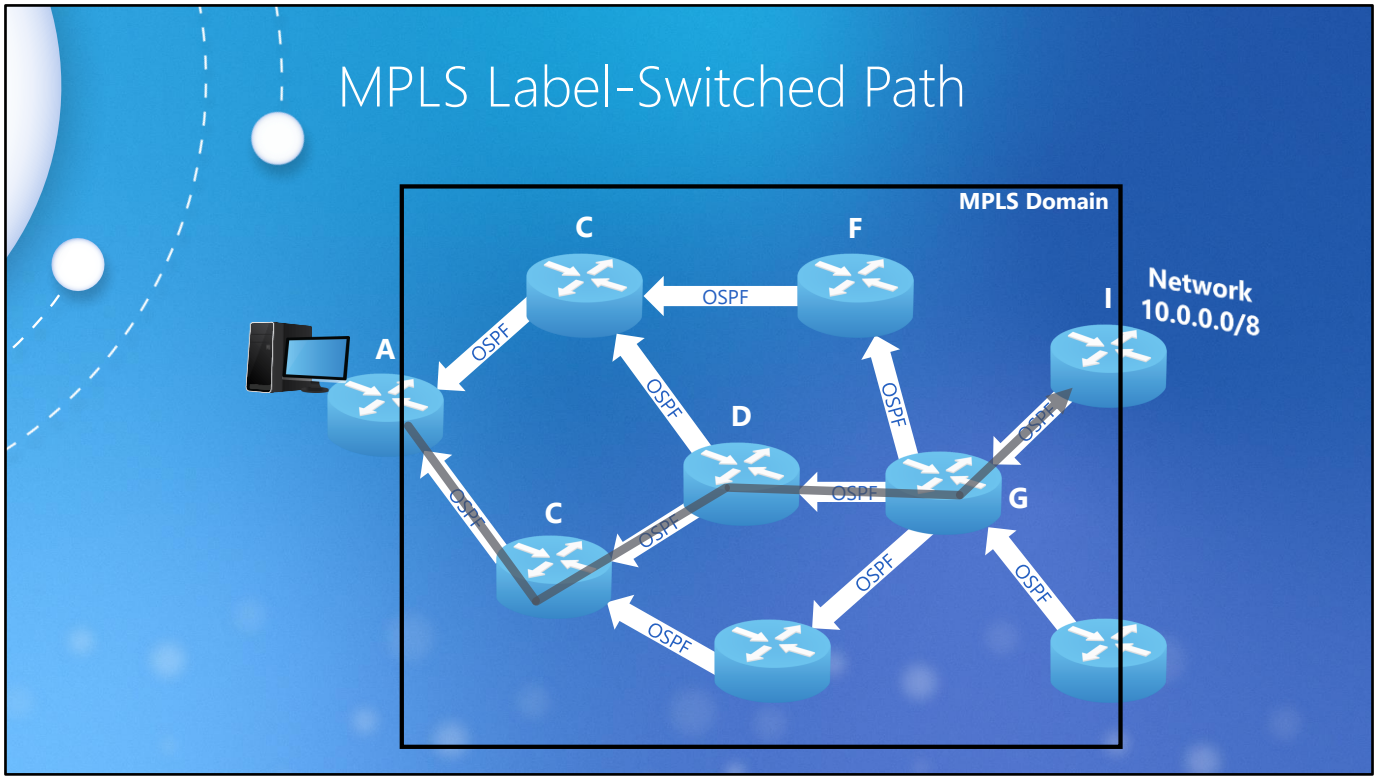
Label	Network
4	192.168.1.0/24
27	10.0.1.0/24

Label	Network
56	192.168.1.0/24
77	10.0.1.0/24

Label	Network
2	192.168.1.0/24
65	10.0.1.0/24

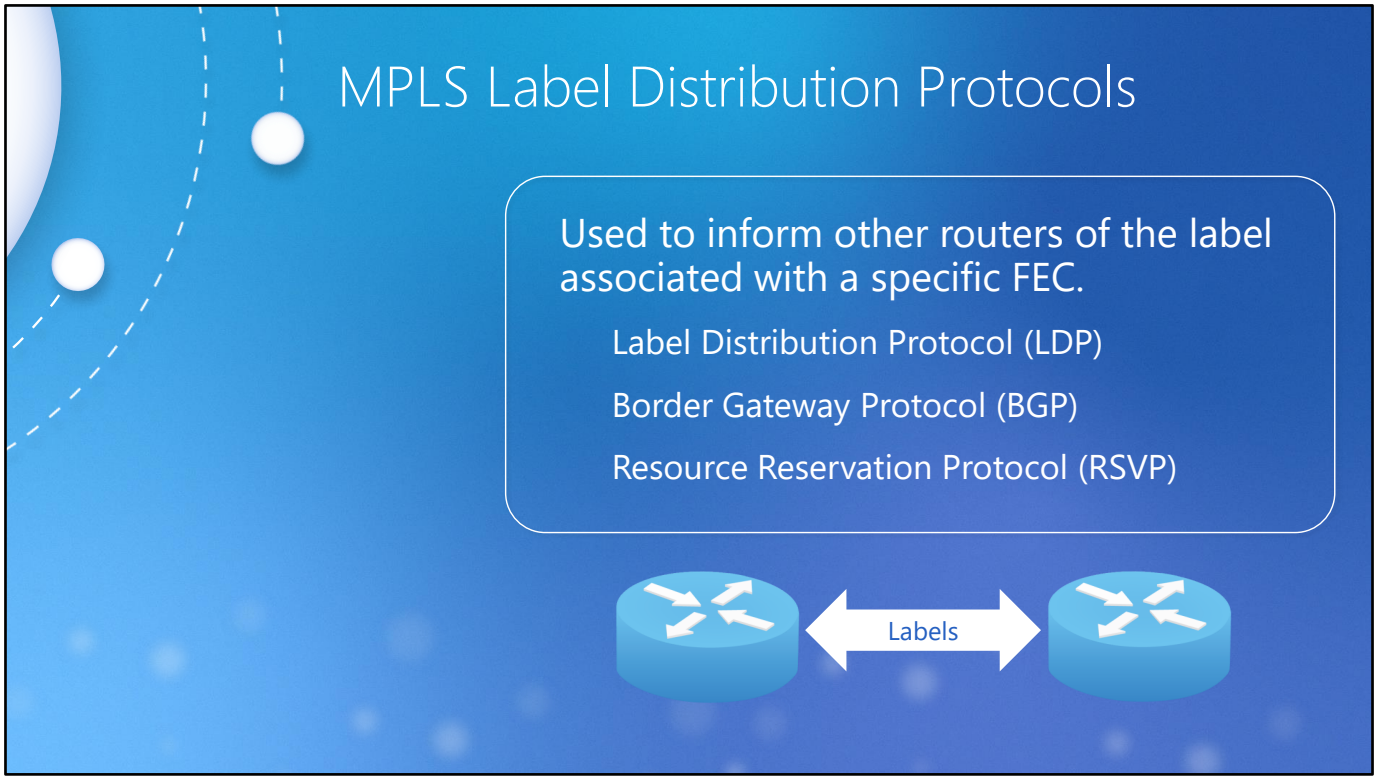
Label	Network
24	192.168.1.0/24
34	10.0.1.0/24

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



The LSP will be based on the best path chosen by the IGP that is running inside the MPLS domain.

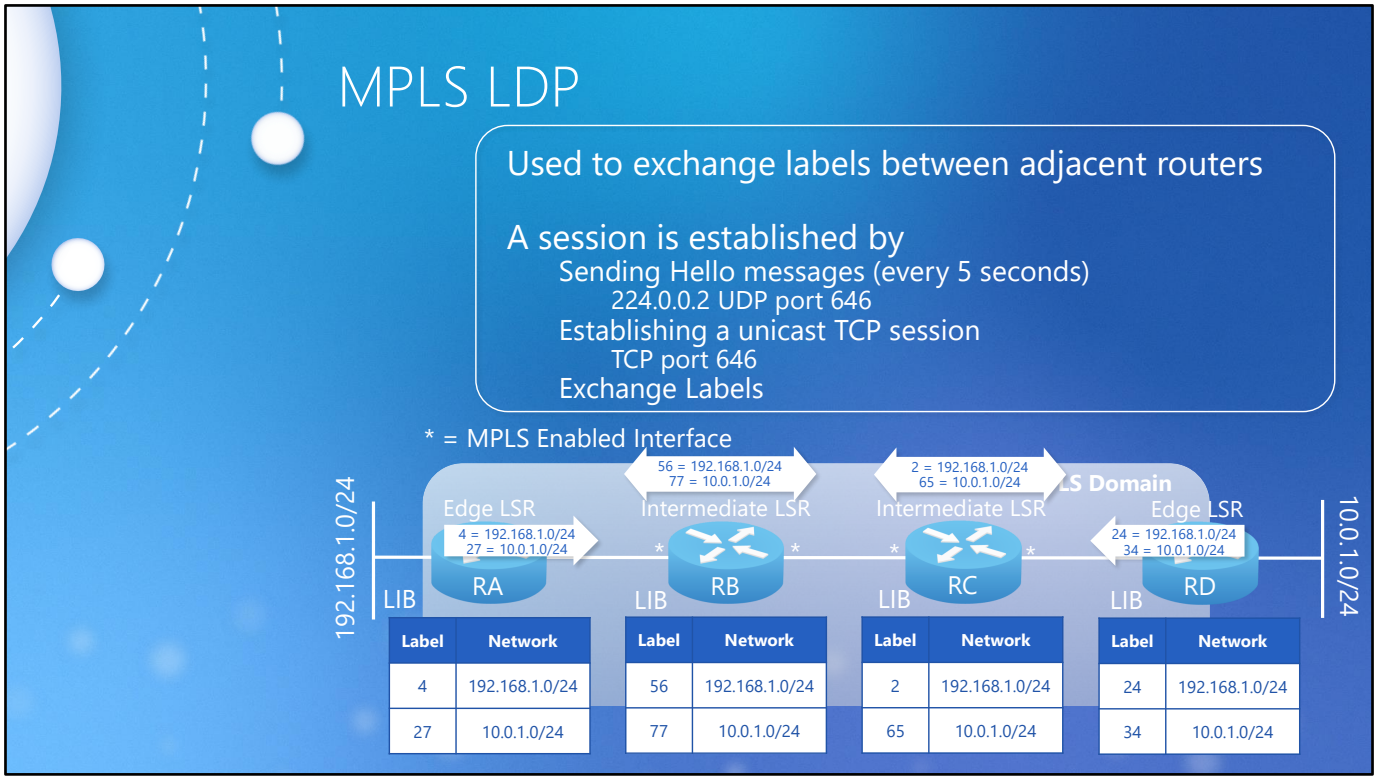
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



FEC = Forwarding Equivalence Class which is a group of packets that are forwarded in the same manner, over the same path, and with the same forwarding treatment.

LDP – an industry standard protocol for MPLS labels… the most common method used to distribute the labels for IGP prefixes.
BGP – used for MPLS L3 VPNs labels
RSVP – used for MPLS TE (Traffic Engineering) ***EXAM***

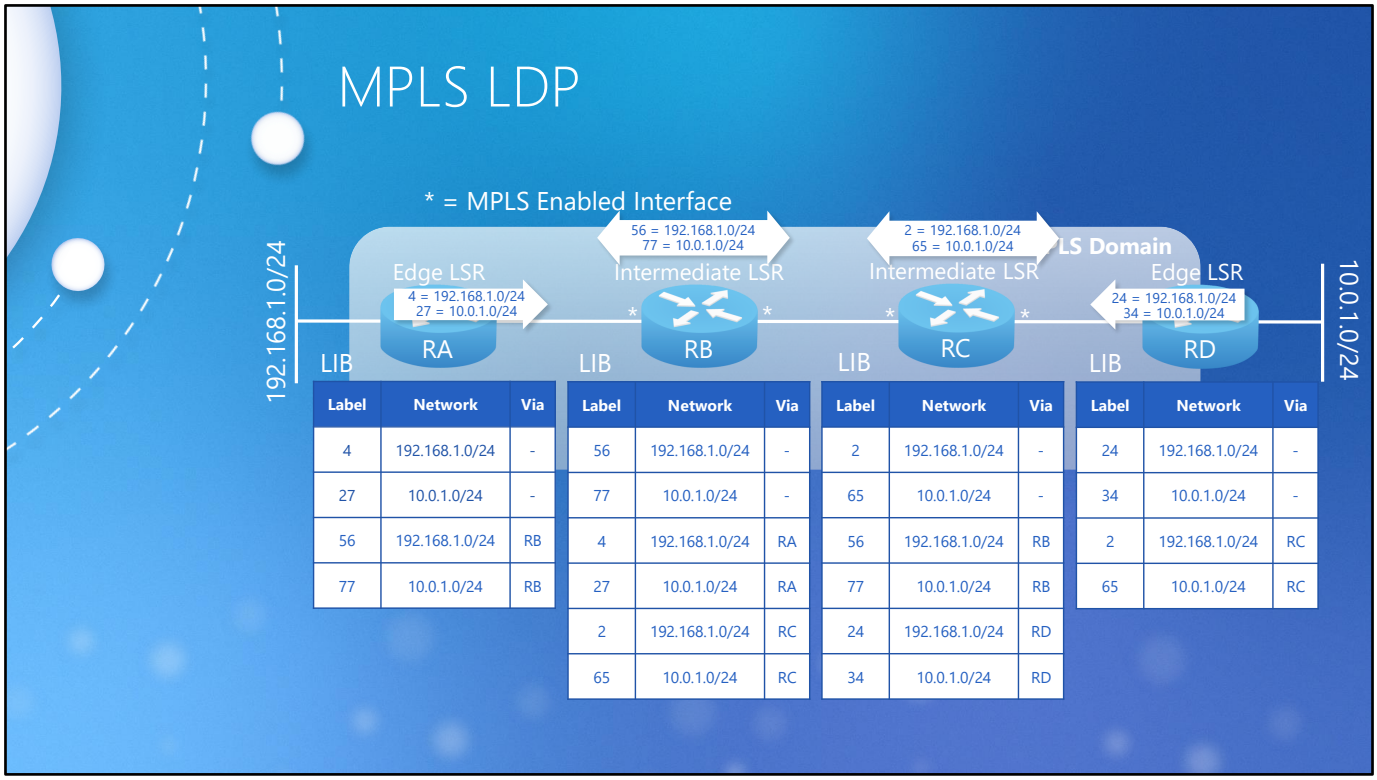
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



EXAM Hellos are sent every 5 seconds, once both routers see each other they use TCP to establish a session with each other and once the session is established they will exchange labels with each other.

Discuss how the labels are being exchanged

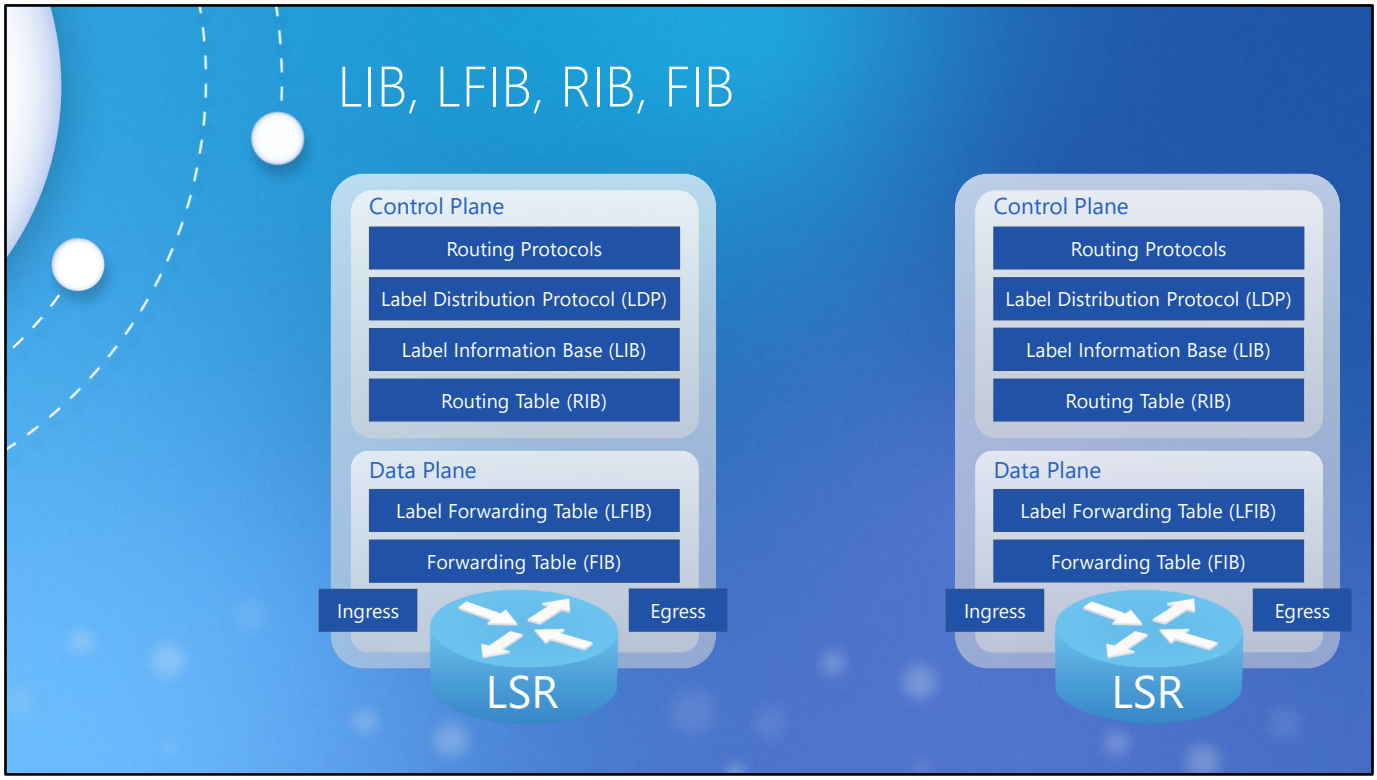
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



At this point now…. The labels have been exchanged and placed in the LIB.

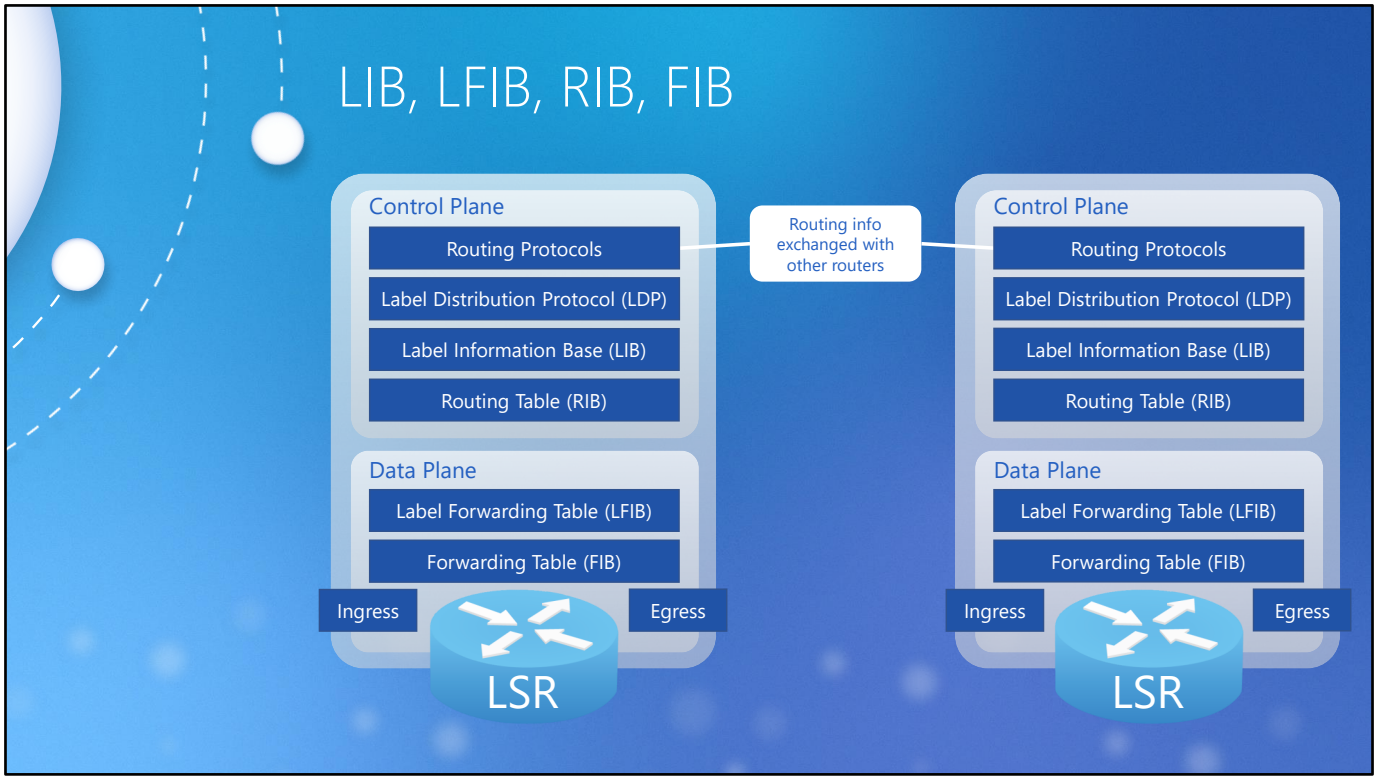
A LIB, or Label Information Base, is essentially a database used by MPLS routers (label switch routers, or LSRs) to store label mappings for forwarding MPLS packets. Each entry in the LIB correlates incoming labels with outgoing labels and includes information necessary for the router to forward the packet correctly.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



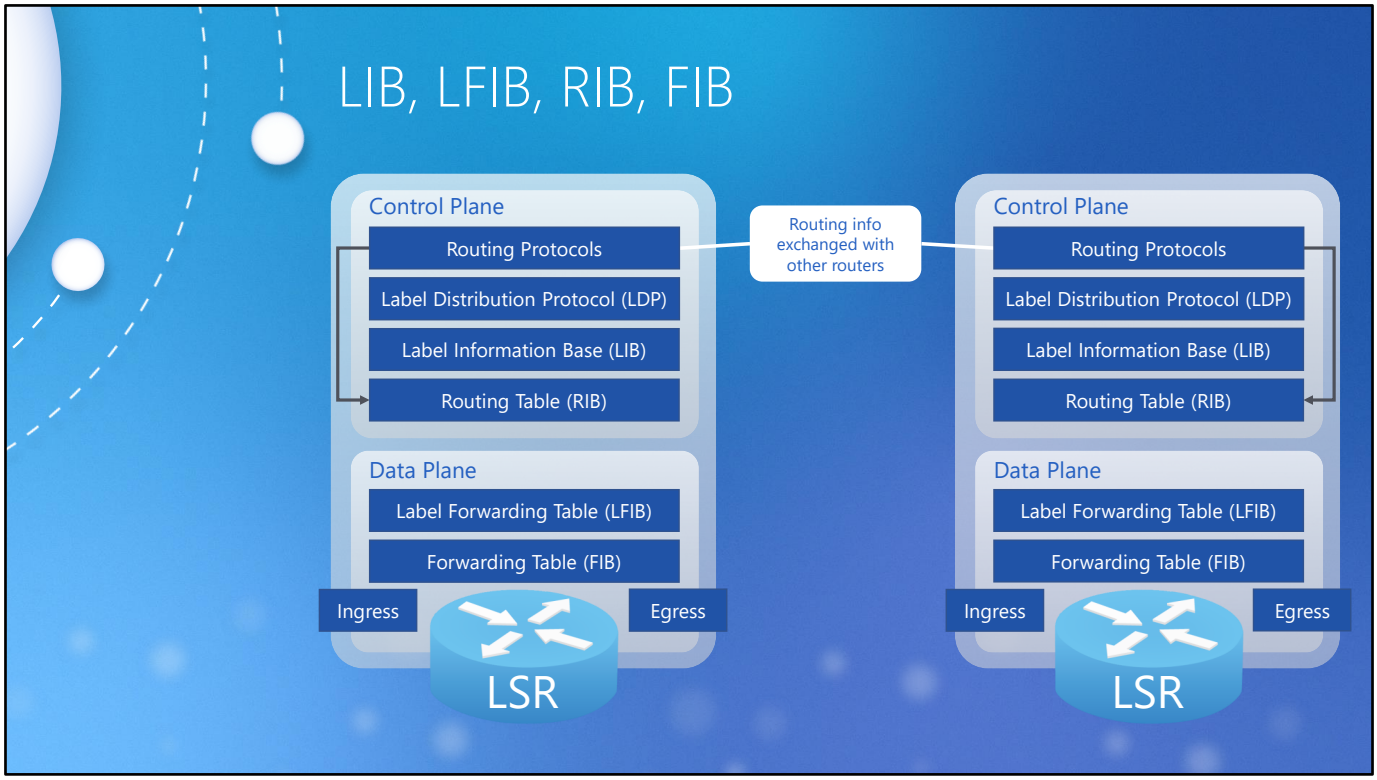
Let’s now examine the LIB, LFIB, RIB and FIB in regards to the Control and Data Planes

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



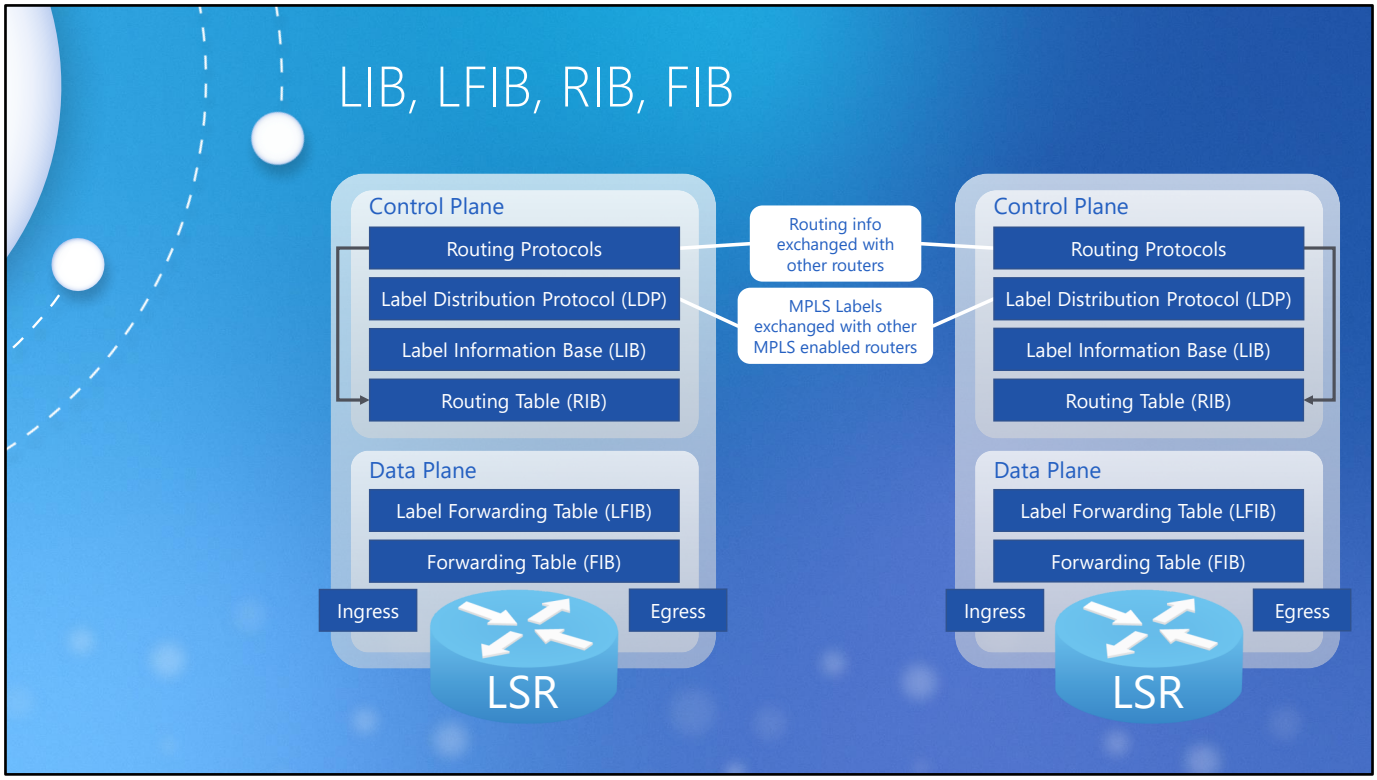
Control plane uses protocols to build the RIB and the LIB. Protocols such as OSPF, EIGRP, IS-IS ……

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



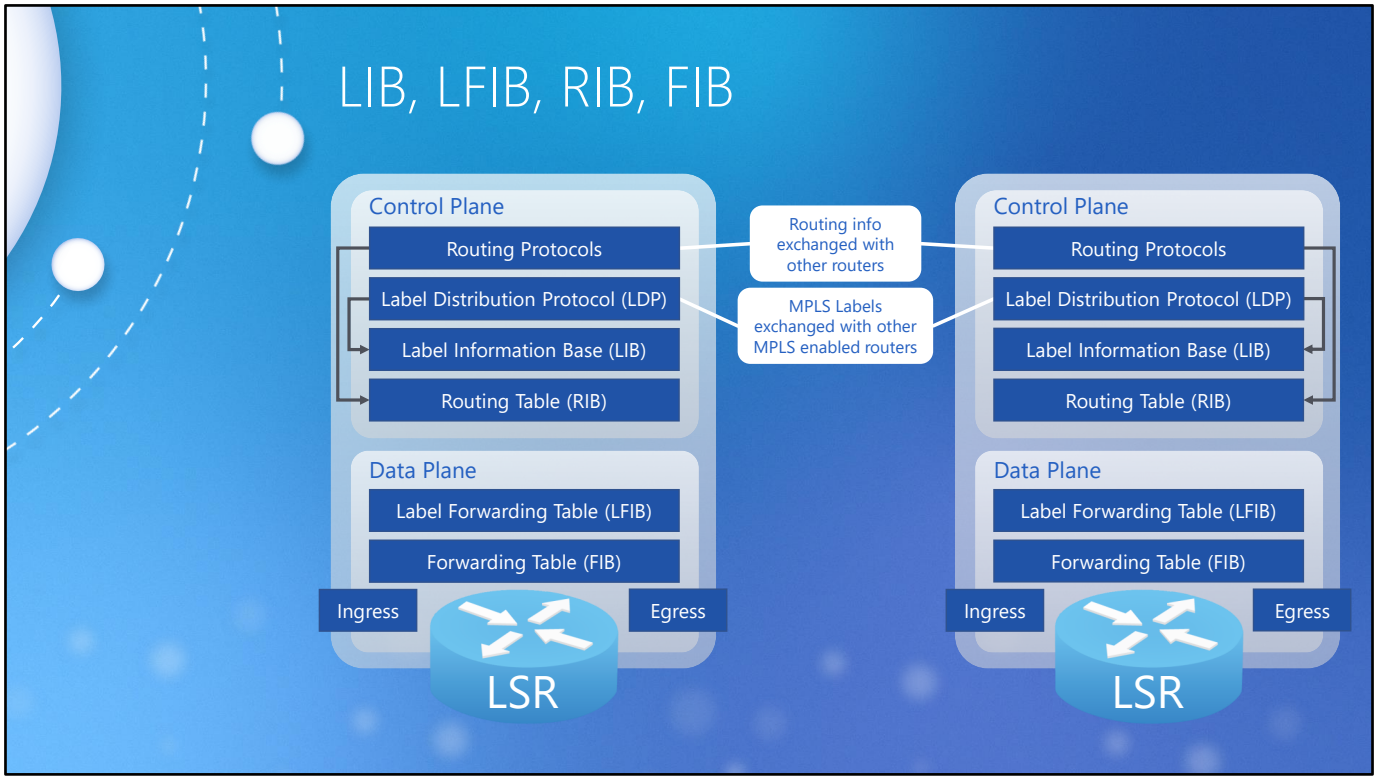
can be used to exchange ip prefixes which populate the ip routing table known as the RIB.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



A protocol such as LDP can be used to exchange labels…..

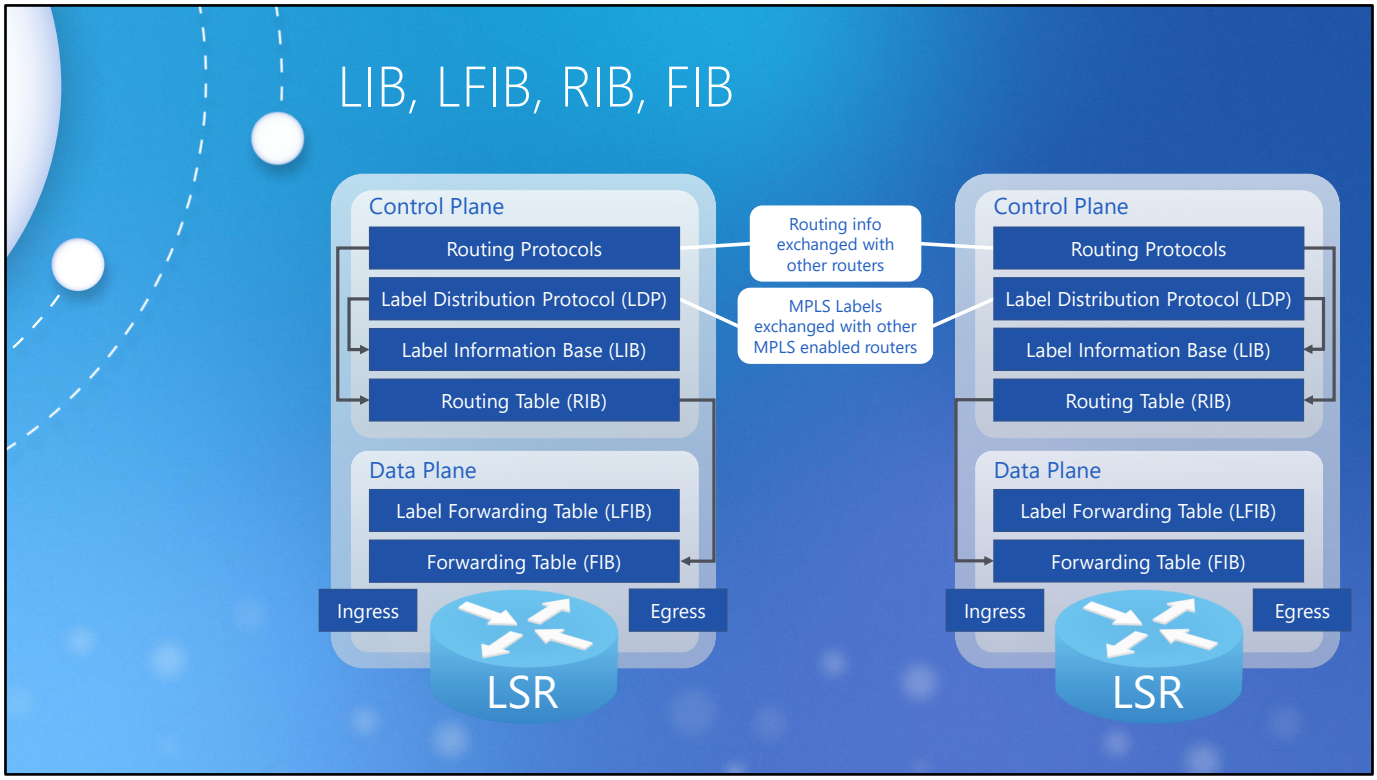
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



which will populate the label database known as the LIB.

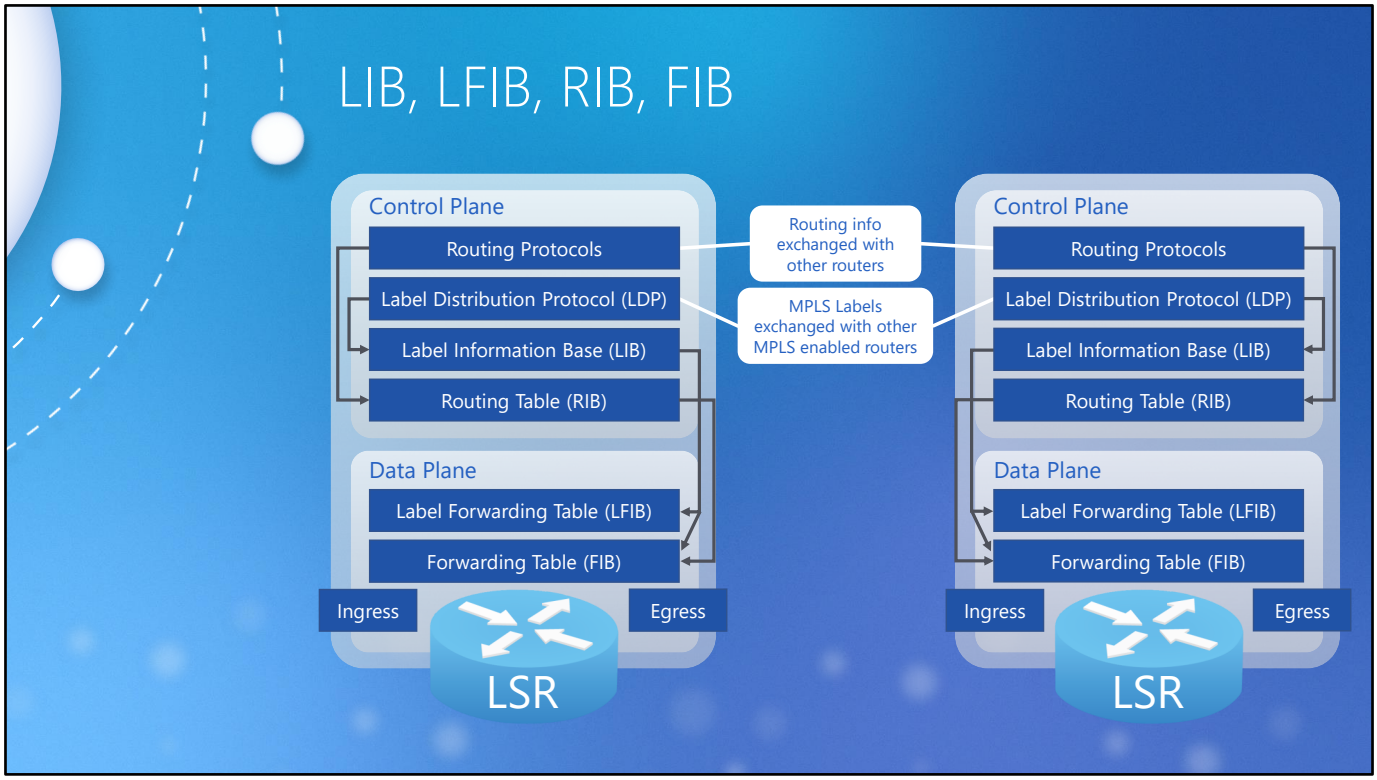
Show mpls ldp binding to view lib

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



The Data Plane is used as the forwarding engine in our routers. The information in the RIB is used to populate the hardware based (CEF) ip forwarding tables in the data plane (the FIB) and

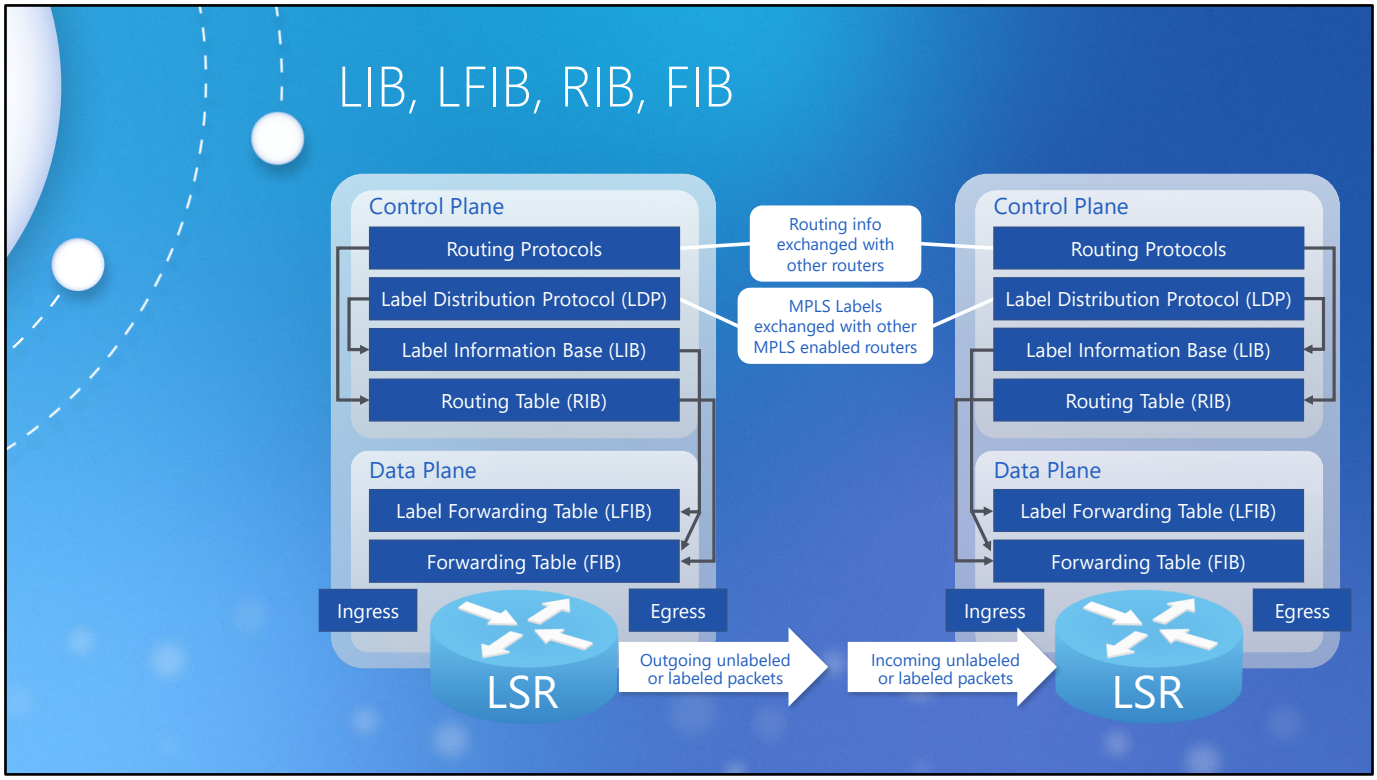
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



the LIB is used to populate the hardware based (CEF) label forwarding table in the data plane (the LFIB) as well as the FIB. WHY??????

Show mpls forwarding-table to view the lfib

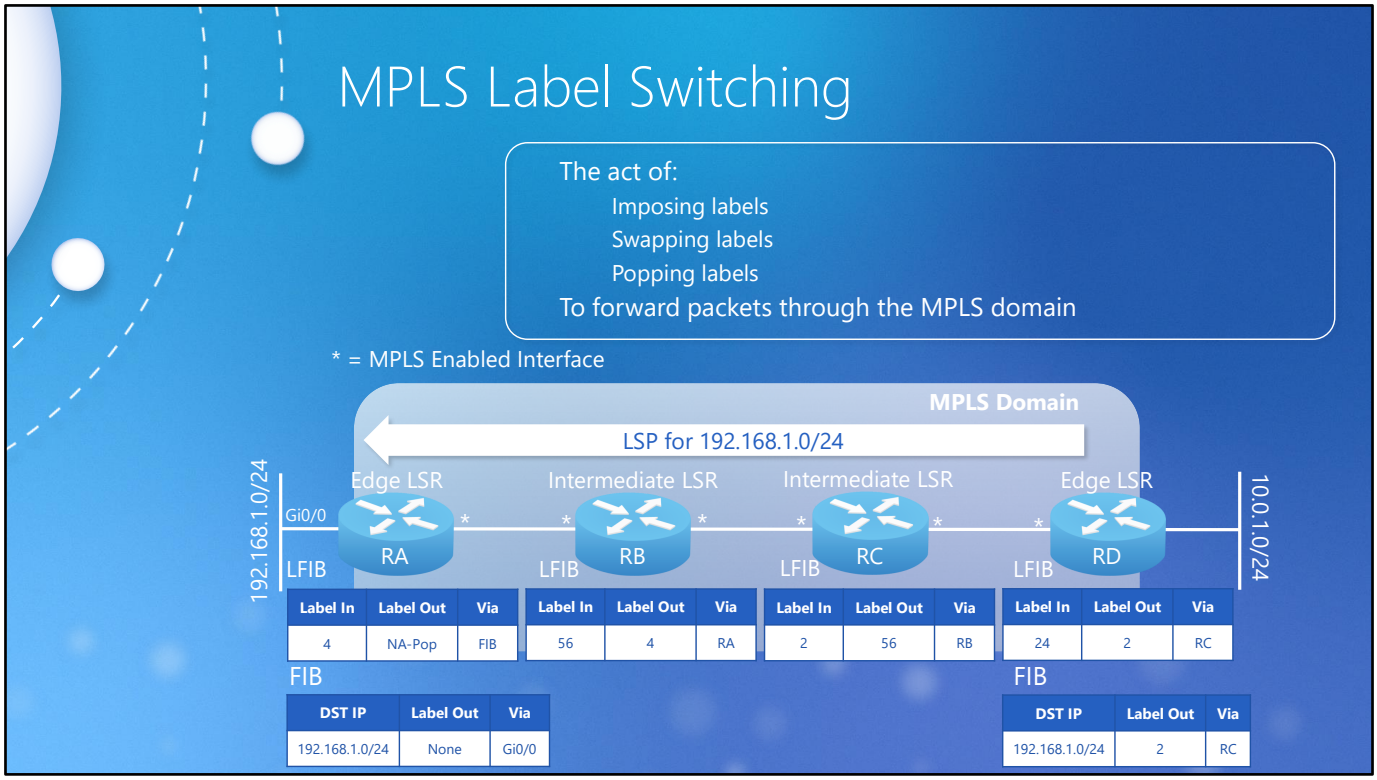
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



The FIB will be used when an unlabeled packet arrives at the device. If the packet needs to be forwarded out a non-MPLS enabled interface it will be sent out the interface unlabeled. However, if the FIB states that the packet is to be forwarded out an MPLS enabled interface a label needs to be imposed and the router will impose the label and forward it out the interface.

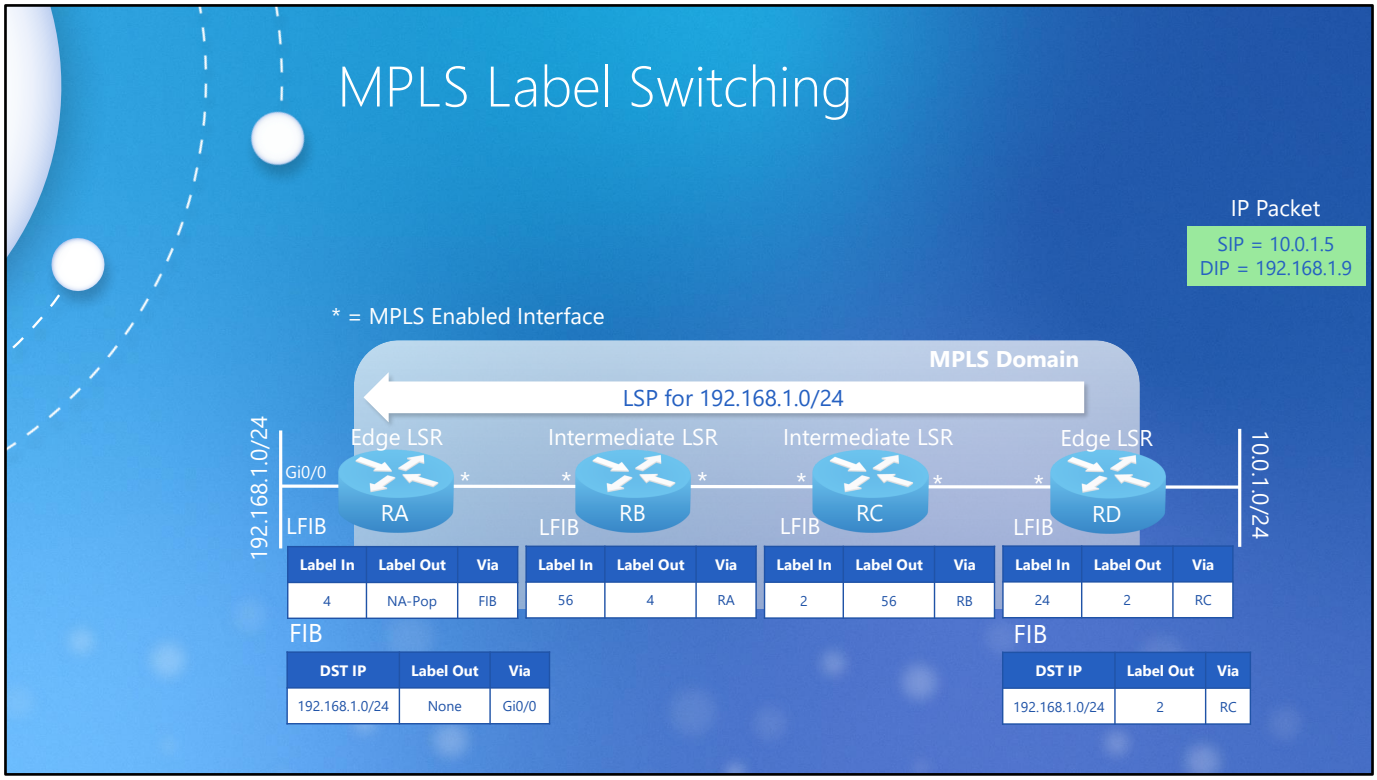
The LFIB will be used when a labeled packet arrives on an MPLS enabled interface. A label lookup will occur, if the destination is out an MPLS enabled interface the router will swap the label based on the info in the LFIB and forward the packet out the MPLS enabled interface. However, when a labeled packet arrives on an MPLS enabled interface and the LFIB indicates that the destination is out a non-MPLS enabled interface the label gets popped and the packet gets sent to the FIB for normal routing out the non-MPLS enabled interface.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



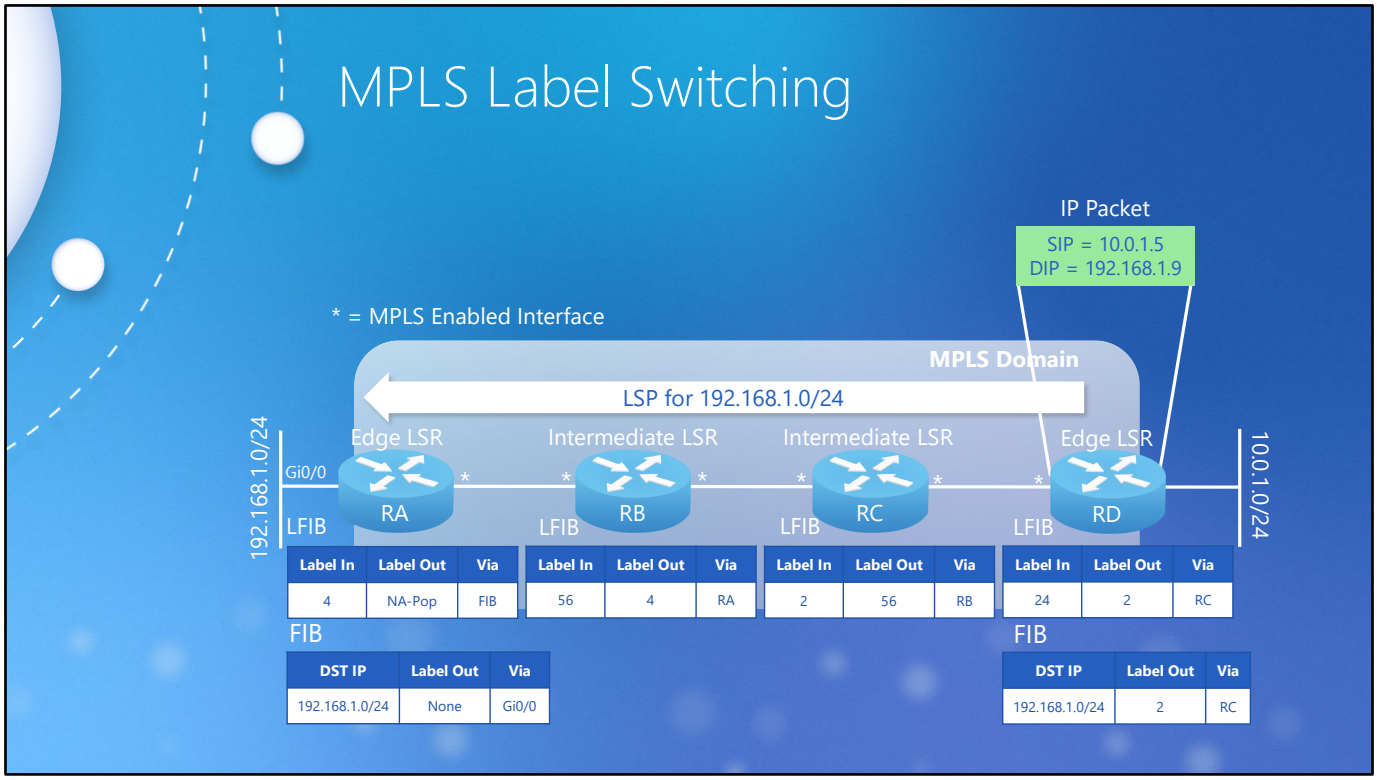
Pop = imp-null

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Pop = imp-null

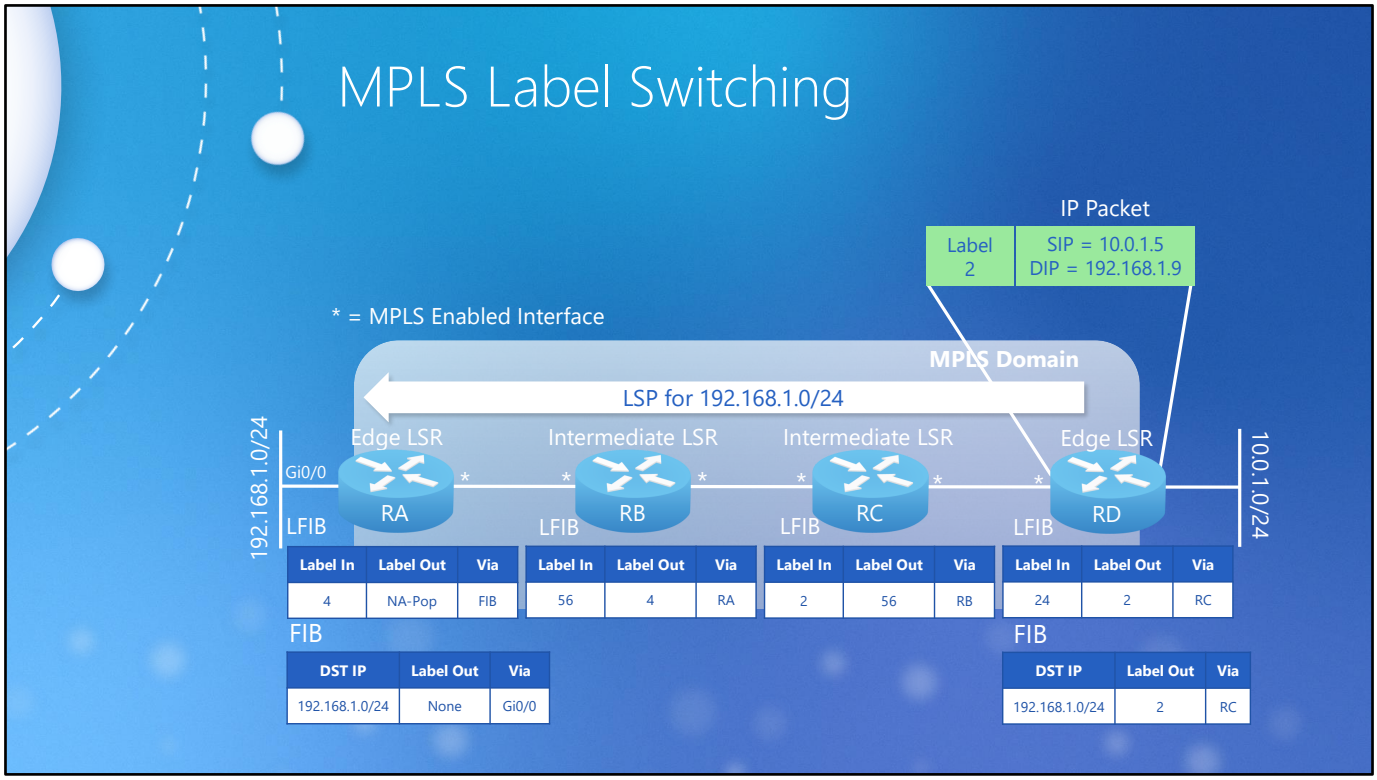
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



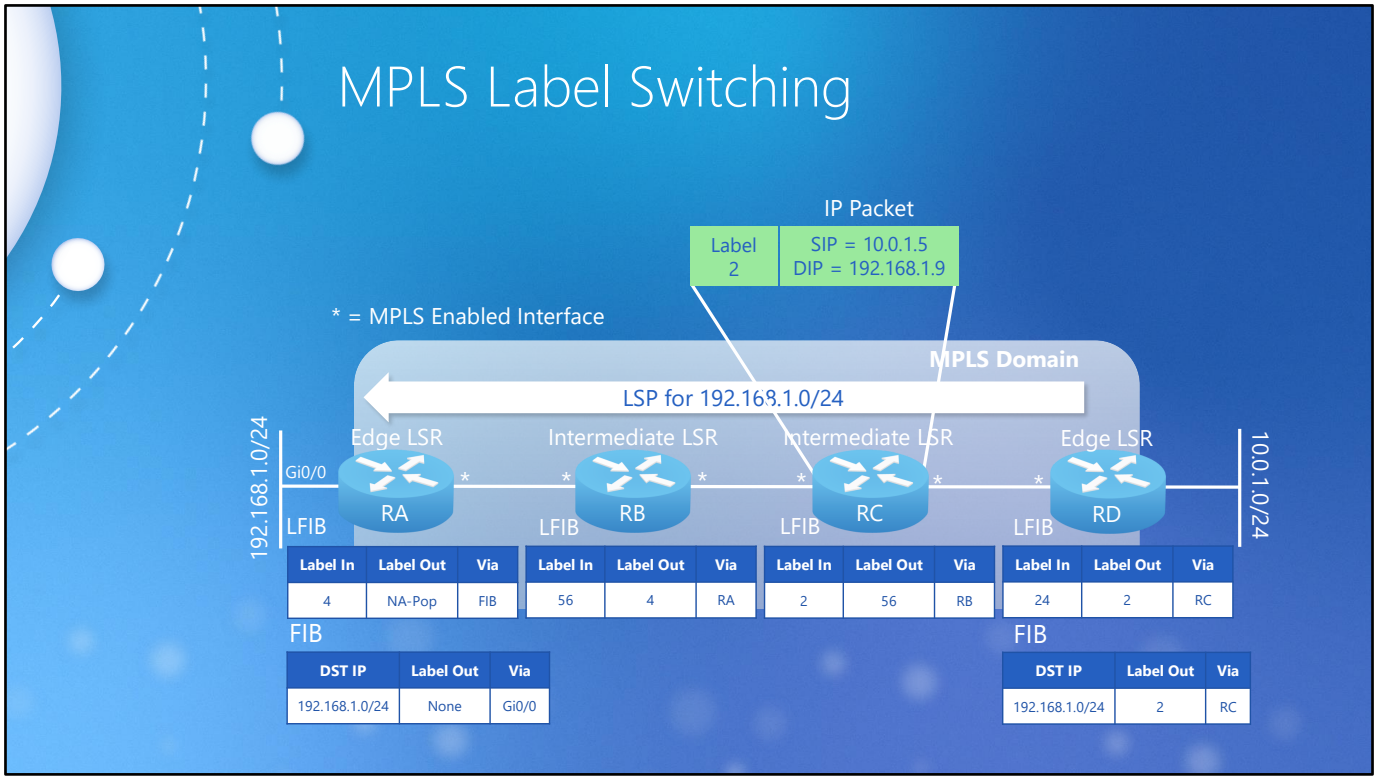
Impose label 2

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

MPLS Label Switching

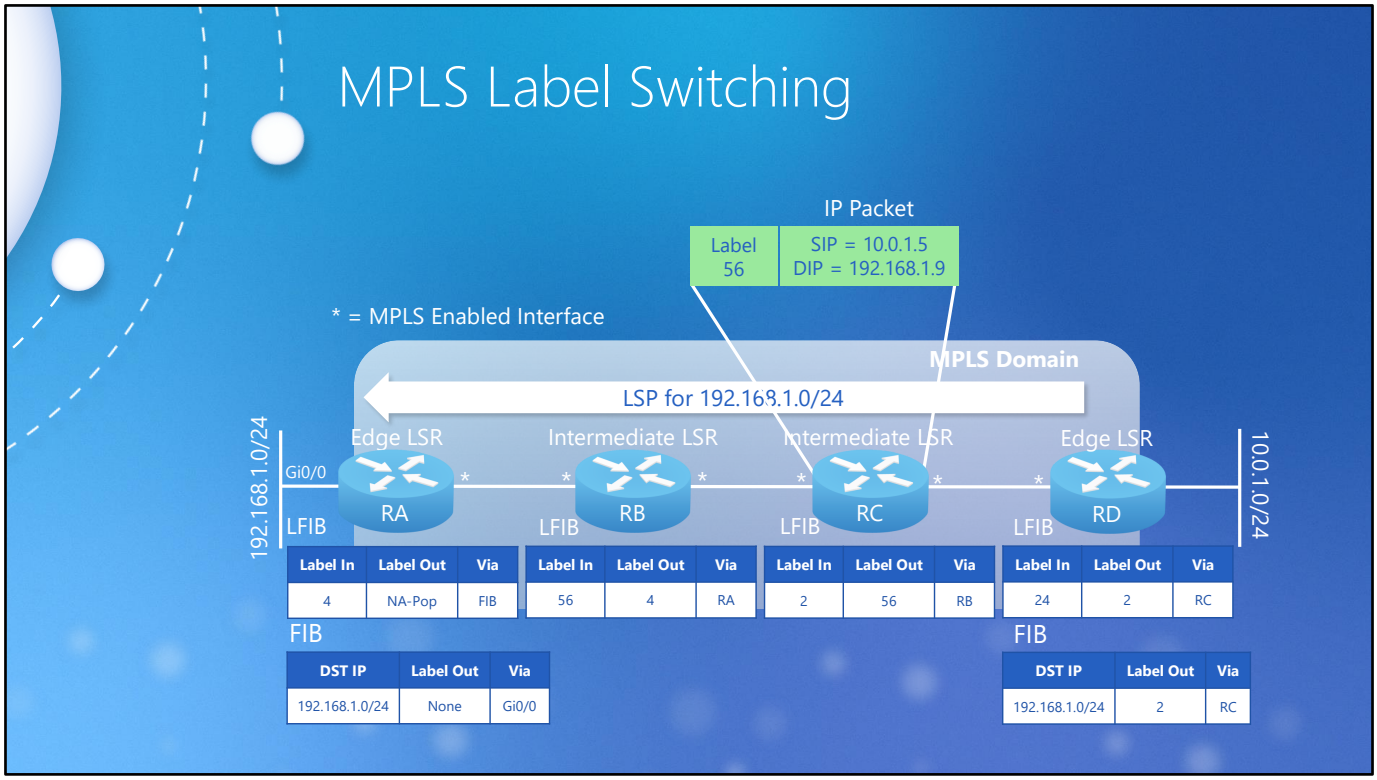


©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



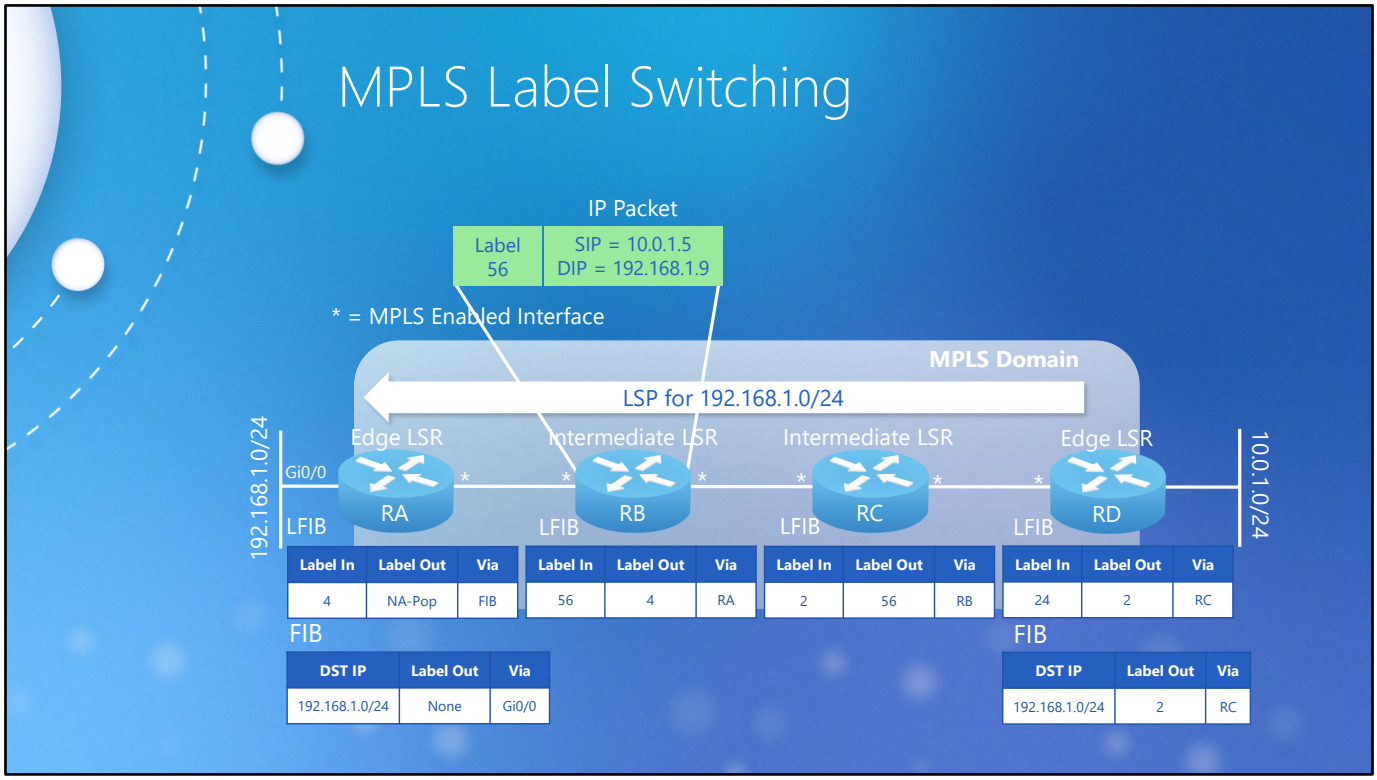
Swap 2 for 56

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



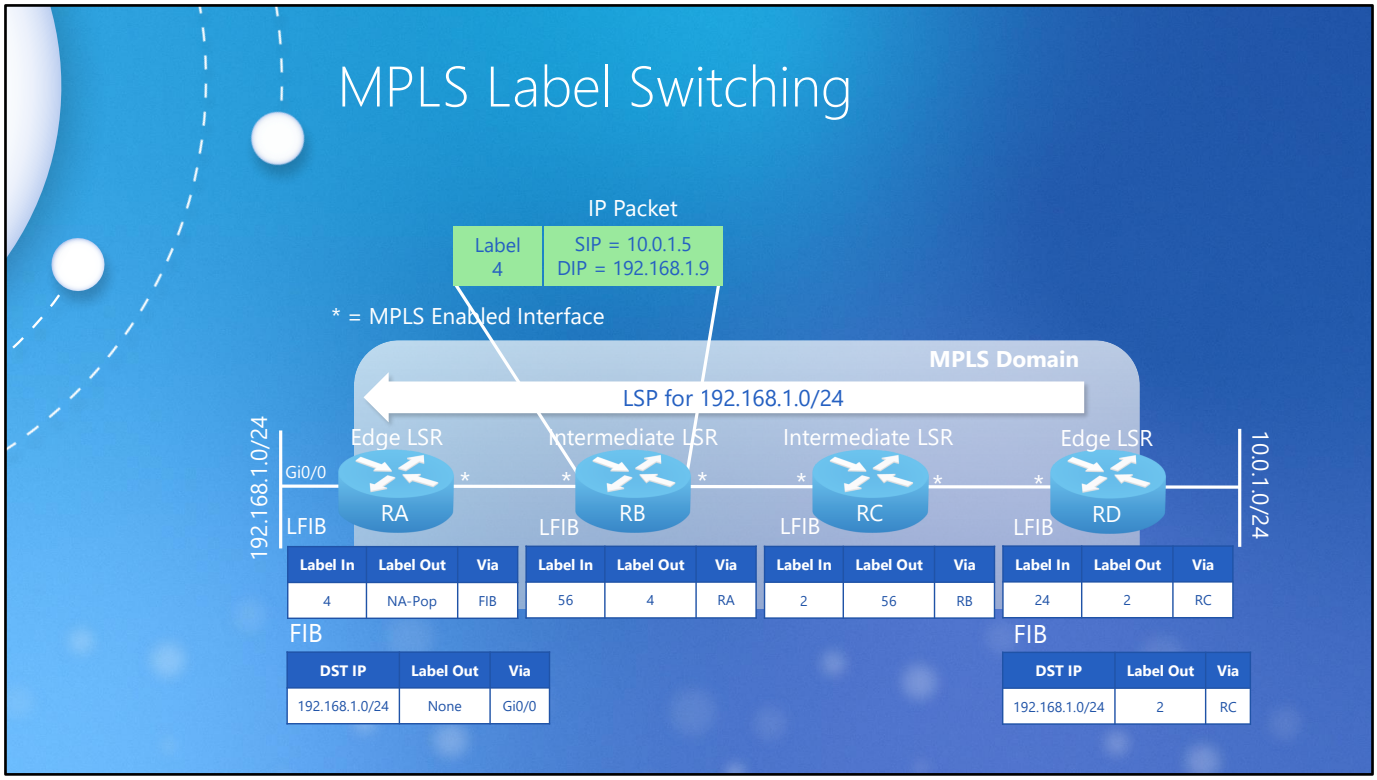
Swap 2 for 56

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



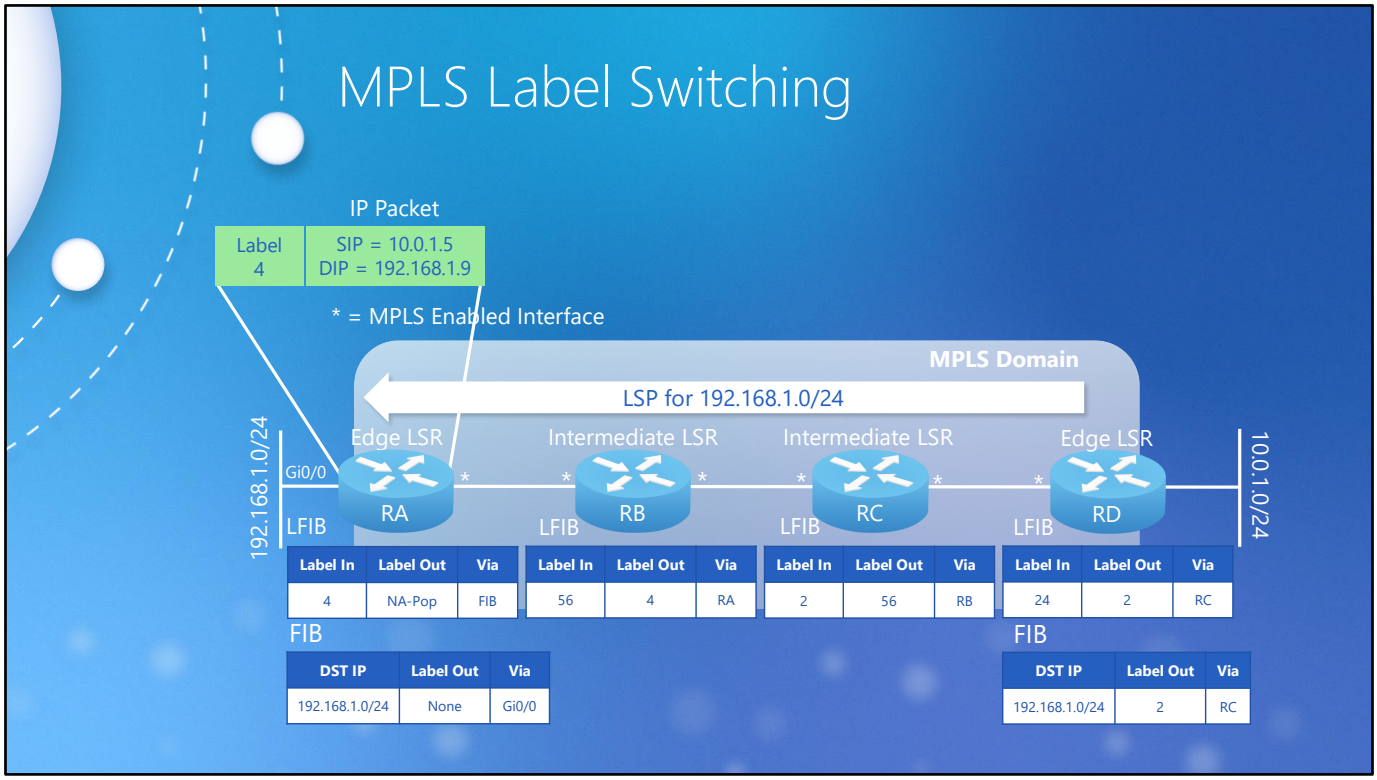
Swap 56 for 4

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



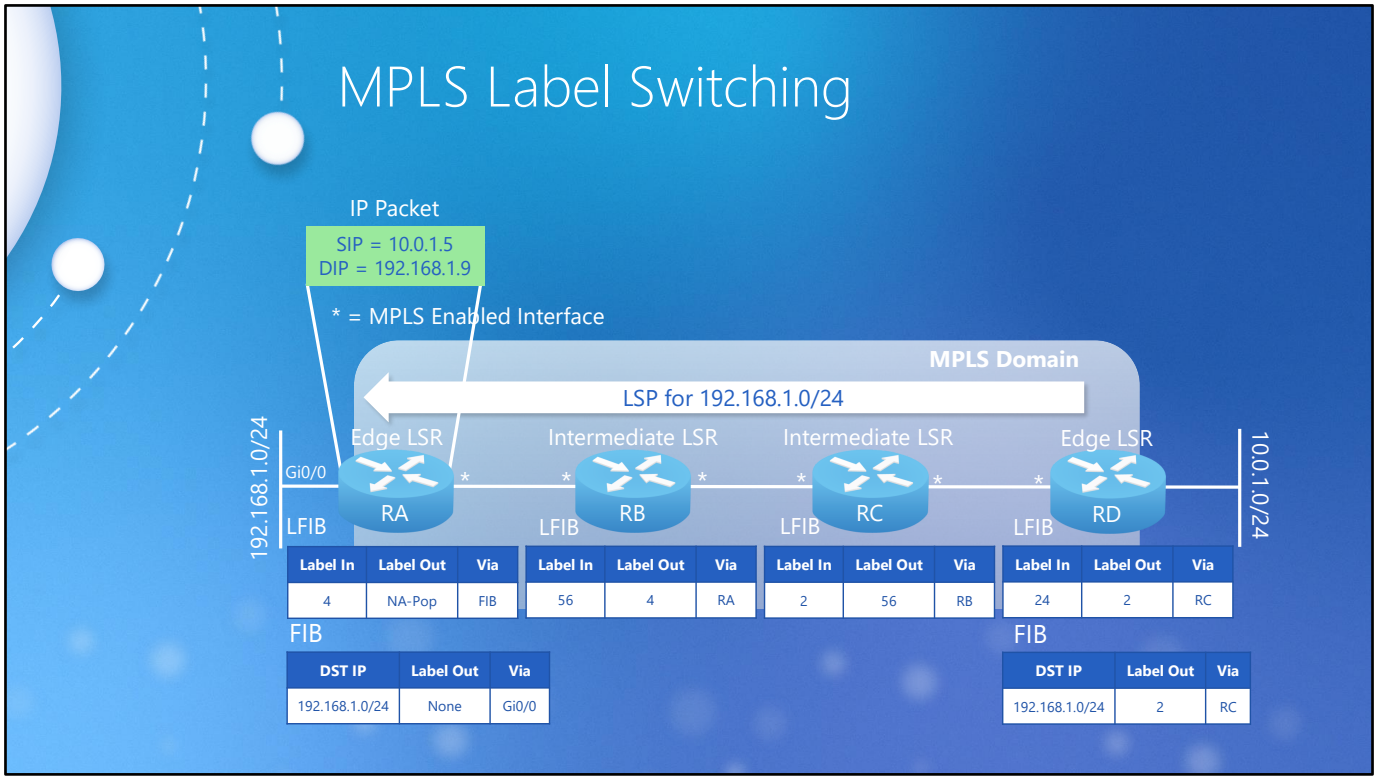
Swap 56 for 4

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



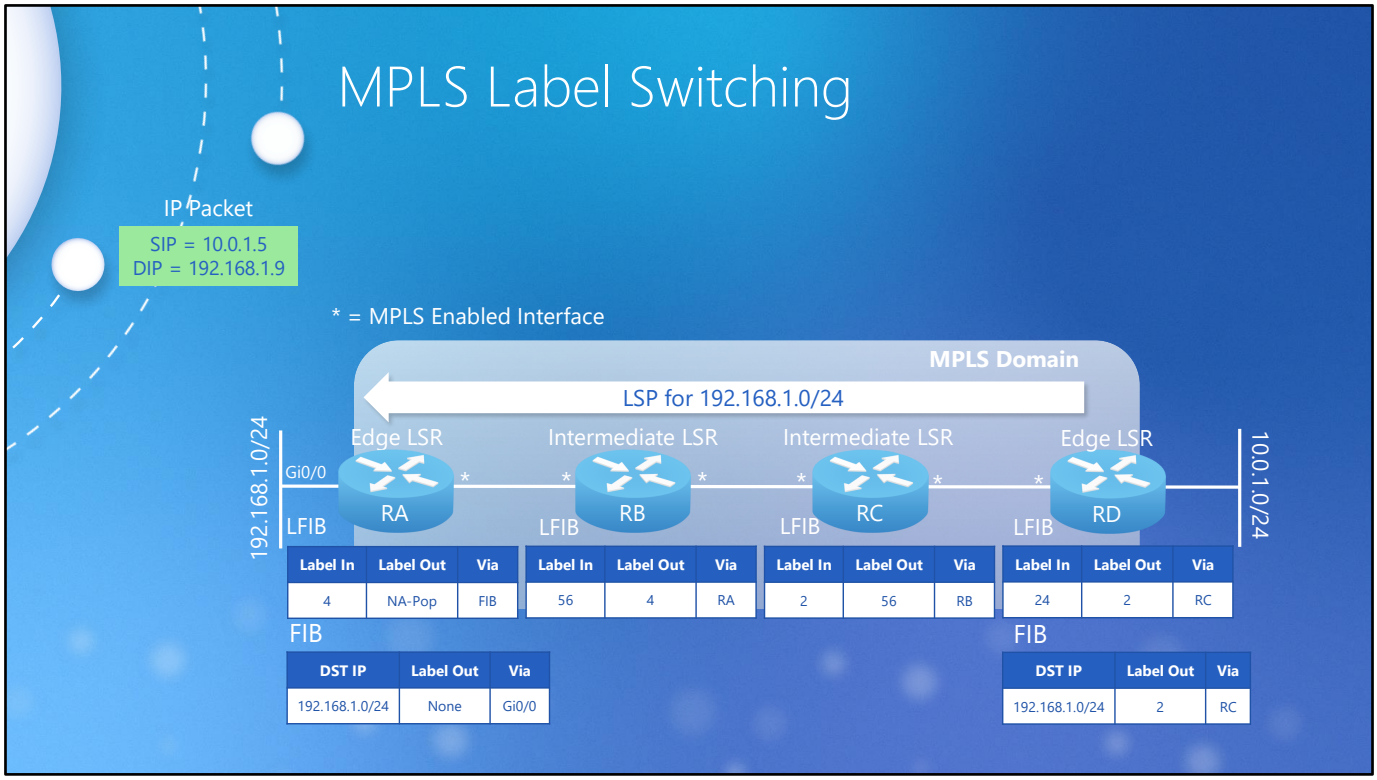
Pop = imp-null label 4

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



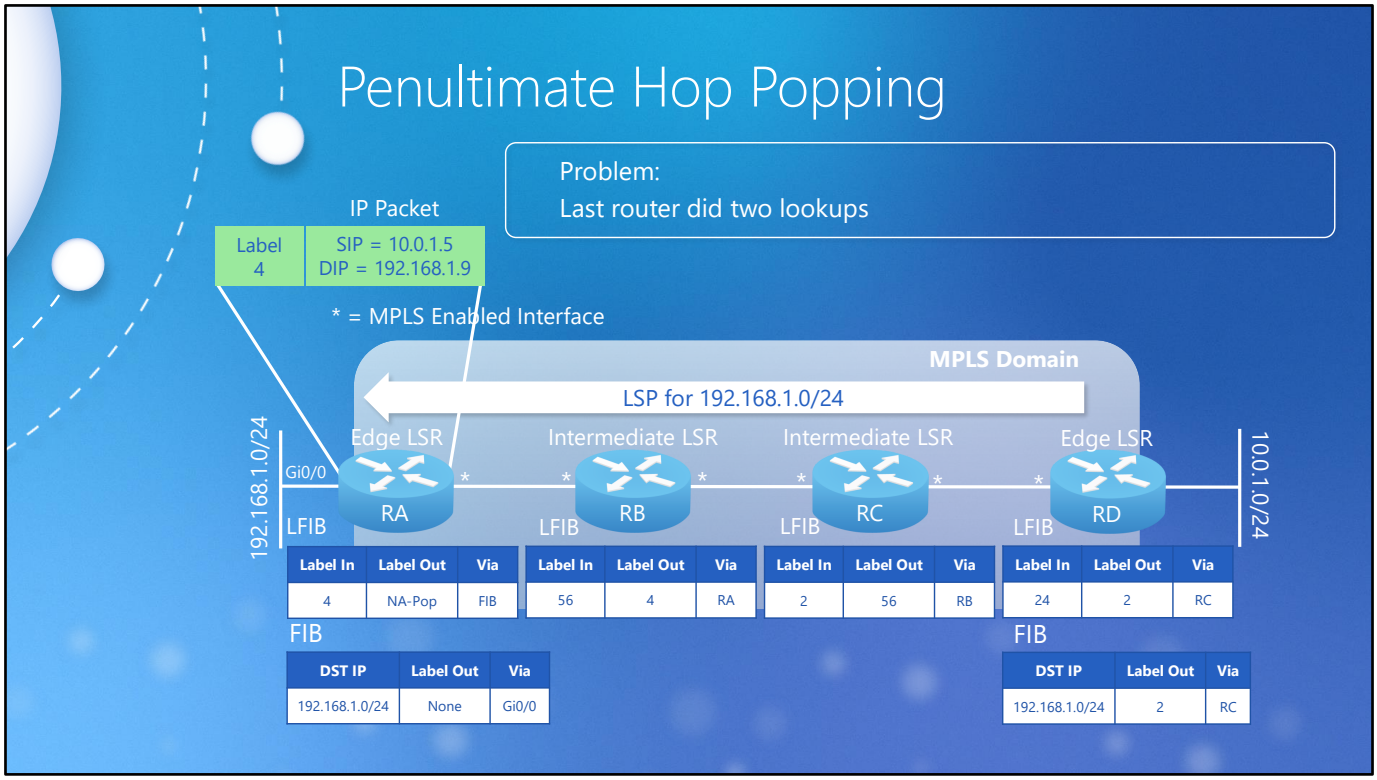
Now the router has to do another lookup… to determine how to get to the IP.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



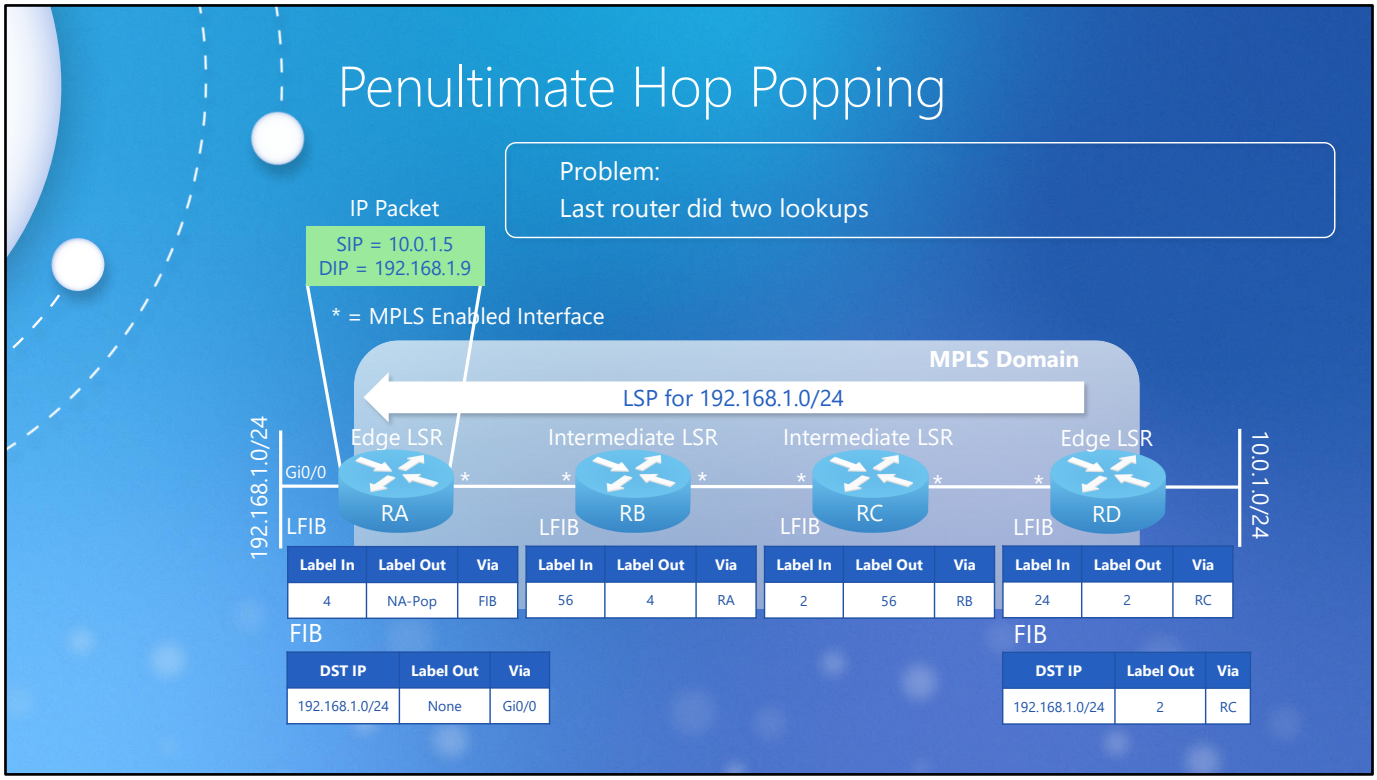
Pop = imp-null

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



It had to look up the label….

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



It had to look up the dst ip

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Penultimate Hop Popping

Problem:
Last router did two lookups

IP Packet
SIP = 10.0.1.5
DIP = 192.168.1.9



Label In	Label Out	Via
4	NA-Pop	FIB

Label In	Label Out	Via
56	4	RA

Label In	Label Out	Via
2	56	RB

Label In	Label Out	Via
24	2	RC

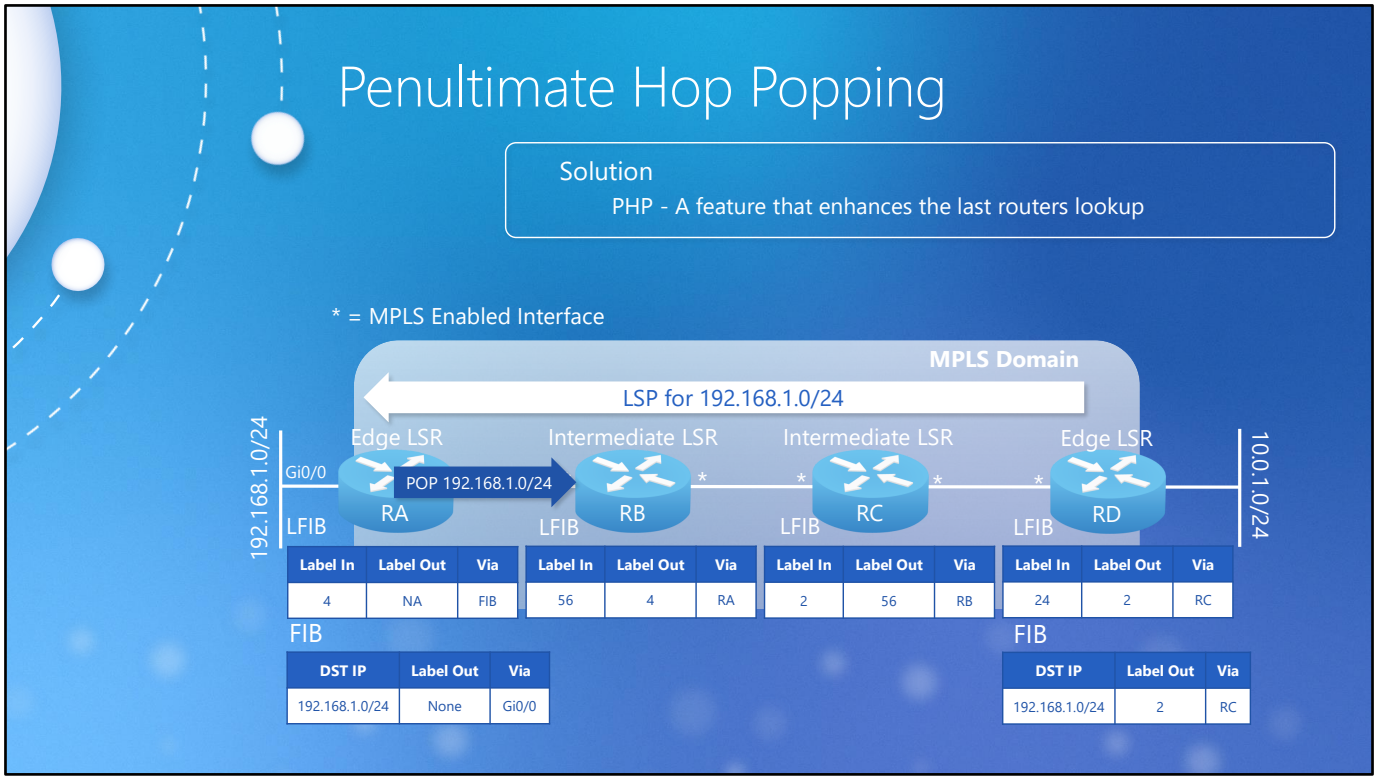
FIB

DST IP	Label Out	Via
192.168.1.0/24	None	Gi0/0

FIB

DST IP	Label Out	Via
192.168.1.0/24	2	RC

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



It is enabled by default and you what to use it.

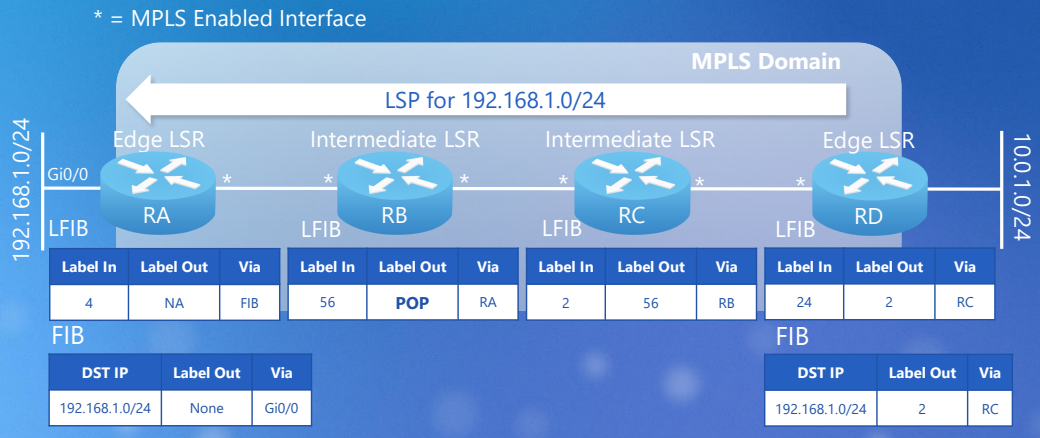
RA is telling RB to POP the label ahead of time.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

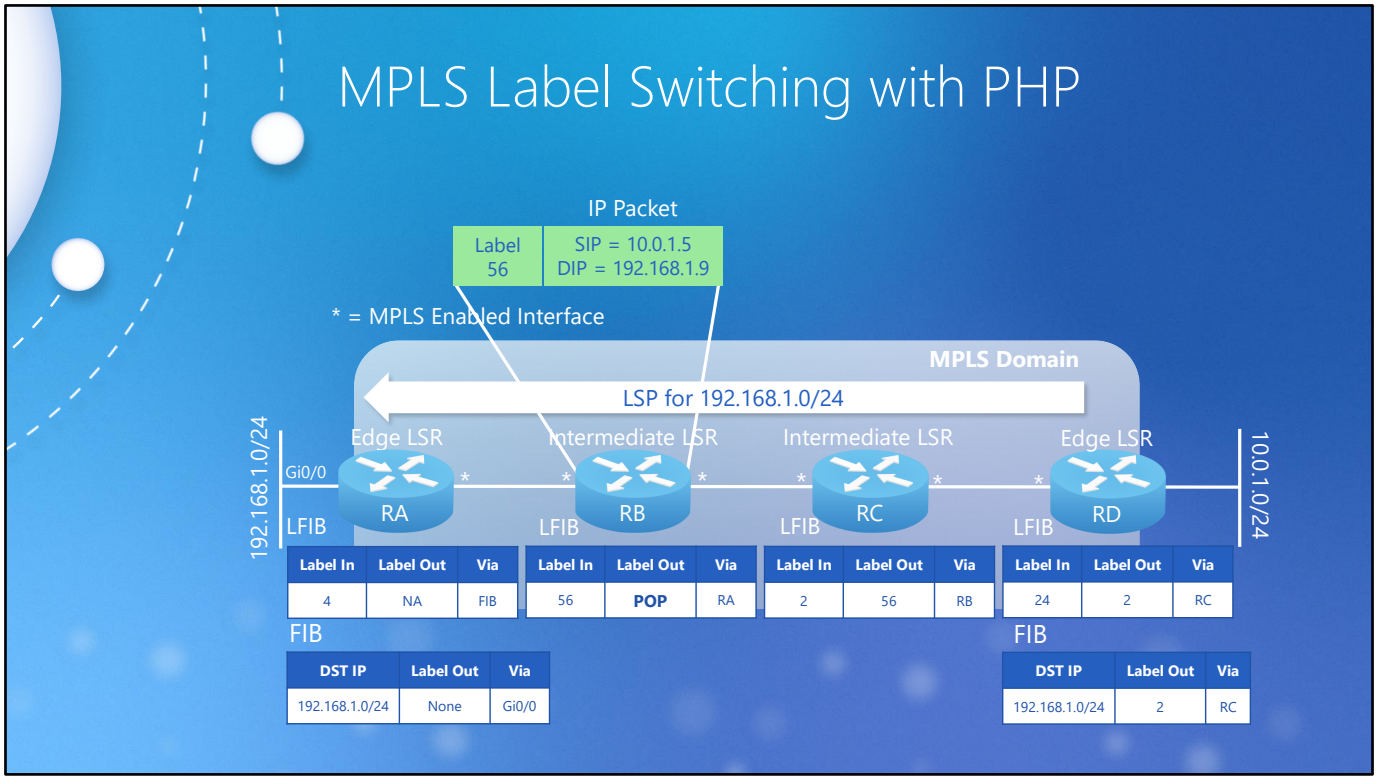
Penultimate Hop Popping

Solution

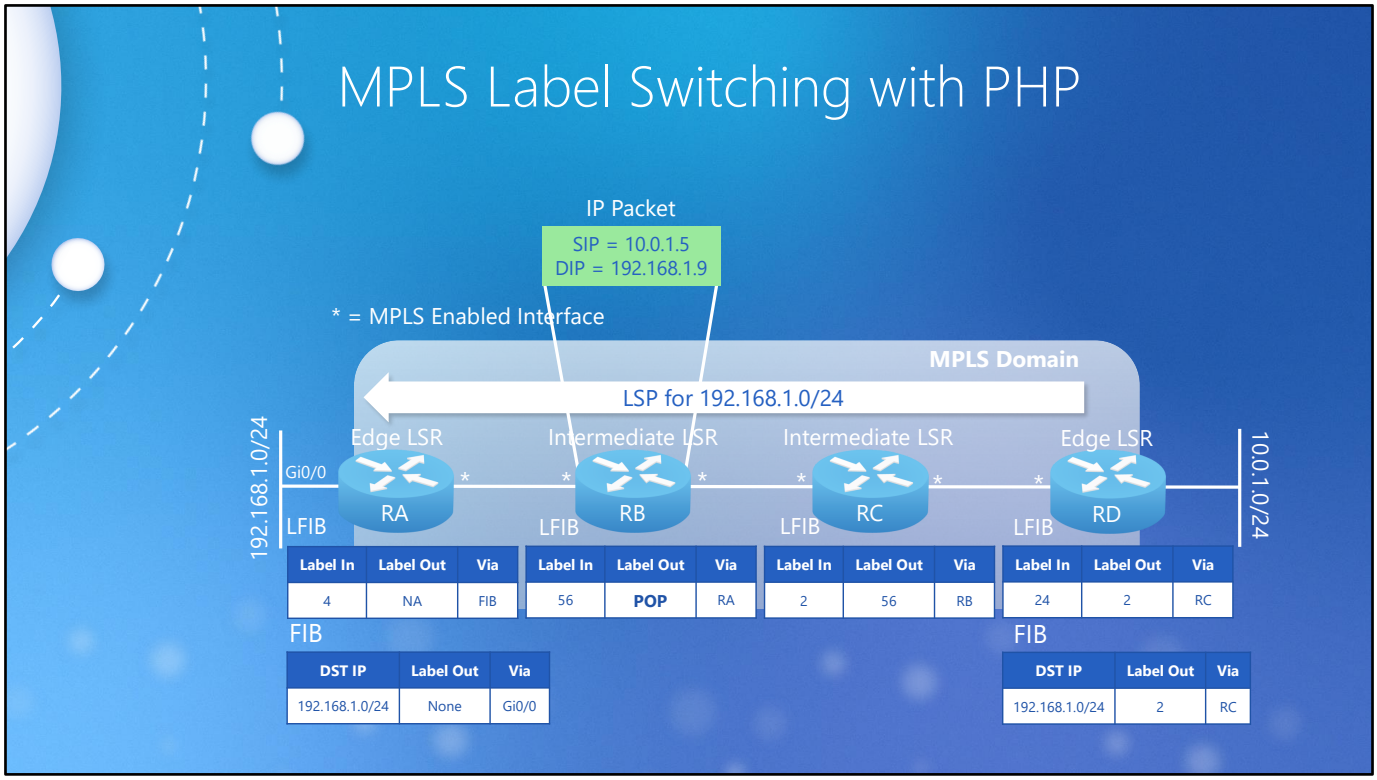
PHP - A feature that enhances the last routers lookup



©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

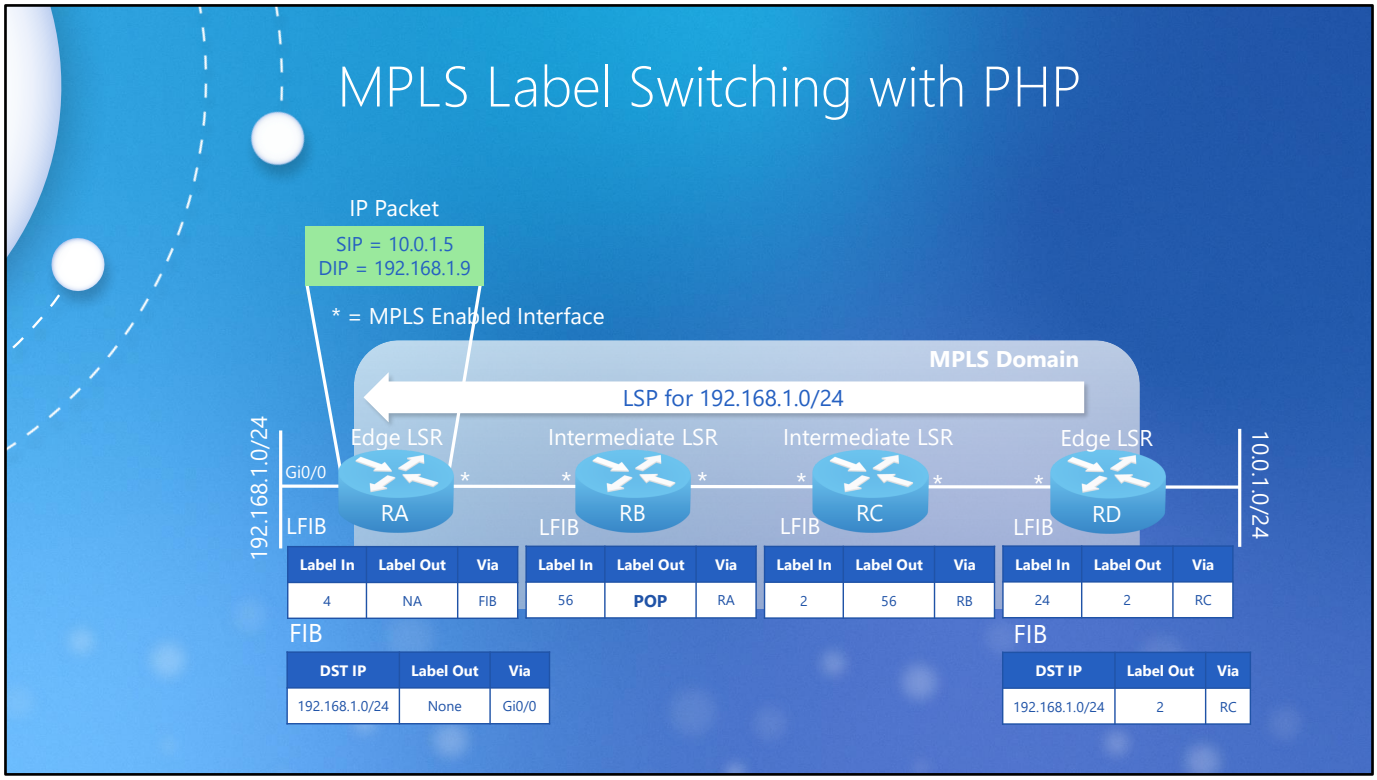


©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

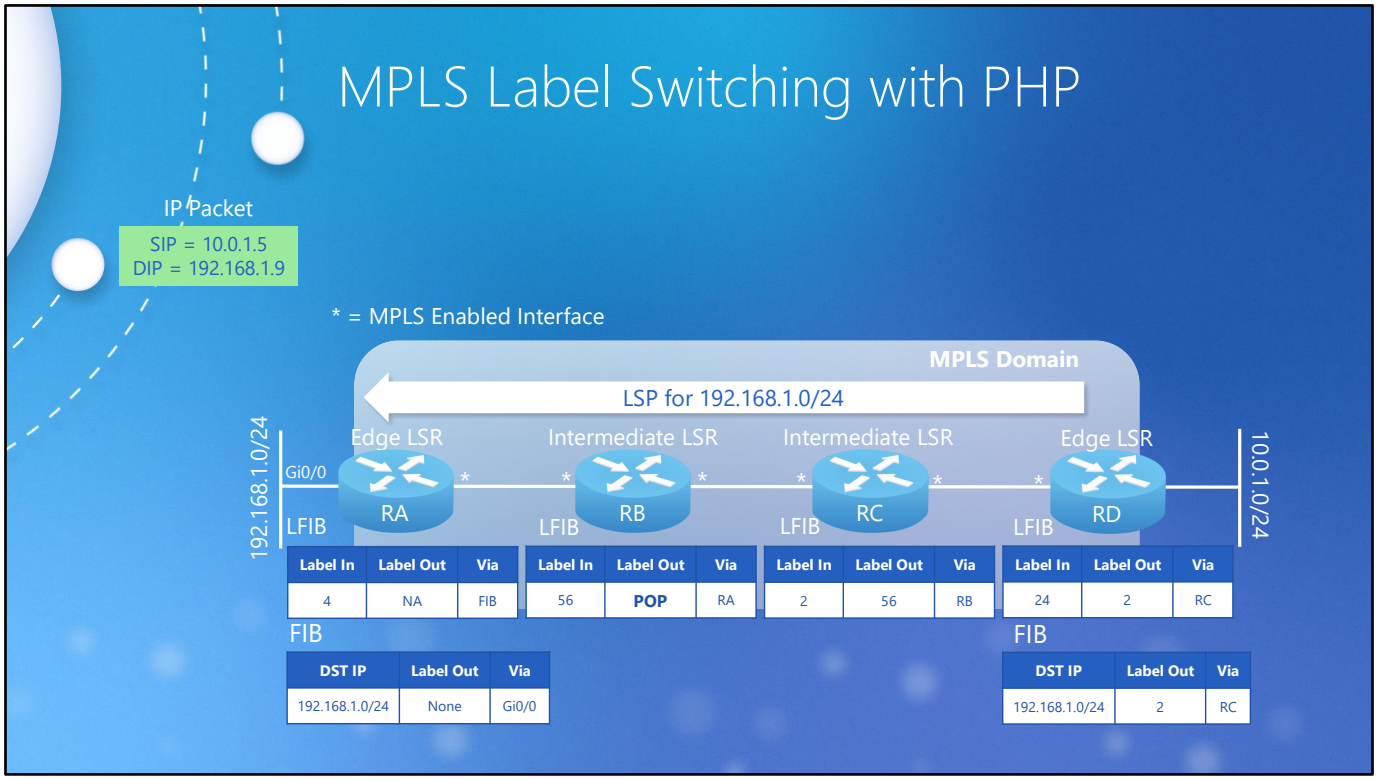


©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

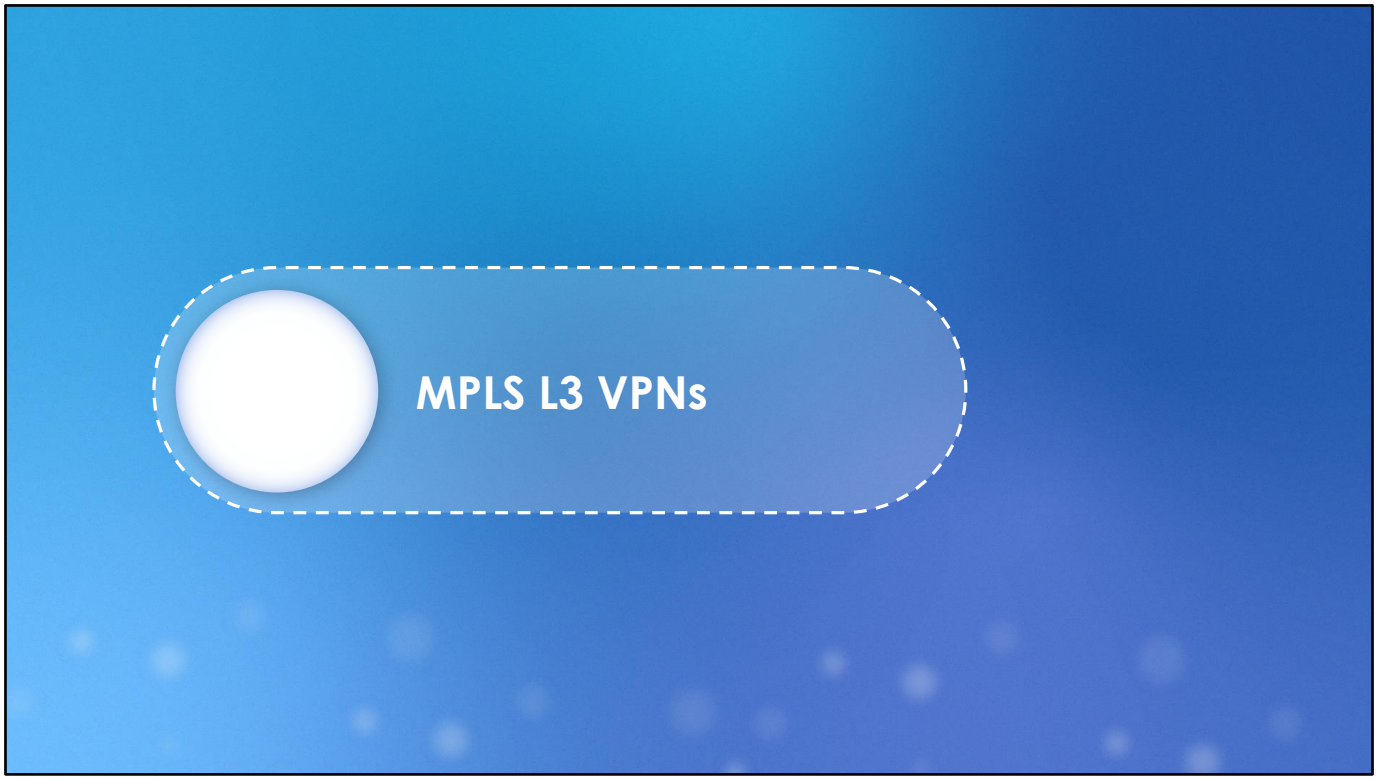
MPLS Label Switching with PHP



©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

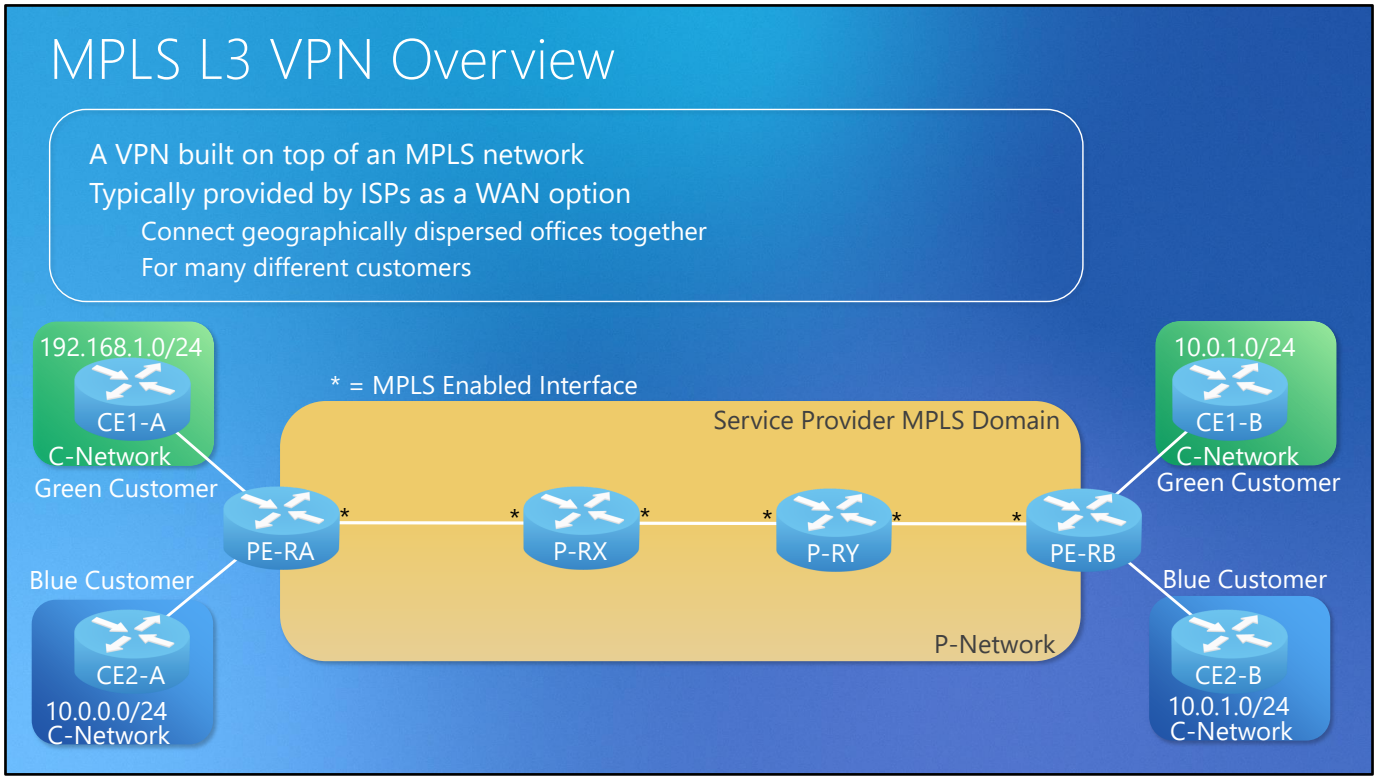


©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



2.2 Describe MPLS Layer 3 VPN

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



An MPLS Layer 3 VPN allows for the provisioning of secure, scalable, and isolated virtual private network services over an MPLS backbone.

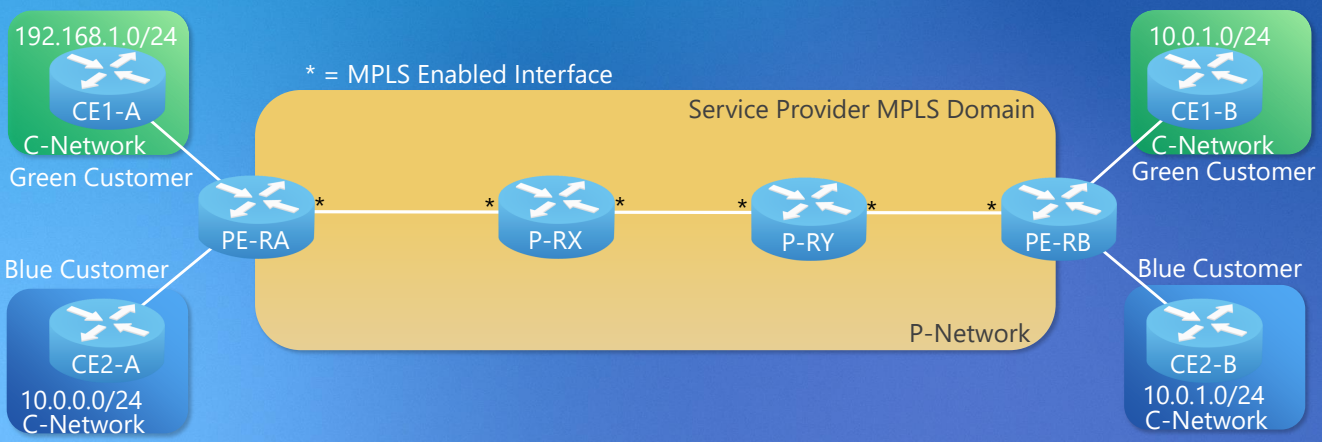
In an MPLS L3 VPN, the service provider's network is responsible for routing customer packets, leveraging MPLS technology to create virtualized, isolated routing instances for each VPN customer. This ensures that the traffic of different customers is kept separate, even though it may traverse the same physical infrastructure.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

MPLS L3 VPN Overview

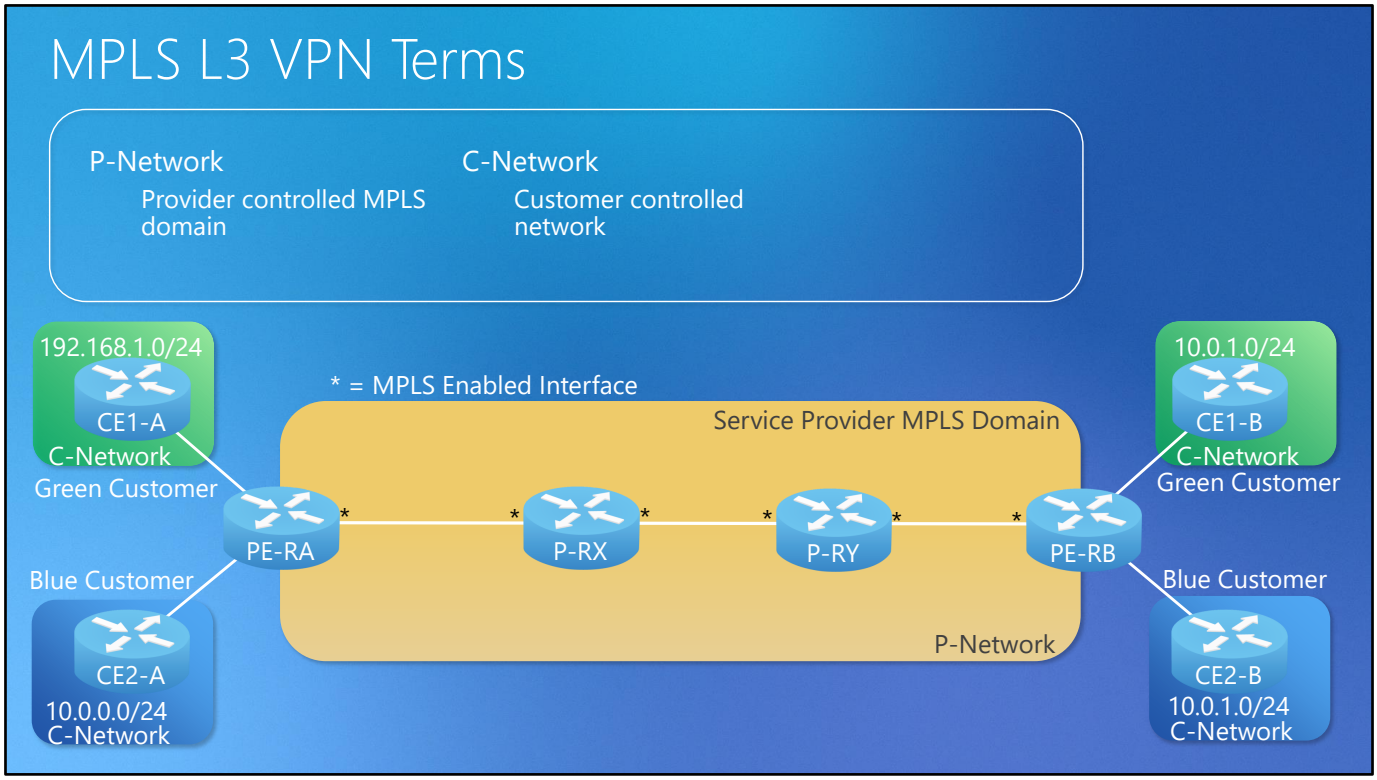
Allows for customer sites to learn of routes from their other sites.

Allows for customer traffic to be routed from one site to another.

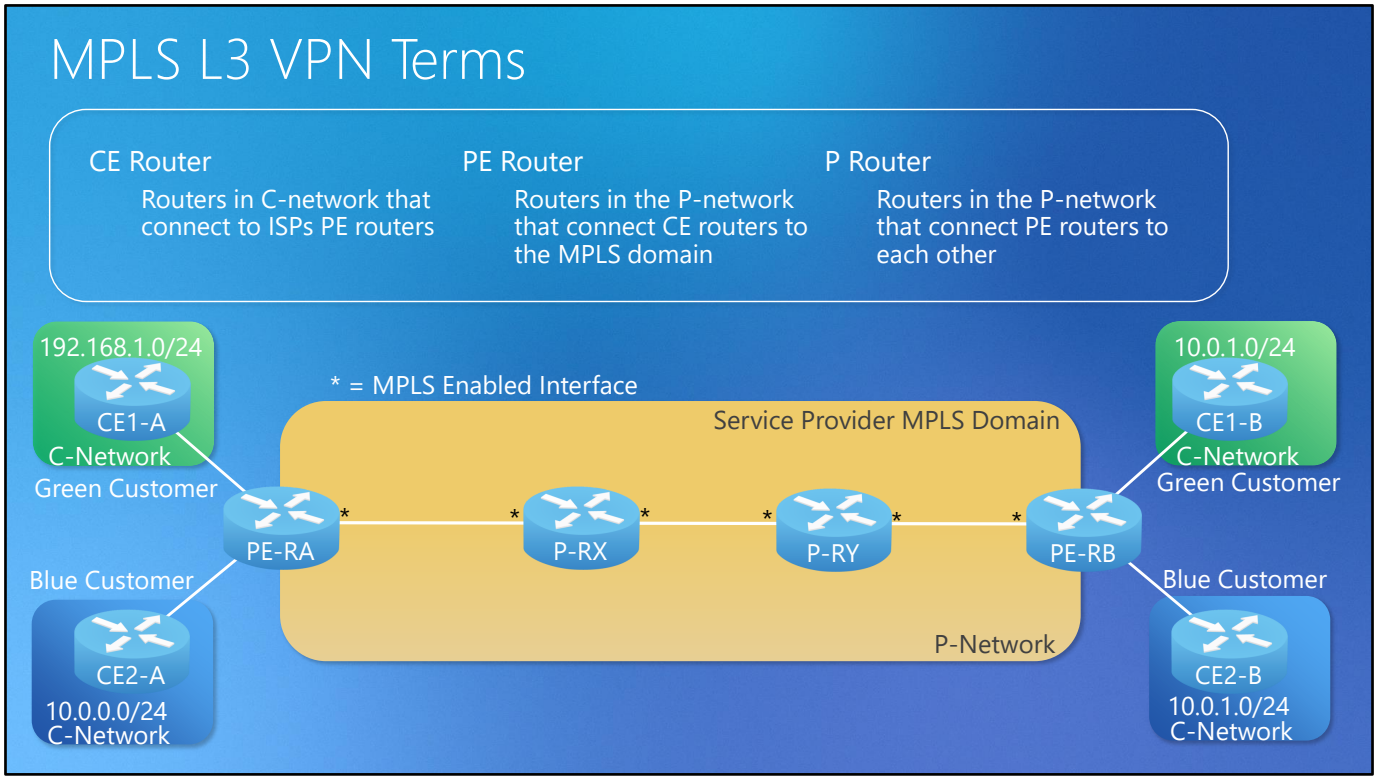


©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

MPLS L3 VPN Terms

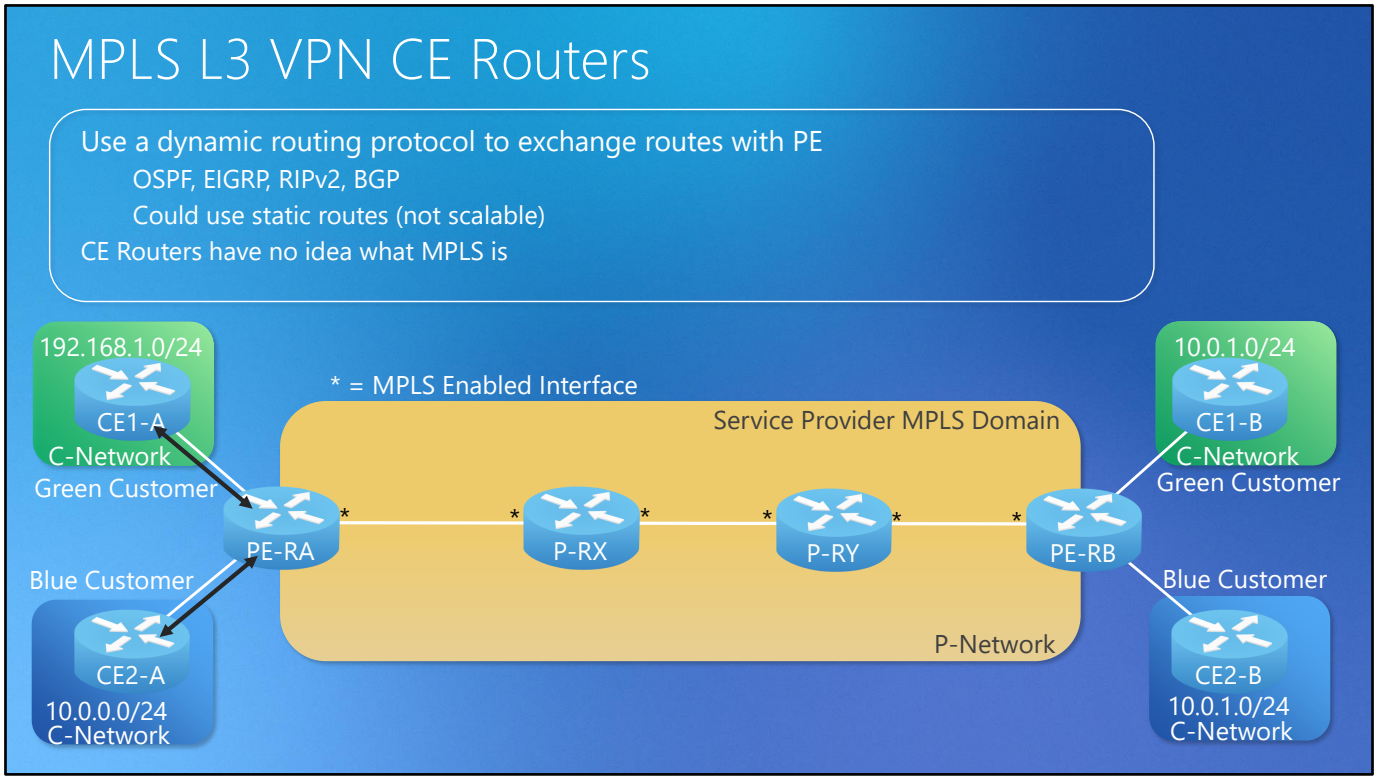


©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



PE = edge LSR
P = intermediate LSR

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

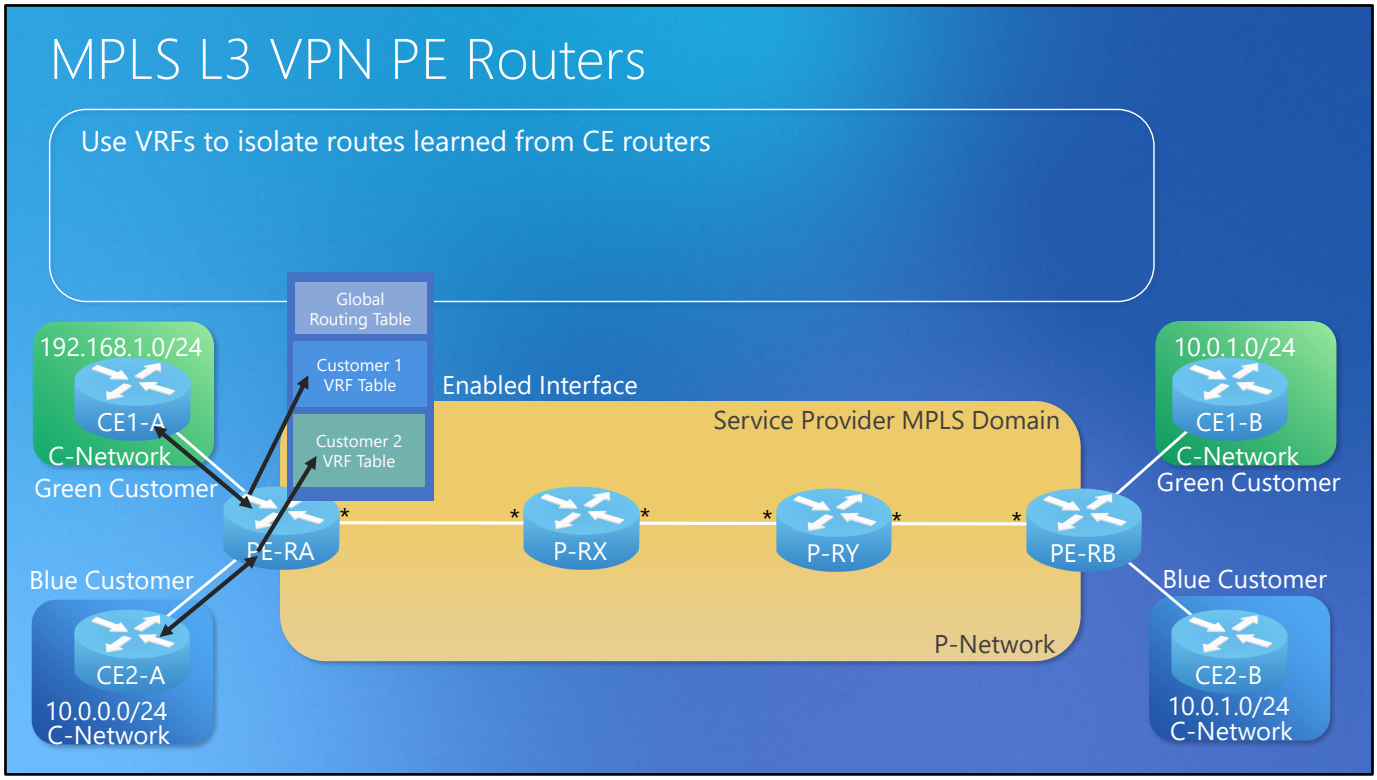


CE routers have no idea what MPLS is. ☺

PE = edge LSR
P = intermediate LSR

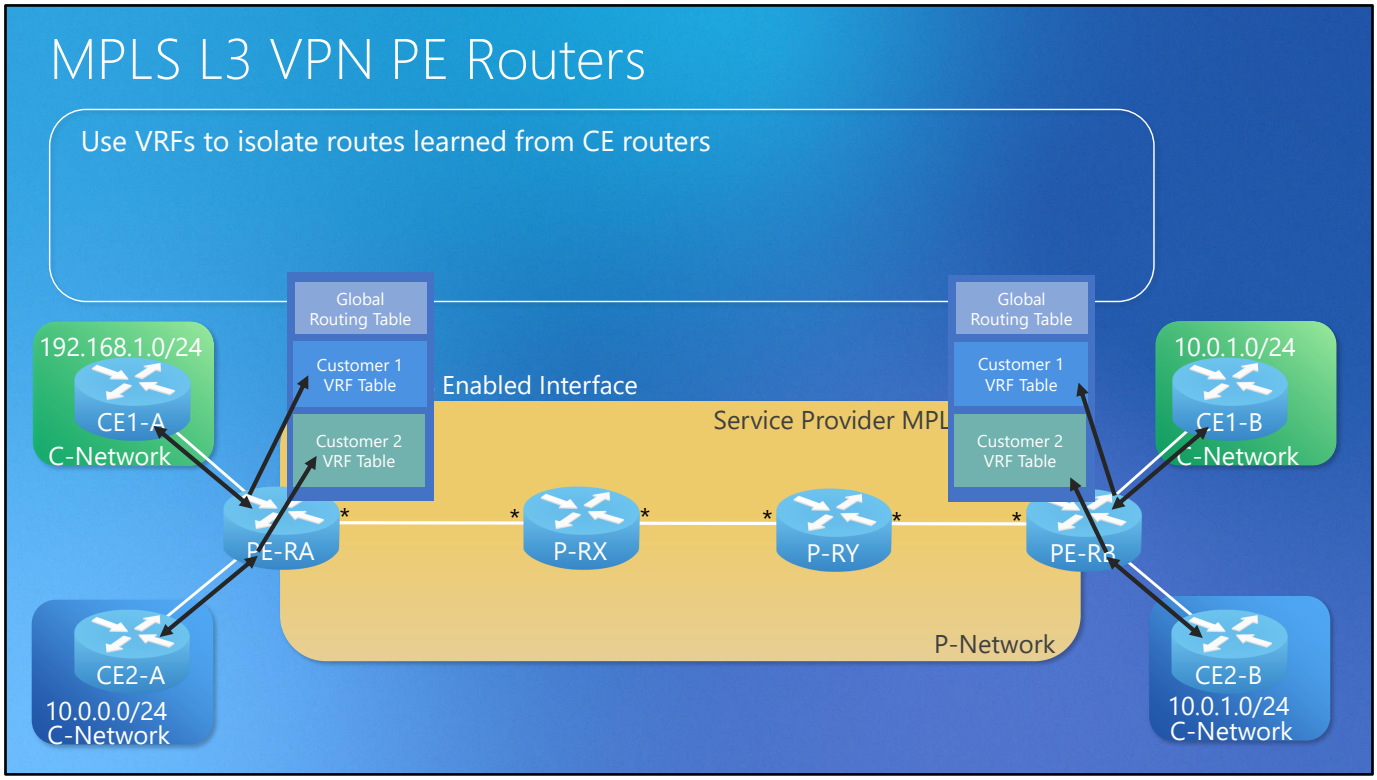
RIPv2 with multiple contexts on the PE
OSPF with multiple process on the PE
BGP with multiple contexts
EIGRP with multiple contexts

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



The global routing table will be used for core routing through the MPLS domain (P-Network)

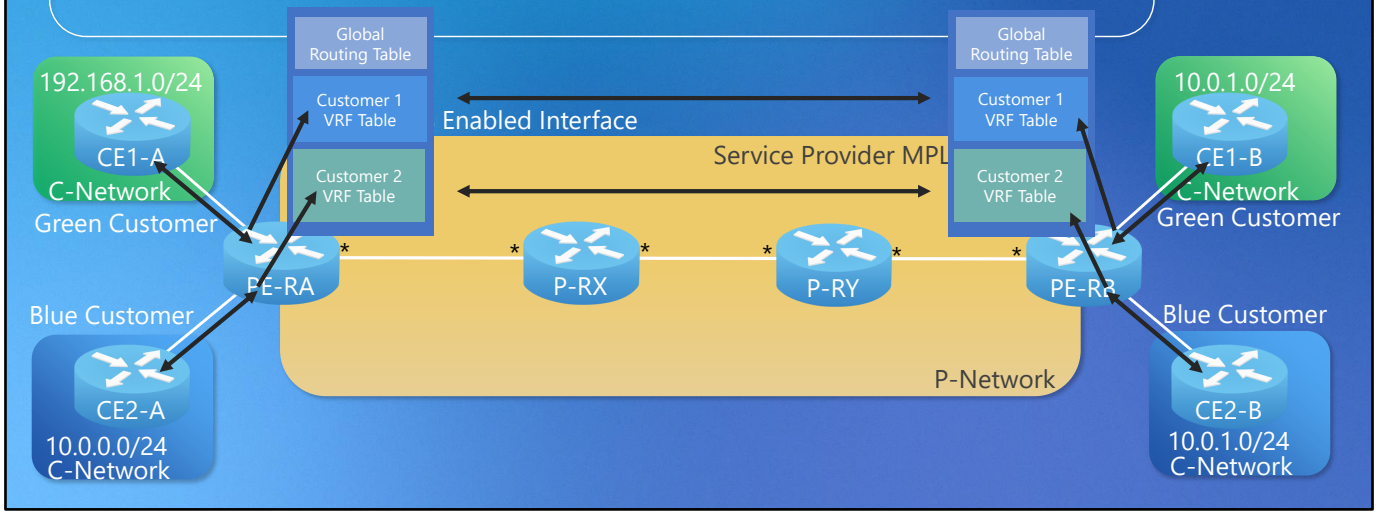
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



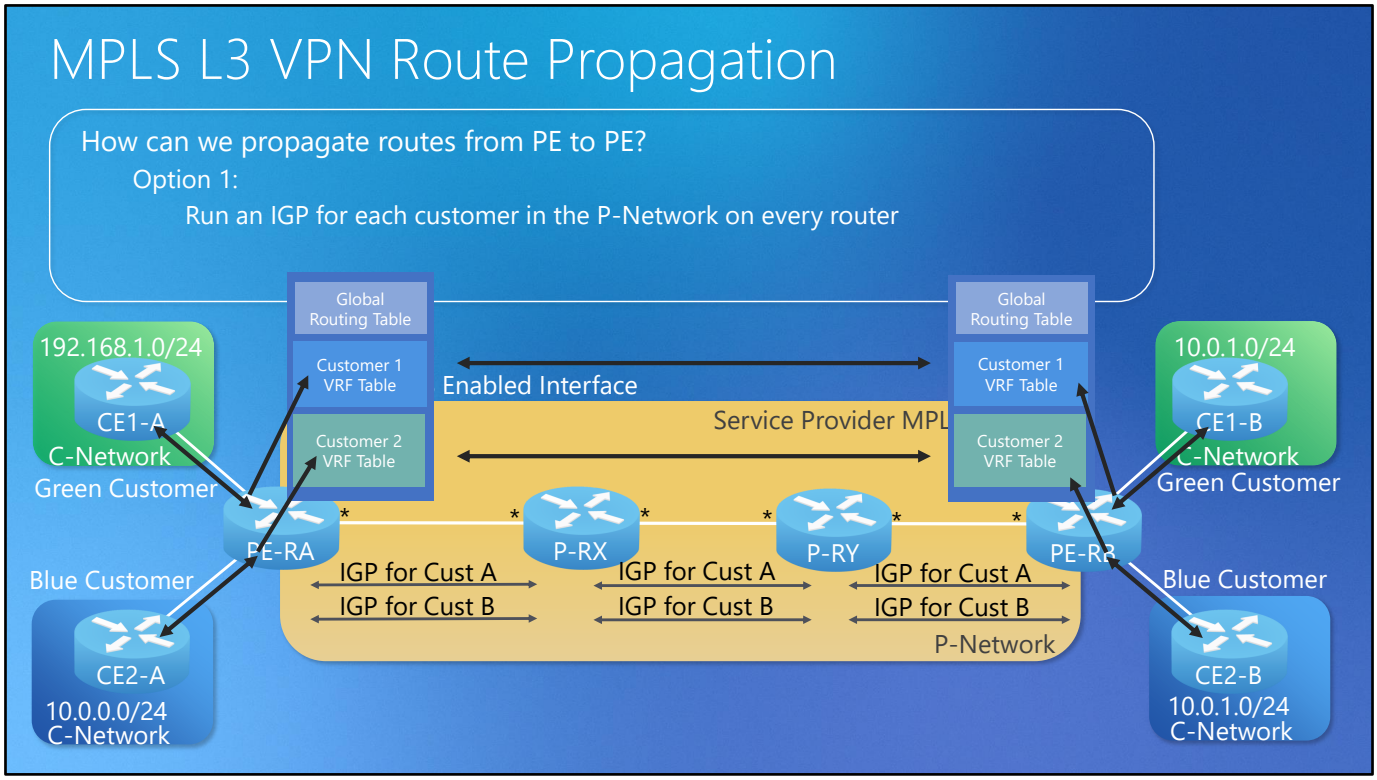
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

MPLS L3 VPN Route Propagation

How can we propagate routes from PE to PE?

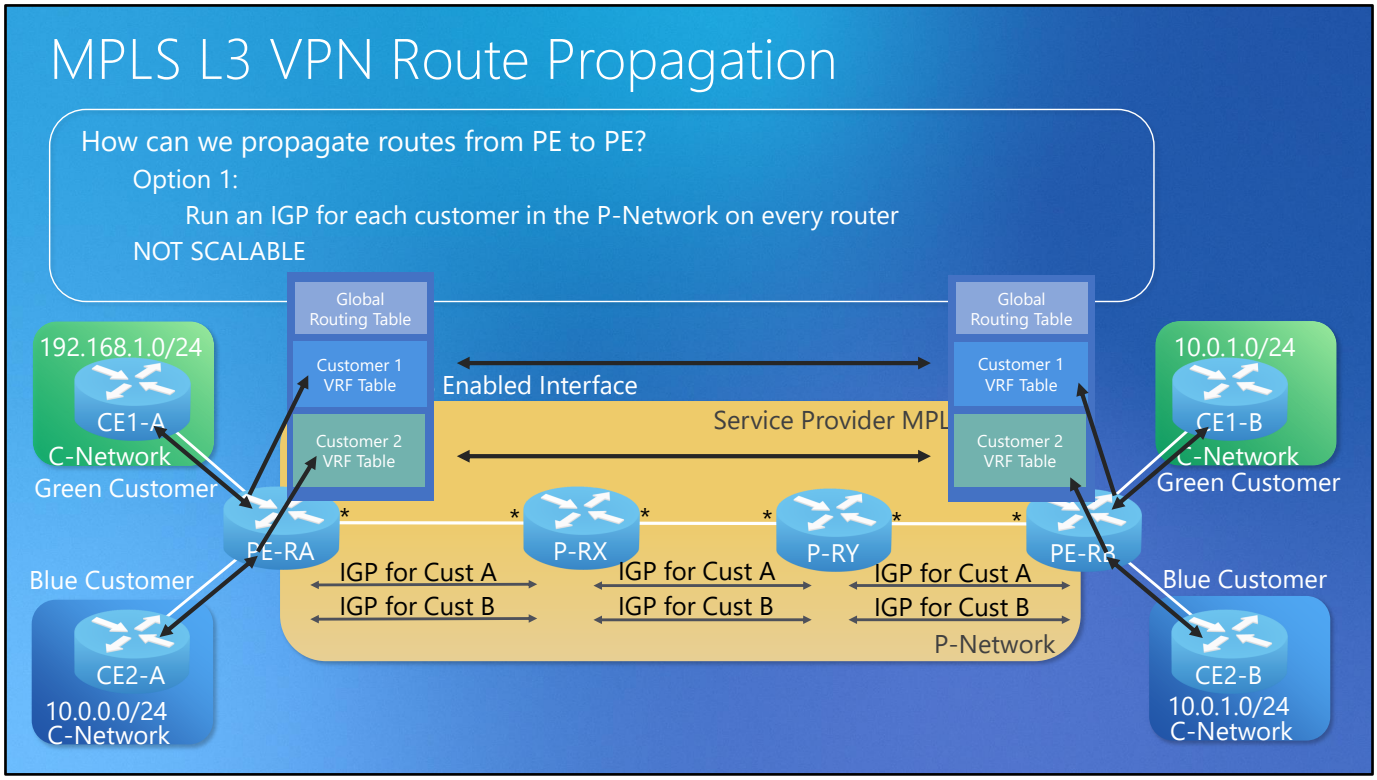


©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Essentially vrf lite

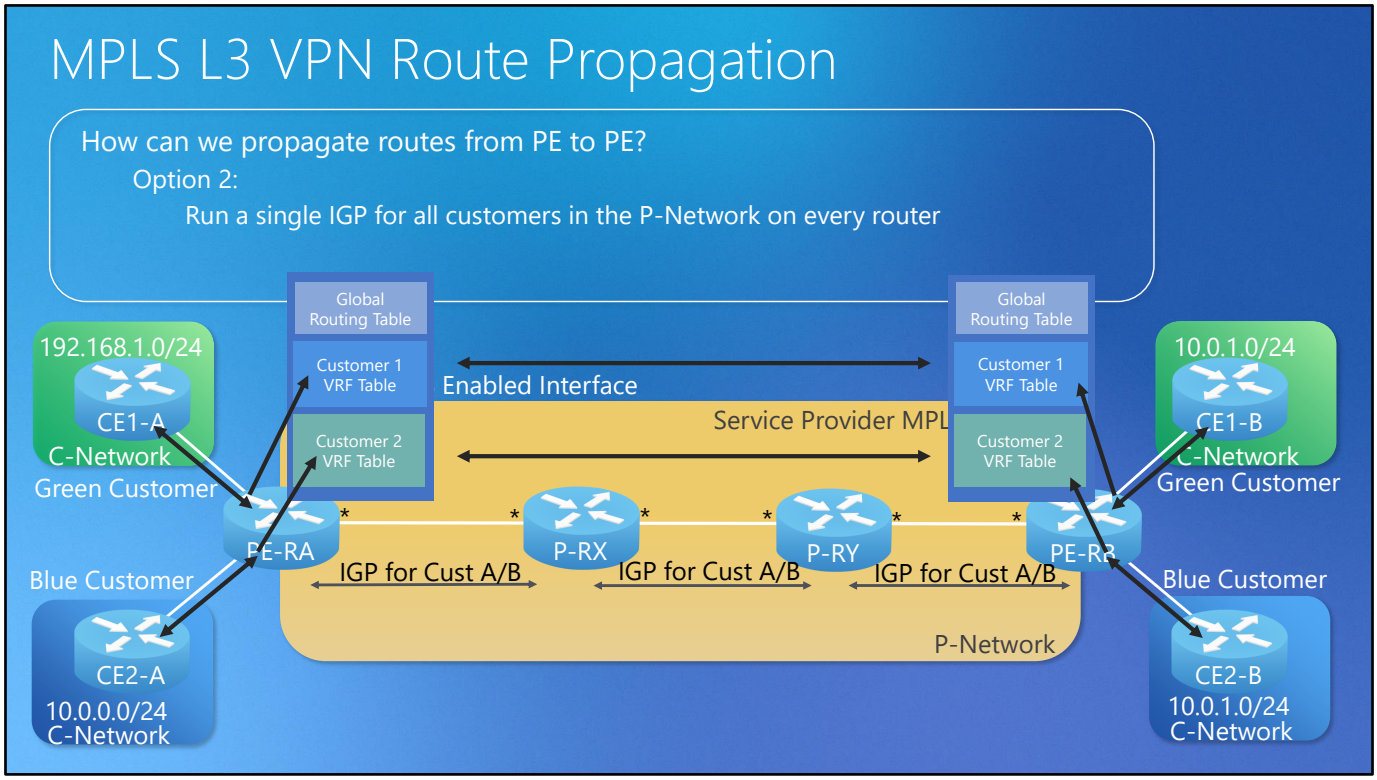
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



NOT scalable and all P routers have to learn all Customer ROUTES which can be resource intensive and a security issue.

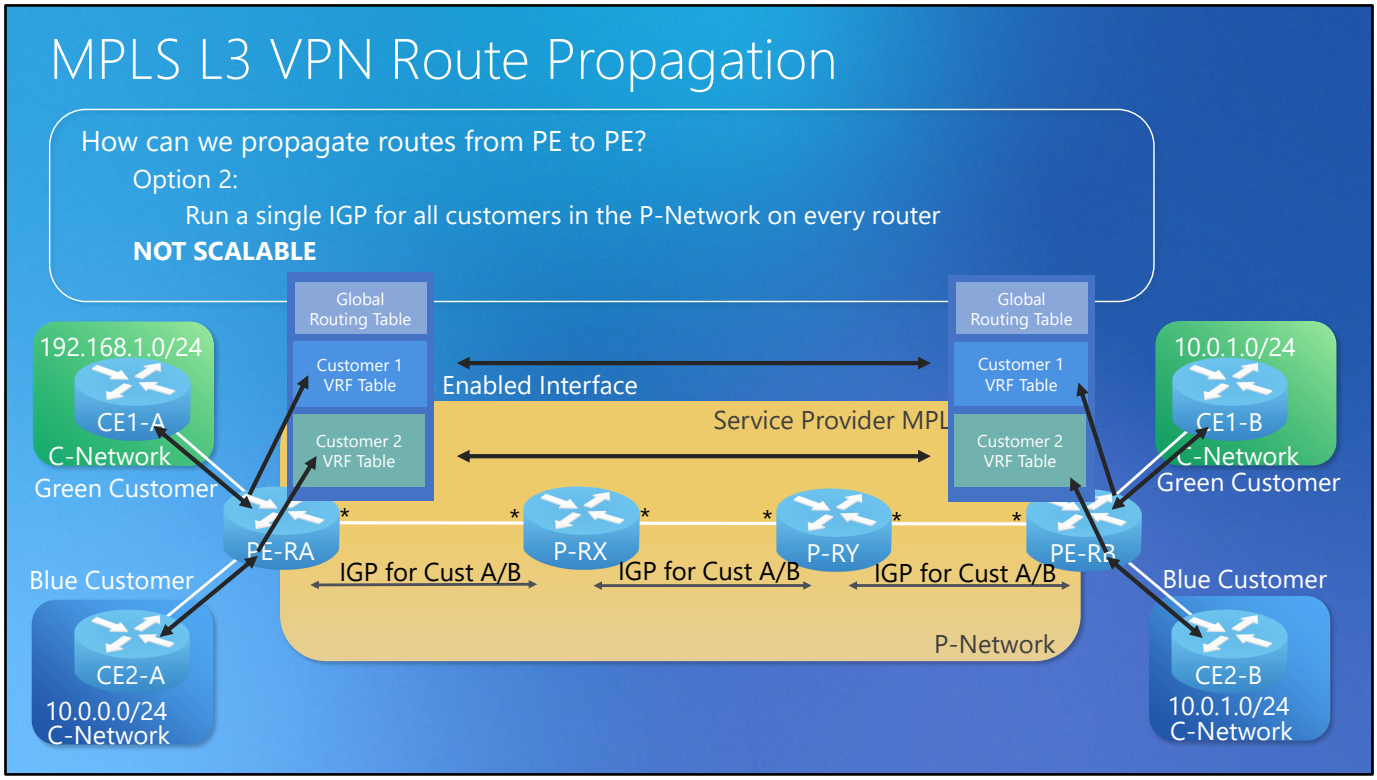
If we have hundreds of routers in the MPLS domain and a single new site is added we have to adjust all routers.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Better than the last option but still NOT scalable and all P routers have to learn all Customer ROUTES which can be resource intensive and a security issue.

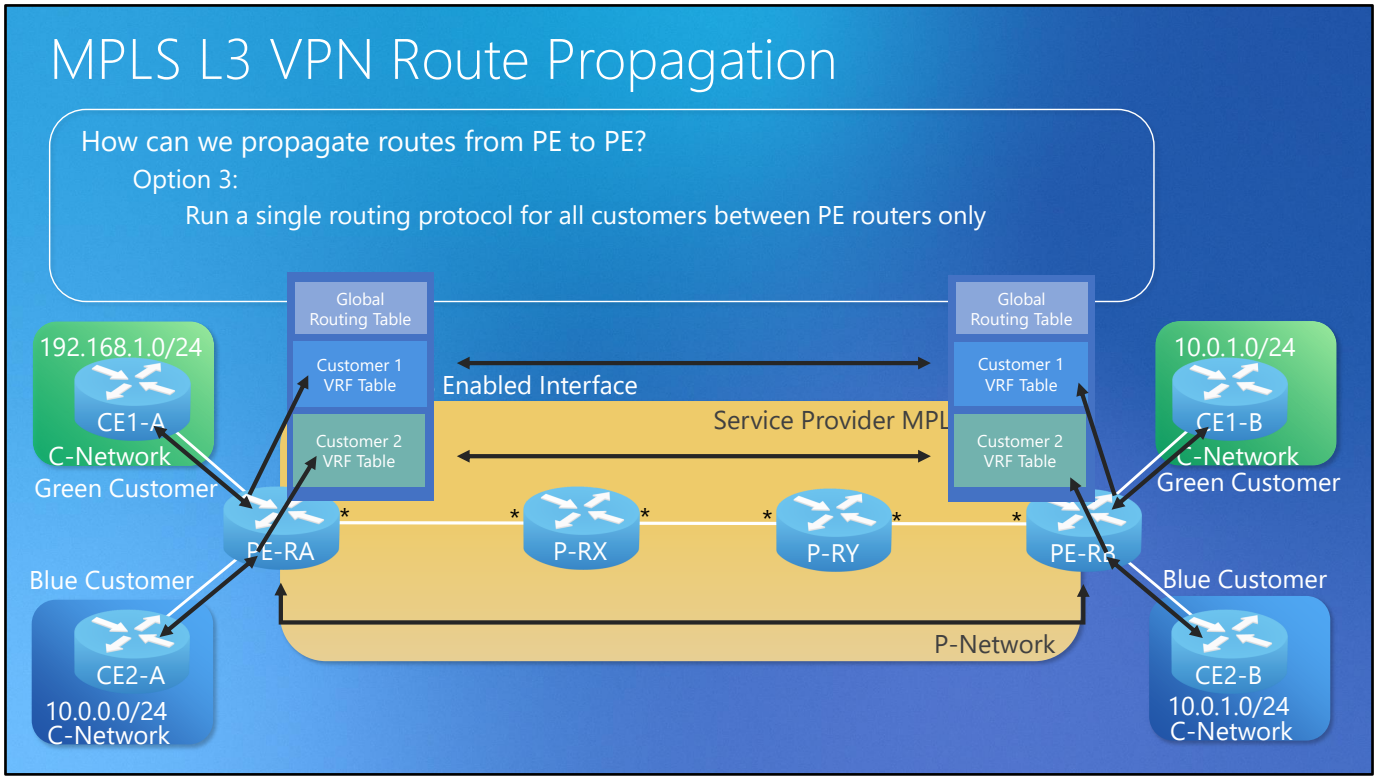
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Better than the last option but still NOT scalable and all P routers have to learn all Customer ROUTES which can be resource intensive and a security issue.

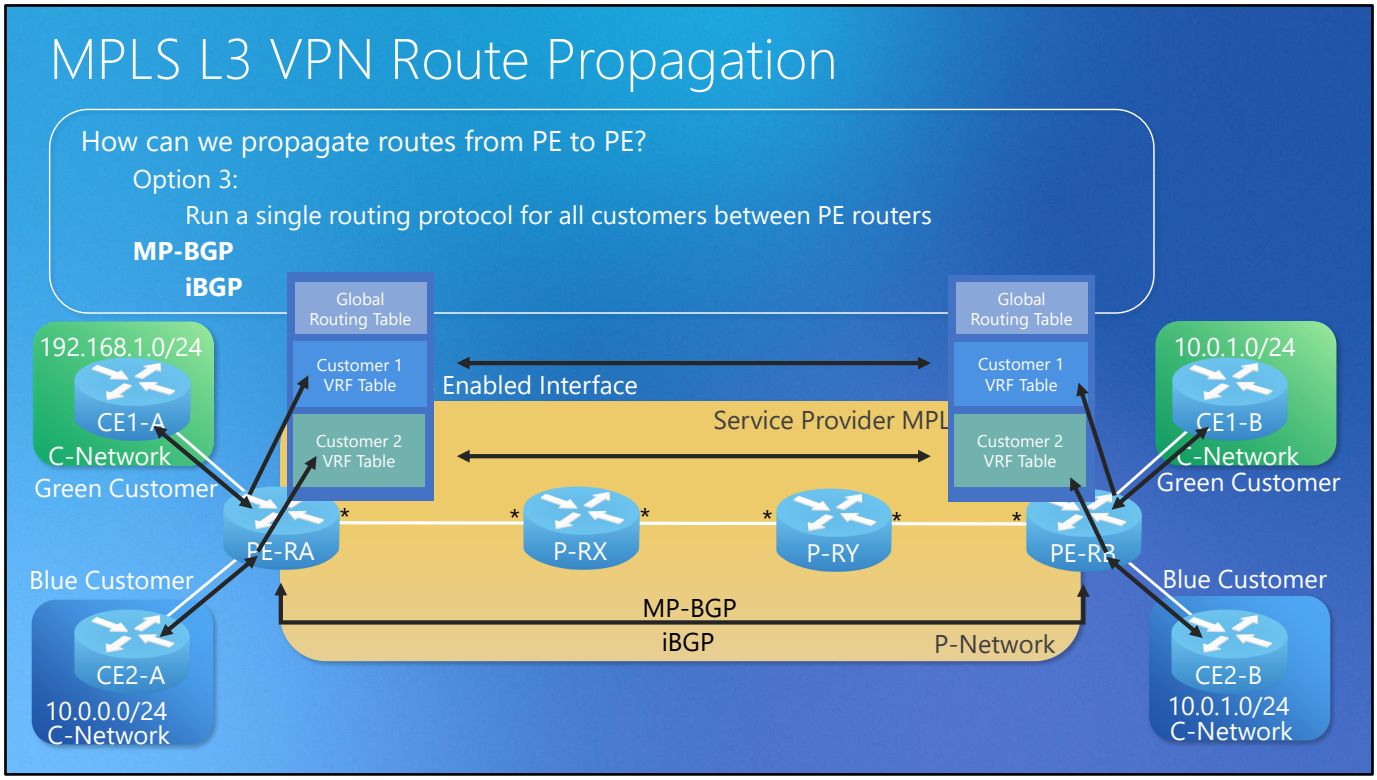
If we have hundreds of routers in the MPLS domain and a single new site is added we have to adjust all routers.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Scalable – P routers do not learn of customer routes.
Regardless of the number of customers added or removed only 1 protocol is required

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

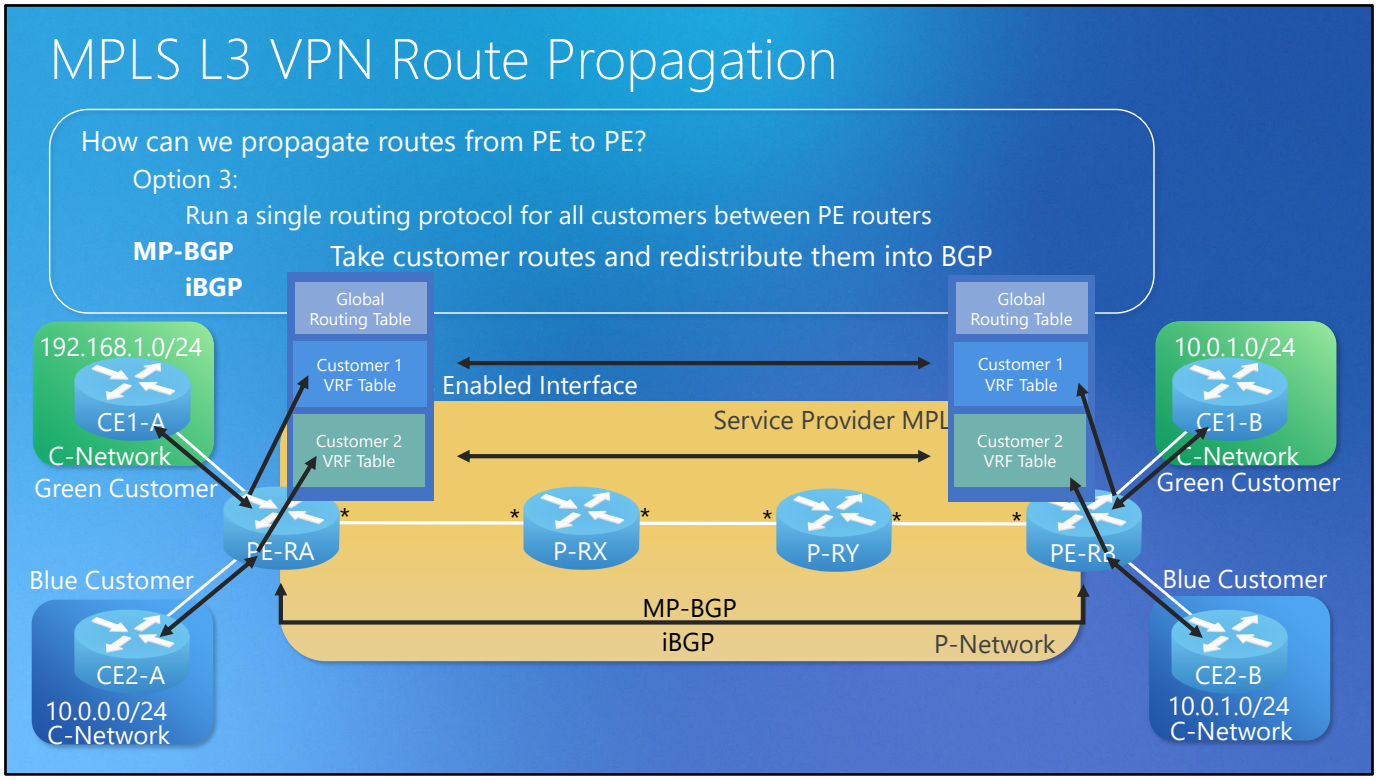


MP-BGP is the best option because it is the most scalable. If we have hundreds of routers in the MPLS domain and a single new site is added we only have to adjust the PE routers.

In this example we are using iBGP because the PE routers are in the same AS. However, if the PE routers are in different ASs then eBGP can be used as well.

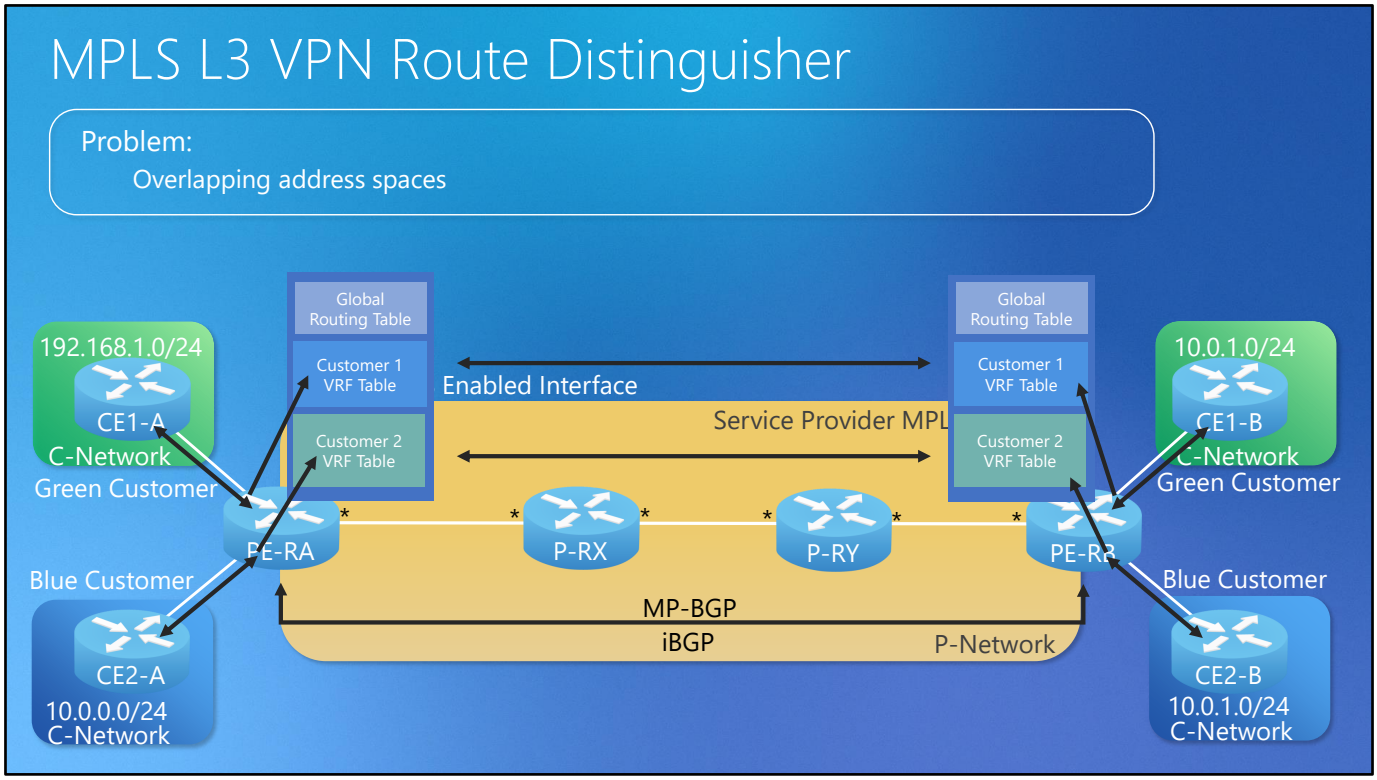
You are subject to the iBGP split horizon rule here. So for complex deployments you might have to do a full mesh of iBGP peerings between the PEs or use a RR.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Take the routes in the VRFs and redistribute them into a single instance of BGP.

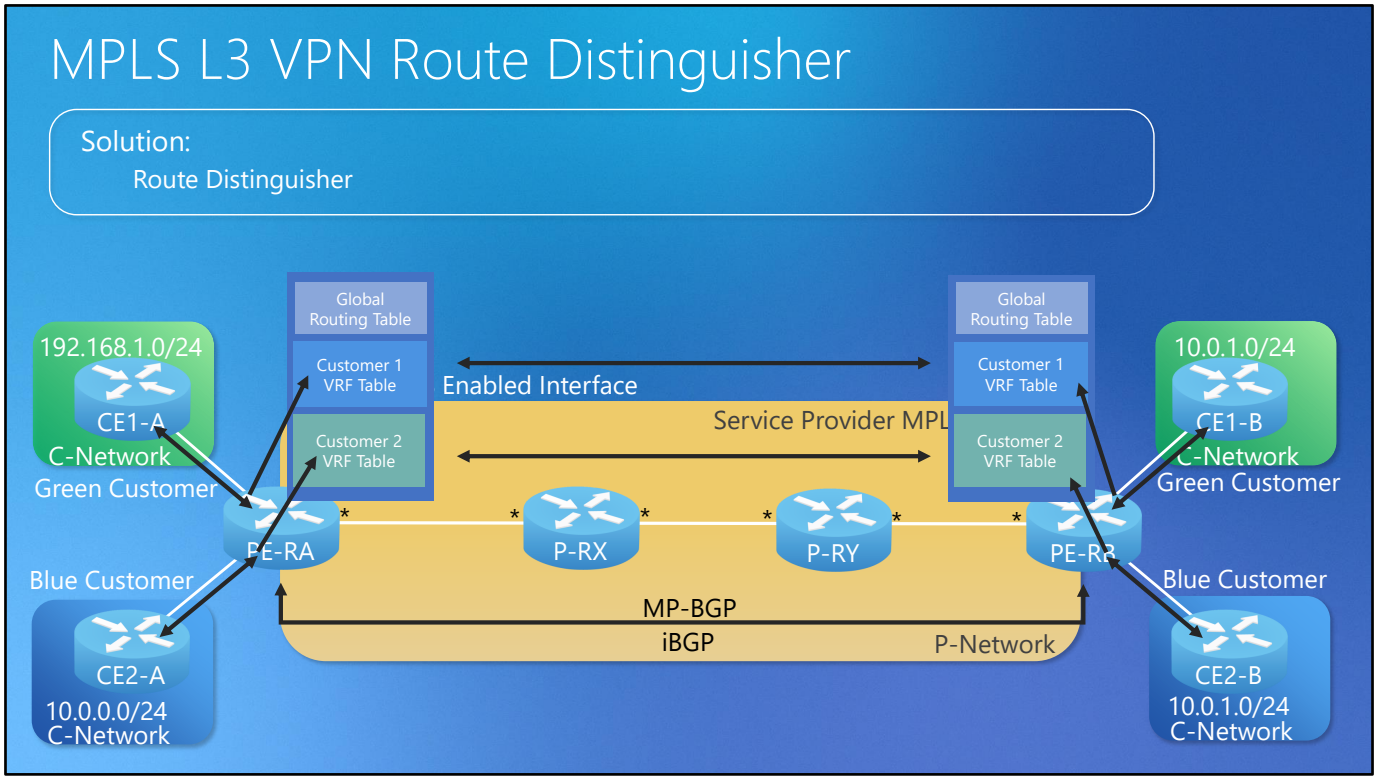
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



10.0.1.0/24 is overlapping between Customer 1 and Customer 2.

So when we redistribute into BGP…. how does BGP deal with these overlapping address spaces and make them unique?

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

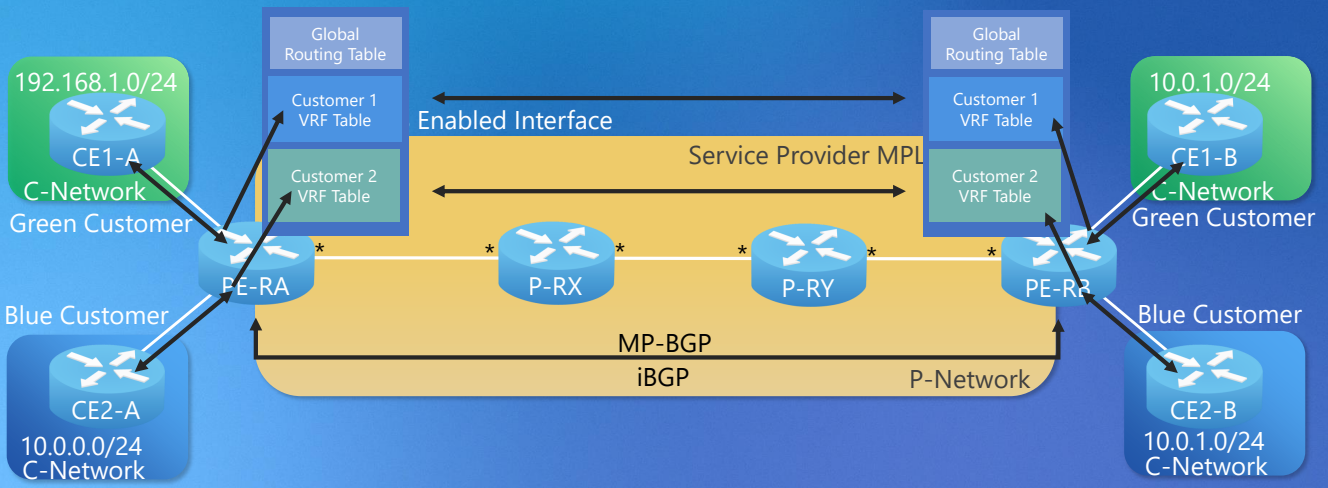


A Route Distinguisher (RD) is a key concept in the context of MPLS (Multiprotocol Label Switching) VPNs, specifically within Layer 3 VPNs. It is an identifier added to the IP addresses of customer routes, allowing multiple customers to use the same IP address space without causing IP address conflicts within the service provider's network. The RD makes identical addresses distinct across the MPLS network, enabling the coexistence of overlapping IP addresses from different VPNs on the same network infrastructure.

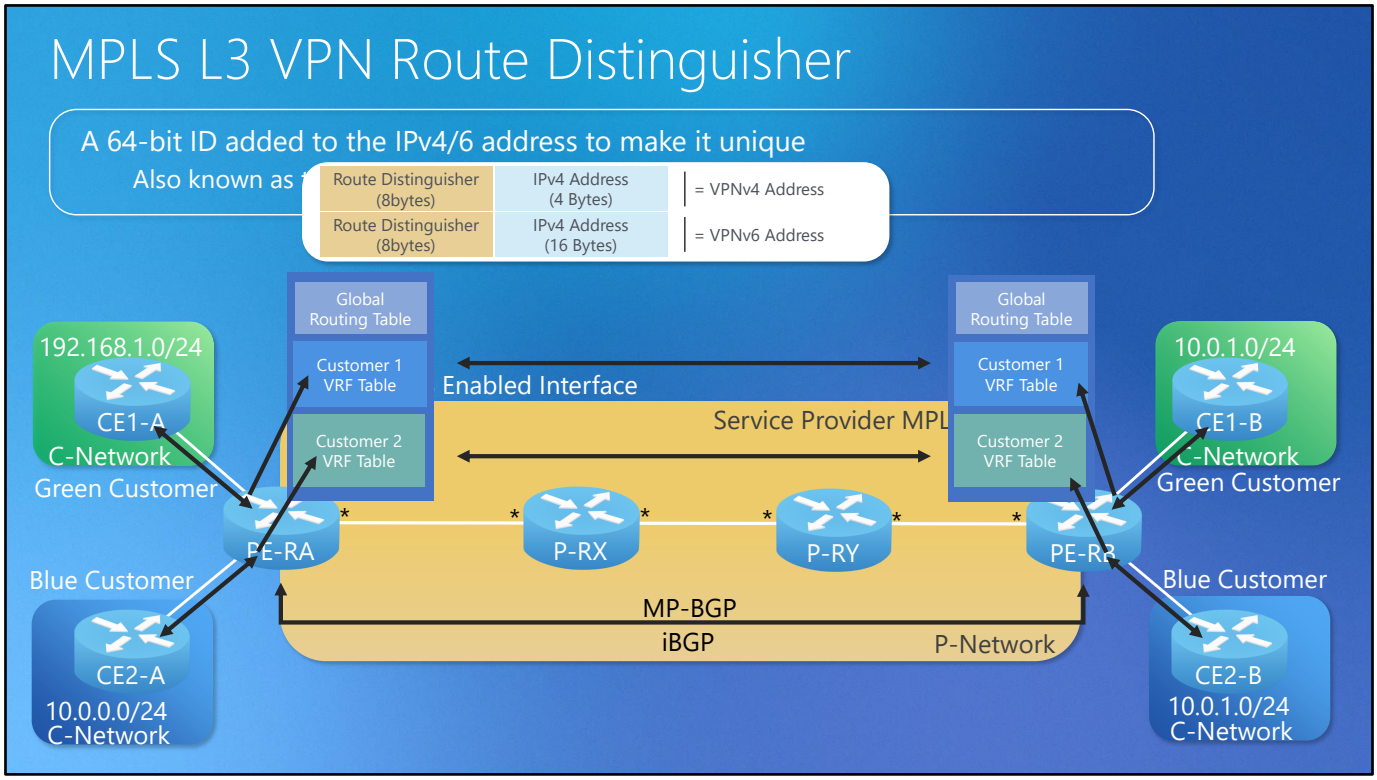
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

MPLS L3 VPN Route Distinguisher

A 64-bit ID added to the IPv4/6 address to make it unique
Also known as the VPN identifier



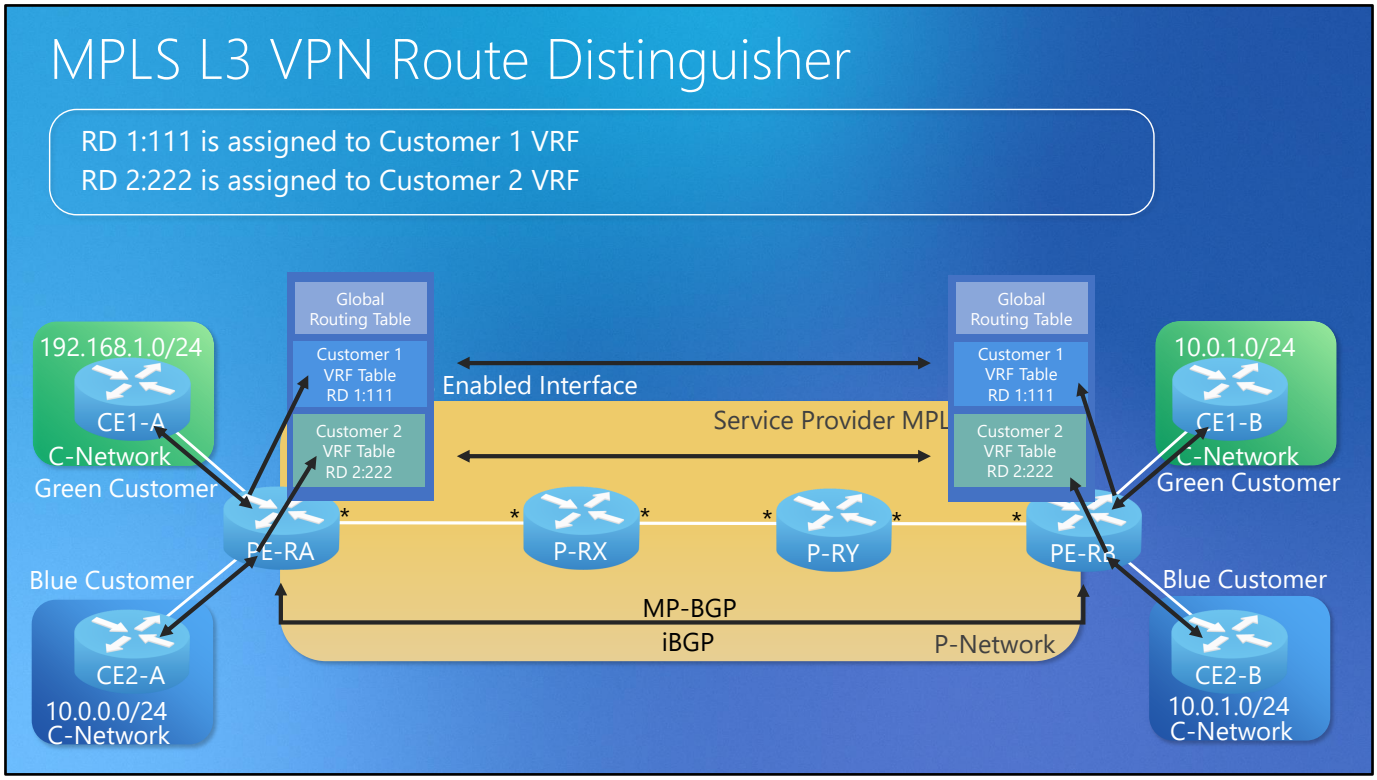
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Since it is a VPN identifier, we now have what are called VPNv4 and VPNv6 address.

Total size for IPv4 = 96bits
Total size for IPv6 = 192bits

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

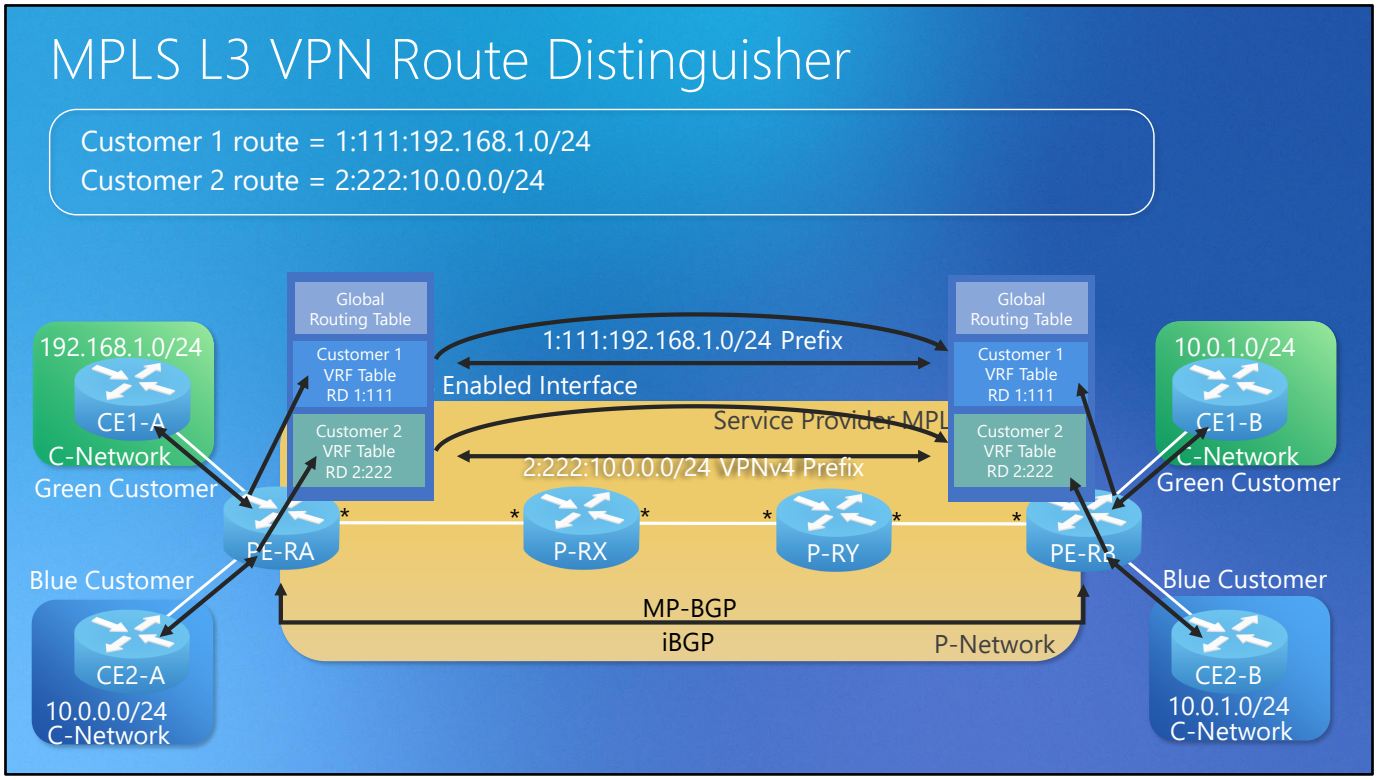


An RD can be composed in several ways, but the most common formats are:

1.ASN:nn (Autonomous System Number: Number): Where "ASN" is a 16-bit autonomous system number and "nn" is a 32-bit number. (65001:100)
2.IP-address:nn (IP Address: Number): Where "IP-address" is a 32-bit IP address and "nn" is a 16-bit number. (192.168.100.1:25)

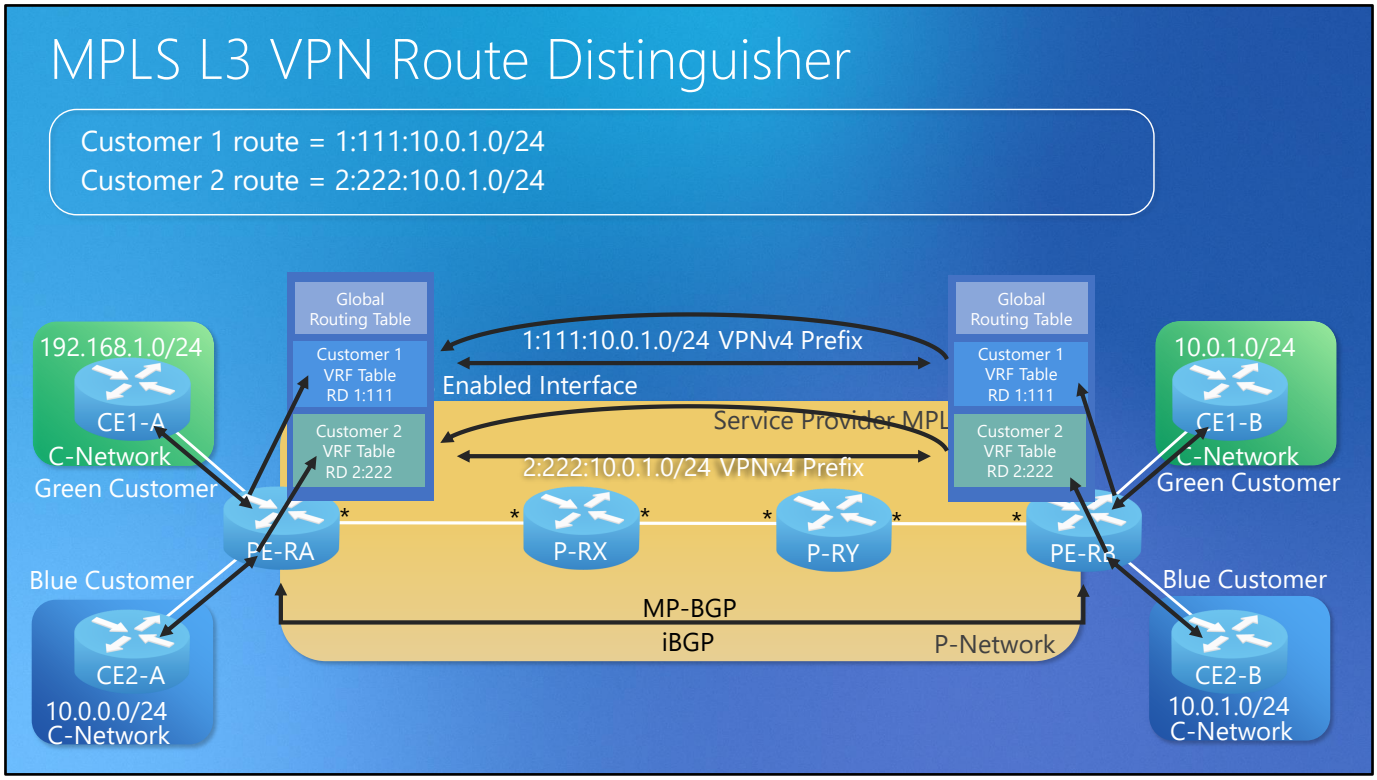
In our case we are going to keep it simple and small and use 1:111 for Cust 1 VRF and 2:222 for Cust 2 VRF.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Now MPBGP can distinguish between the routes especially when they are overlapping.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



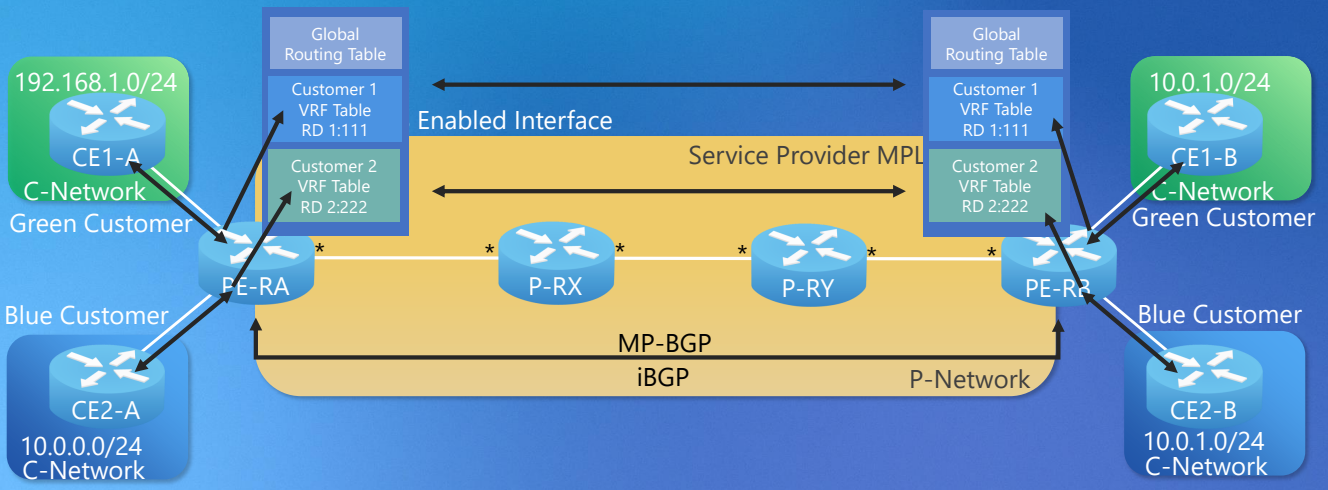
UNIQUE
Now MPBGP can distinguish between the routes especially when they are overlapping.

It now knows exactly what VRF it has to dump them into.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

MPLS L3 VPN Route Target

How do we ensure isolation when sharing routes?

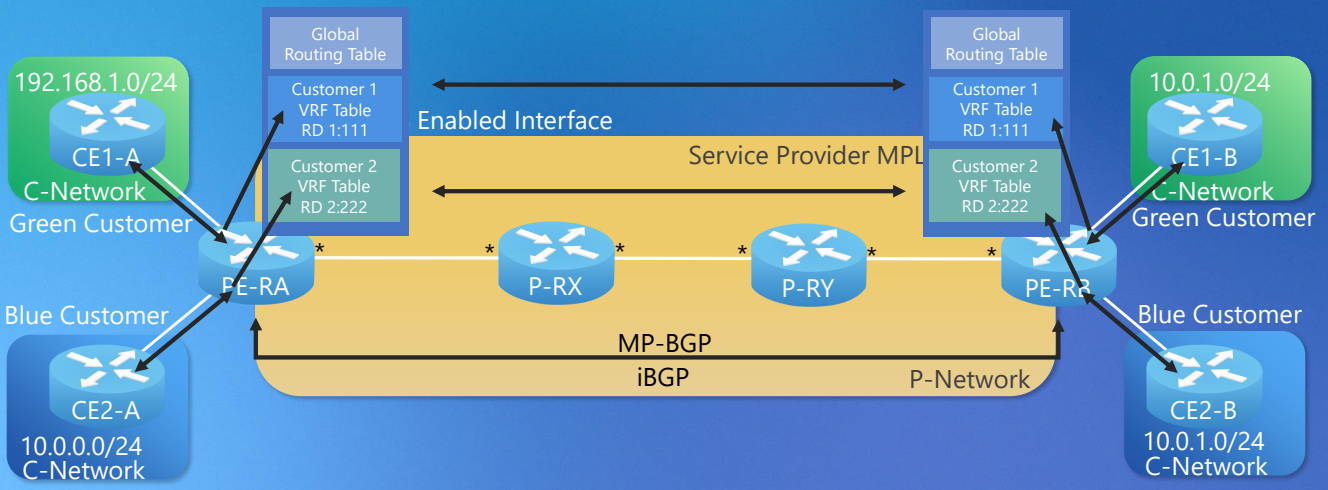


©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

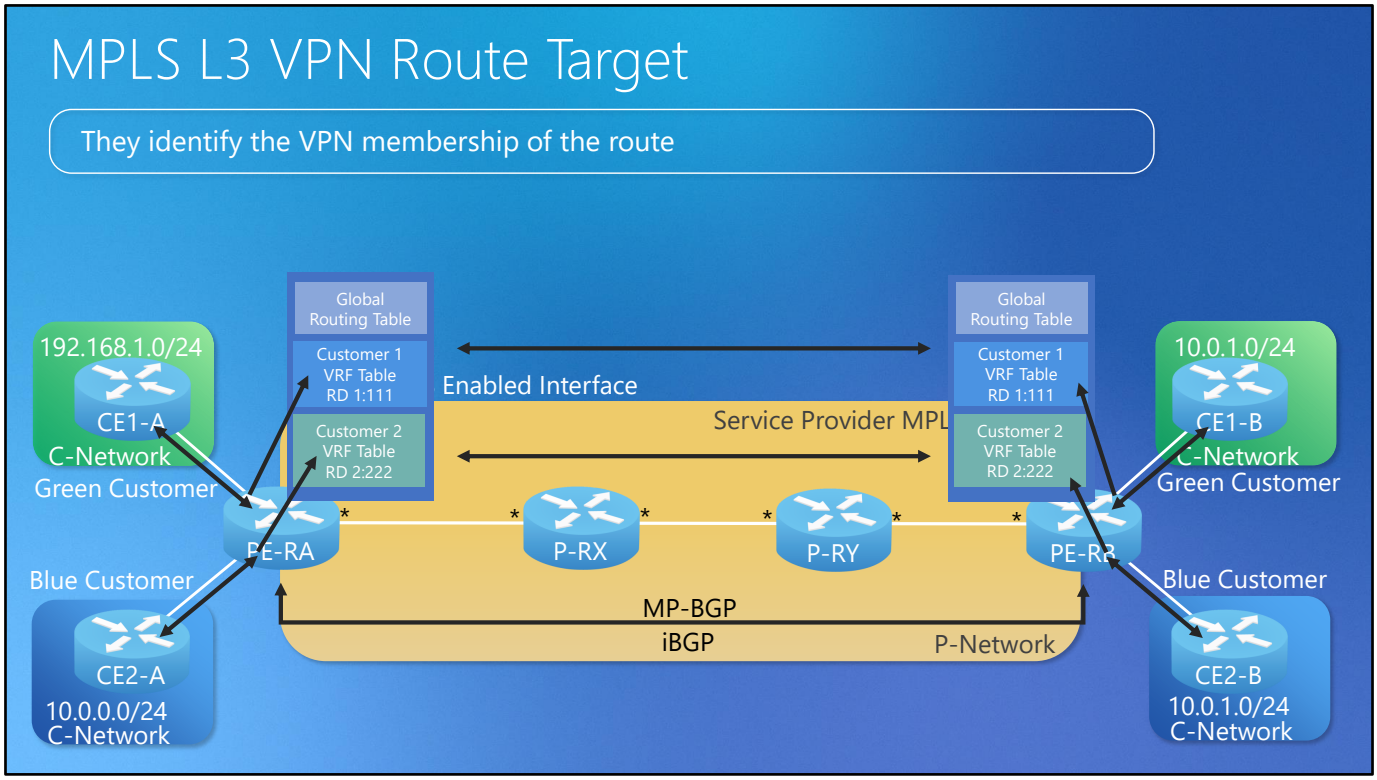
MPLS L3 VPN Route Target

How do we ensure isolation when sharing routes?

Route Targets

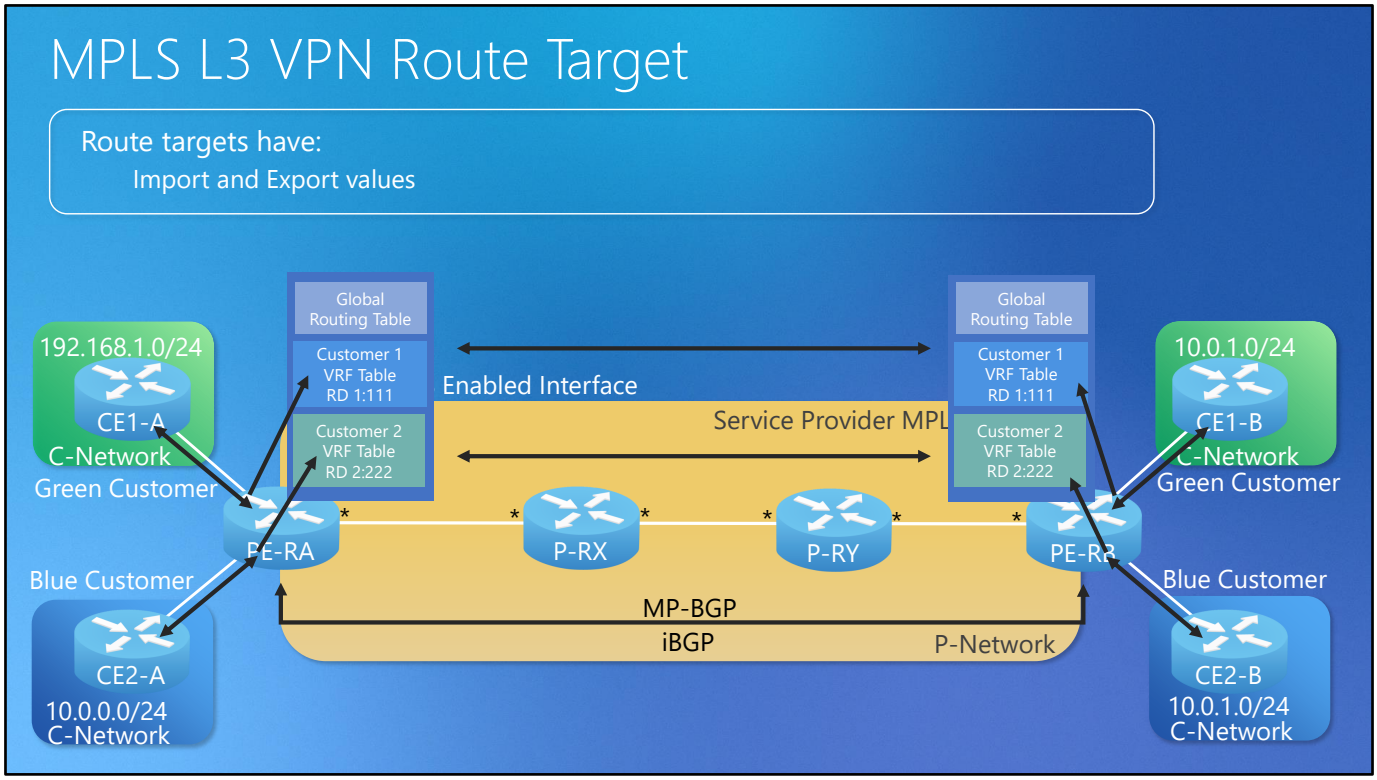


©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



A Route Target (RT) is an extended community attribute used in MPLS VPNs, particularly Layer 3 VPNs, to control the import and export of routes among different Virtual Routing and Forwarding (VRF) instances on Provider Edge (PE) routers.

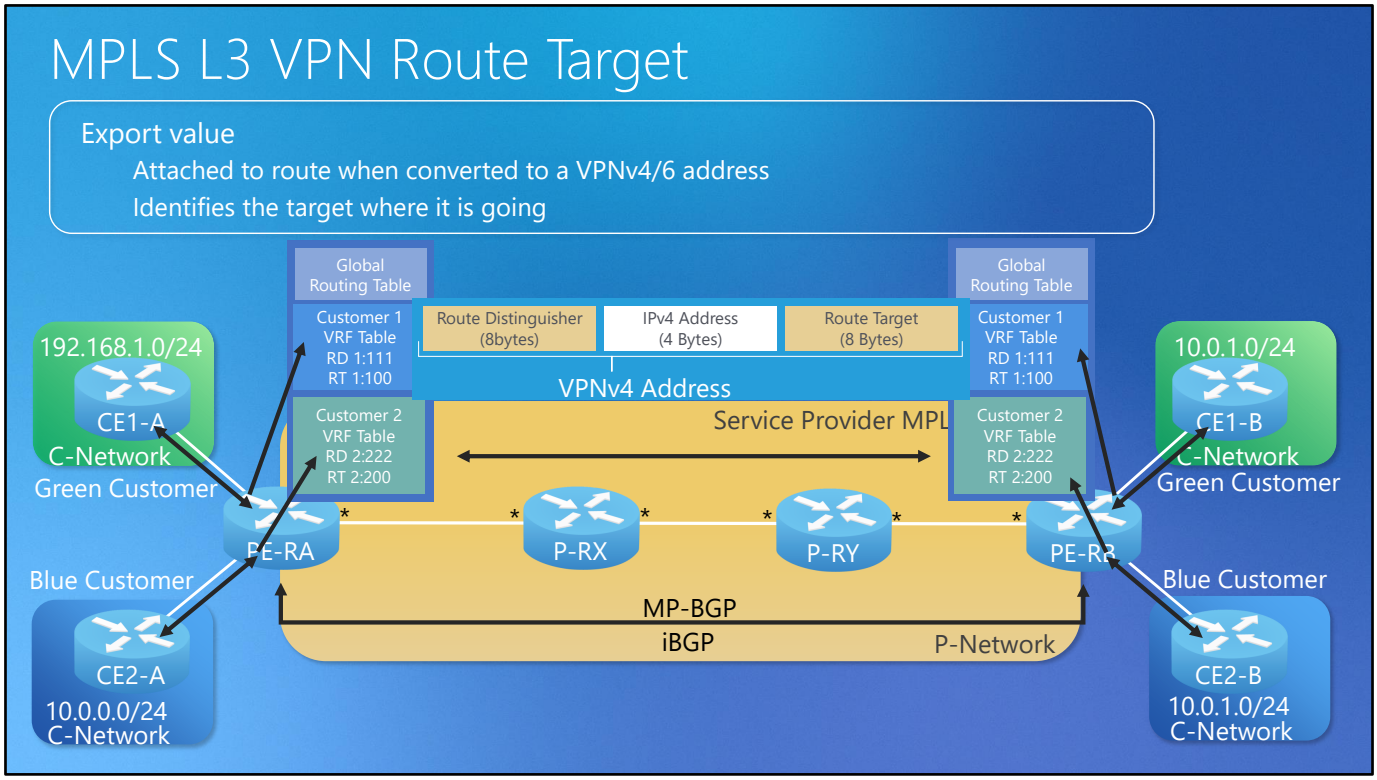
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



While a Route Distinguisher (RD) makes customer routes unique across the MPLS network, the RT plays a crucial role in defining which routes are imported into and exported from a VRF, essentially determining the VPN membership of these routes.

An RT is similar in format to an RD and can be expressed in two main ways:
•**ASN:nn (Autonomous System Number: Number):** For example, 65001:100, where 65001 is the ASN and 100 is a numerical identifier.
•**IP-address:nn (IP Address: Number):** For example, 192.168.100.1:25, where 192.168.100.1 is an IP address and 25 is a numerical identifier.

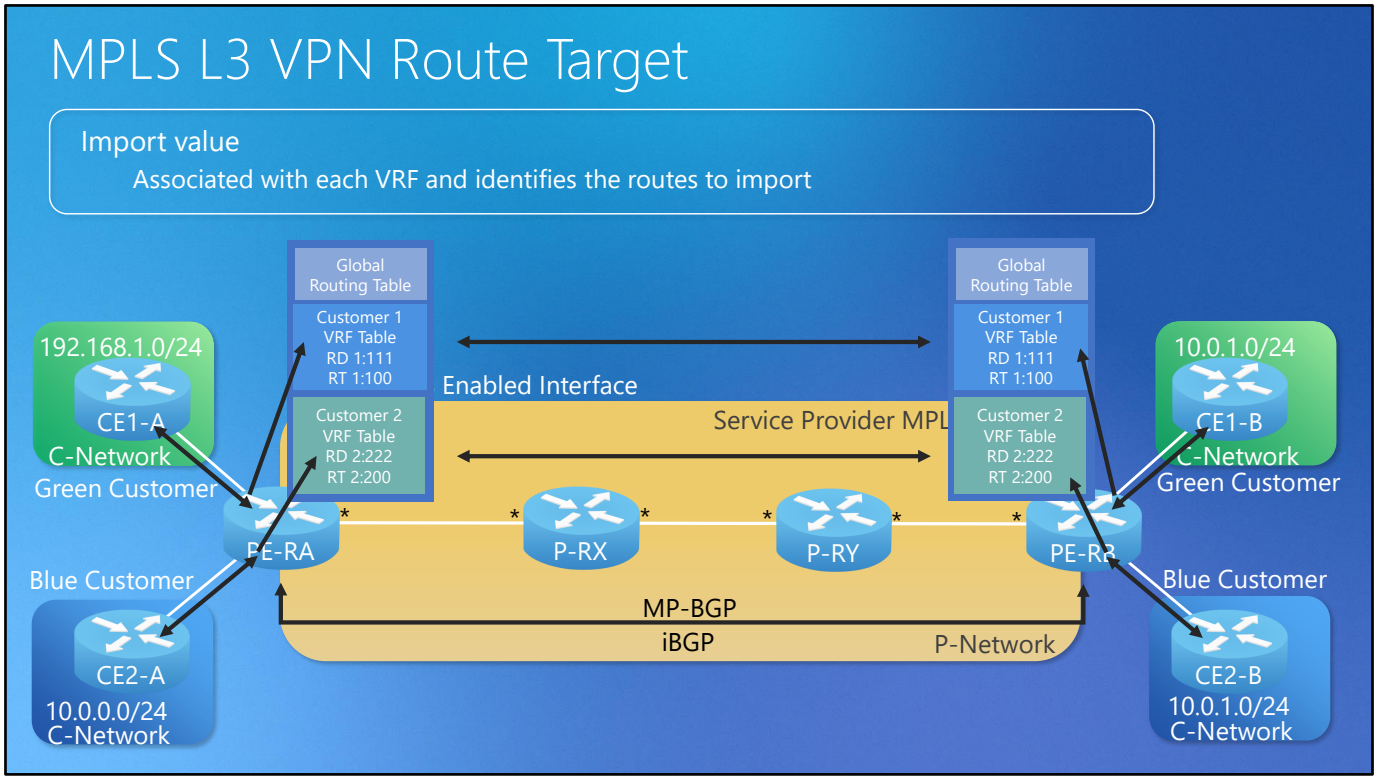
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



In this case we will keep it simple and use 1:100 for CUST 1 and 2:200 for Cust 2.

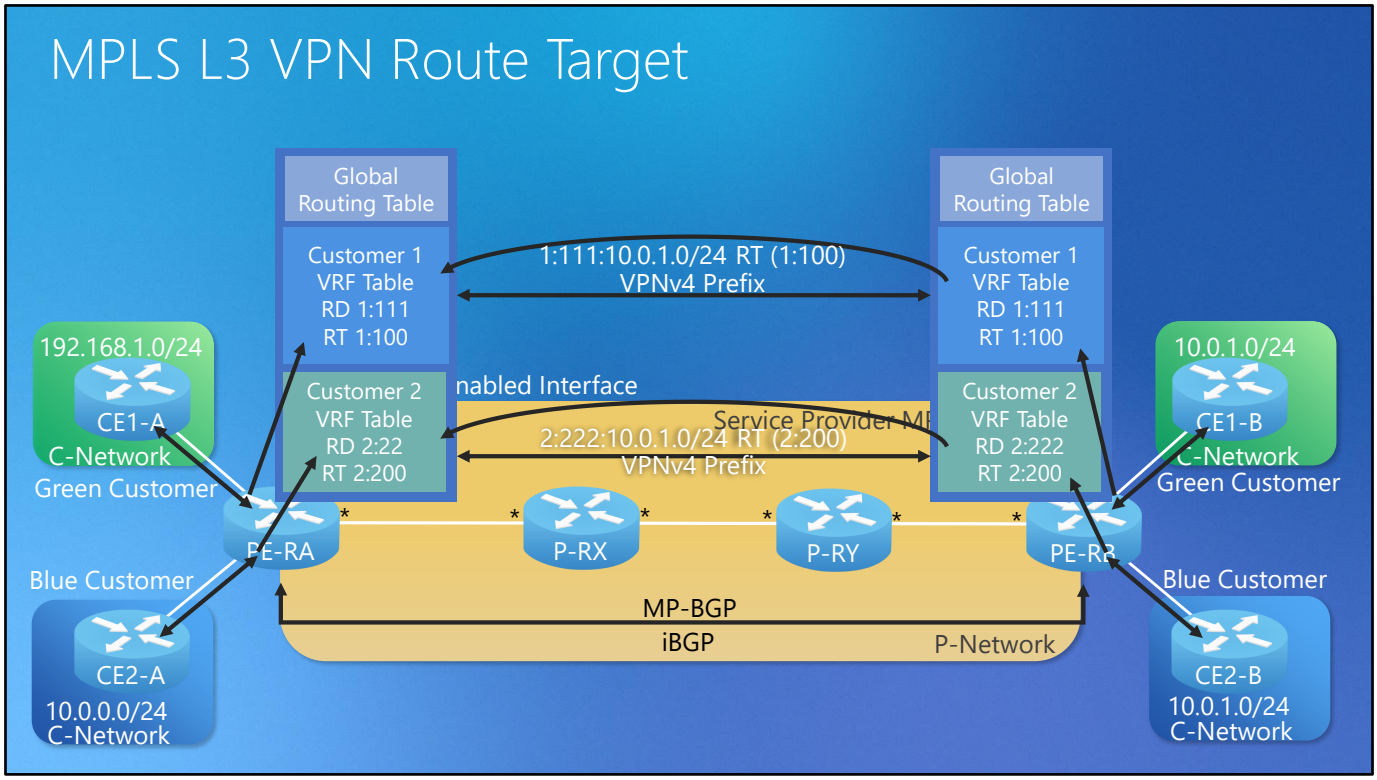
Exporting Routes: When a route is exported from a VRF on a PE router, the router attaches an RT to the route. This RT acts like a tag that identifies which VPN(s) the route belongs to.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



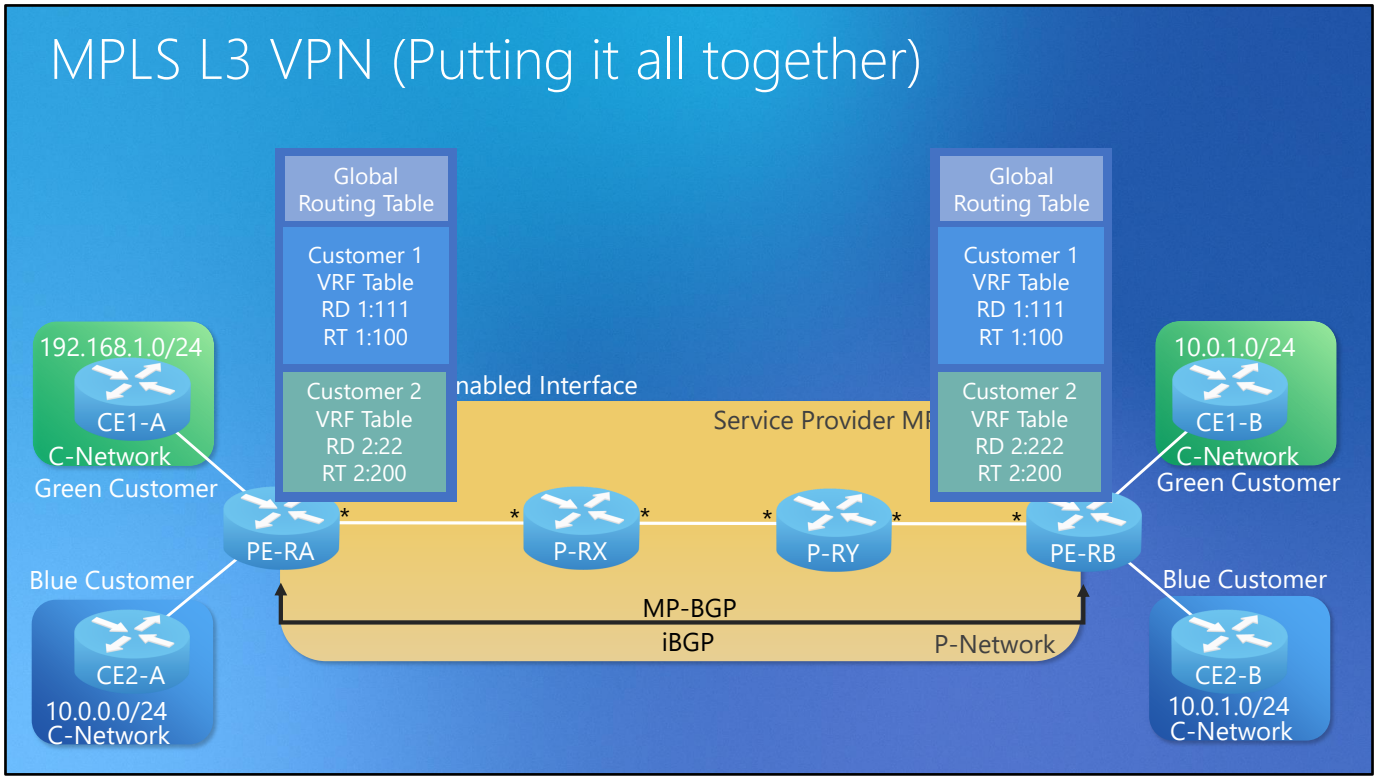
Importing Routes: Conversely, each VRF is configured with one or more RTs that it is interested in. When a PE router receives a route from another PE router (via MP-BGP, for example), it looks at the RT attached to the route. If the RT matches one of the RTs configured for import in a VRF, the route is imported into that VRF.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



The VPNv4 or VPNv6 address is tagged with the route target on export so the receiving device can import it properly. In this case me are using the same number for import and export. But you can use different numbers for import and export as well.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Instructor Note: Raymond annotate….

Please note…. We are not talking about packet forwarding yet. We are only talking about route learning.

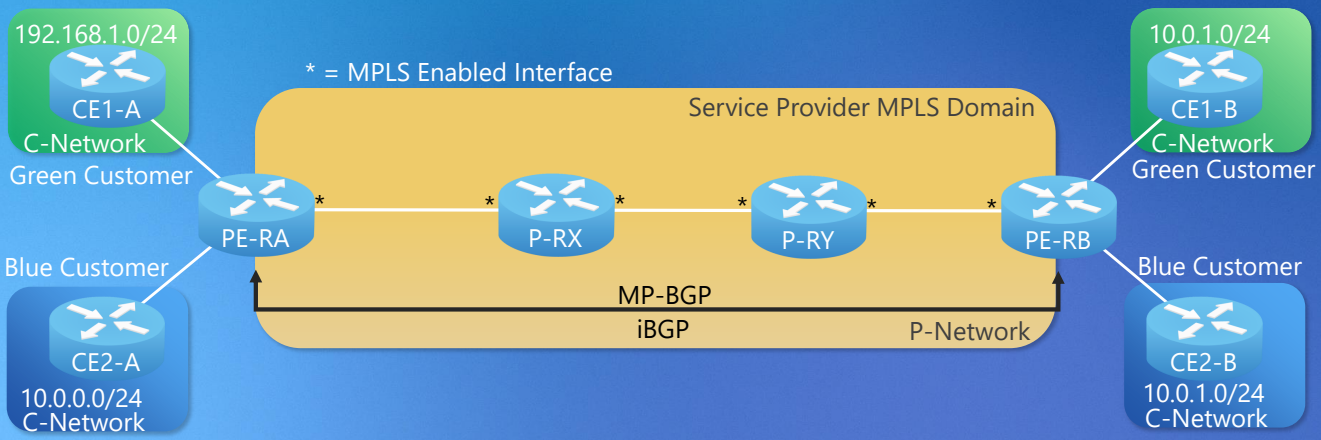
CE1-A is sending route 192.168.1.0/24 to PE-RA using an IGP.
PE-RA installs the route in Customer 1s VRF table.
PE-RA redistributes the route into BGP and when doing so creates the VPNv4 routes by appending the RD of 1:111 to the address 192.168.1.0/24.
PE-RA then uses MP-BGP to send the VPNv4 route to PE-RB and attaches an export target of 1:100 to it.
PE-RB receives the VPNv4 route from MP-BGP and based on the RT of 1:100 and RD or 1:111 places the route in the Customer 1 VRF table as a BGP route.
PE-RB then redistributes the 192.168.1.0/24 BGP route into the IGP that is used with CE1-B so it can share the route with CE1-B.

Now CE1-B knows about the 192.168.1.0/24 network. However, it will not learn any other Customers networks(such as Cust2 because they are separated via VRFs/RDs/RTs.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

MPLS L3 VPN Packet Forwarding

Forwarding is accomplished with Labels

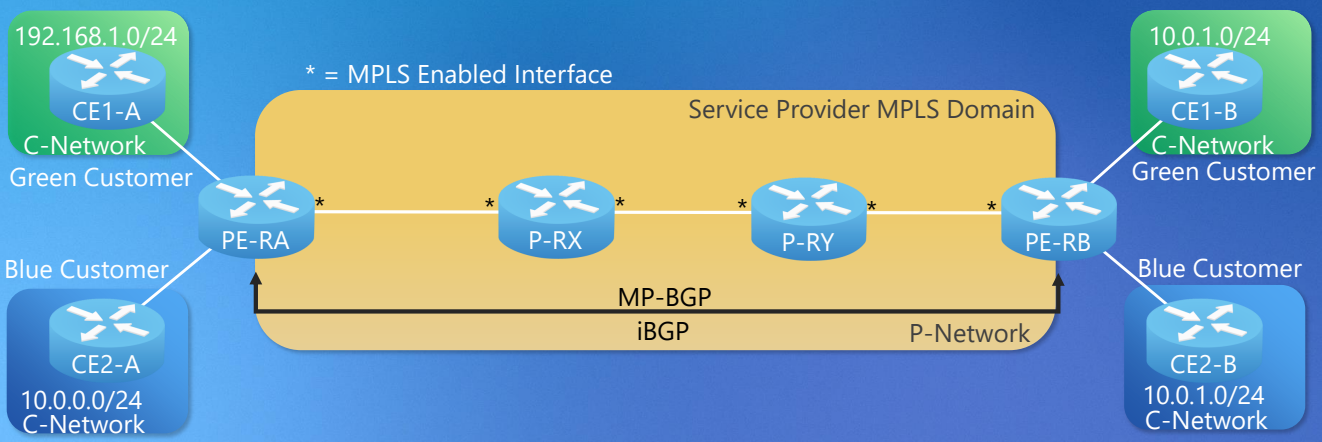


©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

MPLS L3 VPN Label Stack

2 labels are needed for packet forwarding
- 1 to forward from PE to PE through the MPLS domain
- 1 to tell the egress PE what to do with the packet

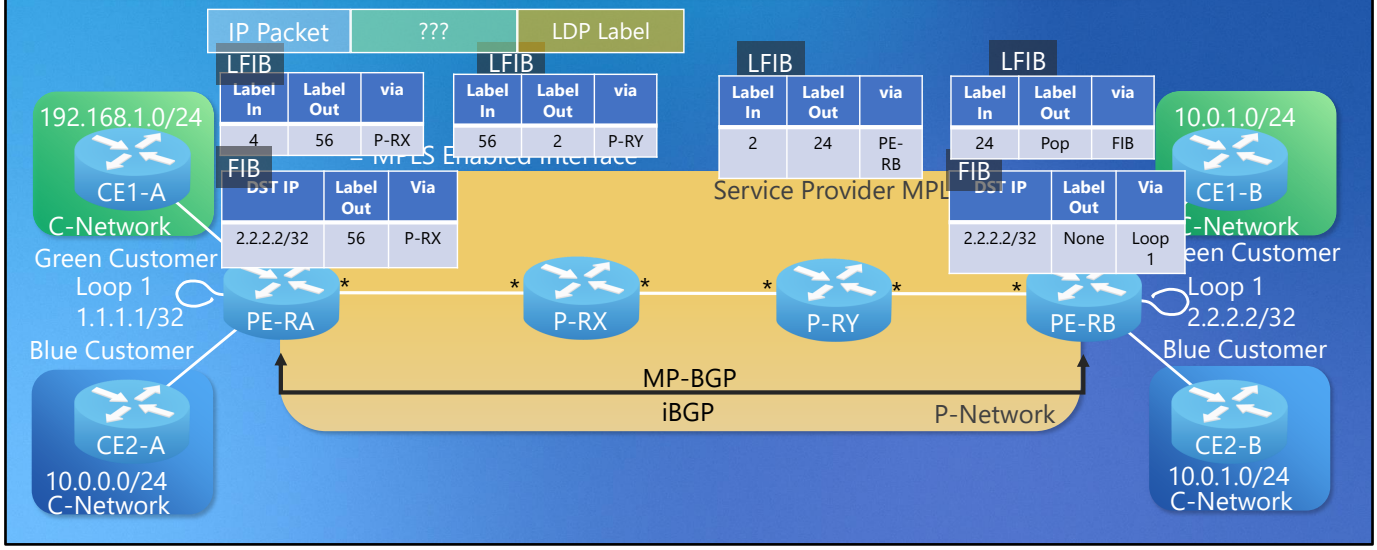
Known as a Label Stack



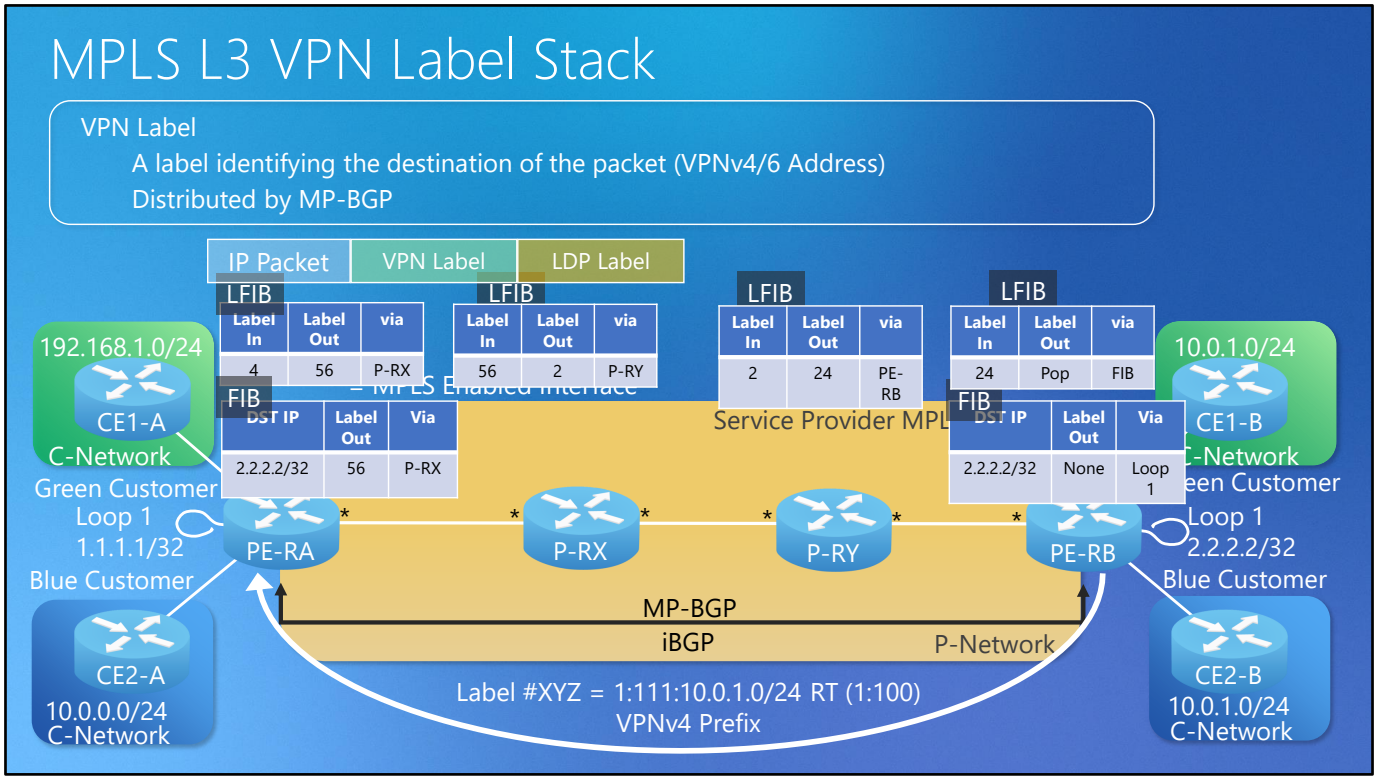
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

MPLS L3 VPN Label Stack

LDP Label
- Know as the top label for forwarding through MPLS domain
- Distributed by LDP



©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

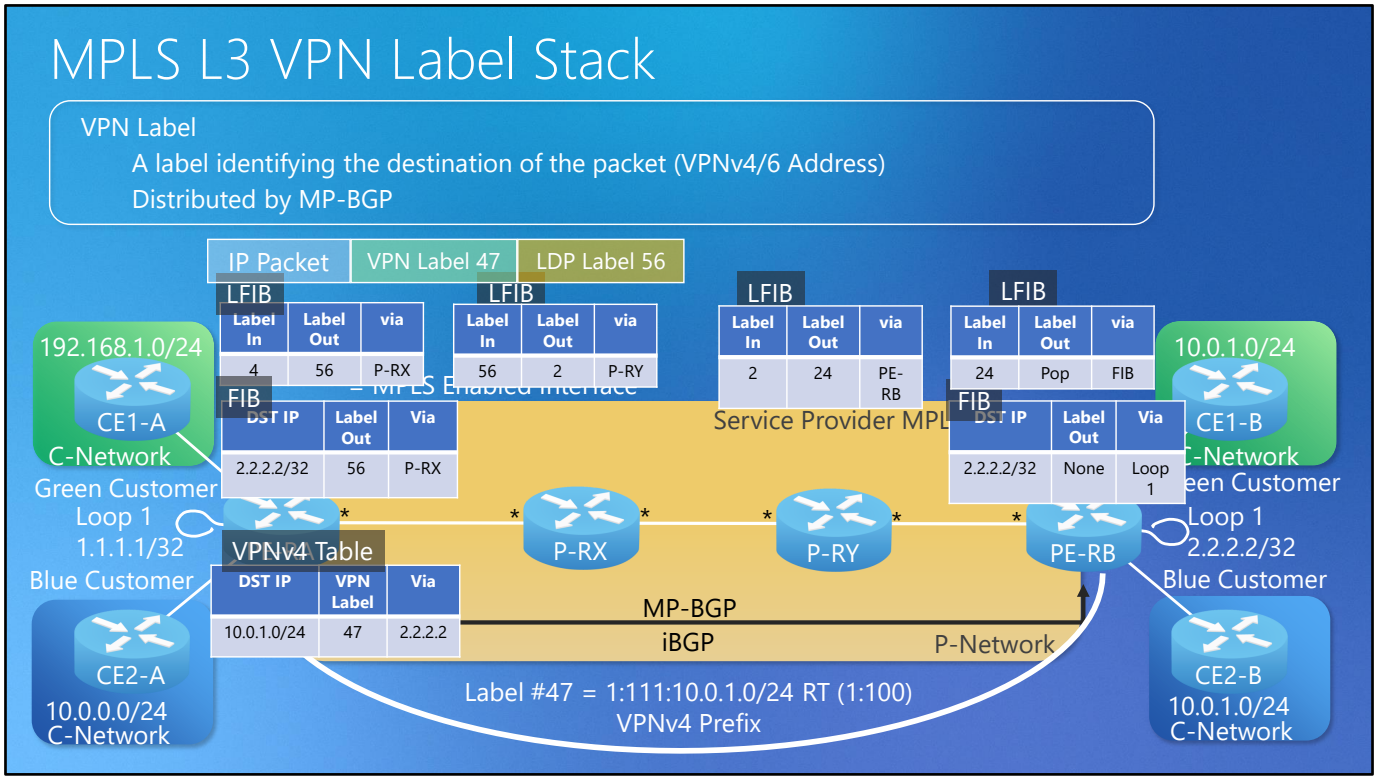


As we said this one is used to tell the egress PE what to do with the packet

VPN label is generated by PE-RB in this case and sent via MP-BGP to PE-RA.

You can verify the VPN labels locally on the device that generated them with the command **show mpls forwarding vrf *vrf_name***
You can verify the learned MP-BGP VPN labels with he command **show bgp vpnv4 unicast all labels**

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

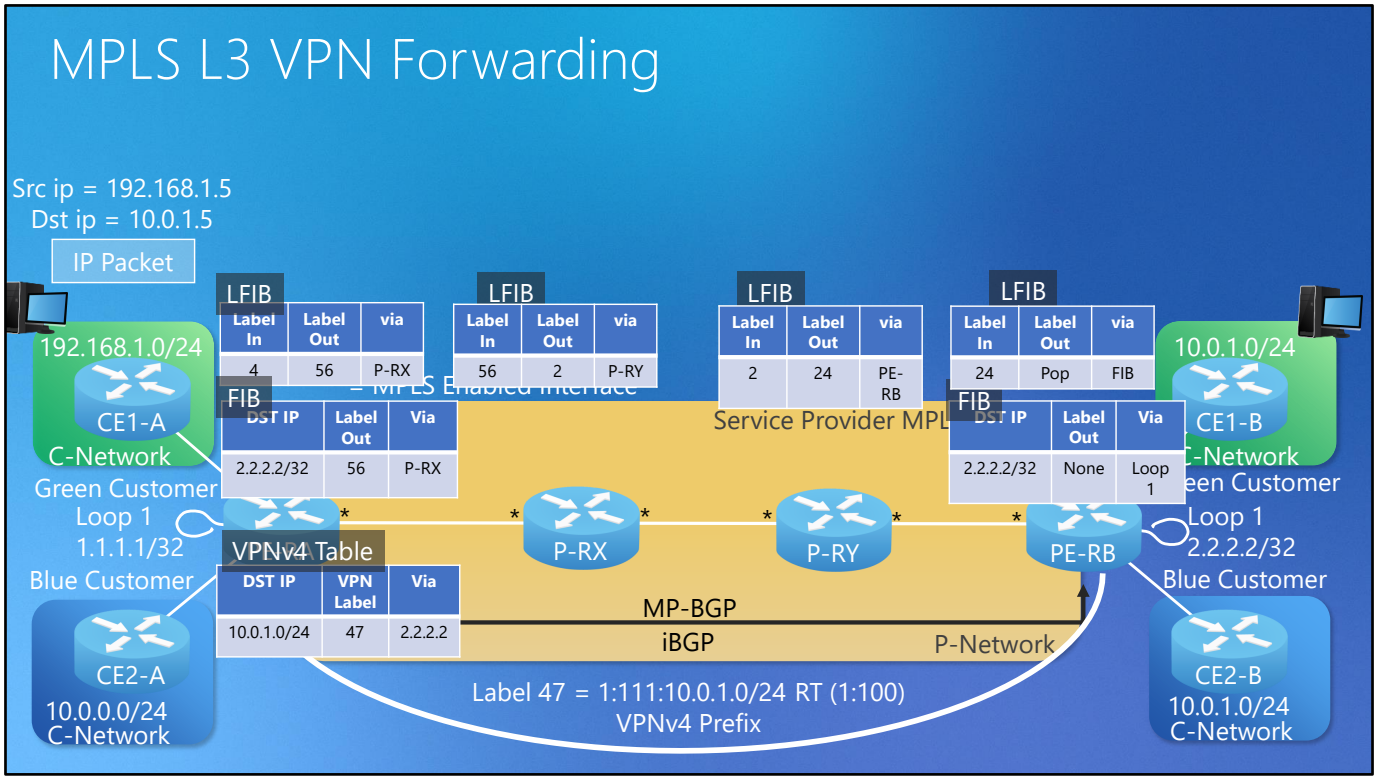


As we said this one is used to tell the egress PE what to do with the packet

VPN label is generated by PE-RB in this case and sent via MP-BGP to PE-RA.

You can verify the VPN labels locally on the device that generated them with the command **show mpls forwarding vrf *vrf_name***
You can verify the learned MP-BGP VPN labels with he command **show bgp vpnv4 unicast all labels**

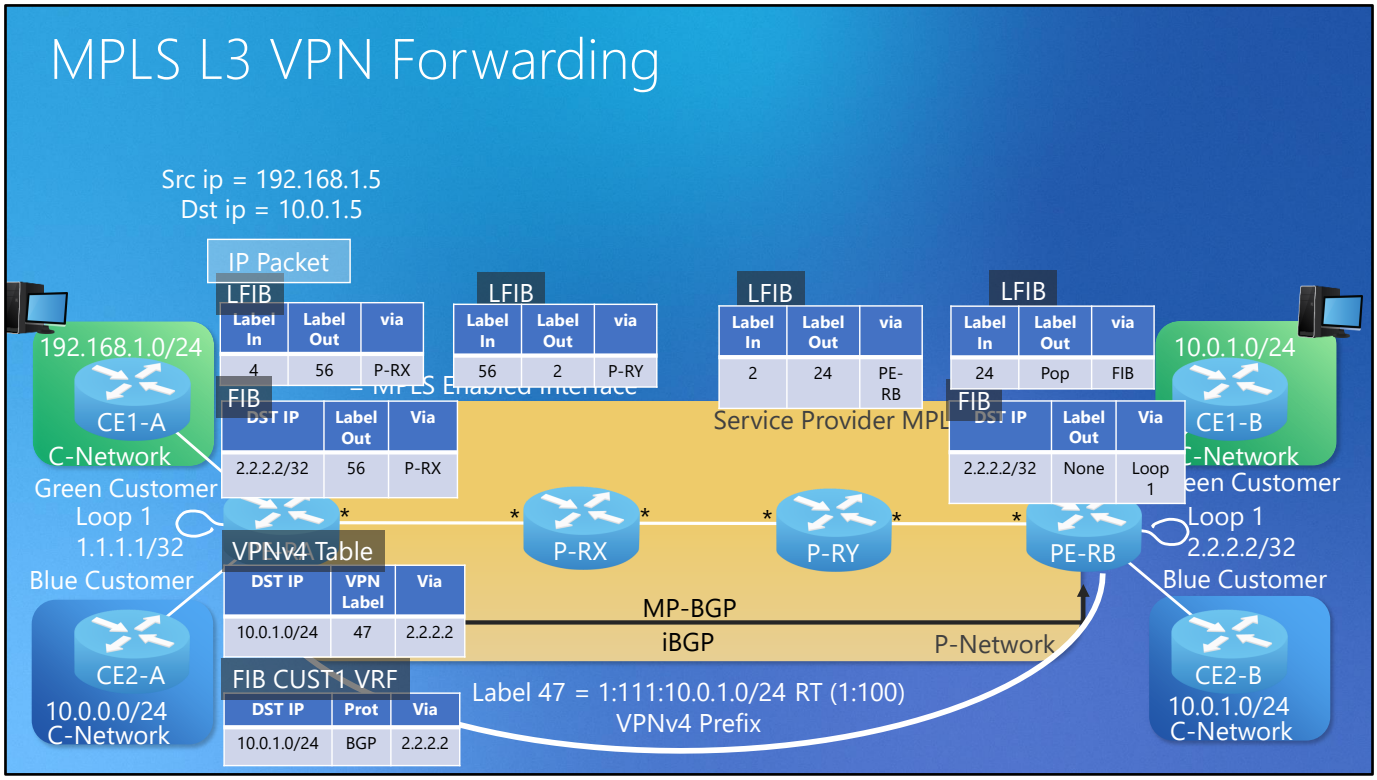
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Src ip = 192.168.1.5
Dst ip = 10.0.1.5

You can verify the VPN labels locally on the device that generated them with the command **show mpls forwarding vrf *vrf_name***
You can verify the learned MP-BGP VPN labels with he command **show bgp vpnv4 unicast all labels**

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



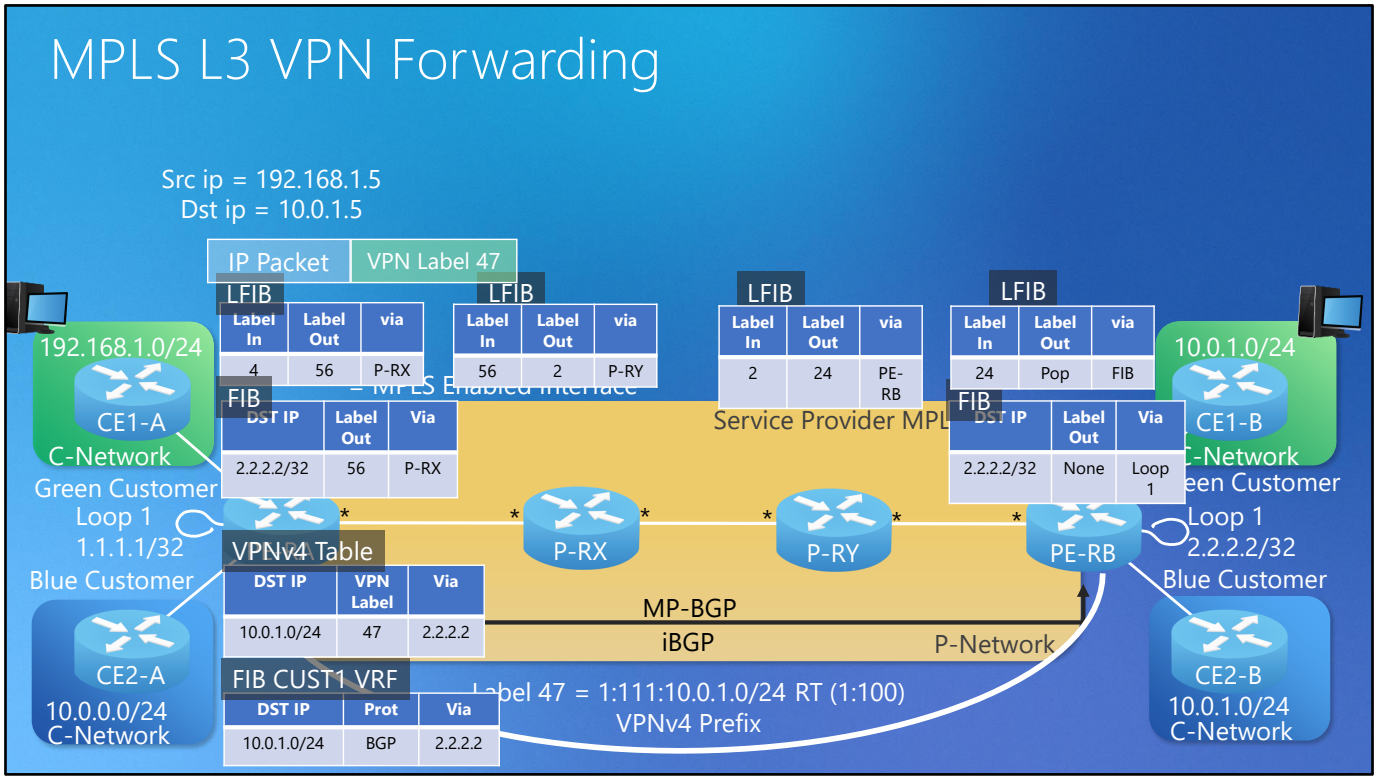
Src ip = 192.168.1.5
Dst ip = 10.0.1.5

The packet arrives at PE-RA ingress on a CUST1 VRF interface. It is not labeled so we do the destination lookup in the FIB for CUST1 VRF based on the dest IP address 10.0.1.5. In this case, it states that we get to 10.0.1.0/24 via 2.2.2.2 which is learned via the BGP VPNv4 address family.

So now we have to do a lookup in the VPNv4 table (You can verify the learned MP-BGP VPN labels with he command **show bgp vpnv4 unicast all labels)** to find the VPN label we need to attach. In this case it is 47.

You can verify the VPN labels locally on the device that generated them with the command **show mpls forwarding vrf *vrf_name***
You can verify the learned MP-BGP VPN labels with he command **show bgp vpnv4 unicast all labels**

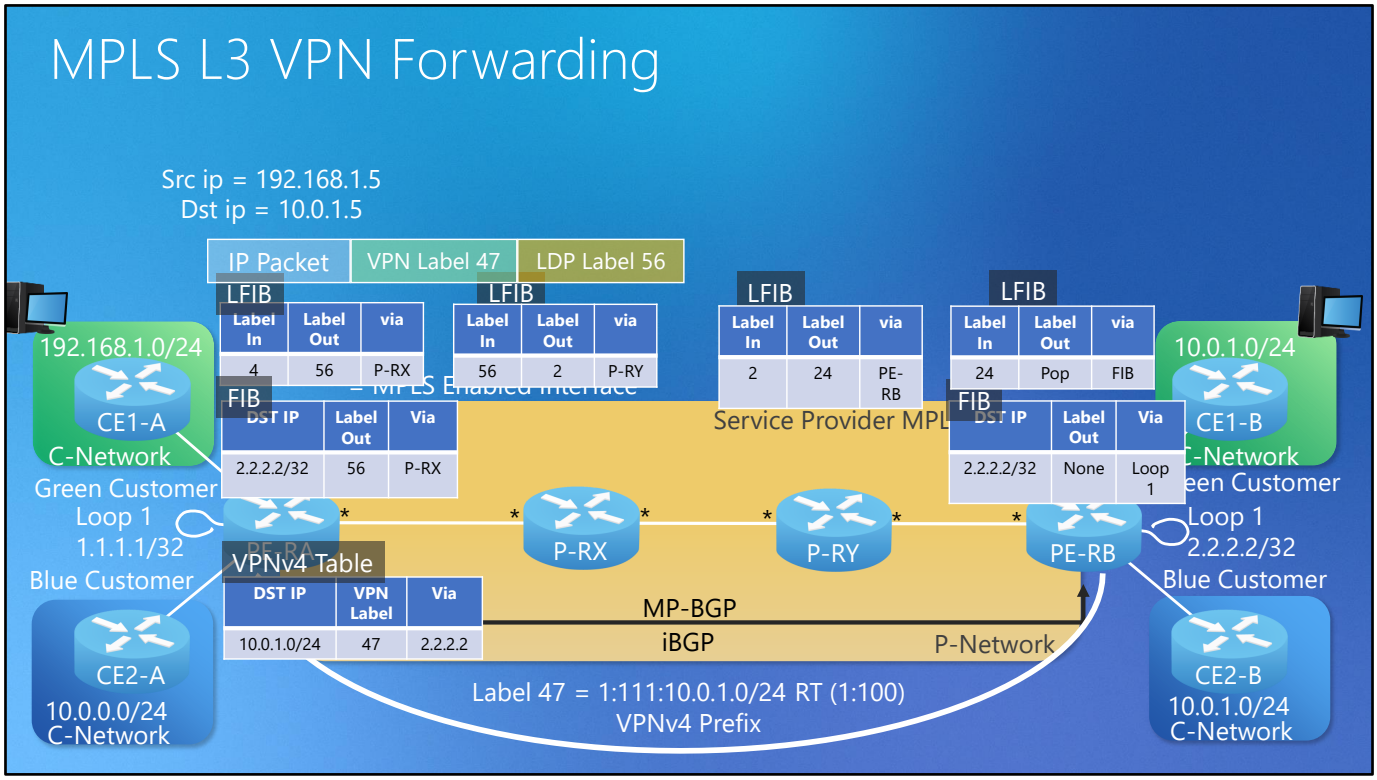
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Now that the VPN label is attached the router has to figure out how to get to 2.2.2.2 in the global routing table. The FIB states that 2.2.2.2 is reachable via P-RX out an MPLS enabled interface therefore a label needs to be attached. The FIB states that label 56 needs to be attached. (notice the FIB is used here not the LFIB because there was no incoming label.)

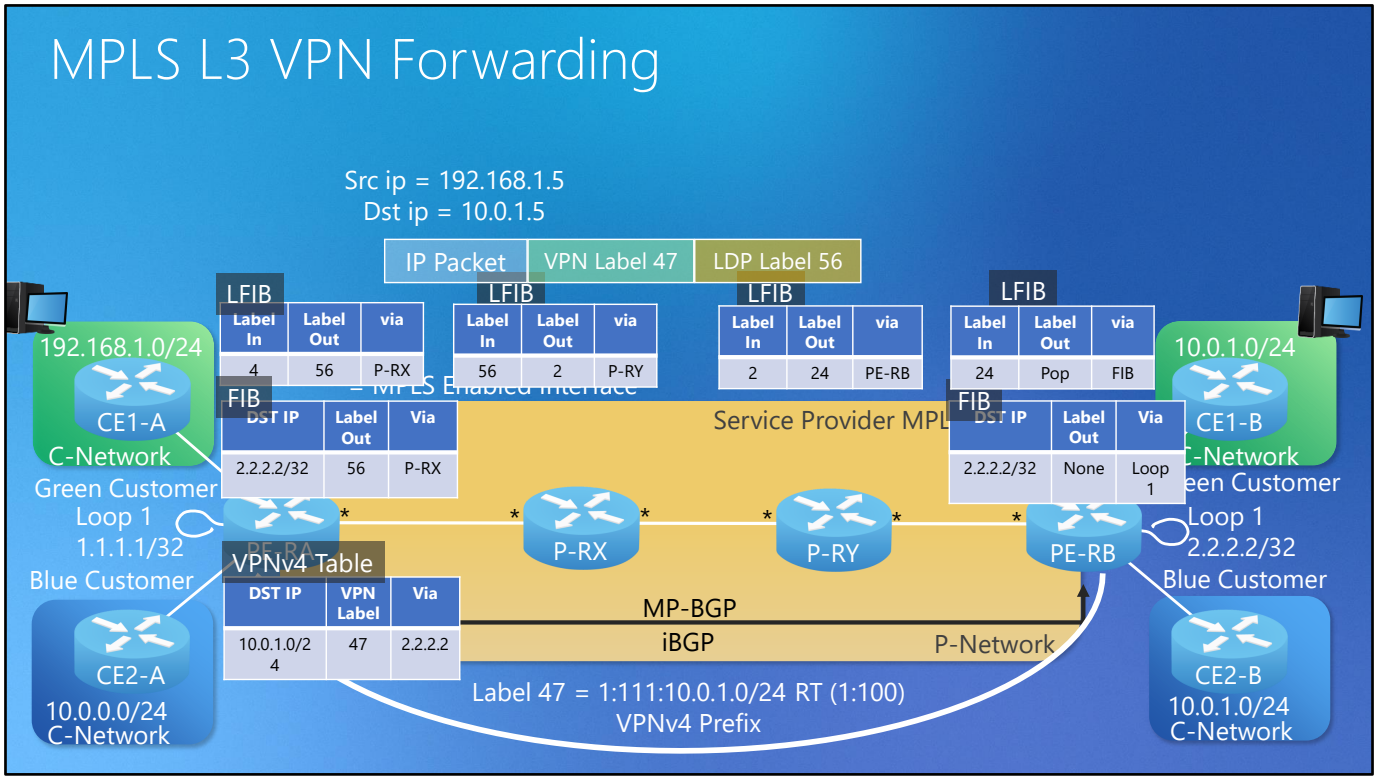
So we attached the label of 56 to the label stack.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Here is the label stack. Now we forward.

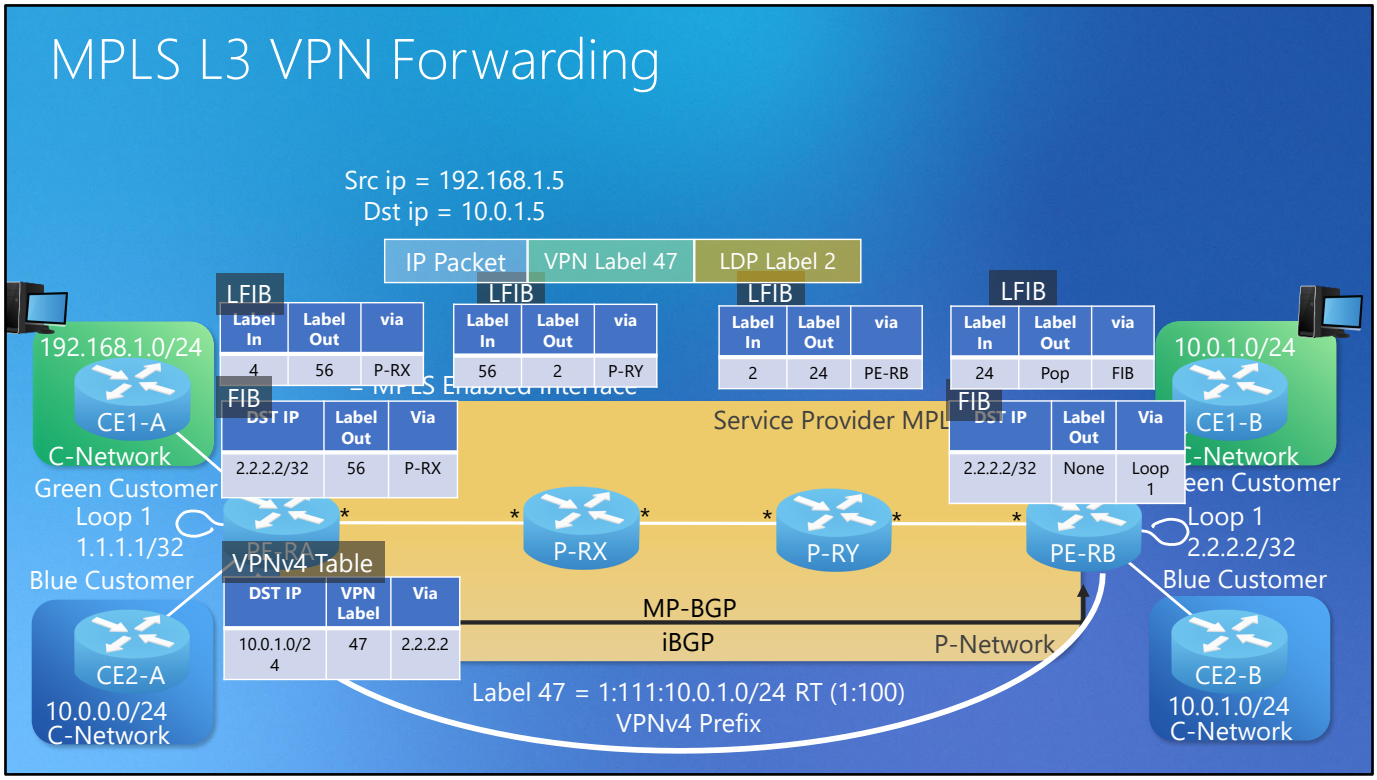
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



PRX looks at the top label and the LFIB states that it needs to be swapped with 2.

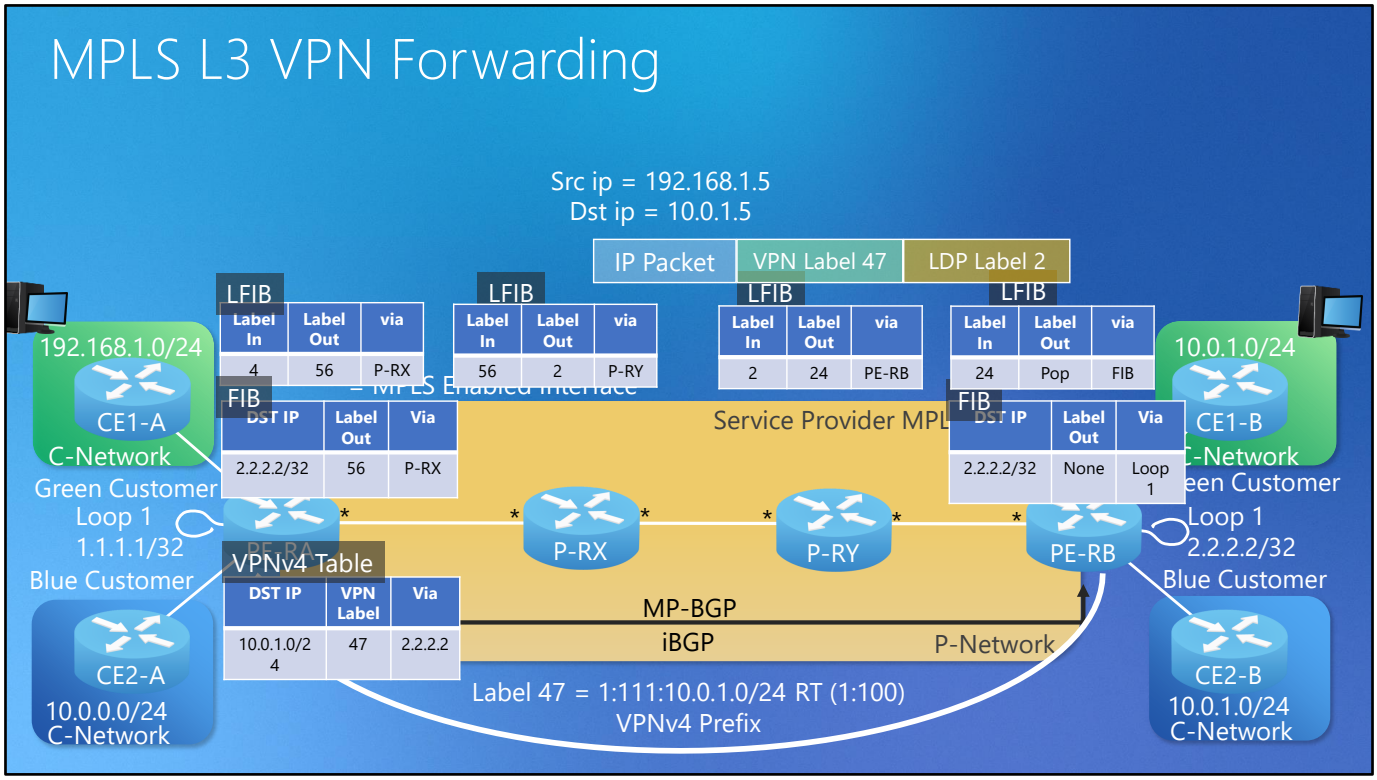
So let's swap/

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Now we forward

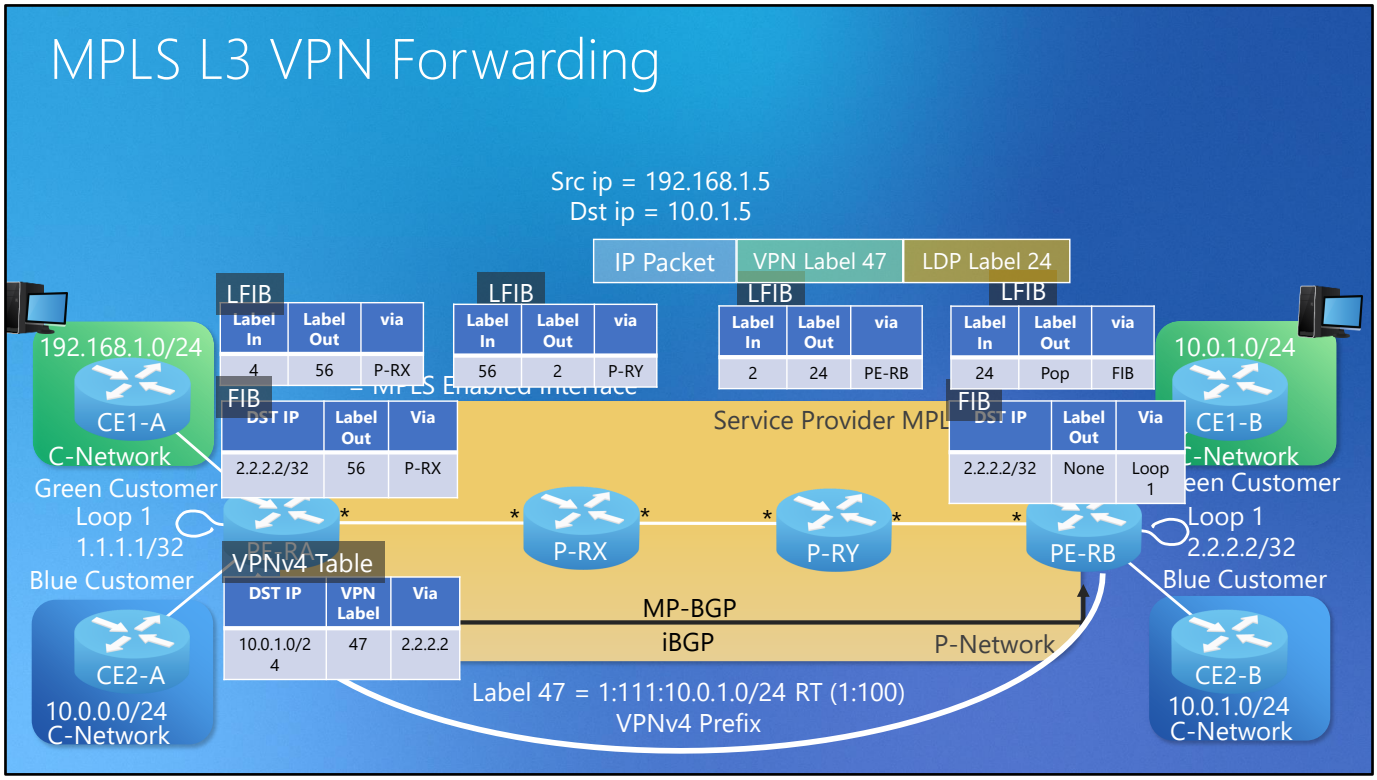
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



PRY looks at the label of 2 and the LFIB says to swap it with a label of 24 and forward it to PE-RB

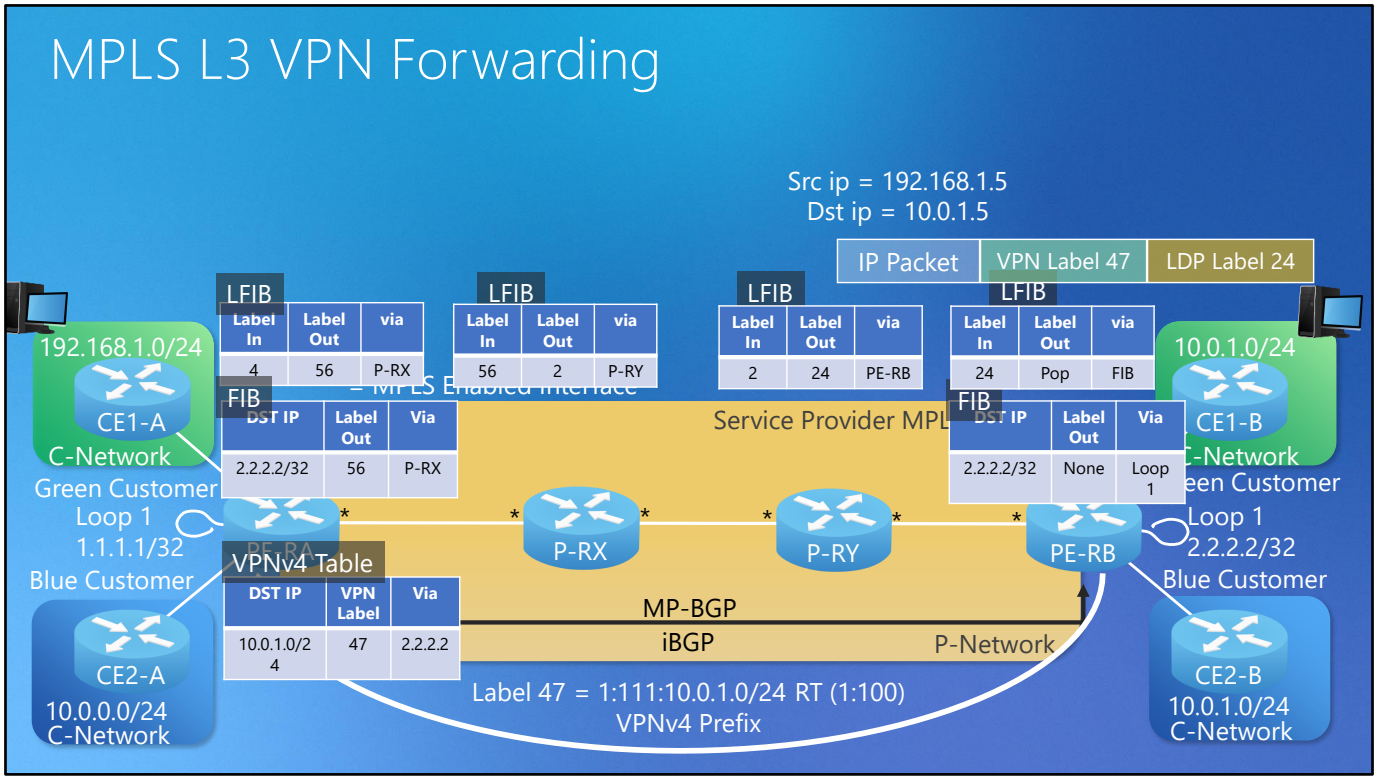
So let's swap

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



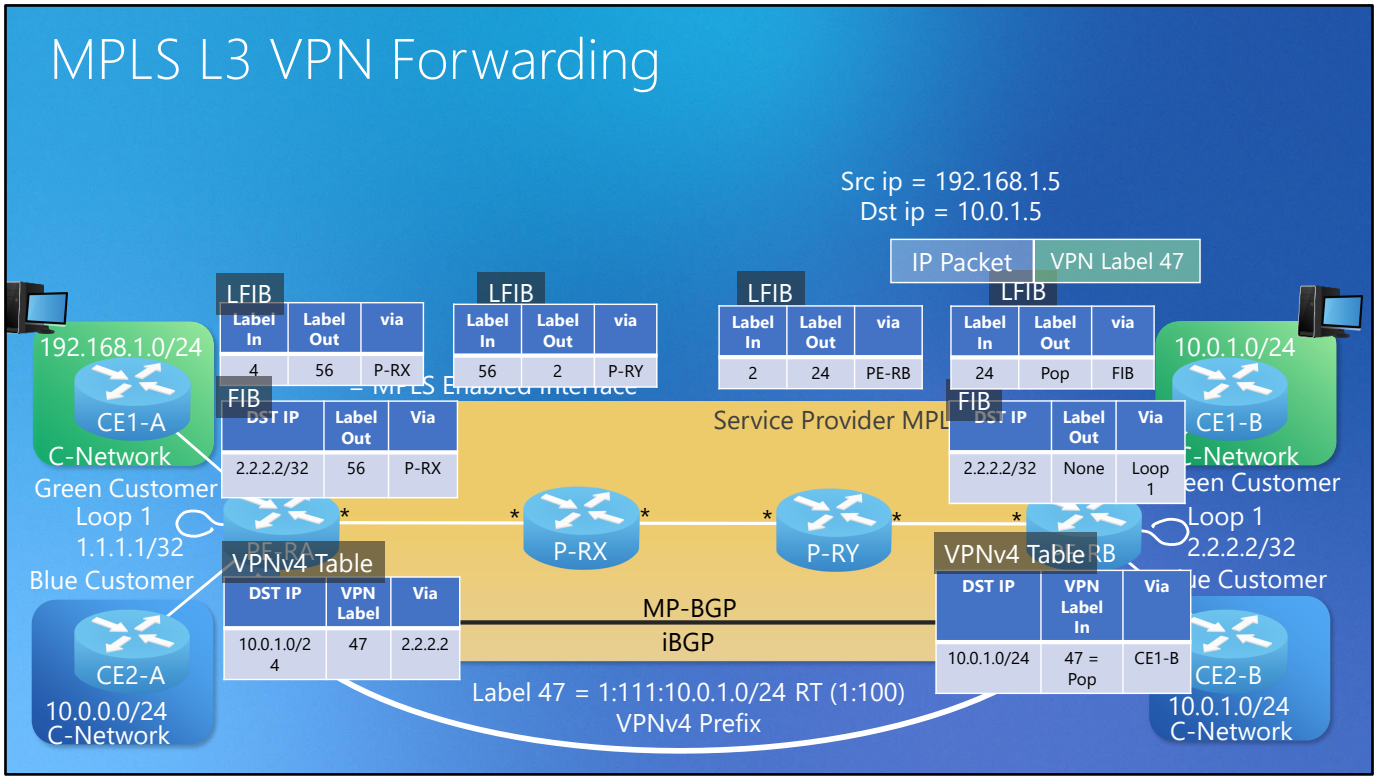
Now we forward

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



PE-RB receives a label of 24 and the LFIB says to POP it and examine the fib. The FIB states that the destination is the local device.

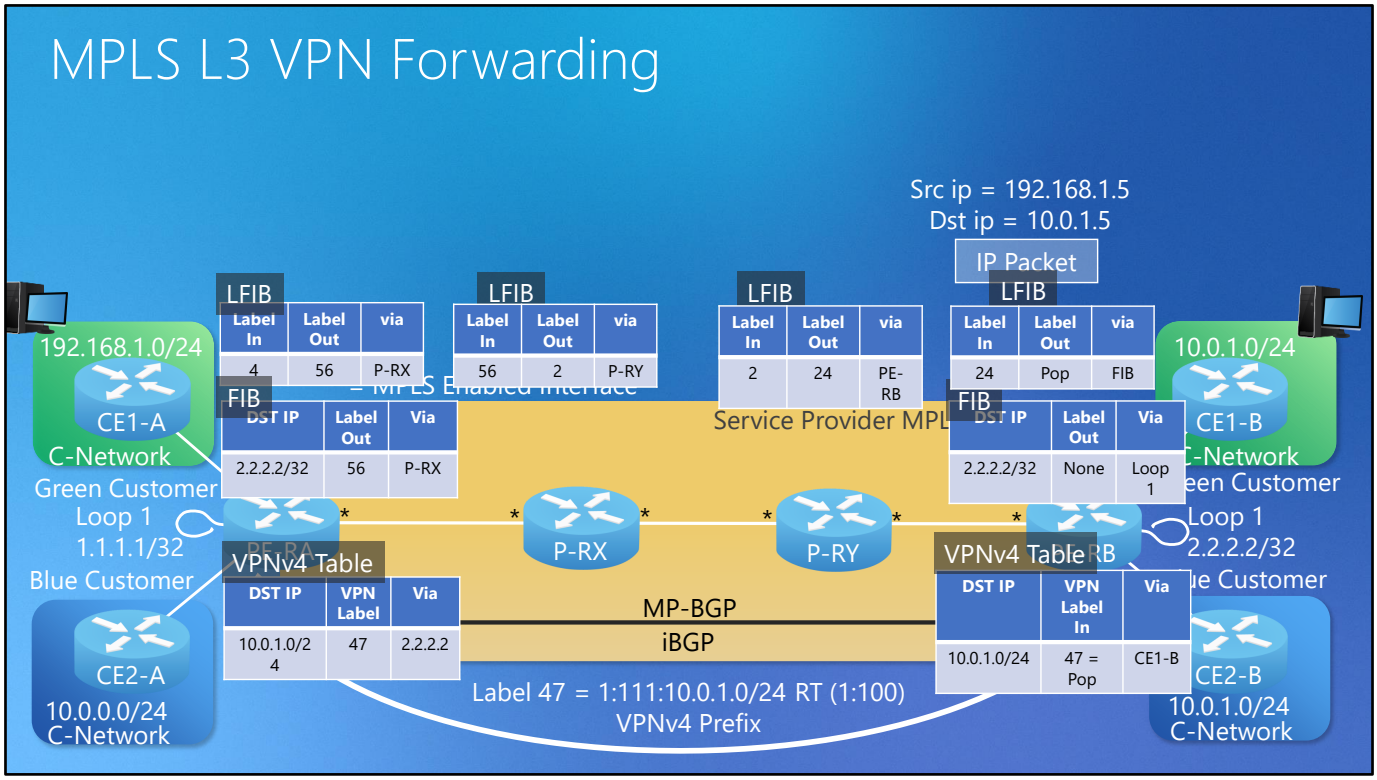
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Now there is another label. The VPN label which has a value of 47. 47 corresponds to 10.0.1.0/24 and VRF CUST1… and it says to pop the label and forward to CE1-B.

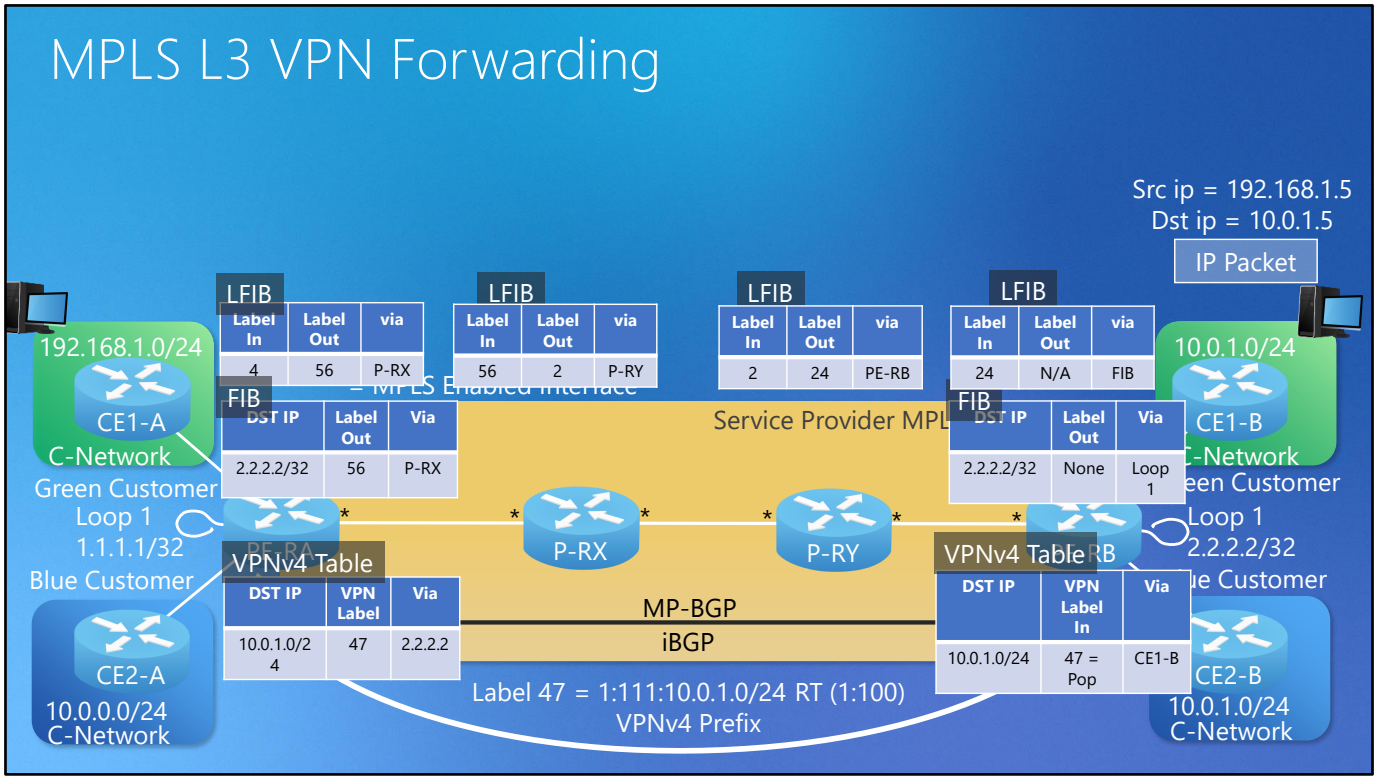
So let's pop

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

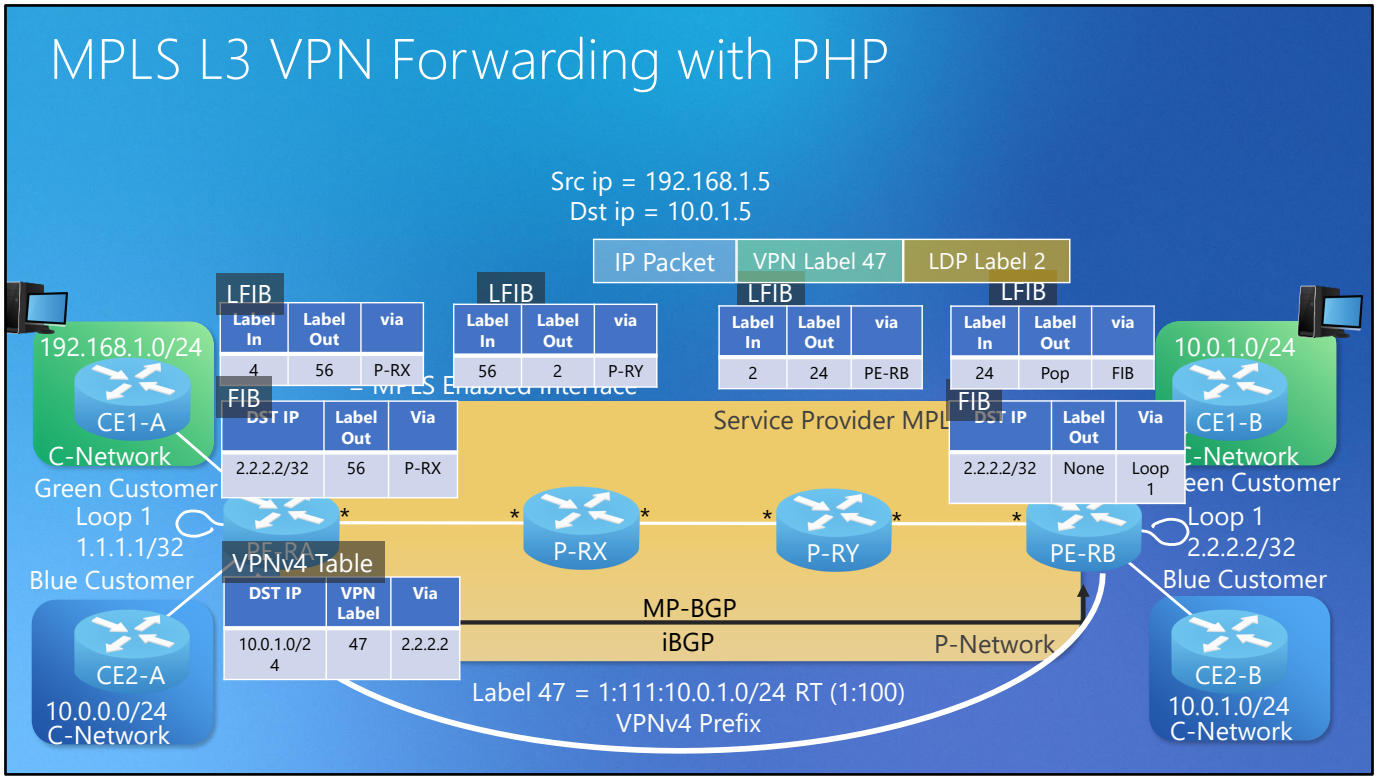


Now lets forward.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

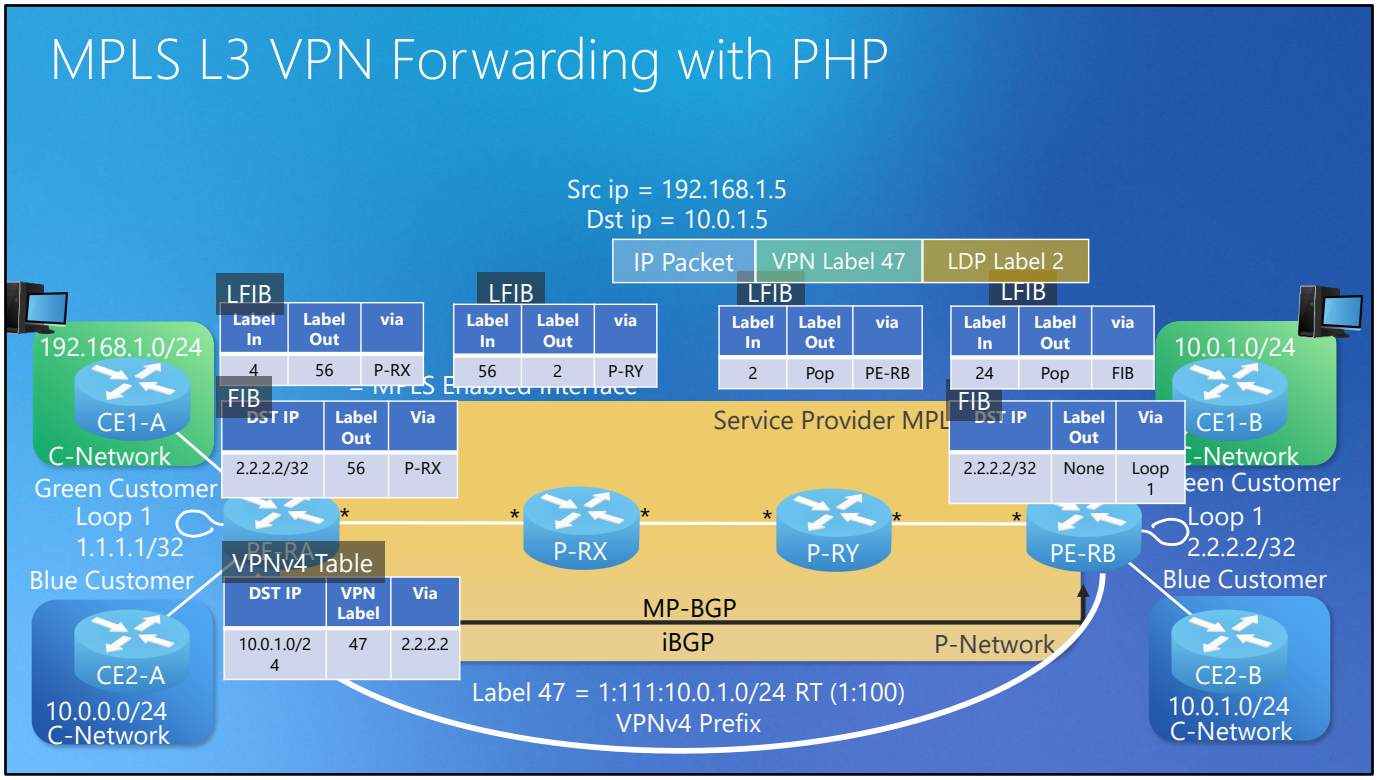


REWIND…….

As before we can take advantage of Penultimate Hop Popping.

In this case, PE-RB will tell P-RY to POP the label for destination 2.2.2.2.

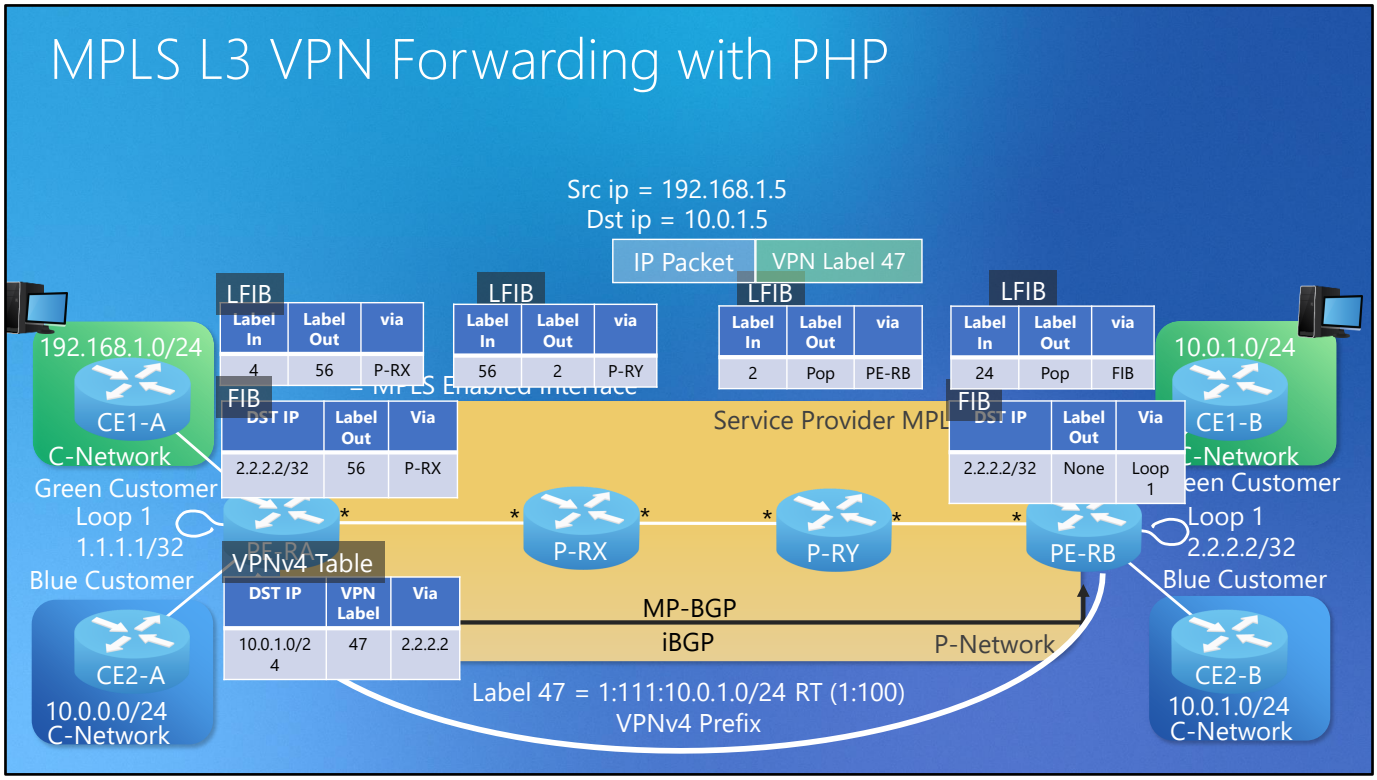
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



As before we can take advantage of Penultimate Hop Popping.

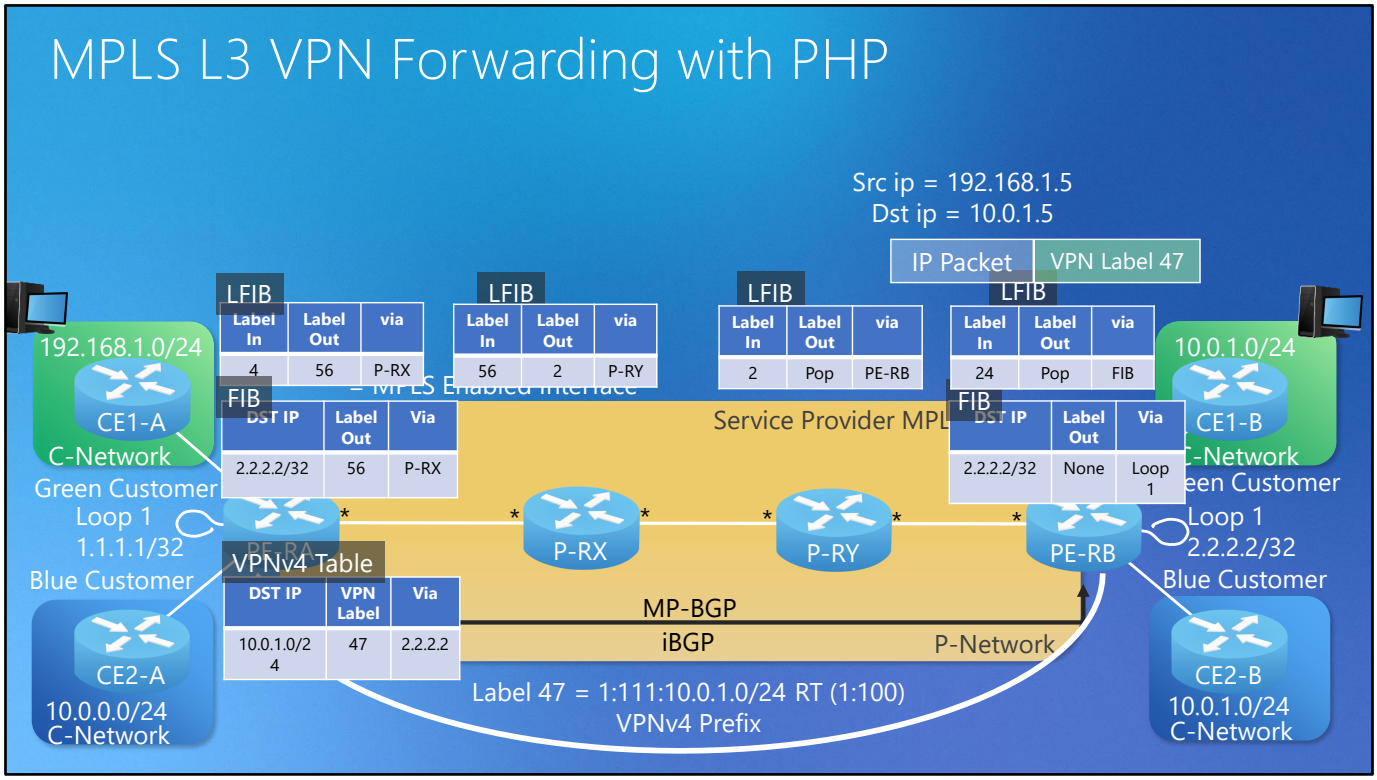
In this case, PE-RB will tell P-RY to POP the label for destination 2.2.2.2.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



So now p-RY pops the label.

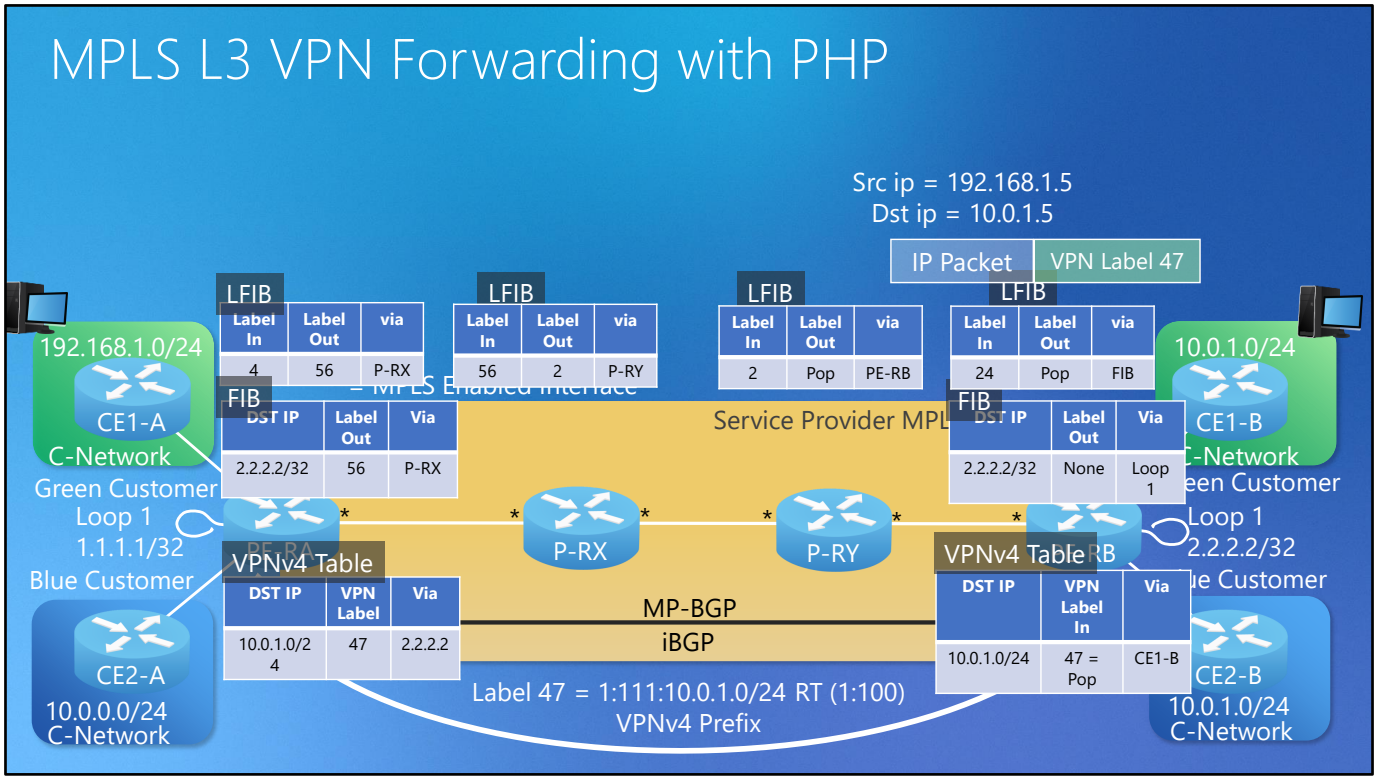
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Forwards the remaining packet and vpnv4 label to PE-RB…

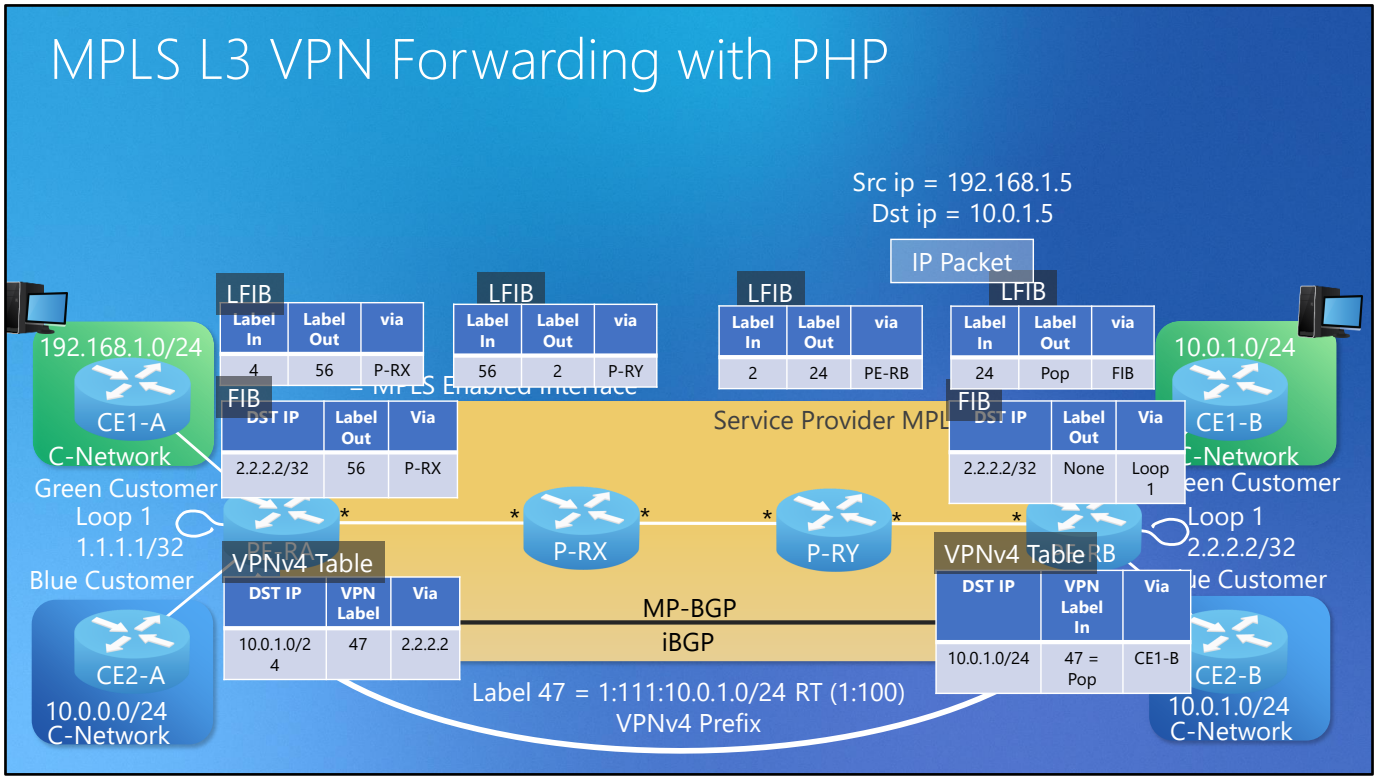
And now PE-RB only have to do the VPNv4 lookup.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



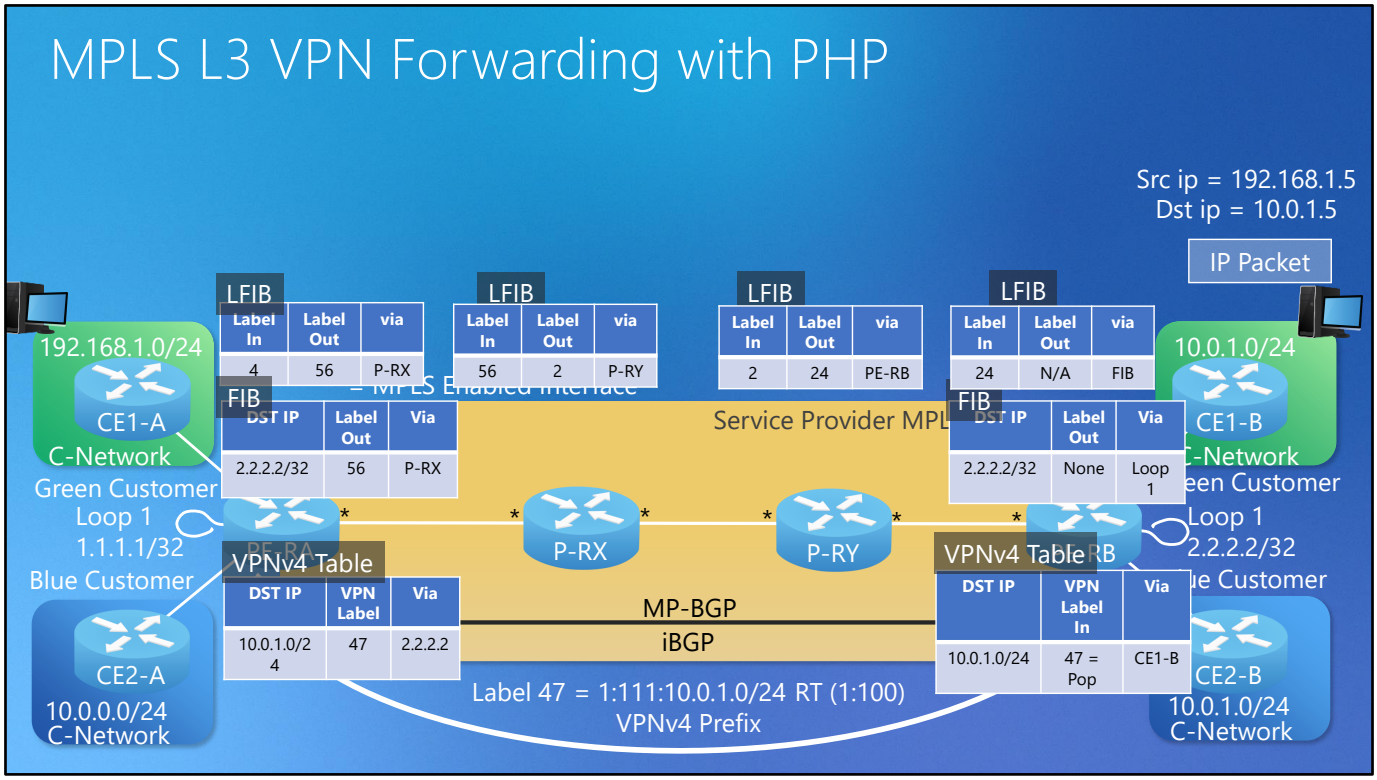
As before, PE-RB pops the label and forwards to CE1-B

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



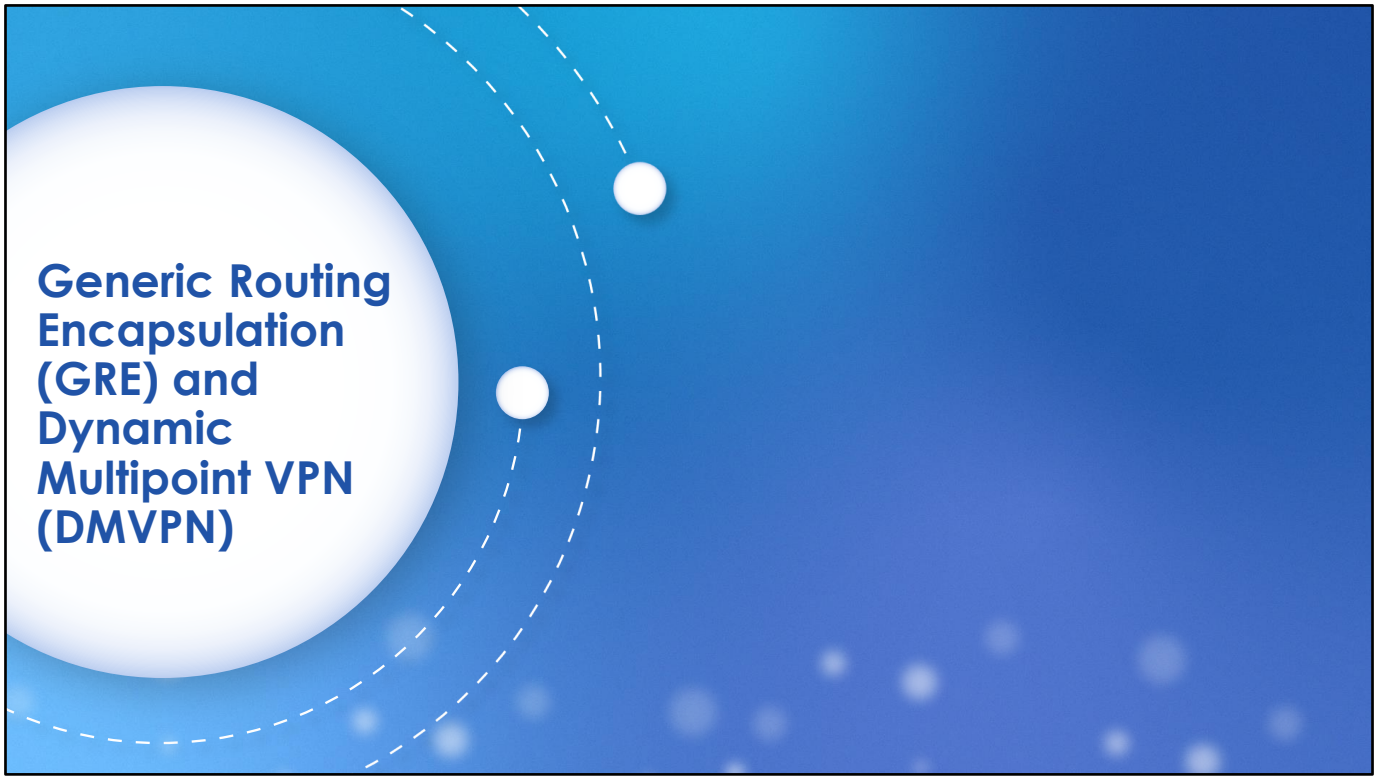
POP

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Forward.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

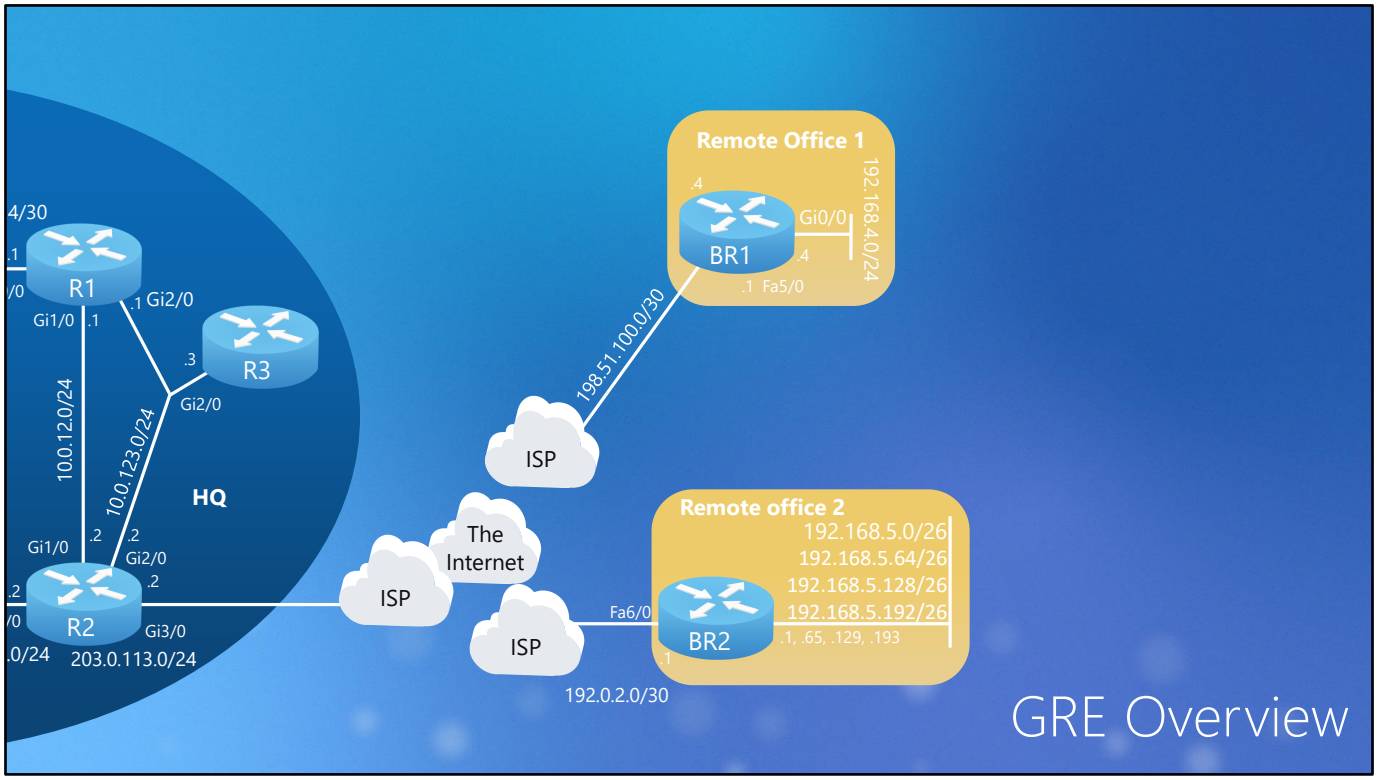


©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Title slide

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



For every spoke you need a different tunnel as GRE by default is point-to-point.
For every spoke you will need to manage the IPSEC parameters and configurations. (PAINFUL)
No matter what all traffic has to pass from spoke to hub to spoke for spoke-to-spoke communication. (Resource intensive on the hub and diminishes throughput)

GRE/IPSEC CONFIG R2

```
interface Tunnel21
 ip address 172.16.21.2 255.255.255.0
 tunnel source GigabitEthernet3/0
 tunnel destination 198.51.100.1
!
interface Tunnel22
 ip address 172.16.22.2 255.255.255.0
 tunnel source GigabitEthernet3/0
 tunnel destination 192.0.2.1

router eigrp ENARSI
```

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

```
 address-family ipv4 unicast autonomous-system 100
  network 172.16.21.2 0.0.0.0
  network 172.16.22.2 0.0.0.0

crypto isakmp policy 10
authentication pre-share
encryption aes 256
group 16
hash sha256
exit
crypto isakmp key PASSWORDBR1 address 198.51.100.1
crypto isakmp key PASSWORDBR2 address 192.0.2.1

crypto ipsec transform-set IPSEC_VPN_TRANSFORM esp-aes 256 esp-sha256-hmac
mode transport
exit
ip access-list extended IPSEC_VPN_ACL_BR1
permit gre 203.0.113.2 0.0.0.0 198.51.100.1 0.0.0.0
ip access-list extended IPSEC_VPN_ACL_BR2
permit gre 203.0.113.2 0.0.0.0 192.0.2.1 0.0.0.0
exit
crypto map IPSEC_VPN_CM 10 ipsec-isakmp
match address IPSEC_VPN_ACL_BR1
set peer 198.51.100.1
set transform-set IPSEC_VPN_TRANSFORM
crypto map IPSEC_VPN_CM 20 ipsec-isakmp
match address IPSEC_VPN_ACL_BR2
set peer 192.0.2.1
set transform-set IPSEC_VPN_TRANSFORM

int gig 3/0
crypto map IPSEC_VPN_CM


IPSEC CONFIG BR1
interface Tunnel21
 ip address 172.16.21.1 255.255.255.0
 tunnel source FastEthernet5/0
 tunnel destination 203.0.113.2
router eigrp BRANCH1
 address-family ipv4 unicast autonomous-system 100
  network 172.16.21.1 0.0.0.0
```

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

```
configure terminal
crypto isakmp policy 10
authentication pre-share
encryption aes 256
group 16
hash sha256
exit
crypto isakmp key PASSWORDBR1 address 203.0.113.2

crypto ipsec transform-set IPSEC_VPN_TRANSFORM esp-aes 256 esp-sha256-hmac
mode transport
exit
ip access-list extended IPSEC_VPN_ACL
permit gre 198.51.100.1 0.0.0.0 203.0.113.2 0.0.0.0
exit
crypto map IPSEC_VPN_CM 10 ipsec-isakmp
match address IPSEC_VPN_ACL
set peer 203.0.113.2
set transform-set IPSEC_VPN_TRANSFORM

int fast 5/0
crypto map IPSEC_VPN_CM


GRE/IPSEC CONFIG BR2
interface Tunnel22
 ip address 172.16.22.1 255.255.255.0
 tunnel source FastEthernet6/0
 tunnel destination 203.0.113.2
router eigrp BRANCH2
 address-family ipv4 unicast autonomous-system 100
  network 172.16.22.1 0.0.0.0

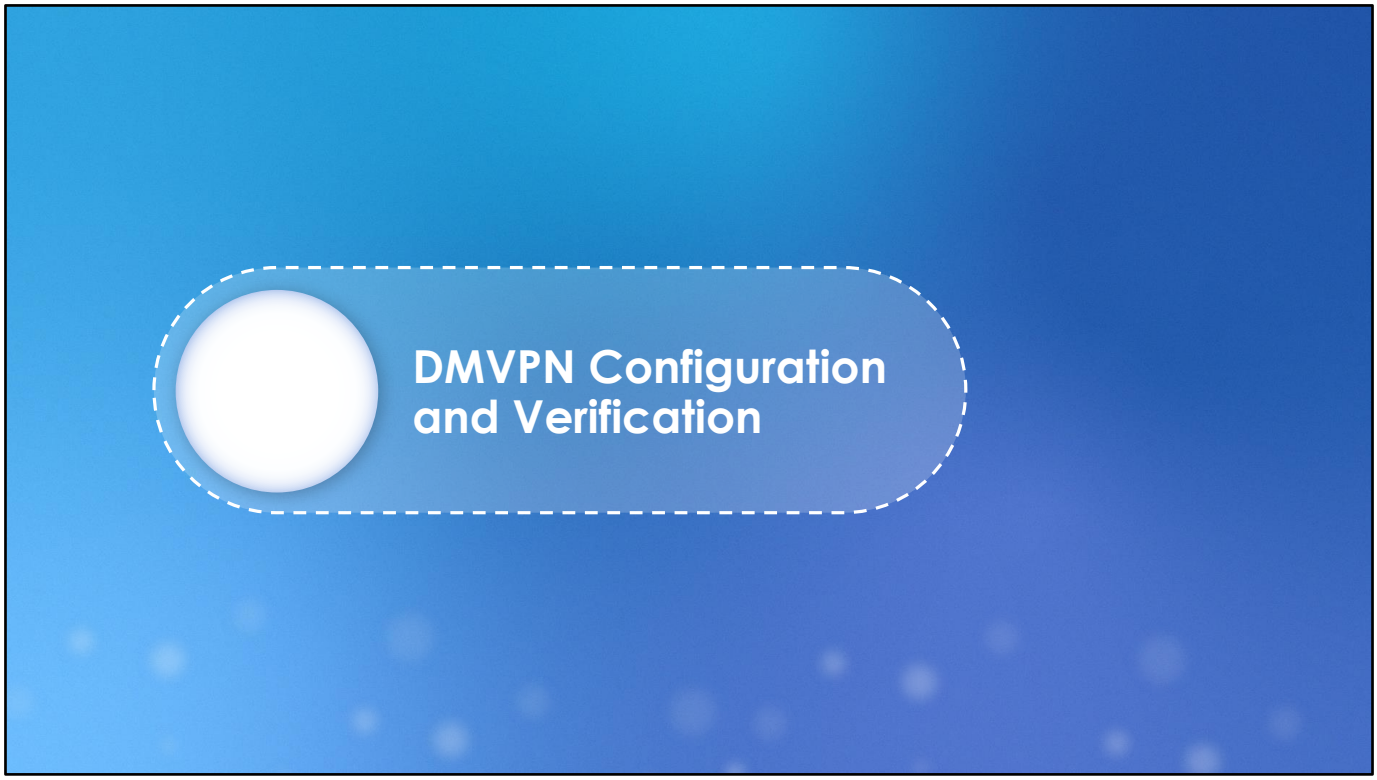
crypto isakmp policy 10
authentication pre-share
encryption aes 256
group 16
hash sha256
exit
crypto isakmp key PASSWORDBR2 address 203.0.113.2
```

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

crypto ipsec transform-set IPSEC_VPN_TRANSFORM esp-aes 256 esp-sha256-hmac
mode transport
exit
ip access-list extended IPSEC_VPN_ACL
permit gre 192.0.2.1 0.0.0.0 203.0.113.2 0.0.0.0
exit
crypto map IPSEC_VPN_CM 10 ipsec-isakmp
match address IPSEC_VPN_ACL
set peer 203.0.113.2
set transform-set IPSEC_VPN_TRANSFORM

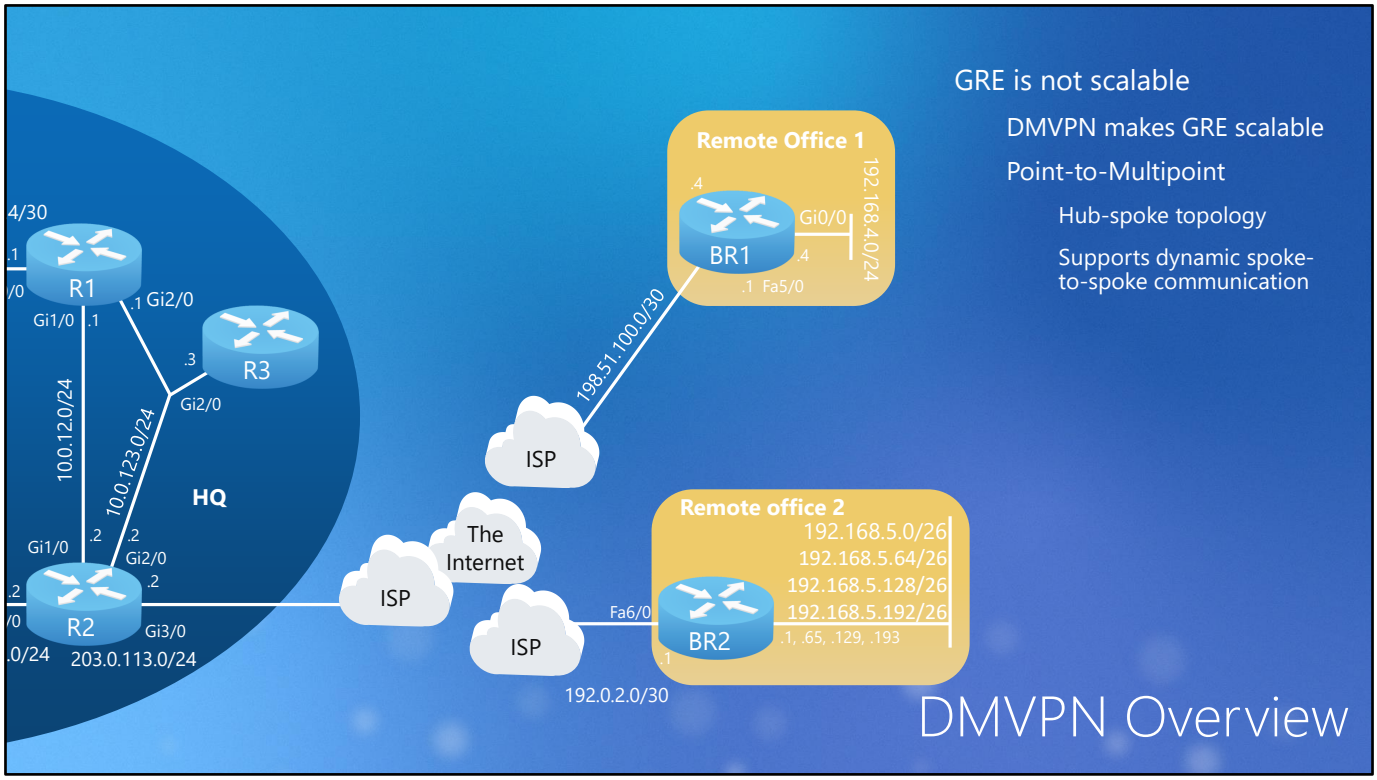
int fast 6/0
crypto map IPSEC_VPN_CM

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



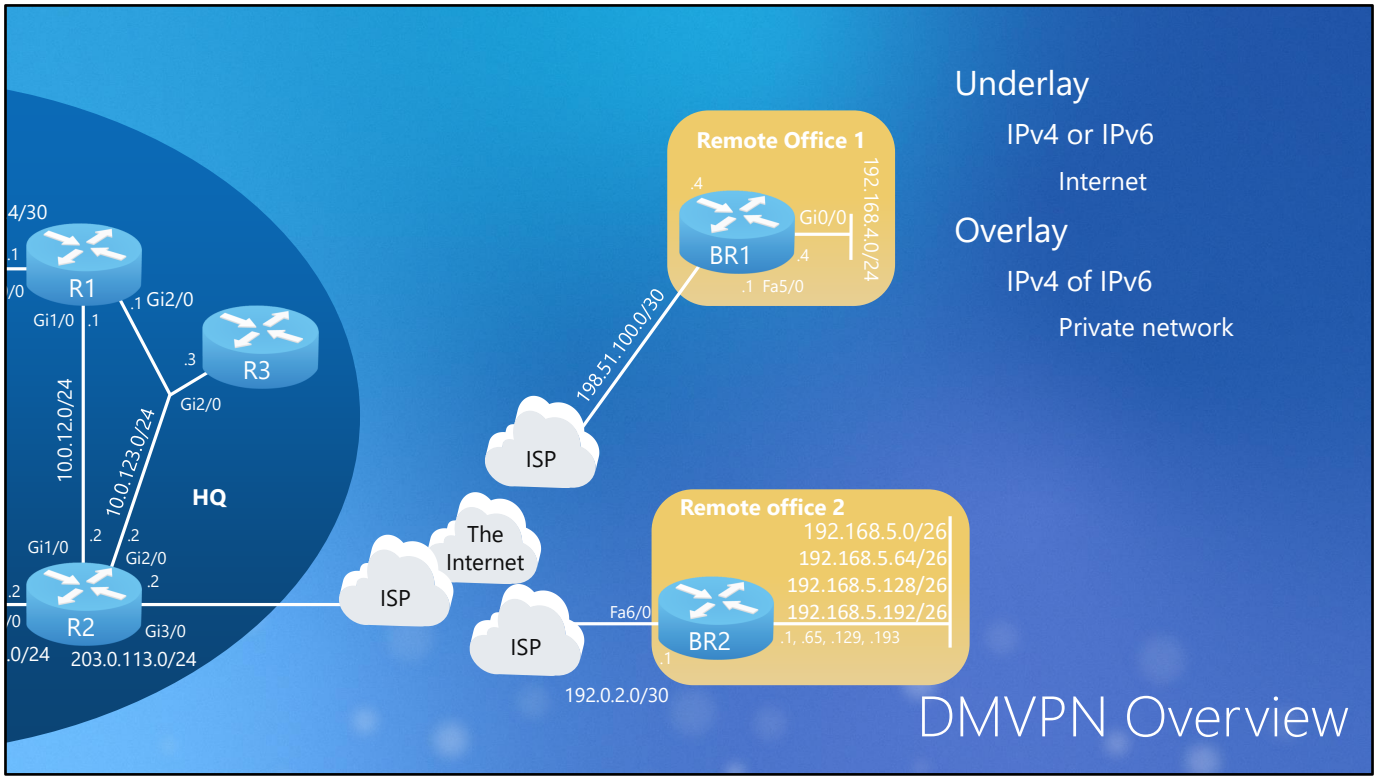
Title slide

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



DMVPN (Dynamic Multipoint Virtual Private Network) is a network framework that enables secure, scalable, and dynamic communication between sites without requiring direct connections between them. It combines several technologies, including GRE (Generic Routing Encapsulation), NHRP (Next Hop Resolution Protocol), and IPsec (Internet Protocol Security), to create a dynamic and efficient VPN network.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



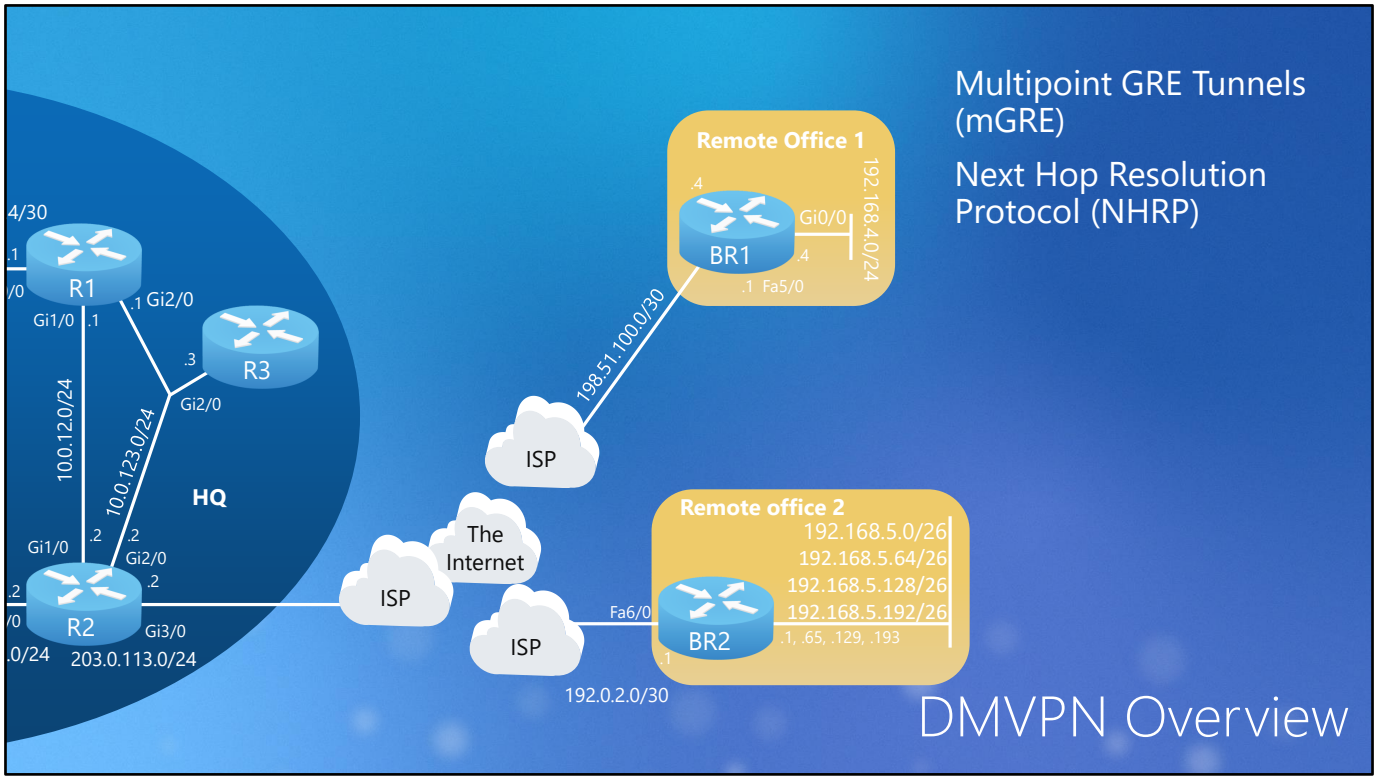
LIKE GRE…

Underlay – only requirement IP connectivity…. So as long as you can ping an IPv4 or IPv6 address through the provider network you are set for DMVPN. (The same is true for GRE)

Overlay – your private tunnels running over the underlay.

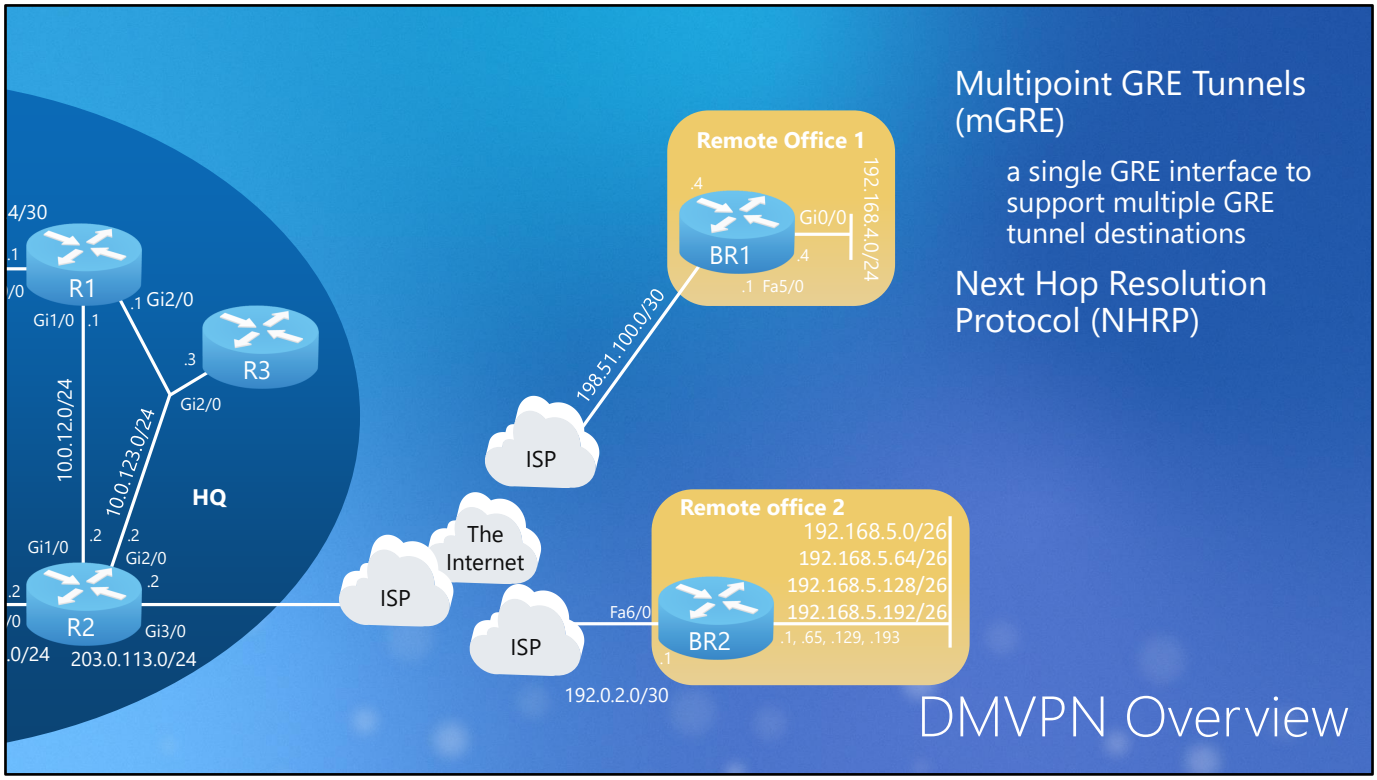
Also, it does not matter what protocols the provider is using, you can use whatever you want for the overlay. For example with MPLS if the provider says you have to use BGP then you have to use BGP. But with DMVPNs (GRE) you can run whatever DRP you want.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Here are two new terms you need to become familiar with.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



mGRE – this allows for a single GRE interface to support multiple GRE tunnel destinations. By default GRE is point-to-point which means a 1:1 mapping between a source and destination. So you would need one tunnel from R2 to BR1 with it's own IP addressing space and one tunnel from R2 to BR2 with it's own IP addressing space. But with mGRE you can have a 1:many mapping between a source and destinations in the same subnet. So the HQ and all Branch interfaces can be in the same ip addressing space.

With mGRE we define the source of the tunnel but not the destination. Therefore, NHRP is used to share and resolve the destination.

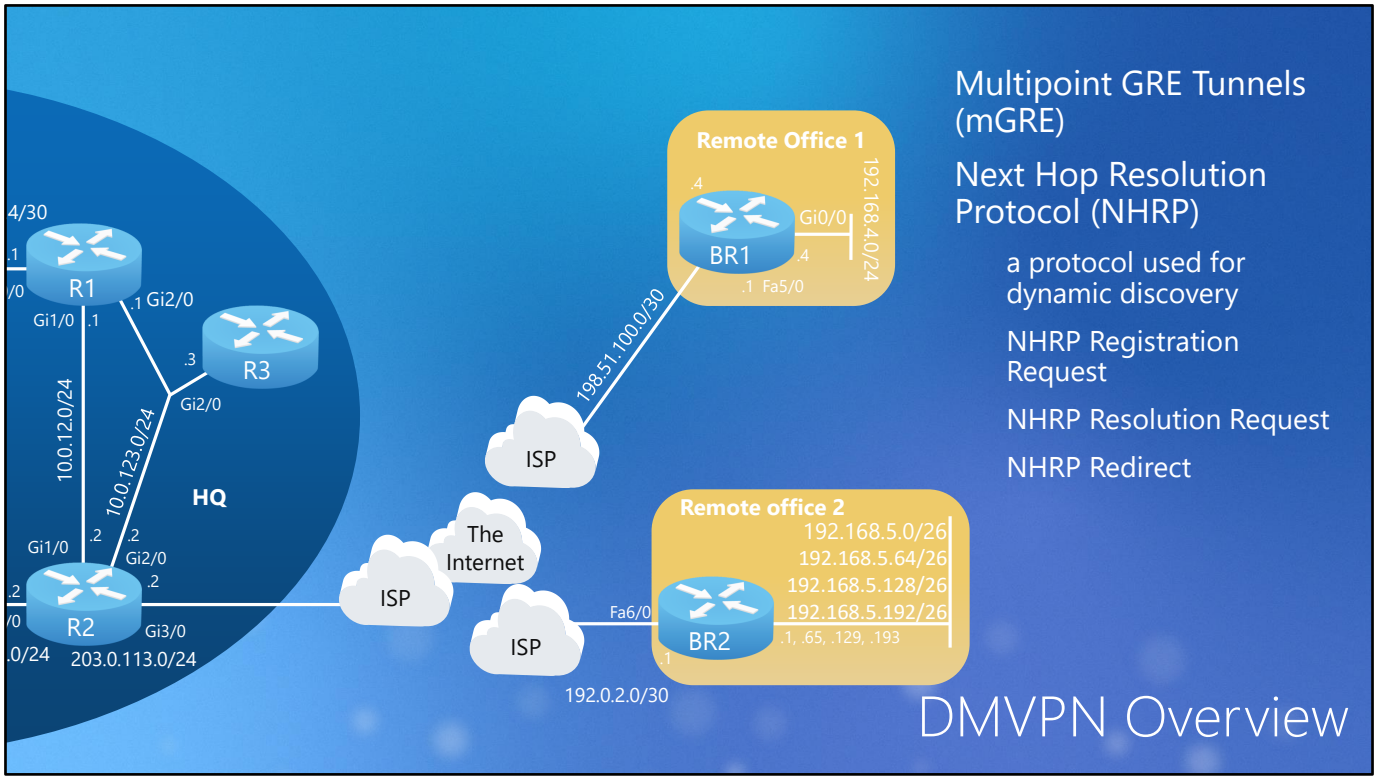
NHRP – a protocol used for dynamic discovery. It is like ARP. Recall that ARP is used to determine the MAC address of a known IP address. Well NHRP is used to map the spokes private overlay tunnel IP address (VPN address) to the public underlay ip address (NBMA address). So, for example when BR1 turns on, it will use NHRP to tell the HUB (R2) what it's private to public mapping is. This provides you with the ability to use static IPs on the BRs or DHCP address from the ISP on the BRs because the BRs can update the Hub when changes in IPs occur.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Hub = server / spoke = client

Security is provided with IPSEC (more on that later)
Supports routing with any routing protocol

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

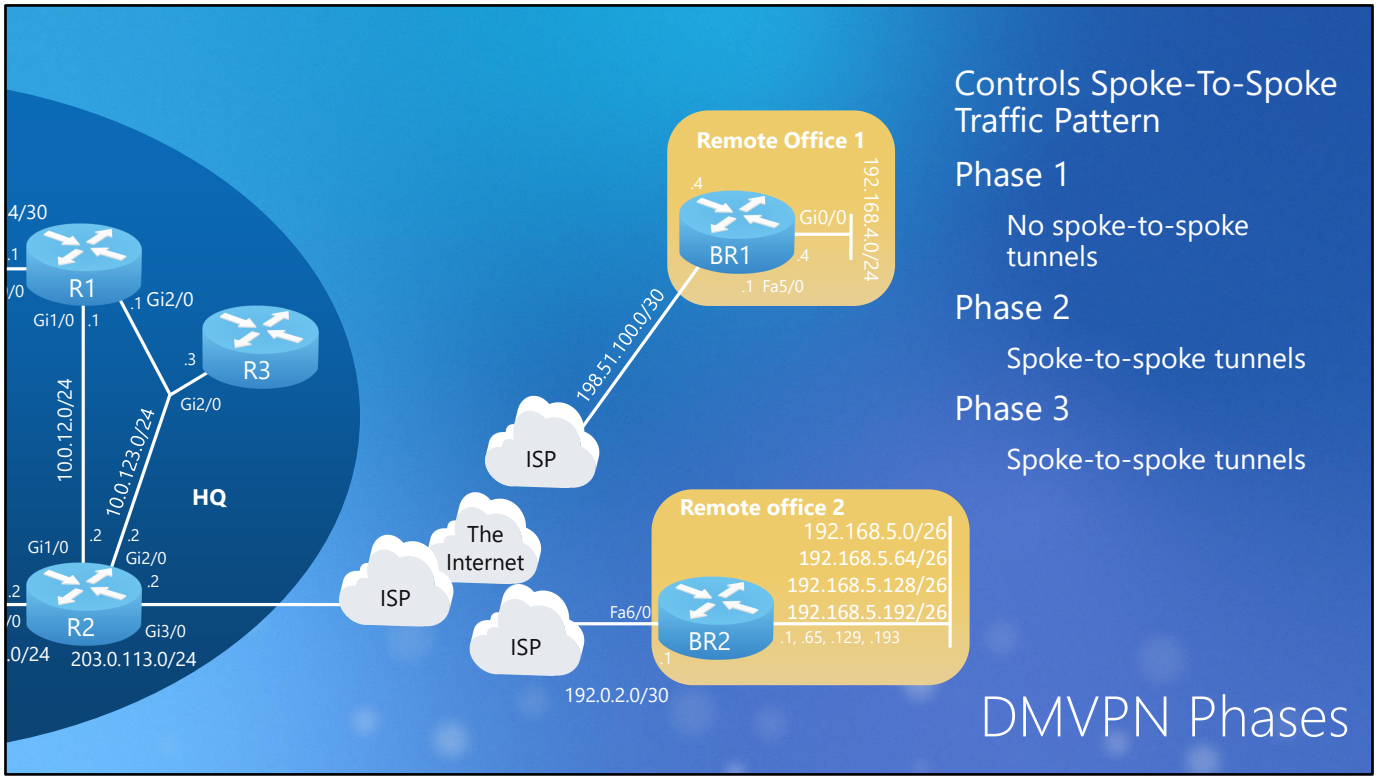


NHRP – a protocol used for dynamic discovery. It is like ARP. Recall that ARP is used to determine the MAC address of a known IP address. Well NHRP is used to map the spokes private overlay tunnel IP address (VPN address) to the public underlay ip address (NBMA address). So, for example when BR1 turns on, it will use NHRP to tell the HUB (R2) what it's private to public mapping is. This provides you with the ability to use static IPs on the BRs or DHCP address from the ISP on the BRs because the BRs can update the Hub when changes in IPs occur.

Hub = server / spoke = client

Security is provided with IPSEC (more on that later)
Supports routing with any routing protocol

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



So there are different phases (versions) of DMVPN. Each phase has different characteristics. Therefore, the phase you choose will be based on your objectives.

PHASES = VERSIONS

Phase 1: first DMVPN version ever created. tunnels only exist between hub and spokes, all traffic from spoke to spoke must go through hub. Supports summarization and default routes advertised from hub to spokes.

Phase 2: introduced to allow dynamic on-demand spoke-to-spoke tunnels. However, it does not allow summarization from spoke to hub and therefore does not scale well and does not support spoke-to-spoke communication between different DMVPN networks. (you will not really use this any more… use phase 3 instead)

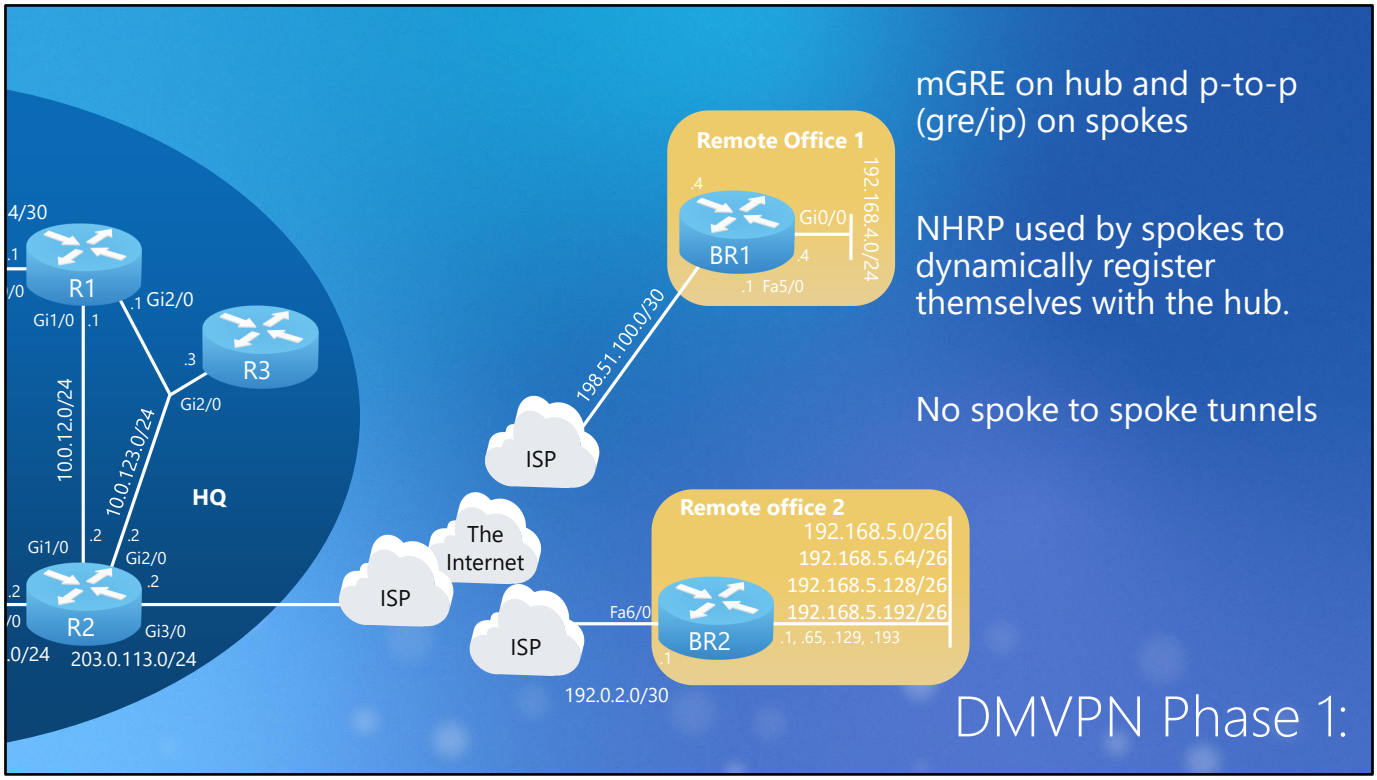
Phase 3: introduced to allow dynamic on-demand spoke-to-spoke tunnels like p2 but also sopports hierarchical tree spoke-to-spoke tunnels, so tunnels between routers in different DMVPN networks. Therefore it Uses redirect messages to accomplish this so that shortcut routes can be added to the routing table on the fly.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

It also supports summarization and as such scales better than Phase 2.

In conclusion… .use phase1 if you only want hub and spoke tunnels… use phase3 if you want spoke to spoke tunnels.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



mGRE on hub and p-to-p (gre/ip) on spokes

NHRP used by spokes to dynamically register themselves with the hub.

No spoke to spoke tunnels

Summarization/default routing allowed from hub to spokes as it does not break routing.

DEMO CONFIG:
HUB:

```
interface tunnel 0
 tunnel mode gre multipoint
 ip address 172.16.123.2 255.255.255.0
 tunnel source gig 3/0
 tunnel key 123456789 (you can run multiple hubs (tunnel interfaces) on the same physical interface. This key ensures they stay isolated)
 ip nhrp network-id 9 (identifies an NHRP server by its ID – because you can have multiple NHRP servers on a single router)
 ip nhrp authentication ENARSI (authenticates the NHRP server)
```

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

ip nhrp map multicast dynamic (specifies that multicast addresses from routing protocols will be dynamically learned from the spokes – this ensures that multicast and broadcast traffic will be allowed on the tunnel – enables psudo-broadcast / replicated unicast where broadcasts/multicasts are encapsulated in unicast for each destination.)

SPOKE BR1:
interface tunnel 0
tunnel mode gre ip
ip address 172.16.123.10 255.255.255.0
tunnel source fast 5/0
tunnel destination 203.0.113.2 (only required because we are p-to-p on spoke (gre/ip))
tunnel key 123456789
ip nhrp network-id 9
ip nhrp authentication ENARSI
ip nhrp nhs 172.16.123.2 (statically maps the NHRP server)
ip nhrp map 172.16.123.2 203.0.113.2 (indicates how to get to nhrp server)
ip nhrp map multicast 203.0.113.2 (enabes psudo-broadcast and sends them to hub only – needed for dynamic routing protocols)

SPOKE BR2:
interface tunnel 0
tunnel mode gre ip
ip address 172.16.123.20 255.255.255.0
tunnel source fast 6/0
tunnel destination 203.0.113.2
tunnel key 123456789
ip nhrp network-id 9
ip nhrp authentication ENARSI
ip nhrp nhs 172.16.123.2
ip nhrp map 172.16.123.2 203.0.113.2
ip nhrp map multicast 203.0.113.2

Verification

show ip nhrp – displays NHRP-mapping information on a device

Show interface tunnel – verify the state of the GRE tunnel

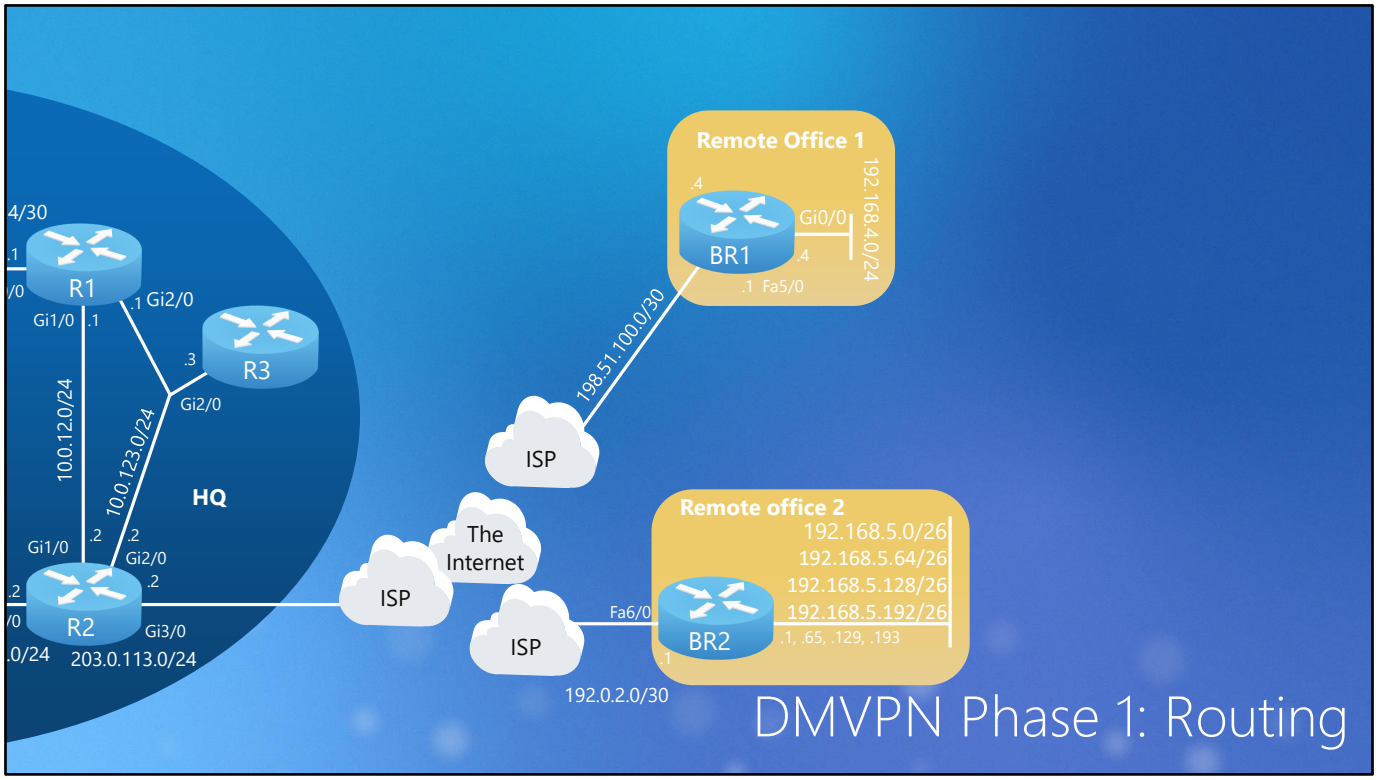
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Show ip nhrp nhs detail – displays NHRP next-hop server information (NOTE: if req-failed is greater than 0 it typically means there is a nhrp network ID or authentication mismatch… or maybe a connectivity problem with the nh server.

Show dmvpn detail – verify proper operation of DMVPN control functions (includes: IPSEC information, local and remote ip, number of packets encrypted and decrypted.

Show ip route – verify routes

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



DEMO ROUTING with EIGRP (already preconfigured everywhere but DMVPN tunnels):

R2(config)#router eigrp ENARSI
R2(config-router)#address-family ipv4 unicast autonomous-system 100
R2(config-router-af)#network 172.16.123.2 0.0.0.0 (add the tunnel interface)

BR1(config-router)#router eigrp BRANCH1
BR1(config-router)#address-family ipv4 unicast autonomous-system 100
BR1(config-router-af)#network 172.16.123.10 0.0.0.0 (add the tunnel interface)

BR2(config)#router eigrp BRANCH2
BR2(config-router)#address-family ipv4 unicast autonomous-system 100
BR2(config-router-af)#network 172.16.123.20 0.0.0.0 (add the tunnel interface)

VERIFY:
PROBLEM: BR1 does not teach BR2 and vice versa because of SPLIT HORIZON.
SOLUTION: Disable split horizon on R2 tunnel interface.

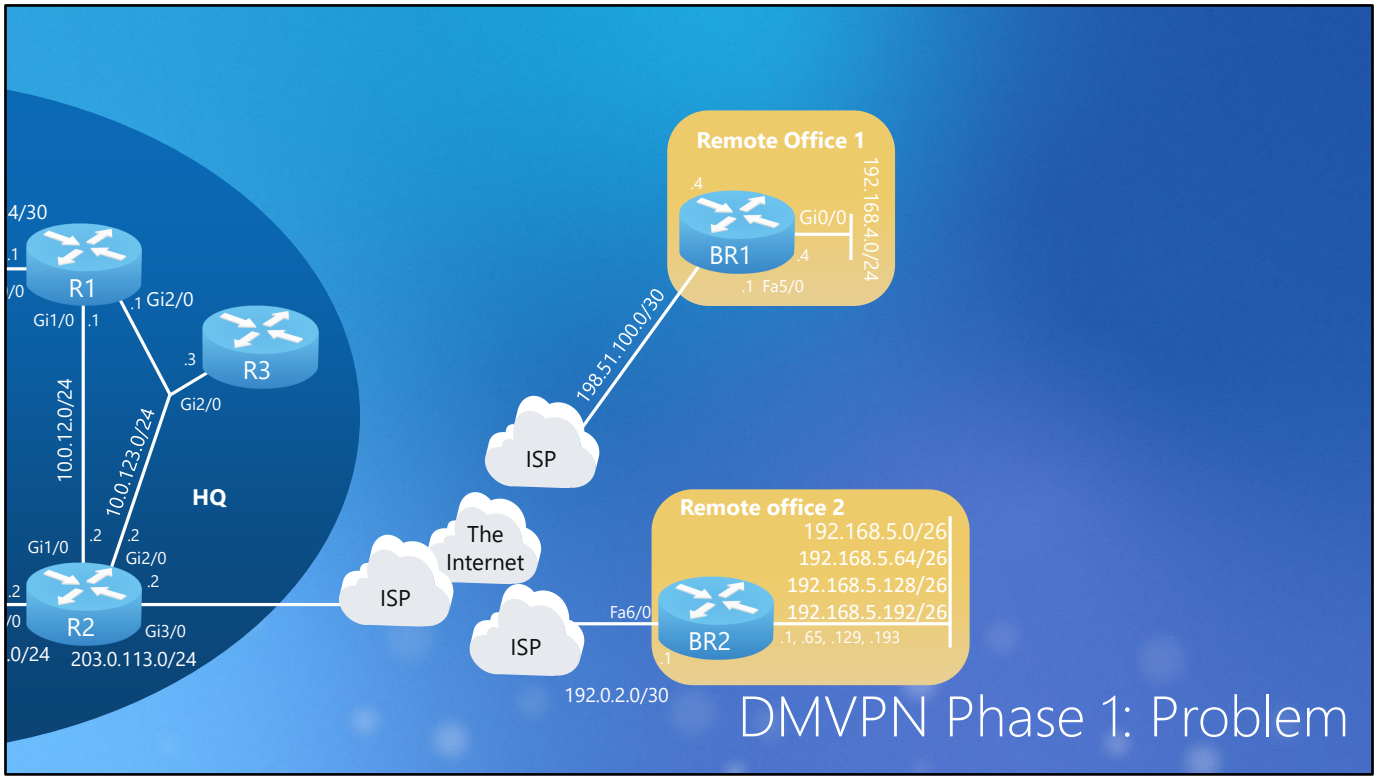
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

R2(config)#router eigrp ENARSI
R2(config-router)#address-family ipv4 unicast autonomous-system 100
R2(config-router-af)#af-interface tunnel 0
R2(config-router-af-interface)#no split-horizon

BECAREFUL… do you really want to advertise everything from everyone to everywhere…. Depends on your needs and the number of spokes you have. The more you advertise the more pressure it puts on your DMVPN solution. In this case, I could just advertise a default route to BR1 and BR2 from R2 or you could perform summarization on R2 towards BR1 and BR2 by going to the tunnel interface and using the summary address command on the tunnel interface.

WITH OSPF THE SIMPLIEST SOLUTION IS TO SET THE HUB OSPF TUNNEL INTERFACE TO NETWORK TYPE point-to-multipoint and the SPOKES TUNNEL INTERFACE TO NETWORK TYPE point-to-point. This eliminates the DR and BDR election altogether and makes OSPF think it is a bunch of point to point interfaces and preserves the next hop of the HUB. ***NOTE you can't summarize or use a default with OSPF because of the OSPF hierarchy. So, with DMVPNs OSPF is not the best solution because all the spokes need to be in the same area and if there is a flapping network it requires a recalculation to occur on all the routers. Essentially, it does not scale well. So in the real world we typically avoid OSPF on DMVPN and use EIGRP, BGP or RIP. For example, you might use RIP in the DMVPN and redistribute from OSPF into RIP and then into OSPF. Or if it is a new deployment you might want to make DMVPN area 0 and then every part of the network a different area and you can do type 3 and 5 summaries in and out of the DMVPN.*** Moral of the story… EIGRP, RIP, BGP = easy DMVPN… OSPF = difficult DMVPN.**

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



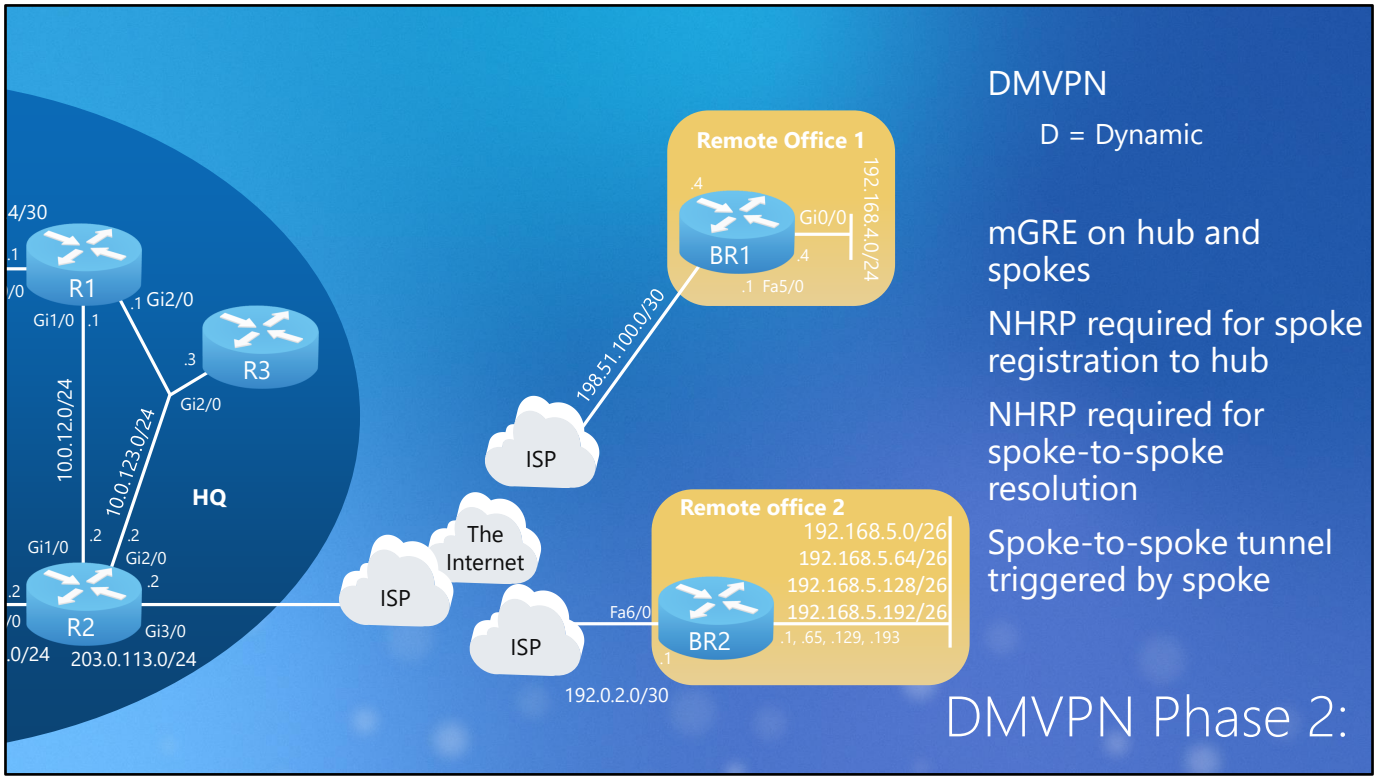
In this case all traffic must flow through the HUB.

Do a trace from BR1 to BR2

Trace 192.168.5.1 source 192.168.4.4

This is known as DMVPN PHASE 1 which is really not what you want because everything has to go through the hub. HUB has to decrypt, deencap, reencap, and reencrypt for spoke-to-spoke.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Spokes Dynamic learning of spoke private to public mappings with NHRP

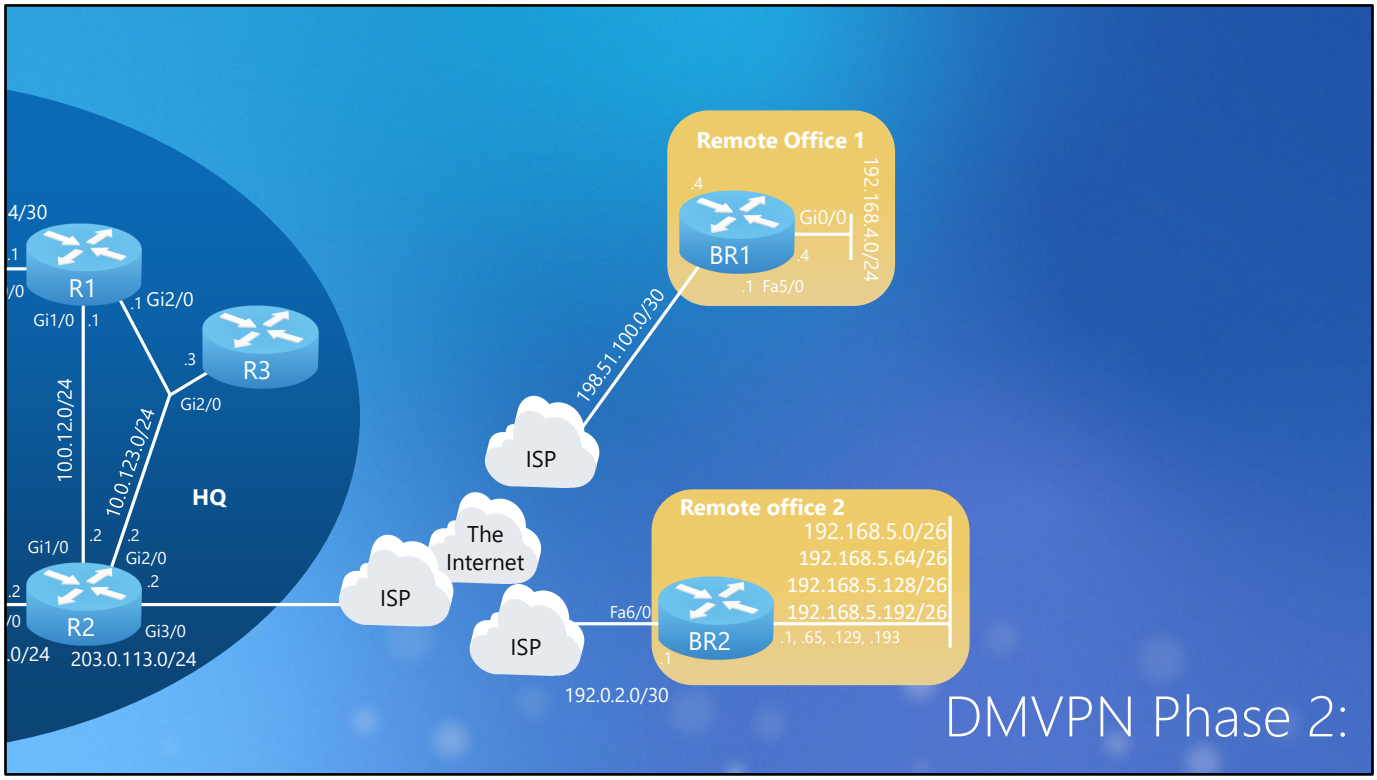
Spokes Dynamic "on-demand" formation of spoke-to-spoke tunnels
Created when needed based on traffic patterns and torn down when no longer in use (when traffic ceases to cross)

THIS IS WHAT MAKES IT SCALABLE

mGRE on hub and spokes
NHRP required for spoke registration to hub
NHRP required for spoke-to-spoke resolution
Spoke-to-spoke tunnel triggered by spoke

Summarization/default routing at hub is not allowed as it breaks spoke-to-spoke tunnels and everything ends up being hub and spoke. Summarization and default routing not allowed because the HUB would then be using a next-hop as itself when it advertises the summary or default and therefore the spoke to spoke tunnels could not be formed.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



PHASE 2 config adjustment…

BR1 and BR2:
Int tunnel 0
No tunnel destination
Tunnel mode gre multipoint

Show how a tunnel is created dynamically (show dmvpn) but the next hop (show ip route) is still R2….

For EIGRP you have to modify the next-hop
R2:
Router eigrp ENARSI
Address-famil ipv4 unicast auto 100
Af-interface tunn 0
no next-hop-self

For OSPF you would (forces R2 to be the DR.)
Set the interface ospf network type to broadcast on all the routers

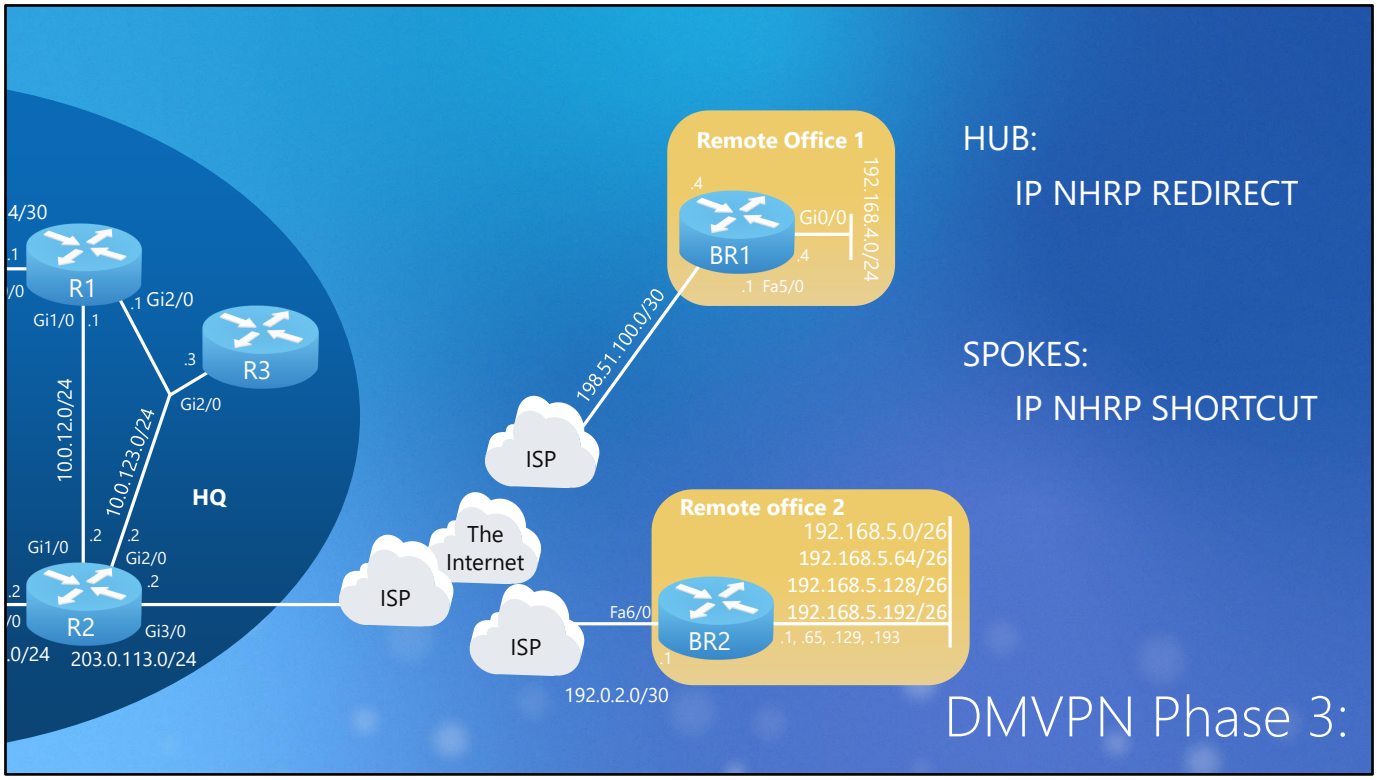
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Set the hub interface to have a pri of 1 or higher (255 is best incase you forget to set some new spoke to 0)
Set the spoke interfaces to have a pri of 0.

WHY DO WE DO THIS!!!(Because point-to-multipoint network type OSPF leaves the next hop as the HUB and in this case we need the next hop to be the spokes for the dynamic tunnels to be formed.)

Summarization/default routing at hub is “not allowed” as it breaks spoke-to-spoke tunnels and everything ends up being hub and spoke in the end. The reason is that with Summarization and default routing the HUB would then be using a next-hop as itself when it advertises the summary or default and therefore the spoke to spoke tunnels could not be formed because the route to get to each spoke would be through the summary or the default that is advertised by the HUB. So you have to the Hub via the summary to get to the spokes.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Because Phase 2 does not support summarization and default routing for spoke-to-spoke you really do not want to use it because it can't scale at all. Phase 3 is the solution to this. With Phase 3….

mGRE on hub and spokes
NHRP required for spoke registration to hub
NHRP required for spoke to spoke resolution

Allows for summarization and default routing DYNAMICALLY because…

When hub receives packet from spoke that is destined to another spoke

it sends NHRP redirect message back to originating spoke telling the spoke which "new" next-hop IP should be used to communicate directly with the spoke instead of the hubs ip, when it sends the next packet.

It also forwards the original packet to spoke, so it gets to destination.

The spokes will then create an on the fly tunnel between themselves to send the rest of the packets over.

So even though we might be using default routing from spoke to hub… the hub

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

realizes the packet is spoke to spoke, so it responds with the redirect. (So, the redirect is the hack on phase 2 and therefore we call it phase 3 which is the best of the phases.

Note the spoke actually adjusts it routing table because of the redirect.

Control plane is hub and spoke but data plane is full mesh.

PHASE 3 config adjustment when compared to PHASE 2….

BR1 and BR2:
Int tunnel 0
ip nhrp shortcut (used to tell routers to install NHRP routes.)

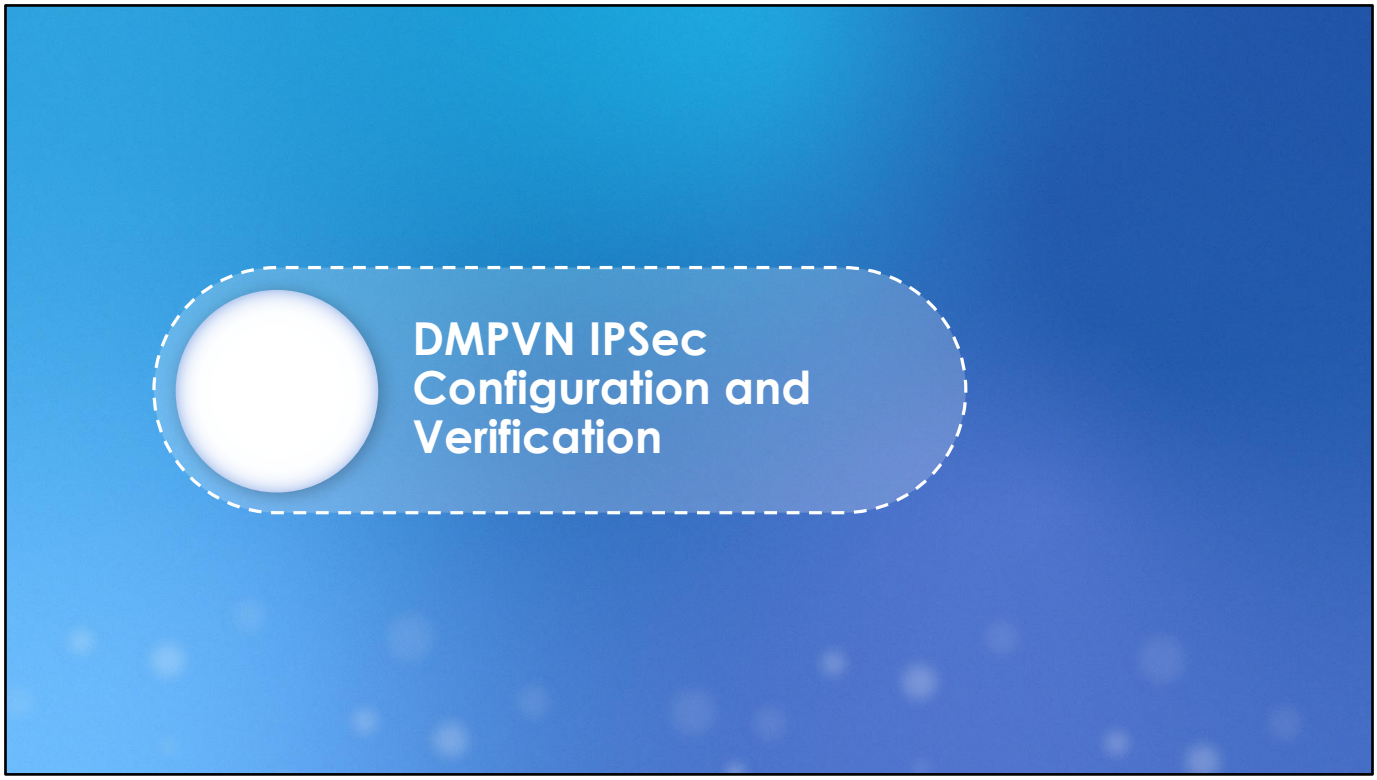
Show how a tunnel is created dynamically but the next hop is still R2….

For EIGRP you have to modify the next-hop
R2:
Int tunnel 0
Ip nhrp redirect (used to tell router to inform spokes of alternate next hop routes)
Router eigrp ENARSI
Address-famil ipv4 unicast auto 100
Af-interface tunn 0
next-hop-self

For OSPF you would (forces R2 to be the DR and ensure that tunnel interfaces have shortcut and redirect commands)
Set the interface ospf network type to broadcast on all the routers
Set the hub interface to have a pri of 1 or higher
Set the spoke interfaces to have a pri of 0.

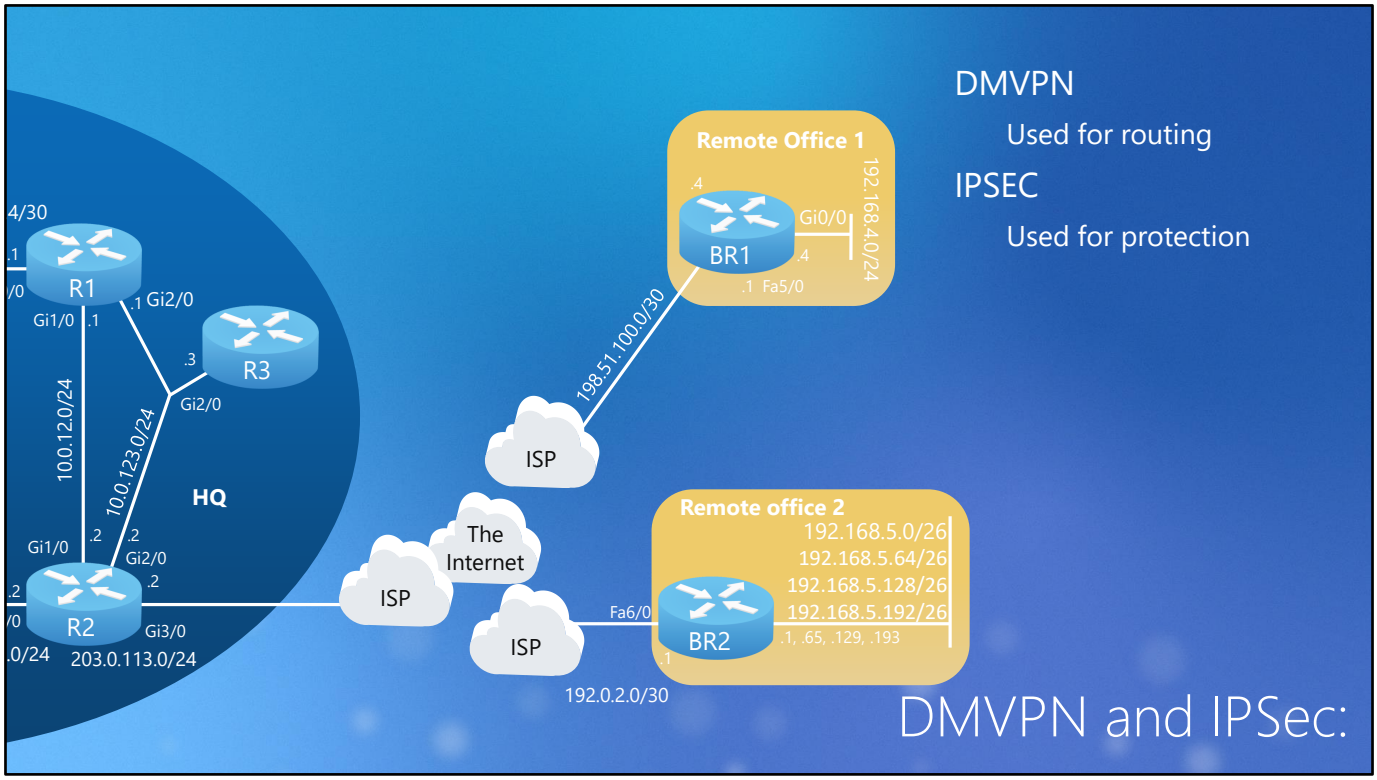
However, it does not solve the OSPF Area design issues.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

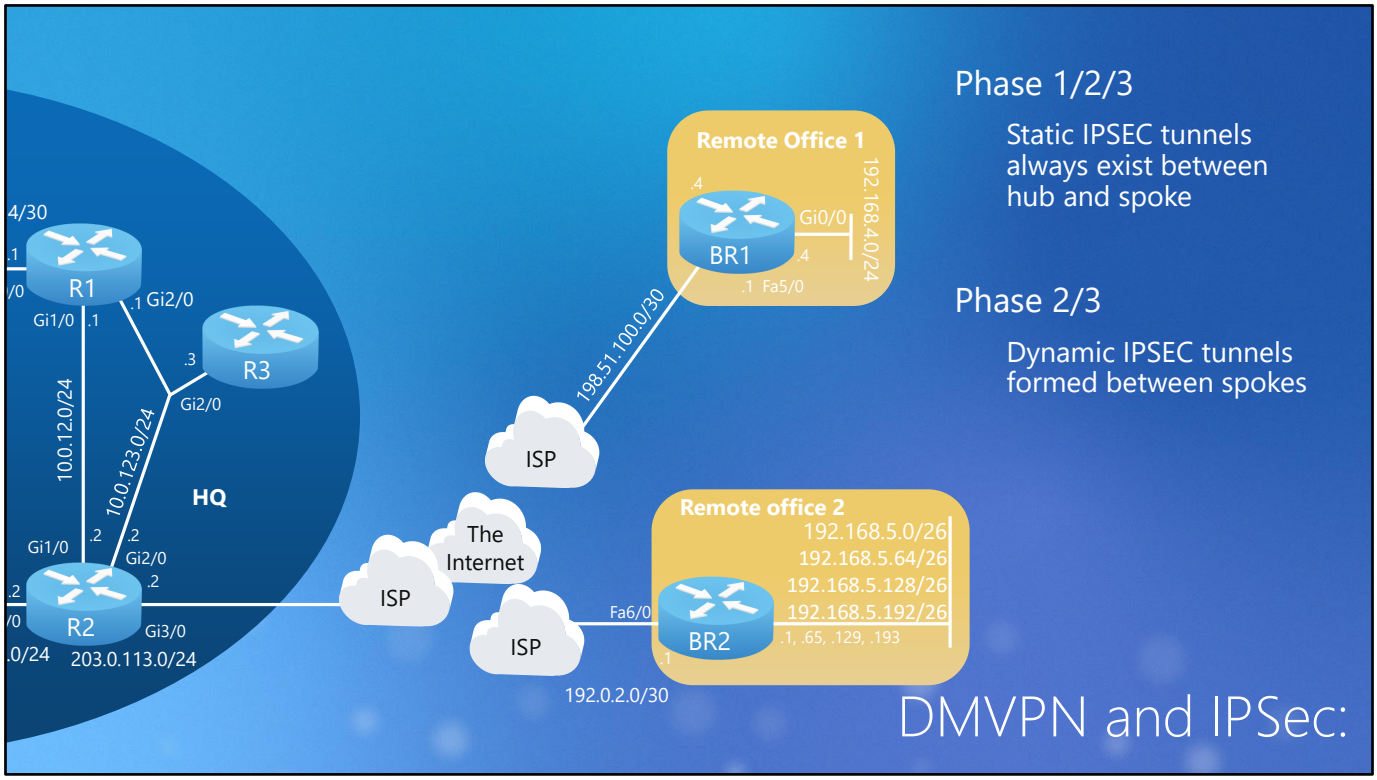


Title slide

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

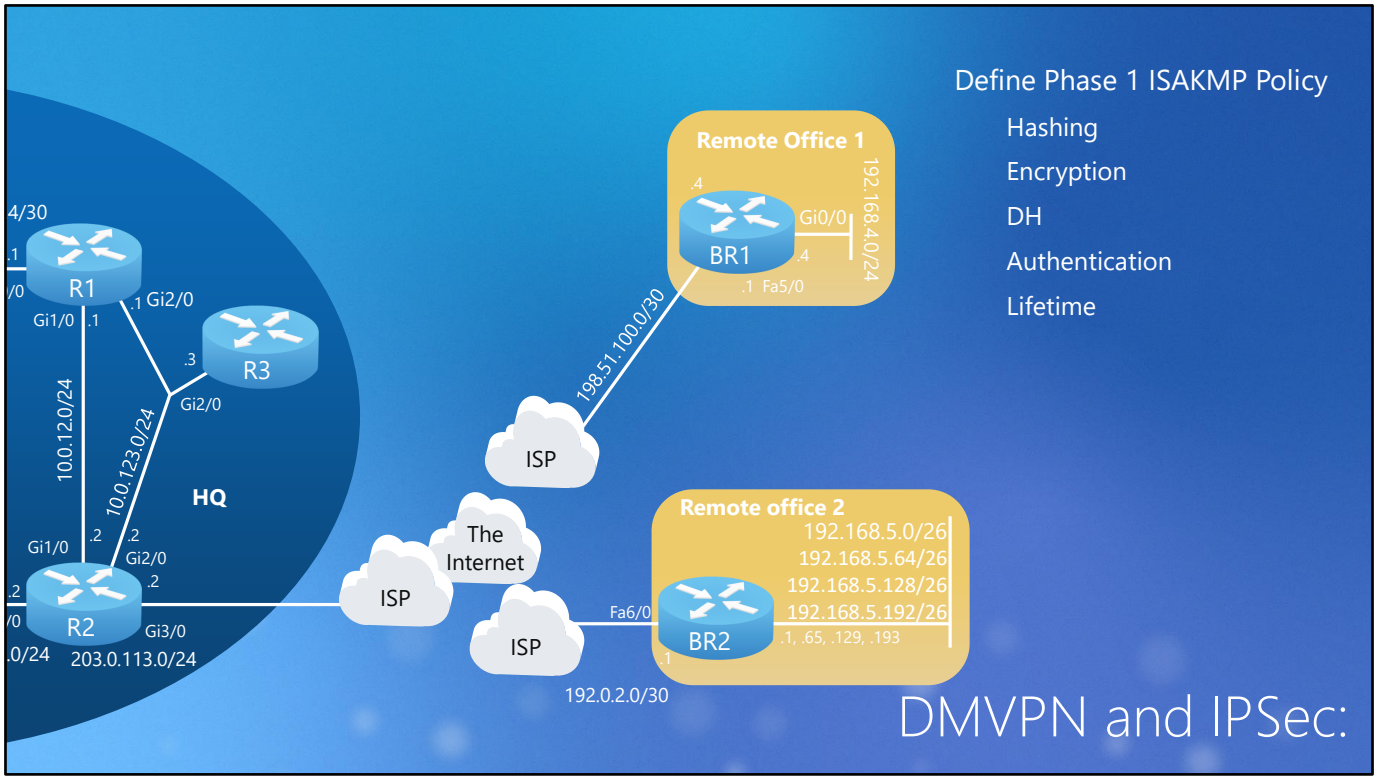


©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



For this to work we always need tunnels between hub and spokes (IPSEC SA always exists)…. However, dynamic tunnels can be formed between spokes (IPSEC SA created on-demand and torn down when no longer needed)

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



In the real world certificates are the best option for authentication not pre-shared. But we only need to worry about pre-shared for ENARSI.

```
IKE Phase 1 Configuration:
R2#configure terminal
R2(config)#crypto isakmp policy 10
R2(config-isakmp)#authentication pre-share
R2(config-isakmp)#encryption aes 256
R2(config-isakmp)#group 16
R2(config-isakmp)#hash sha256
R2(config-isakmp)#exit
R2(config)#crypto isakmp key PASSWORD address
198.51.100.1 (exam use 0.0.0.0 which means everyone)
R2(config)#crypto isakmp key PASSWORD address 192.0.2.1
R2(config)#end
R2#

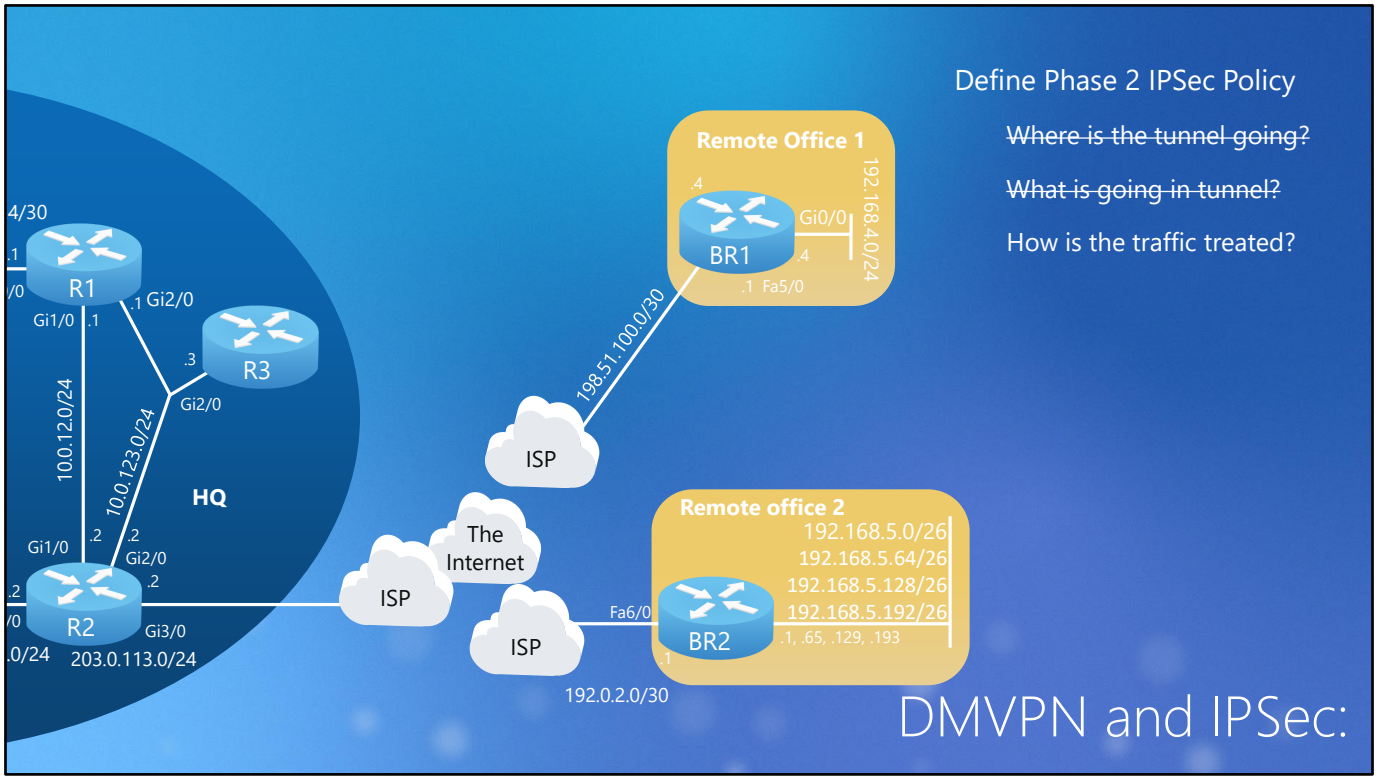
BR1#configure terminal
```

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

```
BR1(config)#crypto isakmp policy 10
BR1(config-isakmp)#authentication pre-share
BR1(config-isakmp)#encryption aes 256
BR1(config-isakmp)#group 16
BR1(config-isakmp)#hash sha256
BR1(config-isakmp)#exit
BR1(config)#crypto isakmp key PASSWORD address 192.0.2.1
BR1(config)#crypto isakmp key PASSWORD address
203.0.113.2
BR1(config)#end
BR1#

BR2#configure terminal
BR2(config)#crypto isakmp policy 10
BR2(config-isakmp)#authentication pre-share
BR2(config-isakmp)#encryption aes 256
BR2(config-isakmp)#group 16
BR2(config-isakmp)#hash sha256
BR2(config-isakmp)#exit
BR2(config)#crypto isakmp key PASSWORD address
198.51.100.1
BR2(config)#crypto isakmp key PASSWORD address
203.0.113.2
BR2(config)#end
BR2#
```

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Changes here. We only need to define the transform-set…. So how is the traffic treated and we do this in a crypto ipsec profile instead of a crypto map.

IKE Phase 2 Configuration:
Define Phase 2 IPSec Policy

Where is the tunnel going? (IP address of hostname) SET (NOT NEEDED BECAUSE THE TUNNEL DESTINATION is dynamically leanred)

What is going in tunnel? (ACLs) MATCH (NOT NEEDED BECAUSE IT IS GRE traffic which is defined by the interface)

How is the traffic treated? (Transform Set) (encyp, hash, etc) SET (In this case we will be using what is called a Crypto IPSec Profile instead of a Crypto MAP)

Must match on devices creating tunnels

On all the routers:
crypto ipsec transform-set DMVPN_TRANSFORM esp-aes 256 esp-sha256-hmac

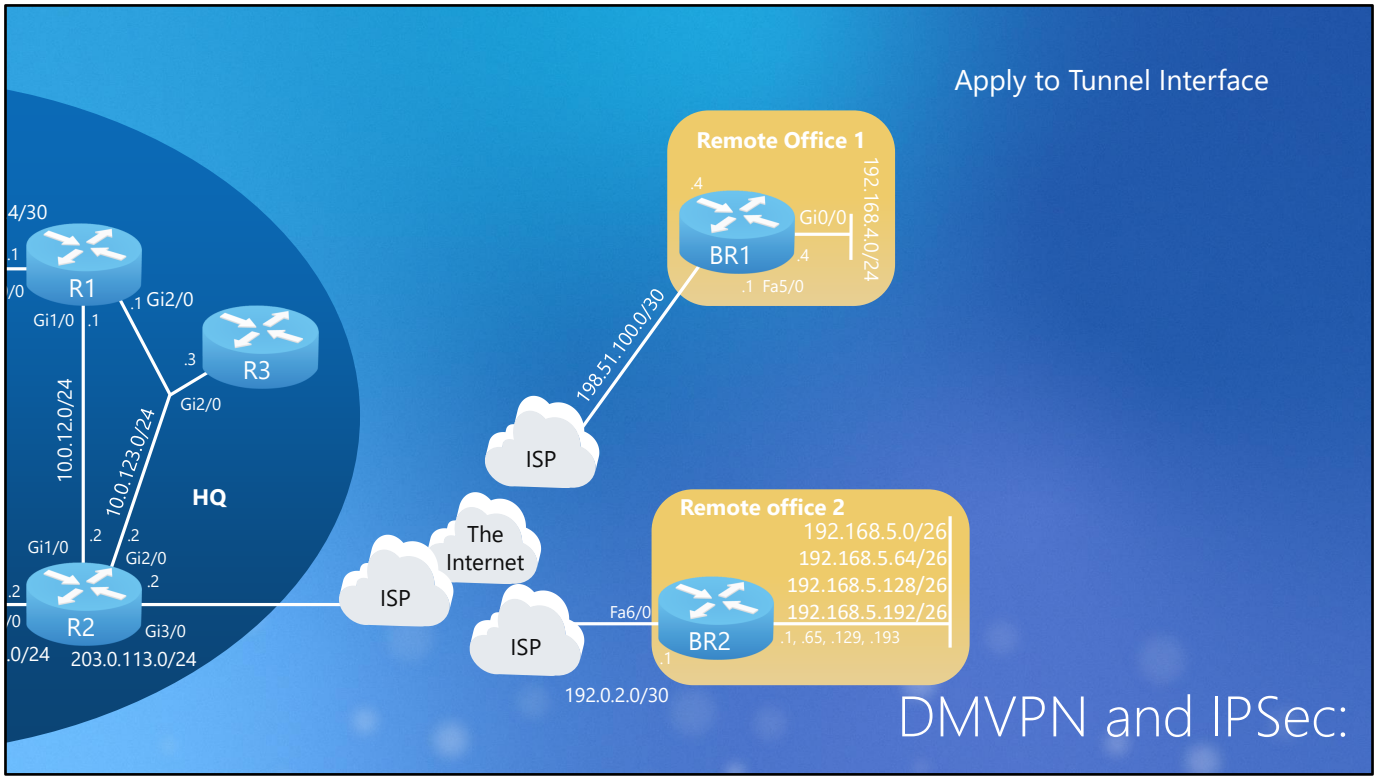
Tunnel mode ??? (default is tunnel mode)

exit

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

```
crypto ipsec profile DMVPN_IPSEC_PROFILE
        set transform-set DMVPN_TRANSFORM
```

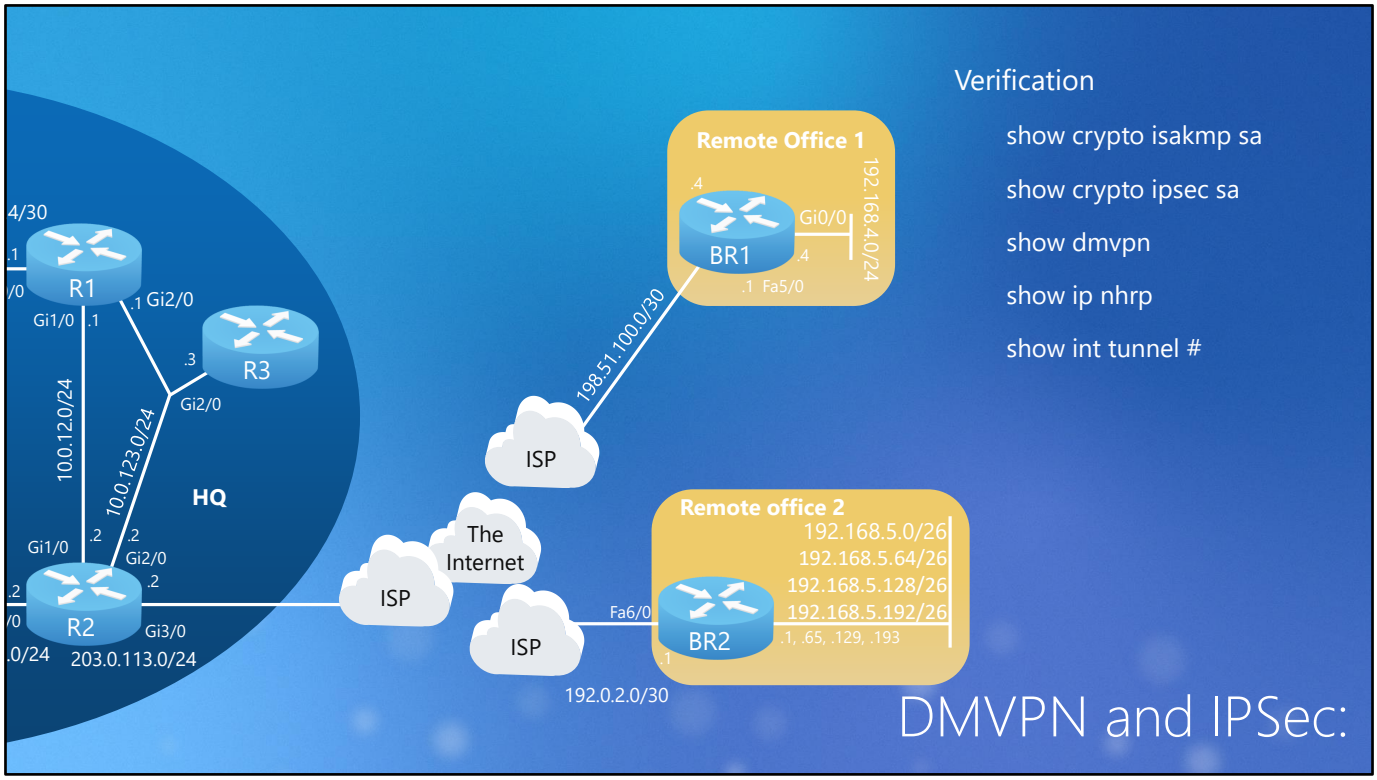
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



inter tunn 0
tunnel protection ipsec profile DMVPN_IPSEC_PROFILE

(Bounce all tunnel interfaces to be on the safe side)

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



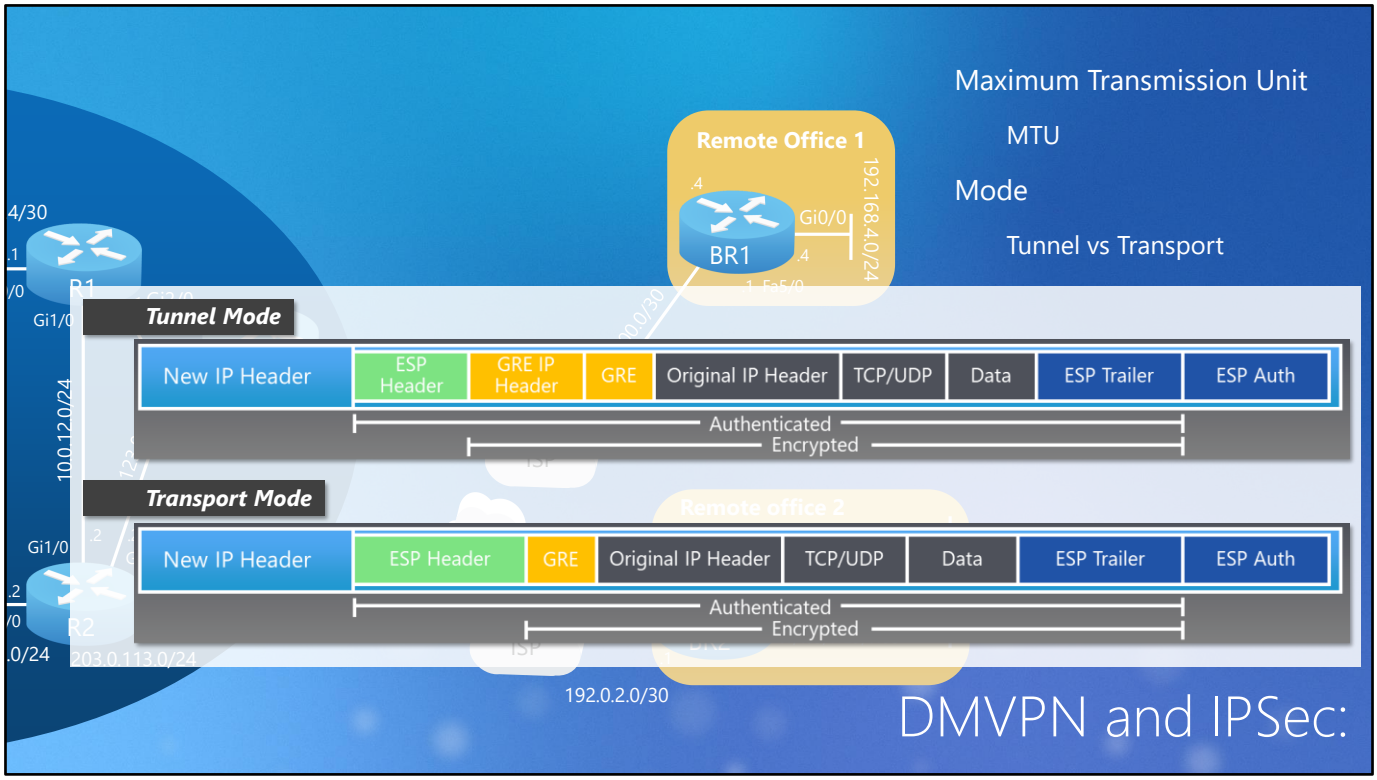
Remember order of operations when verifying… crypto first… if working… then nhrp and dmvpn…

So as the number of spokes grows the number of IPSEC tunnels from hub to spoke will grow in a linear fashion. The spoke to spoke tunnels will scale on demand.

If for some reason you get to the point where IPSEC SA scaling is becoming an issue because of the number of associates and keys (too many sites) you will want to consider GETVPN which uses GDOI (Group Domain of Interpretation) so that the routers can all use the same keying material for all the tunnels instead of having to use different keying material for each tunnel.

Keep in mind that GETVPN is a transport encryption not a tunnel encryption. So there are no “tunnels” created which means it can’t be used over internet by default. However, DMVPN allows us to create a tunnel that we can then use GETVPN to encrypt at a transport level. So we get any to any encryption where IPSEC by default is 1:1 or point to point.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



(TUNNEL MODE IS THE DEFAULT)

MTU = 1500 by default (Maximum size of a packet that can fit in an ethernet frame)

If we leave it as such client to client communication may need to be fragmented by the routers before they send the packets because the routers have to add on GRE headers and IPSEC headers.

So, we should lower the interface MTU to 1400 so that when the clients do PMTU discovery they will not send packets larger than 1400 bytes and therefore, once the GRE and IPSEC headers are added they will be less than 1500 bytes.

int tun 0
    Ip mtu 1400
Also it is recommend that you set the maximum segment size as well to 1360.
    ip tcp adjust-mss 1360

crypto ipsec transform-set DMVPN_TRANSFORM esp-aes 256 esp-sha256-hmac
    Mode transport

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



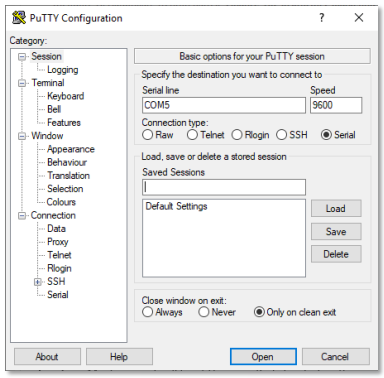
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

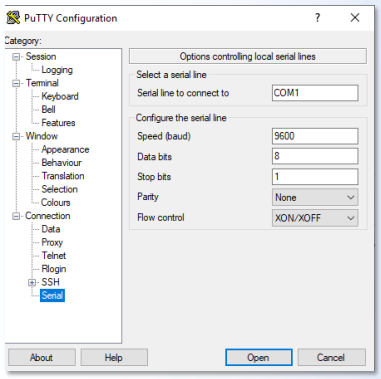


Title slide

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Console Connection







USB-to-Serial Port Adapter



Console Port



Mini USB Console Cable



Console Cable

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Securing Console and VTY Lines

Line Passwords

```
R1#show run | b line
line con 0
 exec-timeout 0 0
 password cisco
 login
 logging synchronous
 stopbits 1
line vty 0 4
 exec-timeout 0 0
 password cisco
 login
!
end
```

logging synchronous: prevents logs from interrupting command input
password: sets password on the line
login: enables the use of the password on the line
exec-timeout: controls idle timer for auto logout

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Securing Console and VTY Lines

Usernames and Passwords

```
R1 #configure terminal
R1(config)#username RAYMOND password AWESOME
…or…
R1(config)#username RAYMOND secret AWESOME
R1(config)#line vty 0 4
R1(config-line)#login local
R1(config-line)#end
R1#show run | b line
line vty 0 4
 exec-timeout 0 0
 password cisco
 login local
!
End
R1#show run | include username
username RAYMOND password 0 AWESOME
username RAYMOND secret 5 $1$TP/I$47x2WjpeZYFbPdw7fKqQh1
```

login local: enables the password on the line using the local username and password database / ignores the line password

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Securing Console and VTY Lines

Usernames and Passwords

```
R1 #configure terminal
R1(config)#username RAYMOND password AWESOME
…or…
R1(config)#username RAYMOND secret AWESOME
```

```
R1(config)#username RAYMOND algorithm-type ?
  md5     Encode the password using the MD5 algorithm
  scrypt  Encode the password using the SCRYPT hashing algorithm
  sha256  Encode the password using the PBKDF2 hashing algorithm

R1(config)#username RAYMOND algorithm-type sha256 secret cisco

R1(config)#do sho run | i username
username RAYMOND secret 8 $8$yqKZVyUNhfu2UF$dS1EXlZxv.tSqvO3XmzPn73euFLBZwA4.rKW8ypaJQM
```

```
username RAYMOND password 0 AWESOME
username RAYMOND secret 5 $1$TP/I$47x2WjpeZYFbPdw7fKqQh1
```

login local: enables the password on the line using the local username and password database / ignores the line password

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Verifying Console and VTY Connections

Verifying connections with **show users:**

```
R1#show users
    Line     User       Host(s)     Idle       Location
   0 con 0               idle        00:00:00
*  1 vty 0               idle        00:00:00   192.168.2.103
   2 vty 1   admin       idle        00:00:08   172.16.34.3


! To clear a session type:
clear line line_number

line_number = the number on the left of the output
```

To verify console and vty connections.

- Indicates that is the session you are using right row. So I typed this command from the connection I have to vty line 0.
- The fist # is the session number the second number refers to the actual line number.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Securing Privileged EXEC Mode

By default authentication is not required to access privileged EXEC mode:

Enable password prevents unauthorized access to privilege mode

```
R1(config)# enable password cisco
```

Enable secret stores the password as a hash

```
R1(config)# enable secret cisco
```

Enable secret stores the password as a hash

```
R1#show run | include enable
enable secret 5 $1$b0RL$rJiwafa.QEWOB992KQzCS0
enable password cisco
```

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Securing Privileged EXEC Mode

Enable secret options

```
R1(config)#enable secret ?
  0       Specifies an UNENCRYPTED password will follow
  5       Specifies a MD5 HASHED secret will follow
  8       Specifies a PBKDF2 HASHED secret will follow
  9       Specifies a SCRYPT HASHED secret will follow
  LINE    The UNENCRYPTED (cleartext) 'enable' secret
  level   Set exec level password
```

Enable algorithm-type

```
R1(config)#enable algorithm-type ?
  md5      Encode the password using the MD5 algorithm
  scrypt   Encode the password using the SCRYPT hashing algorithm
  sha256   Encode the password using the PBKDF2 hashing algorithm
```

Enable algorithm-type stores the password as a hash

```
R1(config)#enable algorithm-type sha256 secret cisco
R1(config)#do sho run | i enable
enable secret 8 $8$9F9awpzr9kDJXm$VIWU3nfsY7Ee/u.rJUwdLQtUW5sg2qo0kCo99FRvZdk
```

Md5 = 5
Scrypt = 9
Sha256 = 8

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Encrypting Plain-Text Passwords

To encrypt plain text passwords, use this command:

```
R1#show run | include enable
enable secret 5 $1$b0RL$rJiwafa.QEWOB992KQzCS0
enable password cisco

R1(config)#service password-encryption

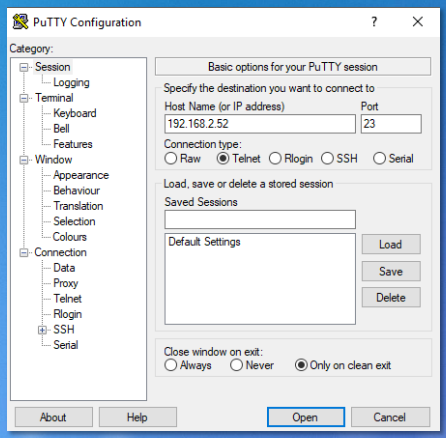
R1#show run | include enable
enable secret 5 $1$b0RL$rJiwafa.QEWOB992KQzCS0
enable password 7 110A1016141D
R1#show run | b line
line con 0
 exec-timeout 0 0
 password 7 0822455D0A16091610
 logging synchronous
 stopbits 1
line vty 0 4
 exec-timeout 0 0
 password 7 0822455D0A16091610
 login
```

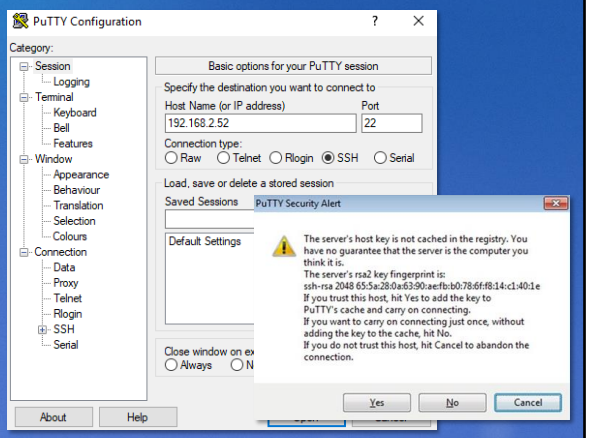
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Telnet vs SSH

Telnet:
Non-Encrypted communication

SSH:
Encrypted communication





©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Configure Secure Shell (SSH)

```
Router#config t
R1(config)#hostname R1
R1(config)#ip domain-name stormwindciscodemos.com
R1(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: R1.stormwindciscodemos.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-
exportable...[OK]

R1(config)#username raymond secret awesome
R1(config)#line vty 0 4
R1(config-line)#login local
R1(config-line)#transport input ssh
R1(config-line)#exit
R1(config)#ip ssh version 2
R1(config)#ip ssh authentication-retries 2
R1(config)#ip ssh time-out 90
```

```
ip ssh authentication-retries 2 (default is 3)
     Specifies the number of authentication attempts
     allowed before the connection is dropped.

ip ssh time-out 90 (default is 120)
     Specifies the inactivity timeout in seconds
```

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

SSH Verification

To verify that SSH is enabled: **show ip ssh**

```
R1#show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 90 secs; Authentication retries: 2
```

To view any active SSH sessions: **show ssh**

```
R1#show ssh
%No SSHv1 server connections running.
%No SSHv2 server connections running.
```

```
R1#show ssh
%No SSHv1 server connections running.
Connection Version Mode Encryption  Hmac         State              Username
1          2.0     IN   aes256-cbc  hmac-sha1    Session started    raymond
1          2.0     OUT  aes256-cbc  hmac-sha1    Session started    raymond
```

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Configure HTTP/HTTPS

Configuring access to a built in GUI (if it exists)

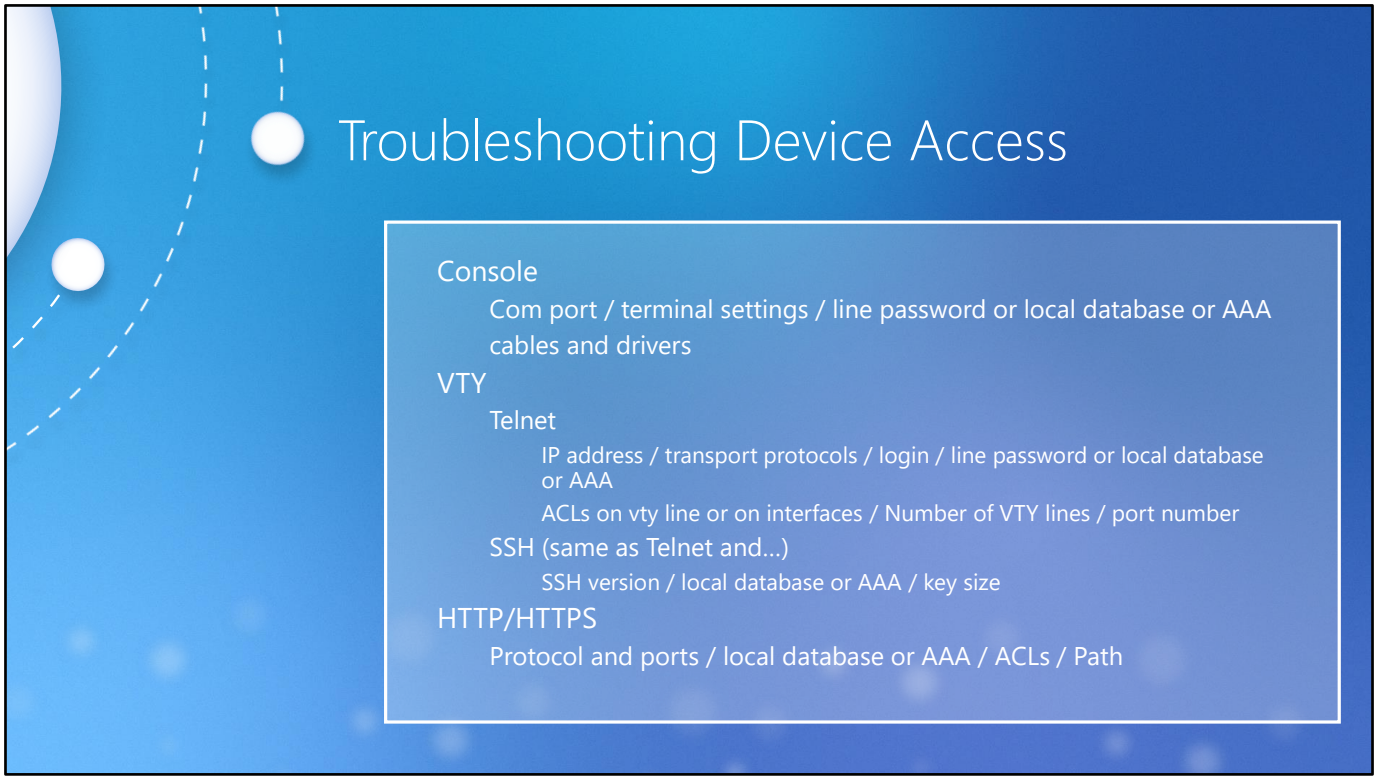
```
R1#config t
R1(config)#username raymond privilege 15 secret awesome
R1(config)#ip http server
R1(config)#ip http secure-server
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 5 seconds)
R1(config)#
*Feb 25 20:01:24.620: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config)#ip http authentication local
R1(config)#ip http access-class 3
R1(config)#ip http path flash:/GUI
R1(config)#access-list 3 permit 10.0.0.0 0.0.0.255
```

```
ip http authentication local
     Use local username and password database

ip http access-class 3
     Only allow access from devices with a source IP
     address listed in acl 3

ip http path flash:/GUI
     Identifies the root folder of the GUI
```

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Console:

■ Has the correct COM port been selected in the terminal program? Most times, multiple COM (communication) ports are displayed in the terminal program; however, the last one listed in the drop-down list is usually the correct one to use. However, if it is not, try a different one. This is really a trial-and-error process. It might help to d etermine the COM port numbers of the operating system you are using to run the terminal program. For example, with Windows 10 you can identify COM port n umbers in Device Manager.

■ Are the terminal program's settings configured correctly? Cisco devices use the following default values: 9600 baud, 8 data bits, 1 stop bit, and no parity.

■ Is a line password used to authenticate to the console? If a line password is being used, the login command needs to be configured as well. The login command and a line password are not configured by default.

■ Are a local username and password used to authenticate to the console? If local authentication is being used, a username and password must exist in the local database, and the login local command is required on the line.

■ Is an AAA (authentication, authorization, and accounting) server used to authenticate to the console? If AAA authentication is being used, a method list needs to be defined with the login authentication {default | list_name} command in line

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

console configuration mode.

■ Are the correct cable and drivers being used to connect to the console port? Check your device's documentation to see what is needed. Newer devices use a mini-USB port as the console port (with drivers required on a PC), and older devices use the serial-to-RJ45 console (rollover) cable; if a device does not have a serial port, you need a USB-to-serial cable to connect to the console cable and the correct drivers on your PC to use it.

Telnet

■ Is the IP address of the remote router/switch reachable? You can test this with the ping command.

■ Are the correct transport protocols defined for the line? By default, with IOS 15.0 and later, Telnet and SSH are allowed, and if other protocols are supported, they are typically allowed as well; however, with the transport input command, you can change which transport protocols are allowed. You can verify the allowed protocols with the command show line vty line_number | include Allowed, as shown in Example 23-1. In this example, Telnet and SSH are allowed for inbound and outbound connections.

■ Is the line configured to ask the user for credentials? By default, it is. The login command tells the line to prompt the user for a password, as shown in Example 23-2. However, if you need to authenticate the user through the local database, the login local command is required, and if you need to authenticate the user through AAA, the login authentication {default | list_name} command is required.

■ Is a password specified? Because the login command is enabled by default, a password is required. If the password is not set, the error message "Password required, but none set" appears. If you are using the login local command or AAA, you are prompted for a username and password. However, if the username and password are not stored in the database, your login is invalid and fails.

■ Is there an ACL (access control list) defining which management stations, based on IP address, can access the router/switch? Example 23-3 shows ACL 1 applied to the vty lines. It only allows access from the IP address 192.168.1.11. Notice the explicit deny that was added to keep track of the number of denied remote access attempts that have occurred (seven in this case). To receive a log message indicating which IP address was denied, you need to add the log keyword to the end of the explicit deny entry in the ACL. The following log message appears if the log keyword is added: "%SEC-6-IPACCESSLOGS: list 1 denied 10.1.12.2 1 packet."

■ Are all vty lines busy? By default, there are five vty lines on Cisco routers and switches, numbered 0 to 4. Some devices have more. However, regardless of the number, if all the lines have established connections, a new connection will not be made, as shown in Example 23-4. In this case, the show users command on SW1 indicates that there is one console connection, and there are five vty connections on lines 0 to 4. The next device that tries to use Telnet will be refused and will receive

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

the message “Password required, but none set,” even though that is not technically the issue. If you need to manually clear the lines, use the clear line command followed by the line number specified before vty, as shown in Example 23-4, rather than the actual vty number listed after vty.

■ Is there an ACL in the path between the client and the device blocking port 23? Telnet uses TCP port 23. If an ACL configured on a router or firewall is blocking port 23, you will be unable to make a successful Telnet connection.

SSH

With Secure Shell (SSH), you may experience the same issues as described with Telnet, in addition to several others. Consider the following additional issues when troubleshooting SSH access to a device:

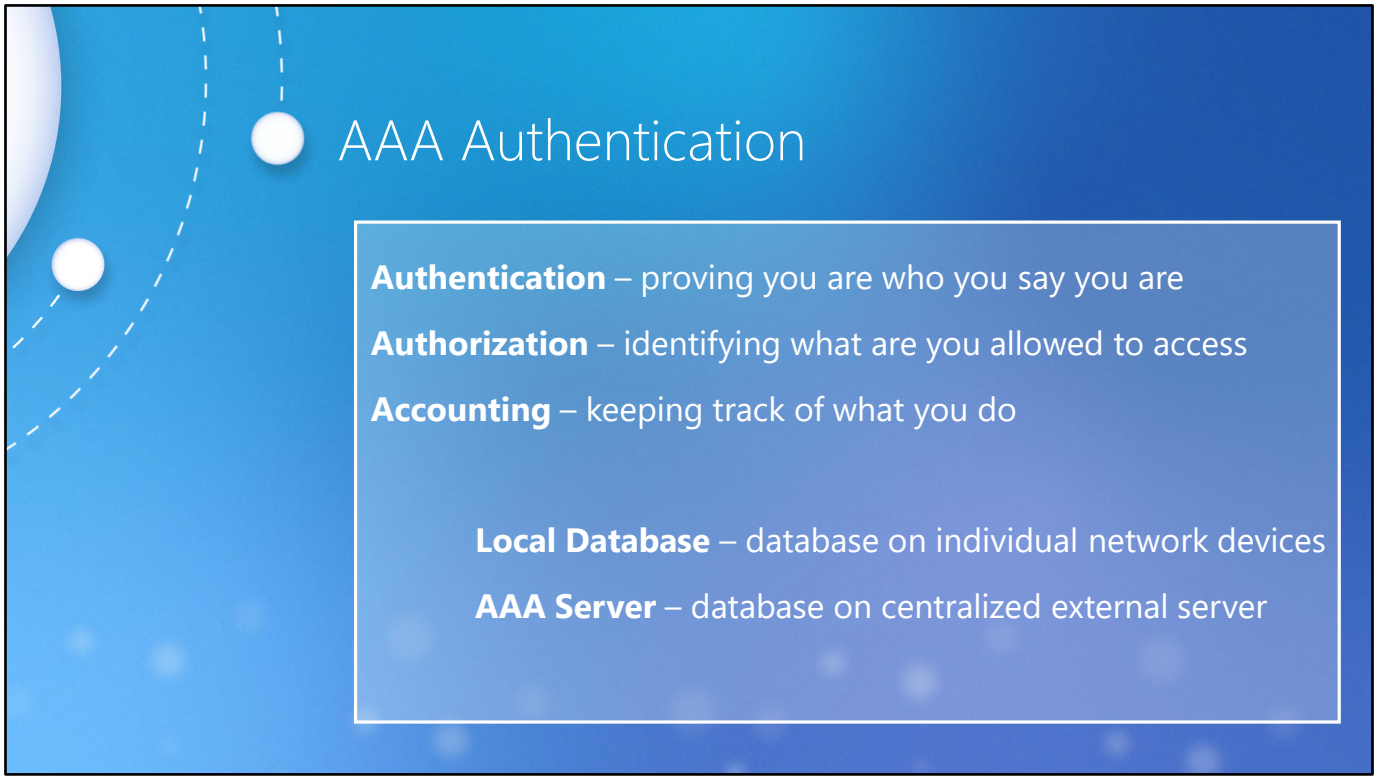
■ Is the correct version of SSH specified? By default, both version 1 and 2 are enabled. However, with the ip ssh version {1 | 2} command, you can change the version to just 1 or 2. If clients are connecting with version 2 and the device is configured for version 1, the SSH connection will fail; the same is true if clients are using version 1 and the devices are configured for version 2. To check the version of SSH that is running, use the show ip ssh command, as shown in Example 23-5. If it states version 1.99, it means versions 1 and 2 are running. If it states version 1, then SSHv1 is running, and if it states version 2, then SSHv2 is running.

■ Has the correct login command been specified? SSH uses a username and password for authentication. Therefore, the login command does not work in this case because it only requests a password. You need to use the login local command to authenticate with the local database or the login authentication {default | list_name} command to authenticate with an AAA server. Example 23-6 shows the login local command specified.

■ Has the correct key size been specified? SSHv2 uses an RSA key size of 768 or greater. If you were using a smaller key size with SSHv1 and then switched to SSHv2, you would need to create a new key with the correct size; otherwise, SSHv2 would not work. If you are using SSHv2 but accidentally specify a key size less than 768, SSHv2 connections are not allowed.

■ Is there an ACL in the path between the client and the device blocking port 22? SSH uses TCP (Transmission Control Protocol) port 22. If an ACL blocking port 22 is configured on a router or firewall, you will be unable to make a successful SSH connection.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

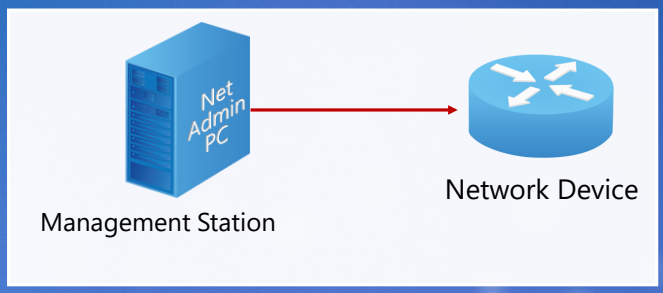


Note: AAA can use the local database instead of a AAA server. Just much harder to manage.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

AAA Configuration – Local Database

```
R1#configure terminal
R1(config)#username raymond privilege 15 secret awesome
R1(config)#aaa new-model
R1(config)#aaa authentication login AAA_AUTH local
R1(config)#aaa authorization exec AAA_AUTH local
R1(config)#line vty 0 4
R1(config-line)#login authentication AAA_AUTH
R1(config-line)#
```



User establishes connection with the router

Router prompts user for a username and password

Username and password are compared to the local database

If there is a match… authentication is successful, if there is not a match the user is denied.

Note: if you applied this to the console line the authorization would not be applied. This is done to make sure that if authorization has been misconfigured you don't prevent yourself from being able to fix the issue. Therefore, for the console port (your last resort for fixing a misconfiguration) you would login with the username and

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

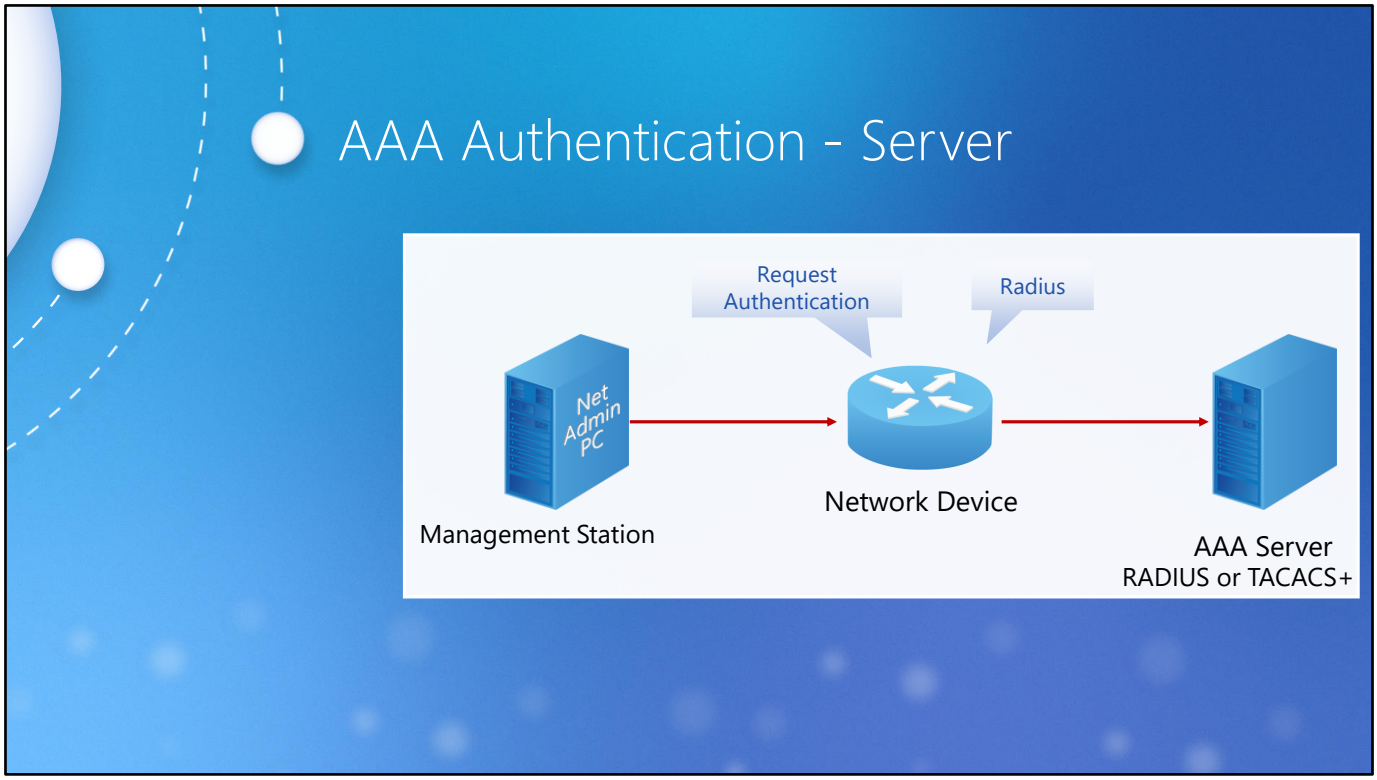
password and then use the enable command and put in the enable password to get to global configuration mode. However, if you wanted to use AAA authorization you would have to add the **aaa authorization console** command.

****EXAM***
QUESTION: what happens if you turn on aaa (aaa new-model) but don't create a method list. The vty line automatically uses the default method list which requires a local username and password by default. So if you do not have a username and password set on the device you are locked out of the vty lines until you configure one.

What happens with the console port? Nothing. It remains as is until you apply a method list to it. So if you are using no password or the line password you will continue to do so.

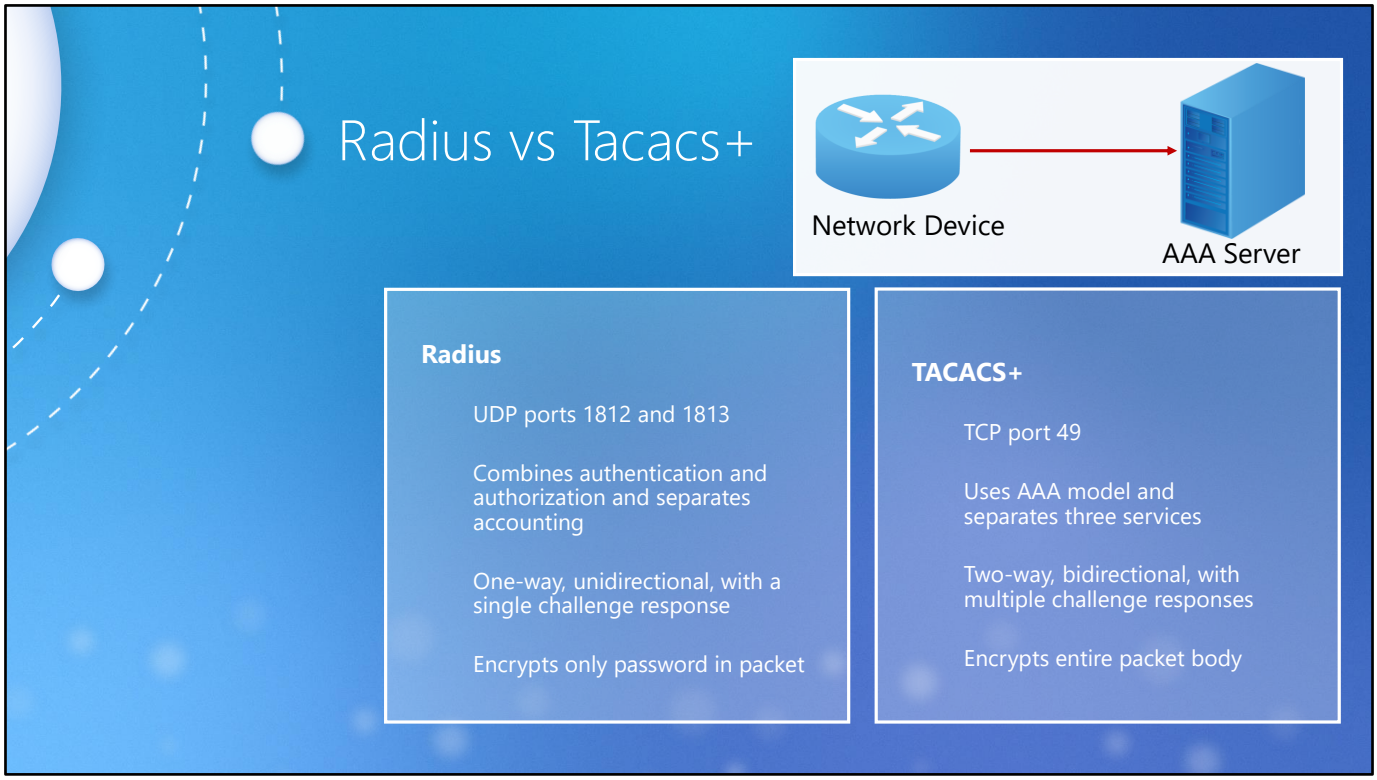
Warning: The **aaa new-model** command immediately applies local authentication to all lines and interfaces (except console line **line con 0**). If a telnet session is opened to the router after enabling this command (or if a connection times out and has to reconnect), then the user has to be authenticated using the the local database of the router. To avoid being locked out of the router, we recommend that you define a username and password on the access server before starting the AAA configuration. Do this a follows:
Router(config)# username xxx password yyy **Tip:** Save your configuration prior to configuring your AAA commands. Only after you have completed all your AAA configuration (and are satisfied that it works correctly) should you save the configuration again. This allows you to recover from unforeseen lockouts (prior to saving the configuration) by reloading the router.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



User establishes connection with the router
Router prompts the user for a username and password
The router passes the username and password to the AAA server (Cisco ISE which also supports profiling, posture assessment, and centralized web authentication as an example)
The server comapres the username and password to the centralized database
If there is a match the server tells the router to allow the user… if there is no match the server tells the router to deny the user.

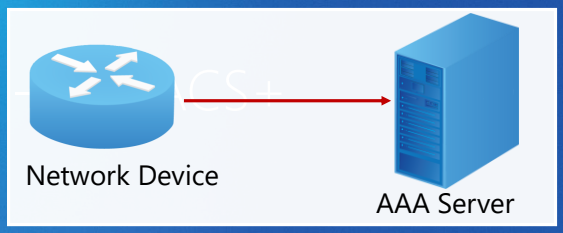
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Rad Ports = auth/authorization and acct cisco defaults are UDP/1645 for autentication and authorization, and UDP/1646 for acct

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

AAA Configuration Tacacs+




```
R1#configure terminal
R1(config)#username raymond privilege 15 secret awesome
R1(config)#aaa new-model
R1(config)#tacacs server TACSRV1
R1(config-server-tacacs)#address ipv4 10.0.3.8
R1(config-server-tacacs)#port 49
R1(config-server-tacacs)#key PASSWORD
R1(config-server-tacacs)#exit
R1(config)#aaa group server tacacs+ TACGROUP
R1(config-sg-tacacs+)#server name TACSRV1
R1(config-sg-tacacs+)#exit
R1(config)#aaa authentication login AAA_AUTH group TACGROUP local
R1(config)#aaa authorization exec AAA_AUTH group TACGROUP local
R1(config)#aaa accounting exec AAA_AUTH start-stop group TACGROUP
R1(config)#aaa accounting commands 15 AAA_AUTH stop-only group TACGROUP
R1(config)#line vty 0 4
R1(config-line)#login authentication AAA_AUTH
```

If you want to enable per-command authorization you can use:

aaa authorization commands 15 AAA_AUTH group TACGROUP local

This requires the device to consult the TACACS+ server anytime the admin enters a priv level 15 EXEC command

aaa authorization config-commands

This requires the device to consult the TACACS+ server anytime the admin enters any config commands.

***If the admin is authorized the command executes normally…. If not, the commands has no effect and an error message will be displayed.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

If you need to keep accounting records you will need to set up a method list for accounting.

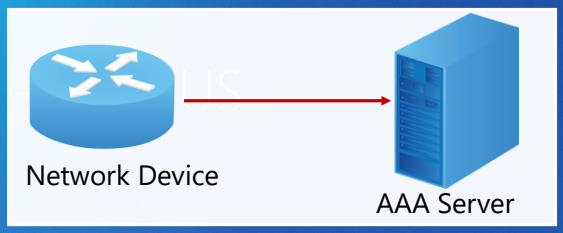
Accounting method lists are specific to the type of accounting being requested. AAA supports six different types of accounting:
Network--Provides information for all PPP, SLIP, or ARAP sessions, including packet and byte counts.
EXEC--Provides information about user EXEC terminal sessions of the network access server.
Command--Provides information about the EXEC mode commands that a user issues. Command accounting generates accounting records for all EXEC mode commands, including global configuration commands, associated with a specific privilege level.
(**The Cisco Systems implementation of RADIUS does not support command accounting.)**
Connection--Provides information about all outbound connections made from the network access server, such as Telnet, local-area transport (LAT), TN3270, packet assembler/disassembler (PAD), and rlogin.
System--Provides information about system-level events.
Resource--Provides “start” and “stop” records for calls that have passed user authentication, and provides “stop” records for calls that fail to authenticate.

****

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

AAA Configuration – Radius




```
R1#configure terminal
R1(config)#username raymond privilege 15 secret awesome
R1(config)#aaa new-model
R1(config)#radius server RADSRV1
R1(config-radius-server)#address ipv4 10.0.3.8 auth-port 1812 acct-port 1813
R1(config-radius-server)#key PASSWORD
R1(config-radius-server)#exit
R1(config)#aaa group server radius RADGROUP
R1(config-sg-radius)#server name RADSRV1
R1(config-sg-radius)#exit
R1(config)#aaa authentication login AAA_AUTH_RAD group RADGROUP local
R1(config)#aaa authorization exec AAA_AUTH_RAD group RADGROUP local
R1(config)#aaa accounting exec AAA_AUTH_RAD start-stop group RADGROUP
R1(config)#line vty 0 4
R1(config-line)#login authentication AAA_AUTH_RAD
```

These commands will be used for 802.1X as well

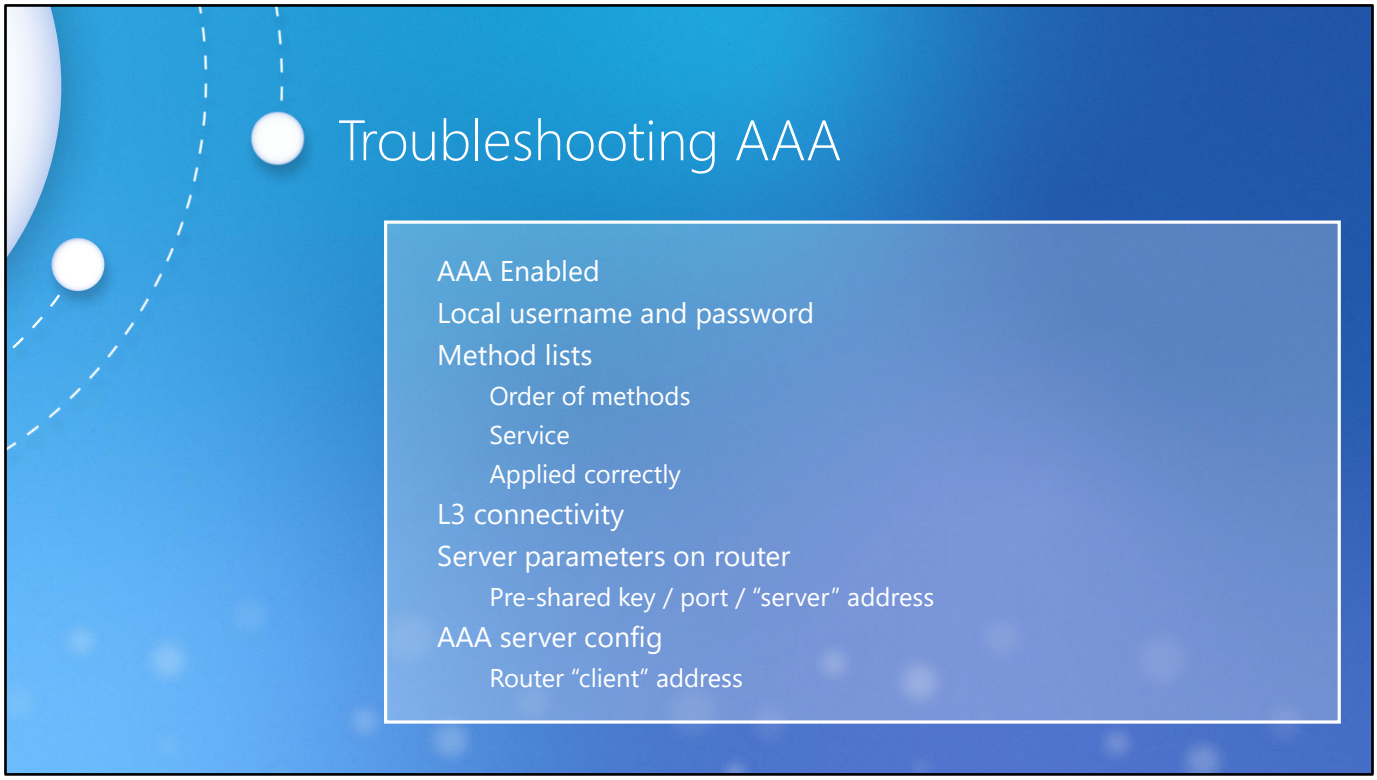
radius server RADSRV1
  address ipv4 10.0.3.6 auth-port 1812 acct-port 1813
  key PASSWORD

aaa group server radius RADGROUP
  server name RADSRV1

****

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



consider the following when troubleshooting Cisco IOS AAA authentication:

■ AAA needs to be enabled: AAA is disabled by default on Cisco routers and switches. To enable AAA, use the aaa new-model command. Local authentication is immediately applied to all lines except the console line. Therefore, you will not be able to access the device remotely if the local database does not store the username and password. Console access is still capable with no username or password.

■ AAA relies on the local username and password database or an AAA server such as RADIUS or TACACS+: By default, AAA uses the local username and password database for authentication. If no username and password exist that can be used for remote access, authentication fails. Therefore, if you are using local authentication, a username and password need to exist on the local device. However, if you are using an AAA server, you should still configure at least one username and password in the local database that can be used for fallback purposes in case the AAA server is not available. In Example 22-1, the username admin with the password letmein can be used for AAA authentication.

■ A method list defines the authentication methods: When no method list exists, the vty lines use the local username and password database by default. However, with the method list, you can define what methods of authentication will be used and in what order. In Example 22-1, a user-defined method list for login authentication

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

called VTY_ACCESS will use the servers in the RADIUS group RADIUSMETHOD, and if the servers are not accessible, local authentication will be used as the fallback method. Please note that if there is no username or password in the database, authentication fails because the servers are not available.

■ Method list service is incorrect: When you create a method list, you specify the service that method list is for. For example, the AAA authentication login method list is for authenticating the console and vty lines. The AAA authentication PPP method list is for authenticating PPP sessions. The AAA authentication dot1x method list is for authenticating users connecting to a dot1x-enabled interface. Therefore, if you create a method list for login and then apply it to your PPP interfaces, it will not work. If you create a method list for dot1x and then apply it to the vty lines, it will not work. The method list service must match the service for which you are creating the list.

■ AAA method lists are applied to the lines: The method list that will be used to define how authentication will occur for the vty lines or console line needs to be applied with the login authentication {default | list_name} command. In Example 22-1, the VTY_ACCESS method list is attached to the vty lines, and the CONSOLE_ACCESS method list is attached to the console line.

■ The router needs to be able to reach the AAA server: Use the test aaa command on the router or use Telnet to reach the authentication port number of the AAA server to verify connectivity.

■ The router needs to be configured with the correct pre-shared key: Ensure that the router and the AAA server are configured with the same pre-shared key. In this case, the pre-shared key for the RADIUS server is RADIUSPASSWORD, and the pre-shared key for the TACACS+ server is TACACSPASSWORD.

■ The correct authenticating and accounting ports need to be configured: RADIUS uses ports 1812 or 1645 (Cisco default) for authentication and 1813 or 1646 (Cisco default) for accounting. So, if your RADIUS server is using ports 1812 and 1813, you have to configure the port numbers on your Cisco devices as they use 1645 and 1646 by default. TACACS+ uses port 49.

■ Usernames and passwords need to be configured on the AAA server: Double-check to make sure the correct usernames and passwords are configured on the AAA server.

■ The AAA server group needs to have the correct AAA server IP addresses: Ensure that the IP addresses of the servers in the AAA server group are correct.

■ User can authenticate but can’t execute any commands: Make sure the user has been authorized on the server to execute the commands he or she needs to execute.

■ IP address of client configured on AAA server: When configuring an AAA server, you must specify the client IP address, which would be the router in this case. Remember that when a router sources packets, it uses the exit interface as the source of a packet. If the exit interface is not configured with the IP address that the AAA server is expecting, the client cannot use the AAA server and its services. It is recommended that the IP address of a loopback interface be used for the source of packets and as the client IP address that is configured on the AAA server. Therefore, you must

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

configure the router with the ip radius source-interface interface_type interface_number command or the ip tacacs source-interface interface_type interface_number command so that it sources RADIUS and TACACS packets with the correct IP address every time.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

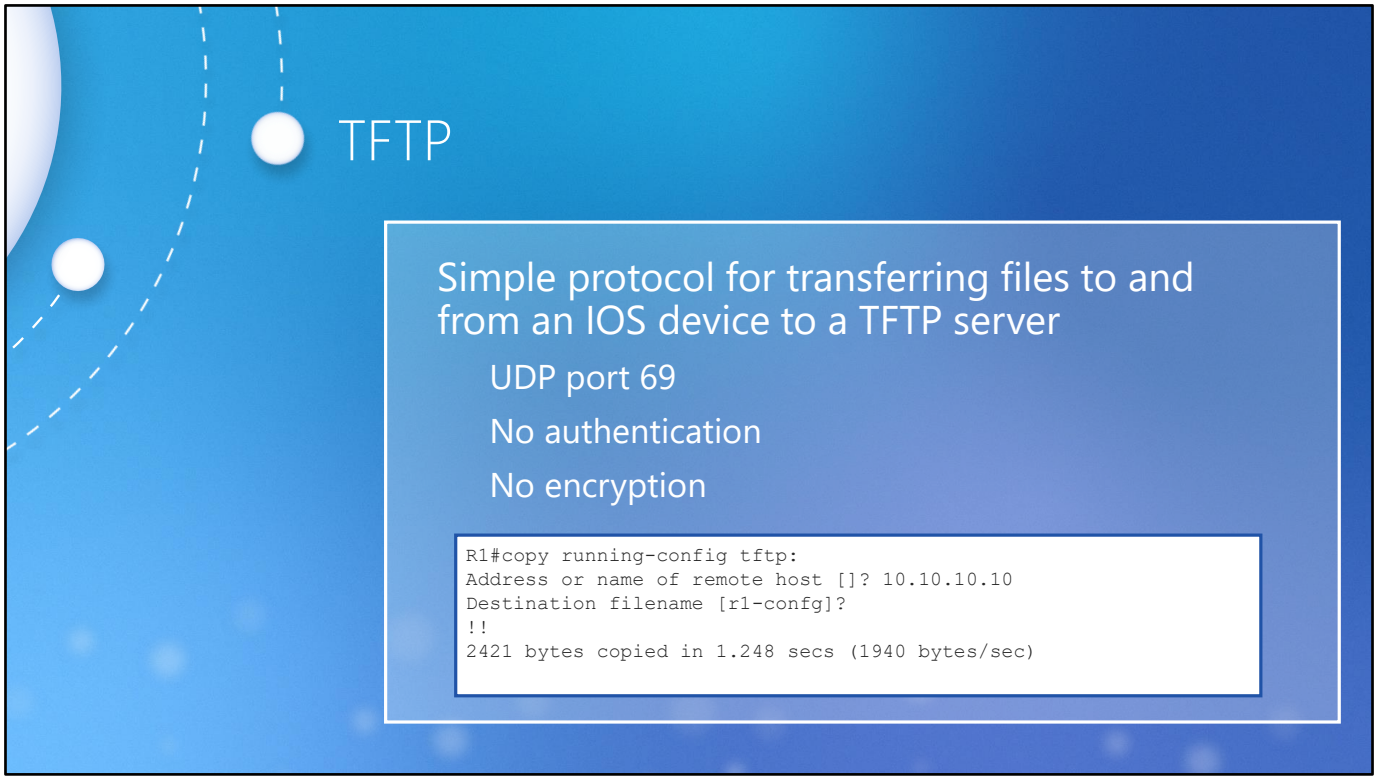


©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Title slide

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



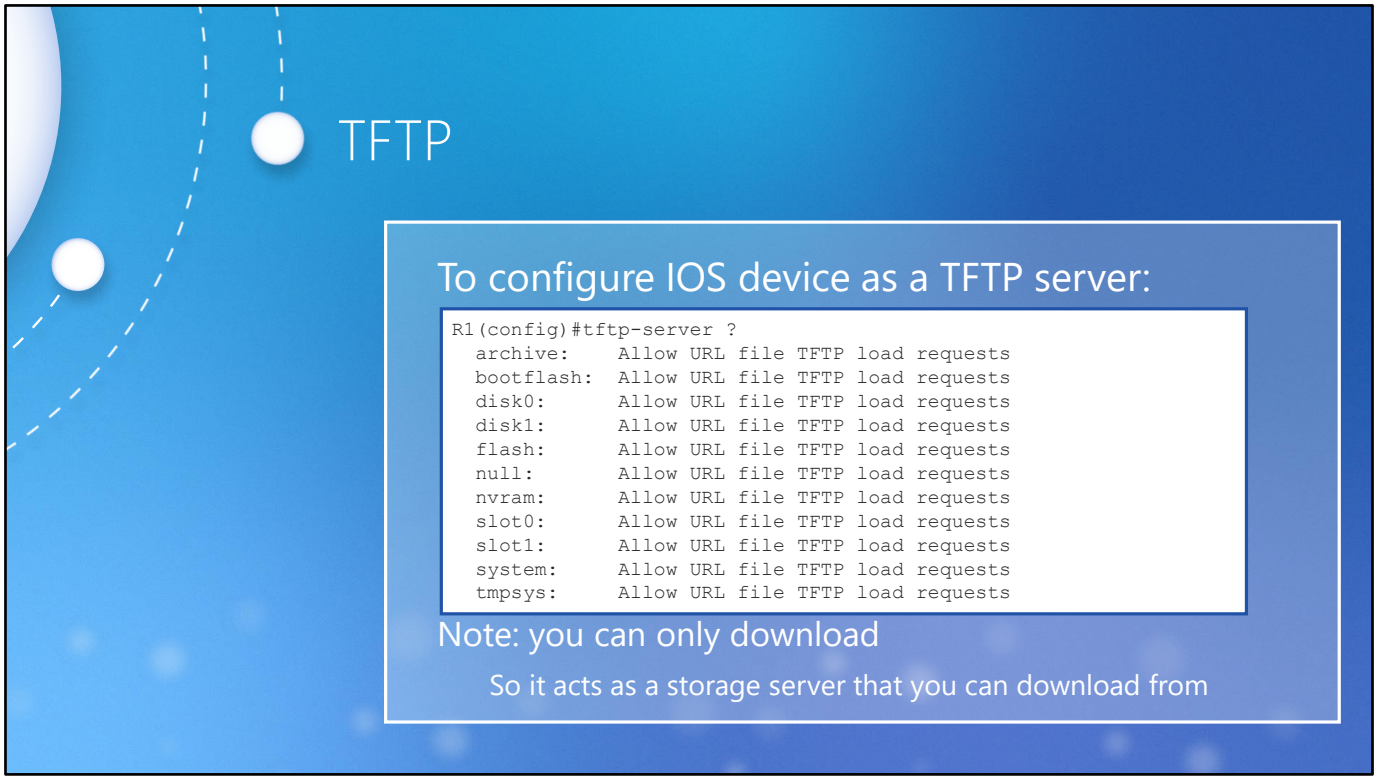
https://help.ubuntu.com/community/TFTP

■ When copying to a TFTP server, make sure the TFTP server has enough storage space.
■ When copying from a TFTP server, make sure the storage location on the Cisco device has enough storage space. Use the show flash command to verify the amount of free
23
space available and compare it to the size of the file you want to copy. If you copy a file larger than the available space, it will be partially copied, and then you get the failure message “buffer overflow - xxxx /xxxx”. The first four x’s identify the number of bytes read from the source file, and the second four x’s identify the number of bytes available on the destination.
■ Ensure that the TFTP server is reachable from the Cisco device.
■ Check along the path from source to destination for access lists that might be blocking TFTP traffic.
■ If you are using a management interface for TFTP traffic, use the ip tftp sourceinterface interface_type interface_number command to specify that the management interface will be used for sourcing TFTP traffic.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

■ Ensure that you are using the copy command correctly:
copy source destination copy tftp://10.0.3.8/cisco_ios_files/c3900-universalk9-mz.SPA.156-3. M6a.bin flash:c3900-universalk9-mz.SPA.156-3.M6a.bin copy flash:c3900-universalk9-mz.SPA.156-3.M6a.bin http://10.0.3.8/cisco_ios_files/c3900-universalk9-mz.SPA.156-3.M6a.bin
■ When copying to flash, make sure the filename is not longer than 63 characters. There is a 63-character limit on filenames in flash memory.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



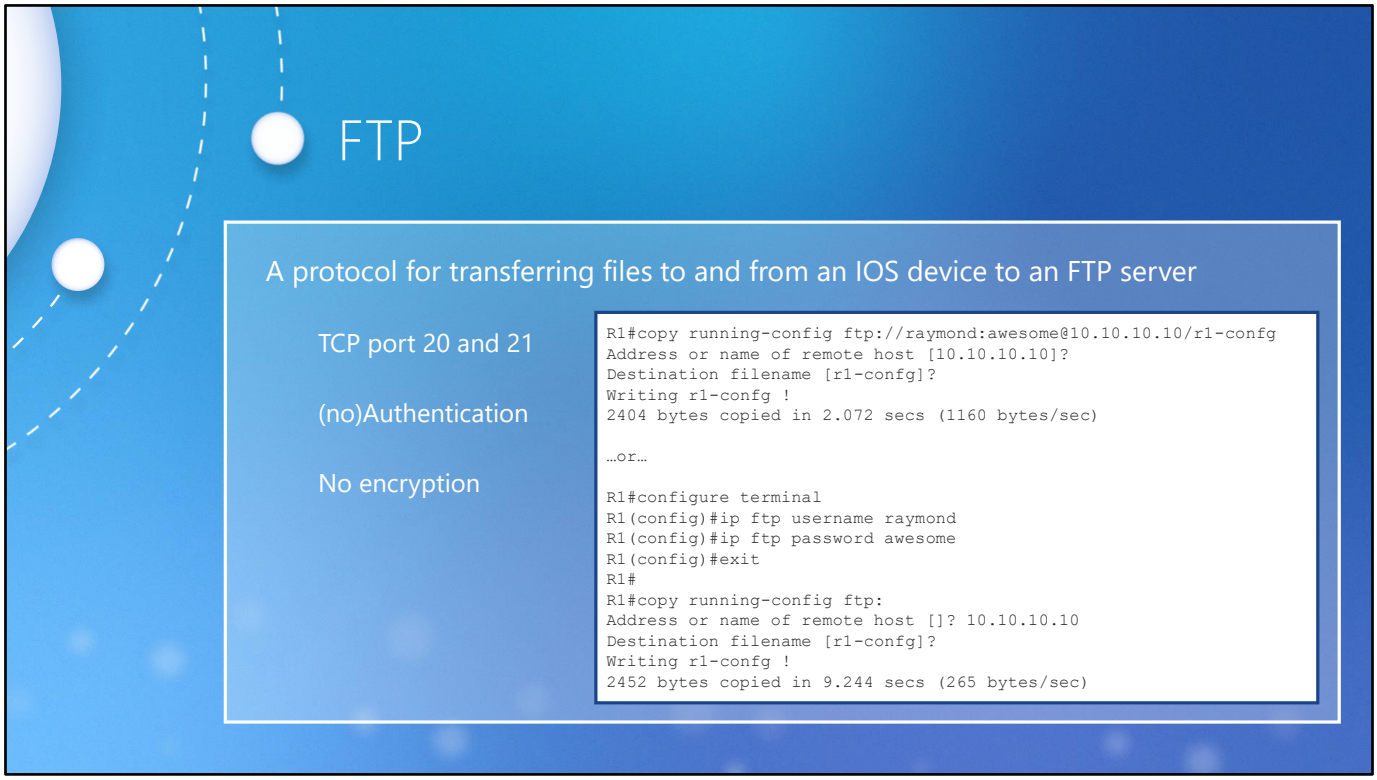
https://help.ubuntu.com/community/TFTP

■ When copying to a TFTP server, make sure the TFTP server has enough storage space.
■ When copying from a TFTP server, make sure the storage location on the Cisco device has enough storage space. Use the show flash command to verify the amount of free
23
space available and compare it to the size of the file you want to copy. If you copy a file larger than the available space, it will be partially copied, and then you get the failure message “buffer overflow - xxxx /xxxx”. The first four x’s identify the number of bytes read from the source file, and the second four x’s identify the number of bytes available on the destination.
■ Ensure that the TFTP server is reachable from the Cisco device.
■ Check along the path from source to destination for access lists that might be blocking TFTP traffic.
■ If you are using a management interface for TFTP traffic, use the ip tftp sourceinterface interface_type interface_number command to specify that the management interface will be used for sourcing TFTP traffic.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

■ Ensure that you are using the copy command correctly:
copy source destination copy tftp://10.0.3.8/cisco_ios_files/c3900-universalk9-mz.SPA.156-3. M6a.bin flash:c3900-universalk9-mz.SPA.156-3.M6a.bin copy flash:c3900-universalk9-mz.SPA.156-3.M6a.bin http://10.0.3.8/cisco_ios_files/c3900-universalk9-mz.SPA.156-3.M6a.bin
■ When copying to flash, make sure the filename is not longer than 63 characters. There is a 63-character limit on filenames in flash memory.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

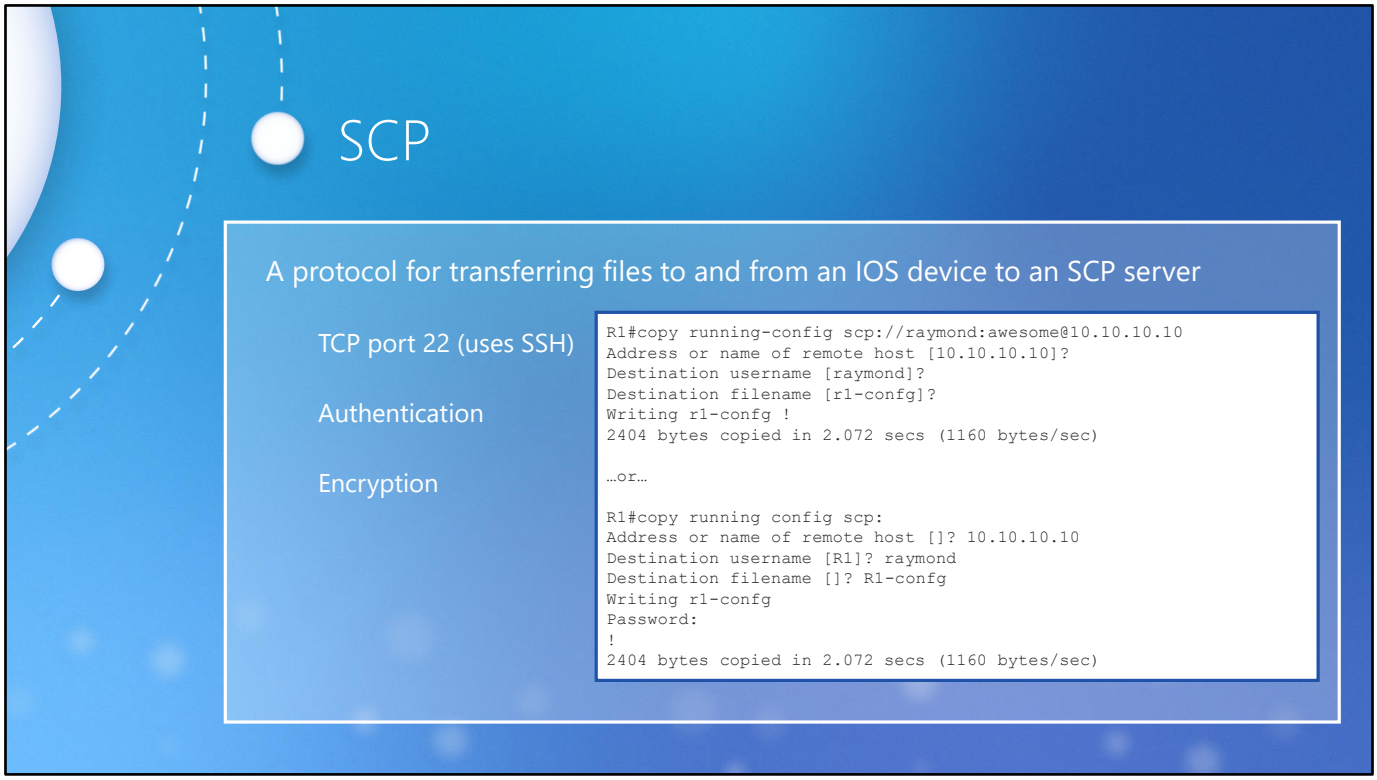


20 is for control
21 is for data

Could have anonymous authentication

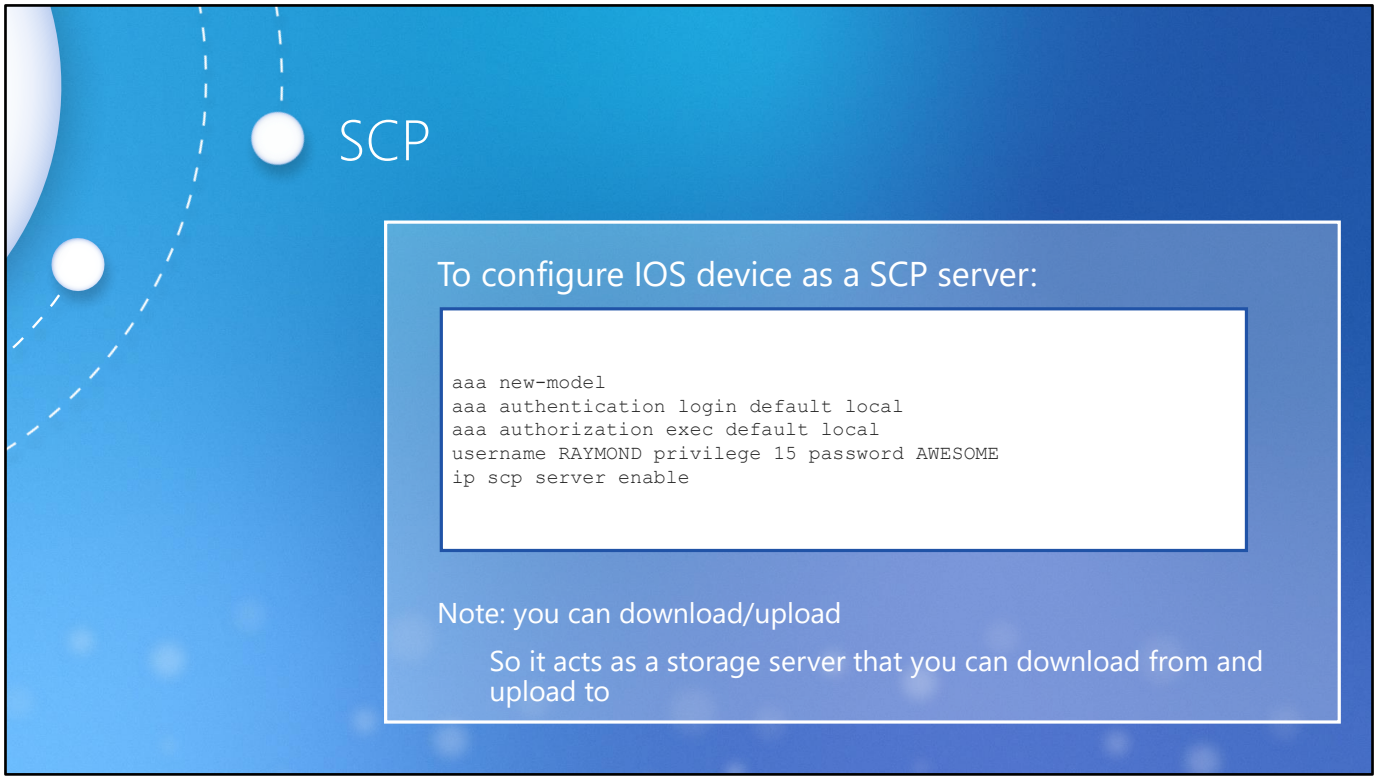
(NOTE: you used to be able to configure a router as an FTP server but that has been deprecated due to explioits)

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Your scp server needs to be set up properly of course.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_ssh/configuration/xe-16/sec-usr-ssh-xe-16-book/sec-usr-ssh-sec-copy.html

To be an SCP server you have to use AAA (local or external server)

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

HTTP/HTTPs

A protocol for transferring files to and from an IOS device to an HTTP/HTTPs server

TCP port 80/443

(no)Authentication

(no)Encryption

```
R1#copy running-config http://raymond:awesome@10.10.10.10/r1-confg
Address or name of remote host [10.10.10.10]?
Destination filename [r1-confg]?
Writing r1-confg !
2404 bytes copied in 2.072 secs (1160 bytes/sec)

…or…

R1#configure terminal
R1(config)#ip http client username raymond
R1(config)#ip http client password awesome
R1(config)#exit
R1#
R1#copy running-config http:
Address or name of remote host []? 10.10.10.10
Destination filename [r1-confg]?
Writing r1-confg !
2452 bytes copied in 9.244 secs (265 bytes/sec)
```

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/https/configuration/xe-16/https-xe-16-book/HTTP_1-1_Web_Server_and_Client.html

With http you could have anonymous authentication or authentication
With HTTPS you want authentication
With http it is no encryption
With https it requires encryption

■ Make sure your Cisco device supports the HTTP client. You can do this with the show ip http client all command. If the command works, the client is supported.
■ Check that your router can connect to the web server: Use the ping command on the Cisco device and ping the URL of the web server or its IP address.
■ Ensure that the correct URL or IP address of the web server has been specified in the copy command. The copy command requires you to specify a source and destination, in that order. As an example, when copying from a web server to flash, the source would be the web server, as shown here with the IP address 10.0.3.8:
copy http://10.0.3.8/cisco_ios_files/c3900-universalk9-mz.SPA.156-3. M6a.bin flash:c3900-universalk9-mz.SPA.156-3.M6a.bin

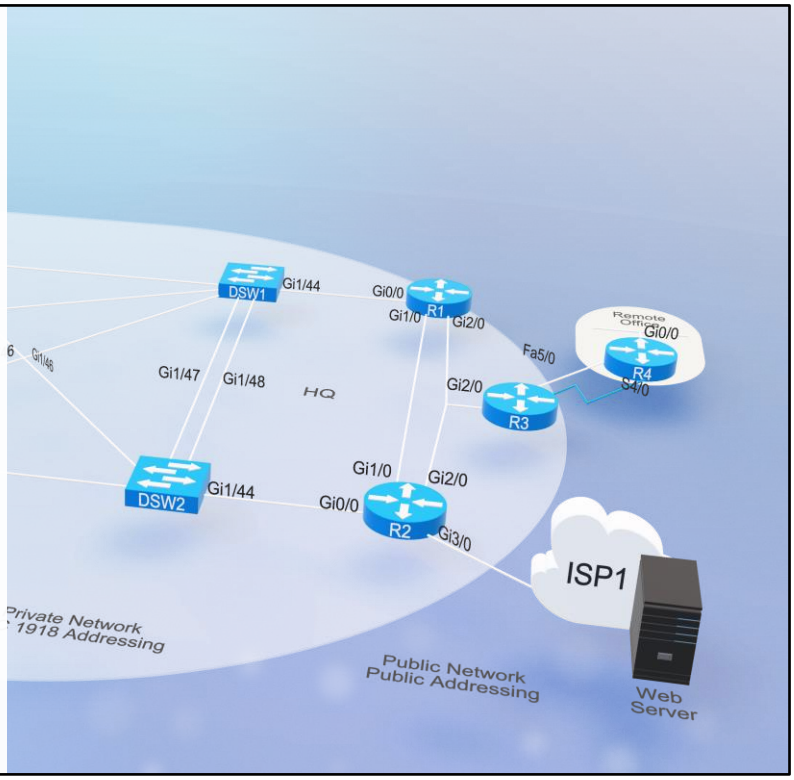
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

■ When copying to a web server from flash, the destination would be the web server, as seen here with the IP address 10.0.3.8:
copy flash:c3900-universalk9-mz.SPA.156-3.M6a.bin http://10.0.3.8/ cisco_ios_files/c3900-universalk9-mz.SPA.156-3.M6a.bin
■ Ensure that the correct filename is specified in the copy command.
■ Make sure the correct username and password are specified in the copy command. In this case, the username is user1, and the password is mypassword:
copy http://user1:mypasswrod@10.0.3.8/cisco_ios_files/c3900- universalk9-mz.SPA.156-3.M6a.bin flash:c3900-universalk9-mz. SPA.156-3.M6a.bin
You can also specify the authentication credentials with the ip http client username command and the ip http client password password command. Note that the username and password used with the copy command override the ones in these other commands.
■ Check that the correct port is specified in the copy command. By default, HTTP uses port 80, and HTTPS uses port 443, but you can configure your web server to use whatever you want. In this example, the port number being specified is 8080:
copy http://user1:mypasswrod@10.0.3.8:8080/cisco_ios_files/ c3900-universalk9-mz.SPA.156-3.M6a.bin flash: c3900-universalk9mz.SPA.156-3.M6a.bin
■ Check that packets to the web server from the Cisco device are being sourced from the correct IP address. If not, it is possible that an ACL along the path might be dropping the packets. You can configure the source IP address by using the ip http client source-interface interface-id command.
■ Make sure you specified the correct protocol: HTTP or HTTPS. If you are connecting to an HTTP server, your URL should begin with http. If you are connecting to an HTTPS server, your URL should begin with HTTPS.
■ For additional help with troubleshooting HTTP and HTTPS copy issues, use the debug ip http client all command.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Ping

A tool that can be used to test connectivity between two devices



Really great at identifying MTU as well by sweeping a range of packet sizes and setting the DF bit.

Talk about standard and extended.

```
R1#ping 192.168.4.4 ?
  data     specify data pattern
  df-bit   enable do not fragment bit in IP header
  repeat   specify repeat count
  size     specify datagram size
  source   specify source address or name
  timeout  specify timeout interval
  tos      specify type of service value
  validate validate reply data
  <cr>
```

https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13730-ext-ping-trace.html
https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-software-

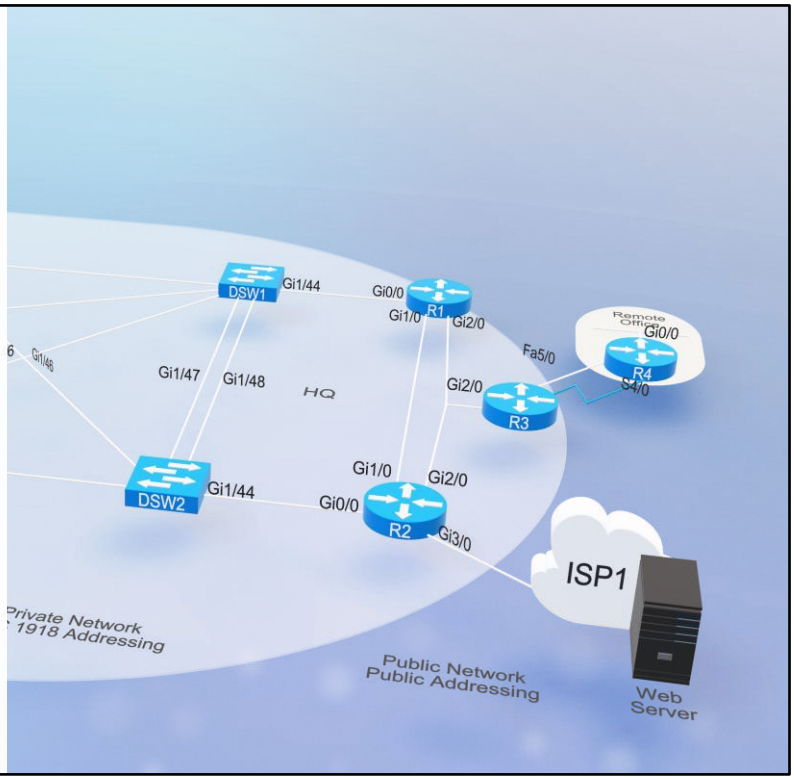
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

releases-121-mainline/12778-ping-traceroute.html#ping_com

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Traceroute

A tool that can be used to verify the path that traffic takes through the network.



Really great at identifying routing loops as we saw with our redistribution discussion, really great for verifying PBR paths, really great at identifying the path packets are taking after adjusting BGP attributes.

Talk about standard and extended

```
R1#traceroute 192.168.4.4 ?
  numeric  display numeric address
  port     specify port number
  probe    specify number of probes per hop
  source   specify source address or name
  timeout  specify time out
  ttl      specify minimum and maximum ttl
  <cr>
```

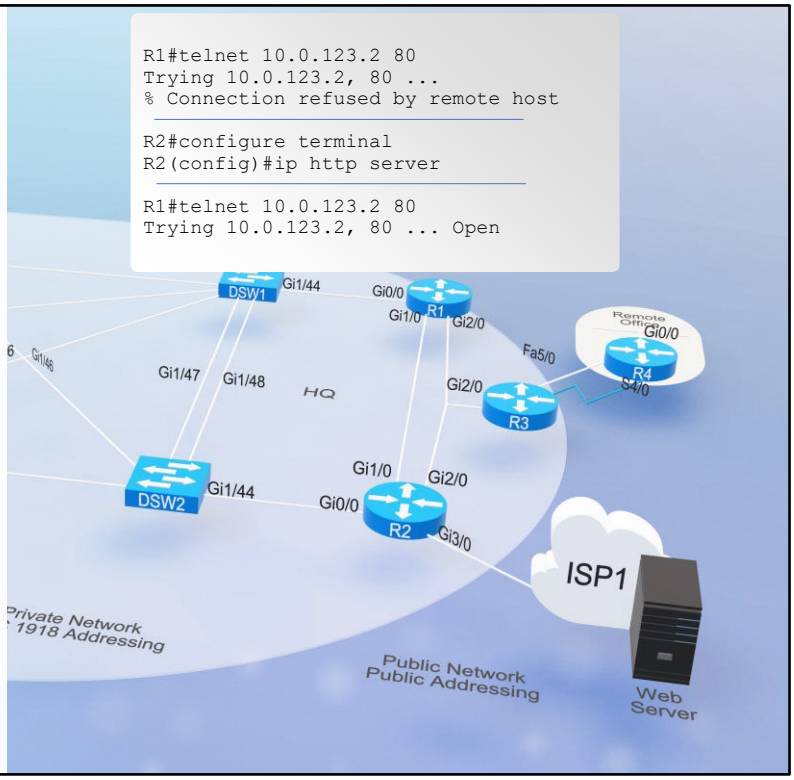
https://www.cisco.com/E-Learning/bulk/public/tac/cim/cib/using_cisco_ios_software/cmdrefs/traceroute.htm

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Telnet

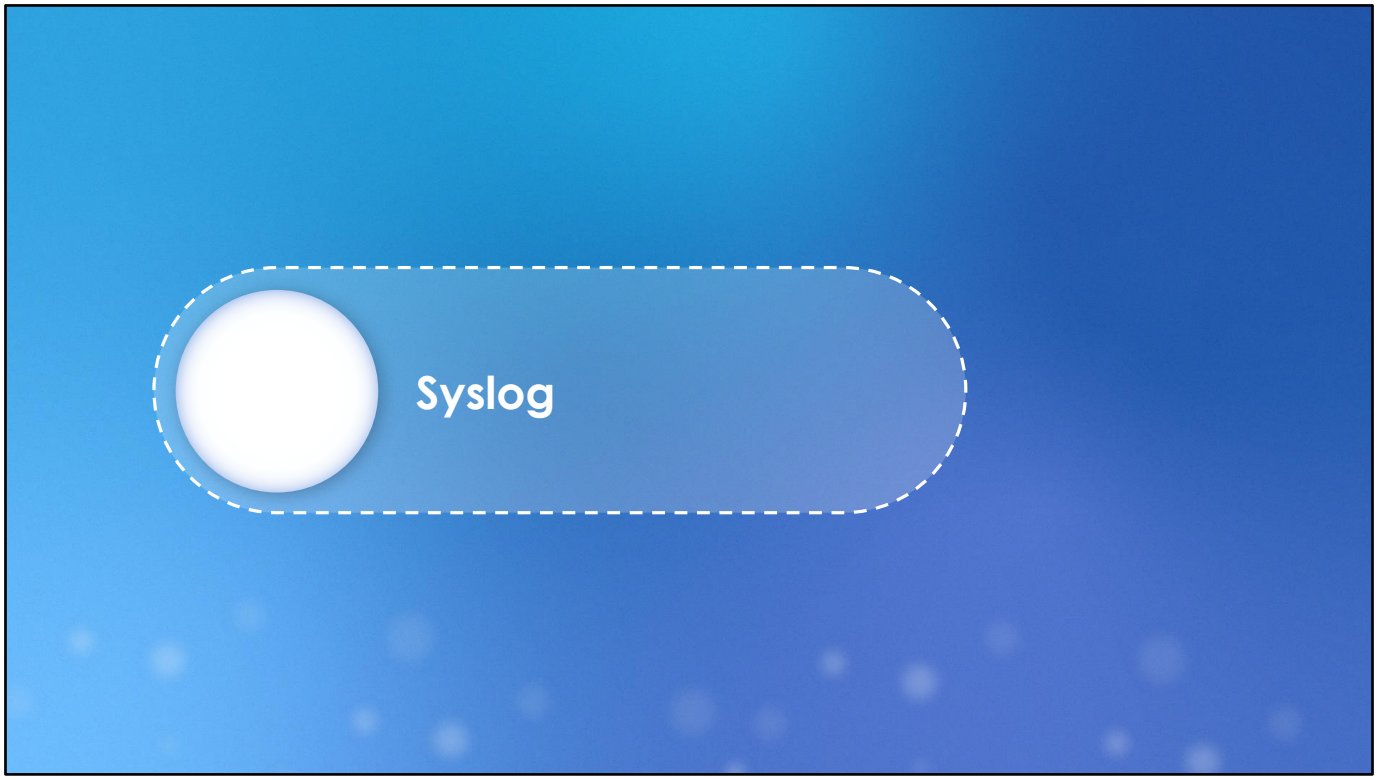
A tool that can be used to remotely connect to devices for management purposes

A tool that you can use to test connectivity to other ports



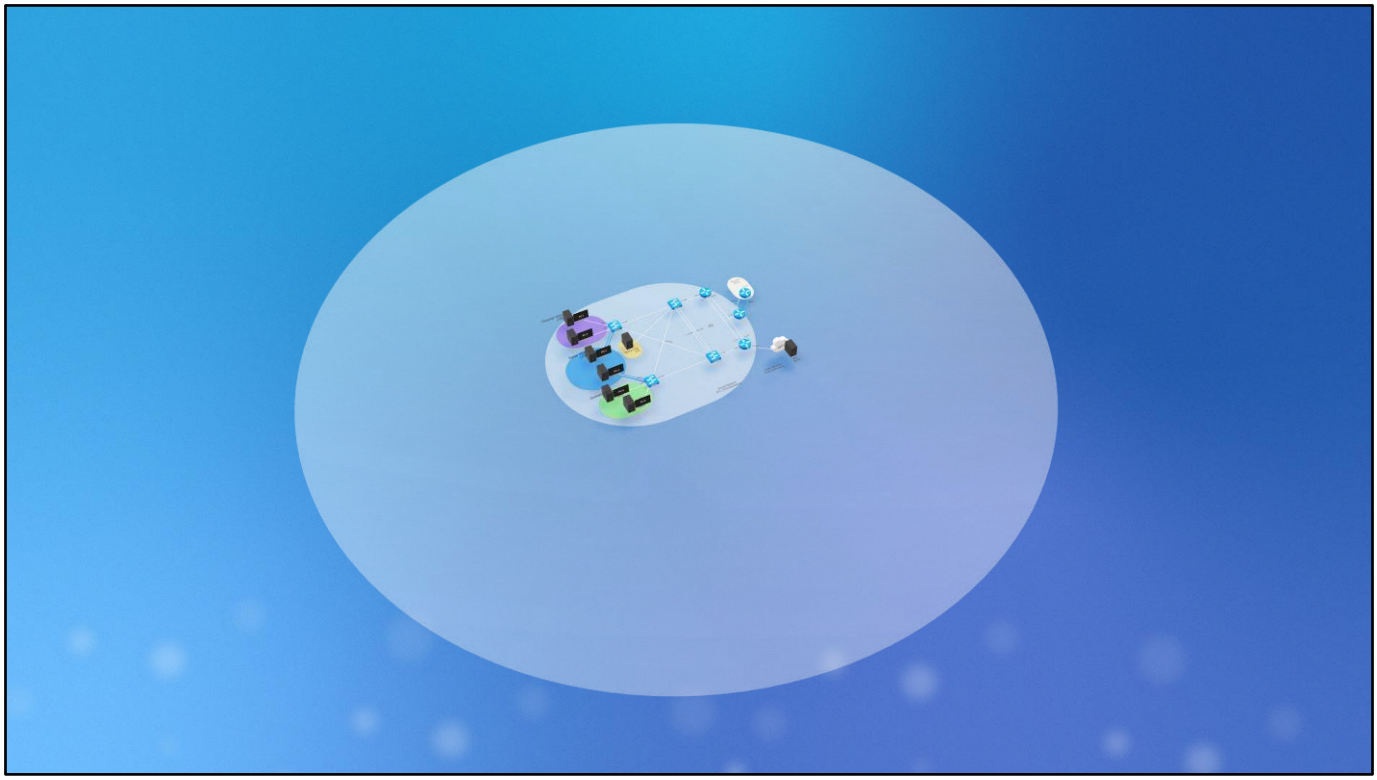
Telnet

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Title slide

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

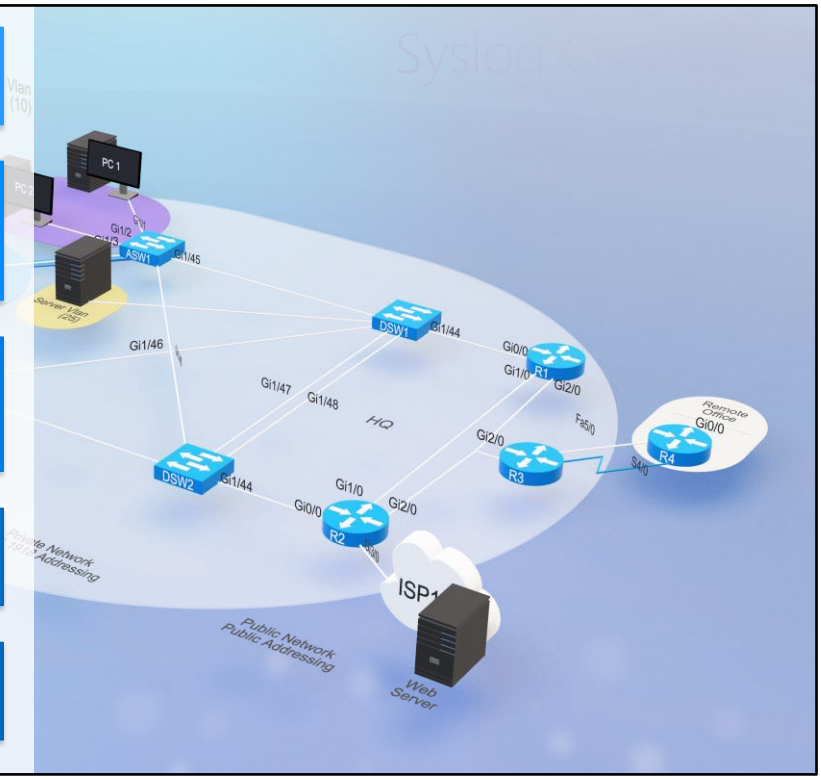
Syslog is used for monitoring and auditing.

Generally, when an event that is deemed important by a service occurs, the service generates a Syslog message to document the event.

On Cisco IOS devices, Syslog messages are sent to the console, vty lines, and ram by default.

Optimally, Syslog messages should be sent to a centralized repository such as a syslog server.

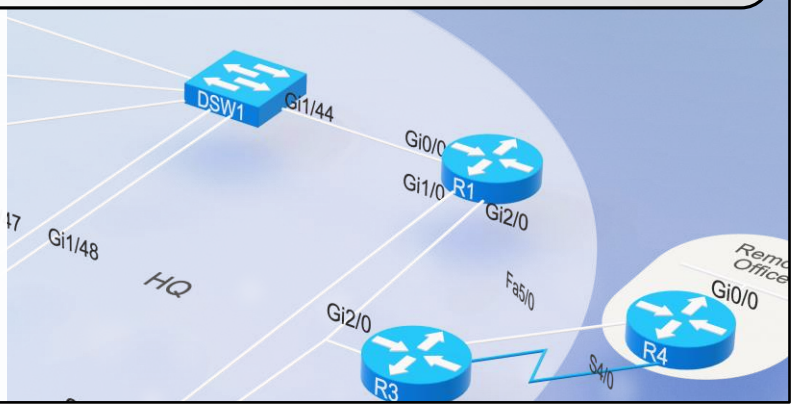
Syslog defines severity levels 0-7. The lower the number, the more severe the issue.



©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Syslog

```
R1(config)#int gigabitEthernet 1/0
R1(config-if)#shut
R1(config-if)#
*Sep 22 13:05:08.981: %DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 10.0.12.2 (GigabitEthernet1/0) is down:
interface down
R1(config-if)#
*Sep 22 13:05:10.933: %LINK-5-CHANGED: Interface GigabitEthernet1/0, changed state to administratively
down
*Sep 22 13:05:11.933: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0, changed state
to down
R1(config-if)#
```



Data and Time – if time is not showing use the (service timestamps log/debug datetime) command. (if you don't want to use date and time you can use sequence numbers instead with the (**service sequence-numbers) command. (You can use both at the same time.)**
*****EXAM*** by default logs use UTC time. To display in "local time of the device" use the localtime keyword (service timestamps log datetime localtime)**
Facility – the service/function that triggered the message (the source of the message)
Severity – 0-7
Mnemonic – device specific code to uniquely identify the message
Message/Description – a brief message about the fault.

*****important****
Having log messages and debug messages timestamped is critical for troubleshooting. If no timestamps are included with either log messages or debug messages, it is because the no service timestamps command has been executed. To configure timestamps, use the service timestamps [debug | log] [datetime | uptime] command. The datetime option includes the date and time the log or debug message occurred. Therefore, it is important to have an accurate calendar and time set. Use

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

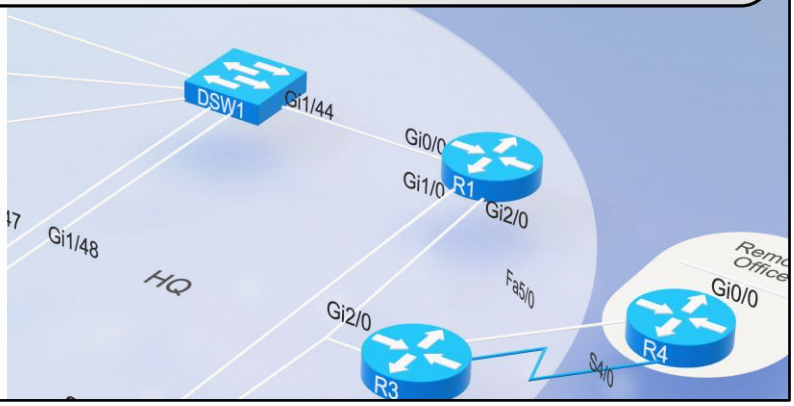
NTP (Network Time Protocol) for this. The uptime option provides a timestamp based on the amount of time that has passed since the last reboot.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Syslog

```
R1(config)#int gigabitEthernet 1/0
R1(config-if)#shut
R1(config-if)#
*Sep 22 13:05:08.981: %DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 10.0.12.2 (GigabitEthernet1/0) is down:
interface down
R1(config-if)#
*Sep 22 13:05:10.933: %LINK-5-CHANGED: Interface GigabitEthernet1/0, changed state to administratively
down
*Sep 22 13:05:11.933: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0, changed state
to down
R1(config-if)#
```

emergencies	0
alerts	1
critical	2
errors	3
warnings	4
notifications	5
informational	6
debugging	7



Data and Time – if time is not showing use the (service timestamps log/debug datetime) command. (if you don't want to use date and time you can use sequence numbers instead with the (**service sequence-numbers) command. (You can use both at the same time.)**
*****EXAM*** by default logs use UTC time. To display in "local time of the device" use the localtime keyword (service timestamps log datetime localtime)**
Facility – the service/function that triggered the message (the source of the message)
Severity – 0-7
Mnemonic – device specific code to uniquely identify the message
Message/Description – a brief message about the fault.

*****important****
Having log messages and debug messages timestamped is critical for troubleshooting. If no timestamps are included with either log messages or debug messages, it is because the no service timestamps command has been executed. To configure timestamps, use the service timestamps [debug | log] [datetime | uptime] command. The datetime option includes the date and time the log or debug message occurred. Therefore, it is important to have an accurate calendar and time set. Use

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

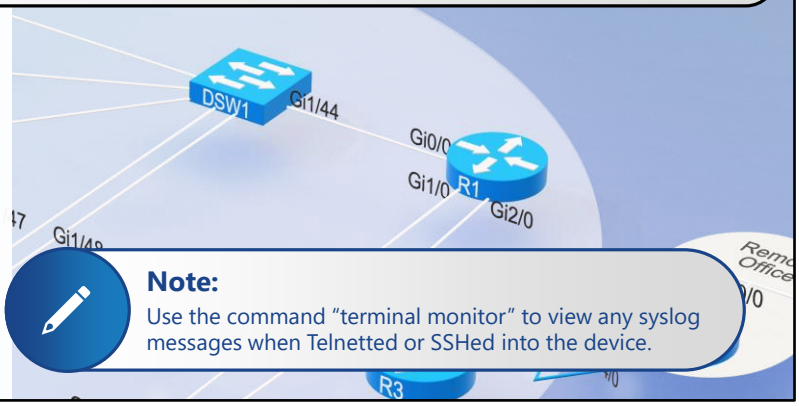
NTP (Network Time Protocol) for this. The uptime option provides a timestamp based on the amount of time that has passed since the last reboot.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

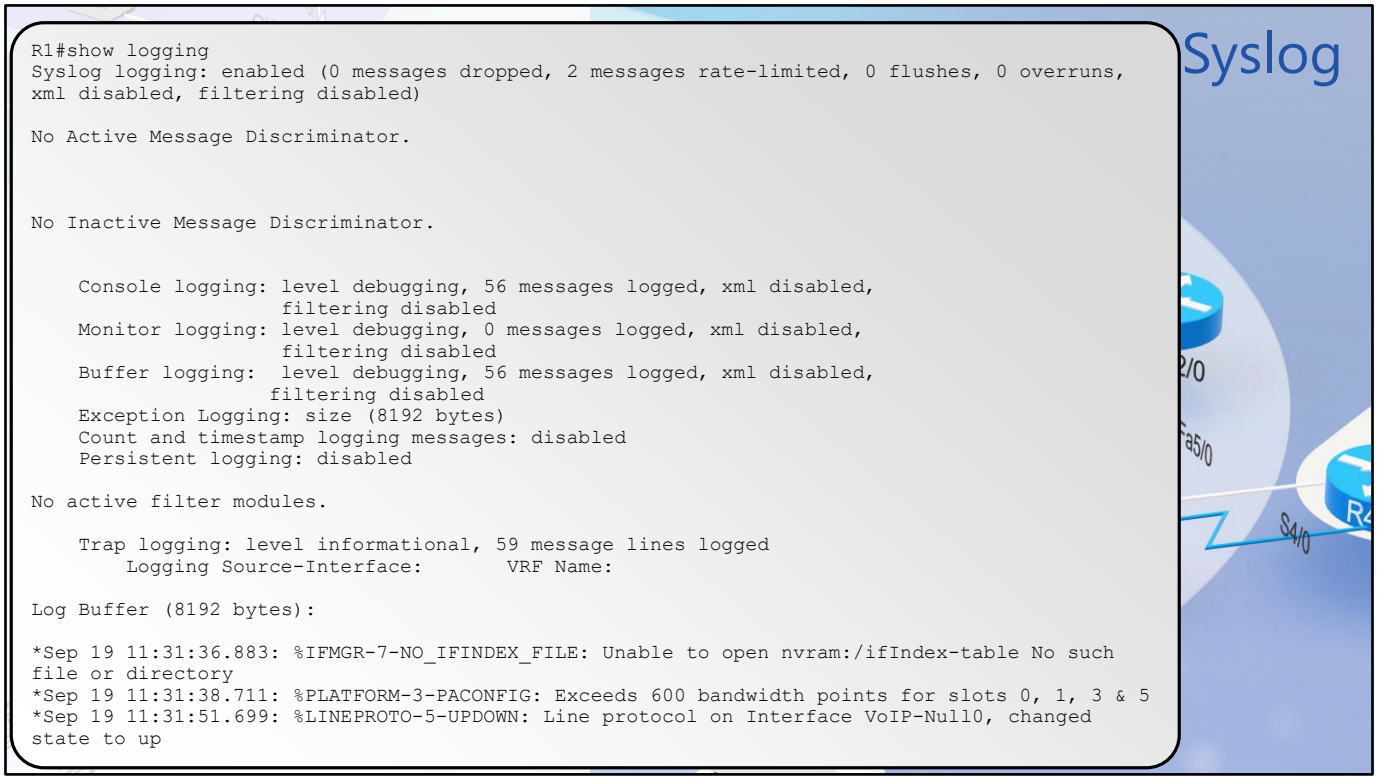
Syslog

```
R1(config)#int gigabitEthernet 1/0
R1(config-if)#shut
R1(config-if)#
*Sep 22 13:05:08.981: %DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 10.0.12.2 (GigabitEthernet1/0) is down:
interface down
R1(config-if)#
*Sep 22 13:05:10.933: %LINK-5-CHANGED: Interface GigabitEthernet1/0, changed state to administratively
down
*Sep 22 13:05:11.933: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0, changed state
to down
R1(config-if)#
```

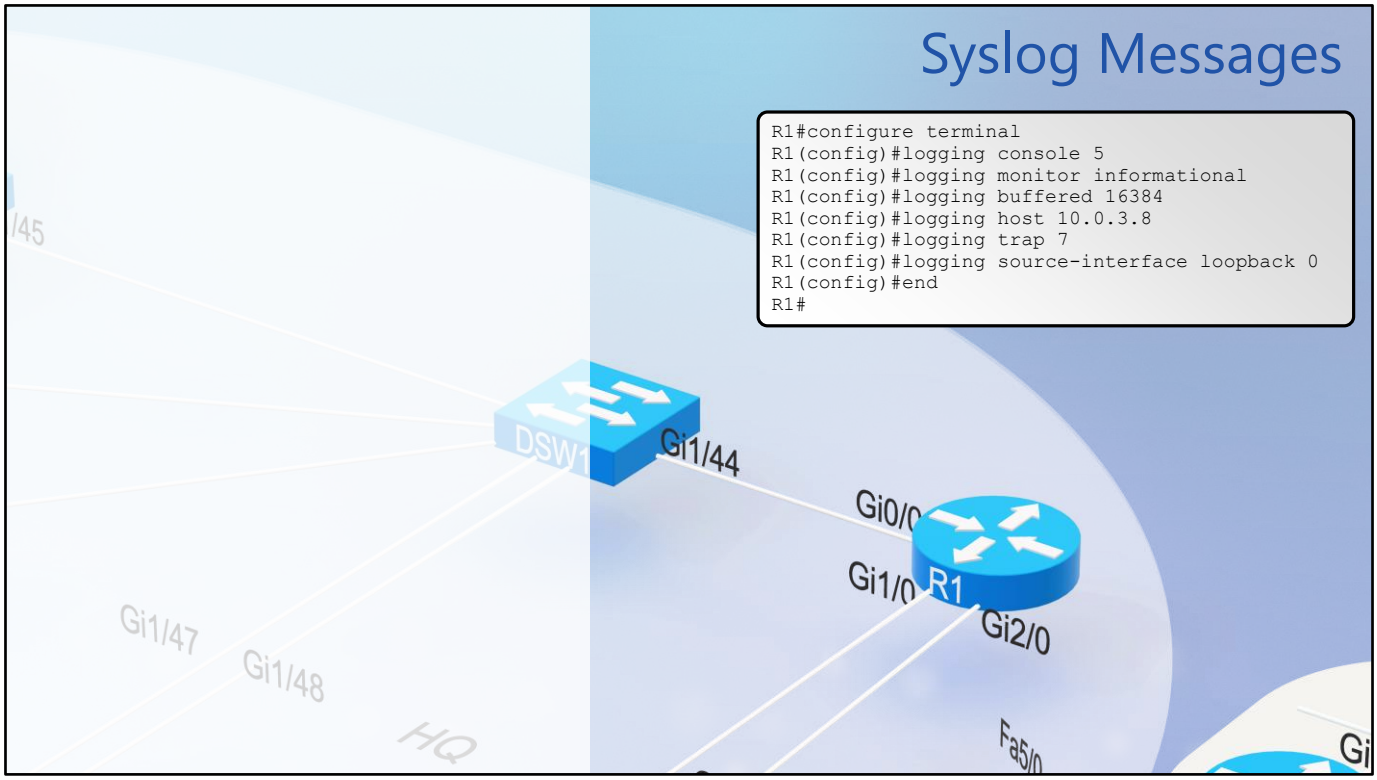
emergencies	0
alerts	1
critical	2
errors	3
warnings	4
notifications	5
informational	6
debugging	7



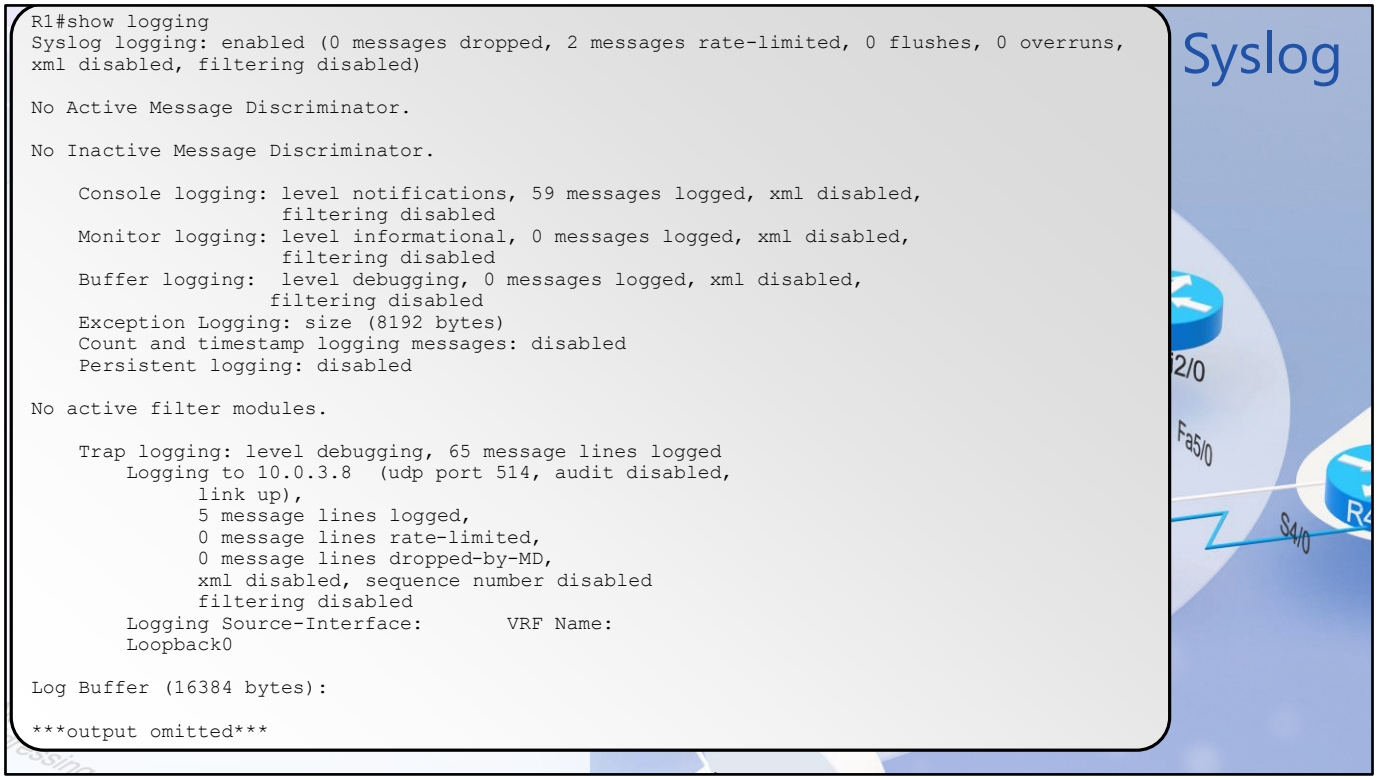
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



So when troubleshooting

1. Is logging enabled? (logging on)
    1. Logging console (it will state disabled if not on)
    2. Logging monitor (it will state disabled if not on)
    3. Logging buffered (it will state disabled if not on)
2. Are the severity levels correct
3. Is the ip correct for the syslog server
4. Is the buffer size correct for the buffer
5. When using telnet or ssh… did you type in terminal monitor to see the syslog messages?
6. Are you getting timestamps… if not enable them with service timestamps.
7. Are your timestamps displaying local time or UTC time. What do you want? If it is UTC time add the localtime keyword to service timestamps

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Debugs

- Show commands are a snap-shot in time
  - Information provided at the moment you executed the command
- Debugs are real-time
  - Information provided as changes occur
    - Automatically sent to
      - Console
      - Monitor
      - Buffer

DON’T forget that if you are telnetted or sshed into a device the messages will not be displayed until you type in terminal monitor.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Debugs

Example:

show ip route will not show you adds and deletes from the routing table

debug ip routing will show you adds and deletes from the routing table

```
R1#show ip route
…output omitted…

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
C        10.0.12.0/24 is directly connected, GigabitEthernet1/0
L        10.0.12.1/32 is directly connected, GigabitEthernet1/0
C        10.0.14.0/24 is directly connected, GigabitEthernet0/0
L        10.0.14.1/32 is directly connected, GigabitEthernet0/0
D        10.0.24.0/24 [90/3072] via 10.0.14.4, 00:23:29, GigabitEthernet0/0
                      [90/3072] via 10.0.12.2, 00:23:29, GigabitEthernet1/0
      13.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        13.13.13.0/24 is directly connected, GigabitEthernet2/0
…output omitted…
```

Show ip route gives you a snap shot in time.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Debugs

Example:

show ip route will not show you adds and deletes from the routing table

debug ip routing will show you adds and deletes from the routing table

```
R1#debug ip routing
IP routing debugging is on
R1#
*Sep 12 14:48:45.551: RT: updating eigrp 10.0.44.0/24 (0x0):
    via 10.0.14.4 Gi0/0  1048578

*Sep 12 14:48:45.555: RT: add 10.0.44.0/24 via 10.0.14.4, eigrp metric [90/3072]
*Sep 12 14:48:45.583: RT: updating eigrp 10.0.44.0/24 (0x0):
    via 10.0.14.4 Gi0/0  1048578

*Sep 12 14:48:45.587: RT: updating eigrp 10.0.44.0/24 (0x0):
    via 10.0.12.2 Gi1/0  1048578

*Sep 12 14:48:45.591: RT: rib update return code: 19
R1#
```

Real time output

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Debugs

Example:

show ip route will not show you adds and deletes from the routing table

debug ip routing will show you adds and deletes from the routing table

```
R1#show ip route
…output omitted…

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
C        10.0.12.0/24 is directly connected, GigabitEthernet1/0
L        10.0.12.1/32 is directly connected, GigabitEthernet1/0
C        10.0.14.0/24 is directly connected, GigabitEthernet0/0
L        10.0.14.1/32 is directly connected, GigabitEthernet0/0
D        10.0.24.0/24 [90/3072] via 10.0.14.4, 00:26:48, GigabitEthernet0/0
                      [90/3072] via 10.0.12.2, 00:26:48, GigabitEthernet1/0
D        10.0.44.0/24 [90/3072] via 10.0.14.4, 00:02:34, GigabitEthernet0/0
      13.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        13.13.13.0/24 is directly connected, GigabitEthernet2/0
…output omitted…
```

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Debugs

- Invokes Process switching on the device
  - CPU needs to process the packet
  - Could slow down the device as it processes and generates debugs
- RISKS
  - Turning to many on at the same time
  - Leaving debugs enabled
- Use **undebug all (u all)** to disable all debugs that might be enabled

Debug ? Shows that there are tons of debugs… too many to cover.

You could create am EEM applet that can run **u all** automatically for you in case you or anyone else forgets.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Debugs

CISCO WARNING:

Use debug commands with caution. In general, it is recommended that these commands only be used under the direction of your router technical support representative when troubleshooting specific problems.

Enabling debugging can disrupt operation of the router when internetworks are experiencing high load conditions. Hence, if logging is enabled, the access server can intermittently freeze as soon as the console port gets overloaded with log messages.

Source: many cisco documents at www.cisco.com

Debug ? Shows that there are tons of debugs… too many to cover.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Conditional Debugs

Provides debug filtering to limit the output generated

***this list will vary based on device and IOS version

```
R1#debug condition ?
  application  Application
  called       called number
  calling      calling
  cpl          Cisco Provisioning Language debugging
  glbp         interface group
  interface    interface
  ip           IP address
  mac-address  MAC address
  match-list   apply the match-list
  profile      Media Services Profile
  standby      interface group
  username     username
  vcid         VC ID
  voice-port   voice-port number
  vrf          Virtual Routing and Forwarding
  xconnect     Xconnect conditional debugging on segment pair
```

For example, if you only want debugs based on a certain mac address… you can… if you only want debugs for a certain interface… you can… debug based on a certain ip address… you can

THIS IS NOT CONDITIONAL DEBUGGING
R2#debug eigrp packets ?
 SIAquery EIGRP SIA-Query packets
 SIAreply EIGRP SIA-Reply packets
 ack EIGRP ack packets
 hello EIGRP hello packets
 ipxsap EIGRP ipxsap packets
 query EIGRP query packets
 reply EIGRP reply packets
 request EIGRP request packets
 retry EIGRP retransmissions
 stub EIGRP stub packets
 terse Display all EIGRP packets except Hellos
 update EIGRP update packets

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

```
  verbose   Display all EIGRP packets
  <cr>
```

```
R2#debug eigrp packets
```

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Conditional Debugs

```
R1#debug ip packet
IP packet debugging is on
R1#
*Sep 12 15:16:00.523: IP: s=10.0.14.1 (local), d=224.0.0.10 (GigabitEthernet0/0), len 60, sending broad/multicast
*Sep 12 15:16:00.531: IP: s=10.0.14.1 (local), d=224.0.0.10 (GigabitEthernet0/0), len 60, sending full packet
*Sep 12 15:16:02.691: IP: s=10.0.14.4 (GigabitEthernet0/0), d=224.0.0.10, len 60, rcvd 0
*Sep 12 15:16:02.695: IP: s=10.0.14.4 (GigabitEthernet0/0), d=224.0.0.10, len 60, input feature, packet consumed, MCI
Check(101), rtype 0, forus FALSE, sendself FALSE, mtu 0, fwdchk FALSE
*Sep 12 15:16:02.931: IP: s=10.0.12.1 (local), d=224.0.0.10 (GigabitEthernet1/0), len 60, sending broad/multicast
*Sep 12 15:16:02.939: IP: s=10.0.12.1 (local), d=224.0.0.10 (GigabitEthernet1/0), len 60, sending full packet
*Sep 12 15:16:03.015: IP: s=10.0.12.2 (GigabitEthernet1/0), d=224.0.0.10, len 60, rcvd 0
*Sep 12 15:16:03.019: IP: s=10.0.12.2 (GigabitEthernet1/0), d=224.0.0.10
, len 60, input feature, packet consumed, MCI Check(101), rtype 0, forus FALSE, sendself FALSE, mtu 0, fwdchk FALSE
*Sep 12 15:16:04.419: IP: s=13.13.13.1 (local), d=13.13.13.3 (GigabitEthernet2/0), len 59, sending
*Sep 12 15:16:04.427: IP: s=13.13.13.1 (local), d=13.13.13.3 (GigabitEthernet2/0), len 59, sending full packet
*Sep 12 15:16:04.675: IP: s=13.13.13.3 (GigabitEthernet2/0), d=13.13.13.1, len 40, rcvd 0
*Sep 12 15:16:04.679: IP: s=13.13.13.3 (GigabitEthernet2/0), d=13.13.13.1, len 40, input feature, packet consumed, MCI
Check(101), rtype 0, forus FALSE, sendself FALSE, mtu 0, fwdchk FALSE
*Sep 12 15:16:04.943: IP: s=10.0.14.1 (local), d=224.0.0.10 (GigabitEthernet0/0), len 60, sending broad/multicast
*Sep 12 15:16:04.951: IP: s=10.0.14.1 (local), d=224.0.0.10
R1#(GigabitEthernet0/0), len 60, sending full packet
R1#u all
All possible debugging has been turned off
R1#
```

For example, if you only want debugs based on a certain mac address… you can… if you only want debugs for a certain interface… you can… debug based on a certain ip address… you can

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Conditional Debugs

```
R1#debug condition interface gigabitEthernet 0/0
Condition 1 set
R1#debug ip packet
IP packet debugging is on
R1#
*Sep 12 15:17:58.251: IP: s=10.0.14.4 (GigabitEthernet0/0), d=224.0.0.10, len 60, rcvd 0
*Sep 12 15:17:58.255: IP: s=10.0.14.4 (GigabitEthernet0/0), d=224.0.0.10, len 60, input feature, packet consumed, MCI
Check(101), rtype 0, forus FALSE, sendself FALSE, mtu 0, fwdchk FALSE
R1#
*Sep 12 15:17:59.495: IP: s=10.0.14.1 (local), d=224.0.0.10 (GigabitEthernet0/0), len 60, sending broad/multicast
*Sep 12 15:17:59.503: IP: s=10.0.14.1 (local), d=224.0.0.10 (GigabitEthernet0/0), len 60, sending full packet
R1#
*Sep 12 15:18:03.131: IP: s=10.0.14.4 (GigabitEthernet0/0), d=224.0.0.10, len 60, rcvd 0
*Sep 12 15:18:03.135: IP: s=10.0.14.4 (GigabitEthernet0/0), d=224.0.0.10, len 60, input feature, packet consumed, MCI
Check(101), rtype 0, forus FALSE, sendself FALSE, mtu 0, fwdchk FALSE
R1#
*Sep 12 15:18:04.227: IP: s=10.0.14.1 (local), d=224.0.0.10 (GigabitEthernet0/0), len 60, sending broad/multicast
*Sep 12 15:18:04.235: IP: s=10.0.14.1 (local), d=224.0.0.10 (GigabitEthernet0/0), len 60, sending full packet
R1#
*Sep 12 15:18:08.043: IP: s=10.0.14.4 (GigabitEthernet0/0), d=224.0.0.10, len 60, rcvd 0
*Sep 12 15:18:08.047: IP: s=10.0.14.4 (GigabitEthernet0/0), d=224.0.0.10, len 60, input feature, packet consumed, MCI
Check(101), rtype 0, forus FALSE, sendself FALSE, mtu 0, fwdchk FALSE
*Sep 12 15:18:08.971: IP: s=10.0.14.1 (local), d=224.0.0.10 (GigabitEthernet0/0), len 60, sending broad/multicast
*Sep 12 15:18:08.979: IP: s=10.0.14.1 (local), d=224.0.0.10 (GigabitEthernet0/0), len 60, sending full packet
R1#u all
All possible debugging has been turned off
R1#
```

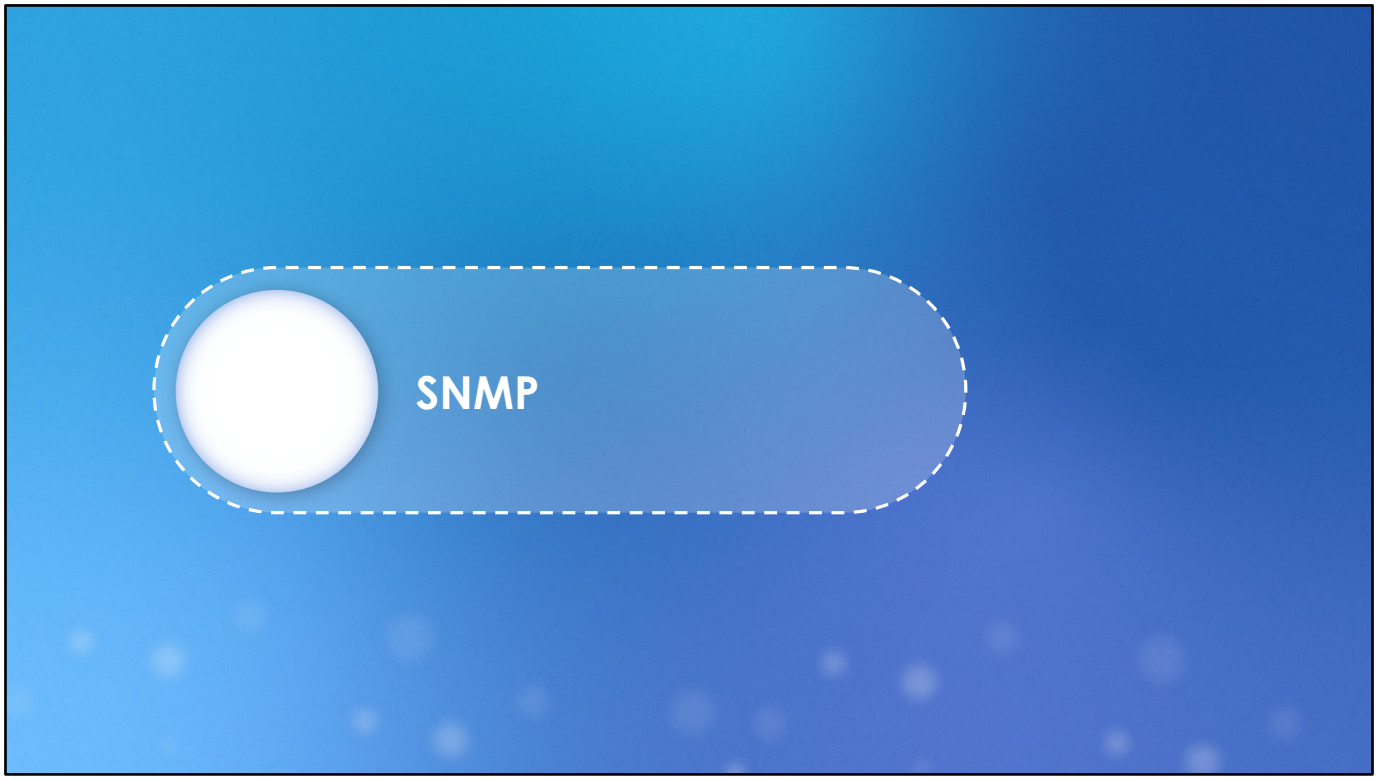
For example, if you only want debugs based on a certain mac address… you can… if you only want debugs for a certain interface… you can… debug based on a certain ip address… you can

You can specify multiple conditions… don't forget to delete the conditions or the next time you debug the same conditions will still be set.

R2#show debugging condition
% No conditions found

R2#no debug condition all (REMOVES ALL CONDITIONS)

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Title slide

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Simple Network Management Protocol (SNMP)

Management protocol used to poll devices such as:

- Routers, Switches, Servers, etc.

Used to collect and organize information about the device's wellbeing.

Information is stored as variables in a database on the device called the MIB (management information base).

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

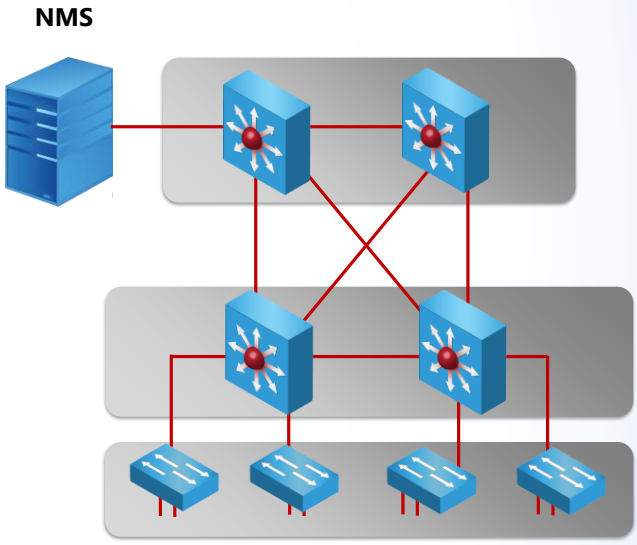
SNMP Overview

The NMS runs the SNMP manager software

The **SNMP agent** runs on the managed devices (i.e IOS routers and switches)

SNMP NMS will poll agent

SNMP **traps** and **informs** are event driven messages sent from the agent to the manager



A quick recap on the difference between TRAPs and INFORMs: A TRAP is a SNMP message sent from one application to another (which is typically on a remote host). They're purpose is merely to notify the other application that something has happened, has been noticed, etc. The big problem with TRAPs is that they're unacknowledged so you don't actually know if the remote application received your oh-so-important message to it. SNMPv2 PDUs fixed this by introducing the notion of an INFORM, which is nothing more than an acknowledged TRAP. IE, when the remote application receives the INFORM it sends back a "I got it" message. This is nice because then the person sending the traps can keep trying until the trap gets through.

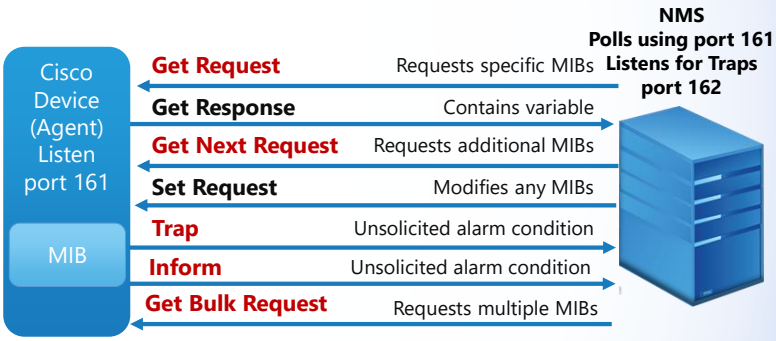
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

SNMP Versions

SNMPv1 - 5 message types

SNMPv2 - Adds 2 types: Get Bulk Request and Inform Request.

SNMPv3 – More secure as it supports: authentication, integrity, encryption, authorization



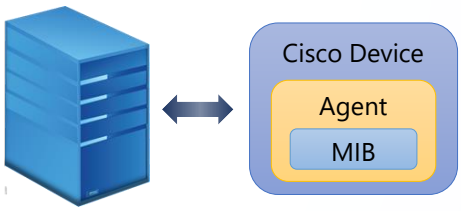
https://en.wikipedia.org/wiki/Simple_Network_Management_Protocol

V2c uses community strings for authentication

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

SNMP Recommendations

Configure as Read Only
Restrict NMS to access only required MIBs
Configure ACLs to restrict NMS access
Use V3 with AuthPriv



Read only unless write is needed
Use a view to restrict access to MIBs
Use ACLs to restrict access to certain servers
Use v3 with auth priv for the highest security

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

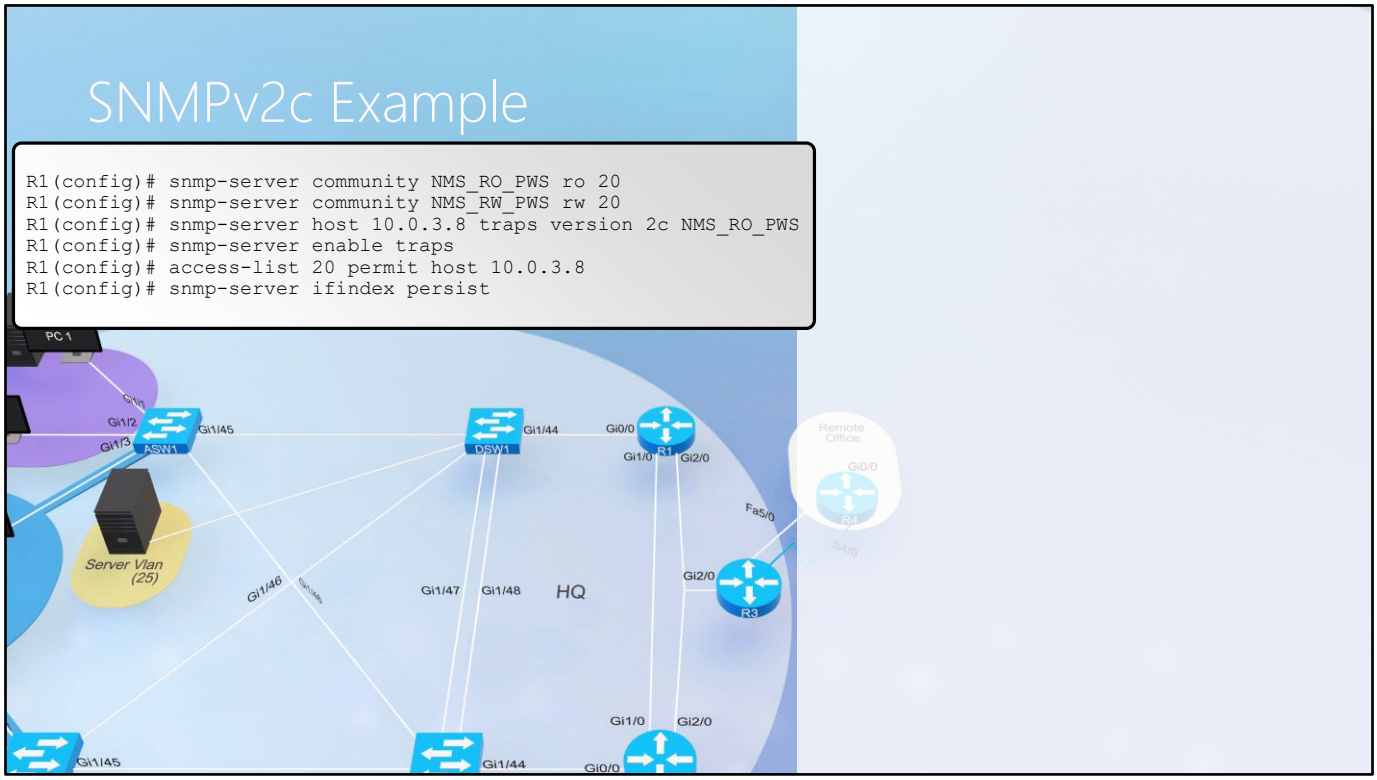
SNMPv2c Example



Talk about standard and extended

```
R1#traceroute 192.168.4.4 ?
  numeric  display numeric address
  port     specify port number
  probe    specify number of probes per hop
  source   specify source address or name
  timeout  specify time out
  ttl      specify minimum and maximum ttl
  <cr>
```

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



EXAM
Question had community with a string but no ro or rw specified and they need rw access. Therefore, it defaults to ro. Also, the ACL was not configured correctly for the management/operations network.

Keep the following in mind as you troubleshoot SNMPv2c:
■ Ensuring that community strings match: For the NMS to read from or write to the agent, the read community string or the read/write community string must match between the NMS and the agent. In Example 23-12, the read-only community string specified is CISCO.
■ Ensuring that ACLs classifying servers are correct: If you are using ACLs to define which NMS (based on IP address) is allowed to retrieve objects from the MIB, the ACL has to accurately define the server addresses. In Example 23-12, ACL 10 is only permitting the NMS with the IP address 10.1.100.100 to read from the MIB using the read-only community string CISCO.
■ Ensuring the correct configuration for notifications: If your agent is configured to send traps or informs, you should verify the following:
■ Ensure that traps are enabled. By default all traps are sent unless you specify

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

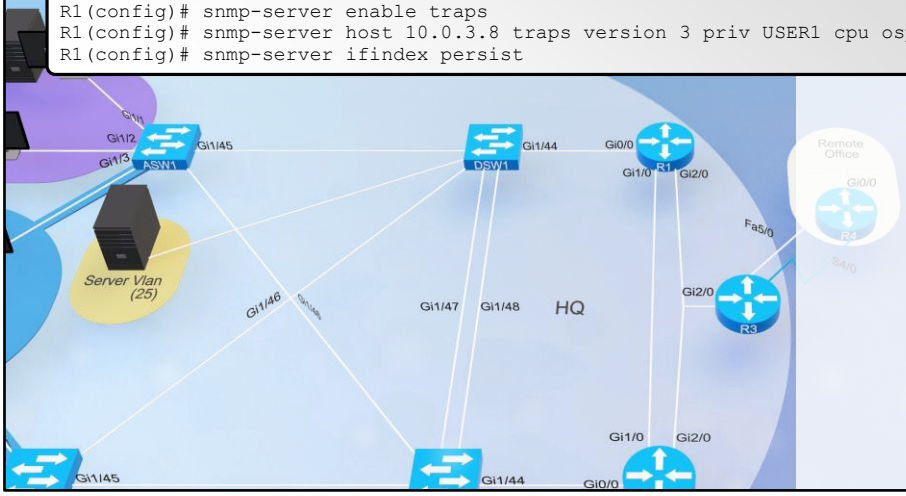
otherwise.
https://www.cisco.com/c/en/us/support/docs/ip/simple-network-management-protocol-snmp/13506-snmp-traps.html

■ Ensure that the correct host (NMS) IP address is specified.
■ Ensure that the correct SNMP version is specified.
■ Ensure that the correct community string is specified.
If you did not want all traps to be sent, it is imperative that you specify the correct ones to send. In Example 23-12, the snmp-server host command indicates that SNMPv2c informs will be sent to the NMS at 10.1.100.100 with a community string of CISCO.
■ Preventing indexes from shuffling: To prevent index shuffling and guarantee index persistence during reboots or minor software upgrades, use the snmp-server ifindex persist command, which shows up as snmp ifmib ifindex persist in the running configuration.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

SNMPv3 Example

```
R1(config)# access-list 20 permit host 10.0.3.8
R1(config)# snmp-server view MGMT ifAdminStatus include
R1(config)# snmp-server view MGMT ifOperStatus include
R1(config)# snmp-server group TEST v3 priv read MGMT access 20
R1(config)# snmp-server user USER1 TEST v3 auth sha p@ssw0rd priv aes 256 pa55word
R1(config)# snmp-server enable traps
R1(config)# snmp-server host 10.0.3.8 traps version 3 priv USER1 cpu ospf
R1(config)# snmp-server ifindex persist
```



R2(config)#snmp-server group TEST v3 ?
  auth   group using the authNoPriv Security Level
  noauth group using the noAuthNoPriv Security Level
  priv   group using SNMPv3 authPriv security level

By default all traps are sent unless you specify otherwise.
https://www.cisco.com/c/en/us/support/docs/ip/simple-network-management-protocol-snmp/13506-snmp-traps.html

One of the most commonly used identifiers in SNMP-based network management applications is the Interface Index (ifIndex) value. IfIndex is a unique identifying number associated with a physical or logical interface. For most software, the ifIndex is the name of the interface. Although relevant RFCs do not require that the correspondence between particular ifIndex values and their interfaces be maintained across reboots, applications such as device inventory, billing, and fault detection depend on this correspondence.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Retain interface index numbering when a reboot happens.

```
R1(config)# snmp-server ifindex persist
```

****

SNMP does not identify object instances… such as network interfaces… by their names. Instead, these object instances are identified by a numerical value known as an index. When changes to interfaces occur… such as new interfaces are added or old interfaces are removed… or even when a reboot or minor software update happens… the index numbers may be re-shuffled (changed). As a result the SNMP NMS may "mismatch" information about one interface with a different interface that is now using that index number. To prevent this from happening use the **snmp-server ifindex persist** command to guarantee that the index number never changes.

Why is it not enabled by default in IOS???? Because not all platforms support it.

Keep the following in mind as you troubleshoot SNMPv3:

■ Nesting of users, views, and groups: With SNMPv3, you create users with authentication and encryption parameters that are nested into groups that define the servers that are allowed to read from or write to the objects within the MIB on the agent. If you fail to nest the users, views, and groups, SNMPv3 will not function as expected. In Example 23-13, the user NMSERVER is nested into the group NMSREADONLY, which allows read-only access to the object identifiers (OIDs) listed in the view MIBACCESS to the NMS with the IP address 10.1.100.100.

■ Wrong security level specified: SNMPv3 supports three security levels: n oAuthNoPriv, authNoPriv, and authPriv. The security levels specified for the group, for the users, and for the sending of traps must match what is used on the server. In Example 23-13, authPriv is being used extensively (with the priv parameter in the commands), which means that authentication and encryption will be used.

■ Wrong hashing algorithm, encryption algorithm, or passwords defined: When authenticating, the hashing algorithm must match, along with the password; otherwise, authentication will fail. When performing encryption, the encryption algorithm and password must match; otherwise, the NMS will not be able to decrypt

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

the data it receives. In Example 23-13, SHA is being used as the hashing algorithm, AES-256 as the encryption algorithm, and MYPASSWORD as the password.

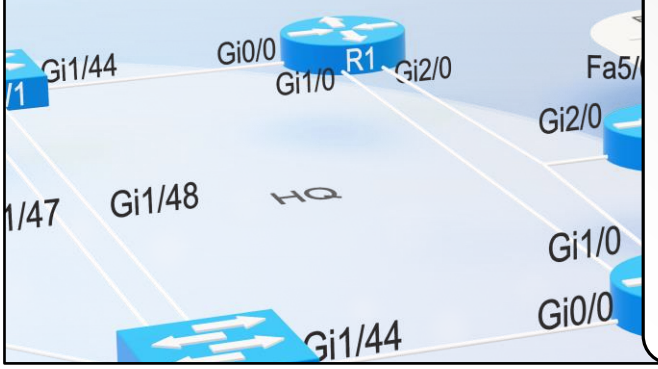
■ Wrong OIDs specified in the view: The views identify the objects within the MIB that the NMS will be able to access. If the wrong objects are defined, SNMPv3 will not produce the desired results. In Example 23-13, the objects sysUpTime, ifAdminStatus, and ifOperStatus are defined in the MIBACCESS view.

■ Notification configuration: If your agent is configured to send traps or informs, you should verify that traps are enabled, the correct host (NMS) IP address is specified, the correct SNMP version is specified, and the correct security level is specified, and you should make sure you specified traps or informs (default is traps). If you do not want all traps to be sent, it is imperative that you specify the correct ones. You also need to specify the correct SNMPv3 username for the authentication/encryption process. In Example 23-13, the snmp-server host command indicates that SNMPv3 will send traps related to the CPU to the NMS at 10.1.100.100, with the authentication and encryption provided by the username NMSERVER.

■ Shuffling indexes: To prevent index shuffling and guarantee index persistence during reboots or minor software upgrades, use the snmp-server ifindex persist command, which shows up as snmp ifmib ifindex persist in the running configuration.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

SNMPv3 Verification




```
R1#show snmp
Chassis: 4279256517
0 SNMP packets input
     0 Bad SNMP version errors
     0 Unknown community name
     0 Illegal operation for community name supplied
     0 Encoding errors
     0 Number of requested variables
     0 Number of altered variables
     0 Get-request PDUs
     0 Get-next PDUs
     0 Set-request PDUs
     0 Input queue packet drops (Maximum queue size 1000)
0 SNMP packets output
     0 Too big errors (Maximum packet size 1500)
     0 No such name errors
     0 Bad values errors
     0 General errors
     0 Response PDUs
     0 Trap PDUs
SNMP Dispatcher:
   queue 0/75 (current/max), 0 dropped
SNMP Engine:
   queue 0/1000 (current/max), 0 dropped

SNMP logging: enabled
    Logging to 10.0.3.8.162, 0/10, 0 sent, 0 dropped.
R1#
```

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

SNMPv3 Verification




```
R1#show snmp view
MGMT ifAdminStatus - included nonvolatile active
MGMT ifOperStatus - included nonvolatile active
*ilmi system - included permanent active
*ilmi atmForumUni - included permanent active
cac_view pimMIB - included read-only active
cac_view msdpMIB - included read-only active
cac_view interfaces - included read-only active
cac_view ip - included read-only active
cac_view ospf - included read-only active
cac_view bgp - included read-only active
cac_view dot1dBridge - included read-only active
cac_view ifMIB - included read-only active
cac_view nhrpMIB - included read-only active
cac_view ipMRouteStdMIB - included read-only active
cac_view igmpStdMIB - included read-only active
cac_view ospfv3MIB - included read-only active
cac_view ipForward - included read-only active
cac_view ipTrafficStats - included read-only active
cac_view ospfTrap - included read-only active
cac_view sysUpTime.0 - included read-only active
cac_view mplsLsrStdMIB - included read-only active
cac_view mplsLdpStdMIB - included read-only active
cac_view ciscoPingMIB - included read-only active
cac_view ciscoIpSecFlowMonitorMIB - included read-only active
cac_view ciscoIpSecPolMapMIB - included read-only active
cac_view ciscoPimMIB - included read-only active
cac_view ciscoBgp4MIB - included read-only active
cac_view ciscoIfExtensionMIB - included read-only active
…output omitted…
```

Talk about standard and extended

```
R1#traceroute 192.168.4.4 ?
  numeric  display numeric address
  port     specify port number
  probe    specify number of probes per hop
  source   specify source address or name
  timeout  specify time out
  ttl      specify minimum and maximum ttl
  <cr>
```

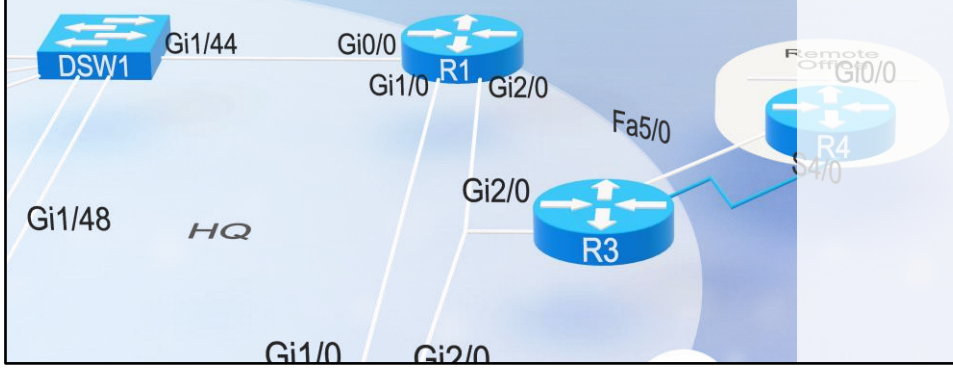
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

SNMPv3 Verification

```
R1#show snmp user

User name: USER1
Engine ID: 800000090300CA0122F40006
storage-type: nonvolatile        active
Authentication Protocol: SHA
Privacy Protocol: AES256
Group-name: TEST

R1#
```

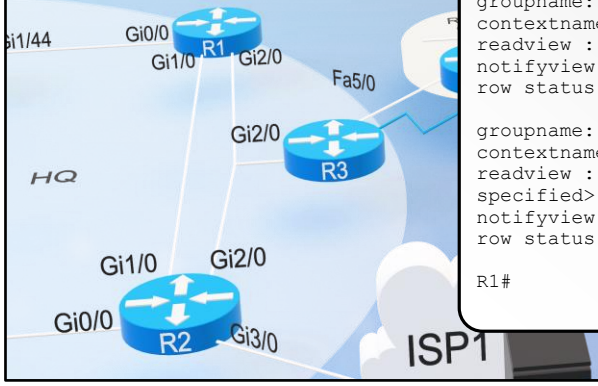


Talk about standard and extended

R1#traceroute 192.168.4.4 ?
  numeric display numeric address
  port   specify port number
  probe   specify number of probes per hop
  source   specify source address or name
  timeout specify time out
  ttl   specify minimum and maximum ttl
  <cr>

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

SNMPv3 Verification




```
R1#show snmp group
groupname: ILMI                                 security model:v1
contextname: <no context specified>             storage-type: permanent
readview : *ilmi                                writeview: *ilmi
notifyview: <no notifyview specified>
row status: active

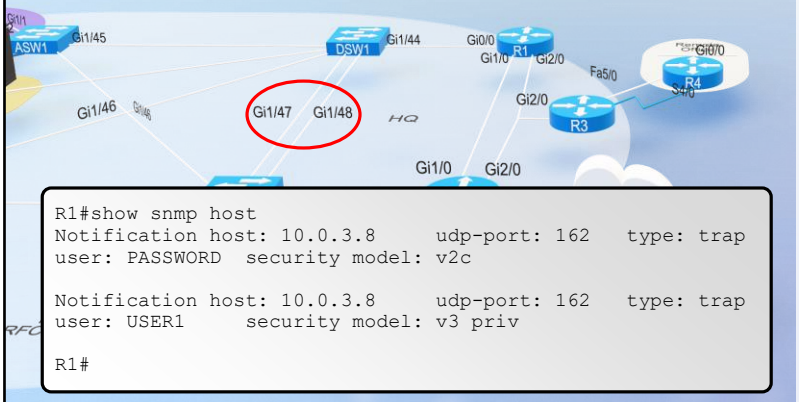
groupname: ILMI                                 security model:v2c
contextname: <no context specified>             storage-type: permanent
readview : *ilmi                                writeview: *ilmi
notifyview: <no notifyview specified>
row status: active

groupname: TEST                                 security model:v3 priv
contextname: <no context specified>             storage-type: nonvolatile
readview : MGMT                                 writeview: <no writeview
specified>
notifyview: *tv.00000000.00000000.00000800.0
row status: active

R1#
```

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

SNMPv3 Verification




```
R1#show snmp host
Notification host: 10.0.3.8     udp-port: 162   type: trap
user: PASSWORD  security model: v2c

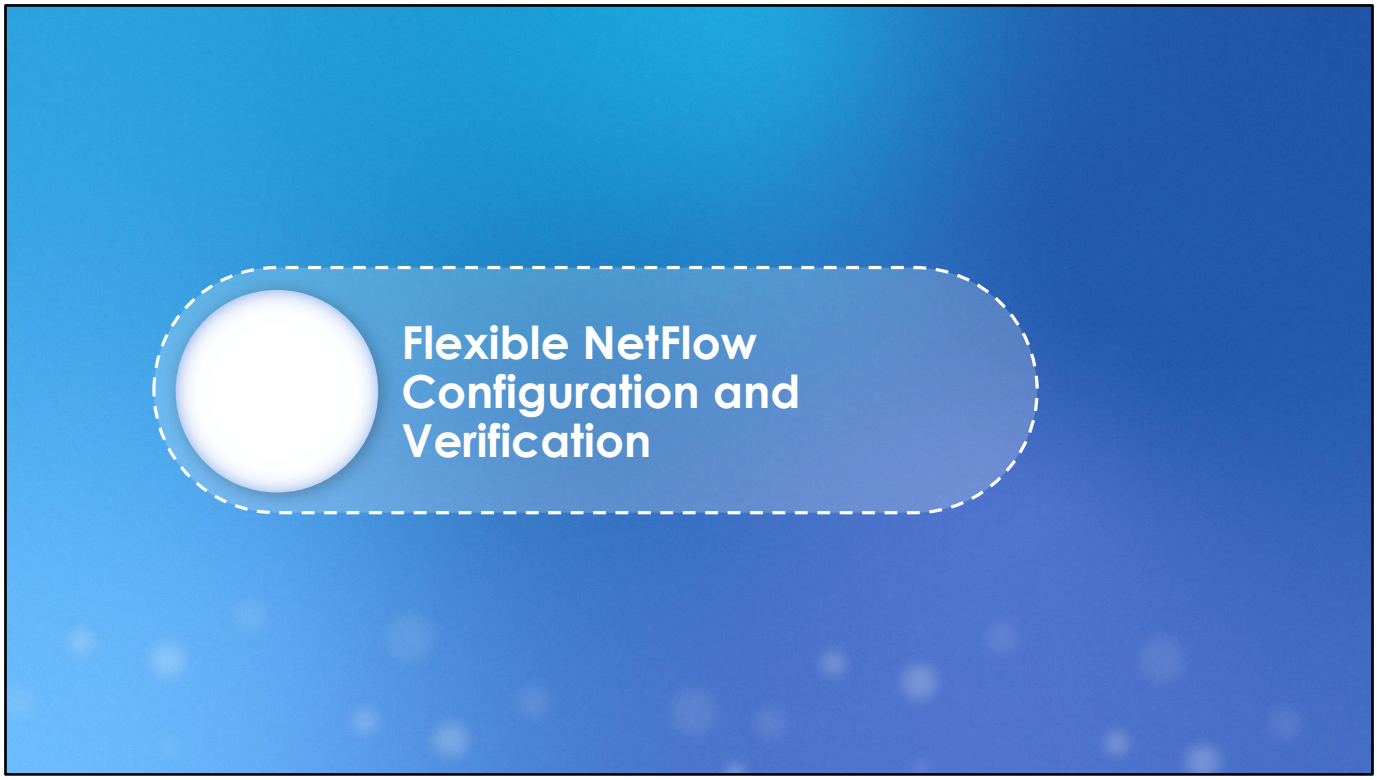
Notification host: 10.0.3.8     udp-port: 162   type: trap
user: USER1     security model: v3 priv

R1#
```

Talk about standard and extended

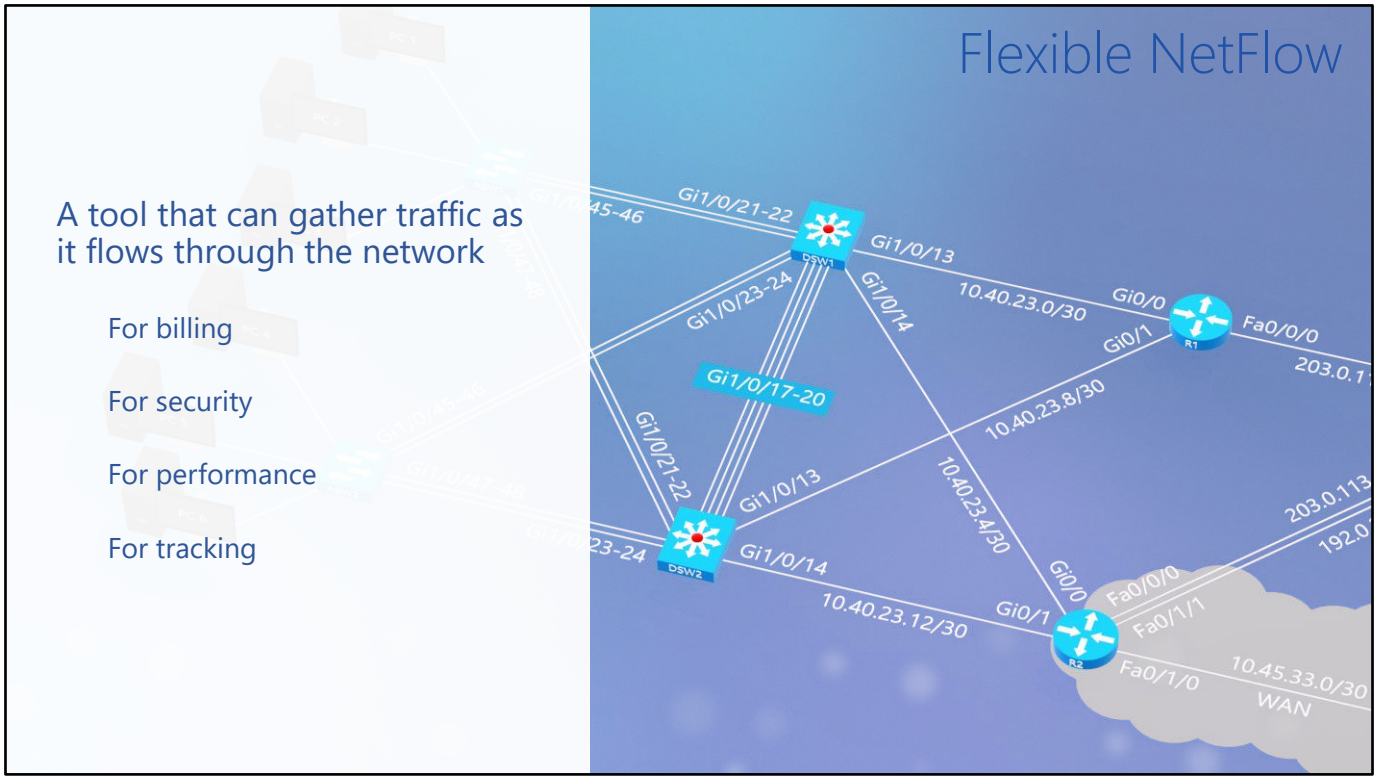
R1#traceroute 192.168.4.4 ?
- numeric display numeric address
- port specify port number
- probe specify number of probes per hop
- source specify source address or name
- timeout specify time out
- ttl specify minimum and maximum ttl
- <cr>

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



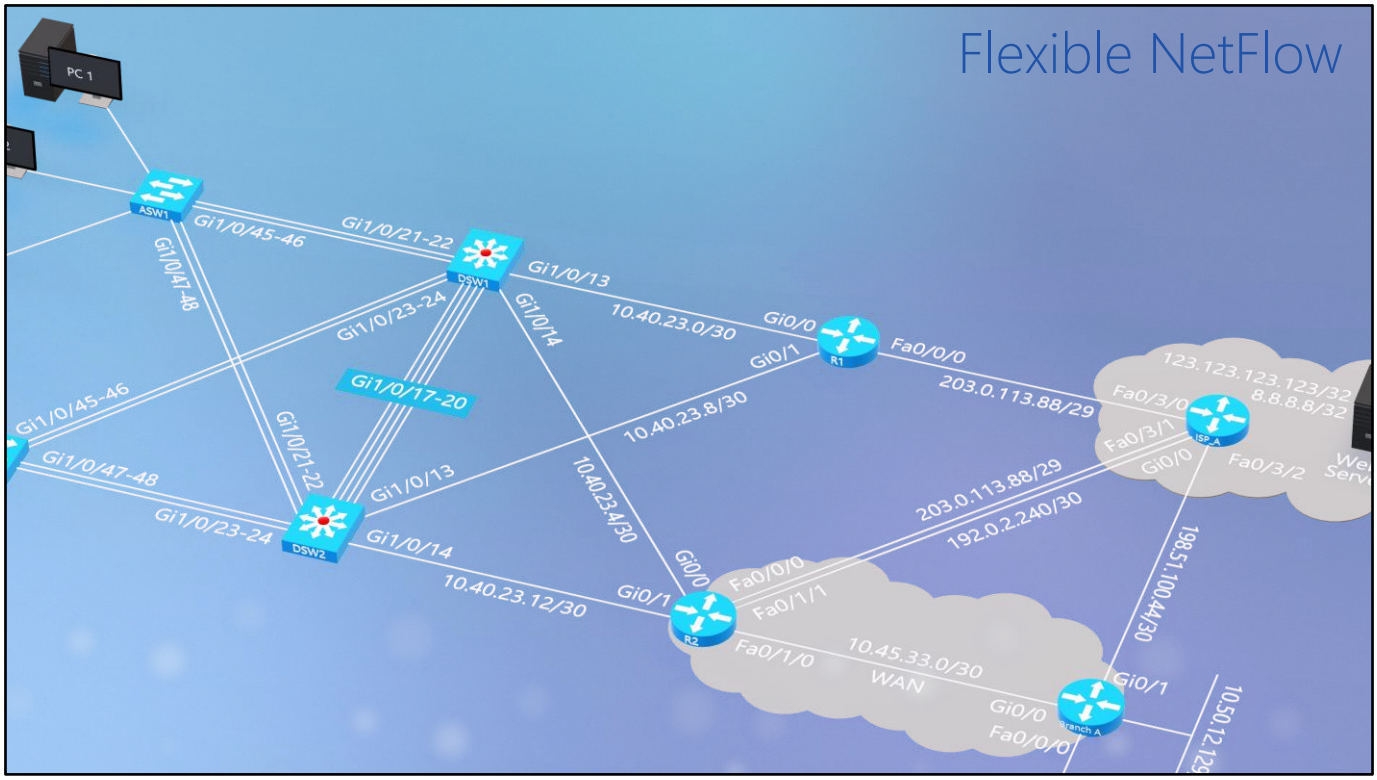
Title slide

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



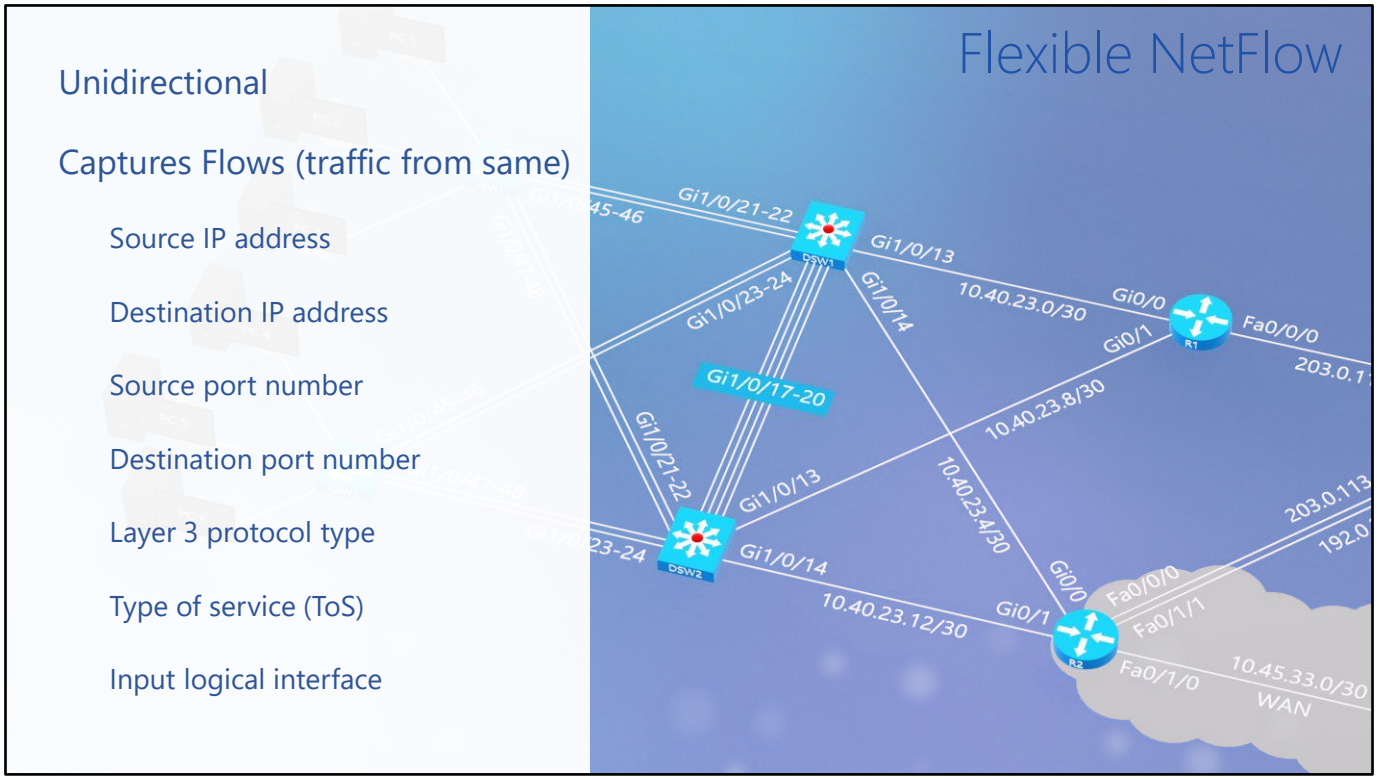
EXAM - Which component does Cisco Threat Defense use to measure bandwidth, application performance, and utilization?
NETFLOW

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Annotate traffic going from PC1 to Internet (THROUGH R1). Discuss how we can use NetFlow to capture the packets as they arrive inbound on any interface in the path or leave any interface in the path.

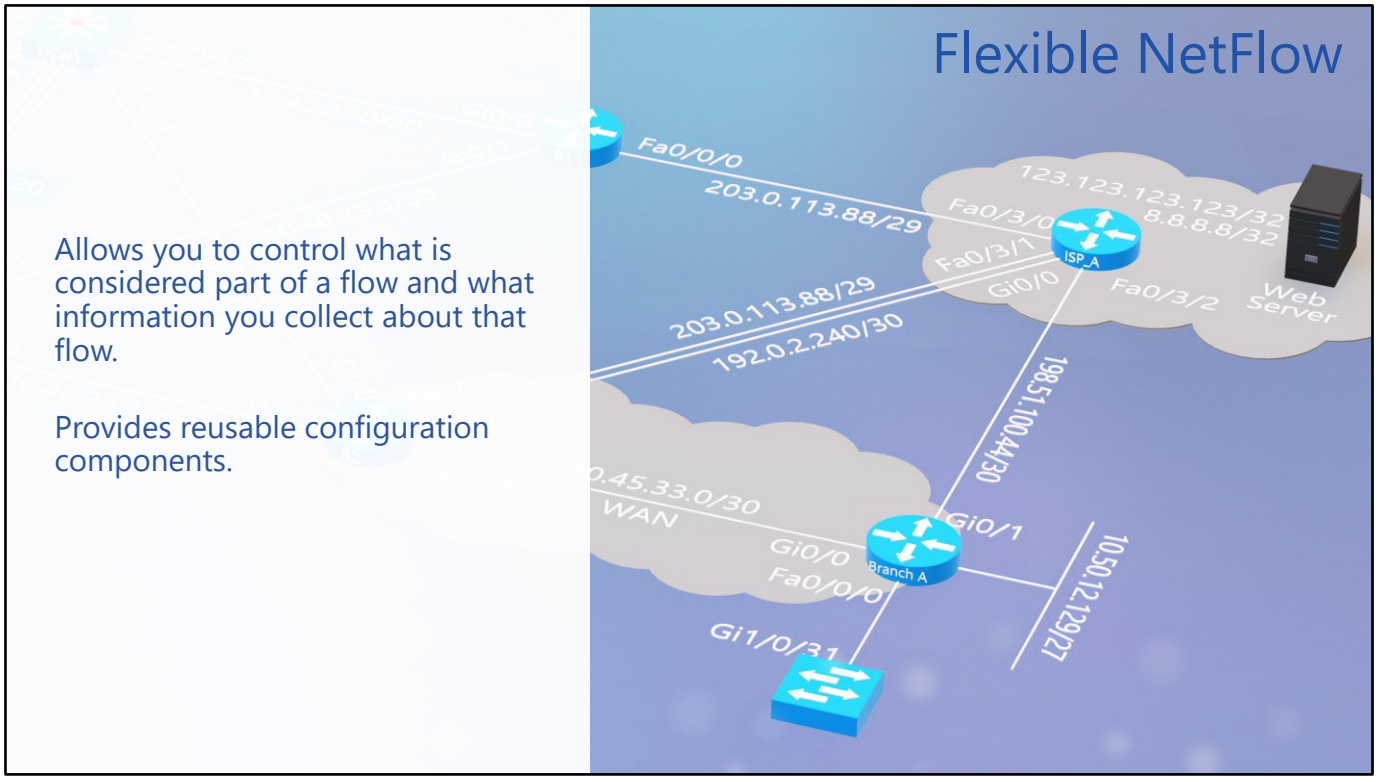
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



With Flexible NetFlow a flow is anything you want it to me. A traditional flow is based on these 7 elements.

However, with flexible netflow you can configure the flow to be based on a multitude of elements.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fnetflow/configuration/15-mt/fnf-15-mt-book/fnf-fnetflow.html

NETFLOW version 2.0 (it is the new version of netflow)

This means that multiple different flow policies can be applied to the same traffic as it flows through a device. If two different departments have a reason to analyze the traffic, both can do so by using different parameters in each flow monitor.

REGULAR NETFLOW ONLY DOES:

Captures Flows (traffic from same)

Source IP address

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Destination IP address

Source port number

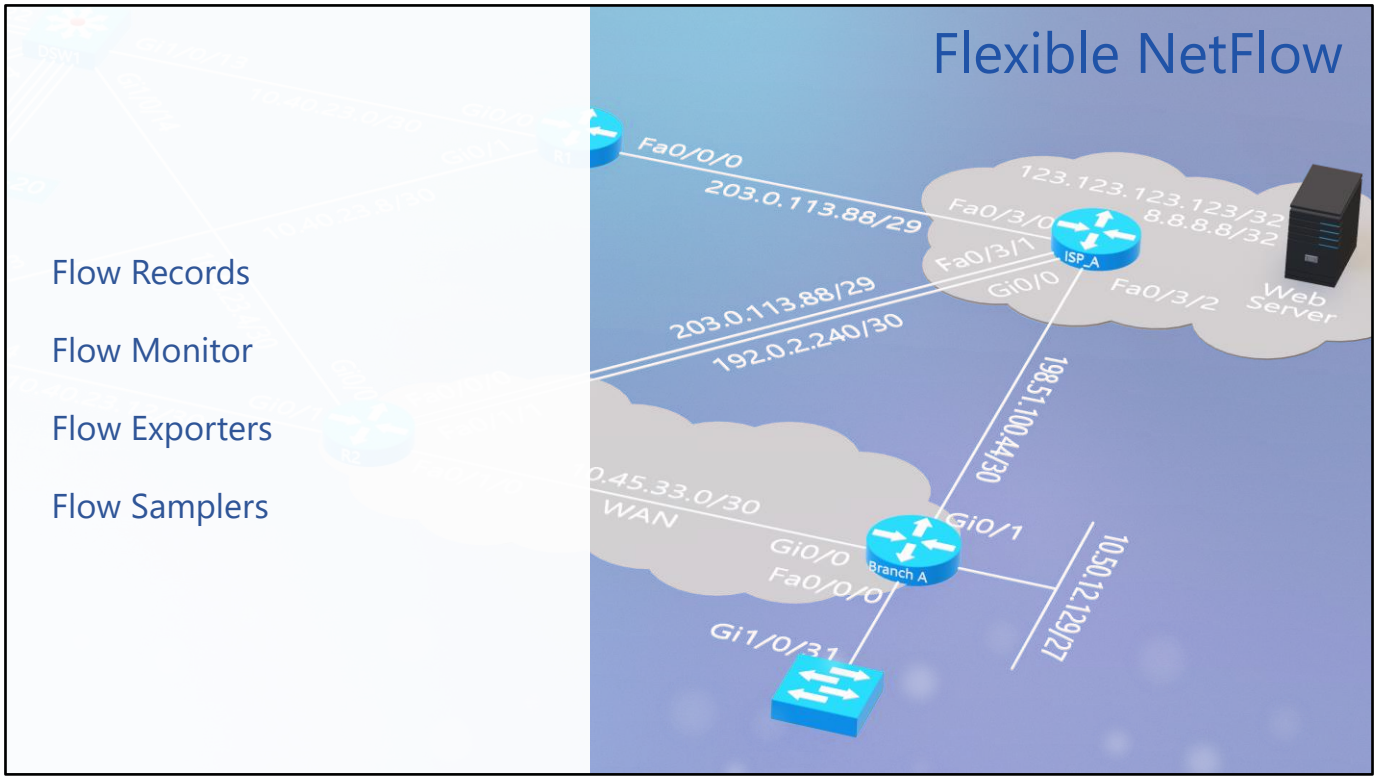
Destination port number

Layer 3 protocol type

Type of service (ToS)

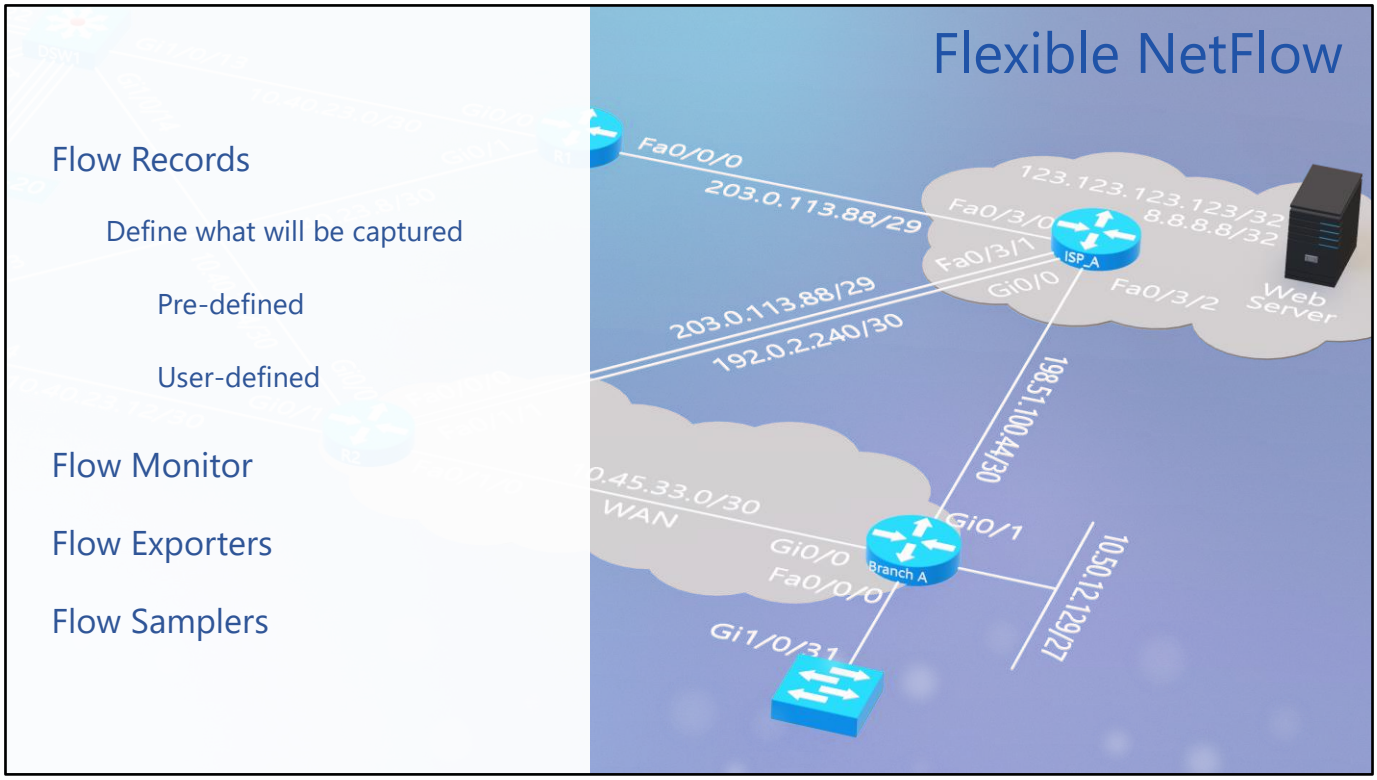
Input logical interface

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



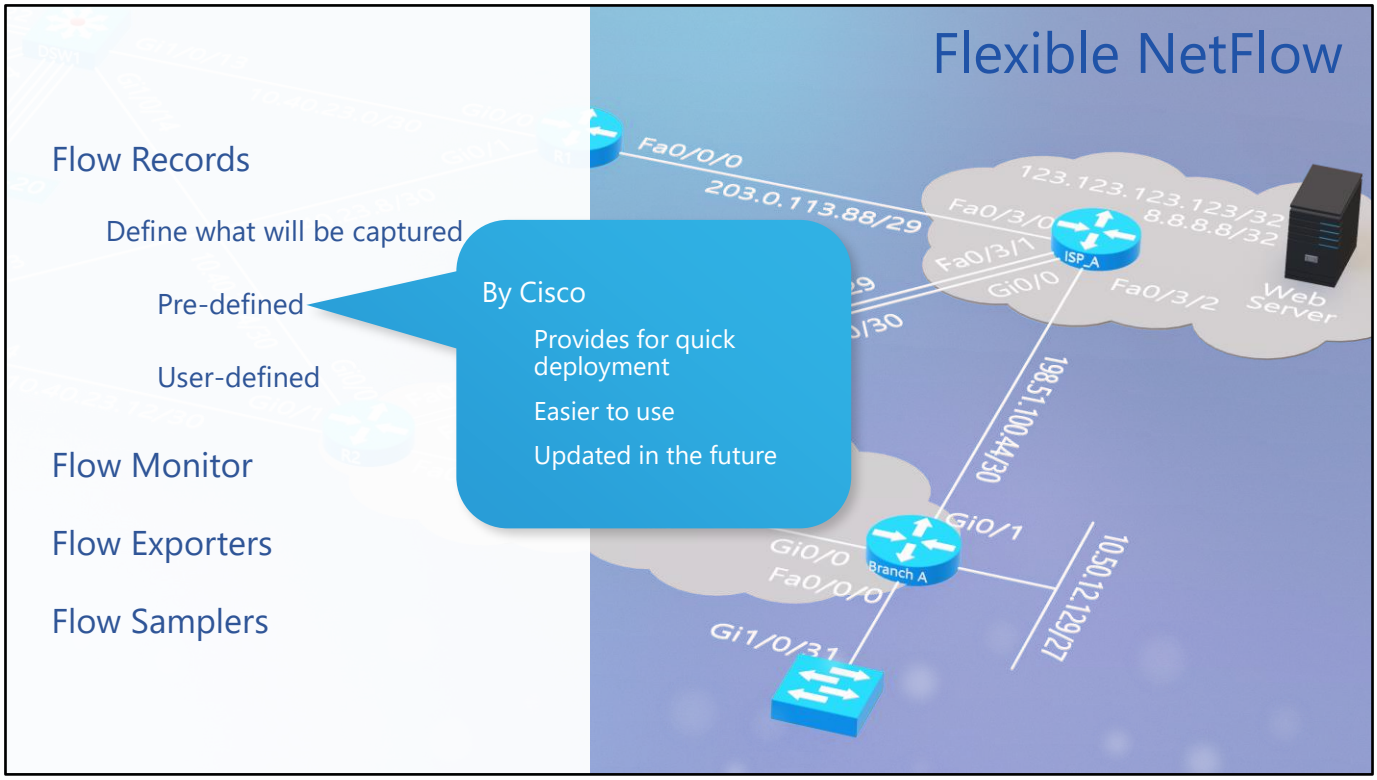
NETFLOW version 2.0 (it is the new version of netflow)

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



NETFLOW version 2.0 (it is the new version of netflow)

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



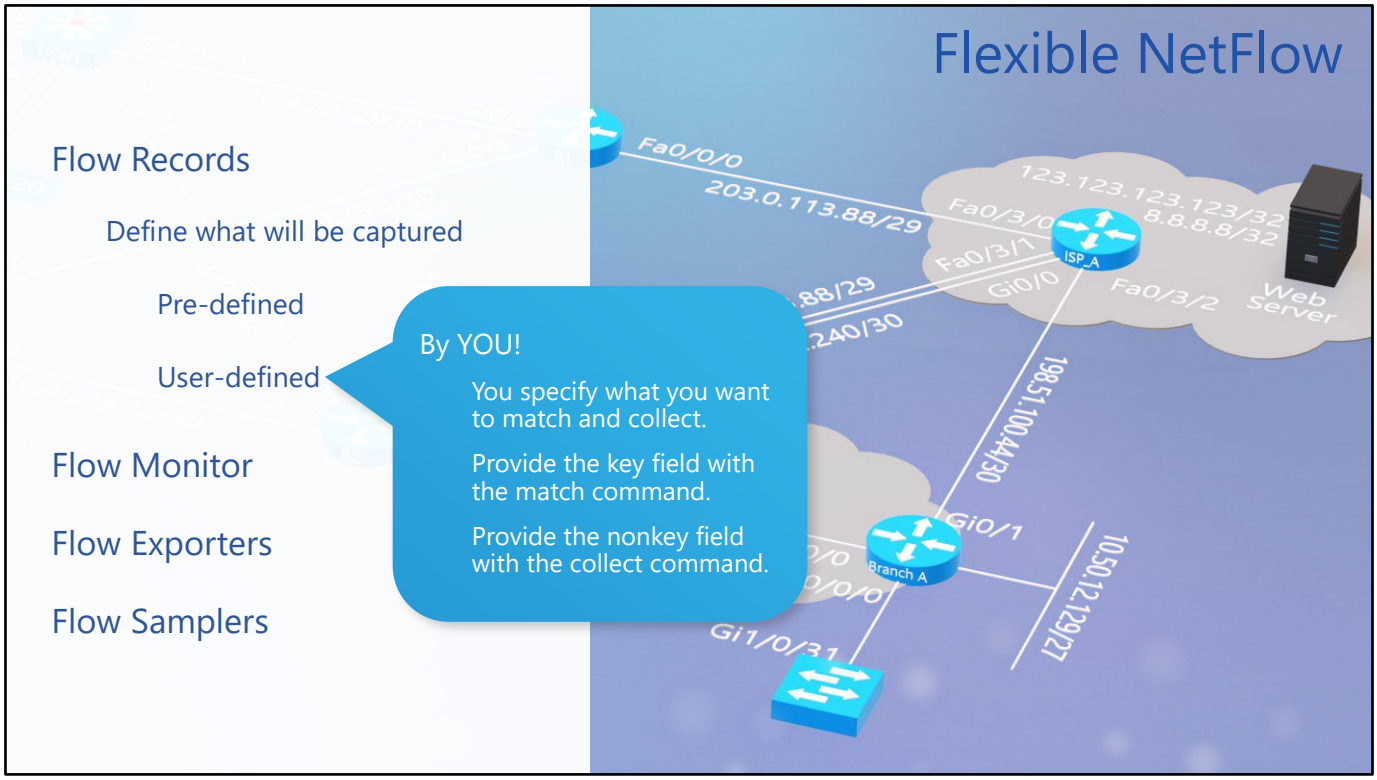
Updated – popular user-defined may eventually become pre-defined.

Examples: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fnetflow/configuration/15-mt/fnf-15-mt-book/fnf-fnetflow.html
Benefits of Flexible NetFlow Predefined Records
NetFlow Original and NetFlow IPv4 Original Input Predefined Records
NetFlow IPv4 Original Output Predefined Record
NetFlow IPv6 Original Input Predefined Record
NetFlow IPv6 Original Output Predefined Record
Autonomous System Predefined Record
Autonomous System ToS Predefined Record
BGP Next-Hop Predefined Record
BGP Next-Hop ToS Predefined Record
Destination Prefix Predefined Record
Destination Prefix ToS Predefined Record
Prefix Predefined Record
Prefix Port Predefined Record
Prefix ToS Predefined Record
Protocol Port Predefined Record

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

[Protocol Port ToS Predefined Record](#)
[Source Prefix Predefined Record](#)
[Source Prefix ToS Predefined Record](#)

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



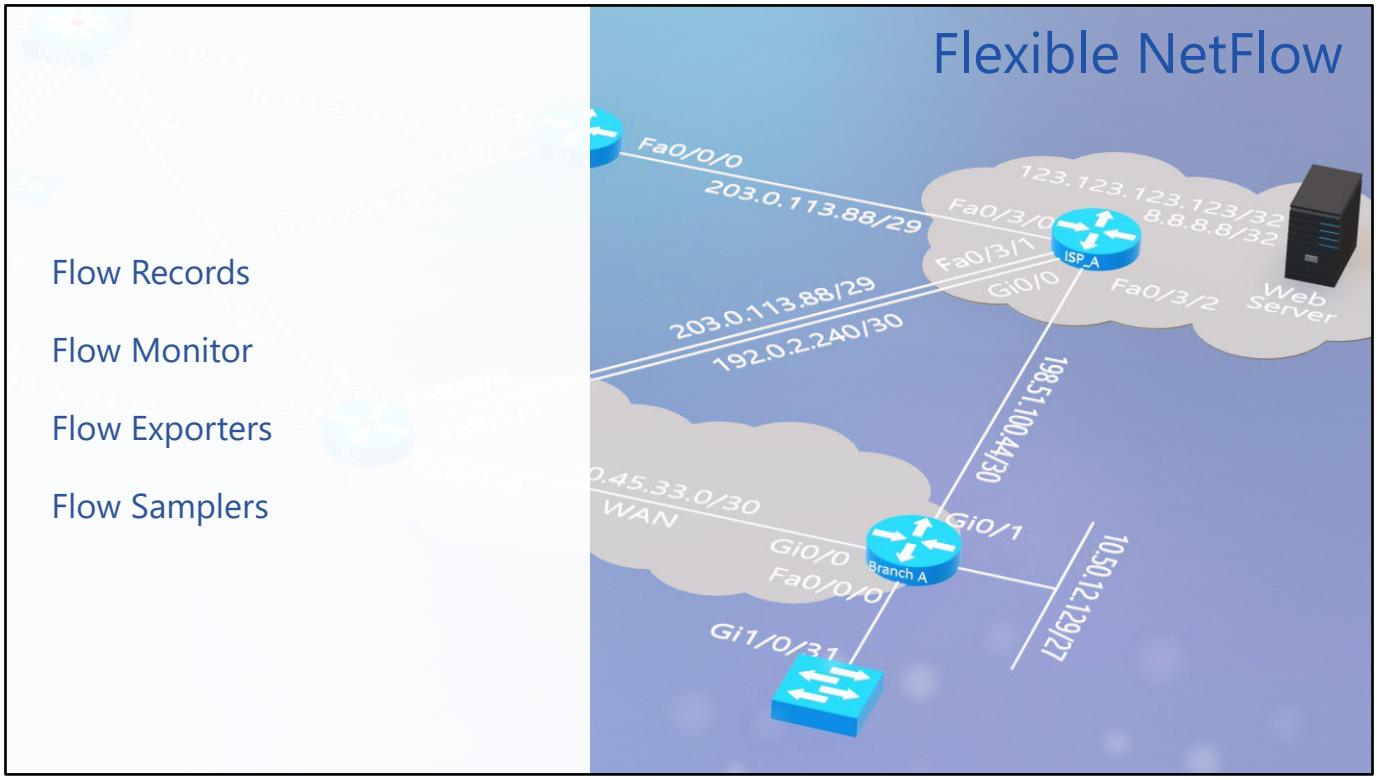
Updated – popular user-defined may eventually become pre-defined.

Examples: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fnetflow/configuration/15-mt/fnf-15-mt-book/fnf-fnetflow.html
Benefits of Flexible NetFlow Predefined Records
NetFlow Original and NetFlow IPv4 Original Input Predefined Records
NetFlow IPv4 Original Output Predefined Record
NetFlow IPv6 Original Input Predefined Record
NetFlow IPv6 Original Output Predefined Record
Autonomous System Predefined Record
Autonomous System ToS Predefined Record
BGP Next-Hop Predefined Record
BGP Next-Hop ToS Predefined Record
Destination Prefix Predefined Record
Destination Prefix ToS Predefined Record
Prefix Predefined Record
Prefix Port Predefined Record
Prefix ToS Predefined Record
Protocol Port Predefined Record

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

[Protocol Port ToS Predefined Record](#)
[Source Prefix Predefined Record](#)
[Source Prefix ToS Predefined Record](#)

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

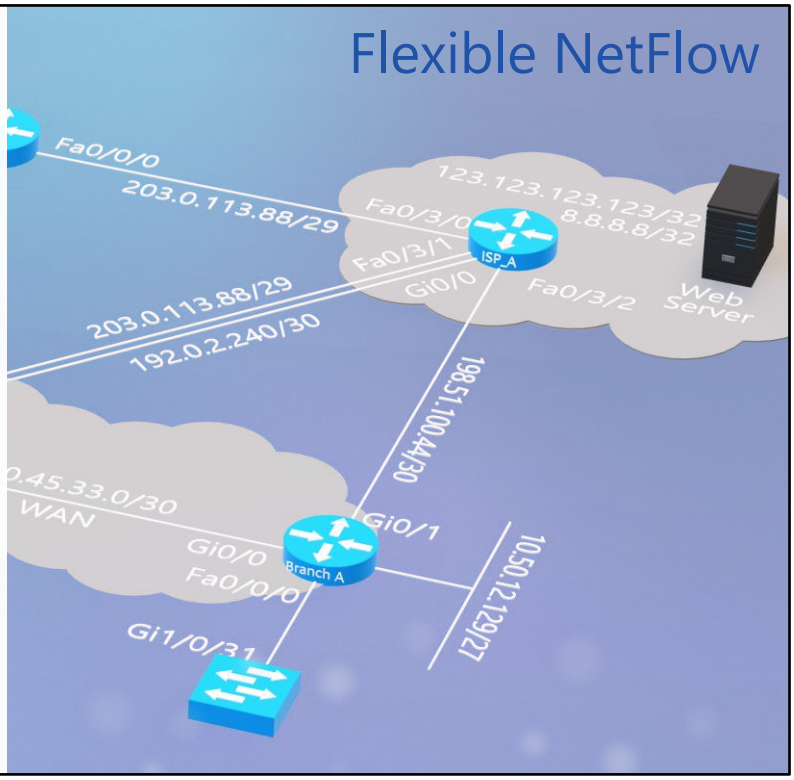


NETFLOW version 2.0 (it is the new version of netflow)

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

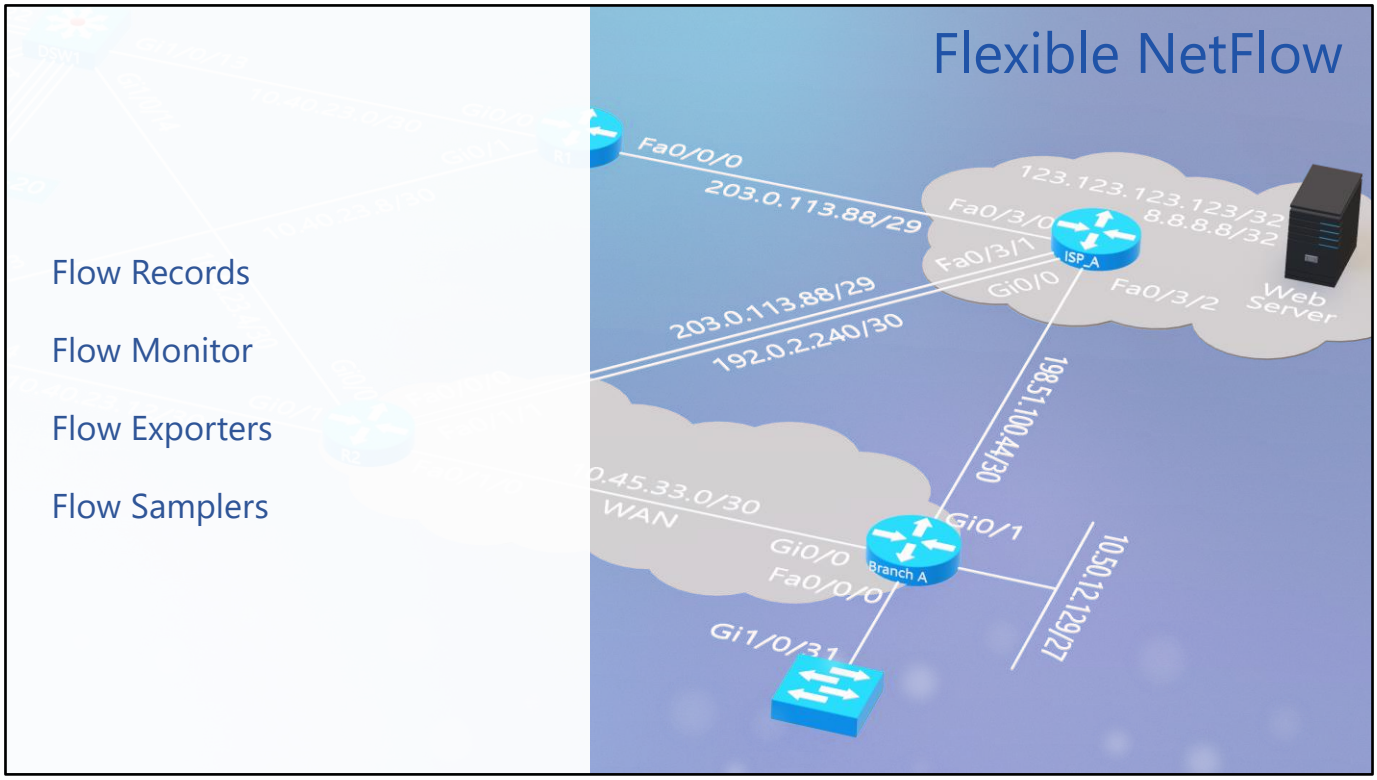
Flexible NetFlow

- Flow Records
- Flow Monitor
  - Performs the monitoring
    - Applied to interface
    - Defines flow record
    - Defines flow exporter
  - Stores results in the flow monitor cache
- Flow Exporters
- Flow Samplers



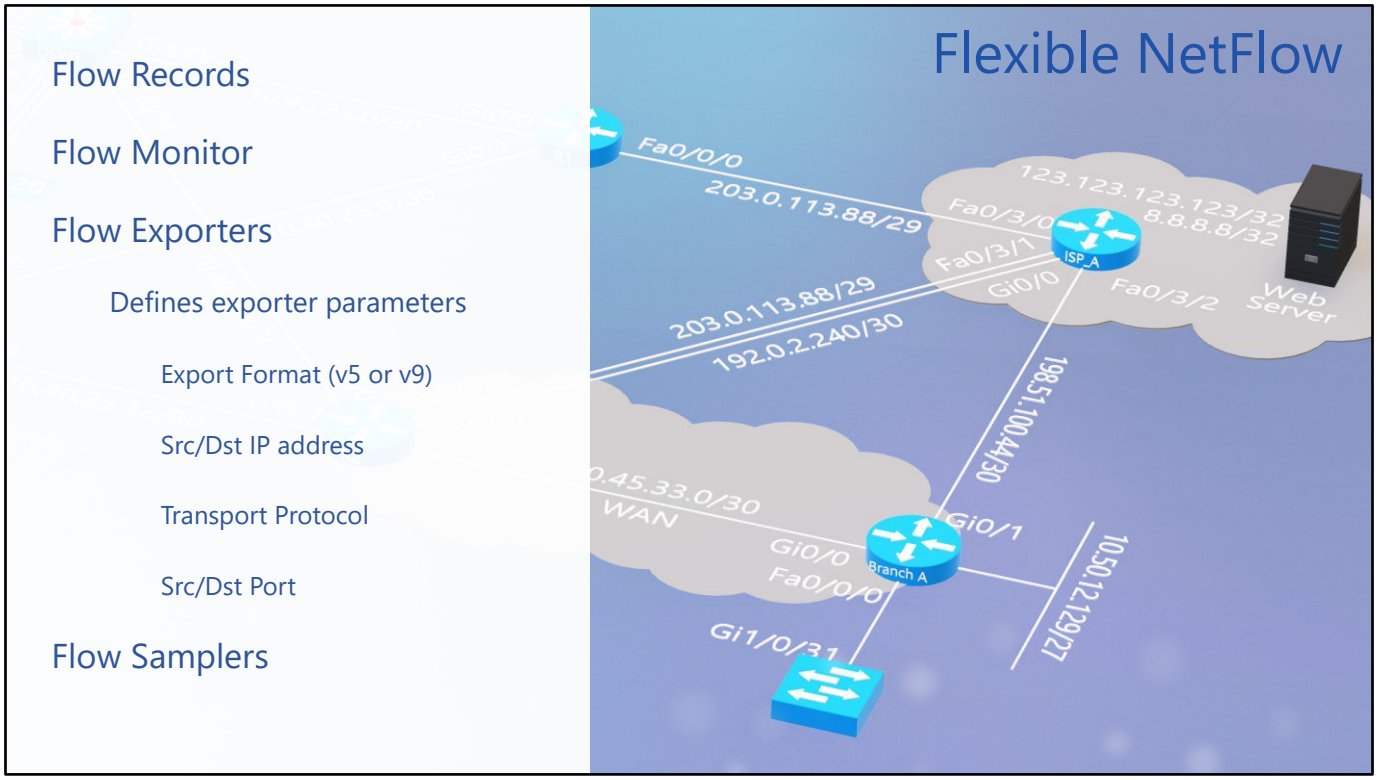
NETFLOW version 2.0 (it is the new version of netflow)

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



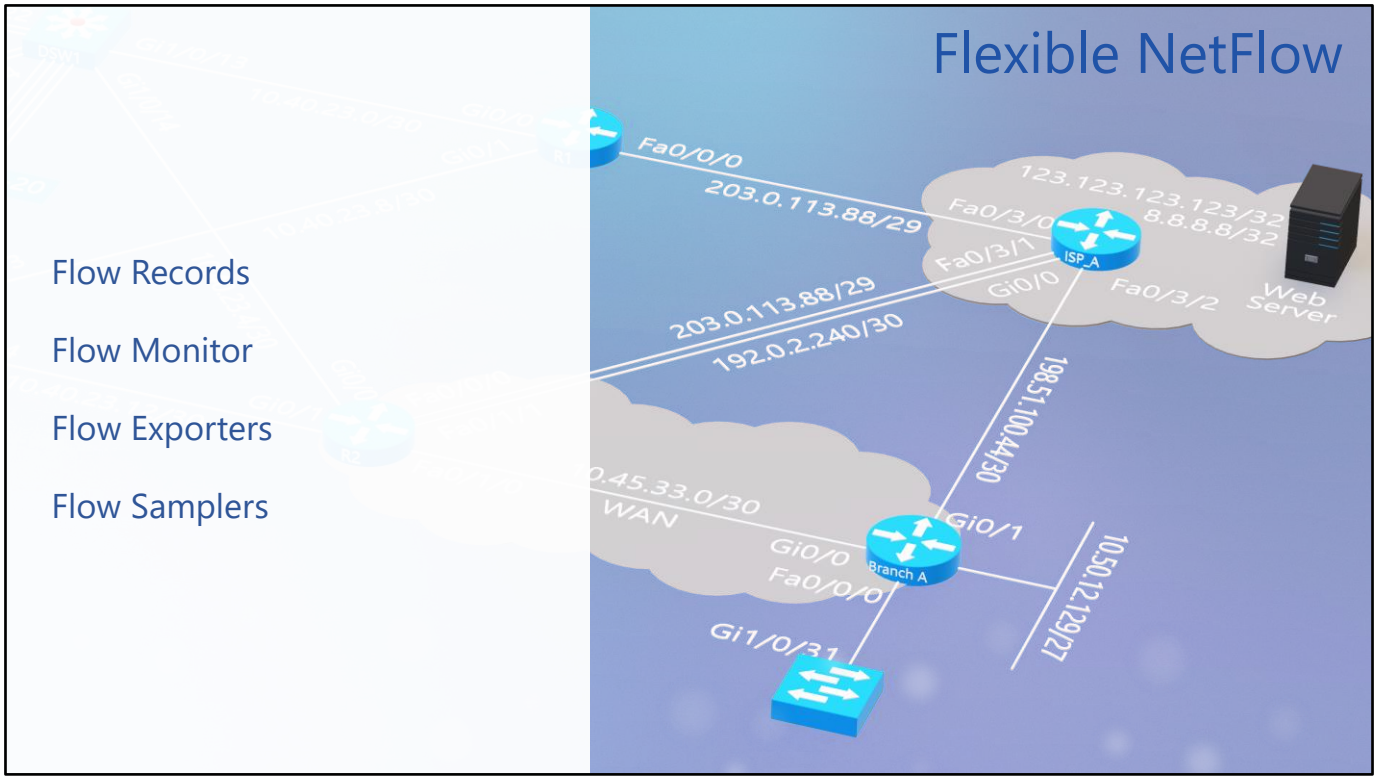
NETFLOW version 2.0 (it is the new version of netflow)

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



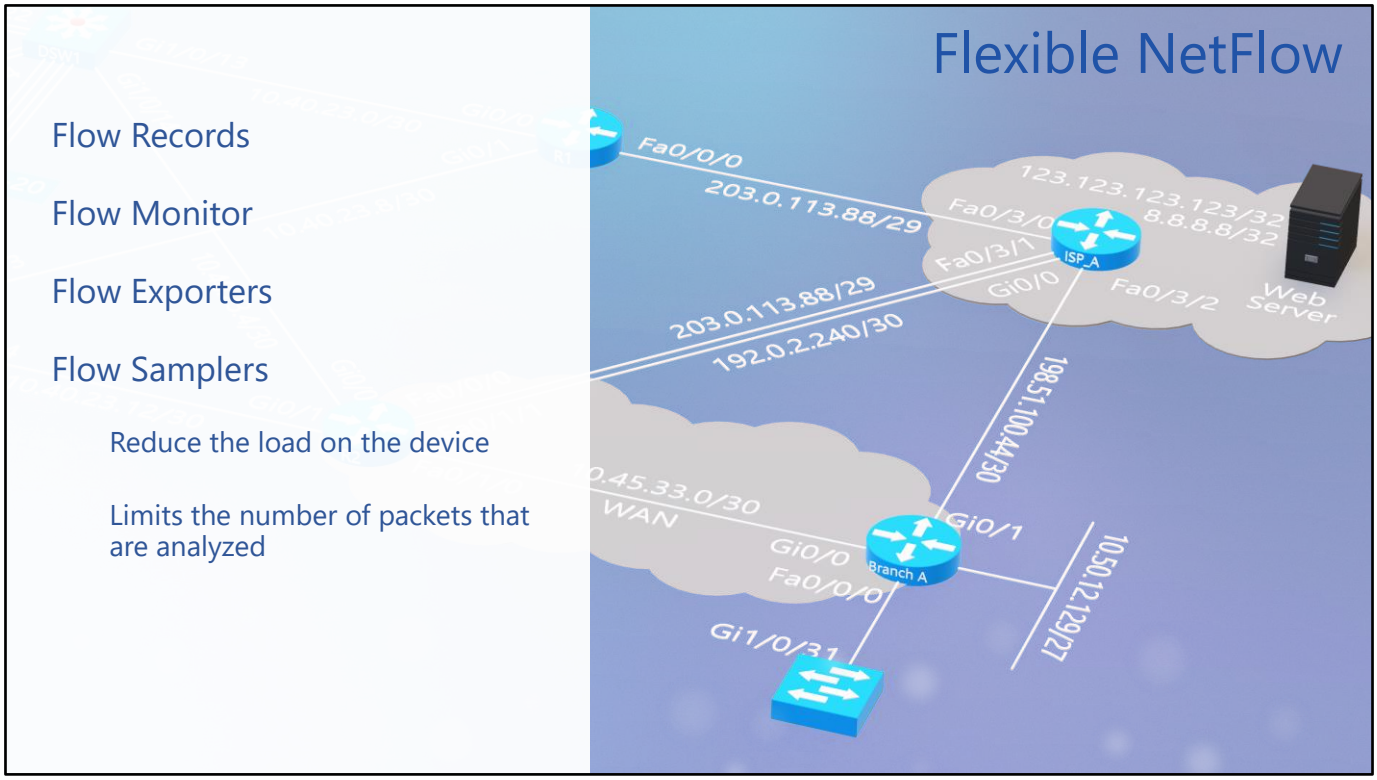
NETFLOW version 2.0 (it is the new version of netflow)

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



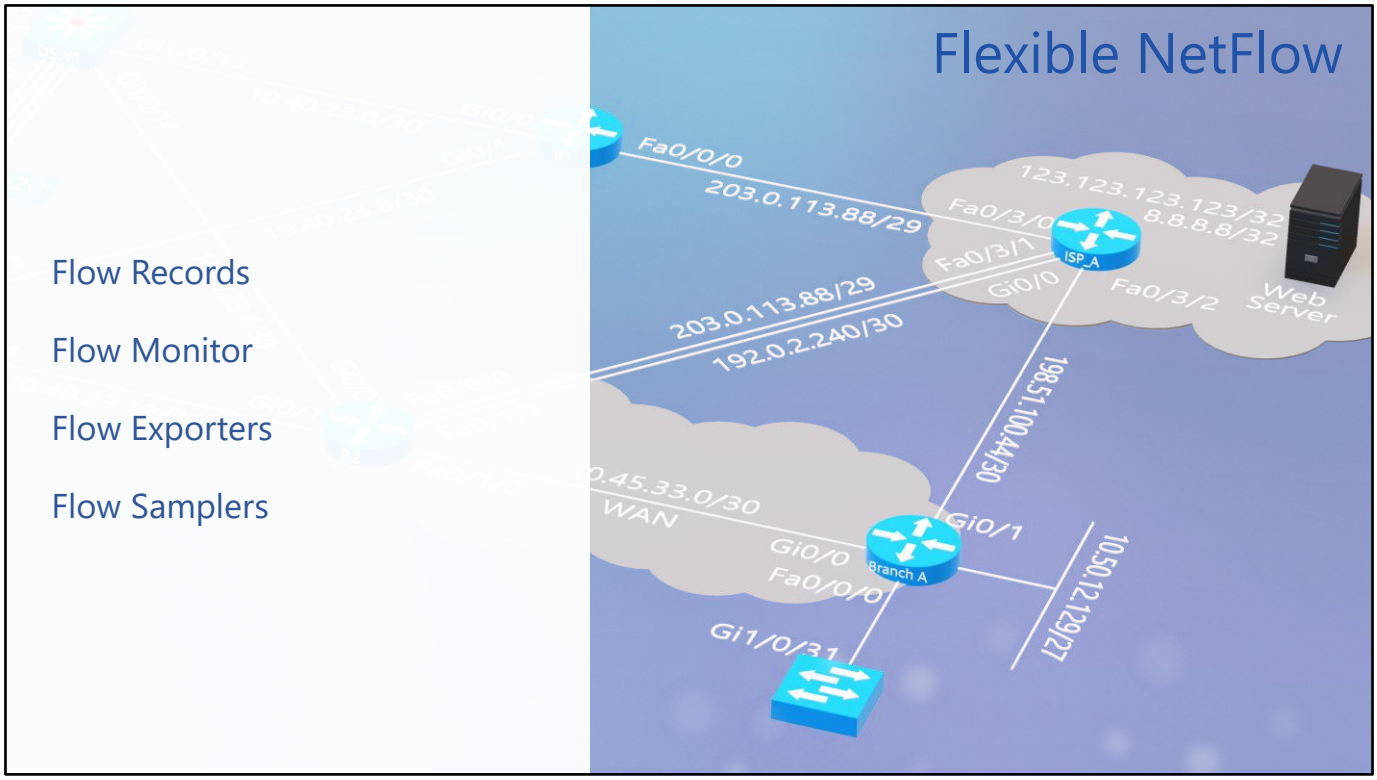
NETFLOW version 2.0 (it is the new version of netflow)

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



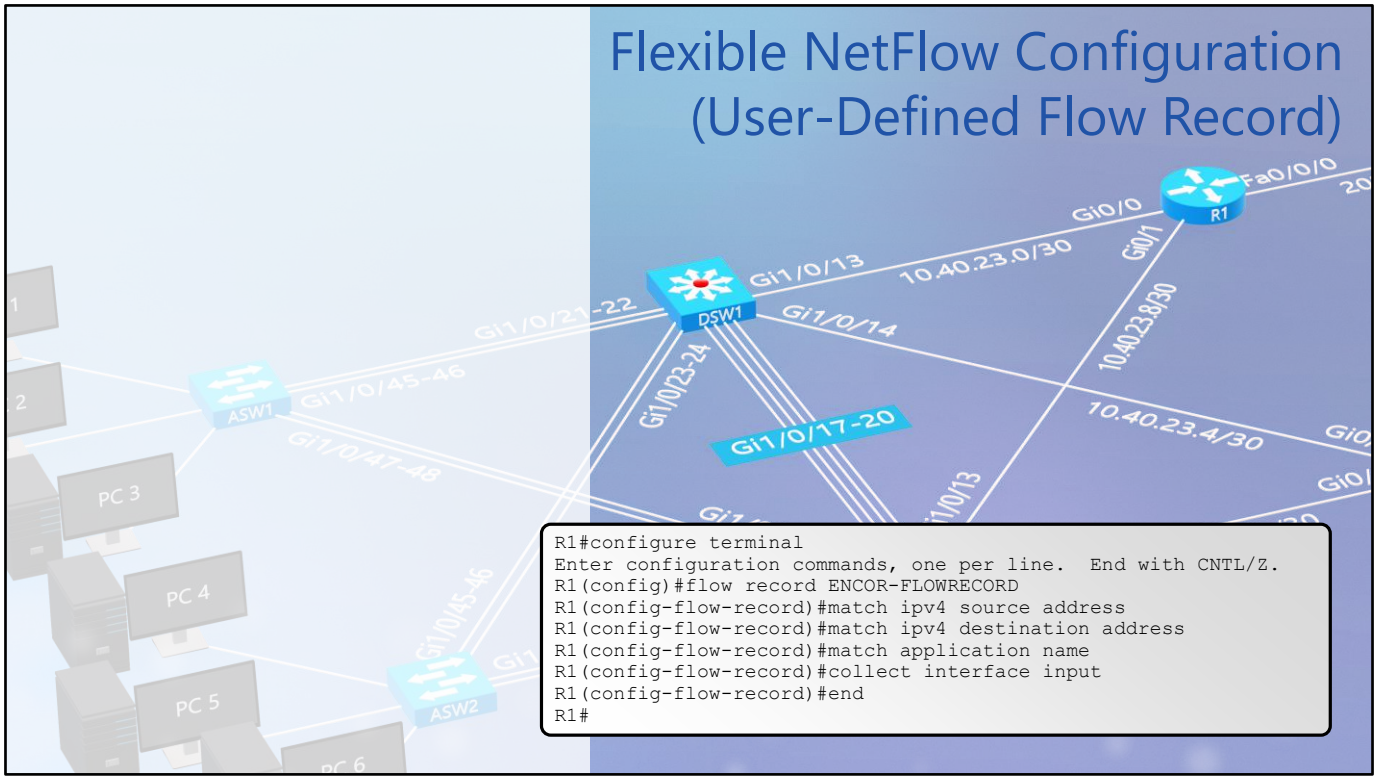
NETFLOW version 2.0 (it is the new version of netflow)

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



NETFLOW version 2.0 (it is the new version of netflow)

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Key field is used to define what is part of the same flow and will be used for collection
Nonkey field is used as just extra information that will be collected as part of that flow

With NETFLOW…. All this is set in stone…. With FLEXIBLE you can define what you want and more.

Captures Flows (traffic from same)

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Source IP address

Destination IP address

Source port number

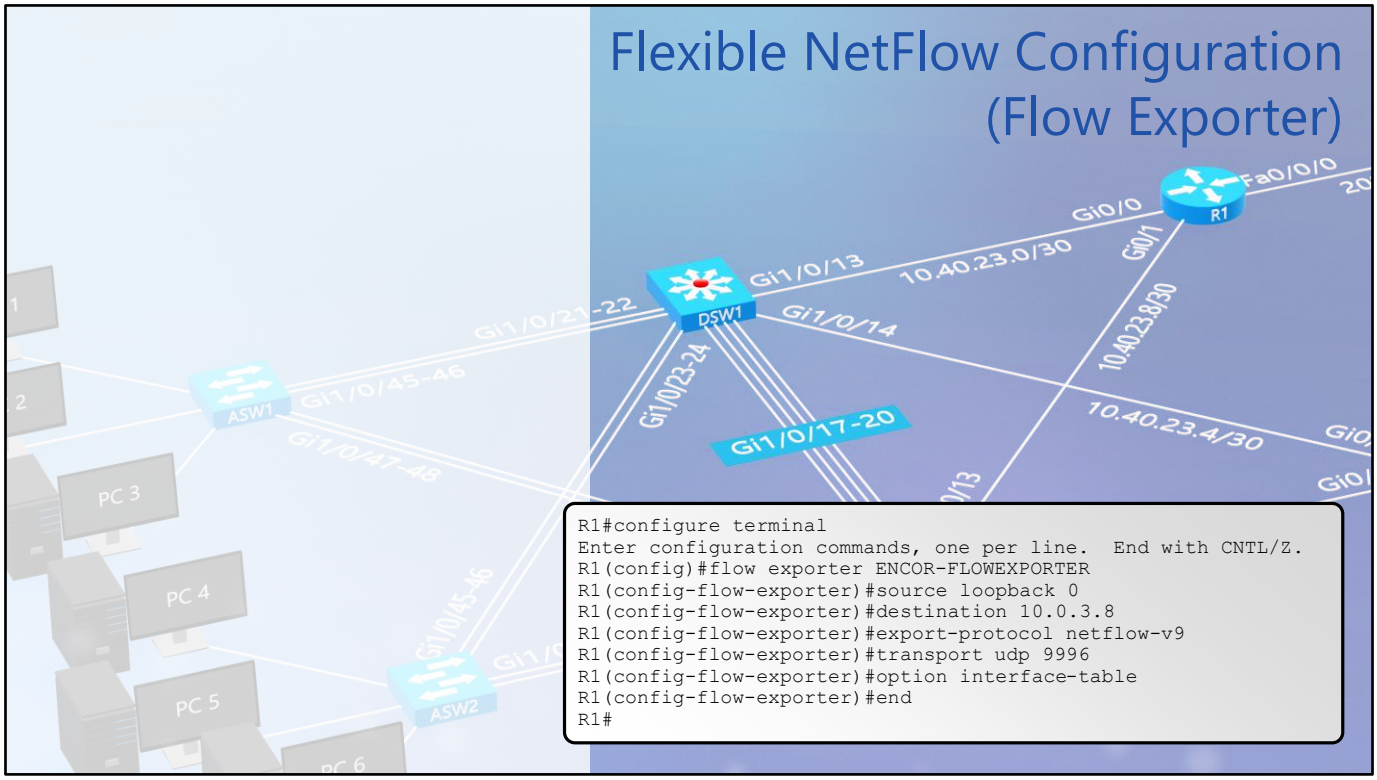
Destination port number

Layer 3 protocol type

Type of service (ToS)

Input logical interface

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



*****EXAM*** how many flow exporters are needed per network device in a flexible netflow configuration?**
*****Exam*** you need to add the SNMP interface table to the NetFlow protocol flow records. Where do you do this???option interface-table** This command causes the periodic sending of an options table, which will allow the collector to map the interface SNMP indexes provided in the flow records to interface names. The optional timeout can alter the frequency at which the reports are sent. **(https://www.cisco.com/c/en/us/td/docs/ios/fnetflow/command/reference/fnf_book/fnf_02.html)**

Flow exporter with dual stack…. Your config can only support an ipv4 or ipv6 stack. So if you have a dual stack scenario you would have to create an exporter for ipv4 and one for ipv6 and then attach them both to your flow monitor.

Either ipv4 or ipv6…. It can't be both. If you try to configure both an IPv4 and IPv6 address in this config the overwrite each other.

So if you have 1 collector that supports both v4 and v6 communication and I wanted to use both v4 and v6…

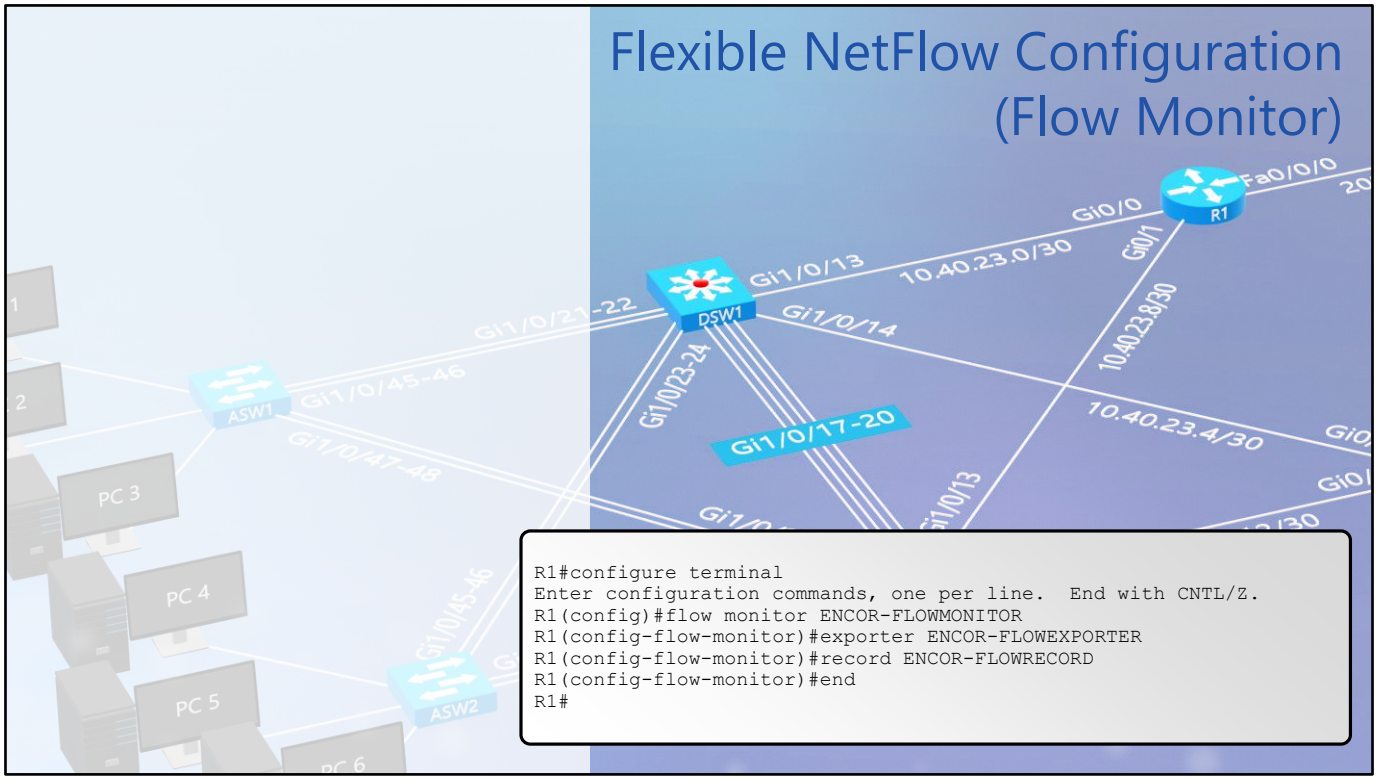
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

So I would need one exporter for v4 configured
And 1 exporter for v6 configured and then in the flow monitor I would have to specify both.

What about redundant v4/v6 collectors. So let's say you have 2 collectors and you needed v4 and v6 configs for both. You would now need 4 exporters 1v4 for the first collector, 1v6 for the first collector, 1v4 for the second collector, and 1v6 for the second collector.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

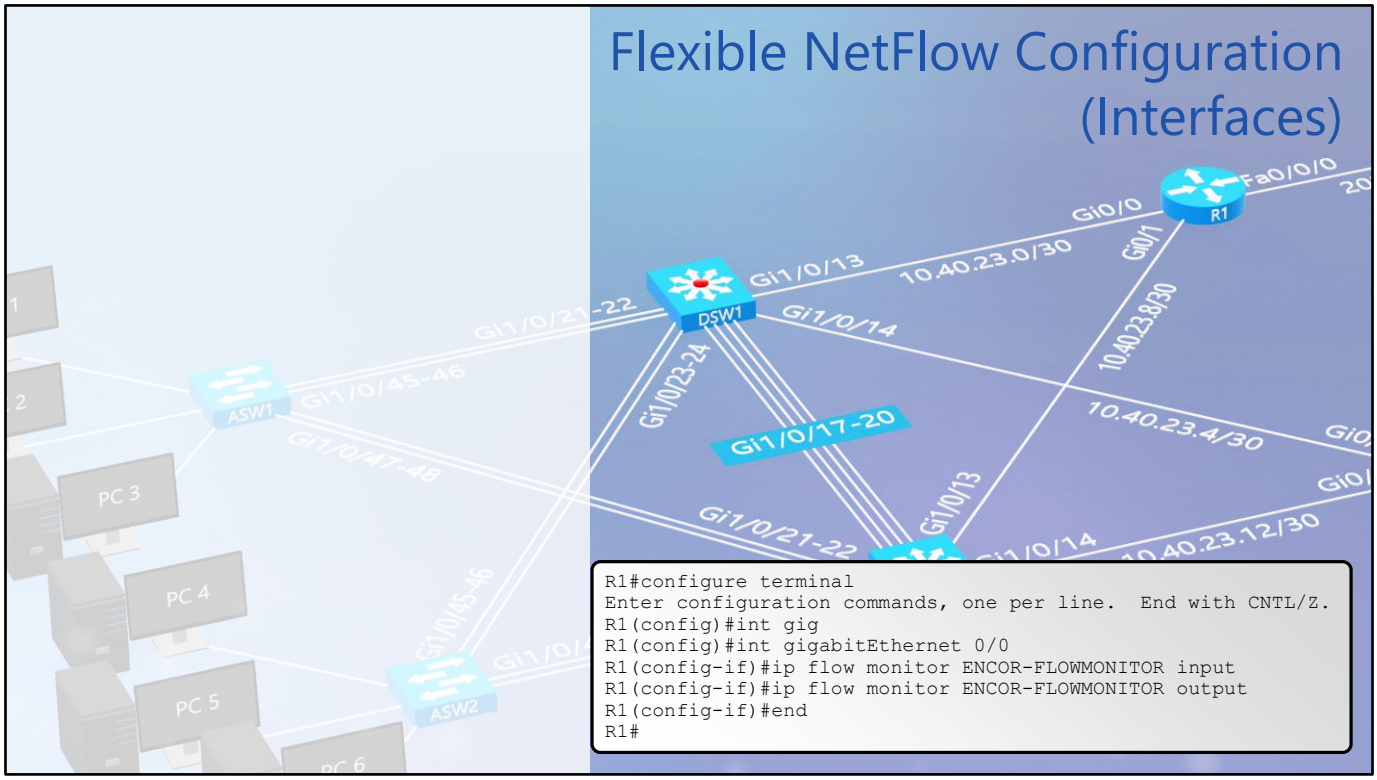
Flexible NetFlow Configuration (Flow Monitor)




```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#flow monitor ENCOR-FLOWMONITOR
R1(config-flow-monitor)#exporter ENCOR-FLOWEXPORTER
R1(config-flow-monitor)#record ENCOR-FLOWRECORD
R1(config-flow-monitor)#end
R1#
```

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

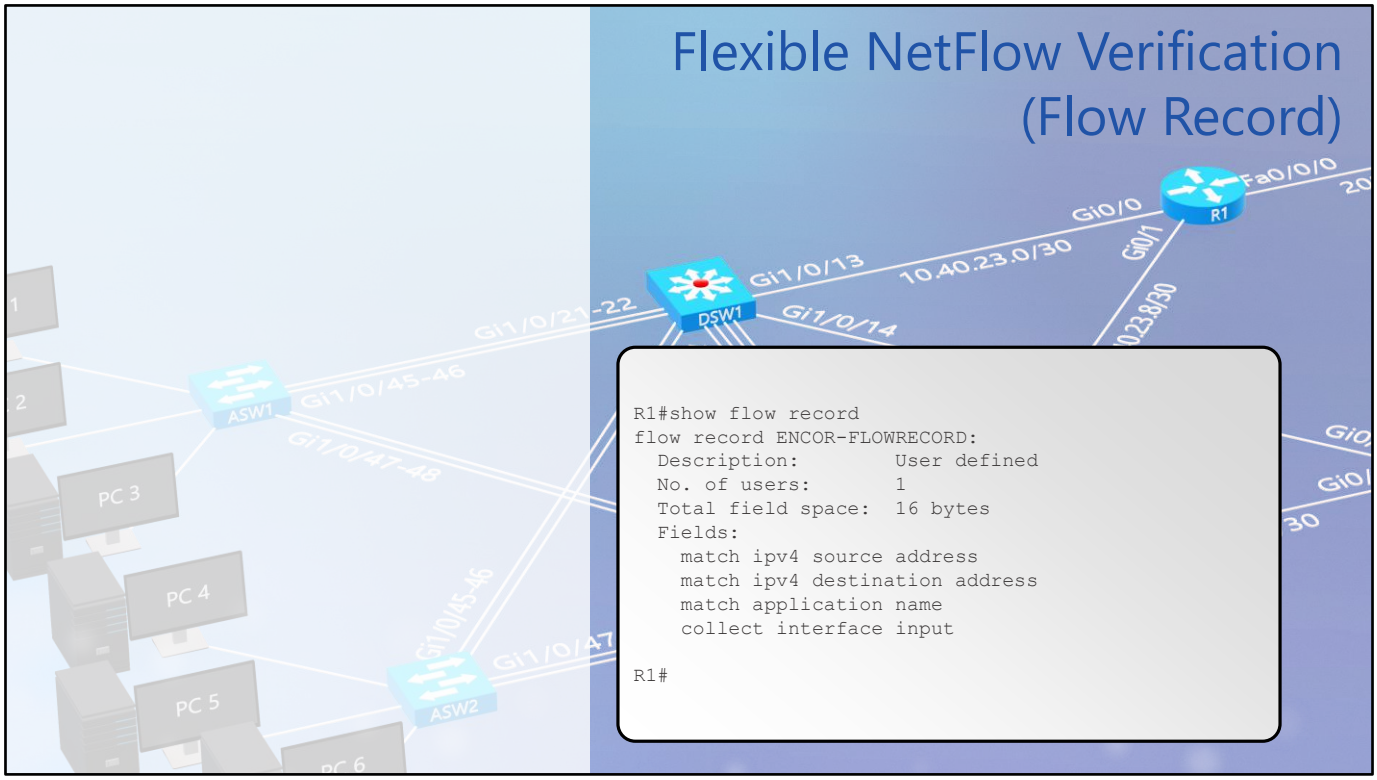
Flexible NetFlow Configuration (Interfaces)




```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int gig
R1(config)#int gigabitEthernet 0/0
R1(config-if)#ip flow monitor ENCOR-FLOWMONITOR input
R1(config-if)#ip flow monitor ENCOR-FLOWMONITOR output
R1(config-if)#end
R1#
```

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Flexible NetFlow Verification (Flow Record)

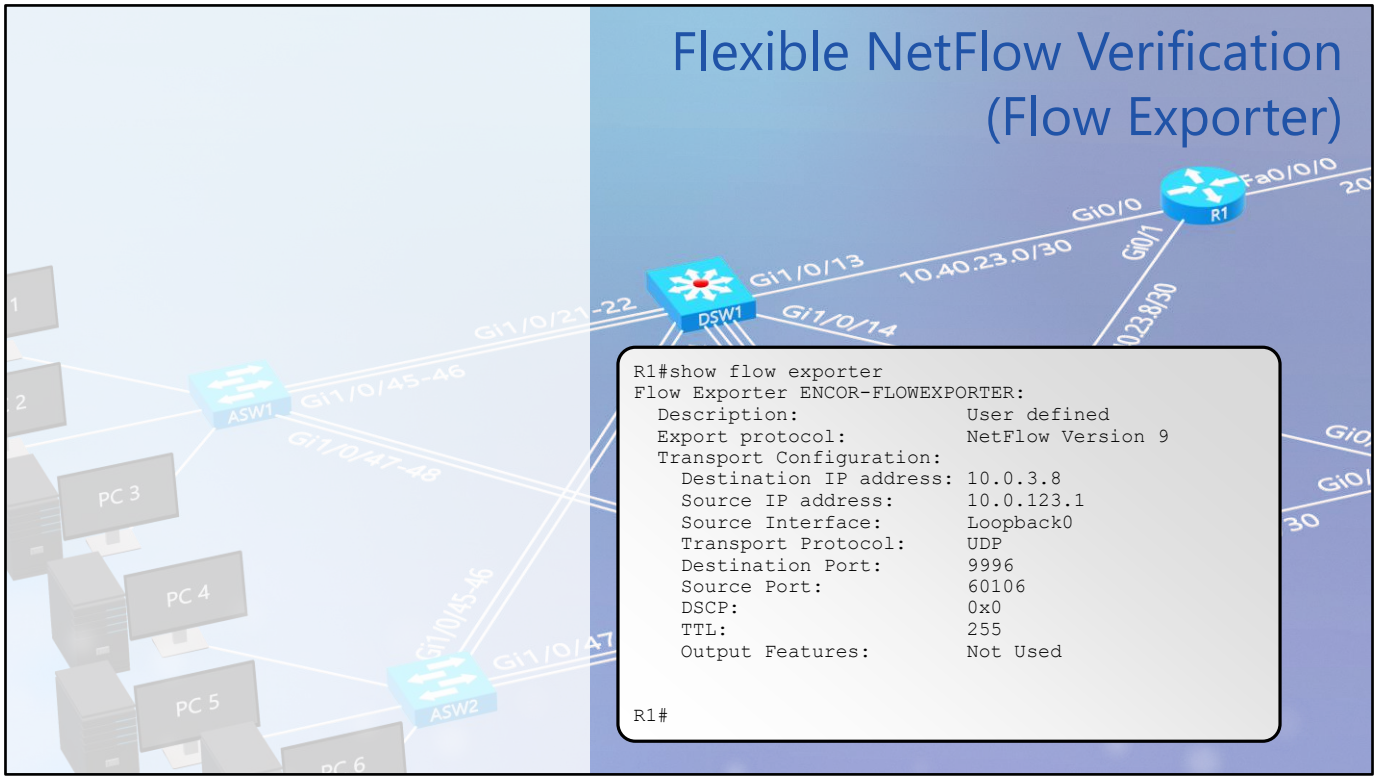



```
R1#show flow record
flow record ENCOR-FLOWRECORD:
  Description:        User defined
  No. of users:       1
  Total field space:  16 bytes
  Fields:
    match ipv4 source address
    match ipv4 destination address
    match application name
    collect interface input

R1#
```

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Flexible NetFlow Verification (Flow Exporter)

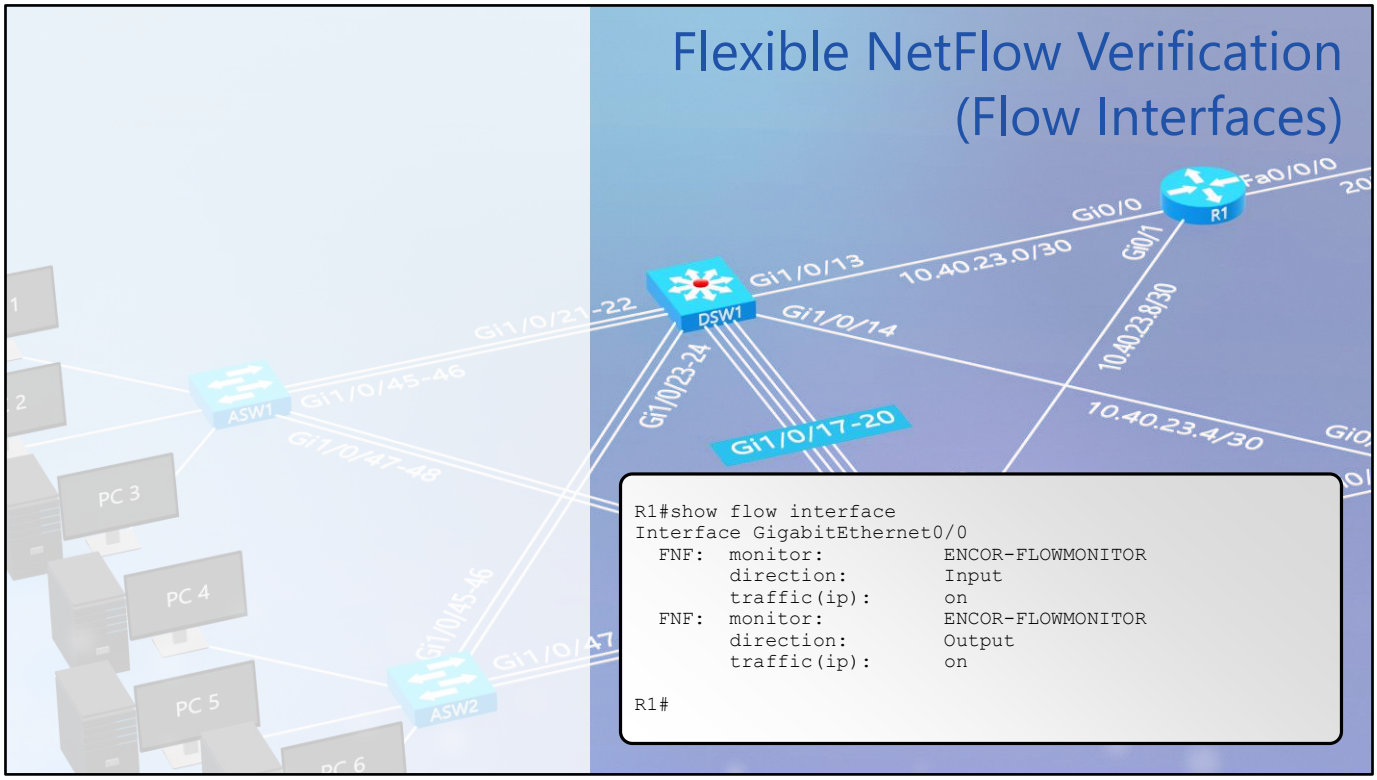



```
R1#show flow exporter
Flow Exporter ENCOR-FLOWEXPORTER:
  Description:               User defined
  Export protocol:           NetFlow Version 9
  Transport Configuration:
    Destination IP address: 10.0.3.8
    Source IP address:       10.0.123.1
    Source Interface:        Loopback0
    Transport Protocol:      UDP
    Destination Port:        9996
    Source Port:             60106
    DSCP:                    0x0
    TTL:                     255
    Output Features:         Not Used


R1#
```

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Flexible NetFlow Verification (Flow Interfaces)

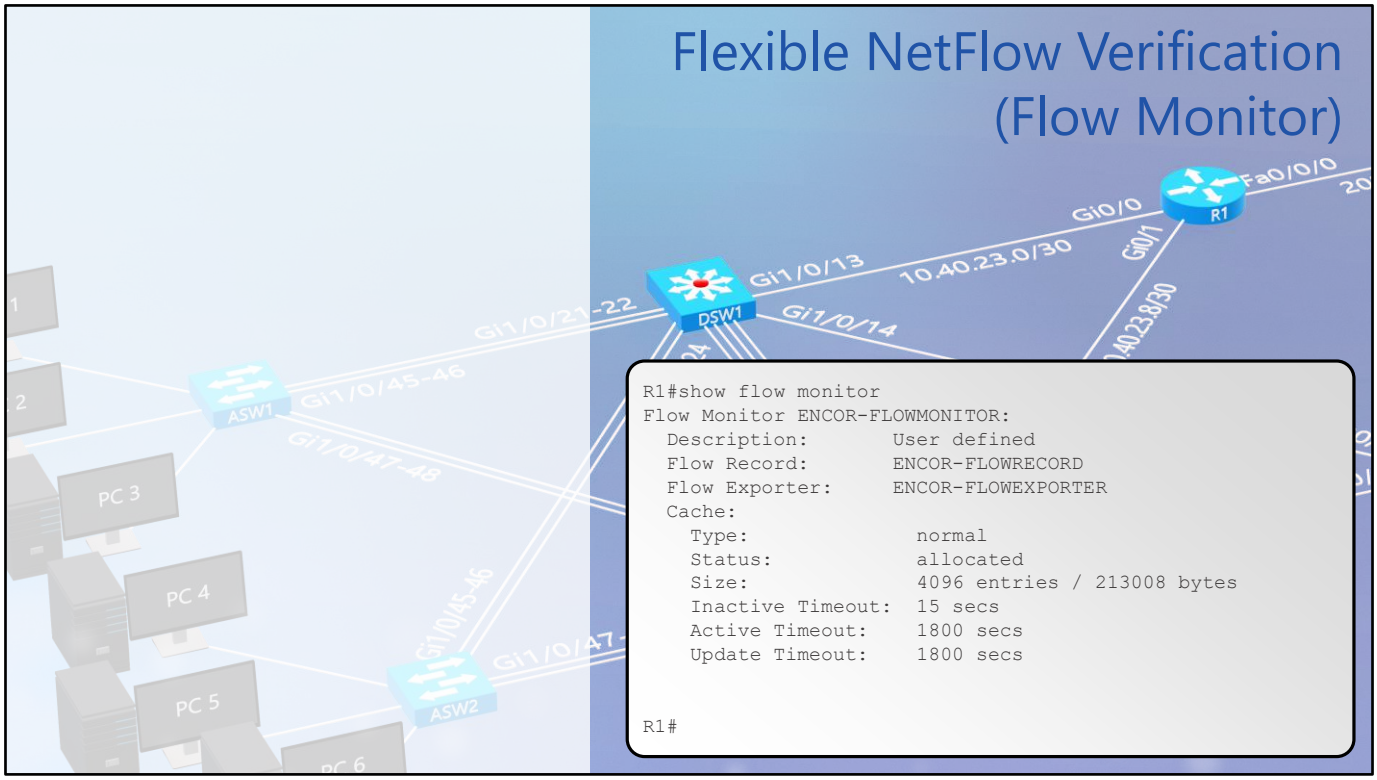



```
R1#show flow interface
Interface GigabitEthernet0/0
  FNF:  monitor:           ENCOR-FLOWMONITOR
        direction:         Input
        traffic(ip):       on
  FNF:  monitor:           ENCOR-FLOWMONITOR
        direction:         Output
        traffic(ip):       on

R1#
```

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Flexible NetFlow Verification (Flow Monitor)




```
R1#show flow monitor
Flow Monitor ENCOR-FLOWMONITOR:
  Description:       User defined
  Flow Record:       ENCOR-FLOWRECORD
  Flow Exporter:     ENCOR-FLOWEXPORTER
  Cache:
    Type:              normal
    Status:            allocated
    Size:              4096 entries / 213008 bytes
    Inactive Timeout:  15 secs
    Active Timeout:    1800 secs
    Update Timeout:    1800 secs


R1#
```

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Flexible NetFlow Verification (Flow Cache)

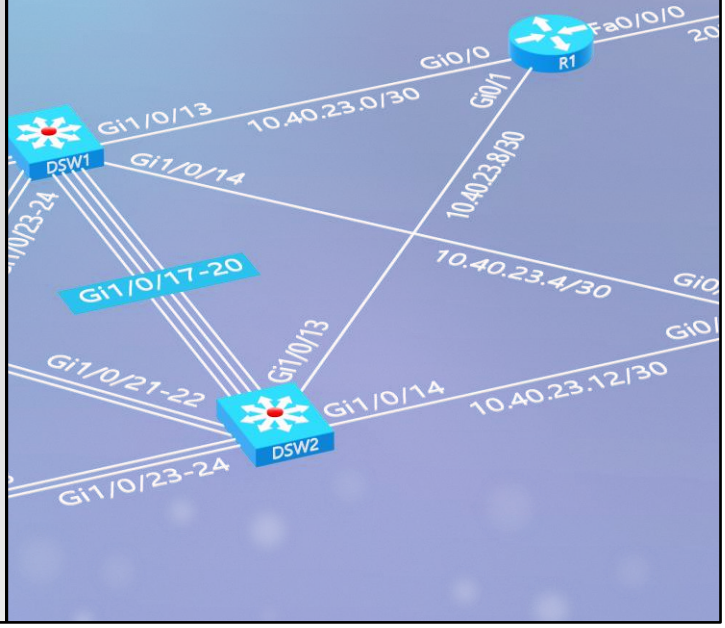
```
R1#show flow monitor name ENCOR-FLOWMONITOR cache
  Cache type:                                Normal
  Cache size:                                  4096
  Current entries:                                4
  High Watermark:                                 5

  Flows added:                                    5
  Flows aged:                                     1
    - Active timeout      (  1800 secs)           0
    - Inactive timeout    (    15 secs)           1
    - Event aged                                  0
    - Watermark aged                              0
    - Emergency aged                              0

IPV4 SOURCE ADDRESS:       10.0.10.2
IPV4 DESTINATION ADDRESS:  224.0.0.10
APPLICATION NAME:          prot eigrp
interface input:           Gi0/0

IPV4 SOURCE ADDRESS:       10.0.10.2
IPV4 DESTINATION ADDRESS:  10.0.12.1
APPLICATION NAME:          prot icmp
interface input:           Gi0/0

IPV4 SOURCE ADDRESS:       10.0.10.2
IPV4 DESTINATION ADDRESS:  192.168.4.4
APPLICATION NAME:          prot icmp
```



It is important to note that flows are temporary on the local Cisco device. If they are not exported to a NetFlow collector, the flows will be removed from the cache at some point to free up resources. Flows are exported to the NetFlow collector only if you set up the device to export the flows and only after the flows expire in the flow cache on the local device.

A flow expires and is exported under the following scenarios:

■ When the flow has been idle or inactive (for 15 seconds by default), it can be removed from the cache and exported.

■ When the flow's max age has been reached (30 minutes by default), known as the active timer, the flow can be removed from the cache and exported.

■ When the cache is full, heuristics are applied to age out older flows immediately, and they are exported.

■ When the TCP connection has been closed (that is, the FIN byte has been seen) or reset (that is, the RST byte has been seen), the flow can be removed from the cache and exported.

If needed, you can modify the expiration settings for the flow monitor in flow monitor configuration mode. Use the **cache entries** command to change the size of the cache if it is filling up too often. Use the **cache timeout active** command to modify the max

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

age of a flow (active timer). Use the c**ache timeout inactive** command to modify the idle (inactive) timer.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

```
  Current entries:                              4
  High Watermark:                               5

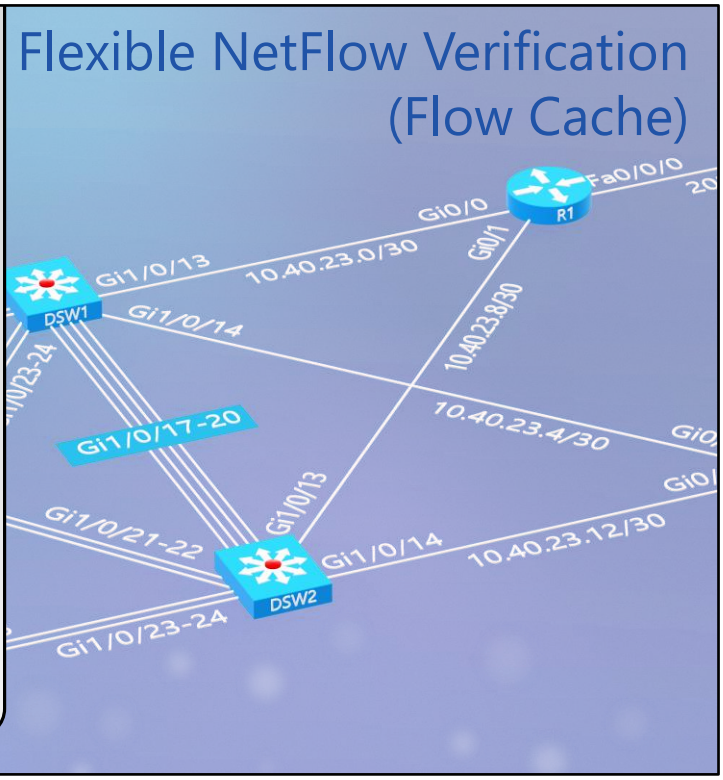
  Flows added:                                  5
  Flows aged:                                   1
    - Active timeout      (  1800 secs)         0
    - Inactive timeout    (    15 secs)         1
    - Event aged                                0
    - Watermark aged                            0
    - Emergency aged                            0

IPV4 SOURCE ADDRESS:        10.0.10.2
IPV4 DESTINATION ADDRESS:   224.0.0.10
APPLICATION NAME:           prot eigrp
interface input:            Gi0/0

IPV4 SOURCE ADDRESS:        10.0.10.2
IPV4 DESTINATION ADDRESS:   10.0.12.1
APPLICATION NAME:           prot icmp
interface input:            Gi0/0

IPV4 SOURCE ADDRESS:        10.0.10.2
IPV4 DESTINATION ADDRESS:   192.168.4.4
APPLICATION NAME:           prot icmp
interface input:            Gi0/0

IPV4 SOURCE ADDRESS:        192.168.4.4
IPV4 DESTINATION ADDRESS:   10.0.10.2
APPLICATION NAME:           prot icmp
interface input:            Gi2/0
```



It is important to note that flows are temporary on the local Cisco device. If they are not exported to a NetFlow collector, the flows will be removed from the cache at some point to free up resources. Flows are exported to the NetFlow collector only if you set up the device to export the flows and only after the flows expire in the flow cache on the local device.

A flow expires and is exported under the following scenarios:

■ When the flow has been idle or inactive (for 15 seconds by default), it can be removed from the cache and exported.

■ When the flow's max age has been reached (30 minutes by default), known as the active timer, the flow can be removed from the cache and exported.

■ When the cache is full, heuristics are applied to age out older flows immediately, and they are exported.

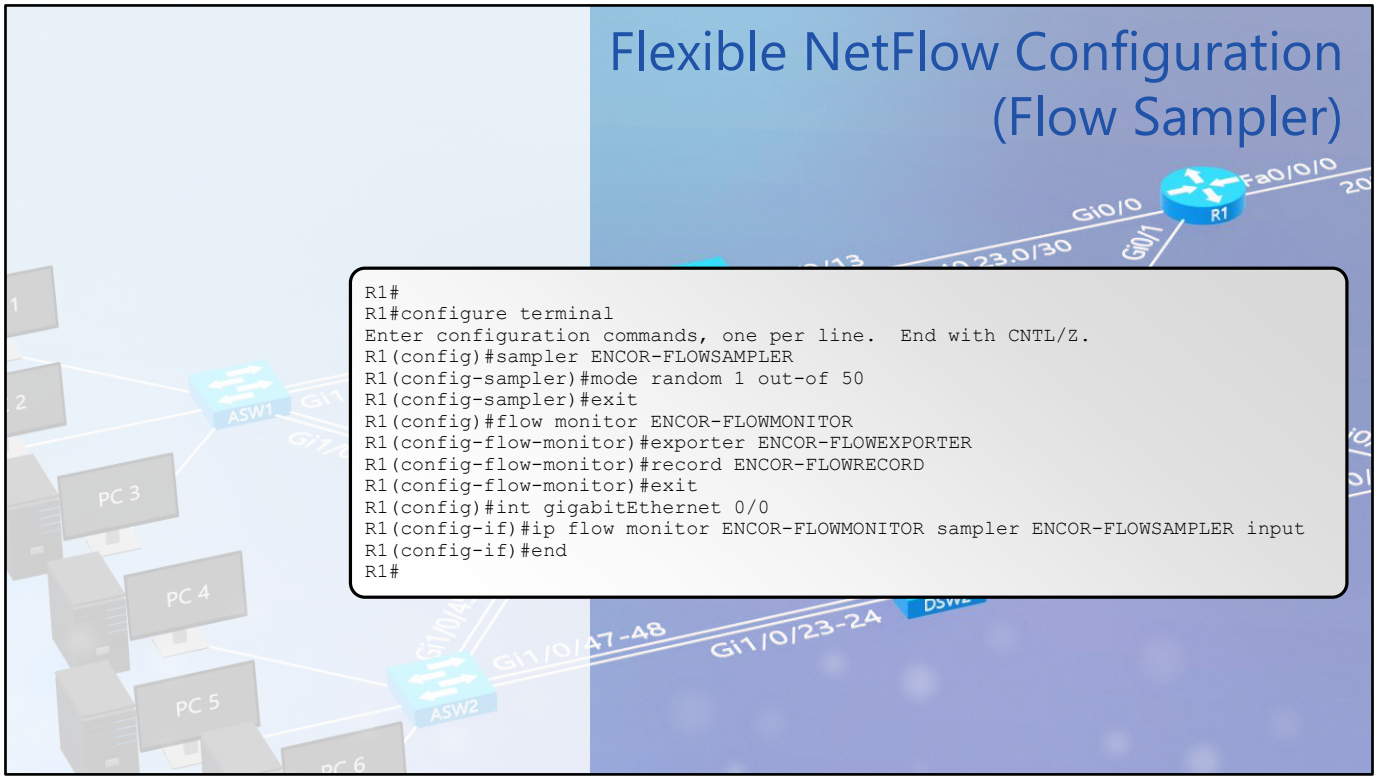
■ When the TCP connection has been closed (that is, the FIN byte has been seen) or reset (that is, the RST byte has been seen), the flow can be removed from the cache and exported.

If needed, you can modify the expiration settings for the flow monitor in flow monitor configuration mode. Use the **cache entries** command to change the size of the cache if it is filling up too often. Use the **cache timeout active** command to modify the max

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

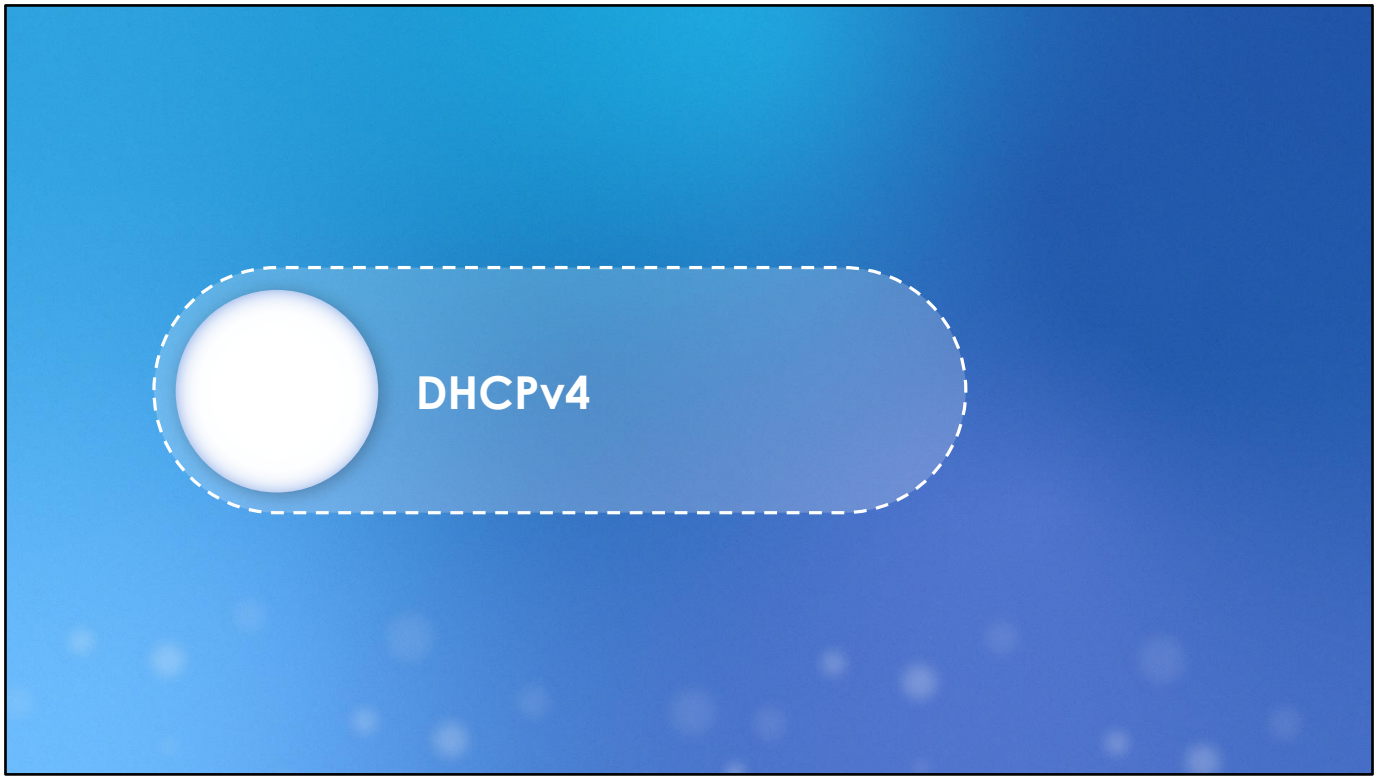
age of a flow (active timer). Use the c**ache timeout inactive** command to modify the idle (inactive) timer.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Exam - configure and apply flow sampler
Exam - flow sampler reduces cpu and memory utilization because the number of packets that are being analyzed are reduced.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Title slide

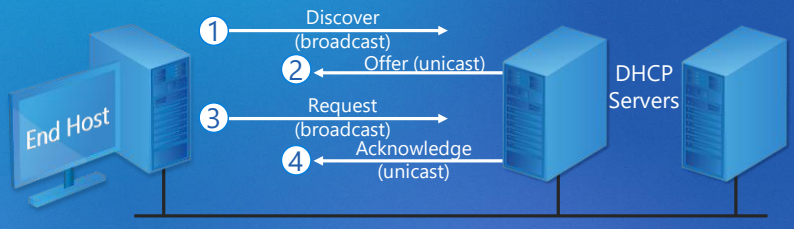
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

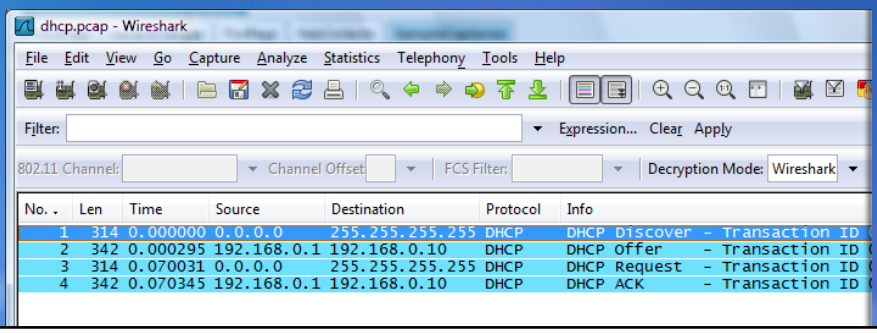


Much better than manual/static configuration of this information.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

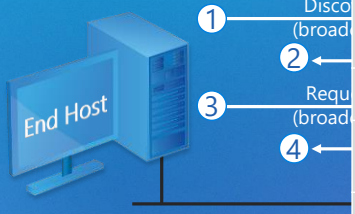
DHCPv4 Communication

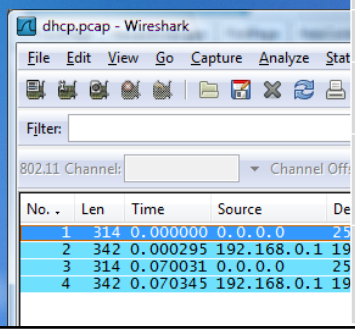




©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

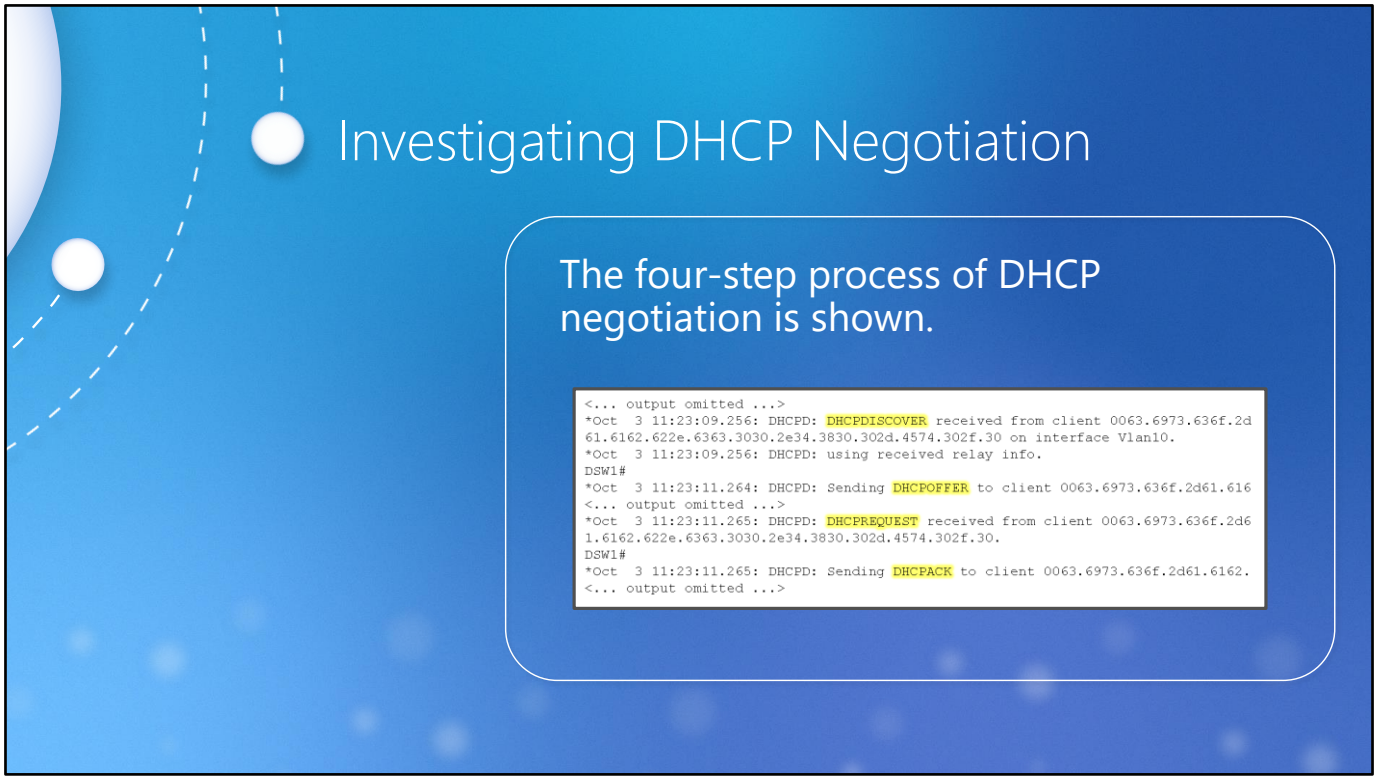
DHCPv4 Communication





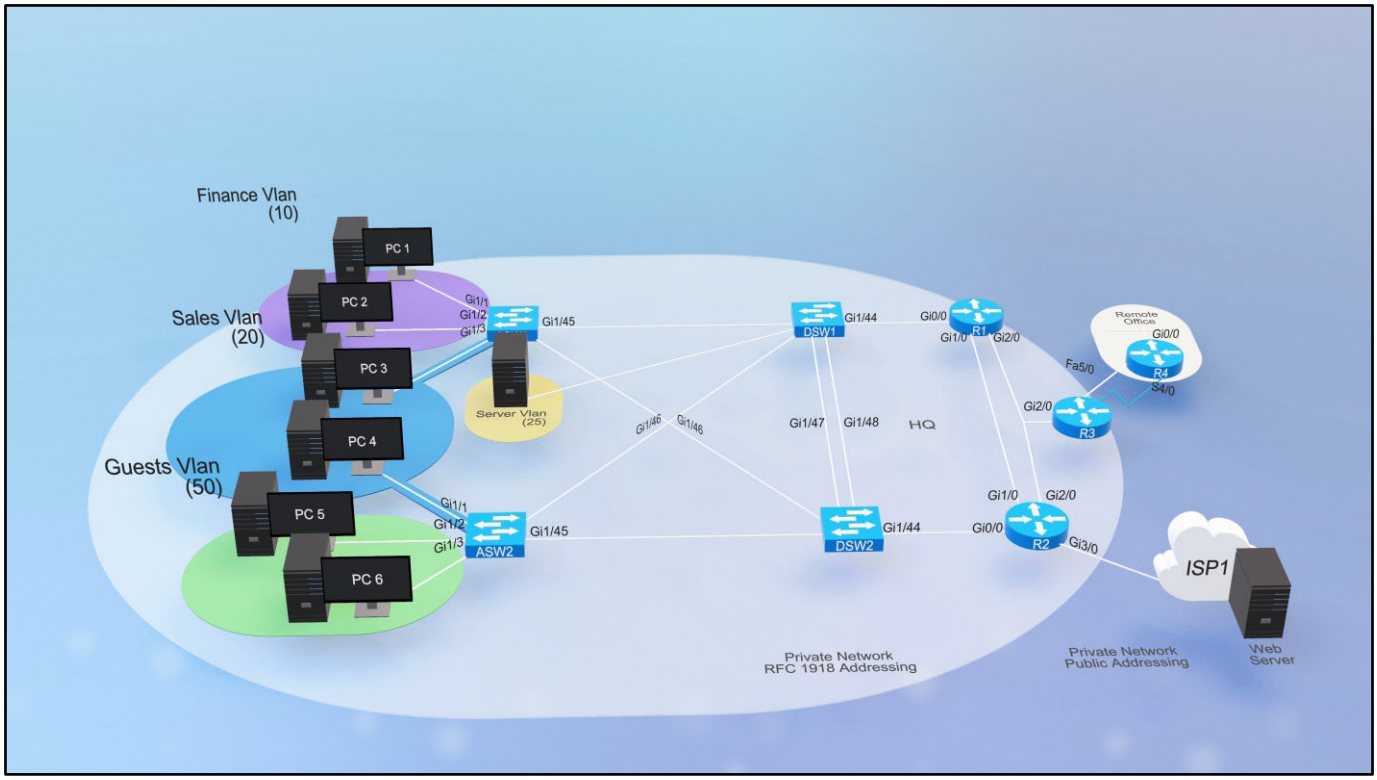
DHCP Message	Description
DHCPDISCOVER	A client sends this message in an attempt to locate a DHCP server. This message is sent to a broadcast IP address of 255.255.255.255 using UDP port 67.
DHCPOFFER	A DHCP server sends this message in response to a DHCPDISCOVER message using UDP port 68.
DHCPREQUEST	This broadcast message is a request from the client to the DHCP server for the IP addressing information and options that were received in the DHCP Offer message.
DHCPDECLINE	This message is sent from a client to a DHCP server to inform the server that an IP address is already in use on the network.
DHCPACK	A DHCP server sends this message to a client and includes IP configuration parameters.
DHCPNAK	A DHCP server sends this message to a client and informs the client that the DHCP server declines to provide the client with the requested IP configuration information.
DHCPRELEASE	A client sends this message to a DHCP server and informs the DHCP server that the client has released its DHCP lease, thus allowing the DHCP server to reassign the client IP address to another client.
DHCPINFORM	This message is sent from a client to a DHCP server and requests IP configuration parameters. Such a message might be sent from an access server requesting IP configuration information for a remote client attaching to the access server.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



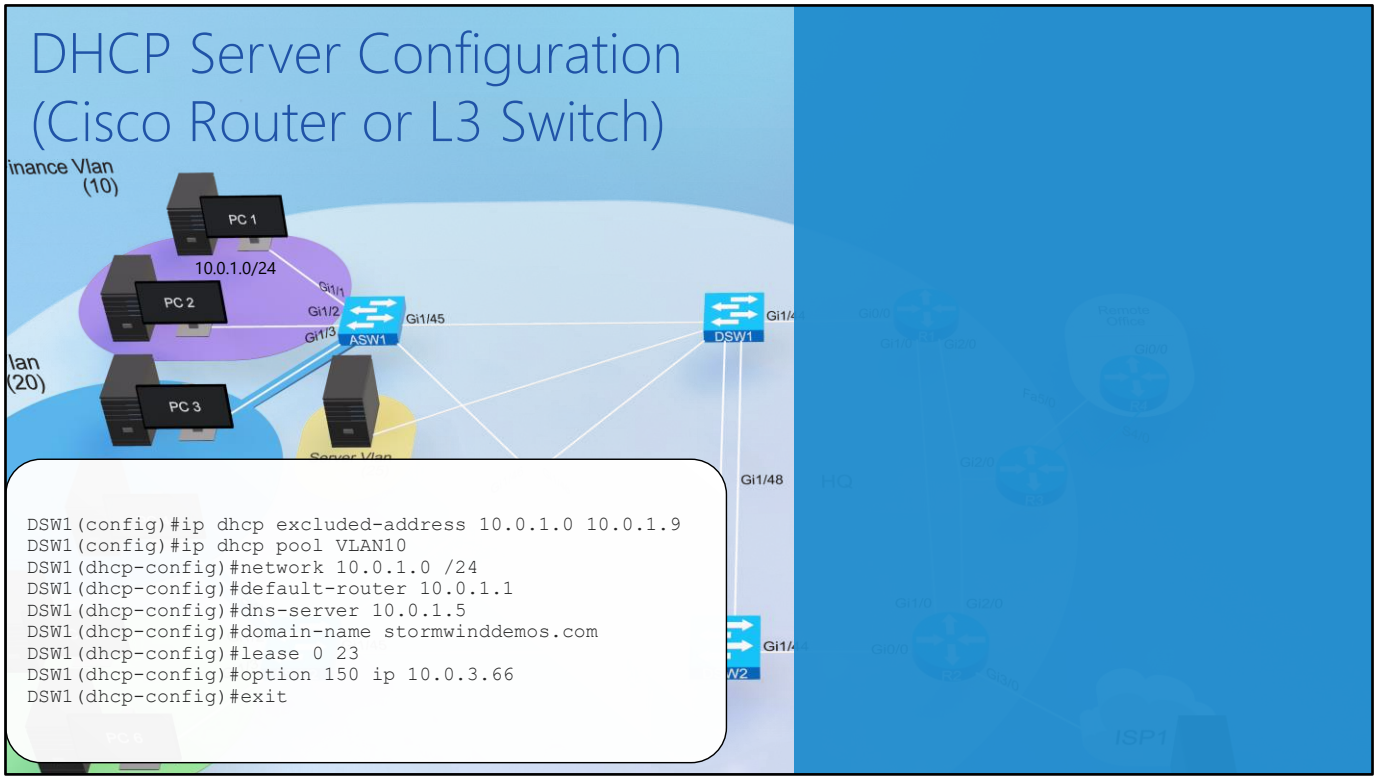
Debug dhcp packet

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



The need for VLANs

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Option 150 is cisco proprietary and option 66 is the IEEE standard for the same thing. IP address of a TFTP server. Great for phones so that they can download their configuration files from a TFTP server.

EXAM
How many addresses does this config support?
254

What would happen if you had 300 users that needed an address all at the same time?
Exhaustion and 46 users would not get an address

What would happen if you had 300 users that need access at different times of the day for only 2hrs each?
Exhaustion because the lease is 23 hrs. Even when the devices are not connected the address is still reserved for them.
However, if you reduce the lease time to let's say 2 hrs you could over subscribe the pool in this case because after two hrs addresses are available again.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

DHCP Options

Carry advanced configuration parameters and control information

Option 43: inform a lightweight AP where the WLC is located or tell a device where the Cisco DNA Center is

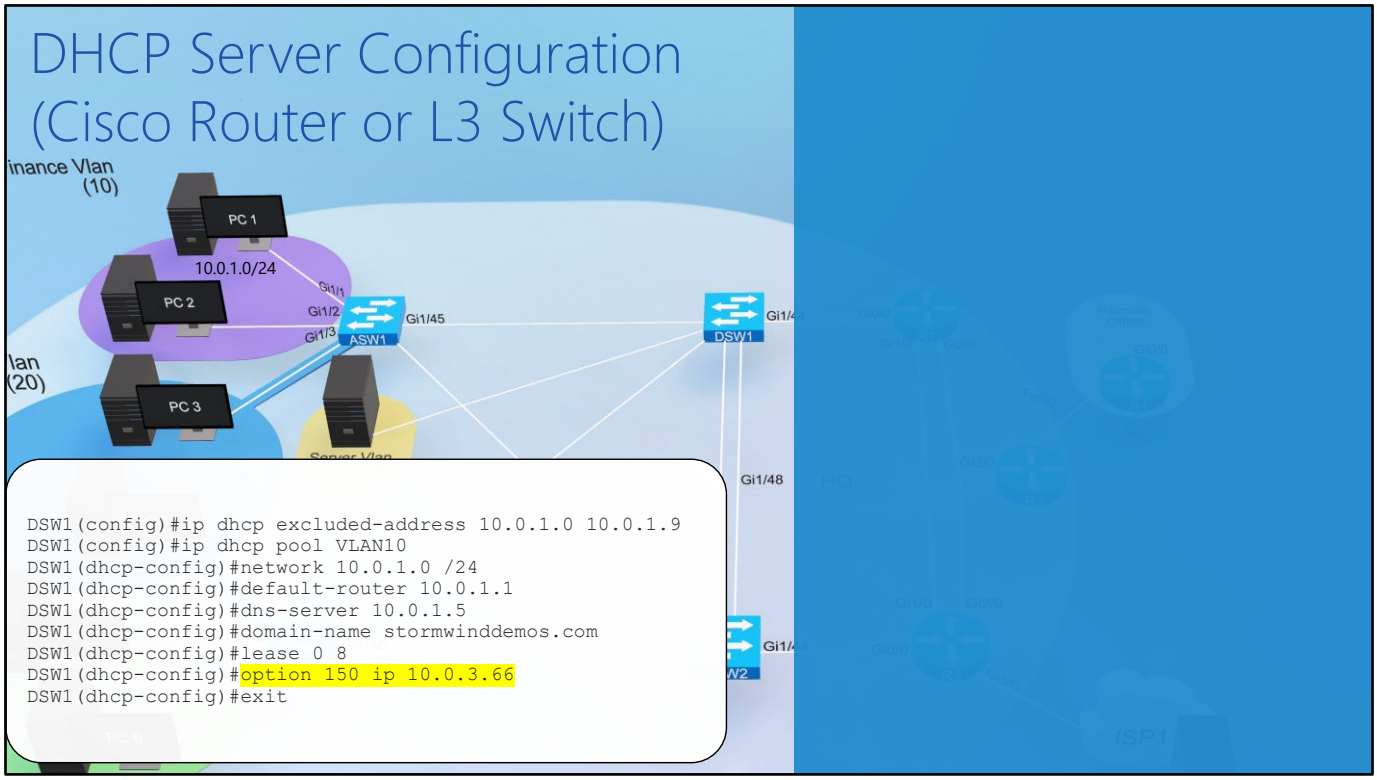
Option 69: notify a client which SMTP server to use

Option 70: notify a client which POP3 server to use

Option 150: notify IP phones which TFTP server to download a configuration file from

43 is a vendor specific option that can be used for want ever you need.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Option 150 is cisco proprietary and option 66 is the IEEE standard for the same thing. IP address of a TFTP server. Great for phones so that they can download their configuration files from a TFTP server.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

DHCP Server Configuration (Cisco Router or L3 Switch)




```
C:\PC1>ipconfig /all

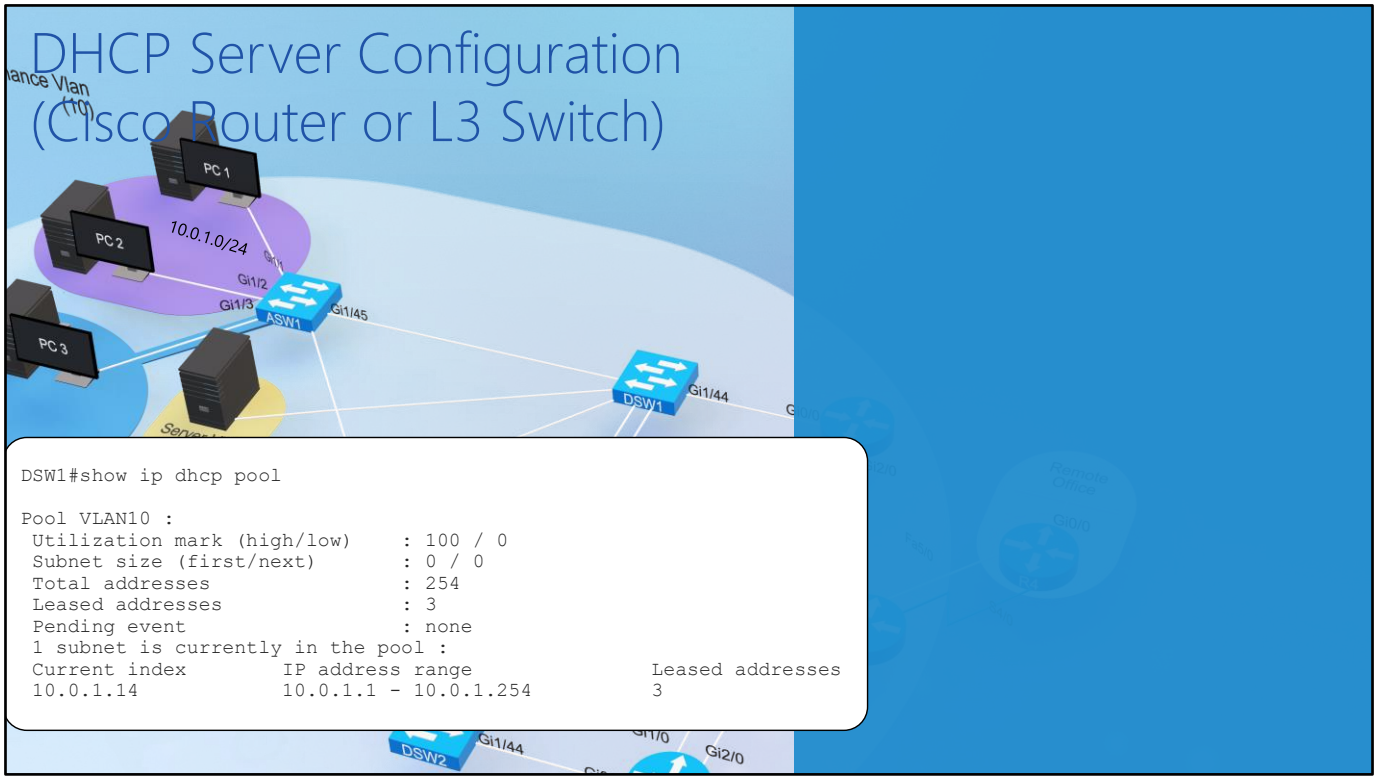
Windows IP Configuration

Ethernet adapter PC1:

   Connection-specific DNS Suffix  . : stormwinddemos.com
   Description . . . . . . . . . . . : Intel(R) PRO/1000 MT Desktop Adapter #2
   Physical Address. . . . . . . . . : 08-00-27-38-00-11
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::d0f1:42c9:dcdb:ef43%7(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.0.1.13(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Friday, April 19, 2019 4:35:43 AM
   Lease Expires . . . . . . . . . . : Friday, April 19, 2019 12:35:43 PM
   Default Gateway . . . . . . . . . : 10.0.1.1
   DHCP Server . . . . . . . . . . . : 10.0.1.1
   DHCPv6 IAID . . . . . . . . . . . : 302514215
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-24-41-0D-94-08-00-27-14-A8-FB
   DNS Servers . . . . . . . . . . . : 10.0.1.5
```

Option 150 is cisco proprietary and option 66 is the IEEE standard for the same thing. IP address of a TFTP server. Great for phones so that they can download their configuration files from a TFTP server.

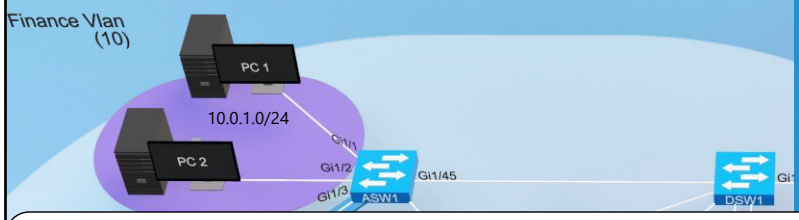
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Option 150 is cisco proprietary and option 66 is the IEEE standard for the same thing. IP address of a TFTP server. Great for phones so that they can download their configuration files from a TFTP server.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

DHCP Server Configuration (Cisco Router or L3 Switch)




```
DSW1#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
10.0.1.11           0100.e04c.6985.d0       Apr 19 2019 07:37 AM    Automatic
10.0.1.12           0100.e04c.6987.25       Apr 19 2019 07:38 AM    Automatic
10.0.1.13           0108.0027.3800.11       Apr 19 2019 07:42 AM    Automatic
```

```
DSW1#show ip dhcp conflict
IP address        Detection method   Detection time          VRF
10.0.1.10         Ping               Apr 18 2019 11:37 PM
```

01 in client ID means the client is using ethernet.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

DHCP Relay Agent

A centralized DHCP solution provides several benefits:

Ensuring consistency to avoid errors

Managing a single DHCP server across multiple locations can reduce time

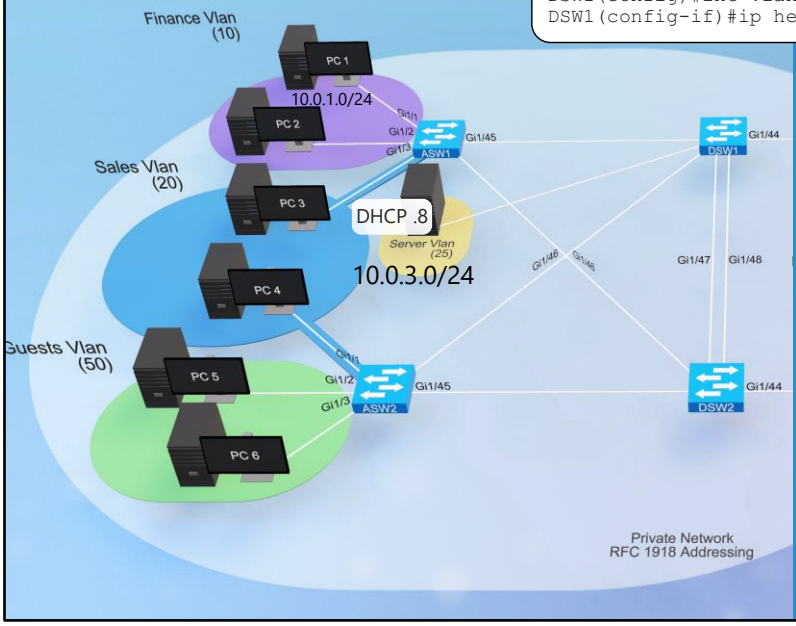
Problem: DHCP Discover Broadcast is confined to the broadcast domain and will not reach the server

Solution: DHCP Relay Agent

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

DHCP Relay Agent (Cisco Router or L3 Switch)

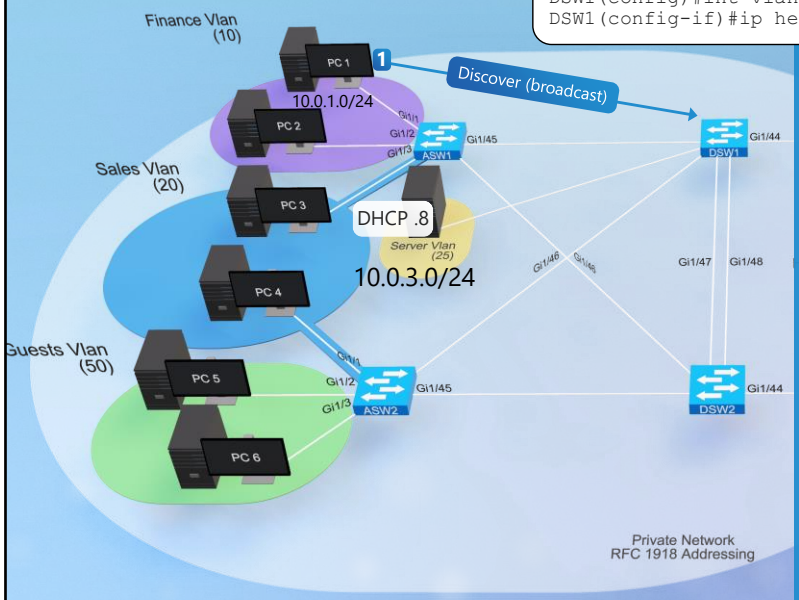
```
DSW1(config)#int vlan 10
DSW1(config-if)#ip helper-address 10.0.3.8
```



©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

DHCP Relay Agent (Cisco Router or L3 Switch)

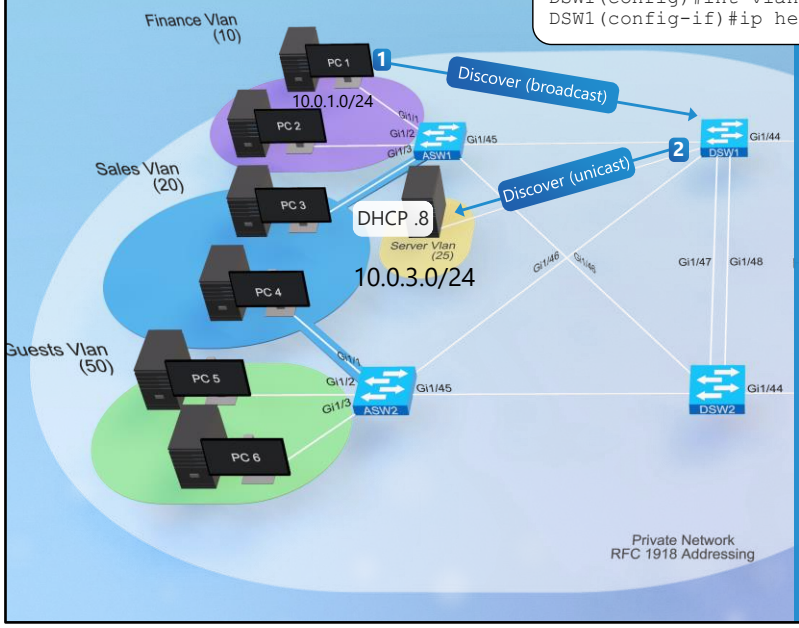
```
DSW1(config)#int vlan 10
DSW1(config-if)#ip helper-address 10.0.3.8
```



©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

DHCP Relay Agent (Cisco Router or L3 Switch)

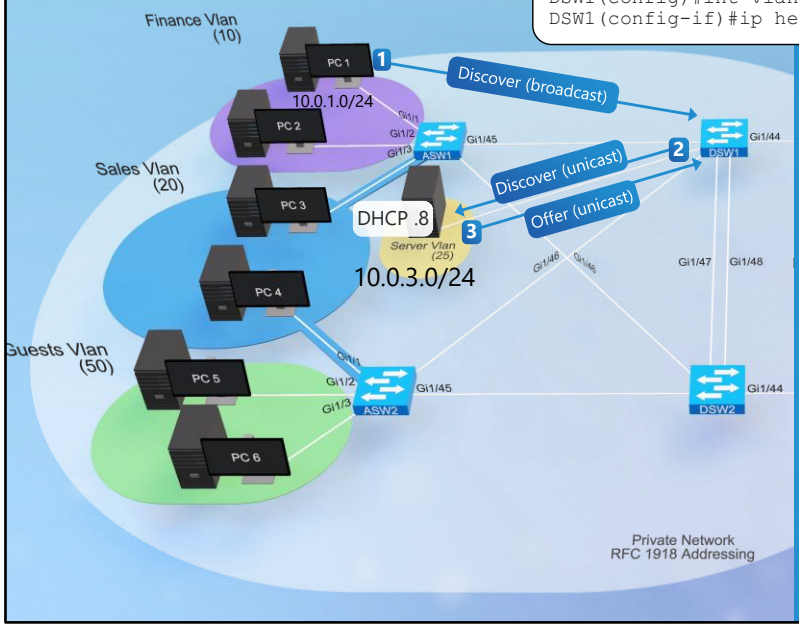
```
DSW1(config)#int vlan 10
DSW1(config-if)#ip helper-address 10.0.3.8
```



©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

DHCP Relay Agent (Cisco Router or L3 Switch)

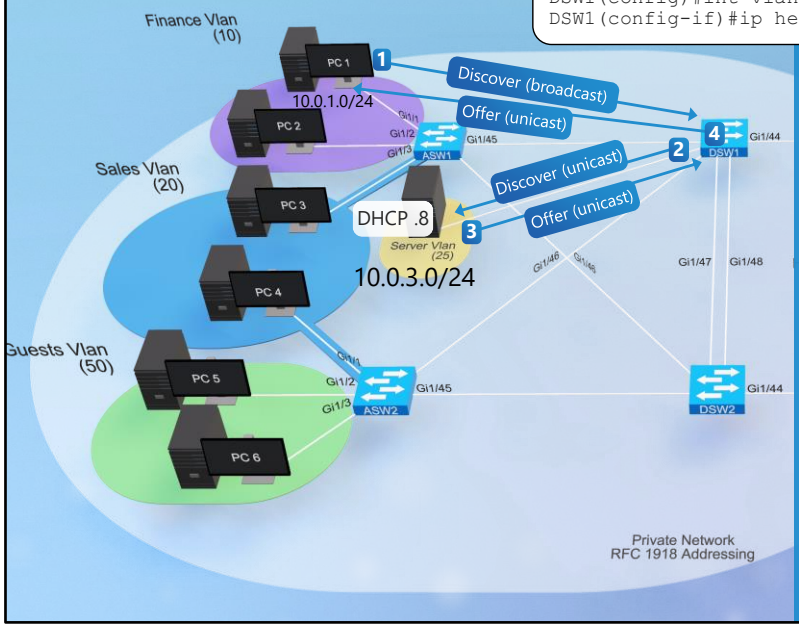
```
DSW1(config)#int vlan 10
DSW1(config-if)#ip helper-address 10.0.3.8
```



©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

DHCP Relay Agent (Cisco Router or L3 Switch)

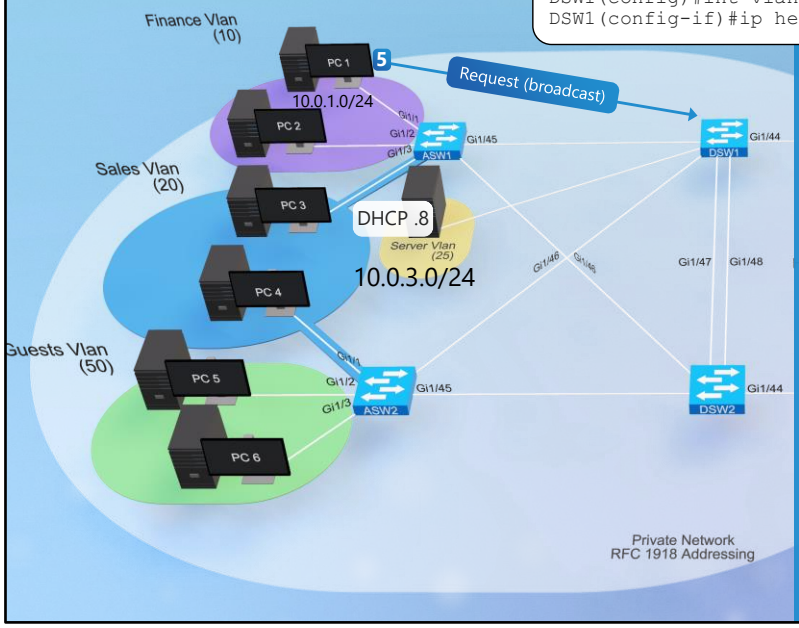
```
DSW1(config)#int vlan 10
DSW1(config-if)#ip helper-address 10.0.3.8
```



©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

DHCP Relay Agent (Cisco Router or L3 Switch)

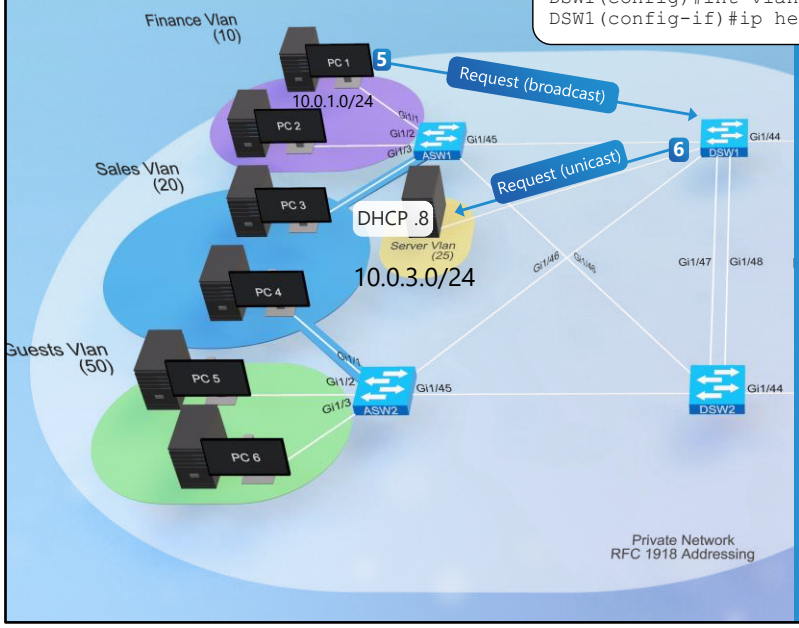
```
DSW1(config)#int vlan 10
DSW1(config-if)#ip helper-address 10.0.3.8
```



©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

DHCP Relay Agent (Cisco Router or L3 Switch)

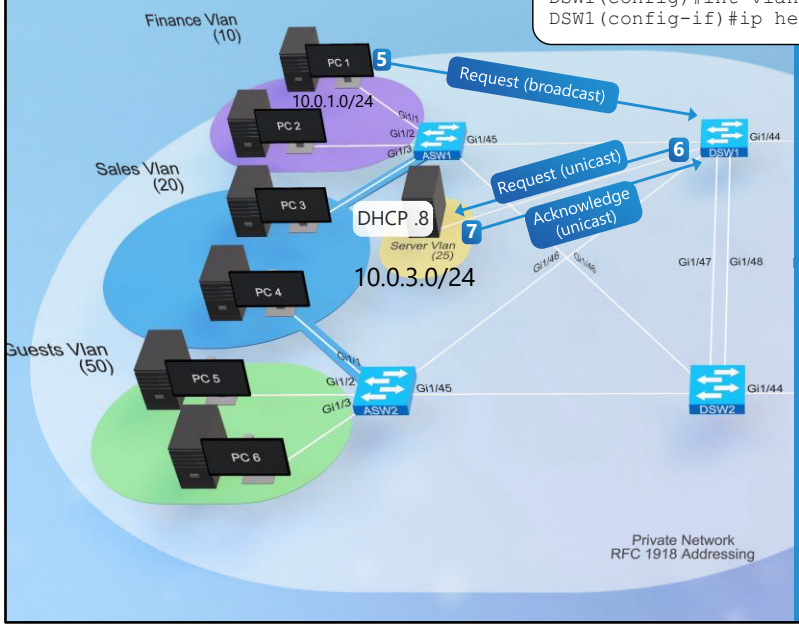
```
DSW1(config)#int vlan 10
DSW1(config-if)#ip helper-address 10.0.3.8
```



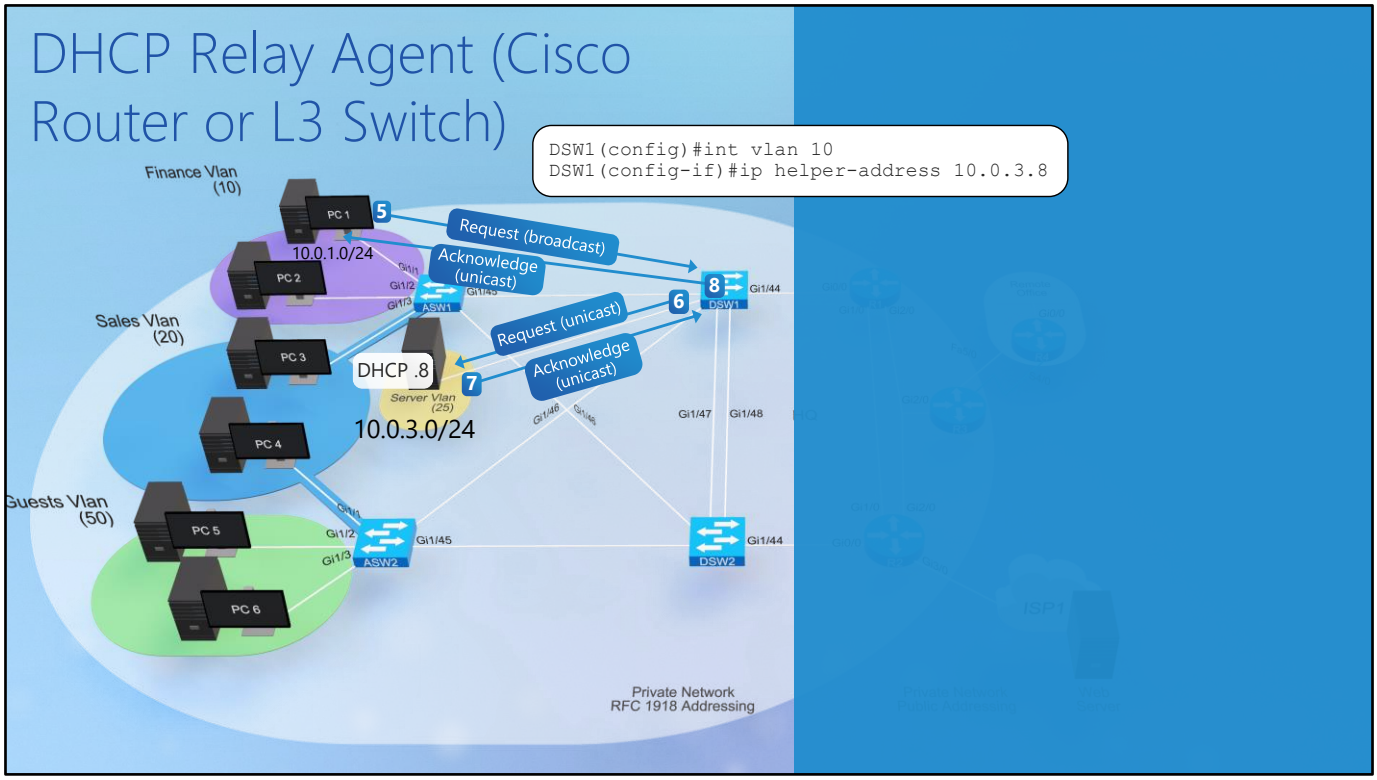
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

DHCP Relay Agent (Cisco Router or L3 Switch)

```
DSW1(config)#int vlan 10
DSW1(config-if)#ip helper-address 10.0.3.8
```



©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



You can troubleshoot this process by debug dhcp messages on the device.

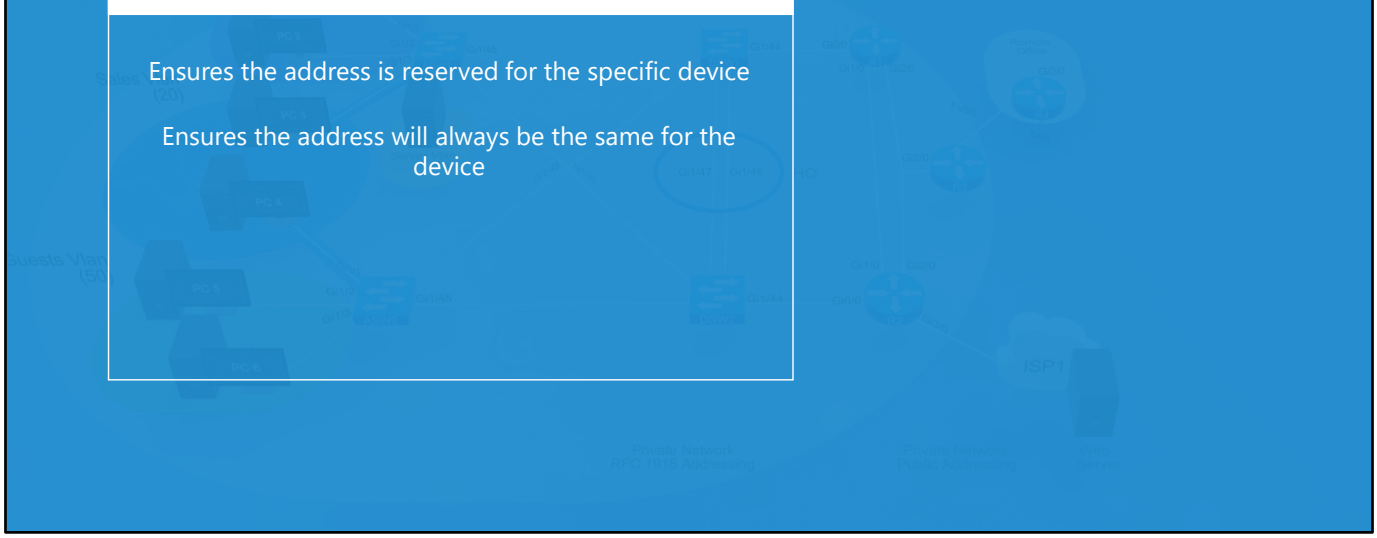
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

DHCP Manual Address Binding

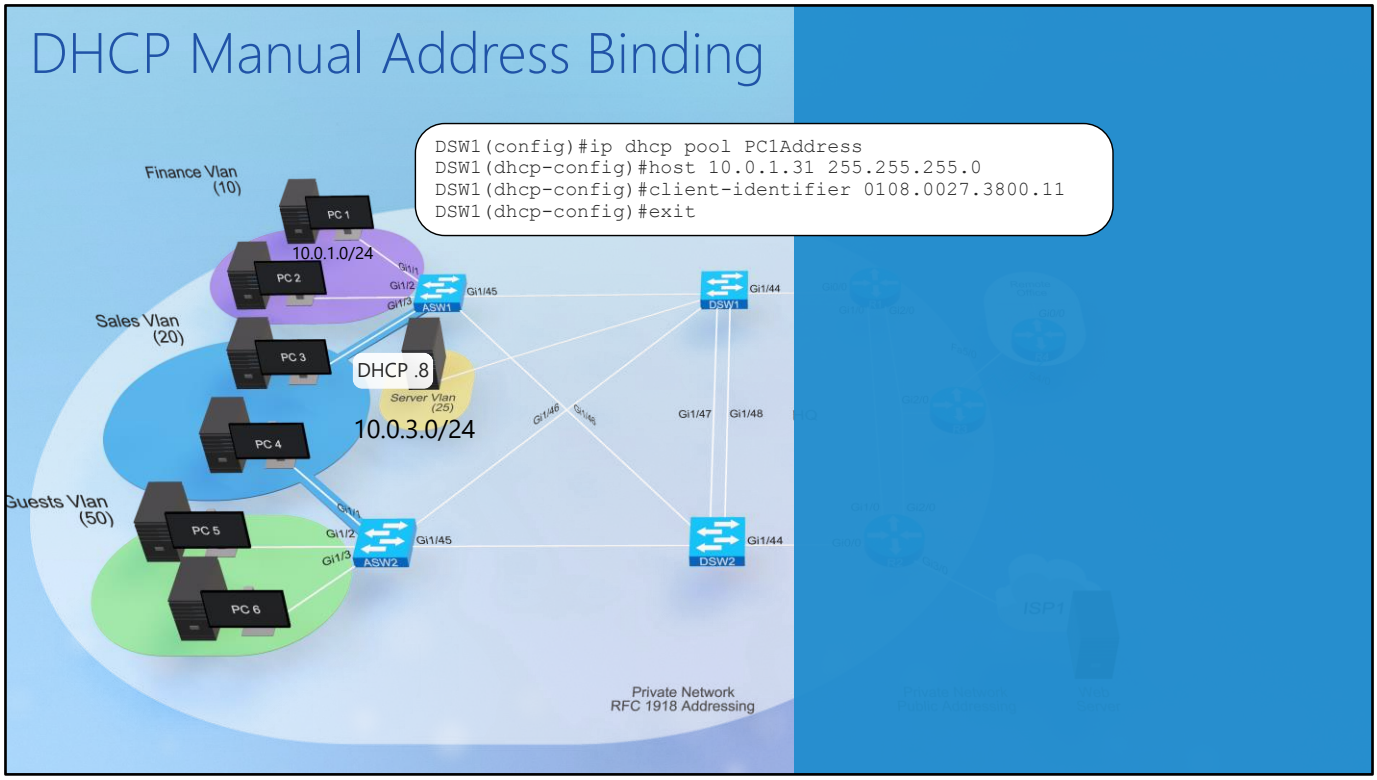
The same address is provided to the device every time

Ensures the address is reserved for the specific device

Ensures the address will always be the same for the device



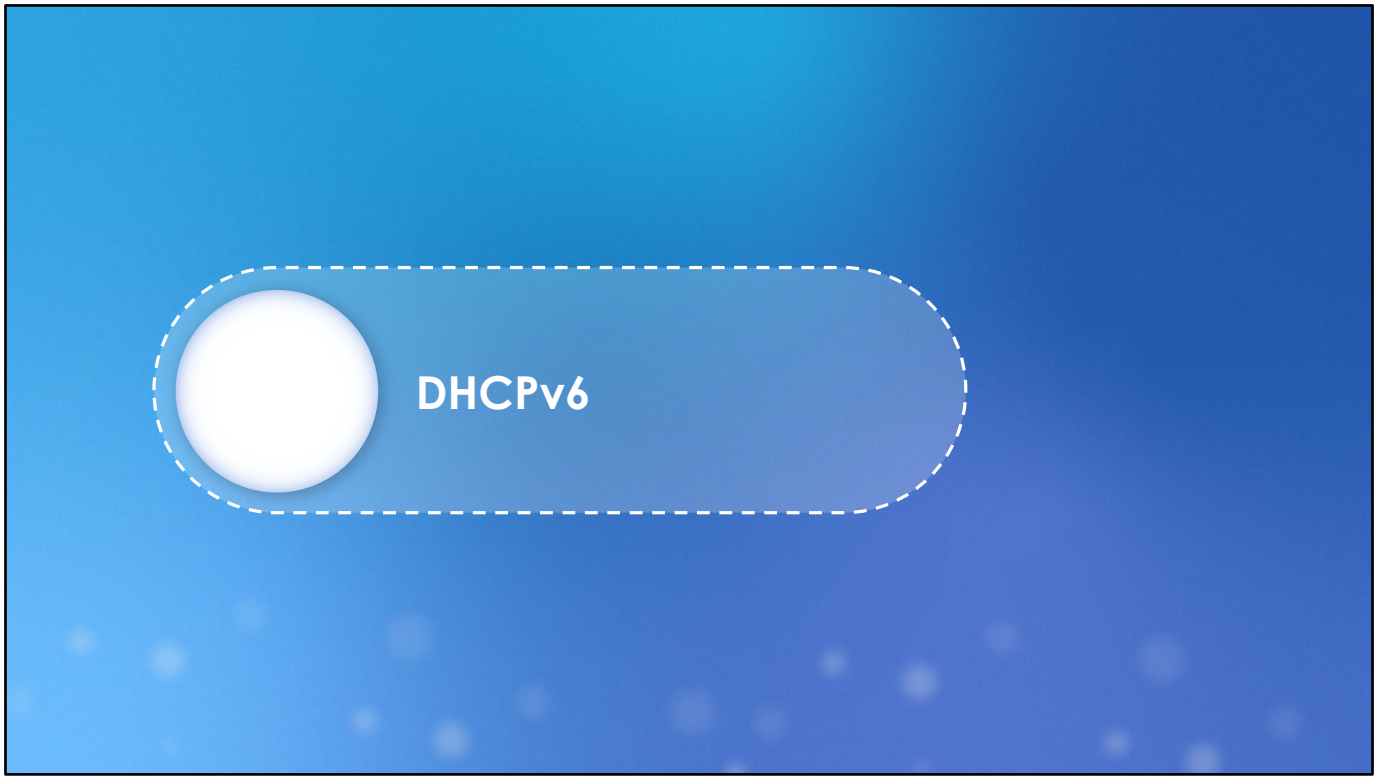
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Normally the client identifier is made up of 01 which means ethernet followed by the MAC address of the device in the format displayed on the slide.

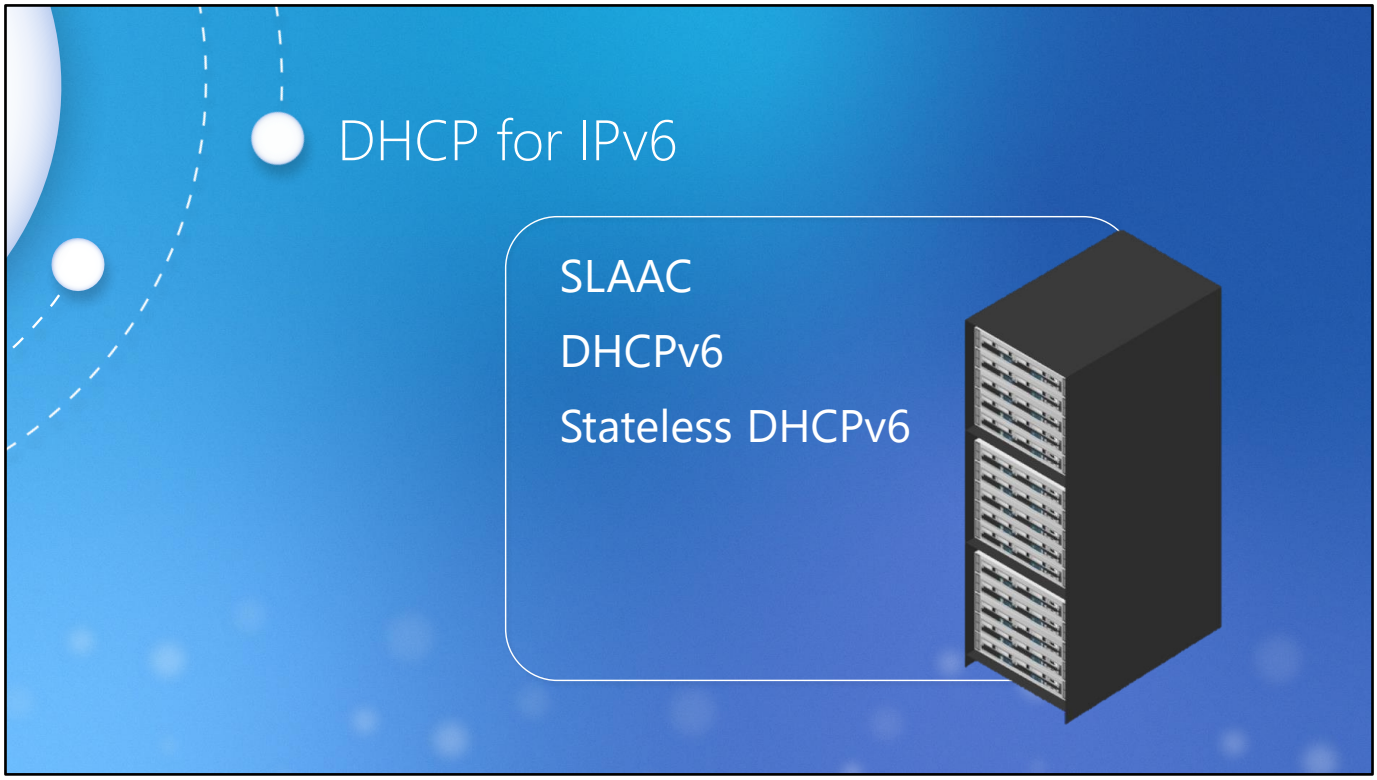
If you try that and it is not working for you, you can figure out the client-identifier by using the **debug ip dhcp server** command.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



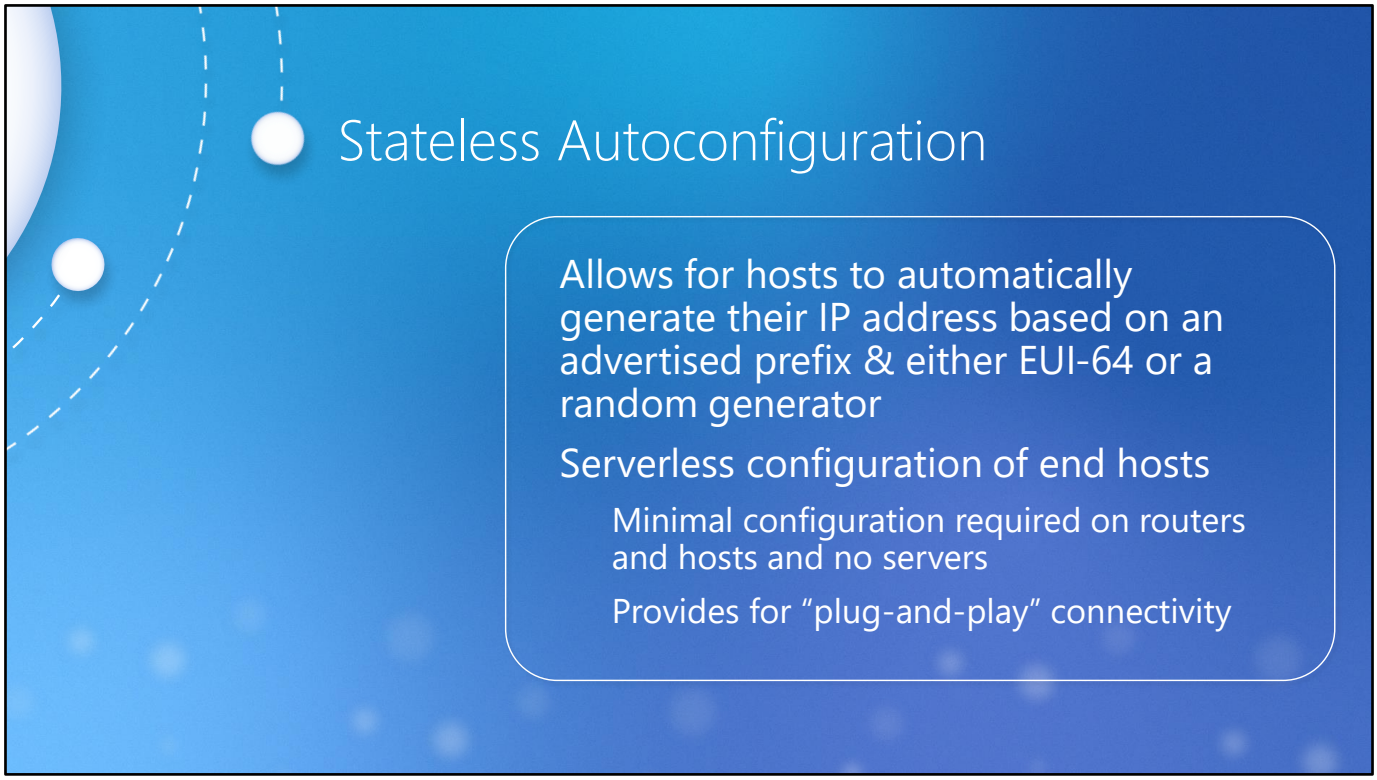
Title slide

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Des Paste in CLI

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

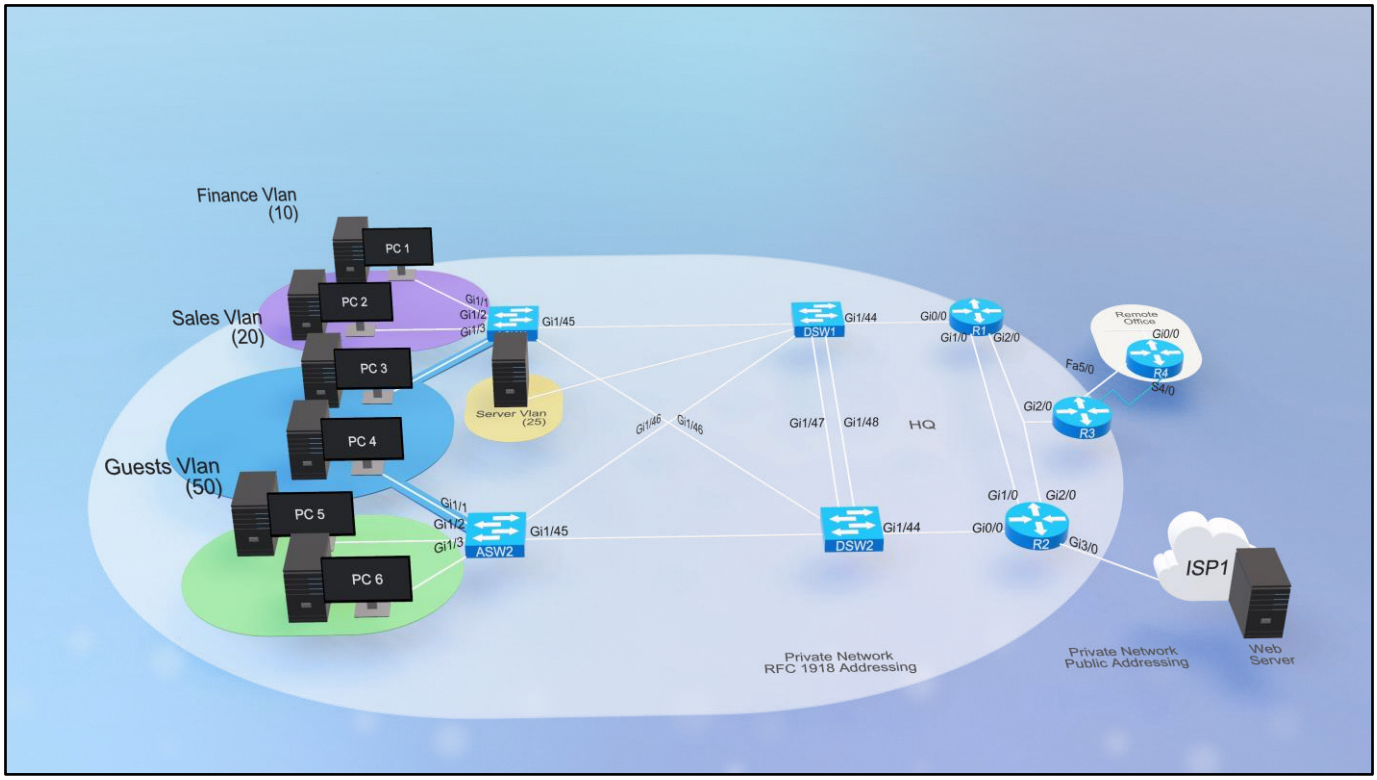


The end host can obtain:
An ipv6 prefix to auto configure an IPv6 address
The default router/gateway address (LL)
The hop limit
The MTU
The Validity lifetime
The DNS server address (not supported on all platforms but is based on RFC 6106)

Interface command

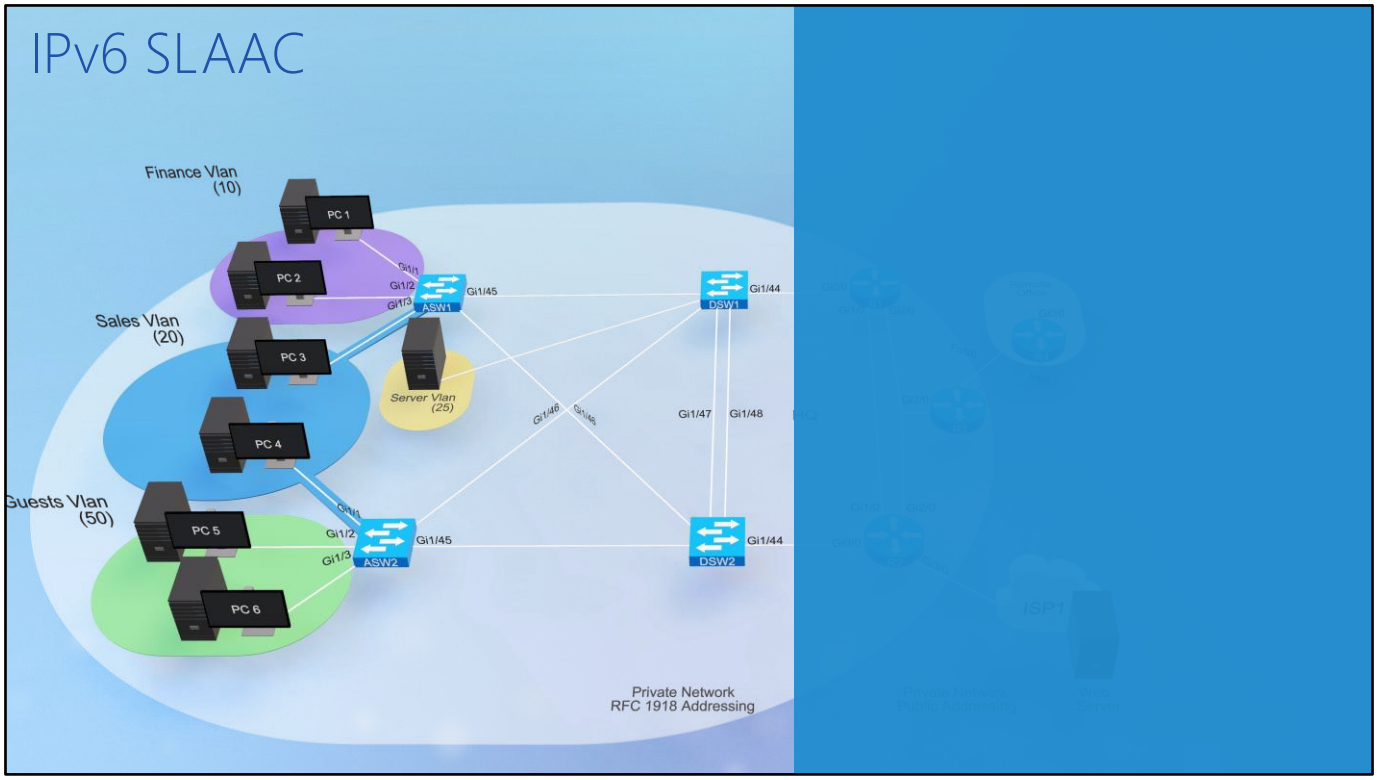
ipv6 nd ra dns server *ipv6 address of dns server*

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



The need for VLANs

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



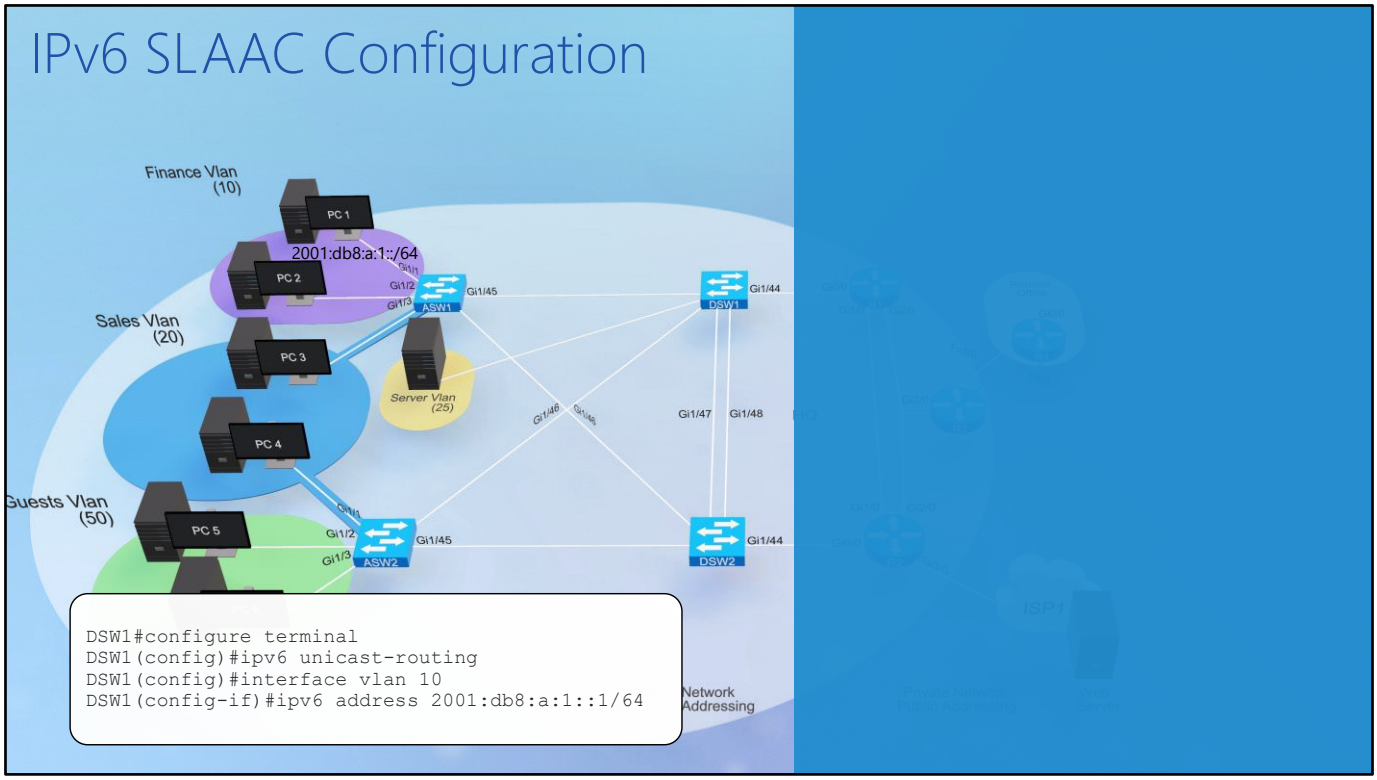
1. As soon as the client is enabled for IPv6 it generates a LL address (typically starts with FE80)
2. The device will then send out a DAD to determine if the LL address is unique on the network. If so, it will use it. If not, it will change the LL address and redo a DAD.
3. Next the device will join the all hosts-multicast group (FF02::01) and send out a RS if it has not already received an RA.
4. Once the DG router receives the RS it sends out an RA. (Note that routers are always sending RAs so even if it does not get an RS it is still sending RAs by default on the link.) The RA is sent to the address FF02::1 which is the all hosts-multicast group with a source of the routers LL address of the interface connected to the network.)
    1. The RA includes
        1. A prefix and prefix length (2001:db8:A:1::/64) (must be /64 for slaac to work)
        2. An A config flag set to 1, an O and M config flag set to 0.
            1. The A flag informs the client to use the prefix and SLAAC to auto generate an address.
            2. The O and M config flags tell the client to hook up with

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

a DHCPv6 server. Since the flags are set to 0 it means there is no other information that needs to be obtained from a DHCPv6 server. Therefore, the client will not start the DHCPv6 process to locate a server in this case.

5. Now that the client has the RA it will process it and, in this case, use the prefix and a OS specific random generator to come up with it an IPv6 global unicast address.
6. The client will then perform DAD to determine if the address is unique. If so, it uses it, if not it generates a new address and then uses DAD again.
7. Once the address is unique the client will use the LL address of the router that was in the RA as the default gateway.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



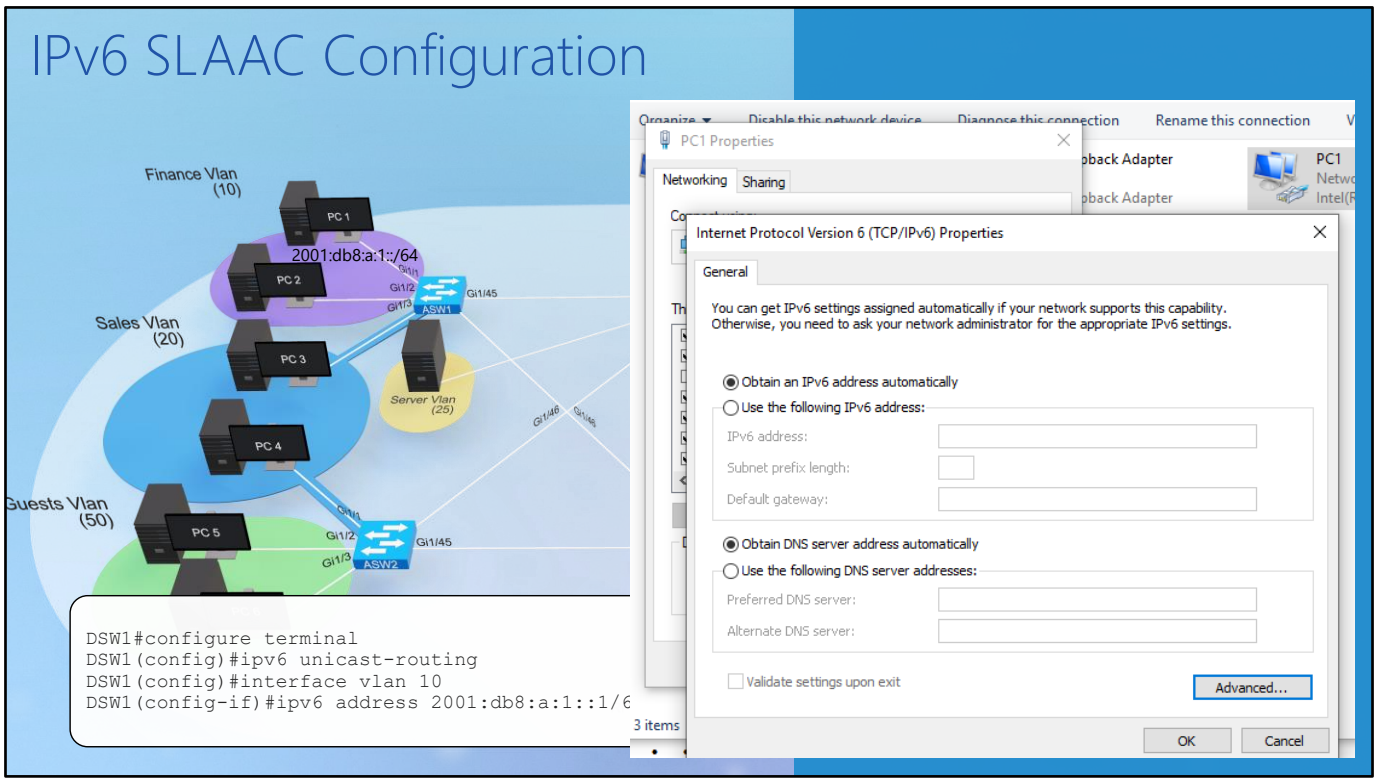
1. As soon as the client is enabled for IPv6 it generates a LL address (typically starts with FE80)
2. The device will then send out a DAD to determine if the LL address is unique on the network. If so, it will use it. If not, it will change the LL address and redo a DAD.
3. Next the device will join the all hosts-multicast group (FF02::01) and send out a RS if it has not already received an RA.
4. Once the DG router receives the RS it sends out an RA. (Note that routers are always sending RAs so even if it does not get an RS it is still sending RAs by default on the link.) The RA is sent to the address FF02::1 which is the all hosts-multicast group with a source of the routers LL address of the interface connected to the network.)
    1. The RA includes
        1. A prefix and prefix length (2001:db8:A:1::/64) (must be /64 for slaac to work)
        2. An A config flag set to 1, an O and M config flag set to 0.
            1. The A flag informs the client to use the prefix and SLAAC to auto generate an address.
            2. The O and M config flags tell the client to hook up with

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

a DHCPv6 server. Since the flags are set to 0 it means there is no other information that needs to be obtained from a DHCPv6 server. Therefore, the client will not start the DHCPv6 process to locate a server in this case.

5. Now that the client has the RA it will process it and, in this case, use the prefix and a OS specific random generator to come up with it an IPv6 global unicast address.
6. The client will then perform DAD to determine if the address is unique. If so, it uses it, if not it generates a new address and then uses DAD again.
7. Once the address is unique the client will use the LL address of the router that was in the RA as the default gateway.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



1. As soon as the client is enabled for IPv6 it generates a LL address (typically starts with FE80)
2. The device will then send out a DAD to determine if the LL address is unique on the network. If so, it will use it. If not, it will change the LL address and redo a DAD.
3. Next the device will join the all hosts-multicast group (FF02::01) and send out a RS if it has not already received an RA.
4. Once the DG router receives the RS it sends out an RA. (Note that routers are always sending RAs so even if it does not get an RS it is still sending RAs by default on the link.) The RA is sent to the address FF02::1 which is the all hosts-multicast group with a source of the routers LL address of the interface connected to the network.)
    1. The RA includes
        1. A prefix and prefix length (2001:db8:A:1::/64) (must be /64 for slaac to work)
        2. An A config flag set to 1, an O and M config flag set to 0.
            1. The A flag informs the client to use the prefix and SLAAC to auto generate an address.
            2. The O and M config flags tell the client to hook up with

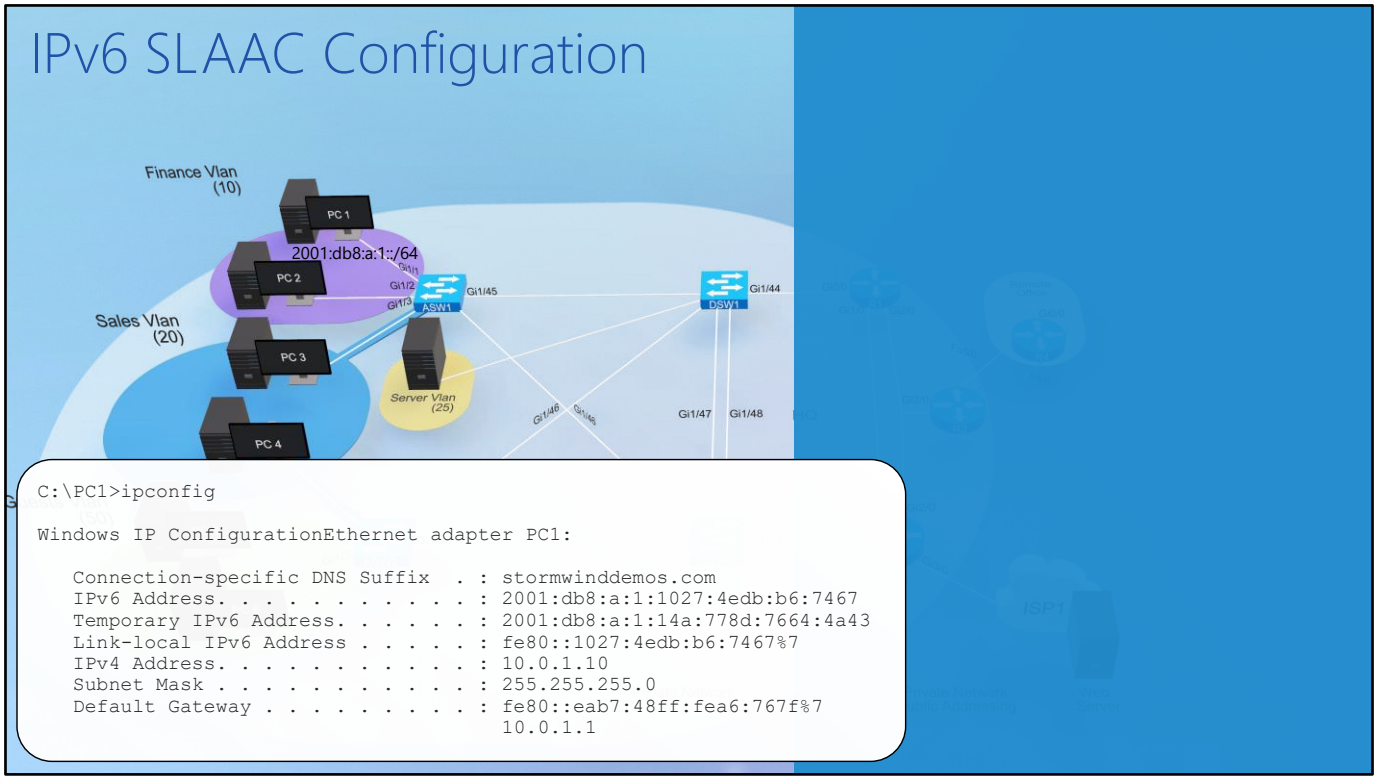
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

a DHCPv6 server. Since the flags are set to 0 it means there is no other information that needs to be obtained from a DHCPv6 server. Therefore, the client will not start the DHCPv6 process to locate a server in this case.

5. Now that the client has the RA it will process it and, in this case, use the prefix and a OS specific random generator to come up with it an IPv6 global unicast address.
6. The client will then perform DAD to determine if the address is unique. If so, it uses it, if not it generates a new address and then uses DAD again.
7. Once the address is unique the client will use the LL address of the router that was in the RA as the default gateway.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

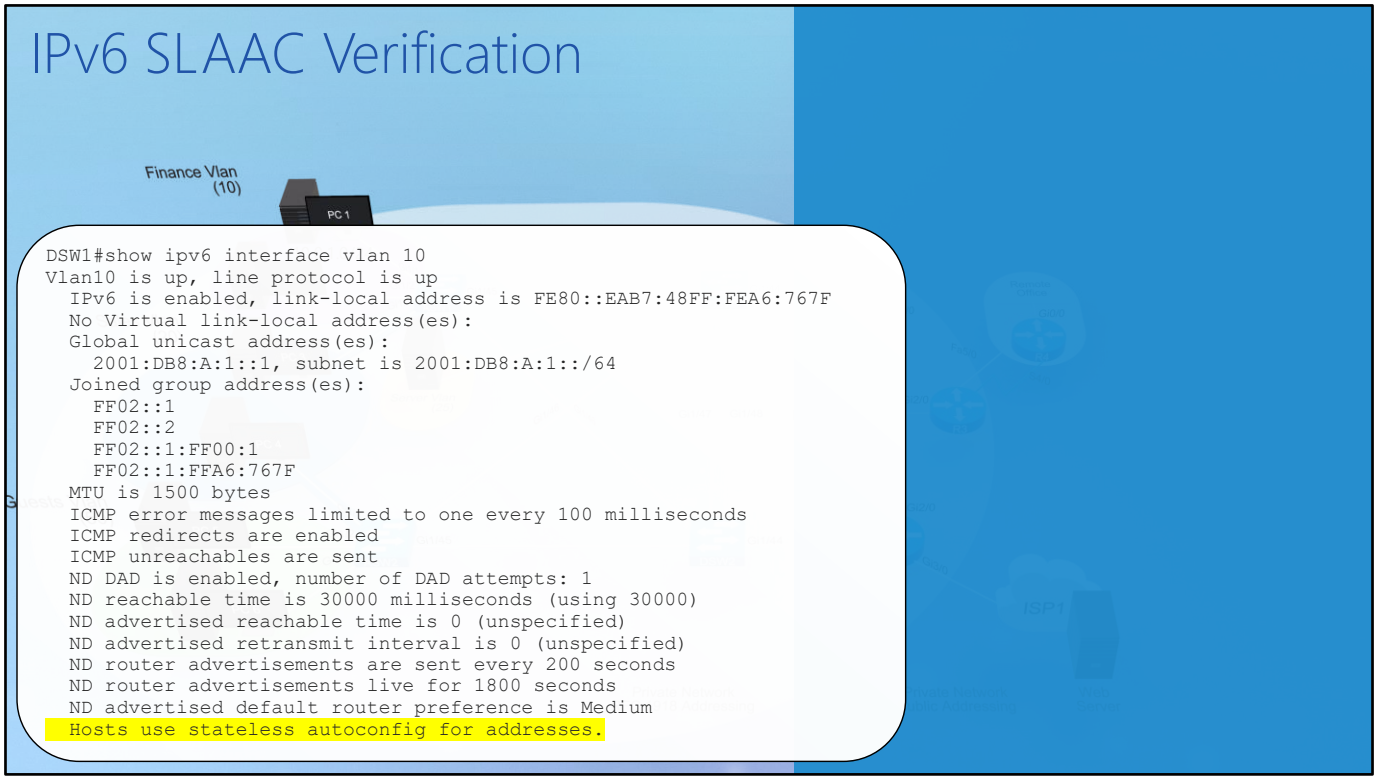
IPv6 SLAAC Configuration



1. Default valid lifetime is 2592000 seconds (30 days)

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

IPv6 SLAAC Verification



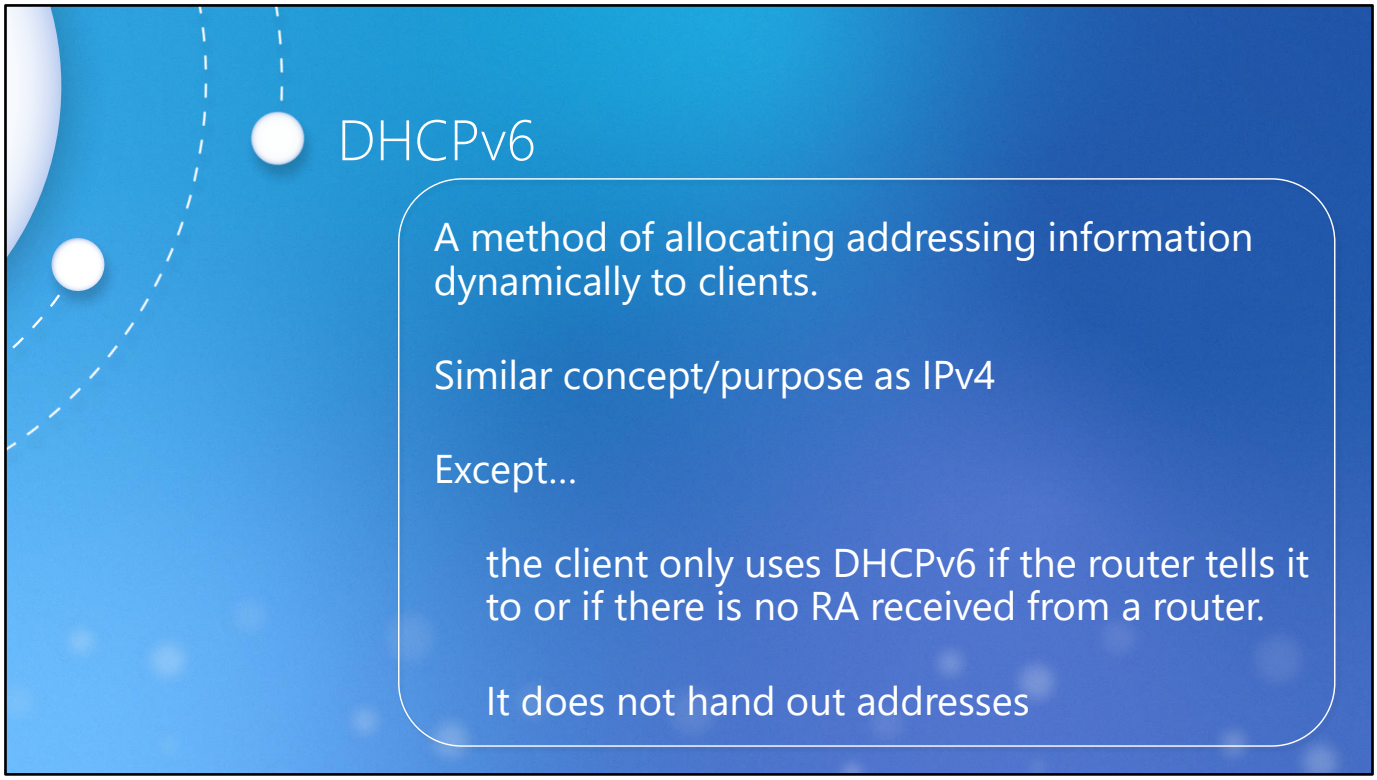
1. As soon as the client is enabled for IPv6 it generates a LL address (typically starts with FE80)
2. The device will then send out a DAD to determine if the LL address is unique on the network. If so, it will use it. If not, it will change the LL address and redo a DAD.
3. Next the device will join the all hosts-multicast group (FF02::01) and send out a RS if it has not already received an RA.
4. Once the DG router receives the RS it sends out an RA. (Note that routers are always sending RAs so even if it does not get an RS it is still sending RAs by default on the link.) The RA is sent to the address FF02::1 which is the all hosts-multicast group with a source of the routers LL address of the interface connected to the network.)
    1. The RA includes
        1. A prefix and prefix length (2001:db8:A:1::/64) (must be /64 for slaac to work)
        2. An A config flag set to 1, an O and M config flag set to 0.
            1. The A flag informs the client to use the prefix and SLAAC to auto generate an address.
            2. The O and M config flags tell the client to hook up with

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

a DHCPv6 server. Since the flags are set to 0 it means there is no other information that needs to be obtained from a DHCPv6 server. Therefore, the client will not start the DHCPv6 process to locate a server in this case.

5. Now that the client has the RA it will process it and, in this case, use the prefix and a OS specific random generator to come up with it an IPv6 global unicast address.
6. The client will then perform DAD to determine if the address is unique. If so, it uses it, if not it generates a new address and then uses DAD again.
7. Once the address is unique the client will use the LL address of the router that was in the RA as the default gateway.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



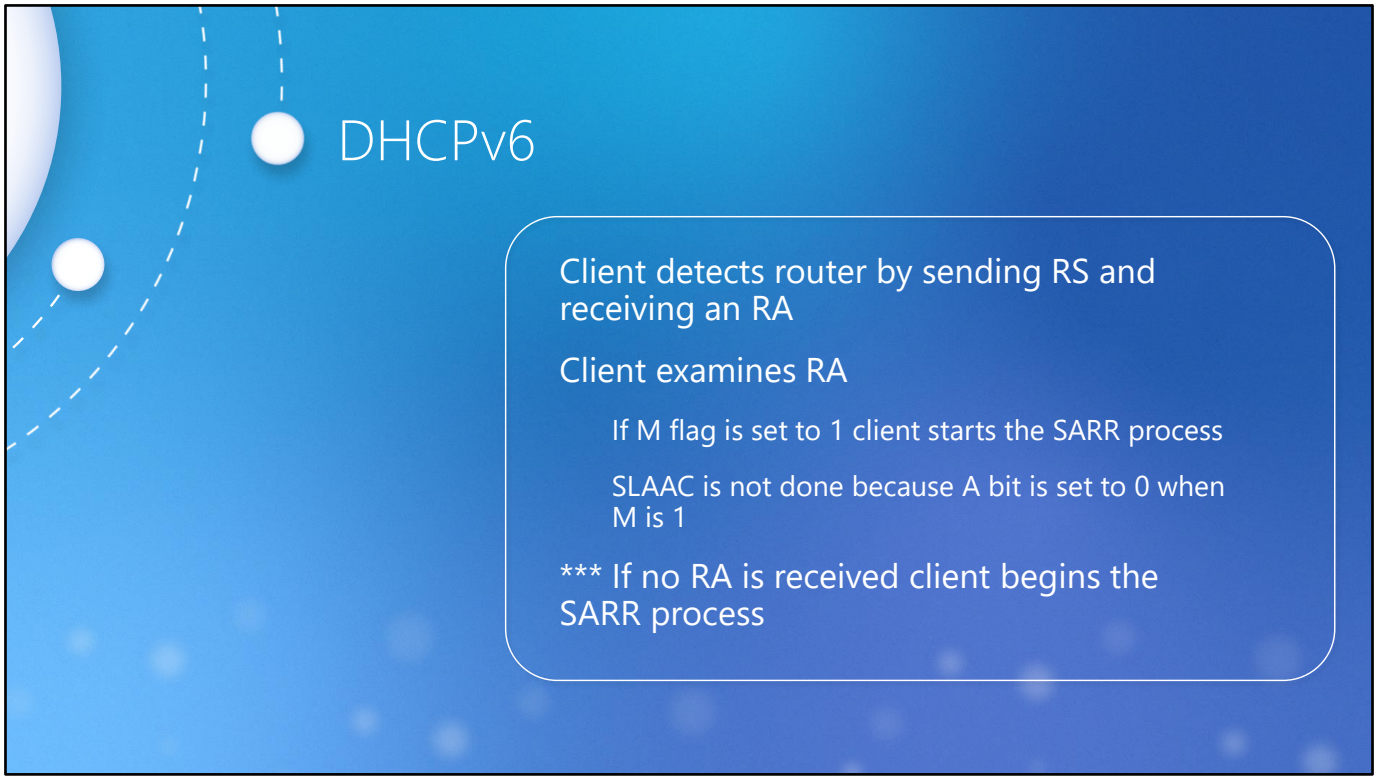
Alternate DHCPv6 to 4-step is “2-step” with just “Solicity & Reply” but both client/server need to be configured w/ Rapid

Tell client to use DHCPv6 server
ipv6 nd managed-config-flag

To shut of RAs
ipv6 nd ra suppress

Keep in mind that if you want to support DDNS you will need to have a DHCPv6 server.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

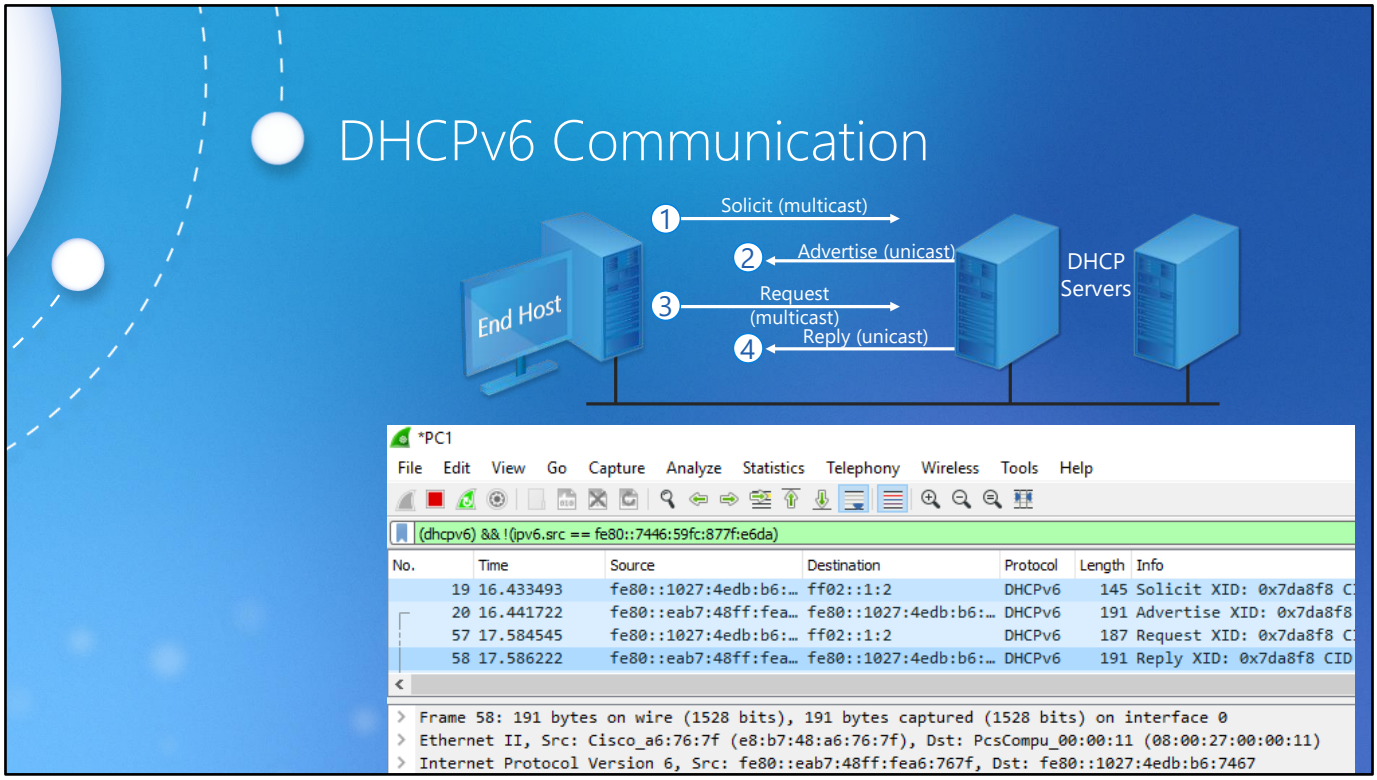


Alternate DHCPv6 to 4-step is “2-step” with just “Solicity & Reply” but both client/server need to be configured w/ Rapid

Tell client to use DHCPv6 server
ipv6 nd managed-config-flag

To shut of RAs
ipv6 nd ra suppress

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Solicit

Advertise

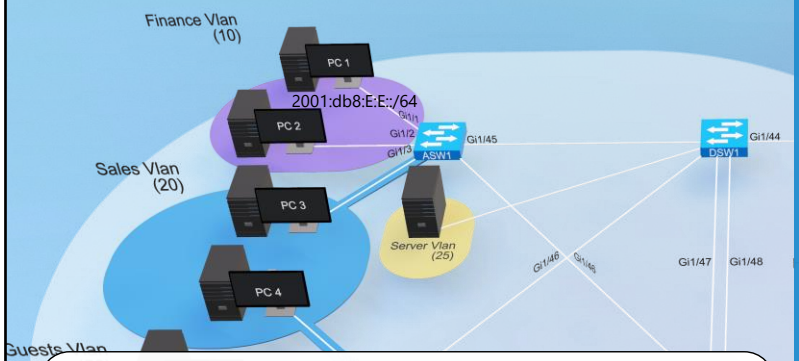
Request

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Reply

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

DHCPv6 Configuration

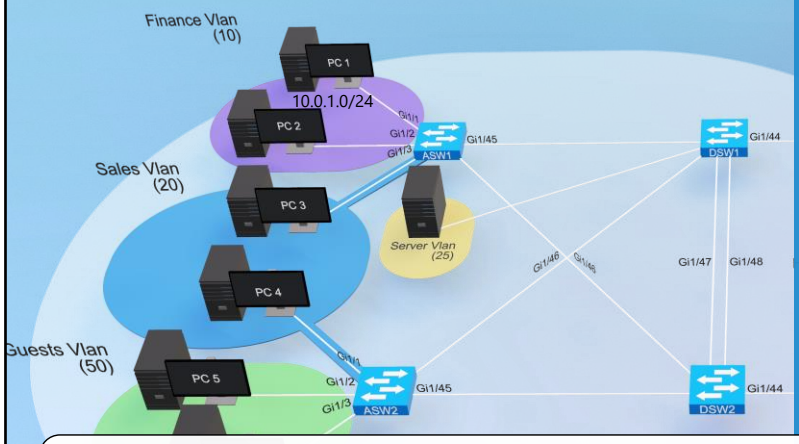



```
DSW1#config terminal
DSW1(config)#ipv6 dhcp pool ENARSI
DSW1(config-dhcpv6)#address prefix 2001:db8:E:E::/64
DSW1(config-dhcpv6)#dns-server 2001:db8:e:1::100
DSW1(config-dhcpv6)#domain-name ipv6stormwinddemo.local
DSW1(config-dhcpv6)#exit
DSW1(config)#
DSW1(config)#
DSW1(config)#int vlan 10
DSW1(config-if)#ipv6 dhcp server ENARSI
DSW1(config-if)#ipv6 nd managed-config-flag
```

`DSW1(config-if)#ipv6 nd managed-config-flag`
sets the M flag to 1 to tell the client to use DHCPv6 and start the SARR and sets the A flag to 0 to disable SLACC

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

DHCPv6 Configuration

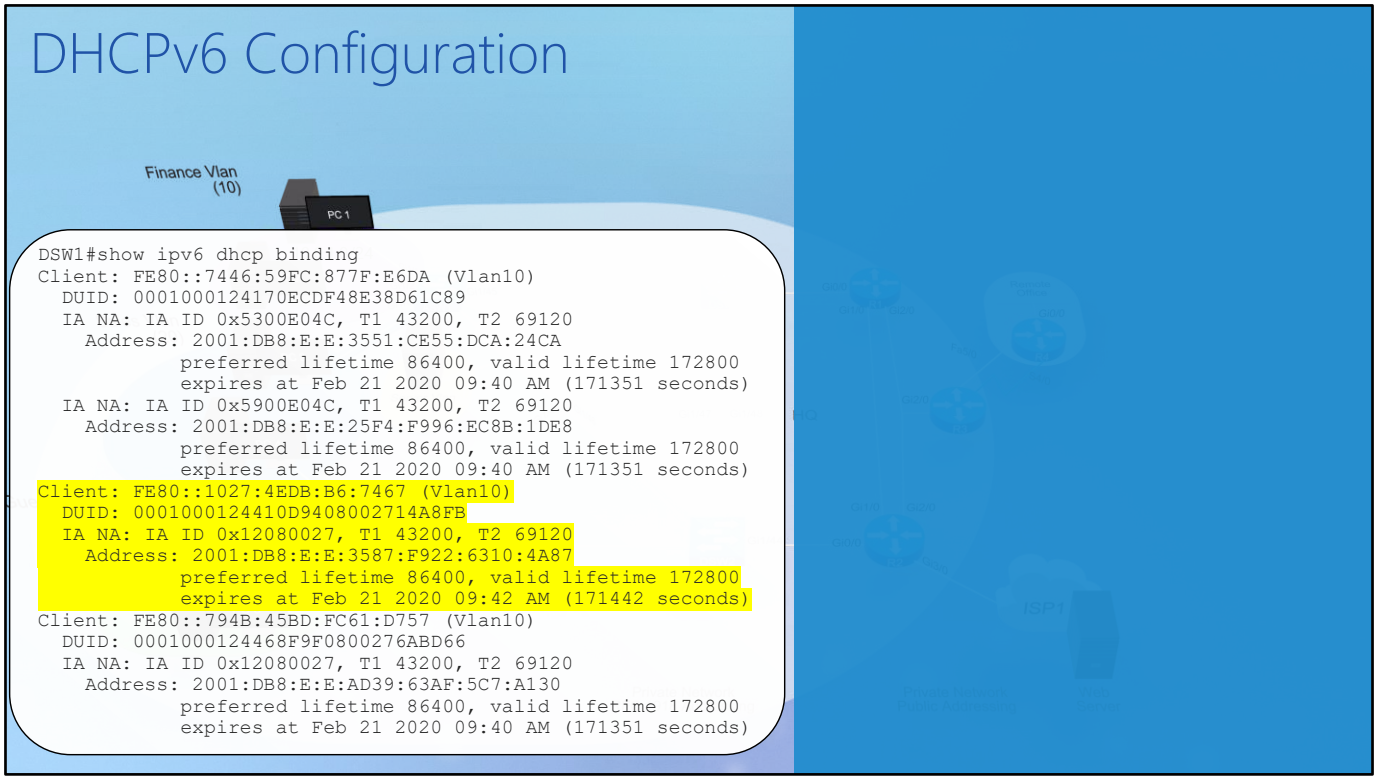



```
DSW1#show ipv6 dhcp pool
DHCPv6 pool: ENARSI
  Address allocation prefix: 2001:DB8:E:E::/64 valid 172800 preferred 86400 (4 in use, 0 conflicts)
  DNS server: 2001:DB8:E:1::100
  Domain name: ipv6stormwinddemo.local
  Active clients: 3
```

`DSW1(config-if)#ipv6 nd managed-config-flag`
sets the M flag to 1 to tell the client to use DHCPv6 and start the SARR and sets the A flag to 0 to disable SLACC

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

DHCPv6 Configuration



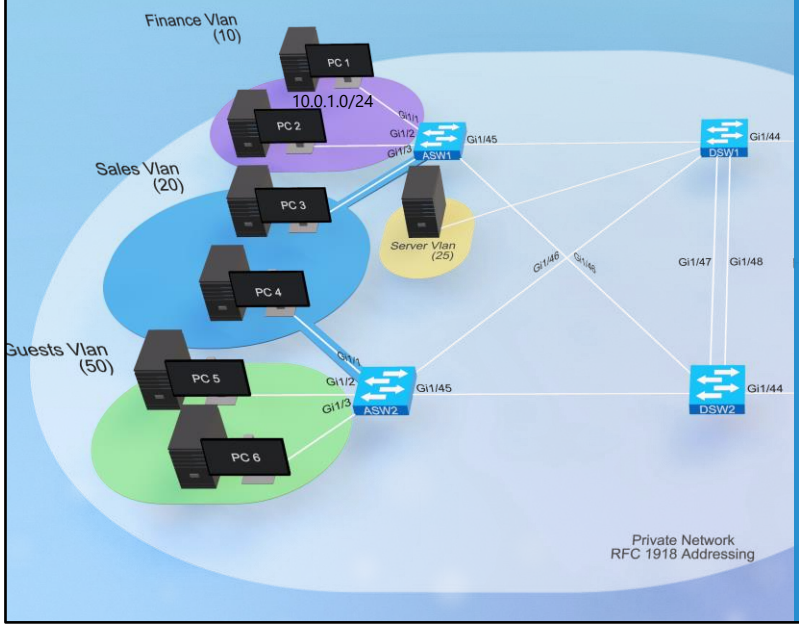
`DSW1(config-if)#ipv6 nd managed-config-flag`
sets the M flag to 1 to tell the client to use DHCPv6 and start the SARR and sets the A flag to 0 to disable SLACC

This is why it is called STATEFULL… the DHCPv6 keeps track of who is using the DHCPv6 service based on their LINK LOCAL ADDRESS and what they configured their address as.

`The middle one is PC1……`

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Stateless DHCPv6



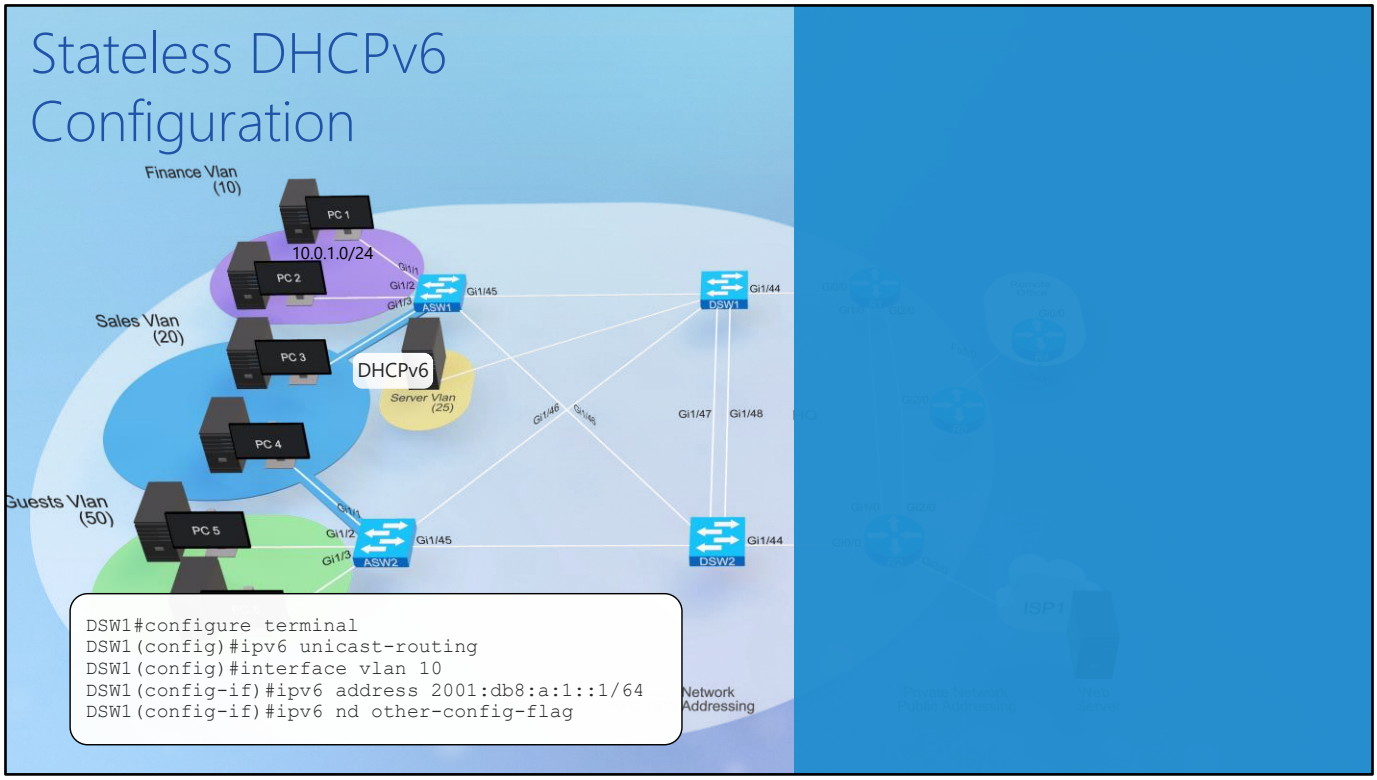
Combination of SLAAC and DHCPv6

- SLAAC used for prefix, default gateway info
- DHCPv6 used to provide
  - NTP server
  - DNS server
  - Domain name
  - … and more.

*AKA: DHCPv6 Lite

COMBO MODE

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



1. As soon as the client is enabled for IPv6 it generates a LL address (typically starts with FE80)
2. The device will then send out a DAD to determine if the LL address is unique on the network. If so, it will use it. If not, it will change the LL address and redo a DAD.
3. Next the device will join the all hosts-multicast group (FF02::01) and send out a RS if it has not already received an RA.
4. Once the DG router receives the RS it sends out an RA. (Note that routers are always sending RAs so even if it does not get an RS it is still sending RAs by default on the link.) The RA is sent to the address FF02::1 which is the all hosts-multicast group with a source of the routers LL address of the interface connected to the network.)
    1. The RA includes
        1. A prefix and prefix length (2001:db8:A:1::/64) (must be /64 for slaac to work)
        2. An A and O config flag set to 1, an M config flag set to 0.
            1. The A flag informs the client to use the prefix and SLAAC to auto generate an address.
            2. The O flag informs the client to contact a DHCPv6

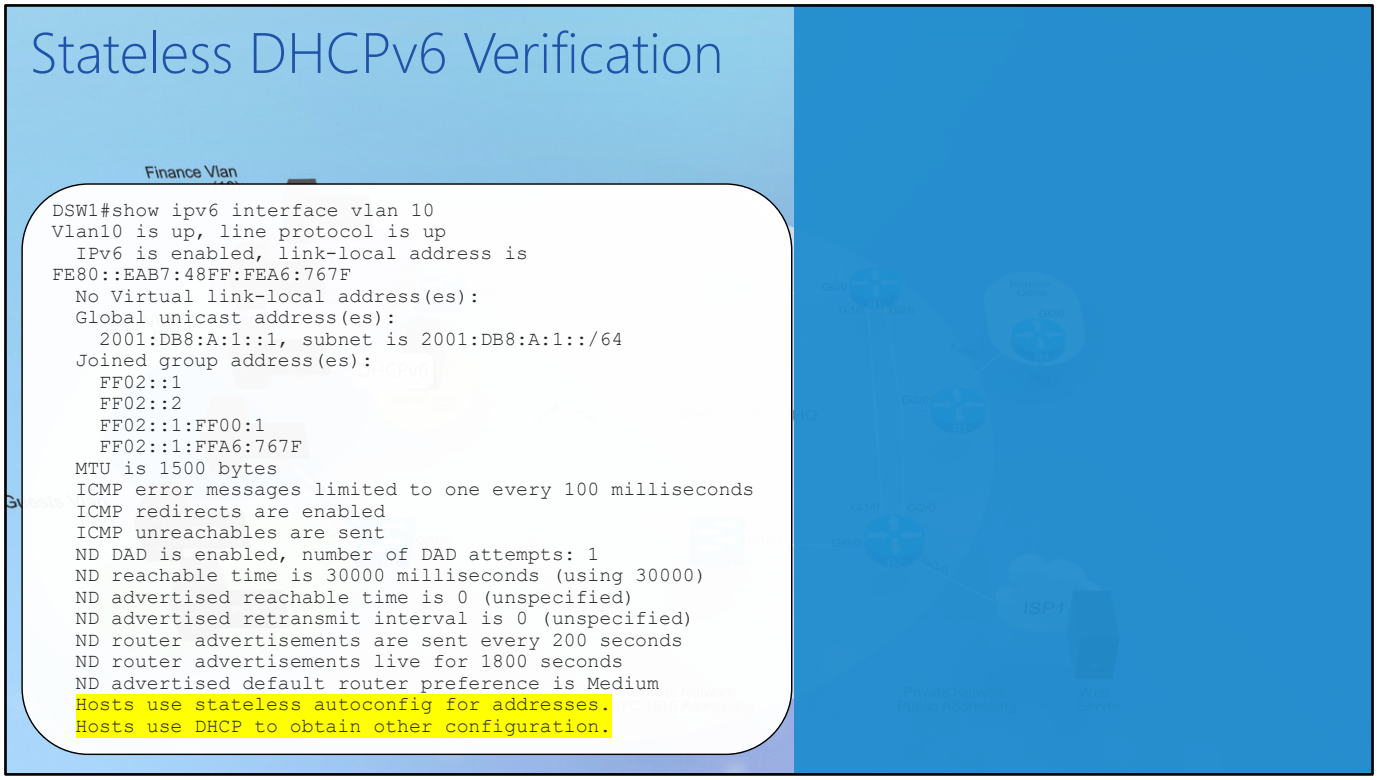
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

server for other information.
3. and M config flags is set to 0 therefore the client will not contact the dhcpv6 server to get addressing information from the server. It will use slacc.

1. Now that the client has the RA it will process it and, in this case, use the prefix and a OS specific random generator to come up with it an IPv6 global unicast address.
2. The client will then perform DAD to determine if the address is unique. If so, it uses it, if not it generates a new address and then uses DAD again.
3. Once the address is unique the client will use the LL address of the router that was in the RA as the default gateway.
4. The client will contact a DHCPv6 server using the SARR process to get other information.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Stateless DHCPv6 Verification



1. As soon as the client is enabled for IPv6 it generates a LL address (typically starts with FE80)
2. The device will then send out a DAD to determine if the LL address is unique on the network. If so, it will use it. If not, it will change the LL address and redo a DAD.
3. Next the device will join the all hosts-multicast group (FF02::01) and send out a RS if it has not already received an RA.
4. Once the DG router receives the RS it sends out an RA. (Note that routers are always sending RAs so even if it does not get an RS it is still sending RAs by default on the link.) The RA is sent to the address FF02::1 which is the all hosts-multicast group with a source of the routers LL address of the interface connected to the network.)
    1. The RA includes
        1. A prefix and prefix length (2001:db8:A:1::/64) (must be /64 for slaac to work)
        2. An A config flag set to 1, an O and M config flag set to 0.
            1. The A flag informs the client to use the prefix and SLAAC to auto generate an address.
            2. The O and M config flags tell the client to hook up with

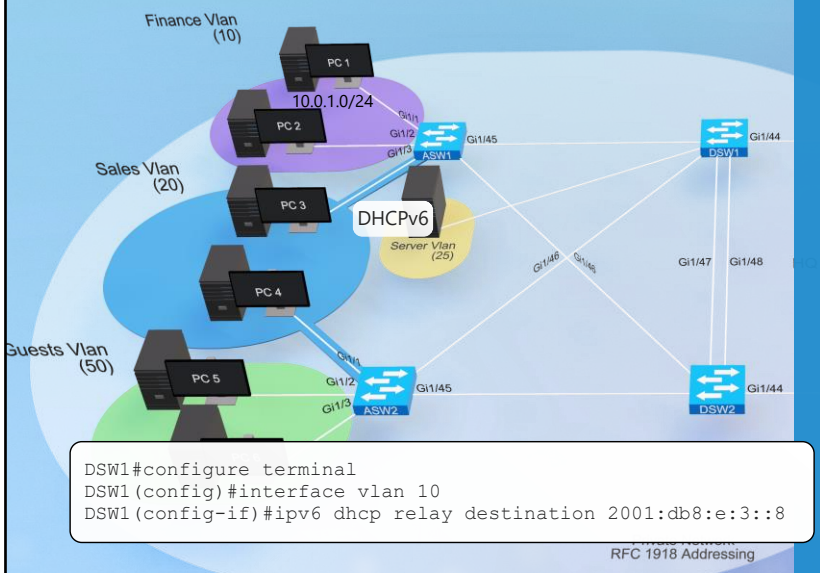
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

a DHCPv6 server. Since the flags are set to 0 it means there is no other information that needs to be obtained from a DHCPv6 server. Therefore, the client will not start the DHCPv6 process to locate a server in this case.

5. Now that the client has the RA it will process it and, in this case, use the prefix and a OS specific random generator to come up with it an IPv6 global unicast address.
6. The client will then perform DAD to determine if the address is unique. If so, it uses it, if not it generates a new address and then uses DAD again.
7. Once the address is unique the client will use the LL address of the router that was in the RA as the default gateway.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

DHCPv6 Relay Agent




```
DSW1#configure terminal
DSW1(config)#interface vlan 10
DSW1(config-if)#ipv6 dhcp relay destination 2001:db8:e:3::8
```

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Troubleshooting DHCPv4

- Server Misconfigured
- Duplicate IP address
- DHCP pool exhaustion
- Relay agent not forwarding messages
- Client is not requesting an address
- Redundant DHCP service not working

Server Misconfigured - pool, gateway, DNS, excluded addresses

Duplicate IP address - ipv4 static address conflicts with dynamic address (only IPv4 because IPv6 uses DAD) use the **show ip dhcp conflict** command to discover duplicates.

DHCP pool exhaustion - server runs out of addresses because the pools are too small / a DoS attack that depletes the pool.

Relay agent not forwarding messages – configured on wrong interface / address not correct.

Client is not requesting an address – is DHCP enabled on the client. Also remember that dhcp is a pull model so the clients pull from the server, the server does not push to the clients… any updates need to be triggered from the client not the server. Use the **debug ip dhcp server events** command to view the DHCP negotiation process on a route.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Troubleshooting DHCPv6

- SLAAC
  - prefix must be /64 on router interface
  - ipv6 unicast routing needs to be enabled
- DHCPv6
  - M flag needs to be set to 1
- Stateless DHCPv6
  - O flag needs to be set to 1
- Relay agent not forwarding messages
- Client is not requesting an address

Set M flag

ipv6 nd managed-config-flag

Set O flag

ipv6 nd other-config-flag

Relay agent not forwarding messages – configured on wrong interface / address not correct.

Client needs to be enabled to obtain IPv6 address automatically.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

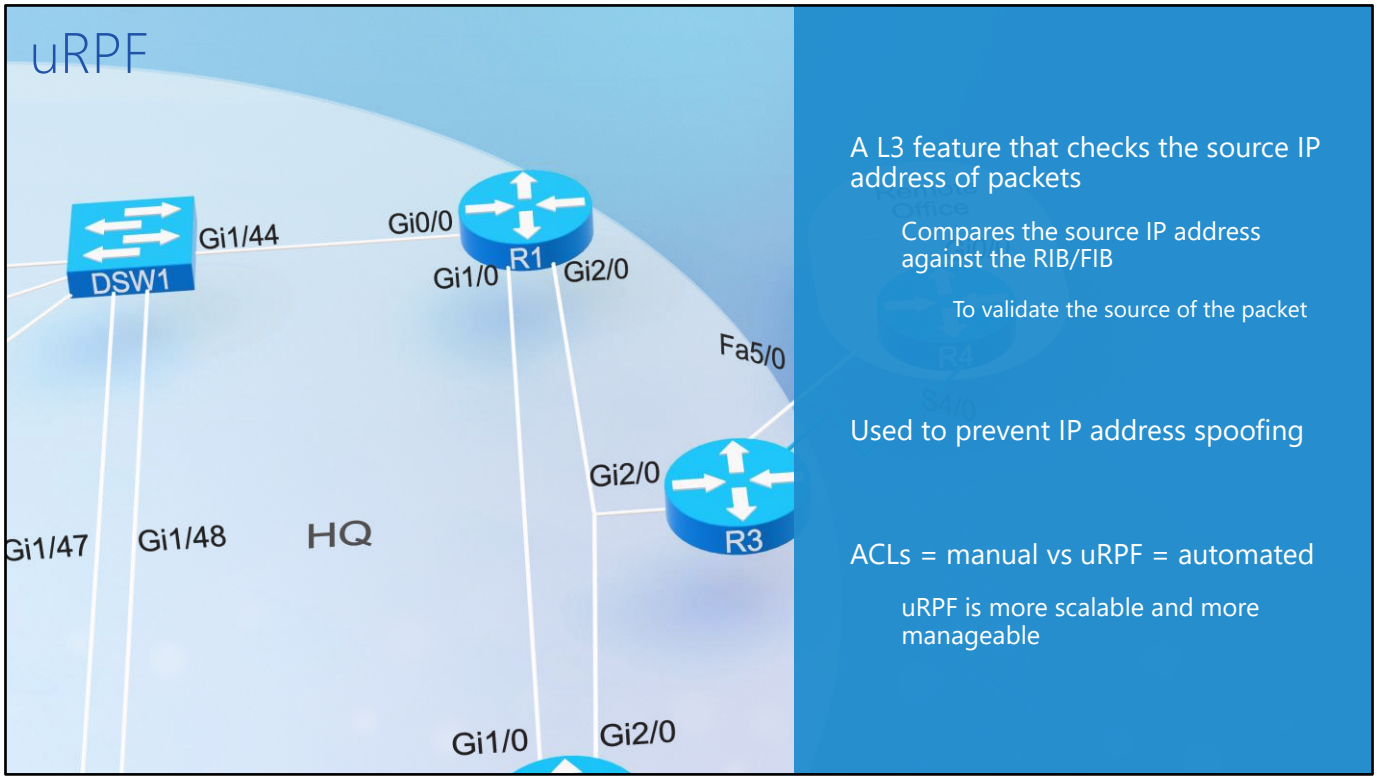


©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Title slide

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



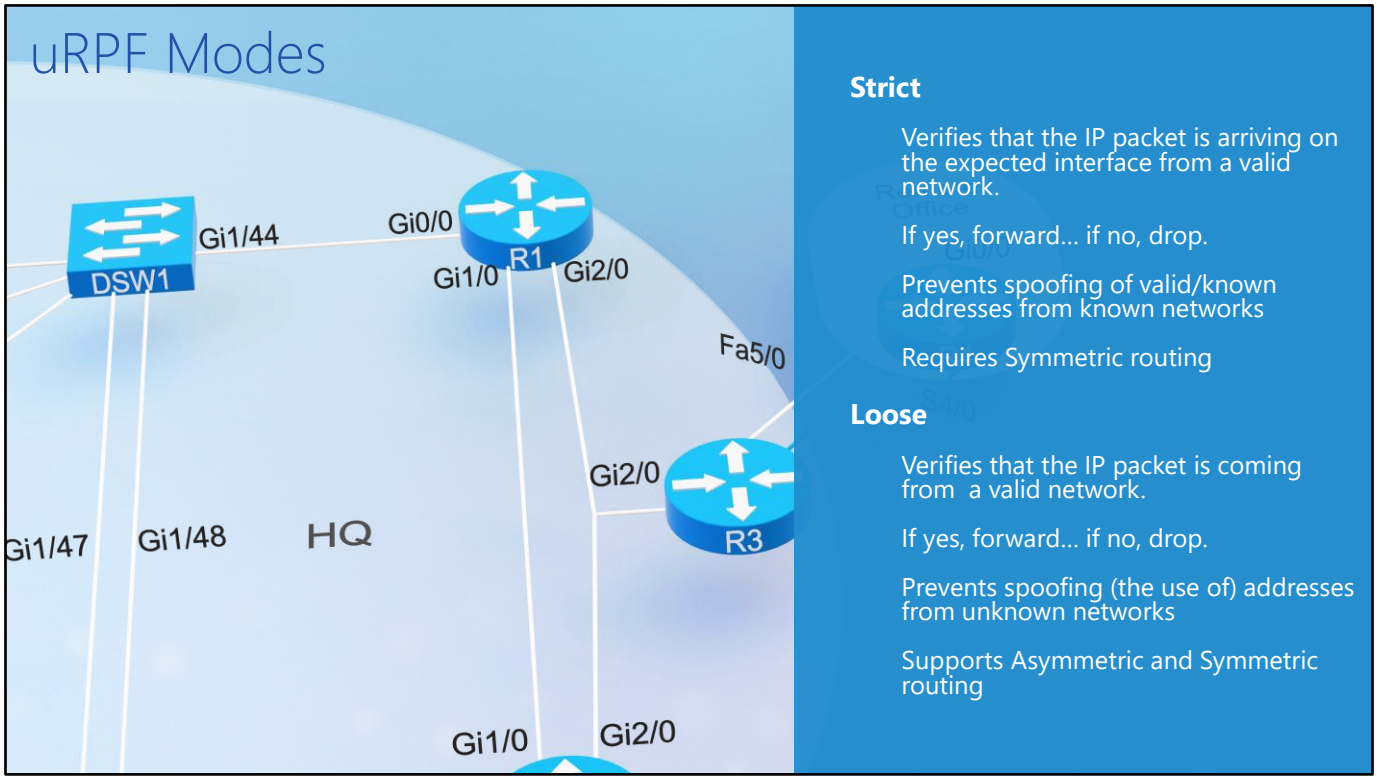
Alternative = manually configure ingress and egress ACLs on interfaces in the network.

uRPF attempts to automate the same process which makes it more scalable and manageable.

Note: uRPF is only as secure as your routing information. If the routing table has been compromised because of rogue routers joining the routing domain and injecting false information, then uRPF is compromised as well.

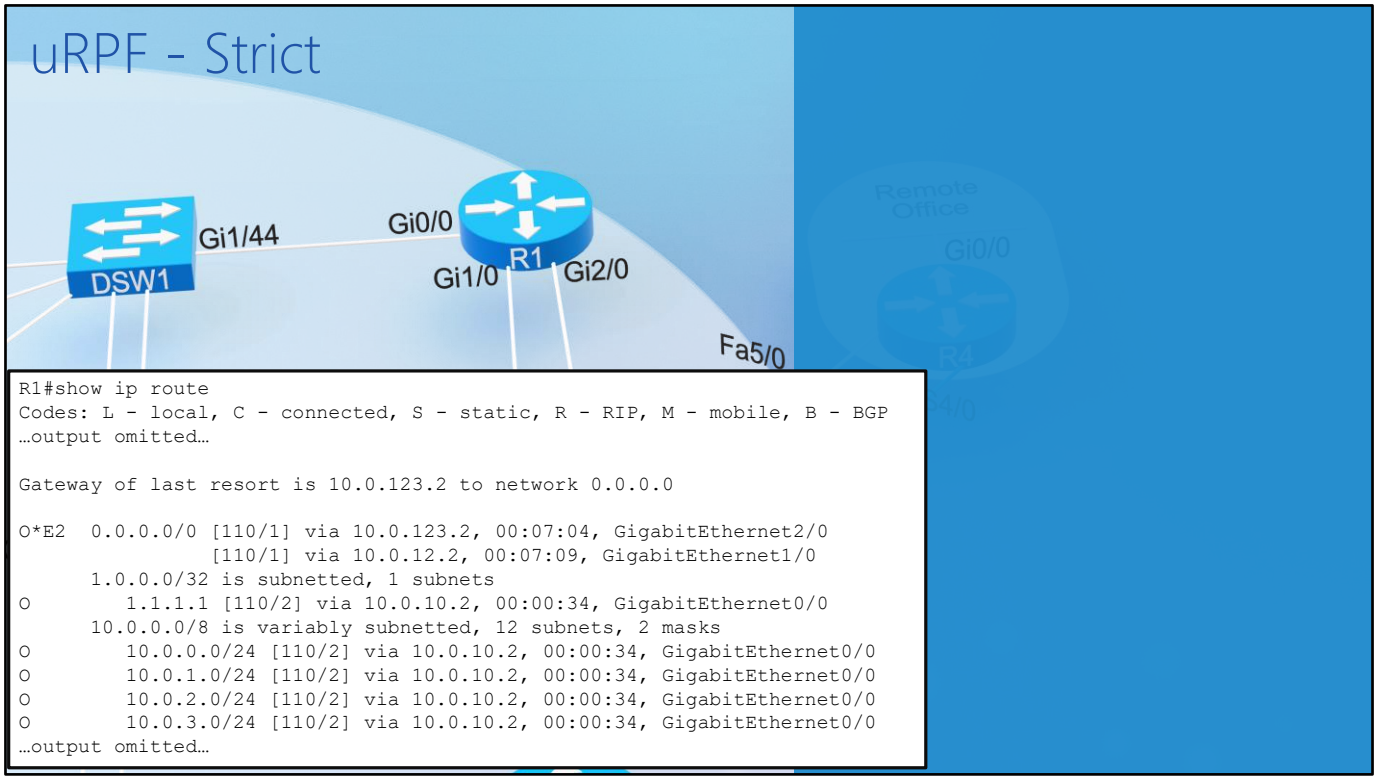
It is available on IOS routers, IOS L3 switches, ASAs.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



NOTE: there is also something known as VRF mode which is used for VRFs so that uRPF is VRF specific.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



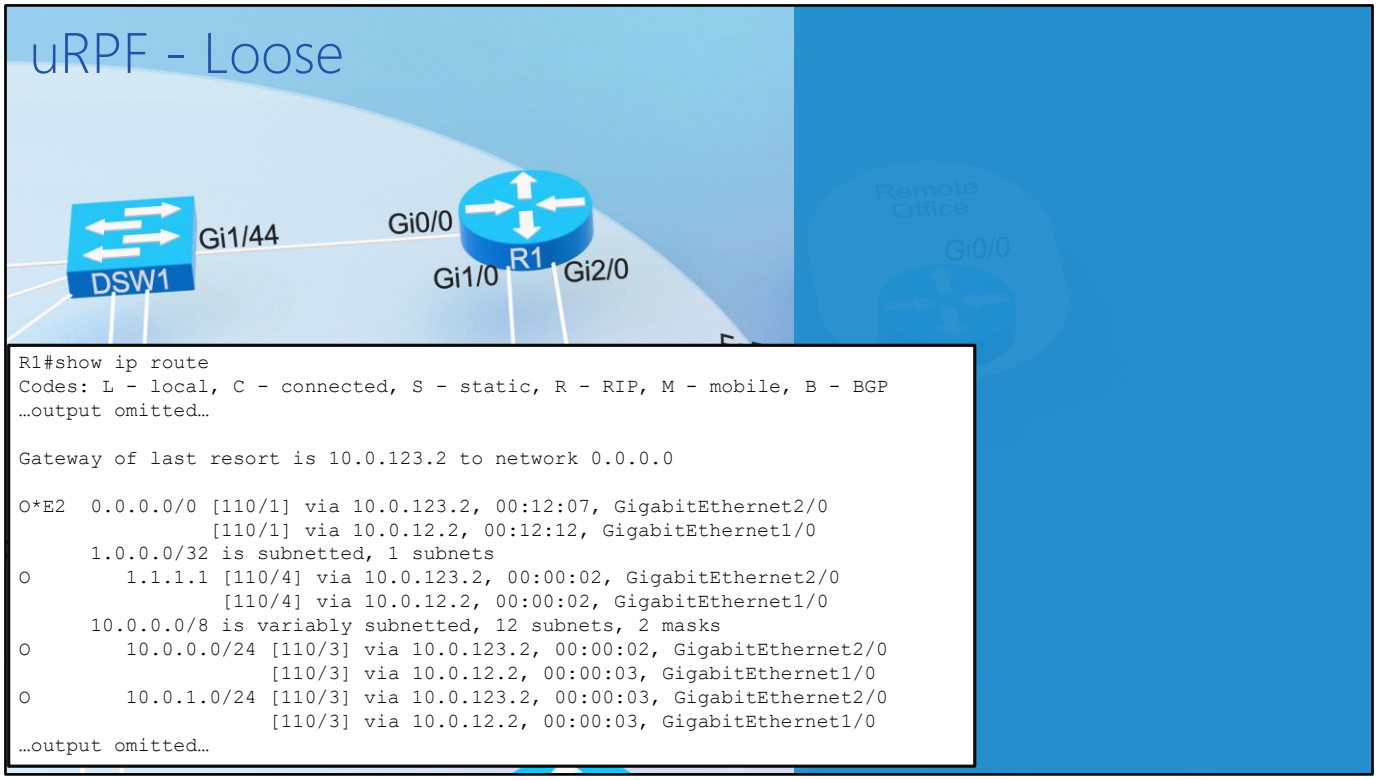

```
R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
…output omitted…

Gateway of last resort is 10.0.123.2 to network 0.0.0.0

O*E2  0.0.0.0/0 [110/1] via 10.0.123.2, 00:07:04, GigabitEthernet2/0
                [110/1] via 10.0.12.2, 00:07:09, GigabitEthernet1/0
      1.0.0.0/32 is subnetted, 1 subnets
O        1.1.1.1 [110/2] via 10.0.10.2, 00:00:34, GigabitEthernet0/0
      10.0.0.0/8 is variably subnetted, 12 subnets, 2 masks
O        10.0.0.0/24 [110/2] via 10.0.10.2, 00:00:34, GigabitEthernet0/0
O        10.0.1.0/24 [110/2] via 10.0.10.2, 00:00:34, GigabitEthernet0/0
O        10.0.2.0/24 [110/2] via 10.0.10.2, 00:00:34, GigabitEthernet0/0
O        10.0.3.0/24 [110/2] via 10.0.10.2, 00:00:34, GigabitEthernet0/0
…output omitted…
```

Example:
Let's say uRPF strict mode has been enabled on Gi0/0
Packet arrives on R1 Gig 0/0 from 10.0.0.10 (PC 1)
uRPF extracts the IP source address and uses it to search the FIB to find the location of the network that matches the IP address. In this case 10.0.0.0/24.
If the FIB entry indicates that the return path to reach the network is out the interface Gi0/0 then the packet is valid and will be forwarded.
If the FIB entry indicates that the return path to reach the network is out any other interface other than Gi0/0 then the packet is dropped.

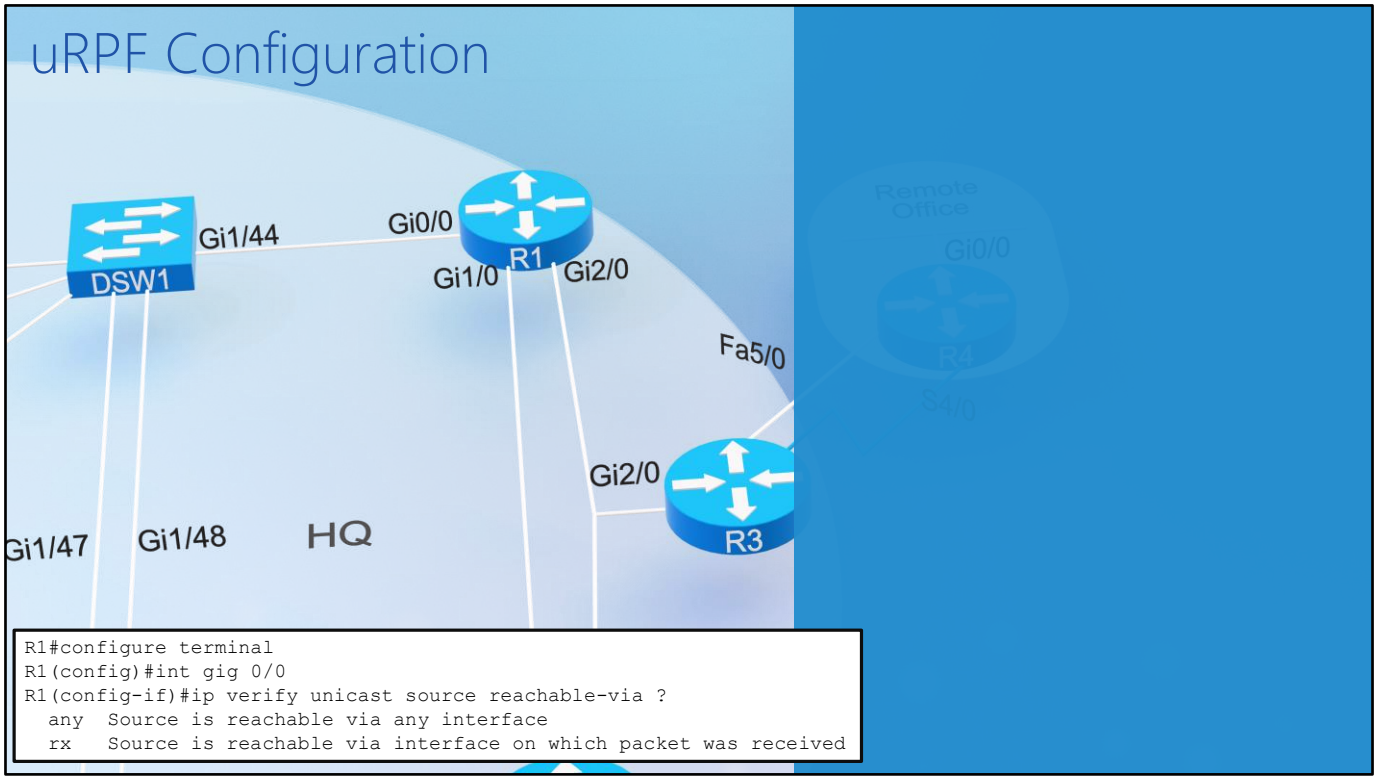
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Example:
Let's say uRPF loose mode has been enabled on Gi0/0
Packet arrives on R1 Gig 0/0 from 10.0.0.10 (PC 1)
uRPF extracts the IP source address and uses it to search the FIB to find if the router has an entry in the table for the network the packet belongs to. In this case 10.0.0.0/24.
If the FIB contains the network the packet is valid and will be forwarded.
If the FIB does not contain the network the packet is dropped.

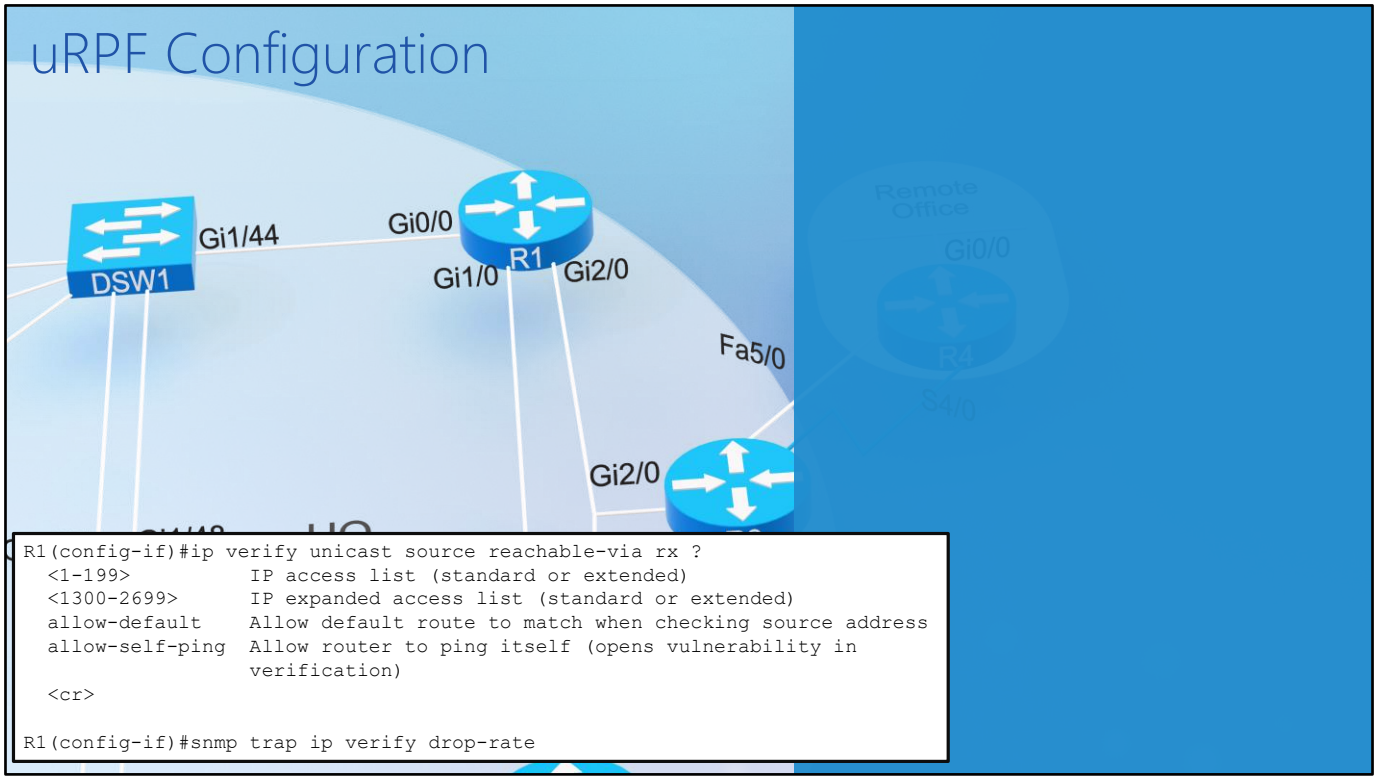
So in this case even though the packet arrival interface and return interface are different (asymmetric routing) uRPF will still forward the packet.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Note that CEF is required for uRPF to work.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Allow-default – used if you want the default route to be considered a valid route for validation. By default it is not. With strict the ingress interface would have to match the interface the default route is using for the packet to be valid. With loose the default route just has to exist which really defeats the purpose of setting up uRPF. So it is recommended that you do not use this option with Loose.

Allow-self-ping – used to allow the router to ping its own interface. Without… the packets are not considered valid and they are dropped. (R1 ping 10.0.10.1 would fail without this option)

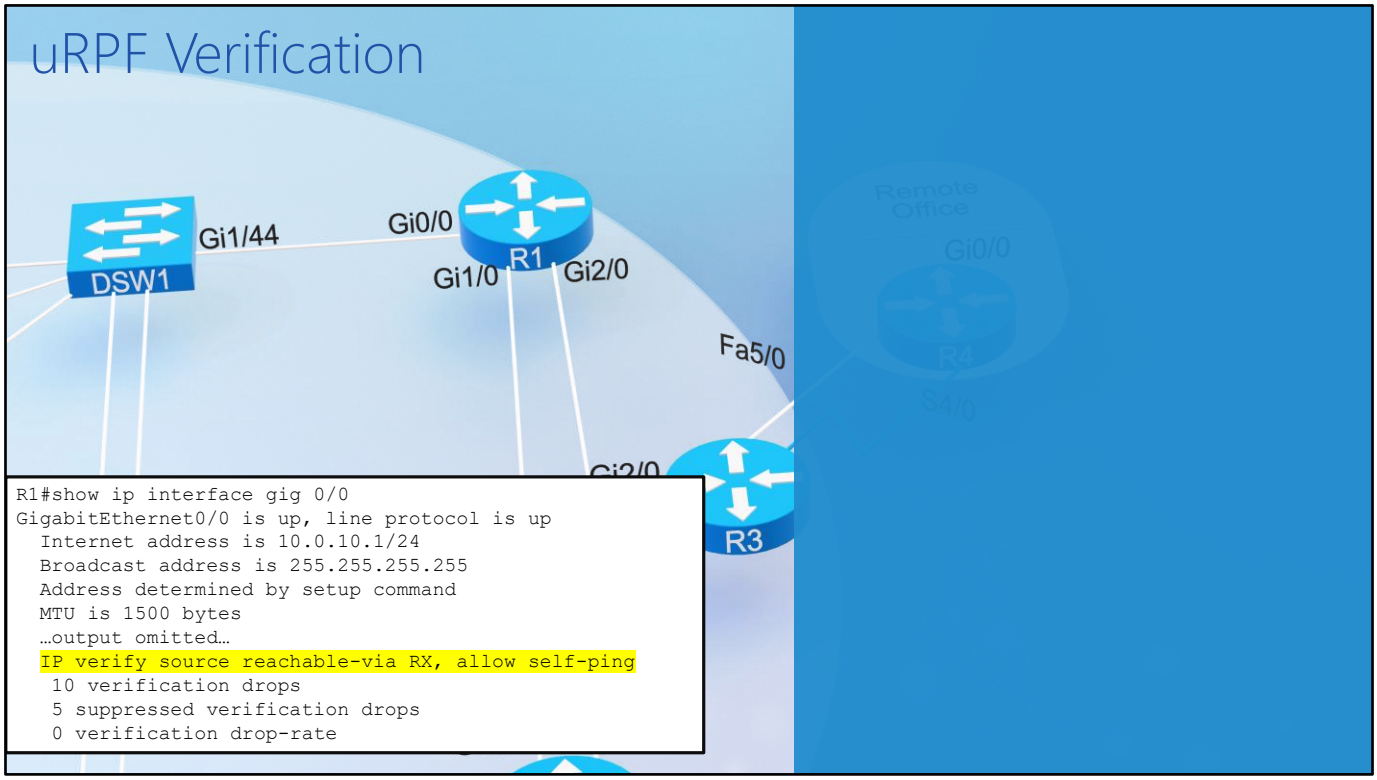
ACLs – used to create an exception list that would override the uRPF decision. For example, you can make an exception to ensure that no matter what…. packets from a certain IP or range of Ips are always forwarded no matter what uRPF decides. Example (access-list 100 permit ip 10.0.0.0/24 0.0.0.255 any)

Or you might just want to log with syslog all uRPF dropped hits. You can do that with for example (access-list 100 deny ip any log-input)

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

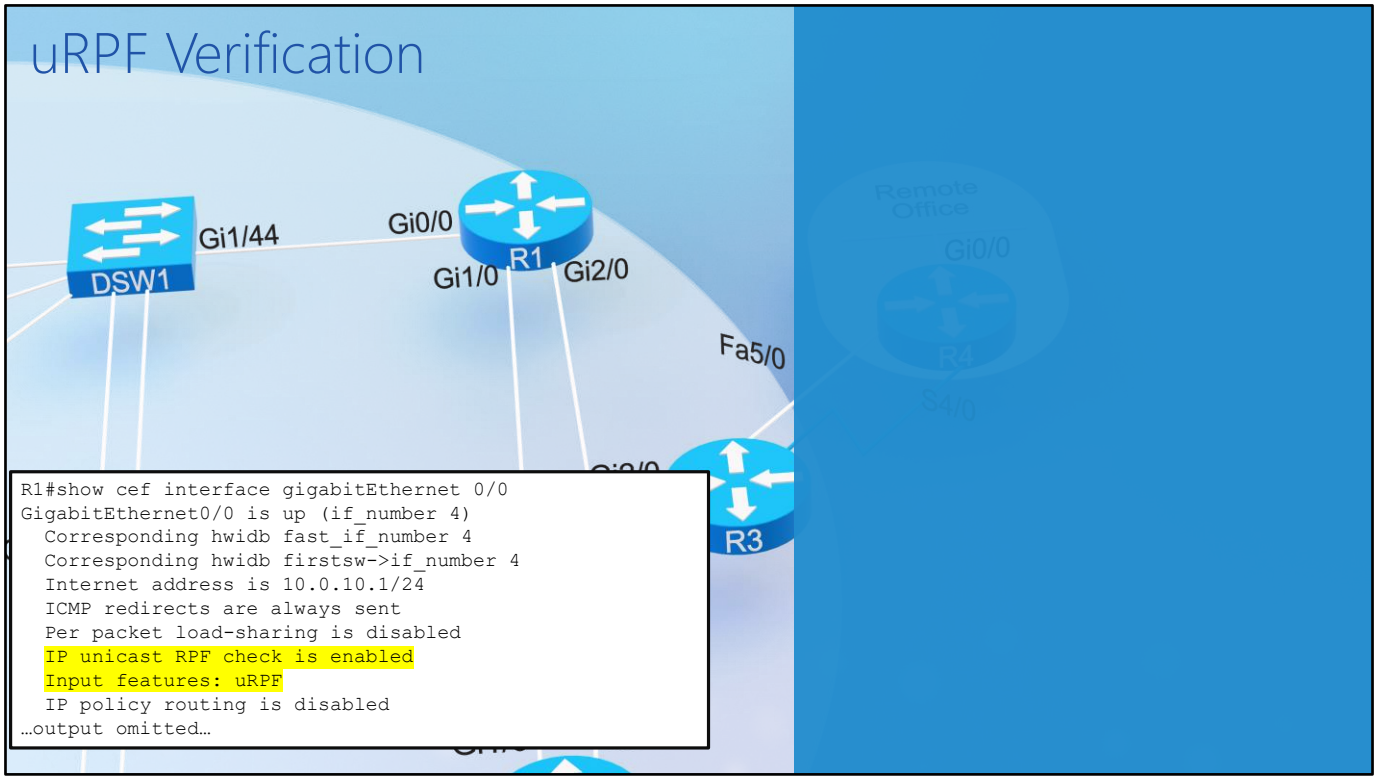
snmp trap ip verify drop-rate – this is used to configure uRPF to send all uRPF-related traps to all configured SNMP server destinations that have been set up on the device.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



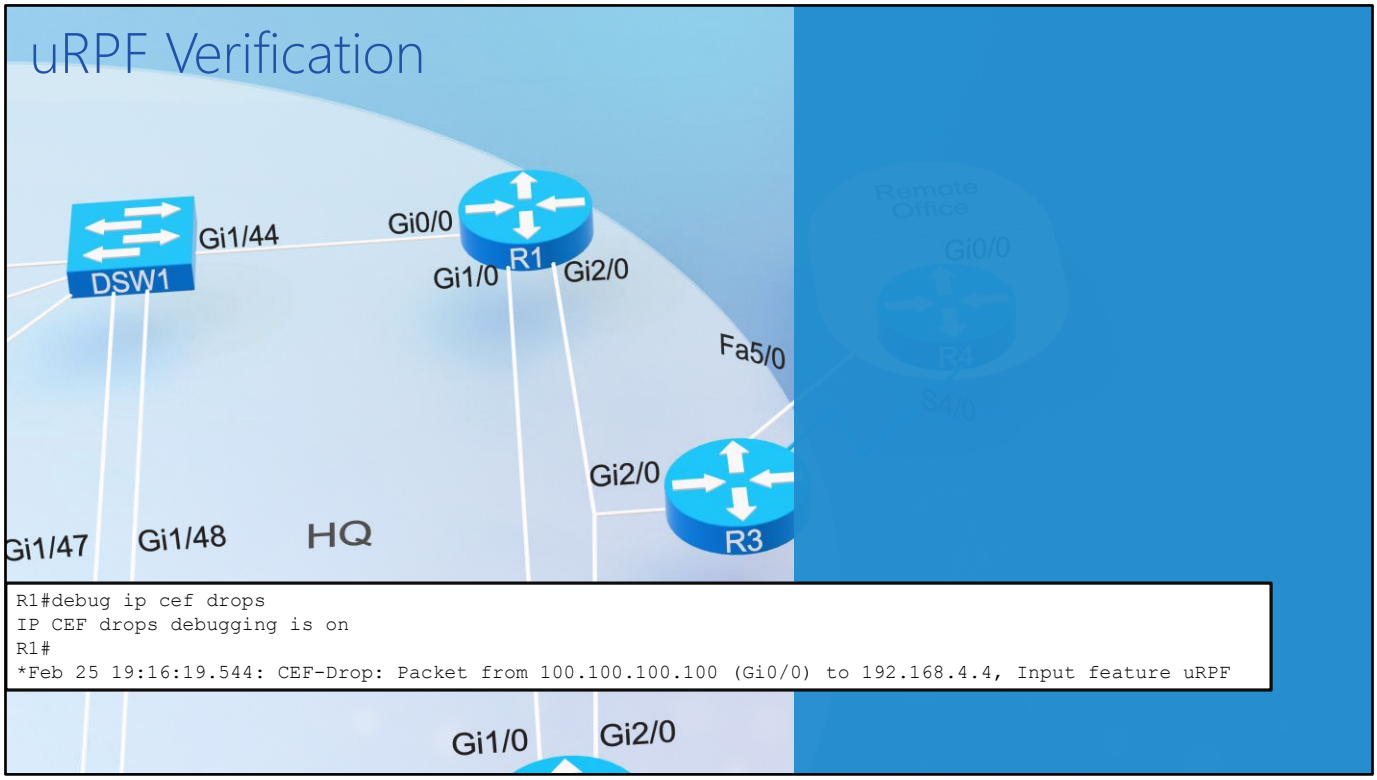
Verify if uRPF is enabled on the interface and the number of drops.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



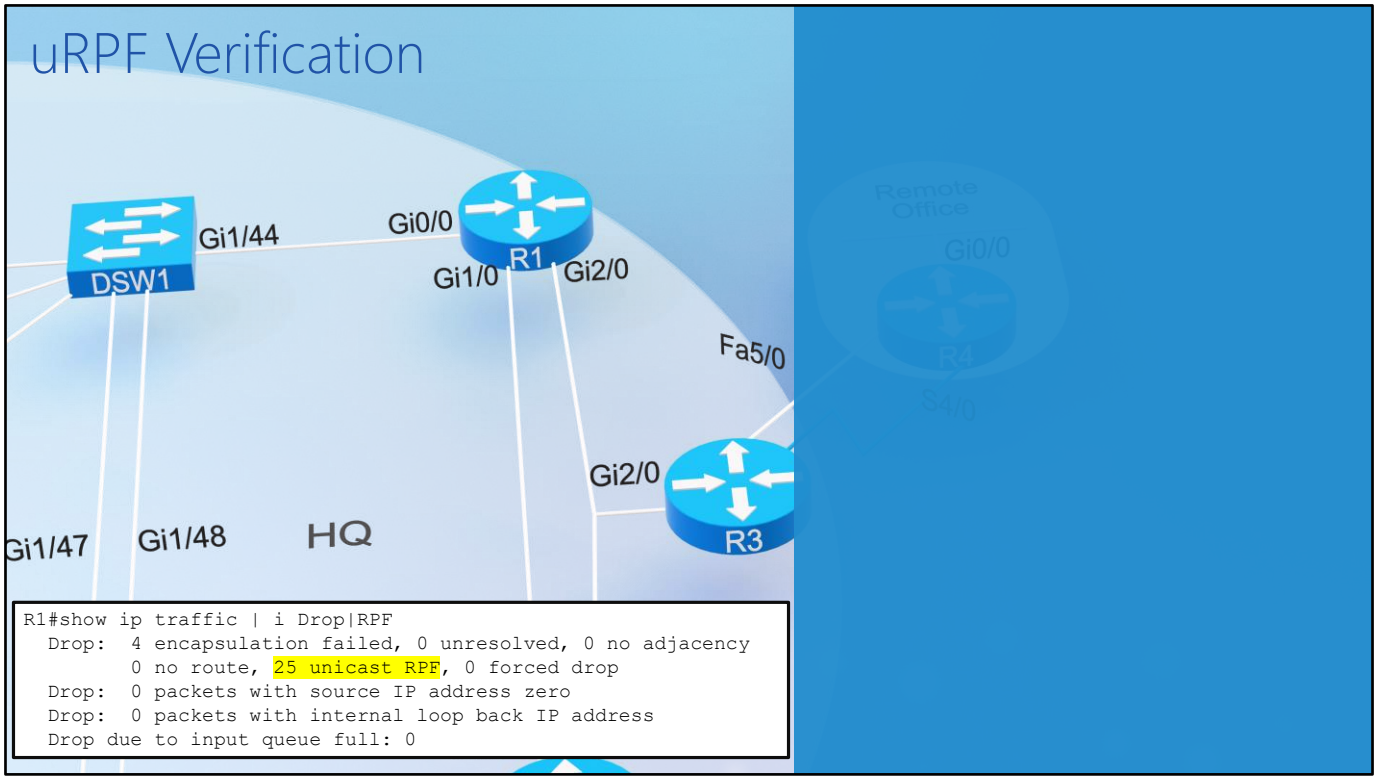
Verify if uRPF is enabled on the interface.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



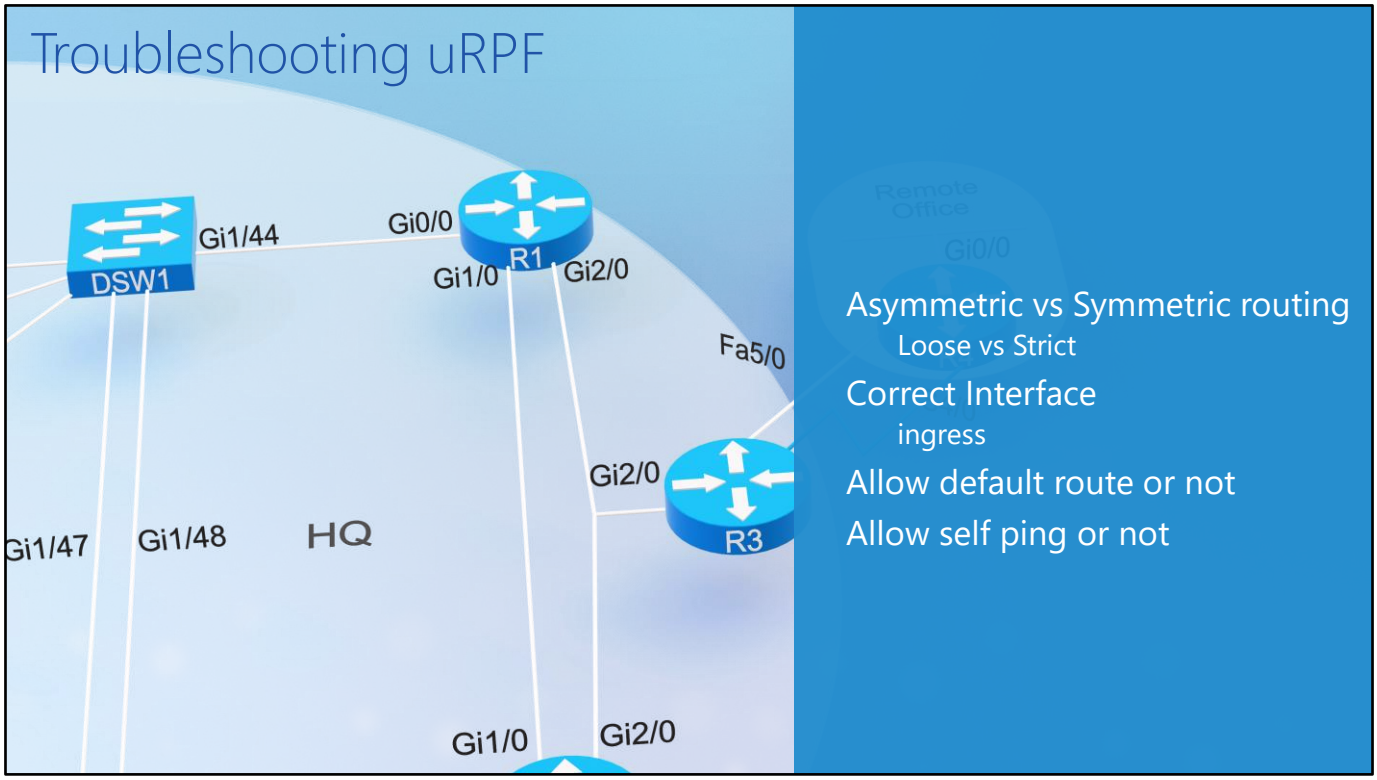
Verify if uRPF drops in real time.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



See number of ip traffic drops due to uRPF.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



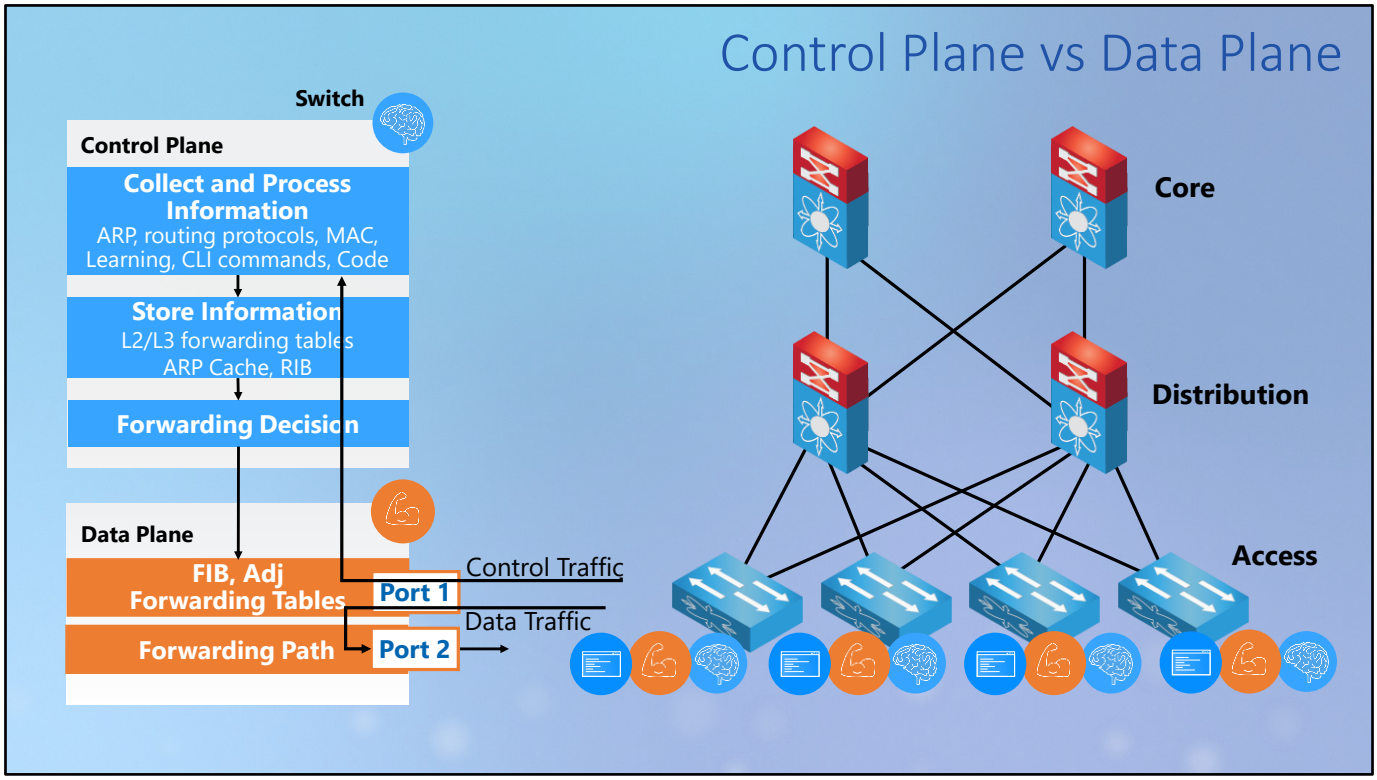
See number of ip traffic drops due to uRPF.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Title slide

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



https://www.cisco.com/c/en/us/about/security-center/copp-best-practices.html

IP carries all packets within a single pipe. Thus, IP network devices such as routers and switches must be able to distinguish between data plane, control plane, and management plane packets to treat each packet appropriately.

Data plane packets – End-station, user-generated packets that are always forwarded by network devices to other end-station devices. From the perspective of the network device, data plane packets always have a transit destination IP address and can be handled by normal, destination IP address-based forwarding processes.

Control plane packets – Network device generated or received packets that are used for the creation and operation of the network itself. From the perspective of the network device, control plane packets always have a receive destination IP address and are handled by the CPU in the network device route processor. Examples include protocols such as ARP, BGP, OSPF, and other protocols that glue the network together.

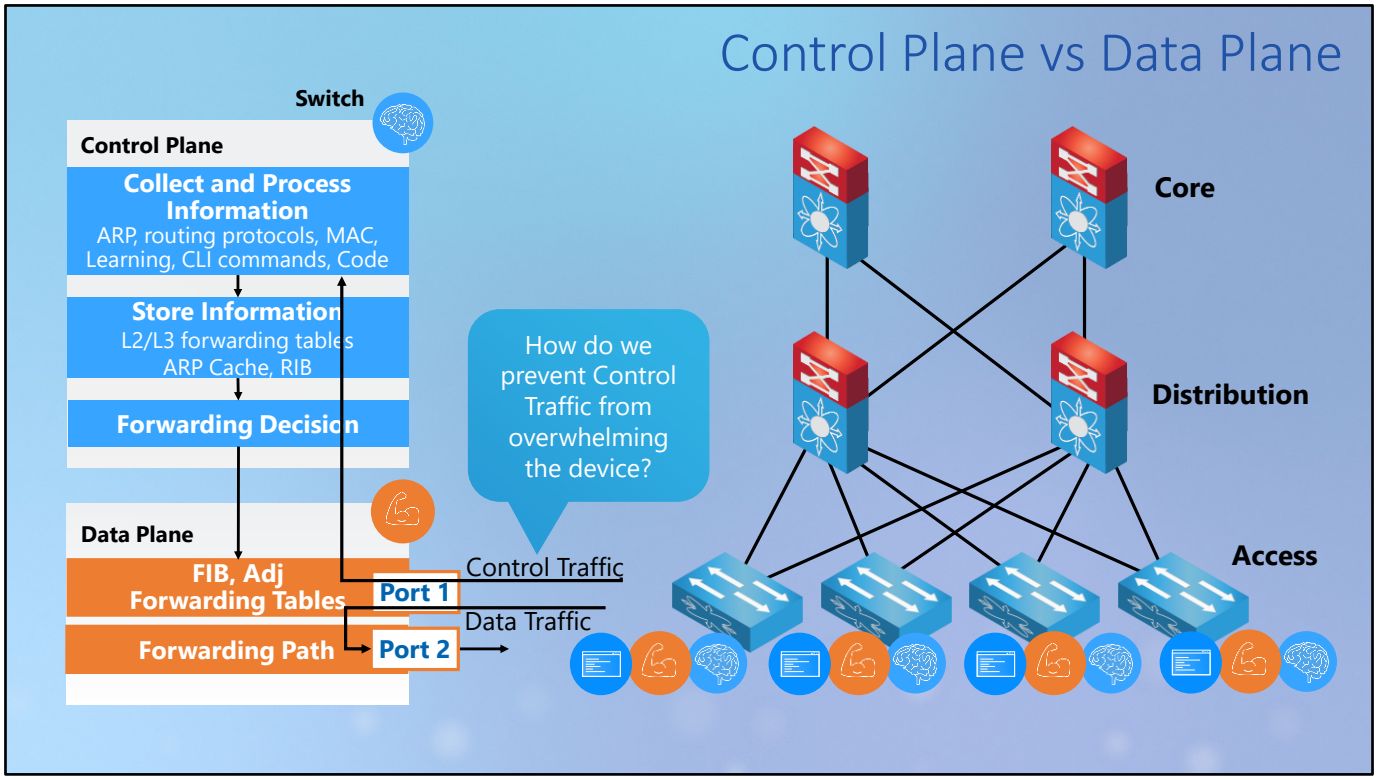
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Management plane – You also have the management plane where device configuration and monitoring is done by an admin using protocols like telnet, ssh, snmp, etc.

Services plane - ?????

“Punt” is often used to describe the action of moving a packet from the fast path (data plane) to the route processor (control plane) for handling.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



https://www.cisco.com/c/en/us/about/security-center/copp-best-practices.html

Under normal network operating conditions, the vast majority of packets handled by network devices are data plane packets. (TCP/UDP) (Voice, Video, Data). These packets are handled in the fast path. Network devices are optimized to handle these fast path packets efficiently. Typically, considerably fewer control and management plane packets are required to create and operate IP networks. Thus, the punt path and route processor are significantly less capable of handling the kinds of packets rates experienced in the fast path since they are never directly involved in the forwarding of data plane packets.

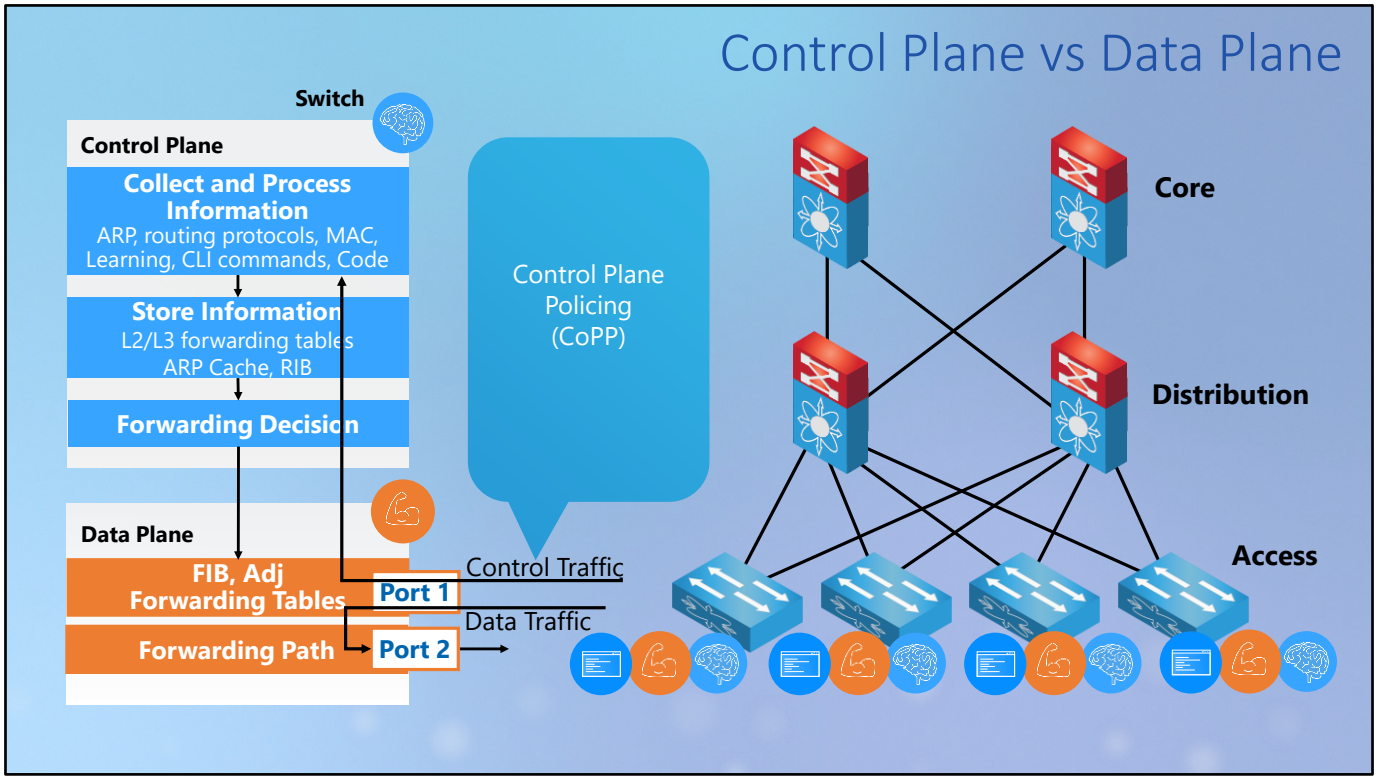
When high packet rates overload the control and/or management plane, route processor resources can be overwhelmed, reducing the availability of these resources for tasks critical to the operation and maintenance of the network. For example, if a high volume of rogue packets generated by a virus or worm is presented to the control plane, the router will spend an excessive amount of time processing and discarding unnecessary traffic. The route processor is thus not available to support its required tasks such as computing periodic routing

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

table updates, maintaining the CEF table, which is actually used for the forwarding of data plane packets, and maintaining interface link states

When considering route processor attack scenarios, it is natural to think only of malicious events. However, both malicious and non-malicious events can overwhelm route processor resources. Malicious events include crafted packet attacks or simply high rates of packets directed at the control plane. Non-malicious events may result from router or network misconfigurations, software bugs, or in some circumstances, network failure reconvergence events. From the perspective of the router, the underlying condition is irrelevant when the result is the same. It is important to take appropriate steps to protect the route processor from being overwhelmed, whether by malicious or non-malicious events.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

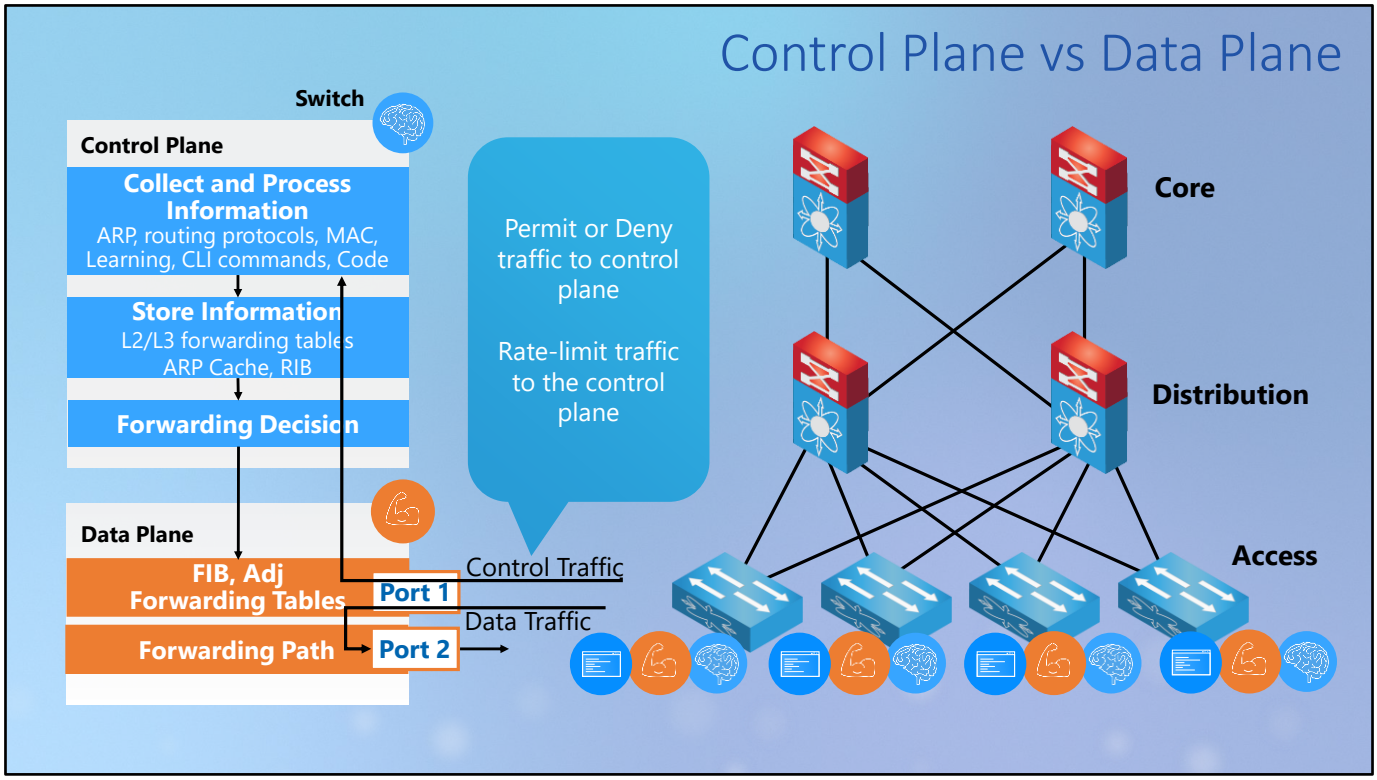


https://www.cisco.com/c/en/us/about/security-center/copp-best-practices.html

Control Plane Policing (CoPP) – CoPP is the Cisco IOS-wide route processor protection mechanism designed to allow users to manage the flow of traffic handled by the route processor of their network devices. CoPP is designed to prevent unnecessary traffic from overwhelming the route processor, memory, buffers, and ingress queues, that, if left unabated, could affect system performance. CoPP is deployed once to the punt path of the router and applies to all packets that punt to the route processor for handling.

Although we keep saying control plane… let's not forget about management plane traffic here. When you telnet, ssh, or use various management protocols they are punted to the control plane as well for processing. So to ensure that your device is not overwhelmed by management protocol traffic you can use CoPP.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



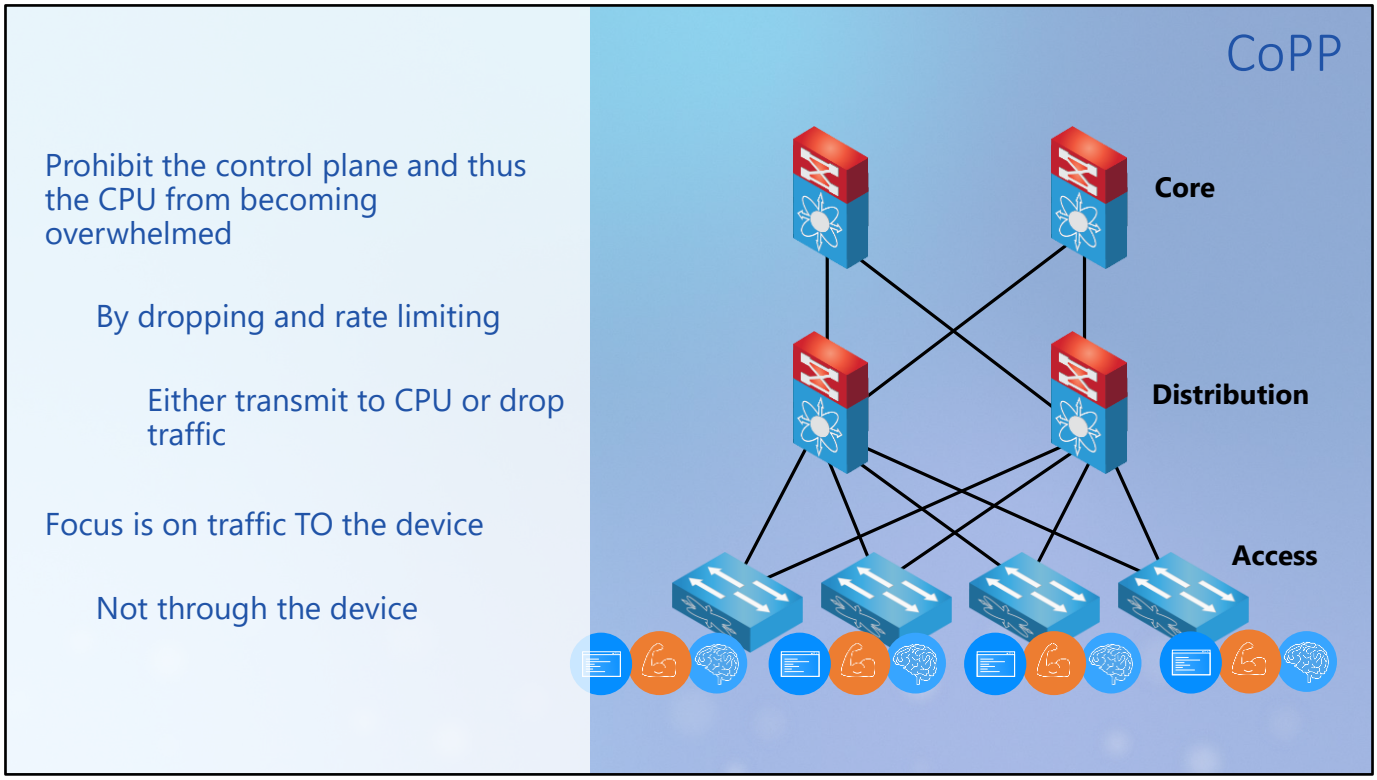
https://www.cisco.com/c/en/us/about/security-center/copp-best-practices.html

Control Plane Policing (CoPP) – CoPP is the Cisco IOS-wide route processor protection mechanism designed to allow users to manage the flow of traffic handled by the route processor of their network devices. CoPP is designed to prevent unnecessary traffic from overwhelming the route processor, memory, buffers, and ingress queues, that, if left unabated, could affect system performance. CoPP is deployed once to the punt path of the router and applies to all packets that punt to the route processor for handling.

Although we keep saying control plane… let's not forget about management plane traffic here. When you telnet, ssh, or use various management protocols they are punted to the control plane as well for processing. So to ensure that your device is not overwhelmed by management protocol traffic you can use CoPP.

This traffic includes (control plane), (management plane), and (slow data plane path traffic)

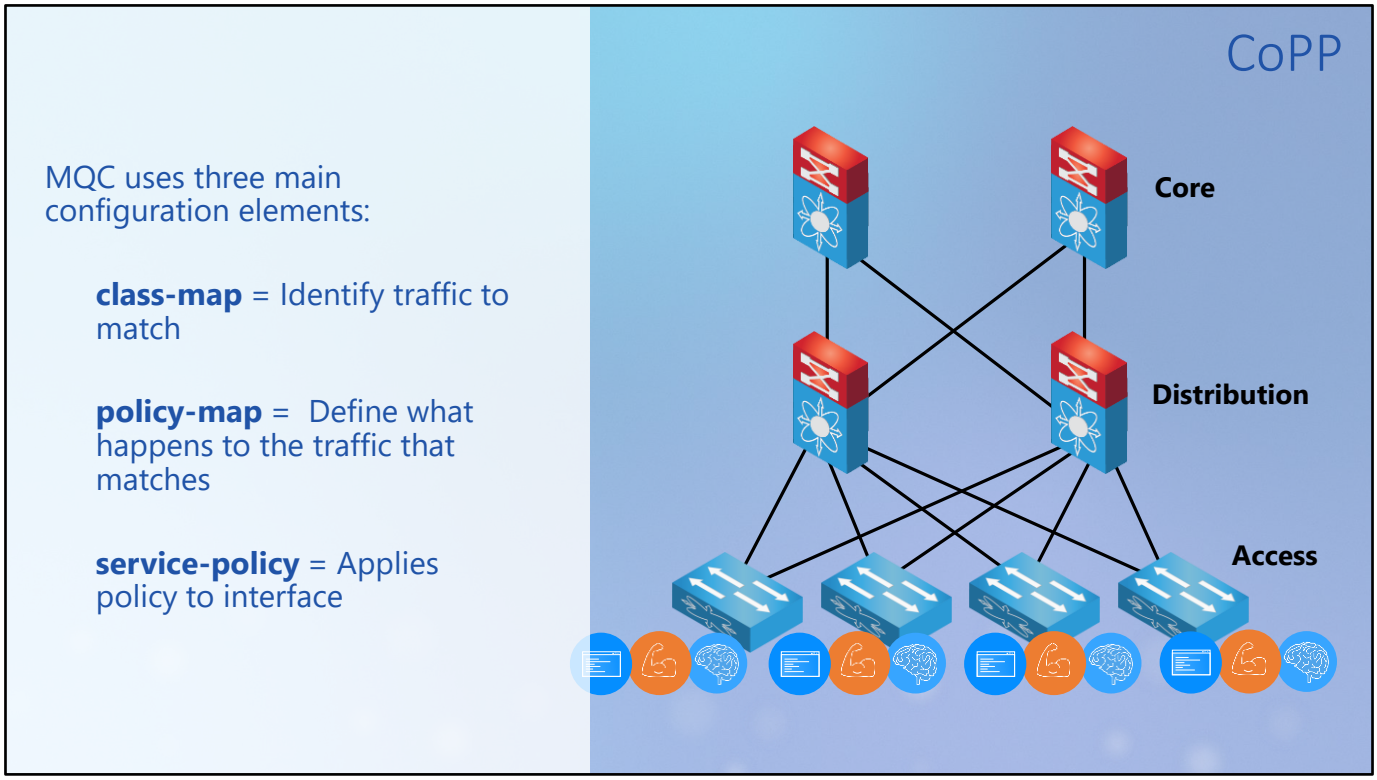
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



https://www.cisco.com/c/en/us/about/security-center/copp-best-practices.html

CoPP

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

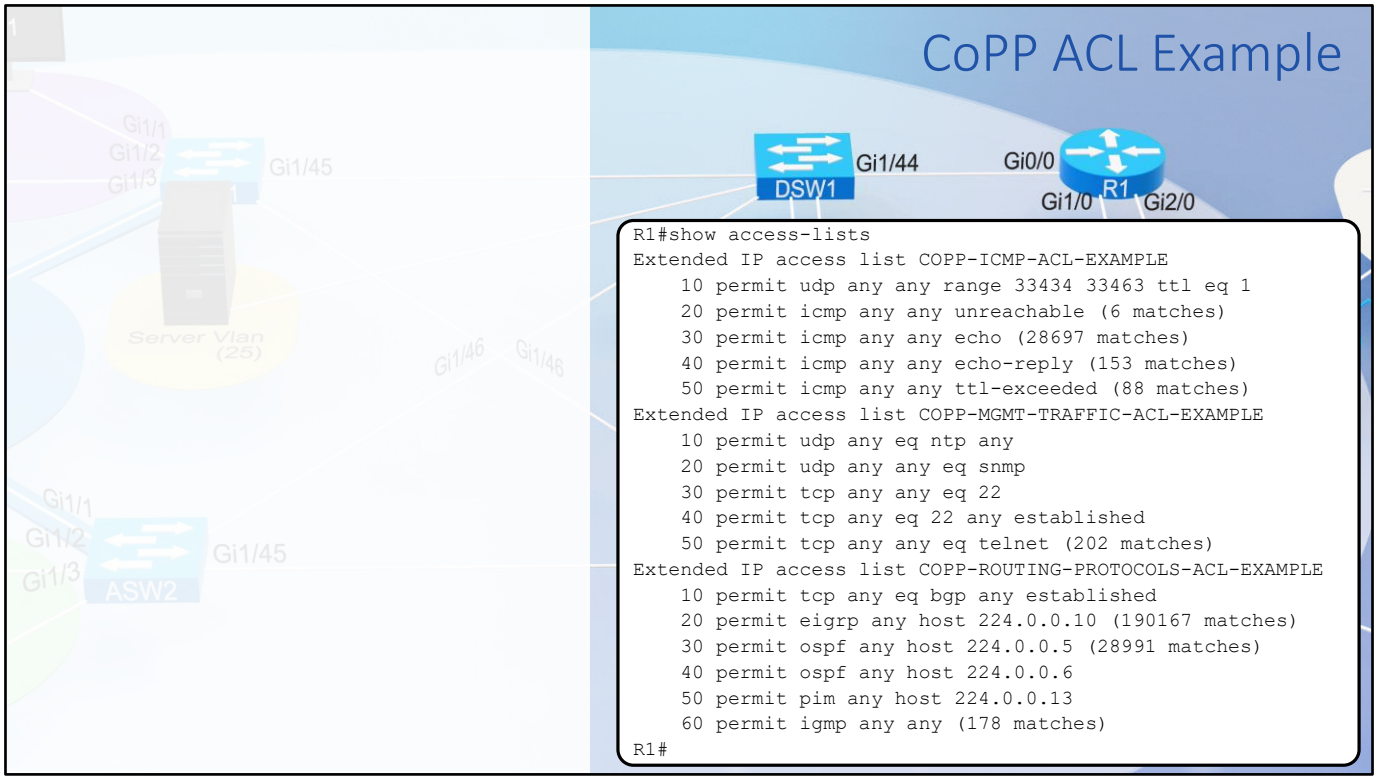


https://www.cisco.com/c/en/us/about/security-center/copp-best-practices.html

CoPP is implemented using the Modular QoS CLI (MQC) framework for policy construction. In this way, in addition to simply permit and deny functions, specific packets may be permitted but rate-limited. This behavior substantially improves the ability to define an effective CoPP policy. (Note: that "Control Plane Policing" is something of a misnomer because CoPP generally protects the punt path to the route processor and not solely the control plane.)

NOTE: It is important to note that MQC is a general framework used for enabling all QoS throughout Cisco IOS, and not exclusively for CoPP. Not all features available within the MQC framework are available or applicable to CoPP policies. For example, only certain classification (match) criteria are applicable to CoPP. In some instances, there are MQC platform and/or IOS-dependencies that may apply to CoPP.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



RATE LIMITING EXAMPLE FIRST AND THEN A DROP EXAMPLE.

For initial or pilot CoPP deployments, you may wish to be less restrictive on IP source and destination addresses. Over time and with more experience, refinements may be appropriate.

For example:
Permit eigrp any any
Permit ospf any any
Permit icmp any any

And then get more granular over time.

**********Troubleshooting**********
When troubleshooting ACLs for CoPP, you need to focus on the following:
■ Grouping: When grouping traffic types together, ensure that they are grouped based on function within the network. For example, routing protocols (BGP, OSPF, and EIGRP) may be grouped together, and management protocols (SSH, Telnet,

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

HTTP(s), TFTP, SNMP, NTP, and DNS) may be grouped together. If you mix and match various protocols, the policies you apply later may not work for the type of traffic in question.

■ Action: With ACLs, you can specify a permit or deny action. For CoPP, permit means to match the traffic and apply the policy. Deny means to exclude that traffic from the class and move on to the next class. So, if you are troubleshooting a CoPP scenario and there is a class that is not being applied but should be, check to see if the ACL is a permit or deny. If it is a deny, that is likely the reason the traffic is not matching that class.

■ Protocol: In an ACL, you can define a protocol that you want to match. If the wrong protocol is specified in the ACL, then the wrong type of traffic will be matched in the class. So, when troubleshooting, verify that the correct protocol is being specified in the ACL.

■ Source and destination: Because ACLs allow you to specify source and destination addresses, you can be granular with your CoPP policies and match only if the traffic is from a specific source or destination. Therefore, it is imperative that the ACLs have the correct source and destination IP addresses applied, or the traffic will not be matched when it should be. When troubleshooting scenarios where specific source and destination IP addresses are used in the ACL, it is recommended that you change the IPs in the ACL to any / any. If the match is successful, then there is an issue with the original IP addresses. If not, the IP addresses were likely not the problem.

Operators and ports: Protocols, applications, and services all have port numbers associated with them. ACLs allow you to define operators such as greater-than, less-than, and equal-to and port numbers such as 179, 21, 22, 23, 80, and 443. Ensuring that you have the correct operator and port numbers defined in your ACLs is paramount for CoPP success.

Avoid using log and log-input with CoPP. These keywords have been known to cause unexpected variable results with CoPP operations, so Cisco recommends to avoid them.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

CoPP ACL Example

Troubleshooting:

- Grouping
- Action
- Protocol
- Source and Destination
- Operators and Ports
- Log / Log-input




```
R1#show access-lists
Extended IP access list COPP-ICMP-ACL-EXAMPLE
    10 permit udp any any range 33434 33463 ttl eq 1
    20 permit icmp any any unreachable (6 matches)
    30 permit icmp any any echo (28697 matches)
    40 permit icmp any any echo-reply (153 matches)
    50 permit icmp any any ttl-exceeded (88 matches)
Extended IP access list COPP-MGMT-TRAFFIC-ACL-EXAMPLE
    10 permit udp any eq ntp any
    20 permit udp any any eq snmp
    30 permit tcp any any eq 22
    40 permit tcp any eq 22 any established
    50 permit tcp any any eq telnet (202 matches)
Extended IP access list COPP-ROUTING-PROTOCOLS-ACL-EXAMPLE
    10 permit tcp any eq bgp any established
    20 permit eigrp any host 224.0.0.10 (190167 matches)
    30 permit ospf any host 224.0.0.5 (28991 matches)
    40 permit ospf any host 224.0.0.6
    50 permit pim any host 224.0.0.13
    60 permit igmp any any (178 matches)
R1#
```

For initial or pilot CoPP deployments, you may wish to be less restrictive on IP source and destination addresses. Over time and with more experience, refinements may be appropriate.

For example:
Permit eigrp any any
Permit ospf any any
Permit icmp any any

And then get more granular over time.

**********Troubleshooting**********
When troubleshooting ACLs for CoPP, you need to focus on the following:
■ Grouping: When grouping traffic types together, ensure that they are grouped based on function within the network. For example, routing protocols (BGP, OSPF, and EIGRP) may be grouped together, and management protocols (SSH, Telnet, HTTP(s), TFTP, SNMP, NTP, and DNS) may be grouped together. If you mix and match various protocols, the policies you apply later may not work for the type of traffic in

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

question.

■ Action: With ACLs, you can specify a permit or deny action. For CoPP, permit means to match the traffic and apply the policy. Deny means to exclude that traffic from the class and move on to the next class. So, if you are troubleshooting a CoPP scenario and there is a class that is not being applied but should be, check to see if the ACL is a permit or deny. If it is a deny, that is likely the reason the traffic is not matching that class.

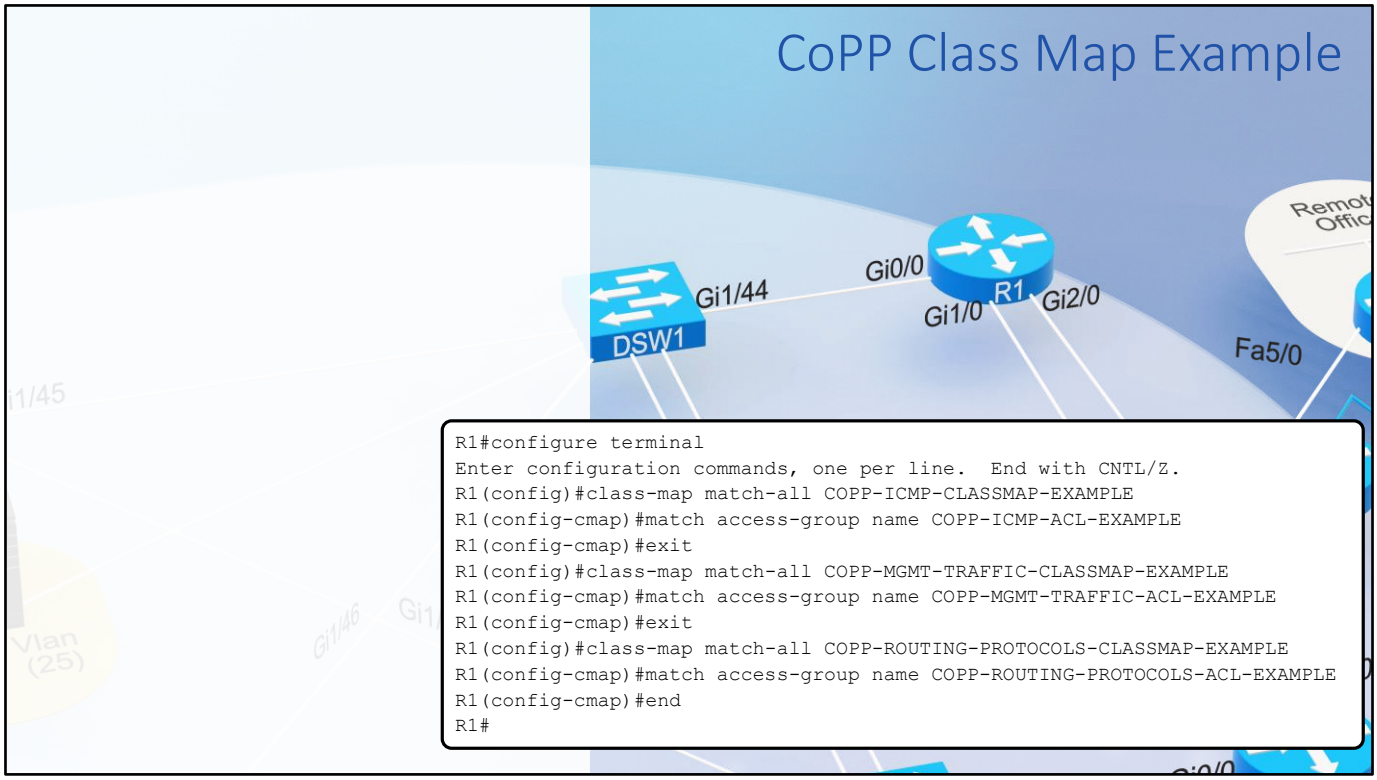
■ Protocol: In an ACL, you can define a protocol that you want to match. If the wrong protocol is specified in the ACL, then the wrong type of traffic will be matched in the class. So, when troubleshooting, verify that the correct protocol is being specified in the ACL.

■ Source and destination: Because ACLs allow you to specify source and destination addresses, you can be granular with your CoPP policies and match only if the traffic is from a specific source or destination. Therefore, it is imperative that the ACLs have the correct source and destination IP addresses applied, or the traffic will not be matched when it should be. When troubleshooting scenarios where specific source and destination IP addresses are used in the ACL, it is recommended that you change the IPs in the ACL to any / any. If the match is successful, then there is an issue with the original IP addresses. If not, the IP addresses were likely not the problem.

Operators and ports: Protocols, applications, and services all have port numbers associated with them. ACLs allow you to define operators such as greater-than, less-than, and equal-to and port numbers such as 179, 21, 22, 23, 80, and 443. Ensuring that you have the correct operator and port numbers defined in your ACLs is paramount for CoPP success.

Avoid using log and log-input with CoPP. These keywords have been known to cause unexpected variable results with CoPP operations, so Cisco recommends to avoid them.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



In MQC, the **class-map** command is used to define a traffic class. A traffic class contains three major elements: a name, one or a series of match commands, and an instruction on how to evaluate these match commands. Match commands are used to specify various criteria for classifying packets. Packets are checked to see whether they match the criteria specified in the match commands. If a packet matches the specified criteria, that packet is considered a member of the class and is treated according to the QoS specifications set in the service policy. Packets that fail to meet any of the matching criteria are classified as members of the default class.

The instruction for evaluating match commands is specified as either **match-any** or **match-all**. When more than one match statement is included, match-any requires that a packet match at least one of the statements to be included in the class. If match-all is used, a packet must match all of the statements to be included in the class.

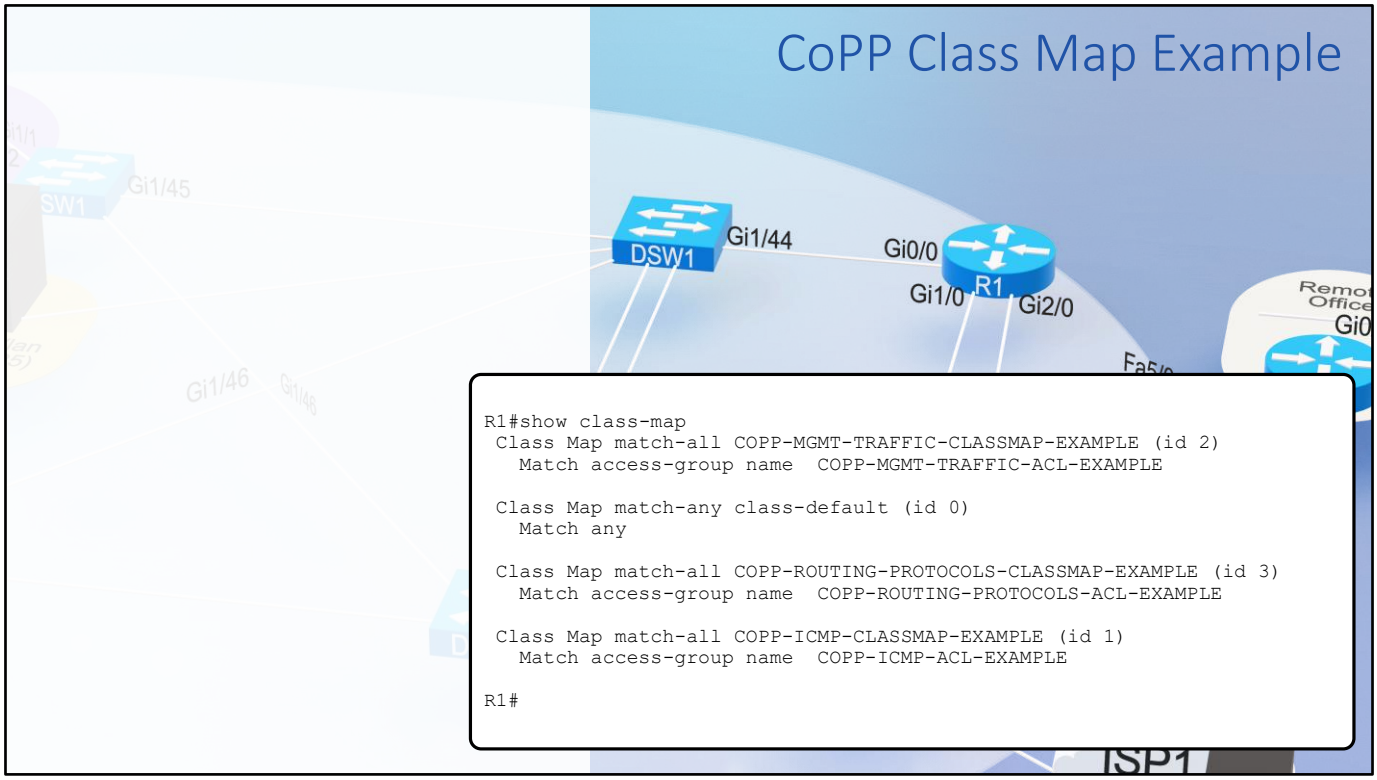
the **match** keyword supports the following classification mechanisms for CoPP: Standard and extended numbered or named IP access lists (ACLs) using the match access-group keyword. (In certain Cisco IOS releases, named ACLs may

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

not be available for CoPP use).
IP TOS values, including match ip dscp and match ip precedence keywords.
ARP protocol packets using match protocol arp command. (The Cisco IOS 12.2SX release does not support the match protocol arp command.)

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

CoPP Class Map Example




```
R1#show class-map
 Class Map match-all COPP-MGMT-TRAFFIC-CLASSMAP-EXAMPLE (id 2)
   Match access-group name  COPP-MGMT-TRAFFIC-ACL-EXAMPLE

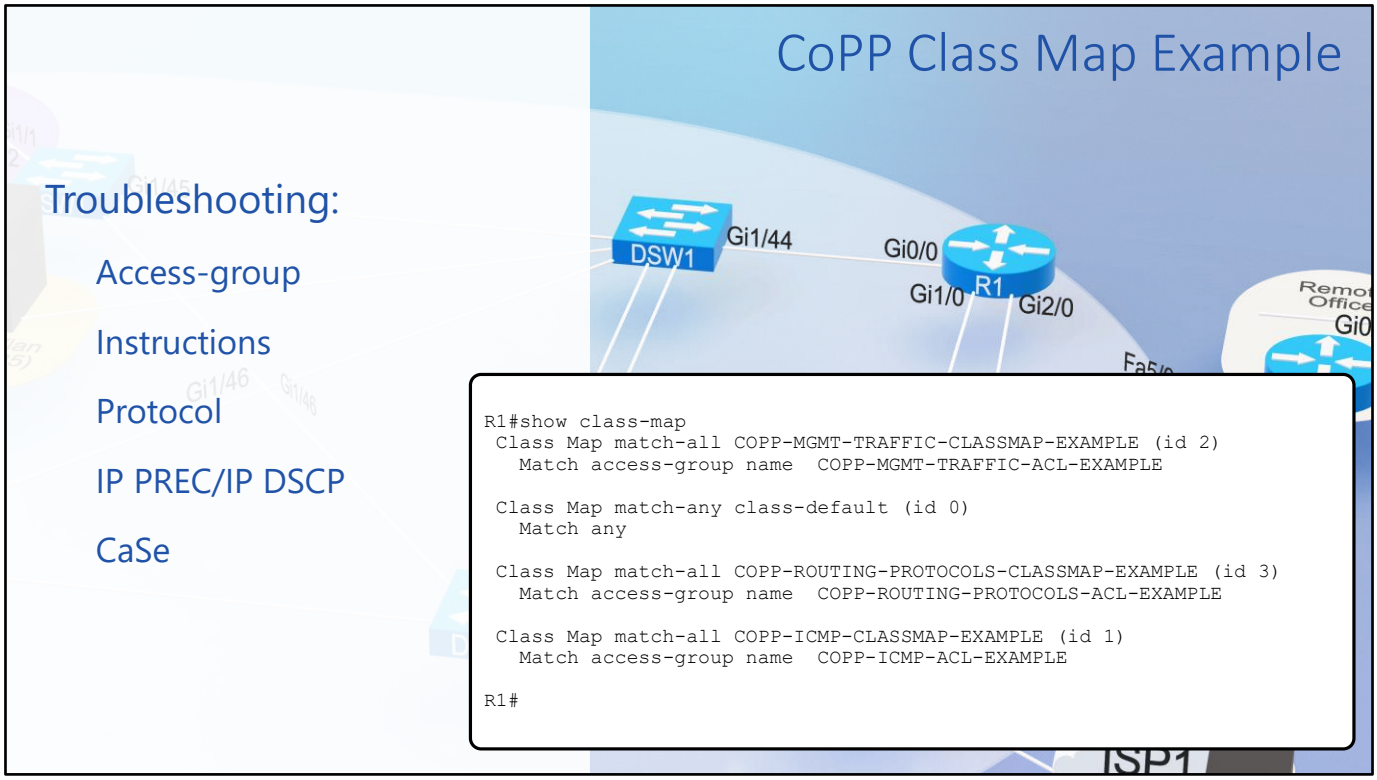
 Class Map match-any class-default (id 0)
   Match any

 Class Map match-all COPP-ROUTING-PROTOCOLS-CLASSMAP-EXAMPLE (id 3)
   Match access-group name  COPP-ROUTING-PROTOCOLS-ACL-EXAMPLE

 Class Map match-all COPP-ICMP-CLASSMAP-EXAMPLE (id 1)
   Match access-group name  COPP-ICMP-ACL-EXAMPLE

R1#
```

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



■ Access group: Is the correct ACL being used in the match command? The ACL in the class map is responsible for defining the interesting traffic (packets) that must be matched. If matched, the packets are classified as being members of the class, and the correct service policy applies. If the wrong ACL is applied, the desired results are not achieved. In addition, the ACL may not contain the correct protocol, or address, or operator, or port, or action, and therefore the traffic is not matched by the class map. If that is the case, you have to troubleshoot the ACL.

■ Instruction: A class map may contain one of two instructions: match-any or matchall. Using the correct instruction is important only if you have multiple match commands in the class map. If you have only one match command in the class map, the instruction does not matter. Let's say you do have multiple match commands in a single class map. If you use match-any, it means the traffic must match one of the match commands to be classified as part of the traffic class. If you use match-all, the traffic must match all the match commands to be part of the traffic class. This is where people get caught when troubleshooting. In Example 22-5, notice that the class map is using the match-all instruction. Based on the match commands and the ACLs, does this make sense? If you are not sure, think about whether it is possible for a packet

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

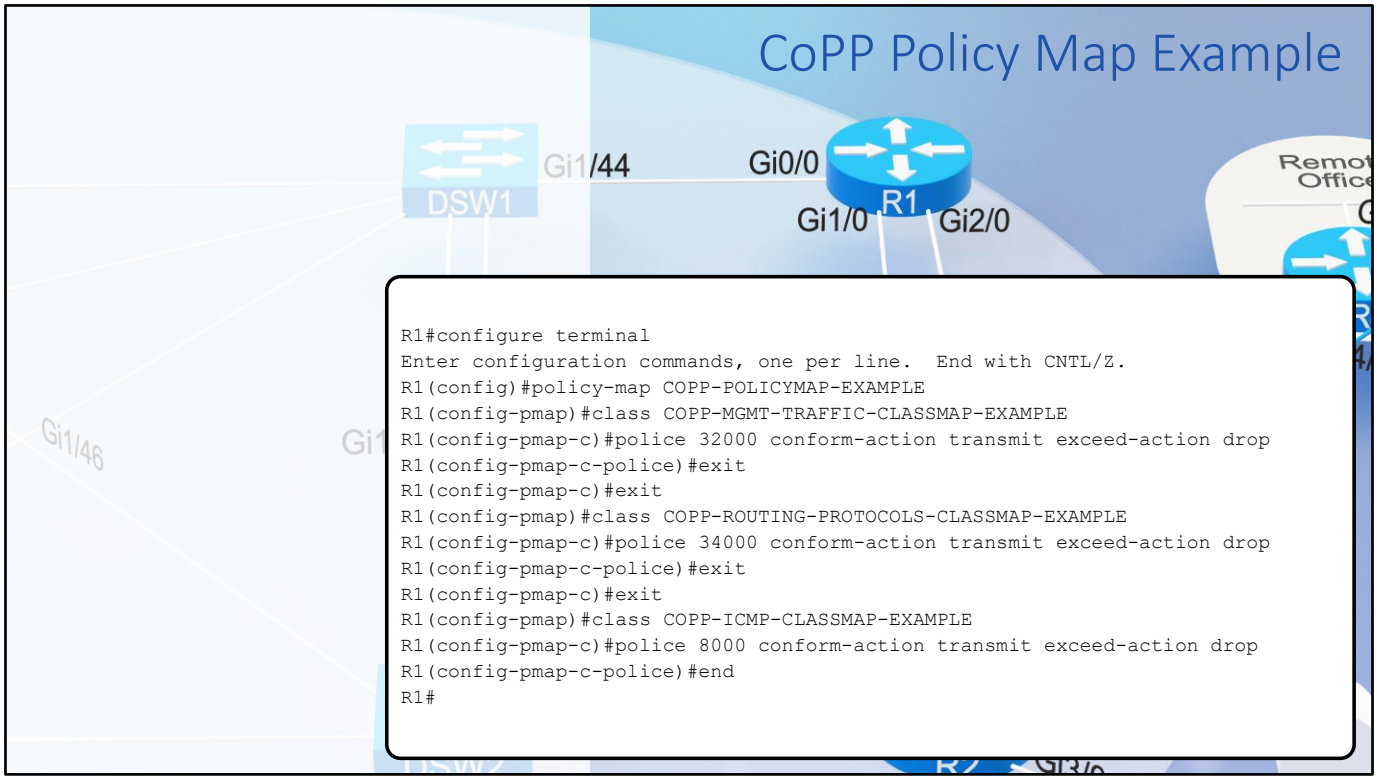
to be ICMP (Internet Control Message Protocol), BGP (Border Gateway Protocol), and EIGRP (Enhanced Interior Gateway Routing Protocol) at the same time. Of course it's not. So, the traffic would never match the CoPP-CLASS class map and therefore would never be subject to the implicit default class. In this case, the correct option would be the match-any instruction instead of the match-all instruction.

■ Protocol: If you choose not to use an ACL for matching, you can use the built-in protocol options of the match command. When using the protocol option, you must ensure that the correct protocol has been specified. For example, if you want to match ARP (Address Resolution Protocol) packets, you use the match protocol arp command.

■ IP PREC/IP DSCP: If you only need to match based on IP precedence or IP DSCP (Differentiated Services Code Point) values, you can use the ip prec or ip dscp options of the match command. Based on the traffic you want to match, make sure the correct one has been chosen and ensure that the correct values have been specified.

■ Case: ACL names are case sensitive. When specifying an ACL in a class map, doublecheck to make sure the name matches exactly.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



The **policy-map** command is used to associate a traffic class, defined by the **class-map** command, with one or more QoS policies. The result of this association is called a service policy. A service policy contains three elements: a name, a traffic class (specified with the **class** command), and the QoS policies. The purpose of the service policy is to associate a traffic class with one or more QoS policies. Classes included within policy maps are processed top-down. When a packet is found to match a class, no further processing is performed. That is, a packet can only belong to a single class, and it is the first one to which a match occurs. When a packet does not match any of the defined classes, it is automatically placed in the class **class-default**. The default class is always applied, whether it is explicitly configured or not.

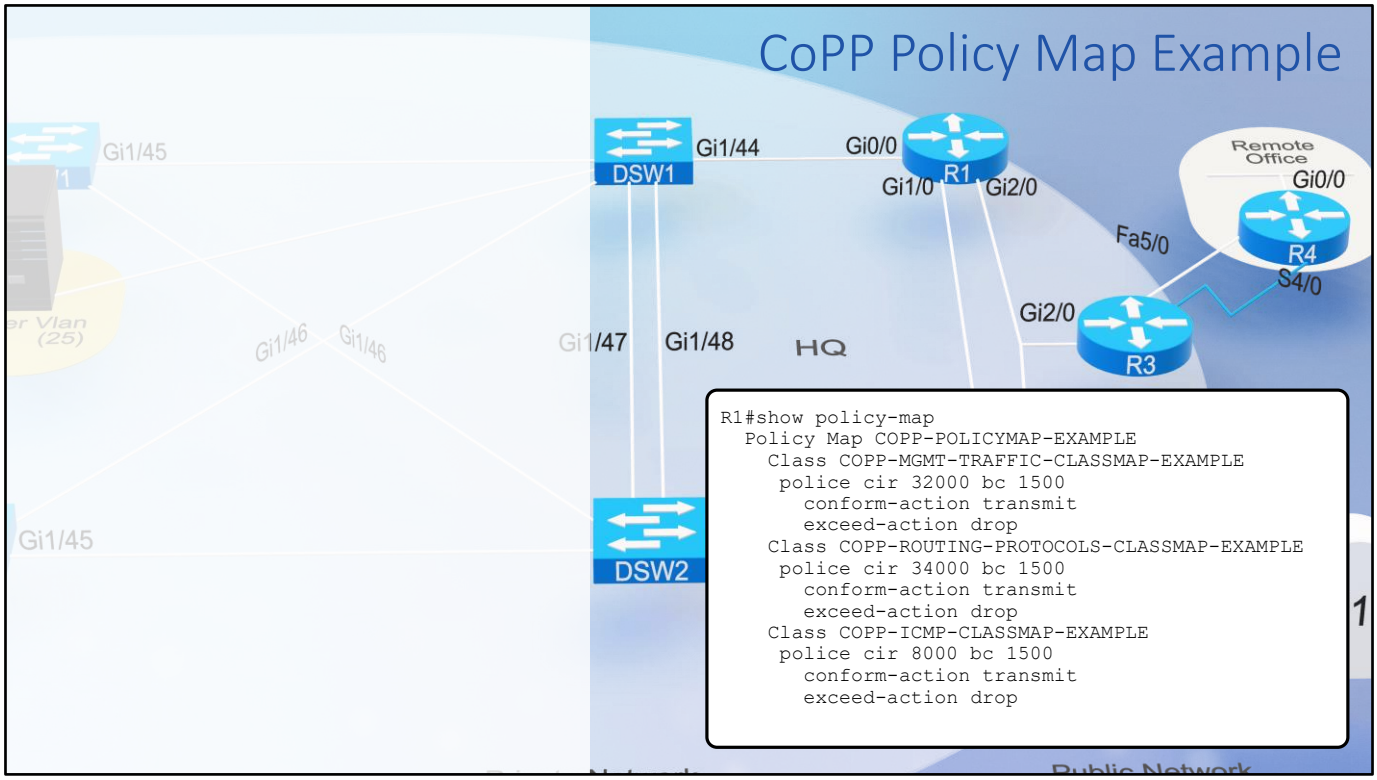
For CoPP deployments, the **police** keyword is typically used to define the traffic policy.

When more than one class of traffic is defined within a policy-map, the order of classes is important, as traffic is compared against successive classes, top-down, until a match is recorded. Once a packet has matched a class, no further comparisons are made. If no match is found after processing all classes,

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

packets automatically match the always-defined class, **class-default**. The class **class-default** is special in MQC because it is always automatically placed at the end of every policy map. Match criteria cannot be configured for **class-default** because it automatically includes an implied match for all packets. Only a traffic policy can be configured for **class-default**.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



When more than one class of traffic is defined within a policy-map, the order of classes is important, as traffic is compared against successive classes, top-down, until a match is recorded. Once a packet has matched a class, no further comparisons are made. If no match is found after processing all classes, packets automatically match the always-defined class, **class-default**. The class **class-default** is special in MQC because it is always automatically placed at the end of every policy map. Match criteria cannot be configured for **class-default** because it automatically includes an implied match for all packets. Only a traffic policy can be configured for **class-default**.

The class **class-default** is automatically placed at the end of the policy map. By the nature of CoPP matching mechanisms, certain traffic types will always end up falling into the default class. This includes traffic such as Layer 2 keepalives and non-IP traffic such as certain ISIS packets. Because these traffic types are required to maintain the network control plane,**class-default** must never be policed with both conform and exceed being set with an action of drop. It is generally considered best practice never to rate-limit the class **class-default**.

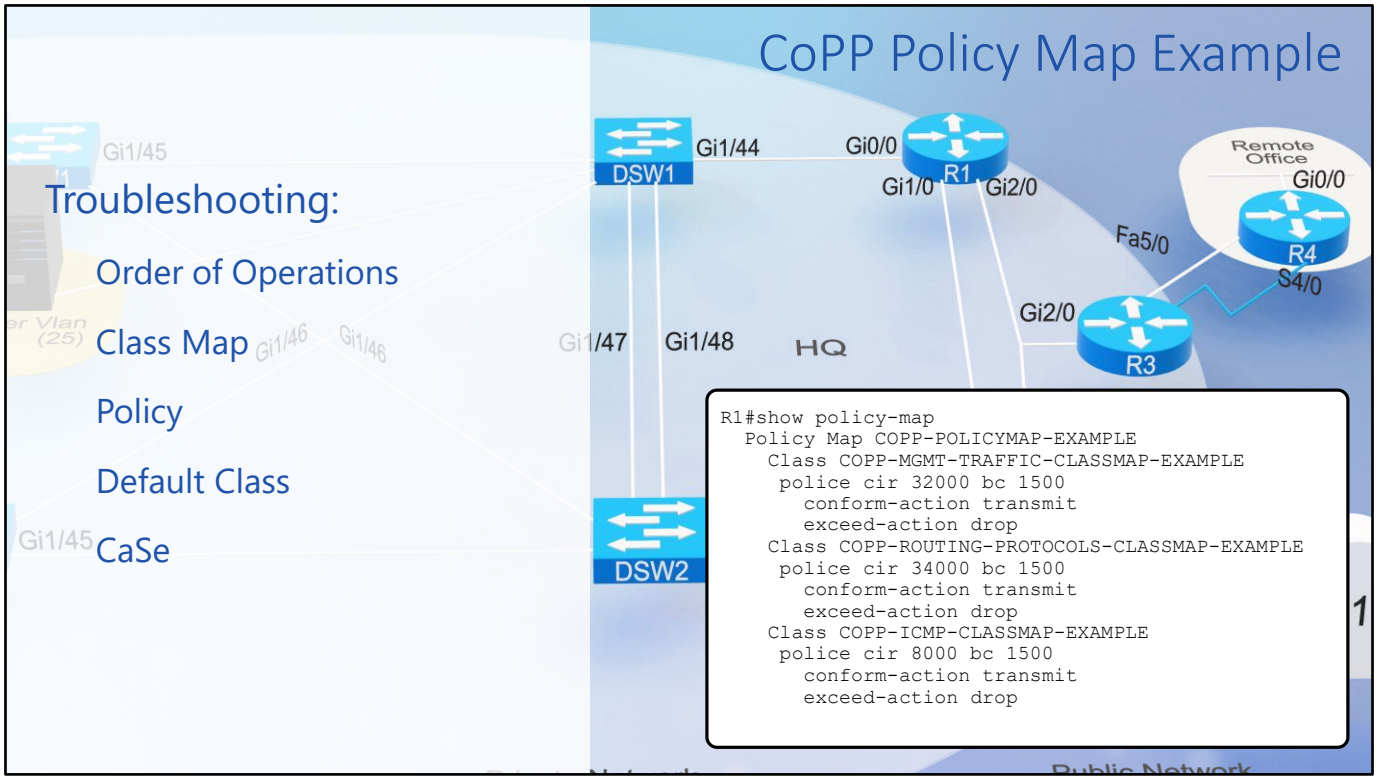
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

****

Bc is an amount of traffic that would be "confirmed" per time interval, called Tc.
Tc = Bc / CIR
Everything else would violate your policer.
So, if you say police 8000 bps with Bc = 8000 bits, it means that during single second (Tc = Bc/CIR = 1 second) you could send no more than 8000 bits of traffic.
If you say police 8000 with Bc=2000 bits, it means that during the period of 250ms (Tc = 2000/8000 = 250ms), you could send no more than 2000 bits of traffic == 8000 bps.
So, the lower Bc, the smoother policing you do (cutting spikes).

Be is an amount of traffic that would be "exceeded" per time interval (applicable for 3-colors policers).

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



■ Order of operations: Policy maps are processed from the top down. Therefore, if there is more than one class specified, the first class listed is evaluated first, then the second, then the third, and so on down the list until you reach the default class at the end. If at any point the traffic matches any of the classes from the top down, the evaluation stops (no further processing is performed), and the policy along with its actions is applied to the traffic. This is important because if you have a policy map with seven classes, and a packet ends up matching the third and fifth class listed, only the third class is matched and applied as it is the first one in the list from the top down.
Therefore, if you are expecting the fifth class in the list to be matched but you are not getting the expected results, check to see if an earlier class is being applied instead.
■ Class map: Has the correct class map been defined in the policy map? If it has, you still need to check that the class map has been constructed properly based on the class map discussion earlier in this chapter. You also need to ensure that the ACLs are being crafted correctly for the desired outcome, as discussed earlier.
■ Policy: In the policy, make sure the correct CIR (in bits per second) has been applied or the correct RATE (in packets per second) has been applied. For

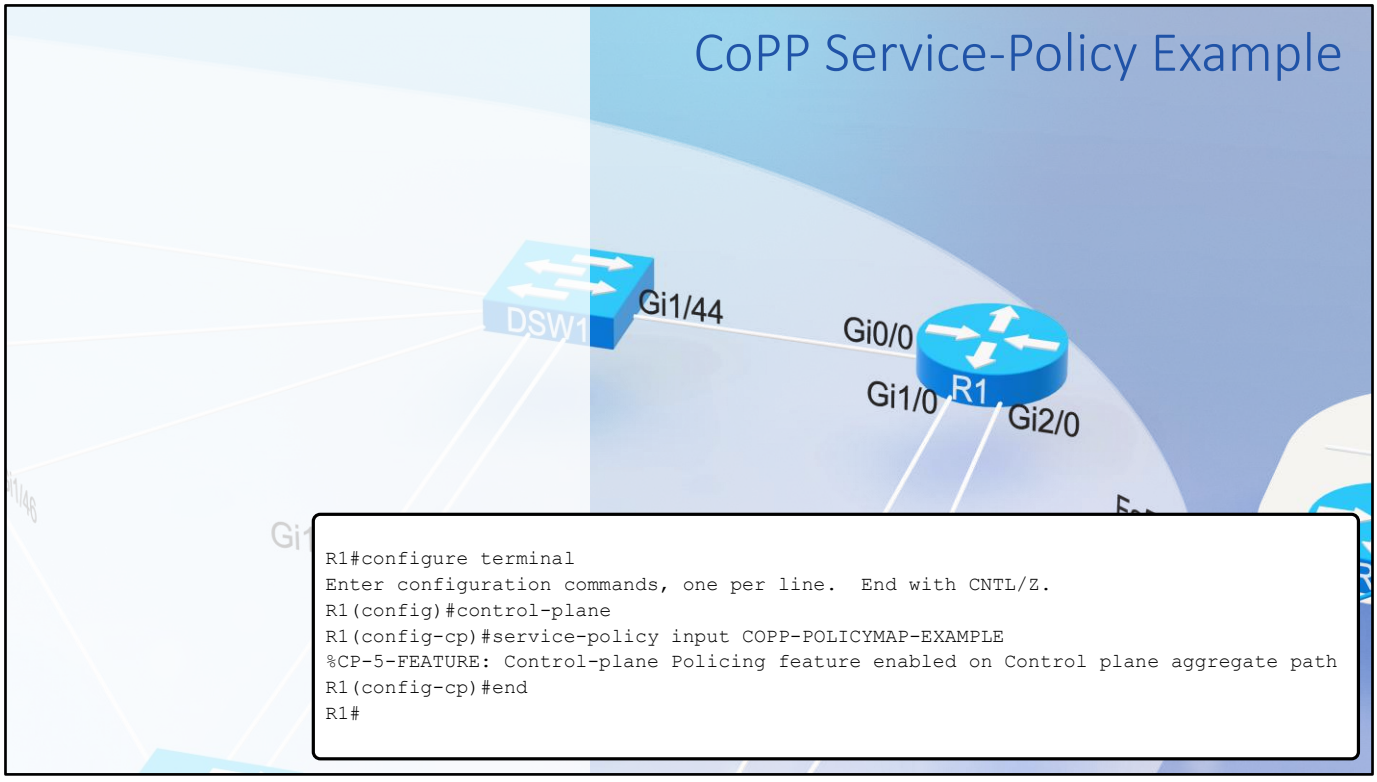
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

conform-action, you can either transmit or drop, and you need to ensure that the correct one is applied; for exceed-action, you can either transmit or drop, and you need to ensure that the correct one is applied. Note that in some versions of IOS, if your plan is to drop all the traffic that matches the class, you can replace the police command with just the keyword drop.

■ Default class: Remember that if a packet does not match any of the defined classes, it is subject to the conditions laid out in the default class. Therefore, if traffic is falling into the default class (which is likely to occur), you need to ensure that the default class is handling the traffic as intended.

■ Case: Class map names are case sensitive. When specifying the class map in the policy map, double-check to make sure the name matches exactly.

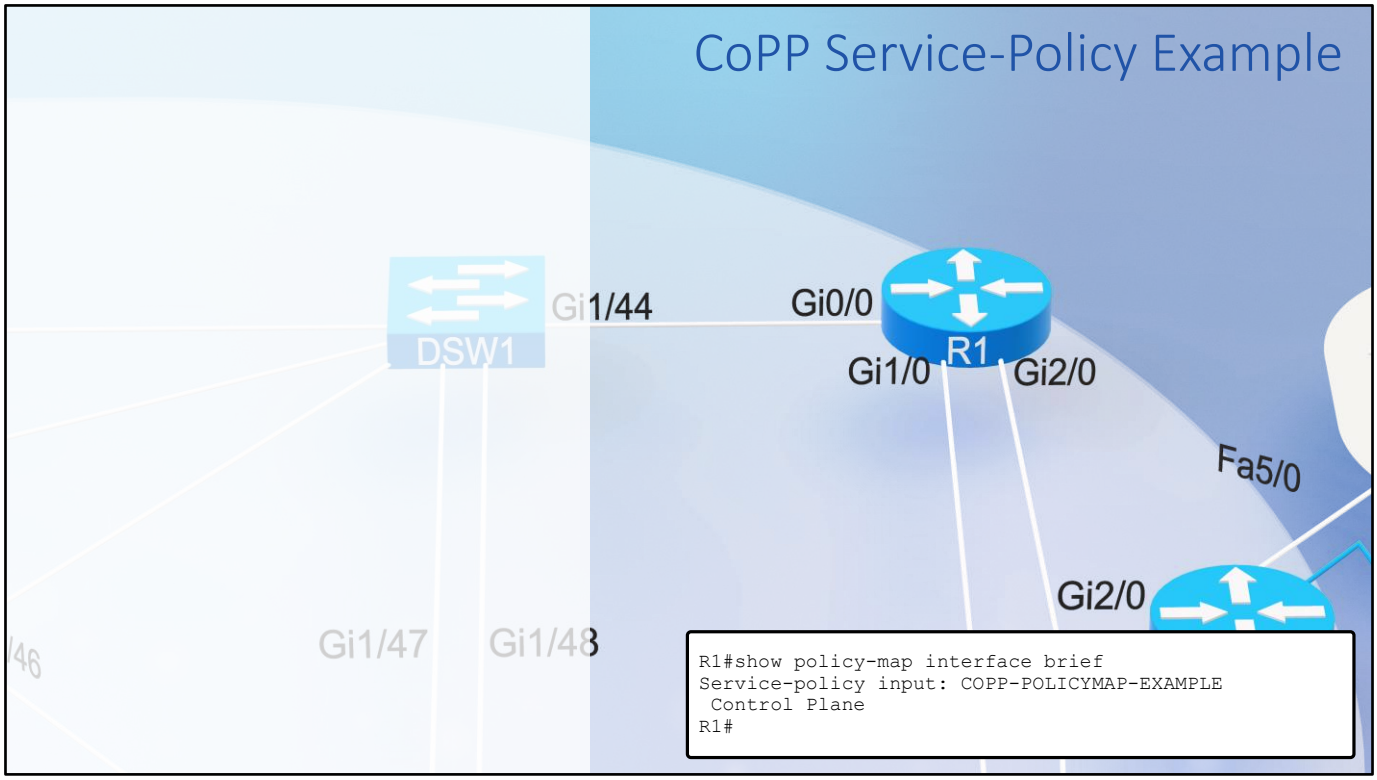
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



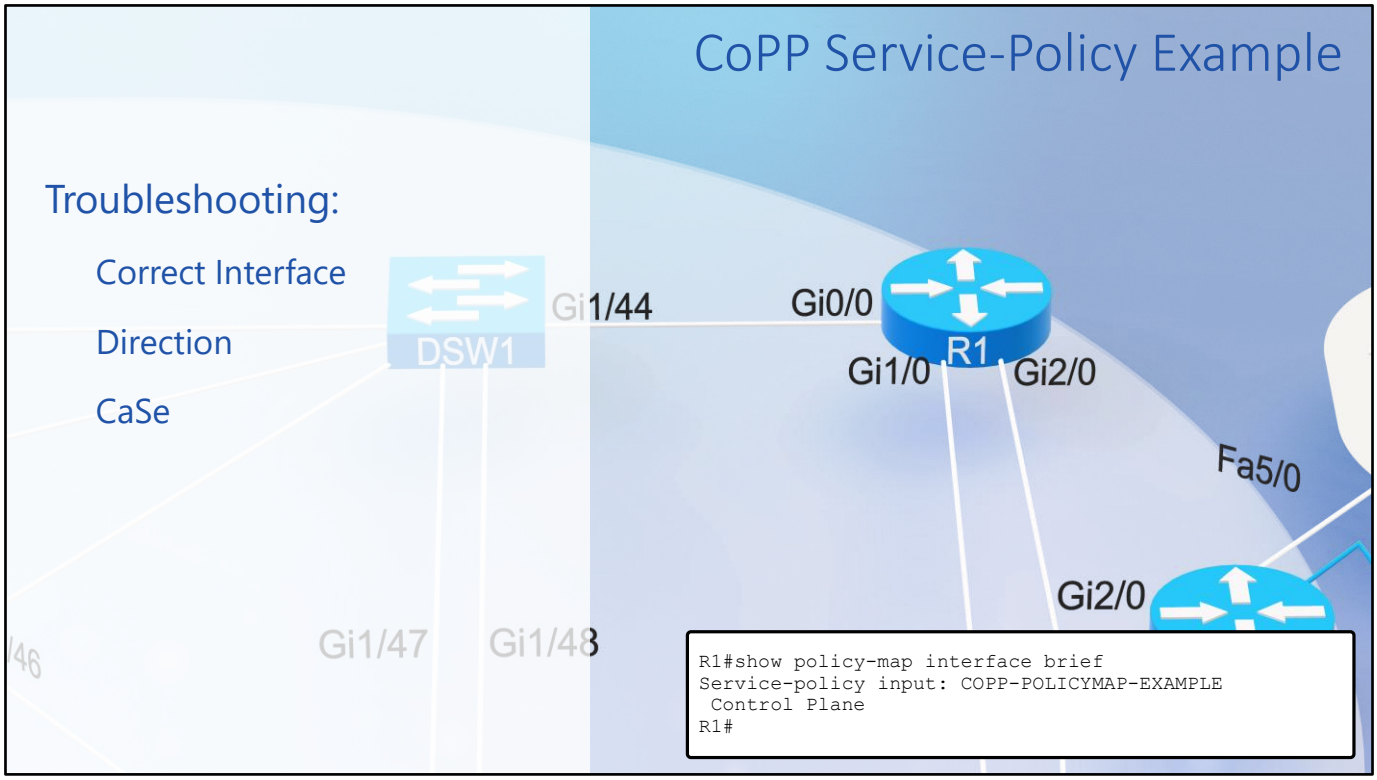
The service-policy command is used to attach the service policy, as specified with the policy-map command, to an interface. In the case of CoPP, this is the control-plane interface. Because the elements of the service policy can be applied to packets entering, or in some versions of CoPP, leaving the interface, users are required to specify whether the service policy characteristics should be applied to incoming or outgoing packets.

This is known as a “virtual aggregate CPU bound queue” or the “control-plane interface”

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



■ The correct interface: There is only one interface to which you can apply CoPP, the control plane interface, so this one is easy to troubleshoot: It is either applied or not applied. You can verify this with the show policy-map control-plane [input | output] command, as shown in Example 22-10.
■ Direction: CoPP can be applied to packets entering or leaving the control plane interface. Therefore, the correct direction needs to be specified. For incoming packets, you specify input, and for outgoing packets you specify output. Direction can be verified with the output of show policy-map control-plane as well. Note that not all versions support output CoPP, and for the ones that do, you need to ensure that the correct traffic is being classified in the ACLs and the class maps. For example, when it comes to BGP, OSPF (Open Shortest Path First), and EIGRP, you typically use output CoPP for the replies that are being sent because of an already received packet. For ICMP, it would be error and informational reply messages. For Telnet, SSH (Secure Shell), HTTP (Hypertext Transfer Protocol), or SNMP (Simple Network Management Protocol), you would be dealing with replies or traps. If the ACL and class map are not configured appropriately for the replies, the desired result will not be achieved.
■ Case: Policy map names are case sensitive. When attaching a policy map to

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

the control plane interface, double-check to make sure the names match exactly

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

CoPP Verification Example

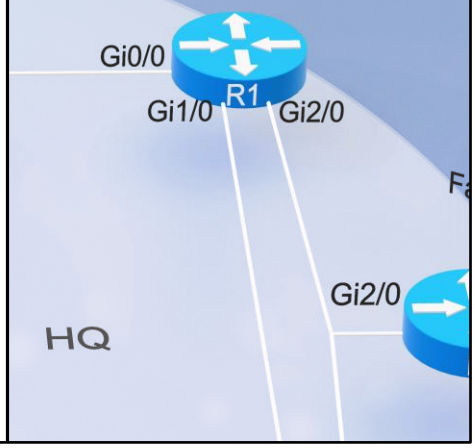
```
R1#show policy-map control-plane
 Control Plane

  Service-policy input: COPP-POLICYMAP-EXAMPLE

    Class-map: COPP-MGMT-TRAFFIC-CLASSMAP-EXAMPLE (match-all)
      120 packets, 6662 bytes
      5 minute offered rate 1000 bps, drop rate 0000 bps
      Match: access-group name COPP-MGMT-TRAFFIC-ACL-EXAMPLE
      police:
          cir 32000 bps, bc 1500 bytes
        conformed 120 packets, 6662 bytes; actions:
          transmit
        exceeded 0 packets, 0 bytes; actions:
          drop
        conformed 1000 bps, exceeded 0000 bps

    Class-map: COPP-ROUTING-PROTOCOLS-CLASSMAP-EXAMPLE (match-all)
      94 packets, 9104 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: access-group name COPP-ROUTING-PROTOCOLS-ACL-EXAMPLE
      police:
          cir 34000 bps, bc 1500 bytes
        conformed 94 packets, 9104 bytes; actions:
          transmit
        exceeded 0 packets, 0 bytes; actions:
          drop
        conformed 0000 bps, exceeded 0000 bps

    Class-map: COPP-ICMP-CLASSMAP-EXAMPLE (match-all)
      200 packets, 196412 bytes
```



GRAPHICS: Any way on click to make the white box animate so the bottom half is shown. Essentially once the animation is done the slide should look like the next one.

Notes: The show policy-map control-plane command displays the dynamic information about the actual policy applied including rate information and the number of bytes (and packets) that conformed to or exceeded the configured policies.

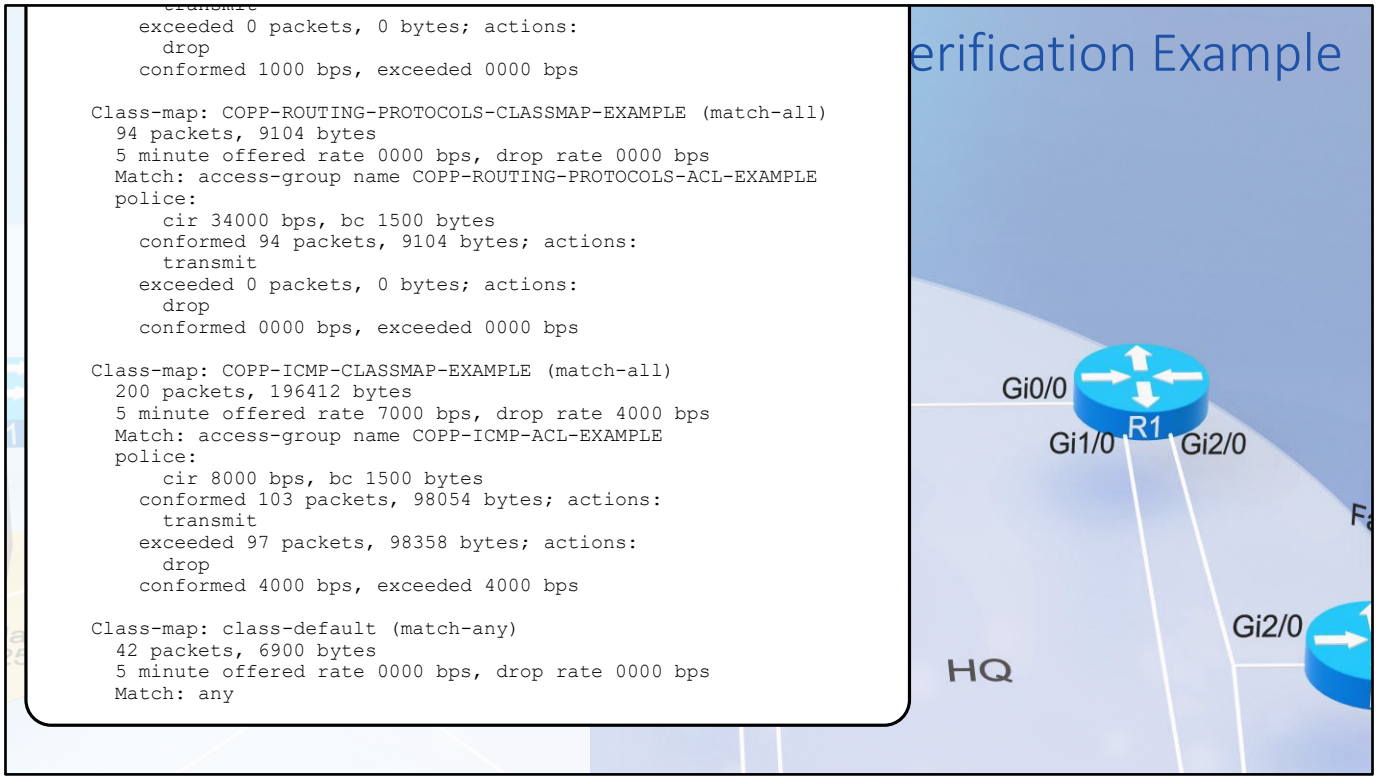
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

```
      transmit
      exceeded 0 packets, 0 bytes; actions:
        drop
      conformed 1000 bps, exceeded 0000 bps

  Class-map: COPP-ROUTING-PROTOCOLS-CLASSMAP-EXAMPLE (match-all)
    94 packets, 9104 bytes
    5 minute offered rate 0000 bps, drop rate 0000 bps
    Match: access-group name COPP-ROUTING-PROTOCOLS-ACL-EXAMPLE
    police:
        cir 34000 bps, bc 1500 bytes
      conformed 94 packets, 9104 bytes; actions:
        transmit
      exceeded 0 packets, 0 bytes; actions:
        drop
      conformed 0000 bps, exceeded 0000 bps

  Class-map: COPP-ICMP-CLASSMAP-EXAMPLE (match-all)
    200 packets, 196412 bytes
    5 minute offered rate 7000 bps, drop rate 4000 bps
    Match: access-group name COPP-ICMP-ACL-EXAMPLE
    police:
        cir 8000 bps, bc 1500 bytes
      conformed 103 packets, 98054 bytes; actions:
        transmit
      exceeded 97 packets, 98358 bytes; actions:
        drop
      conformed 4000 bps, exceeded 4000 bps

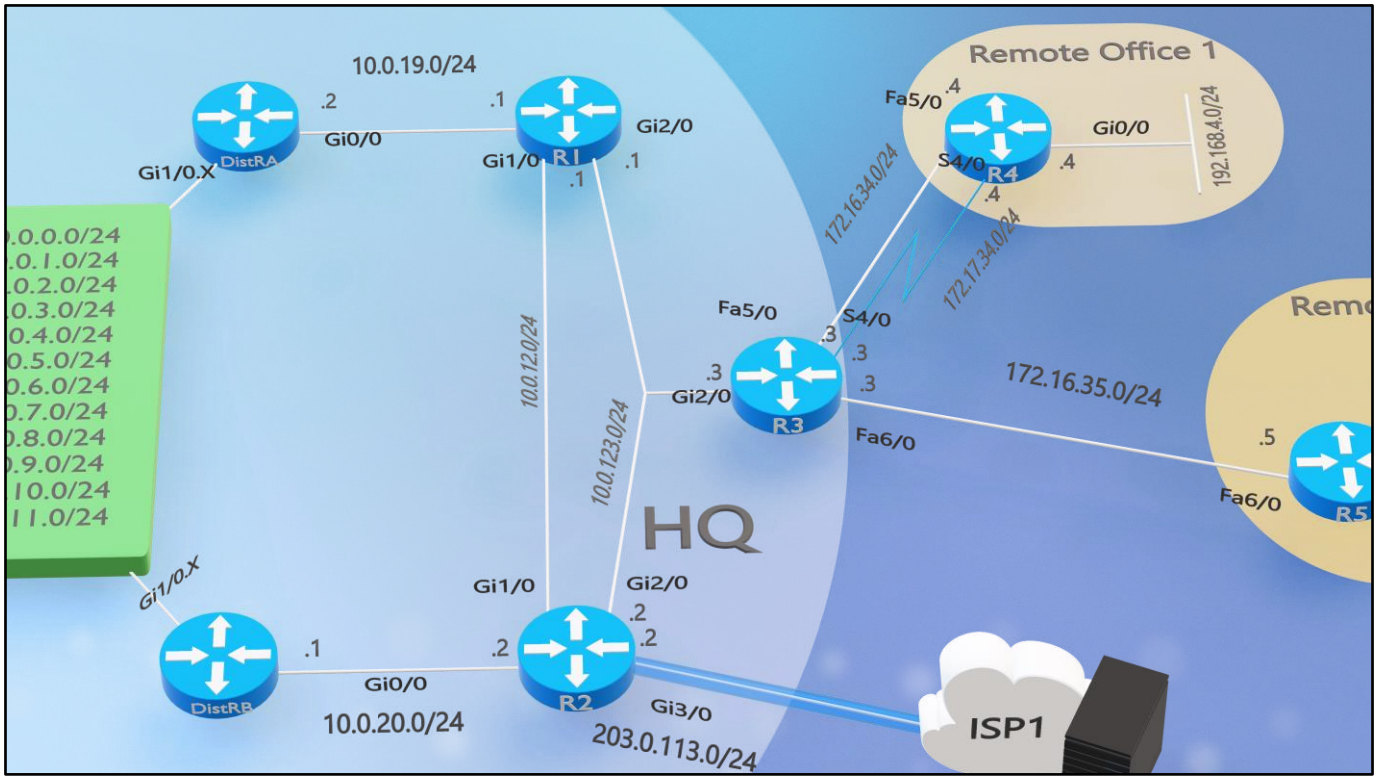
  Class-map: class-default (match-any)
    42 packets, 6900 bytes
    5 minute offered rate 0000 bps, drop rate 0000 bps
    Match: any
```



GRAPHICS: Any way on click to make the white box animate so the bottom half is shown. Essentially once the animation is done the slide should look like the next one.

Notes: The show policy-map control-plane command displays the dynamic information about the actual policy applied including rate information and the number of bytes (and packets) that conformed to or exceeded the configured policies.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

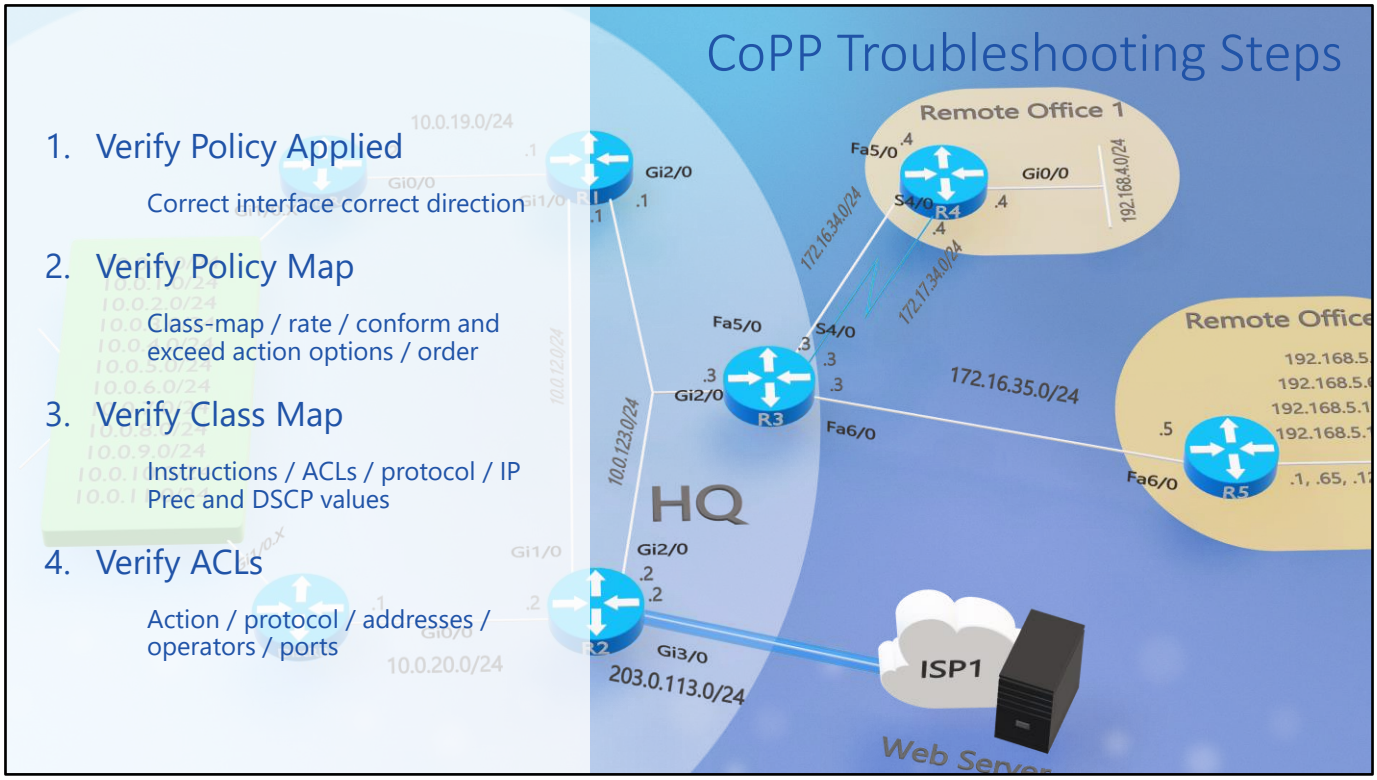


Do a demo of using COPP for dropping (filtering packets headed to the Control Plane) instead of rate limiting. This would be similar to having an ACL on an interface that drops unwanted packets ingress.

A simple example between R1 and R2.
access-list 100 permit eigrp host 10.0.12.2 host 224.0.0.10
class-map match-all CM_EIGRP_DROP
 match access-group 100
policy-map PM_EIGRP_DROP
 class CM_EIGRP_DROP
  drop
Control-plane
 service-policy input PM_EIGRP_DROP

Show policy-map control-plane

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Step 1. Verify that the service policy is applied and in the correct direction by using the show policy-map control-plane command. If it is not, fix the issue. If it is, move on to step 2.

Step 2. Verify that the policy map is configured correctly with either the show policymap control-plane command or the show policy-map command. Check that the correct class-map, rate/cir, conform-action, and exceed-action options have been applied. Also ensure that the classes are defined in the correct order, based on top-down processing. If not, fix the issues. If everything is correct, move on to step 3.

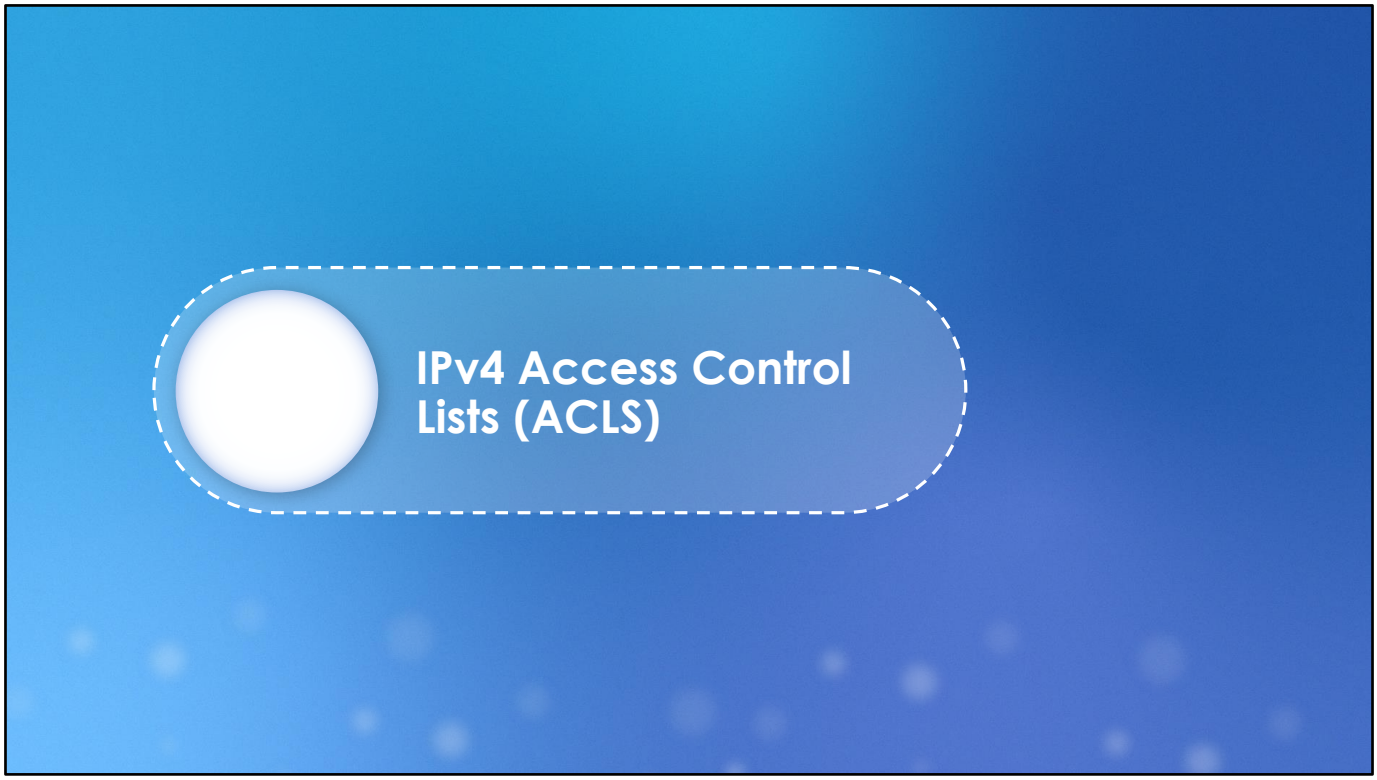
Step 3. Verify that the class map is configured correctly by using the show c lass-map command. Verify that the correct instructions (match-any, match-all) are applied, along with the correct ACL, protocol, IP precedence, or IP DSCP v alues. If not, fix the issues. If everything is correct, move on to step 4.

Step 4. Verify that the ACLs have been configured correctly for the types of t raffic you want to match by using the show access-list command. This requires you to verify the action (permit, deny), protocol, addresses, operators, port n umbers, and anything else you can use to identify interesting traffic. If you find any issues, fix them.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

At this point, everything should be working as intended. If not, go back and verify e verything again because you missed something.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Title slide

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Access Control List

ACL

An ACL provides traffic identification

When traffic is identified, a variety of actions can be applied based on purpose:

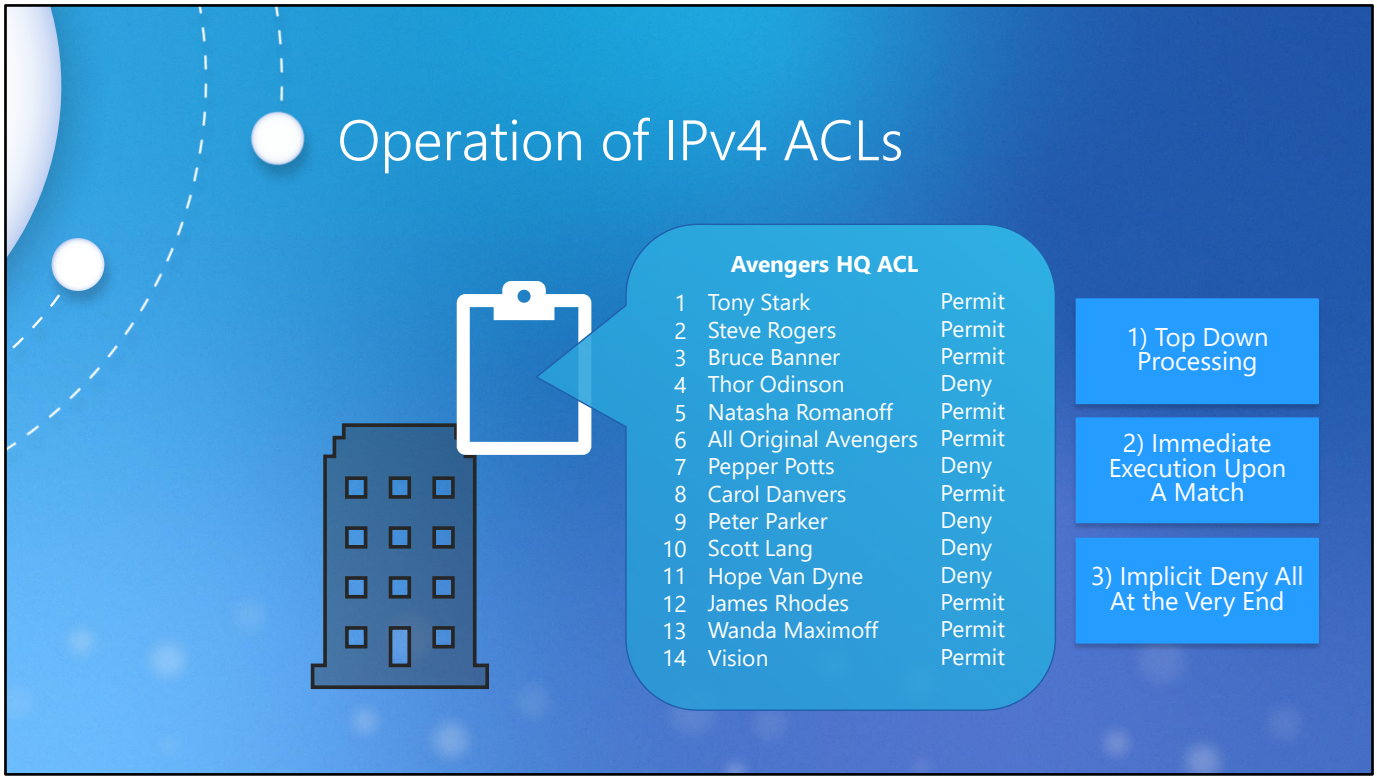
- Permit, Deny, Change traffic direction, and more
  - NAT, Traffic Filter, QoS, PBR, Route Filter, etc…

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Access Control List

ACL
An ACL is made of Access Control Entries (ACEs)
ACEs can be permit and deny statements
Access Lists can be used on routers and switches

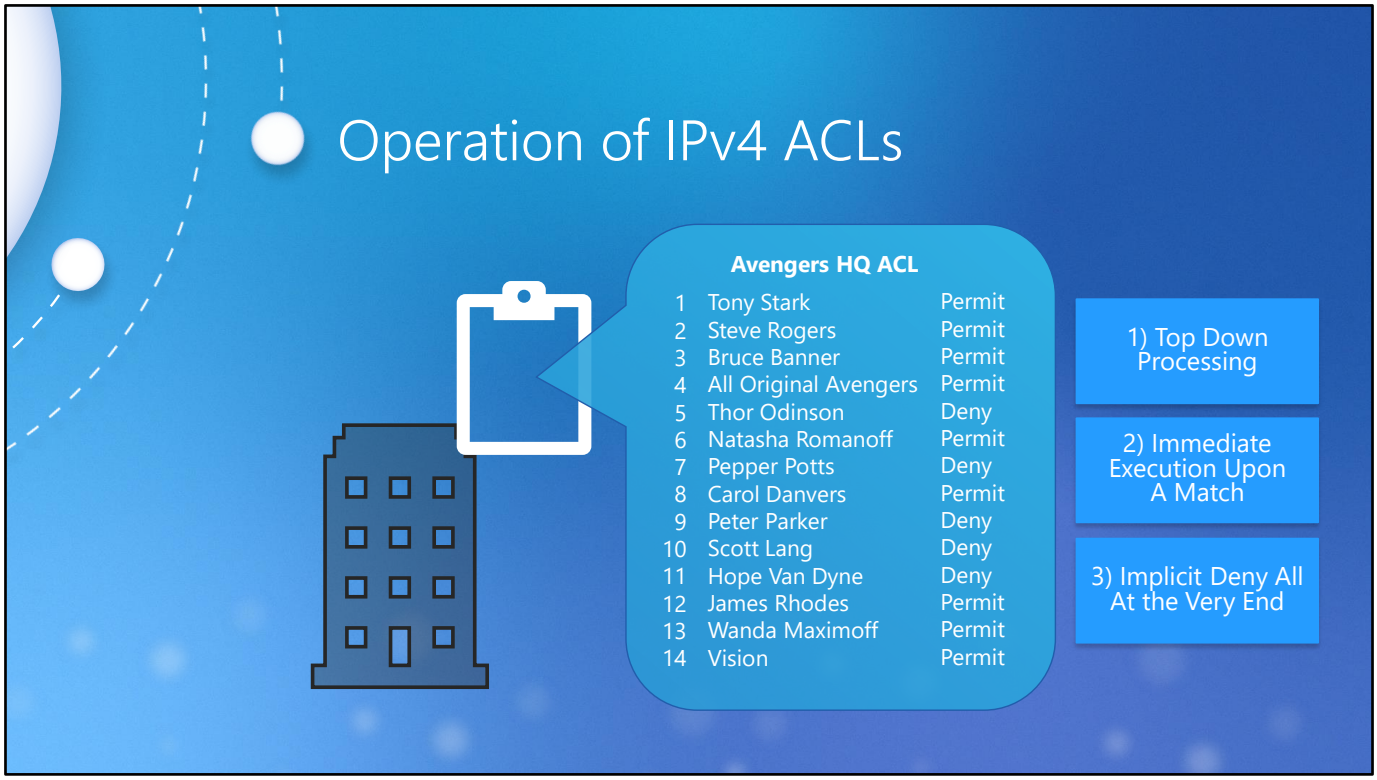
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



All Original = Steve, Tony, Bruce, Thor, Natasha, Clint Barton

If THOR shows up at the door and knocks…. What happens????

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

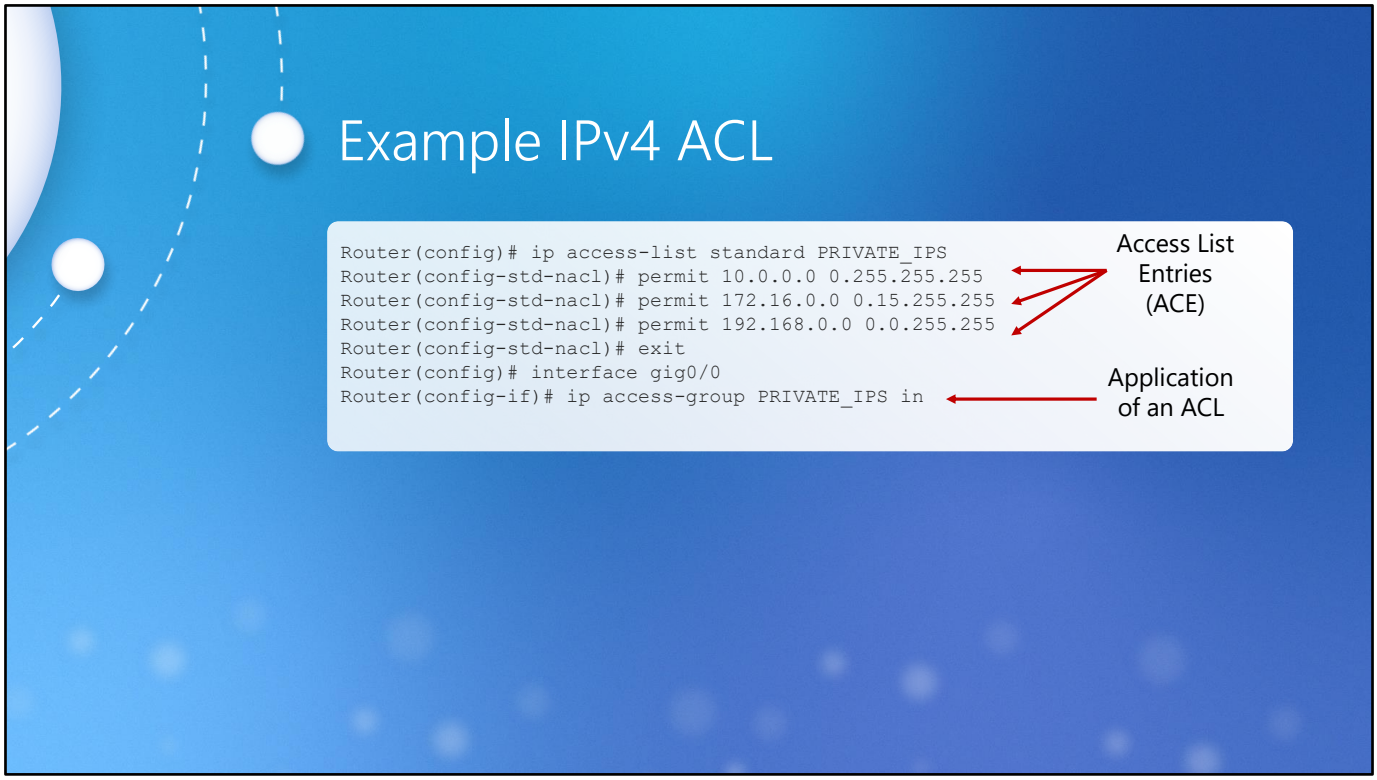


All Original = Steve, Tony, Bruce, Thor, Natasha, Clint Barton

If THOR shows up at the door and knocks…. What happens????

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Example IPv4 ACL



Application varies.

Apply to interface to control traffic in and out of interface

Identify interesting traffic for QoS

Identify traffic for Policy Based Routing

Identify packets that need to be Network Address Translated.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Operation of IPv4 ACLs

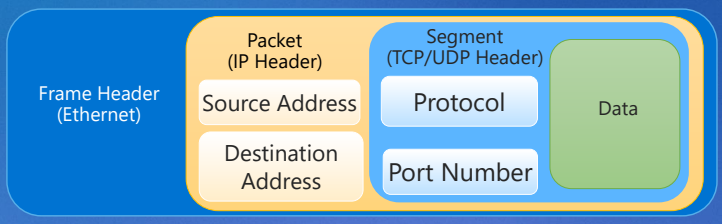


©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

IPv4 ACL Types

Standard ACL

Only filters based on source IP address of packet



Extended ACL

Can filter based on source and destination IP address
Can filter based on different types of Layer 4 Protocols
Can filter based on different port numbers

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

IPv4 ACL Types

There are two ways to ID your ACLs		
ID	**IPv4 ACL Type**	**Number Range or Identifier**
Number	Standard	1-99, 1300-1999
Number	Extended	100-199, 2000-2699
Name	Standard	*Name*
Name	Extended	*Name*

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

IPv4 Numbered Standard ACLs

To configure a Numbered ACL, you will use “access-list”

```
Router(config)#access-list 5 permit 10.1.1.0 0.0.0.255
```

*If no mask specified, default is 0.0.0.0 (Standard ACLs only)

```
Router#show access-lists
Standard IP access list 5
     10 permit 10.1.1.0, wildcard bits 0.0.0.255
```

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

IPv4 Named Standard ACLs

To configure Named Standard ACLs, you must use “ip access-list”

```
Router(config)#ip access-list standard TEST
Router(config-std-nacl)#permit 10.1.1.1
Router(config-std-nacl)#permit 10.2.0.0 0.0.255.255
```

```
Router #show access-lists
Standard IP access list TEST
    10 permit 10.1.1.1
    20 permit 10.2.0.0, wildcard bits 0.0.255.255
```

*Numbers can be used as name, may be just me but could be a good thing to bring up-Russ

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



A critical part of the ACL is the wildcard mask…. This is true for both standard and extended.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

What binary bits mean in a wildcard mask:

A 0 bit means **match**

"I care about this bit", "use this bit", "preserve this bit", "carry this bit down"

A 1 bit means **ignore**

"I DON'T care about this bit", "DON'T use this bit", "DON'T preserve this bit", "DON'T carry this bit down"

```
Router(config)#access-list 5 permit 10.1.1.0 0.0.0.255
```

00001010.00000001.00000001.00000000 – IP address in binary

00000000.00000000.00000000.11111111 – Wildcard Mask in Binary

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

What binary bits mean in a wildcard mask:

A 0 bit means **match**

"I care about this bit", "use this bit", "preserve this bit", "carry this bit down"

A 1 bit means **ignore**

"I DON'T care about this bit", "DON'T use this bit", "DON'T preserve this bit", "DON'T carry this bit down"

```
Router(config)#access-list 5 permit 10.1.1.0 0.0.0.255
```

00001010.00000001.00000001.00000000 – IP address in binary

00000000.00000000.00000000.11111111 – Wildcard Mask in Binary

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

What binary bits mean in a wildcard mask:

A 0 bit means **match**

"I care about this bit", "use this bit", "preserve this bit", "carry this bit down"

A 1 bit means **ignore**

"I DON'T care about this bit", "DON'T use this bit", "DON'T preserve this bit", "DON'T carry this bit down"

```
Router(config)#access-list 5 permit 10.1.1.0 0.0.0.255
```

00001010.00000001.00000001.00000000 – IP address in binary

00000000.00000000.00000000.11111111 – Wildcard Mask in Binary

00001010.00000001.00000001.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

What binary bits mean in a wildcard mask:

A 0 bit means **match**

"I care about this bit", "use this bit", "preserve this bit", "carry this bit down"

A 1 bit means **ignore**

"I DON'T care about this bit", "DON'T use this bit", "DON'T preserve this bit", "DON'T carry this bit down"

```
Router(config)#access-list 5 permit 10.1.1.0 0.0.0.255
```

00001010.00000001.00000001.00000000 – IP address in binary

00000000.00000000.00000000.11111111 – Wildcard Mask in Binary

00001010.00000001.00000001.XXXXXXXX – X = 0 or 1 since we "do not care"

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

What binary bits mean in a wildcard mask:

A 0 bit means **match**

"I care about this bit", "use this bit", "preserve this bit", "carry this bit down"

A 1 bit means **ignore**

"I DON'T care about this bit", "DON'T use this bit", "DON'T preserve this bit", "DON'T carry this bit down"

```
Router(config)#access-list 5 permit 10.1.1.0 0.0.0.255
```

00001010.00000001.00000001.00000000 – IP address in binary

00000000.00000000.00000000.11111111 – Wildcard Mask in Binary

00001010.00000001.00000001.XXXXXXXX – X = 0 or 1 since we "do not care"

10. 1. 1. 0 – If X's are all 0's

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

What binary bits mean in a wildcard mask:

A 0 bit means **match**

"I care about this bit", "use this bit", "preserve this bit", "carry this bit down"

A 1 bit means **ignore**

"I DON'T care about this bit", "DON'T use this bit", "DON'T preserve this bit", "DON'T carry this bit down"

```
Router(config)#access-list 5 permit 10.1.1.0 0.0.0.255
```

00001010.00000001.00000001.00000000 – IP address in binary

00000000.00000000.00000000.11111111 – Wildcard Mask in Binary

00001010.00000001.00000001.XXXXXXXX – X = 0 or 1 since we "do not care"

10. 1. 1. 0 – If X's are all 0's

10. 1. 1. 255 – If X's are all 1's

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

What binary bits mean in a wildcard mask:

A 0 bit means **match**

"I care about this bit", "use this bit", "preserve this bit", "carry this bit down"

A 1 bit means **ignore**

"I DON'T care about this bit", "DON'T use this bit", "DON'T preserve this bit", "DON'T carry this bit down"

```
Router(config)#access-list 5 permit 10.1.1.0 0.0.0.255
```

00001010.00000001.00000001.00000000 – IP address in binary

00000000.00000000.00000000.11111111 – Wildcard Mask in Binary

00001010.00000001.00000001.XXXXXXXX – X = 0 or 1 since we "do not care"

Range
- 10. 1. 1. 0 – If X's are all 0's
- 10. 1. 1. 255 – If X's are all 1's

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

What binary bits mean in a wildcard mask:

A 0 bit means **match**

"I care about this bit", "use this bit", "preserve this bit", "carry this bit down"

A 1 bit means **ignore**

"I DON'T care about this bit", "DON'T use this bit", "DON'T preserve this bit", "DON'T carry this bit down"

```
Router(config)#access-list 5 permit 10.1.1.0 0.0.0.15
```

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

What binary bits mean in a wildcard mask:

A 0 bit means **match**

"I care about this bit", "use this bit", "preserve this bit", "carry this bit down"

A 1 bit means **ignore**

"I DON'T care about this bit", "DON'T use this bit", "DON'T preserve this bit", "DON'T carry this bit down"

```
Router(config)#access-list 5 permit 10.1.1.0 0.0.0.15
```

00001010.00000001.00000001.00000000 – IP address in binary

00000000.00000000.00000000.00001111 – Wildcard Mask in Binary

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

What binary bits mean in a wildcard mask:

A 0 bit means **match**

"I care about this bit", "use this bit", "preserve this bit", "carry this bit down"

A 1 bit means **ignore**

"I DON'T care about this bit", "DON'T use this bit", "DON'T preserve this bit", "DON'T carry this bit down"

```
Router(config)#access-list 5 permit 10.1.1.0 0.0.0.15
```

00001010.00000001.00000001.00000000 – IP address in binary

00000000.00000000.00000000.00001111 – Wildcard Mask in Binary

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

What binary bits mean in a wildcard mask:

A 0 bit means **match**

"I care about this bit", "use this bit", "preserve this bit", "carry this bit down"

A 1 bit means **ignore**

"I DON'T care about this bit", "DON'T use this bit", "DON'T preserve this bit", "DON'T carry this bit down"

```
Router(config)#access-list 5 permit 10.1.1.0 0.0.0.15
```

00001010.00000001.00000001.00000000 – IP address in binary

00000000.00000000.00000000.00001111 – Wildcard Mask in Binary

00001010.00000001.00000001.0000

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

What binary bits mean in a wildcard mask:

A 0 bit means **match**

"I care about this bit", "use this bit", "preserve this bit", "carry this bit down"

A 1 bit means **ignore**

"I DON'T care about this bit", "DON'T use this bit", "DON'T preserve this bit", "DON'T carry this bit down"

```
Router(config)#access-list 5 permit 10.1.1.0 0.0.0.15
```

00001010.00000001.00000001.00000000 – IP address in binary

00000000.00000000.00000000.00001111 – Wildcard Mask in Binary

00001010.00000001.00000001.0000XXXX – X = 0 or 1 since we "do not care"

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

What binary bits mean in a wildcard mask:

A 0 bit means **match**

"I care about this bit", "use this bit", "preserve this bit", "carry this bit down"

A 1 bit means **ignore**

"I DON'T care about this bit", "DON'T use this bit", "DON'T preserve this bit", "DON'T carry this bit down"

```
Router(config)#access-list 5 permit 10.1.1.0 0.0.0.15
```

00001010.00000001.00000001.00000000 – IP address in binary

00000000.00000000.00000000.00001111 – Wildcard Mask in Binary

00001010.00000001.00000001.0000XXXX – X = 0 or 1 since we "do not care"

10. 1. 1. 0 – If X's are all 0's

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

What binary bits mean in a wildcard mask:

A 0 bit means **match**

"I care about this bit", "use this bit", "preserve this bit", "carry this bit down"

A 1 bit means **ignore**

"I DON'T care about this bit", "DON'T use this bit", "DON'T preserve this bit", "DON'T carry this bit down"

```
Router(config)#access-list 5 permit 10.1.1.0 0.0.0.15
```

00001010.00000001.00000001.00000000 – IP address in binary

00000000.00000000.00000000.00001111 – Wildcard Mask in Binary

00001010.00000001.00000001.0000XXXX – X = 0 or 1 since we "do not care"

10. 1. 1. 0 – If X's are all 0's

10. 1. 1. 15 – If X's are all 1's

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

What binary bits mean in a wildcard mask:

A 0 bit means **match**

"I care about this bit", "use this bit", "preserve this bit", "carry this bit down"

A 1 bit means **ignore**

"I DON'T care about this bit", "DON'T use this bit", "DON'T preserve this bit", "DON'T carry this bit down"

```
Router(config)#access-list 5 permit 10.1.1.0 0.0.0.15
```

00001010.00000001.00000001.00000000 – IP address in binary

00000000.00000000.00000000.00001111 – Wildcard Mask in Binary

00001010.00000001.00000001.0000XXXX – X = 0 or 1 since we "do not care"

Range
- 10. 1. 1. 0 – If X's are all 0's
- 10. 1. 1. 15 – If X's are all 1's

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

What binary bits mean in a wildcard mask:

A 0 bit means **match**

"I care about this bit", "use this bit", "preserve this bit", "carry this bit down"

A 1 bit means **ignore**

"I DON'T care about this bit", "DON'T use this bit", "DON'T preserve this bit", "DON'T carry this bit down"

```
Router(config)#access-list 5 permit 10.1.1.64 0.0.0.15
```

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

What binary bits mean in a wildcard mask:

A 0 bit means **match**

"I care about this bit", "use this bit", "preserve this bit", "carry this bit down"

A 1 bit means **ignore**

"I DON'T care about this bit", "DON'T use this bit", "DON'T preserve this bit", "DON'T carry this bit down"

```
Router(config)#access-list 5 permit 10.1.1.64 0.0.0.15
```

00001010.00000001.00000001.01000000 – IP address in binary

00000000.00000000.00000000.00001111 – Wildcard Mask in Binary

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

What binary bits mean in a wildcard mask:

A 0 bit means **match**

"I care about this bit", "use this bit", "preserve this bit", "carry this bit down"

A 1 bit means **ignore**

"I DON'T care about this bit", "DON'T use this bit", "DON'T preserve this bit", "DON'T carry this bit down"

```
Router(config)#access-list 5 permit 10.1.1.64 0.0.0.15
```

00001010.00000001.00000001.01000000 – IP address in binary

00000000.00000000.00000000.00001111 – Wildcard Mask in Binary

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

What binary bits mean in a wildcard mask:

A 0 bit means **match**

"I care about this bit", "use this bit", "preserve this bit", "carry this bit down"

A 1 bit means **ignore**

"I DON'T care about this bit", "DON'T use this bit", "DON'T preserve this bit", "DON'T carry this bit down"

```
Router(config)#access-list 5 permit 10.1.1.64 0.0.0.15
```

00001010.00000001.00000001.01000000 – IP address in binary

00000000.00000000.00000000.00001111 – Wildcard Mask in Binary

00001010.00000001.00000001.0100

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

What binary bits mean in a wildcard mask:

A 0 bit means **match**

"I care about this bit", "use this bit", "preserve this bit", "carry this bit down"

A 1 bit means **ignore**

"I DON'T care about this bit", "DON'T use this bit", "DON'T preserve this bit", "DON'T carry this bit down"

```
Router(config)#access-list 5 permit 10.1.1.64 0.0.0.15
```

00001010.00000001.00000001.01000000 – IP address in binary

00000000.00000000.00000000.00001111 – Wildcard Mask in Binary

00001010.00000001.00000001.0100XXXX – X = 0 or 1 since we "do not care"

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

What binary bits mean in a wildcard mask:

A 0 bit means **match**

"I care about this bit", "use this bit", "preserve this bit", "carry this bit down"

A 1 bit means **ignore**

"I DON'T care about this bit", "DON'T use this bit", "DON'T preserve this bit", "DON'T carry this bit down"

```
Router(config)#access-list 5 permit 10.1.1.64 0.0.0.15
```

00001010.00000001.00000001.01000000 – IP address in binary

00000000.00000000.00000000.00001111 – Wildcard Mask in Binary

00001010.00000001.00000001.0100XXXX – X = 0 or 1 since we "do not care"

10. 1. 1. 64 – If X's are all 0's

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

What binary bits mean in a wildcard mask:

A 0 bit means **match**

"I care about this bit", "use this bit", "preserve this bit", "carry this bit down"

A 1 bit means **ignore**

"I DON'T care about this bit", "DON'T use this bit", "DON'T preserve this bit", "DON'T carry this bit down"

```
Router(config)#access-list 5 permit 10.1.1.64 0.0.0.15
```

00001010.00000001.00000001.01000000 – IP address in binary

00000000.00000000.00000000.00001111 – Wildcard Mask in Binary

00001010.00000001.00000001.0100XXXX – X = 0 or 1 since we "do not care"

10. 1. 1. 64 – If X's are all 0's

10. 1. 1. 79 – If X's are all 1's

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

What binary bits mean in a wildcard mask:

A 0 bit means **match**

"I care about this bit", "use this bit", "preserve this bit", "carry this bit down"

A 1 bit means **ignore**

"I DON'T care about this bit", "DON'T use this bit", "DON'T preserve this bit", "DON'T carry this bit down"

```
Router(config)#access-list 5 permit 10.1.1.64 0.0.0.15
```

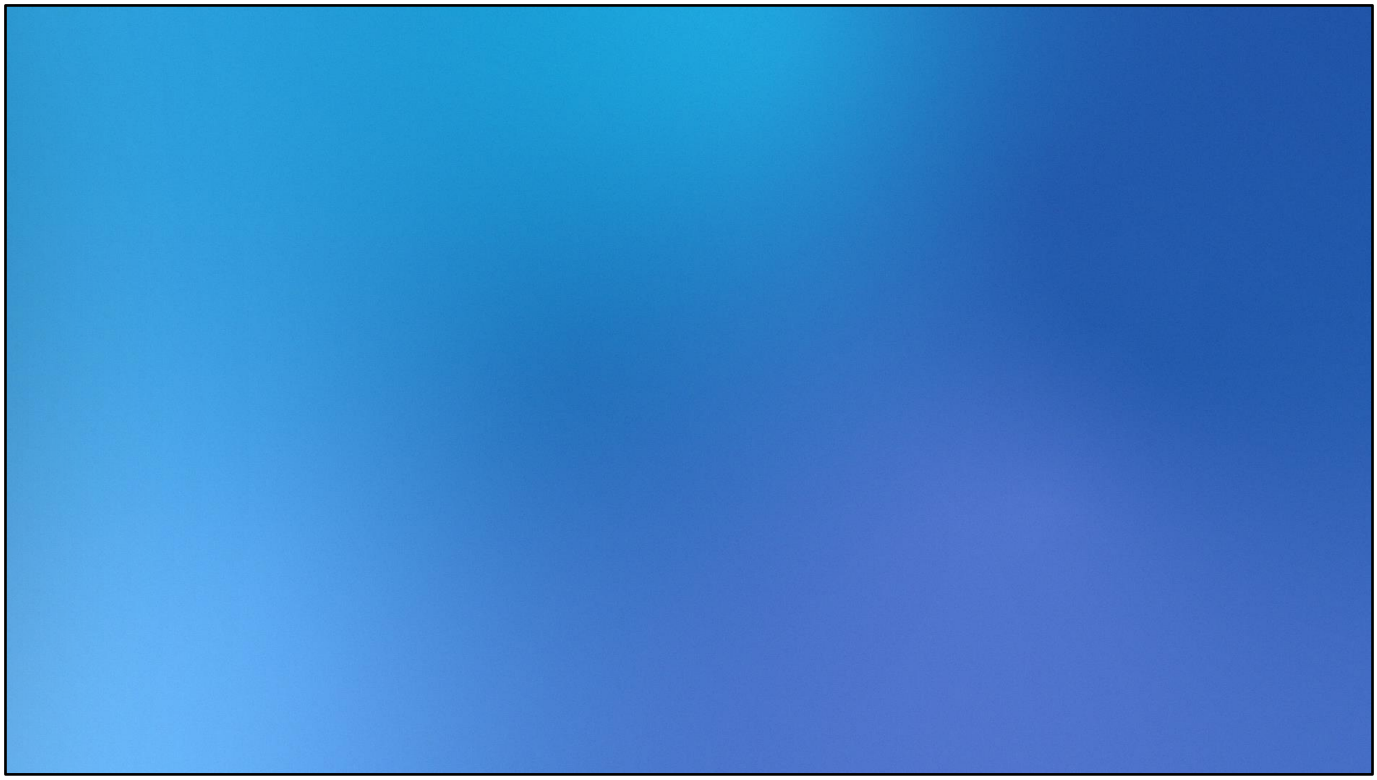
00001010.00000001.00000001.01000000 – IP address in binary

00000000.00000000.00000000.00001111 – Wildcard Mask in Binary

00001010.00000001.00000001.0100XXXX – X = 0 or 1 since we "do not care"

Range
- 10. 1. 1. 64 – If X's are all 0's
- 10. 1. 1. 79 – If X's are all 1's

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Instructor Notes:
The physical topology and the logical topology.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

Scenario:

You want an ACL that will permit all traffic for the 10.1.1.0/24 network. What address and wildcard mask combination will accomplish this for you?

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

Scenario:

You want an ACL that will permit all traffic for the 10.1.1.0/24 network. What address and wildcard mask combination will accomplish this for you?

A quick way to determine a wildcard mask is subtracting the subnet mask from 255.255.255.255

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

Scenario:

You want an ACL that will permit all traffic for the 10.1.1.0/24 network. What address and wildcard mask combination will accomplish this for you?

A quick way to determine a wildcard mask is subtracting the subnet mask from 255.255.255.255

255.255.255.255 - All 255s
- 255.255.255. 0 - Subnet mask

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

Scenario:

You want an ACL that will permit all traffic for the 10.1.1.0/24 network. What address and wildcard mask combination will accomplish this for you?

A quick way to determine a wildcard mask is subtracting the subnet mask from 255.255.255.255

255.255.255.255 - All 255s
- 255.255.255. 0 - Subnet mask
0. 0. 0.255 – Wildcard Mask

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

Scenario:

You want an ACL that will permit all traffic for the 10.1.1.0/24 network. What address and wildcard mask combination will accomplish this for you?

A quick way to determine a wildcard mask is subtracting the subnet mask from 255.255.255.255

255.255.255.255 - All 255s
- 255.255.255. 0 - Subnet mask
0. 0. 0.255 – Wildcard Mask

```
Router(config)#access-list 5 permit 10.1.1.0 0.0.0.255
```

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

Scenario:

You want an ACL that will permit all traffic for the 10.1.1.0/28 network. What address and wildcard mask combination will accomplish this for you?

A quick way to determine a wildcard mask is subtracting the subnet mask from 255.255.255.255

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

Scenario:

You want an ACL that will permit all traffic for the 10.1.1.0/28 network. What address and wildcard mask combination will accomplish this for you?

A quick way to determine a wildcard mask is subtracting the subnet mask from 255.255.255.255

255.255.255.255 - All 255s
- 255.255.255.240 - Subnet mask

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

Scenario:

You want an ACL that will permit all traffic for the 10.1.1.0/28 network. What address and wildcard mask combination will accomplish this for you?

A quick way to determine a wildcard mask is subtracting the subnet mask from 255.255.255.255

255.255.255.255 - All 255s
- 255.255.255.240 - Subnet mask
0. 0. 0. 15 – Wildcard Mask

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

Scenario:

You want an ACL that will permit all traffic for the 10.1.1.0/28 network. What address and wildcard mask combination will accomplish this for you?

A quick way to determine a wildcard mask is subtracting the subnet mask from 255.255.255.255

255.255.255.255 - All 255s
- 255.255.255.240 - Subnet mask
0. 0. 0. 15 – Wildcard Mask

```
Router(config)#access-list 5 permit 10.1.1.0 0.0.0.15
```

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

Scenario:

You want an ACL that will permit all traffic for the 10.1.1.64/28 network. What address and wildcard mask combination will accomplish this for you?

A quick way to determine a wildcard mask is subtracting the subnet mask from 255.255.255.255

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

Scenario:

You want an ACL that will permit all traffic for the 10.1.1.64/28 network. What address and wildcard mask combination will accomplish this for you?

A quick way to determine a wildcard mask is subtracting the subnet mask from 255.255.255.255

255.255.255.255 - All 255s
- 255.255.255.240 - Subnet mask

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

Scenario:

You want an ACL that will permit all traffic for the 10.1.1.64/28 network. What address and wildcard mask combination will accomplish this for you?

A quick way to determine a wildcard mask is subtracting the subnet mask from 255.255.255.255

255.255.255.255 - All 255s
- 255.255.255.240 - Subnet mask
0. 0. 0. 15 – Wildcard Mask

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

Scenario:

You want an ACL that will permit all traffic for the 10.1.1.64/28 network. What address and wildcard mask combination will accomplish this for you?

A quick way to determine a wildcard mask is subtracting the subnet mask from 255.255.255.255

255.255.255.255 - All 255s
- 255.255.255.240 - Subnet mask
0. 0. 0. 15 – Wildcard Mask

```
Router(config)#access-list 5 permit 10.1.1.64 0.0.0.15
```

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

Scenario:

You need an ACL that will permit all traffic for the 172.16.0.0/24 network to the 172.16.31.0/24 network inclusive. What address and wildcard mask combination will accomplish this for you?

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

Scenario:

You need an ACL that will permit all traffic for the 172.16.0.0/24 network to the 172.16.31.0/24 network inclusive. What address and wildcard mask combination will accomplish this for you?

First of all we could create 32 different entries using the technique we just covered.

```
Router(config)#access-list 10 permit 172.16.0.0 0.0.0.255
Router(config)#access-list 10 permit 172.16.1.0 0.0.0.255
Router(config)#access-list 10 permit 172.16.2.0 0.0.0.255
Router(config)#access-list 10 permit 172.16.3.0 0.0.0.255
……..etc…….
Router(config)#access-list 10 permit 172.16.29.0 0.0.0.255
Router(config)#access-list 10 permit 172.16.30.0 0.0.0.255
Router(config)#access-list 10 permit 172.16.31.0 0.0.0.255
```

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

Scenario:

You need an ACL that will permit all traffic for the 172.16.0.0/24 network to the 172.16.31.0/24 network inclusive. What address and wildcard mask combination will accomplish this for you?

Or we could create an ACL that groups them together.

```
Router(config)#access-list 10 permit 172.16.0.0 0.0.31.255
```

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

Scenario:

```
Router(config)#access-list 10 permit 172.16.0.0 0.0.0.255
Router(config)#access-list 10 permit 172.16.1.0 0.0.0.255
Router(config)#access-list 10 permit 172.16.2.0 0.0.0.255
Router(config)#access-list 10 permit 172.16.3.0 0.0.0.255
…….etc…….
Router(config)#access-list 10 permit 172.16.29.0 0.0.0.255
Router(config)#access-list 10 permit 172.16.30.0 0.0.0.255
Router(config)#access-list 10 permit 172.16.31.0 0.0.0.255
```

them together.

```
Router(config)#access-list 10 permit 172.16.0.0 0.0.31.255
```

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

Scenario:

You need an ACL that will permit all traffic for the 172.16.0.0/24 network to the 172.16.31.0/24 network inclusive. What address and wildcard mask combination will accomplish this for you?

Or we could create an ACL that groups them together.

172.16.0.0 - 10101100.00010000.00000000.00000000
172.16.31.0 - 10101100.00010000.00011111.00000000

Since all the addresses are consecutive in this case you only need the first and the last address as all the others are guaranteed to fall in between.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

Scenario:

You need an ACL that will permit all traffic for the 172.16.0.0/24 network to the 172.16.31.0/24 network inclusive. What address and wildcard mask combination will accomplish this for you?

Or we could create an ACL that groups them together.

172.16.0.0 - 10101100.00010000.00000000.00000000
172.16.31.0 - 10101100.00010000.00011111.00000000

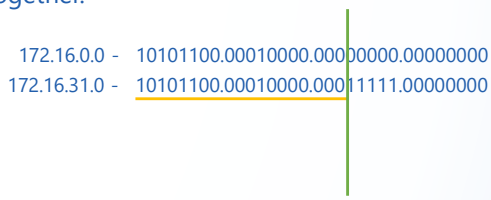
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

Scenario:

You need an ACL that will permit all traffic for the 172.16.0.0/24 network to the 172.16.31.0/24 network inclusive. What address and wildcard mask combination will accomplish this for you?

Or we could create an ACL that groups them together.



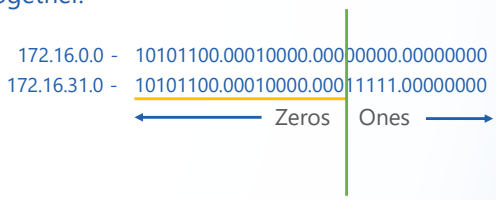
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

Scenario:

You need an ACL that will permit all traffic for the 172.16.0.0/24 network to the 172.16.31.0/24 network inclusive. What address and wildcard mask combination will accomplish this for you?

Or we could create an ACL that groups them together.



Everything underlined is a 0 and everything not underlined is a 1.

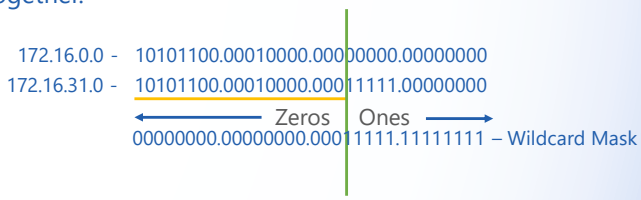
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

Scenario:

You need an ACL that will permit all traffic for the 172.16.0.0/24 network to the 172.16.31.0/24 network inclusive. What address and wildcard mask combination will accomplish this for you?

Or we could create an ACL that groups them together.



Everything underlined is a 0 and everything not underlined is a 1.

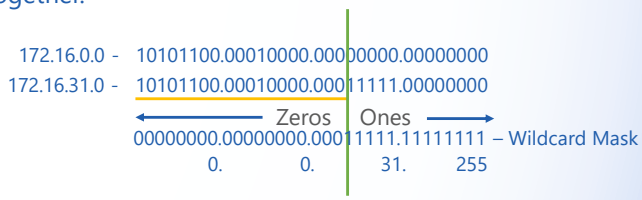
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

Scenario:

You need an ACL that will permit all traffic for the 172.16.0.0/24 network to the 172.16.31.0/24 network inclusive. What address and wildcard mask combination will accomplish this for you?

Or we could create an ACL that groups them together.



Everything underlined is a 0 and everything not underlined is a 1.

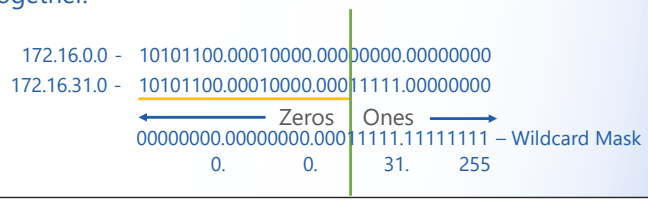
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

Scenario:

You need an ACL that will permit all traffic for the 172.16.0.0/24 network to the 172.16.31.0/24 network inclusive. What address and wildcard mask combination will accomplish this for you?

Or we could create an ACL that groups them together.




```
Router(config)#access-list 10 permit 172.16.0.0 0.0.31.255
```

Everything underlined is a 0 and everything not underlined is a 1.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

Scenario: Be Careful

You need an ACL that will permit all traffic for the 172.16.10.0/24 network to the 172.16.26.0/24 network inclusive. What address and wildcard mask combination will accomplish this for you?

This would include 172.16.0.0/24 to 172.16.31.0.24 when we only need 172.16.10.0/24 to 172.16.26.0/24. All because of powers of 2.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

Scenario: Be Careful

You need an ACL that will permit all traffic for the 172.16.10.0/24 network to the 172.16.26.0/24 network inclusive. What address and wildcard mask combination will accomplish this for you?

Or we could create an ACL that groups them together.

172.16.10.0 - 10101100.00010000.00001010.00000000
172.16.26.0 - 10101100.00010000.00011010.00000000

This would include 172.16.0.0/24 to 172.16.31.0.24 when we only need 172.16.10.0/24 to 172.16.26.0/24. All because of powers of 2.

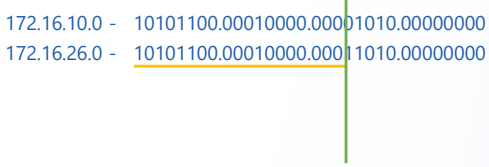
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

Scenario: Be Careful

You need an ACL that will permit all traffic for the 172.16.10.0/24 network to the 172.16.26.0/24 network inclusive. What address and wildcard mask combination will accomplish this for you?

Or we could create an ACL that groups them together.



This would include 172.16.0.0/24 to 172.16.31.0.24 when we only need 172.16.10.0/24 to 172.16.26.0/24. All because of powers of 2.

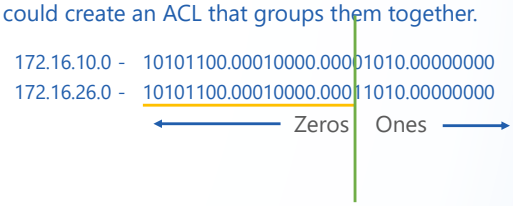
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

Scenario: Be Careful

You need an ACL that will permit all traffic for the 172.16.10.0/24 network to the 172.16.26.0/24 network inclusive. What address and wildcard mask combination will accomplish this for you?

Or we could create an ACL that groups them together.



This would include 172.16.0.0/24 to 172.16.31.0.24 when we only need 172.16.10.0/24 to 172.16.26.0/24. All because of powers of 2.

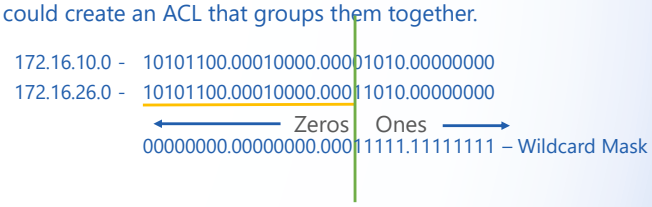
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

Scenario: Be Careful

You need an ACL that will permit all traffic for the 172.16.10.0/24 network to the 172.16.26.0/24 network inclusive. What address and wildcard mask combination will accomplish this for you?

Or we could create an ACL that groups them together.



This would include 172.16.0.0/24 to 172.16.31.0.24 when we only need 172.16.10.0/24 to 172.16.26.0/24. All because of powers of 2.

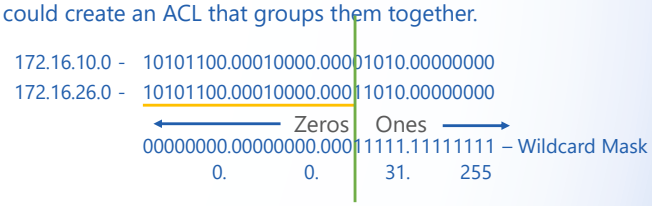
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

Scenario: Be Careful

You need an ACL that will permit all traffic for the 172.16.10.0/24 network to the 172.16.26.0/24 network inclusive. What address and wildcard mask combination will accomplish this for you?

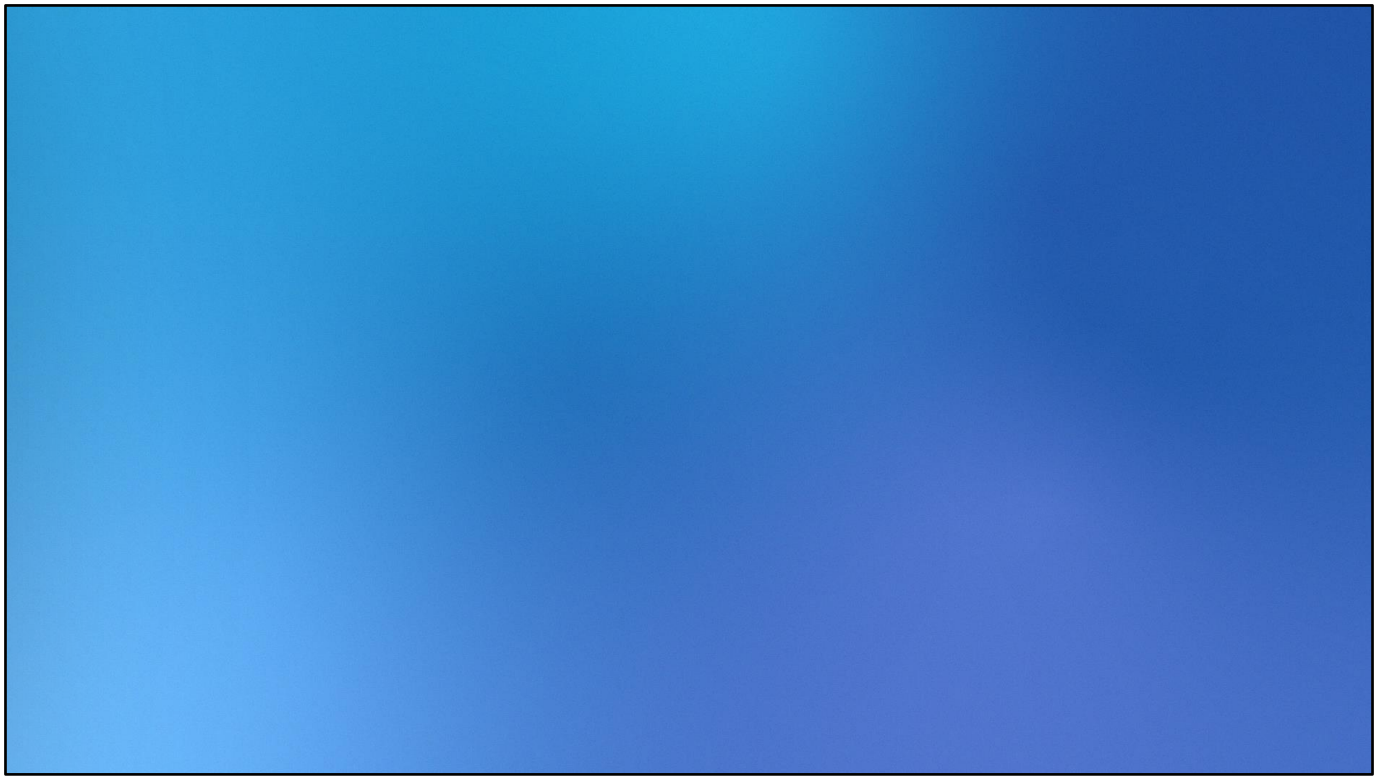
Or we could create an ACL that groups them together.




```
Router(config)#access-list 10 permit 172.16.0.0 0.0.31.255
```

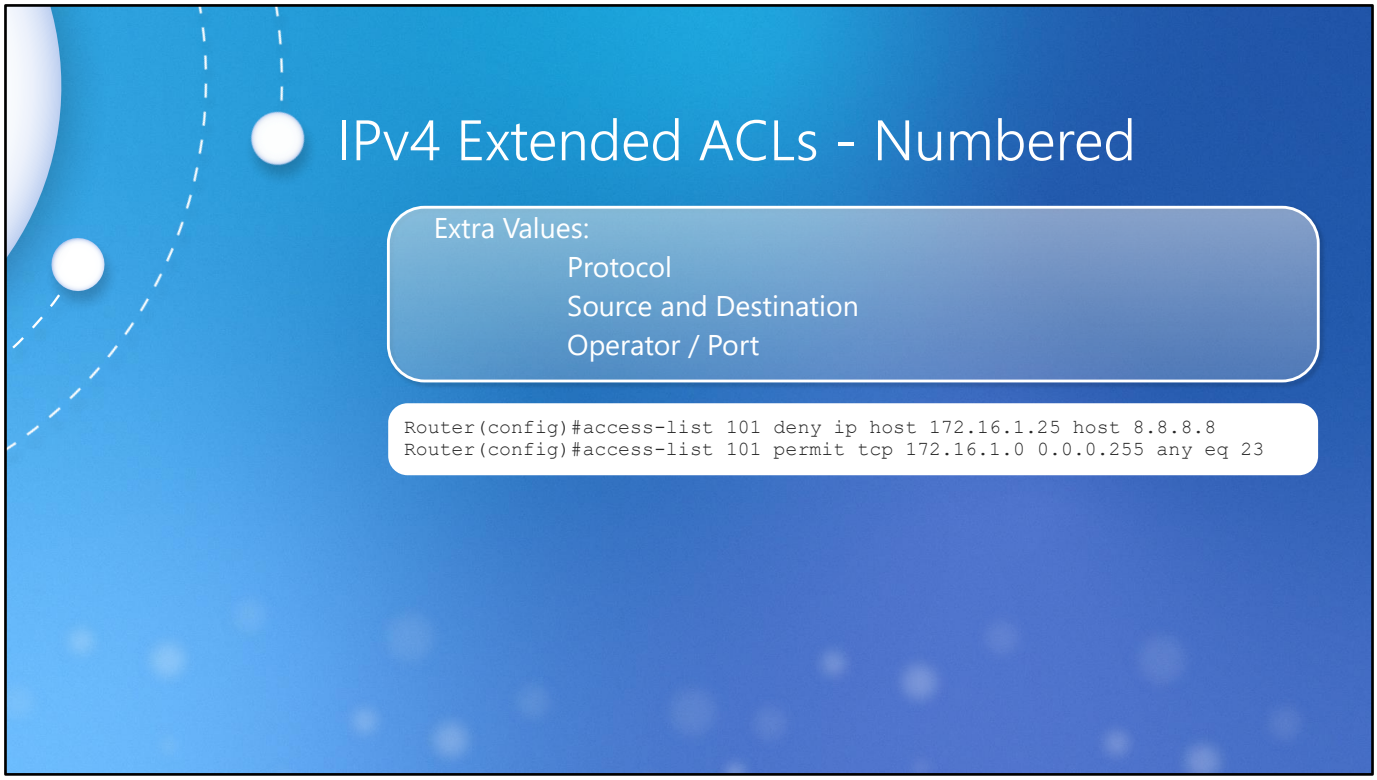
This would include 172.16.0.0/24 to 172.16.31.0.24 when we only need 172.16.10.0/24 to 172.16.26.0/24. All because of powers of 2.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Instructor Notes:
The physical topology and the logical topology.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Numbered – don't need the "ip" but will need to keep using the numeric value
Implicit deny

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

IPv4 Extended ACLs - Named

```
Router(config)#ip access-list extended TEST
Router(config-ext-nacl)# deny ip host 172.16.1.25 host 8.8.8.8
Router(config-ext-nacl)# deny ip host 172.16.1.50 any
Router(config-ext-nacl)# deny tcp 172.16.1.0 0.0.0.255 any eq 23
Router(config-ext-nacl)# permit ip any any


Router # show access-list
Extended IP access list TEST
    10 deny ip host 172.16.1.25 host 8.8.8.8
    20 deny ip host 172.16.1.50 any
    30 deny tcp 172.16.1.0 0.0.0.255 any eq telnet
    40 permit ip any any
```

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Editing IPv4 Named ACLs

To remove a single line item from a named ACL, you can use the "no <seq #>" command

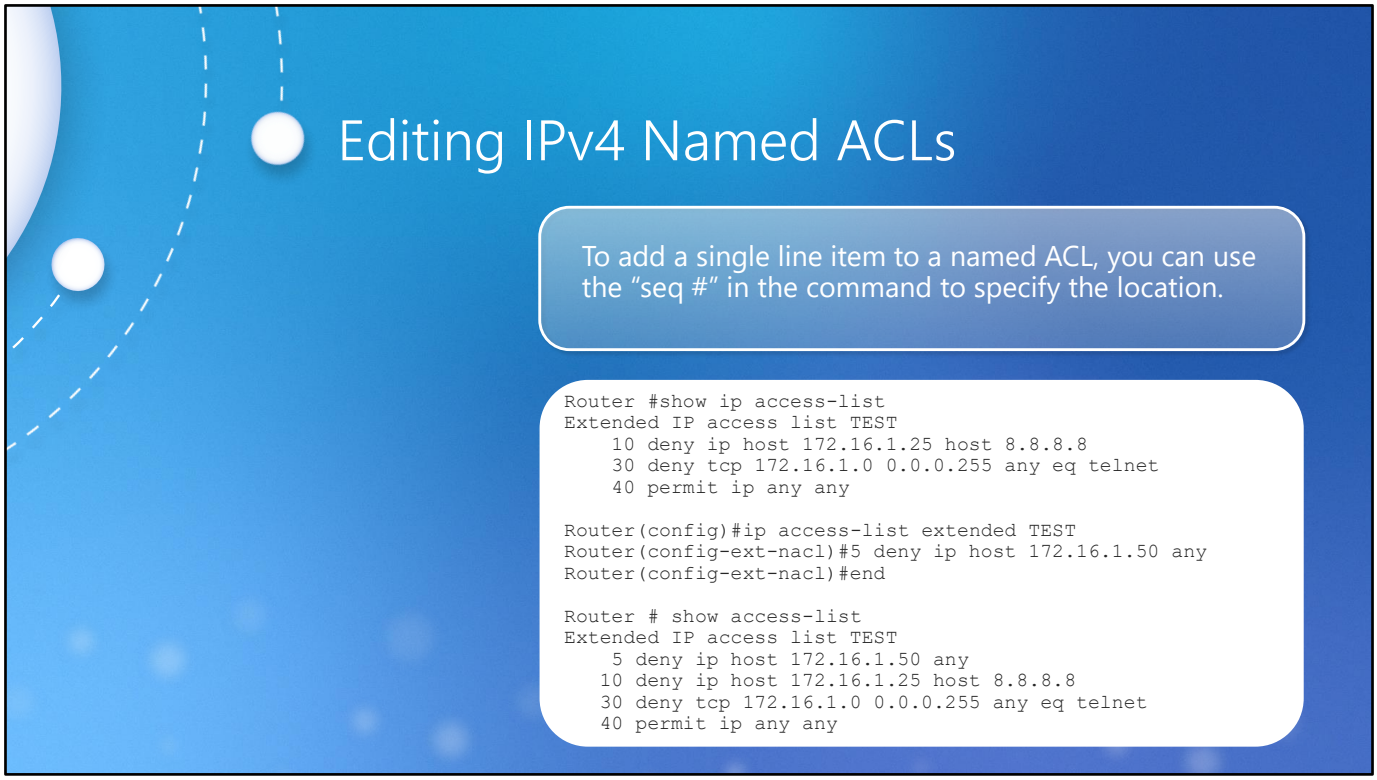
```
Router # show access-list
Extended IP access list TEST
    10 deny ip host 172.16.1.25 host 8.8.8.8
    20 deny ip host 172.16.1.50 any
    30 deny tcp 172.16.1.0 0.0.0.255 any eq telnet
    40 permit ip any any

Router(config)#ip access-list extended TEST
Router(config-ext-nacl)#no 20
Router(config-ext-nacl)#end

Router #show ip access-list
Extended IP access list TEST
    10 deny ip host 172.16.1.25 host 8.8.8.8
    30 deny tcp 172.16.1.0 0.0.0.255 any eq telnet
    40 permit ip any any
```

You can also use "show ip access-list"

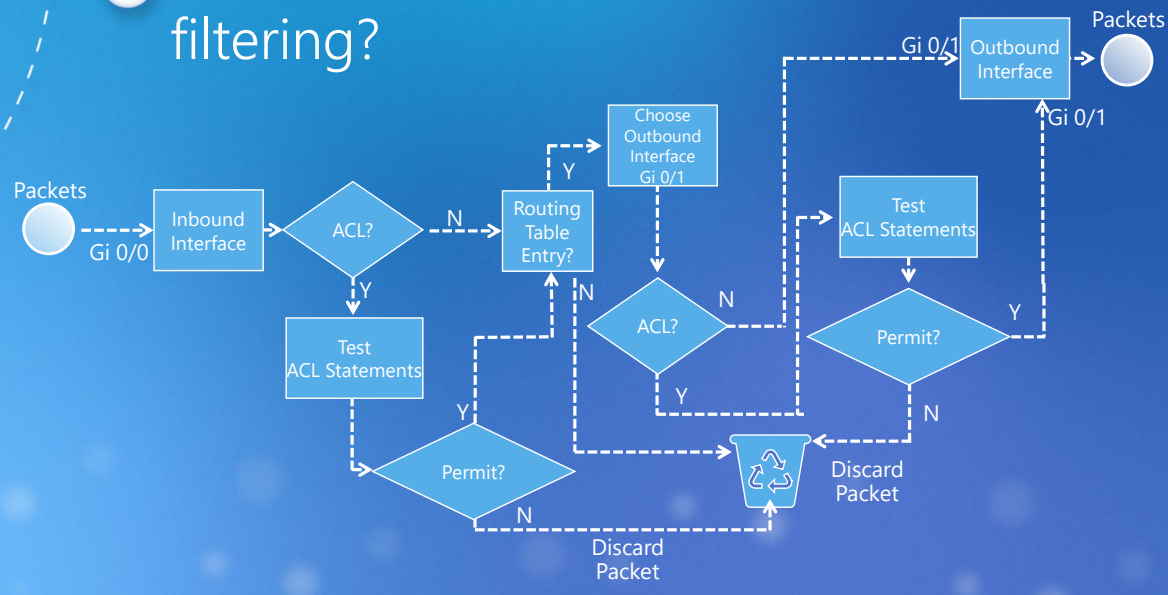
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



You can also use "show ip access-list"

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

When is an IPv4 ACL checked for traffic filtering?



©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Applying IPv4 ACLs for traffic filtering

```
Router(config)#int gigabitethernet 0/0
Router(config-if)#ip access-group TEST {in | out}
```

Important: Only one ACL is allowed per protocol, direction, and interface.

Consider adding “show ip interface s 0/0”

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

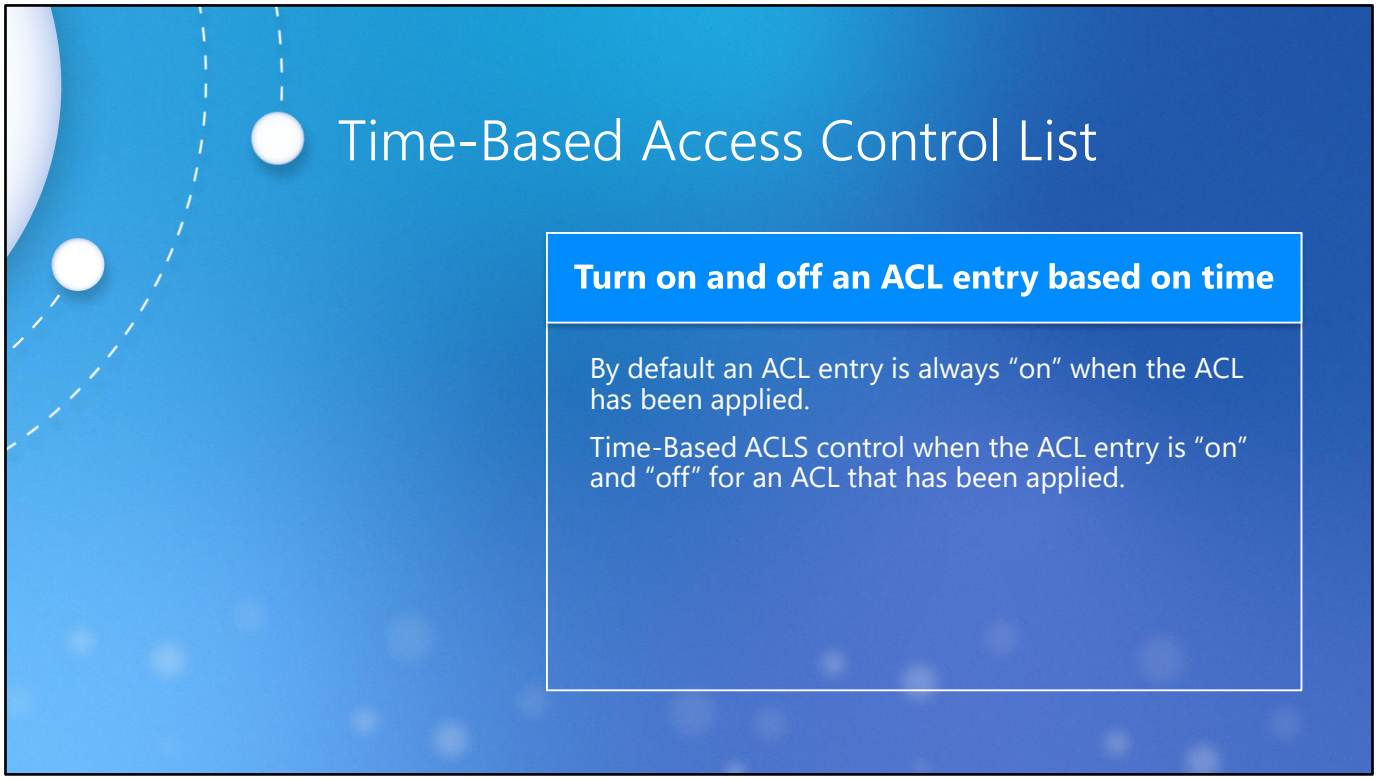
Verifying IPv4 ACLs

```
Router#show access-lists
Standard IP access list SALES
    10 deny 10.1.1.0, wildcard bits 0.0.0.255
    20 permit 10.3.3.1
    30 permit 10.4.4.1
    40 permit 10.5.5.1
Extended IP access list HR
    10 permit tcp host 10.22.22.1 any eq telnet (25 matches)
    20 permit tcp host 10.33.33.1 any eq ftp
    30 permit tcp host 10.44.44.1 any eq ftp-data
```

```
Router#show ip interface GigabitEthernet 0/0
GigabitEthernet0/0 is up, line protocol is up
    Internet address is 10.1.1.1/24
    Broadcast address is 255.255.255.255
    Address determined by setup command
    MTU is 1500 bytes
    Helper address is not set
    Directed broadcast forwarding is disabled
    Outgoing access list is not set
    Inbound access list is SALES
    Proxy ARP is enabled
    Local Proxy ARP is disabled
    <text omitted>
```

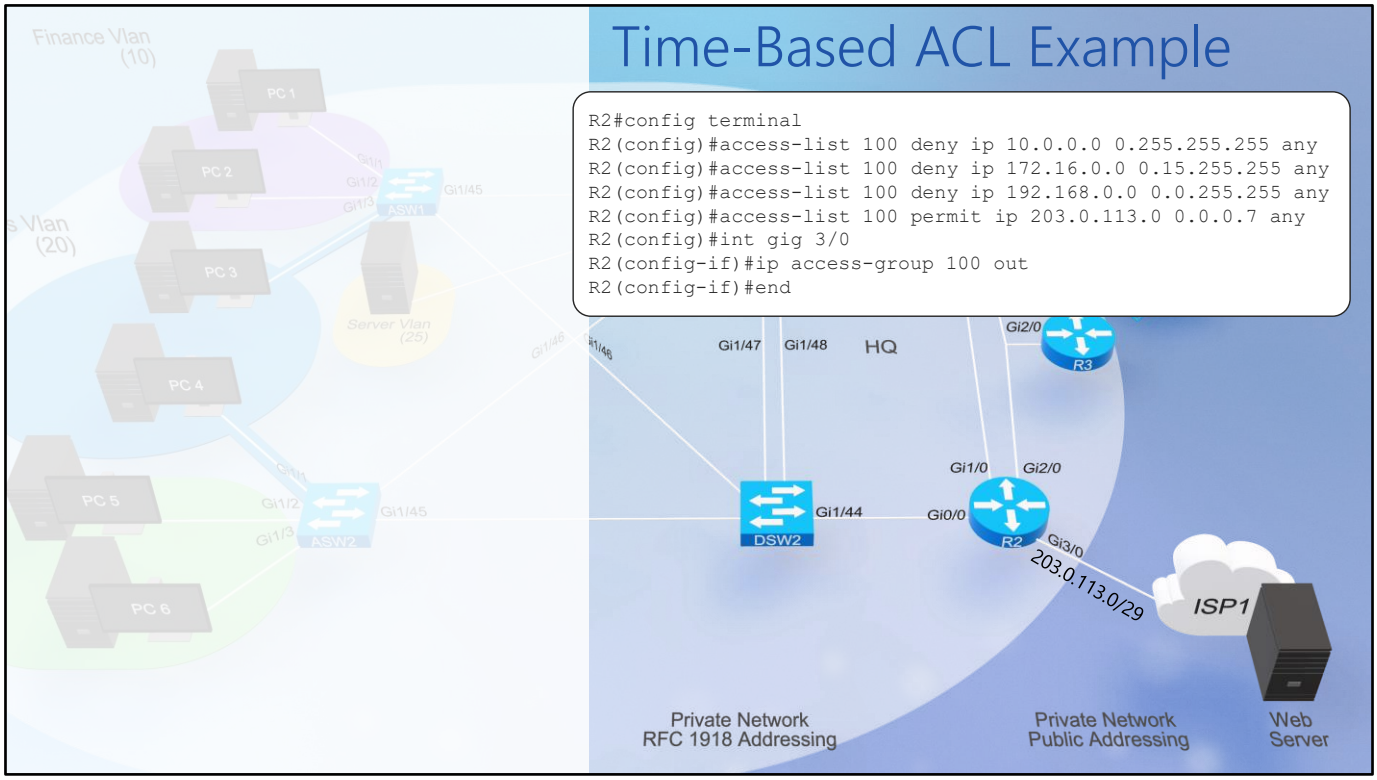
Consider adding “show ip interface s 0/0”

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



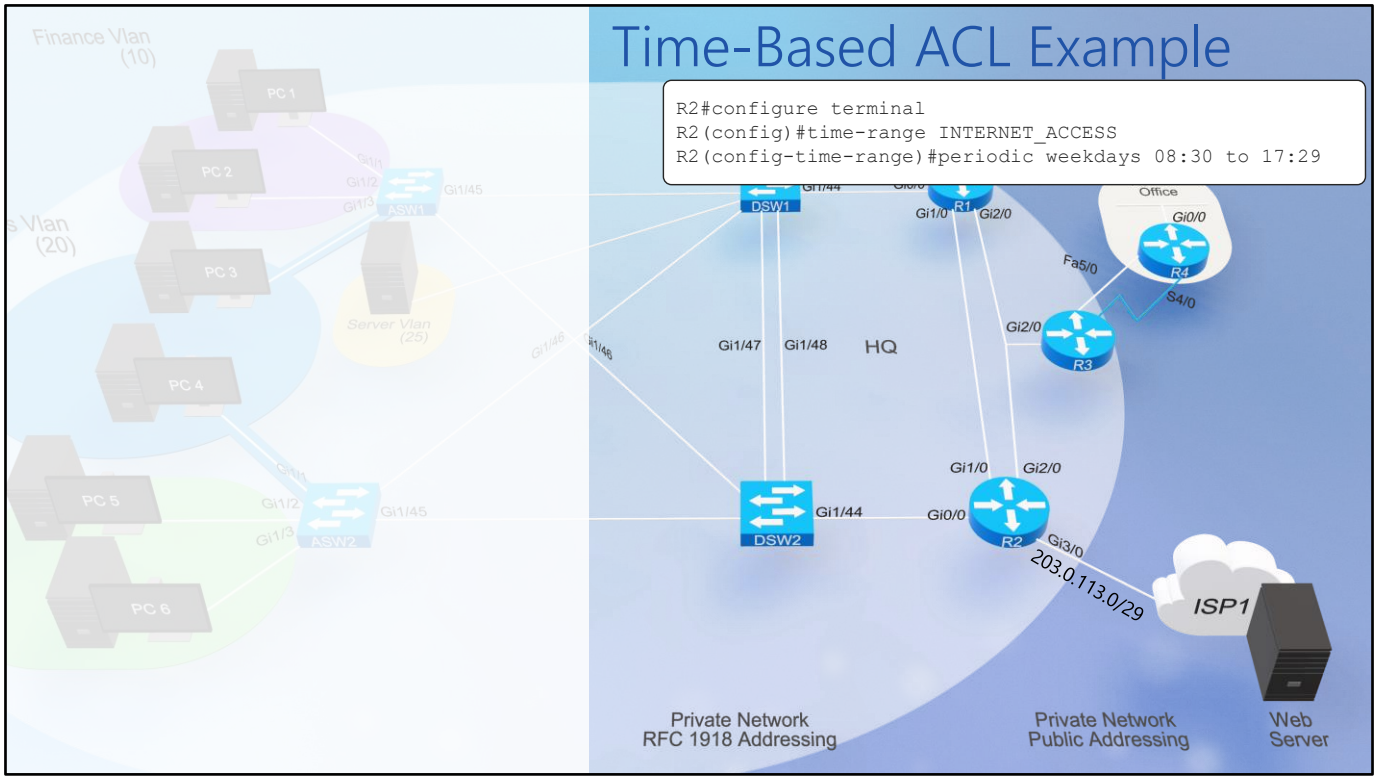
For example, what if you want to prevent traffic from going to the internet after hours and only allow it during business house. You can use a Time-Based ACL to control this. What if you want to allow access to a specific resource at a certain time every day for 1hr. You can use a Time-Based ACL to control this.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



In this case, ACL 10 permits traffic sourced from `203.0.113.0` to `203.0.113.7` to go to the internet 24hrs a day 7 days a week.

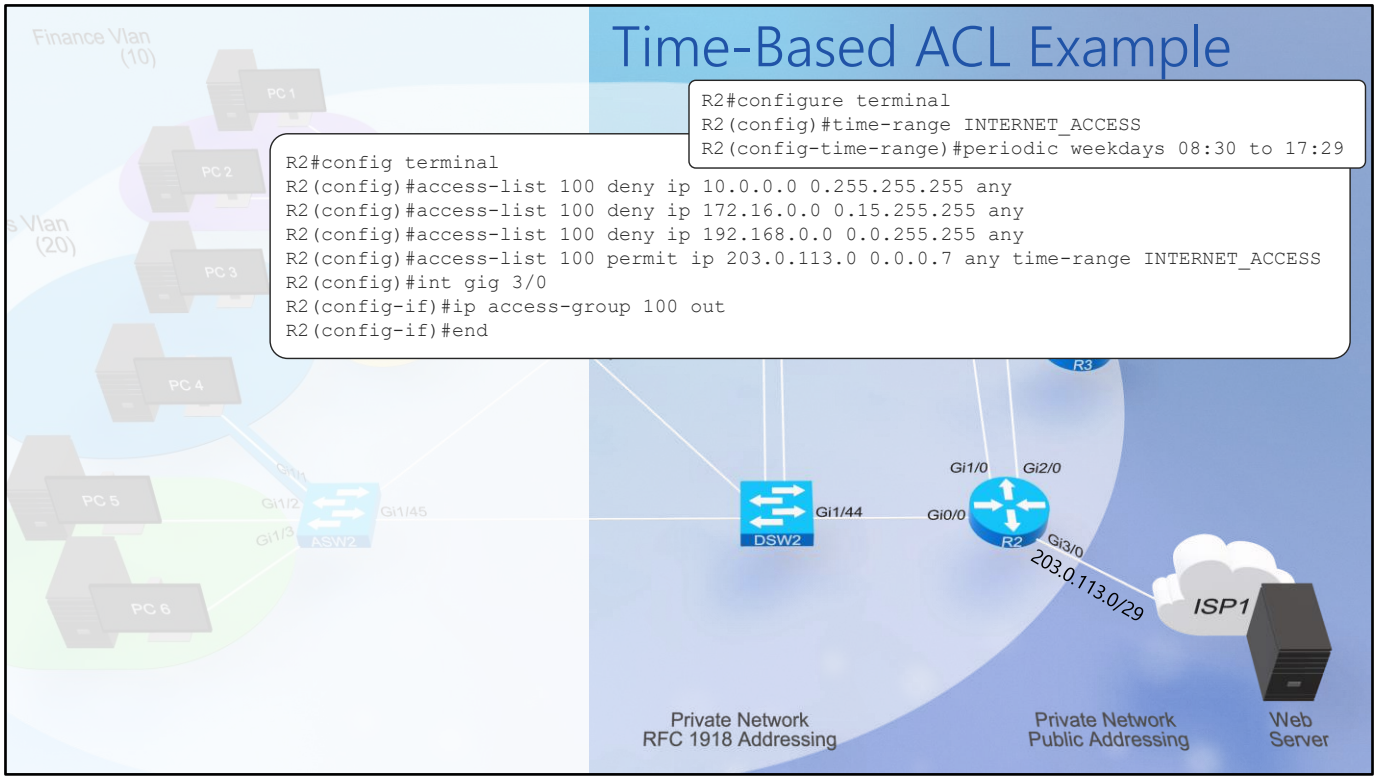
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



We have created a time range that states From 830am to 530pm… that is right 5:30pm… why??? See note below.

NOTE: hh:mm Ending time - stays valid until beginning of next minute

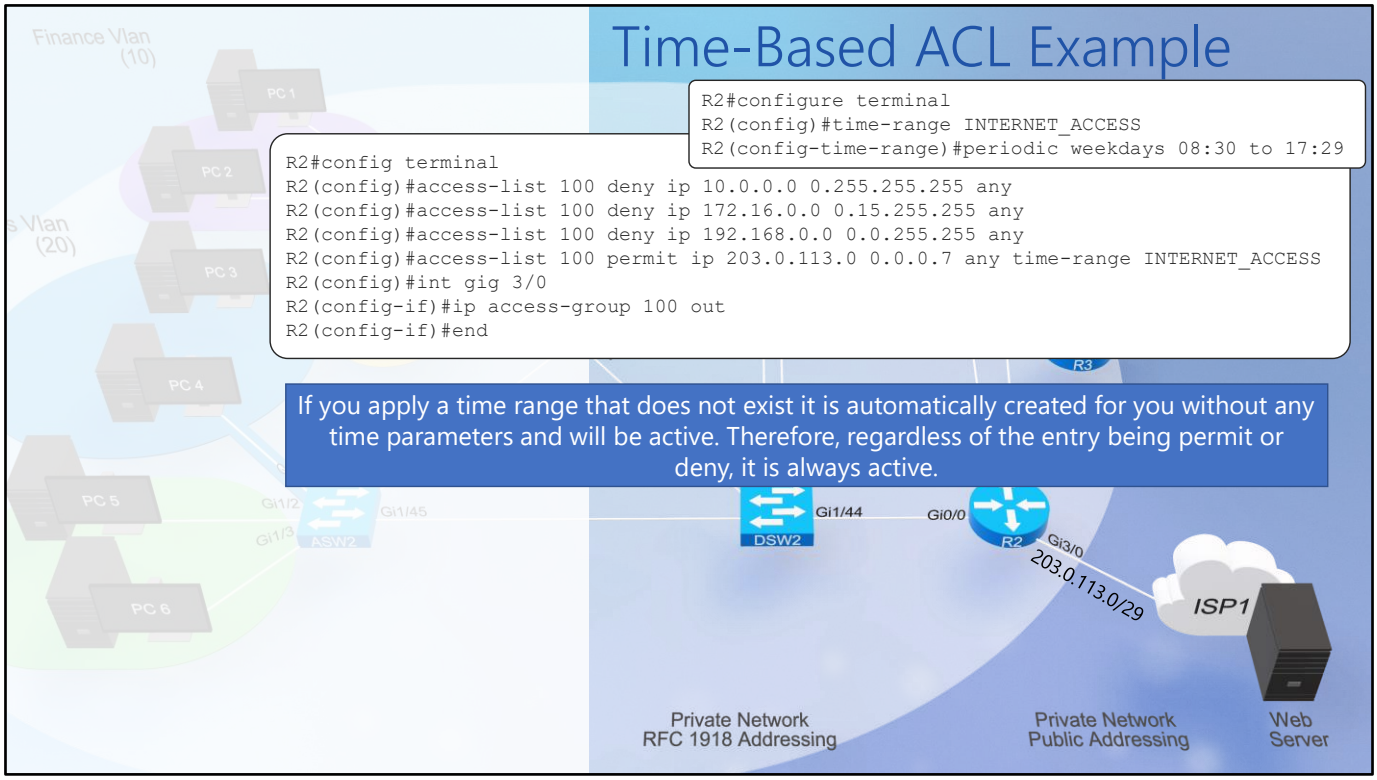
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



We have created a time range that states From 830am to 530pm… that is right 5:30pm… why??? See note below.

NOTE: hh:mm Ending time - stays valid until beginning of next minute

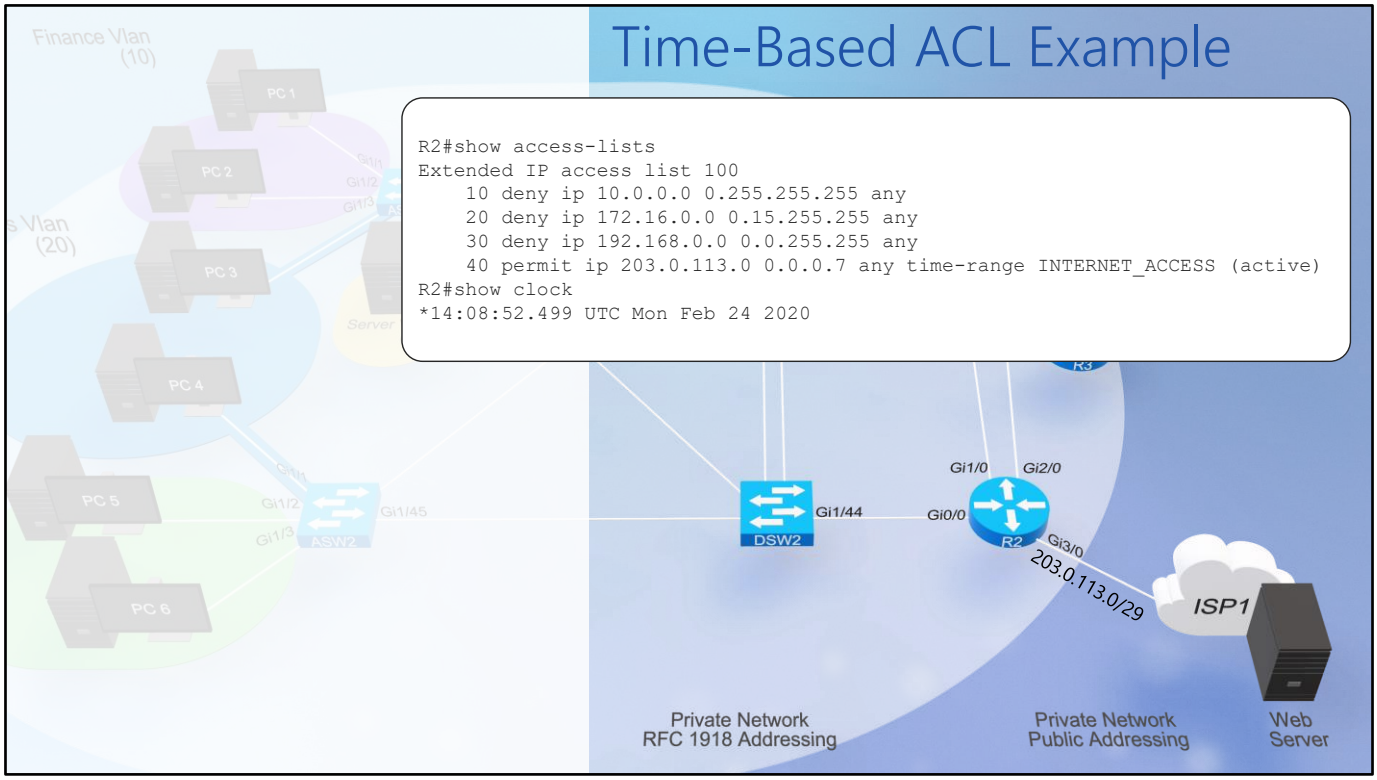
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



We have created a time range that states From 830am to 530pm… that is right 5:30pm… why??? See note below.

NOTE: hh:mm Ending time - stays valid until beginning of next minute

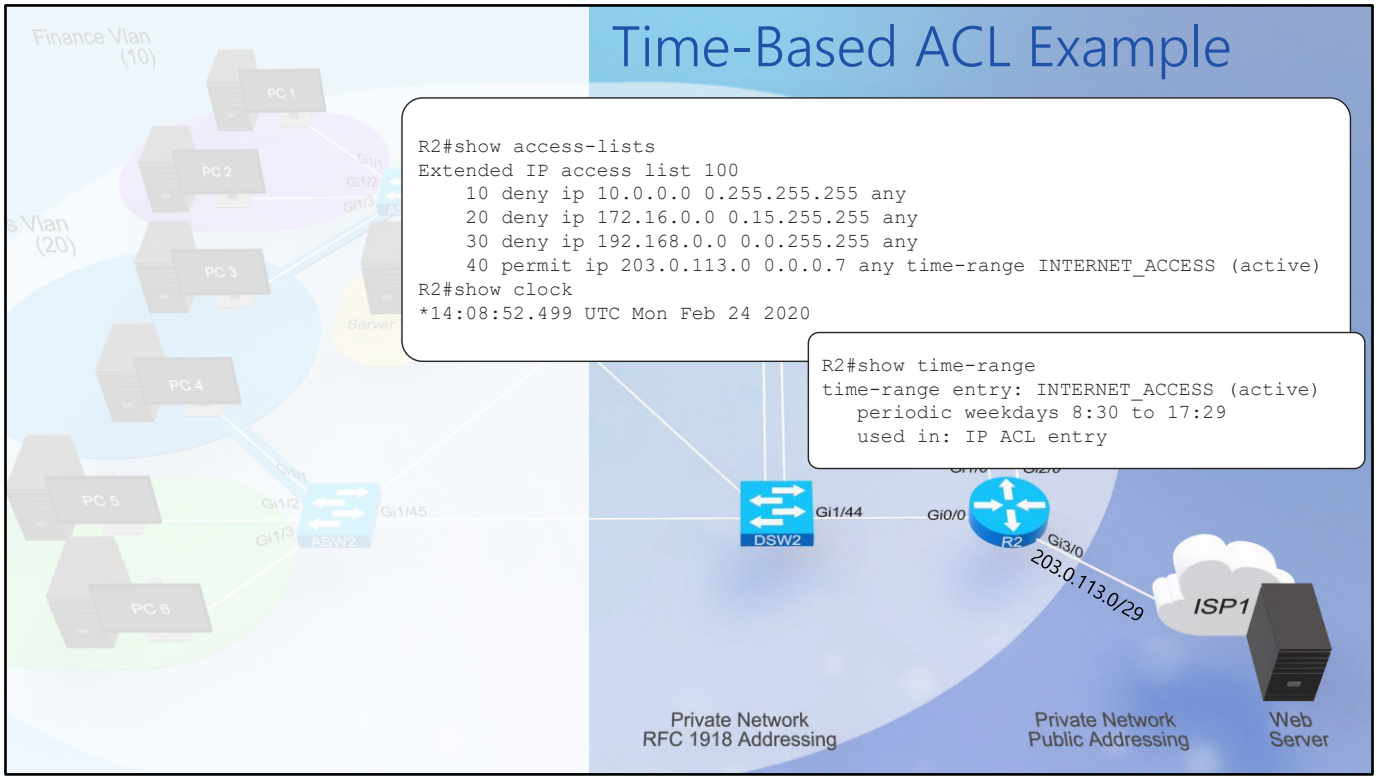
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



We have created a time range that states From 830am to 530pm… that is right 5:30pm… why??? See note below.

NOTE: hh:mm Ending time - stays valid until beginning of next minute

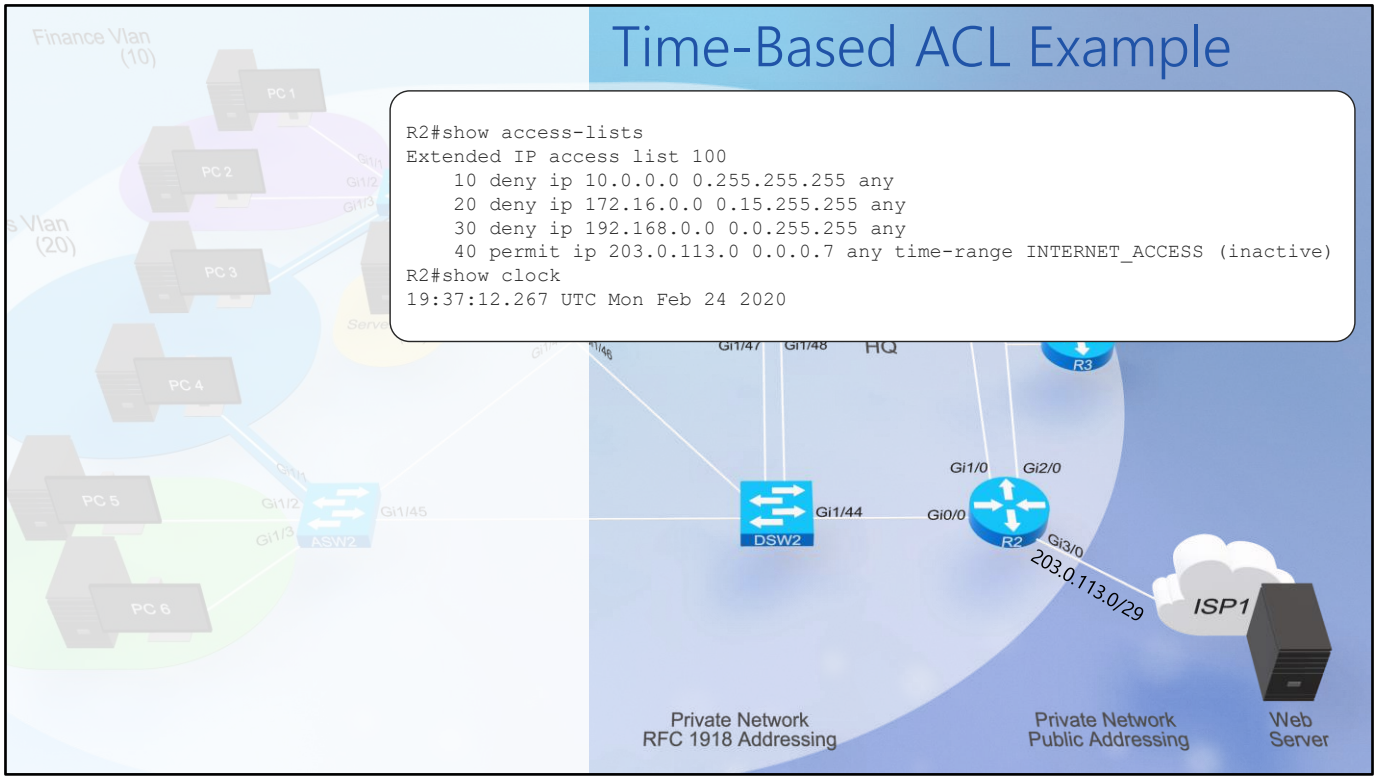
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



We have created a time range that states From 830am to 530pm… that is right 5:30pm… why??? See note below.

NOTE: hh:mm Ending time - stays valid until beginning of next minute

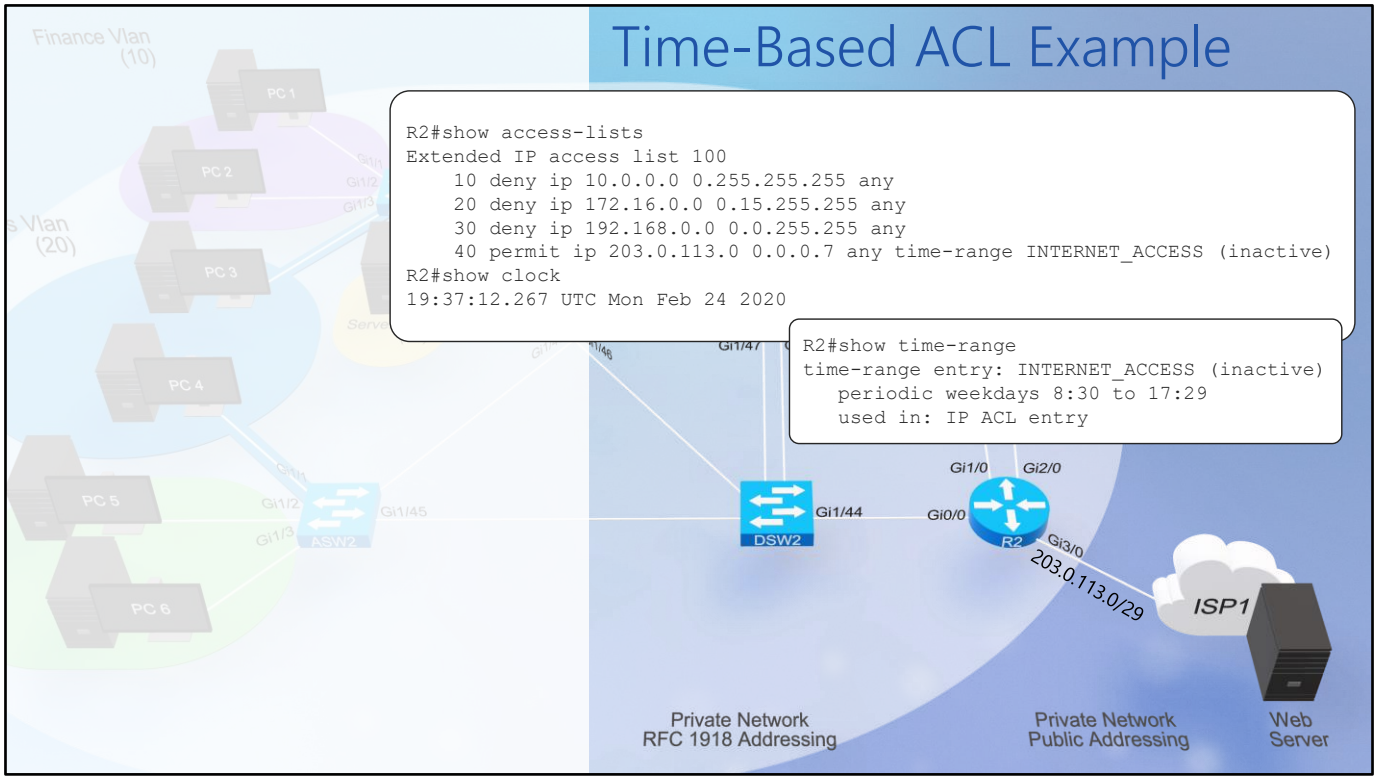
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



We have created a time range that states From 830am to 530pm… that is right 5:30pm… why??? See note below.

NOTE: hh:mm Ending time - stays valid until beginning of next minute

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

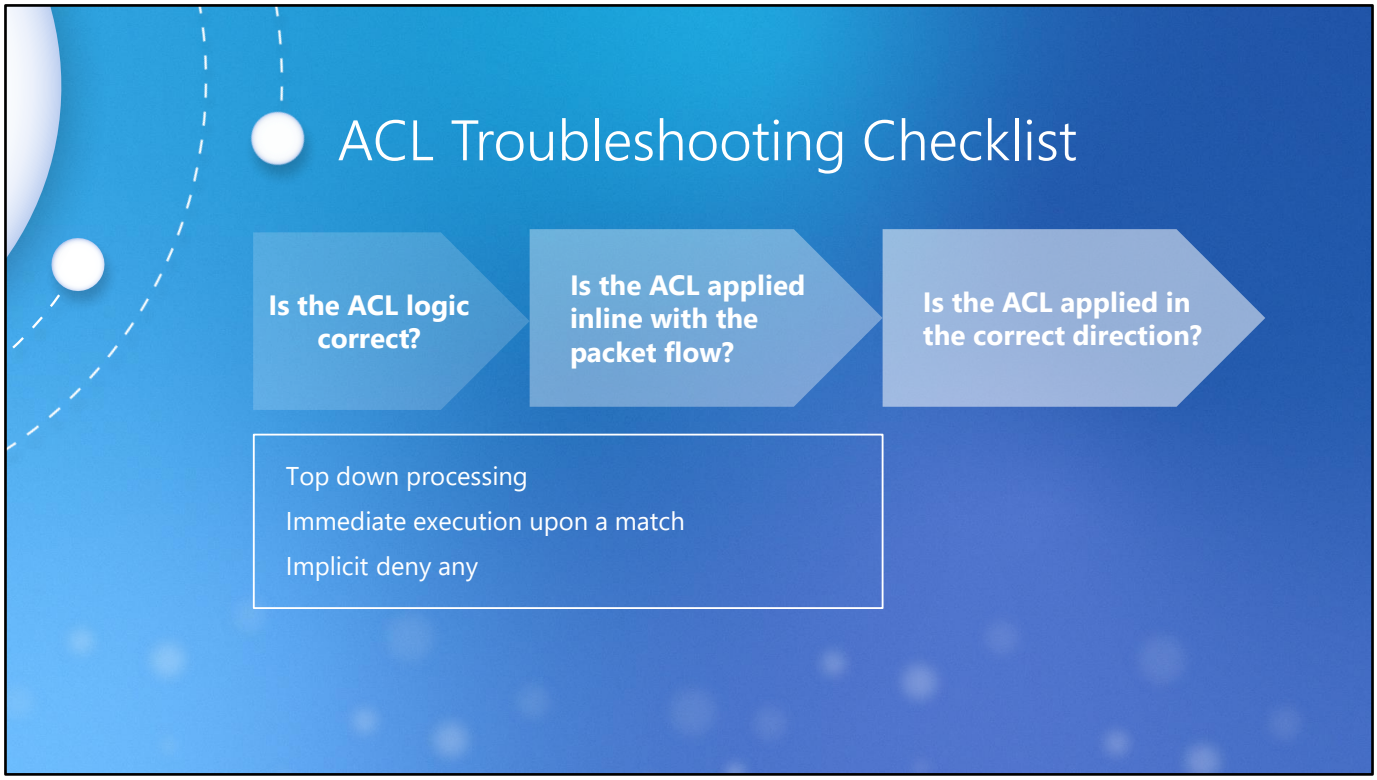


We have created a time range that states From 830am to 530pm… that is right 5:30pm… why??? See note below.

NOTE: hh:mm Ending time - stays valid until beginning of next minute

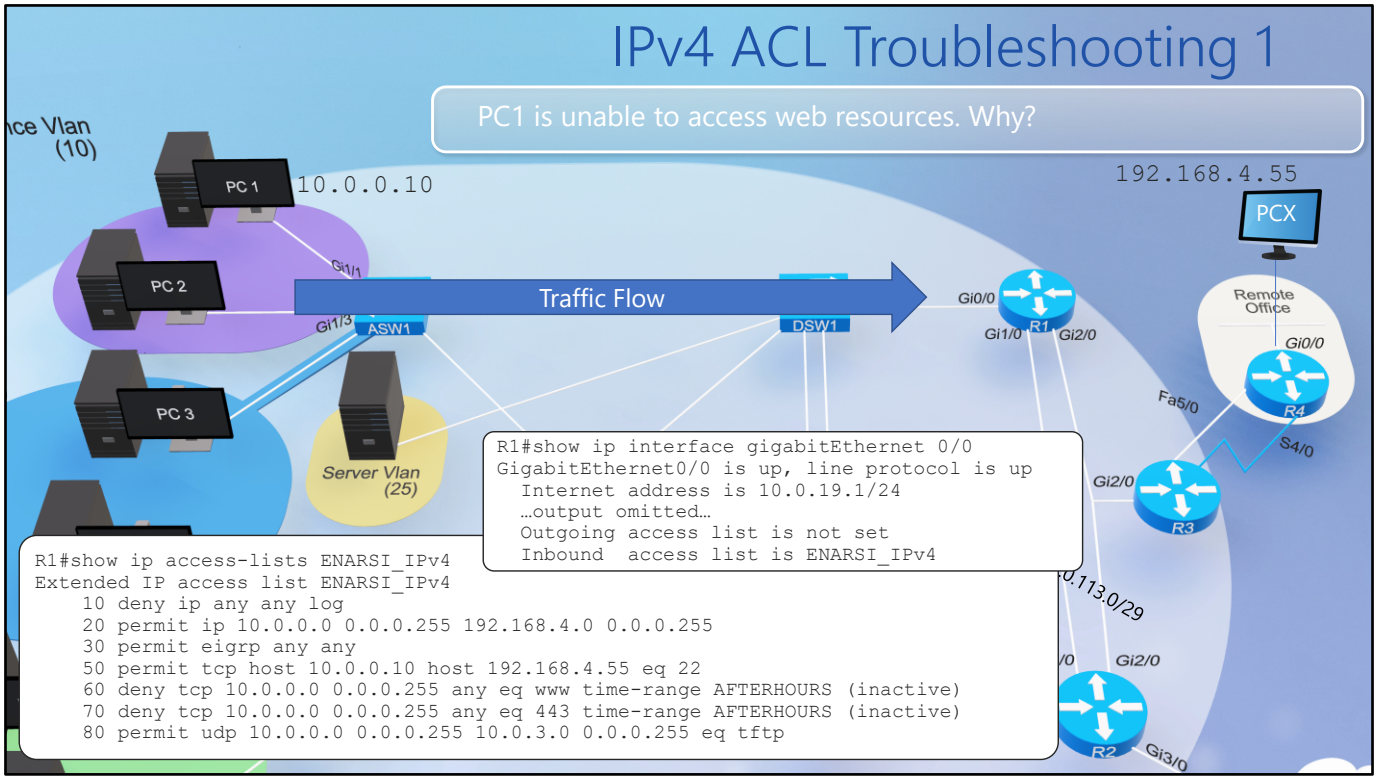
Please NOTE: inactive does not mean the opposite… permit becomes deny or deny becomes permit… it means ignore. So, seq 40 will not be checked at this time. Therefore, the implicit deny will drop the packets.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Consider adding “show ip interface s 0/0”

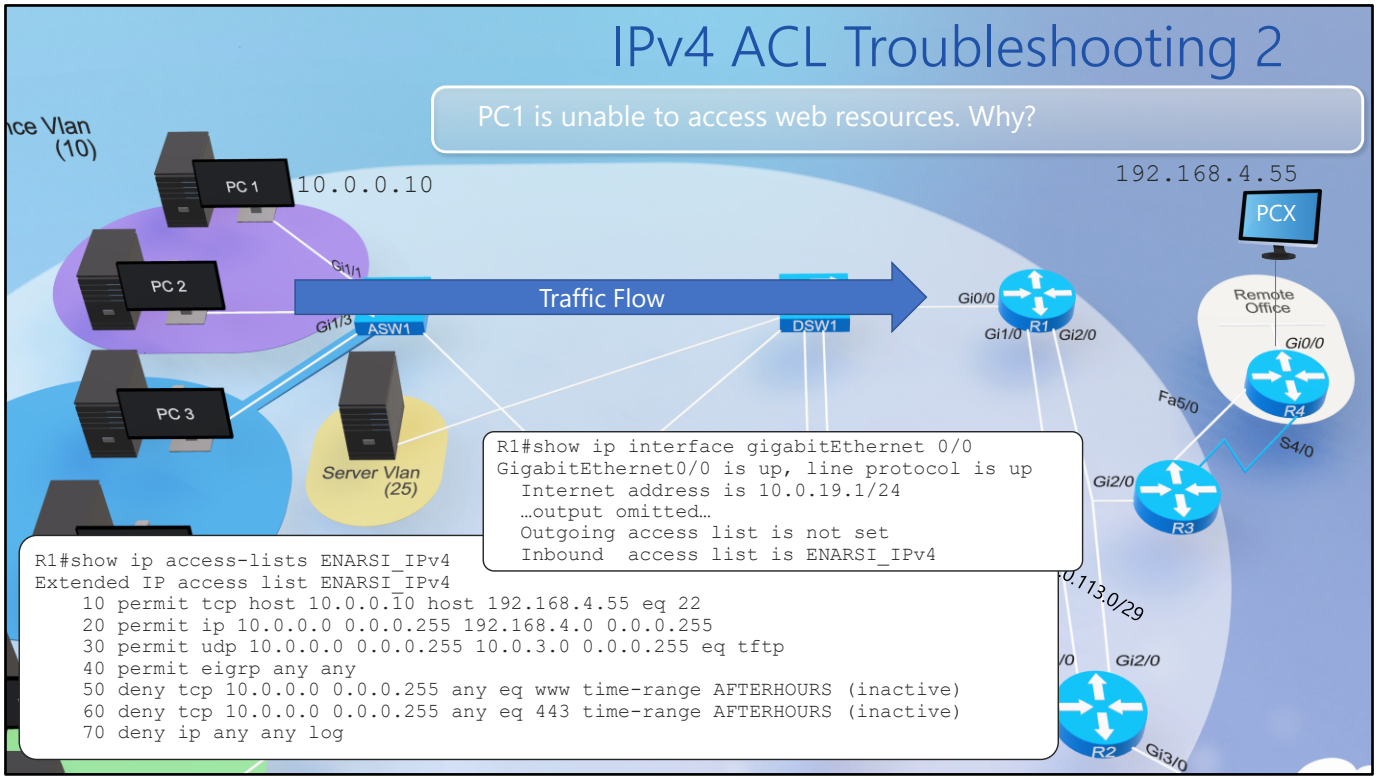
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Seq 60 and 70 are inactive which means deny is not ineffect therefore web traffic is permitted.

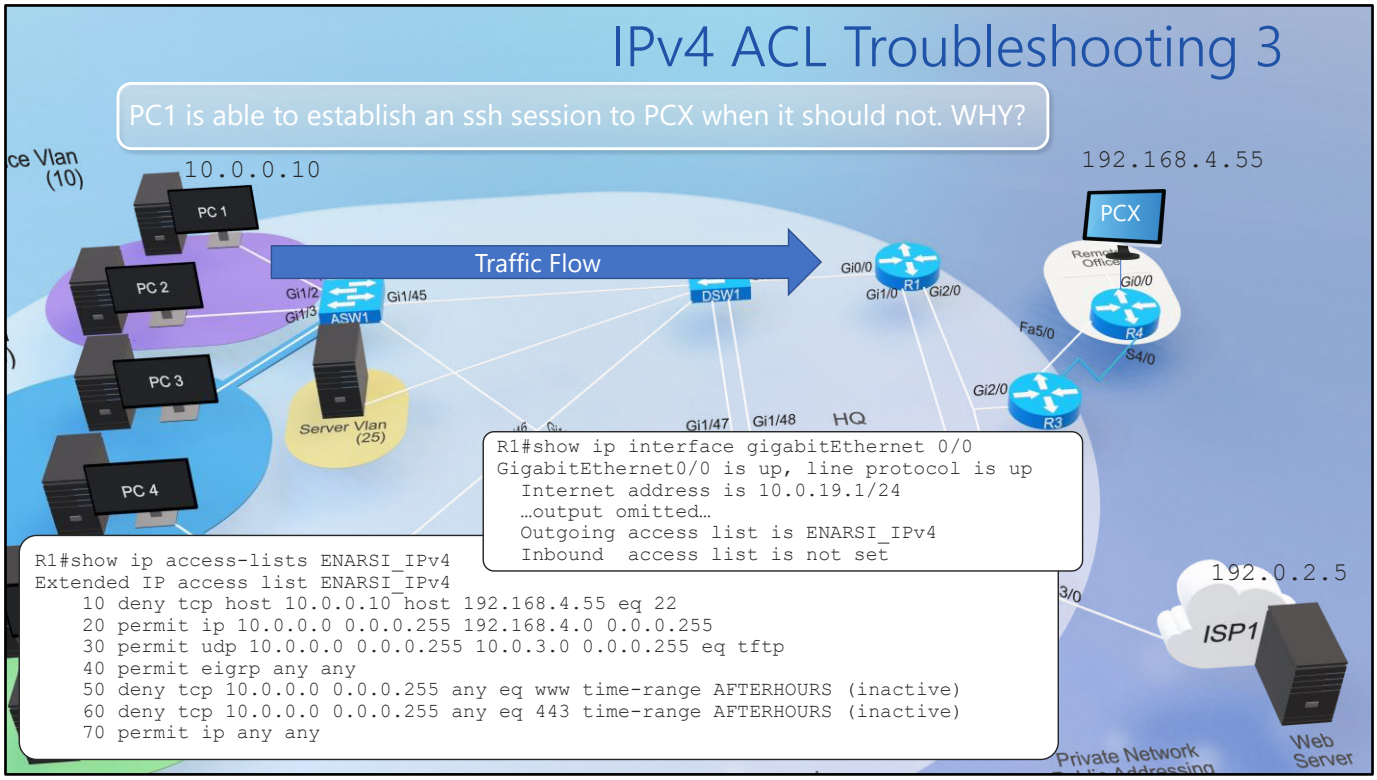
The real problem is order of operations. This ACL is all messed up and we have many problems here all because deny ip any any is listed first. EIGRP packets are even being denied therefore there is no neighborship between DSW1 and R1 therefore packets are being dropped on DSW1 because it does not have a route to the destination. ☺

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



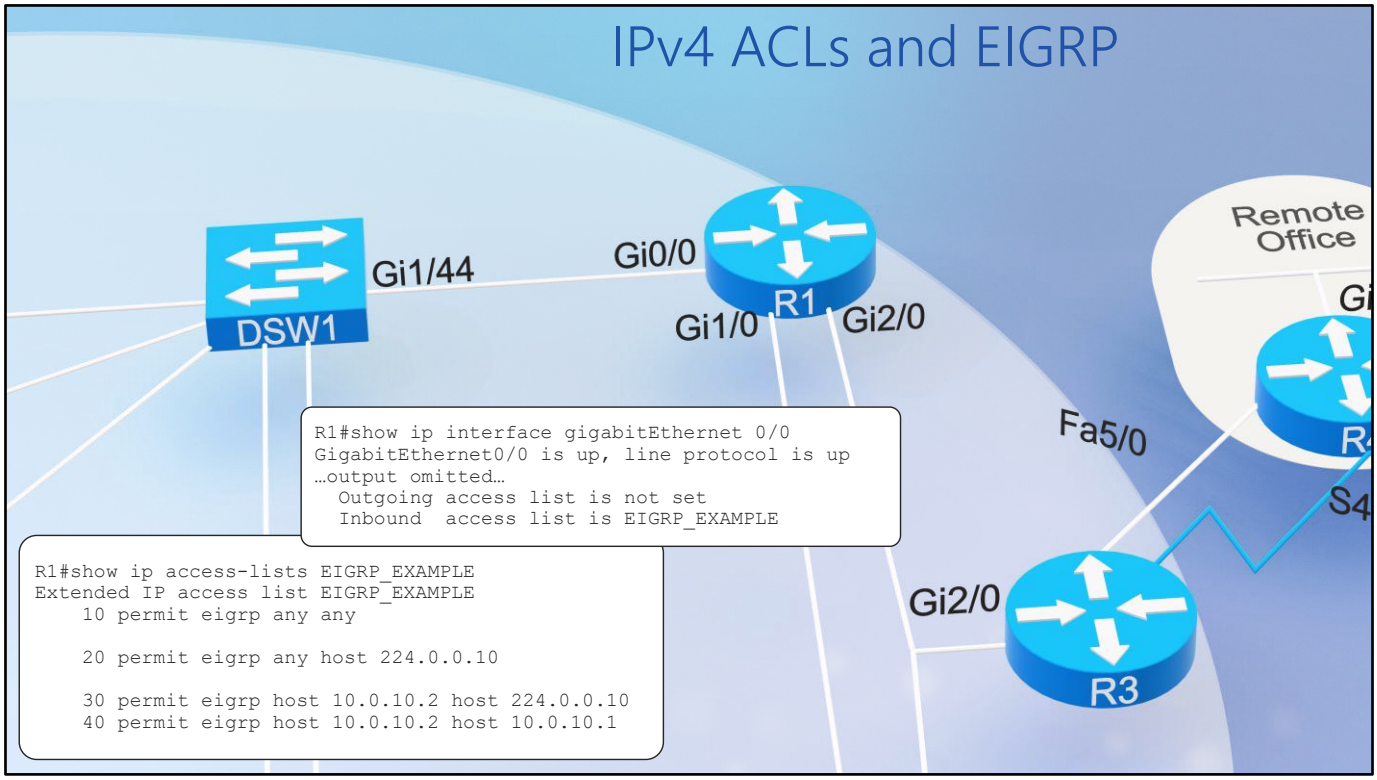
Seq 50 and 60 are inactive therefore it is not afterhours and web traffic would not be denied. However, it is not being permitted either. Therefore, it is being denied by seq 70. You would need to permit port 80 and 443 traffic after seq 50 and 60 to solve this issue.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



The ACL is applied in the wrong direction.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



FIRST…. Only inbound ACLs affect EIGRP packets, outbound ACLs do not.

All of these options could have eigrp or 88 listed.

EIGRP establishes a neighbor adjacency using multicast (unless you configure a unicast neighbor adjacency)

- Interface address as source
- 224.0.0.10 as the destination.

EIGRP exchanges update packets using unicast

- Interface address as source
- Interface address as destination

Options:

`permit eigrp any any (this would take care of both multicast and unicast eigrp packets)`

`permit eigrp any host 224.0.0.10 (this would take care of just the multicast packets)`

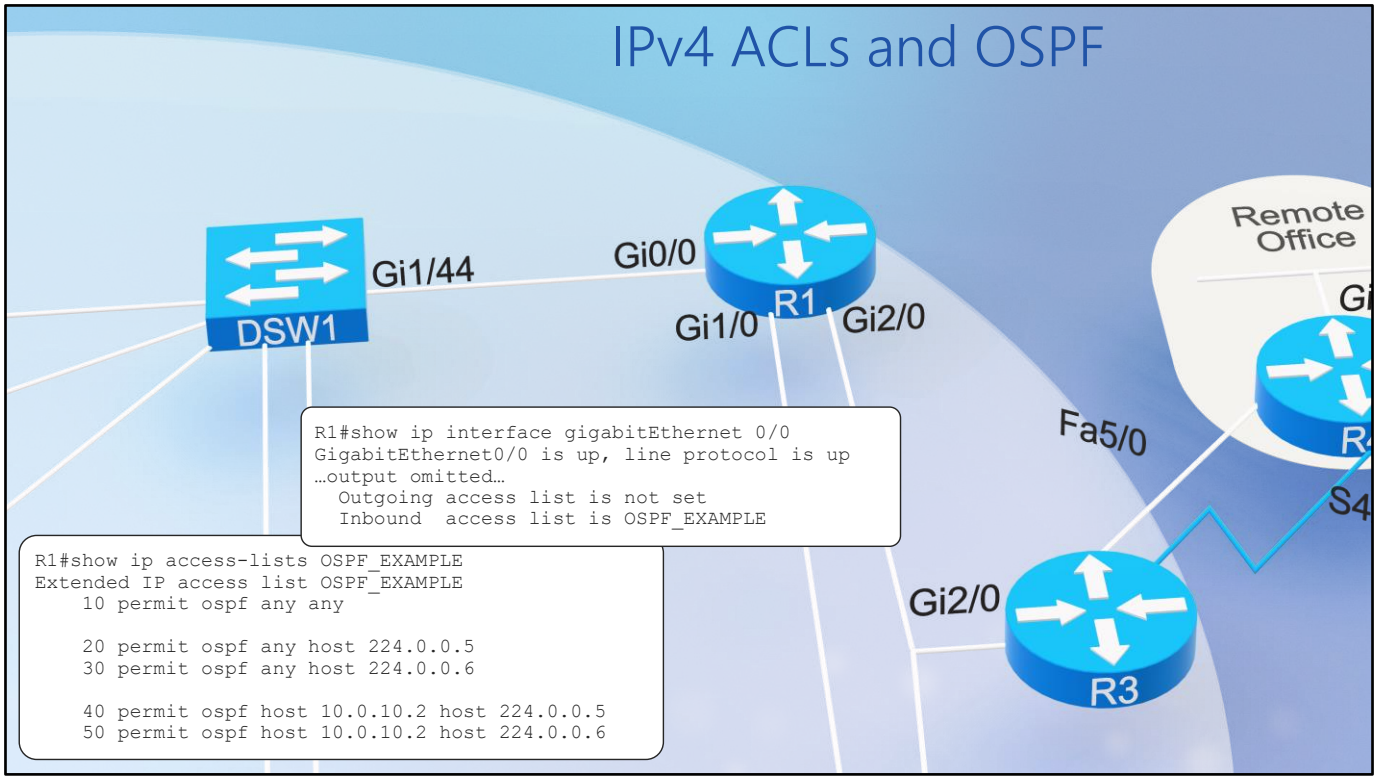
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

```
permit eigrp host 10.0.10.2 host 10.0.10.1 (you would
need this to take care of the unicast packets)

permit eigrp host 10.0.10.2 host 224.0.0.10 (this would
take care of multicast from that source)
permit eigrp host 10.0.10.2 host 10.0.10.1 (this would
take care of unicast from that source)
```

You can usually recognize an ACL neighbor issue because one neighbor sees the other router but the other router does not see the neighbor. In this case if the ACL was not correct then DSW1 would see R1 as a neighbor in the neighbor table but R1 would not see DSW1 in its neighbor table.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



FIRST…. Only inbound ACLs affect OSPF packets, outbound ACLs do not.

All of these options could have ospf or 89 listed

OSPF establishes a neighbor adjacency and exchanges packets using multicast (unless you configure a unicast neighbor adjacency)

Interface address as source

224.0.0.5 as the destination (for hellos and to send info (updates) to all ospf routers) or 224.0.0.6 as the destination for the DR.

Options:

```
permit ospf any any (this takes care of all ospf packets)

permit ospf any host 224.0.0.5 (this takes care of
anything destined to 224.0.0.5 from anyone)
permit ospf any host 224.0.0.6 (this takes care of
anything destined to DR from anyone)

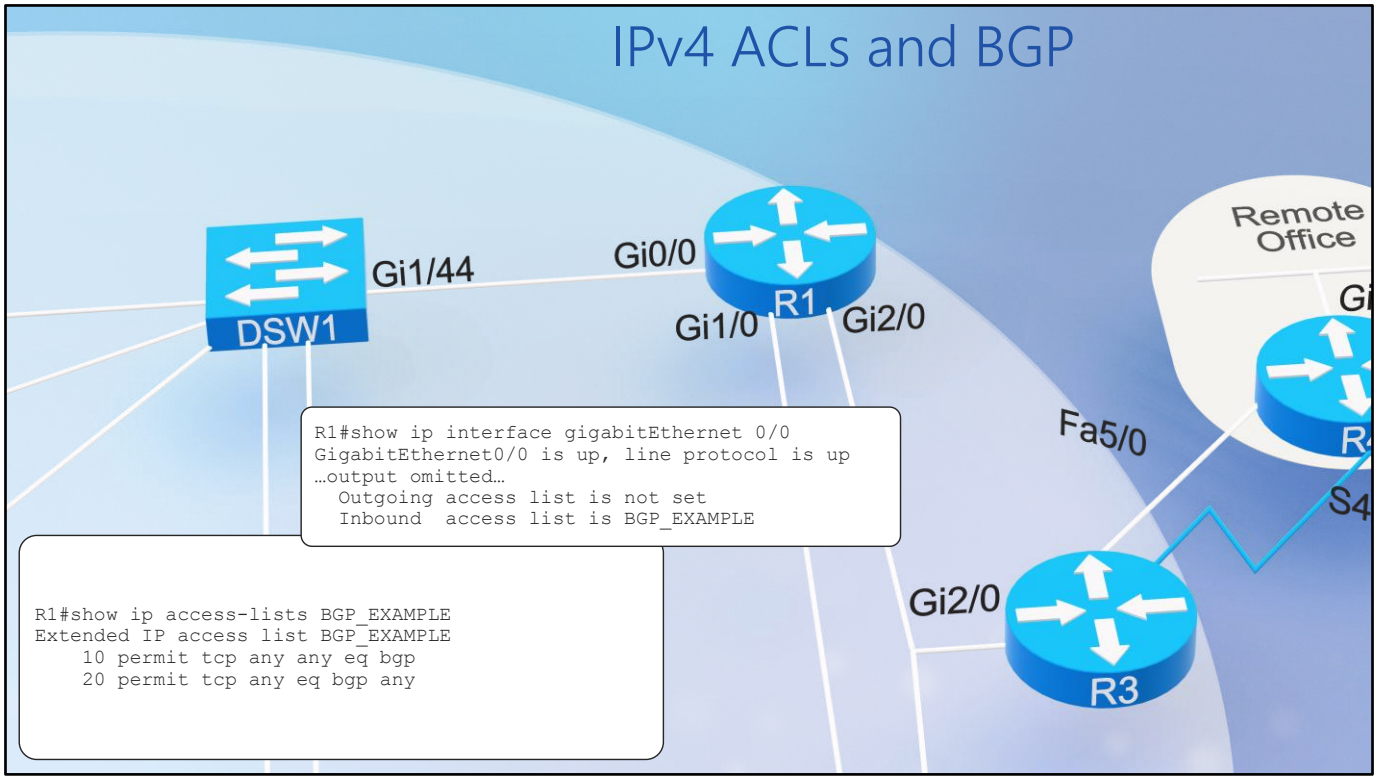
permit ospf host 10.0.10.2 host 224.0.0.5 (this takes
care of anything destined to 224.0.0.5 from the specific
```

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

```
neighbor)
permit ospf host 10.0.10.2 host 224.0.0.6 (this takes
care of anything destined to DR from the specific
neighbor)
```

You can usually recognize an ACL neighbor issue because one neighbor sees the other router but the other router does not see the neighbor. In this case if the ACL was not correct then DSW1 would see R1 as a neighbor in the neighbor table but R1 would not see DSW1 in its neighbor table.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



FIRST…. Only inbound ACLs affect BGP packets, outbound ACLs do not.

Ok… remember that BGP is a client/server peer-to-peer unicast neighbor relationship.

Both routers attempt to be the client and the server by default unless you force one or the other to be the client or the server.

So, in this case I am setting up the router to accept incoming requests to the server port… or incoming requests to the client port

```
permit tcp any any eq bgp (this entry is used if R1 is
the server. It allows the tcp packets destined to port
179 to be allowed in from any client using any port
number)
permit tcp any eq bgp any (this entry is used if R1 is
the client. It allows the tcp packets destined to the
random port number of R1[client] from the server using
TCP179 to be allowed in.

You can be more granular and specify the source and
```

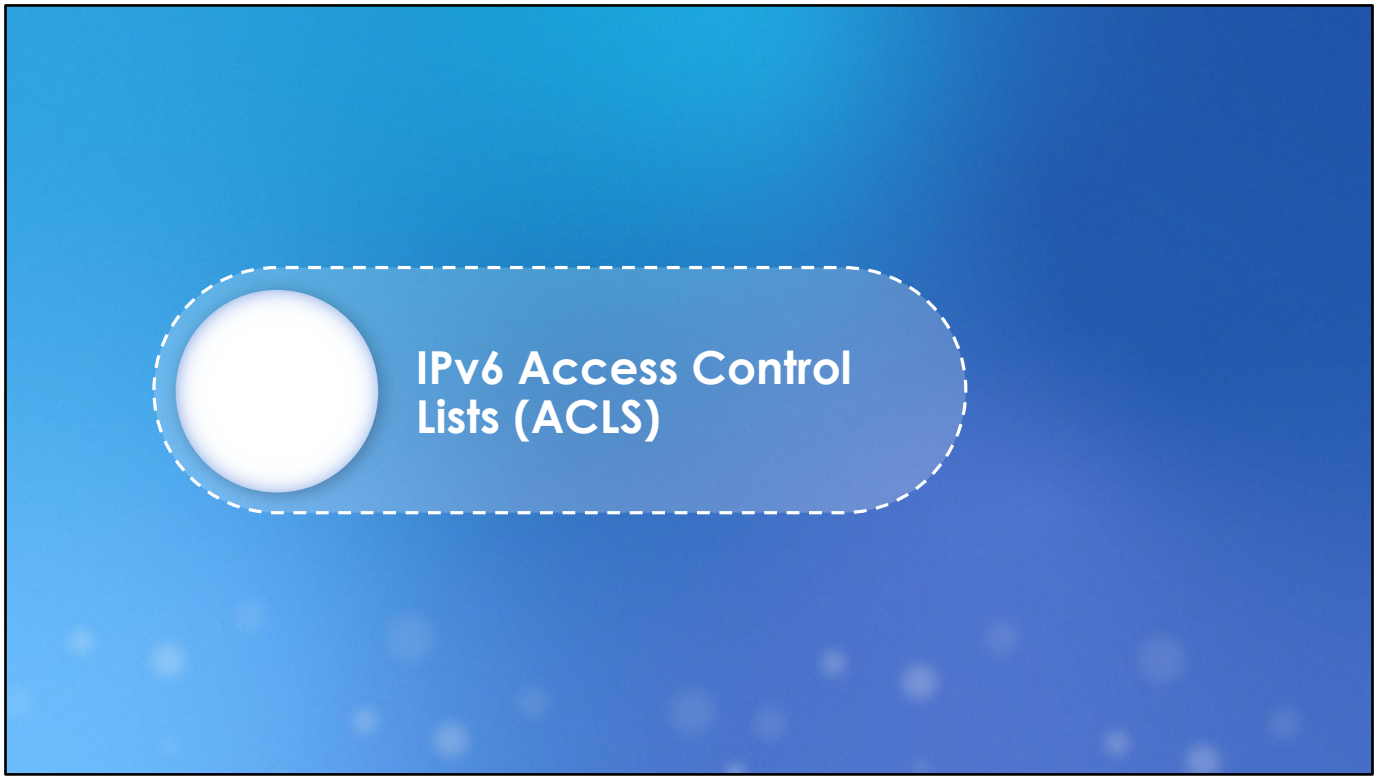
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

destination address of the BGP packets for added security.

Now, are both required. No. For example if you have set up the routers so that one is going to be the server (passive) and the other is going to be the client (active) then you can just set up a single ACL based on the traffic flow.

However, what you just set up one without forcing the routers to be a client/server (for example **permit tcp any any eq bgp**). Well in this case BGP packets destined to TCP 179 are allowed in which means R1 will become the server as BGP client packets are not allowed in. So, it would still work and forces one router to be the server and the other to be the client.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Title slide

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Access Control List

ACL

An ACL provides traffic identification

When traffic is identified, a variety of actions can be applied based on purpose:

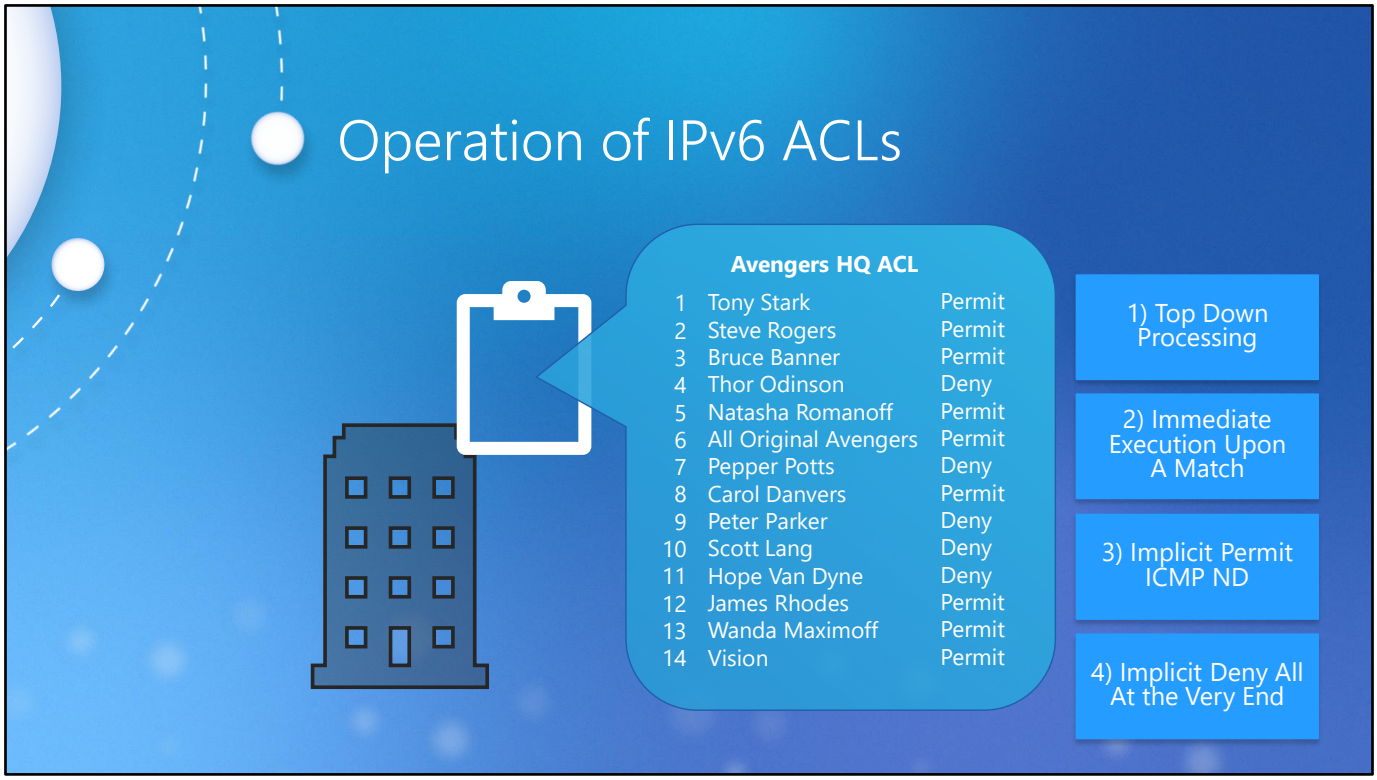
- Permit, Deny, Change traffic direction, and more
  - NAT, Traffic Filter, QoS, PBR, Route Filter, etc…

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Access Control List

ACL
An ACL is made of Access Control Entries (ACEs)
ACEs can be permit and deny statements
Access Lists can be used on routers and switches

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

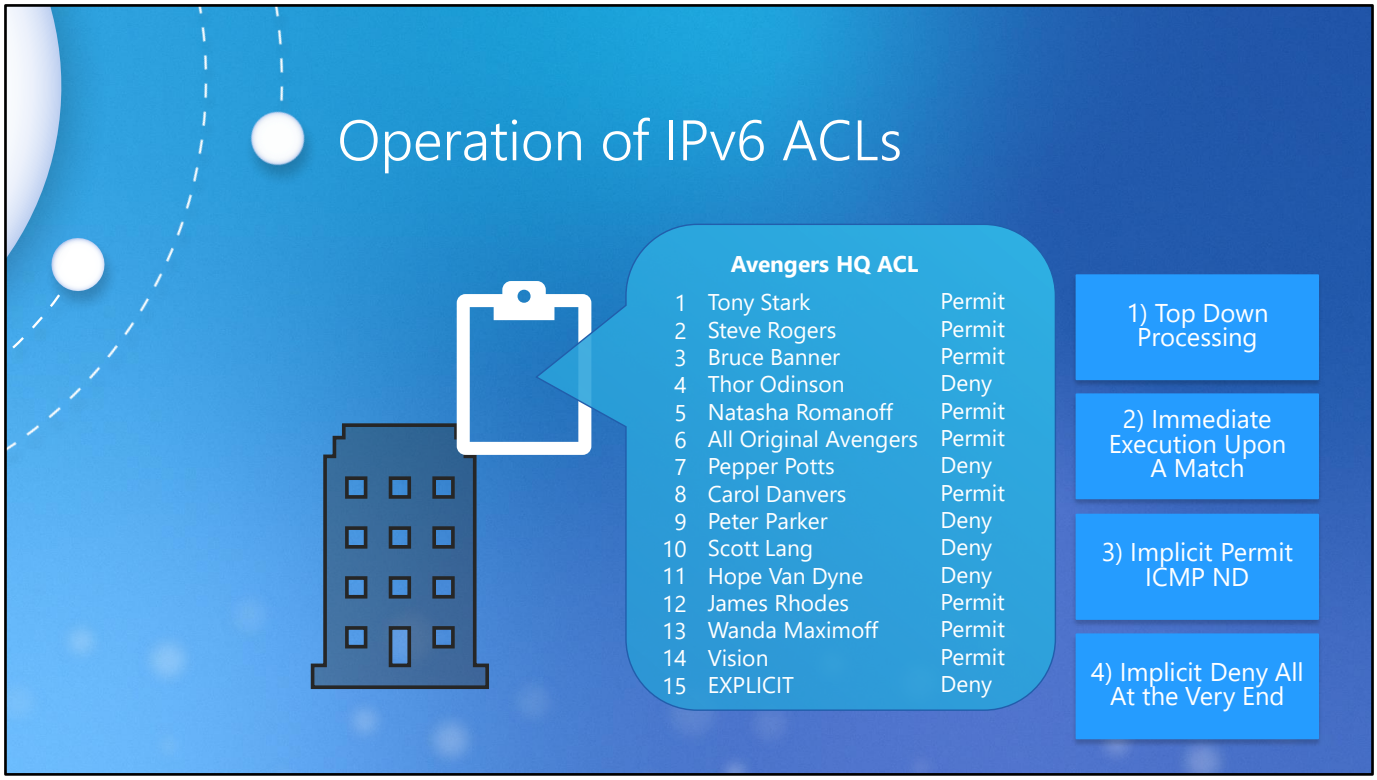


All Original = Steve, Tony, Bruce, Thor, Natasha, Clint Barton

If THOR shows up at the door and knocks…. What happens????

ICMP ND is used for address resolution (it does the same thing as ARP for IPv4). The invisible implicit permit ICMP ND entry is used to ensure that ND messages are permitted. (permit icmp na, permit icmp ns)

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



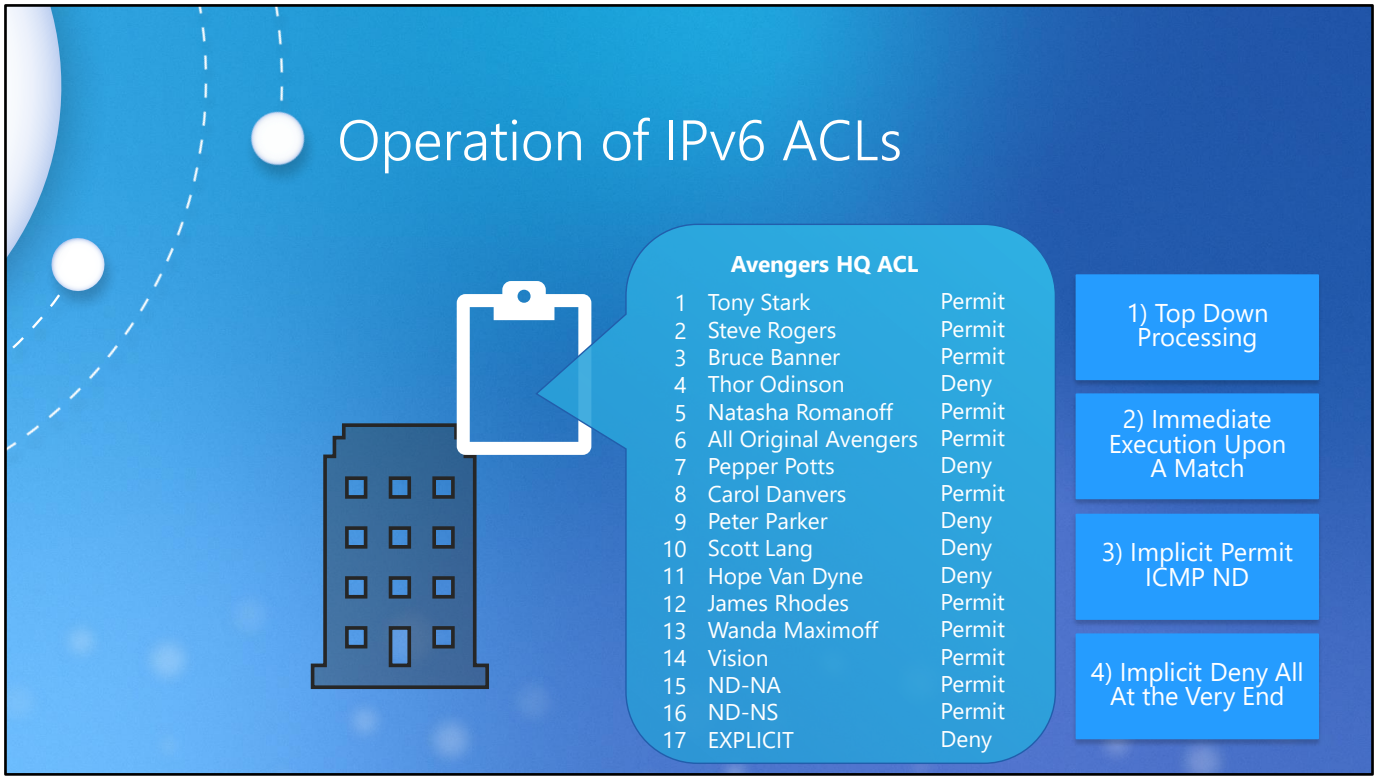
All Original = Steve, Tony, Bruce, Thor, Natasha, Clint Barton

If THOR shows up at the door and knocks…. What happens????

ICMP ND is used for address resolution. The invisible implicit permit ICMP ND entry is used to ensure that ND messages are permitted.

So what happens if you create an explicit deny entry for logging at the end of the ACL????
The explicit deny comes after 2 and before 3 in the list. Therefore, all ND messages will be denied.
The solution…. Create explicit ND permit entries.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



All Original = Steve, Tony, Bruce, Thor, Natasha, Clint Barton

If THOR shows up at the door and knocks…. What happens????

ICMP ND is used for address resolution. The invisible implicit permit ICMP ND entry is used to ensure that ND messages are permitted.

So what happens if you create an explicit deny entry for logging at the end of the ACL????
The explicit deny comes after 2 and before 3 in the list. Therefore, all ND messages will be denied.
The solution…. Create explicit ND permit entries.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

IPv6 ACL Configuration

Only 1 option which is like Named IPv4 Extended ACLs

```
R1#config terminal
R1(config)#ipv6 access-list ENARSI
R1(config-ipv6-acl)#deny ipv6 2001:db8:0:A::10/128 2001:db8:0:B::34/128
R1(config-ipv6-acl)#permit ipv6 2001:db8:0:A::/64 2001:db8:0:B::/64
R1(config-ipv6-acl)#deny tcp 2001:db8:0:A::/64 any eq 23
R1(config-ipv6-acl)#deny tcp 2001:db8:0:A::/64 any eq 80 time-range AFTERHOURS
R1(config-ipv6-acl)#deny tcp 2001:db8:0:A::/64 any eq 443 time-range AFTERHOURS
R1(config-ipv6-acl)#permit icmp any any nd-na
R1(config-ipv6-acl)#permit icmp any any nd-ns
R1(config-ipv6-acl)#deny ipv6 any any log
R1(config-ipv6-acl)#exit
R1(config)#int gig 0/0
R1(config-if)#ipv6 traffic-filter ENARSI ?
  in   inbound packets
  out  outbound packets
R1(config-if)#ipv6 traffic-filter ENARSI in
```

/128 means match the first 128 bits… which would be all which technically means this address exactly which means host.

/64 means match the first /64 bits and ignore the last /64 bits which would mean match all ipv6 hosts in this /64 network.

What if the prefix length was /80? This would mean match the first 80 bits and ignore the remining 48 bits.

Troubleshooting
So what are things to look out for here??????

- Action (permit vs deny)
- Protocol (is it the correct protocol)
- Source address
- Source operator and port
  - (Remember that port numbers can go on the source or the destination…. So understanding the flow of traffic is very important so that the port number goes in the correct spot.)
- Destination address

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Destination operator and port

(Remember that port numbers can go on the source or the destination…. So understanding the flow of traffic is very important so that the port number goes in the correct spot.)

Time-range

Correct interface

Correct direction

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

IPv6 ACL Verification

Verifying IPv6 ACL entries

```
R1#show ipv6 access-list
IPv6 access list ENARSI
    deny ipv6 host 2001:DB8:0:A::10 host 2001:DB8:0:B::34 sequence 10
    permit ipv6 2001:DB8:0:A::/64 2001:DB8:0:B::/64 sequence 20
    deny tcp 2001:DB8:0:A::/64 any eq telnet sequence 40
    deny tcp 2001:DB8:0:A::/64 any eq www time-range AFTERHOURS (active) sequence 50
    deny tcp 2001:DB8:0:A::/64 any eq 443 time-range AFTERHOURS (active) sequence 60
    permit icmp any any nd-na sequence 70
    permit icmp any any nd-ns sequence 80
    deny ipv6 any any log sequence 90
```

Notice how the /128 was replaced with host.

What is the prefix length was /80? This would mean match the first 80 bits and ignore the rest.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

IPv6 ACL Verification

Verifying IPv6 ACL applied to interface

```
R1#show ipv6 interface gigabitEthernet 0/0
GigabitEthernet0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::C801:2BFF:FE88:8
  No Virtual link-local address(es):
  No global unicast address is configured
  Joined group address(es):
    FF02::1
    FF02::1:FF88:8
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  Input features: Access List
  Inbound access list ENARSI
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds (using 30000)
  ND NS retransmit interval is 1000 milliseconds
```

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

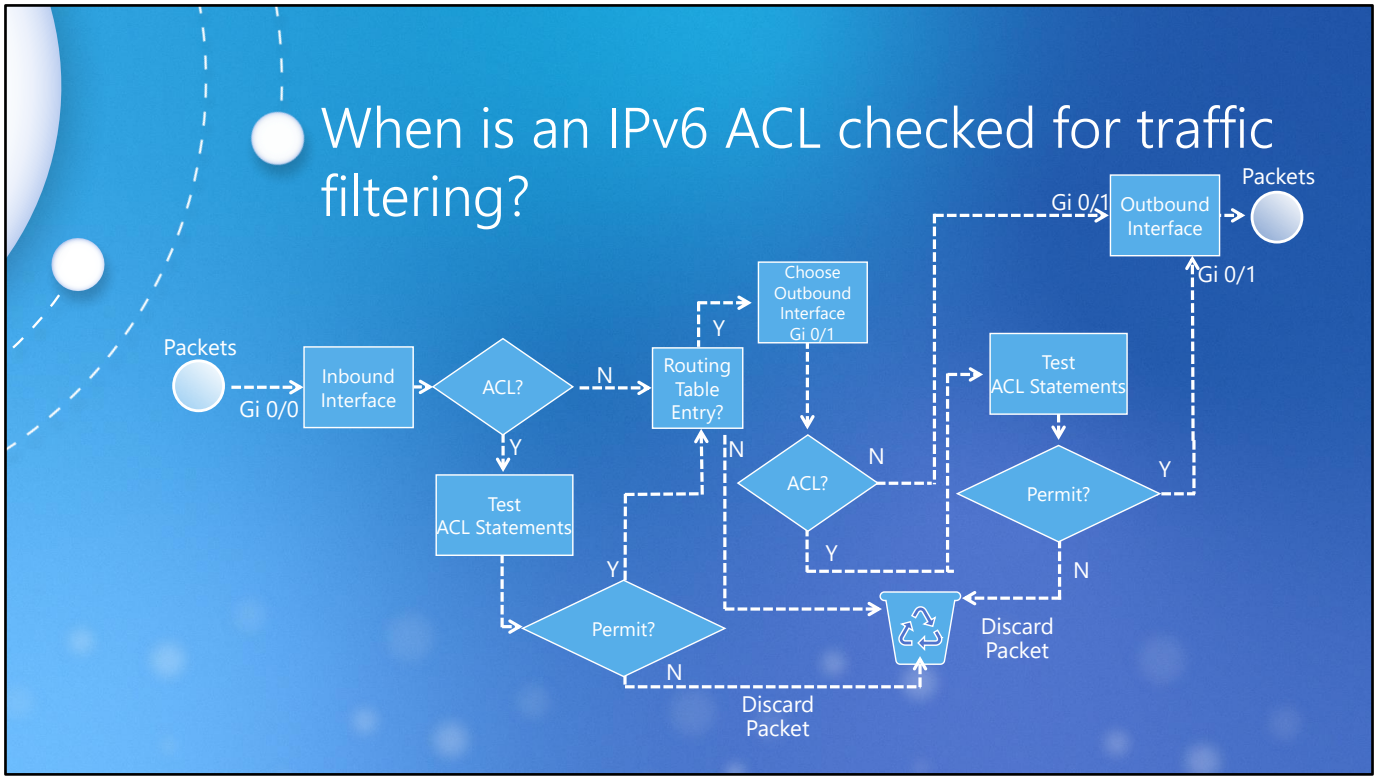
IPv6 ACL Verification

Identify all interfaces with a traffic filter applied

```
R1#show running-config | include interface|traffic-filter
interface Ethernet0/0
interface GigabitEthernet0/0
 ipv6 traffic-filter ENARSI in
interface GigabitEthernet1/0
interface GigabitEthernet2/0
interface GigabitEthernet3/0
```

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

When is an IPv6 ACL checked for traffic filtering?



©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

IPv6 ACL Troubleshooting Checklist

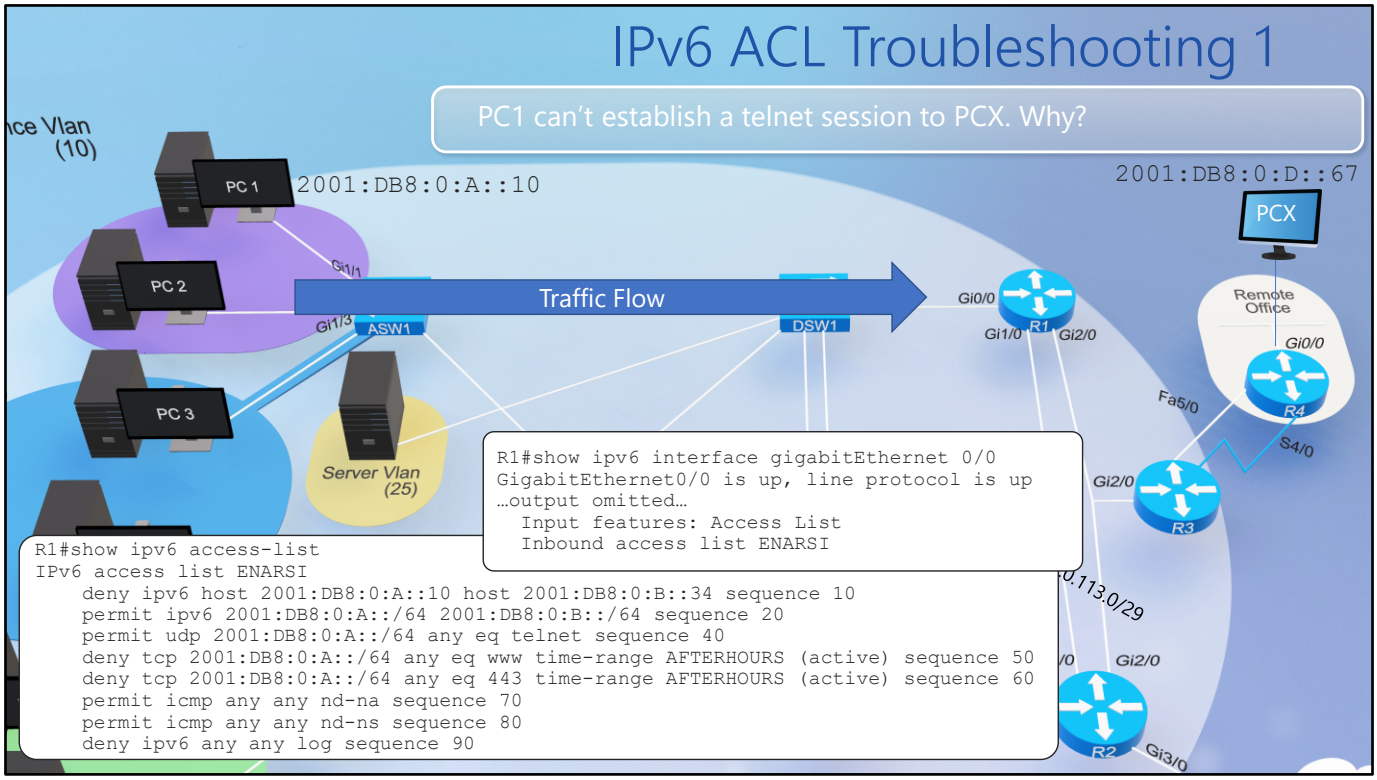
Is the ACL logic correct?

Is the ACL applied inline with the packet flow?

Is the ACL applied in the correct direction?

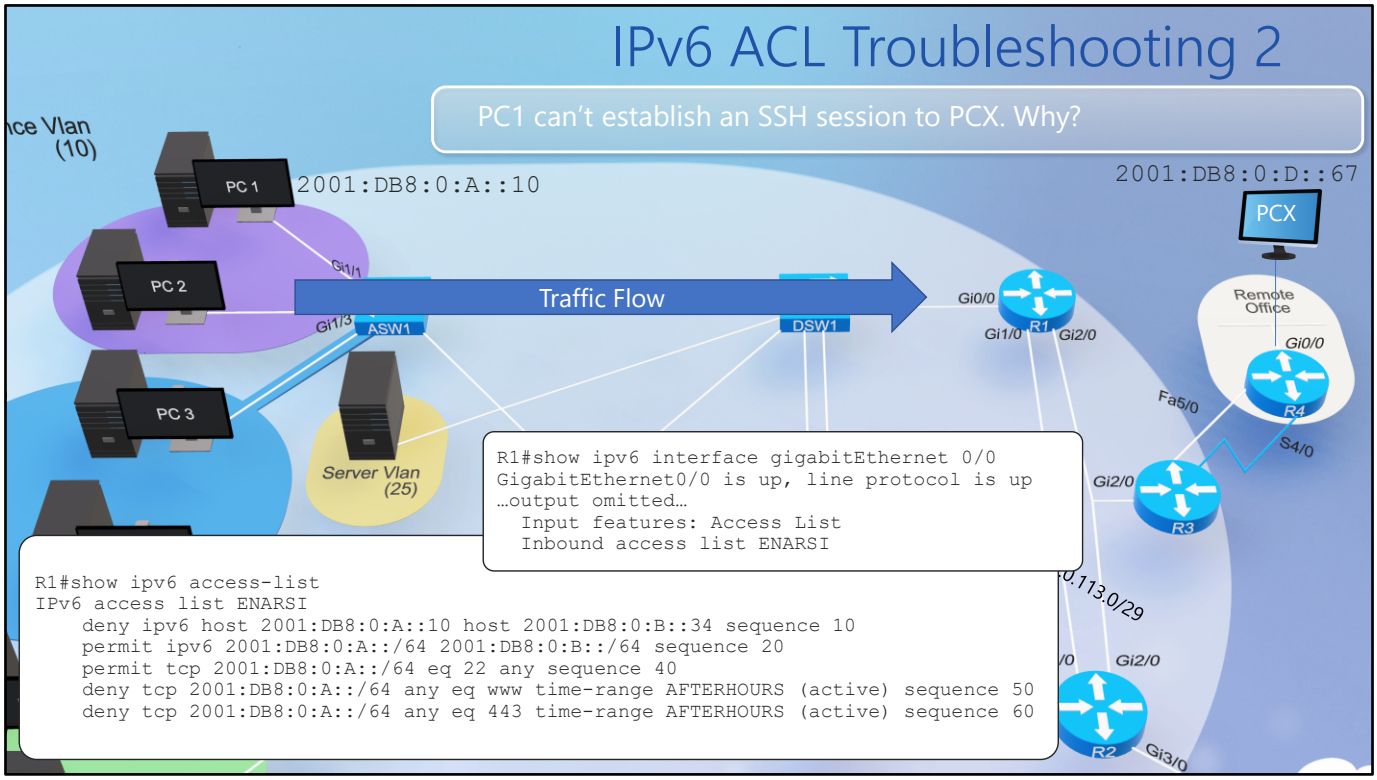
- Top down processing
- Immediate execution upon a match
- Implicit permit nd
- Implicit deny any

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



TELNET IS TCP NOT UDP.
Therefore sequence 90 is dropping the traffic.

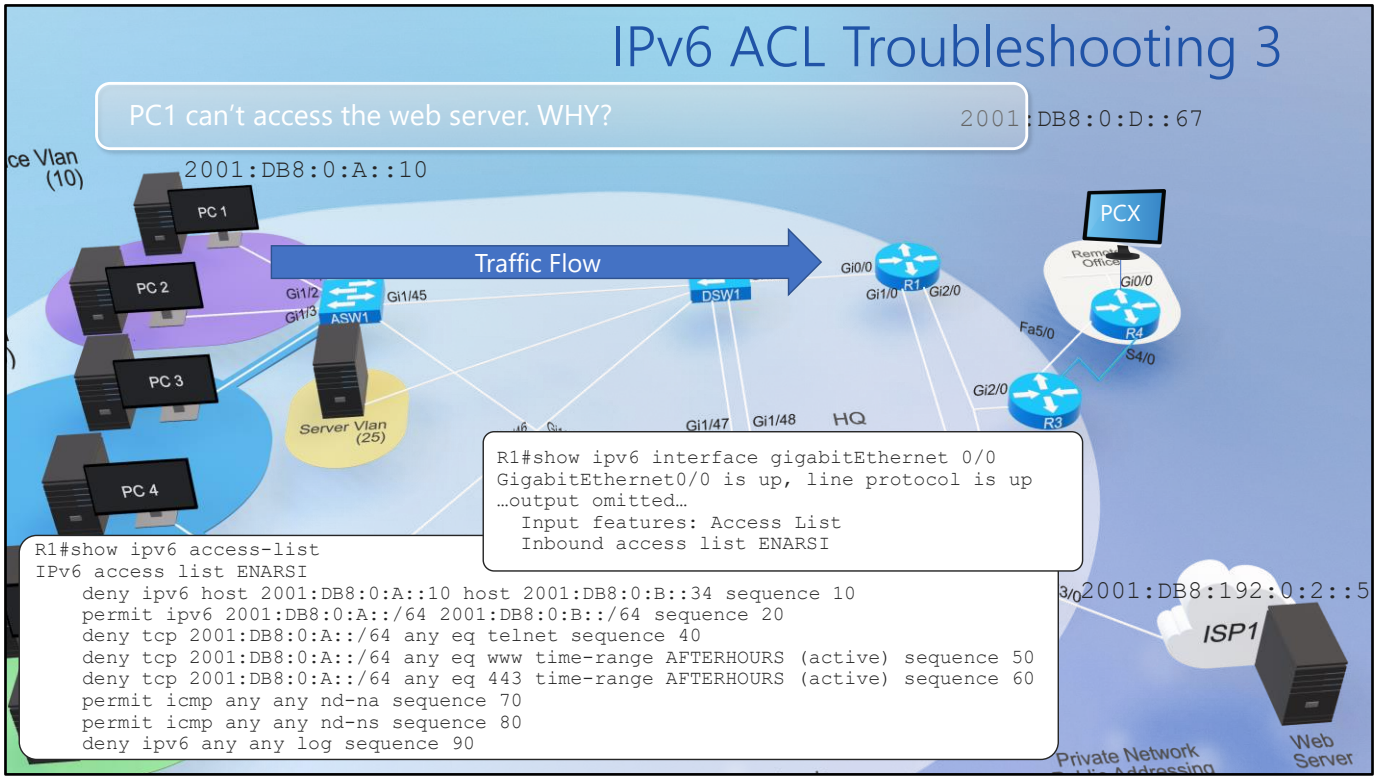
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Traffic is being denied by the implicit deny because no other sequence matches. But what account seq 40

The operator and port are in the wrong spot. The destination is port 22 not the source. That is why it is not working.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



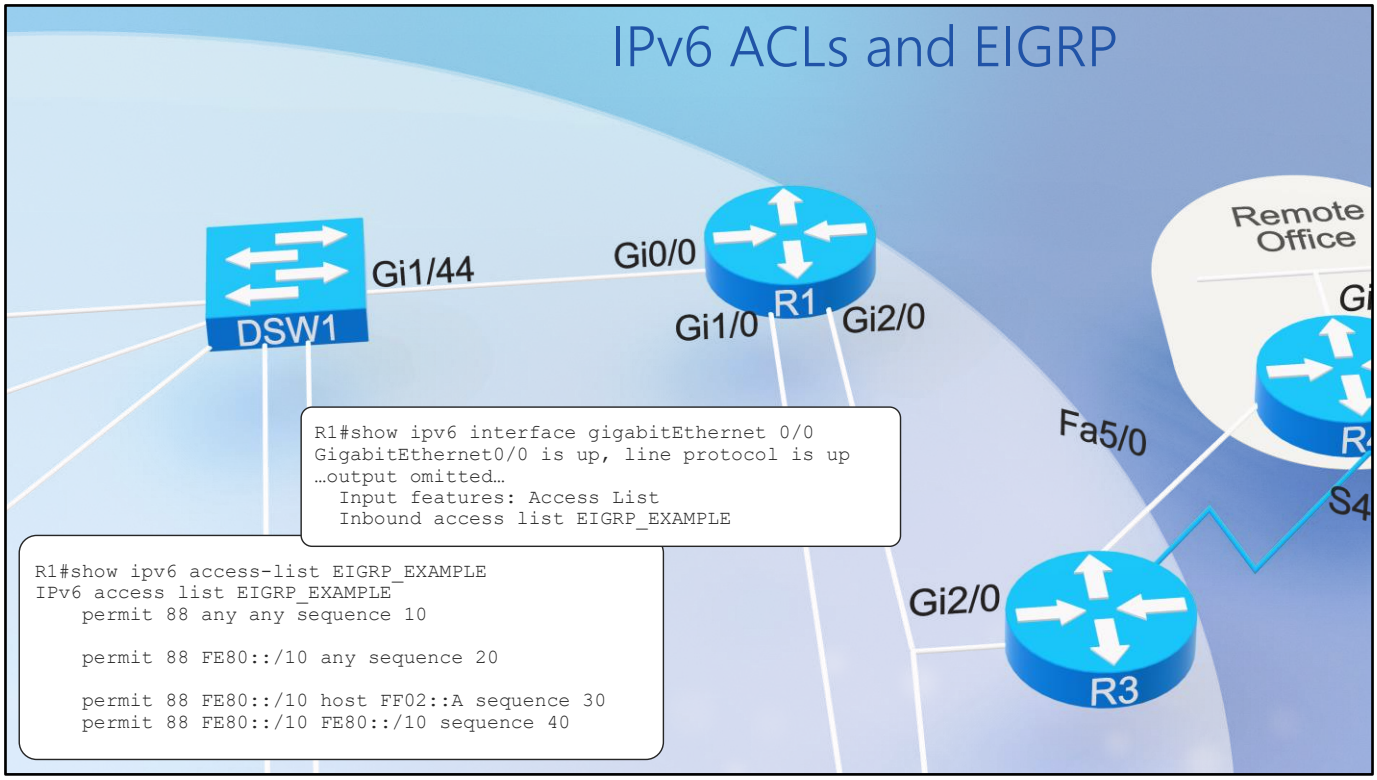
It is after hours because the time-range is listed as active.

If this is correct nothing needs to be done. If it is not correct, then you might have to adjust the time range or the clock on the device or remove it completely.

As we mentioned before:

> If you apply a time range that does not exist it is automatically created for you without any time parameters and will be active. Therefore, regardless of the entry being permit or deny, it is always active.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



FIRST…. Only inbound ACLs affect EIGRP packets, outbound ACLs do not.

EIGRP establishes a neighbor adjacency using multicast (unless you configure a unicast neighbor adjacency)

- Link local address as source
- FF02::A as the destination.

EIGRP exchanges update packets using unicast

- Link local address as source
- Link local address as destination

Options:
Permit 88 any any (this will take care of both the unicast and the multicast, but it is the least specific)

`permit 88 FE80::/10 any` (this will take care of both the unicast and the multicast as well and it is a little more specific)

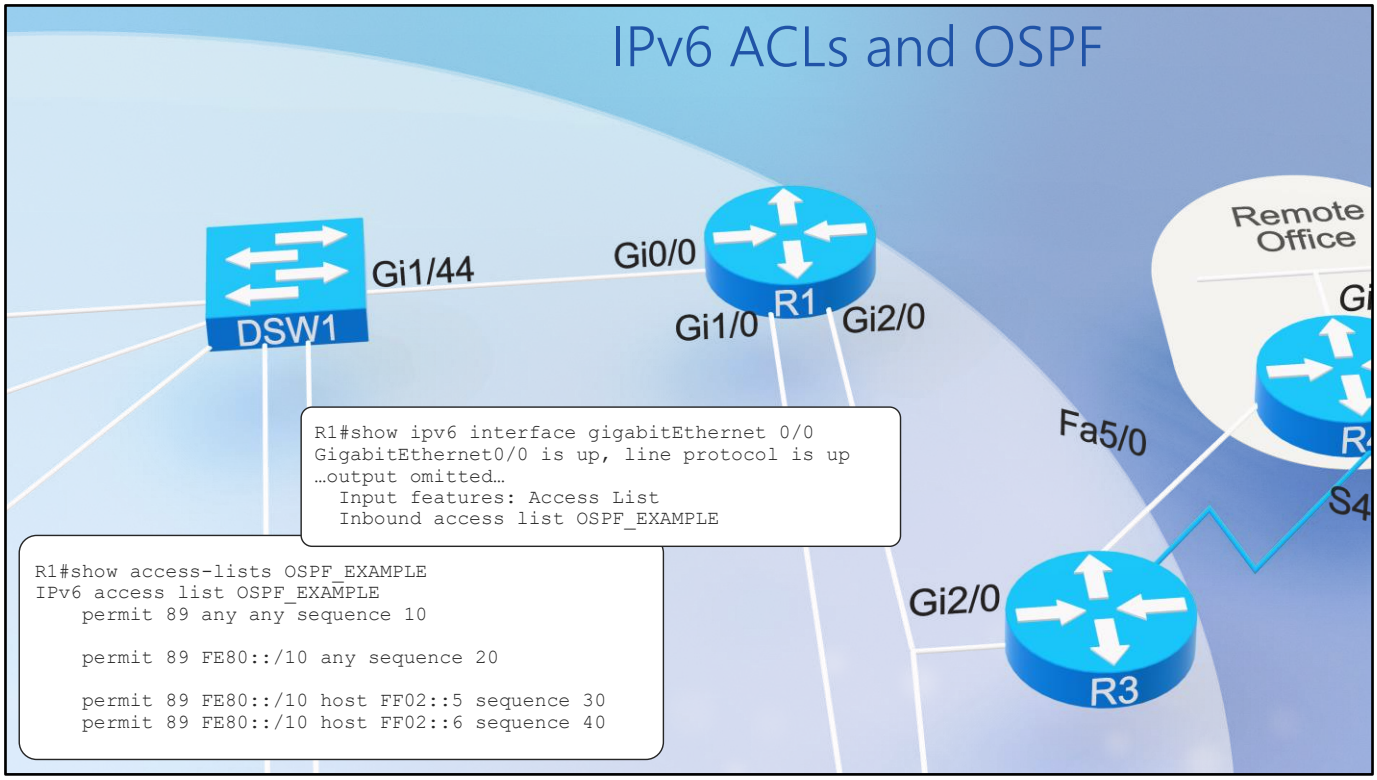
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

```
permit 88 FE80::/10 host FF02::A (this will take care of
the multicast)
permit 88 FE80::/10 FE80::/10 (this will take care of the
unicast)

To take it further you could specify the actual LL
address of the source and destination for the greatest
security.
```

You can usually recognize an ACL neighbor issue because one neighbor sees the other router but the other router does not see the neighbor. In this case if the ACL was not correct then DSW1 would see R1 as a neighbor in the neighbor table but R1 would not see DSW1 in its neighbor table.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



FIRST…. Only inbound ACLs affect OSPF packets, outbound ACLs do not.

OSPF establishes a neighbor adjacency and exchanges packets using multicast (unless you configure a unicast neighbor adjacency)

Link local address as source

FF02::5 as the destination (for hellos and to send info (updates) to all ospf routers) or FF02::6 as the destination for the DR.

Options:

`permit 89 any any (will take care of everything)`

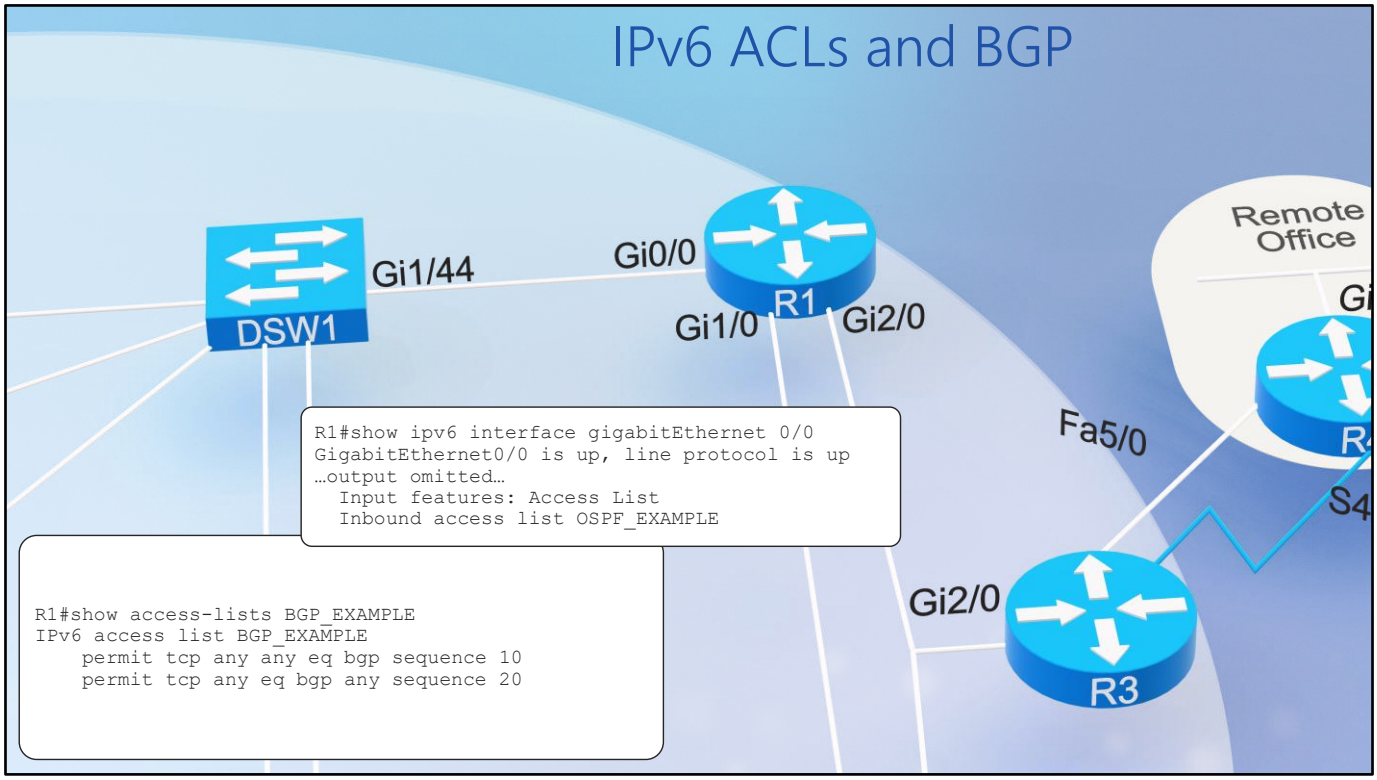
`permit 89 FE80::/10 any (will take care of everything and is more granular than the previous option)`

`permit 89 FE80::/10 host FF02::5 (this will take care of the` hellos and updates)
`permit 89 FE80::/10 host FF02::6 (this will take care of updates send to the DR) So in this case if R1 is the DR this would be required.`

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

You can usually recognize an ACL neighbor issue because one neighbor sees the other router but the other router does not see the neighbor. In this case if the ACL was not correct then DSW1 would see R1 as a neighbor in the neighbor table but R1 would not see DSW1 in its neighbor table.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



FIRST…. Only inbound ACLs affect BGP packets, outbound ACLs do not.

Ok… remember that BGP is a client/server peer-to-peer unicast neighbor relationship.

Both routers attempt to be the client and the server by default unless you force one or the other to be the client or the server.

So, in this case I am setting up the router to accept incoming requests to the server port… or incoming requests to the client port

```
permit tcp any any eq bgp (this entry is used if R1 is
the server. It allows the tcp packets destined to port
179 to be allowed in from any client using any port
number)
permit tcp any eq bgp any (this entry is used if R1 is
the client. It allows the tcp packets destined to the
random port number of R1[client] from the server using
TCP179 to be allowed in.

You can be more granular and specify the source and
```

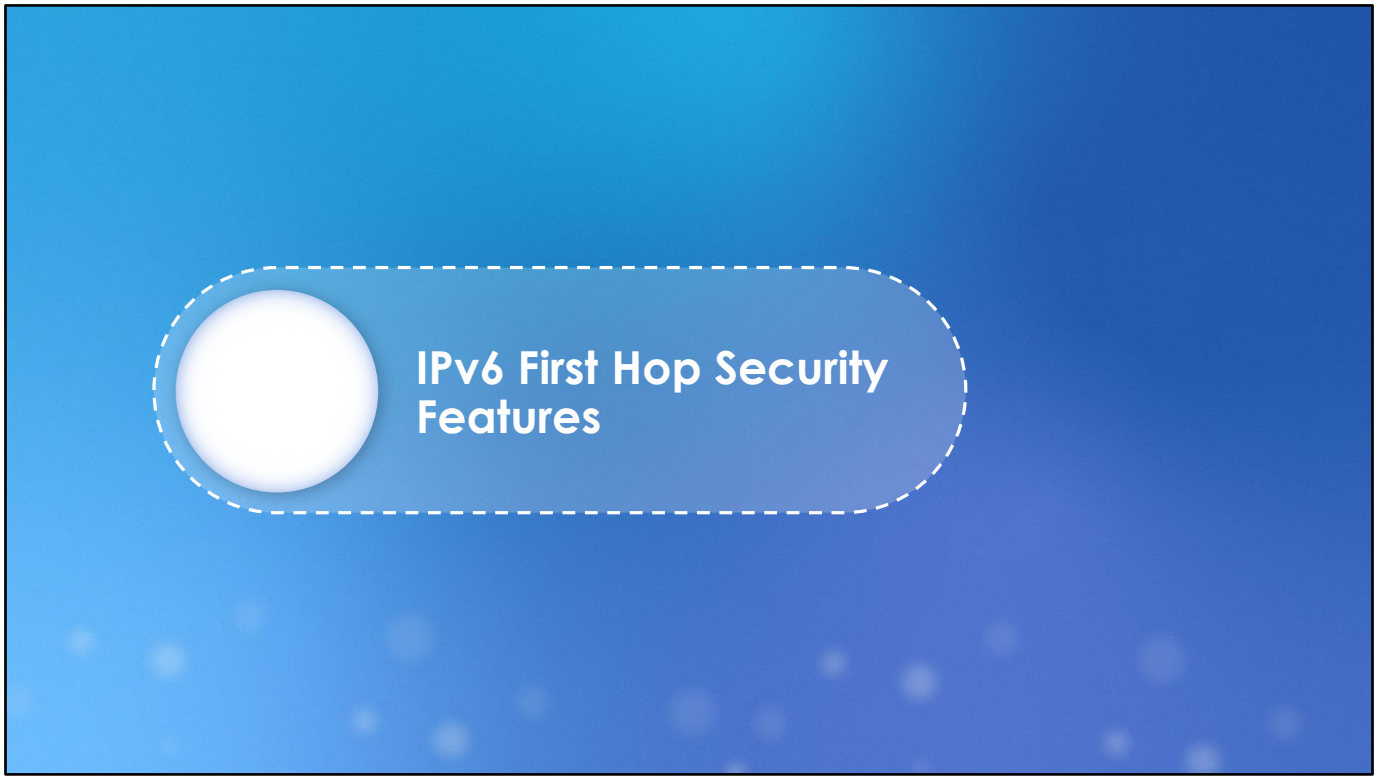
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

destination address of the BGP packets for added security.

Now, are both required. No. For example if you have set up the routers so that one is going to be the server (passive) and the other is going to be the client (active) then you can just set up a single ACL based on the traffic flow.

However, what you just set up one without forcing the routers to be a client/server (for example **permit tcp any any eq bgp**). Well in this case BGP packets destined to TCP 179 are allowed in which means R1 will become the server as BGP client packets are not allowed in. So, it would still work and forces one router to be the server and the other to be the client.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Title slide

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

IPv6 First Hop Security Features

- RA Guard
- DHCP Guard
- Binding Table
- ND inspection/snooping
- Source Guard
- Destination Guard

Use the following articles to teach this!!!

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_fhsec/configuration/xe-16/ip6f-xe-16-book.html

https://www.cisco.com/en/US/docs/ios-xml/ios/15-0se/features/ip6-snooping.html

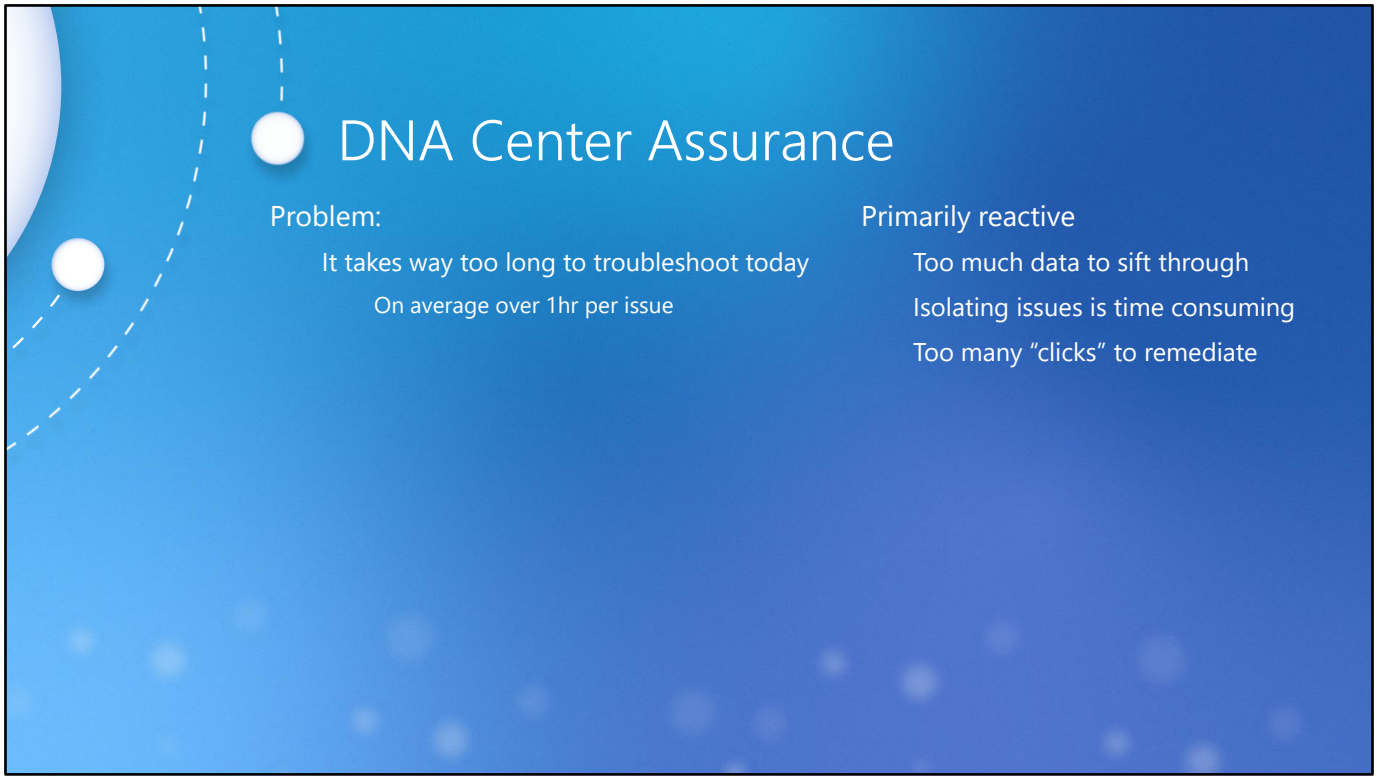
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



5.2 Configure and verify infrastructure security features
5.2.a ACLs

https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/digital-network-architecture/nb-06-dna-assurance-cte-en.html?oid=otren016866
https://www.cisco.com/c/m/en_us/solutions/enterprise-networks/intent-based-networking-guide/network-monitoring-assurance.html

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Why does it take on average over 1hr per issue?

Because it takes a long time to drill down to the actual reason behind the issue.

What is causing the problem?

For example – some users are indicating that it takes a long time to get on the wireless network.

This could be because of a multitude of issues.

Where do you begin?

We have the tools but it takes forever for us to find the information we are looking for.

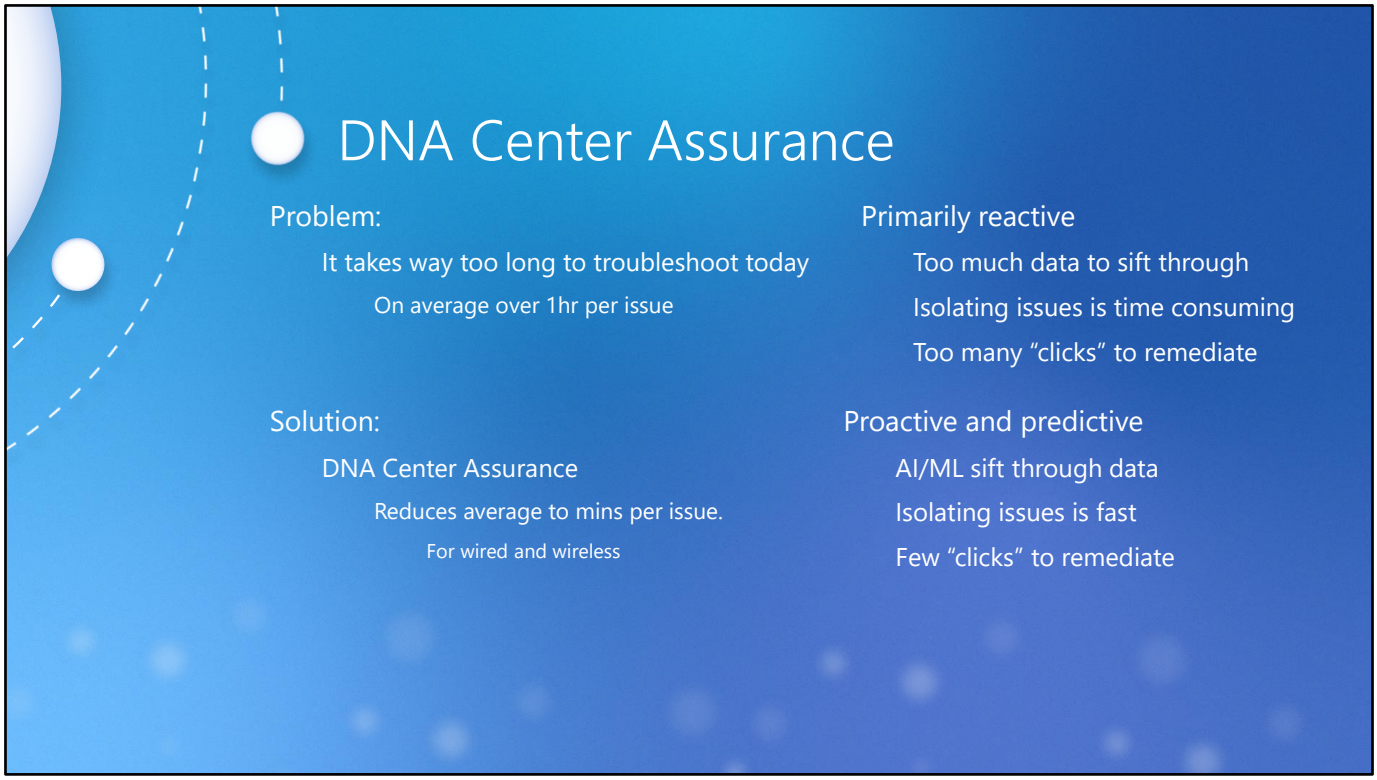
What might we do…

Run some pings / Run some traces to get an idea where things are breaking down

From there we might analyze some log files and so on.

All very time consuming

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



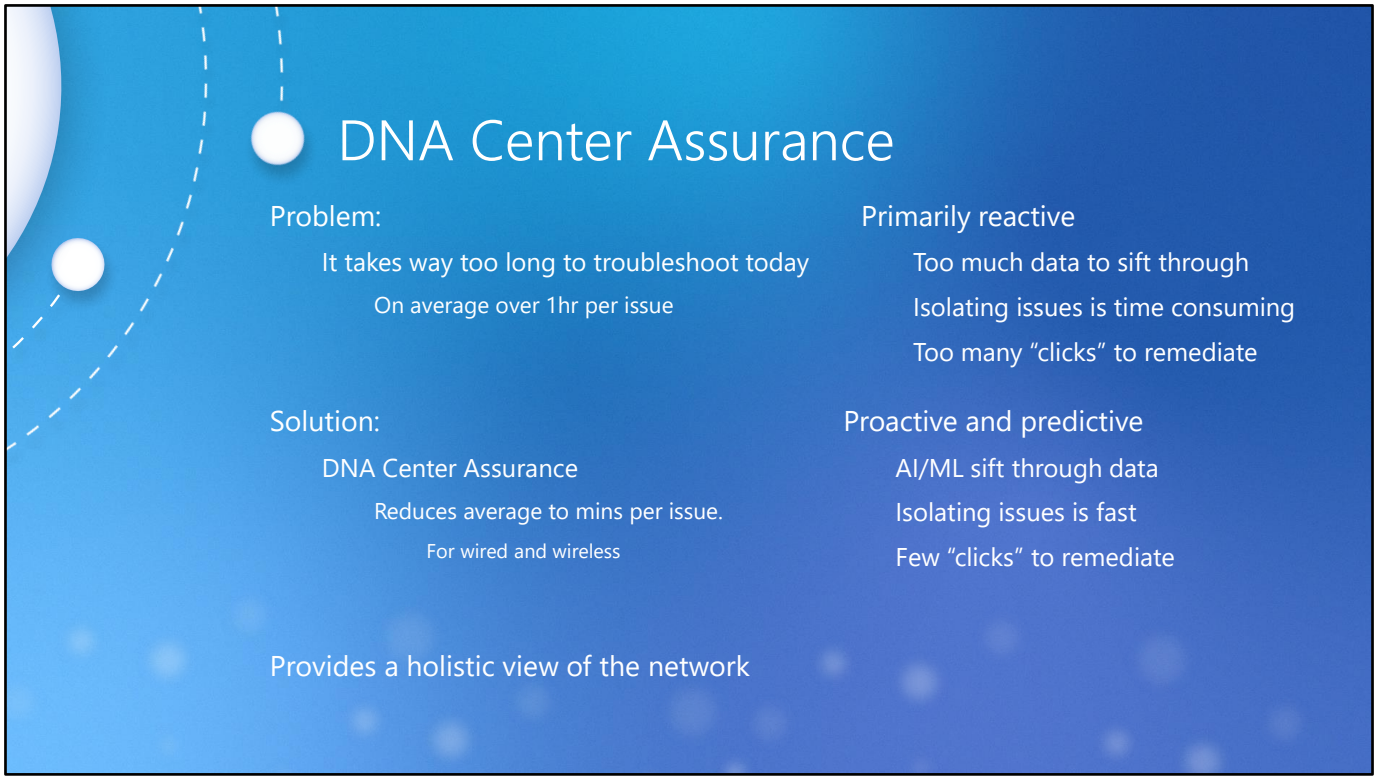
DNA Center Assurance

A feature built into Cisco DNA Center that reduces our troubleshooting efforts down to minutes for both wired and wireless networks.

How… by…

1) Every device becoming a sensor on the network
   Sending streaming telemetry (collection of measurements)
   About application performance and user connectivity in real time.
   so every client, network device, service, and application contributes to DNA Center Assurance
2) Artificial Intelligence (AI) and Machine Learning (ML)
   Analyze the information collected to provide
   Insights – to improve the network
   Notifications – about issues
   Suggestions – on how to remediate an issue
   Automation – remediate the issue without user involvement

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



With DNA Center Assurance you get a holistic view of the network. Therefore, baselines and thresholds can be determined based on real information and the real performance of the network and the devices on that network. Algorithms have the ability to determine what is good vs bad instead of humans just guessing and hoping.

So remember our users that were indicating it takes a long time to get on the wireless network… well DNA Center Assurance was quick to point out that during the "onboarding process"… (which for wireless is made up of the Association, AAA, and DHCP process, and for a dot1x enabled wired client the AAA and DHCP processes)… that DHCP was timing out. So, now that we know that… lets look into DHCP. Without DNA Center Assurance it would have taken us a long time to determine that DHCP was the actual issue here based on all the different variables we would have considered.

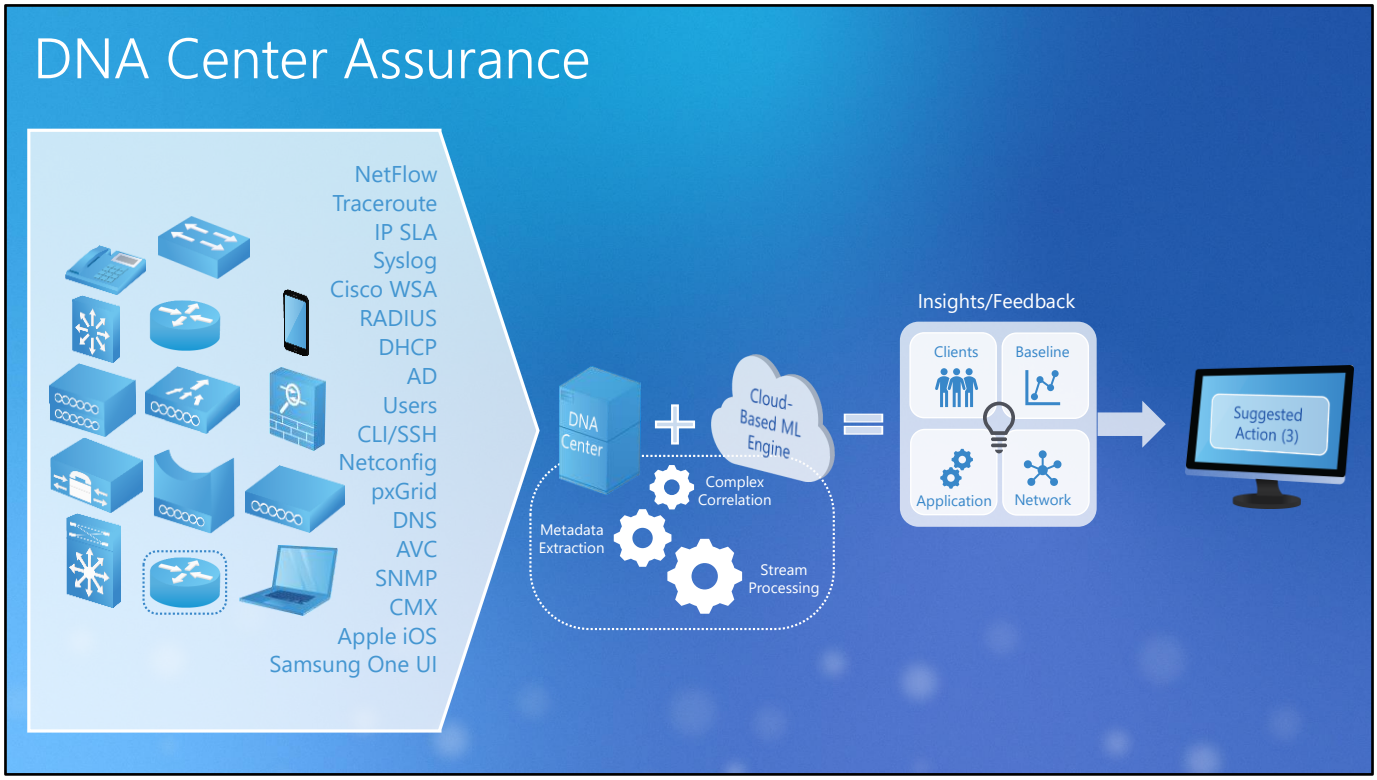
Take into consideration a user having issues with a video call…
you have to take into account
the nature of the application,
video codec parameters,
the states of the network (data rate, RF, etc.),

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

the current observed load on the network,
the destination being reached
Etc

You hrs…. DNA Center Assurance… mins.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Cisco DNA Center Assurance collects data (KPIs) from many different source types in real time, including NetFlow, traceroute, IP SLA, syslog, Cisco Web Security Appliance (WSA), RADIUS, Dynamic Host Configuration Protocol (DHCP), Active Directory and users, command-line interface and Secure Shell (CLI/SSH), netconfig, pxGrid, DNS, AVC, Simple Network Management Protocol (SNMP), Cisco Connected Mobile Experiences (CMX), Apple iOS, and Samsung One UI.

Cisco AI Network Analytics, uses a combination of local and cloud-based AI-driven analytics engines to make sense out of all this data and automate the process of issue resolution and performance enhancement. These analytics engines divides the event processing between critical metrics, which need instantaneous action, and noncritical metrics. Distributed on-device analytics located on select Cisco switches, routers, and wireless controllers handle critical decisions in real time and at the source of the incident. Cisco DNA Center's centralized analytics engine can collect and process the full set of data coming from all areas of the network. Cisco AI Network Analytics customizes your network baseline for alerts, reducing noise and false positives while enabling IT teams to very accurately identify issues, trends, anomalies, and root causes. It also allows comparative benchmarking between peers or sites to improve

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

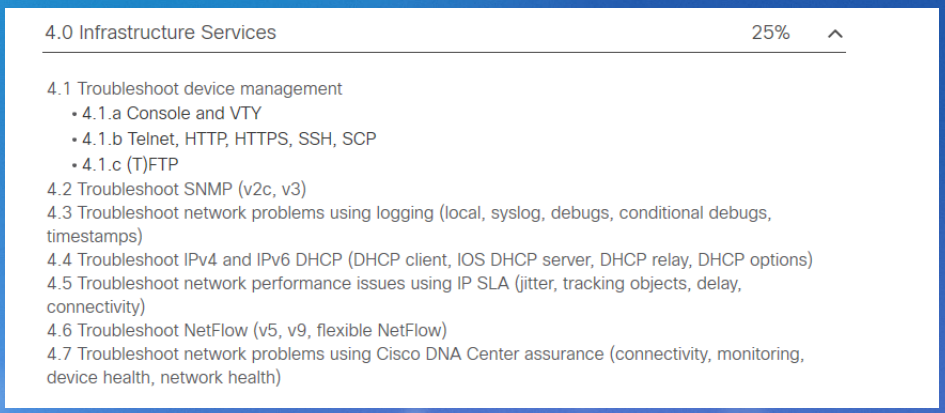
network performance consistency across branch offices and can identify network optimization opportunities and allocate IT resources efficiently. Cisco AI Network Analytics uses machine reasoning to automate logical remediation options for appropriate workflows and client issue resolution. It is fast, simple, and intuitive for greater IT efficiency. This results in an intuitive interface requiring little or no training of your IT team.

Insights and feedback are then provided for clients, applications, network devices, and baselines are established.

If any remediation is required, DNA Center will make suggestions when required.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Cisco DNA Center Assurance Exam Objectives



https://learningnetwork.cisco.com/s/enarsi-exam-topics

This exam objective and the exam are not aligned at all. ☹

SO…..

I am going to focus on exactly what we need… the information can be found in the user guides and installation guides for DNA Center in sections that are not related to DNA CENTER Assurance.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

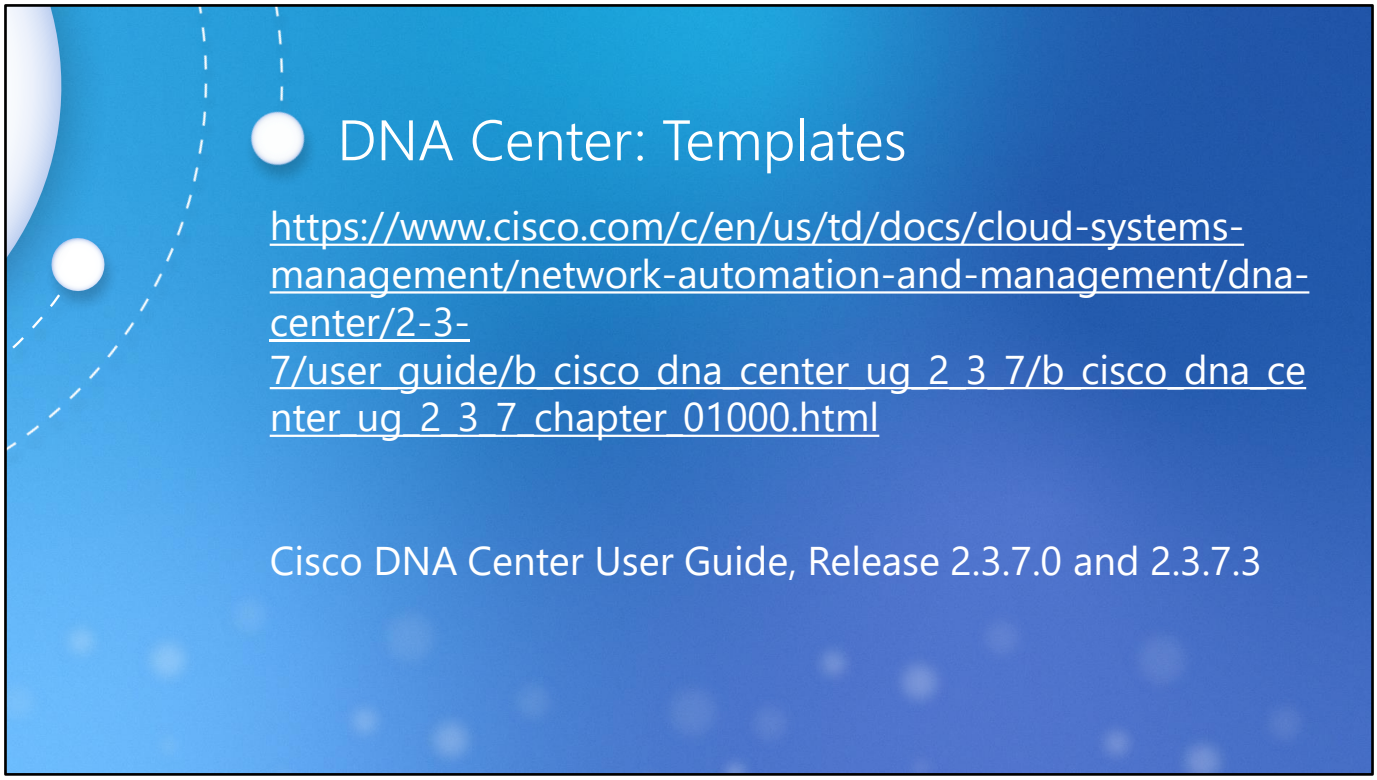
Cisco DNA Center Assurance Documentation

https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center-assurance/2-3-7/b_cisco_dna_assurance_2_3_7_ug/b_cisco_dna_assurance_2_3_6_ug_chapter_01.html

Cisco DNA Assurance User Guide, Release 2.3.7.0 and 2.3.7.3

This is the main page.

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



exam The TAG information and NOTE

Note

Tags are like keywords that help you locate your template more easily.

If you use tags to filter the templates, you must apply the same tags to the device to which you want to apply the templates. Otherwise, you get the following error during provisioning:Cannot select the device. Not compatible with template

https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-3-7/user_guide/b_cisco_dna_center_ug_2_3_7/b_cisco_dna_center_ug_2_3_7_chapter_01000.html

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

DNA Center: Manage Software Images

https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-3-7/user_guide/b_cisco_dna_center_ug_2_3_7/b_cisco_dna_center_ug_2_3_7_chapter_0100.html#id_77074

Cisco DNA Center User Guide, Release 2.3.7.0 and 2.3.7.3

exam Upload Software Images for Devices in Install Mode section

INSTALL MODE

Smu = software maintenance update

https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-3-7/user_guide/b_cisco_dna_center_ug_2_3_7/b_cisco_dna_center_ug_2_3_7_chapter_0100.html#id_77074

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

DNA Center: Troubleshoot the Deployment

https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-3-7/install_guide/2ndgen/b_cisco_dna_center_install_guide_2_3_7_2ndGen/m_troubleshoot_deployment_2_3_7_2ndgen.html

Cisco DNA Center Second-Generation Appliance Installation Guide, Release 2.3.7.0 and 2.3.7.3

exam Reconfigure the Appliance Using the Configuration Wizard Section

And

$ sudo maglev-config update

https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-1-2/install_guide/2ndGen/b_cisco_dna_center_install_guide_2_1_2_2ndGen/m_troubleshoot_deployment_2_1_2_2ndgen.html

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



This is the main page.

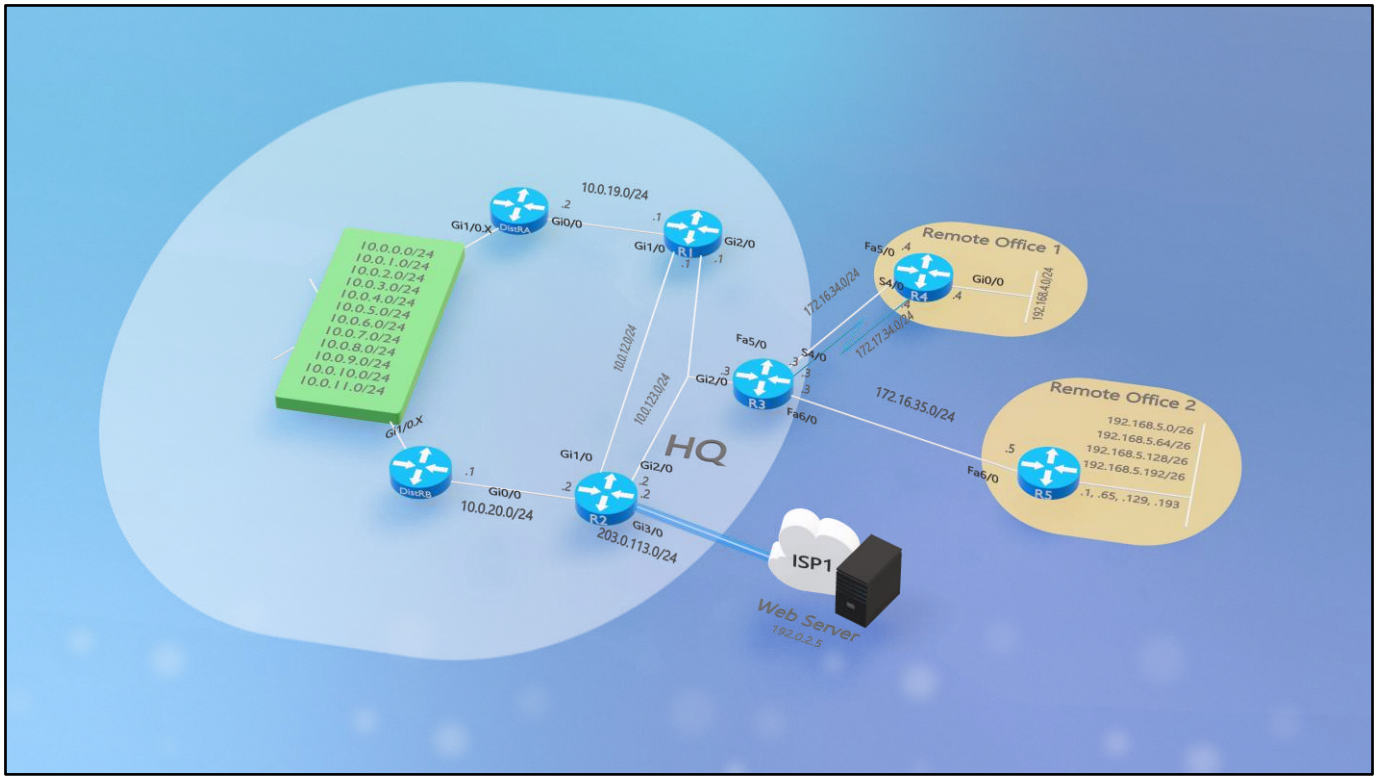
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



DEMO: Configure all interfaces except ISP interface for EIGRP.

Unicast between r3 and r5 as multicast is disabled on interfaces (ACL).

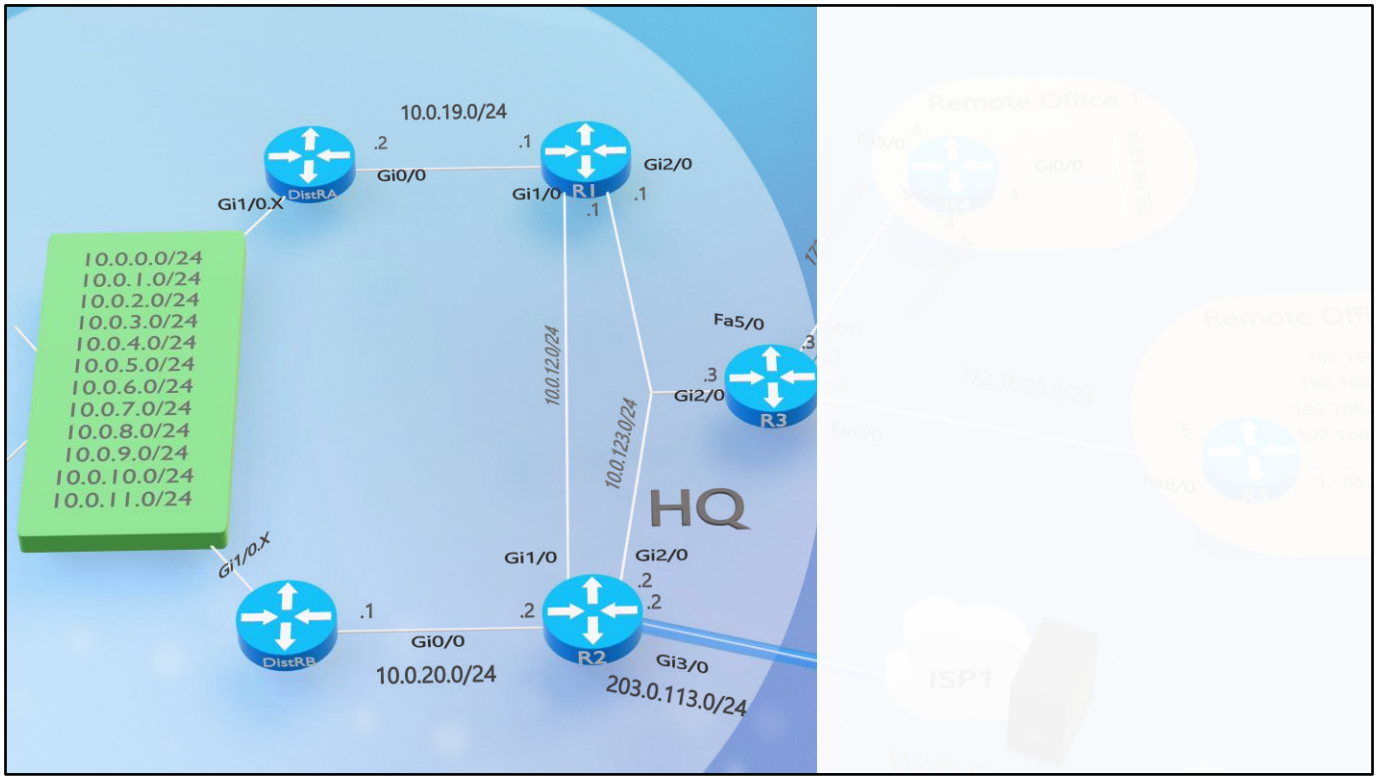
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



DEMO: Configure all interfaces except ISP interface for EIGRP.

Unicast between r3 and r5 as multicast is disabled on interfaces (ACL).

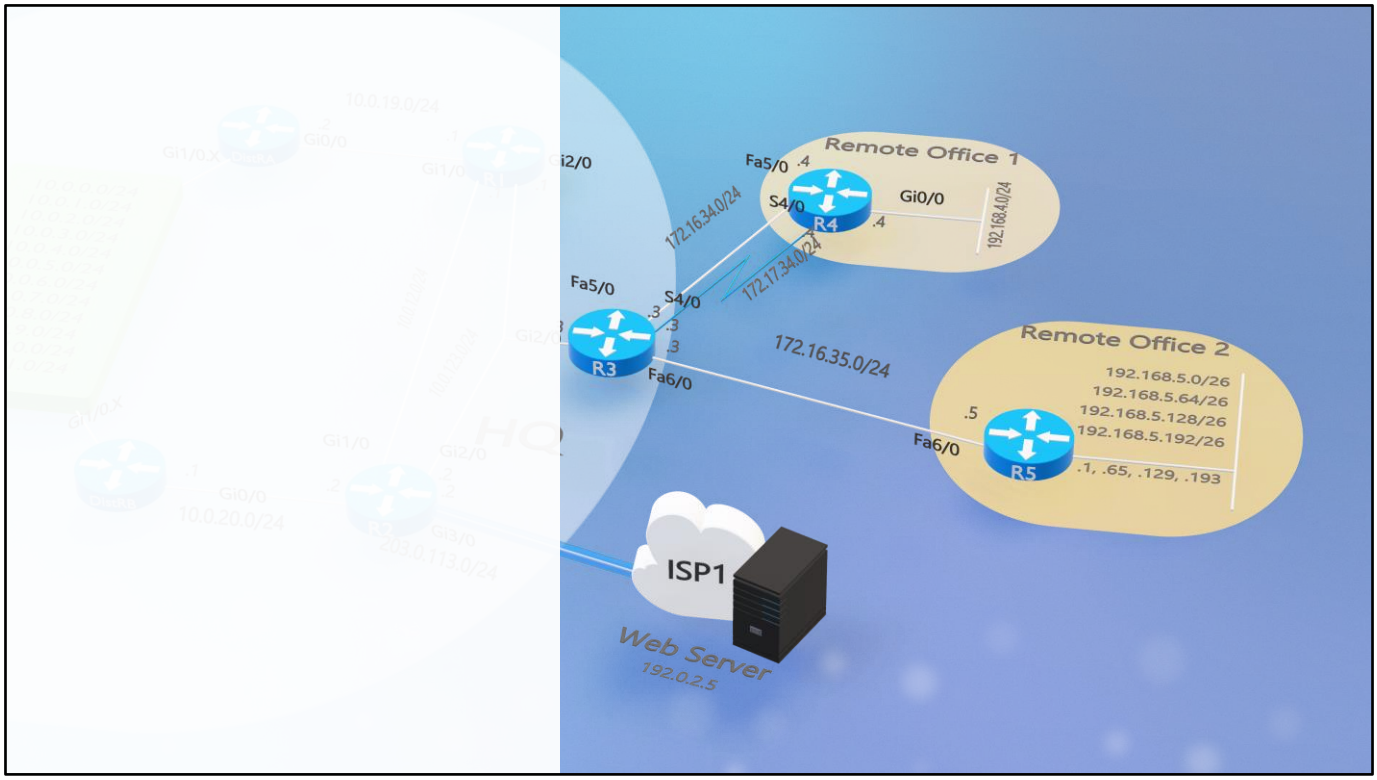
©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



DEMO: Configure all interfaces except ISP interface for EIGRP.

Unicast between r3 and r5 as multicast is disabled on interfaces (ACL).

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



DEMO: Configure all interfaces except ISP interface for EIGRP.

Unicast between r3 and r5 as multicast is disabled on interfaces (ACL).

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



DEMO: Configure all interfaces except ISP interface for EIGRP.

Unicast between r3 and r5 as multicast is disabled on interfaces (ACL).

©2024 by StormWind LLC. All rights reserved.
https://t.me/learningnets
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.